



www.trafmon.org

Use Case 3: Security Auditing

Thomas Grootaers, Luc Lechien

Software Release 1.0

2020-12

© 2020 AETHIS sa/nv Belgium Document version 1.0, 2020-12 All rights reserved -Open Source Apache License v2.0 trafMon Use Case 3: Security Auditing Page: 1/58



COPYRIGHT, LICENSE AND TRADEMARKS

Original text is © 2020 AETHIS sa/nv Belgium, Thomas Grootaers, Luc Lechien

This material is based upon work funded and supported by the European Space Agency and the Belgian Federal Authorities (BELSPO) under GSTP Contract Nr ESRIN 4000128964/19/I-EF with AETHIS sa/nv, Belgium.

The view, opinions, and/or findings contained in this material are those of the authors and subsequent free contributors and should not be construed as an official ESA, Government or AETHIS position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by ESA or AETHIS.

NO WARRANTY. THIS AETHIS MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. AETHIS MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. AETHIS DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT] This material is for approved for public release and unlimited distribution under the terms and conditions of Open Source Apache License v2.0 (<u>https://www.apache.org/licenses/LICENSE-2.0.txt</u>, OSI Approved <u>https://opensource.org/licenses/Apache-2.0</u>), which governs its use, distribution, modification and republication.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries.

AngularJS is a trademark of Google, Inc., https://angularjs.org/

CentOS Marks and JBoss are trademarks of Red Hat, Inc. ("Red Hat").

CERT is a registered trademark owned by Carnegie Mellon University

Eclipse and BIRT are registered trademarks of the Eclipse Foundation, Inc. in the United States, other countries, or both. JQuery and JQuery UI are trademark of OpenJS Foundation, https://openjsf.org/

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

MaxMind, GeoIP, GeoLite, and related trademarks are the trademarks of MaxMind, Inc.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

OpenSSL is a registered trademark of the OpenSSL Software Foundation in the U.S. and other countries.

Oracle, Java, MySQL, WebSphere and Solaris are registered trademarks of Oracle and/or its affiliates in the United States and other countries.

Python is a registered trademark of the Python Software Foundation.

Tomcat® and Apache HTTP Server™ are (registered) trademarks of the Apache Software Foundation.

UNIX is a registered trademark of The Open Group.

WebLogic is a registered trademark of IBM Corp. in the United States, other countries, or both

Wireshark is a registered trademark of the Wireshark Foundation.

All other trademarks are the property of their respective owners.



DOCUMENT HISTORY

Release	Date	Change
1.0	December 2020	First issue



ACKNOWLEDGEMENTS

The authors wish to acknowledge the valuable contributions of all ancient employees of the AETHIS® Company in Belgium, who have worked on the successive versions of the base software and its documentation from which the open source trafMon software is derived.

In particular, special recognition is given to Jacques Maes, David Orban, Jonathan Van den Schrieck, Benoît Liétaer, Julien Denis, Thomas Soupart, Fabien Coenegrachts, who have more specifically participated to its elaboration. Also, a thought is given in memory the authors' deceased associate, Luc Steenput, who has heavily promoted the initial idea and subsequent enhancements of the tool, within the European Space Agency and elsewhere.

Lastly, the authors wish to acknowledge the strong support of ESA staff members: Manfred Lugert, Erling Kristiansen, Johan Stjernevi, Manfred Bertelsmeier, Gioacchino Buscemi, Michele Iapaolo, Andrea Cogliandro and Claudia Neroni, as well as of officers of the Belgian BELSPO Federal Service, Jacques Nijskens, Agnès Grandjean and Hendrick Verbeelen.



TABLE OF CONTENT

1.	SECURITY AUDITING	6
2.	HOST SCANNING BY INTERNET SYSTEMS	7
2.1	LONG DURATION HIDDEN SCANS WITH VERY LOW TRAFFIC PROFILE	7
2.2	2 Exhaustive List of Scanners (and Others)	
2.3	3 SINGLE-DAY SCANS EXAMPLES	
2.4	4 Revealing Hidden Multi-Day Scans	
2.5	5 DISCOVERING BATTERIES OF SCANNERS	27
3.	ABNORMAL DAILY INGRESS VOLUME PEAK	
3.1	1 Per Own System Daily Ingress in Decreasing Order	
3.2	2 SECOND TO TOP DAILY PEAK MULTIPLIER	
4.	SECURITY SUMMARY	40
4.1	1 STORED PROCEDURES	40
5.	DRAWING A SAMPLE BIRT REPORT TEMPLATE	
5.1	1 BIRT DESIGNER SETUP	45
5.2	2 DATA SETS FROM STORED PROCEDURES	45
5.3	3 DRAWING THE STRUCTURE OF THE REPORT	
5.4	4 INSTALLING AND EXECUTING THE NEW REPORT	54



1. SECURITY AUDITING

In this example case of use, we illustrate through real-life examples the power of the trafMon tools in digging the traffic observations, trying to pinpoint security suspicious activity patterns. Not only do we give relevant example data queries with meaningful results, but we also highlight how the boundary between a normal peer communication and that of a security threat is thin.

Although we terminate the presentation by a practical drawing of a synthesis BIRT report template, a real security audit may not concentrate only on the most visible traffic abnormalities (most active scanners, widest scanning of own systems, day with highest increase of ingress traffic ...): the highest threat comes from those network exploits that make the less noise. Hence unacceptable peer activity does not necessarily show up in the Top-5 or even Top-20 figures. A complete security audit must involve second and third level of custom queries, applied to the entire set of first-detected long list of candidates.

This tutorial is also presented as the Use Case web page <u>https://www.trafmon.org/security-auditing/</u>. MySQL stored procedures have been written for the two first-level queries for low-profile traffic and for external ingress volumes, as well as for the associated summarising queries. Those last are the source 'data sets' for the example BIRT report. So, the tutorial is accompanied by an SQL file and a BIRT report template and published as a supplementary package downloadable from the <u>www.trafmon.org</u> web site.



2. HOST SCANNING BY INTERNET SYSTEMS

2.1 LONG DURATION HIDDEN SCANS WITH VERY LOW TRAFFIC PROFILE

When looking at the synthesis reports (Manager and Operator or Conversation reports) at the level of a single system, we observe that a great part of remote Internet peers is exchanging very low profile of traffic spread over a long time period.

Let's have a look at internet host x.x.42.100. Below is the amount of daily traffic with this remote external peer over one month, to and from the top 25 reached local hosts:



And the corresponding Conversation report shows that, despite its low volume, this external remote address reaches quite a lot of different "own systems", using different service ports.

Fortunately, when using FTP, it doesn't succeed of even try to login.

trafMn

An open source network traffic performance monitoring and diagnostics tool.





In details that gives:

			FTP Se	ssion Detail						F	ile Transf	ers Details			
1000						No Login Sessions		2						Commi	and Failures
100						No Cmd Sessions								File GB	ET Success
						No File Xfr Sessions		1-						File GB	BT Failures
10						File Xfr Sessions								File PU	JT Success
						Encrypted Sessions								File PU	JT Failures
							5							Directo	Jey List
•		13	42.100					• <u> </u>		1	42.100				
INGRES	S														
Host	Heat DNS	Protoco	Application	Peer Location	Peer Address	Peer DNS	Bit Rate	Bytes	IP Bytes	Protocol Overh	cad Percent Retransmit	Payload Bytes	Retransmitted Payland	Avg Last Wine	dow Avg Max Window
A&1585.42.100	vm- 2 chi3 southat Shift com	tcp	ftp	EXPORT	141.253.221.27	Signipf xi company con	3.13 b/s	10.26 KB	10.26 KB	95.73 %	93.71.96	1.08 KB	61 P	14,488	14,487.54
				IIKM	141.253.218.54	o.local.company.co	9.34 b/s	26.51 KB	26.51 KB	92.46 %	54.77 %	7.74 KB	486 B	14,387	14,386.713
					141.253.221.111	st. xi.company.com.	3.10 0.5	10.39 KB	10.39 KB	92.04 %		1.10 KB		14,405	14,405.284
					141.253.221.216	3.221.26	3.07 b/s	10.30 KB	10.30 KB	95.62 %		1.12 KB		14,405	14,405.284
					141.253.221.31 141.253.221.7	満式など).xi.company.com.	8.01 b/s 7.63 b/s	26.45 KB 24.96 KB	26.45 KB 24.96 KB	90.90 %	29.78 %	6.20 KB 7.36 KB		13,986 14,155	14,235.859 14,404.319
					141.253.221.95	xi company.com.	3.10 b/s	10.22 KB	10.22 KB	95.65 %		1.10 KB		14,237	14,486.575
				MGT	141.253.221.106	See company.com.	9.42 b/s	31.52 KB	31.52 KB	98.14 %	77.43 %	4.87 KB		14,656	14,656
				SALES	141.253.221.173	oce ref-	10.02 b/s	32.92 KB	32.92 KB	98.17 %	77.37 %	4.96 KB		14,656	14,656
				User_Services	141.253.221.91	Company com	3.90 b/s	13.04 KB	13.04 KB	86.27 %		3.81 KB		13,735	13,735.394
			http	ADMINISTRA	I <u>141.253.221.134</u>	An administration	0.73 b/s	132 B	132 B						32,767.5
					141.253.221.145	Sign administration	0.67 b/s	40 B	40 B					32,768	32,767.5
				FINANCE	141.253.221.105	w.xi.company.com.	0.73 b/s	44 B	44 B						32,767.5
				IIDA	141.253.221.105	ompany.com.	0.75 0.5	44.7	44.7						22,101.5
				HKM	141.253.218.40	signal local company.com	0.73 b/s	132 B	132 B						32,767.5
					141.253.218.52	dishare local comp	0.73 b/s	88 B	SS B					22.769	32,767.5
					141.253.218.57	second an in local compa	0.73 b/s	132 B	132 B					32,100	32,767.5
					141.253.221.100 141.253.221.110	Second and a second a second and a second a sec	0.73 b/s 0.73 b/s	44 B 44 B	44 B						32,767.5
					141.253.221.116	ay xi company.com	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.12	Aref. ref-	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.135	zes ale2 xi.company.com	0.73 b/s	132 B	88 B						21,845
					141.253.221.16 141.253.221.204	Set Company.com.	0.73 b/s 0.73 b/s	44 B 44 B	44 B 44 B						32,767.5
					141.253.221.23	xi.company.com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.29	company.com.	0.73 b/s	132 B	132 B						32,767.5
					141.253.221.31	Sat Art Company com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.7	23 Chicompany.com.	0.73 b/s	44 B	44 B						32,767.5
				and the second second	141.253.221.89	strong xi company.com.	0.73 b/s	88 B	88 B						32,767.5
				LOGISTICS	141.253.218.27	designed to the second	0.73 b/s	44 B	44 B						32,767.5
					141.253.218.33 141.253.218.42	of warer2.local.company.	0.73 b/s	44 B 88 B	88 B						32 767 5
				MGT	141.253.221.215	Construis-	0.73 b/s	44 B	44 B						32,767.5
				SALES	141.253.221.109	sibe ops-	0.73 b/s	132 B	132 B						32,767.5
						i.company.com.									



Peri	Hard DNR	D	I line to the	Dans I a	Pers Add	Prov DNR	Pie De-	Pete	15.5	Protocol Occ. 1. 1.2	P	Batas	Aug I - MP - I	too Manuary -																		
Host	Host DNS	Protoco	Application	Peer Location	Peer Address	Peer DNS	Bit Rate	Extea	IP Bytes	Protocol Overhead Percent Retransmi	Payload Bytes	Retransmitted Payload	Avg Last Winds	aw Avg Max Window																		
\$ 35.42.100	Vm-	tcp	ftp	EXPORT	141.253.221.27	A si i company con	4.47 b/s	14.96 KB	14.96 KB	95.73 %			209,096	7,210.207																		
	2.Cu131W/040929:0001.			HKM	141.253.218.49	is selected al company.c	9.10 0.5	25.68 KB	25.68 KB	98.40 %			055,057	24,187.278																		
					141.253.210.54	Action State Company.co	441 h/s	14 70 KB	14 70 KB	95.64 %			211 528	7 204 060																		
						west and mpany.com																										
					141.253.221.210	de for unit oany.com.	4.44 b/s	14.79 KB	14.79 KB	95.54 %			421,288	14,527.172																		
					141.253.221.26	1.26	4.47 b/s	14.90 KB	14.90 KB	95.62 %			416,445	14,360.184																		
					141.253.221.31	a service ompany.com.	0./903 627.b/s	22.02 KB	22.02 KB	90.90 %			205,477	2,085,397																		
					141.255.221.7	A Anthennany.com.	0.2705	20.03 MD	20.05 MD	91.35 %			05,050	2,091.300																		
					141.253.221.95	.company.com	4.47 b/s	15.01 KB	15.01 KB	95.65 %			409,205	14,110.529																		
				MGT	141.253.221.100	198	8.34 b/s	27.79 KB	27.79 KB	98.14 %			211,556	7,295.034																		
				CALES	141 262 221 172	S. Wany.com.	0.56 h/s	20 40 20	20 40 VD	09179			211 594	2.106																		
				SALLO	141.100.111.110	apany.com.	0.2002	10.40 110	10.70110	20.11 10				1,220																		
				User_Services	141.253.221.91	\$17.84°	4.47 b/s	14.72 KB	14.72 KB	86.27 %			416,397	14,358.529																		
			1.00	ADD CONTENTE AT	1 41 929 991 19	is for spany.com.	1.75	240.7	240.0				0.040	0.000																		
			nub	ADMINISTRA	141.253.221.134	State Aministration	1.33 03	240.5	240 B				8,/00	2,920																		
					141.253.221.145	408.	0.67 b/s	40 B	40 B																							
					a hard here a	de se aministration o																										
				EXPORT	141.253.221.35	in Asia y is xi company.c	0.67 b/s	120 B					2.202	2.200																		
				FINANCE	141.253.221.105	www.company.com.	1.33 0 S	80 B	80 B				7,300	7,300																		
					141.100.221.100	a santany.com.	1.35 0 5	90 D	30.7				1,000	1,000																		
				HRM	141.253.218.46	company.com	1.33 b/s	80 B	80 B				2,920	2,920																		
					141.253.218.49	cal company c	1.33 b/s	240 B	240 B				21,900	7,300																		
					141.253.218.52	and the second company	1.33 b/s	160 B	160 B				14,600	7,300																		
					141 253 218 57	strain local company.	133 hs	240 B	240 B				8 760	2 920																		
					141.253.218.58	Alsen w company com	0.67 b/s	80 B	1.02				0,100																			
					141.253.218.61	wiss and company.com	0.67 b/s	40 B																								
					141.253.221.100	in the second second	0.67 b/s	40 B																								
					141.253.221.110	State of the same and same	1.33 b/s	80 B	80 B				7,300	7,300																		
					141.253.221.111	ACT	0.67 b's	40 B																								
						a mpany.com.																										
					141.253.221.110	pany.com.	1.33 b/s	80 B	SO B				14,600	14,600																		
					141.253.221.12	A share com	1.33 0/5	80 B	80 B				14,600	14,600																		
											141.253.221.121	Sales	0.67 b/s	40 B																		
																							and the second second	a sweet sompany.com.								
																												141.253.221.135	Company.com	1.11 b/s	200 B	160 B
					141.253.221.130	A company con	122 h/s	120 B	20 P				14,600	14.600																		
					141.253.221.204	States.	1.33 b/s	80 B	SO B				2.920	2.920																		
					1. 1. A. 1.	AAN M Dany com																										
					141.253.221.210	is sections.	0.67 b/s	40 B																								
					141.253.221.21	Agented F.	0.07 0.5	40 B																								
					141.253.221.219	1.219	0.67 b/s	40 B																								
					141.253.221.226	CONTRACT.	0.67 b/s	80 B																								
					1 (1 152 221 22	so an a soany com.	1 22 5 -	20.7	20.7				2.020	2.020																		
					141 253 221 23	information 1 234	0.67 h/s	120 B	50 B				2,920	2,920																		
					141.253.221.26	1.26	0.67 b/s	80 B																								
					141.253.221.29	sal systemany.com.	1.33 b/s	240 B	240 B				21,900	7,300																		
					141.253.221.31	des a Simpany.com.	1.33 b/s	80 B	80 B				7,300	7,300																		
					141.253.221.37	Sola to industry com	1.33.6%	80 B	80 B				7,300	7,300																		
					141.253.221.7	Are .	1.33 b/s	80 B	80 B				2,920	2,920																		
						water smpany.com.			100000																							
					141.253.221.89	xi.company.co	1.33 b/s	160 B	160 B				5,840	2,920																		
					141.253.221.93	Sector Comment	0.07 6/5	40 B																								
					141.253.221.94	a state asfer-	0.67 b/s	40 B																								
						Sompany.com.	0.000																									
				1.00107107	141.253.221.95	Sale Company.com	0.67 b/s	40 B																								
				LOGISTICS	141.253.218.10	al company of	0.07 5/5	80 B																								
					141.253.218.16	Martin State	0.67 b/s	120 B																								
						al.company.co	8																									
					141.253.218.20	Log Strat	0.67 b/s	40 B																								
					141 253 218 21	Solution of the second	0.67 hs	40 B																								
						al.company.co																										
					141.253.218.22	Charles 19-	0.67 b/s	40 B																								
					141 361 318 33	al.company.co	122 6.4	20 D																								
					141.253.218.23	NO2 (37.97/07-	1.33 0.5	20 B																								



2.2 EXHAUSTIVE LIST OF SCANNERS (AND OTHERS)

A more systematic search for remote external scanners starts with the creation of a table with all pairs of one external system (non-private IP address, without Activity nor Location qualifier) and one own system (with designated Activity and/or Location), summing-up the number of packets and of bytes exchanged each individual day.

This *lowTraffic* table is ordered, first, by ascending external IP address (using INET_ATON(remote)) then, second, by ascending "own" address (using INET_ATON(local)), then only by service port and day.

The sql query looks like:



In the above SQL statement, low traffic is already at a high limit (30 packets and 3000 bytes a day).

The reason for this is to produce (or regularly recreate at night) a persistent table encompassing, among other, all interesting patterns for further inspection. This has been implemented as a stored procedure, in the downloadable add-on *trafMon_SecurityExample* package:

`trafMon_SecurityProcs`.`Refresh_lowTraffic`(IN `_DBname` VARCHAR(20))

At the time of manual analysis, it is then quicker to extract from this prepared *lowTraffic* table those lines matching a more reduced volume of exchanges (e.g. 10 or 20 packets a day for a total of 1000 or 2000 bytes).

From this result, ANY suspicious scanning patterns deserves further manual examination. It is a rather tedious process, but it allows to avoid black-listing true clients that otherwise conduct more



normal (and necessary) protocol communications, but being exhaustive in identifying the undesired spies.

Here are some relevant practical examples extracted and anonymised, from real trafMon observations.



2.3 SINGLE-DAY SCANS EXAMPLES

By browsing through (excerpts of) the lowTraffic table, we easily identify when, in a same day, a same remote IP address appears in consecutive lines whose local address field consecutive values form a nearly complete sequence of our own address's ranges.

at remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-26	141.253.221.102	65535	8	1171	United States	Redmond	135 3 14.50	AS8068 Microsoft Corporation
2017-07-07	141.253.221.102	65535	8	1723	United States	Redmond	5 (TAY 5 80	AS8068 Microsoft Corporation
2017-07-28 25 45 5.80	141.253.221.102	65535	8	1895	United States	Redmond	<u>10</u> 00€9.5.80	AS8068 Microsoft Corporation
2017-08-05	2 141.253.221.102	05535	8	344	United States	Redmond	· · · · · · · · · · · · · · · · · · ·	AS8068 Microsoft Corporation
2017-08-05 6.16	3 141.253.221.102	65535	7	300	United States	Redmond	o 6 163	AS8068 Microsoft Corporation
2017-08-05	00 141.253.221.102	65535	12	524	United States	Redmond	Apr 6 21.200	AS8068 Microsoft Corporation
2017-08-30	0 141.253.221.102	65535	13	1753	United States	Redmond	High 42.10	AS8068 Microsoft Corporation
2017-08-05 42.1	1 141.253.221.102	65535	8	344	United States	Redmond	21 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	AS8068 Microsoft Corporation
2017-07-07	4 141.253.218.10	21	3	152	Republic of Korea	Incheon	with the second s	OTHER
2017-07-30 3:126.85.0	141.253.218.33	80	14	1103	United States	Seattle	Star And And And Star School School amazonaws.com	OTHER
2017-07-29 2 126.85.0	141.253.221.93	80	1	40	United States	Seattle	sector anazonaws.com.	OTHER
2017-08-02	141.253.221.218	80	1	40	United States	Seattle	An Antonio State State Concerning an azonaws.com	OTHER
2017-08-05 3 126.85.0	141.253.221.219	80	6	264	United States	Seattle	Sec. 25 Sec. 20 Market Sompute amazonaws.com.	OTHER
2017-08-01 126.85.0	141.253.221.234	80	1	40	United States	Seattle	Compute amazonaws.com	OTHER
2017-07-26 36 126.141	36 141.253.218.11	443	4	168	United States	Seattle	A state of the sta	OTHER
2017-07-26 126.141	36 141.253.218.12	443	3	124	United States	Seattle	$\sqrt{(x_1^2)^2}\sqrt{(x_2^2)^2}\sqrt{(x_2^2)^2}\sqrt{(x_2^2)^2}$ 1.compute.amazonaws.com	OTHER
2017-07-26 2126.141	36 141.253.218.22	443	3	124	United States	Seattle	i i de la compute amazonaws.com	OTHER
2017-07-26	36 141.253.218.23	443	3	124	United States	Seattle	anazonaws.com	OTHER
2017-07-26 2126.141	36 141.253.218.24	443	6	248	United States	Seattle	YAN WAR STATES AND LOOMPUTE amazonaws.com	OTHER
2017-07-26 126.141	36 141.253.218.25	443	3	124	United States	Seattle	(4)	OTHER
2017-07-26	36 141.253.218.26	443	3	124	United States	Seattle	which we have we compute amazonaws.com.	OTHER
2017-07-26 10126.141	36 141.253.218.27	443	4	168	United States	Seattle	(A) x x x A (A) A (x x x x 1.compute amazonaws.com	OTHER
2017-07-26 2126.141	36 141.253.218.33	443	5	208	United States	Seattle	2.2	OTHER
2017-07-26 126.141	36 141.253.218.36	443	3	124	United States	Seattle	X	OTHER
2017-07-26 3126.141	36 141.253.218.38	443	2	80	United States	Seattle	1. compute amazonaws.com	OTHER
2017-07-26	36 141.253.218.42	443	3	124	United States	Seattle	(Set) best to \$ 10 (\$ \$ 10 1 compute amazonaws.com	OTHER
2017-07-26 39126.141	36 141.253.218.43	443	3	124	United States	Seattle	1994 West And Andrew 1. compute amazonaws.com	OTHER
2017-07-26 38 126.141	36 141.253.218.46	443	3	124	United States	Seattle	A Contract of the second secon	OTHER
2017-07-26 23,126.141.	36 141.253.218.49	443	4	164	United States	Seattle	Wとどがおいて表示が新していた。	OTHER
2017-07-26 126.141	36 141.253.218.54	443	1	40	United States	Seattle	Market Strange Market Stranget A. Compute amazonaws.com	OTHER
2017-07-26 126.141	36 141.253.218.56	443	1	40	United States	Seattle	A Standard Strange 1 compute amazonaws.com	OTHER
2017-07-26	36 141.253.218.61	443	1	40	United States	Seattle	Sec > 2 Mile 2 Alt Sec 9 1 1. compute amazonaws.com	OTHER
2017-07-26 01126.141	36 141.253.218.65	443	1	40	United States	Seattle	⇒ y where q = 1, w 1.compute.amazonaws.com	OTHER
2017-07-26 126.141	36 141.253.218.72	443	3	124	United States	Seattle	shift of the second sec	OTHER
2017-07-26 00 126.141	36 141.253.218.102	443	1	40	United States	Seattle	rest of the second seco	OTHER
2017-07-26 .02.126.141	36 141.253.218.105	443	3	124	United States	Seattle	A State of the sta	OTHER
2017-07-26 20126.141	36 141.253.221.7	443	3	124	United States	Seattle	(c)	OTHER
2017-07-26 👾 126.141	36 141.253.221.12	443	2	80	United States	Seattle	$\{y^{\alpha},y^{\alpha},y^{\alpha}\}, (y^{\alpha}), (y^{\alpha}), (y^{\alpha}), (y^{\alpha}), (y^{\alpha})\} \}$ 1.compute amazonaws.com	OTHER
2017-07-26 2, 126.141	36 141.253.221.14	443	1	40	United States	Seattle	And the second s	OTHER
2017-07-26 20126.141	36 141.253.221.23	443	3	124	United States	Seattle	Pipe Washers Rev and a compute amazonaws.com	OTHER
2017-07-26 2126.141	36 141.253.221.28	443	1	40	United States	Seattle	3. A straight of the state of t	OTHER
2017-07-26	36 141.253.221.27	443	2	108	United States	Seattle	State of the second sec	OTHER
2017-07-26 00126.141	36 141.253.221.29	443	3	124	United States	Seattle	2013 Section 2014 (12, 2014) Loompute amazonaws.com	OTHER
2017-07-26 28 126.141	36 141.253.221.31	443	3	124	United States	Seattle	section (Net of Net Section 1.compute amazonaws.com	OTHER
2017-07-26 22 126.141	36 141.253.221.35	443	1	40	United States	Seattle	200 1 - 200 Carried 1. compute amazonaws.com.	OTHER
2017-07-26 🕺 126.141	36 141.253.221.37	443	1	40	United States	Seattle	452 Start Contracts 1.compute amazonaws.com.	OTHER
2017-07-26 126.141	36 141.253.221.85	443	3	124	United States	Seattle	200 State State Compute amazonaws.com	OTHER
2017-07-26 22,126.141	36 141.253.221.91	443	2	80	United States	Seattle	$V_{abc} = \int dd_{abc} dd_{abc$	OTHER
2017-07-26 3 126.141	36 141.253.221.93	443	1	40	United States	Seattle	A second	OTHER
2017-07-26 2126.141	36 141.253.221.95	443	1	40	United States	Seattle	A second se	OTHER
2017-07-26 \$2126.141	36 141.253.221.100	443	1	40	United States	Seattle	ジンディー 名字 子子 子子 小 1.compute amazonaws.com	OTHER

And the above list continues after the bottom of the picture.



In the following example, the scanner tests the HTTP (80) service, but also another unprivileged port number (65535 stands for 'high port' above 1024). Here also, the figure shows only a part of the scan sequence.

- Unserver localnost » 🗐 D	atabase: tranvion	> 🚮 190	18: 19W	Thanhe				
Browse 🥻 Structure	e 📝 SQL	Sea	rch	34 0	nsert 🐻 Export	🖬 Import 🥒	Operations 😹 Triggers	
2011-01-2112 0-33201.112	141.205.218.21	801	3	124	United States	Unevenne	AV&ALvm.com.	ASA ANT ANT ANT ANT ALL
2017-07-21 2010 201 172	141 253 218 27	65535	3	124	United States	Chevenne	A Star com	ASA AND AND THE I C
2017-07-21 201 172	141 253 218 31	80	1	40	United States	Chevenne	in set and com	ASSIGN/ MAGALYERS LLC
2017-07-21 242-026 201 172	141 253 218 31	85535	4	40	United States	Chevenne	h white com	AS A REAL PARTY FROM LC
2011-07-21 93 98 201.172	141.253.210.31	00000		404	United States	Chausers	Contraction and	AC AWAY STRATTOP IL C
2017-07-21 32,347-201.172	141.233.216.33	00		124	United States	Cheyerne	Servicem.	Rotan Contraction
2017-07-21 (15-389.201.172	141.253.218.33	65535	1	40	United States	Cheyenne	N _N Y's givm.com.	AS WEAT THE PRODUCT
2017-07-21 23:55 201.172	141.253.218.36	80	3	124	United States	Cheyenne	2 Vervm.com.	ASM ACT STATERS LLC
2017-07-21	141.253.218.36	65535	1	40	United States	Cheyenne	wi§4svm.com.	ASAME AN ANY ERS LLC
2017-07-21	141.253.218.38	80	া	40	United States	Cheyenne	i⊋ gi≮(vm.com.	AS-100 AS-100 AS-100 ERS LLC
2017-07-21 38 34 201.172	141.253.218.38	65535	1	40	United States	Cheyenne	Start wm.com.	AS THE COURSE TERS LLC
2017-07-21	141.253.218.42	80	3	124	United States	Cheyenne	Sugar wm.com.	AS CONTRACTOR OF A STATE OF A STA
2017-07-21 3 9 35 201.172	141.253.218.42	65535	1	40	United States	Cheyenne	v www.com.	ASA Your Print ERS LLC
2017-07-21 202-59 201.172	141.253.218.43	80	1	40	United States	Cheyenne	ise a five com.	AS AN
2017-07-21 21:55 201.172	141.253.218.43	65535	1	40	United States	Chevenne	Kirwin com.	AS A WALL THERS LLC
2017-07-21 201172	141.253.218.46	80	3	124	United States	Chevenne	A COMPANY COM	ASANA ANA ANA ERS LLC
2017-07-21 35-85-201 172	141 253 218 48	85535	4	40	United States	Chevenne	www.wm.com	ASPANNING THERS ILC
2017 07 24 12/14 201 472	144.252.210.40	00000	2	104	United Ciston	Chausana	The second second	ACCOUNT AND THE PLACE
2011-01-21 265 29 201.112	141.203.216.48	00	-14-	124	United States	oneyenne	sy wear on	Advision and the second
at userine I	local	port	pkts	bytes	country	city	- 3 7 9	A Set .
2017-07-21	141.253.218.49	65535	1	40	United States	Cheyenne	ing we will com.	AS(2,48) AN AN ERS LLC
2017-07-21	141.253.218.52	80	3	124	United States	Cheyenne	Construction.	AS(****************************
2017-07-21	141.253.218.52	65535	1	40	United States	Cheyenne	vm.com.	AS 6 29 (TRS LLC
2017-07-21	141.253.218.54	80	1	40	United States	Cheyenne	Calify win com.	AS A STATE AS LLC
2017-07-21 0.25 5.201.172	141.253.218.54	65535	1	40	United States	Cheyenne	()+)/s.vm.com.	AS COMPANY AND TERS LLC
2017-07-21 - 5 16 201.172	141.253.218.56	80	2	80	United States	Cheyenne	်ရန်(ဖွားym.com.	ASA SAL CUTATION LLC
2017-07-21	141.253.218.56	65535	2	80	United States	Cheyenne	rive sigvm.com.	ASA MANA RES LLC
2017-07-21 21:00 201.172	141.253.218.57	80	3	124	United States	Cheyenne	Wilksym.com.	ASHING ANY ERS LLC
2017-07-21 201.172	141.253.218.57	65535	2	80	United States	Chevenne	Parative com.	ASHORE STOLERS LLC
2017-07-21 3014 201 172	141 253 218 58	80	1	40	United States	Chevenne	Server wm com	AS& WATWARD RES LLC
2017-07-21 (4):58: 201 172	141 253 218 58	85535	4	40	United States	Chevenne	Les Sum com	ASHING WERS U.C.
2017 07 21 06 201 172	141 252 219 81	200000		40	United States	Chovenne	in the second	ACCESSION ACCESSION
2011-01-21 33334 201.172	141.253.210.01	REEDE	- 1	40	United States	Chavenne	i e Avenue en	AS ALL AND AN AVERSION OF THE ALL O
2017-07-21 33 33:201.172	141.203.218.01	00030	.1	40	United States	Cneyenne	A Second Com.	ASIGN TO ASIGN THE ASIGN THE
2017-07-21 25,912,201.172	141.203.218.00	80	3	324	United States	Gneyenne	savaevm.com.	ASIA (S) A TREAMERS LLC
2017-07-21	141.253.218.65	65535	4	164	United States	Cheyenne	A Systym.com.	ASOUR, NOTAS ERS LLC
2017-07-21 23-234 201.172	141.253.218.70	80	1	40	United States	Cheyenne	wigsterm.com.	AS the U. OLD CHERS LLC
2017-07-21	141.253.218.70	65535	1	40	United States	Cheyenne	initiation.	AS4000 CASHERS LLC
2017-07-21 201.172	141.253.218.102	80	1	40	United States	Cheyenne	(v, h) vm.com.	ASARA ASARA BERS LLC
2017-07-21	141.253.218.102	65535	1	40	United States	Cheyenne	Steenwork.	AS A SALE AND A REAL LLC
2017-07-21 201.172	141.253.218.105	80	1	40	United States	Cheyenne	YW/22(vm.com.	ASAL THE HAVE AN LLC
2017-07-21 58 22.201.172	141.253.218.105	65535	1	40	United States	Cheyenne	Selfer vm.com.	AS4000 STATERS LLC
2017-07-21 37 mat 201.172	141.253.221.7	80	з	124	United States	Cheyenne	No Arvm.com.	AS 20 4 (36 S) HERS LLC
2017-07-21 3 3 2 201.172	141.253.221.12	80	3	124	United States	Cheyenne	and Statement	AS AS A REAL AND A REAL
2017-07-21	141.253.221.14	80	1	40	United States	Chevenne	Protocom.	ASHING THIS LLC
2017-07-21 49 /03/0 201 172	141 253 221 16	80	3	124	United States	Chevenne	Survey ym com	ASANA
2017-07-21 24-232 201 172	141 253 221 23	80	2	124	United States	Chevenne	Seal and an	ASPANAL AND FERSILS
2017 07 21 8 201 172	141 252 221 28	00		40	United States	Chausana		ACTIVITY AND ALL AND A
2017-07-21 2313235.201.172	141.203.221.20	00	1	40	United States	Chevenne	We we with com.	Assistant and the second
2017-07-21 01-3-2-201.172	141.293.221.27	80	3	124	United States	Cheyenne	Martin vm.com.	Rowing Conters LLC
2017-07-21	141.253.221.29	80	3	124	United States	Cheyenne	24 Yearver.com.	AS 05 W 01 WOOD YERS LLC
2017-07-21 24-5-0.201.172	141.253.221.31	80	3	124	United States	Cheyenne	3.9-30 vm.com	ASA ANA ANA ERS LLC
2017-07-21 2020 201.172	141.253.221.35	80	- 31	40	United States	Cheyenne	Si Syvm.com.	AS# AS# FERS LLC
2017-07-21 33 3 201.172	141.253.221.36	80	1	40	United States	Cheyenne	(grigelystym.com.	AS AS A STATERS LLC
2017-07-21	141.253.221.37	80	3	124	United States	Cheyenne	wm.com.	ASIS AN ANY ERS LLC
2017-07-21 201.172	141.253.221.60	80	1	40	United States	Cheyenne	∰⊈≵ _{rev} vm.com.	ASS AND ASS AND TERS LLC
2017-07-21 201.172	141.253.221.85	80	1	40	United States	Cheyenne	S. Sevm.com.	AS AS THE PART OF
2017-07-21 4 20 201 172	141.253.221.89	80	3	124	United States	Chevenne	W.L.R. vm.com.	AS WERE AN A REAL OF A REA



In the following example, the remote system seems to perform complete daily scans, <u>repeated on</u> <u>11 different days</u> of about a one-month period, using <u>different target service ports – FTP (21), HTTP</u> (80), HTTPS (443). The figure is truncated, there are 1078 rows like that in the pattern.

at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-06-27	180.164	141.253.218.6	21	6	240	United States	OTHER	20 9	AS17 Communications
2017-06-29	A 180.164	141.253.218.6	21	8	320	United States	OTHER	Contemp: 180.164	AS17
2017-07-14	AL 180.164	141.253.218.6	21	1	40	United States	OTHER	AZ	AS17 Communications
2017-07-16	ACA 21 180 184	141.253.218.6	21	2	80	United States	OTHER	180.164	AS17 Solar Communications
2017-06-27	5 180.164	141.253.218.6	80	4	160	United States	OTHER	7.180.164	AS17
2017-06-28	180.164	141.253.218.6	80	4	160	United States	OTHER	180.180.164	AS17
2017-06-29	180.164	141.253.218.6	80	4	160	United States	OTHER	180.164	AS17
2017-06-30	180.164	141.253.218.6	80	4	160	United States	OTHER	AMAN 180.164	AS17
2017-07-14	180.164	141.253.218.6	80	2	80	United States	OTHER	AC. 180.164	AS17
2017-07-17	24-48-180.164	141.253.218.6	80	2	80	United States	OTHER	180.184	AS17 AS17 Communications
2017-07-21	Sel 359, 180, 184	141.253.218.6	80	2	80	United States	OTHER	180.164	AS17
2017-07-17	Se 84, 180, 164	141.253.218.6	443	2	80	United States	OTHER	A 180.184	AS17
2017-06-27	180.164	141.253.218.7	21	6	240	United States	OTHER	AND 180.164	AS17 Communications
2017-06-29	Vers 2, 180, 164	141.253.218.7	21	4	160	United States	OTHER	180.164	AS17 Communications
2017-07-16	a 180,164	141.253.218.7	21	2	80	United States	OTHER	We W. 180, 164	AS17 Communications
2017-06-27	180.164	141.253.218.7	80	2	80	United States	OTHER	4.448 180 164	AS17% West Communications
2017-06-28	180 184	141 253 218 7	80	2	80	United States	OTHER	180 164	AS17
2017-06-29	No. 64 180 184	141 253 218 7	80	6	240	United States	OTHER	Sec. 180 184	AS17
2017-06-30	A 180 184	141 253 218 7	80	8	320	United States	OTHER	180 180 184	AS174 Size Communications
2017-07-13	0.14 180 184	141 253 218 7	80	2	80	United States	OTHER	180 184	AS17 A Mode Communications
2017-07-14	And JAN 180 184	141 253 218 7	80	2	80	United States	OTHER	180 184	AS175 Communications
2017-07-17	180 184	141 253 218 7	80	4	160	United States	OTHER	20 22 180 184	AS17 (VSA) Communications
2017-07-21	ALANA 180 184	141 253 218 7	80	2	80	United States	OTHER		AS178 With Communications
2017-07-21	100.104 100.104	141.253.210.7	442	5	204	United States	OTHER	SAN 100 184	AS172 Communications
2017-07-17	120100100104	141.253.210.7	24	5	204	United States	OTHER	100.100.104	AS175 Communications
2017-00-21	180,104	141.253.218.10	21	2	200	United States	OTHER	A 427 180.104	AS172 Automotions
2017-00-28	X0222 X 180, 104	141.253.218.10	21	2	20	United States	OTHER	104 COV 400 104	AS1740 (AStory) Communications
2017-07-10	21. 24. 100.104	141.253.218.10	21	2	00	United States	OTHER	100.104	AS17: ASUS Communications
2017-00-27	A	141.253.218.10	00	4	180	United States	OTHER	100.104	AS17 Communications
2017-00-20	100.104	141.253.218.10	00	-	200	United States	OTHER	New 201 400 484	AC47/2 June Communications
2017-00-29	100.104	141.203.216.10	00	30	200	United States	OTUER	100,100,104	AG47
2017-00-30	180.104	141.203.218.10	80	12	480	United States	OTHER	A 233,180,104	AST/ Communications
2017-07-13	100,002,180,104	141.253.218.10	80	2	00	United States	OTHER	100.104	AS17 Communications
2017-07-14	180,104	141.203.218.10	80	2	80	United States	OTHER	122-21-180.104	ASTA 23 Get Communications
2017-07-17	100.104	141.203.218.10	80	2	30	United States	OTUER	100 100 100 104	AST AST Communications
2017-07-21	-x ₂ /2/2/180.104	141.253.218.10	80	2	80	United States	OTHER	22 32 180.104	AST/: Communications
2017-07-17	180.104	141.203.218.10	443	0	204	United States	OTHER	Sec. 180, 104	AST AST AST COmmunications
2017-06-27	22. 52. 180.164	141.253.218.11	21	0	240	United States	OTHER	2,52,7,180,104	AS176 Sugar Communications
2017-06-29	218,035,180,164	141.253.218.11	21	2	80	United States	OTHER	21.124.180.164	AS1/Communications
2017-07-14	180.164	141.253.218.11	21	2	80	United States	OTHER	26 - 180.164	AS179. Communications
2017-07-16	284.027.180.164	141.253.218.11	21	2	80	United States	OTHER	2.180.164	AS174 Communications
2017-06-28	Servi C 180.164	141.253.218.11	80	4	160	United States	OTHER	38, 65, 180, 164	AS17 AS17 Communications
2017-06-29	asesa 180.164	141.253.218.11	80	3	120	United States	OTHER	1990 N. 180, 184	AS17 Communications
2017-06-30	354 AM 180.164	141.253.218.11	80	6	240	United States	OTHER	667.5.180.164	AS17
2017-07-04	Net 180.184	141.253.218.11	80	2	80	United States	OTHER	405 K 180.164	AS17 Communications
2017-07-14	180,164	141.253.218.11	80	2	80	United States	OTHER	25.251.180.164	AS1777 Communications
2017-07-17	NO 321, 180, 164	141.253.218.11	80	2	80	United States	OTHER	23 429 2.180.164	AS17 State Communications
2017-07-21	· 3月六天 180.164	141.253.218.11	80	2	80	United States	OTHER	2.207.180.164	AS17 Communications
2017-07-17	180.164 (K)	141.253.218.11	443	5	204	United States	OTHER	AV-05.180.164	AS17 : Organic Communications
2017-06-27	180.184	141.253.218.12	21	6	240	United States	OTHER	Y 4× 180.164	AS17
2017-06-29	A 180.164	141.253.218.12	21	2	80	United States	OTHER	180.184	AS17 Communications
2017-07-14	Association 180,164	141.253.218.12	21	2	80	United States	OTHER	Mar 180.164	AS17 State Communications
2017-07-16	1.25.3.25 180 184	141 253 218 12	21	2	0.0	Linited States	OTHER	180 180 184	AS171 AVA Communications

© 2020 AETHIS sa/nv Belgium Document version 1.0, 2020-12 -

All rights reserved -Open Source Apache License v2.0



<u>Searching on the basis of DNS domain name part</u> highlights what seems to be different complete daily scans (same remote address for a given day), but repeated by different remote addresses on different days, all belonging to the same DNS domain name, although geo-located in totally different countries and cities.

✓ Showing rows 1 - 482 (483 total, Query took 0.1289 st	ec)
SELECT * FROM 'lowTraffic' WHERE 'DNS' LIKE '%%%%com.' ORDER BY INET ATON(LOCAL) , INET ATON(remote) , port, at LIMIT 1 , 3000	

Here below, the first, the fifth and the last page of the result of the query.

_



at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-18	36 37.110.191	141.253.218.6	80	1	40	Singapore	Singapore	110.19 Jetrcom.	AS20
2017-07-04	AX 169 194	141.253.218.6	80	1	40	United States	Miami	1017 169 164 St. com.	AS20 ASA MANA LLC
2017-07-16	10 105 37.11	141.253.218.6	80	1	40	Netherlands	Amsterdam	62:19-37.11. Ave 2m.	AS20
2017-07-18	117,149	141.253.218.6	80	1	40	United States	Matawan	S	AS20-WERTS LAG. LLC
2017-07-01	AND 122 157	141 253 218.6	85535		40	United States	Matawan	25-06-122 18- 200 com	AS20020 Storma LLC
2017-07-08	4.45361 207 191	141 253 218 8	80	1	40	United States	Los Angeles	Shift 207 262 Stroom	AS20/64: Stational LLC
2017-08-20	A 10 1 82 101	141 253 218 7	20	-	40	United States	Los Angeles	600 82 10	AS20ASS Section LLC
2017-00-28	22. 440 404	141.200.210.7	00		40	Cinganase	Cinamara	100 100 100 100 100 nom	A02042 4 2 2 4 3 4 4 1 C
2017-07-04	2446 480 404	141.255.210.7	00	-	40	United States	Minai	Sunda 480 4020 and another	AS20 ACTING THE LLC
2017-07-04	24, 4, 9, 108, 184	141.200.210.7	00		40	Matheologia	Antehnologi	VERY TOB. HE SHOW DOM.	AS2010 STEVE LLC
2017-07-10	Vision and	141.203.216.7	00		40	Netherlands	Amsterdam	Activity of the state of the	AS20491CTRASA
2017-07-18	¥8.94.117.148	141.203.218.7	80	-	40	United States	Matawan	20219-117-1468-9189 com.	AS204703 Migaa, LLC
2017-07-01	12 A 122.151	141.253.218.7	05535	3	40	United States	Matawan	28-01122.15919-96100m.	AS208 Kawawa, LLC
2017-07-06	2421.207.191	141.253.218.7	80	1	40	United States	Los Angeles	1.207. Star. Syr.com.	AS204
2017-07-18	àga an 110, 191	141.253.218.10	80	2	80	Singapore	Singapore	2013 110.19 Sol Acom.	AS20 AS20 Coversa, LLC
2017-07-04	AN 169.194	141.253.218.10	80	1	40	United States	Miami	22 % 169.115 % 2 com.	AS20 AS20 AS ANA LLC
2017-07-16	领制37.11	141.253.218.10	80	1	40	Netherlands	Amsterdam	1975(37.11) April m.	AS2012 AS2012 ASSA LLC
2017-07-18	46.34.117.149	141.253.218.10	80	1	40	United States	Matawan	**************************************	AS20 AS ACTION A LLC
2017-07-01	· 122.157	141.253.218.10	65535	1	40	United States	Matawan	149/5 122.196 vis com.	AS20 A Makaa LLC
2017-06-29	91.50.18	141.253.218.10	80	1	40	United States	Elk Grove Village	14:50 - Say com.	AS20 AS20 AS LLC
2017-07-18	Gran 110.191	141.253.218.11	80	1	40	Singapore	Singapore	110.16 Albacom	AS204- AS204 AND
at	kalate	local	port	pkts	bytes	country	city	also.	ASN
2017-07-04	3x27.169.194	141.253.218.11	80	1	40	United States	Miami	User 169 1Fb, we com.	AS20-X-Second LLC
2017-07-16	Sec. 8,37,11	141.253.218.11	80	1	40	Netherlands	Amsterdam	W10737.11.w/2015m	AS204 Standa LLC
2017-07-17	A 117 149	141 253 218 11	80		40	United States	Matawan	\$45,2117 1492/kishom	AS206 Source LLC
2017-07-18	Sec. 117 149	141 253 218 11	80		40	United States	Matawan	143570117 14V2/162com	AS208/WARKAGING LLC
2017-07-01	345 3 122 157	141 253 218 11	85535	-	40	United States	Matawan	2 P (\$2/122 112) (-X (com)	AS20X Services LLC
2017-01-01	76(0) 122.101	141.253.210.11	00000	-	40	Cinganoro	Cingapore	St. A. 110 10: 10: 10: 00m.	ACONTENANT LLC
2017-07-10	ALL 10.181	141.200.210.12	00	-	40	United Oteran	Minut	AND ADD AND AND AND	According to the
2017-07-04	1004,8.108.184	141.200.210.12	OU DEEDE	4	40	United States	Wielfi	Contraction and a second second	AS2019 Marchard LLC
2017-07-01	Q14 58, 122, 101	141.203.218.12	00030		40	United States	wiatawan	PAL 2 122. Physiol. com.	AS20CHT NY CLA, LLC
2017-07-18	110.191	141.253.218.10	80	1	40	Singapore	Singapore	-25-55 110, 165 (3, 55; com.	AS20, We way at LLC
2017-07-04	Ref. 169.194	141.253.218.16	80	1	40	United States	Miami	PRESENTED THE SECTION.	AS20*/ 229/9 ya, LLC
2017-07-18	12(5),117.149	141.253.218.18	80	1	40	United States	Matawah	117.14 a 56.00m.	AS206 AS206 AS206 LLC
2017-07-01	· 2014年122.157	141.253.218.16	65535	1	40	United States	Matawan	122.15 Com.	AS204- / Akyya, LLC
2017-07-18	Sec. 110.191	141.253.218.20	80	1	40	Singapore	Singapore	2.110.19 (j.f. com.	AS204 AS204 ASA LLC
2017-07-04	2 169,194	141.253.218.20	80	1	40	United States	Miami	4844 169 159 499 com	AS20 AS20 ASIA LLC
2017-07-15	37.11	141.253.218.20	80	1	40	Netherlands	Amsterdam	404 37.11.517 Zen.	AS20 AS20 ASA LLC
2017-07-18	公司3,117.149	141.253.218.20	80	1	40	United States	Matawan	19/2 117.144 (com.	AS20 Arg Source, LLC
2017-07-01	31 H 122.157	141.253.218.20	65535	1	40	United States	Matawan	122.11 Section.	AS20
2017-07-05	68 X.75.114	141.253.218.20	80	1	40	United States	Matawan	48 0 75.11 Som	OTHES
2017-07-18	sec.29.110.191	141.253.218.21	80	1	40	Singapore	Singapore	20110.19	AS20 AS20 AS ASA AS
2017-07-04	Vic 169.194	141.253.218.21	80	1	40	United States	Miami	16 189 169 160 act com.	AS204 Asta is LLC
at	in the	local	port	pkts	bytes	country	city	KANA .	ASN
2017-08-29	£ \$4.22.172	141.253.218.21	80	1	40	United States	Elk Grove Village	144 22.172	AS204 ASSAMA LLC
2017-07-18	PA-05.37.11	141.253.218.21	80	1	40	Netherlands	Amsterdam	37.11 Jac Lim	AS204 Accessa LLC
2017-07-18	Se 117 149	141,253,218,21	80		40	United States	Matawan	-2 117,19 8 bom	AS20 MAN W Ha LLC
2017-07-01	127 122 157	141 253 218 21	85535	1	40	United States	Matawap	230 04122 15 4 Chingson	AS2012-10-10-10-11-0
2017-07-19	110 101	141 253 218 22	20		40	Singapore	Singanore	Solte 110 100 me more	AS20ex/5,336-25ia 11.0
2017.07.04	Same 180 104	141 252 219 22	00		40	United States	Minmi	A The 180 Merst Set open	AS20 AS20 AS20 AS20 AS20
2011-01-04	A A 117 140	141.250.210.22	00		40	United States	Matawas	Walk 105 Tor Care Com	AS2042 AS2042 AS204
2017-01-16	N. J. 400 457	141.235.216.22	000	-	40	United States	Matawan	CALIFICATION AND DATE COMME	Account States LLC
2017-07-01	24 39-122-101	141.203.216.22	00030		40	United States	Matawan	145/20122.159 (255-00m.	AS204 Provide LLC
2017-06-29	-88(*200.237.8	141.253.218.22	80	1	40	United States	Dallas	2/1/1/20.237/5/2/2/ com.	AS200 AS200
2017-07-18	No. 110.191	141.253.218.23	80	1	40	Singapore	Singapore	Teger 110.18 rest from	AS20strong Parketa, LLC
2017-07-04	\$ 169.194	141.253.218.23	80	1	40	United States	Miami	1975 (\$109.154 (\$100m.	AS20 20 ANA Ma, LLC
2017-07-15	122-92.37.11	141.253.218.23	80	1	40	Netherlands	Amsterdam	2010137.11	AS20mg Colorida, LLC
2017-07-18	法法:117.149	141.253.218.23	80	1	40	United States	Matawan	ाज (त. 117.14) solar com.	AS20
2017-07-01	122.157	141.253.218.23	85535	1	40	United States	Matawan	3.0 3 122.15 Secom.	AS20
2017-07-18	Gay, 110, 191	141.253.218.24	80	1	40	Singapore	Singapore	2 3 110.19 (j. 5 com.	AS20 AS20 Asa, LLC
2017-07-04	159 194	141.253.218.24	80	1	40	United States	Miami	20169.112 Scom.	AS20 KANA ALC
2017-08-29	14 An 20.17	141.253.218.24	80	1	40	United States	Elk Grove Village	20.17 - 42 atom.	AS20 AS20 AS AS AS AS
2017-07-15	\$ 779.37.11	141.253.218.24	80	1	40	Netherlands	Amsterdam	37.11 (Asym.	AS204 AS204 LLC
2017-07-17	A 117.149	141.253.218.24	80	1	40	United States	Matawan	12 14 117.14 r. bom.	AS20
2017-07-01	C = 122.157	141.253.218.24	85535	1	40	United States	Matawan	22 122 15 Scom.	AS20-12-2408 ma, LLC

© 2020 AETHIS sa/nv Belgium Document version 1.0, 2020-12 -

All rights reserved -Open Source Apache License v2.0 trafMon Use Case 3: Security Auditing Page: 17/58



at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-06-27	() () () () () () () () () () () () () (141.253.221.18	80	11	2702	United States	Matawan	81.13% Com.	OTHER
2017-07-02	Sec. 181.139	141.253.221.18	80	11	2666	United States	Matawan	wif) 81.13A (5 com.	OTHER
2017-07-04	35 181.139	141.253.221.10	80	11	2702	United States	Matawan	5- 81.13	OTHER
2017-07-08	AS\$2181.139	141.253.221.18	80	12	2670	United States	Matawan	2 99 81.13(5) a com.	OTHER
2017-07-13	Store 181.130	141.253.221.18	80	3	144	United States	Matawan	\$5,000 81,136 g () com.	OTHER
2017-07-21	Ar 181.139	141.253.221.18	80	6	1700	United States	Matawan	44 64 81 139 (com.	OTHER
2017-08-29	183.69	141.253.221.18	80	12	2742	United States	Matawan	(1997) 83.69 (c) om.	OTHER
2017-07-17	183.69	141.253.221.18	80	12	2735	United States	Matawan	379 37 83.69 (J.k.), om.	OTHER
2017-07-22	€ 183.69	141.253.221.18	80	11	2663	United States	Matawan	No. 10 83.69 Storagon.	OTHER
2017-08-29	AP-0 (185.187	141.253.221.18	80	12	2975	United States	Matawan	**************************************	OTHER
2017-06-28	CH_4 187.151	141.253.221.10	80	12	2737	United States	Matawan	87.15 com.	OTHER
2017-08-29	a 187.151	141.253.221.16	80	11	2709	United States	Matawan	87.15 (com.	OTHER
2017-07-01	26 187.151	141.253.221.18	80	4	184	United States	Matawan	87.15 com.	OTHER
2017-07-26	Sept. 33.0	141.253.221.16	80	12	2798	United States	Matawan	April (\$3.0 western	OTHER
2017-07-06	54.112	141.253.221.18	80	11	2638	United States	Matawan	4.112 or om	OTHER
2017-07-08	하는 2054,112	141.253.221.16	80	11	2678	United States	Matawan	Sec 94.112 Xigs.com.	OTHER
2017-07-17	As 54.112	141.253.221.18	80	11	2694	United States	Matawan	34.112	OTHER
2017-07-19	2017 54.112	141.253.221.18	80	11	2697	United States	Matawan	4.112 (Sirvion.	OTHER
2017-07-05	60.56	141.253.221.10	80	12	2937	United States	Matawan	a.Y. 940.56.v. setu sem.	OTHER
2017-07-05	ia(//₹ ¹ 60.122	141.253.221.16	80	12	2935	United States	Matawan	10.122 - 4-2 om.	OTHER
at	Well Vie	local	port	pkts	bytes	country	city	NOT:	ASN
2017-08-29	60.132	141.253.221.18	80	12	2985	United States	Matawan	14-110.132.4 (www.om.	OTHER
2017-08-28	SNC 761.35	141.253.221.16	80	12	2991	United States	Matawan	Sec. 91.35. 446 Jum.	OTHER
2017-06-27	61.132	141.253.221.18	80	12	2975	United States	Matawan	2011132 QQ jom.	OTHER
2017-07-04	62.201	141.253.221.18	80	11	2872	United States	Matawan	76/14/02.2010/uF/com	OTHER
2017-07-04	63.29	141.253.221.18	80	11	2911	United States	Matawan	x84 \$13.29.v.24 (im.	OTHER
2017-07-02	63.253	141.253.221.16	80	12	2991	United States	Matawan	13.253	OTHER
2017-08-28	38.176.164	141.253.221.18	80	11	2658	Germany	Frankfurt am Main	B. 178 A. altr.com	AS20 Servina, LLC
2017-07-01	845 88.178.184	141.253.221.18	80	11	2724	Germany	Frankfurt am Main	AND B. 176 TWH altr.com.	AS200 MichaelLC
2017-07-02	20:38.178.184	141.253.221.18	80	11	2870	Germany	Frankfurt am Main	999 8.176 9 19 altr.com.	AS20 AS20 a, LLC
2017-07-14	38.176.164	141.253.221.16	80	11	2674	Germany	Frankfurt am Main	3.176 Mainditr.com.	AS20-5 Preventa, LLC
2017-07-16	34 88 176 164	141.253.221.18	80	11	2698	Germany	Frankfurt am Main	3. Post 3. 176 Marchiltr.com	AS20 AS20 Asia a LLC
2017-07-20	98.178.164	141.253.221.18	80	11	2676	Germany	Frankfurt am Main	8.176 Weekiltr.com.	AS20*/ Asiges, LLC
2017-07-21	1442038.178.184	141.253.221.18	80	11	2677	Germany	Frankfurt am Main	(43) 8.176 (今) ltr.com.	AS20 9 C Logala, LLC
2017-07-04	35% 38.188.134	141.253.221.16	80	12	2987	France	Aubervilliers	3/18.188.1%; 3/1tr.com.	AS20(7) AS20(7
2017-07-04	38.188.197	141.253.221.18	80	12	2980	France	Aubervilliers	2017-8.188 (Applith.com)	AS20 AS20 ANA, LLC
2017-07-02	38, 189, 106	141.253.221.18	80	12	2992	France	Aubervilliers	**************************************	AS20/2014 Asta LLC
2017-08-29	38, 189, 186	141.253.221.18	80	12	2991	France	Aubervilliers	Sec. 189 Key ultr.com.	AS200 Sa, LLC
2017-07-03	(\$38,190,162	141.253.221.16	80	12	2976	France	Aubervilliers	Rest 8.190 Weiltr.com.	AS2011 AS2011 ASIA LLC
2017-07-01	253 38.191.233	141.253.221.18	80	12	2995	France	Aubervilliers	(-)治(-)名.191.20余(-Altr.com:	AS20 Arania, LLC
2017-07-04	01.48.217	141.253.221.18	80	11	2902	France	Saint-Denis	Act K1.48.2 Singst.com	AS20401 Standa LLC
at	<i>idale</i>	local	port	pkts	bytes	country	city	(第4)	ASN
2017-06-28	31.48.242	141.253.221.18	80	12	2993	France	Saint-Denis	46.2% str.com.	AS20 AN ANA ARA LLC
2017-08-29	91.62.148	141.253.221.18	80	12	2975	France	Saint-Denis	18,079(1.62.1)(NA))(r.com)	AS20% SANA HIC
2017-07-03	215 1.209.138	141.253.221.18	80	12	2983	France	Paris	209.1% (ppr.com.	AS20 AS20 ASA ALLC
2017-07-04	2 Aug 99.70.38	141.253.221.18	80	12	2981	Denmark	Skanderborg	1341039.70.3⊈ (/shoom.	AS20010 Storya, LLC
2017-07-18	Sec. 110.191	141.253.221.23	80	8	340	Singapore	Singapore	10.19 Sea com.	AS20 As LLC
2017-07-04	169.194 Jack	141.253.221.23	80	3	124	United States	Miami	4. Con 69.194 . 4.65 com.	AS2011 小市社会a, LLC
2017-07-09	《资源7.217	141.253.221.23	21	20	1267	United States	Matawan	1.217. (m.	AS203 Markina, LLC
2017-07-15	款为在7.217	141.253.221.23	21	19	1220	United States	Matawan	运行的1217.4%为hm.	AS20 AS2 Areaa, LLC
2017-07-16	37.11	141.253.221.23	80	4	168	Netherlands	Amsterdam	an 1097.11. Seriam.	AS20
2017-07-18	117.149	141.253.221.23	80	3	124	United States	Matawan	17.14 com.	AS204 Ciglinguna, LLC
2017-07-18	Set 110.191	141.253.221.28	80	1	40	Singapore	Singapore	50 2 10.19 yes (com.	AS20 AS20 ASA ALLC
2017-07-04	NC 25 169 194	141.253.221.28	80	1	40	United States	Miami	00.19 (Jane com.	AS207 Standa, LLC
2017-06-29	大程全;75.157	141.253.221.26	80	1	40	United States	Elk Grove Village	2425-5.157% Ashiom.	AS20
2017-07-16	MX 37.11	141.253.221.28	80	1	40	Netherlands	Amsterdam	Shiphes 17.11. salastem.	AS20 (Majagaja, LLC
2017-07-18	Se & 117,149	141.253.221.28	80	2	80	United States	Matawan	A 39 17.142 Secon.	AS20
2017-07-18	S 54, 110, 191	141.253.221.27	80	7	298	Singapore	Singapore	12 3 8t 10.19 4 46 com.	AS20 AS20 ASSA LLC
2017-07-04	法: 34,169.194	141.253.221.27	80	3	124	United States	Miami	\$14571.169.19: 344 com.	AS20 4 Melaa, LLC
2017-07-18	3, 117, 149	141.253.221.27	80	3	124	United States	Matawan	45-6-17.14% so com.	AS20 AS20 As LLC
2017-07-18	.12, 110, 191	141.253.221.29	80	3	124	Singapore	Singapore	10.19 com.	AS20
2017-07-04	50 2 169 194	141.253.221.29	80	3	124	United States	Miami	9.19 com.	AS2013 MULTINA, LLC

© 2020 AETHIS sa/nv Belgium Document version 1.0, 2020-12 -

All rights reserved -Open Source Apache License v2.0 trafMon Use Case 3: Security Auditing Page: 18/58



201707-18 VIT.140 VIT.241 VIT.243 VIT.243 VIT.244 VIT.245	2017-07-18 26 76 37.11	141.253.221.137	80	1	40	Netherlands	Amsterdam	12. 11. 17.11. (Sec. 19)m.	AS207013509Ma, LLC
2017.07.07 Strate Singapore Singapore <ths< td=""><td>2017-07-18</td><td>141.253.221.137</td><td>80</td><td>1</td><td>40</td><td>United States</td><td>Matawan</td><td>TAL-17.1 Construction</td><td>AS20 AS20 ASIA, LLC</td></ths<>	2017-07-18	141.253.221.137	80	1	40	United States	Matawan	TAL-17.1 Construction	AS20 AS20 ASIA, LLC
201707432 201707432 201707432 201707432 201707432 201707433 <t< td=""><td>2017-07-18 4 502 110.191</td><td>141.253.221.145</td><td>80</td><td>3</td><td>120</td><td>Singapore</td><td>Singapore</td><td>(http://10.15).det.com</td><td>AS20 AS4 May Ha, LLC</td></t<>	2017-07-18 4 502 110.191	141.253.221.145	80	3	120	Singapore	Singapore	(http://10.15).det.com	AS20 AS4 May Ha, LLC
20170-58 241-35.221145 80 2 80 Methad Sample > 312.4400m A32.4400m	2017-07-04 2 3 169.194	141.253.221.145	80	2	80	United States	Miami	128 57 569.1 (0% met com.	AS20 AS20 ASIA
20170776 37.11 411.93.221145 60 2 60 Indee Samadam 37.711 cm A32.4 212.0 2017.0 71.1 411.93.221145 60 2 60 Undee Same Marana 7.711 cm A32.4 212.0 Co Undee Same Marana 7.711 cm A32.4 212.0 Co Co Marana 7.711 cm A32.4 212.0 Co Co Marana 7.711 cm A32.4 Co Lo Co Marana 7.711 Co A32.4 Co Lo Co Marana 7.711 Co A32.4 Co Lo Co Marana 7.711 Co A32.4 Lo Lo Co Marana 7.711 Co A32.4 Lo Lo Co Marana 7.711 Marana	2017-06-29 38 28 78.129	141.253.221.145	80	2	80	United States	Elk Grove Village	12 6-01 - 8.12 - 4-100m.	AS200 AS200 ASIA
2017-07-06 4:1 9:1 9:0 2 9:0 Under States Materian 21:1 1:1	2017-07-16 62 5.37.11	141.253.221.145	80	2	80	Netherlands	Amsterdam	44 33-07.11. See Juam.	AS200 STANCE AR, LLC
2017-07-08 -7.7114 +1123-221148 60 2 100 Under States Manuam 50.5114 -5114 -5014 -	2017-07-18 44/46/117.149	141.253.221.145	80	2	80	United States	Matawan	1945 65 17.1 # Kards com.	AS20 AN RIGHTA LLC
2017.07.01 2017.07.01 2017.07.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.02 2017.	2017-07-05	141 253 221 145	80	2	80	United States	Matawan	30-5 11 0 0 0 0 mm	OTHIE
D10170716 C D10170716 C D20170716 C D10170716 C D20170716 C D10170716 C D20170716 C D10170716 C D20170716 C D10170716 C D10170716 C D10170716 D10170716 <thd10170< td=""><td>2017-07-18 365 3 110 191</td><td>141 253 221 163</td><td>80</td><td>4</td><td>164</td><td>Singapore</td><td>Singapore</td><td>Store 10 1Felix-Nicom</td><td>AS205 AS20 AS10A LLC</td></thd10170<>	2017-07-18 365 3 110 191	141 253 221 163	80	4	164	Singapore	Singapore	Store 10 1Felix-Nicom	AS205 AS20 AS10A LLC
2017.07.07 2017.07.04 2017.07.04 2017.07.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05.05 2017.05	2017-07-04 11-85 189 194	141 253 221 183	80	3	124	United States	Miami	NA-20 69 120 Accom	AS20000 Versia LLC
2017-07-06 11 14 28.2.2.170 80 1 40 Surgeores Surge	2017-07-18 ************************************	141 253 221 183	80	4	168	United States	Matawan	43:44:5:17 1.000 com	AS200-X Welcus LLC
2011-0763 V:10 14 2022.170 80 1 40 United States Name 51 60 10 40.20 10 40.20 10	2017-07-18 20:00 110 191	141 253 221 170	80		40	Singapore	Sindapore	Constant ID 1E45 the com	AS200 March 11C
2011-01-05 2117-01	2017-07-04 01/20180 104	141 253 221 170	80	1	40	United States	Miami	A Shrill BD 13hori Groom	4520 At 1025 As 11 C
2017-07-08 v10.101 41233.221.170 08 1 40 Unded States Material Control for the second states Control for the second states	2017-07-18 2006 117 140	141 253 221 170	80		40	United States	Matawan	St. 4517 LiBissic com	AS200 AISTONIA LLC
2017-07-16 110.101 141.283.221.173 20 1 40 Dingapore Singapore 10.11* Com AS201 yaa, LLC 2017-07-16 yi10.101 141.283.221.173 80 1 40 United States Main Color AS201 yaa, LLC 2017-07-16 yi10.101 141.283.221.173 80 1 40 United States Main AS201 yaa, LLC 2017-07-16 yi10.101 141.283.221.204 80 8 400 Singapore Singapore Yi10.101 AS203 yaa, LLC 2017-07-16 yi10.101 141.283.221.204 80 3 124 United States Karavan Yi17.176 AS203 yaa, LLC 2017-07-16 yi17.144 141.283.221.204 80 5 221 United States Matavan Yi17.149 AS203 yaa, LLC 2017-07-16 yi17.140 141.283.221.214 80 5 221 United States Matavan Yi17.149 AS203 yaa, LLC	2017.07.05 24 30.75 114	141 253 221 170	20	-	40	United States	Matawan	12 12 5 11 A Discom	OTHIN:
2017-07-04 100.19 41.2023.21173 00 1 40 Unined States Amaterian Association	2017.07.19 22 20110 101	141 252 221 172	00		40	Cingapore	Singapore	Second de tres au pom	ASSOCIATE AND THE
Barton Barton<	2017-07-04 28 100-104	141.253.221.173	00		40	United States	Miami	RD 11 A BD 11 A BD 10 A BD AD	ASSOCIATION ASSOCIATION
2011-01-11 Control Provide Instructure Provide I	2017-07-15 28-20-27-11	141.253.221.175	00		40	Methodands	Amsterdam	Contra de l'actuação com	AS200 States LLC
2017-07-04 Control Protochled States National Mathem Control of the States ASN 2017-07-18 1101101 141253.221.204 60 8 40 Singapore 510.107 101.107 ASN ASSC vs. LLC 2017-07-18 1101.101 141253.221.204 80 3 124 Unled States EK Grove Village 101.17 ASSC vs. LLC 2017-07-16 171.11 141253.221.204 80 5 212.10Hed States Maravan 101.17 ASSC vs. LLC 2017-07-16 120.71 141253.221.214 80 5 122.10Hed States Maravan 5.116 vs. M. ASSC vs. LLC 2017-07-16 110.111 141.253.221.214 80 7 120.114 ASSC vs. M. LLC 2017-07-16 110.111 141.253.221.214 80 124 Numed States Maravan 47.17.14 ASSC vs. LLC 2017-07-16 177.14 141.253.221.214 80 3 124 Unled States <	2017-07-10 54-2 37.11	141.203.221.173	00	-	40	Netherlands	Amsterdam	And Stripe 11 gave some	AS2017 Mappina, LLC
att open point po	2011-01-11 99955,111,149	141.203.221.173	00	1	40	United States	Matawan	CROCKER IV. PRODUCTION	ASZUP promosia, LLC
2011-01-16 >1010 101 141 253 221 204 60 5 240 Singapote Singapote 170 171 243 221 204 80 3 124 Unled States EK Grove Village 175 171 34 253 221 204 80 5 124 Unled States EK Grove Village 175 171 34 253 221 204 80 5 124 Unled States Maawan 177 476 37 37 11 412 253 221 204 80 5 124 Unled States Maawan 177 476 37 37 11 412 253 221 204 80 5 212 Unled States Maawan 177 476 37 37 11 412 253 221 214 80 5 212 Unled States Maawan 57 117 476 37 37 11 412 253 221 214 80 5 124 Unled States Maawan 57 117 476 30 43 520 124 44 30 31 24 Unled States 50 11 176 30 43 17 117 49 412 253 221 214 80 3 124 Unled States Maawan 57 117 147 450 530 43 520 124 40 31 44 12 53 221 214 80 3 124 Unled States Maawan 57 117 147 450 530 43 520 124 40 31 42 12 16 12 10 114 12 53 221 214 80 3 124 Unled States Maawan 57 117 147 520 530 43 530 12 40 51 12 40 530 43 124 Unled States Maawan 57 117 14 50 530 43 530	at gamae	local	port	PKts	bytes	country	city	1475	ASN
2017-01-04 c, 108.104 c, 12.32.21.204 SU S 124 United States Mam Sec Cost Sec Cost ASSC Sec Cost	2017-07-18 2322:110.191	141.253.221.204	80	8	340	Singapore	Singapore	10.119 com.	ASZIS OPAPATA, LLC
2017-05-29 - 217 141 235 22104 80 5 124 Unided States Bix Grove Village ASS0 ASS0 <t< td=""><td>2017-07-04 31.2.169.194</td><td>141.253.221.204</td><td>80</td><td>3</td><td>124</td><td>United States</td><td>Miami</td><td>19 00 00 1 8 00 00 00 00 00 00 00 00 00 00 00 00 0</td><td>AS2040C 32 Avia, LLC</td></t<>	2017-07-04 31.2.169.194	141.253.221.204	80	3	124	United States	Miami	19 00 00 1 8 00 00 00 00 00 00 00 00 00 00 00 00 0	AS2040C 32 Avia, LLC
2017-07-16 a. 37.11 141253221204 80 5 121 Netherlands Amsterdam event of the second ASSC type use LC 2017-07-16 avent of the second ASSC type use LC Difference ASSC type use LC Difference ASSC type use LC 2017-07-16 avent of the second ASSC type use LC Difference ASSC type use LC 2017-07-16 avent of the second ASSC type use LC Control to the second ASSC type use LC 2017-07-16 avent to the second ASSC type use LC ASSC type use LC Control to the second ASSC type use LC	2017-06-29 2411 (21.75	141.253.221.204	80	3	124	United States	Elk Grove Village	Markey 1.75 Western.	AS2034 AS2034004 AS2034 AS2034 AS2034 AS2034 AS2034 AS2034 AS2034 AS2034 AS2034
2017-07-18 av 111 112 2212 24 80 3 124 Unled States Matawan av 111 av com AS2G* av AS2G* av AS2G* av Com AS2G* av Com AS2G* ava LLC 2017-07-16 37.11 141.253.221.214 80 3 124 Unled States Matawan 447.7 As2G* ava LLC 2017-07.65 75.116 112.25.221.214 80 3 124 Unled States Matawan 447.7 As2G* ava LLC 2017-07.65 75.163 141.253.221.214 80 3 124 Unled States Matawan 45.17 As7.7 As2G* ava LLC 2017-07.45 110.111 As2	2017-07-16 2019-37.11	141.253.221.204	80	5	212	Netherlands	Amsterdam	and 55(57.11,-32-3 jam.	AS2044 State Ada, LLC
2017-07-05 × 76.114 141 253.221 204 80 5 212 United States Matawan Control Control Association Associatiotio	2017-07-18 48 44117.149	141.253.221.204	80	3	124	United States	Matawan	· 新行17.1%公式 com.	AS200 and a LLC
2017-07-06 2 207.19 141 253 221 204 80 4 164 Unide States Los Angeles Singapore Singapore 207.7 Chrom AS3C area, BLC 2017-07-16 V-108-104 141 253 221 214 80 3 124 United States Miami 50 11.5 AS3C area, BLC 2017-07-16 V-107-11 141 253 221 214 80 3 124 United States Miami 50 11.5 Com AS3C area, BLC 2017-07-16 V-107-11 141 253 221 214 80 1 24 United States Matawan 51 11.5 Com AS3C area, BLC 2017-07-16 V-107-16 V-107-16 S0 7.5 11.4 141 253 221 21.5 80 3 124 United States Matawan 51 16 Com AS3C area, BLC 2017-07-46 V-101.91 141 253 221 215 80 3 124 United States Matawan 51 16 Com AS3C area, BLC 2017-07-46 V-101.91 141 253 221 215 80 1 40 Singapore	2017-07-05 44525, 75.114	141.253.221.204	80	5	212	United States	Matawan	(H.) 5.110 so com	OTHER
2017-07-16 S 110.19 141.253.221.214 80 7 206 Singapore 10.17 songapore Singapore Singapore 10.17 songapore Singapore 10.17 songapore Singapore <	2017-07-05 207.191	141.253.221.204	80	4	164	United States	Los Angeles	207 tr.com.	AS2000 Sickya, LLC
2017-07-04 N 1014 1124 101And States Miami 00-15 AS20 As20 <td>2017-07-18</td> <td>141.253.221.214</td> <td>80</td> <td>7</td> <td>296</td> <td>Singapore</td> <td>Singapore</td> <td>And State 10.19 Addiscom.</td> <td>AS206 Mona, LLC</td>	2017-07-18	141.253.221.214	80	7	296	Singapore	Singapore	And State 10.19 Addiscom.	AS206 Mona, LLC
2017-07-16 24 111 112 Netherlands Amsterdam 7111 (a y Lum, AS20 System LLC 2017-07-16 y 117.149 114.1283.221.214 80 1 40 United States Matawan 17.149 com AS20 ysta, LLC 2017-07-16 y 114.1253.221.214 80 3 124 United States Matawan 49.7 com OTH14 2017-06-29 y 141.253.221.215 80 3 124 United States Matawan 49.7 com OTH14 2017-07-16 y 110.19 141.253.221.215 80 3 124 United States Matawan 49.7 com AS24 ysta, LLC 2017-07-17 y 110.19 141.253.221.215 80 1 40 United States Matawan 49.7 AS24 ysta, LLC 2017-07-16 y 110.19 141.253.221.217 80 1 40 United States Matawan 47.	2017-07-04 169.194	141.253.221.214	80	3	124	United States	Miami	(5.5) >69.1 (com.	AS2010 AS2000 AS2010 AS2000 AS20000 AS20000 AS20000 AS200000 AS20000000 AS20000000000
2017-07-17 - - 117.149 141.253.221.214 80 1 40 Unide States Matawan - 17.149 - AS20 - - AS21 - AS21 - - AS21 - - AS20 - - AS20 - - AS20 -	2017-07-16 20137.11	141.253.221.214	80	3	124	Netherlands	Amsterdam	1057-17.1116923.com	AS20/13 Missiona, LLC
2017-07-16 y	2017-07-17	141.253.221.214	80	1	40	United States	Matawan	284-28-17.101 & com.	AS200
2017-07-05 249-72 141283 221214 80 3 124 United States Matawan 5.49.7	2017-07-18 30 3 117.149	141.253.221.214	80	4	168	United States	Matawan	22 (17.1%) (5) com.	AS20 AS20 ASA EAA, LLC
2017-07-06 Ser. 75.114 141.253.221.214 80 3 124 United States Matawan Mer. 75.116 OTHER 2017-07-26 S. 10.0 141.253.221.215 80 3 124 United States Los Angeles 57.16 Jon. AS2C4 yas, LLC 2017-07-04 199.194 141.253.221.215 80 3 124 United States Miami 59.15 Jon. AS2C4 yas, LLC 2017-07-14 110.191 141.253.221.216 80 1 40 United States Miami 59.14 Jon. AS2C yas, LLC 2017-07-04 159.194 141.253.221.217 80 1 40 United States Miami 29.14 Jon. AS2C yas, LLC 2017-07-04 169.194 141.253.221.217 80 1 40 Nined States Miami 29.11 Jon. AS2C yas, LLC 2017-07-16 117.140 141.253.221.217 80 1 40 United States Miami<	2017-06-29 249.72	141.253.221.214	80	3	124	United States	Matawan	19 3 49.7 m Som.	OTH(2)
2017-06-20 27 76.163 141.253.221.215 80 3 124 United States Los Angeles 75.163 om AS2C+ space 10.11 com AS2C+ space LLC 2017-07-14 110.191 141.253.221.215 80 4 108 United States Maxwan 13.17.16 space 10.11 com AS2C+ space 10.11 space 10.11 <td< td=""><td>2017-07-05 10 75.114</td><td>141.253.221.214</td><td>80</td><td>3</td><td>124</td><td>United States</td><td>Matawan</td><td>146-14-15.114 (Storm</td><td>OTHIN</td></td<>	2017-07-05 10 75.114	141.253.221.214	80	3	124	United States	Matawan	146-14-15.114 (Storm	OTHIN
2017-07-18 S 2 110.191 141.253.221.215 80 8 340 Singapore Singapore C 10.122scom AS2C s. LLC 2017-07-04 100.194 141.253.221.215 80 4 168 United States Miami 0.01.122scom AS2C s. LLC 2017-07-04 110.110 141.253.221.216 80 1 40 United States Miami 0.01.112scom AS2C s. LLC 2017-07-04 109.194 141.253.221.217 80 1 40 United States Miami 0.01.112scom AS2C s. a. LLC 2017-07-04 1.104.11 141.253.221.217 80 1 40 United States Miami 0.01.1 AS2C s. a. LLC 2017-07-16 1.171.19 141.253.221.217 80 1 40 United States Miami 7.11 m. AS2C s. a. LLC 2017-07-16 110.191 141.253.221.218 80 1 40 United States Miatavan 7.11 m. AS2C	2017-08-29 2049 75.163	141.253.221.215	80	3	124	United States	Los Angeles	20 V 5.16 3 Som	AS204 AS204 LLC
2017-07-04 169.194 141.253.221.215 80 3 124 United States Miami 40.00.117.100 AS20 49.1LC 2017-07-17 1117.140 141.253.221.215 80 4 108 United States Matavan 51.17.140 100.14 com AS20 sa.LLC 2017-07-18 110.191 141.253.221.216 80 1 40 Singapore Singapore 10.11.4 com AS20 sa.LLC at asae local port pkts bytes country city AS AS20 sa.LLC 2017-07-04 1412.53.221.217 80 1 40 Netherlands Amsterdam 7.11. ma AS20 sa.LLC 2017-07-16 171.71.40 141.253.221.217 80 1 40 Netherlands Amsterdam 7.11. ma AS20 sa.LLC 2017-07-18 110.101 141.253.221.218 80 1 40 Singapore Singapore 10.16	2017-07-18 29 2 110.191	141.253.221.215	80	8	340	Singapore	Singapore	24(5)):10.112: Graticom.	AS20409 glinuja, LLC
2017-07-17 5117.149 141.253.221.215 80 4 168 United States Matawan 51.017.15 S1.00 AS2.0 A.3.1 2017-07-14 110.191 141.253.221.216 80 1 40 Singapore Singapore 10.15 com AS2.0 A.3.1 2017-07-14 160.194 141.253.221.217 80 1 40 Singapore Singapore 10.11 com AS2.0 A.3.N 2017-07-18 2.100.191 141.253.221.217 80 1 40 Singapore Singapore 10.11 com AS2.0 A.3.1 2017-07-16 2.37.11 141.263.221.217 80 1 40 Vinted States Matawan 7.11 m AS2.0 Asa.LCC 2017-07-17 117.149 141.253.221.218 80 1 40 Singapore Singapore 10.161 com AS2.0 Asa.LCC 2017-07-17 117.149 141.253.221.218 80 1 40 United States<	2017-07-04 30 169.194	141.253.221.215	80	3	124	United States	Miami	12-12-00-16	AS20+
2017-07-18 (110.191 141.253.221.216 80 1 40 Singapore Singapore 10.15 AS2C as. at Ios ale Ios ale port pits bytes country city N AS3C as. AS3C as. 2017-07-04 -110.191 141.253.221.217 80 1 40 United States Miami AS3C AS3C as. AS3C 2017-07-16 -37.11 141.253.221.217 80 1 40 United States Miami -0.011.1 AS2C -a. LLC 2017-07-16 -37.11 141.253.221.217 80 1 40 United States Miawan -7.11 AS2C -a. LLC 2017-07-16 -110.191 141.253.221.218 80 1 40 United States Miami -7.001.1 AS2C -a. LLC 2017-07-16 -110.191 141.253.221.218 80 1 40 United States Miawan -7	2017-07-17 32 3117.149	141.253.221.215	80	.4	168	United States	Matawan	9:34417.14 (Micom	AS20 Y ANNA LLC
2017-07-04 2017-07-04 2017-07-04 2012 2012 2017 Port por	2017-07-18 2016 110.191	141.253.221.216	80	1	40	Singapore	Singapore	10.1% 20.0% com.	AS202 ASA ANA LLC
at local port pkts bytes country city bytes country city bytes com ASN 2017-07-18 - 110.19 141.253.221.217 80 1 40 Singapore Singapore - 110.11 - com AS2C - Asa 2017-07-16 - 37.11 141.253.221.217 80 1 40 United States Miami 60.15 com AS2C - a.LC 2017-07-16 - 37.11 141.253.221.217 80 1 40 United States Miatawan 1.7.1 m AS2C - a.LC 2017-07-44 -180.194 141.253.221.218 80 1 40 United States Miami 60.15 com AS2C - a.LC 2017-07-44 -180.194 141.253.221.219 80 1 40 United States Miami 60.15 com AS2C -<	2017-07-04 20:00 169 194	141.253.221.216	80	1	40	United States	Miami	2163 - 69.1+ 8-ct.com.	AS209 MARK Sia, LLC
2017-07-18 110.191 141.253.221.217 80 1 40 Singapore Singapore 101.11 com AS20 coal 2017-07-04 160.194 141.253.221.217 80 1 40 United States Miami 7.11 m AS20 coal 4.20 2017-07-16 37.11 141.253.221.217 80 1 40 Netherlands Mateval 7.11 m AS20 coal 4.20 2017-07-17 117.149 141.253.221.218 80 1 40 United States Matawan 17.11 com AS20 com AS20 </td <td>at Six-be</td> <td>local</td> <td>port</td> <td>pkts</td> <td>bytes</td> <td>country</td> <td>city</td> <td>(134)</td> <td>ASN</td>	at Six-be	local	port	pkts	bytes	country	city	(134)	ASN
2017-07-04 198 194 141.253.221.217 80 1 40 United States Miami 0.98 1 com AS20 wa.LLC 2017-07-16 37.11 141.253.221.217 80 1 40 Netherlands Amsterdam 7.11 um AS20 ya.LLC 2017-07-18 110.191 141.253.221.218 80 1 40 United States Matawan 17.11 um AS20 ya.LLC 2017-07-04 110.191 141.253.221.218 80 1 40 United States Miami X 98.11 ya.LLC 2017-07-04 110.191 141.253.221.218 80 1 40 United States Miami X 98.11 ya.LLC 2017-07-18 110.191 141.253.221.219 80 1 40 United States Miami 68.11 ya.LLC 2017-07-18 110.191 141.253.221.219 80 1 40 United States Miami 69.11 ya.LLC 2	2017-07-18	141,253,221,217	80	1	40	Singapore	Singapore	10-40 5110.115 Card com	AS20 A Statute LLC
2017-07-16 37.11 141.253.221.217 80 1 40 Netherlands Amsterdam 47.11, m. AS2C 4a, LLC 2017-07-17 117.149 141.253.221.217 80 1 40 Singapore Singapore 10.16 com AS2C 4a, LLC 2017-07-18 110.191 141.253.221.218 80 1 40 United States Maiawan 17.11 com AS2C 4a, LLC 2017-07-17 110.191 141.253.221.218 80 1 40 United States Maiawan 17.1 4.00 AS2C 4a, LLC 2017-07-04 110.191 141.253.221.219 80 1 40 United States Maiawan 17.1 4.020 AS2C 4a, LLC 2017-07-04 180.194 141.253.221.219 80 1 40 Vinted States Maiawan 17.1 4.020 AS2C 4a, LLC 2017-07-18 111.191 141.253.221.224 80 1 40 Vinted States	2017-07-04 444-169 194	141.253.221.217	80	1	40	United States	Miami	2.4.3 69.1 = 38a com.	AS20 Proving LLC
2017-07-17 117 149 141.253.221.217 80 1 40 United States Matawan 17.11 Com AS2C ya LLC 2017-07-18 110.191 141.253.221.218 80 1 40 Singapore Singapore 10.11 com AS2C ya LLC 2017-07-18 110.191 141.253.221.218 80 1 40 United States Miami 408.1 com AS2C ya LLC 2017-07-18 110.191 141.253.221.218 80 1 40 United States Miami 408.1 com AS2C ya LLC 2017-07-16 10.191 141.253.221.219 80 1 40 United States Miami 69.1 scom AS2C ya LLC 2017-07-18 117.149 141.253.221.219 80 1 40 United States Miami 69.1 com AS2C ya LLC 2017-07-18 110.191 141.253.221.224 80 1 40 United States <td< td=""><td>2017-07-16 2032/37 11</td><td>141 253 221 217</td><td>80</td><td>1</td><td>40</td><td>Netherlands</td><td>Amsterdam</td><td>54 10 17 11 Storem</td><td>AS20 ANA LLC</td></td<>	2017-07-16 2032/37 11	141 253 221 217	80	1	40	Netherlands	Amsterdam	54 10 17 11 Storem	AS20 ANA LLC
2017-07-18	2017-07-17 34 35 117 149	141 253 221 217	20		40	United States	Matawan	25/50-17 12-3 \$90 com	AS20er Mirking LLC
2017-07-04	2017-07-18 346 259110 101	141 253 221 218	20		40	Singapore	Singanore	ANCHIO 10 Million	AS2[AS2[AS2] AS2[ASA
2017-07-17 117.149 141.253.221.218 80 1 40 United States Matawan 17.1 A.com AS2C	2017-07-04 20-53-160 104	141 253 221 212	20	-	40	United States	Miami	HANDER BO 1 Stand - com	AS2000 Standard LLC
2017-07-18 110.191 141.253.221.219 80 1 40 Singapore Singapore 10.11 Singapore	2017-07-17	141 253 221 218	20		40	United States	Matawap	Variation 17 1 section open	AS2Create Include LLC
2017-07-04 169.194 141.253.221.219 80 1 40 United States Miami 60.1% </td <td>2017-07-18 153 44 110 101</td> <td>141 252 221 210</td> <td>00</td> <td>1.14</td> <td>40</td> <td>Singapore</td> <td>Singanora</td> <td>ALSE TID THE STOOT</td> <td>45202/05/361/06 11 C</td>	2017-07-18 153 44 110 101	141 252 221 210	00	1.14	40	Singapore	Singanora	ALSE TID THE STOOT	45202/05/361/06 11 C
2017-07-18 37.11 141.253.221.219 80 1 40 Ontice dates Main To do 1, see 3, other AS22, sea 1, LC 2017-07-18 37.11 141.253.221.219 80 1 40 Netherlands Amsterdam 5 67.11, sea 3, m AS22, sea LLC 2017-07-18 110.191 141.253.221.224 80 1 40 Singapore Singapore 10.15, seam AS22, sea, LLC 2017-07-18 110.191 141.253.221.224 80 1 40 United States Miami 60.15, seam AS22, sea, LLC 2017-07-04 169.194 141.253.221.224 80 1 40 United States Miami 60.15, seam AS22, sea, LLC 2017-07-16 37.11 141.253.221.224 80 1 40 United States Matawan 7.11, seam AS22, sea, LLC 2017-07-18 37.11 141.253.221.224 80 1 40 United States Matawan 7.11, seam AS22, sea, LLC 2017-07-18 110.191	2017-07-04 124-2(180-104	141 252 224 240	00		40	United Chater	Miami	Anada BD 1000 Adams	ASSCIEVE ASSCIEVE
2017-07-16 37.11 14.253.221.24 80 1 40 Vertications Anternations Anternatio	2017-07-04 //20197-14	141.203.221.218	00	-	40	Mathematicales	American	Carden on register com	ADDOLLAR STORAGE LLC
2017-07-18 -117.149 141.253.221.224 80 1 40 Onned States Mianwain Act 17.15 Act 17.15 <td>2017-07-10 22 20 31.11</td> <td>141.203.221.218</td> <td>00</td> <td></td> <td>40</td> <td>Netherlands</td> <td>Amsterdam</td> <td>a togor negative and</td> <td>Abdon and a LLC</td>	2017-07-10 22 20 31.11	141.203.221.218	00		40	Netherlands	Amsterdam	a togor negative and	Abdon and a LLC
2017-07-18	2017-07-18 14 31-117.149	141.203.221.219	80	1	40	United States	Matawan	746.45-17.199.658 com.	AS200 (SC) (Magaal LUC
2017-07-04 > 109.194 141.253.221.224 80 1 40 United States Mamin 64.015 Accord AS2C Add LLC 2017-07-06 37.11 141.253.221.224 80 1 40 United States Attanta 41.11 41.11 AS2C 40.4 LLC 2017-07-16 37.11 141.253.221.224 80 1 40 Netherlands Amsterdam 7.11 m AS2C 40.4 LLC 2017-07-17 4.11.11 141.253.221.224 80 1 40 United States Matawan 7.11 m AS2C 40.4 LLC 2017-07-18 -110.191 141.253.221.225 80 1 40 Singapore Singapore -10.10 AS2C 40.4 LCC 2017-07-16 -37.11 141.253.221.225 80 1 40 Netherlands Amsterdam -7.11 AS2C 40.4 LCC 2017-07-17	2017-07-18 22.22 110.191	141.253.221.224	80		40	Singapore	Singapore	and a 10.19 we com	ASZLANT SAMA B. LLL
2017-06-29 23 241.53 141.253.221.224 80 1 40 United States Attanta Additional Addited adited adited adited adited adited adited adited adited adi	2017-07-04	141.253.221.224	80	1	40	United States	Miami	State OU. 1 Sector Com.	ASZLAN STANDARA, LLC
2017-07-16 2017-07-16 2017-07-16 2017-07-17 111.253.221.224 80 1 40 Netherlands Amsterdam 7.11 rm AS20 As20<	2017-06-29 28:32-214.153	141.253.221.224	80	1	40	United States	Atlanta	104 (15:14.1 (14:0) com.	AS204 Melauritya, LLC
2017-07-17 Av. 117.149 141.253.221.224 80 1 40 United States Matawan Av. 17.146 AS20 Available 2017-07-18 4110.191 141.253.221.225 80 1 40 Singapore Singapore n10.15 As20 As	2017-07-16	141.253.221.224	80	1	40	Netherlands	Amsterdam	145 94 7.11 ASP Sam.	AS20 AS20 AS A LLC
2017-07-18 4-10.191 141.253.221.225 80 1 40 Singapore Singapore Art 10.10 AS2Let voltage AS2L	2017-07-17 10:05 117.149	141.253.221.224	80	1	40	United States	Matawan	server 17.1 style a com	AS204 AS204 Activity Research
2017-07-04 See 169.194 141.253.221.225 80 1 40 United States Miami See 169.194 AS2C Asa LLC 2017-07-16 37.11 141.253.221.225 80 1 40 Netherlands Amsterdam See 7.11, See com AS2C	2017-07-18 2010.191	141.253.221.225	80	1	40	Singapore	Singapore	And An 10.10 Selecom	AS208 AS248 AS248, LLC
2017-07-16 37.11 141.253.221.225 80 1 40 Netherlands Amsterdam 37.11 AS2C 34.25 AS2C 34.25 Association	2017-07-04 3450 169.194	141.253.221.225	80	1	40	United States	Miami	2012 10 69.16 Victor	AS20 AS20 ANA, LLC
2017-07-17 3 11 141.253.221.225 80 1 40 United States Matawan 41.17.14 AS2 As2 As2 As1 at +5.57e local port pkts bytes country city ASN 2017-07-18 4.110.191 141.253.221.234 80 1 40 Singapore Singapore Singapore Singapore 10.10.10.10.10.10.10.10.10.10.10.10.10.1	2017-07-16 37.11	141.253.221.225	80	1	40	Netherlands	Amsterdam	156-207.11 (Section.	AS20AU SUBAR LLC
at byse local port pkts bytes country city ASN 2017-07-18 54 110.191 141.253.221.234 80 1 40 Singapore Singapore Singapore Singapore 10.10.10.10.10.10.10.10.10.10.10.10.10.1	2017-07-17 34 117.149	141.253.221.225	80	1	40	United States	Matawan	17.14 com	AS200 AS200 AS
2017-07-18 36 to 110.191 141.253.221.234 80 1 40 Singapore	at style	local	port	pkts	bytes	country	city	14	ASN
2017-07-04 Acroscol 141.253.221.234 80 1 40 United States Miami 352.560.12 cm AS20.5 cm<	2017-07-18 36 40 110.191	141.253.221.234	80	1	40	Singapore	Singapore	5 x 2 x 10.1(* 1) y com.	AS20 AS2 ASIA LLC
2017-07-18 2017-17-149 141.253.221.234 80 1 40 United States Matawan 2017-07-18 Company Company AS20-12 2017-07-18	2017-07-04 2 169 194	141.253.221.234	80	1	40	United States	Miami	9572-7-89.1524 com.	AS20
	2017-07-18 117.149	141.253.221.234	80	1	40	United States	Matawan	17.14 x com	AS20 AS20 ANA LLC

© 2020 AETHIS sa/nv Belgium Document version 1.0, 2020-12 -

All rights reserved -Open Source Apache License v2.0 trafMon Use Case 3: Security Auditing Page: 19/58



Only the first, the fifth and the last pages of the query result are shown above, to demonstrate the span of own systems actually reached.

When looking, for instance, at the volumes shown by some remote systems from France and Germany (that are in the red rectangle of the second image above) there seems to be a more significant volume exchanged. So, we need to further analyse the TCP connection counters related to the entire traffic for the available time span of observations (a bit more than July 2017).

We can then sum-up the daily traffic (packets and bytes) of each (uni-directional or bi-directional) flow with, for instance, the remote system from Frankfurt, in order to ensure that it isn't a normally behaving peer.

Viii 10 10 27 Viii 10 10 27 Viii 10 10 10 10 Viii 10 10 10 10 Viii 10 10 10 10 10 Viii 10 10 <t< th=""><th>WHERE flowID LIKE</th><th>.176.16</th><th>4%:8</th><th>80_%</th><th>GROUP BY rangeStart, flowID ORDER BY rangeStart, flo</th></t<>	WHERE flowID LIKE	.176.16	4%:8	80_%	GROUP BY rangeStart, flowID ORDER BY rangeStart, flo
No. 10. 0 Besugnet 41 2932 11.03.0 gu umm N17070 100000 10 276 N17. 0 Besugnet 42 2932 11.03.0 gu umm N17070 100000 6 000 N17. 0 Besugnet 42 2932 11.03.0 gu umm N17070 100000 6 000 N17. 0 Besugnet 42 2932 11.03.0 gu umm N17070 100000 6 000 N17. 0 Besugnet 41 2932 11.03.0 gu umm N17070 200000 6 000 N17. 0 Besugnet 41 2932 11.03.0 gu umm N17070 200000 6 000 N17. 0 Besugnet 41 2932 11.03.0 gu umm N17070 200000 6 000 N17. 0 Besugnet 41 2932 11.03.0 gu umm N17070 200000 6 000 N17. 0 Besugnet 41 2932 11.03.0 gu umm N17070 200000 6 000 N17. 0 Besugnet 41 2932 11.03.0 gu umm N17070 200000 6 000 N17. 0 Besugnet 42 293 11.03.0 gu umm N17070 200000 6 000 N17. 0 Besugnet 223 11.03.0 gu umm N17070 200000 6 000 N170 10 Besugnet 223 11.03.0 gu umm N17070 200000 6 000 N170 10 Besugnet 223 11.03.0 gu umm N17070 200000 6 000 N170 10 Besugnet 223 11.03.0 gu umm N17070 200000 6					
	22-21176.164:high<>141.253.221.16:80_tcp_trafmo	2017-07-01 00:00:00	11	2724	
	25:52, 176, 164; high>141, 253, 218, 52:80 top_trafmon	2017-07-01 00:00:00	15	1044	
10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10	176.184 high>141.253.221.16:80 top trafmon	2017-07-01 00:00:00	5	626	
01110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 0110 <td>176 164 biob<141 253 218 52 80 top trafmon</td> <td>2017-07-02 00:00:00</td> <td>61</td> <td>81123</td> <td></td>	176 164 biob<141 253 218 52 80 top trafmon	2017-07-02 00:00:00	61	81123	
1000000000000000000000000000000000000	201 176 164 higher 141 253 221 16:80 ten trafmon	2017-07-02 00:00:00	8	2082	
1011010100000000000000000000000000000	+0.55 178 184 high = 141 253 218 52 20 ton trafmo	2017-07-02 00:00:00	20	82242	
International and the second	176 176 184 bioban 141 253 211 18-90 too trafma	2017-07-02 00:00:00	11	2870	
Numerical Numerical Numerical Numerical Numerical No Numerical Nume	<pre>Sign: 10.104.mgn </pre> 141.208.221.10.80_10p_trainio	2017-07-02 00.00.00	11	2010	
		rangestart	packets	bytes	1
	56.39 170.104.high=141.203.218.02.80_cp_traimon	2017-07-02 00:00:00	20	1120	
Angel 11: Bis Hamper 14: 20: 21: Big tag partners. 2017;47:10:00000 24: 2017;40: 201	21. 10. 104 nign=141.203.221.10.80_tcp_tratmon	2017-07-02 00:00:00	0	800	
0.0011701 (0.01.mgs. prime. 0017-07-08 000000 00 104999 0.0011701 (0.01.mgs. prime. 0017-07-08 000000 00 10399 0.0011701 (0.01.mgs. prime. 0017-07-08 000000 01 10399 0.0011701 (0.01.mgs. prime. 0017-07-08 000000 102 10399 0.0011701 (0.01.mgs. prime. 0017-07-08 000000 12 10399 0.0011701 (0.01.mgs. prime. 0017-07-04 000000 10 103999 0	Prov. 176.164:high<141.253.218.52:80_top_tratmon	2017-07-03 00:00:00	285	399329	
Calo 174 188 to spin-141.283 188 to 280 to 124 1767 to 300 000 00 Calo 174 776 000 000 0 Calo 174 7776 0000 000 0 Calo 174 776 000 000 0 Calo 174 776 000 000 0	v: 2.176.164.high<141.253.221.16.80_tcp_trafmon	2017-07-03 00:00:00	36	12492	
Appl. 10 detemptor 141.322.318.22.00 µu _thrman. 2017-07-08 00000 124 170 Appl. 170 164.4120-141.223.318.22.00 µu _thrman. 2017-07-08 00000 124 170 Appl. 170 164.4120-141.223.318.22.00 µu _thrman. 2017-07-08 00000 124 170 Appl. 170 164.4120-141.223.118.22.00 µu _thrman. 2017-07-08 00000 124 170 Appl. 170 164.4120-141.223.118.22.00 µu _thrman. 2017-07-08 00000 124 170 Appl. 170 164.4120-141.223.118.22.00 µu _thrman. 2017-07-04 00000 124 170 Appl. 170 164.4120-141.223.211.82.00 µu _thrman. 2017-07-04 00000 124 170 Appl. 170 164.4120-141.223.211.82.00 µu _thrman. 2017-07-04 00000 124 170 Appl. 171 164.4120-141.223.211.82.00 µu _thrman. 2017-07-04 00000 124 170 Appl. 171 170 <t< td=""><td>k;;;k%.176.164:high<>141.253.218.52:80_tcp_trafmo</td><td>2017-07-03 00:00:00</td><td>409</td><td>406947</td><td></td></t<>	k;;;k%.176.164:high<>141.253.218.52:80_tcp_trafmo	2017-07-03 00:00:00	409	406947	
	た。計算、176.164:high<>141.253.221.16:80_tcp_trafmo	2017-07-03 00:00:00	68	16322	A delbi / localbost / trafMon / insttable agor 1d phpMvAdmin 401015 - Google -
	* 176.164:high>141.253.218.52:80_tcp_trafmon	2017-07-03 00:00:00	124	7618	DWW service and the service of the s
01/01/17.0144/spor411.3232108.218.01/6.2 101/07.074.000000 104 138283 01/01/17.0144/spor411.3232108.228.01/6.2 201/07.074.000000 140 138484 01/01/17.0144/spor411.2332108.28.02 101/07.074.000000 140 138484 01/01/17.0144/spor411.233210.28.02 101/07.074.000000 140 138484 01/01/17.0144/spor411.233210.28.02 101/07.074.000000 10 1216 01/01/17.0144/spor411.233210.28.02 102/07.074.000000 10 1216 01/01/17.0144/spor411.233210.28.02 102/07.074.000000 20 22383 01/01/18.04/spor411.233210.28.04 102/07.074.0000000 20 2238 01/01/18.04/spor411.233212.02.04 102/07.074.0000000 20 2238 01/01/18.04/spor411.233212.02.04 102/07.074.0000000 20 2238 01/01/18.04/spor411.233212.02.04 102/07.074.0000000 20 2384 01/01/18.04/spor411.233212.02.04 102/07.074.0000000 20 2384 01/01/18.04/spor411.2332.02.02.04 101/07.074.0000000 20 2384 01/01/18.04/spor411.2332.02.02.04 101/07.074.0000000 20 2184 01/01/18.04/spor411.2332.02.02.04<	a 176.164:high>141.253.221.16:80_tcp_trafmon	2017-07-03 00:00:00	32	3830	A Not secure delhi/phpmyadmin/querywindow.php?token=30ae7776305d46e8ba6
Sult 3184-spin-t412323221 80.00 top tarkeno. 2017-0740 00000 140 1498 Sult 318 52.00 top tarkeno. 2017-0740 00000 24 Sult 318 52.00 top tarkeno. 2017-0740 00000 25 Sult 318 52.00 top tarkeno. 2017-074 000000 2 Sult 318 52.00 top tarkeno. 201	176.164:high<141.253.218.52:80_tcp_trafmon	2017-07-04 00:00:00	96	133823	
Prog. 17.8 144 mijore 141 232 218 22.01, 201, 2017.07.4000000 140 1284 mijore 141 232 218 22.01, 201, 2017.07.4000000 24 1285 218 22.01, 201, 2017.07.4000000 24 1285 218 22.01, 2017.07.4000000 24 1285 218 22.01, 2017.07.4000000 24 1285 218 22.01, 2017.07.4000000 24 1285 218 22.01, 2017.07.4000000 24 1285 218 22.01, 2017.07.4000000 24 1285 218 22.01, 2017.07.4000000 24 1285 218 22.01, 2017.07.4000000 24 1285 211.000 up tafmon. 2017.07.4000000 24 1285 22.11.000 up tafmon. 2017.07.4000000 25 1486 mijor 141.235 218 22.00 up tafmon. 2017.07.41.4000000 25 1486 mijor 141.235 218 22.00 up tafmon. 2017.07.41.4000000 25 1486 mijor 141.235 218 22.00 up tafmon. 2017.07.41.4000000 25 1486 mijor 141.235 218 22.00 up tafmon. 2017.07.41.4000000 2017.07.41.4000000 2017.07.41.4000000 25 1486 mijor 141.235 218 22.00 up tafmon. 2017.07.41.4000000 2017.07.41.	And A 176.184 high<141.253.221.16:80_tcp_trafmon	2017-07-04 00:00:00	12	4176	📓 SQL 👼 Import files 📳 SQL history
	176.164:high<>141.253.218.52:80_tcp_trafmo	2017-07-04 00:00:00	140	136435	Run SQL query/queries on database trafMon:
Comparison 112:00:00:00:00:00:00:00:00:00:00:00:00:00	21 2 176.184 high<>141.253.221.16:80_tcp_trafmo	2017-07-04 00:00:00	22	5392	
mage:Lat 176.194-mpro-141.283.216.82.80_top_trafmon. 2017-07-80 000000 24 288372 2017-07-80 000000 24 288372 2017-07-14 000000 25 288372 2017-07-14 000000 24 2017-07-14 000000 25 288372 2017-07-14 000000 25 288372 2017-07-14 000000 25 1884 2017-07-14 000000 25 1884 2017-07-14 000000 26 1884 2017-07-16 000000 26 1884 2017-07-16 000000 26 1884 2017-07-16 000000 26 1884 2017-07-16 000000 26 2017-07-16 000000 26 2017-07-16 000000 2017-07-20 0000000	2.176.164:high>141.253.218.52:80_tcp_trafmon	2017-07-04 00:00:00	44	2612	Caluma
222 3176 104 https://14.253.216.82.80_tp_trainer. 2017-07-46 00:000 24 8330 2017-07-46 00:000 20 228872 2017-07-46 00:000 44 6532 2017-07-46 00:000 14 20532 2017-07-46 00:000 14 20532 2017-07-46 00:000 11 2074 2017-07-46 00:000 12 1000 2017-07-46 00:000 12 21438 2017-07-46 00:000 12 2014 2017-07-46 00:000 12 2014 2017-07-2000:000 12 2014 2017-07-2000:000 12 2014 2017-07-2000:000 12 2014 2017-07-2000:000 12 2014 2017-07-2000:000 12 2014 2017-07-2000:000 12 2014 2017-07-2100:000 12 2014 2017-07-2100:000 12 2014 2017-07-2100:000 12 2017-000 2017-07-2100:000 12 2017-000 2017-0	176.164.high>141.253.221.16.80_tcp_trafmon	2017-07-04 00:00:00	10	1216	1 SELECT flowid, rangestart, sum(population) as packets, sum(sum) as bytes FROM lpsztable aggr 10 WHERE flowID like 705,558,176.1648:80,X GROUP flowID
178.194.https:/141.253.218.52.01.jp.trafmon. 2017-07-06 000000 24 9326 178.194.https:/141.253.218.52.01.jp.trafmon. 2017-07-06 000000 95 9306 178.194.https:/141.253.218.52.00_jp.trafmon. 2017-07-16 000000 84 96536 178.194.https:/141.253.218.52.00_jp.trafmon. 2017-07-16 000000 8 9204 178.194.https:/141.253.218.52.00_jp.trafmon. 2017-07-16 000000 8 6204 178.194.https:/141.253.218.52.00_jp.trafmon. 2017-07-16 000000 8 6204 178.194.https:/141.253.218.52.00_jp.trafmon. 2017-07-16 000000 8 6204 178.194.https:/141.253.218.52.00_jp.trafmon. 2017-07-16 000000 8 68107 178.194.https:/141.253.218.52.00_jp.trafmon. 2017-07-16 000000 8 68107 178.194.https:/141.253.218.52.00_jp.trafmon. 2017-07-16 000000 7 69738 178.194.https:141.253.218.52.00_jp.trafmon. 2017-07-1	176.164:high<141.253.218.52:80 top trafmon	2017-07-05 00:00:00	202	283372	BY rangeStart , flowID ORDER BY rangeStart , flowID rangeStart
0:1178.194.htgh=0141.253.218.52.00_tp_tafmo. 2017-07-05 00000 297 28732 0:1176.194.htgh=141.253.221.630_tp_tafmo. 2017-07-05 00000 44 10686 1176.194.htgh=141.253.221.52.00_tp_tafmo. 2017-07-05 00000 64 65330 1176.194.htgh=141.253.221.52.00_tp_tafmo. 2017-07-05 00000 6 65330 1176.194.htgh=141.253.221.630_tp_tafmo. 2017-07-16 000000 6 20544 1176.194.htgh=141.253.221.630_tp_tafmo. 2017-07-14 000000 6 20544 1176.194.htgh=141.253.221.1630_tp_tafmo. 2017-07-14 000000 12 28643 1176.194.htgh=141.253.221.1630_tp_tafmo. 2017-07-14 000000 5 62034 1176.194.htgh=141.253.221.1630_tp_tafmo. 2017-07-16 000000 5 62034 1176.194.htgh=141.253.221.1630_tp_tafmo. 2017-07-16 000000 5 20234 1176.194.htgh=141.253.221.1630_tp_tafmo. 2017-07-16 000000 5 20234	176.164.high<141.253.221.16.80 top trafmon	2017-07-05 00:00:00	24	8328	lower
176.164.mgh<141.253.218.22.01.cg_tafmen	176.164.high<>141.253.218.52.80 top trafmo	2017-07-05 00:00:00	297	288732	upper
178.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.05 00.000.00 02 228 176.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.05 00.000.00 20 228 176.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.07.000.000 8 265 176.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.14 00.0000 8 2654 176.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.14 00.0000 8 2654 176.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.14 00.0000 1 2674 176.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.14 00.0000 6 2624 176.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.14 00.0000 6 2624 176.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.16 00.0000 7 97583 176.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.20 00.0000 7 97583 176.184.mjbr/141.253.218.52.00_top_trafmon 2017.07.20 00.0000	222176 184 high<>141 253 221 18:80 top trafmo	2017-07-05 00:00:00	44	10616	minimum
176 144.ges/21 141 252 176	178 184 highs141 253 218 52 80 ten trafmon	2017-07-05 00:00:00	05	5360	average
rangestrit packet bytes 176 164 high 142.83.218.82.80 log_trafmon 2017.07.14 00:000 48 06558 176.184 high 142.83.211.82.02 log_trafmon 2017.07.14 00:000 73 0707 176.184 high 143.253.211.82.82.100 log_trafmon 2017.07.14 00:000 73 0707 176.184 high 143.253.211.82.00 log_trafmon 2017.07.14 00:000 5 0205 176.184 high 143.253.211.82.00 log_trafmon 2017.07.14 00:000 5 0205 176.184 high 143.253.211.82.00 log_trafmon 2017.07.14 00:000 5 0205 176.184 high 143.253.211.82.00 log_trafmon 2017.07.16 00:000 6 88883 176.184 high 143.253.211.82.00 log_trafmon 2017.07.16 00:000 1 2068 176.184 high 143.253.211.82.00 log_trafmon 2017.07.16 00:000 1 2068 176.184 high 143.253.211.82.00 log_trafmon 2017.07.16 00:000 5 818 176.184 high 143.253.211.82.00 log_trafmon 2017.07.20 00:000 6 818 176.184 high 143.253.211.82.00 log_trafmon 2017.07.20 00:00	4 1/200 176 184 high 141 253 221 18 80 ten trafmon	2017-07-05 00:00:00	20	2288	population
International and the second secon		connectort	nackate	butac	sum
2017-07-14 00:000 8 00000 11 267 1176.184-high<141.253.218.252.01.68.0 top_trafmo. 2017-07-14 00:000 73 07977 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-14 00:000 8 0000 11 2674 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-14 00:000 6 6 050 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-14 00:000 6 6 050 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-14 00:000 6 6 050 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-14 00:000 6 8 08813 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-16 00:000 8 8 08813 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-16 00:000 11 2686 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-16 00:000 70 67588 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-16 00:000 70 67588 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-16 00:000 70 67588 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-20 00:000 0 5 2021 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-20 00:000 0 5 2021 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-20 00:000 0 5 2021 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-20 00:000 0 5 2025 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-20 00:000 0 5 2025 1176.184-high<141.253.218.52.01.top_trafmo. 2017-07-21 00		rangestart	packets	bytes	sumOfSquares
Victor 10: 164:mgn<141.252.211.1630_tcp_trafmo.	<pre>>> provide the second sec</pre>	2017-07-14 00:00:00	48	00039	(SELECT) (SELECT) (INSERT) (UPDATE) (DELETE) (Clear)
176:164:high<>141:253:218:52:80_icp_trafmo. 2017-07:14:00:00:00 125:164:high 1276:164:high 1276:164:high 1278:164:high 1278:164:	y 2/12, 1/6.164:high<141.253.221.16:80_tcp_tratmon	2017-07-14 00:00:00	0	2054	
And Proceedings of the second	34.176.164:high<>141.253.218.52:80_tcp_trafmo	2017-07-14 00:00:00	73	67977	
170: 104-high=141.253.218.52.00_tcp_trafmon. 2017-07-14 00:00:00 5 170: 104-high=141.253.218.52.00_tcp_trafmon. 2017-07-16 00:00:00 61 66883 170: 104-high=141.253.218.52.00_tcp_trafmon. 2017-07-16 00:00:00 61 2017-07-16 00:00:00 6 2017-07-16 00:00:00 6 2017-07-16 00:00:00 6 2017-07-16 00:00:00 6 2017-07-16 00:00:00 6 2017-07-16 00:00:00 7 170: 104-high=141.253.218.52.00_tcp_trafmon. 2017-07-16 00:00:00 1 2017-07-16 00:00:00 1 2017-07-16 00:00:00 1 2017-07-16 00:00:00 1 2017-07-16 00:00:00 1 2017-07-16 00:00:00 1 170: 104-high=141.253.218.52.80_tcp_trafmon. 2017-07-16 00:00:00 2 170: 104-high=141.253.218.52.80_tcp_trafmon. 2017-07-16 00:00:00 5 2017-07-16 00:00:00 5 2017-07-16 00:00:00 5 2017-07-20 00:00:00 7 170: 104-high=141.253.218.52.80_tcp_trafmon. 2017-07-20 00:00:00 7 2017-07-20 00:00:00 7 170: 104-high=141.253.218.52.80_tcp_trafmon. 2017-07-20 00:00:00 7 2017-07-20 00:00:00 7 170: 104-high=141.253.218.52.80_tcp_trafmon. 2017-07-20 00:00:00 7 2017-07-20 00:00:00 7 170: 104-high=141.253.218.52.80_tcp_trafmon. 2017-07-20 00:00:00 5 2005	x4/34.176.184.high<>141.253.221.16.80_tcp_trafmo	2017-07-14 00:00:00	11	2674	
x176.194.high<2141.253.221.68.00 top_trafmon.	\$2,59,176.164:high>141.253.218.52:80_tcp_trafmon	2017-07-14 00:00:00	25	1438	
with y 176.164 high<141.253.218.52.80_tsp_traffmon	176.164.high>141.253.221.16:80_tcp_trafmon	2017-07-14 00:00:00	5	620	De act evenuels this avery from evicide the window
Market 176.104-high<141.253.221.10:80_tep_trafmon	176.164:high<141.253.218.52:80_tcp_trafmon	2017-07-16 00:00:00	61	86883	Delimiter :] Z Show this query here again
215:176.184.high<>141.253.218.528.0_top_trafmo 2017-07-18 00:00:00 11 2068 217.76.184.high 2017-07-18 00:00:00 2 1314 217.76.184.high 218.52.20_top_trafmo 2017-07-18 00:00:00 2 1314 217.76.184.high 218.52.80_top_trafmo 2017-07-18 00:00:00 2 1314 217.76.184.high 11.253.221.16.80_top_trafmo 2017-07-18 00:00:00 5 616 217.76.184.high 211.253.221.05.00_top_trafmo 2017-07-20 00:00:00 5 2021 177.6.184.high 218.25.28.00_top_trafmo 2017-07-20 00:00:00 67 89061 217.67.184.high 218.52.80_top_trafmo 2017-07-20 00:00:00 67 89061 217.67.184.high 218.52.80_top_trafmo 2017-07-20 00:00:00 67 89061 217.67.184.high 218.52.80_top_trafmo 2017-07-20 00:00:00 68 865 217.61.84.high 218.21.85.280_top_trafmo 2017-07-21 00:00:00 64 81284 217.61.84.high 218.23.18.52.80_top_trafmo 2017-07-21 00:00:00 5 2005 217.61.84.high 218.25.25.25.20_top_trafmo 2017-07-21 00:00:00 5 200	k*r * 176.164:high<141.253.221.16:80_tcp_trafmon	2017-07-16 00:00:00	6	2082	G
N2::::::::::::::::::::::::::::::::::::	176.164:high<>141.253.218.52:80_tcp_trafmo	2017-07-16 00:00:00	83	88197	
3.5 176.164.high>141.253.218.52.80_top_trafmon. 2017.07.16 00.00.00 5 616 4.176.164.high>141.253.218.52.80_top_trafmon. 2017.07.20 00.00.00 5 2021 176.164.high>141.253.218.52.80_top_trafmon. 2017.07.20 00.00.00 5 2021 176.164.high>141.253.218.52.80_top_trafmon. 2017.07.20 00.00.00 5 2021 176.164.high<141.253.218.52.80_top_trafmon.	3. p(x, 176.164:high⇔141.253.221.16:80_tcp_trafmo	2017-07-16 00:00:00	11	2698	
Xi, Yi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-20 00:00:00 5 618 Xi, Yi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-20 00:00:00 6 2021 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-20 00:00:00 6 2021 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-20 00:00:00 6 2021 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-20 00:00:00 11 2676 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-20 00:00:00 11 2676 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-20 00:00:00 11 2676 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-20 00:00:00 6 655 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-21 00:00:00 6 655 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-21 00:00:00 5 2005 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-21 00:00:00 5 2005 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-21 00:00:00 5 2005 Xi 70, 184, high<>141,253,221,16:80,tcp_trafmon. 2017-07-21 00:00:00 5 2017	176.184:high>141.253.218.52:80_tcp_trafmon	2017-07-16 00:00:00	22	1314	
176.184.high<141.253.218.52.80_top_trafmon	2.5.176.184:high>141.253.221.16:80_tcp_trafmon	2017-07-16 00:00:00	5	616	
176.184.high<141.253.221.16.80_tp_trafmon	176.164.high<141.253.218.52.80_tcp_trafmon	2017-07-20 00:00:00	70	97538	
176.184.high<>141.253.218.52.80_top_trafmon 2017-07-20 00:00:00 97 99051 1776.184.high<>141.253.221.18:30_top_trafmon 2017-07-20 00:00:00 1 2676 1776.184.high>>141.253.221.18:30_top_trafmon 2017-07-20 00:00:00 6 655 1776.184.high>>141.253.221.18:30_top_trafmon 2017-07-20 00:00:00 6 9254 1776.184.high>>141.253.221.18:30_top_trafmon 2017-07-20 00:00:00 6 9254 1776.184.high>>141.253.221.18:30_top_trafmon 2017-07-20 00:00:00 6 9254 1776.184.high<>141.253.221.52:80_top_trafmon 2017-07-20 00:00:00 6 92734 1776.184.high<>141.253.218.52:80_top_trafmon 2017-07-21 00:00:00 12 2077 1776.184.high<>141.253.218.52:80_top_trafmon 2017-07-21 00:00:00 8 92734 1776.184.high<>141.253.218.52:80_top_trafmon 2017-07-21 00:00:00 12 2077 1776.184.high<>141.253.218.52:80_top_trafmon 2017-07-21 00:00:00 12 2077 1776.184.high<>141.253.218.52:80_top_trafmon 2017-07-21 00:00:00 12 2077 1176.184.high<>141.253.218.52:80_top_trafmon 2017-07-21 00:00:00 12 2077 1176.184.high<>141.253.218.52:80_top_trafmon<	176.164 high<141.253.221.16:80_tcp_trafmon	2017-07-20 00:00:00	5	2021	
176.184-high<>141.253.221.16:80_top_trafmon 2017-07-20 00:00:00 11 2676 176.184-high>141.253.216:52.80_top_trafmon 2017-07-20 00:00:00 27 1513 176.184-high>141.253.216:52.80_top_trafmon 2017-07-20 00:00:00 6 855 176.184-high>141.253.216:52.80_top_trafmon 2017-07-21 00:00:00 64 855 176.184-high<141.253.216:52.80_top_trafmon	176.164:high<>141.253.218.52:80 tcp trafmo	2017-07-20 00:00:00	97	99051	
176.184.high>141.253.218.52.80_top_trafmon 2017-07-20 00:00:00 27 1513 176.184.high>141.253.221.85.280_top_trafmon 2017-07-20 00:00:00 6 855 176.184.high<141.253.221.85.280_top_trafmon	176.164:high<>141.253.221.16:80 top trafmo	2017-07-20 00:00:00	11	2676	
x1176.184.high<141.253.221.16.80_top_trafmon.	176.164:high>141.253.218.52:80 ten trafmon	2017-07-20 00:00:00	27	1513	
An 176.164.high<141.253.218.52.80_top_trafmon	2 Xi 176 184 biobo141 253 221 18:50 ton traimon	2017-07-20 00-00-00	8	855	
176.184.high<141.253.221.68.00_top_trafmon.	74 (2) 178 184 biobc141 252 210 52 00 to to to to	2017 07 21 00-00-00	84	01284	
2017-07-21 00:00-00 10 2017-07-21 00:00:00 10 2003 2015 2015 176.184-high<>141.253.218.52:80_top_trafmon 2017-07-21 00:00:00 89 92734 2015 2017-07-21 00:00:00 11 2677 2015 2017-07-21 00:00:00 25 1450	repart ro. 104.11gths r41.203.210.02.00_(Cp_tramon	2017-07-21 00:00:00	6	91264	
rangestart packets bytes 176.164.high⇔141.253.218.52:80_top_trafmon 2017-07-21 00:00:00 89 92734 2017-07-21 00:00:00 11 2677 2017.07.21 00:00:00 25 1450	141.253.221.16:80_tcp_trafmon	2017-07-21 00:00:00	5	2005	
43.22, 176.164-high≪141.253.218.52:80_tcp_trafmo2017-07-21.00:00:00 89 92734 22, 176.164-high≪141.253.221.16:80_tcp_trafmo2017-07-21.00:00:00 11 2677 22, 176.164-high=141.253.218.52:80_tcp_trafmon2017-07-21.00:00:00 25 1450	es.	rangestart	packets	bytes	
\[\laphi_176.164\:high<>\141.253.221.18.30_tcp_trafmo 2017-07-21 00:00:00 11 2677 \[\laphi_176.164\:high>\141.253.218.52:80_tcp_trafmo 2017-07-21 00:00:00 25 1450 \] \[A 2 176.164:high<>141.253.218.52:80_tcp_trafmo	2017-07-21 00:00:00	89	92734	
www.176.184.high>141.253.218.52:80_top_trafmon 2017-07-21 00:00:00 25 1450	24.176.184 high<>141.253.221.16:80_tcp_trafmo	2017-07-21 00:00:00	11	2677	
	\$2.176.164:high>141.253.218.52:80_tcp_trafmon	2017-07-21 00:00:00	25	1450	

© 2020 AETHIS sa/nv Belgium Document version 1.0, 2020-12

All rights reserved -Open Source Apache License v2.0



Indeed, this peer has several more significant HTTP exchanges, as also exhibited by the corresponding trafMon Manager report over July 2017.



As a conclusion, many of the remote peers belonging to the identified DNS domain name look like scanners, but some such peers cannot be de facto considered as malevolent. Their communications behaviour would require more dedicated monitoring.



2.4 REVEALING HIDDEN MULTI-DAY SCANS

Up to now, we have identified systems that were scanning multiple addresses in a same day.

Even the day can be a long-time span, but when these scans occur within a small time-window, they can be detected and rejected by intrusion detection systems (IDS).

However, there are even more vicious scanning behaviours, where it is very difficult to detect that our several own systems have actually been reached.

Let's take a look at the following figure. We see that a remote system from Malaysia is actually reaching a sequence of or own systems. But this is because we have ordered our lowTraffic table by local addresses.

at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-04-29	x.y.118.105	141.253.218.10	1 80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provider
2017-03-29	x.y.118.105	141.253.218.12	1 80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provider
2017-03-23	x.y.118.105	141.253.218.21	65535	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
2017-04-06	x.y.118.105	141.253.218.24	1 80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provider
2017-03-21	x.y.118.105	141.253.218.25	80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provider
2017-05-04	x.y.118.105	141.253.218.25	1 80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provider
017-03-23	x.y.118.105	141.253.218.27	80	11	492	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provider
017-03-29	x.y.118.105	141.253.218.27	1 80	11	492	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-03-22	x.y.118.105	141.253.218.33	80	11	492	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-03-17	x.y.118.105	141.253.218.52	1 80	12	532	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-04-15	x.y.118.105	141.253.218.54	1 80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide
017-04-21	x.y.118.105	141.253.218.54	1 80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-03-22	x.y.118.105	141.253.218.58	80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-04-21	x.y.118.105	141.253.218.65	1 80	13	596	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide
017-03-20	x.y.118.105	141.253.221.16	80	11	492	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide
017-03-26	x.y.118.105	141.253.221.29	80	18	796	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-04-10	x.y.118.105	141.253.221.90	80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide
017-04-04	x.y.118.105	141.253.221.94	1 80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-04-18	x.y.118.105	141.253.221.94	08	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-03-19	x.y.118.105	141.253.221.110	1 80	10	452	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-05-01	x.y.118.105	141.253.221.111	1 80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-03-26	x.y.118.105	141.253.221.112	1 80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-04-17	x.y.118.105	141.253.221.117	I 80	12	532	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-04-29	x.y.118.105	141.253.221.117	80	11	492	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:
017-04-07	x.y.118.105	141.253.221.121	80	1	1 40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provide:



When <u>we order the query by increasing dates</u>, we can see that the scan was occurring over 19 different days out of a period of 188 days.

t	remote	local	port	pkts	bytes	country	city	DNS	ASN
017-03-17	x.y.118.105	141.253.218.52	80	12	532	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-19	x.y.118.105	141.253.221.110	80	10	452	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-20	x.y.118.105	141.253.221.16	80	11	492	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-21	x.y.118.105	141.253.218.25	80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-22	x.y.118.105	141.253.218.33	80	11	492	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-22	x.y.118.105	141.253.218.58	80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-23	x.y.118.105	141.253.218.21	65535	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-23	x.y.118.105	141.253.218.27	1 80	11	492	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-26	x.y.118.105	141.253.221.29	80	18	796	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-26	x.y.118.105	141.253.221.112	80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-29	x.y.118.105	141.253.218.12	80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-03-29	x.y.118.105	141.253.218.27	80	11	492	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-04-04	x.y.118.105	141.253.221.94	80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-04-06	x.y.118.105	141.253.218.24	80	1	1 40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-04-07	x.y.118.105	141.253.221.121	80	1	1 40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-04-10	x.y.118.105	141.253.221.90	80	1	1 40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-04-15	x.y.118.105	141.253.218.54	1 80	1	1 40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-04-17	x.y.118.105	141.253.221.117	80	12	532	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-04-18	x.y.118.105	141.253.221.94	80	1	40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
017-04-21	x.y.118.105	141.253.218.54	80	1	1 40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-04-21	x.y.118.105	141.253.218.65	80	13	596	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-04-29	x.y.118.105	141.253.218.10	80	1	1 40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-04-29	x.y.118.105	141.253.221.117	80	11	492	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-05-01	x.y.118.105	141.253.221.111	1 80	1 1	1 40	Malaysia	Pantai	x.y.118.105	AS47zz, Internet Svc Provid
17-05-04	I x.v.118.105	1 141.253.218.25	1 80	1 1	1 40	Malavsia	Pantai	1 x.v.118.105	AS47zz, Internet Svc Provid



This system from Russia seems <u>also scanning several own systems spread over several days</u>: first ordered by local addresses.

🖌 Showi	ng rows 0 - 20 (2	1 total, Query took	0.1207	sec)					
SELECT FROM WHERE LIMIT 0	* owTraffic` `remote` <u>LII</u> , 30	<u>(E</u> 102	.129'						
Show :	Start row: 0	Number of re	ows: 3	D	Head	ers every	100	rows	
+ Options									
at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-29	nin 102.129	141.253.218.20	21	4	240	Russia	Tomsk	102-129 As.su.	AS31 Press Constant Avenue (17, Ltd.
2017-08-05	· 新新新新.102.129	141.253.218.20	21	6	284	Russia	Tomsk	7/w/2/102-129 (65.su.	AS31-7 TV. Ltd.
2017-07-05	102.129	141.253.218.42	21	16	1567	Russia	Tomsk	2/3/ 102-129 su.	AS31 North March Miles TV, Ltd.
2017-07-07	16.995Å102.129	141.253.218.49	65535	10	666	Russia	Tomsk	2 102-129 Sasu.	AS310 State State State TV. Ltd.
2017-07-12	102.129	141.253.218.49	65535	7	380	Russia	Tomsk	4 Km 102-129 su.	AS31 AS Mark Street 2 West TV, Ltd.
2017-07-05	AX 102.129	141.253.218.54	21	12	815	Russia	Tomsk	2032-102-129 (2.su.	AS31
2017-07-14	102.129	141.253.221.7	21	7	468	Russia	Tomsk	> 102-129 - su.	AS31 AV ANT AVE AND TV. Ltd.
2017-07-07	102.129	141.253.221.31	21	8	542	Russia	Tomsk	102-129 (2) su.	AS31 Storage States TV. Ltd.
2017-07-07	102.129	141.253.221.36	21	11	703	Russia	Tomsk	102-129 Adisu.	AS31 State V. Ltd.
2017-07-18	3/1/2,102.129	141.253.221.60	21	.4	240	Russia	Tomsk	102-129 (V.su.	AS31 Weeks My ConvertV. Ltd.
2017-07-05	45 to 102.129	141.253.221.90	21	11	753	Russia	Tomsk	0-102-129 (S.su.	AS3100 AUTOS OF TV. Ltd.
2017-07-05	102.129	141.253.221.91	21	10	702	Russia	Tomsk	102-129 (m.su.	AS312 Assa Demonstration TV. Ltd.
2017-07-05	ge 34/2.102.129	141.253.221.93	21	11	703	Russia	Tomsk	3	AS31 AFA WERE TV. Ltd.
2017-07-05	A	141.253.221.94	21	11	753	Russia	Tomsk	36 4 102-129 MA su.	AS3143 Standards No. TV. Ltd.
2017-07-16	2)4 (0.102.129	141.253.221.95	21	11	703	Russia	Tomsk	3-102-129 (su.	AS31 TV, Ltd.
2017-07-20	102.129	141.253.221.109	21	11	703	Russia	Tomsk	(102-129 (s. su.	AS3104 Store Same Average TV. Ltd.
2017-07-07	×× 102.129	141.253.221.111	65535	7	441	Russia	Tomsk	102-129-102-129-102-5U.	AS31 W As A State West
2017-07-12	102.129	141.253.221.112	21	11	754	Russia	Tomsk	AC71-102-129 20 su.	AS31 22 She Ringer Marshov TV, Ltd.
2017-07-07	2 102.129	141.253.221.138	21	11	753	Russia	Tomsk	20 8 102-129 M. su.	AS31 Street and a start TV, Ltd.
2017-07-08	Aug 102.129	141.253.221.137	21	11	967	Russia	Tomsk	102-129 su.	AS31 Line the she shows TV. Ltd.
2017-07-10	AN 102.129	141.253.221.173	85535	7	441	Russia	Tomsk	28.30 102-129 (sc.su.	AS31 A A Star Sure TV, Ltd.



Then ordered by date of occurrence.

🖌 Showi	ng rows 0 - 20 (2	1 total, Query took	0.1223 :	sec)						
SELECT FROM I WHERE ORDER LOCAL) LIMIT 0	SELECT * FROM lowTraffic' WHERE 'remote' LIKE 102.129' ORDER BY at, INET_ATON(LOCAL) LIMIT 0 , 30 Show : Start row: 0 Number of rows: 30 Headers every 100 rows									
Show :	Start row: 0	Number of ro	ws: 3	5	Head	ers every	100	rows		
			90-							
+ Options										
at	remote	local	port	pkts	bytes	country	city	DNS	ASN	
2017-07-05	New 102.129	141.253.218.42	21	16	1567	Russia	Tomsk	-102-129.nts.su.	AS31 AV Ltd.	
2017-07-05	Sec. 102.129	141.253.218.54	21	12	815	Russia	Tomsk	(아무) - 102-129.nts.su.	AS31 Assessment States TV. Ltd.	
2017-07-05	A 201,102,129	141.253.221.90	21	11	753	Russia	Tomsk	😒 ça 2102-129.nts.su.	AS31 2 Constant Present TV, Ltd.	
2017-07-05	\$\$* \$ \$.102.129	141.253.221.91	21	10	702	Russia	Tomsk	(高))为(102-129.nts.su.	AS310 State Active TV. Ltd.	
2017-07-05	ેટ∰.102.129	141.253.221.93	21	11	703	Russia	Tomsk	91.02-129.nts.su.	AS31	
2017-07-05	102.129	141.253.221.94	21	11	753	Russia	Tomsk	000000102-129.nts.su.	AS31-Constant and the TV. Ltd.	
2017-07-07	20112.102.129	141.253.218.49	65535	10	666	Russia	Tomsk	102-129.nts.su.	AS31 A MARKAGE TV. Ltd.	
2017-07-07	SA 841.102.129	141.253.221.31	21	8	542	Russia	Tomsk	2400-102-129.nts.su.	AS310 TORNAL STREET, TV. Ltd.	
2017-07-07	102.129	141.253.221.36	21	11	703	Russia	Tomsk	102-129.nts.su.	AS317 - Auto Antiger John 12 TV, Ltd.	
2017-07-07	한 102.129	141.253.221.111	65535	7	441	Russia	Tomsk	-102-129.nts.su.	AS31 AVE TV. Ltd.	
2017-07-07	N. 9.995.102.129	141.253.221.136	21	11	753	Russia	Tomsk	空間の102-129.nts.su.	AS31 A Strategies TV. Ltd.	
2017-07-08	102.129	141.253.221.137	21	11	967	Russia	Tomsk	(\$149-102-129.nts.su.	AS31 A TV. Ltd.	
2017-07-10	5 (A. 102.129	141.253.221.173	65535	7	441	Russia	Tomsk	102-129.nts.su.	AS31 CONST STRATE TV. Ltd.	
2017-07-12	Cizel 102.129	141.253.218.49	65535	7	380	Russia	Tomsk	/ພາ)/ໂຽະ102-129.nts.su.	AS31 WAR STAR STAR	
2017-07-12	342.102.129	141.253.221.112	21	11	754	Russia	Tomsk	*** -102-129.nts.su.	AS31 AND A LICE TV. Ltd.	
2017-07-14	A 102.129	141.253.221.7	21	7	468	Russia	Tomsk	33379-102-129.nts.su.	AS31 ALTRACTICKS DATE: TV. Ltd.	
2017-07-16	A 102.129	141.253.221.95	21	11	703	Russia	Tomsk	102-129.nts.su.	AS31 (Margare Margare TV, Ltd.	
2017-07-18	A 28 102.129	141.253.221.60	21	4	240	Russia	Tomsk	**************************************	AS31 We was shared to TV. Ltd.	
2017-07-20	of 102.129	141.253.221.109	21	11	703	Russia	Tomsk	102-129.nts.su.	AS31 (AS31) AND	
2017-07-29	200 CR. 102.129	141.253.218.20	21	4	240	Russia	Tomsk	-04 S-102-129.nts.su.	AS31 AS TALE AND AND TV. Ltd.	
2017-08-05	AN 102.129	141.253.218.20	21	6	264	Russia	Tomsk	☆○次≦>102-129.nts.su.	AS31 V. Ltd.	



Now we can look at what this system actually performed in using FTP protocol. So, we retrieve its bidirectional flows and look at values of its relevant FTP Counters: 3 times (on 3 different days 5th, 7th and 8th of July 2017) it failed to login. But on the 12th, it succeeded to get in and to conduct a directory listing in passive mode.

Either this system is a normal (but not expert) client, or its fourth try did succeed !?!

Showing rows 0 - 3 (4 total. Query took 0.0004 sec)						
SELECT 'rangeStart', 'flowID', 'noLoginSessions_sum', 'failedLogins_sum', 'noFilex ''commandFallures_sum' FROM 'ftpttable_aggr_1d' WHERE flowid LIKE '身点的。102.129:%<>%' ORDER BY 'rangeStart', 'flowID' LIMIT 0, 30	ferSessions_sum' .	fileXferSessions	s_sum', 'passiveConr	ections_sum" , " dirList	tCount_sum` ,	ĺ
				Profiling [Inline] [Edit]	[[Explain SQL]] Cre	ate PHP Code] [Refresh]
Show : Start row: 0 Number of rows: 30 Headers every 100 rows Sort by key: None • <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>						
+ Options			F11 44 . P 1			
+ - + Trange Start NowID	noLoginSessions_sum	tailedLogins_sum	not-ilexterSessions_sum	passiveConnections_sum	dirListCount_sum	commandFailures_sum
Copy Delete 2017-07-05 00:00 00 07: \$%, 102 129:high >141 253 218.42:21_tcp_trafmon	1		0	0	0	
Copy Delete 2017-07-07 00:00 00 12/25 102 129 high > 141 253 221 36:21_tcp_trafmon_	1	1	0	0	0	1
□ 2 Edit 12 Copy Copy Copy Copy Copy Copy Copy Copy	1	1	0	0	0	1
📄 🥜 Edit 🐉 Copy 🍘 Delete 2017-07-12 00 00:00 💈 🖉 👘 102 129 high 🗢 141 253 218 49 21_tcp_trafmon	0	0	1	1	1	0

_



2.5 DISCOVERING BATTERIES OF SCANNERS

When browsing and carefully inspecting the *lowTraffic* table, and thanks to the fact that remote addresses are also ordered, we can see that <u>patterns</u>, <u>supposedly identified as scans</u>, <u>are repeated</u> <u>for different remote addresses that belong to a same range</u>.

This is as if a battery of several different remote systems were sharing the scanning work. This is also something difficult to detect, unless when inspecting long term data sorted in meaningful order.

The three views below are displaying a part (top, middle and bottom) of a long result of 1037 rows, which seems to indicate multi-day scans conducted by a group of remote systems with addresses close to each other: x.y.**42.60**, x.y.**42.100**, x.y.**42.101**, x.y.**42.102**, x.y.**42.103** and x.y.**42.107**.



First Page: lowest "own" address:

Showing rows 0 - 1036 (1037 total, Query took 0.1259 sec)									
SELECT	* lowTraffic`								
WHERE	`remote` LI	KE 144.42	%						
ORDER	BY INET_ATC	N(
LOCAL)	, port, at, IN	IET_ATON(ren	note)						
LIMITO	, 3000								
				r	_	1			
Show :	Start row: 0	Number of	rows:	3000	He	eaders every	20	rows	
2010/02									
+ Options									
at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-26	42.100	141.253.218.6	80	2	80	United States	Chicago	vm-2.chi3.n. actives.com	AS32
2017-07-26	Apr: 12.42.103	141.253.218.6	80	1	40	United States	Chicago	vm-5.chi3.sty say as com	AS32 h A at a size p. Inc.
2017-07-26	39:2-8.42.107	141.253.218.6	80	1	40	United States	Chicago	vm-6.chi3	AS3244 ANGAMP, Inc.
2017-07-27	44, SN:42.101	141.253.218.6	80	1	40	United States	Chicago	vm-3.chi3.dia and com	AS32 destablished opening, Inc.
2017-07-27	42.103	141.253.218.6	80	1	40	United States	Chicago	vm-5.chi3. An the com	AS32 A A A A A A A A A A A A A A A A A A A
2017-07-27	前, 129.42.107	141.253.218.6	80	1	40	United States	Chicago	vm-6.chi3.chi3.com	AS32 AND AND AND INC.
2017-07-28	45.42.103	141.253.218.6	80	2	80	United States	Chicago	vm-5.chi3	AS32 Scherencep, Inc.
2017-07-28	ASP 482.42.107	141.253.218.6	80	1	40	United States	Chicago	vm-6.chi3	AS324 Storage p. Inc.
2017-07-26	A.42.60	141.253.218.7	80	2	80	United States	Chicago	vm-1.chi3.	AS3298 Conserver Inc.
2017-07-26	A	141.253.218.7	80	1	40	United States	Chicago	vm-4.chi3.a com	AS32 A State op. Inc.
2017-07-27	A2.100	141.253.218.7	80	1	40	United States	Chicago	vm-2.chi3. White the com	AS32 A Style p. Inc.
2017-07-27	St. 42.101	141.253.218.7	80	1	40	United States	Chicago	vm-3.chi3.com	AS32
2017-07-27	A.42.103	141.253.218.7	80	. 1	40	United States	Chicago	vm-5.chi3	AS32 AS4 P. Inc.
2017-07-27	(m - x - 42.107	141.253.218.7	80	1	40	United States	Chicago	vm-6.chi3. Ke Start com	AS32-F-1-4-1- AS32-F-1 Inc.
2017-07-28	· #+- + + 42.60	141.253.218.7	80	2	80	United States	Chicago	vm-1.chi3.severy skicy+1.com	AS32 AS32 p. Inc.
2017-07-28	26/2 42.107	141.253.218.7	80	1	40	United States	Chicago	vm-6.chi3 ktore com	AS32 Age Strate As Inc.
2017-08-05	sg3/4 30.42.107	141.253.218.7	80	4	172	United States	Chicago	vm-6.chi3	AS32(4) Ministration Inc.
2017-07-17	(h) (4.42.107	141.253.218.10	80	1	40	United States	Chicago	vm-6.chi3.	AS32* A PLACE A p. Inc.
2017-07-20	42.101	141.253.218.10	80	1	40	United States	Chicago	vm-3.chi3.vsr4.ksf4, com	AS32 AWW READD, Inc.
2017-07-26	War 97.42.100	141.253.218.10	80	1	40	United States	Chicago	vm-2.chi3 vase di v.com	AS32 AN Start p. Inc.
at	indin-ste	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-26	strain, 42,101	141.253.218.10	80	1	40	United States	Chicago	vm-3.chi3 (Com	AS32 AS32 Ap, Inc.
2017-07-26	13233.42.107	141.253.218.10	80	1	40	United States	Chicago	vm-6.chi3	AS32
2017-07-27	15.42.60	141.253.218.10	80	2	80	United States	Chicago	vm-1.chi3 value of com	AS32 AS A PARTY P. Inc.
2017-07-27	12 Ha.42.102	141.253.218.10	80	2	80	United States	Chicago	vm-4.chi3.z x 2 x com	AS32 ASSA
2017-07-28	\$1.42.60	141.253.218.10	80	1	40	United States	Chicago	vm-1.chi3	AS32 ASA AP, Inc.
2017-07-28	184 8/29.42.100	141.253.218.10	80	1	40	United States	Chicago	vm-2.chi3.kk/	AS32 No March Inc.
2017-07-26	34/2012.42.101	141.253.218.11	80	1	40	United States	Chicago	vm-3.chi3.sheets	AS32 / AS32 Inc.
2017-07-26	10.46.42.103	141.253.218.11	80	1	40	United States	Chicago	vm-5.chi3	AS32
2017-07-26	6 42.107	141.253.218.11	80	1	40	United States	Chicago	vm-6.chi3.com	AS32
2017-07-27	da = 0€.42.60	141.253.218.11	80	2	80	United States	Chicago	vm-1.chi3	AS32
2017-07-27	Acres 42.102	141.253.218.11	80	3	120	United States	Chicago	vm-4.chi3	AS32 AS A P. Inc.
2017-07-28	champe: 42.101	141.253.218.11	80	1	40	United States	Chicago	vm-3.chi3.chi3.com	AS3249 States op. Inc.
2017-07-28	Sp. 84.42.102	141.253.218.11	80	1	40	United States	Chicago	vm-4.chi3.com	AS324 HIR AVER Inc.
2017-07-28	AN 14.42.103	141.253.218.11	80	1	40	United States	Chicago	vm-5.chi3.cby, gorgan com	AS324 AS4 A P. Inc.
2017-07-17	A42.228	141.253.218.12	80	1	40	United States	Chicago	vm-7.chi3	AS32
2017-07-26	N. 2 199.42.101	141.253.218.12	80	2	80	United States	Chicago	vm-3.chi3.com	AS32
2017-07-26	12	141.253.218.12	80	1	40	United States	Chicago	vm-5.chi3.zagasterus.com	AS32

© 2020 AETHIS sa/nv Belgium Document version 1.0, 2020-12 -

All rights reserved Open Source Apache License v2.0 trafMon Use Case 3: Security Auditing Page: 28/58



Middle Page:

2017-07-26	de 6 + 42.103	141.253.218.105	80	1	40	United States	Chicago	vm-5.chi3.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	AS32
2017-07-26	42.107	141.253.218.105	80	1	40	United States	Chicago	vm-6.chi3.j. to s.com.	AS32 AS the up, Inc.
2017-07-27	10 42.60	141.253.218.105	80	2	80	United States	Chicago	vm-1.chi3.kashicash.com.	AS32 Astanop. Inc.
2017-07-27	65,095,42.102	141.253.218.105	80	2	80	United States	Chicago	vm-4.chi3. 2000	AS32
2017-07-28	144-12 42.101	141.253.218.105	80	1	40	United States	Chicago	vm-3.chi3.com.	AS32 ASSA TO Up. Inc.
2017-07-28	Key 20 42.102	141.253.218.105	80	1	40	United States	Chicago	vm-4.chi3.g stort of com.	AS32 AV ANA Section Inc.
2017-07-28	100 A 103	141.253.218.105	80	1	40	United States	Chicago	vm-5.chi3. Wile and com.	AS32 No Antip Inc.
2017-08-05	42.60	141.253.218.105	80	6	260	United States	Chicago	vm-1.chi3.s/w/www.i.com.	AS32 YA SAMP, Inc.
2017-08-05	國 104 42.102	141.253.218.105	80	13	560	United States	Chicago	vm-4.chi3.	AS32 And the state of the line.
at	SALA WAR	local	port	pkts	bytes	country	city	DNS	ASN
2017-06-26	42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.sk con.	AS32 Schene p. Inc.
2017-06-27	(1) 42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3. see the com.	AS324 A Storage Inc.
2017-06-28	42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.or \$100 \$10 com.	AS324000 http://p.inc.
2017-06-29	42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3	AS32
2017-06-30	AN: 42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.jse.evez.e.com.	AS32 A A A A A A A A A A A A A A A A A A A
2017-07-01	42.100	141.253.221.7	21	27	1540	United States	Chicago	vm-2.chi3.	AS32 (9: 1/e)(9:0) Inc.
2017-07-02	42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3. www.swiste.com.	AS32
2017-07-03	Net 14 42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.2 Auda A.com.	AS32 AS32 ASA Dp. Inc.
2017-07-04	1 42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.sessesses.com.	AS32
2017-07-05	WAR 42,100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.www.com.	AS32 MAN A MAN SUD. Inc.
2017-07-06	×42.100	141,253,221,7	21	28	1664	United States	Chicago	vm-2.chi3.bics.com	AS32 A ANA MANA INC. Inc.
2017-07-07	42.100	141.253.221.7	21	28	1664	United States	Chicado	vm-2.chi3.%444%334.com.	AS32 State ASSA No. Inc.
2017-07-08	197 385 42 100	141 253 221 7	21	14	832	United States	Chicago	vm-2 chi3 Statesticks.com	AS32
2017-07-09	NOV 16142 100	141,253,221,7	21	14	832	United States	Chicago	vm-2.chi3.www.abits.com.	AS32 Market AS ap. Inc.
2017-07-10	Gen - C 42 100	141 253 221 7	21	28	1664	United States	Chicago	vm-2 chi3 www.above.com	AS32
2017-07-11	3. 36.42 100	141 253 221 7	21	28	1664	United States	Chicago	vm-2 chi3 washing com	AS32404704049640 Inc
2017-07-12	3442 100	141 253 221 7	21	28	1664	United States	Chicago	vm-2 chi3 www.exist.com	AS32
2017-07-13	100 42 100	141 253 221 7	21	28	1884	United States	Chicago	vm-2 chi3 viet both is com	AS328 Vortee King Inc.
2017-07-14	10 - 42 100	141 253 221 7	21	14	832	United States	Chicago	vm-2 chi3 www.subic com	AS322 Were los
2017-07-15	WE /2 42 100	141 253 221 7	21	17	1018	United States	Chicago	vm-2 chi3 ke-20/ke/a com	AS32.44 At dealers Inc.
at	ACADAG	local	nort	nkts.	hytes	country	city	DNS	ASN
2017-07-16	Sec. 8:42 100	141 253 221 7	21	28	1884	United States	Chicago	vm-2 chi3 active Sty com	AS324 AVAILATING INC.
2017-07-17	No.3 -5 42 100	141 253 221 7	21	28	1884	United States	Chicago	vm-2 chi3 Statistics com	AS326 Children Inc.
2017-07-18	Cit-12-100	141 253 221 7	21	14	832	United States	Chicago	vm-2 chi3 white back com	AS326002000 Inc.
2017-07-10	42.100	141 252 221 7	21	14	222	United States	Chicago	vm-2 chi2 which which a com	AS32x8 as as a store inc.
2017-07-20	10:00:042 100	141 253 221 7	21	28	1884	United States	Chicago	vm-2 chi2 this of the com	AS32 Marine Annual
2017-07-20	15 1 20 42.100	141.253.221.7	21	20	1884	United States	Chieseo	vm-2 obi2 store com	ASSOCIATION INC.
2017-07-21	42,100	141.253.221.1	21	20	1718	United States	Chicago	vm.2 chi2 della Solia com	ACCOUNTER AND AND INC.
2017-07-22		141.253.221.7	21	20	1884	United States	Chiesee	wm 2 shi2 kinistichini som	ACCOUNT A STATE IN THE
2017-07-28	NA2 100	141.253.221.7	21	4.4	0004	United States	Chiango	vm-2.chi0.002000000	ACODINE OF SUCCESSION INC.
2017-07-20	202 1 32 42.100	141.200.221.7	2.1	1.4	032	onlied states	Chicago	VIII-2. CHIS. St. VSAVSOVAL COIN.	Abozara agagination mo.
2017-07-27	A COMPANY OF A COMPANY OF A COMPANY	444 050 004 7	2.4	100 C	1 A 10 A 10 A 10	Linder of Charles of	Chinese	And the state of the state of the second	A COO Stores has been been
	33029,42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3	AS32 + 2 + 12 / 2+p. Inc.
2017 07 20	42.100	141.253.221.7 141.253.221.7	21 21	28	1664	United States	Chicago Chicago	vm-2.chi3 the start com. vm-2.chi3 the start com.	AS32 A A A A A A A A A A A A A A A A A A A
2017-07-29	42.100 42.100 42.100	141.253.221.7 141.253.221.7 141.253.221.7	21 21 21	28 28 28	1864 1864 1864	United States United States United States	Chicago Chicago Chicago	vm-2 chi3 the source com. vm-2 chi3 the source of com. vm-2 chi3 the source of com.	AS32 A to the step inc. AS32 A to the step inc. AS32 A to the step inc.
2017-07-29 2017-07-30	42.100 42.100 42.100 42.100	141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7	21 21 21 21 21	28 28 28 28 28	1664 1664 1664 1664	United States United States United States United States	Chicago Chicago Chicago Chicago	vm-2.chi3 (22, 24, 24, 25, com, vm-2.chi3 (24, 24, 24, 25, com, vm-2.chi3 (24, 24, 24, com, vm-2.chi3 (24, 24, 24, com,	AS32 A A A A A A A A A A A A A A A A A A A
2017-07-29 2017-07-30 2017-07-31	42.100 42.100 42.100 42.100 42.100 42.100 42.100	141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7	21 21 21 21 21 21	28 28 28 28 28 28	1004 1004 1004 1004 1004 1004	United States United States United States United States United States	Chicago Chicago Chicago Chicago Chicago	vm-2 chi3 122 2025 2 com vm-2 chi3 2025 2 com vm-2 chi3 2025 2 com vm-2 chi3 2025 2 com vm-2 chi3 2025 2 com	AS324712 + 447446, Inc. AS32147104 (2014) Inc. AS3214714 - 2014 (2014) AS3214714 - 2014 (2014) AS3214714 - 2014 (2014) AS3214714 - 2014 (2014)
2017-07-29 2017-07-30 2017-07-31 2017-07-26	42.100 42.100 42.100 42.100 42.100 42.100 42.100 42.102	141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7	21 21 21 21 21 21 80	28 28 28 28 28 6	1664 1664 1664 1664 1664 248	United States United States United States United States United States United States	Chicago Chicago Chicago Chicago Chicago Chicago	vm-2 chi3 2000 com vm-2 chi3 2000 com vm-4 chi3 2000 com	AS3247 (A + 4 c) 4 p Inc. AS3247 (C + 4 p Inc. AS3247 (C + 2 c + 2 p Inc. AS3247 (C + 2 c + 2 p Inc. AS3247 (C + 2 p Inc. AS3247 (C + 2 p Inc.
2017-07-29 2017-07-30 2017-07-31 2017-07-26 2017-07-27	42.100 42.100 42.100 42.100 42.100 42.100 42.100 42.100	141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7	21 21 21 21 21 21 80 80	28 28 28 28 28 28 6 3	1664 1664 1664 1664 1664 248 124	United States United States United States United States United States United States	Chicago Chicago Chicago Chicago Chicago Chicago	vm-2 chi3 (2000 com vm-2 chi3 (2000 com vm-4 chi3 (2000 com vm-2 chi3 (2000 com	AS324 CALLER AND ADDRESS AND A
2017-07-28 2017-07-30 2017-07-31 2017-07-26 2017-07-27 2017-07-27	42.100 42.100 42.100 42.100 42.100 42.100 42.100 42.100 42.101	141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7	21 21 21 21 21 80 80 80	28 28 28 28 28 6 3 3	1884 1884 1884 1884 1884 248 124 124	United States United States United States United States United States United States United States	Chicago Chicago Chicago Chicago Chicago Chicago Chicago	vm-2 chi3 (22) (22) (22) (20) vm-2 chi3 (22) (22) (20) vm-2 chi3 (22) (22) (20) vm-2 chi3 (22) (22) (20) vm-2 chi3 (22) (20) vm-4 chi3 (22) (20) vm-2 chi3 (20) v	AS324 2 + 4 yep Inc. AS323 2 + 4 yep Inc. AS3234 2 + 4 yep Inc. AS324 2 + 4 yep Inc.
2017-07-29 2017-07-30 2017-07-31 2017-07-26 2017-07-27 2017-07-27 2017-07-27	42,100 42,100 42,100 42,100 42,100 42,100 42,100 42,101 42,103	141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7	21 21 21 21 21 80 80 80 80	28 28 28 28 28 8 3 3 3	1684 1684 1684 1684 1684 1684 248 124 124 124	United States United States United States United States United States United States United States United States	Chicago Chicago Chicago Chicago Chicago Chicago Chicago	vm-2 chi3 (22) (22) (22) (20) vm-2 chi3 (22) (22) (20) vm-2 chi3 (22) (22) (20) vm-2 chi3 (22) (22) (20) vm-2 chi3 (22) (22) (20) vm-4 chi3 (22) (22) (20) vm-2 chi3 (22) (22) (20) vm-3 chi3 (22) (22) (20) vm-3 chi3 (22) (22) (20)	AS324 2 + 4 yep Inc. AS323 2 + 4 yep Inc. AS3234 2 + 4 yep Inc. AS324 4 + 6 yep Inc. AS324 4 + 6 yep Inc. AS324 4 + 6 yep Inc. AS324 4 + 7 yep Inc. AS324 4 + 7 yep Inc. AS324 4 + 7 yep Inc.
2017-07-29 2017-07-29 2017-07-30 2017-07-27 2017-07-27 2017-07-27 2017-07-27 2017-07-27	42,100 42,100 42,100 42,100 42,100 42,100 42,101 42,103 42,103 42,103	141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7	21 21 21 21 21 80 80 80 80 80	28 28 28 28 6 3 3 3 3 3	1684 1664 1664 1664 1664 248 124 124 124 124	United States United States United States United States United States United States United States United States	Chicago Chicago Chicago Chicago Chicago Chicago Chicago Chicago	vm-2 chi3 (22) (22) (22) (20) vm-2 chi3 (22) (22) (20) vm-3 chi3 (22) (22) (20) vm-5 chi3 (22) (22) (20) vm-5 chi3 (22) (22) (20)	AS32 A LAND A LA
2017-07-29 2017-07-29 2017-07-30 2017-07-31 2017-07-26 2017-07-27 2017-07-27 2017-07-27 2017-07-27	42,100 42,100 42,100 42,100 42,100 42,100 42,100 42,101 42,103 42,103 42,101	141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7	21 21 21 21 21 80 80 80 80 80 80 80	28 28 28 28 8 3 3 3 3 3 3 3 3	1884 1884 1884 1884 1884 248 124 124 124 124 124	United States United States United States United States United States United States United States United States United States United States	Chicago Chicago Chicago Chicago Chicago Chicago Chicago Chicago Chicago	vm-2 chi3 (22) (22) (22) (20) vm-2 chi3 (22) (22) (20) vm-3 chi3 (22) (22) (20) vm-5 chi3 (22) (22) (20) vm-6 chi3 (22) (22) (22) (20)	AS32 A LAND A LA
2017-07-29 2017-07-30 2017-07-30 2017-07-31 2017-07-26 2017-07-27 2017-07-27 2017-07-27 2017-07-28 at	42,100 42,100 42,100 42,100 42,100 42,100 42,101 42,101 42,103 42,101 42,101 42,101	141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7 141.253.221.7	21 21 21 21 21 80 80 80 80 80 80 80 80	28 28 28 28 6 3 3 3 3 3 9 kts	1684 1664 1664 1664 1664 248 124 124 124 124 124 124 124 bytes	United States United States	Chicago Chicago Chicago Chicago Chicago Chicago Chicago Chicago Chicago Chicago	vm-2 chi3 22 com vm-2 chi3 22 com vm-4 chi3 22 com vm-2 chi3 22 com vm-3 chi3 22 com vm-5 chi3 22 com vm-6 chi3 22 com vm-3 chi3 22 com vm-3 chi3 22 com	AS324 2 + 4 yep Inc. AS323 2 + 4 yep Inc. AS323 2 + 4 yep Inc. AS32 4 + 4 yep Inc. AS324 4 + 9 yep Inc.



Last Page: highest "own" address

	The second								a grant with a straight of the
2017-07-27	chg 799.42.107	141.253.221.217	80	1	40	United States	Chicago	vm-6.chi3, specific v., com.	AS32KP2 Aga avo. Inc.
2017-07-28	(Alth) (A4.42.101	141.253.221.217	80	1	40	United States	Chicago	vm-3.chi3	AS32 Stars and Inc.
2017-07-28	133-05.42.102	141.253.221.217	80	2	80	United States	Chicago	vm-4.chi3/stops attracom.	AS32, Strangero, Inc.
2017-08-05	Acres 42.101	141.253.221.217	80	7	304	United States	Chicago	vm-3.chi3.	AS32 A Structure Inc.
2017-07-26	第四次第142.101	141.253.221.218	80	1	40	United States	Chicago	vm-3.chi3.442.445.com.	AS32/34/28/28/28/20, Inc.
2017-07-26	(4) C \$.42.103	141.253.221.218	80	্	40	United States	Chicago	vm-5.chi3	AS32. A Kieskyp, Inc.
2017-07-26	······································	141.253.221.218	80	1	40	United States	Chicago	vm-6.chi3.com.	AS32 Ad State Street Inc.
2017-07-27	42.60	141.253.221.218	80	1	40	United States	Chicago	vm-1.chi3.com.	AS32 Margaranzo, Inc.
2017-07-27	A 42.102	141.253.221.218	80	1	40	United States	Chicago	vm-4.chi3.state 25-25.com.	AS32 ASSA Contraction Inc.
2017-07-28	42.101	141.253.221.218	80	1	40	United States	Chicago	vm-3.chi3.chi3.com.	AS32 A single of Inc.
2017-07-28	·2.42.102	141.253.221.218	80	1	40	United States	Chicago	vm-4.chi3	AS32 AN AND NO. Inc.
2017-07-28	A C +8.42.103	141.253.221.218	80	1	40	United States	Chicago	vm-5.chi3.	AS32a 2 2 2 A Market No. Inc.
2017-08-05	47.42.102	141.253.221.218	80	6	264	United States	Chicago	vm-4.chi3.asi com.	AS3250 Mt We Wo Inc.
2017-07-26	Sec. 56.42.60	141.253.221.219	80	:1	40	United States	Chicago	vm-1.chi3.	AS32 ACCOMMENTED, Inc.
2017-07-26	An	141.253.221.219	80	2	80	United States	Chicago	vm-4.chi3.key and the com.	AS32 Shink Kop. Inc.
at	una se	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-27	105 AV 42 100	141 253 221 219	80	1	40	United States	Chicago	vm-2 chi3	AS32 AND ASSARD INC.
2017-07-27	635 536 42 101	141 253 221 219	80	1	40	United States	Chicago	vm-3 chi3 see to way on the	AS32942 State Provide Inc.
2017-07-27	Q (Per 42 102	141 253 221 210	80	4	40	United States	Chicago	vm-5 chi3 bis Chaby is com	4832 - 36 - 36 - 10 - 100
2017-07-27	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	141.253.221.218	00	4	40	United States	Chinago	vm 8 chi2 1 trick with some	ACCOMMENDED INC.
2017-07-27	AN 100 42 107	141.253.221.218	00	4	40	United States	Chieses	VIII-O. CHIS S. Water Street Com.	ABBZING ABBZING INC.
2017-07-20	V2.559.42.101	141.203.221.219	00	2	40	United States	Chinese	VIII-S.CHIS MARKEN AREA.COM.	ABSZA A MARKAND, INC.
2017-07-28	A200199.42.102	141.203.221.218	80	2	80	United States	Chicago	vm-4.cnia and mars.com.	ASSAN AN ANY AND INC.
2017-08-05	Mar. 103	141.253.221.219	80	11	476	United States	Chicago	vm-5.chi3. And a text.com.	AS32.4 States for Inc.
2017-07-26	42.101	141.253.221.224	80	1	40	United States	Chicago	vm-3.chi3.lateray gra.i.com.	AS32 And Assert 28:55 Inc.
2017-07-26	Aga: 14.42.103	141.253.221.224	80	1	40	United States	Chicago	vm-5.chi3	AS32 State Association Inc.
2017-07-26	\$\$\$\$\$\$.42.107	141.253.221.224	80	1	40	United States	Chicago	vm-6.chi3	AS32 AND AND INC.
2017-07-27	资料为.42.60	141.253.221.224	80	2	80	United States	Chicago	vm-1.chi3. www.kk.com.	AS32 V Howkers, Inc.
2017-07-27	编》 14.42.102	141.253.221.224	80	2	80	United States	Chicago	vm-4.chi3 while Suffe com.	AS32 / Variation Inc.
2017-07-28	37,953,42.101	141.253.221.224	80	1	40	United States	Chicago	vm-3.chi3	AS32 A History Inc.
2017-07-28	Apr. 109.42.102	141.253.221.224	80	1	40	United States	Chicago	vm-4.chi3	AS32 Arentwick p. Inc.
2017-07-28	你来给.42.103	141.253.221.224	80	1	40	United States	Chicago	vm-5.chi3 编译教教会:com.	AS32 Average average for Inc.
2017-08-05	我们会会,42.60	141.253.221.224	80	2	80	United States	Chicago	vm-1.chi3	AS320 AS320 ASSA
2017-08-05	前令:49.42.102	141.253.221.224	80	2	80	United States	Chicago	vm-4.chi3	AS32/2 1-10000 (%o. Inc.
2017-07-26	60 (NB).42.100	141.253.221.225	80	1	40	United States	Chicago	vm-2.chi3.xiv (see com.	AS32: 4 4 4 4 50. Inc.
2017-07-26	42.101	141.253.221.225	80	1	40	United States	Chicago	vm-3.chi3/ Ave St. com.	AS32 ANA Secondo, Inc.
2017-07-26	PAS 5.42.107	141.253.221.225	80	1	40	United States	Chicago	vm-6.chi3	AS32 ASA AND Inc.
at	10000	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-27	AN 34.42.60	141.253.221.225	80	2	80	United States	Chicago	vm-1.chi3	AS32 A Single Series Inc.
2017-07-27	A	141.253.221.225	80	2	80	United States	Chicago	vm-4.chi32546.com.	AS32 AS TANKS No. Inc.
2017-07-28	A2.60	141.253.221.225	80	1	40	United States	Chicago	vm-1.chi3	AS32 ASSA AUGULTO, Inc.
2017-07-28	AV 2.42.100	141,253,221,225	80	1	40	United States	Chicago	vm-2.chi3/2005-com.	AS32
2017-07-28	A 8 42.107	141,253,221,225	80	1	40	United States	Chicago	vm-6.chi3.chi3.com.	AS32
2017-08-05	24 2 42 60	141 253 221 225	80	1	40	United States	Chicago	vm-1 chi3 46-380% d com	AS32 Hot sharest stud Inc.
2017-08-05	GREGA 42 100	141 253 221 225	80	7	304	United States	Chicago	vm-2 chi3 fatavetali com	49323 9 10 100 Inc
2017-07-28	St 378 42 100	141 253 221 224	20	1	40	United States	Chicago	vm-2 chi3 (fint) (sink) com	4922 And Catholica Inc.
2017-07-20	291.35 42 100	141.253.221.234	00	্ৰ	40	United States	Chiango	vm 2 chi2 (section) and	ACCOMMENTAL ACCOMMENTAL
2017-07-20	942(83-42.101	141.200.221.234	00	1	40	United States	Chieses	vm-a.onia.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.	A 999/2010/2012/2012 100
2017-07-20	ALL 103	141.200.221.234	80	1	40	United Otates	Chicago	win-otoniorgraphic exercision.	A0022 11 200 000 100.
2017-07-27	7% 7% 42.100	141.203.221.234	80	1	40	United States	Unicago	vm-2.cnis segue segs.com.	A0325 19 (1996) 94(49), Inc.
2017-07-27	751, 179,42,101	141.253.221.234	80	1	40	United States	Chicago	vm-3.chi3.gateste are com.	AS32 MATAN SCALD, Inc.
2017-07-27	16.42.107	141.253.221.234	80	1	40	United States	Chicago	vm-6.chi3	AS3Zer And Active Xo. Inc.
2017-07-28	SEC. 42.100	141.253.221.234	80	1	40	United States	Chicago	vm-2.chi3 (As a start com.	AS32(hhttp://www.io.inc.
2017-07-28	19-5 (Q.42.101	141.253.221.234	80	1	40	United States	Chicago	vm-3.chi3. rate com.	AS32 Conversion Inc.
2017-07-28	如何, 19.42.103	141.253.221.234	80	1	40	United States	Chicago	vm-5.chi3.xsetAs WX.com.	AS32 Contraction Inc.



3. ABNORMAL DAILY INGRESS VOLUME PEAK

After having looked at apparent scanning patterns, we can also focus on possible attempts to overload own systems. These would exhibit abnormal daily peak of ingress traffic volume.

3.1 PER OWN SYSTEM DAILY INGRESS IN DECREASING ORDER

First, we create a table *in_VolumesExtern*, by summing up the packets and bytes counters coming from all external systems (not private IP addresses, without assigned Activity/Location) towards own systems (with assigned Activity and/or Location).

```
CREATE TABLE in_VolumesExtern
  SELECT local, rangeStart, MAX(in_bytes) AS in_bytes
   FROM (
         SELECT address1 AS local, rangeStart, SUM(in_bytes) AS in_bytes
        FROM activityvolumetable_agg_ld
WHERE ( (location1 IS NOT NULL AND location1 ↔ 'N/A') OR (activity1 IS NOT NULL AND activity1 ↔ 'N/A') )
AND (location2 = 'N/A' OR location2 IS NULL) AND (activity2 = 'N/A' OR activity2 IS NULL)
AND address2 NOT LIKE '10.%.%' AND address2 NOT LIKE '192.168.%.%'
                                                                   AND INET_ATON(address2) NOT BETWEEN INET_ATON('172.16.0.0')
                                                                                                                  AND INET_ATON('172.31.255.255')
        GROUP BY address1, rangeStart
     UNION
         SELECT address2 AS local, rangeStart, SUM(out_bytes) AS in_bytes
        FROM activityvolumetable_aggr_1d
        WHERE ( (location2 IS NOT NULL AND location2 <> 'N/A') OR (activity2 IS NOT NULL AND activity2 <> 'N/A') )
AND (location1 = 'N/A' OR location1 IS NULL) AND (activity1 = 'N/A' OR activity1 IS NULL)
AND address1 NOT LIKE '10.%.%.' AND address1 NOT LIKE '192.168.%.%'
                                                                  AND INET_ATON(address1) NOT BETWEEN INET_ATON('172.16.0.0')
AND INET_ATON('172.31.255.255')
        GROUP BY address2, rangeStart
   GROUP BY local, rangeStart
  HAVING in_bytes >
  ORDER BY INET_ATON(local) ASC, in_bytes ASC
```

The above SQL statement covers the entire span of available data. The resulting *in_VolumesExtern* table should therefore be recreated regularly at night. This has been implemented as a <u>stored</u> <u>procedure</u>, in the downloadable add-on *trafMon_SecurityExample* package:

```
`trafMon_SecurityProcs`.`Refresh_ExternInPeaks`(IN `_DBname` VARCHAR(20))
```

At the time of manually conducting the security analysis, it suffices to dig into this already prepared table to retrieve peak daily volumes of interest.

© 2020 AETHIS sa/nv Belgium	-	All rights reserved -	trafMon Use Case 3: Security Auditing
Document version 1.0, 2020-12		Open Source Apache License v2.0	Page: 31/58



By browsing through the *in_VolumesExtern* table, we can easily compare the daily ingress traffic peaks, numerically sorted, and detect abnormal jumps.

The following example concerns a system (141.253.218.2) that has been applied a Nessus security scan on the 26 May 2017. We see that its top ingress traffic <u>daily peak is **23 times higher** than the value of its second ingress daily peak</u>.

++ local	rangeStart	in_bytes
141.253.216.11 141.253.216.32 141.253.218.2 <	2016-12-22 00:00:00 00 2017-05-26 00:00:00 00 2017-05-26 00:00:00 00 2017-05-26 00:00:00 00 2017-06-17 00:00:00 00 2016-11-25 00:00:00 00 2016-11-11 00:00:00 00 2016-11-18 00:00:00 00 2016-12-21 00:00:00 00 2016-12-21 00:00:00 00 2016-12-21 00:00:00 00 2016-12-21 00:00:00 00 2016-12-20 00:00:00 00 2016-11-20 00:00:00 00 2016-11-20 00:00:00 00 2016-11-29 00:00:00 00 2016-11-29 00:00:00 00 2016-11-29 00:00:00 00 2016-11-29 00:00:00 00 2016-11-29 00:00:00 00 2016-11-29 00:00:00 00 2016-11-09 00:00:00 00 <th>180 180 180 1066296 46548 10332 10335 10335 10455 10455 10455 10555 104556 10555 10555 10555 10555 10555 10555 10555 10555</th>	180 180 180 1066296 46548 10332 10335 10335 10455 10455 10455 10555 104556 10555 10555 10555 10555 10555 10555 10555 10555

So we take a closer look at this server traffic on that top peak day:

-

SELECT address1, port1, direction, address2, port2, SUM(sum) as bytes
FROM flowtable a, ipsztable_aggr_1d b
WHERE a.flowID = b.flowID AND rangeStart = '2017-05-26 00:00'
 AND (address1 = '141.253.218.2' OR address2 = '141.253.218.2')
 AND direction IN ('<', '>')
GROUP BY rangeStart, address1, port1, direction, address2, port2
ORDER BY rangeStart, address1, port1, address2, port2, direction;



address1	portl	direction	address2	port2	bytes	141.253.218 141.253.218	2 223 224	> <	160.22.36.108 160.22.36.108	65535 65535	40 48
141.253.218.2	NULL	<	160, 22, 36, 108	NULL	92	141,253,218	3.2 224 3.2 243	> < <	160.22.36.108 160.22.36.108	65535 65535	40 48
141.253.218.2	NULL	>	224.176.218.1	NULL	63552	141, 253, 218	8.2 243 3.2 245	>	160.22.36.108 160.22.36.108	65535 65535	40
141.253.218.2	i i	~ <	160, 22, 36, 108	65535	40	141.253.218	3.2 246 3.2 247	< <	160.22.36.108	65535 65535	48
141.253.218.2	4	> <	160.22.36.108	65535	40	141.253.218	2 256	1	160.22.36.108	65535	710
141,253,218,2	5	2	160.22.36.108	65535	40	141.253.218	.2 257	-	160.22.36.108	65535	627
141.253.218.2	, je	2	160, 22, 36, 108	65535	40	141.253.218	3.2 257 3.2 258	<	160.22.36.108	65535	48
141.253.218.2	15	÷.	160, 22, 36, 108	65535	48	141,253,218	8.2 259 8.2 259	<	160.22.36.108 160.22.36.108	65535 65535	650 1078
141,253,218,2 141,253,218,2	21	< <	160.22.36.108 160.22.36.108	65535	136 48	141.253.218	3.2 260 3.2 261	<	160.22.36.108	65535 65535	48
141,253,218,2 141,253,218,2	22 22	<	160.22.36.108 160.22.36.108	65535	5856 3096	141.253.218	262	1	160.22.36.108	65535	48
141.253.218.2	23 25	< <	160.22.36.108	65535	108	141.253.218	2 263	<	160.22.36.108	65535	48
141.253.218.2	25	2	160.22.36.108	65535	40	141.253.218	2 264	3	160.22.36.108	65535	796
141.253.218.2	31	<	160 22 36 108	65535	48	141.253.218	3.2 265	>	160.22.36.108	65535	48
141.253.218.2	35	<	160.22.36.108	65535	48	141, 253, 218	8.2 266 3.2 281	<	160.22.36.108 160.22.36.108	65535 65535	48
141.253.218.2 141.253.218.2	35	>	160, 22, 36, 108	65535	40	141.253.218	3.2 282 3.2 284	>	160.22.36.108 160.22.36.108	65535 65535	40
141.253.218.2	38 38	<	160.22.36.108	65535	48	141, 253, 218	285	2	160.22.36.108	65535	40
141, 253, 218, 2	41	<	160,22,36,108	65535	48	141.253.218	.2 287	-	160.22.36.108	65535	40
141,253,218,2	44	>	160.22.36.108	65535	40	141.253.218	3.2 309	2	160.22.36.108	65535	40
141,253,218,2	46	2	160, 22, 36, 108	65535	48	141.253.218	3.2 310 3.2 313	× <	160.22.36.108	65535 65535	40
141.253.218.2	46	~	160.22.36.108	65535	40	141,253,218	3.2 313 3.2 314	> <	160.22.36.108 160.22.36.108	65535 65535	40
141.253.218.2	48	< <	160,22,36,108 160,22,36,108	65535	48	141.253.218	8.2 315 8.2 315	<	160.22.36.108	65535 65535	48
141.253.218.2 141.253.218.2	50 52	> <	160.22.36.108	65535 65535	40	141.253.218	3.2 317	5	160.22.36.108	65535	48
141,253,218,2	52	2	160.22.36.108	65535	40	141, 253, 218	.2 322	2	160.22.36.108	65535	48
141.253.218.2	55	<	160.22.36.108	65535	48	141.253.218	.2 344	>	160.22.36.108	65535	40
141.253.218.2	57	÷.	160.22.36.108	65535	48	141, 253, 218	3.2 350 3.2 350	>	160.22.36.108 160.22.36.108	65535 65535	48
141,253,218,2 141,253,218,2	57	~	160.22.36.108	65535	40	141.253.218	3.2 352 3.2 356	< <	160.22.36.108 160.22.36.108	65535 65535	48
141,253,218,2 141,253,218,2	58 59	>	160.22.36.108	65535 65535	40	141, 253, 218	356	>	160.22.36.108	65535	40
141.253.218.2	61 63	< <	160.22.36.108	65535	48	141.253.218	3.2 358	<	160.22.36.108	65535	96
141.253.218.2	66	2	160.22.36.108	65535	40	141.253.218	359	<	160.22.36.108	65535	48
141.253.218.2	67	2	160 22 36 108	65535	40	141.253.218	.2 361	i c	160.22.36.108	65535	48
141,253,218,2	69	÷.	160, 22, 36, 108	65535	48	141.253.218	3.2 362 3.2 362	>	160.22.36.108	65535	48
141.253.218.2	71	<	160.22.36.108	65535	40	141,253,218	8.2 363 3.2 365	<	160.22.36.108 160.22.36.108	65535 65535	48
141,253,218,2 141,253,218,2	75 77	>	160, 22, 36, 108 160, 22, 36, 108	65535	40	141.253.218	3.2 366 3.2 368	< <	160.22.36.108	65535 65535	48
141.253.218.2 141.253.218.2	78 79	<	160.22.36.108 160.22.36.108	65535	48	141, 253, 218	368	2	160.22.36.108	65535	40
141.253.218.2	80	<	160, 22, 36, 108	65535	446242	141.253.218	2 370	<	160.22.36.108	65535	48
141.253.218.2	81	<	160.22.36.108	65535	108	141.253.218	371	i a	160.22.36.108	65535	48
141.253.218.2	82	< l	160, 22, 36, 108	65535	48	141.253.218	.2 375	<	160.22.36.108	65535	48
141.253.218.2	85	< <	160.22.36.108	65535	48	141, 253, 218	3.2 375 3.2 376	>	160.22.36.108 160.22.36.108	65535 65535	40
141,253,218,2 141,253,218,2	86 87	>	160, 22, 36, 108 160, 22, 36, 108	65535	40	141.253.218	8.2 377 3.2 379	< <	160.22.36.108 160.22.36.108	65535 65535	48
141,253,218,2 141,253,218,2	90 92	> <	160.22.36.108	65535 65535	40	141, 253, 218	3.2 382	< <	160.22.36.108	65535 65535	48
141,253,218,2	92 97	>	160, 22, 36, 108	65535	40	141.253.218	384	2	160.22.36.108	65535	40
141.253.218.2	99	>	160.22.36.108	65535	40	141.253.218	3.2 385	2	160.22.36.108	65535	40
141.253.218.2	101	R	160, 22, 36, 108	65535	48	141.253.218	.2 389	>	160.22.36.108	65535	40
141.253.218.2	103	>	160.22.36.108	65535	40	141, 253, 218	3.2 391 3.2 397	< >	160.22.36.108 160.22.36.108	65535 65535	48
141,253,218,2 141,253,218,2	105	~	160, 22, 36, 108 160, 22, 36, 108	65535 65535	40	141.253.218	3.2 399 3.2 400	< <	160.22.36.108 160.22.36.108	65535 65535	48
141.253.218.2 141.253.218.2	107 108	< <	160.22.36.108 160.22.36.108	65535	48	141,253,218	2 401	>	160.22.36.108	65535	40
141.253.218.2	110	>	160.22.36.108	65535	40	141.253.218	404	2	160.22.36.108	65535	40
141.253.218.2	111	>	160.22.36.108	65535	40	141.253.218	.2 407	<	160.22.36.108	65535	212
141.253.218.2	113	2	160.22.36.108	65535	48	141.253.218	.2 409 3.2 409	>	160.22.36.108	65535	48
141,253,218,2 141,253,218,2	120	>	160.22.36.108	65535	48	141.253.218	410 2 412	~	160.22.36.108 160.22.36.108	65535 65535	40
141.253.218.2 141.253.218.2	123 123	<	160.22.36.108	65535 65535	200	141, 253, 218	1.2 413	< >	160.22.36.108	65535 65535	48
141.253.218.2	124	<	160.22.36.108	65535	48	141.253.218	8.2 415	>	160, 22, 36, 108	65535	40

© 2020 AETHIS sa/nv Belgium Document version 1.0, 2020-12 -

All rights reserved -Open Source Apache License v2.0





© 2020 AETHIS sa/nv Belgium Document version 1.0, 2020-12

All rights reserved -Open Source Apache License v2.0



Inspecting the above results, we see some significant outgoing bytes towards a multicast address (224.176.218.1), and all the rest is related to <u>the port scan and the penetration testing by a Nessus</u> <u>scanner</u> (*fake address 160.22.36.108*):

- limited SSH exchanges (port 22),
- more significant HTTP volume (port 80),
- NTP (port 123) attempt,
- SNMP (port 161) attempt,
- CheckPoint-specific attempt (ports 256-259, 264, 900),
- exchanges in HTTPS (port 443),
- IKE (port 500) attempt,
- unknown attempt to port 848,
- voluminous exchanges on port 900 (CheckPoint-specific HTTP Client Authentication),
- and <u>significant</u> exchanges on unprivileged high ports (65535 stands for "above 1024").

_



3.2 SECOND TO TOP DAILY PEAK MULTIPLIER

So, the method of identifying, for our own systems, where the top ingress daily peak is a multiple of the second higher ingress daily peak, is a good way to point to potential traffic overload attempts.

By what factor is the volume first peak larger than the second peak?

Based on the table *in_VolumesExtern* presented above, the <u>following queries sequence</u> automatically retrieves:

- 1. the value of the <u>top peak</u>
- 2. the value of the second highest peak

In order to compute the <u>percentage of sudden increase</u>, and to sort the resulting list of potential bombarding of our own systems, we use the following query:

```
-- Computes the jump between daily peaks from the in_VolumesExtern
-- already ordered by increasing peaks
 CREATE TEMPORARY TABLE in VolumesExtern jump
   SELECT local, rangestart, in_bytes,
           @delta:= IF(@prevAddr <> local, 0, @prevBytes) as prev_bytes,
           @prevAddr:= local, @prevBytes:= in_bytes
   FROM in_VolumesExtern,
         (SELECT @prevAddr:='') b,
         (SELECT @prevBytes:= 0) c;
- -
-- Retrieves those days where each own systems receives its top peak
-- or external systems data
 CREATE TEMPORARY TABLE in_VolumesExtern_max
   SELECT local, MAX(in bytes) AS max in bytes
   FROM in_VolumesExtern_jump
   GROUP BY local;
-- Keeps those lines with the per own system top peak and previous top peak
-- and computes the pecentage of the jump between the two top peaks
- -
-- Where the jump percentage is high (e.g. > 100 %), it is suspected that the
-- corresponding own system has been bombarded on that top peak day.
-- ==> Its corresponding traffic requires further inspection
- -
 SELECT a.local, rangestart, in_bytes, ROUND((in_bytes / prev_bytes) *100) AS jump_pct
   FROM in_VolumesExtern_jump a, in_VolumesExtern_max b
   WHERE a.in bytes = b.max in bytes AND a.local = b.local
         AND in_bytes > prev_bytes AND prev_bytes > 0
   ORDER BY jump_pct DESC
```



	L	P	e	and an and a second		a contract and some party later and	
1	,	l in human	· · · · · · · · · · · · · ·	141.25	3.218.61	2017-07-19 00:00:00	212396419
ocal	rangestart	in_bytes	jump_pct	141.25	3.218.6	2017-07-14 00:00:00	96523885003
	+		++	141.25	3.218.16	2017-06-27 00:00:00	55959061
141.253.221.27	2017-08-06 00:00:00	8822458492	4250722	141.25	3.221.214	2017-08-06 00:00:00	2533404
141.253.218.57	2017-08-06 00:00:00	136744746	187237	141.25	3.221.112	2017-07-12 00:00:00	690335274107
141.253.221.109	2017-08-06 00:00:00	230368171	17471	141.25	3.218.65	2017-07-22 00:00:00	235496
141.253.218.54	2017-07-27 00:00:00	25835191	14722	141.25	3.218.20	2017-06-28 00:00:00	45419851
141.253.218.58	2017-07-17 00:00:00	2944709	12108	141.25	3.221.91	2017-08-06 00:00:00	8832723593
141.253.221.103	2017-07-18 00:00:00	250653159	11735	141.25	3.221.117	2017-07-02 00:00:00	1281021
141.253.221.31	2017-07-18 00:00:00	670835566	11322	141.25	3.221.95	2017-07-17 00:00:00	2580316
141.253.221.37	2017-08-06 00:00:00	192924267	7490	141.25	3.218.7	2017-07-29 00:00:00	10542761
141.253.218.25	2017-08-01 00:00:00	18333478	7343	141.25	3.221.102	2017-07-21 00:00:00	58980175492
141,253,218,52	2017-08-06 00:00:00	2193061022	2948	141.25	3.221.89	2017-08-05 00:00:00	218458
41.253.218.36	2017-08-06 00:00:00	10011160	2530	141.25	3.218.24	2017-07-21 00:00:00	19298237
141.253.221.29	2017-07-18 00:00:00	163694588	1802	141.25	3.221.100	2017-07-09 00:00:00	2059944
141.253.221.163	2017-07-19 00:00:00	131157906	1497	141.25	3.218.12	2017-07-21 00:00:00	12259723
141.253.221.170	2017-08-06 00:00:00	78212	1473	141.25	3.221.215	2017-07-27 00:00:00	7881112
141.253.218.56	2017-06-30 00:00:00	40476541	1306	141.25	3.218.105	2017-07-12 00:00:00	16043568
141, 253, 221, 134	2017-07-21 00:00:00	2507852944	1302	141.25	3.218.10	2017-07-26 00:00:00	16340300
141, 253, 221, 35	2017-07-14 00:00:00	23752345	1262	141.25	3.221.135	2017-06-29 00:00:00	18886214
141.253.221.90	2017-06-29 00:00:00	73232517	1068	141.25	3.218.11	2017-07-21 00:00:00	13037643
41, 253, 221, 105	2017-08-06 00:00:00	153183662	931	141.25	3.221.23	2017-07-27 00:00:00	1725154356
141, 253, 221, 108	2017-07-17 00:00:00	230748636	404	141.25	3.218.27	2017-07-31 00:00:00	4935846
41 253 221 234	2017-08-06 00:00:00	21907	375	141.25	3.221.225	2017-06-28 00:00:00	1576080353
41 253 221 93	2017-06-27 00:00:00	73698924557	316	141.25	3.218.46	2017-07-12 00:00:00	43087706
41,253,218,70	2017-07-19 00:00:00	328114	300	141.25	3.218.23	2017-07-21 00:00:00	11830691
41, 253, 218, 42	2017-06-29 00:00:00	2819808079	297	141.25	3.218.43	2017-07-27 00:00:00	6342041913
41 253 221 85	2017-07-11 00:00:00	656252875	290	141.25	3.221.216	2017-07-09 00:00:00	1434075
41 253 221 11	2017-07-19 00:00:00	309193482	288	141.25	3.221.217	2017-07-18 00:00:00	1708558
41 253 221 110	2017-06-29 00:00:00	5214579	243	141.25	3.221.204	2017-07-01 00:00:00	2167311
141 253 221 14	2017-08-05-00:00:00	29090	238	141.25	3.218.21	2017-07-12 00:00:00	13704535
1/11 253 218 26	2017-07-22 00:00:00	3/8575	223	141.25	3.221.168	2017-07-03 00:00:00	544848062
	2017-07-07 00:00:00	2610314	201	141.25	3.218.38	2017-07-06 00:00:00	53101056
141 252 219 22	2017-07-19-00:00:00	2/9701	100	141.25	3.221.26	2017-07-17 00:00:00	31173
41 253 221 136	2017-07-17 00:00:00	11/1858/180	197	141.25	3.221.224	2017-06-29 00:00:00	1658847797
	2017-07-17 00:00:00	4700411	197	141.25	3.221.13	2017-07-31 00:00:00	25232
141.253.221.175	2017-07-27 00:00:00	110774606	107	141.25	3.221.145	2017-07-09 00:00:00	630447
	2017-07-10 00.00.00	1606455	176	141.25	3.221.111	2017-07-31 00:00:00	2851536
	2017-08-03 00.00.00	42260027	160	141.25	3.221.99	2017-07-03 00:00:00	5187925647
41.255.210.49	2017-07-21 00.00.00	43309027	100	141.25	3.218.71	2017-07-07 00:00:00	7344492
41,255,218,33	2017-07-19 00:00:00	501252824	158	141.25	3.221.218	2017-07-19 00:00:00	1120448
41,253,221,106	2017-07-11 00:00:00	508553708	151	141.25	3.221.116	2017-07-09 00:00:00	1302187
141.253.218.72	2017-07-11 00:00:00	198419914	149	141.25	3.221.94	2017-07-03 00:00:00	1864104
141.253.221.219	2017-08-06 00:00:00	1/09312	144	141.25	3.221.169	2017-07-27 00:00:00	356856
141.253.218.102	2017-06-30 00:00:00	1646/988	139	141.25	3.221.137	2017-07-10 00:00:00	2143425
141.253.221.7	2017-06-29 00:00:00	160/262	138	141.25	3.221.121	2017-07-17 00:00:00	27156
141.253.218.31	2017-07-30 00:00:00	302123708	130	+		+	-+
41.253.221.60	2017-06-30 00:00:00	8676876	126	90 rows	in set (0.)	69 sec)	

And, in order to further identify the cause of a jump in traffic volume towards a given own system, the following query is meaningful:



Once again, the result is ambiguous. The 8 GB big ingress peak to the HTTP server from the Ukraine system is accompanied by quite more normal traffic patterns exchanged with peers from the same DNS domain, and belonging to the same class B address.

- So either this Ukraine-based Organisation is a normal partner. And one of their system has once provided us a big amount of data.
- Or all these systems were jointly participating to an attack attempt

2017-08-06 141,253,221,27 cs2devipf.xi.company.com. http tcp 852251572 0 579,120,172 Ukraine OTHER A528005 A528	+ PeakDay	Local	LocalName	Svc	Pro	Ingress	Egress	Remote	Country	City	ASN	DNS
2017.08.06 141.253.221.27 cs2devinf.xi.company.com http://to./	2017-08-06 2017-08-06 2017-08-06 2017-08-06 2017-08-06 2017-08-06 2017-08-06 2017-08-06 2017-08-06 2017-08-06	141.253,221.27 141.253,221.27 141.253,221.27 141.253,221.27 141.253,221.27 141.253,221.27 141.253,221.27 141.253,221.27 141.253,221.27 141.253,221.27 141.253,221.27	cs2devipf.xi.company.com. cs2devipf.xi.company.com. cs2devipf.xi.company.com. cs2devipf.xi.company.com. cs2devipf.xi.company.com. cs2devipf.xi.company.com. cs2devipf.xi.company.com. cs2devipf.xi.company.com. cs2devipf.xi.company.com. cs2devipf.xi.company.com. cs2devipf.xi.company.com.	http http http http http ftp ftp http	tcp tcp tcp tcp tcp tcp tcp tcp tcp	8822351872 73744 14919 3602 2736 1834 1283 1089 815 786	0 0 12045 1501 1748 1097 1201 1645 1999 1413	54,78,120,172 5498,125,184 5529,127,176 558,124,156 359,124,156 359,124,156 359,224,156 359,224,055 359,224,055 357,224,95,106 57,94,123,40 52,524,51,06 57,94,123,40 52,524,51,06 57,94,123,40 57,51,06 57,94,123,40 57,51,06 57,94,123,40 57,51,06 57,52,50 57,51,06,50,50,50,50,50,50,50,50,50,50,50,50,50,	Ukraine Ukraine Ukraine Ukraine Italy Ukraine Canada Seychelles Ukraine	OTHER OTHER OTHER OTHER Milan OTHER Toronto OTHER OTHER OTHER	AS2800 or respectively formed Ltd. AS2800 of the series of the series Ltd.	<pre>constant int int int int int int int int int i</pre>

Anyway, this type of second step query is so classical in conducting security audit of the trafMon collected observations, that is has also been implemented as the stored procedure

```
`trafMon_SecurityProcs`.`Top_IngressTo`(_DBname, _Date, _Local, _topN)
```

Although trafMon is counting a large amount of ingress packets and bytes from the remote system on Aug 6th, 2017, no single corresponding egress packet is counted for that day. It may be due to the saturation of the switch span port that fed the probe (which occurred regularly). However, related suspicious security patterns, in two directions this time, have been observed the day before.

Indeed, on Aug 5th, this remote system behaved like a scanner: mostly very few small packets exchanged with several own systems of the same address segment. Note also that the set of related remote peers, from the same class B, appear in **15 917 rows** of our *lowTraffic* table, and <u>only during the two consecutive days</u>: 5 and 6 Aug, 2017!



+ flowID	rangeStart	lower	upper	minimum	maximum	average	population	sum
+ 2009 120 172 bigh<141 253 218 33 80 ten trafmon-loc-prb-dmz:p2n1	2017-08-05 00:00:00	1 0	200	44	44	44	6	264
9 120 172 high 141 253 221 109 80 tcp trafmon-loc-prh-dmz p201	2017-08-05 00:00:00	i õ	200	44	44	44	4	176
9,120,172;high<141,253,221,110;80,tcp_trafmon-loc-prb-dmz;p201	2017-08-05 00:00:00	iõ	200	44	44	44	6	264
9,120,172;high<141,253,221,117;80,tcp_trafmon-loc-prb-dmz;p201	2017-08-05 00:00:00	i õ	200	44	44	44	6	264
© .120.172:high<141.253.221.12:80 tcp trafmon-loc-prb-dmz:p2p1	2017-08-05 00:00:00	i o	200	44	44	44	9	396
9.120.172:high<141.253.221.134:80 tcp trafmon-loc-prb-dmz:p2p1	2017-08-05 00:00:00	i o	200	44	44	44	6	264
9.120.172:high⇔141.253.221.105:80 tcp trafmon-loc-prb-dmz:p2p1	2017-08-05 00:00:00	0	200	40	44	43.4286	7	304
%(5,99.120.172:high<>141.253.221.109:80 tcp trafmon-loc-prb-dmz:p2p1	2017-08-05 00:00:00	0	200	40	44	43.3333	12	520
9.120.172:high<>141.253.221.110:80_tcp_trafmon-loc-prb-dmz:p2p1	2017-08-05 00:00:00	0	200	40	44	43.4286	7	304
微調9.120.172:high<>141.253.221.117:80_tcp_trafmon-loc-prb-dmz:p2p1	2017-08-05 00:00:00	0	200	40	44	43.4286	7	304
% %9,120,172:high<>141.253.221.12:80_tcp_trafmon-loc-prb-dmz:p2p1	2017-08-05 00:00:00	0	200	40	44	43.3333	18	780
10,309.120.172:high<>141.253.221.134:80_tcp_trafmon-loc-prb-dmz:p2p1	2017-08-05 00:00:00	0	200	40	44	43.4286	7	304
<pre>%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%</pre>	2017-08-05 00:00:00	0	200	40	44	43.4286	7	304
9.120.172:high<>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1	2017-08-06 00:00:00	0	200	40	178	62.34	100	6234
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	2017-08-06 00:00:00	200	400	237	334	269.333	21	5656
A 339 120 172 high <>141 253 221 31 80 tcp_tratmon-loc prb-dmz:p2p1	2017-08-05 00:00:00	0	200	40	44	43	4	172
<pre>/ 0.120.172:high>141.253.221.110:80_tcp_tratmon-Loc-prb-dmz:p2p1</pre>	2017-08-05 00:00:00	0	200	40	40	40	1	40
9.120.172:h1gh>141.253.221.117:80_tcp_tratmon-Loc-prb-dmz:p2p1	2017-08-05 00:00:00	0	200	40	40	40	1	40
3. 39.120.172:high>141.253.221.12:80_tcp_tratmon_loc-prb-dmz:p2p1	2017-08-05 00:00:00	0	200	40	40	40	<u>+</u>	40
3, 349, 120, 172; high>141, 253, 221, 134; 80_tcp_tratmon-Loc-prb-dmz; p2p1	2017-08-05 00:00:00	0	200	40	40	40	1	40
9.120.172:high>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1	2017-08-06 00:00:00		200	52	144	81.9921	12/	10413
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	2017-08-06 00:00:00	200	400	212	389	2/2.083	12	3265
1 1/2 1/2 1/2 1/2 1/2 1/2 1/2 1/2 1/2 1/	2017-08-06 00:00:00	400	600	405	596	546.857	42	22968
1 3 3 3 9.120.172:high>141.253.221.27:80_tcp_traimon-toc-prb-dm2:p2p1	2017-08-06-00-00-00	800	1000	019	799	000 957	2/	18907
1 25 269 120 172 high=141 253 221 27:80 tcp_trafmon_loc_prb_dm2:p2p1	2017-08-06-00-00-00	1000	1200	1016	1102	1026 61	124	445550
See 120, 172, high=141, 253, 221, 27, 80 top_trafmon_loc.prb.dmz;p2p1	2017-08-06 00:00:00	1200	1400	1010	1206	1220.01	434	27922
3339 120 172 high=141.253.221.27.80 tcp_trafmon_loc.prb.dmz.p2p1	2017-08-06 00:00:00	1400	65535	1416	1500	1500	5189370	778/050000
+	2017-00-00-00.00.00	1400	000000	1410	1500	1500	5165570	·/····



4. SECURITY SUMMARY

Although the presented security investigations are by far not exhaustive, quite a lot of interesting results have been obtained by concentrating on low profile daily traffic and on explosion of daily peak ingress volume.

Hence it is time to formalise the first step of the investigation as a series of MySQL stored procedures. An example synthesis report can be drawn, which presents only the most visible tip of the iceberg; hence the security auditor should most extensively browse to every occurrences of suspicious patterns.

4.1 STORED PROCEDURES

As said above, two stored procedures are preparing the base data in two persistent tables (*lowTraffic* and *in_VolumeExtern*). These should be regularly called for maintaining those tables up-to-date:

```
`trafMon_SecurityProcs`.`Refresh_lowTraffic`(IN `_DBname` VARCHAR(20))
```

see above

```
`trafMon_SecurityProcs`.`Refresh_ExternInPeaks`(IN `_DBname` VARCHAR(20))
```

see above



One routine, called once per investigation, prepares a temporary table that supports the scanners related analysis:

```
-- For those IP addresses that are NOT private (10.x.x.x, 192.168.x.x
-- from 172.16.0.0 to 172.31.255.255), and that are NEITHER assigned
-- an Activity NOR a Location (i.e. Peers on the Internet, not belonging
-- to known universe of the Organisation's own systems),
-- sum-up the packets and bytes exchanged in both directions ('<' and '>')
-- from the table storing the daily distribution of packet sizes.
-- Keep only those "low profile" remote peers exchanging up to _maxPkts
-- and up to _maxBytes with each own system.
-- TABLE lowTraffic already contains this for highest possible boundaries:
-- _____maxPkts =30 and __maxBytes = 3000
CREATE TEMPORARY TABLE scansFrom
     SELECT * FROM lowTraffic
       WHERE pkts <= _maxpkts AND bytes <= _maxBytes;
-- Intermediate table with pairs of remote/local and number of occurrences
-- of each
CREATE TEMPORARY TABLE scansPairs (remote VARCHAR(18), local VARCHAR(18),
ct_rem INT, ct_loc INT,
country VARCHAR(30), city VARCHAR(30),
                                             DNS VARCHAR(100), ASN VARCHAR(80));
INSERT INTO scansPairs
     SELECT remote, local, COUNT(remote) as ct_rem, COUNT(local) as ct_loc,
           country, city, DNS, ASN
FROM scansFrom GROUP BY remote, local
```



This scanners analysis is implemented by the three procedures:

```
`trafMon_SecurityProcs`.`Top_Scanners`(_DBname, _maxPkts, _maxBytes, _topN)
```

```
-- Count the number of different local own systems that are reached by
-- each "low profile" remote peers
CREATE TEMPORARY TABLE wideScanners
  SELECT remote, COUNT(local) as count_of_local_hosts, country, city, DNS, ASN
     FROM scansPairs
     GROUP BY remote
    ORDER BY count_of_local_hosts DESC, INET_ATON(remote) ASC;
-- Retrieves those remote scanners whose number of scanned own systems
-- is within the Top-N
-- First: which is the Top-N lowest value ?
SET @min_N = (SELECT MIN(count_of_local_hosts) FROM
  (SELECT DISTINCT count_of_local_hosts FROM wideScanners
        ORDER BY count_of_local_hosts DESC
        LIMIT _topN) A );
- -
-- Then retrieves the remote systems scanning as much as `Top-N lowest value'
-- different own systems or more
SELECT remote, count_of_local_hosts, country, city, DNS, ASN
  FROM wideScanners
  WHERE count_of_local_hosts >= @min_N;
```

`trafMon_SecurityProcs`.`Top_Scanned`(_DBname, _maxPkts, _maxBytes, _topN)

- --- Count the number of different remote peers that are reaching -- each own system with "low profile" exchanges CREATE TEMPORARY TABLE wideScanned SELECT local, COUNT(remote) as count_scanners FROM scansPairs GROUP BY local ORDER BY count_scanners DESC, INET_ATON(local) ASC; -- Retrieves those scanned own systems whose number of remote scanners -- is within the Top-N -- First: which is the Top-N lowest value ? SET @min_N = (SELECT MIN(count_scanners) FROM (SELECT DISTINCT count scanners FROM wideScanned ORDER BY count_scanners DESC LIMIT _topN) A); -- Then retrieves the remote systems scanning as much as `Top-N lowest value' -- different own systems or more SELECT local, DNS, count_scanners FROM wideScanned, ipinfotable WHERE count_scanners >= @min_N AND local=IP



- -

`trafMon_SecurityProcs`.`Top_ActiveScanners`(_DBname, _maxPkts, _maxBytes, _topN)

-- Count the number of times each low-traffic remote scanner has -- reached, within a day, one of the own systems --SELECT remote, SUM(ct_loc) as count_of_scans, country, city, DNS, ASN FROM scansPairs GROUP BY remote ORDER BY count_of_scans DESC LIMIT topN

Two other procedures are involved by first search for bombarding remote systems:

`trafMon_SecurityProcs`.`TopJumps_DailyPeak`(_DBname, _maxPkts, _maxBytes, _topN)

-- Computes the jump between daily peaks from the in_VolumesExtern -- already ordered by increasing peaks CREATE TEMPORARY TABLE in_VolumesExtern_jump SELECT local, rangestart, in_bytes, @delta:= IF(@prevAddr <> local, 0, @prevBytes) as prev_bytes, @prevAddr:= local, @prevBytes:= in_bytes FROM in_VolumesExtern, (SELECT @prevAddr:='') b, (SELECT @prevBytes:= 0) c; -- Retrieves those days where each own systems receives its top peak -- or external systems data CREATE TEMPORARY TABLE in VolumesExtern max SELECT local, MAX(in_bytes) AS max_in_bytes FROM in_VolumesExtern_jump GROUP BY local; -- Keeps those lines with the per own system top peak and previour top peak -- and computes the pecentage of the jump between the two top peaks 2.2 -- Where the jump percentage is high (e.g. > 100 %), it is sustected that the -- corresponding own system has been bombed on that top peak day. -- ==> Its corresponding traffic requires further inspection SELECT a.local, rangestart, in_bytes, ROUND((in_bytes / prev_bytes) *100) AS jump_pct
FROM in_VolumesExtern_jump a, .in_VolumesExtern_max b WHERE a.in_bytes = b.max_in_bytes AND a.local = b.local AND in_bytes > prev_bytes AND prev_bytes > 0 ORDER BY jump_pct DESC;



And, in order to further identify the cause of a jump in traffic volume towards a given own system, the following query is meaningful:

```
`trafMon_SecurityProcs`.`Top_IngressTo`(_DBname, _Date, _Local, _topN)
```

 Retrieves the TopN remote senders to the given local own system and order them by decreasing ingress volume
<pre>SELECT DATE(rangeStart) AS PeakDay, address1 AS Local, dns1 AS LocalName, sPro As Svc, Pro, in_bytes as Ingress, out_bytes as Egress, address2 AS Remote, Country, City, ASN, DNS FROM activityvolumetable_aggr_1d a, ipinfotable b WHERE rangeStart = _Date AND address1 = _Local AND (location2 = 'N/A' OR location2 IS NULL) AND (activity2 = 'N/A' OR activity2 IS NULL) AND address2 NOT LIKE '10.%.%.%' AND address2 NOT LIKE '192.168.%.%' AND INET_ATON(address2) NOT BETWEEN INET_ATON('172.16.0.0') AND INET_ATON('172.31.255.255') AND address2 = b.IP OPDERE RY Ingress DESC LIMITtopN:</pre>



5. DRAWING A SAMPLE BIRT REPORT TEMPLATE

We take party of this illustrative tutorial on security auditing examples and, in particular, on the above presented set of stored procedures extracting the Top-N most significant patterns, to give a <u>practical example on how to create your own BIRT report template</u> based on trafMon collected observations.

5.1 BIRT DESIGNER SETUP

- Download and install the <u>BIRT Designer</u>: preferably within Eclipse, to have a workspace with the trafMon project and its structure with the report templates and subdirect.
- Copy the hierarchy of all. rptdesign files and its sub-directories Library/ and Scripts/
- Create a <u>new report called</u> "SecuritySynthesis.rptdesign"
- In the Resource Explorer, drag the <u>Shared Resources/Library/trafMonDb.rptlibrary/Data</u> <u>Sources/trafmonDb</u> to the Data Explorer <u>Data Sources</u>. This defines the connection to the database
- In the *Resource Explorer*, drag the <u>Shared Resources/Library/trafMonDb.rptlibrary/Report</u> <u>Parameters/**DBname**</u> to the *Data Explorer* Report Parameters
- In the *Data Explorer*, add three additional Report Parameters: "**max Daily Packets**" (Integer, default 20), "**max Daily Bytes**" (Integer, default 2000) and "**top N**" (Integer default 5).

5.2 DATA SETS FROM STORED PROCEDURES

Create a Data Set "**Top_ActiveScanners**" with the sole available Data Source.

- Query: CALL trafMon_SecurityProcs.Top_ActiveScanners('trafMon', 10, 1000, 5)
- Property Binding:

"CALL `trafMon_SecurityProcs`.`Top_ActiveScanners`(""

+params["DBname"].value+"","+params["max Daily Packets"].value

+","+params["max daily Bytes"].value+","+params["top N"].value+")"

Create a Data Set "**Top_Scanners**" with the sole available Data Source.

- Query: CALL trafMon_SecurityProcs.Top_Scanners('trafMon', 10, 1000, 5)
- Property Binding:

"CALL `trafMon_SecurityProcs`.`Top_Scanners`(""+params["DBname"].value

+"","+params["max Daily Packets"].value+","

+params["max daily Bytes"].value+","+params["top N"].value+")"

© 2020 AETHIS sa/nv Belgium	-	All rights reserved	-	trafMon Use Case 3: Security Auditing
Document version 1.0, 2020-12		Open Source Apache Licen	se v2.0	Page: 45/58



Create a Data Set "**Top_Scanned**" with the sole available Data Source.

- Query: CALL trafMon_SecurityProcs.Top_Scanned('trafMon', 10, 1000, 5)
- Property Binding:

"CALL `trafMon_SecurityProcs`.`Top_Scanned`("'+params["DBname"].value +"","+params["max Daily Packets"].value+","

+params["max daily Bytes"].value+","+params["top N"].value+")"

Create a Data Set "**TopJumps_DailyPeak**" with the sole available Data Source.

- Query: CALL trafMon_SecurityProcs.TopJumps_DailyPeak('trafMon')
- Property Binding:

"CALL `trafMon_SecurityProcs`.`TopJumps_DailyPeak`("" +params["DBname"].value+")"

Create a Data Set "**Top_IngressForLocalIP_Date**" with the sole available Data Source.

- Query: CALL trafMon_SecurityProcs.Top_IngressTo(?, ?, ?, ?)
- Parameters:
 - **db**, String, Linked to Report Parameter *DBname*
 - peakDate, String, Default Value 2017-07-12 00:00:00
 - **peakLocalIP**, String, Default Value 141.253.12.3
 - **topN**, Integer, Linked to Report Parameter *top N*

Create a Data Cube "Scanners by Country" with Primary dataset: Top_Scanners

- Drag **country** to *Groups* (Dimensions)
- Drag count_of_local_hosts to Summary Fields (Measures)
- Drag **remote** to *Summary Fields (Measures)*



🔅 Palette	β Data Explorer 😒
🗸 🚞 Dat	a Sources
	trafMonDb
🗸 🚞 Dat	a Sets
> 8	Top_ActiveScanners
> 8	Top_IngressForLocallP_Date
> 8	Top_Scanned
> 8	Top_Scanners
> 9	TopJumps_DailyPeak
🗸 🚞 Dat	a Cubes
> 😂	Scanners by Country
🗸 💼 Rep	ort Parameters
{ ì	DBname
{}	max Daily Packets
{}	max daily Bytes
{}	top N
🖬 Vari	ables

e drag fields from the availab	ole data sets to grouping hierarchies and summary data fields.			
Data Set Groups and Summaries Link Groups	Groups and Summaries			
	Available Fields:	Groups and Summaries: Groups (Dimensions) (Drop a field here to create a group) Countries Country Summary Fields (Measures) (Drop a field here to create a summary field) Summary Field Count_of_local_hosts(SUM) Summary Field Fremote(COUNT)	Ac Ec Del	b



5.3 DRAWING THE STRUCTURE OF THE REPORT

Warning: explicit dimensions (using units like cm or in) as well as adjusting sizes with mouse dragging do never have the expected effect:

First, the effect on the pseudo WYSIWYG Designer view is often surprising.

But more importantly, the actual generated report does not respect the intended sizes.

In addition, there is always this difference in character sizes when mapping fonts between Linux (X Windows) and Microsoft Windows.

The Best is always to dimension everything as <u>explicit percentage</u>. And this must be exhaustive: do not leave the width of the last column empty (supposing it will occupy the rest of the percentage); but assign its percentage width explicitly, in such a way to correctly reach 100% by summing all elements widths.

Create a Grid with 1 column and 6 rows: these are the main sections of your report.

- > In the top row cell, create a Grid with 1 column and 3 rows
 - In the top row cell, create a **Dynamic Text** (Bold 16):

"Top "+params["top N"].value.toString() +" most active remote scanners (with low daily traffic profile: up to " +params["max Daily Packets"].value+" packets and up to " +params["max daily Bytes"].value+" bytes)"

- In the mid row cell, create a **Text** (centered Bold 12): Based on count of # daily reaches of any of the own systems
- In the bottom row cell, create a Grid with 2 columns and 1 row
 - In the left cell (80% width), <u>drag the Data Set **Top ActiveScanners**</u>. Reorder the columns, adapt their labels. Assign percentage width (12, 8, 10, 30, 34, 6)



	62	6	Based on count	of # daily reaches of any of the own sy	vstems	
Scanner	Country	City	DNS name	Provider	#	
[remote]	[country]	[city]	[DNS]	[ASN]	[count_	
Footer Row	N		1			
e Script XML S Column 없 [ighlights	ource] Error Log	Properties			
General						

In the right cell (20% width), <u>create a pie chart</u>. Use data from: *TopActiveScanners*. Drag **count_of_scans** as <u>Slice Size Definition (Series 1</u> – on the left of the pie). Drag **remote** as <u>Category Definition</u> (below the pie) and specify <u>Descending Sorting</u>. In the *Format Chart*, <u>suppress visibility for title and Legend</u>, and <u>remove the title</u> of Value Series <u>in the Series tab</u>.

				-	
Silice Size Definition:* eries 1 $\Sigma \rightarrow row["count_of, \checkmark f_x]$		Optional Gr	ouping:	# [count_	
Category Definitio	n:* row["remote"]	Sorting Data Sorting:	Descending		~
Select Data		Sort On:	row["count_of_scar	ıs"] ·	✓ <i>f</i> _X
Olehavit Data	Inherit Columns and Grouns	Locale:	Auto		~
Use Data from		Strength:	TERTIARY		-
Data Preview Use the right-click menu to bind Show data preview	Data Preview Use the right-click menu to bind the data to chart Show data preview				
ASN		Intervali 1	•		
DNS		interval.			
city (Function: Si	um	~	
city					



- In the 2nd row cell, create a **Dynamic Text** (Bold 16): "Widest remote scanners: reaching the most (Top " +params["top N"].value.toString()+") of own systems"
- > In the 3rd row cell, create a **Text** (centered Bold 12): *Based on count of different own systems*

reached (SUM of the first column of below table)

> In the 4th row cell, create a Grid with 1 column and 2 rows

- In the top row, create a Grid with 2 column and 1 row
 - In the first columns (60%), <u>drag the Data Cube</u> Scanners by Country. Rename and restyle the columns labels (*Country, #Scanned Systems (SUM), # Scanners*). Select the <u>Chart option</u> for the 2nd column. <u>Delete the Footer</u> of this 2nd column. Select the entire <u>Cross Tab</u> and, in the below <u>Property Editor</u>, used the <u>Sorting</u> tab to add a <u>Descending sort for data["count of local hosts Countries/country"]</u>.

	Based on cou	nt of different	own systems	reached (SUM o	of the first o
	Country	Drop dat	a field(s) to defi	ne columns here	
		# Scanned Systems (SUM)		# Scann	iers
	[country]	-	Σ	[remote_Countries]] 💷
ut Master Pa operty Edito erties Bindir ort on:	nge Script XML Source r - Cross Tab 🕄 🖭 Problems 🥹 Error Log 🔲 Properties ng Row Area Column Area Map Highlights Sorting Filters				
iut Master Pa roperty Edito ierties Bindir iort on: iroup Level	age Script XML Source r - Cross Tab 🕸 🏦 Problems 🧐 Error Log 🔲 Properties ag Row Area Column Area Map Highlights Sorting Filters Key		Direction	Sort locale	Sort strength

In the 2nd column (40%), <u>create a pie chart with Use Data From Scanners by Country</u>.
 Drag the field count_of_local_hosts to the <u>Slice Size definitions / Series</u> 1. Drag the field country to the <u>Category Definition</u> and define a Descending Sorting on



count_of_local_hosts. Then, in Format Chart tab, specify a <u>Title</u>, let the <u>Legend</u> be <u>visible</u> and, in Series, <u>remove the Title of Value Series</u>.



- > In the 5th row cell, create a **Grid with 1 column and 2 rows**
 - In the top row, create a Grid with 2 column and 1 row
 - In the top row cell, create a **Dynamic Text** (Bold 16):

"Top "+params["top N"].value.toString()+" most scanned own systems"

- $\circ~$ In the bottom row cell, create a Grid with 2 columns and 1 row
 - In the left cell (50%), <u>drag</u> the Data Set **Top_Scanned**, adjust the <u>column</u> widths (28, 50 and 22 %). Re-label and re-style the <u>headings</u> (*Own Systems, DNS* name, # remote scanners).
 - In the right cell (50%), <u>create a pie chart</u> that Use Data From Top_Scanned. Drag the field count_scanners to Slice Size Definition / Series 1. Drag the field local to Category Definition, and select <u>Sorting Descending</u> on row["count_scanners"]. In Format Chart tab, <u>suppress visibility</u> of Title and of Legend; in Series, <u>remove the Title for Value Series</u>, <u>Select Value Series</u> and activate the <u>check box</u> Show Series Label.

trafMn

An open source network traffic performance monitoring and diagnostics tool.

Edit Chart		×					
Edit Chart Select the data to display	in the chart and bind it to the series.						
Select Chart Type	Select Data 📊 Format Chart						
	Chart Preview	5					
Slice Size Definition:* Series 1 Σ * row["count_sc		Optional Grouping:					
	Category Definition:* row["local"]						
	Select Data	Grouping and Sorting					
	O Inherit Data from Container Inherit Columns and Groups	Sorting					
	Use Data from Top_Scanned	Data Sorting: Descending					
	Data Preview	Sort On: row["count_scanners"] \checkmark $f_{\rm K}$					
	Use the right-click menu to bind the data to chart	Locale: Auto -10					
	Show data preview	Strength: TERTIARY					
	DNS						
	local	Grouping					
		Type: Text VInit: String VInit: Interval: 1 Function: Sum V					
		OK Cancel					

> In the 6th row cell, create a **Grid with 1 column and 2 rows**

• In the top row, create a Grid with 2 column and 1 row

0

• In the top row cell, create a **Dynamic Text** (Bold 16):

"Bombarded own systems: high jump of external ingress volume from 2nd to highest daily peak"

In the bottom row cell, create a Grid with 2 columns and 1 row

In the left cell (30%), <u>drag</u> the Data Set **TopJumps_DailyPeak**, adjust the <u>column widths</u> (30, 20, 35 and 15%). Re-label and re-style the <u>headings</u> (*Own System*, *Day*, *Ingress Bytes*, *Peak jump* (%)).

© 2020 AETHIS sa/nv Belgium	-	All rights reserved	-	trafMon Use Case 3: Security Auditing
Document version 1.0, 2020-12		Open Source Apache License	e v2.0	Page: 52/58



- In the right cell (60%), create a Grid with 1 column and 2 rows
 - In the top row cell, <u>create a pie chart</u> that Use Data From
 TopJumps_DailyPeak. Drag the field jump_pct to Slice Size Definition / Series 1. Drag the field local to Category Definition, and select <u>Sorting Descending on row["jump_pct"]</u>. In Format Chart tab, <u>suppress visibility</u> of Title but <u>keep visibility</u> of Legend; in Series, <u>remove the Title for Value Series</u>.
 - In the bottom row, <u>create a List</u> for Data Set **TopJumps_DailyPeak**. <u>Keep the fields</u> **local**, **rangestart** (the day of the top peak) and **jump_pct**. In the below *Property Editor*, in *Sorting* tab, <u>sort Descending</u> <u>on row["jump_pct"]</u>. In the below *Property Editor*, in *Filters* tab, <u>Expression</u> row["jump_pct"] <u>Operator</u> Top n, <u>Value 1</u> params["top N"].value — there will be as much elements (tables) in the list as specified by the value assigned to the top N parameter of the report. Leave the *Header* and *Footer* empty.
 - In the <u>Detail</u>, <u>drag</u> the Data Set **Top_IngressForLocalIP_Date**. In the below Property Editor, Binding tab: assign the DataSet Parameter Binding as
 - *db* is **params["DBname"].value**
 - peakDate is row["rangestart"]
 - peakLocalIP is row["local"]
 - o topN is params["top N"].value
 - Then re-organise the table:
 - Select the *Heading* row and <u>insert one row above</u>.
 - <u>Move</u> **[Local]** in *first heading row, first column*, and <u>delete</u> **Local** label.
 - <u>Move</u> [LocalName] in *first heading row, third column*, and <u>delete</u> LocalName label.
 - <u>Move</u> [Remote] and Remote label to first column.
 - <u>Move</u> [Svc] and Svc label to second column.
 - <u>Move</u> [**Pro**] on top of [**Svc**] (*at right side*): it goes to a new row, below the target; and <u>delete</u> **Pro** label.
 - <u>Move</u> [Ingress] and Ingress label to third column (below [LocalName]).
 - <u>Move</u> [City] below [Country].

© 2020 AETHIS sa/nv Belgium	-	All rights reserved -		trafMon Use Case 3: Security Auditing
Document version 1.0, 2020-12		Open Source Apache License v	2.0	Page: 53/58



- Move [ASN] below [DNS].
- Delete the useless columns.
- <u>Rename</u> and re-style the *heading labels*: *Remote, Svc, Ingress, Egress Country/City, DNS/Provider* (respectively 13, 5, 10, 10, 31 and 41 % width).

-1							
	🗆 📄 Header						
	[Local]		[LocalN:	ame]			
	Remote	Svc	Ingress	Egress	Country/City	DNS/Provider	
	[Remote]	[Svc]	[Ingress]	[Egress]	[Country]	[DNS]	
		[Pro]			[City]	[ASN]	
	Footer Row						
	E Footer						

5.4 INSTALLING AND EXECUTING THE NEW REPORT

You can now copy your SecuritySynthesis.rptdesign report template to /var/lib/tomcat/webapps/birt/trafMon_reports/

Then invoke it via the URL (supposedly your Tomcat installation is reached via http://localhost:8080/):

http://localhost:8080/birt/run?__report=trafMon_reports/SecuritySynthesis.rptdesign

This will pop-up a form querying values for the four report parameters



() Enter da	tabase name: *		
trafMon	5		
() max Dai	y Packets: *		
20			
() max dail	y Bytes: *		
2000			
() top N: *			
5			



K	TRAFMO	N Security Synthesis		
after	$\rightarrow \rightarrow \rightarrow$			
÷				
op 5 mos	st active remote	e scanners (with low daily	traffic profile: up to 20 pa	ackets and up to 2000 bytes)
		Based on count of	# daily reaches of any of the own s	systems
anner 30.43.31.2	Country City United Mount	DNS name	Provider AS11	# 5475
(38.77 (42.125.159	States Vernon China Hangzhou 9 Japan Tokyo	(nl. 38.77 159 members linode.com.	AS41.4379.5375 AS634.4 747.5375.0C	1782
32.111.147 13.65.58	7 Japan Tokyo China Jinan	2/ 04-147.members.linode.com. 2021 #33.65.58	AS635 AS48 AS48 P China169 Ba	1357 ackbone 1181
Videst re	mote scanners:	reaching the most (Top 5) of own systems	adawa of holow table)
	Country	# Scanned	# Scanners	Dia il celow table)
	United States	Systems (SUM)	88	Distribution of widest scanners
	China		34	United State
	France	- E	9	France Japan
	Japan	i i	8	Russia
	Russia	1	6	
	Republic of Korea	1	5	
	Germany	1	5	
	Netherlands	1	3	
	Ukraine	1	2	
	Taiwan		2	
	Israel	T	2	
	Hong Kong	1	1	
	Puerto Rico	1	1	
	Vietnam	1	1	
	OTHER	1	1	
	Switzerland	1	1	
	Seychelles	1	1	
	Spain		1	
	1200000	100		



#	Scanner	Country	City	DNS Name	Provider
83	225927.180.164	United States	OTHER	180.164	AS1340klaste Quasiunications
83	0.44	United States	San Francisco		ASI're deres in, Inc.
83	0.183	United States	San Francisco	com.	ASIs and a start and a start and a start a sta
83	\$632.37	United States	San Francisco	-07-03-8/- 5/# (mail com	AS15 Asis and Inc.
83	(2.3.91.118	United States	Fremont	18.mem . 18.mem	AS6 million and a state
83	106.170	United States	Fremont	170 mer ale state com	ASSISTER
83	6.3.158	United States	Fremont	WESSERV5-is.e. A Set The Actoring in	AS62.732 26-562 252
83	624948.204.173	China	Nanjing	92532 204.173	AS4 - States
83	\$ 18./1.100	Hong Kong	Central District	W 466 /1.100	AST AND SHOW FOR New World Telephone Ltd.
83	Sec. 1.38.77	China	Hangzhou	2010-00-08.77	A54 16 / 19 (6) (4)
83	30,051.38.78	China	Hangznou	Francis 105 70	AD4 Caller and Caller
00	2.120.193.22	China Ducata Dian	Wunan	5.7 198 193 22 ·	ADT 19 CROMMENT
00	10162	United States	Chandler.	2 0 162	A SATURA STANDARD THE PUBLIC RECO
02	102 204	United States	San Diago	1000 1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0	A S Land Cold American Street
83	02.204	Russia	OTHER	12 21-54-25 to 2-10 4-64% anaramah m	A CALIFORNIA CONTRACTOR
83	And on 143 243	Natharlands	OTHER	where worldback and a space we state	A SAUSSIN IN CRASSICUS B V
83	8.132.3	Republic of	OTHER	132.3	ASIA
	14 P	Korea	Station 1		and the second
83	36,168,20	United States	San Francisco	101-05-31-1 1 5 42 948, com	AS14 Stockerstown Inc.
83	36.177.92	United States	San Francisco	12034-07-03-2126-00 (00-com	ASI Carlos Andreas Ann. Inc.
83	Apr +36.182.70	United States	San Francisco	Media - 05-31-27	ASI we want in Inc.
83	36.188.93	United States	San Francisco	107-03-45 (sec. 23) com	ASI Store States and Inc.
83	36.191.42	United States	San Francisco	1516414-05-31-32	AS1 and the second for the second sec
83	36.191.171	United States	San Francisco	14.160-07-03-1 (14-2) com	AS1 20 Asta fan Inc.
83	70.200.227	United States	San Francisco	New Porker-0 William Schoid.com	AS1 A Long Inc.
83	70.222.100	United States	San Francisco	conter-0 conter-0 conter-0	AS1 to a Anter Ant
83		United States	San Francisco	www.worker-0	AS1 total Automation Inc.
83	73.250.103	United States	Buffalo	and 3-250-11 group rossing.com	AS3 CT AVALANCE
83	(284.56.81	China	Beijing	\$rxy(\$4.56.81	AS5 20 Achang Network Security Technology Co.,Ltd.
83	109.20	China	Guizhoumanzuxi	e	AS4 Strategy
83	45.148.153	China	Foshan	6.148.15	AS15 Total Asia State Control of
83	45.148.158	China	Foshan	gi and 6.148.157	ASI AND AND T Guangdong province network
83	2.229.18	China	Hangzhou	s)-d2-229.18	AS43 China169 Backbone
83	10 (14.84.10	China	Zhengzhou	4.84.10	AS40 China109 Backbone
83	2 a 7:0.157.43	Vietnam	Hanoi	in inpr.vn.	AS4000 BORNESS AND
83	80.00.08	China	Jinan		AS452 0 20 20 20 China109 Backbone
83	49.20.14	China United States	Shenzhen	200 909 20.14 201 - 240 22 20 20 20 20 20 20 20 20 20 20 20 20	AST STATES
83	57-748.22.79	United States	Scottsdale	11-1-1-148-12-1499 (Avgegervernet.	ASZ
83	NOT 146 252 10	Germany	Aacnen	sacren nscans. () - rae () - ga acnen. de.	A SH Weize Har Stewart University
0.0	19 40.233.19	Germany	Talma	Statistic set and set a	AS1/2012 West Contention
0.0	62 100.257	Japan	Tokyo	Service 147 meet Victoria and	A DECEMBER OF THE STATE OF THE
0.0	2 1/ 62 114 154	Tanan	Tokyo	181 TAX 154 mant a statistic com	A SAMAA STRUCTURE AND AND A SAMA STRUCTURE
83	19:00 62 125 00	Tanan	Tokyo	(a) and manufactoria from	156 West methods in
83	62 125 159	Japan	Tokyo	History 150 met 10734 Mail com	AS6 de la companya de
83	5 05 64 239	Russia	Moscow	-12:12:55.64.239	AS42 AS42 AS42 AS42 AS42 AS42 AS42 AS42
83	AM -32.91.0	France	OTHER	st what 164-132 man and	ASIdosector
83	32.91.12	France	OTHER	2001-164-13 and 40	ASI
83	29.3.91	United States	Berkelev	Stavishescan1 Ber Handwey EDU.	AS2 ¹²
83	30.157.42	United States	Fremont	Constantory9-sc. of the Withershittoring in.	AS6 with a second
83	SE 53.227.152	China	Shanghai	\$54. 58.227.15	AS4 (Second Group)
83	8.77.208	China	Beijing	1 1 1 77.208	AS2 A State Felecommunications Corporation
83	29.160.229	China	OTHER.		AS4 sector
83	2g. e0.4.190	Russia	OTHER	4.190	AS5+24 122 Age av rePlus LLC
83	\$4-\$6.249.136	Russia	Moscow	249.13C	AS6 as5-74-56 mited
83	303 5.113.151	United States	Los Angeles	20 113.151 38 (mart com.	ASS IN TRANSPORT
83	26.23.152.89	United States	Salt Lake City	264 152.89	AS4
83	00,000,0152.104	United States	Salt Lake City	152.104	AS42 A State of Anology Services Santa Clara, LLC
83	282709.152.118	United States	Salt Lake City	17 18 132.118	A Structure Santa Clara, LLC
00	20.130.4	United States	San Diego	5000000100.4 500000000000	ASI AND AND A SI-TIC
00	10100 AD 31.2	China	Mount vernori	2010 12 - DO	A CALLER THE ALSO
00	0.20	China	Nanjing	2-02-12-20 	ADT TALKONDOL
22	108 (050 50 4	Republic of	Secul	2000	4 SOUND Strange Total of Co I to
1 °°	W.F.C. Secondary	Korea		Solard Strength	and a state of the
83	1040 - A1 200 108	China	Shenzhen	945/st 200 108	AS1 Store Live Shenzen network
83	1 1 22 105 50	Republic of	OTHER		AS40 as was the same
	Sec. Sec. 19 2.2.2	Korea	O III DIA	1201 / Print	and the strated (Switching
83	86.34.44	China	Naniing	66. 65.34.44	AS2 ANA ANA for CHINANET itangsu province backbone
83	\$6.34.144	China	Nanjing	15 1:35.34.144	AS2 3 for CHINANET itangsu province backbone
82	82.199	United States	Boydton	\$2.199	ASS AND AND Provide Providence
82	\$5.201.172	United States	Chevenne	Starte Arm. com.	AS4400 KING SILC
82	ftered.2.237	United States	San Francisco	com.	AS1 States in Inc.
82	4.114	United States	San Francisco	10154-06-23-10 an area com	ASI AND ASIA MAIN, Inc.
82	12:00:4.236	United States	San Francisco		AS1, an and an Inc.
82	\$ 5.53	United States	San Francisco	16/3.9 -06-23-5 - 19 9 9 - 2 - 0m	AS1200 Con Inc.
82	97-9.5.240	United States	San Francisco		AS1 AND AND AND INC.
82	Te. 6.203	United States	San Francisco	1 48 05-31-1 2 2 2 2 - 1 com.	ASI No. 19 St. 7 St. Inc.
82	A 12.7.57	United States	San Francisco	1. com.	AS14.43. 2004.0(-\$, m, Inc.
82	7.141	United States	San Francisco	and the last of th	ASI was free of the second sec
82	(<u>)</u> 0 (.9.114	United States	San Francisco	47:12-24-14-5 47:144242 com.	AS123 No. 1 An. Inc.

© 2020 AETHIS sa/nv Belgium Document version 1.0, 2020-12 -

All rights reserved -Open Source Apache License v2.0 trafMon Use Case 3: Security Auditing Page: 57/58



79 (XS2) 3.200	United	States San Fran	CISCO THE	(199-UD-31-09.9)。	\$4.00 H	sim.		AS16652	scenet seven, inc.
70 15 17 103	France	OTHER		27-15-51 retrief	Sec. the	way com		ASTWORNS	States Street
70 64 100 52 14	2 China	Manija	K.S. S	2 53 142	An west			ACAN	
70 3 3 3 3 3 3 7 4	a china	ryanjing	55	1177.00				A04.00.2	No. of Control of Cont
19 2 2 3.1/3.0	8 Israel	OTHER	1.2	305.175.08	1. 1.	0		ASI	An winnications Ltd.
79 385 26.145.	154 United	States San Fran	cisco	1 4 - 0721d-6.5684	ALCONT .	Se. 1.		ASIW	and the second s
79 0.202	69 United	States San Fran	cisco tak	orker-07-Gib.	13863	d.com.		AS1-Seco	and the same inc.
70 3/80 2.64 1	33 France	OTHER	1.1	2-64-133 pla	A. S. C.	larom en		ASISTO	A REAL PROPERTY OF THE REAL
70	50 France	OTUPP	500	0 97 150 -6	CP-designed and	States and		ACTOSTIC	
19 20112.01.1	50 France	OTHER	30	12-07-13012-2	121.00	on on en		A DI DE C	Sector Sector
19 24 9 2.95.1	/ France	OTHER	100		网络中国	psym.eu.		ASIZ	Que Anno 1997
79 234 106.1	62 China	Nanjing	20	×.106.162				AS2.8 5.5	for CHINANET jiangsu province backbone
79 36.50.1	77 China	Nanjing	200	6.50.177				AS22424	www.wow.cor CHINANET jiangsu province backbone
The second		and a second second second	1000						
1 op 5 mos	st scani	ied own sy	stems						
Own Systams		DNS name			# ren	note scenners			
141 252 218 52	i 6	inimandahara lasa	1		5741	note scamers		3.7.	31 —
141.200.210.02		omandshare.ioca	i.company.co	om.	3/41			(f).	- 5 741
141.255.218.42	1	xilogistics.local.c	ompany.com	1.	3/31				-1.1.
141.253.218.33		giserver2.local.co	mpany.com.		3610				
141.253.221.135		inflame2.xi.comp	any.com.		3376				
141 252 219 65		mime karisma las	al company	com	2260			2 (10	
141.255.218.05		munis-karisma.iot	ar company.	com:	3300			3,010	
141.253.221.110		savoir.company.c	om.		3300				
									3 360
									2,200
								2.276	
								0/ درد	
									- 3,360
									100 S 40 * 54 S2
Demberl	1		: _ l. :				- I 6	and the last	tabast dathers als
Dombarde	ed own	systems: I	ngn jur	np of exter	nal	ingress v	olume i	rom 2nd to n	lignest daily peak
Own system	Dav	Ingress Bytes	Peak			100 M			
A CONTRACTOR OF			immo			-	100		141 253 221 27
			Jump			1	100		171.000.001.01
10.0005076.200784.30			(90)						141 253 218 57
141.253.221.27	17-08-06	8822458492	4250722	2					111100-110-0
141 253 218 57	17-08-06	136744746	187237						141 253 221 109
141 252 221 100	17 08 06	220269171	17471				and the same		111100000000000000000000000000000000000
141.235.221.109	17-08-00	2505061/1	1/4/1						141.253.218.54
141.253.218.54	17-07-27	25835191	14722						
141.253.218.58	17-07-17	2944709	12108						141.253.218.58
141 253 221 103	17-07-18	250653159	11735					_	
141 252 221 21	17 07 19	670925566	11222						141.253.221.103
141.235.221.51	17-07-18	070855500	11522						
141.253.221.37	17-08-06	192924267	7490						141.253.221.31
141.253.218.25	17-08-01	18333478	7343						
141 253 218 52	17-08-06	2103061022	2048	141 253 221 1	27	cs2devinf	vi compan	V.com.	
141 363 310 36	17 08 06	10011160	2520			condeript	ancompan	, com	
141.235.216.50	17-08-00	10011100	2350	Remote	Svc	Ingress	Egress	Country/City	DNS/Provider
141.253.221.29	1/-0/-18	103094588	1802	9.120.172	http	8822351872		Ukraine	120.172. 32 2 3 1 st.
141.253.221.163	17-07-19	131157906	1497		tcp			OTHER	5 0 507 Interior Science, td.
141 253 221 170	17-08-06	78212	1473	2000 125 194	http	73744		Likraina	5 5175 184 was at wat
141 253 218 56	17-06-30	40476541	1306	1.405.123.164	nup	12/11		OTUDD	
141.255.210.30	17-00-30	404/0341	1300	Section 200	tcp			OTHER	28 28 and Interset Sate by ita.
141.253.221.134	17-07-21	250/852944	1302	A 9.127.176	http	14919	12045	Ukraine	27.176
141.253.221.35	17-07-14	23752345	1262		tcp			OTHER	Children of Intervention and the
141 253 221 90	17-06-29	73232517	1068	200 124 156	latter.	3602	1501	Likraine	100 00 124 156 / State and
141 253 221 105	17-08-06	153183662	031	177751124.130	mup	3002	1501	OTUTE	The second s
141.253.221.105	17-03-00	220240626	101		tcp			UTHER	Called and Interster and deal and
141.255.221.108	1/-0/-1/	250/48050	404	45.144.16	ntp	2736	1748	Italy	Alfred D. bilink.
141.253.221.234	17-08-06	21907	375	52 8 652 C	udp			Milan	Metrodate State
141.253.221.93	17-06-27	73698924557	316	141 253 210	17	taalharm	in local -	IN DAME COM	and the second
141 253 218 70	17-07-10	328114	300	141.233.218.3	21	100100XM	ain.iocai.co	impany.com.	to the second
141 252 219 42	17.06 20	2810808070	207	Remote	Svc	Ingress	Egress	Country/City	rovider
141.053.001.05	17-00-29	1019000019	200	18. 29 65 144	http	136723220	1255001293	SUnited States	12485-856-249-692-534-556-slehot.com
141.255.221.85	1/-0/-11	0002028/0	7011	Total States and	ten			and the second	
					ULD.			Maramille	Line of 160 Granewick
141.253.221.11	17-07-19	309193482	288	William er en	les.	0005		Marysville	169 Googram
141.253.221.11 141.253.221.110	17-07-19	309193482 5214579	288 243	2.403.65.58	https	8885		Marysville China	69 Googe 88. (1997) 3.65.58
141.253.221.11 141.253.221.110 141.253.221.14	17-07-19 17-06-29 17-08-05	309193482 5214579 29090	288 243 238	<2-y≪13.65.58	https tcp	8885		Marysville China Jinan	්ද ෝලි Googe යන 3.65.58 දේශී 27 CNC0වරුදු ආක169 Backbone
141.253.221.11 141.253.221.110 141.253.221.14 141.253.221.14	17-07-19 17-06-29 17-08-05	309193482 5214579 29090 348575	288 243 238	24, <03.65.58	https tcp ntp	8885 4332	4560	Marysville China Jinan	dev 169 Googe 38 13 65.58 2 8 9 7 CNC0ros S→9 haal 69 Backbone 2 8 9 50m91-ex 3 et 3 maanv.com.
141.253.221.11 141.253.221.110 141.253.221.14 141.253.218.26	17-07-19 17-06-29 17-08-05 17-07-22	309193482 5214579 29090 348575	288 243 238 223	्रस्य २३.65.58 (२६) २ (३.5.19	https tcp ntp udp	8885 4332	4560	Marysville China Jinan	59 Googram 3.65.58 5.57 CNC055 Straphinal 69 Backbone 5.20 Storp 1-2 Start Straphing Com. 5.21 The Bit Manuel (HO)
141.253.221.11 141.253.221.110 141.253.221.14 141.253.218.26 141.253.221.12	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07	309193482 5214579 29090 348575 2610314	288 243 238 223 201	 24g≪(3.65.58) (14, 12, 13.5.19) 	https tcp ntp udp	8885 4332	4560	Marysville China Jinan	de (169 Googe 34) (3.65.58 (2.65.7 CNCOros S= 9 nal 69 Backbone (2.65 cm91-exa) (4.7 shpany.com. (4.55 The Bit: storage, (HQ)
141.253.221.11 141.253.221.110 141.253.221.14 141.253.218.26 141.253.221.12 141.253.218.22	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19	309193482 5214579 29090 348575 2610314 348701	288 243 238 223 201 199	 24,<03.65.58 (14,)2,03.5.19 √4,03,03.5.18 	https tcp ntp udp ntp	8885 4332 3952	4560 3952	Marysville China Jinan OTHER	59 Googe 3.65.58 57 CNCOrd - Sanal 69 Backbone 53 Som91-et and the pany com 54 The Bits Source (HQ) 53.5.18
141.253.221.11 141.253.221.110 141.253.221.14 141.253.218.26 141.253.218.22 141.253.218.22 141.253.218.22 141.253.218.22	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19 517-07-17	309193482 5214579 29090 348575 2610314 348701 114858480	288 243 238 223 201 199	्रभूव्य3.65.58 (स.ज. 33.5.19 (म्रेन्ट्र 33.5.18	https tcp ntp udp ntp udp	8885 4332 3952	4560 3952	Marysville China Jinan OTHER OTHER	fer f99 Googe 54. 3.65.58 2.6 ≥ 7 CNC075 - ⇒ pinal 69 Backbone 2.10 Som91-2.5 + pinal 69 Backbone 2.10 Som91-2.5 + pinal 69 Backbone 2.10 Som92 + (HQ) 3.5.18 2.2 R
141.253.221.11 141.253.221.110 141.253.221.14 141.253.218.26 141.253.218.22 141.253.218.22 141.253.221.12 141.253.221.135	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19 17-07-17	309193482 5214579 29090 348575 2610314 348701 114858480 4788413	288 243 223 201 199 197	(4) (3.65.58 (4) (3.5.19 (4) (3.5.18 (4) (3.2.21.31	https tcp ntp udp ntp udp http	8885 4332 3952 992	4560 3952 9052	Marysville China Jinan OTHER OTHER United Kingdom	59 Googe 3.65.58 7 CNCOre - 9 na169 Backbone 20 Som91-et, etc., hpany.com. 351 The Bir - 9 sec. (HQ) 35.5.18 8 R 4 R
141.253.221.11 141.253.221.110 141.253.221.14 141.253.221.14 141.253.221.12 141.253.218.22 141.253.218.22 141.253.221.136 141.253.221.136	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19 17-07-17 17-07-27	309193482 5214579 29090 348575 2610314 348701 114858480 4788411	288 243 238 201 199 197 187	944-03.65.58 14-033.5.19 14-033.5.18 14-033.5.18	https tcp ntp udp ntp udp http tcp	8885 4332 3952 992	4560 3952 9052	Marysville China Jinan OTHER OTHER United Kingdom London	<pre>69 Googy 4 3.65.58 7 CNCOpy - Panal 69 Backbone 2005 The Bin Provide (HQ) 3.5.5.18 R cuts-grab - Styler 1 binaryedge ninja. 2004 Physics - Ph</pre>
141.253.221.11 141.253.221.110 141.253.221.14 141.253.218.26 141.253.218.22 141.253.218.22 141.253.221.36 141.253.221.173 141.253.221.36	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19 17-07-17 17-07-27 17-07-10	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696	288 243 238 223 201 199 197 187 183	444403.65.58 (44)203.5.19 (44)203.5.18 (44)202.231.31	https tcp ntp udp ntp udp http tcp	8885 4332 3952 992	4560 3952 9052	Marysville China Jinan OTHER OTHER United Kingdom London	69 Googy 5 3 85.58 5 7 CNCOro - Panal 69 Backbone 20 Som91-2 - Star, ppany.com. 5 1 The Bir Provide (HQ) 5.5.18 5 R 5 R 5 R 5 Cmra-grab - Star Manayedge ninja.
141.253.221.11 141.253.221.10 141.253.221.14 141.253.221.12 141.253.221.12 141.253.221.12 141.253.221.13 141.253.221.13 141.253.221.36 141.253.221.36	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19 517-07-17 17-07-27 17-07-10 17-08-05	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455	288 243 238 223 201 199 197 187 183 176	24-x13.65.58 (4-x)53.5.19 (4-x)53.5.18 (4-x)52.231.31 141.253.221.1	https tcp ntp udp ntp udp http tcp 109	8885 4332 3952 992 sales-ops-	4560 3952 9052 apsf.xi.con	Marysville China Jinan OTHER OTHER United Kingdom London apany.com.	69 Googy 4 3.65.58 7 CNCOpp - Panal 69 Backbone 2005 The Blue store (HQ) 4.5.5.18 R R cra-grab - Sociat I binaryedge ninja.
141.253.221.11 141.253.221.11 141.253.221.14 141.253.221.14 141.253.218.26 141.253.218.22 141.253.221.136 141.253.221.136 141.253.221.16 141.253.221.16	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19 17-07-19 17-07-17 17-07-10 17-08-05 17-07-21	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027	288 243 238 223 201 199 197 187 183 176 168	24-43.65.58 (4-23.5.19 (4-2.231.31 141.253.221.1 Remote	https tcp ntp udp ntp udp http tcp 109 Svc	8885 4332 3952 992 sales-ops- Ingress	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London apany.com. Country/City	69 Googy 54 3.65.58 5.7 CNC005 - 9 nal 69 Backbone 2009 - 10 C005 - 9 nal 69 Backbone 2009 -
141.253.221.11 141.253.221.11 141.253.221.14 141.253.211.826 141.253.218.26 141.253.218.22 141.253.221.136 141.253.221.136 141.253.221.36 141.253.221.36 141.253.221.38	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19 5 17-07-19 5 17-07-17 17-07-27 17-07-10 17-08-05 17-07-21 17-07-21	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824	288 243 238 223 201 199 197 187 183 176 168	24-43.65.58 44.253.5.19 441.253.221.1 Remote	https tcp ntp udp ntp udp http tcp 109 Svc	8885 4332 3952 992 sales-ops- Ingress 212008449	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London apany.com. Country/City United Strees	<pre>69 Googy % 3.65.38 9 9 7 CNC050 9 10 2000 2010 2010 2010 9 The Bin 200424 (HQ) 9 3.5.18 9 R 9 Charles 10 2010 2010 9 R 9 Charles 10 2010 9 Charles 10 2010 9 Charles 10 2010 9 Charles 10 2010 9 Charles 10 2010 10 Charles 10 Char</pre>
141.253.221.11 141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.12 141.253.221.12 141.253.221.130 141.253.221.130 141.253.221.16 141.253.221.16 141.253.211.80 141.253.218.49	17-07-19 17-06-29 17-08-05 17-07-22 17-07-19 17-07-19 17-07-17 17-07-27 17-07-27 17-07-21 17-07-21 17-07-19	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 coest2720	288 243 238 223 201 199 197 187 183 176 168 158	24-43.65.58 (4-5)3.5.19 (4-5)3.5.18 (42.231.31 141.253.221.1 Remote (4-5)2.1.64	https tcp ntp udp ntp udp http tcp 109 Svc https	8885 4332 3952 992 sales-ops- Ingress 217998448	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London apany.com. Country/City United States	69 Googy 5 3.65.58 7 CNCOro Service Panal 69 Backbone 2009 1 - 200 Arg Service (HQ) 1.35.18 R stra-grab Service (HQ) 1.35.18 Service (HQ) 1.35.1
141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.12 141.253.221.12 141.253.221.136 141.253.221.36 141.253.221.36 141.253.221.36 141.253.221.30 141.253.221.30	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19 17-07-17 17-07-17 17-07-17 17-07-21 17-07-21 17-07-19 17-07-11	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708	288 243 238 223 201 199 197 187 183 176 168 158 151	24	https tcp ntp udp ntp udp http tcp 109 Svc https tcp	8885 4332 3952 992 sales-ops- Ingress 217998448	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London pany.com. Country/City United States San Francisco	<pre>69 Googy 4 3.65.38 7 CNCOps</pre>
141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.12 141.253.221.12 141.253.221.136 141.253.221.136 141.253.221.16 141.253.221.16 141.253.221.18 141.253.221.106	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19 5 17-07-19 17-07-10 17-07-10 17-08-05 17-07-21 17-07-11 17-07-11 17-07-11	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914	288 243 238 223 201 199 197 187 183 176 168 158 151 149	24-43.65.58 44-253.5.19 42-231.31 141.253.221.1 Remote 45-2-21.64 45-42.124.139	https tcp ntp udp http tcp 109 Svc https tcp http	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London apany.com. Country/City United States San Francisco Ukraine	69 Googy 3.65.58 7 CNCOro 17 DNCOro 17 DNCOro 17 Dne Bill, Howage, (HQ) 13.5.18 18 18 18 19 10 10 10 10 10 10 10 10 10 10
141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.12 141.253.221.12 141.253.221.136 141.253.221.36 141.253.221.36 141.253.221.36 141.253.221.31 141.253.221.31 141.253.221.31 141.253.221.31 141.253.221.210	17-07-19 17-08-05 17-07-22 17-07-07 17-07-19 17-07-19 17-07-10 17-07-10 17-08-05 17-07-21 17-07-19 17-07-19 17-07-11 17-07-11 17-07-11 17-08-06	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914 1709312	288 243 238 223 201 199 197 187 183 176 168 158 151 149 144	24-<3.65.58 (%) 33.5.19 (%) 33.5.18 (41.253.221.1 Remote (%) 2.21.64 (%) 124.139	https tcp ntp udp http tcp 109 Svc https tcp https tcp	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London apany.com. Country/City United States San Francisco Ukraine OTHER	<pre>69 Googy 4 3.65.38 7 CNC050</pre>
141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.12 141.253.221.12 141.253.221.136 141.253.221.136 141.253.221.36 141.253.221.36 141.253.221.36 141.253.221.106 141.253.221.106 141.253.221.106 141.253.221.106	17-07-19 17-06-29 17-08-05 17-07-22 17-07-22 17-07-19 17-07-19 17-07-17 17-07-10 17-08-05 17-07-11 17-07-19 17-07-11 17-07-11 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-06 17-08-05 17-07-11 17-08-05 17-08-05 17-07-11 17-08-05 17-08-05 17-07-11 17-08-05 17-08-	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914 1709312 16467988	288 243 238 223 201 199 197 187 183 176 168 158 151 149 144 144	24-43.65.58 33.5.19 33.5.18 341.253.221.1 Remote 34.21.64 34.124.139 34.124.139	https tcp ntp udp http tcp 109 Svc https tcp http tcp	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014 1042473	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London npany.com. Country/City United States San Francisco Ukraine OTHER Ubited States	<pre>69 Googy 4 3.65.58 7 CNC0ro</pre>
141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.12 141.253.221.136 141.253.221.36 141.253.221.36 141.253.221.33 141.253.221.83 141.253.221.83 141.253.221.219 141.253.221.219 141.253.221.219	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-17 17-07-17 17-07-17 17-07-17 17-07-10 17-08-05 17-07-21 17-07-11 17-07-11 17-08-06 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-06-30 17-07-11 17-07-11 17-07-11 17-07-12 17-07-11 17-07-11 17-08-05 17-07-11 17-08-05 17-07-11 17-08-05 17-07-11 17-08-05 17-07-11 17-08-05 17-07-11 17-08-05 17-07-11 17-08-05 17-06-30 17-06-	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914 1709312 16467988	288 243 238 223 201 199 197 187 183 176 168 158 151 168 158 151 149 144 139	24-43.65.58 44-43.5.19 44-43.5.18 42.231.31 141.253.221. Remote 42-21.64 44-42.124.139 142.122.71	https tcp ntp udp http tcp 109 Svc https tcp http tcp http tcp	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014 1042473	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London Apany.com. Country/City United States San Francisco Ukraine OTHER United States	 69 Googe 4
141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.12 141.253.221.136 141.253.221.36 141.253.221.36 141.253.221.36 141.253.221.36 141.253.221.30 141.253.221.106 141.253.221.106 141.253.221.219 141.253.221.219 141.253.221.219 141.253.221.219	17-07-19 17-06-29 17-08-05 17-07-22 17-07-07 17-07-19 17-07-19 17-07-10 17-07-27 17-07-10 17-08-05 17-07-19 17-07-19 17-07-11 17-07-11 17-07-11 17-07-01 17-08-05 17-07-19 17-07-19 17-07-19 17-07-27 17-07-27 17-07-19 17-07-27 17-07-19 17-07-27 17-07-19 17-07-27 17-07-19 17-08-05 17-07-19 17-07-19 17-08-05 17-08-05 17-07-19 17-08-05 17-08-	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914 1709312 16467988 1607262	288 243 238 223 201 199 197 187 183 157 168 158 151 149 144 151 149 138	24-43.65.58 44.253.519 441.253.221.31 141.253.221.3 Remote 45.2.21.64 44.22.71	https tcp ntp udp http tcp 109 Svc https tcp https tcp https tcp	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014 1042473	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London pany.com. Country/City United States San Francisco Ukraine OTHER United States Ann Arbor	 69 Googy 4. 3.65.58 7 CNC070 Service Annual 69 Backbone 10 The Bit Strategy (HQ) 4.3.5.18 R 4.7 cmc2 and a strategy (HQ) 4.3.5.18 R 4.7 cmc2 and a strategy (HQ) 4.3.5.18 R 4.7 cmc2 and a strategy (HQ) 5.7 cmc2 and a strategy (HQ) 5.1 cmc2 and a strategy (HQ) 5.7 cmc2 and a strategy
141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.13 141.253.221.13 141.253.221.36 141.253.221.36 141.253.221.36 141.253.213.49 141.253.218.49 141.253.218.49 141.253.218.10 141.253.221.219 141.253.221.219	17-07-19 17-06-29 17-06-29 17-07-02 17-07-02 17-07-07 17-07-19 17-07-19 17-07-10 17-07-10 17-07-21 17-07-21 17-07-19 17-07-19 17-07-19 17-07-19 17-07-19 17-07-20 17-07-21 17-07-21 17-07-21 17-07-20 17-07-21 17-07-20 17-07-	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914 1709312 16467988 1607262 302123708	288 243 288 201 199 197 187 183 176 168 158 151 149 144 139 138 130	24-43.65.58 33.5.19 33.5.18 341.253.221.1 Remote 32.1.64 344.124.139 344.124.139 344.124.122.71 344.122.19	https tcp ntp udp ntp udp http tcp 109 Svc https tcp https tcp https tcp https	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014 1042473 866922	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London apany.com. Country/City United States San Francisco Ukraine OTHER United States Ann Arbor Ukraine	 69 Googe 4
141.253.221.11 141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.12 141.253.221.136 141.253.221.36 141.253.221.36 141.253.221.36 141.253.221.36 141.253.221.106 141.253.221.106 141.253.221.109 141.253.221.219 141.253.221.219 141.253.221.219 141.253.221.219 141.253.221.31 141.253.221.31	17-07-19 17-06-29 17-06-29 17-07-07 17-07-07 17-07-07 17-07-19 17-07-19 17-07-19 17-07-19 17-07-19 17-07-11 17-07-10 17-07-10 17-06-29 17-06-29 17-07-30 17-07-30	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914 1709312 16467988 1607262 302123708 212396419	288 243 238 223 201 197 187 183 176 168 158 151 149 144 139 138 130 126	24-43.65.58 44.253.221.31 141.253.221.3 Remote 2.21.64 2.22.71 2.2.124.139 2.4.122.19	https tcp ntp udp ntp udp http tcp http tcp https tcp https tcp https tcp	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014 1042473 866922	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London apany.com. Country/City United States San Francisco Ukrsine OTHER United States Ann Arbor Ukrsine OTHER	 69 Googy 4. 3.65.58 7 CNCOro Stranspany.com. 9 The Bin Stranspace (HQ) 4.5.5.18 R. stra-grab Stranspace (HQ) 4.5.5.18 R. stra-grab Stranspace (HQ) 5.5.19 R. stra-grab Stranspace (HQ) 5.5.19 R. stranspace (HQ) 5.5.10 R. stranspace (HQ) 5.5.10 Stranspace (HQ) 5.5.10 St
141.253.221.11 141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.12 141.253.221.13 141.253.221.36 141.253.221.36 141.253.221.36 141.253.218.49 141.253.218.49 141.253.218.49 141.253.218.49 141.253.218.20 141.253.221.219 141.253.221.219 141.253.221.219 141.253.221.31 141.253.221.31 141.253.221.8,31 141.253.218.31	17-07-19 17-06-29 17-06-29 17-07-22 17-07-22 17-07-27 17-07-19 17-07-19 17-07-10 17-07-21 17-07-21 17-07-21 17-07-19 17-07-19 17-07-19 17-07-19 17-07-19 17-07-19 17-07-19 17-07-19 17-07-19 17-07-19 17-07-21 17-07-19 17-07-21 17-07-21 17-07-21 17-07-21 17-07-21 17-07-21 17-07-21 17-07-21 17-07-21 17-07-21 17-07-21 17-07-21 17-07-21 17-07-19 17-07-10 17-07-19 17-07-10 17-07-	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914 1709312 16467988 1607262 302123708 212396419 8476876	288 243 228 223 201 199 197 187 183 176 168 151 144 139 138 130 126	44-43.65.58 43.5.19 44.253.221.31 141.253.221. Remote 45.2.1.64 4.44.139 4.12.122.71 4.122.19 4.122.19	https tcp ntp udp ntp udp http tcp https tcp https tcp https tcp https https tcp https htt	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014 1042473 866922 700358	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London apany.com. Country/City United States San Francisco Ukraine OTHER United States Ann Arbor Ukraine OTHER United States	 69 Googe 4. 3.65.58 7 CNC000 Service panal 69 Backbone (NC000) 7 The Bit Stronger (HQ) 7 3.5.18 8 8 8 8 9 9 9 10 bit Stronger (HQ) 10 bit Stronger (HQ
141.253.221.11 141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.136 141.253.221.36 141.253.221.36 141.253.221.36 141.253.221.36 141.253.221.106 141.253.221.106 141.253.221.106 141.253.221.106 141.253.221.106 141.253.221.219 141.253.221.219 141.253.221.219 141.253.221.219 141.253.221.80 141.253.221.810 141.253.221.800 141.253.221.8100 141.253.221.8100 141.253.221.8100 141.253.221.8	17-07-19 17-06-29 17-06-29 17-07-07 17-07-07 17-07-07 17-07-19 17-07-19 17-07-21 17-07-21 17-07-21 17-07-21 17-07-10 17-08-06 17-07-11 17-07-11 17-08-06 17-06-29 17-07-19 17-07-19 17-07-19 17-07-20 17-07-20 17-07-21 17-07-20 17-06-29 17-07-19 17-07-19 17-07-19 17-07-30 17-07-	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914 1709312 16467988 1607262 302123708 212396419 8676876	288 243 238 223 201 199 197 187 183 176 168 151 149 144 138 130 126 126 126	24-43.65.58 44.253.221.31 141.253.221.3 Remote 45.2.124.139 141.21.22.71 141.22.19 141.22.19 141.22.19	https tcp ntp udp http tcp http tcp https tcp https tcp https https	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014 1042473 866922 790358	4560 3952 9052 apsf.xi.con Egress 2018844	Marysville China Jinan OTHER OTHER United Kingdom London apany.com. Country/City United States San Francisco Ukraine OTHER United States Ann Arbor Ukraine OTHER United States OTHER United States	 69 Googe 4. 3.65.58 7 CNC070 Service Appany com. 9 The Bin Strategy (HQ) 4.5.5.18 R stra-grab Service Abinaryedge ninja. 89 Tovider 49 Linoig 5. 19 Tovider 40 January Service Abinaryedge ninja. 10 Digitize Service Abinaryedge November Abina
141.253.221.11 141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.13 141.253.221.13 141.253.221.36 141.253.221.36 141.253.218.49 141.253.218.49 141.253.218.49 141.253.218.49 141.253.218.49 141.253.221.70 141.253.221.70 141.253.221.80	17-07-19 17-08-05 17-07-22 17-07-02 17-07-02 17-07-19 17-07-19 17-07-19 17-07-19 17-07-10 17-07-10 17-07-10 17-07-11 17-07-11 17-07-11 17-08-05 17-07-11 17-08-05 17-07-11 17-08-05 17-07-19 17-07	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914 1709312 16467988 1607262 302123708 212396419 8676876 96523885003	288 243 228 223 201 199 197 187 183 176 168 158 151 144 139 138 130 126 125	24-43.65.58 43.5.19 44.253.221.1 Remote 42.21.64 44.124.139 44.12.122.19 44.122.19 44.122.19 44.122.19	https tcp ntp udp http tcp 109 Svc https tcp https tcp https tcp https tcp tcp https tcp	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014 1042473 866922 790358	4560 3952 9052 apsf.xi.con Egress	Marysville China Jinan OTHER OTHER United Kingdom London apany.com. Country/City United States San Francisco Ukraine OTHER United States Ann Arbor Ukraine OTHER United States San Jose	 69 Googe 4. 3.65.58 7 CNC000 - 9 nal 69 Backbone 17 DNC000 - 9 nal 69 Backbone 17 Dn Bli 19 may com. 17 Dn Bli 19 may com. 18 Data 19 Linos 18 Provider 49 Linos 70 Provider 40 32.38 pr
141.253.221.11 141.253.221.14 141.253.221.14 141.253.221.14 141.253.221.12 141.253.221.12 141.253.221.12 141.253.221.36 141.253.221.36 141.253.221.36 141.253.221.33 141.253.221.219 141.253.221.219 141.253.221.219 141.253.221.219 141.253.221.219 141.253.221.31 141.253.221.810 141.253.218.31 141.253.218.31 141.253.218.61 141.253.218.61 141.253.218.61	17-07-19 17-06-29 17-06-29 17-07-22 17-07-07 17-07-07 17-07-19 17-07-19 17-07-10 17-08-05 17-07-21 17-07-20 17-06-29 17-07-19 17-07-	309193482 5214579 29090 348575 2610314 348701 114858480 4788411 119774696 1606455 43369027 301252824 508553708 198419914 1709312 16467988 1607262 302123708 212396419 8676876 96522885003 55959061	288 243 238 223 201 199 197 187 183 176 168 158 151 149 144 139 138 150 126 126 125 121	24-43.65.58 44.253.21.31 141.253.221. Remote 45.21.64 45.122.19 141.253.2164 45.122.19 141.253.2147 141.253.218.5	https tcp ntp udp http tcp 109 Svc https tcp https tcp https tcp https tcp Svc	8885 4332 3952 992 sales-ops- Ingress 217998448 9039014 1042473 866922 790358 django.jo	4560 3952 9052 apsf.xi.con Egress 2018844 cal.compar	Marysville China Jinan OTHER OTHER OTHER United Kingdom London apany.com. Country/City United States San Francisco Ukraine OTHER United States Ann Arbor Ukraine OTHER United States San Jose ty.com.	 69 Googe 4. 3.65.38 7 CNC050 5 - 9 mal 69 Backbone 3.7 The Bin 1994 2000 (HQ) 4.5.5.18 R tra-grab 5.0 m (HQ) 4.5.5.18 R 5.7 Tovider 4.6 32.0 m (HQ) 5.7 Tovider 5.7 Tovider