An open source network traffic performance monitoring and diagnostics tool.

www.trafmon.org

Use Case 3: Security Auditing

Thomas Grootaers, Luc Lechien

Software Release 1.0

2020-12

COPYRIGHT, LICENSE AND TRADEMARKS

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.

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

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.

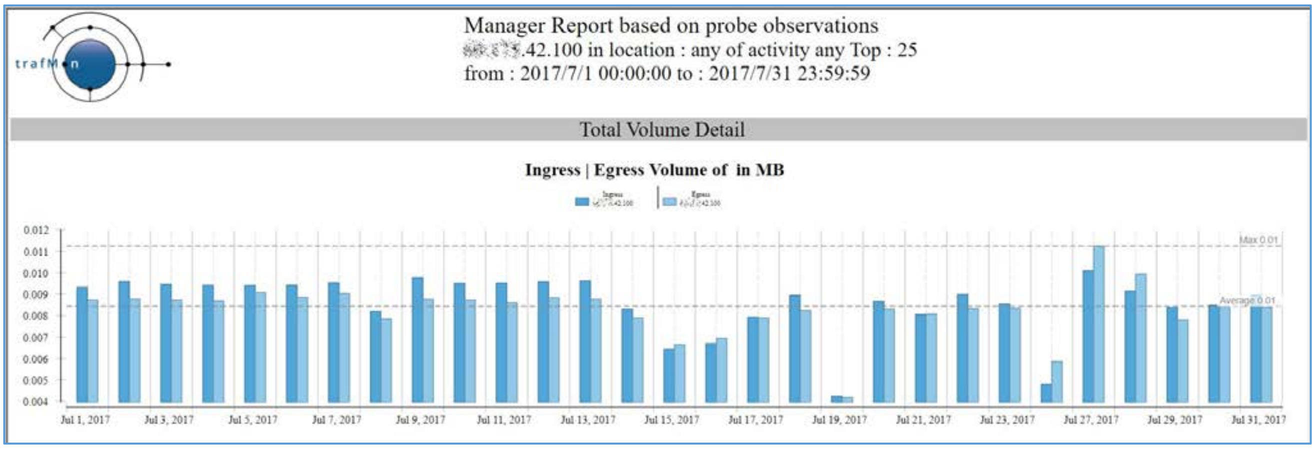
This tutorial is also presented as the Use Case web page https://www.trafmon.org/security-auditing/. MySQL stored procedures have been written for the two first-level queries for low-profile traffic and for external ingress volumes, as well as for the associated summarising queries. Those last are the 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 www.trafmon.org 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:



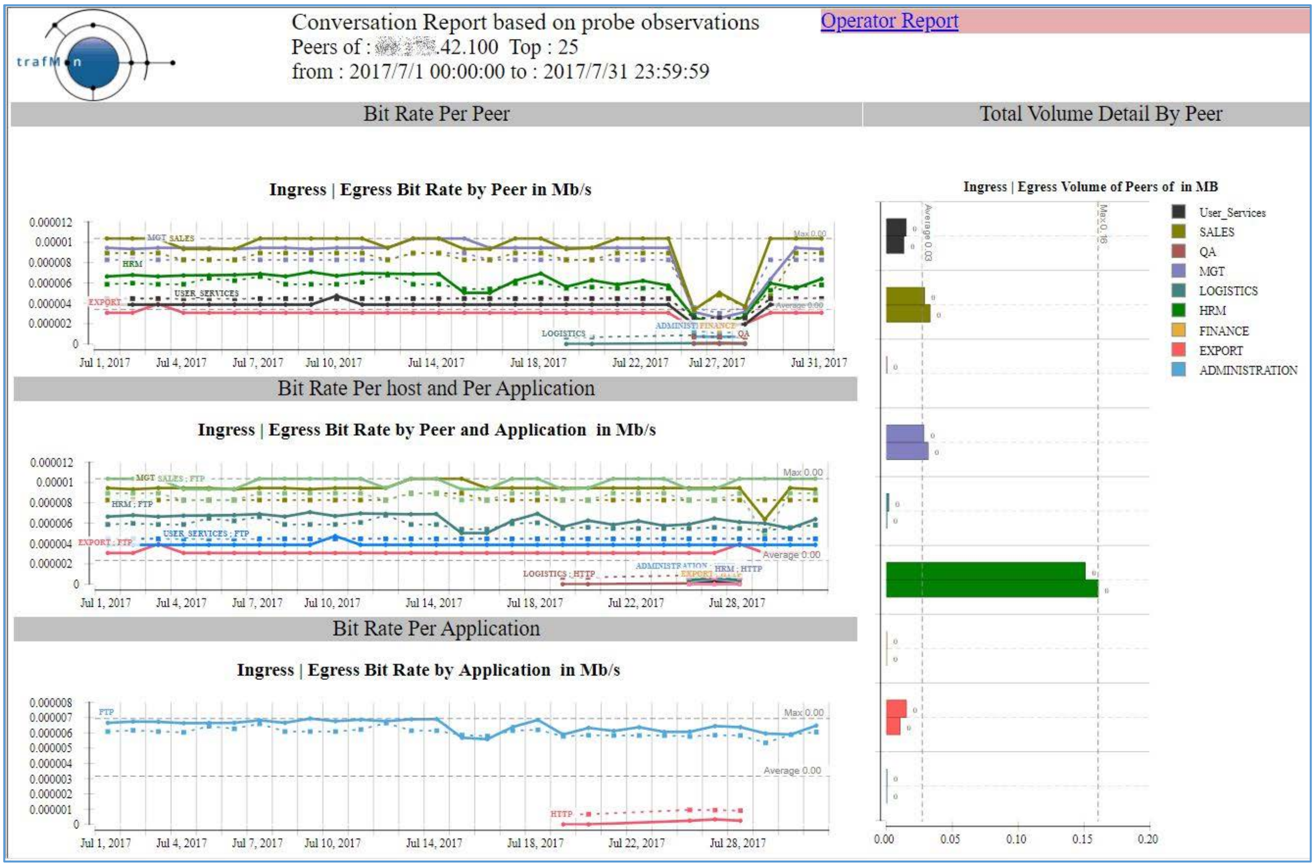
Manager Report based on probe observations
[redacted].42.100 in location : any of activity any Top : 25
from : 2017/7/1 00:00:00 to : 2017/7/31 23:59:59

Total Volume Detail

Ingress | Egress Volume of in MB

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.



Conversation Report based on probe observations
Peers of : [redacted].42.100 Top : 25
from : 2017/7/1 00:00:00 to : 2017/7/31 23:59:59

Operator Report

Bit Rate Per Peer

Ingress | Egress Bit Rate by Peer in Mb/s

Total Volume Detail By Peer

Ingress | Egress Volume of Peers of in MB

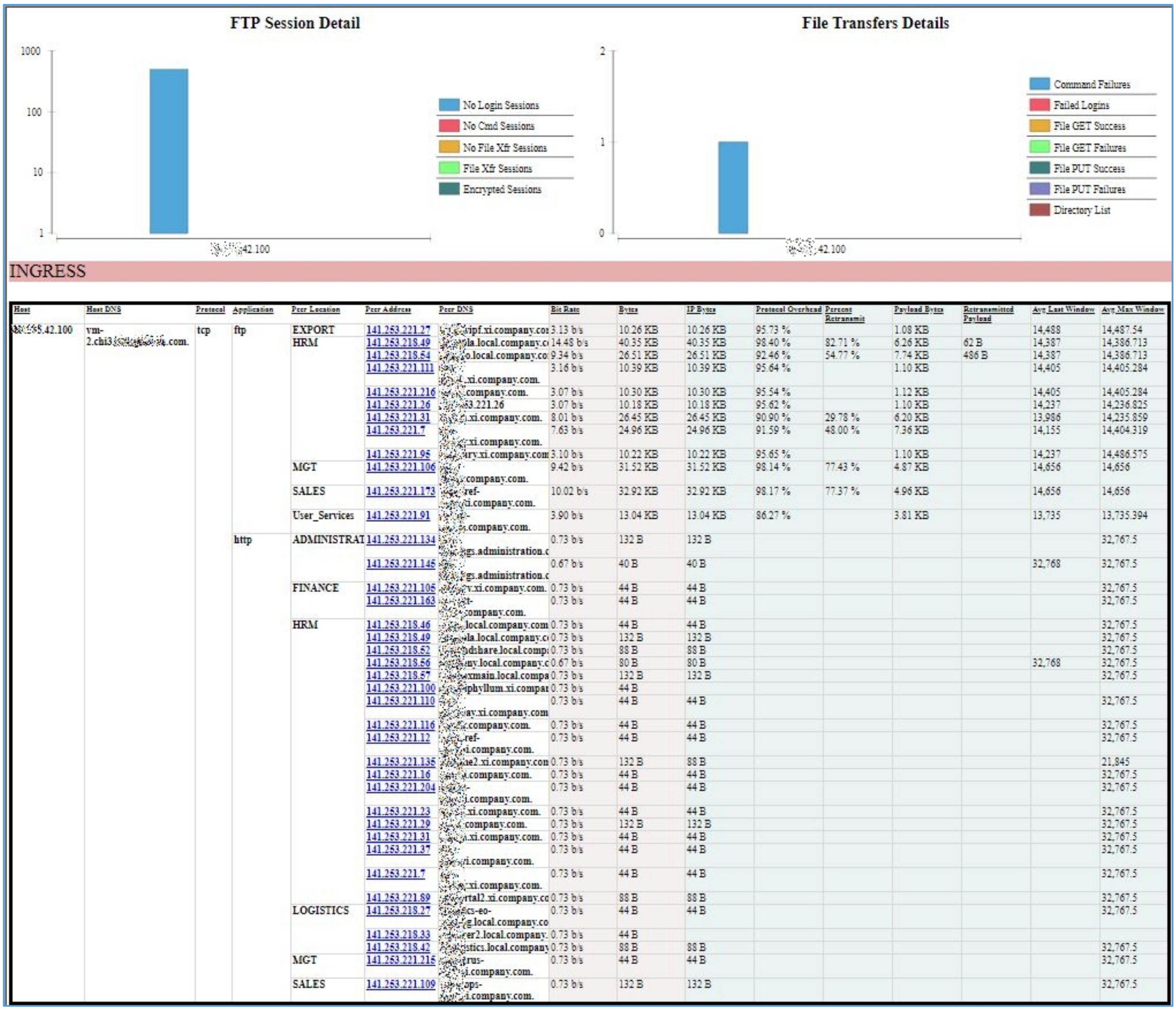
Bit Rate Per host and Per Application

Ingress | Egress Bit Rate by Peer and Application in Mb/s

Bit Rate Per Application

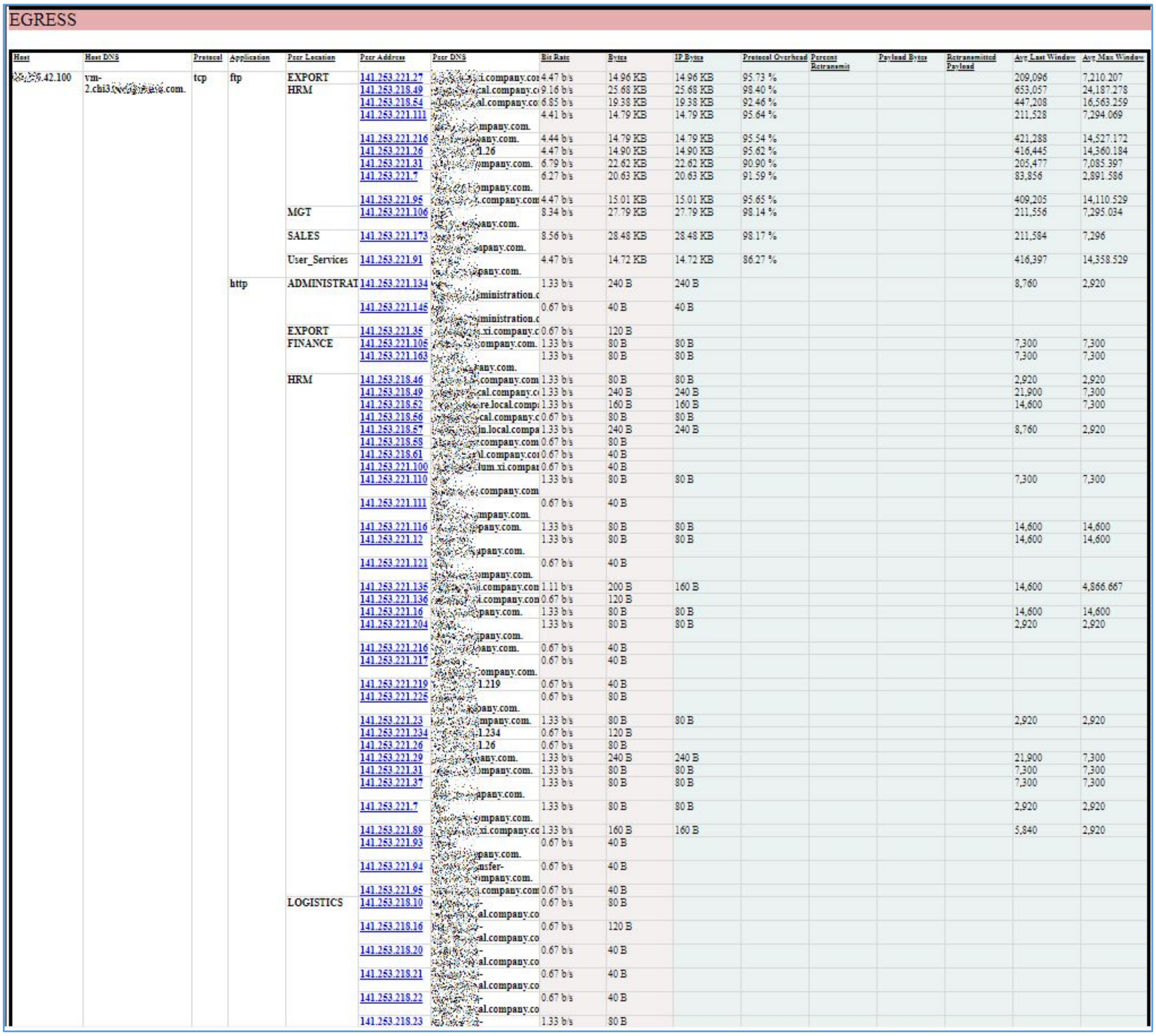
Ingress | Egress Bit Rate by Application in Mb/s

In details that gives:



INGRESS

Host	Host DNS	Protocol	Application	Peer Location	Peer Address	Peer DNS	Bit Rate	Bytes	IP Bytes	Protocol Overhead	Percent Retransmit	Payload Bytes	Retransmitted Payload	Avg Last Window	Avg Max Window
[redacted]5.42.100	vm-2.chi3[redacted].com.	tcp	ftp	EXPORT	141.253.221.27	[redacted]ipf.xi.company.co	3.13 b/s	10.26 KB	10.26 KB	95.73 %		1.08 KB		14,488	14,487.54
				HRM	141.253.218.49	[redacted]la.local.company.c	14.48 b/s	40.35 KB	40.35 KB	98.40 %	82.71 %	6.26 KB	62 B	14,387	14,386.713
					141.253.218.54	[redacted]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	[redacted].xi.company.com.	3.16 b/s	10.39 KB	10.39 KB	95.64 %		1.10 KB		14,405	14,405.284
					141.253.221.216	[redacted]company.com.	3.07 b/s	10.30 KB	10.30 KB	95.54 %		1.12 KB		14,405	14,405.284
					141.253.221.26	[redacted]53.221.26	3.07 b/s	10.18 KB	10.18 KB	95.62 %		1.10 KB		14,237	14,236.825
					141.253.221.31	[redacted].xi.company.com.	8.01 b/s	26.45 KB	26.45 KB	90.90 %	29.78 %	6.20 KB		13,986	14,235.859
					141.253.221.7	[redacted]xi.company.com.	7.63 b/s	24.96 KB	24.96 KB	91.59 %	48.00 %	7.36 KB		14,155	14,404.319
					141.253.221.95	[redacted]ry.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	[redacted]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	[redacted]ref- [redacted]i.company.com.	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	[redacted]- [redacted].company.com.	3.90 b/s	13.04 KB	13.04 KB	86.27 %		3.81 KB		13,735	13,735.394
			http	ADMINISTRAT	141.253.221.134	[redacted]gs.administration.c	0.73 b/s	132 B	132 B						32,767.5
					141.253.221.145	[redacted]gs.administration.c	0.67 b/s	40 B	40 B					32,768	32,767.5
				FINANCE	141.253.221.105	[redacted]v.xi.company.com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.163	[redacted]t- [redacted]ompany.com.	0.73 b/s	44 B	44 B						32,767.5
				HRM	141.253.218.46	[redacted]local.company.com	0.73 b/s	44 B	44 B						32,767.5
					141.253.218.49	[redacted]la.local.company.c	0.73 b/s	132 B	132 B						32,767.5
					141.253.218.52	[redacted]dshare.local.comp	0.73 b/s	88 B	88 B						32,767.5
					141.253.218.56	[redacted]ny.local.company.c	0.67 b/s	80 B	80 B					32,768	32,767.5
					141.253.218.57	[redacted]xmain.local.compa	0.73 b/s	132 B	132 B						32,767.5
					141.253.221.100	[redacted]iphyllum.xi.compa	0.73 b/s	44 B							
					141.253.221.110	[redacted]ay.xi.company.com	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.116	[redacted].company.com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.12	[redacted]ref- [redacted]i.company.com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.135	[redacted]e2.xi.company.com	0.73 b/s	132 B	88 B						21,845
					141.253.221.16	[redacted].company.com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.204	[redacted]- [redacted]i.company.com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.23	[redacted]xi.company.com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.29	[redacted]company.com.	0.73 b/s	132 B	132 B						32,767.5
					141.253.221.31	[redacted].xi.company.com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.37	[redacted]i.company.com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.7	[redacted]xi.company.com.	0.73 b/s	44 B	44 B						32,767.5
					141.253.221.89	[redacted]rtal2.xi.company.co	0.73 b/s	88 B	88 B						32,767.5
				LOGISTICS	141.253.218.27	[redacted]cs-eo- [redacted]g.local.company.co	0.73 b/s	44 B	44 B						32,767.5
					141.253.218.33	[redacted]er2.local.company.	0.73 b/s	44 B							
					141.253.218.42	[redacted]stics.local.company	0.73 b/s	88 B	88 B						32,767.5
				MGT	141.253.221.215	[redacted]rus- [redacted]i.company.com.	0.73 b/s	44 B	44 B						32,767.5
				SALES	141.253.221.109	[redacted]ops- [redacted]i.company.com.	0.73 b/s	132 B	132 B						32,767.5



EGRESS

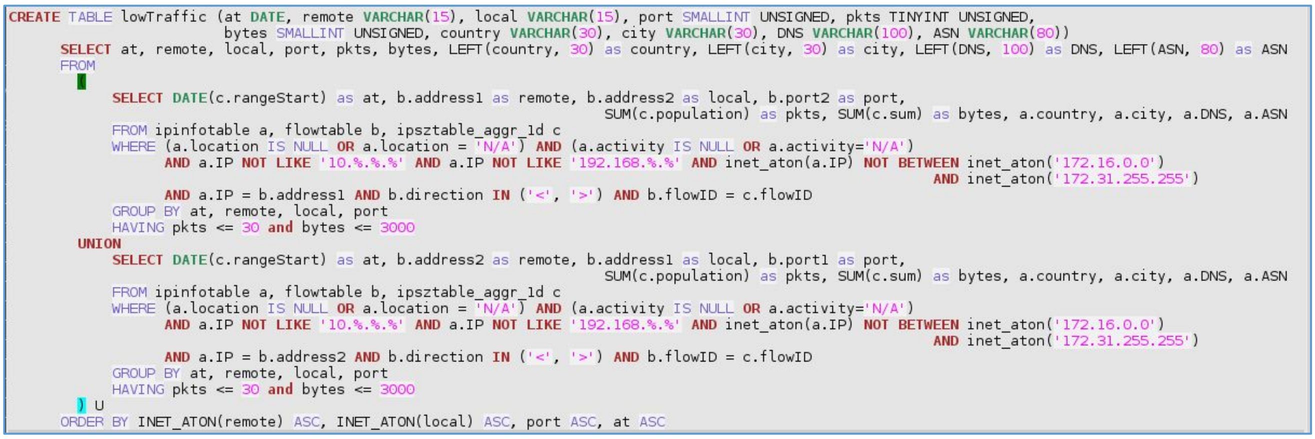
Host	Host DNS	Protocol	Application	Peer Location	Peer Address	Peer DNS	Bit Rate	Bytes	IP Bytes	Protocol Overhead	Percent Retransmit	Payload Bytes	Retransmitted Payload	Avg Last Window	Avg Max Window
[redacted].42.100	vm-2.chi3[redacted].com.	tcp	ftp	EXPORT	141.253.221.27	[redacted]i.company.coı	4.47 b/s	14.96 KB	14.96 KB	95.73 %				209,096	7,210.207
				HRM	141.253.218.49	[redacted]cal.company.c	9.16 b/s	25.68 KB	25.68 KB	98.40 %				653,057	24,187.278
					141.253.218.54	[redacted]al.company.co	6.85 b/s	19.38 KB	19.38 KB	92.46 %				447,208	16,563.259
					141.253.221.111	[redacted]mpany.com.	4.41 b/s	14.79 KB	14.79 KB	95.64 %				211,528	7,294.069
					141.253.221.216	[redacted]any.com.	4.44 b/s	14.79 KB	14.79 KB	95.54 %				421,288	14,527.172
					141.253.221.26	[redacted]1.26	4.47 b/s	14.90 KB	14.90 KB	95.62 %				416,445	14,360.184
					141.253.221.31	[redacted]mpany.com.	6.79 b/s	22.62 KB	22.62 KB	90.90 %				205,477	7,085.397
					141.253.221.7	[redacted]ompany.com.	6.27 b/s	20.63 KB	20.63 KB	91.59 %				83,856	2,891.586
					141.253.221.95	[redacted].company.com	4.47 b/s	15.01 KB	15.01 KB	95.65 %				409,205	14,110.529
				MGT	141.253.221.106	[redacted]any.com.	8.34 b/s	27.79 KB	27.79 KB	98.14 %				211,556	7,295.034
				SALES	141.253.221.173	[redacted]apany.com.	8.56 b/s	28.48 KB	28.48 KB	98.17 %				211,584	7,296
				User_Services	141.253.221.91	[redacted]pany.com.	4.47 b/s	14.72 KB	14.72 KB	86.27 %				416,397	14,358.529
			http	ADMINISTRAT	141.253.221.134	[redacted]ministration.c	1.33 b/s	240 B	240 B					8,760	2,920
					141.253.221.145	[redacted]ministration.c	0.67 b/s	40 B	40 B						
				EXPORT	141.253.221.35	[redacted].xi.company.c	0.67 b/s	120 B							
				FINANCE	141.253.221.105	[redacted]ompany.com.	1.33 b/s	80 B	80 B					7,300	7,300
					141.253.221.163	[redacted]any.com.	1.33 b/s	80 B	80 B					7,300	7,300
				HRM	141.253.218.46	[redacted].company.com	1.33 b/s	80 B	80 B					2,920	2,920
					141.253.218.49	[redacted]cal.company.c	1.33 b/s	240 B	240 B					21,900	7,300
					141.253.218.52	[redacted]re.local.comp	1.33 b/s	160 B	160 B					14,600	7,300
					141.253.218.56	[redacted]cal.company.c	0.67 b/s	80 B	80 B						
					141.253.218.57	[redacted]in.local.compa	1.33 b/s	240 B	240 B					8,760	2,920
					141.253.218.58	[redacted].company.com	0.67 b/s	80 B							
					141.253.218.61	[redacted]l.company.coı	0.67 b/s	40 B							
					141.253.221.100	[redacted]lum.xi.compaı	0.67 b/s	40 B							
					141.253.221.110	[redacted].company.com	1.33 b/s	80 B	80 B					7,300	7,300
					141.253.221.111	[redacted]mpany.com.	0.67 b/s	40 B							
					141.253.221.116	[redacted]pany.com.	1.33 b/s	80 B	80 B					14,600	14,600
					141.253.221.12	[redacted]apany.com.	1.33 b/s	80 B	80 B					14,600	14,600
					141.253.221.121	[redacted]mpany.com.	0.67 b/s	40 B							
					141.253.221.135	[redacted]i.company.con	1.11 b/s	200 B	160 B					14,600	4,866.667
					141.253.221.136	[redacted]i.company.con	0.67 b/s	120 B							
					141.253.221.16	[redacted]pany.com.	1.33 b/s	80 B	80 B					14,600	14,600
					141.253.221.204	[redacted]pany.com.	1.33 b/s	80 B	80 B					2,920	2,920
					141.253.221.216	[redacted]any.com.	0.67 b/s	40 B							
					141.253.221.217	[redacted]company.com.	0.67 b/s	40 B							
					141.253.221.219	[redacted]1.219	0.67 b/s	40 B							
					141.253.221.225	[redacted]pany.com.	0.67 b/s	80 B							
					141.253.221.23	[redacted]mpany.com.	1.33 b/s	80 B	80 B					2,920	2,920
					141.253.221.234	[redacted]1.234	0.67 b/s	120 B							
					141.253.221.26	[redacted]1.26	0.67 b/s	80 B							
					141.253.221.29	[redacted]any.com.	1.33 b/s	240 B	240 B					21,900	7,300
					141.253.221.31	[redacted]mpany.com.	1.33 b/s	80 B	80 B					7,300	7,300
					141.253.221.37	[redacted]apany.com.	1.33 b/s	80 B	80 B					7,300	7,300
					141.253.221.7	[redacted]ompany.com.	1.33 b/s	80 B	80 B					2,920	2,920
					141.253.221.89	[redacted]xi.company.co	1.33 b/s	160 B	160 B					5,840	2,920
					141.253.221.93	[redacted]pany.com.	0.67 b/s	40 B							
					141.253.221.94	[redacted]nsfer- [redacted]mpany.com.	0.67 b/s	40 B							
					141.253.221.95	[redacted].company.com	0.67 b/s	40 B							
				LOGISTICS	141.253.218.10	[redacted]- [redacted]al.company.co	0.67 b/s	80 B							
					141.253.218.16	[redacted]- [redacted]al.company.co	0.67 b/s	120 B							
					141.253.218.20	[redacted]- [redacted]al.company.co	0.67 b/s	40 B							
					141.253.218.21	[redacted]- [redacted]al.company.co	0.67 b/s	40 B							
					141.253.218.22	[redacted]- [redacted]al.company.co	0.67 b/s	40 B							
					141.253.218.23	[redacted]-	1.33 b/s	80 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:



```
CREATE TABLE lowTraffic (at DATE, remote VARCHAR(15), local VARCHAR(15), port SMALLINT UNSIGNED, pkts TINYINT UNSIGNED,
                         bytes SMALLINT UNSIGNED, country VARCHAR(30), city VARCHAR(30), DNS VARCHAR(100), ASN VARCHAR(80))
      SELECT at, remote, local, port, pkts, bytes, LEFT(country, 30) as country, LEFT(city, 30) as city, LEFT(DNS, 100) as DNS, LEFT(ASN, 80) as ASN
      FROM
        (
            SELECT DATE(c.rangeStart) as at, b.address1 as remote, b.address2 as local, b.port2 as port,
                                                          SUM(c.population) as pkts, SUM(c.sum) as bytes, a.country, a.city, a.DNS, a.ASN
            FROM ipinfotable a, flowtable b, ipsztable_aggr_1d c
            WHERE (a.location IS NULL OR a.location = 'N/A') AND (a.activity IS NULL OR a.activity='N/A')
                  AND a.IP NOT LIKE '10.%.%.%' AND a.IP NOT LIKE '192.168.%.%' AND inet_aton(a.IP) NOT BETWEEN inet_aton('172.16.0.0')
                                                                                                     AND inet_aton('172.31.255.255')
                  AND a.IP = b.address1 AND b.direction IN ('<', '>') AND b.flowID = c.flowID
            GROUP BY at, remote, local, port
            HAVING pkts <= 30 and bytes <= 3000
        UNION
            SELECT DATE(c.rangeStart) as at, b.address2 as remote, b.address1 as local, b.port1 as port,
                                                          SUM(c.population) as pkts, SUM(c.sum) as bytes, a.country, a.city, a.DNS, a.ASN
            FROM ipinfotable a, flowtable b, ipsztable_aggr_1d c
            WHERE (a.location IS NULL OR a.location = 'N/A') AND (a.activity IS NULL OR a.activity='N/A')
                  AND a.IP NOT LIKE '10.%.%.%' AND a.IP NOT LIKE '192.168.%.%' AND inet_aton(a.IP) NOT BETWEEN inet_aton('172.16.0.0')
                                                                                                     AND inet_aton('172.31.255.255')
                  AND a.IP = b.address2 AND b.direction IN ('<', '>') AND b.flowID = c.flowID
            GROUP BY at, remote, local, port
            HAVING pkts <= 30 and bytes <= 3000
        ) U
      ORDER BY INET_ATON(remote) ASC, INET_ATON(local) ASC, port ASC, at ASC
```

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))
```

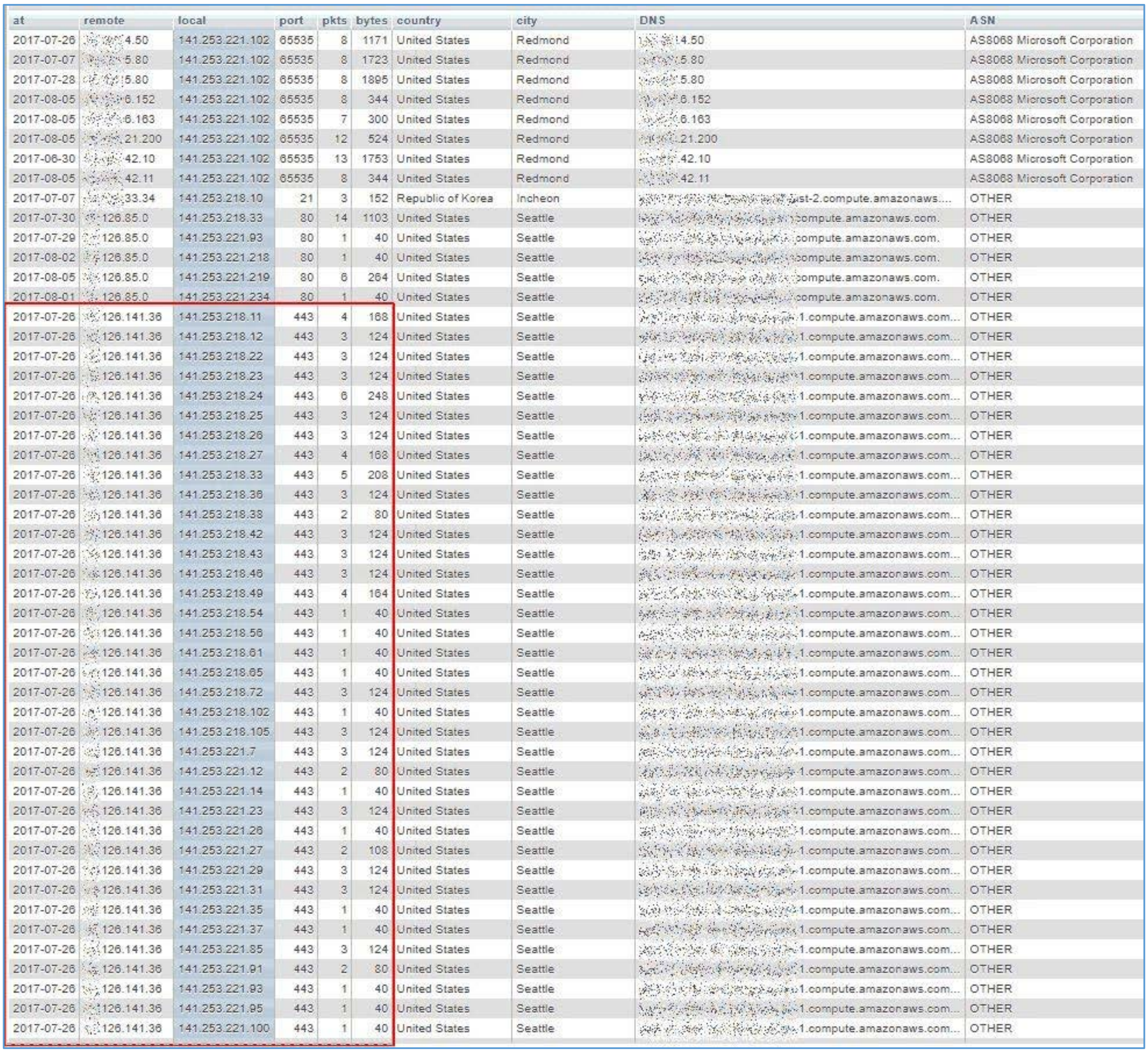
At the time of manual analysis, it is then quicker to extract from this prepared *lowTraffic* table those lines matching a more reduced volume of exchanges (e.g. 10 or 20 packets a day for a total of 1000 or 2000 bytes).

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

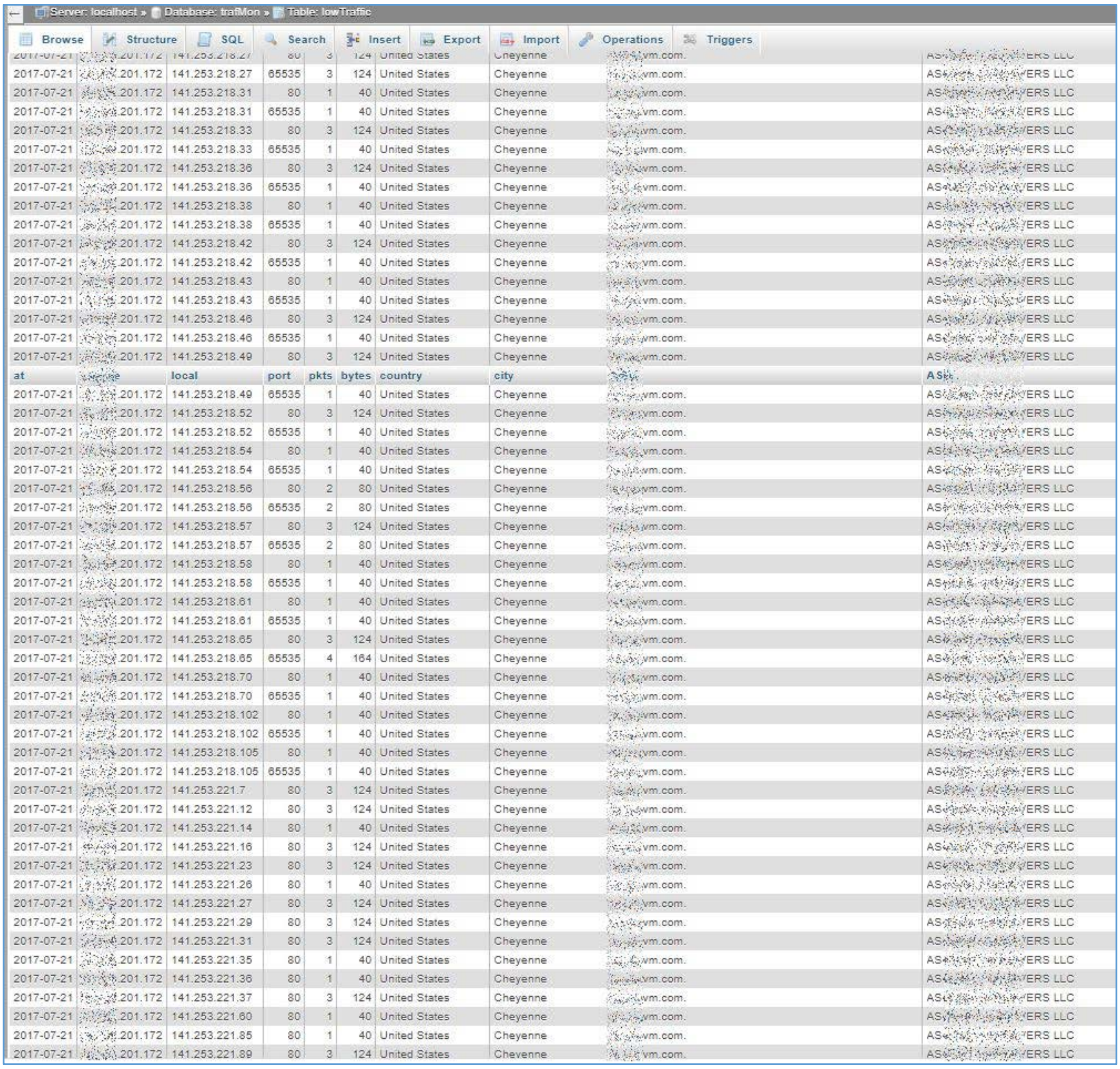
By browsing through (excerpts of) the lowTraffic table, we easily identify when, in a same day, a same remote IP address appears in consecutive lines whose local address field consecutive values form a nearly complete sequence of our own address’s ranges.



at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-26	[redacted]4.50	141.253.221.102	65535	8	1171	United States	Redmond	[redacted]4.50	AS8068 Microsoft Corporation
2017-07-07	[redacted]5.80	141.253.221.102	65535	8	1723	United States	Redmond	[redacted]5.80	AS8068 Microsoft Corporation
2017-07-28	[redacted]5.80	141.253.221.102	65535	8	1895	United States	Redmond	[redacted]5.80	AS8068 Microsoft Corporation
2017-08-05	[redacted]6.152	141.253.221.102	65535	8	344	United States	Redmond	[redacted]6.152	AS8068 Microsoft Corporation
2017-08-05	[redacted]6.163	141.253.221.102	65535	7	300	United States	Redmond	[redacted]6.163	AS8068 Microsoft Corporation
2017-08-05	[redacted]21.200	141.253.221.102	65535	12	524	United States	Redmond	[redacted]21.200	AS8068 Microsoft Corporation
2017-06-30	[redacted]42.10	141.253.221.102	65535	13	1753	United States	Redmond	[redacted]42.10	AS8068 Microsoft Corporation
2017-08-05	[redacted]42.11	141.253.221.102	65535	8	344	United States	Redmond	[redacted]42.11	AS8068 Microsoft Corporation
2017-07-07	[redacted]33.34	141.253.218.10	21	3	152	Republic of Korea	Incheon	[redacted]st-2.compute.amazonaws....	OTHER
2017-07-30	[redacted]126.85.0	141.253.218.33	80	14	1103	United States	Seattle	[redacted]compute.amazonaws.com.	OTHER
2017-07-29	[redacted]126.85.0	141.253.221.93	80	1	40	United States	Seattle	[redacted]compute.amazonaws.com.	OTHER
2017-08-02	[redacted]126.85.0	141.253.221.218	80	1	40	United States	Seattle	[redacted]compute.amazonaws.com.	OTHER
2017-08-05	[redacted]126.85.0	141.253.221.219	80	6	264	United States	Seattle	[redacted]compute.amazonaws.com.	OTHER
2017-08-01	[redacted]126.85.0	141.253.221.234	80	1	40	United States	Seattle	[redacted]compute.amazonaws.com.	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.11	443	4	168	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.12	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.22	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.23	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.24	443	6	248	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.25	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.26	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.27	443	4	168	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.33	443	5	208	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.36	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.38	443	2	80	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.42	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.43	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.46	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.49	443	4	164	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.54	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.56	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.61	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.65	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.72	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.102	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.218.105	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.7	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.12	443	2	80	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.14	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.23	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.26	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.27	443	2	108	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.29	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.31	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.35	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.37	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.85	443	3	124	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.91	443	2	80	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.93	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.95	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER
2017-07-26	[redacted]126.141.36	141.253.221.100	443	1	40	United States	Seattle	[redacted]1.compute.amazonaws.com...	OTHER

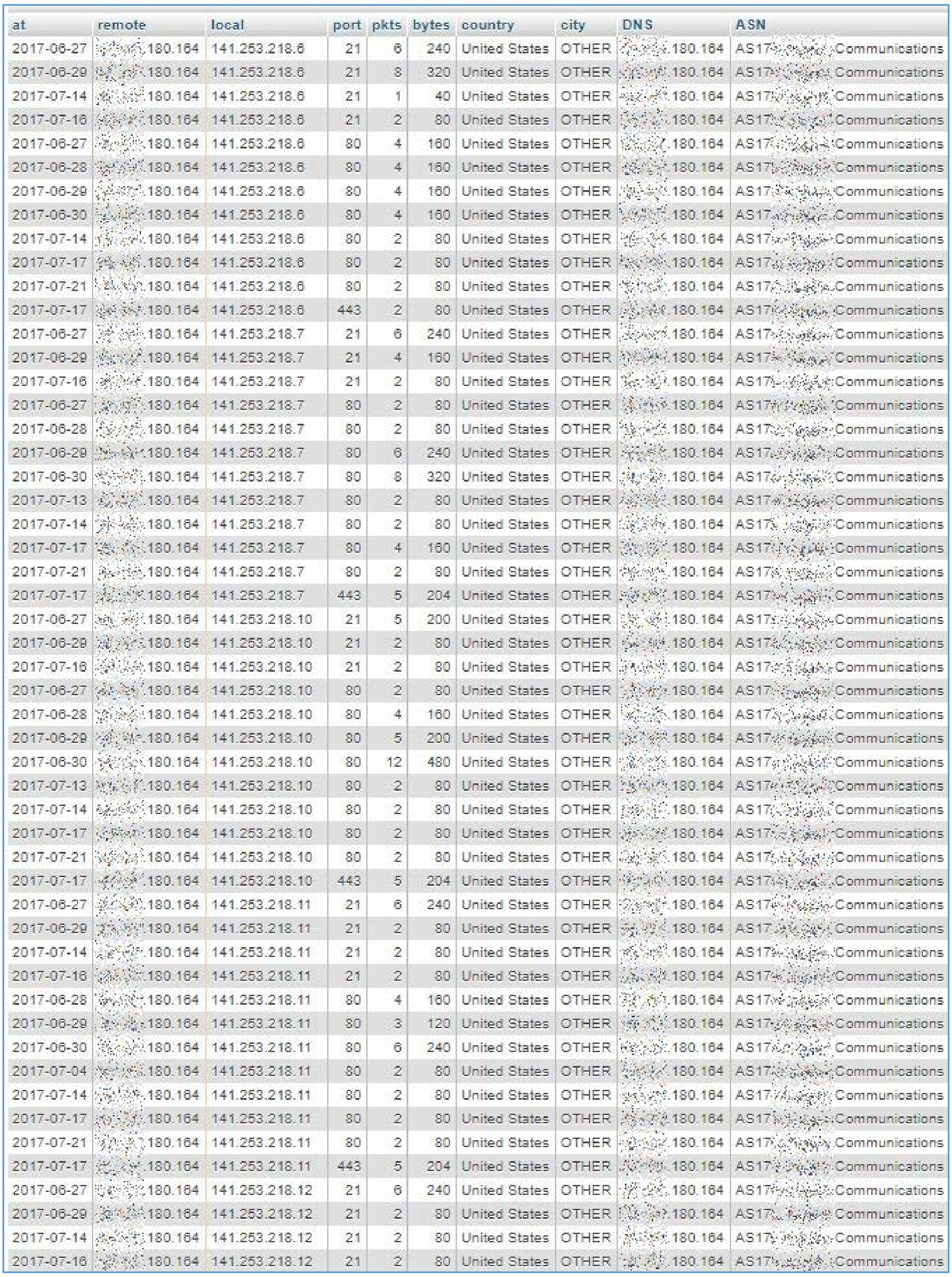
And the above list continues after the bottom of the picture.

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.



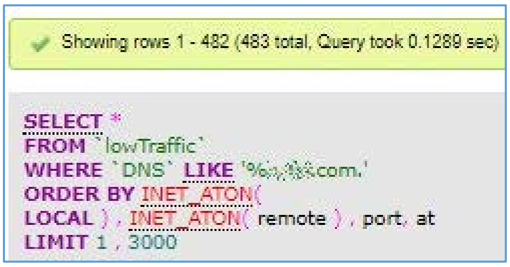
2017-07-21	[redacted].201.172	141.253.218.27	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.27	65535	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.31	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.31	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.33	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.33	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.36	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.36	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.38	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.38	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.42	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.42	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.43	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.43	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.46	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.46	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.49	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
at	[redacted]	local	port	pkts	bytes	country	city	[redacted]	AS[redacted]
2017-07-21	[redacted].201.172	141.253.218.49	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.52	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.52	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.54	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.54	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.56	80	2	80	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.56	65535	2	80	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.57	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.57	65535	2	80	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.58	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.58	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.61	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.61	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.65	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.65	65535	4	164	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.70	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.70	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.102	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.102	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.105	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.218.105	65535	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.7	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.12	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.14	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.16	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.23	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.26	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.27	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.29	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.31	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.35	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.36	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.37	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.60	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.85	80	1	40	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC
2017-07-21	[redacted].201.172	141.253.221.89	80	3	124	United States	Cheyenne	[redacted]vm.com.	AS[redacted]ERS LLC

In the following example, the remote system seems to perform complete daily scans, repeated on 11 different days of about a one-month period, using different target service ports – FTP (21), HTTP (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	[redacted].180.164	141.253.218.6	21	6	240	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-29	[redacted].180.164	141.253.218.6	21	8	320	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-14	[redacted].180.164	141.253.218.6	21	1	40	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-16	[redacted].180.164	141.253.218.6	21	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-27	[redacted].180.164	141.253.218.6	80	4	160	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-28	[redacted].180.164	141.253.218.6	80	4	160	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-29	[redacted].180.164	141.253.218.6	80	4	160	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-30	[redacted].180.164	141.253.218.6	80	4	160	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-14	[redacted].180.164	141.253.218.6	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-17	[redacted].180.164	141.253.218.6	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-21	[redacted].180.164	141.253.218.6	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-17	[redacted].180.164	141.253.218.6	443	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-27	[redacted].180.164	141.253.218.7	21	6	240	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-29	[redacted].180.164	141.253.218.7	21	4	160	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-16	[redacted].180.164	141.253.218.7	21	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-27	[redacted].180.164	141.253.218.7	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-28	[redacted].180.164	141.253.218.7	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-29	[redacted].180.164	141.253.218.7	80	6	240	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-30	[redacted].180.164	141.253.218.7	80	8	320	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-13	[redacted].180.164	141.253.218.7	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-14	[redacted].180.164	141.253.218.7	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-17	[redacted].180.164	141.253.218.7	80	4	160	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-21	[redacted].180.164	141.253.218.7	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-17	[redacted].180.164	141.253.218.7	443	5	204	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-27	[redacted].180.164	141.253.218.10	21	5	200	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-29	[redacted].180.164	141.253.218.10	21	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-16	[redacted].180.164	141.253.218.10	21	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-27	[redacted].180.164	141.253.218.10	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-28	[redacted].180.164	141.253.218.10	80	4	160	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-29	[redacted].180.164	141.253.218.10	80	5	200	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-30	[redacted].180.164	141.253.218.10	80	12	480	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-13	[redacted].180.164	141.253.218.10	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-14	[redacted].180.164	141.253.218.10	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-17	[redacted].180.164	141.253.218.10	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-21	[redacted].180.164	141.253.218.10	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-17	[redacted].180.164	141.253.218.10	443	5	204	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-27	[redacted].180.164	141.253.218.11	21	6	240	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-29	[redacted].180.164	141.253.218.11	21	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-14	[redacted].180.164	141.253.218.11	21	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-16	[redacted].180.164	141.253.218.11	21	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-28	[redacted].180.164	141.253.218.11	80	4	160	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-29	[redacted].180.164	141.253.218.11	80	3	120	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-30	[redacted].180.164	141.253.218.11	80	6	240	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-04	[redacted].180.164	141.253.218.11	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-14	[redacted].180.164	141.253.218.11	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-17	[redacted].180.164	141.253.218.11	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-21	[redacted].180.164	141.253.218.11	80	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-17	[redacted].180.164	141.253.218.11	443	5	204	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-27	[redacted].180.164	141.253.218.12	21	6	240	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-06-29	[redacted].180.164	141.253.218.12	21	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-14	[redacted].180.164	141.253.218.12	21	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications
2017-07-16	[redacted].180.164	141.253.218.12	21	2	80	United States	OTHER	[redacted].180.164	AS17[redacted]Communications

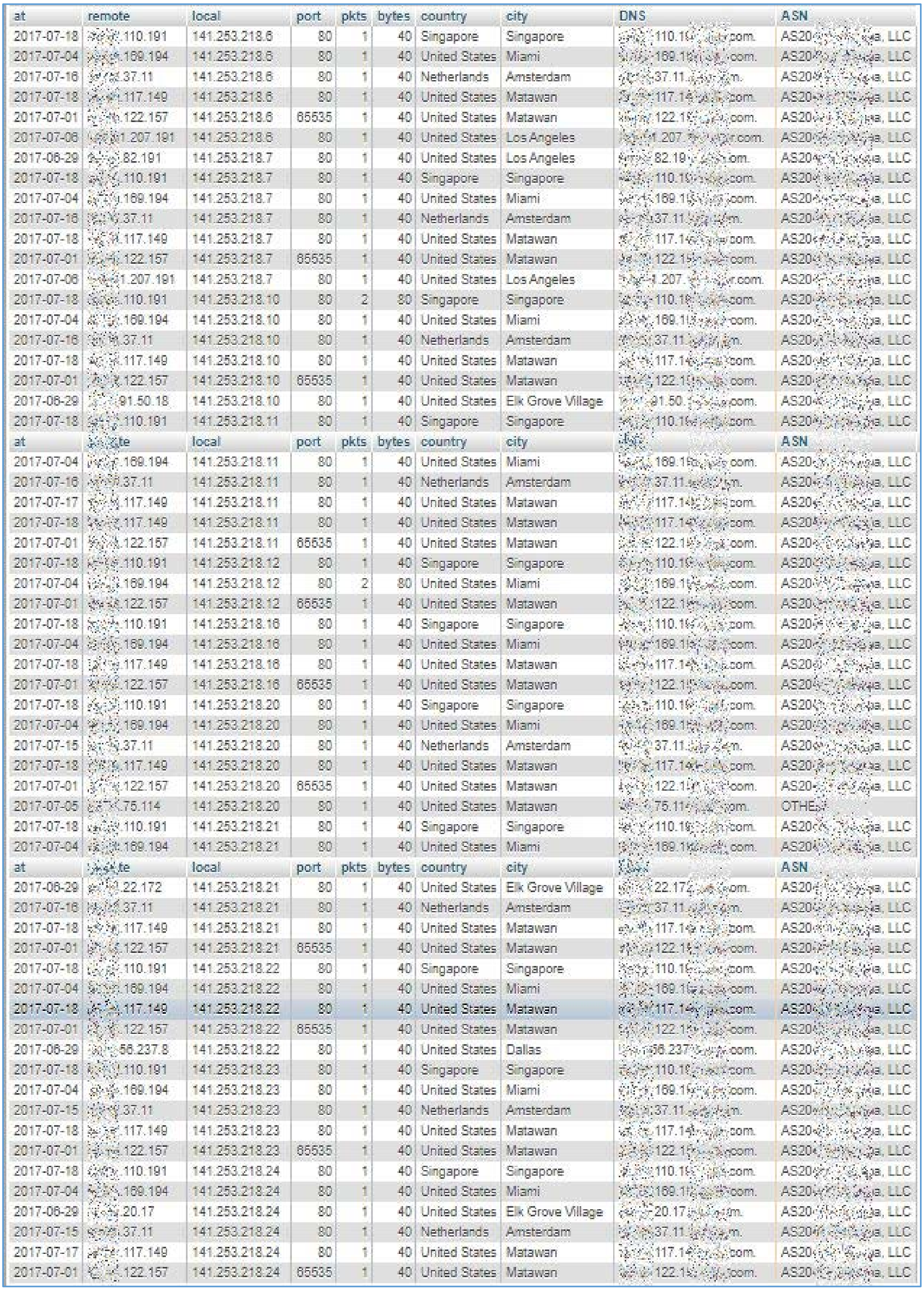
Searching on the basis of DNS domain name part highlights what seems to be different complete daily scans (same remote address for a given day), but repeated by different remote addresses on different days, all belonging to the same DNS domain name, although geo-located in totally different countries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



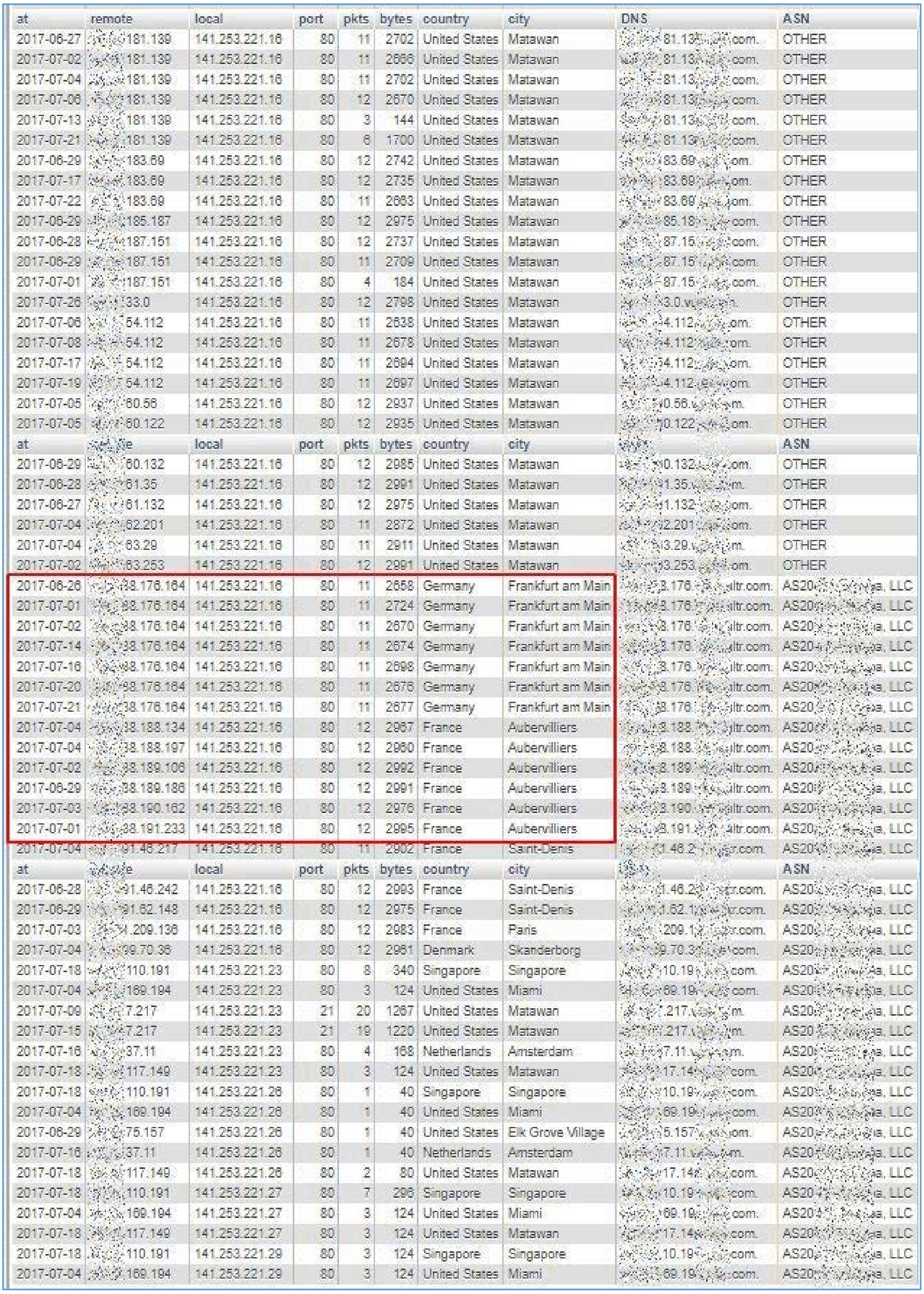
✓ Showing rows 1 - 482 (483 total, Query took 0.1289 sec)

```
SELECT *
FROM `lowTraffic`
WHERE `DNS` LIKE '%[redacted]com.'
ORDER BY INET_ATON(
LOCAL ) , INET_ATON( remote ) , port, at
LIMIT 1 , 3000
```

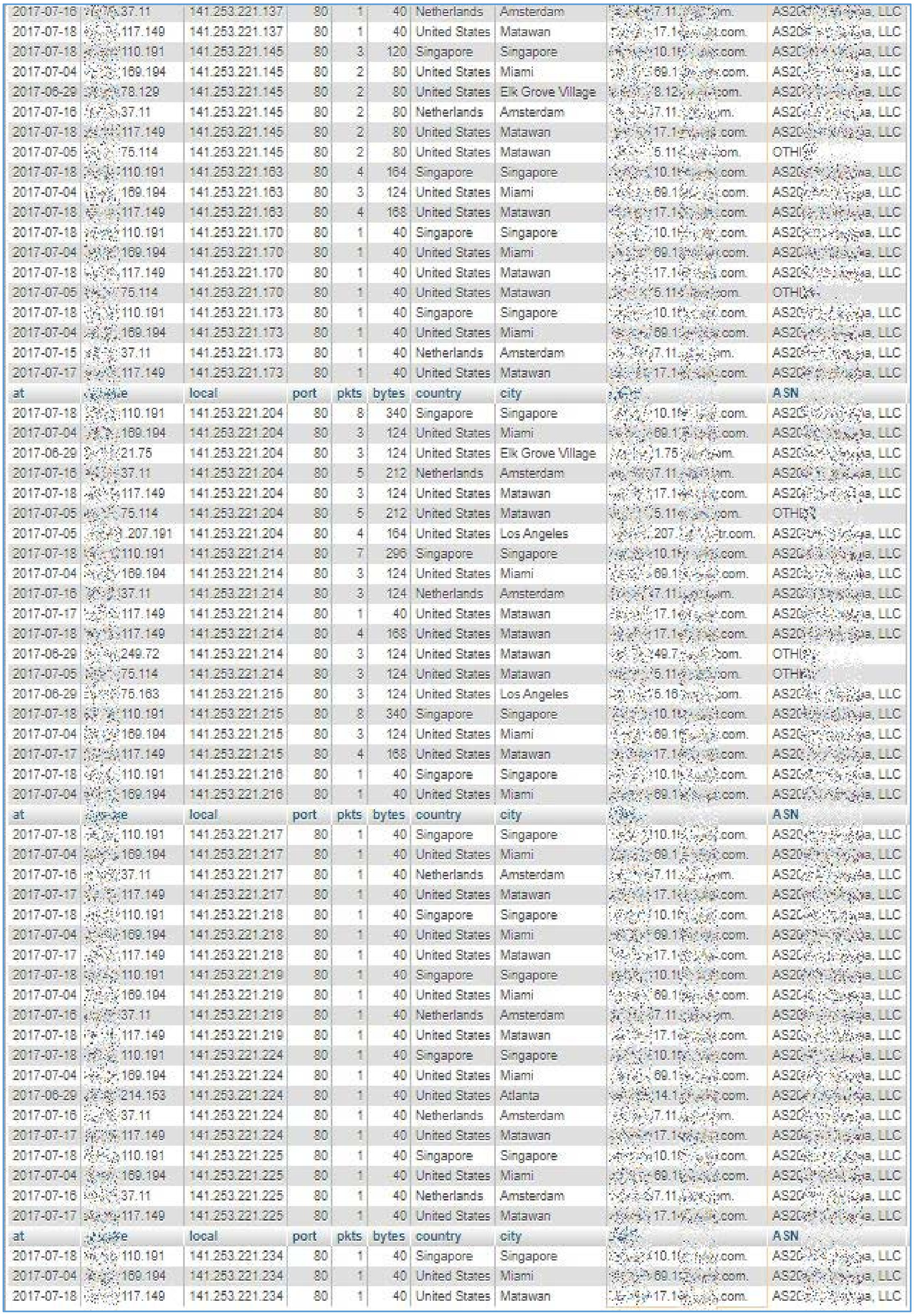
Here below, the first, the fifth and the last page of the result of the query.



at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-18	[redacted].110.191	141.253.218.6	80	1	40	Singapore	Singapore	[redacted]110.1[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted].169.194	141.253.218.6	80	1	40	United States	Miami	[redacted]169.1[redacted].com.	AS20[redacted]a, LLC
2017-07-16	[redacted].37.11	141.253.218.6	80	1	40	Netherlands	Amsterdam	[redacted]37.11[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted].117.149	141.253.218.6	80	1	40	United States	Matawan	[redacted]117.14[redacted]com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.6	65535	1	40	United States	Matawan	[redacted]122.1[redacted].com.	AS20[redacted]a, LLC
2017-07-06	[redacted]1.207.191	141.253.218.6	80	1	40	United States	Los Angeles	[redacted]1.207.[redacted]r.com.	AS20[redacted]a, LLC
2017-06-29	[redacted].82.191	141.253.218.7	80	1	40	United States	Los Angeles	[redacted]82.19[redacted]om.	AS20[redacted]a, LLC
2017-07-18	[redacted].110.191	141.253.218.7	80	1	40	Singapore	Singapore	[redacted]110.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted].169.194	141.253.218.7	80	1	40	United States	Miami	[redacted]169.1[redacted]com.	AS20[redacted]a, LLC
2017-07-16	[redacted].37.11	141.253.218.7	80	1	40	Netherlands	Amsterdam	[redacted]37.11[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted].117.149	141.253.218.7	80	1	40	United States	Matawan	[redacted]117.14[redacted]com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.7	65535	1	40	United States	Matawan	[redacted]122.1[redacted]com.	AS20[redacted]a, LLC
2017-07-06	[redacted]1.207.191	141.253.218.7	80	1	40	United States	Los Angeles	[redacted]1.207.[redacted]r.com.	AS20[redacted]a, LLC
2017-07-18	[redacted].110.191	141.253.218.10	80	2	80	Singapore	Singapore	[redacted]110.1[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted].169.194	141.253.218.10	80	1	40	United States	Miami	[redacted]169.1[redacted]com.	AS20[redacted]a, LLC
2017-07-16	[redacted].37.11	141.253.218.10	80	1	40	Netherlands	Amsterdam	[redacted]37.11[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted].117.149	141.253.218.10	80	1	40	United States	Matawan	[redacted]117.14[redacted]com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.10	65535	1	40	United States	Matawan	[redacted]122.1[redacted].com.	AS20[redacted]a, LLC
2017-06-29	[redacted].91.50.18	141.253.218.10	80	1	40	United States	Elk Grove Village	[redacted]91.50.[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted].110.191	141.253.218.11	80	1	40	Singapore	Singapore	[redacted]110.1[redacted].com.	AS20[redacted]a, LLC
at	[redacted]te	local	port	pkts	bytes	country	city	[redacted]	ASN
2017-07-04	[redacted].169.194	141.253.218.11	80	1	40	United States	Miami	[redacted]169.1[redacted].com.	AS20[redacted]a, LLC
2017-07-16	[redacted].37.11	141.253.218.11	80	1	40	Netherlands	Amsterdam	[redacted]37.11[redacted]m.	AS20[redacted]a, LLC
2017-07-17	[redacted].117.149	141.253.218.11	80	1	40	United States	Matawan	[redacted]117.14[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted].117.149	141.253.218.11	80	1	40	United States	Matawan	[redacted]117.14[redacted]com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.11	65535	1	40	United States	Matawan	[redacted]122.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted].110.191	141.253.218.12	80	1	40	Singapore	Singapore	[redacted]110.1[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted].169.194	141.253.218.12	80	2	80	United States	Miami	[redacted]169.1[redacted].com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.12	65535	1	40	United States	Matawan	[redacted]122.1[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted].110.191	141.253.218.16	80	1	40	Singapore	Singapore	[redacted]110.1[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted].169.194	141.253.218.16	80	1	40	United States	Miami	[redacted]169.1[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted].117.149	141.253.218.16	80	1	40	United States	Matawan	[redacted]117.14[redacted].com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.16	65535	1	40	United States	Matawan	[redacted]122.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted].110.191	141.253.218.20	80	1	40	Singapore	Singapore	[redacted]110.1[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted].169.194	141.253.218.20	80	1	40	United States	Miami	[redacted]169.1[redacted]com.	AS20[redacted]a, LLC
2017-07-15	[redacted].37.11	141.253.218.20	80	1	40	Netherlands	Amsterdam	[redacted]37.11[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted].117.149	141.253.218.20	80	1	40	United States	Matawan	[redacted]117.14[redacted]com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.20	65535	1	40	United States	Matawan	[redacted]122.1[redacted]com.	AS20[redacted]a, LLC
2017-07-05	[redacted].75.114	141.253.218.20	80	1	40	United States	Matawan	[redacted]75.11[redacted]om.	OTHE[redacted]
2017-07-18	[redacted].110.191	141.253.218.21	80	1	40	Singapore	Singapore	[redacted]110.1[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted].169.194	141.253.218.21	80	1	40	United States	Miami	[redacted]169.1[redacted].com.	AS20[redacted]a, LLC
at	[redacted]te	local	port	pkts	bytes	country	city	[redacted]	ASN
2017-06-29	[redacted].22.172	141.253.218.21	80	1	40	United States	Elk Grove Village	[redacted]22.17[redacted]om.	AS20[redacted]a, LLC
2017-07-16	[redacted].37.11	141.253.218.21	80	1	40	Netherlands	Amsterdam	[redacted]37.11[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted].117.149	141.253.218.21	80	1	40	United States	Matawan	[redacted]117.14[redacted]com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.21	65535	1	40	United States	Matawan	[redacted]122.1[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted].110.191	141.253.218.22	80	1	40	Singapore	Singapore	[redacted]110.1[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted].169.194	141.253.218.22	80	1	40	United States	Miami	[redacted]169.1[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted].117.149	141.253.218.22	80	1	40	United States	Matawan	[redacted]117.14[redacted].com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.22	65535	1	40	United States	Matawan	[redacted]122.1[redacted]com.	AS20[redacted]a, LLC
2017-06-29	[redacted].56.237.8	141.253.218.22	80	1	40	United States	Dallas	[redacted]56.237[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted].110.191	141.253.218.23	80	1	40	Singapore	Singapore	[redacted]110.1[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted].169.194	141.253.218.23	80	1	40	United States	Miami	[redacted]169.1[redacted]com.	AS20[redacted]a, LLC
2017-07-15	[redacted].37.11	141.253.218.23	80	1	40	Netherlands	Amsterdam	[redacted]37.11[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted].117.149	141.253.218.23	80	1	40	United States	Matawan	[redacted]117.14[redacted]com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.23	65535	1	40	United States	Matawan	[redacted]122.1[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted].110.191	141.253.218.24	80	1	40	Singapore	Singapore	[redacted]110.1[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted].169.194	141.253.218.24	80	1	40	United States	Miami	[redacted]169.1[redacted]com.	AS20[redacted]a, LLC
2017-06-29	[redacted].20.17	141.253.218.24	80	1	40	United States	Elk Grove Village	[redacted]20.17[redacted]m.	AS20[redacted]a, LLC
2017-07-15	[redacted].37.11	141.253.218.24	80	1	40	Netherlands	Amsterdam	[redacted]37.11[redacted]m.	AS20[redacted]a, LLC
2017-07-17	[redacted].117.149	141.253.218.24	80	1	40	United States	Matawan	[redacted]117.14[redacted]com.	AS20[redacted]a, LLC
2017-07-01	[redacted].122.157	141.253.218.24	65535	1	40	United States	Matawan	[redacted]122.1[redacted]com.	AS20[redacted]a, LLC



at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-06-27	[redacted]181.139	141.253.221.16	80	11	2702	United States	Matawan	[redacted]81.13[redacted]com.	OTHER
2017-07-02	[redacted]181.139	141.253.221.16	80	11	2666	United States	Matawan	[redacted]81.13[redacted]com.	OTHER
2017-07-04	[redacted]181.139	141.253.221.16	80	11	2702	United States	Matawan	[redacted]81.13[redacted]com.	OTHER
2017-07-06	[redacted]181.139	141.253.221.16	80	12	2670	United States	Matawan	[redacted]81.13[redacted]com.	OTHER
2017-07-13	[redacted]181.139	141.253.221.16	80	3	144	United States	Matawan	[redacted]81.13[redacted]com.	OTHER
2017-07-21	[redacted]181.139	141.253.221.16	80	6	1700	United States	Matawan	[redacted]81.13[redacted]com.	OTHER
2017-06-29	[redacted]183.69	141.253.221.16	80	12	2742	United States	Matawan	[redacted]83.69[redacted]om.	OTHER
2017-07-17	[redacted]183.69	141.253.221.16	80	12	2735	United States	Matawan	[redacted]83.69[redacted]om.	OTHER
2017-07-22	[redacted]183.69	141.253.221.16	80	11	2663	United States	Matawan	[redacted]83.69[redacted]om.	OTHER
2017-06-29	[redacted]185.187	141.253.221.16	80	12	2975	United States	Matawan	[redacted]85.18[redacted]com.	OTHER
2017-06-28	[redacted]187.151	141.253.221.16	80	12	2737	United States	Matawan	[redacted]87.15[redacted]com.	OTHER
2017-06-29	[redacted]187.151	141.253.221.16	80	11	2709	United States	Matawan	[redacted]87.15[redacted]com.	OTHER
2017-07-01	[redacted]187.151	141.253.221.16	80	4	184	United States	Matawan	[redacted]87.15[redacted]com.	OTHER
2017-07-26	[redacted]33.0	141.253.221.16	80	12	2798	United States	Matawan	[redacted]3.0.v[redacted]n.	OTHER
2017-07-06	[redacted]54.112	141.253.221.16	80	11	2638	United States	Matawan	[redacted]4.112[redacted]om.	OTHER
2017-07-08	[redacted]54.112	141.253.221.16	80	11	2678	United States	Matawan	[redacted]4.112[redacted]om.	OTHER
2017-07-17	[redacted]54.112	141.253.221.16	80	11	2694	United States	Matawan	[redacted]4.112[redacted]om.	OTHER
2017-07-19	[redacted]54.112	141.253.221.16	80	11	2697	United States	Matawan	[redacted]4.112[redacted]om.	OTHER
2017-07-05	[redacted]60.56	141.253.221.16	80	12	2937	United States	Matawan	[redacted]0.56.[redacted]m.	OTHER
2017-07-05	[redacted]60.122	141.253.221.16	80	12	2935	United States	Matawan	[redacted]0.122[redacted]om.	OTHER
at	[redacted]e	local	port	pkts	bytes	country	city	[redacted]	ASN
2017-06-29	[redacted]60.132	141.253.221.16	80	12	2985	United States	Matawan	[redacted]0.132[redacted]om.	OTHER
2017-06-28	[redacted]61.35	141.253.221.16	80	12	2991	United States	Matawan	[redacted]1.35.[redacted]m.	OTHER
2017-06-27	[redacted]61.132	141.253.221.16	80	12	2975	United States	Matawan	[redacted]1.132[redacted]om.	OTHER
2017-07-04	[redacted]62.201	141.253.221.16	80	11	2872	United States	Matawan	[redacted]2.201[redacted]om.	OTHER
2017-07-04	[redacted]63.29	141.253.221.16	80	11	2911	United States	Matawan	[redacted]3.29.[redacted]m.	OTHER
2017-07-02	[redacted]63.253	141.253.221.16	80	12	2991	United States	Matawan	[redacted]3.253[redacted]om.	OTHER
2017-06-26	[redacted]88.176.164	141.253.221.16	80	11	2658	Germany	Frankfurt am Main	[redacted]3.176[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-01	[redacted]88.176.164	141.253.221.16	80	11	2724	Germany	Frankfurt am Main	[redacted]3.176[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-02	[redacted]88.176.164	141.253.221.16	80	11	2670	Germany	Frankfurt am Main	[redacted]3.176[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-14	[redacted]88.176.164	141.253.221.16	80	11	2674	Germany	Frankfurt am Main	[redacted]3.176[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-16	[redacted]88.176.164	141.253.221.16	80	11	2698	Germany	Frankfurt am Main	[redacted]3.176[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-20	[redacted]88.176.164	141.253.221.16	80	11	2676	Germany	Frankfurt am Main	[redacted]3.176[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-21	[redacted]88.176.164	141.253.221.16	80	11	2677	Germany	Frankfurt am Main	[redacted]3.176[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-04	[redacted]88.188.134	141.253.221.16	80	12	2967	France	Aubervilliers	[redacted]3.188[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-04	[redacted]88.188.197	141.253.221.16	80	12	2960	France	Aubervilliers	[redacted]3.188[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-02	[redacted]88.189.106	141.253.221.16	80	12	2992	France	Aubervilliers	[redacted]3.189[redacted]ltr.com.	AS20[redacted]a, LLC
2017-06-29	[redacted]88.189.186	141.253.221.16	80	12	2991	France	Aubervilliers	[redacted]3.189[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-03	[redacted]88.190.162	141.253.221.16	80	12	2976	France	Aubervilliers	[redacted]3.190[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-01	[redacted]88.191.233	141.253.221.16	80	12	2995	France	Aubervilliers	[redacted]3.191[redacted]ltr.com.	AS20[redacted]a, LLC
2017-07-04	[redacted]91.46.217	141.253.221.16	80	11	2902	France	Saint-Denis	[redacted]1.46.2[redacted]r.com.	AS20[redacted]a, LLC
at	[redacted]e	local	port	pkts	bytes	country	city	[redacted]	ASN
2017-06-28	[redacted]91.46.242	141.253.221.16	80	12	2993	France	Saint-Denis	[redacted]1.46.2[redacted]r.com.	AS20[redacted]a, LLC
2017-06-29	[redacted]91.62.148	141.253.221.16	80	12	2975	France	Saint-Denis	[redacted]1.62.1[redacted]r.com.	AS20[redacted]a, LLC
2017-07-03	[redacted]4.209.136	141.253.221.16	80	12	2983	France	Paris	[redacted]209.1[redacted]r.com.	AS20[redacted]a, LLC
2017-07-04	[redacted]99.70.36	141.253.221.16	80	12	2981	Denmark	Skanderborg	[redacted]9.70.3[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.23	80	8	340	Singapore	Singapore	[redacted]10.19[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.23	80	3	124	United States	Miami	[redacted]69.19[redacted]com.	AS20[redacted]a, LLC
2017-07-09	[redacted]7.217	141.253.221.23	21	20	1267	United States	Matawan	[redacted].217.[redacted]m.	AS20[redacted]a, LLC
2017-07-15	[redacted]7.217	141.253.221.23	21	19	1220	United States	Matawan	[redacted].217.[redacted]m.	AS20[redacted]a, LLC
2017-07-16	[redacted]37.11	141.253.221.23	80	4	168	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.23	80	3	124	United States	Matawan	[redacted]17.14[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.26	80	1	40	Singapore	Singapore	[redacted]10.19[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.26	80	1	40	United States	Miami	[redacted]69.19[redacted]com.	AS20[redacted]a, LLC
2017-06-29	[redacted]75.157	141.253.221.26	80	1	40	United States	Elk Grove Village	[redacted]5.157[redacted]om.	AS20[redacted]a, LLC
2017-07-16	[redacted]37.11	141.253.221.26	80	1	40	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.26	80	2	80	United States	Matawan	[redacted]17.14[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.27	80	7	296	Singapore	Singapore	[redacted]10.19[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.27	80	3	124	United States	Miami	[redacted]69.19[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.27	80	3	124	United States	Matawan	[redacted]17.14[redacted]com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.29	80	3	124	Singapore	Singapore	[redacted]10.19[redacted]com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.29	80	3	124	United States	Miami	[redacted]69.19[redacted]com.	AS20[redacted]a, LLC



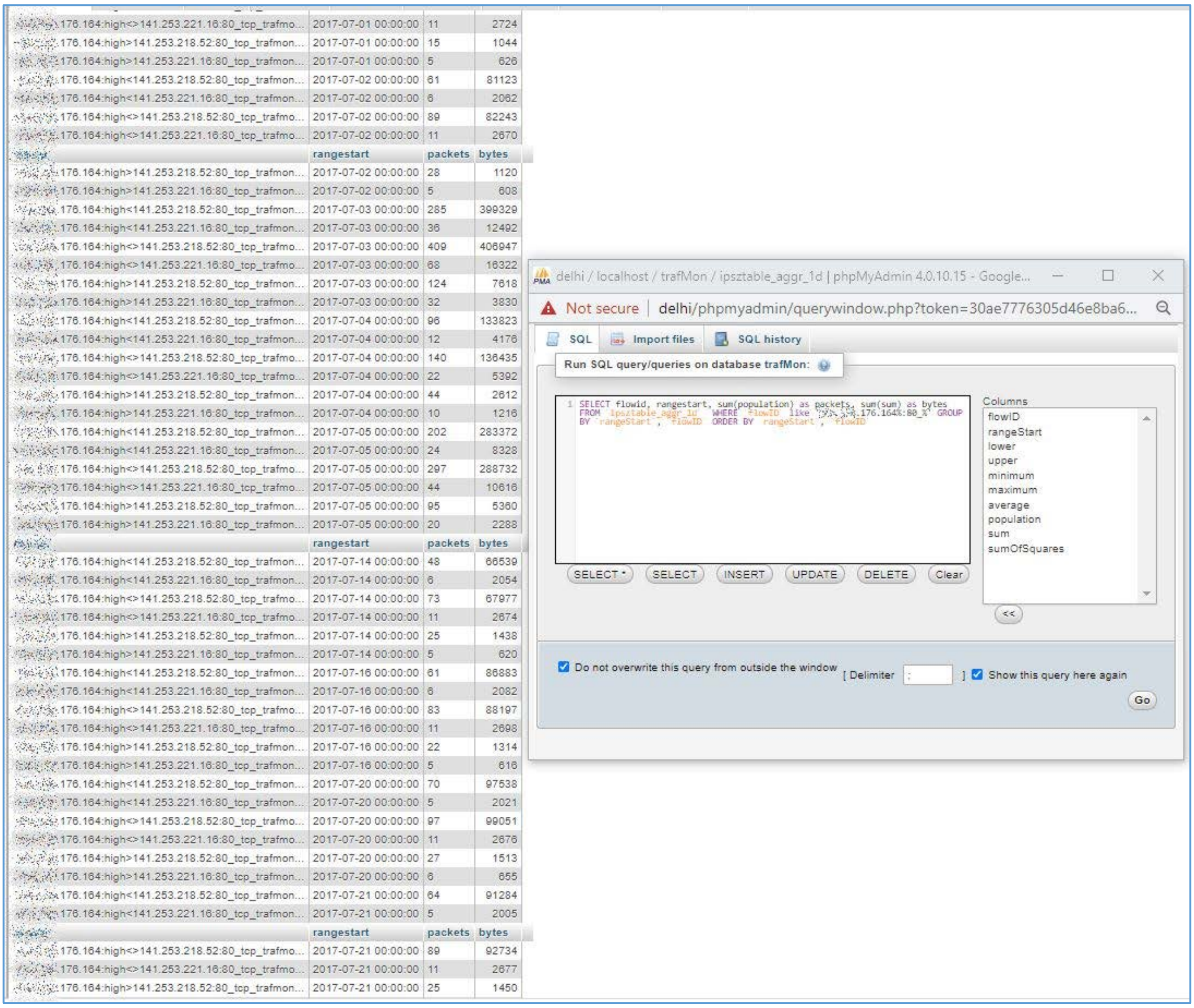
2017-07-16	[redacted]37.11	141.253.221.137	80	1	40	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.137	80	1	40	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.145	80	3	120	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.145	80	2	80	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-06-29	[redacted]78.129	141.253.221.145	80	2	80	United States	Elk Grove Village	[redacted]8.12[redacted]om.	AS20[redacted]a, LLC
2017-07-16	[redacted]37.11	141.253.221.145	80	2	80	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.145	80	2	80	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-05	[redacted]75.114	141.253.221.145	80	2	80	United States	Matawan	[redacted]5.11[redacted]om.	OTH[redacted]
2017-07-18	[redacted]110.191	141.253.221.163	80	4	164	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.163	80	3	124	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.163	80	4	168	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.170	80	1	40	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.170	80	1	40	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.170	80	1	40	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-05	[redacted]75.114	141.253.221.170	80	1	40	United States	Matawan	[redacted]5.11[redacted]om.	OTH[redacted]
2017-07-18	[redacted]110.191	141.253.221.173	80	1	40	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.173	80	1	40	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-07-15	[redacted]37.11	141.253.221.173	80	1	40	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-17	[redacted]117.149	141.253.221.173	80	1	40	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
at	[redacted]e	local	port	pkts	bytes	country	city	[redacted]	ASN
2017-07-18	[redacted]110.191	141.253.221.204	80	8	340	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.204	80	3	124	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-06-29	[redacted]21.75	141.253.221.204	80	3	124	United States	Elk Grove Village	[redacted]1.75[redacted]m.	AS20[redacted]a, LLC
2017-07-16	[redacted]37.11	141.253.221.204	80	5	212	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.204	80	3	124	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-05	[redacted]75.114	141.253.221.204	80	5	212	United States	Matawan	[redacted]5.11[redacted]om.	OTH[redacted]
2017-07-05	[redacted].207.191	141.253.221.204	80	4	164	United States	Los Angeles	[redacted].207.[redacted]tr.com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.214	80	7	296	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.214	80	3	124	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-07-16	[redacted]37.11	141.253.221.214	80	3	124	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-17	[redacted]117.149	141.253.221.214	80	1	40	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.214	80	4	168	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-06-29	[redacted]249.72	141.253.221.214	80	3	124	United States	Matawan	[redacted]49.7[redacted]om.	OTH[redacted]
2017-07-05	[redacted]75.114	141.253.221.214	80	3	124	United States	Matawan	[redacted]5.11[redacted]om.	OTH[redacted]
2017-06-29	[redacted]75.163	141.253.221.215	80	3	124	United States	Los Angeles	[redacted]5.16[redacted]om.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.215	80	8	340	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.215	80	3	124	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-07-17	[redacted]117.149	141.253.221.215	80	4	168	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.216	80	1	40	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.216	80	1	40	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
at	[redacted]e	local	port	pkts	bytes	country	city	[redacted]	ASN
2017-07-18	[redacted]110.191	141.253.221.217	80	1	40	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.217	80	1	40	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-07-16	[redacted]37.11	141.253.221.217	80	1	40	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-17	[redacted]117.149	141.253.221.217	80	1	40	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.218	80	1	40	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.218	80	1	40	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-07-17	[redacted]117.149	141.253.221.218	80	1	40	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.219	80	1	40	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.219	80	1	40	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-07-16	[redacted]37.11	141.253.221.219	80	1	40	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.219	80	1	40	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.224	80	1	40	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.224	80	1	40	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-06-29	[redacted]214.153	141.253.221.224	80	1	40	United States	Atlanta	[redacted]14.1[redacted].com.	AS20[redacted]a, LLC
2017-07-16	[redacted]37.11	141.253.221.224	80	1	40	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-17	[redacted]117.149	141.253.221.224	80	1	40	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]110.191	141.253.221.225	80	1	40	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.225	80	1	40	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-07-16	[redacted]37.11	141.253.221.225	80	1	40	Netherlands	Amsterdam	[redacted]7.11.[redacted]m.	AS20[redacted]a, LLC
2017-07-17	[redacted]117.149	141.253.221.225	80	1	40	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC
at	[redacted]e	local	port	pkts	bytes	country	city	[redacted]	ASN
2017-07-18	[redacted]110.191	141.253.221.234	80	1	40	Singapore	Singapore	[redacted]10.1[redacted].com.	AS20[redacted]a, LLC
2017-07-04	[redacted]169.194	141.253.221.234	80	1	40	United States	Miami	[redacted]69.1[redacted].com.	AS20[redacted]a, LLC
2017-07-18	[redacted]117.149	141.253.221.234	80	1	40	United States	Matawan	[redacted]17.1[redacted].com.	AS20[redacted]a, LLC

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.

```
SELECT flowID, rangeStart, SUM(population) AS packets, SUM(sum) AS bytes FROM ipsztable_aggr_1d
   WHERE flowID LIKE '[redacted].176.164%:80_%' GROUP BY rangeStart, flowID ORDER BY rangeStart, flowID
```



[redacted].176.164:high<>141.253.221.16:80_tcp_trafmo...	2017-07-01 00:00:00	11	2724
[redacted].176.164:high>141.253.218.52:80_tcp_trafmon...	2017-07-01 00:00:00	15	1044
[redacted].176.164:high>141.253.221.16:80_tcp_trafmon...	2017-07-01 00:00:00	5	626
[redacted].176.164:high<141.253.218.52:80_tcp_trafmon...	2017-07-02 00:00:00	61	81123
[redacted].176.164:high<141.253.221.16:80_tcp_trafmon...	2017-07-02 00:00:00	6	2062
[redacted].176.164:high<>141.253.218.52:80_tcp_trafmo...	2017-07-02 00:00:00	89	82243
[redacted].176.164:high<>141.253.221.16:80_tcp_trafmo...	2017-07-02 00:00:00	11	2670
[redacted]	rangestart	packets	bytes
[redacted].176.164:high>141.253.218.52:80_tcp_trafmon...	2017-07-02 00:00:00	28	1120
[redacted].176.164:high>141.253.221.16:80_tcp_trafmon...	2017-07-02 00:00:00	5	608
[redacted].176.164:high<141.253.218.52:80_tcp_trafmon...	2017-07-03 00:00:00	285	399329
[redacted].176.164:high<141.253.221.16:80_tcp_trafmon...	2017-07-03 00:00:00	36	12492
[redacted].176.164:high<>141.253.218.52:80_tcp_trafmo...	2017-07-03 00:00:00	409	406947
[redacted].176.164:high<>141.253.221.16:80_tcp_trafmo...	2017-07-03 00:00:00	68	16322
[redacted].176.164:high>141.253.218.52:80_tcp_trafmon...	2017-07-03 00:00:00	124	7618
[redacted].176.164:high>141.253.221.16:80_tcp_trafmon...	2017-07-03 00:00:00	32	3830
[redacted].176.164:high<141.253.218.52:80_tcp_trafmon...	2017-07-04 00:00:00	96	133823
[redacted].176.164:high<141.253.221.16:80_tcp_trafmon...	2017-07-04 00:00:00	12	4176
[redacted].176.164:high<>141.253.218.52:80_tcp_trafmo...	2017-07-04 00:00:00	140	136435
[redacted].176.164:high<>141.253.221.16:80_tcp_trafmo...	2017-07-04 00:00:00	22	5392
[redacted].176.164:high>141.253.218.52:80_tcp_trafmon...	2017-07-04 00:00:00	44	2612
[redacted].176.164:high>141.253.221.16:80_tcp_trafmon...	2017-07-04 00:00:00	10	1216
[redacted].176.164:high<141.253.218.52:80_tcp_trafmon...	2017-07-05 00:00:00	202	283372
[redacted].176.164:high<141.253.221.16:80_tcp_trafmon...	2017-07-05 00:00:00	24	8328
[redacted].176.164:high<>141.253.218.52:80_tcp_trafmo...	2017-07-05 00:00:00	297	288732
[redacted].176.164:high<>141.253.221.16:80_tcp_trafmo...	2017-07-05 00:00:00	44	10616
[redacted].176.164:high>141.253.218.52:80_tcp_trafmon...	2017-07-05 00:00:00	95	5360
[redacted].176.164:high>141.253.221.16:80_tcp_trafmon...	2017-07-05 00:00:00	20	2288
[redacted]	rangestart	packets	bytes
[redacted].176.164:high<141.253.218.52:80_tcp_trafmon...	2017-07-14 00:00:00	48	66539
[redacted].176.164:high<141.253.221.16:80_tcp_trafmon...	2017-07-14 00:00:00	6	2054
[redacted].176.164:high<>141.253.218.52:80_tcp_trafmo...	2017-07-14 00:00:00	73	67977
[redacted].176.164:high<>141.253.221.16:80_tcp_trafmo...	2017-07-14 00:00:00	11	2674
[redacted].176.164:high>141.253.218.52:80_tcp_trafmon...	2017-07-14 00:00:00	25	1438
[redacted].176.164:high>141.253.221.16:80_tcp_trafmon...	2017-07-14 00:00:00	5	620
[redacted].176.164:high<141.253.218.52:80_tcp_trafmon...	2017-07-16 00:00:00	61	86883
[redacted].176.164:high<141.253.221.16:80_tcp_trafmon...	2017-07-16 00:00:00	6	2082
[redacted].176.164:high<>141.253.218.52:80_tcp_trafmo...	2017-07-16 00:00:00	83	88197
[redacted].176.164:high<>141.253.221.16:80_tcp_trafmo...	2017-07-16 00:00:00	11	2698
[redacted].176.164:high>141.253.218.52:80_tcp_trafmon...	2017-07-16 00:00:00	22	1314
[redacted].176.164:high>141.253.221.16:80_tcp_trafmon...	2017-07-16 00:00:00	5	616
[redacted].176.164:high<141.253.218.52:80_tcp_trafmon...	2017-07-20 00:00:00	70	97538
[redacted].176.164:high<141.253.221.16:80_tcp_trafmon...	2017-07-20 00:00:00	5	2021
[redacted].176.164:high<>141.253.218.52:80_tcp_trafmo...	2017-07-20 00:00:00	97	99051
[redacted].176.164:high<>141.253.221.16:80_tcp_trafmo...	2017-07-20 00:00:00	11	2676
[redacted].176.164:high>141.253.218.52:80_tcp_trafmon...	2017-07-20 00:00:00	27	1513
[redacted].176.164:high>141.253.221.16:80_tcp_trafmon...	2017-07-20 00:00:00	6	655
[redacted].176.164:high<141.253.218.52:80_tcp_trafmon...	2017-07-21 00:00:00	64	91284
[redacted].176.164:high<141.253.221.16:80_tcp_trafmon...	2017-07-21 00:00:00	5	2005
[redacted]	rangestart	packets	bytes
[redacted].176.164:high<>141.253.218.52:80_tcp_trafmo...	2017-07-21 00:00:00	89	92734
[redacted].176.164:high<>141.253.221.16:80_tcp_trafmo...	2017-07-21 00:00:00	11	2677
[redacted].176.164:high>141.253.218.52:80_tcp_trafmon...	2017-07-21 00:00:00	25	1450

delhi / localhost / trafMon / ipsztable_aggr_1d | phpMyAdmin 4.0.10.15 - Google...

Not secure | delhi/phpmyadmin/querywindow.php?token=30ae7776305d46e8ba6...

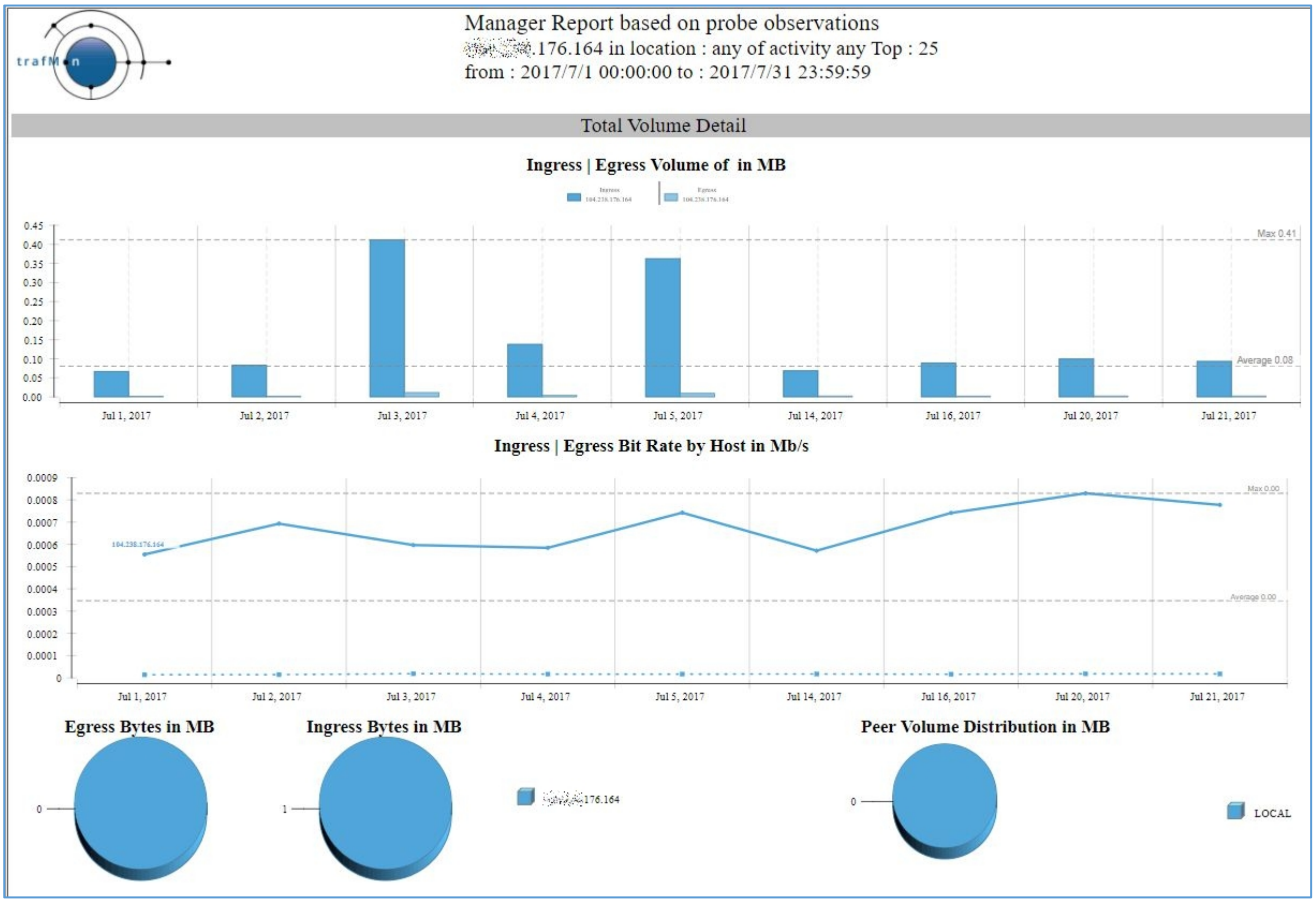
Run SQL query/queries on database trafMon:

```
SELECT flowid, rangestart, sum(population) as packets, sum(sum) as bytes
FROM `ipsztable_aggr_1d` WHERE `flowID` like '[redacted].176.164%:80_%' GROUP
BY `rangeStart`, `flowID` ORDER BY `rangeStart`, `flowID`
```

Columns: flowID, rangeStart, lower, upper, minimum, maximum, average, population, sum, sumOfSquares

☑ Do not overwrite this query from outside the window [Delimiter ;] ☑ Show this query here again

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



Manager Report based on probe observations
[redacted].176.164 in location : any of activity any Top : 25
from : 2017/7/1 00:00:00 to : 2017/7/31 23:59:59

Total Volume Detail

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.

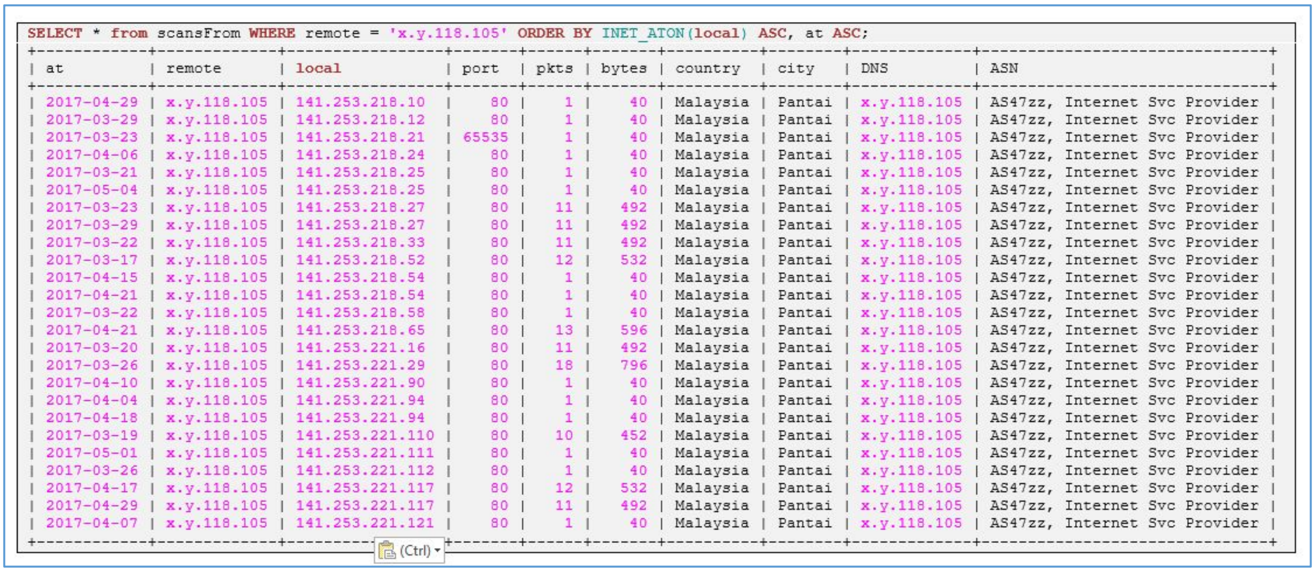
2.4 REVEALING HIDDEN MULTI-DAY SCANS

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).

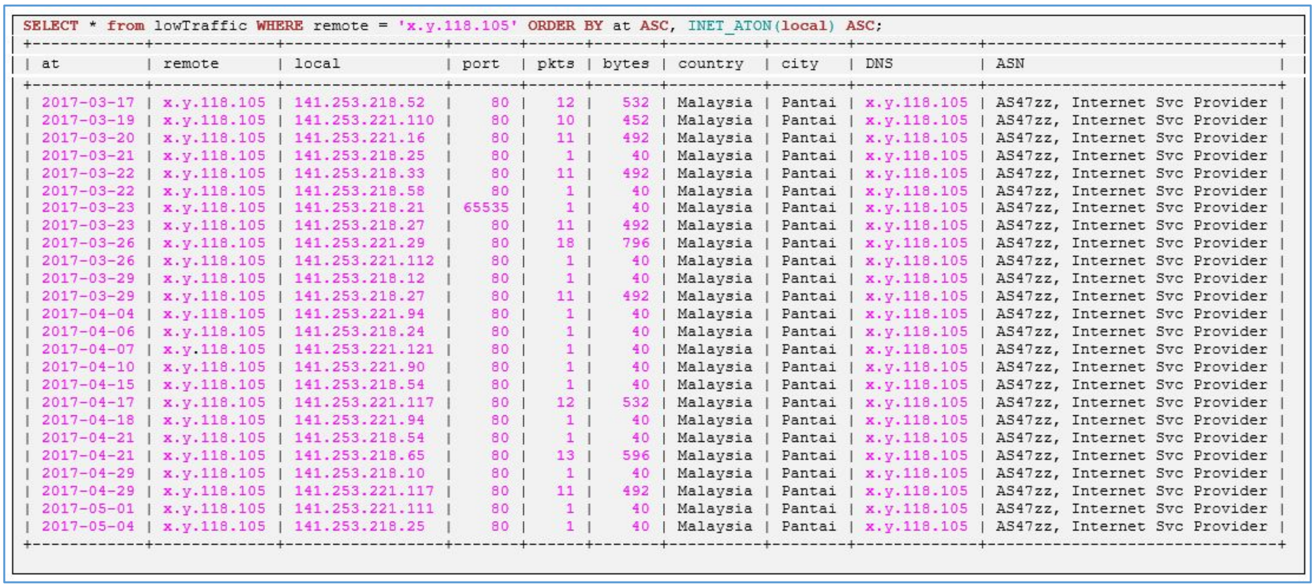
However, there are even more vicious scanning behaviours, where it is very difficult to detect that our several own systems have actually been reached.

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.



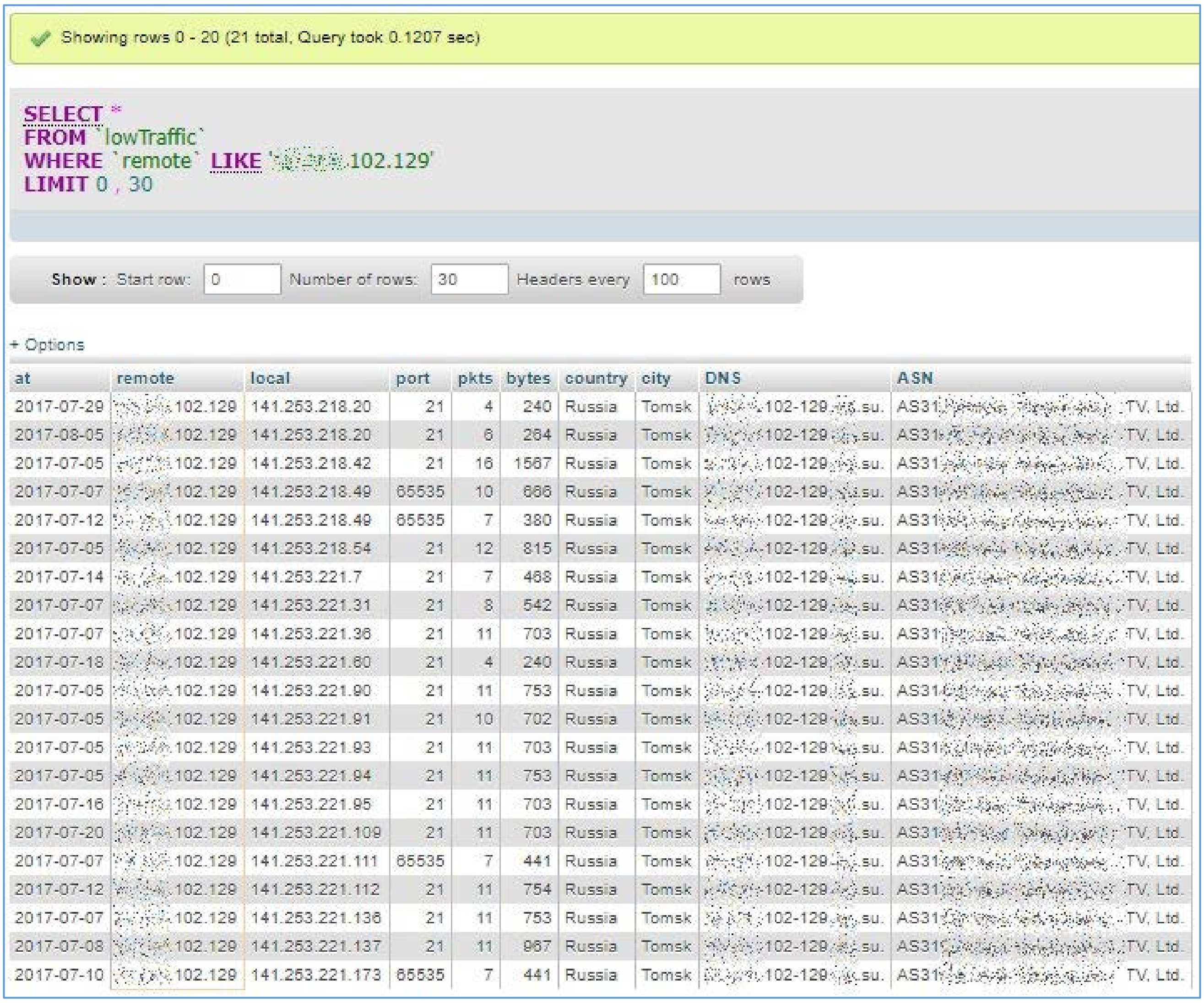
```
SELECT * from scansFrom WHERE remote = 'x.y.118.105' ORDER BY INET_ATON(local) ASC, at ASC;
+------------+-------------+-----------------+-------+------+-------+----------+--------+-------------+-----------------------------------+
| at         | remote      | local           | port  | pkts | bytes | country  | city   | DNS         | ASN                               |
+------------+-------------+-----------------+-------+------+-------+----------+--------+-------------+-----------------------------------+
| 2017-04-29 | x.y.118.105 | 141.253.218.10  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-03-29 | x.y.118.105 | 141.253.218.12  |    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 Provider     |
| 2017-04-06 | x.y.118.105 | 141.253.218.24  |    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  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-03-23 | x.y.118.105 | 141.253.218.27  |    80 |   11 |   492 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-03-29 | x.y.118.105 | 141.253.218.27  |    80 |   11 |   492 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-03-22 | x.y.118.105 | 141.253.218.33  |    80 |   11 |   492 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-03-17 | x.y.118.105 | 141.253.218.52  |    80 |   12 |   532 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-04-15 | x.y.118.105 | 141.253.218.54  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-04-21 | x.y.118.105 | 141.253.218.54  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-03-22 | x.y.118.105 | 141.253.218.58  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-04-21 | x.y.118.105 | 141.253.218.65  |    80 |   13 |   596 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-03-20 | x.y.118.105 | 141.253.221.16  |    80 |   11 |   492 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-03-26 | x.y.118.105 | 141.253.221.29  |    80 |   18 |   796 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-04-10 | x.y.118.105 | 141.253.221.90  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-04-04 | x.y.118.105 | 141.253.221.94  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-04-18 | x.y.118.105 | 141.253.221.94  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-03-19 | x.y.118.105 | 141.253.221.110 |    80 |   10 |   452 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-05-01 | x.y.118.105 | 141.253.221.111 |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-03-26 | x.y.118.105 | 141.253.221.112 |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-04-17 | x.y.118.105 | 141.253.221.117 |    80 |   12 |   532 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-04-29 | x.y.118.105 | 141.253.221.117 |    80 |   11 |   492 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
| 2017-04-07 | x.y.118.105 | 141.253.221.121 |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider     |
+------------+-------------+-----------------+-------+------+-------+----------+--------+-------------+-----------------------------------+
```

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



```
SELECT * from lowTraffic WHERE remote = 'x.y.118.105' ORDER BY at ASC, INET_ATON(local) ASC;
+------------+-------------+-----------------+-------+------+-------+----------+--------+-------------+-------------------------------+
| at         | remote      | local           | port  | pkts | bytes | country  | city   | DNS         | ASN                           |
+------------+-------------+-----------------+-------+------+-------+----------+--------+-------------+-------------------------------+
| 2017-03-17 | x.y.118.105 | 141.253.218.52  |    80 |   12 |   532 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-03-19 | x.y.118.105 | 141.253.221.110 |    80 |   10 |   452 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-03-20 | x.y.118.105 | 141.253.221.16  |    80 |   11 |   492 | 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 |
| 2017-03-22 | x.y.118.105 | 141.253.218.33  |    80 |   11 |   492 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-03-22 | x.y.118.105 | 141.253.218.58  |    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 Provider |
| 2017-03-23 | x.y.118.105 | 141.253.218.27  |    80 |   11 |   492 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-03-26 | x.y.118.105 | 141.253.221.29  |    80 |   18 |   796 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-03-26 | x.y.118.105 | 141.253.221.112 |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-03-29 | x.y.118.105 | 141.253.218.12  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-03-29 | x.y.118.105 | 141.253.218.27  |    80 |   11 |   492 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-04 | x.y.118.105 | 141.253.221.94  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-06 | x.y.118.105 | 141.253.218.24  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-07 | x.y.118.105 | 141.253.221.121 |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-10 | x.y.118.105 | 141.253.221.90  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-15 | x.y.118.105 | 141.253.218.54  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-17 | x.y.118.105 | 141.253.221.117 |    80 |   12 |   532 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-18 | x.y.118.105 | 141.253.221.94  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-21 | x.y.118.105 | 141.253.218.54  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-21 | x.y.118.105 | 141.253.218.65  |    80 |   13 |   596 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-29 | x.y.118.105 | 141.253.218.10  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-04-29 | x.y.118.105 | 141.253.221.117 |    80 |   11 |   492 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-05-01 | x.y.118.105 | 141.253.221.111 |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
| 2017-05-04 | x.y.118.105 | 141.253.218.25  |    80 |    1 |    40 | Malaysia | Pantai | x.y.118.105 | AS47zz, Internet Svc Provider |
+------------+-------------+-----------------+-------+------+-------+----------+--------+-------------+-------------------------------+
```

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



✓ Showing rows 0 - 20 (21 total, Query took 0.1207 sec)

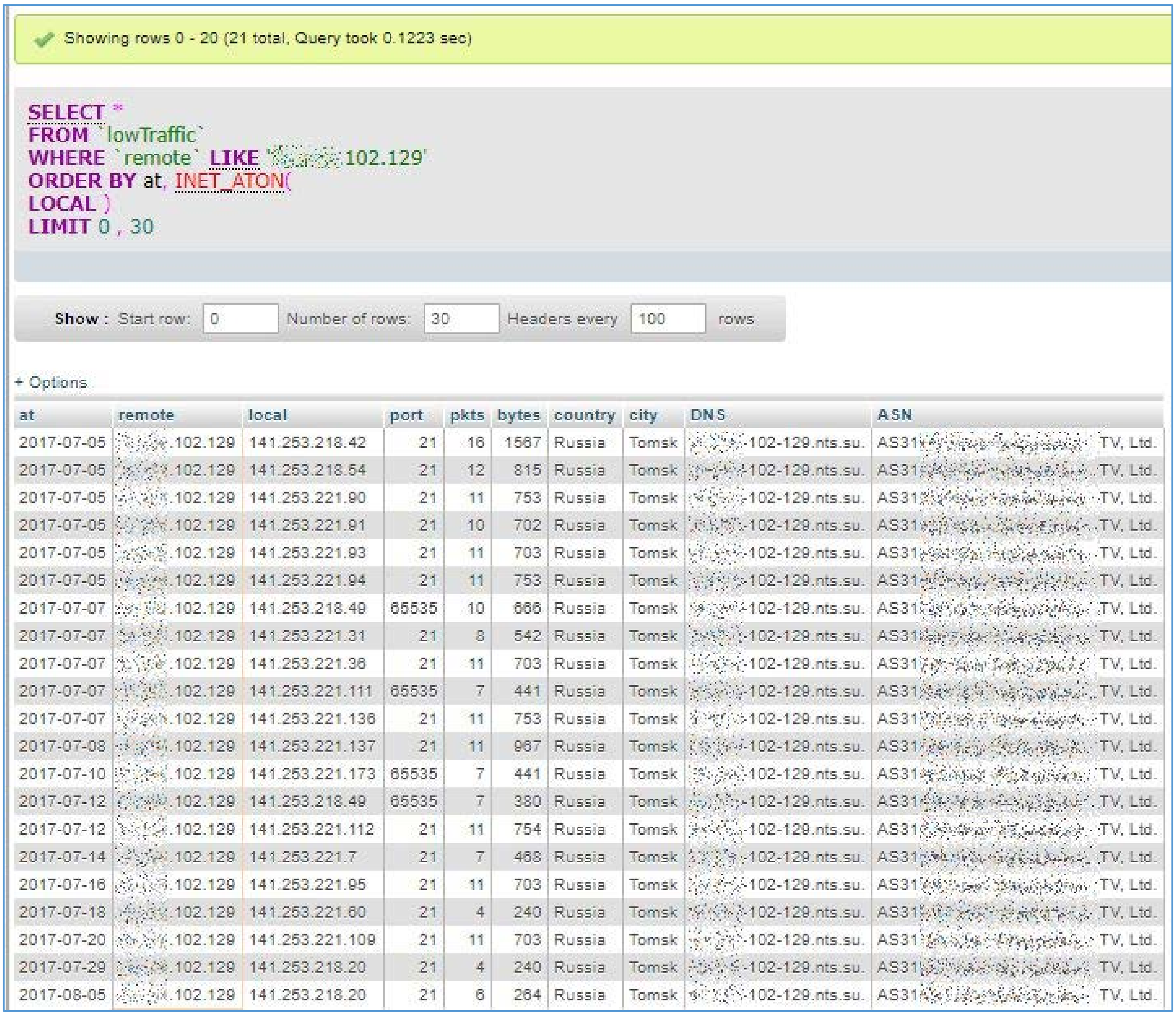
```
SELECT *
FROM `lowTraffic`
WHERE `remote` LIKE '[redacted].102.129'
LIMIT 0 , 30
```

Show : Start row: 0 Number of rows: 30 Headers every 100 rows

+ Options

at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-29	[redacted].102.129	141.253.218.20	21	4	240	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-08-05	[redacted].102.129	141.253.218.20	21	6	284	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.218.42	21	16	1567	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-07	[redacted].102.129	141.253.218.49	65535	10	686	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-12	[redacted].102.129	141.253.218.49	65535	7	380	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.218.54	21	12	815	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-14	[redacted].102.129	141.253.221.7	21	7	468	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-07	[redacted].102.129	141.253.221.31	21	8	542	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-07	[redacted].102.129	141.253.221.36	21	11	703	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-18	[redacted].102.129	141.253.221.60	21	4	240	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.221.90	21	11	753	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.221.91	21	10	702	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.221.93	21	11	703	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.221.94	21	11	753	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-16	[redacted].102.129	141.253.221.95	21	11	703	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-20	[redacted].102.129	141.253.221.109	21	11	703	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-07	[redacted].102.129	141.253.221.111	65535	7	441	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-12	[redacted].102.129	141.253.221.112	21	11	754	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-07	[redacted].102.129	141.253.221.136	21	11	753	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-08	[redacted].102.129	141.253.221.137	21	11	967	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.
2017-07-10	[redacted].102.129	141.253.221.173	65535	7	441	Russia	Tomsk	[redacted]-102-129.[redacted].su.	AS31[redacted] TV, Ltd.

Then ordered by date of occurrence.



✓ Showing rows 0 - 20 (21 total, Query took 0.1223 sec)

```
SELECT *
FROM `lowTraffic`
WHERE `remote` LIKE '[redacted].102.129'
ORDER BY at, INET_ATON(
LOCAL )
LIMIT 0 , 30
```

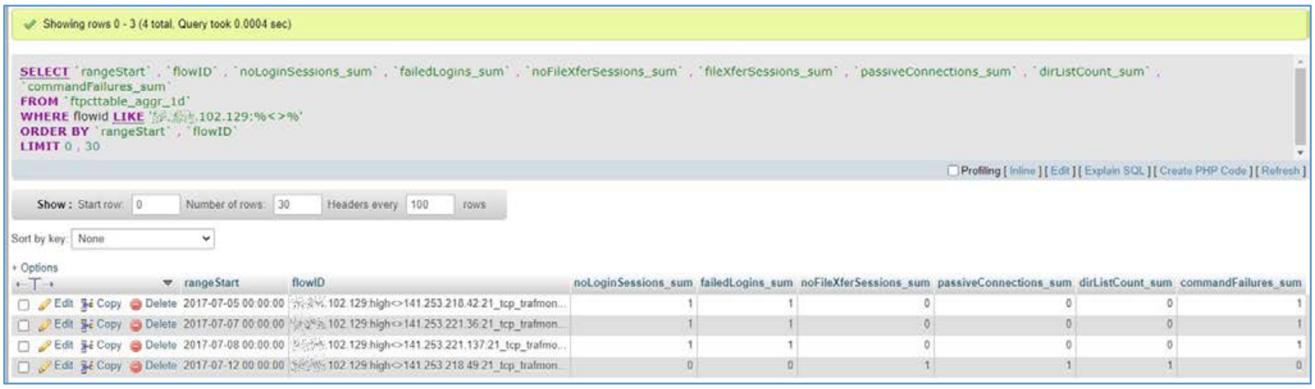
Show : Start row: 0 Number of rows: 30 Headers every 100 rows

+ Options

at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-05	[redacted].102.129	141.253.218.42	21	16	1567	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.218.54	21	12	815	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.221.90	21	11	753	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.221.91	21	10	702	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.221.93	21	11	703	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-05	[redacted].102.129	141.253.221.94	21	11	753	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-07	[redacted].102.129	141.253.218.49	65535	10	666	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-07	[redacted].102.129	141.253.221.31	21	8	542	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-07	[redacted].102.129	141.253.221.36	21	11	703	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-07	[redacted].102.129	141.253.221.111	65535	7	441	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-07	[redacted].102.129	141.253.221.136	21	11	753	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-08	[redacted].102.129	141.253.221.137	21	11	967	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-10	[redacted].102.129	141.253.221.173	65535	7	441	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-12	[redacted].102.129	141.253.218.49	65535	7	380	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-12	[redacted].102.129	141.253.221.112	21	11	754	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-14	[redacted].102.129	141.253.221.7	21	7	468	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-16	[redacted].102.129	141.253.221.95	21	11	703	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-18	[redacted].102.129	141.253.221.60	21	4	240	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-20	[redacted].102.129	141.253.221.109	21	11	703	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-07-29	[redacted].102.129	141.253.218.20	21	4	240	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.
2017-08-05	[redacted].102.129	141.253.218.20	21	6	264	Russia	Tomsk	[redacted]-102-129.nts.su.	AS31[redacted] TV, Ltd.

Now we can look at what this system actually performed in using FTP protocol. So, we retrieve its bi-directional 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` , `noFileXferSessions_sum` , `fileXferSessions_sum` , `passiveConnections_sum` , `dirListCount_sum` ,
`commandFailures_sum`
FROM `ftpcttable_aggr_1d`
WHERE flowid LIKE '[redacted].102.129:%<>%'
ORDER BY `rangeStart` , `flowID`
LIMIT 0 , 30
```

☐ Profiling [Inline] [Edit] [Explain SQL] [Create PHP Code] [Refresh]

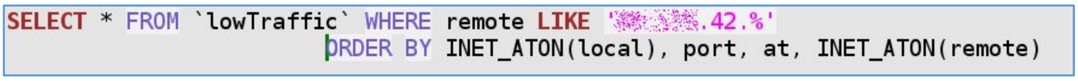
Show : Start row: 0 Number of rows: 30 Headers every 100 rows

Sort by key: None

←T→	rangeStart	flowID	noLoginSessions_sum	failedLogins_sum	noFileXferSessions_sum	passiveConnections_sum	dirListCount_sum	commandFailures_sum
☐ Edit Copy Delete	2017-07-05 00:00:00	[redacted].102.129:high<>141.253.218.42:21_tcp_trafmon...	1	1	0	0	0	1
☐ Edit Copy Delete	2017-07-07 00:00:00	[redacted].102.129:high<>141.253.221.36:21_tcp_trafmon...	1	1	0	0	0	1
☐ Edit Copy Delete	2017-07-08 00:00:00	[redacted].102.129:high<>141.253.221.137:21_tcp_trafmo...	1	1	0	0	0	1
☐ Edit Copy Delete	2017-07-12 00:00:00	[redacted].102.129:high<>141.253.218.49:21_tcp_trafmon...	0	0	1	1	1	0

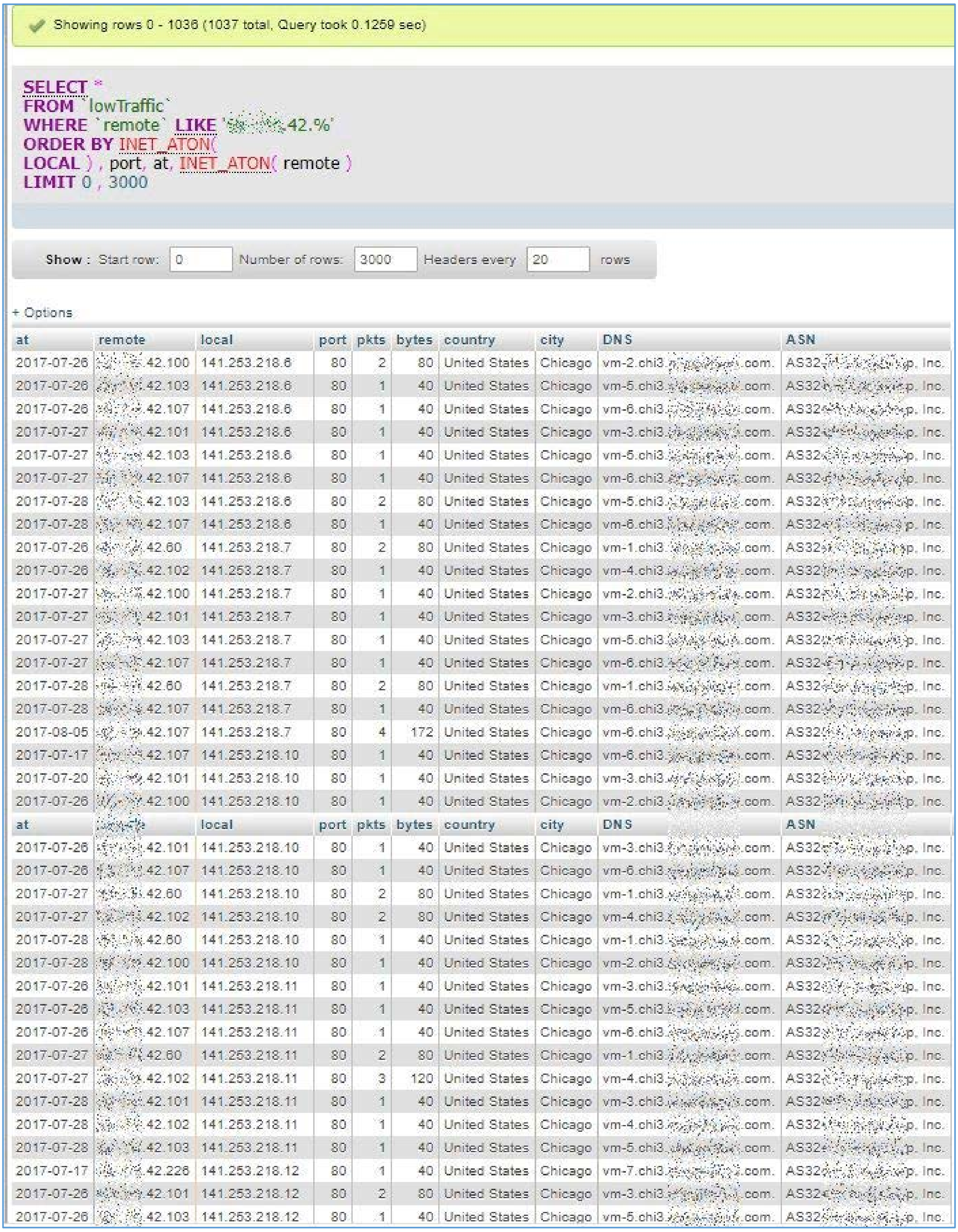
2.5 DISCOVERING BATTERIES OF SCANNERS

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



```
SELECT * FROM `lowTraffic` WHERE remote LIKE '[redacted].42.%'
                        ORDER BY INET_ATON(local), port, at, INET_ATON(remote)
```

First Page: lowest “own” address:



✓ Showing rows 0 - 1036 (1037 total, Query took 0.1259 sec)

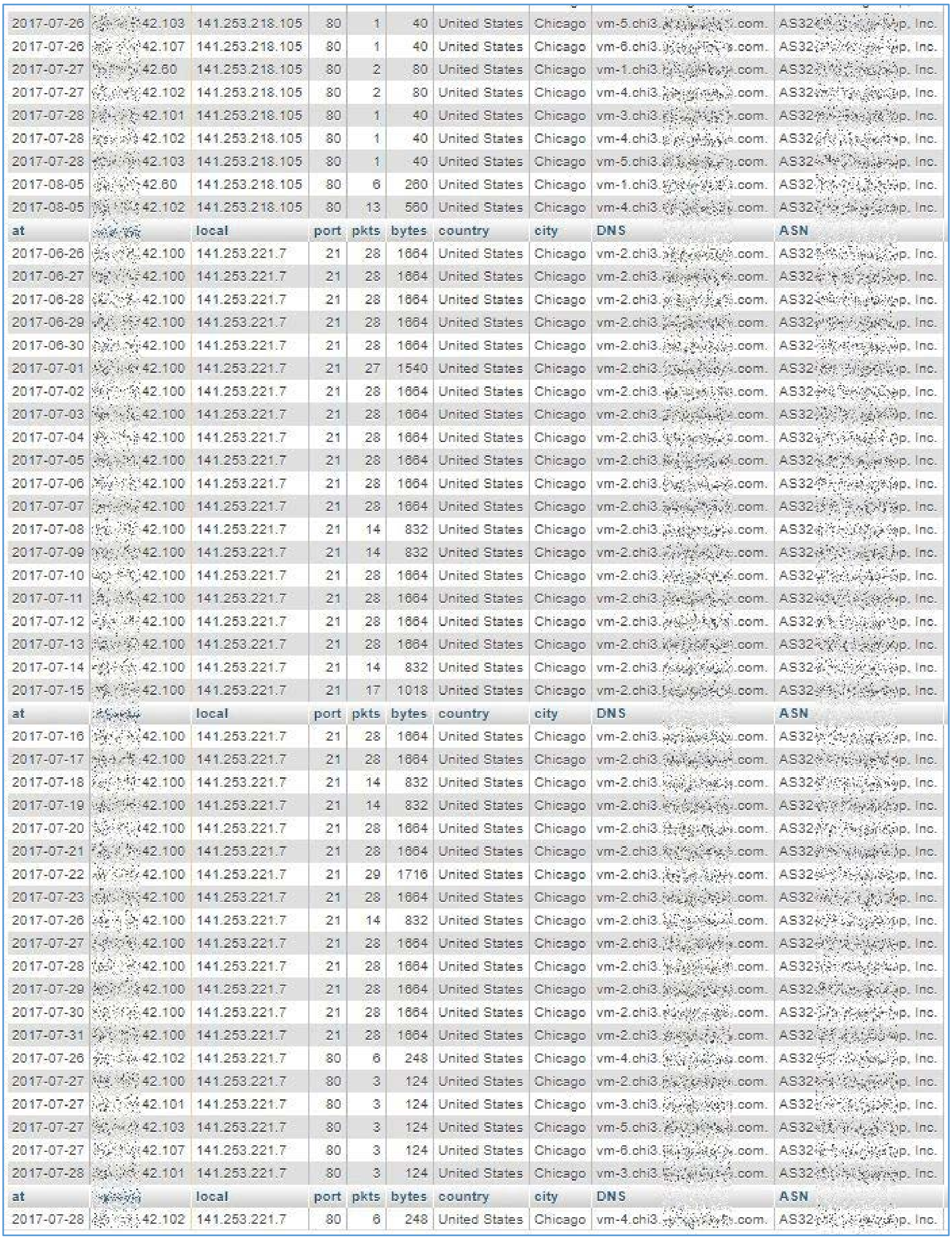
```
SELECT *
FROM `lowTraffic`
WHERE `remote` LIKE '[redacted].42.%'
ORDER BY INET_ATON(
LOCAL ) , port, at, INET_ATON( remote )
LIMIT 0 , 3000
```

Show : Start row: 0 Number of rows: 3000 Headers every 20 rows

+ Options

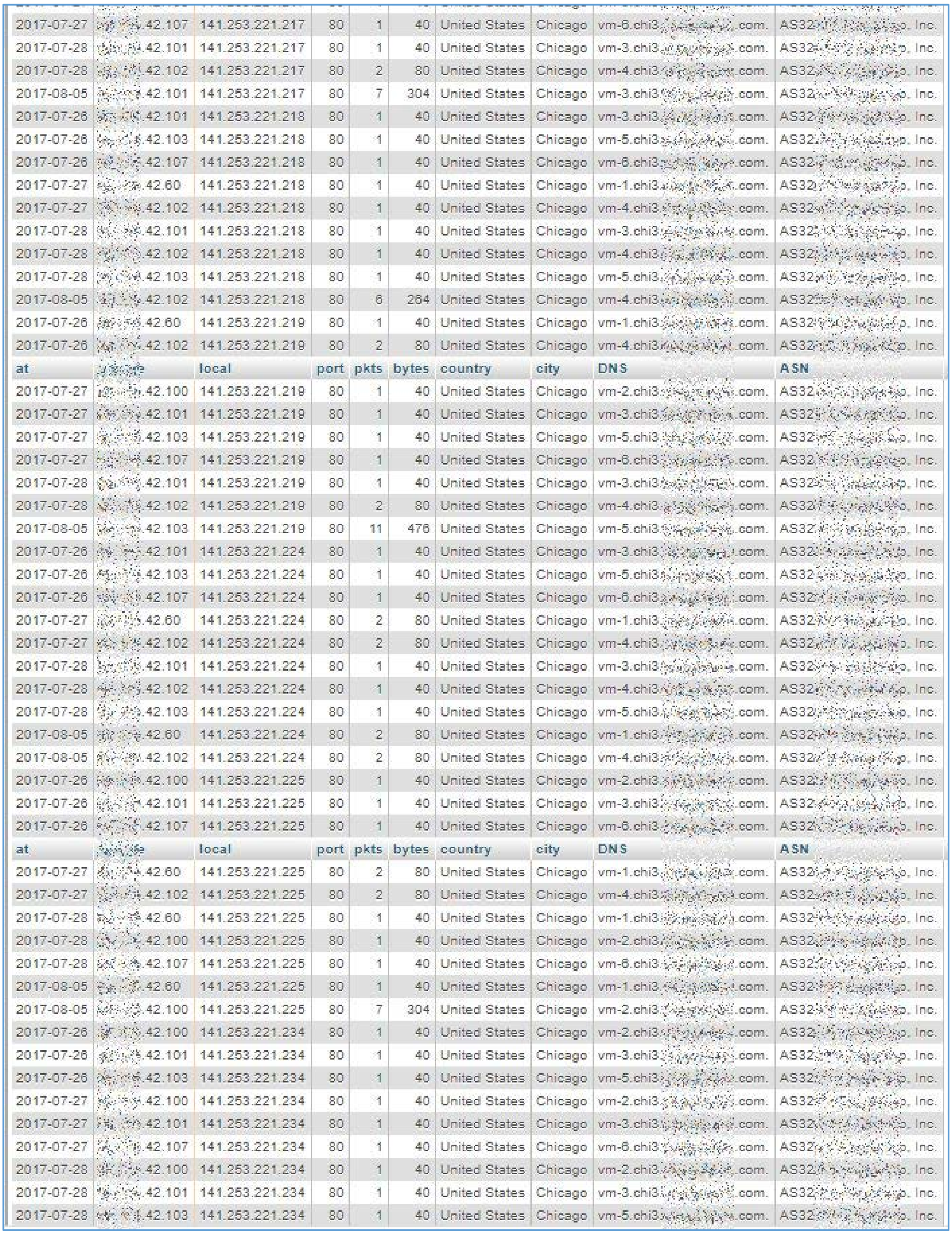
at	remote	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-26	[redacted].42.100	141.253.218.6	80	2	80	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.103	141.253.218.6	80	1	40	United States	Chicago	vm-5.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.107	141.253.218.6	80	1	40	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.101	141.253.218.6	80	1	40	United States	Chicago	vm-3.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.103	141.253.218.6	80	1	40	United States	Chicago	vm-5.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.107	141.253.218.6	80	1	40	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted].42.103	141.253.218.6	80	2	80	United States	Chicago	vm-5.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted].42.107	141.253.218.6	80	1	40	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.60	141.253.218.7	80	2	80	United States	Chicago	vm-1.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.102	141.253.218.7	80	1	40	United States	Chicago	vm-4.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.100	141.253.218.7	80	1	40	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.101	141.253.218.7	80	1	40	United States	Chicago	vm-3.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.103	141.253.218.7	80	1	40	United States	Chicago	vm-5.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.107	141.253.218.7	80	1	40	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted].42.60	141.253.218.7	80	2	80	United States	Chicago	vm-1.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted].42.107	141.253.218.7	80	1	40	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-08-05	[redacted].42.107	141.253.218.7	80	4	172	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-17	[redacted].42.107	141.253.218.10	80	1	40	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-20	[redacted].42.101	141.253.218.10	80	1	40	United States	Chicago	vm-3.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.100	141.253.218.10	80	1	40	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
at	[redacted]	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-26	[redacted].42.101	141.253.218.10	80	1	40	United States	Chicago	vm-3.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.107	141.253.218.10	80	1	40	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.60	141.253.218.10	80	2	80	United States	Chicago	vm-1.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.102	141.253.218.10	80	2	80	United States	Chicago	vm-4.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted].42.60	141.253.218.10	80	1	40	United States	Chicago	vm-1.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted].42.100	141.253.218.10	80	1	40	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.101	141.253.218.11	80	1	40	United States	Chicago	vm-3.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.103	141.253.218.11	80	1	40	United States	Chicago	vm-5.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.107	141.253.218.11	80	1	40	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.60	141.253.218.11	80	2	80	United States	Chicago	vm-1.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted].42.102	141.253.218.11	80	3	120	United States	Chicago	vm-4.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted].42.101	141.253.218.11	80	1	40	United States	Chicago	vm-3.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted].42.102	141.253.218.11	80	1	40	United States	Chicago	vm-4.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted].42.103	141.253.218.11	80	1	40	United States	Chicago	vm-5.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-17	[redacted].42.226	141.253.218.12	80	1	40	United States	Chicago	vm-7.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.101	141.253.218.12	80	2	80	United States	Chicago	vm-3.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted].42.103	141.253.218.12	80	1	40	United States	Chicago	vm-5.chi3.[redacted].com.	AS32[redacted]p. Inc.

Middle Page:



2017-07-26	[redacted]42.103	141.253.218.105	80	1	40	United States	Chicago	vm-5.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted]42.107	141.253.218.105	80	1	40	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted]42.60	141.253.218.105	80	2	80	United States	Chicago	vm-1.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted]42.102	141.253.218.105	80	2	80	United States	Chicago	vm-4.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted]42.101	141.253.218.105	80	1	40	United States	Chicago	vm-3.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted]42.102	141.253.218.105	80	1	40	United States	Chicago	vm-4.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted]42.103	141.253.218.105	80	1	40	United States	Chicago	vm-5.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-08-05	[redacted]42.60	141.253.218.105	80	6	260	United States	Chicago	vm-1.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-08-05	[redacted]42.102	141.253.218.105	80	13	560	United States	Chicago	vm-4.chi3.[redacted].com.	AS32[redacted]p. Inc.
at	[redacted]	local	port	pkts	bytes	country	city	DNS	ASN
2017-06-26	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-06-27	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-06-28	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-06-29	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-06-30	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-01	[redacted]42.100	141.253.221.7	21	27	1540	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-02	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-03	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-04	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-05	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-06	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-07	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-08	[redacted]42.100	141.253.221.7	21	14	832	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-09	[redacted]42.100	141.253.221.7	21	14	832	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-10	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-11	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-12	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-13	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-14	[redacted]42.100	141.253.221.7	21	14	832	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-15	[redacted]42.100	141.253.221.7	21	17	1018	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
at	[redacted]	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-16	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-17	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-18	[redacted]42.100	141.253.221.7	21	14	832	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-19	[redacted]42.100	141.253.221.7	21	14	832	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-20	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-21	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-22	[redacted]42.100	141.253.221.7	21	29	1716	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-23	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted]42.100	141.253.221.7	21	14	832	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-29	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-30	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-31	[redacted]42.100	141.253.221.7	21	28	1664	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-26	[redacted]42.102	141.253.221.7	80	6	248	United States	Chicago	vm-4.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted]42.100	141.253.221.7	80	3	124	United States	Chicago	vm-2.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted]42.101	141.253.221.7	80	3	124	United States	Chicago	vm-3.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted]42.103	141.253.221.7	80	3	124	United States	Chicago	vm-5.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-27	[redacted]42.107	141.253.221.7	80	3	124	United States	Chicago	vm-6.chi3.[redacted].com.	AS32[redacted]p. Inc.
2017-07-28	[redacted]42.101	141.253.221.7	80	3	124	United States	Chicago	vm-3.chi3.[redacted].com.	AS32[redacted]p. Inc.
at	[redacted]	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-28	[redacted]42.102	141.253.221.7	80	6	248	United States	Chicago	vm-4.chi3.[redacted].com.	AS32[redacted]p. Inc.

Last Page: highest "own" address



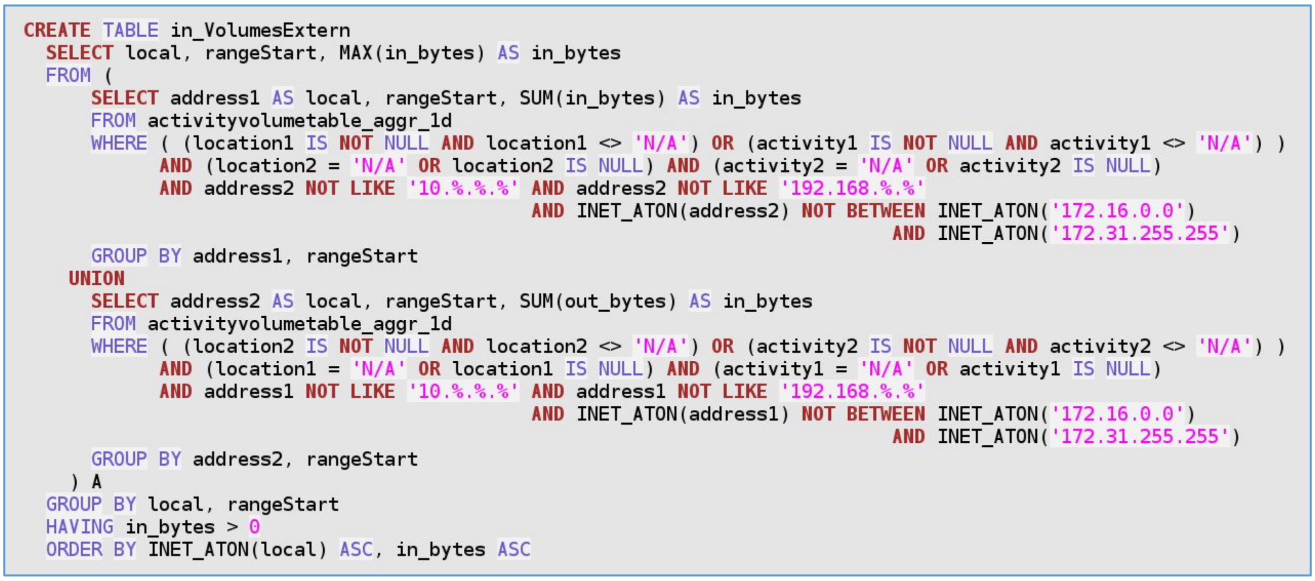
at	[redacted]	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-27	[redacted].42.107	141.253.221.217	80	1	40	United States	Chicago	vm-6.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.101	141.253.221.217	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.102	141.253.221.217	80	2	80	United States	Chicago	vm-4.chi3[redacted].com.	AS32[redacted]. Inc.
2017-08-05	[redacted].42.101	141.253.221.217	80	7	304	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.101	141.253.221.218	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.103	141.253.221.218	80	1	40	United States	Chicago	vm-5.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.107	141.253.221.218	80	1	40	United States	Chicago	vm-6.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.60	141.253.221.218	80	1	40	United States	Chicago	vm-1.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.102	141.253.221.218	80	1	40	United States	Chicago	vm-4.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.101	141.253.221.218	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.102	141.253.221.218	80	1	40	United States	Chicago	vm-4.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.103	141.253.221.218	80	1	40	United States	Chicago	vm-5.chi3[redacted].com.	AS32[redacted]. Inc.
2017-08-05	[redacted].42.102	141.253.221.218	80	6	264	United States	Chicago	vm-4.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.60	141.253.221.219	80	1	40	United States	Chicago	vm-1.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.102	141.253.221.219	80	2	80	United States	Chicago	vm-4.chi3[redacted].com.	AS32[redacted]. Inc.
at	[redacted]	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-27	[redacted].42.100	141.253.221.219	80	1	40	United States	Chicago	vm-2.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.101	141.253.221.219	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.103	141.253.221.219	80	1	40	United States	Chicago	vm-5.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.107	141.253.221.219	80	1	40	United States	Chicago	vm-6.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.101	141.253.221.219	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.102	141.253.221.219	80	2	80	United States	Chicago	vm-4.chi3[redacted].com.	AS32[redacted]. Inc.
2017-08-05	[redacted].42.103	141.253.221.219	80	11	476	United States	Chicago	vm-5.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.101	141.253.221.224	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.103	141.253.221.224	80	1	40	United States	Chicago	vm-5.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.107	141.253.221.224	80	1	40	United States	Chicago	vm-6.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.60	141.253.221.224	80	2	80	United States	Chicago	vm-1.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.102	141.253.221.224	80	2	80	United States	Chicago	vm-4.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.101	141.253.221.224	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.102	141.253.221.224	80	1	40	United States	Chicago	vm-4.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.103	141.253.221.224	80	1	40	United States	Chicago	vm-5.chi3[redacted].com.	AS32[redacted]. Inc.
2017-08-05	[redacted].42.60	141.253.221.224	80	2	80	United States	Chicago	vm-1.chi3[redacted].com.	AS32[redacted]. Inc.
2017-08-05	[redacted].42.102	141.253.221.224	80	2	80	United States	Chicago	vm-4.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.100	141.253.221.225	80	1	40	United States	Chicago	vm-2.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.101	141.253.221.225	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.107	141.253.221.225	80	1	40	United States	Chicago	vm-6.chi3[redacted].com.	AS32[redacted]. Inc.
at	[redacted]	local	port	pkts	bytes	country	city	DNS	ASN
2017-07-27	[redacted].42.60	141.253.221.225	80	2	80	United States	Chicago	vm-1.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.102	141.253.221.225	80	2	80	United States	Chicago	vm-4.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.60	141.253.221.225	80	1	40	United States	Chicago	vm-1.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.100	141.253.221.225	80	1	40	United States	Chicago	vm-2.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.107	141.253.221.225	80	1	40	United States	Chicago	vm-6.chi3[redacted].com.	AS32[redacted]. Inc.
2017-08-05	[redacted].42.60	141.253.221.225	80	1	40	United States	Chicago	vm-1.chi3[redacted].com.	AS32[redacted]. Inc.
2017-08-05	[redacted].42.100	141.253.221.225	80	7	304	United States	Chicago	vm-2.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.100	141.253.221.234	80	1	40	United States	Chicago	vm-2.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.101	141.253.221.234	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-26	[redacted].42.103	141.253.221.234	80	1	40	United States	Chicago	vm-5.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.100	141.253.221.234	80	1	40	United States	Chicago	vm-2.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.101	141.253.221.234	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-27	[redacted].42.107	141.253.221.234	80	1	40	United States	Chicago	vm-6.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.100	141.253.221.234	80	1	40	United States	Chicago	vm-2.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.101	141.253.221.234	80	1	40	United States	Chicago	vm-3.chi3[redacted].com.	AS32[redacted]. Inc.
2017-07-28	[redacted].42.103	141.253.221.234	80	1	40	United States	Chicago	vm-5.chi3[redacted].com.	AS32[redacted]. 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_aggr_1d
      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
    ) A
  GROUP BY local, rangeStart
  HAVING in_bytes > 0
  ORDER BY INET_ATON(local) ASC, in_bytes ASC
```

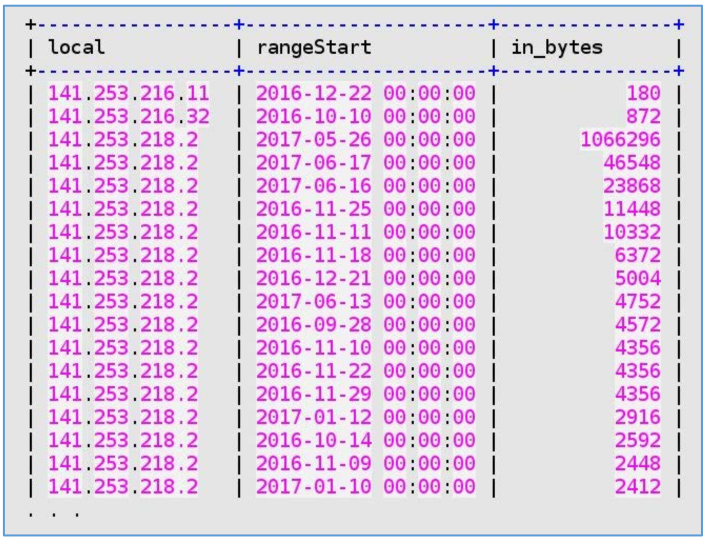
The above SQL statement covers the entire span of available data. The resulting *in_VolumesExtern* table should therefore be recreated regularly at night. This has been implemented as a stored procedure, in the downloadable add-on *trafMon_SecurityExample* package:

```
`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.

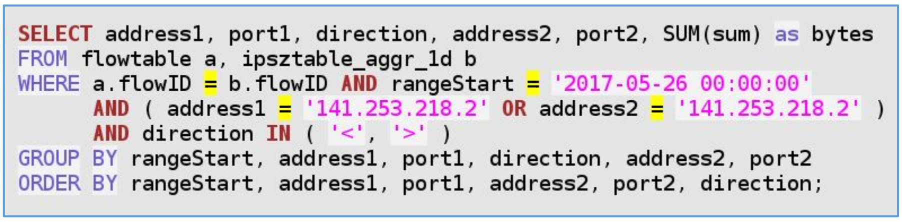
By browsing through the *in_VolumesExtern* table, we can easily compare the daily ingress traffic peaks, numerically sorted, and detect abnormal jumps.

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 daily peak is **23 times higher** than the value of its second ingress daily peak.

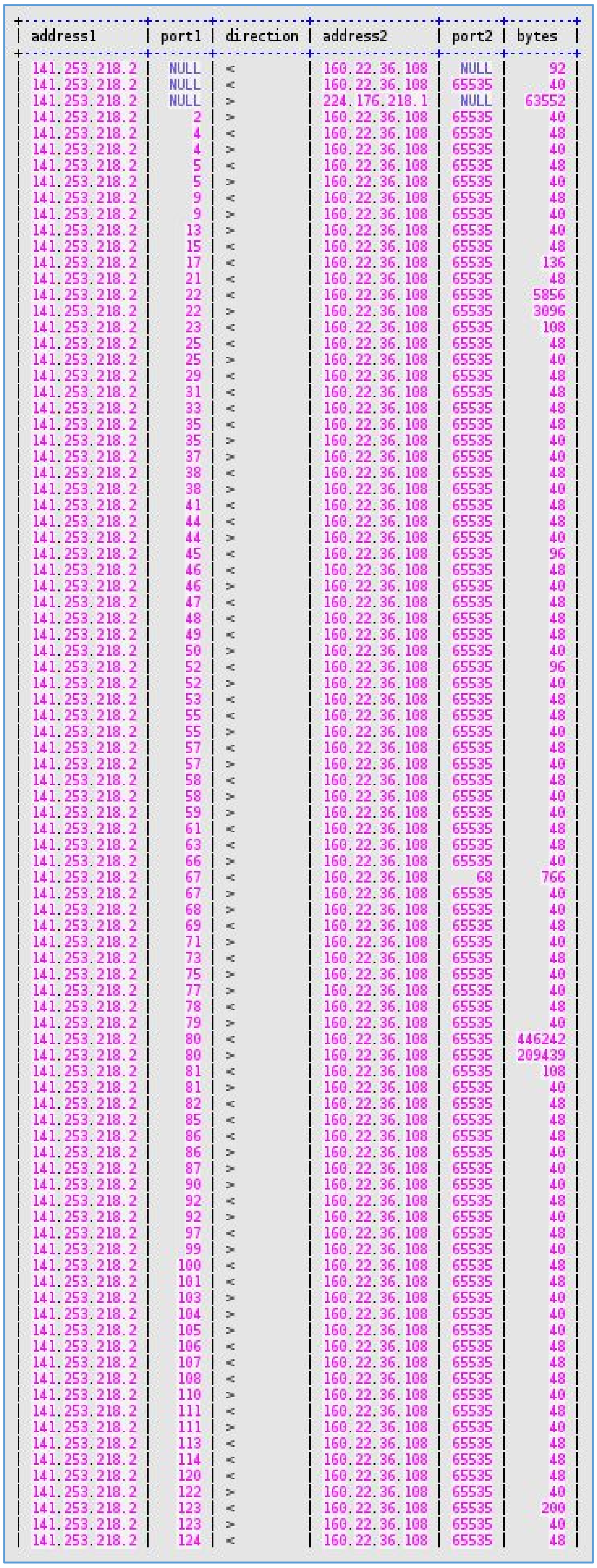


```
+-----------------+---------------------+---------------+
| local           | rangeStart          | in_bytes      |
+-----------------+---------------------+---------------+
| 141.253.216.11  | 2016-12-22 00:00:00 |           180 |
| 141.253.216.32  | 2016-10-10 00:00:00 |           872 |
| 141.253.218.2   | 2017-05-26 00:00:00 |       1066296 |
| 141.253.218.2   | 2017-06-17 00:00:00 |         46548 |
| 141.253.218.2   | 2017-06-16 00:00:00 |         23868 |
| 141.253.218.2   | 2016-11-25 00:00:00 |         11448 |
| 141.253.218.2   | 2016-11-11 00:00:00 |         10332 |
| 141.253.218.2   | 2016-11-18 00:00:00 |          6372 |
| 141.253.218.2   | 2016-12-21 00:00:00 |          5004 |
| 141.253.218.2   | 2017-06-13 00:00:00 |          4752 |
| 141.253.218.2   | 2016-09-28 00:00:00 |          4572 |
| 141.253.218.2   | 2016-11-10 00:00:00 |          4356 |
| 141.253.218.2   | 2016-11-22 00:00:00 |          4356 |
| 141.253.218.2   | 2016-11-29 00:00:00 |          4356 |
| 141.253.218.2   | 2017-01-12 00:00:00 |          2916 |
| 141.253.218.2   | 2016-10-14 00:00:00 |          2592 |
| 141.253.218.2   | 2016-11-09 00:00:00 |          2448 |
| 141.253.218.2   | 2017-01-10 00:00:00 |          2412 |
. . .
```

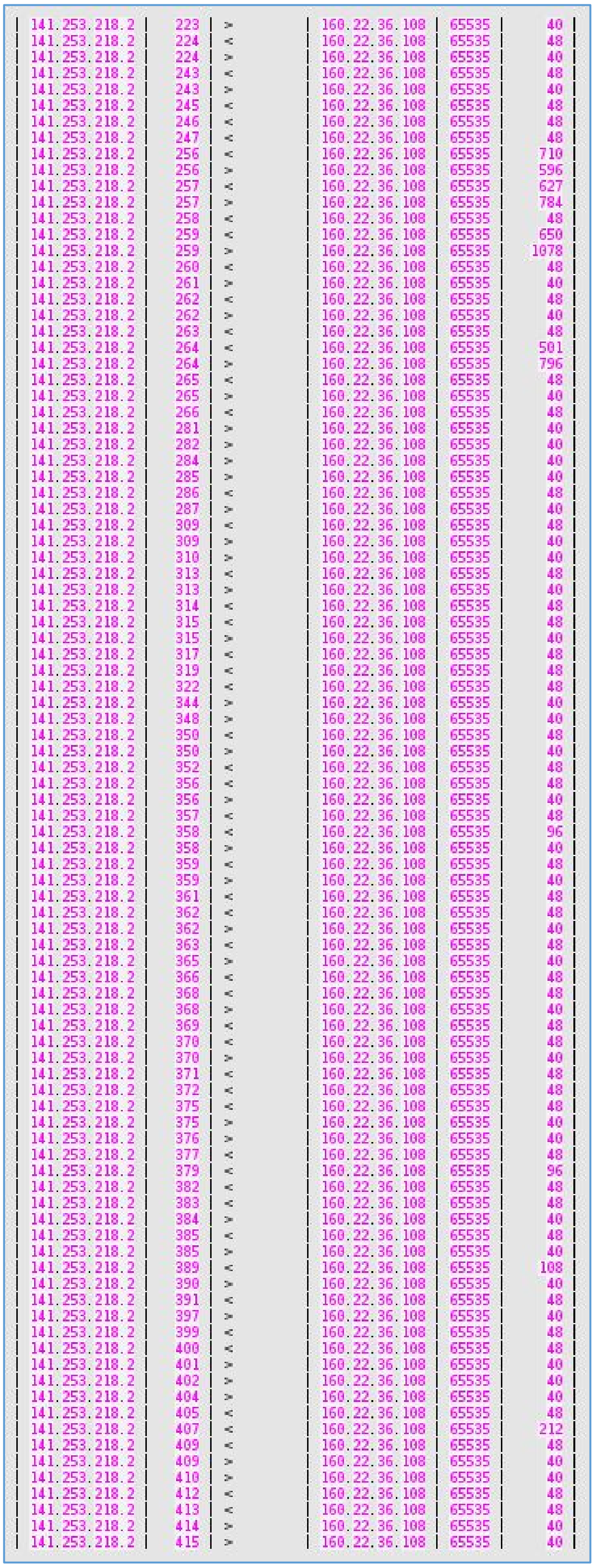
So we take a closer look at this server traffic on that top peak day:



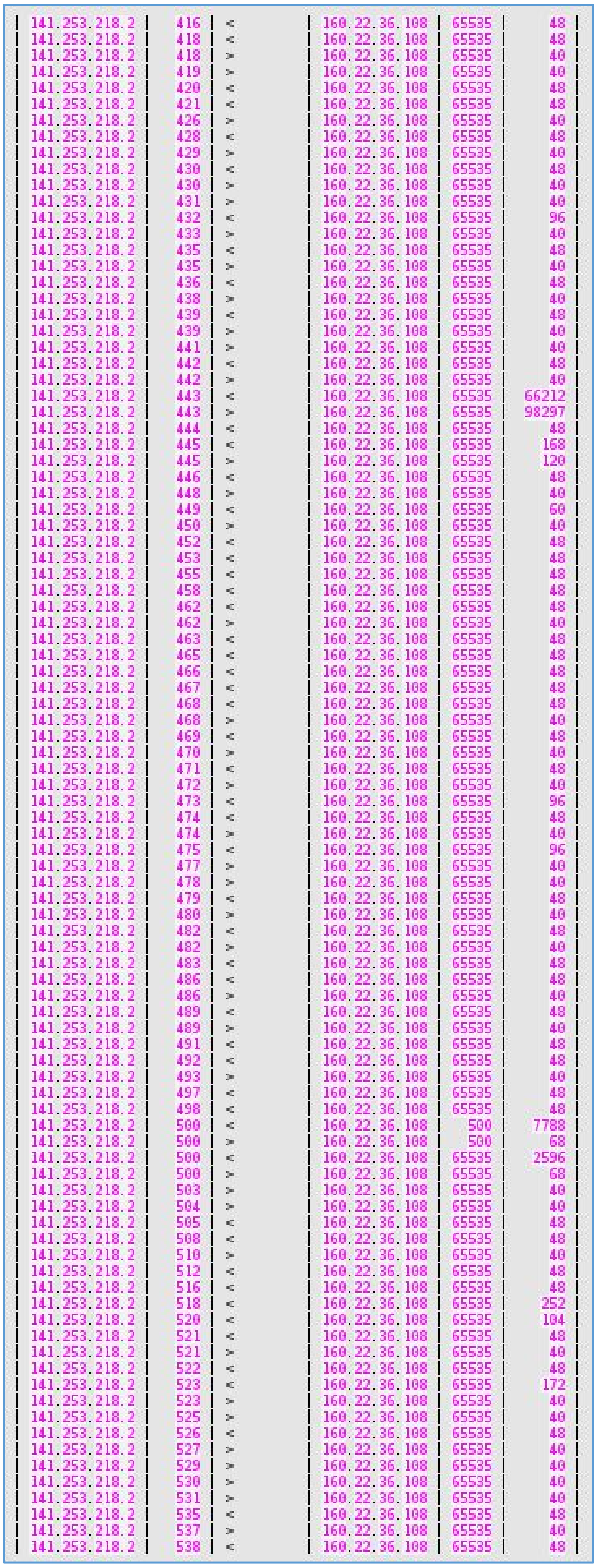
```
SELECT address1, port1, direction, address2, port2, SUM(sum) as bytes
FROM flowtable a, ipsztable_aggr_1d b
WHERE a.flowID = b.flowID AND rangeStart = '2017-05-26 00:00:00'
      AND ( address1 = '141.253.218.2' OR address2 = '141.253.218.2' )
      AND direction IN ( '<', '>' )
GROUP BY rangeStart,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



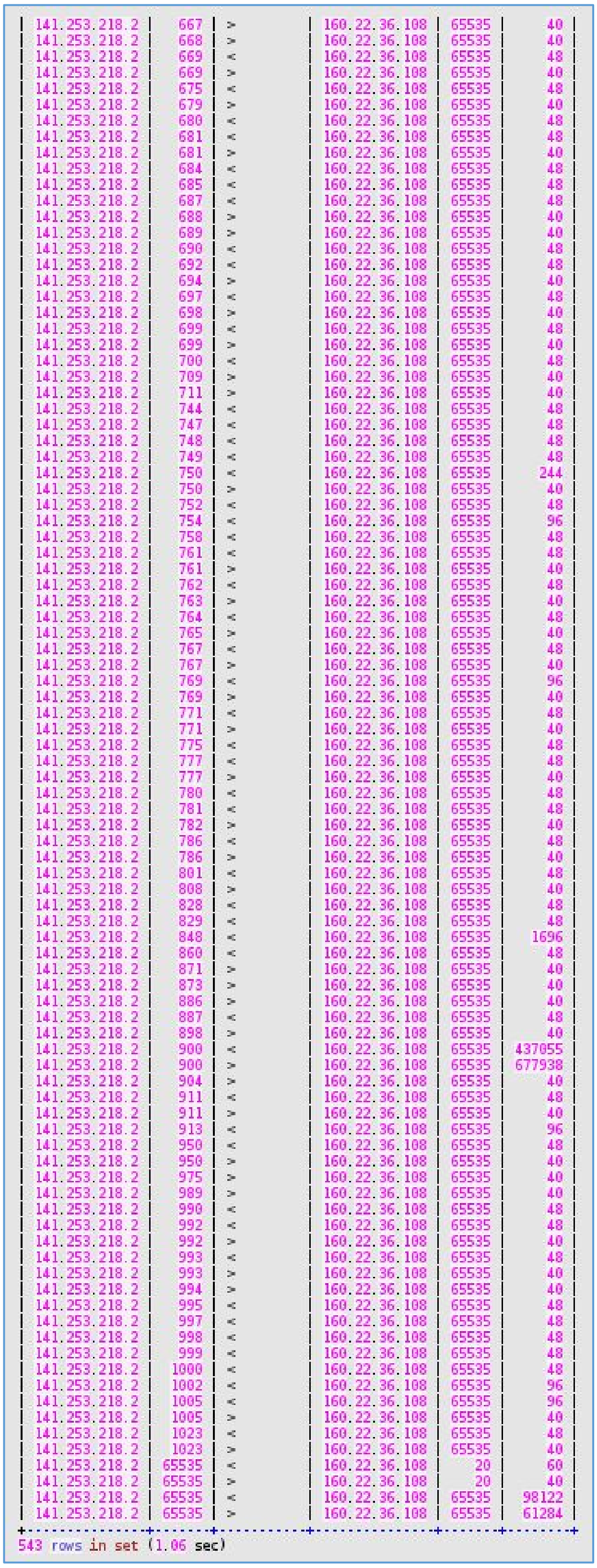
```
+-----------------+-------+-----------+-----------------+-------+--------+
| address1        | port1 | direction | address2        | port2 | bytes  |
+-----------------+-------+-----------+-----------------+-------+--------+
| 141.253.218.2   |  NULL | <         | 160.22.36.108   |  NULL |     92 |
| 141.253.218.2   |  NULL | <         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |  NULL | >         | 224.176.218.1   |  NULL |  63552 |
| 141.253.218.2   |     2 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |     4 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |     4 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |     5 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |     5 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |     9 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |     9 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    13 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    15 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    17 | <         | 160.22.36.108   | 65535 |    136 |
| 141.253.218.2   |    21 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    22 | <         | 160.22.36.108   | 65535 |   5856 |
| 141.253.218.2   |    22 | >         | 160.22.36.108   | 65535 |   3096 |
| 141.253.218.2   |    23 | <         | 160.22.36.108   | 65535 |    108 |
| 141.253.218.2   |    25 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    25 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    29 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    31 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    33 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    35 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    35 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    37 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    38 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    38 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    41 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    44 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    44 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    45 | <         | 160.22.36.108   | 65535 |     96 |
| 141.253.218.2   |    46 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    46 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    47 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    48 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    49 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    50 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    52 | <         | 160.22.36.108   | 65535 |     96 |
| 141.253.218.2   |    52 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    53 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    55 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    55 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    57 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    57 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    58 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    58 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    59 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    61 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    63 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    66 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    67 | <         | 160.22.36.108   |    68 |    766 |
| 141.253.218.2   |    67 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    68 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    69 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    71 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    73 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    75 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    77 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    78 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    79 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    80 | <         | 160.22.36.108   | 65535 | 446242 |
| 141.253.218.2   |    80 | >         | 160.22.36.108   | 65535 | 209439 |
| 141.253.218.2   |    81 | <         | 160.22.36.108   | 65535 |    108 |
| 141.253.218.2   |    81 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    82 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    85 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    86 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    86 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    87 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    90 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    92 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    92 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |    97 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |    99 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   100 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   101 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   103 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   104 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   105 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   106 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   107 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   108 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   110 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   111 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   111 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   113 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   114 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   120 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   122 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   123 | <         | 160.22.36.108   | 65535 |    200 |
| 141.253.218.2   |   123 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   124 | <         | 160.22.36.108   | 65535 |     48 |
```



```
| 141.253.218.2   |   223 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   224 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   224 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   243 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   243 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   245 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   246 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   247 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   256 | <         | 160.22.36.108   | 65535 |    710 |
| 141.253.218.2   |   256 | >         | 160.22.36.108   | 65535 |    596 |
| 141.253.218.2   |   257 | <         | 160.22.36.108   | 65535 |    627 |
| 141.253.218.2   |   257 | >         | 160.22.36.108   | 65535 |    784 |
| 141.253.218.2   |   258 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   259 | <         | 160.22.36.108   | 65535 |    650 |
| 141.253.218.2   |   259 | >         | 160.22.36.108   | 65535 |   1078 |
| 141.253.218.2   |   260 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   261 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   262 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   262 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   263 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   264 | <         | 160.22.36.108   | 65535 |    501 |
| 141.253.218.2   |   264 | >         | 160.22.36.108   | 65535 |    796 |
| 141.253.218.2   |   265 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   265 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   266 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   281 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   282 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   284 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   285 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   286 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   287 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   309 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   309 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   310 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   313 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   313 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   314 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   315 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   315 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   317 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   319 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   322 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   344 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   348 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   350 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   350 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   352 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   356 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   356 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   357 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   358 | <         | 160.22.36.108   | 65535 |     96 |
| 141.253.218.2   |   358 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   359 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   359 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   361 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   362 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   362 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   363 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   365 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   366 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   368 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   368 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   369 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   370 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   370 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   371 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   372 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   375 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   375 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   376 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   377 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   379 | <         | 160.22.36.108   | 65535 |     96 |
| 141.253.218.2   |   382 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   383 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   384 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   385 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   385 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   389 | <         | 160.22.36.108   | 65535 |    108 |
| 141.253.218.2   |   390 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   391 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   397 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   399 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   400 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   401 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   402 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   404 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   405 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   407 | <         | 160.22.36.108   | 65535 |    212 |
| 141.253.218.2   |   409 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   409 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   410 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   412 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   413 | <         | 160.22.36.108   | 65535 |     48 |
| 141.253.218.2   |   414 | >         | 160.22.36.108   | 65535 |     40 |
| 141.253.218.2   |   415 | >         | 160.22.36.108   | 65535 |     40 |
```



```
| 141.253.218.2 |   416 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   418 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   418 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   419 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   420 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   421 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   426 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   428 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   429 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   430 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   430 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   431 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   432 | <          | 160.22.36.108 | 65535 |     96 |
| 141.253.218.2 |   433 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   435 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   435 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   436 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   438 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   439 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   439 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   441 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   442 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   442 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   443 | <          | 160.22.36.108 | 65535 |  66212 |
| 141.253.218.2 |   443 | >          | 160.22.36.108 | 65535 |  98297 |
| 141.253.218.2 |   444 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   445 | <          | 160.22.36.108 | 65535 |    168 |
| 141.253.218.2 |   445 | >          | 160.22.36.108 | 65535 |    120 |
| 141.253.218.2 |   446 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   448 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   449 | <          | 160.22.36.108 | 65535 |     60 |
| 141.253.218.2 |   450 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   452 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   453 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   455 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   458 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   462 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   462 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   463 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   465 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   466 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   467 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   468 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   468 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   469 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   470 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   471 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   472 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   473 | <          | 160.22.36.108 | 65535 |     96 |
| 141.253.218.2 |   474 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   474 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   475 | <          | 160.22.36.108 | 65535 |     96 |
| 141.253.218.2 |   477 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   478 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   479 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   480 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   482 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   482 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   483 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   486 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   486 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   489 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   489 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   491 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   492 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   493 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   497 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   498 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   500 | <          | 160.22.36.108 |   500 |   7788 |
| 141.253.218.2 |   500 | >          | 160.22.36.108 |   500 |     68 |
| 141.253.218.2 |   500 | <          | 160.22.36.108 | 65535 |   2596 |
| 141.253.218.2 |   500 | >          | 160.22.36.108 | 65535 |     68 |
| 141.253.218.2 |   503 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   504 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   505 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   508 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   510 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   512 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   516 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   518 | <          | 160.22.36.108 | 65535 |    252 |
| 141.253.218.2 |   520 | <          | 160.22.36.108 | 65535 |    104 |
| 141.253.218.2 |   521 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   521 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   522 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   523 | <          | 160.22.36.108 | 65535 |    172 |
| 141.253.218.2 |   523 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   525 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   526 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   527 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   529 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   530 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   531 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   535 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   537 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   538 | <          | 160.22.36.108 | 65535 |     48 |
```



```
| 141.253.218.2 |   667 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   668 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   669 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   669 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   675 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   679 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   680 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   681 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   681 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   684 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   685 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   687 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   688 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   689 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   690 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   692 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   694 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   697 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   698 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   699 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   699 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   700 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   709 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   711 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   744 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   747 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   748 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   749 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   750 | <          | 160.22.36.108 | 65535 |    244 |
| 141.253.218.2 |   750 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   752 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   754 | <          | 160.22.36.108 | 65535 |     96 |
| 141.253.218.2 |   758 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   761 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   761 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   762 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   763 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   764 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   765 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   767 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   767 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   769 | <          | 160.22.36.108 | 65535 |     96 |
| 141.253.218.2 |   769 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   771 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   771 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   775 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   777 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   777 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   780 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   781 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   782 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   786 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   786 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   801 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   808 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   828 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   829 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   848 | <          | 160.22.36.108 | 65535 |   1696 |
| 141.253.218.2 |   860 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   871 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   873 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   886 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   887 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   898 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   900 | <          | 160.22.36.108 | 65535 | 437055 |
| 141.253.218.2 |   900 | >          | 160.22.36.108 | 65535 | 677938 |
| 141.253.218.2 |   904 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   911 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   911 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   913 | <          | 160.22.36.108 | 65535 |     96 |
| 141.253.218.2 |   950 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   950 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   975 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   989 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   990 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   992 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   992 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   993 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   993 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   994 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |   995 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   997 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   998 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |   999 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |  1000 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |  1002 | <          | 160.22.36.108 | 65535 |     96 |
| 141.253.218.2 |  1005 | <          | 160.22.36.108 | 65535 |     96 |
| 141.253.218.2 |  1005 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 |  1023 | <          | 160.22.36.108 | 65535 |     48 |
| 141.253.218.2 |  1023 | >          | 160.22.36.108 | 65535 |     40 |
| 141.253.218.2 | 65535 | <          | 160.22.36.108 |    20 |     60 |
| 141.253.218.2 | 65535 | >          | 160.22.36.108 |    20 |     40 |
| 141.253.218.2 | 65535 | <          | 160.22.36.108 | 65535 |  98122 |
| 141.253.218.2 | 65535 | >          | 160.22.36.108 | 65535 |  61284 |
+---------------+-------+------------+---------------+-------+--------+
543 rows in set (1.06 sec)
```

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 the port scan and the penetration testing by a Nessus scanner (*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 significant 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.

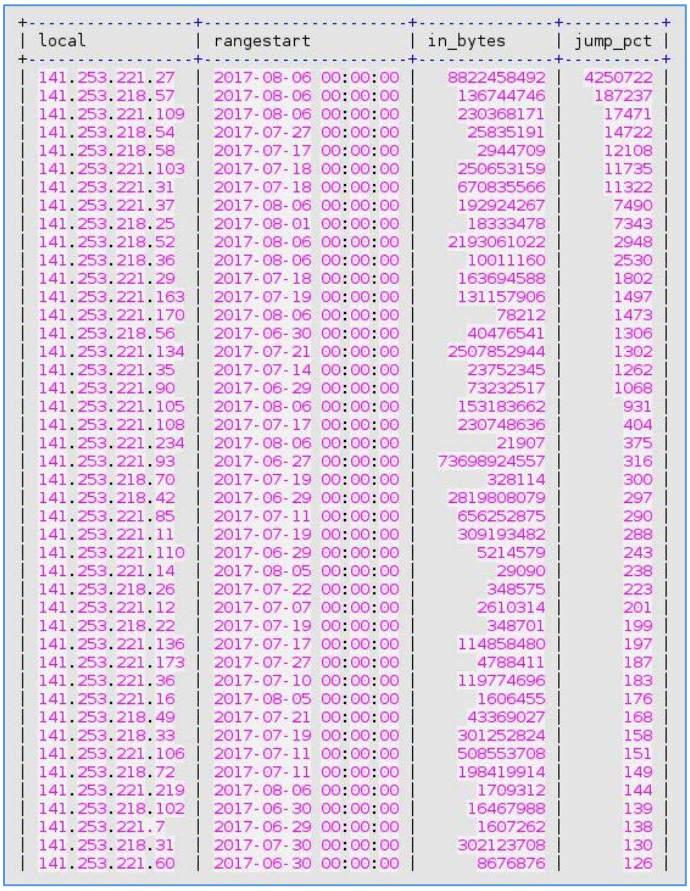
By what factor is the volume first peak larger than the second peak?

Based on the table *in_VolumesExtern* presented above, the following queries sequence automatically retrieves:

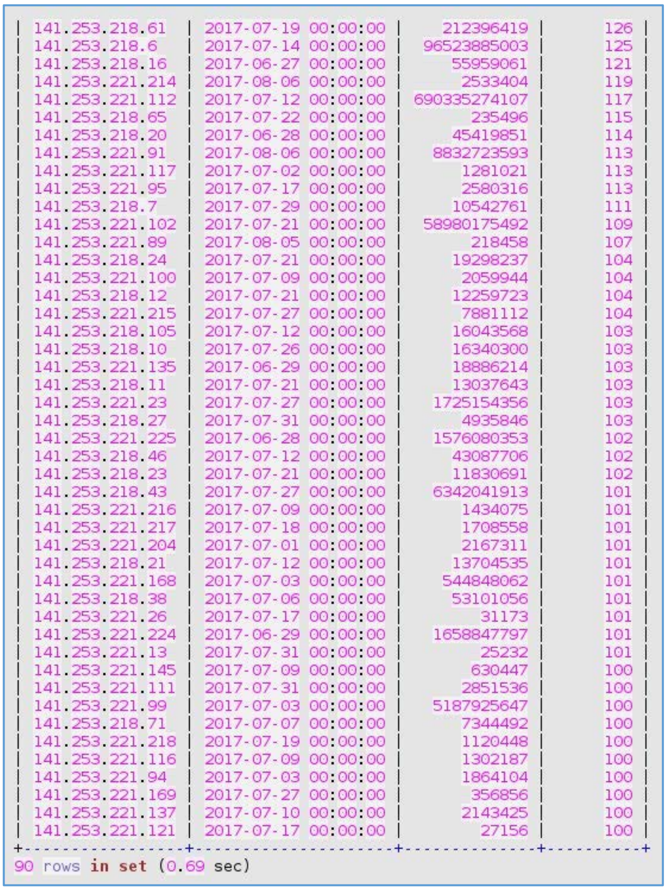
1. the value of the top peak
2. the value of the second highest peak

In order to compute the percentage of sudden increase, 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
```



```
+-----------------+---------------------+-------------+----------+
| local           | rangestart          | in_bytes    | jump_pct |
+-----------------+---------------------+-------------+----------+
| 141.253.221.27  | 2017-08-06 00:00:00 |  8822458492 |  4250722 |
| 141.253.218.57  | 2017-08-06 00:00:00 |   136744746 |   187237 |
| 141.253.221.109 | 2017-08-06 00:00:00 |   230368171 |    17471 |
| 141.253.218.54  | 2017-07-27 00:00:00 |    25835191 |    14722 |
| 141.253.218.58  | 2017-07-17 00:00:00 |     2944709 |    12108 |
| 141.253.221.103 | 2017-07-18 00:00:00 |   250653159 |    11735 |
| 141.253.221.31  | 2017-07-18 00:00:00 |   670835566 |    11322 |
| 141.253.221.37  | 2017-08-06 00:00:00 |   192924267 |     7490 |
| 141.253.218.25  | 2017-08-01 00:00:00 |    18333478 |     7343 |
| 141.253.218.52  | 2017-08-06 00:00:00 |  2193061022 |     2948 |
| 141.253.218.36  | 2017-08-06 00:00:00 |    10011160 |     2530 |
| 141.253.221.29  | 2017-07-18 00:00:00 |   163694588 |     1802 |
| 141.253.221.163 | 2017-07-19 00:00:00 |   131157906 |     1497 |
| 141.253.221.170 | 2017-08-06 00:00:00 |       78212 |     1473 |
| 141.253.218.56  | 2017-06-30 00:00:00 |    40476541 |     1306 |
| 141.253.221.134 | 2017-07-21 00:00:00 |  2507852944 |     1302 |
| 141.253.221.35  | 2017-07-14 00:00:00 |    23752345 |     1262 |
| 141.253.221.90  | 2017-06-29 00:00:00 |    73232517 |     1068 |
| 141.253.221.105 | 2017-08-06 00:00:00 |   153183662 |      931 |
| 141.253.221.108 | 2017-07-17 00:00:00 |   230748636 |      404 |
| 141.253.221.234 | 2017-08-06 00:00:00 |       21907 |      375 |
| 141.253.221.93  | 2017-06-27 00:00:00 | 73698924557 |      316 |
| 141.253.218.70  | 2017-07-19 00:00:00 |      328114 |      300 |
| 141.253.218.42  | 2017-06-29 00:00:00 |  2819808079 |      297 |
| 141.253.221.85  | 2017-07-11 00:00:00 |   656252875 |      290 |
| 141.253.221.11  | 2017-07-19 00:00:00 |   309193482 |      288 |
| 141.253.221.110 | 2017-06-29 00:00:00 |     5214579 |      243 |
| 141.253.221.14  | 2017-08-05 00:00:00 |       29090 |      238 |
| 141.253.218.26  | 2017-07-22 00:00:00 |      348575 |      223 |
| 141.253.221.12  | 2017-07-07 00:00:00 |     2610314 |      201 |
| 141.253.218.22  | 2017-07-19 00:00:00 |      348701 |      199 |
| 141.253.221.136 | 2017-07-17 00:00:00 |   114858480 |      197 |
| 141.253.221.173 | 2017-07-27 00:00:00 |     4788411 |      187 |
| 141.253.221.36  | 2017-07-10 00:00:00 |   119774696 |      183 |
| 141.253.221.16  | 2017-08-05 00:00:00 |     1606455 |      176 |
| 141.253.218.49  | 2017-07-21 00:00:00 |    43369027 |      168 |
| 141.253.218.33  | 2017-07-19 00:00:00 |   301252824 |      158 |
| 141.253.221.106 | 2017-07-11 00:00:00 |   508553708 |      151 |
| 141.253.218.72  | 2017-07-11 00:00:00 |   198419914 |      149 |
| 141.253.221.219 | 2017-08-06 00:00:00 |     1709312 |      144 |
| 141.253.218.102 | 2017-06-30 00:00:00 |    16467988 |      139 |
| 141.253.221.7   | 2017-06-29 00:00:00 |     1607262 |      138 |
| 141.253.218.31  | 2017-07-30 00:00:00 |   302123708 |      130 |
| 141.253.221.60  | 2017-06-30 00:00:00 |     8676876 |      126 |
```



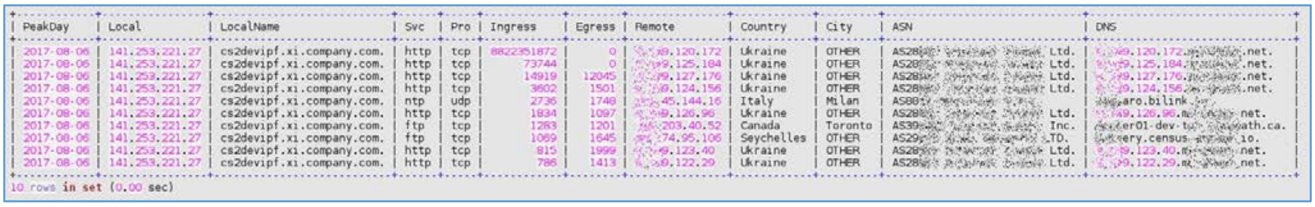
```
| 141.253.218.61  | 2017-07-19 00:00:00 |    212396419 |      126 |
| 141.253.218.6   | 2017-07-14 00:00:00 |  96523885003 |      125 |
| 141.253.218.16  | 2017-06-27 00:00:00 |     55959061 |      121 |
| 141.253.221.214 | 2017-08-06 00:00:00 |      2533404 |      119 |
| 141.253.221.112 | 2017-07-12 00:00:00 | 690335274107 |      117 |
| 141.253.218.65  | 2017-07-22 00:00:00 |       235496 |      115 |
| 141.253.218.20  | 2017-06-28 00:00:00 |     45419851 |      114 |
| 141.253.221.91  | 2017-08-06 00:00:00 |   8832723593 |      113 |
| 141.253.221.117 | 2017-07-02 00:00:00 |      1281021 |      113 |
| 141.253.221.95  | 2017-07-17 00:00:00 |      2580316 |      113 |
| 141.253.218.7   | 2017-07-29 00:00:00 |     10542761 |      111 |
| 141.253.221.102 | 2017-07-21 00:00:00 |  58980175492 |      109 |
| 141.253.221.89  | 2017-08-05 00:00:00 |       218458 |      107 |
| 141.253.218.24  | 2017-07-21 00:00:00 |     19298237 |      104 |
| 141.253.221.100 | 2017-07-09 00:00:00 |      2059944 |      104 |
| 141.253.218.12  | 2017-07-21 00:00:00 |     12259723 |      104 |
| 141.253.221.215 | 2017-07-27 00:00:00 |      7881112 |      104 |
| 141.253.218.105 | 2017-07-12 00:00:00 |     16043568 |      103 |
| 141.253.218.10  | 2017-07-26 00:00:00 |     16340300 |      103 |
| 141.253.221.135 | 2017-06-29 00:00:00 |     18886214 |      103 |
| 141.253.218.11  | 2017-07-21 00:00:00 |     13037643 |      103 |
| 141.253.221.23  | 2017-07-27 00:00:00 |   1725154356 |      103 |
| 141.253.218.27  | 2017-07-31 00:00:00 |      4935846 |      103 |
| 141.253.221.225 | 2017-06-28 00:00:00 |   1576080353 |      102 |
| 141.253.218.46  | 2017-07-12 00:00:00 |     43087706 |      102 |
| 141.253.218.23  | 2017-07-21 00:00:00 |     11830691 |      102 |
| 141.253.218.43  | 2017-07-27 00:00:00 |   6342041913 |      101 |
| 141.253.221.216 | 2017-07-09 00:00:00 |      1434075 |      101 |
| 141.253.221.217 | 2017-07-18 00:00:00 |      1708558 |      101 |
| 141.253.221.204 | 2017-07-01 00:00:00 |      2167311 |      101 |
| 141.253.218.21  | 2017-07-12 00:00:00 |     13704535 |      101 |
| 141.253.221.168 | 2017-07-03 00:00:00 |    544848062 |      101 |
| 141.253.218.38  | 2017-07-06 00:00:00 |     53101056 |      101 |
| 141.253.221.26  | 2017-07-17 00:00:00 |        31173 |      101 |
| 141.253.221.224 | 2017-06-29 00:00:00 |   1658847797 |      101 |
| 141.253.221.13  | 2017-07-31 00:00:00 |        25232 |      101 |
| 141.253.221.145 | 2017-07-09 00:00:00 |       630447 |      100 |
| 141.253.221.111 | 2017-07-31 00:00:00 |      2851536 |      100 |
| 141.253.221.99  | 2017-07-03 00:00:00 |   5187925647 |      100 |
| 141.253.218.71  | 2017-07-07 00:00:00 |      7344492 |      100 |
| 141.253.221.218 | 2017-07-19 00:00:00 |      1120448 |      100 |
| 141.253.221.116 | 2017-07-09 00:00:00 |      1302187 |      100 |
| 141.253.221.94  | 2017-07-03 00:00:00 |      1864104 |      100 |
| 141.253.221.169 | 2017-07-27 00:00:00 |       356856 |      100 |
| 141.253.221.137 | 2017-07-10 00:00:00 |      2143425 |      100 |
| 141.253.221.121 | 2017-07-17 00:00:00 |        27156 |      100 |
+-----------------+---------------------+--------------+----------+
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:

```
--
-- Retrieves the TopN remote senders to the given local own system
-- and order them by decreasing ingress volume
--
  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 = '2017-08-06 00:00:00' AND address1 = '141.253.221.27'
            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
     ORDER BY Ingress DESC LIMIT 10;
```

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



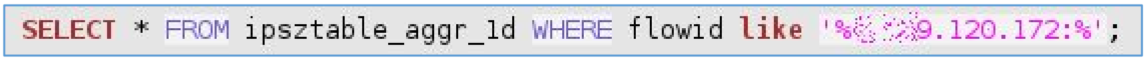
```
+------------+----------------+---------------------------+------+-----+------------+--------+---------------------+------------+---------+----------------------------+------------------------------------------+
| PeakDay    | Local          | LocalName                 | Svc  | Pro | Ingress    | Egress | Remote              | Country    | City    | ASN                        | DNS                                      |
+------------+----------------+---------------------------+------+-----+------------+--------+---------------------+------------+---------+----------------------------+------------------------------------------+
| 2017-08-06 | 141.253.221.27 | cs2devipf.xi.company.com. | http | tcp | 8822351872 |      0 | [redacted]9.120.172 | Ukraine    | OTHER   | AS28[redacted] Ltd.        | [redacted]9.120.172.[redacted].net.      |
| 2017-08-06 | 141.253.221.27 | cs2devipf.xi.company.com. | http | tcp |      73744 |      0 | [redacted]9.125.184 | Ukraine    | OTHER   | AS28[redacted] Ltd.        | [redacted]9.125.184.[redacted].net.      |
| 2017-08-06 | 141.253.221.27 | cs2devipf.xi.company.com. | http | tcp |      14919 |  12045 | [redacted]9.127.176 | Ukraine    | OTHER   | AS28[redacted] Ltd.        | [redacted]9.127.176.[redacted].net.      |
| 2017-08-06 | 141.253.221.27 | cs2devipf.xi.company.com. | http | tcp |       3602 |   1501 | [redacted]9.124.156 | Ukraine    | OTHER   | AS28[redacted] Ltd.        | [redacted]9.124.156.[redacted].net.      |
| 2017-08-06 | 141.253.221.27 | cs2devipf.xi.company.com. | ntp  | udp |       2736 |   1748 | [redacted]45.144.16 | Italy      | Milan   | AS88[redacted]             | [redacted]aro.bilink.[redacted]          |
| 2017-08-06 | 141.253.221.27 | cs2devipf.xi.company.com. | http | tcp |       1834 |   1097 | [redacted]9.126.96  | Ukraine    | OTHER   | AS28[redacted] Ltd.        | [redacted]9.126.96.m[redacted]net.       |
| 2017-08-06 | 141.253.221.27 | cs2devipf.xi.company.com. | ftp  | tcp |       1283 |   1201 | [redacted]203.40.52 | Canada     | Toronto | AS39[redacted] Inc.        | [redacted]er01-dev-[redacted]ath.ca.     |
| 2017-08-06 | 141.253.221.27 | cs2devipf.xi.company.com. | ftp  | tcp |       1069 |   1645 | [redacted]74.95.106 | Seychelles | OTHER   | AS29[redacted]LTD.         | [redacted]ery.census.[redacted]io.       |
| 2017-08-06 | 141.253.221.27 | cs2devipf.xi.company.com. | http | tcp |        815 |   1999 | [redacted]9.123.40  | Ukraine    | OTHER   | AS28[redacted] Ltd.        | [redacted]9.123.40.m[redacted].net.      |
| 2017-08-06 | 141.253.221.27 | cs2devipf.xi.company.com. | http | tcp |        786 |   1413 | [redacted]9.122.29  | Ukraine    | OTHER   | AS28[redacted] Ltd.        | [redacted]9.122.29.m[redacted].net.      |
+------------+----------------+---------------------------+------+-----+------------+--------+---------------------+------------+---------+----------------------------+------------------------------------------+
10 rows in set (0.00 sec)
```

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

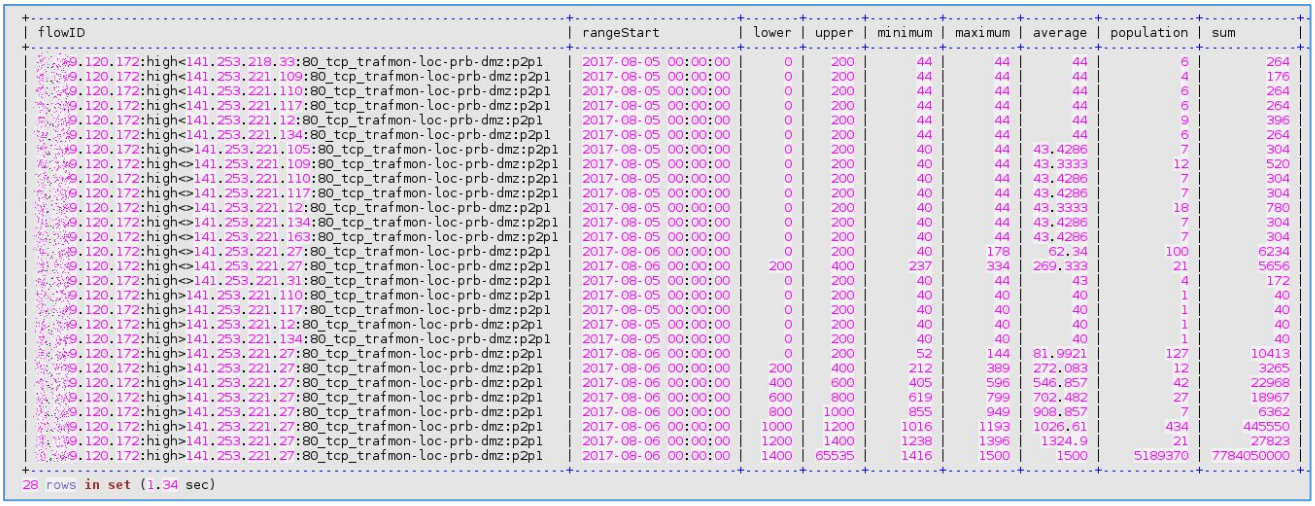
```
`trafMon_SecurityProcs`.`Top_IngressTo`(_DBname, _Date, _Local, _topN)
```

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 only during the two consecutive days: 5 and 6 Aug, 2017!



```
SELECT * FROM ipsztable_aggr_1d WHERE flowid like '%[redacted]9.120.172:%';
```



```
+--------------------------------------------------------------------+---------------------+-------+-------+---------+---------+----------+------------+------------+-
| flowID                                                             | rangeStart          | lower | upper | minimum | maximum | average  | population | sum        |
+--------------------------------------------------------------------+---------------------+-------+-------+---------+---------+----------+------------+------------+-
| [redacted]9.120.172:high<141.253.218.33:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-05 00:00:00 |     0 |   200 |      44 |      44 |       44 |          6 |        264 |
| [redacted]9.120.172:high<141.253.221.109:80_tcp_trafmon-loc-prb-dmz:p2p1   | 2017-08-05 00:00:00 |     0 |   200 |      44 |      44 |       44 |          4 |        176 |
| [redacted]9.120.172:high<141.253.221.110:80_tcp_trafmon-loc-prb-dmz:p2p1   | 2017-08-05 00:00:00 |     0 |   200 |      44 |      44 |       44 |          6 |        264 |
| [redacted]9.120.172:high<141.253.221.117:80_tcp_trafmon-loc-prb-dmz:p2p1   | 2017-08-05 00:00:00 |     0 |   200 |      44 |      44 |       44 |          6 |        264 |
| [redacted]9.120.172:high<141.253.221.12:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-05 00:00:00 |     0 |   200 |      44 |      44 |       44 |          9 |        396 |
| [redacted]9.120.172:high<141.253.221.134:80_tcp_trafmon-loc-prb-dmz:p2p1   | 2017-08-05 00:00:00 |     0 |   200 |      44 |      44 |       44 |          6 |        264 |
| [redacted]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 |
| [redacted]9.120.172: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 |
| [redacted]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 |
| [redacted]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 |
| [redacted]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 |
| [redacted]9.120.172: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 |
| [redacted]9.120.172:high<>141.253.221.163:80_tcp_trafmon-loc-prb-dmz:p2p1  | 2017-08-05 00:00:00 |     0 |   200 |      40 |      44 |  43.4286 |          7 |        304 |
| [redacted]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 |
| [redacted]9.120.172:high<>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1   | 2017-08-06 00:00:00 |   200 |   400 |     237 |     334 |  269.333 |         21 |       5656 |
| [redacted]9.120.172:high<>141.253.221.31:80_tcp_trafmon-loc-prb-dmz:p2p1   | 2017-08-05 00:00:00 |     0 |   200 |      40 |      44 |       43 |          4 |        172 |
| [redacted]9.120.172:high>141.253.221.110:80_tcp_trafmon-loc-prb-dmz:p2p1   | 2017-08-05 00:00:00 |     0 |   200 |      40 |      40 |       40 |          1 |         40 |
| [redacted]9.120.172:high>141.253.221.117:80_tcp_trafmon-loc-prb-dmz:p2p1   | 2017-08-05 00:00:00 |     0 |   200 |      40 |      40 |       40 |          1 |         40 |
| [redacted]9.120.172:high>141.253.221.12:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-05 00:00:00 |     0 |   200 |      40 |      40 |       40 |          1 |         40 |
| [redacted]9.120.172:high>141.253.221.134:80_tcp_trafmon-loc-prb-dmz:p2p1   | 2017-08-05 00:00:00 |     0 |   200 |      40 |      40 |       40 |          1 |         40 |
| [redacted]9.120.172:high>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-06 00:00:00 |     0 |   200 |      52 |     144 |  81.9921 |        127 |      10413 |
| [redacted]9.120.172:high>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-06 00:00:00 |   200 |   400 |     212 |     389 |  272.083 |         12 |       3265 |
| [redacted]9.120.172:high>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-06 00:00:00 |   400 |   600 |     405 |     596 |  546.857 |         42 |      22968 |
| [redacted]9.120.172:high>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-06 00:00:00 |   600 |   800 |     619 |     799 |  702.482 |         27 |      18967 |
| [redacted]9.120.172:high>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-06 00:00:00 |   800 |  1000 |     855 |     949 |  908.857 |          7 |       6362 |
| [redacted]9.120.172:high>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-06 00:00:00 |  1000 |  1200 |    1016 |    1193 |  1026.61 |        434 |     445550 |
| [redacted]9.120.172:high>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-06 00:00:00 |  1200 |  1400 |    1238 |    1396 |   1324.9 |         21 |      27823 |
| [redacted]9.120.172:high>141.253.221.27:80_tcp_trafmon-loc-prb-dmz:p2p1    | 2017-08-06 00:00:00 |  1400 | 65535 |    1416 |    1500 |     1500 |    5189370 | 7784050000 |
+--------------------------------------------------------------------+---------------------+-------+-------+---------+---------+----------+------------+------------+-
28 rows in set (1.34 sec)
```

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))
```

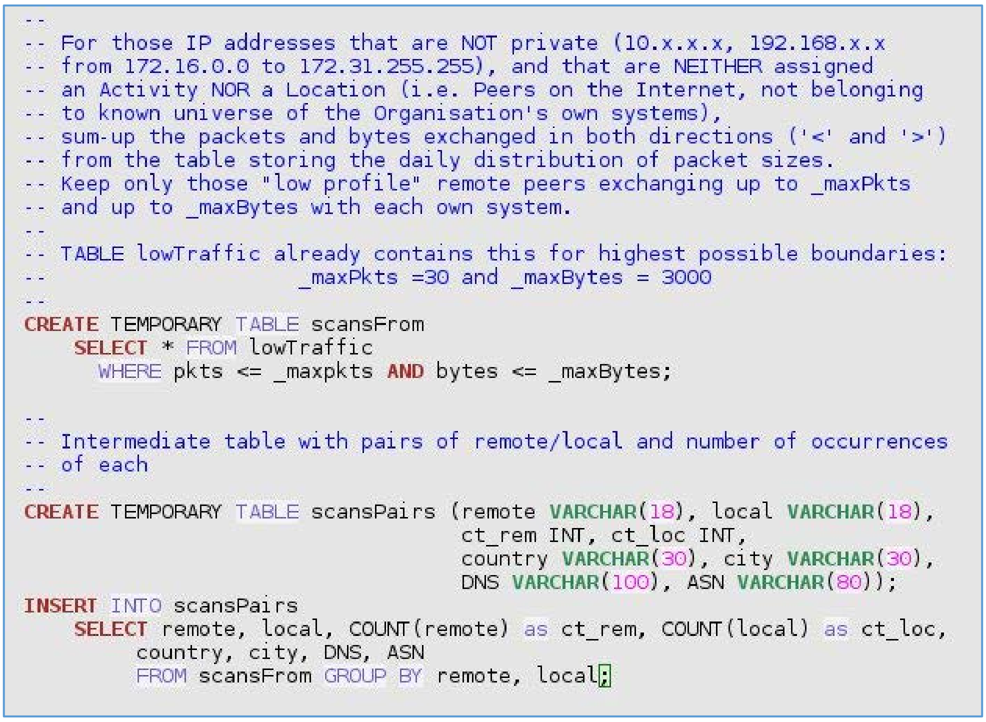
see above

```
`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:

`` `trafMon_SecurityProcs`.`Prepare_for_securityScanners`(_DBname, _maxPkts, _maxBytes) ``

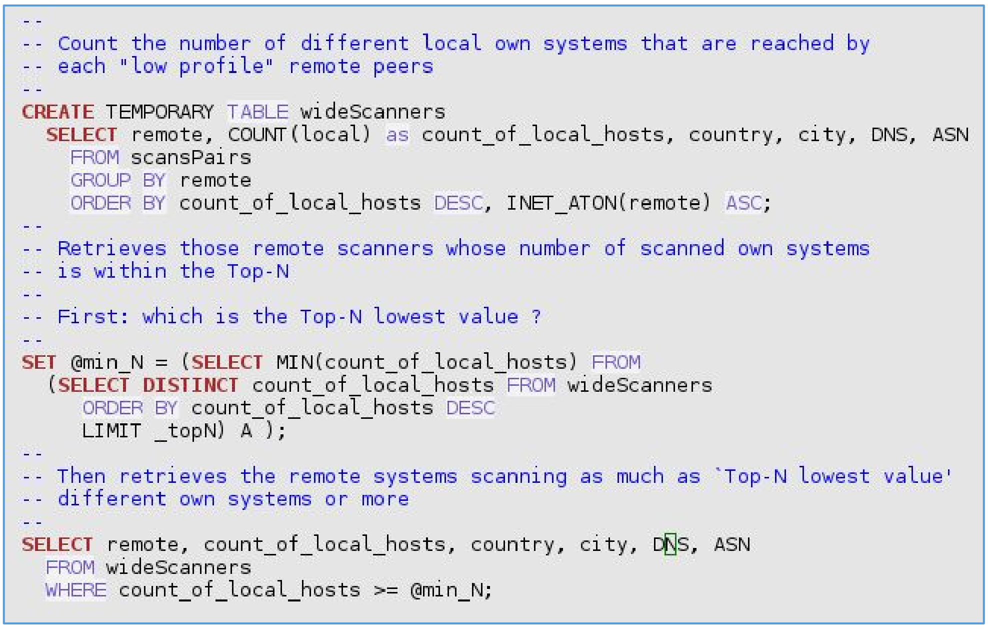


```
--
-- For those IP addresses that are NOT private (10.x.x.x, 192.168.x.x
-- from 172.16.0.0 to 172.31.255.255), and that are NEITHER assigned
-- an Activity NOR a Location (i.e. Peers on the Internet, not belonging
-- to known universe of the Organisation's own systems),
-- sum-up the packets and 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;
```

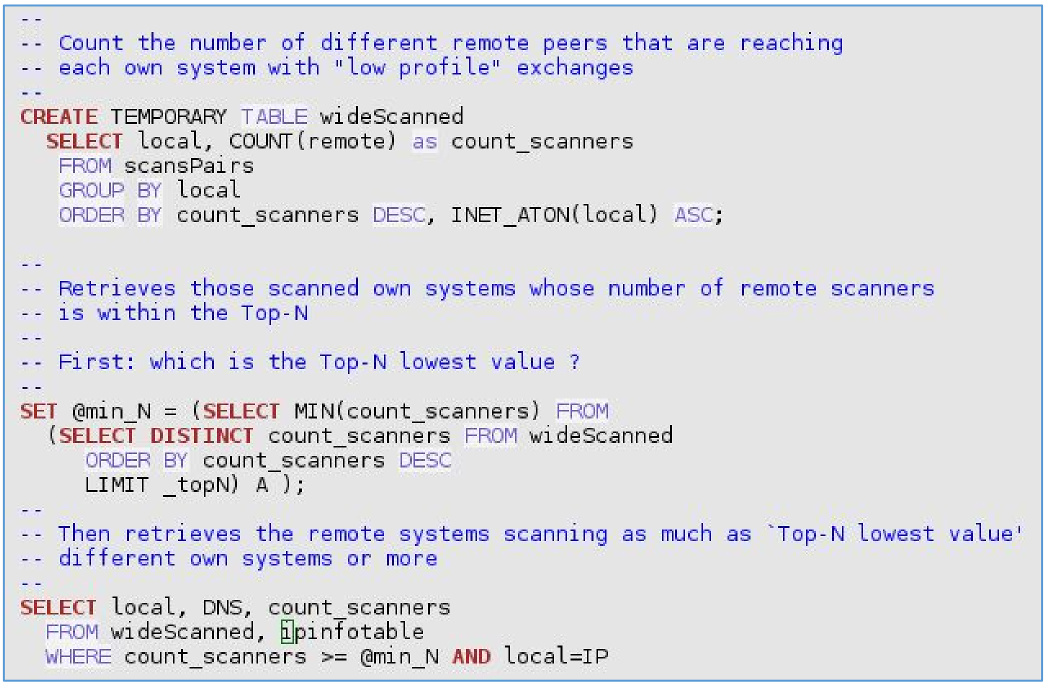
This scanners analysis is implemented by the three procedures:

`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;
```

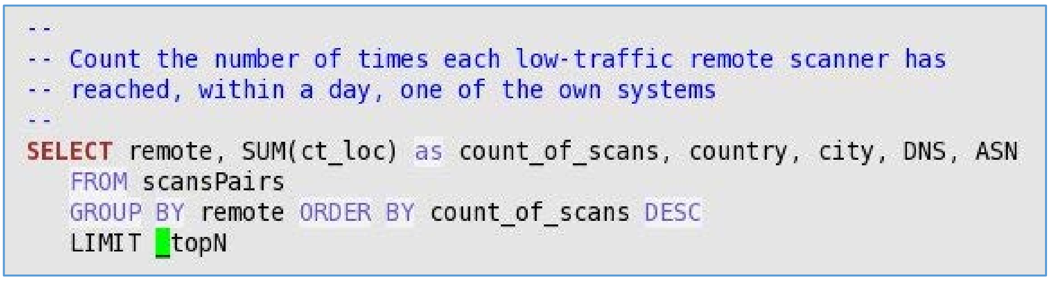
`trafMon_SecurityProcs`.`Top_Scanned`(_DBname, _maxPkts, _maxBytes, _topN)



```
--
-- 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
```

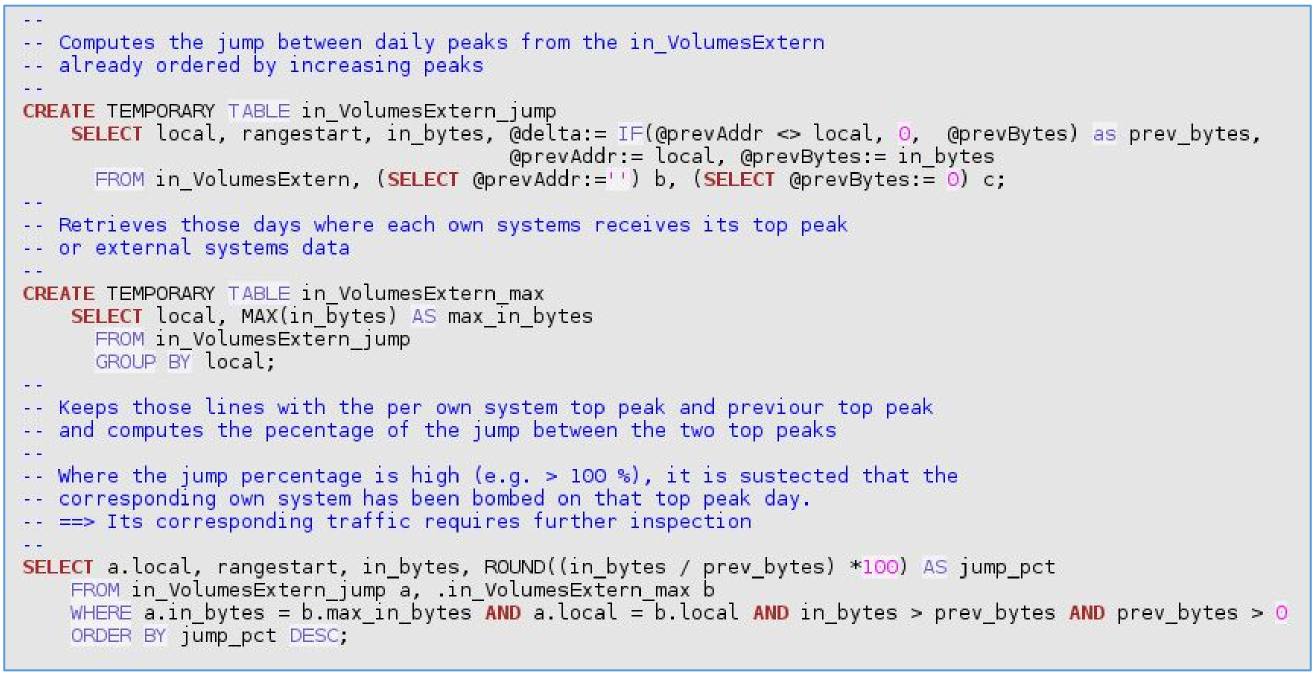
`trafMon_SecurityProcs`.`Top_ActiveScanners`(_DBname, _maxPkts, _maxBytes, _topN)



```
--
-- 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:

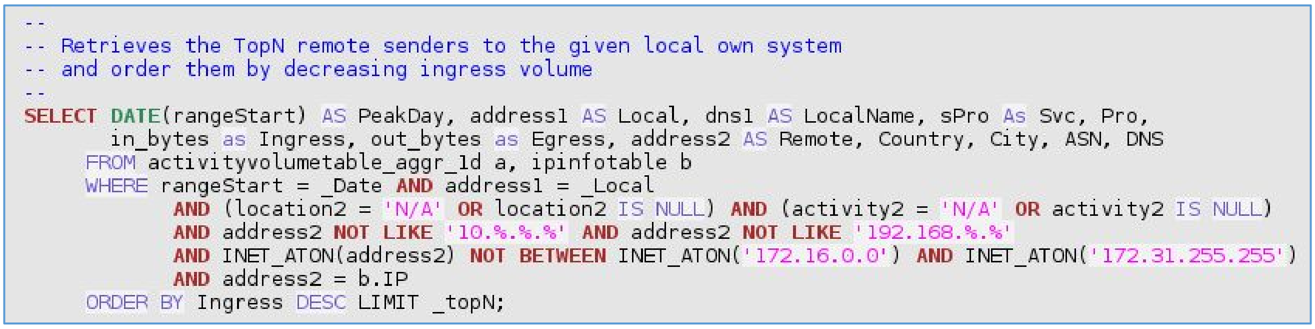
`trafMon_SecurityProcs`.`TopJumps_DailyPeak`(_DBname, _maxPkts, _maxBytes, _topN)



```
--
-- 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
--
-- 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
--
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
     ORDER BY Ingress DESC LIMIT _topN;
```

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 practical example on how to create your own BIRT report template based on trafMon collected observations.

5.1 BIRT DESIGNER SETUP

- Download and install the BIRT Designer: 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 new report called “***SecuritySynthesis***.rptdesign”
- In the *Resource Explorer*, drag the Shared Resources/Library/trafMonDb.rptlibrary/Data Sources/**trafmonDb** to the *Data Explorer* Data Sources. This defines the connection to the database
- In the *Resource Explorer*, drag the Shared Resources/Library/trafMonDb.rptlibrary/Report Parameters/**DBname** 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+”)”

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:

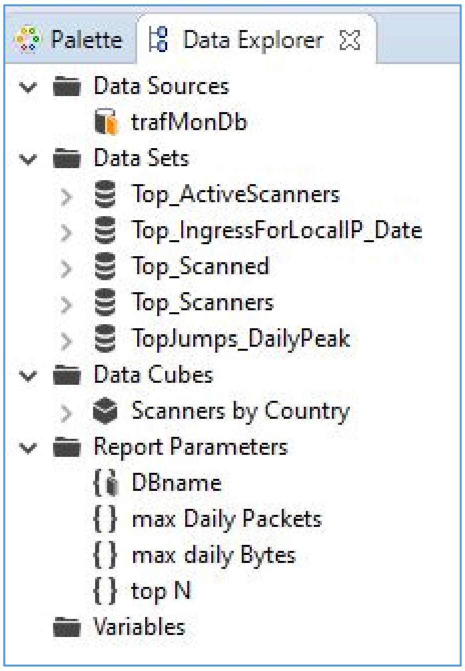
  “CALL `trafMon_SecurityProcs`.`TopJumps_DailyPeak`(‘” +params[“DBname”].value+”)”

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

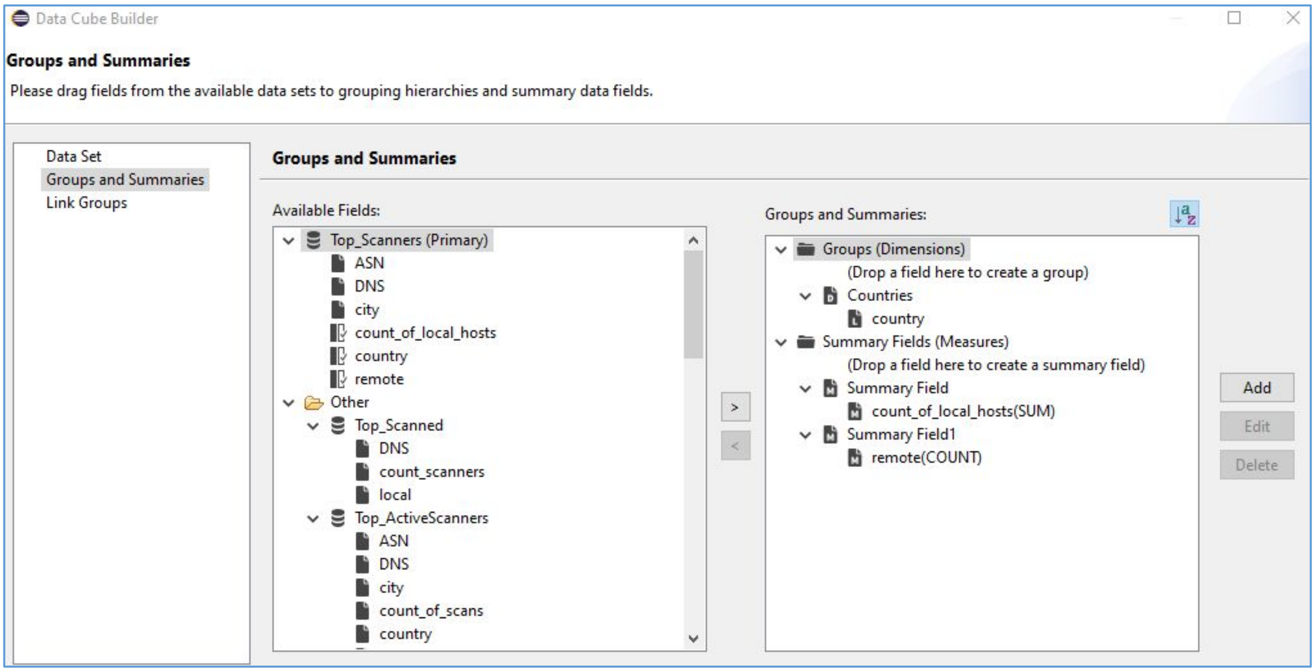
- Query: **CALL trafMon_SecurityProcs.Top_IngressTo(?, ?, ?, ?)**
- Parameters:
  - **db**, String, Linked to Report Parameter *DBname*
  - **peakDate**, String, Default Value *2017-07-12 00:00:00*
  - **peakLocalIP**, String, Default Value *141.253.12.3*
  - **topN** , Integer, Linked to Report Parameter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



- Data Sources
  - trafMonDb
- Data Sets
  - Top_ActiveScanners
  - Top_IngressForLocalIP_Date
  - Top_Scanned
  - Top_Scanners
  - TopJumps_DailyPeak
- Data Cubes
  - Scanners by Country
- Report Parameters
  - DBname
  - max Daily Packets
  - max daily Bytes
  - top N
- Variables



Groups and Summaries

Please drag fields from the available data sets to grouping hierarchies and summary data fields.

Groups and Summaries

Available Fields:

- Top_Scanners (Primary)
  - ASN
  - DNS
  - city
  - count_of_local_hosts
  - country
  - remote
- Other
  - Top_Scanned
    - DNS
    - count_scanners
    - local
  - Top_ActiveScanners
    - ASN
    - DNS
    - city
    - count_of_scans
    - country

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 Field1
    - remote(COUNT)

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.

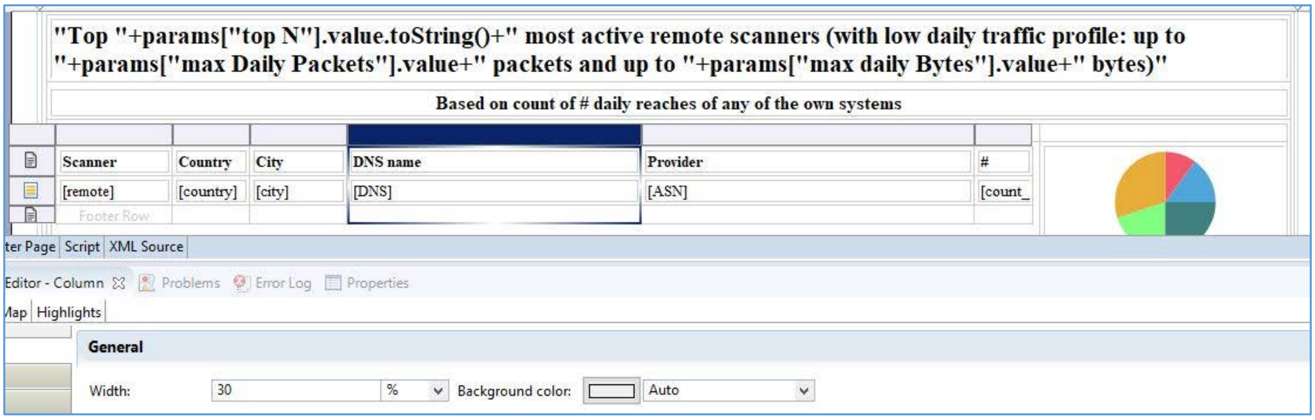
The Best is always to dimension everything as explicit percentage. And this must be exhaustive: do not leave the width of the last column empty (supposing it will occupy the rest of the percentage); but assign its percentage width explicitly, in such a way to correctly reach 100% by summing all elements 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), drag the Data Set **Top_ActiveScanners**. Reorder the columns, adapt their labels. Assign percentage width (12, 8, 10, 30, 34, 6)



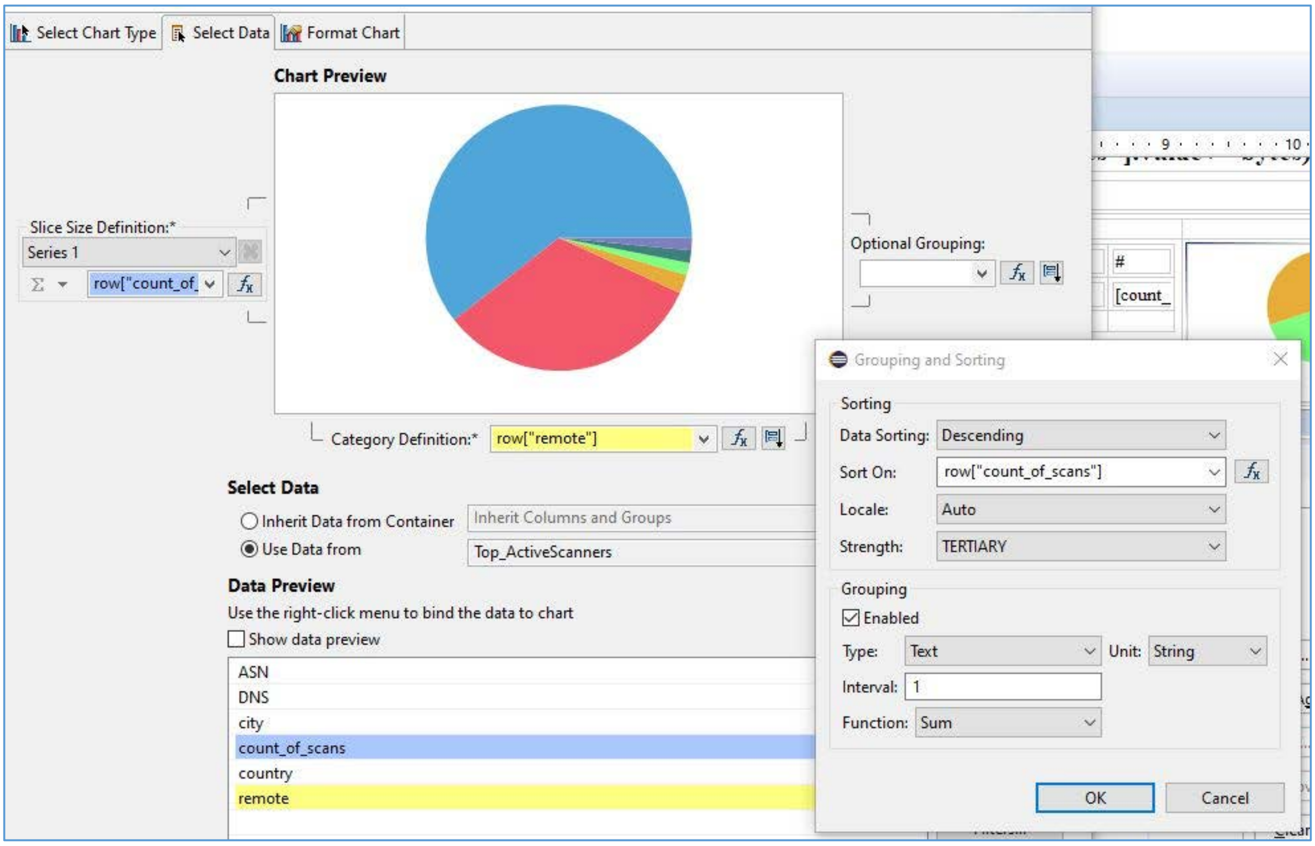
"Top "+params["top N"].value.toString()+" most active remote scanners (with low daily traffic profile: up to "+params["max Daily Packets"].value+" packets and up to "+params["max daily Bytes"].value+" bytes)"

Based on count of # daily reaches of any of the own systems

Scanner	Country	City	DNS name	Provider	#
[remote]	[country]	[city]	[DNS]	[ASN]	[count_
Footer Row					

Width: 30 % Background color: Auto

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



Slice Size Definition:* Series 1

Σ row["count_of_

Category Definition:* row["remote"]

○ Inherit Data from Container: Inherit Columns and Groups

● Use Data from: Top_ActiveScanners

□ Show data preview

ASN
DNS
city
count_of_scans
country
remote

Data Sorting: Descending

Sort On: row["count_of_scans"]

Locale: Auto

Strength: TERTIARY

☑ Enabled

Type: Text Unit: String

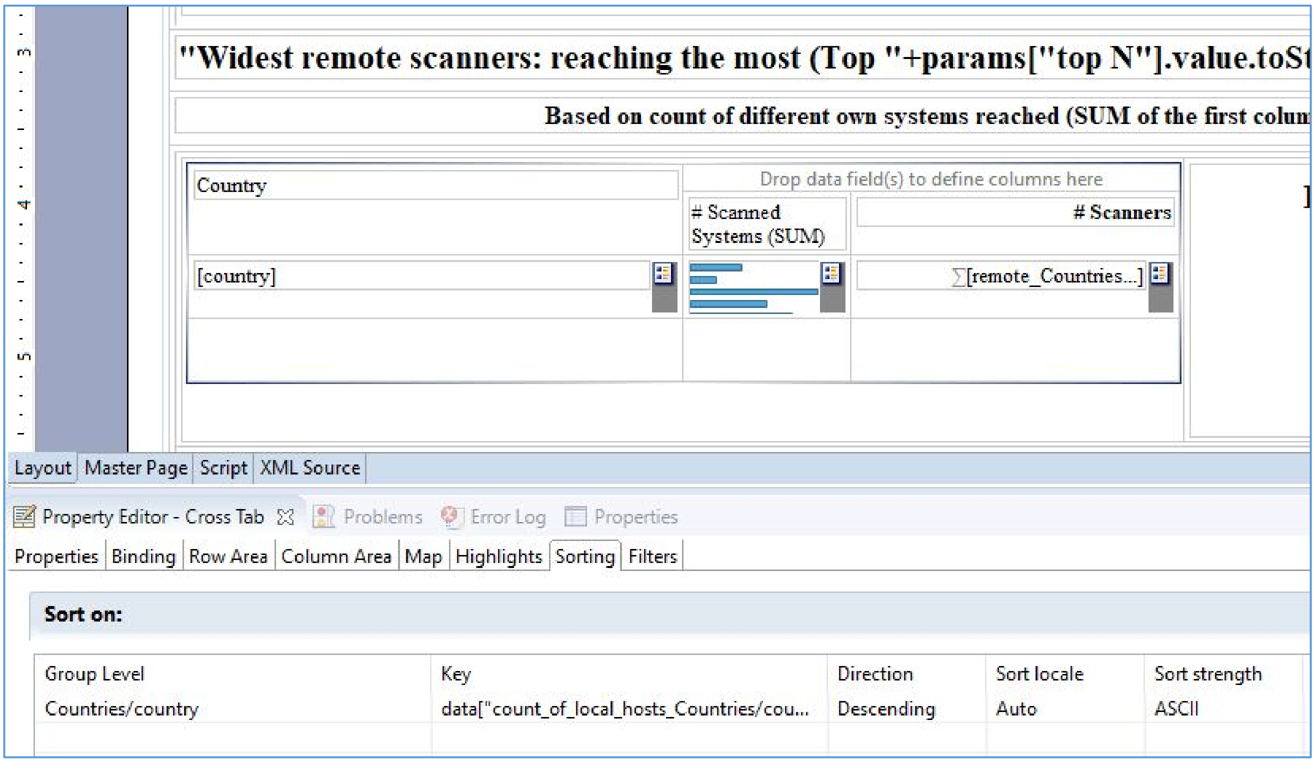
Interval: 1

Function: Sum

- 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%), drag the Data Cube ***Scanners by Country***. Rename and re-style the columns labels (*Country, #Scanned Systems (SUM), # Scanners*). Select the Chart option for the 2nd column. Delete the Footer of this 2nd column. Select the entire Cross Tab and, in the below Property Editor, used the Sorting tab to add a Descending sort for **data[“count_of_local_hosts_Countries/country”]**.



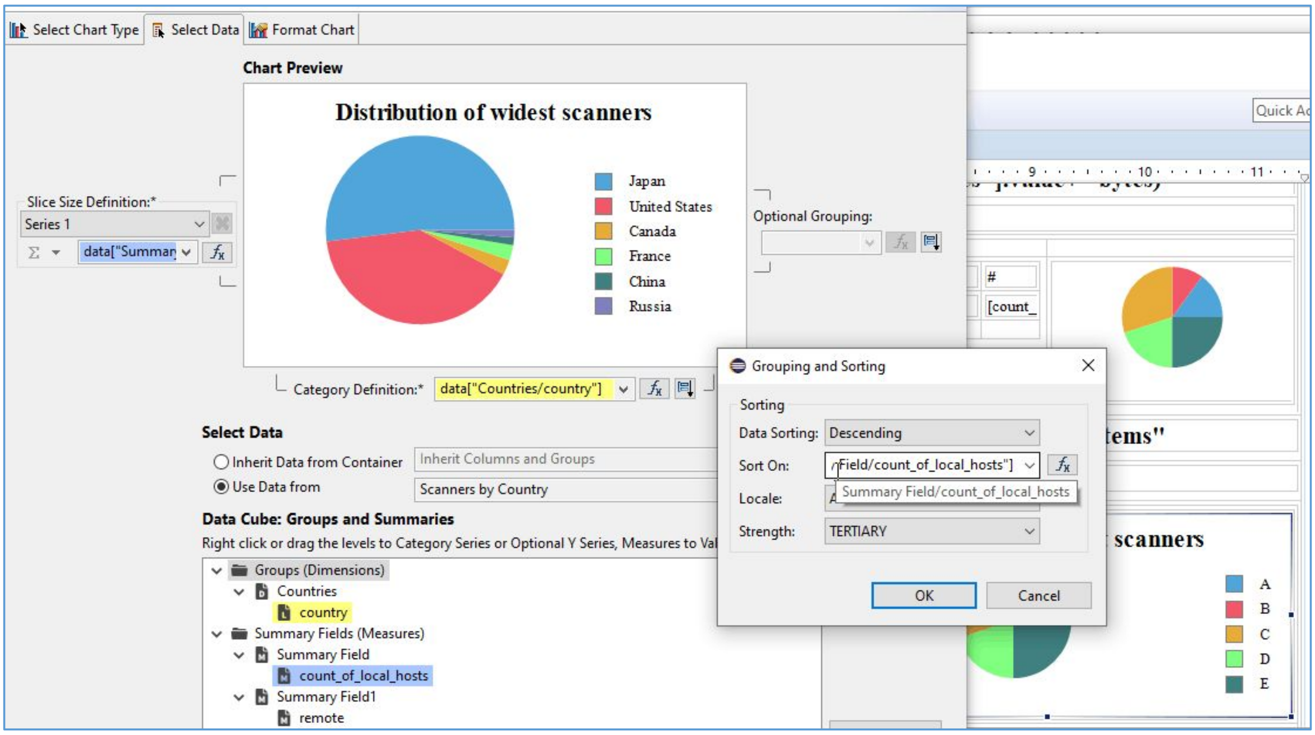
"Widest remote scanners: reaching the most (Top "+params["top N"].value.toSt

Based on count of different own systems reached (SUM of the first colun

Sort on:

Group Level	Key	Direction	Sort locale	Sort strength
Countries/country	data["count_of_local_hosts_Countries/cou...	Descending	Auto	ASCII

    - In the 2nd column (40%), create a pie chart with *Use Data From **Scanners by Country***. Drag the field **count_of_local_hosts** to the Slice Size definitions / Series 1. Drag the field **country** to the Category Definition and define a Descending Sorting on count_of_local_hosts. Then, in Format Chart tab, specify a Title, let the Legend be visible and, in Series, remove the Title of Value Series.



Slice Size Definition:* Series 1
Σ data["Summar

Category Definition:* data["Countries/country"]

Select Data

○ Inherit Data from Container — Inherit Columns and Groups

● Use Data from — Scanners by Country

Data Cube: Groups and Summaries

Right click or drag the levels to Category Series or Optional Y Series, Measures to Val

```
Groups (Dimensions)
  Countries
    country
Summary Fields (Measures)
  Summary Field
    count_of_local_hosts
  Summary Field1
    remote
```

Grouping and Sorting

Sorting

Data Sorting: Descending

Sort On: Field/count_of_local_hosts"]

Summary Field/count_of_local_hosts

Locale: A

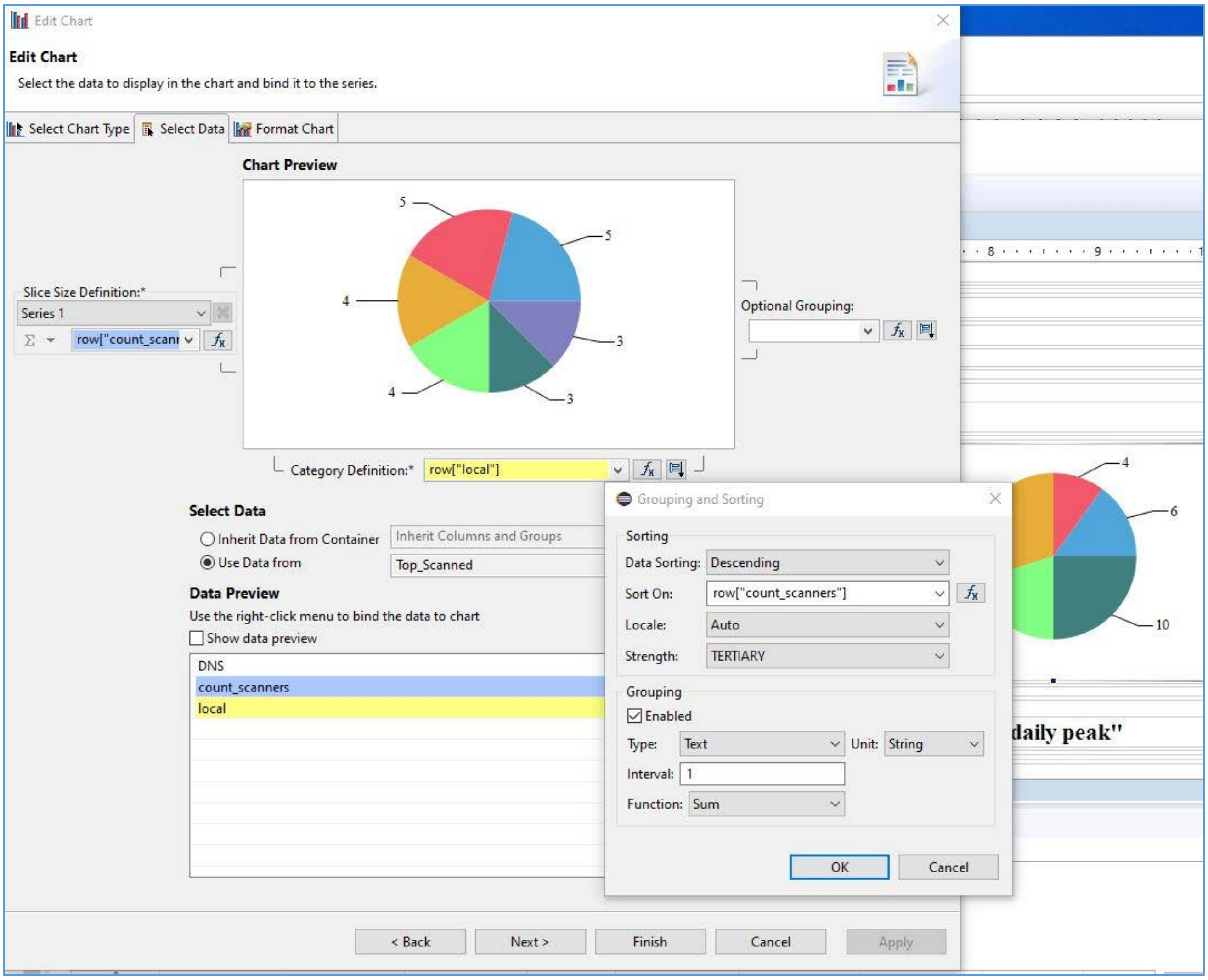
Strength: TERTIARY

OK — Cancel

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

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

    - o In the bottom row cell, create a **Grid with 2 columns and 1 row**
      - ▪ In the left cell (50%), drag the Data Set **Top_Scanned**, adjust the column widths (28, 50 and 22 %). Re-label and re-style the headings (*Own Systems, DNS name, # remote scanners*).
      - ▪ In the right cell (50%), create a pie chart 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 Sorting Descending on **row["count_scanners"]**. In *Format Chart* tab, suppress visibility of *Title* and of *Legend*; in *Series*, remove the Title for Value Series, Select Value Series and activate the check box *Show Series Label*.



Edit Chart

Select the data to display in the chart and bind it to the series.

Slice Size Definition:* Series 1

Σ row["count_scann

Optional Grouping:

Category Definition:* row["local"]

Select Data

○ Inherit Data from Container Inherit Columns and Groups

● Use Data from Top_Scanned

Data Preview

Use the right-click menu to bind the data to chart

□ Show data preview

DNS

count_scanners

local

Grouping and Sorting

Sorting

Data Sorting: Descending

Sort On: row["count_scanners"]

Locale: Auto

Strength: TERTIARY

Grouping

☑ Enabled

Type: Text Unit: String

Interval: 1

Function: Sum

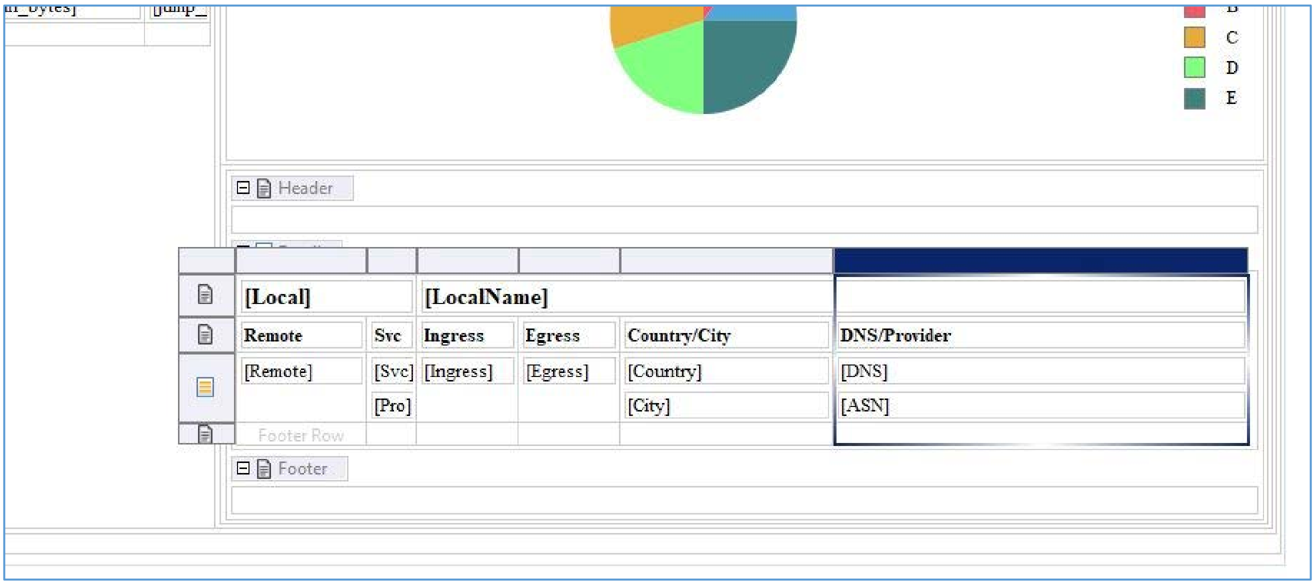
- In the 6th row cell, create a **Grid with 1 column and 2 rows**
  - In the top row, create a Grid with 2 column and 1 row
    - In the top row cell, create a **Dynamic Text** (Bold 16):

```
"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%), drag the Data Set **TopJumps_DailyPeak**, adjust the column widths (30, 20, 35 and 15 %). Re-label and re-style the headings (*Own System, Day, Ingress Bytes, Peak jump (%)*).

- In the right cell (60%), create a **Grid with 1 column and 2 rows**
  - In the top row cell, create a pie chart 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 Sorting Descending on **row["jump_pct"]**. In *Format Chart* tab, suppress visibility of *Title* but keep visibility of *Legend*; in *Series*, remove the Title for Value Series.
  - In the bottom row, create a List for Data Set **TopJumps_DailyPeak**. Keep the fields **local, rangestart** (the day of the top peak) and **jump_pct**. In the below *Property Editor*, in *Sorting* tab, sort Descending on **row["jump_pct"]**. In the below *Property Editor*, in *Filters* tab, Expression **row["jump_pct"]** Operator **Top n**, Value 1 **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 Detail, drag 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"]**
    - *topN* is **params["top N"].value**
  - Then re-organise the table:
    - Select the *Heading* row and insert one row above.
    - Move **[Local]** in *first heading row, first column*, and delete **Local** label.
    - Move **[LocalName]** in *first heading row, third column*, and delete **LocalName** label.
    - Move **[Remote]** and **Remote** label *to first column*.
    - Move **[Svc]** and **Svc** label *to second column*.
    - Move **[Pro]** on top of **[Svc]** (*at right side*): it goes to a new row, below the target; and delete **Pro** label.
    - Move **[Ingress]** and **Ingress** label *to third column* (*below* **[LocalName]**).
    - Move **[City]** *below* **[Country]**.

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



[Local]		[LocalName]			
Remote	Svc	Ingress	Egress	Country/City	DNS/Provider
[Remote]	[Svc]	[Ingress]	[Egress]	[Country]	[DNS]
	[Pro]			[City]	[ASN]

5.4 INSTALLING AND EXECUTING THE NEW REPORT

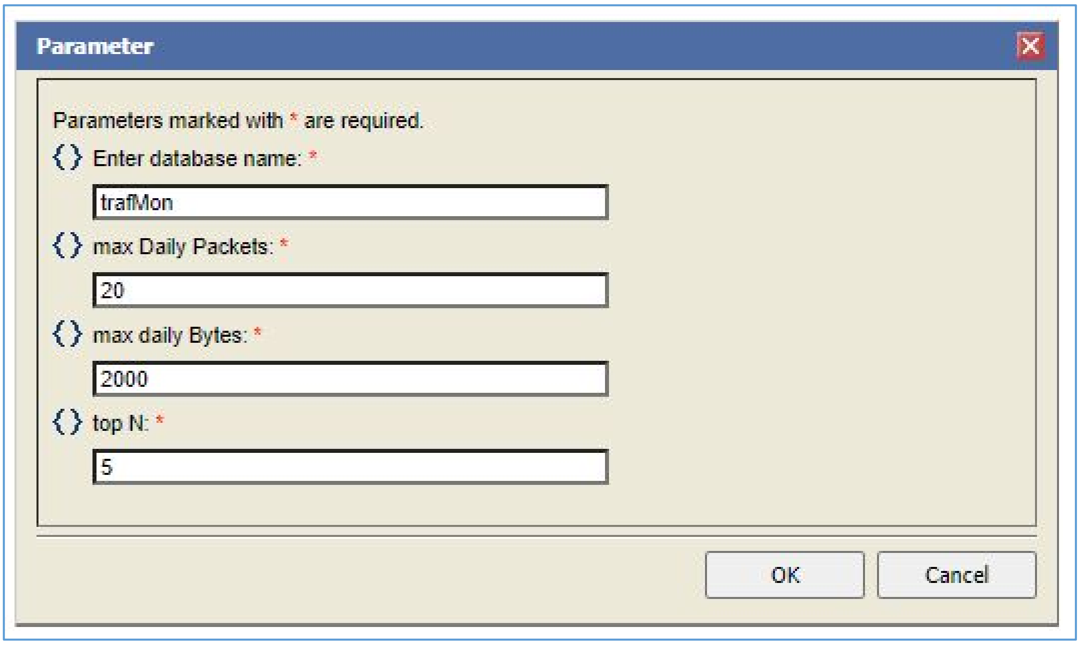
You can now copy your *SecuritySynthesis.rptdesign* report template to /var/lib/tomcat/webapps/birt/trafMon_reports/

```
# chown tomcat
      /var/lib/tomcat/webapps/birt/trafMon_reports/SecuritySynthesis.rptdesign
```

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



Parameters marked with * are required.

{ } Enter database name: *

trafMon

{ } max Daily Packets: *

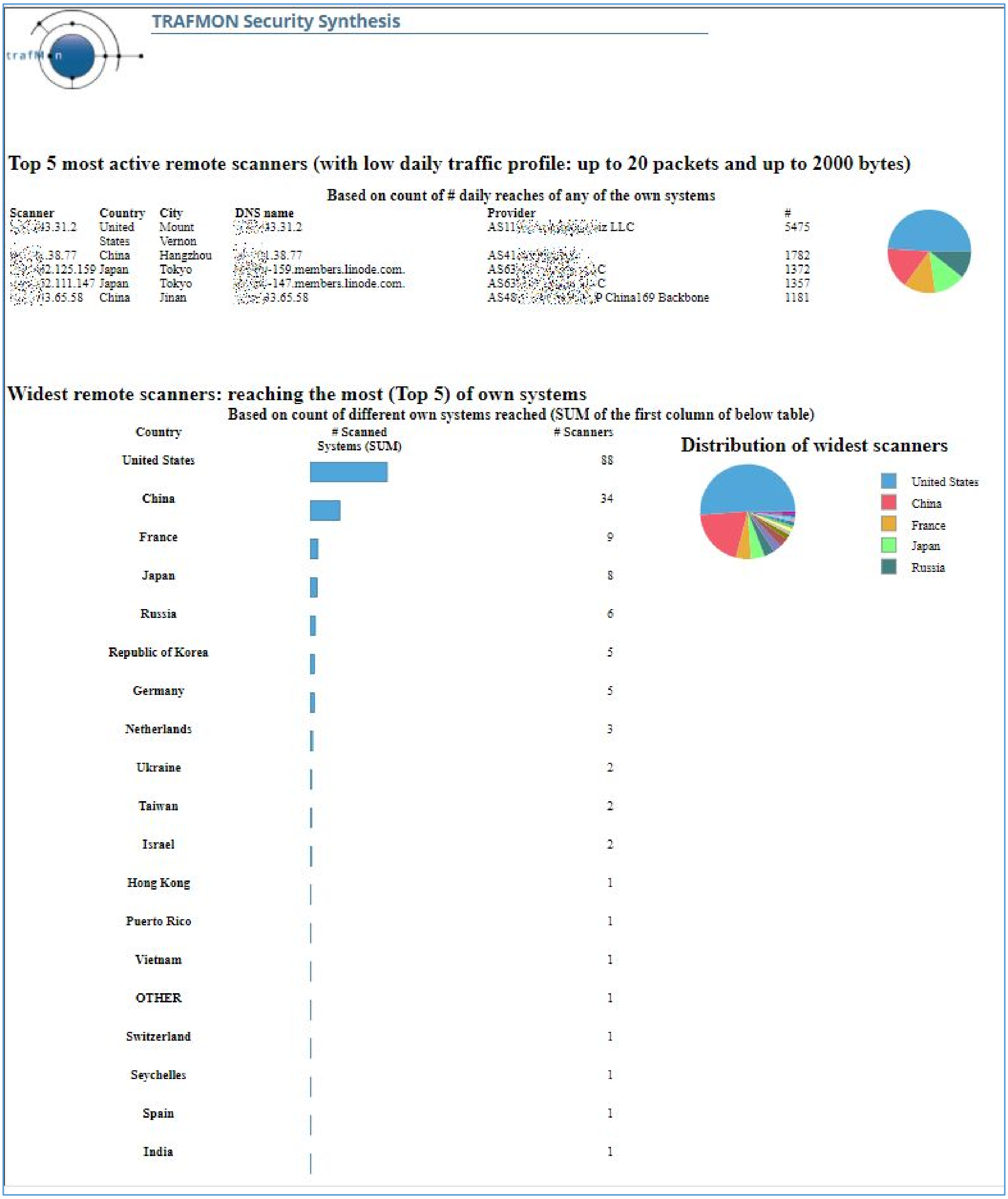
20

{ } max daily Bytes: *

2000

{ } top N: *

5



TRAFMON Security Synthesis

Top 5 most active remote scanners (with low daily traffic profile: up to 20 packets and up to 2000 bytes)

Based on count of # daily reaches of any of the own systems

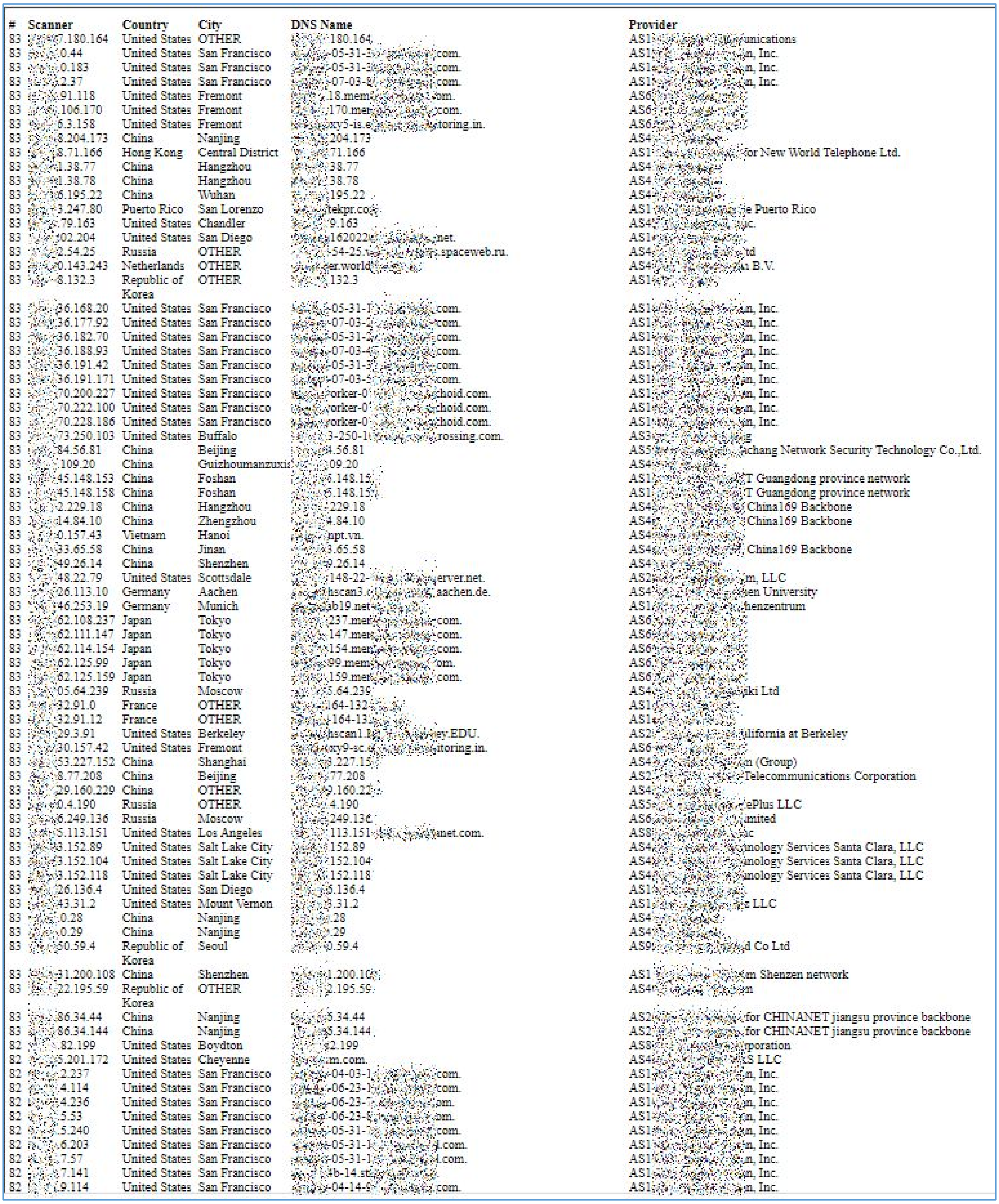
Scanner	Country	City	DNS name	Provider	#
[redacted]43.31.2	United States	Mount Vernon	[redacted]43.31.2	AS11[redacted]iz LLC	5475
[redacted].38.77	China	Hangzhou	[redacted]1.38.77	AS41[redacted]	1782
[redacted]62.125.159	Japan	Tokyo	[redacted]-159.members.linode.com.	AS63[redacted]C	1372
[redacted]32.111.147	Japan	Tokyo	[redacted]-147.members.linode.com.	AS63[redacted]C	1357
[redacted]13.65.58	China	Jinan	[redacted]43.65.58	AS48[redacted]P China169 Backbone	1181

Widest remote scanners: reaching the most (Top 5) of own systems

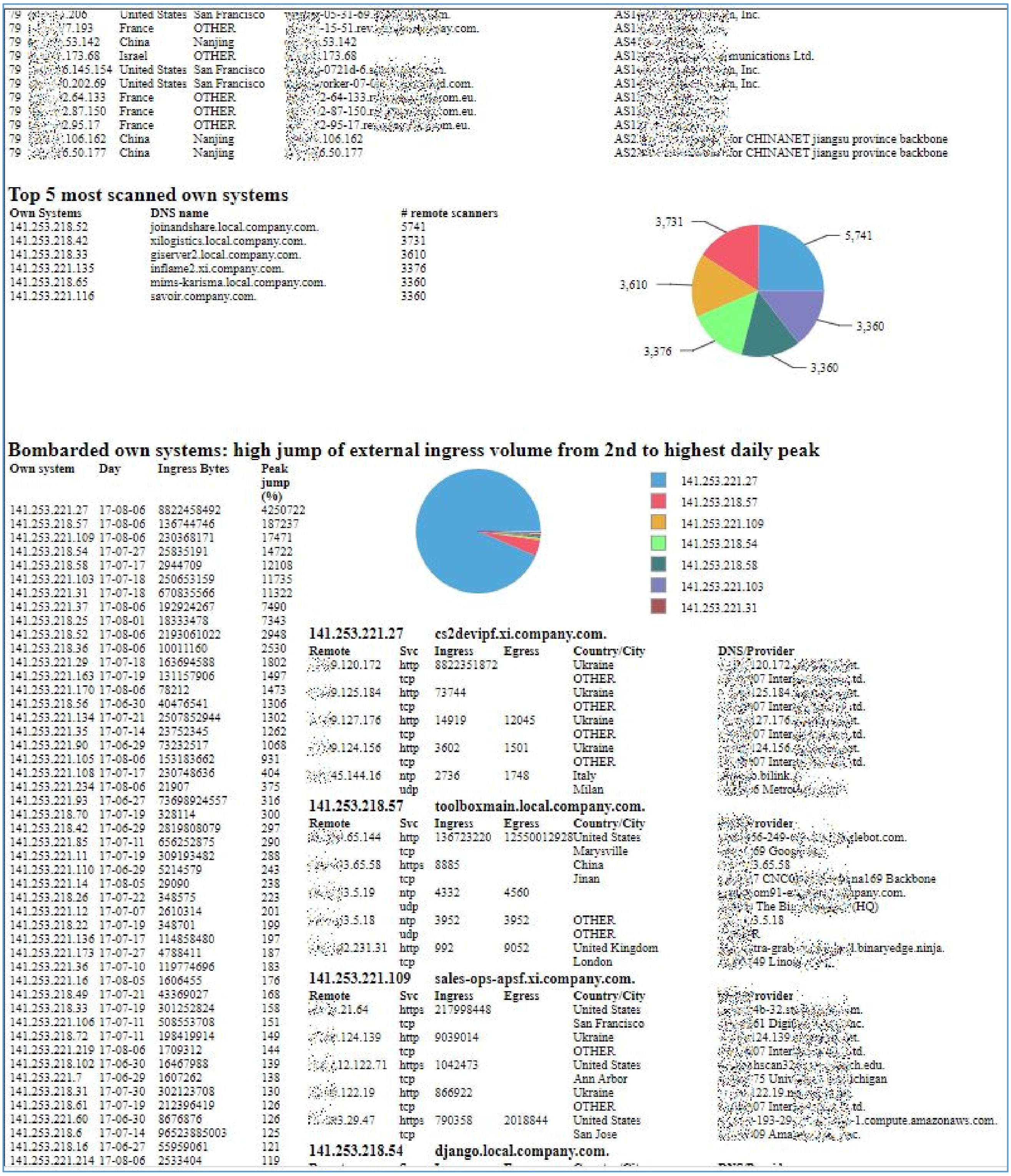
Based on count of different own systems reached (SUM of the first column of below table)

Country	# Scanned Systems (SUM)	# Scanners
United States		88
China		34
France		9
Japan		8
Russia		6
Republic of Korea		5
Germany		5
Netherlands		3
Ukraine		2
Taiwan		2
Israel		2
Hong Kong		1
Puerto Rico		1
Vietnam		1
OTHER		1
Switzerland		1
Seychelles		1
Spain		1
India		1

Distribution of widest scanners



#	Scanner	Country	City	DNS Name	Provider
83	[redacted]7.180.164	United States	OTHER	[redacted]180.164.[redacted]	AS1[redacted]unications
83	[redacted]0.44	United States	San Francisco	[redacted]-05-31-3[redacted]com.	AS1[redacted]n, Inc.
83	[redacted]0.183	United States	San Francisco	[redacted]-05-31-3[redacted]com.	AS1[redacted]n, Inc.
83	[redacted]2.37	United States	San Francisco	[redacted]-07-03-8[redacted]com.	AS1[redacted]n, Inc.
83	[redacted]91.118	United States	Fremont	[redacted]18.mem[redacted]om.	AS6[redacted]
83	[redacted]106.170	United States	Fremont	[redacted]170.me[redacted]com.	AS6[redacted]
83	[redacted]6.3.158	United States	Fremont	[redacted]xy5-is.e[redacted]toring.in.	AS6[redacted]
83	[redacted]8.204.173	China	Nanjing	[redacted]204.173	AS4[redacted]
83	[redacted]8.71.166	Hong Kong	Central District	[redacted]71.166	AS1[redacted]or New World Telephone Ltd.
83	[redacted]1.38.77	China	Hangzhou	[redacted]38.77	AS4[redacted]
83	[redacted]1.38.78	China	Hangzhou	[redacted]38.78	AS4[redacted]
83	[redacted]6.195.22	China	Wuhan	[redacted]195.22	AS4[redacted]
83	[redacted]3.247.80	Puerto Rico	San Lorenzo	[redacted]tekpr.co[redacted]	AS1[redacted]e Puerto Rico
83	[redacted]79.163	United States	Chandler	[redacted]9.163	AS4[redacted]nc.
83	[redacted]02.204	United States	San Diego	[redacted]162022[redacted]net.	AS1[redacted]
83	[redacted]2.54.25	Russia	OTHER	[redacted]-54-25.[redacted].spaceweb.ru.	AS4[redacted]td
83	[redacted]0.143.243	Netherlands	OTHER	[redacted]er.world[redacted]	AS4[redacted] B.V.
83	[redacted]8.132.3	Republic of Korea	OTHER	[redacted]132.3	AS1[redacted]
83	[redacted]36.168.20	United States	San Francisco	[redacted]-05-31-1[redacted]com.	AS1[redacted]n, Inc.
83	[redacted]36.177.92	United States	San Francisco	[redacted]-07-03-2[redacted]com.	AS1[redacted]n, Inc.
83	[redacted]36.182.70	United States	San Francisco	[redacted]-05-31-2[redacted]com.	AS1[redacted]n, Inc.
83	[redacted]36.188.93	United States	San Francisco	[redacted]-07-03-4[redacted]com.	AS1[redacted]n, Inc.
83	[redacted]36.191.42	United States	San Francisco	[redacted]-05-31-3[redacted]com.	AS1[redacted]n, Inc.
83	[redacted]36.191.171	United States	San Francisco	[redacted]-07-03-5[redacted]com.	AS1[redacted]n, Inc.
83	[redacted]70.200.227	United States	San Francisco	[redacted]orker-0[redacted]choid.com.	AS1[redacted]n, Inc.
83	[redacted]70.222.100	United States	San Francisco	[redacted]orker-0[redacted]choid.com.	AS1[redacted]n, Inc.
83	[redacted]70.228.186	United States	San Francisco	[redacted]orker-0[redacted]choid.com.	AS1[redacted]n, Inc.
83	[redacted]73.250.103	United States	Buffalo	[redacted]3-250-1[redacted]rossing.com.	AS3[redacted]g
83	[redacted]84.56.81	China	Beijing	[redacted]4.56.81	AS5[redacted]chang Network Security Technology Co.,Ltd.
83	[redacted]109.20	China	Guizhoumanzuxis	[redacted]09.20	AS4[redacted]
83	[redacted]45.148.153	China	Foshan	[redacted]6.148.15[redacted]	AS1[redacted]T Guangdong province network
83	[redacted]45.148.158	China	Foshan	[redacted]6.148.15[redacted]	AS1[redacted]T Guangdong province network
83	[redacted]2.229.18	China	Hangzhou	[redacted]229.18	AS4[redacted]China169 Backbone
83	[redacted]14.84.10	China	Zhengzhou	[redacted]4.84.10	AS4[redacted]China169 Backbone
83	[redacted]0.157.43	Vietnam	Hanoi	[redacted]npt.vn.	AS4[redacted]
83	[redacted]33.65.58	China	Jinan	[redacted]3.65.58	AS4[redacted], China169 Backbone
83	[redacted]49.26.14	China	Shenzhen	[redacted]9.26.14	AS4[redacted]
83	[redacted]48.22.79	United States	Scottsdale	[redacted]148-22-[redacted]erver.net.	AS2[redacted]m, LLC
83	[redacted]26.113.10	Germany	Aachen	[redacted]hscan3.[redacted]aachen.de.	AS4[redacted]en University
83	[redacted]46.253.19	Germany	Munich	[redacted]ab19.net[redacted]	AS1[redacted]henzentrum
83	[redacted]62.108.237	Japan	Tokyo	[redacted]237.me[redacted]com.	AS6[redacted]
83	[redacted]62.111.147	Japan	Tokyo	[redacted]147.me[redacted]com.	AS6[redacted]
83	[redacted]62.114.154	Japan	Tokyo	[redacted]154.me[redacted]com.	AS6[redacted]
83	[redacted]62.125.99	Japan	Tokyo	[redacted]99.mem[redacted]om.	AS6[redacted]
83	[redacted]62.125.159	Japan	Tokyo	[redacted]159.me[redacted]com.	AS6[redacted]
83	[redacted]05.64.239	Russia	Moscow	[redacted]5.64.239	AS4[redacted]ki Ltd
83	[redacted]32.91.0	France	OTHER	[redacted]164-132[redacted]	AS1[redacted]
83	[redacted]32.91.12	France	OTHER	[redacted]164-13[redacted]	AS1[redacted]
83	[redacted]29.3.91	United States	Berkeley	[redacted]hscan1.[redacted]ey.EDU.	AS2[redacted]lifornia at Berkeley
83	[redacted]30.157.42	United States	Fremont	[redacted]xy9-sc.[redacted]itoring.in.	AS6[redacted]
83	[redacted]53.227.152	China	Shanghai	[redacted]3.227.15[redacted]	AS4[redacted]n (Group)
83	[redacted]8.77.208	China	Beijing	[redacted]77.208	AS2[redacted]Telecommunications Corporation
83	[redacted]29.160.229	China	OTHER	[redacted]9.160.22[redacted]	AS4[redacted]
83	[redacted]0.4.190	Russia	OTHER	[redacted]4.190	AS5[redacted]ePlus LLC
83	[redacted]6.249.136	Russia	Moscow	[redacted]249.136	AS6[redacted]mited
83	[redacted]5.113.151	United States	Los Angeles	[redacted]113.151[redacted]anet.com.	AS8[redacted]c
83	[redacted]3.152.89	United States	Salt Lake City	[redacted]152.89	AS4[redacted]nology Services Santa Clara, LLC
83	[redacted]3.152.104	United States	Salt Lake City	[redacted]152.104	AS4[redacted]nology Services Santa Clara, LLC
83	[redacted]3.152.118	United States	Salt Lake City	[redacted]152.118	AS4[redacted]nology Services Santa Clara, LLC
83	[redacted]26.136.4	United States	San Diego	[redacted]6.136.4	AS1[redacted]
83	[redacted]43.31.2	United States	Mount Vernon	[redacted]3.31.2	AS1[redacted]s LLC
83	[redacted]0.28	China	Nanjing	[redacted].28	AS4[redacted]
83	[redacted]0.29	China	Nanjing	[redacted].29	AS4[redacted]
83	[redacted]50.59.4	Republic of Korea	Seoul	[redacted]0.59.4	AS9[redacted]d Co Ltd
83	[redacted]31.200.108	China	Shenzhen	[redacted]1.200.10[redacted]	AS1[redacted]m Shenzen network
83	[redacted]22.195.59	Republic of Korea	OTHER	[redacted]2.195.59	AS4[redacted]m
83	[redacted]86.34.44	China	Nanjing	[redacted]5.34.44	AS2[redacted]for CHINANET jiangsu province backbone
83	[redacted]86.34.144	China	Nanjing	[redacted]5.34.144	AS2[redacted]for CHINANET jiangsu province backbone
82	[redacted].82.199	United States	Boydton	[redacted]2.199	AS8[redacted]rporation
82	[redacted]5.201.172	United States	Cheyenne	[redacted]m.com.	AS4[redacted]S LLC
82	[redacted]2.237	United States	San Francisco	[redacted]-04-03-1[redacted]com.	AS1[redacted]n, Inc.
82	[redacted]4.114	United States	San Francisco	[redacted]-06-23-1[redacted]com.	AS1[redacted]n, Inc.
82	[redacted]4.236	United States	San Francisco	[redacted]-06-23-[redacted]om.	AS1[redacted]n, Inc.
82	[redacted]5.53	United States	San Francisco	[redacted]-06-23-8[redacted]om.	AS1[redacted]n, Inc.
82	[redacted]5.240	United States	San Francisco	[redacted]-05-31-7[redacted]com.	AS1[redacted]n, Inc.
82	[redacted]6.203	United States	San Francisco	[redacted]-05-31-1[redacted]d.com.	AS1[redacted]n, Inc.
82	[redacted]7.57	United States	San Francisco	[redacted]-05-31-1[redacted]d.com.	AS1[redacted]n, Inc.
82	[redacted]7.141	United States	San Francisco	[redacted]4b-14.st[redacted]	AS1[redacted]n, Inc.
82	[redacted]9.114	United States	San Francisco	[redacted]-04-14-9[redacted]com.	AS1[redacted]n, Inc.



79	[redacted].206	United States	San Francisco	[redacted]-05-31-69.[redacted]m.	AS1[redacted], Inc.
79	[redacted]7.193	France	OTHER	[redacted]-15-51.rev.[redacted]ay.com.	AS1[redacted]
79	[redacted].53.142	China	Nanjing	[redacted].53.142	AS4[redacted]
79	[redacted].173.68	Israel	OTHER	[redacted].173.68	AS1[redacted]munications Ltd.
79	[redacted]6.145.154	United States	San Francisco	[redacted]-0721d-6.[redacted]n.	AS1[redacted]n, Inc.
79	[redacted]0.202.69	United States	San Francisco	[redacted]orker-07-[redacted]d.com.	AS1[redacted]n, Inc.
79	[redacted]2.64.133	France	OTHER	[redacted]2-64-133.r[redacted]om.eu.	AS1[redacted]
79	[redacted]2.87.150	France	OTHER	[redacted]2-87-150.r[redacted]om.eu.	AS1[redacted]
79	[redacted]2.95.17	France	OTHER	[redacted]2-95-17.re[redacted]m.eu.	AS1[redacted]
79	[redacted].106.162	China	Nanjing	[redacted].106.162	AS2[redacted]for CHINANET jiangsu province backbone
79	[redacted]6.50.177	China	Nanjing	[redacted]6.50.177	AS2[redacted]for CHINANET jiangsu province backbone

Top 5 most scanned own systems

Own Systems	DNS name	# remote scanners
141.253.218.52	joinandshare.local.company.com.	5741
141.253.218.42	xilogistics.local.company.com.	3731
141.253.218.33	giserver2.local.company.com.	3610
141.253.221.135	inflame2.xi.company.com.	3376
141.253.218.65	mims-karisma.local.company.com.	3360
141.253.221.116	savoir.company.com.	3360

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

Own system	Day	Ingress Bytes	Peak jump (%)
141.253.221.27	17-08-06	8822458492	4250722
141.253.218.57	17-08-06	136744746	187237
141.253.221.109	17-08-06	230368171	17471
141.253.218.54	17-07-27	25835191	14722
141.253.218.58	17-07-17	2944709	12108
141.253.221.103	17-07-18	250653159	11735
141.253.221.31	17-07-18	670835566	11322
141.253.221.37	17-08-06	192924267	7490
141.253.218.25	17-08-01	18333478	7343
141.253.218.52	17-08-06	2193061022	2948
141.253.218.36	17-08-06	10011160	2530
141.253.221.29	17-07-18	163694588	1802
141.253.221.163	17-07-19	131157906	1497
141.253.221.170	17-08-06	78212	1473
141.253.218.56	17-06-30	40476541	1306
141.253.221.134	17-07-21	2507852944	1302
141.253.221.35	17-07-14	23752345	1262
141.253.221.90	17-06-29	73232517	1068
141.253.221.105	17-08-06	153183662	931
141.253.221.108	17-07-17	230748636	404
141.253.221.234	17-08-06	21907	375
141.253.221.93	17-06-27	73698924557	316
141.253.218.70	17-07-19	328114	300
141.253.218.42	17-06-29	2819808079	297
141.253.221.85	17-07-11	656252875	290
141.253.221.11	17-07-19	309193482	288
141.253.221.110	17-06-29	5214579	243
141.253.221.14	17-08-05	29090	238
141.253.218.26	17-07-22	348575	223
141.253.221.12	17-07-07	2610314	201
141.253.218.22	17-07-19	348701	199
141.253.221.136	17-07-17	114858480	197
141.253.221.173	17-07-27	4788411	187
141.253.221.36	17-07-10	119774696	183
141.253.221.16	17-08-05	1606455	176
141.253.218.49	17-07-21	43369027	168
141.253.218.33	17-07-19	301252824	158
141.253.221.106	17-07-11	508553708	151
141.253.218.72	17-07-11	198419914	149
141.253.221.219	17-08-06	1709312	144
141.253.218.102	17-06-30	16467988	139
141.253.221.7	17-06-29	1607262	138
141.253.218.31	17-07-30	302123708	130
141.253.218.61	17-07-19	212396419	126
141.253.221.60	17-06-30	8676876	126
141.253.218.6	17-07-14	96523885003	125
141.253.218.16	17-06-27	55959061	121
141.253.221.214	17-08-06	2533404	119

141.253.221.27 cs2devipf.xi.company.com.

Remote	Svc	Ingress	Egress	Country/City	DNS/Provider
[redacted]9.120.172	http tcp	8822351872		Ukraine OTHER	[redacted]120.172.[redacted]t. [redacted]07 Inter[redacted]td.
[redacted]9.125.184	http tcp	73744		Ukraine OTHER	[redacted]125.184.[redacted]t. [redacted]07 Inter[redacted]td.
[redacted]9.127.176	http tcp	14919	12045	Ukraine OTHER	[redacted]127.176.[redacted]t. [redacted]07 Inter[redacted]td.
[redacted]9.124.156	http tcp	3602	1501	Ukraine OTHER	[redacted]124.156.[redacted]t. [redacted]07 Inter[redacted]td.
[redacted]45.144.16	ntp udp	2736	1748	Italy Milan	[redacted]b.bilink.[redacted] [redacted]6 Metro[redacted]

141.253.218.57 toolboxmain.local.company.com.

Remote	Svc	Ingress	Egress	Country/City	[redacted]rovider
[redacted].65.144	http tcp	136723220	12550012928	United States Marysville	[redacted]56-249-[redacted]glebot.com. [redacted]69 Goog[redacted]
[redacted]3.65.58	https tcp	8885		China Jinan	[redacted]3.65.58 [redacted]7 CNC[redacted]na169 Backbone
[redacted]3.5.19	ntp udp	4332	4560		[redacted]om91-e[redacted]pany.com. [redacted] The Bi[redacted](HQ)
[redacted]3.5.18	ntp udp	3952	3952	OTHER OTHER	[redacted]3.5.18 [redacted]R
[redacted]2.231.31	http tcp	992	9052	United Kingdom London	[redacted]tra-grab[redacted]1.binaryedge.ninja. [redacted]49 Lino[redacted]

141.253.221.109 sales-ops-apsf.xi.company.com.

Remote	Svc	Ingress	Egress	Country/City	[redacted]rovider
[redacted].21.64	https tcp	217998448		United States San Francisco	[redacted]4b-32.s[redacted]m. [redacted]61 Digi[redacted]nc.
[redacted].124.139	http tcp	9039014		Ukraine OTHER	[redacted]124.139.[redacted]t. [redacted]07 Inter[redacted]td.
[redacted]12.122.71	https tcp	1042473		United States Ann Arbor	[redacted]hscan32[redacted]ch.edu. [redacted]75 Univ[redacted]chigan
[redacted].122.19	http tcp	866922		Ukraine OTHER	[redacted]122.19.n[redacted]t. [redacted]07 Inter[redacted]td.
[redacted]3.29.47	https tcp	790358	2018844	United States San Jose	[redacted]-193-29[redacted]-1.compute.amazonaws.com. [redacted]09 Ama[redacted]nc.

141.253.218.54 django.local.company.com.