Ransomware vs AI. Part 1

Overview of AV bypassing techniques used in targeted ransomware attacks

PRO.M.IS security built in

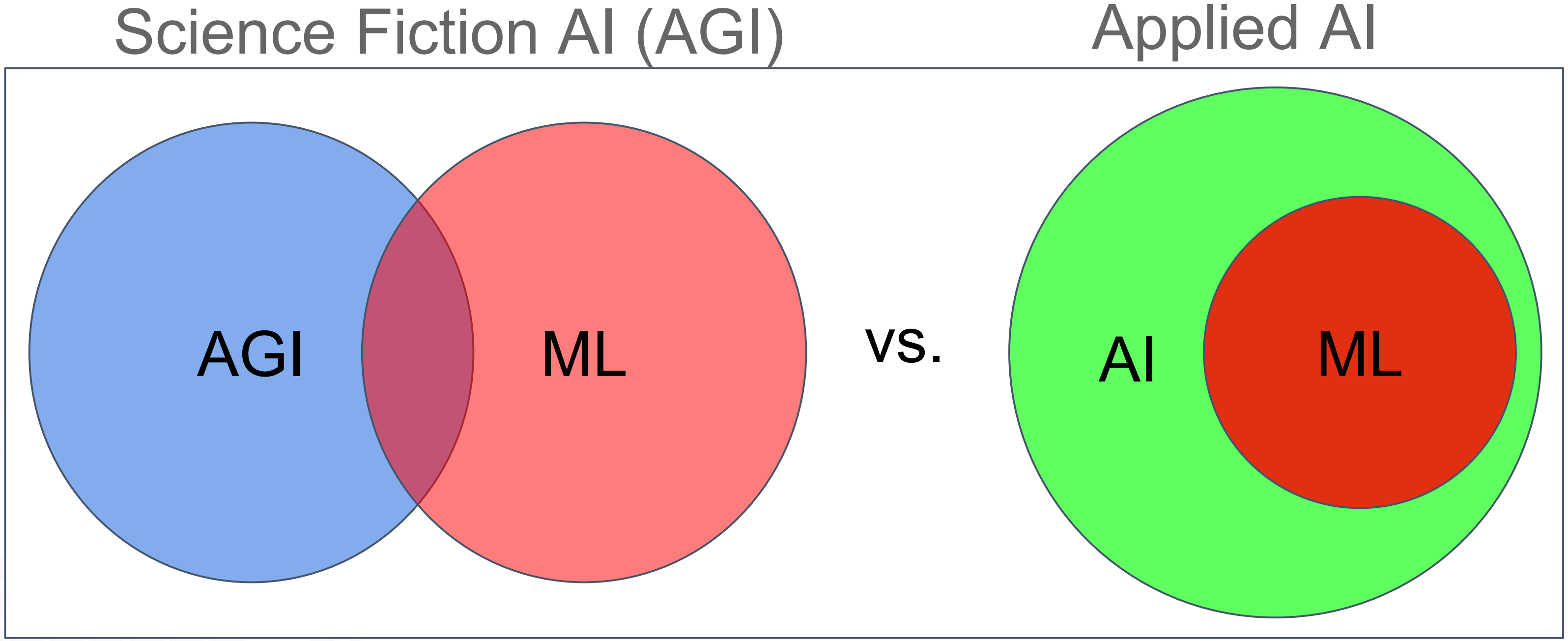
Professional Master in Information Security

Alexander Adamov
oleksandr.adamov@bth.se

agenda

- 5 min to introduce AI & ML
- Current AI approaches to detect ransomware
- Ransomware in 2019/20
- Ransomware bypassing techniques
- PROMIS general information
- Courses
- How to apply

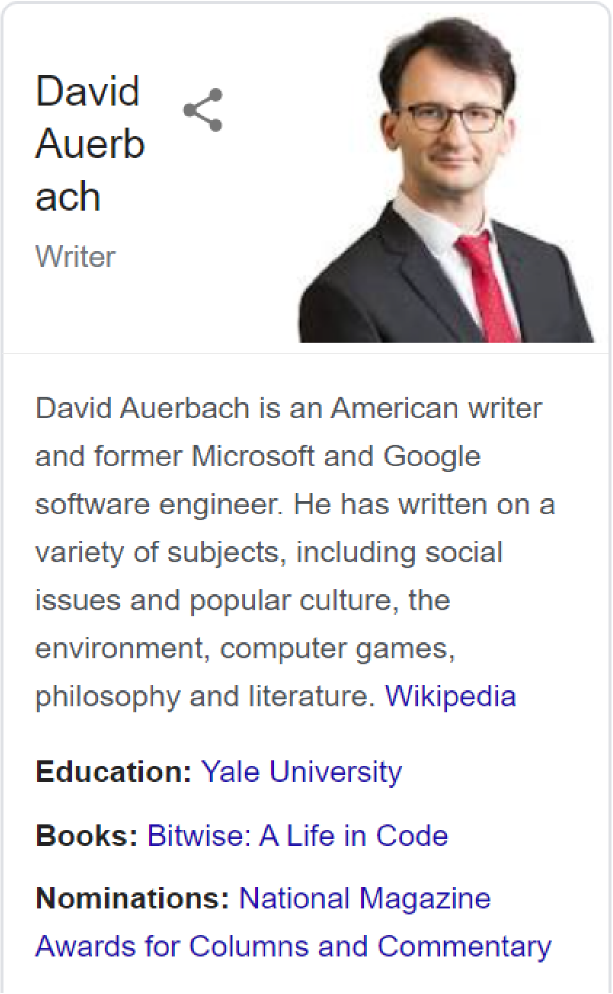
Definition of AI



AI Paradigms

David Auerbach identifies five AI paradigms:

- Speculative (until 1940)
- Cybernetic (1940–1955)
- Symbolic AI (1955–1985)
  - AI winter (1974–80)
- Subsymbolic AI (1985–2010)
  - 2nd AI winter (1987–1993)
- Deep Learning (2010 —...)



David Auerbach

Writer

David Auerbach is an American writer and former Microsoft and Google software engineer. He has written on a variety of subjects, including social issues and popular culture, the environment, computer games, philosophy and literature. Wikipedia

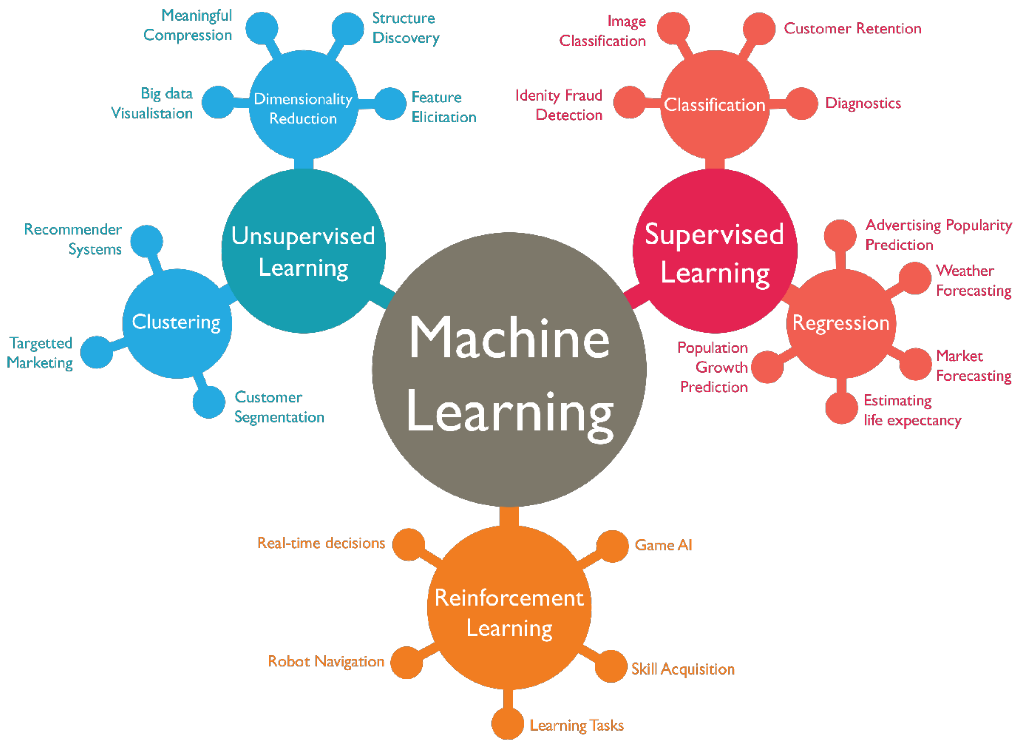
Education: Yale University

Books: Bitwise: A Life in Code

Nominations: National Magazine Awards for Columns and Commentary

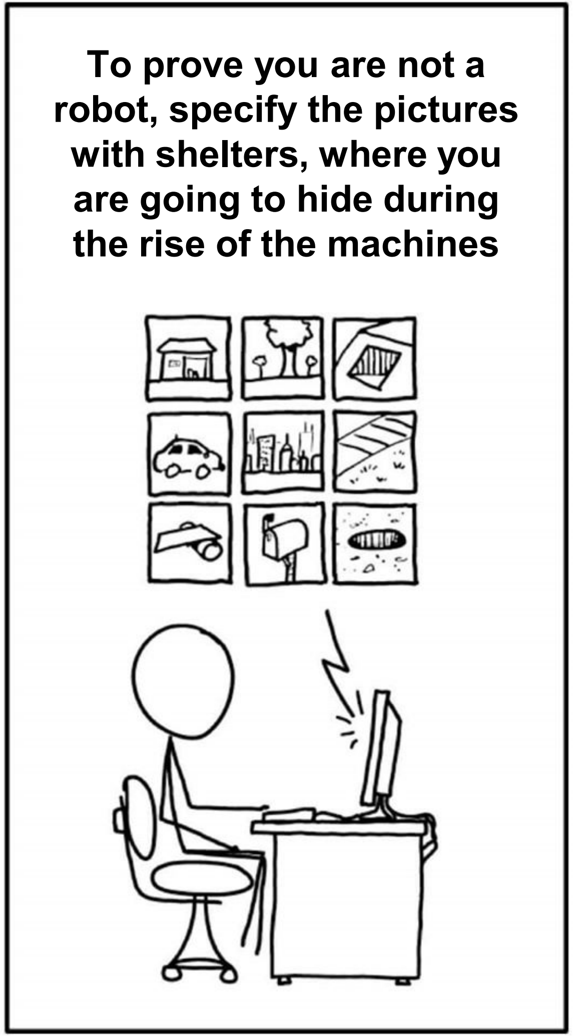
Machine Learning Approaches

1. Supervised learning
2. Unsupervised learning
3. Reinforcement learning
4. Semi-Supervised learning
5. Self-supervised learning



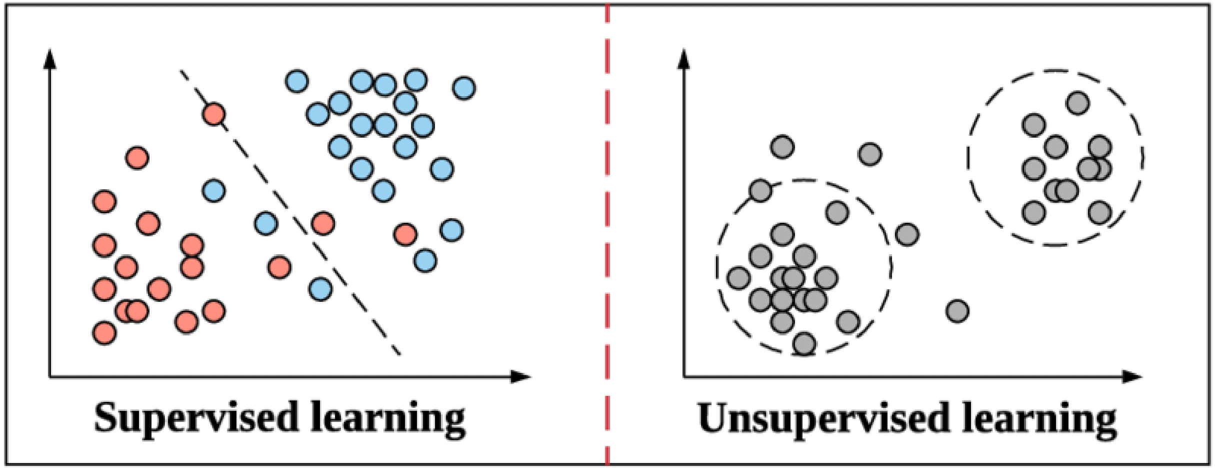
Supervised Learning

1. Classification and recognition;
2. Pattern recognition
3. Supervised anomaly detection
4. Forecasting (regression analysis)


To prove you are not a robot, specify the pictures with shelters, where you are going to hide during the rise of the machines

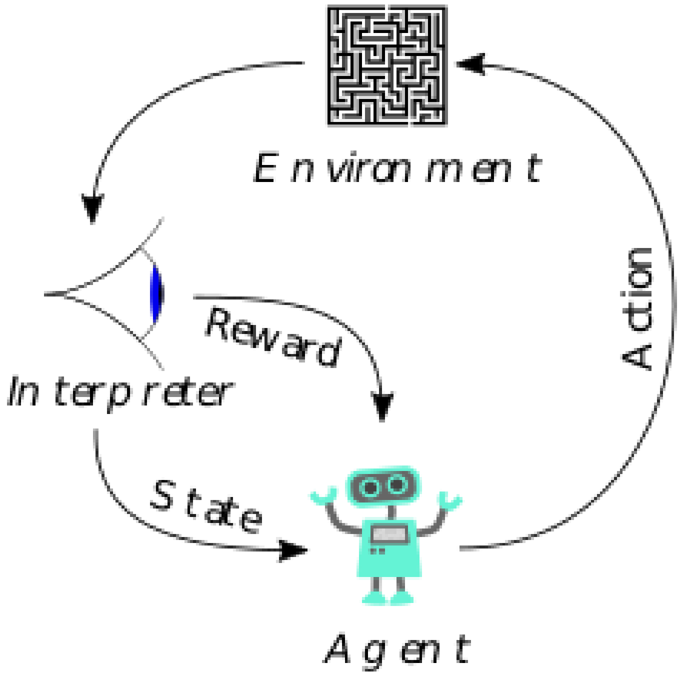
Unsupervised Learning

1. Clustering
2. Unsupervised pattern recognition
3. Unsupervised anomaly detection



Reinforcement Learning

1. Robot control
2. Game theory - AI initially knows only the rules of the game and creates algorithms and strategies while playing with other instances of itself and human players.
   a. Go game (AlphaGo)
   b. Chess (AlphaZero),
   c. other board games,
   d. real time strategy games (AlphaStar).
3. Security testing (e.g. penetration testing, anti-malware testing)



AI/ML methods to detect ransomware

- Anomaly detection
  - UEBA (User and Entity Behavior Analytics)
  - Honeypots
  - Anomalies in files content
- Reputation-based security and Scoring System for apps
- Smart pattern matching
  - Finding malicious code patterns in the process memory
  - Finding ransomware artefacts in already encrypted files

Advantages of unsupervised anomaly detection

- No need in labeled data
- An ability to identify zero-day attacks as well as unknown security threats
- Does not focus on a specific class of threats and can be used to identify data leakages (DLP) as well as functional violations to predict system faults.

Anomaly detection algorithms

- Density-based techniques (k-nearest neighbor,[8][9][10] local outlier factor,[11] isolation forests,[12][13] and many more variations of this concept[14]).
- Subspace-,[15] correlation-based[16] and tensor-based [17] outlier detection for high-dimensional data.[18]
- One-class support vector machines.[19]
- Replicator neural networks.[20], Autoencoders, Long short-term memory neural networks[21]
- Bayesian Networks.[20]
- Hidden Markov models (HMMs).[20]
- Cluster analysis-based outlier detection.[22][23]
- Deviations from association rules and frequent itemsets.
- Fuzzy logic-based outlier detection.
- Ensemble techniques, using feature bagging,[24][25] score normalization[26][27] and different sources of diversity.[28][29]

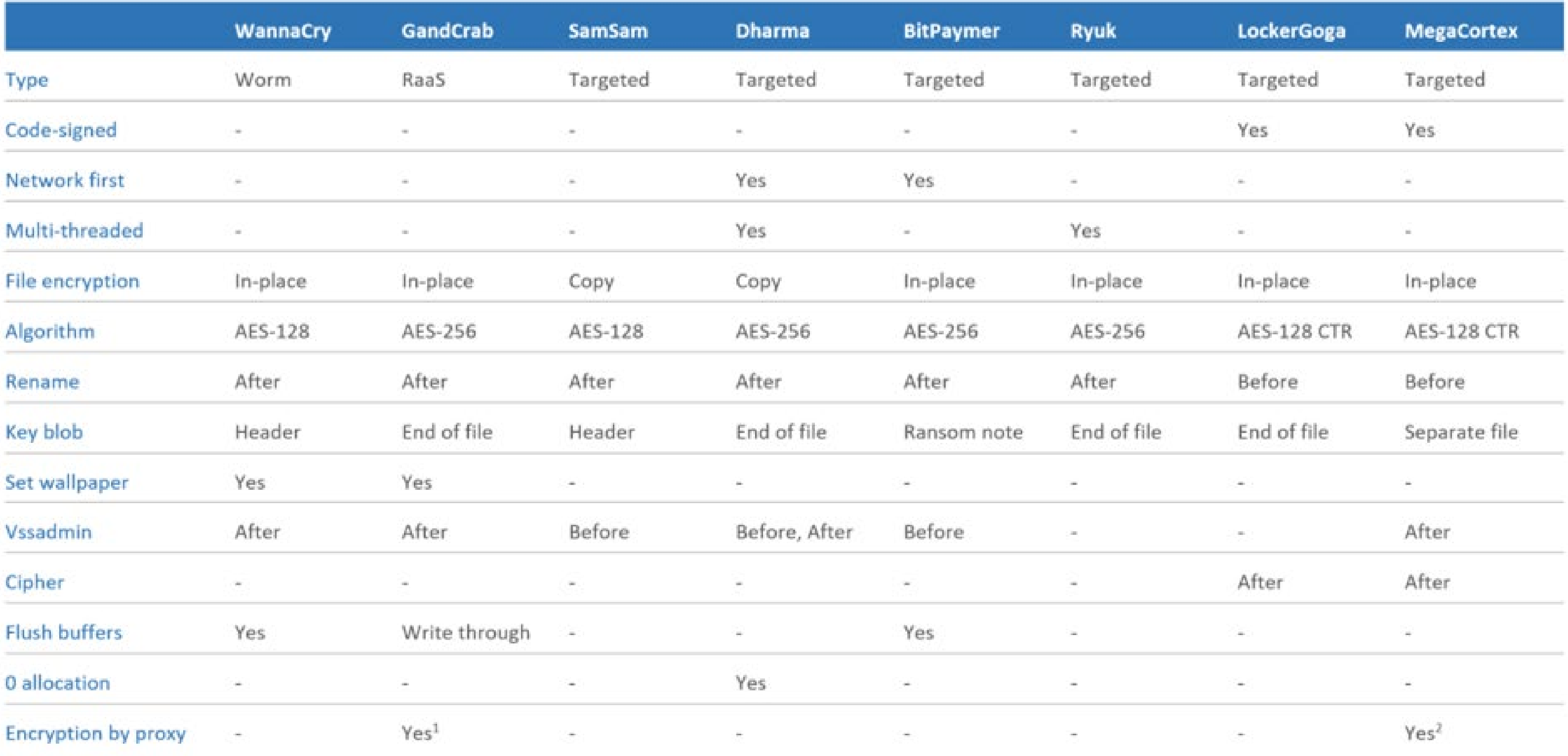
Behavior-based detection

Examples of ransomware behavior:

- Modification of more than N files by a single process
- Writing data with high entropy (packing or encryption)
- Adding the second extension to file names
- Calling CryptoAPI

Ransomware Attacks in 2019

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]

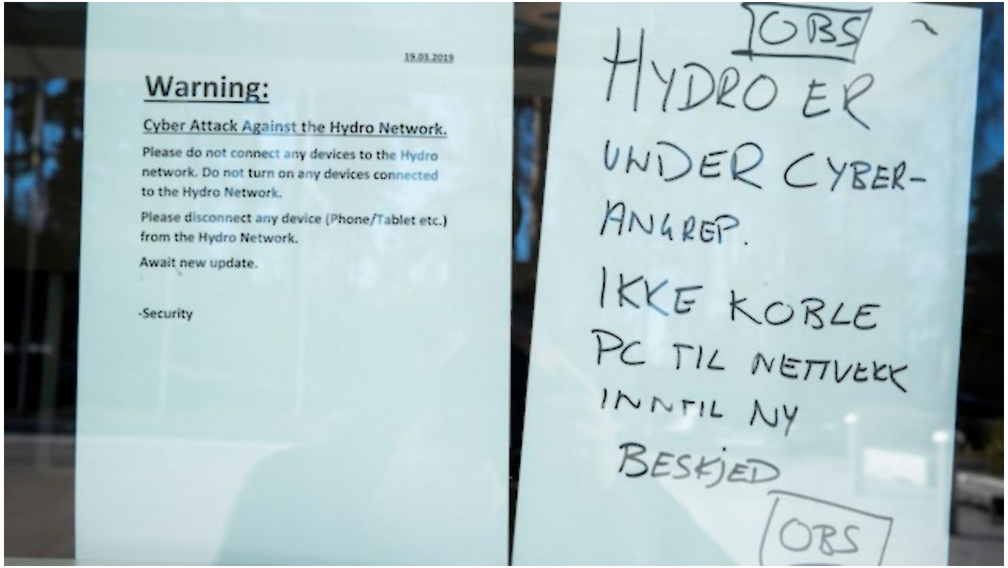
Source: https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/

LockerGoga

January 2019 - Altran Technologies

March 2019 - Norsk Hydra

March 2019 - US chemical companies Hexion and Momentive.



19.03.2019

Warning:

Cyber Attack Against the Hydro Network.

Please do not connect any devices to the Hydro network. Do not turn on any devices connected to the Hydro Network.

Please disconnect any device (Phone/Tablet etc.) from the Hydro Network.

Await new update.

-Security

OBS

HYDRO ER UNDER CYBER-ANGREP.

IKKE KOBLE PC TIL NETTVERK INNTIL NY BESKJED

OBS

MegaCortex

May 2019 - 47 attacks were stopped within 48 hours.

Code Signing Abuse

Chronicle: Abusing Code Signing

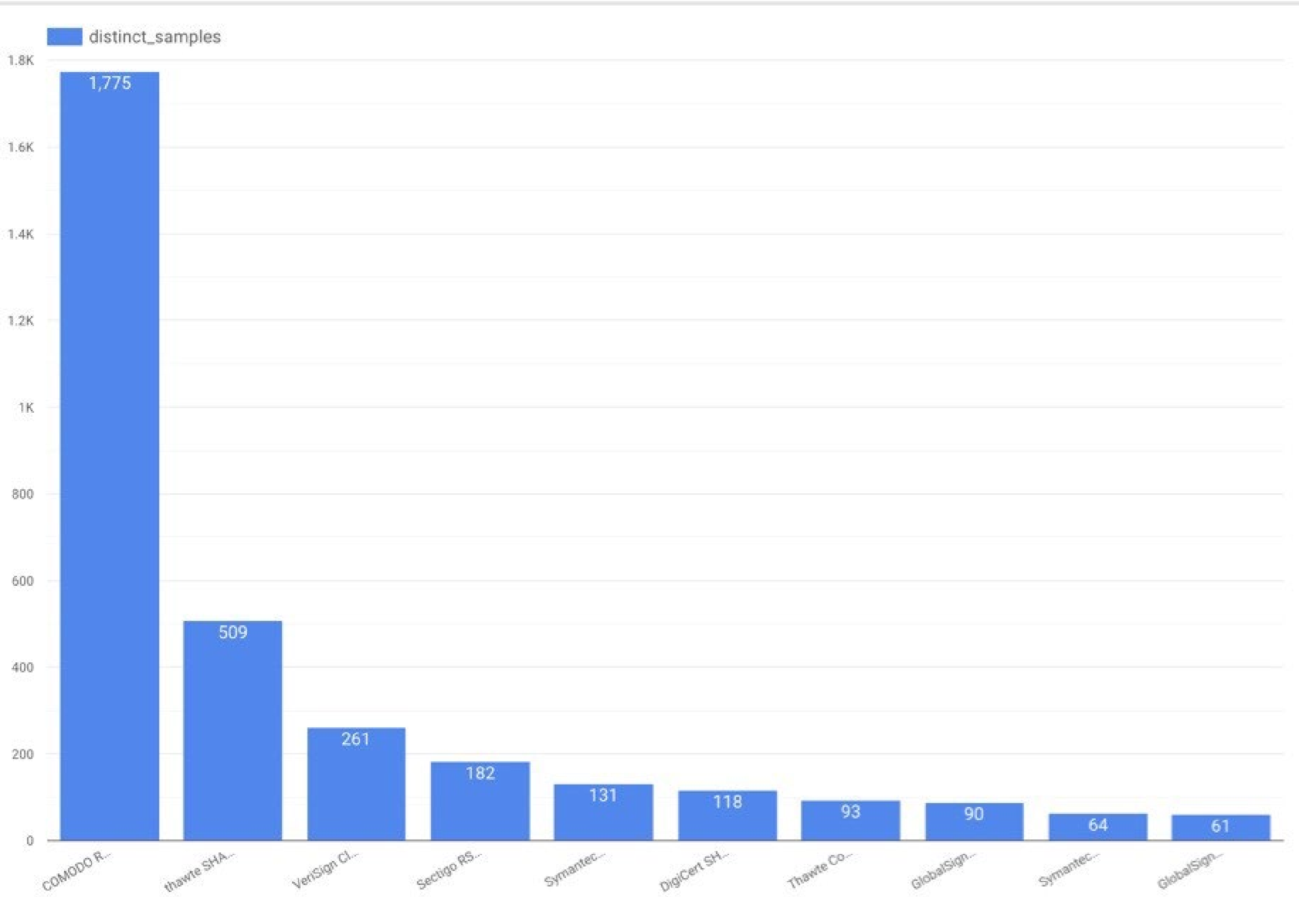
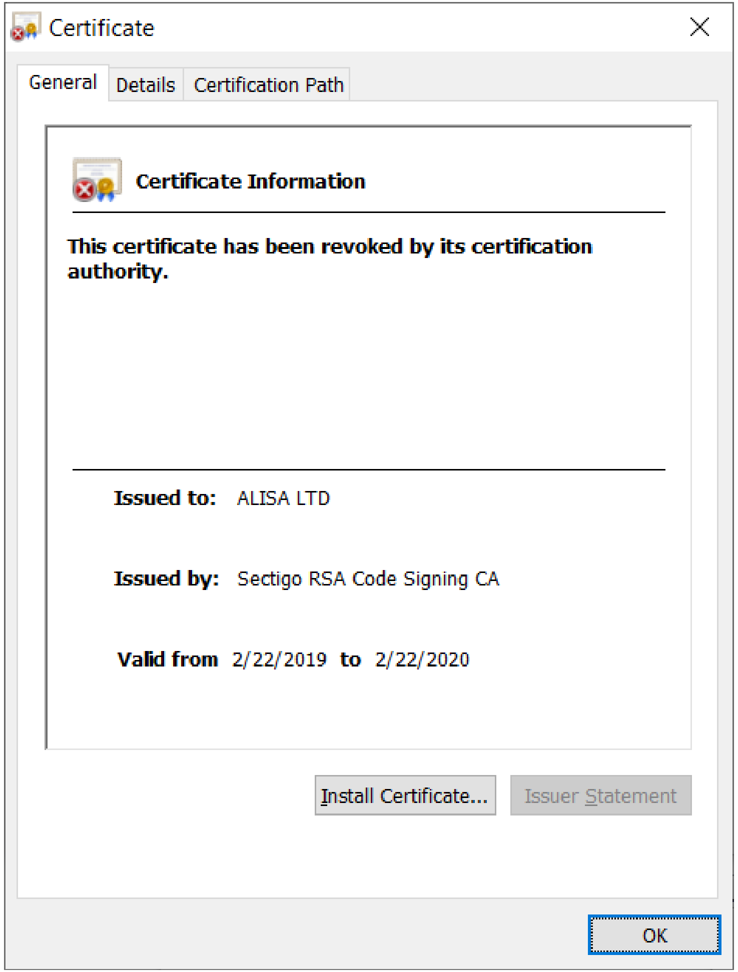


Figure 2. Breakdown of the top 10 signers by distinct sample count. The top 6 signers account for nearly 78% of evaluated samples.

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

LockerGoga Certificates

LockerGoga were supplied with the certificates issued to Alina Ltd, Kitty's Ltd., Mikl Limited, and AB Simba Limited registered in West End, London with 84,673 other companies.



Certificate Information

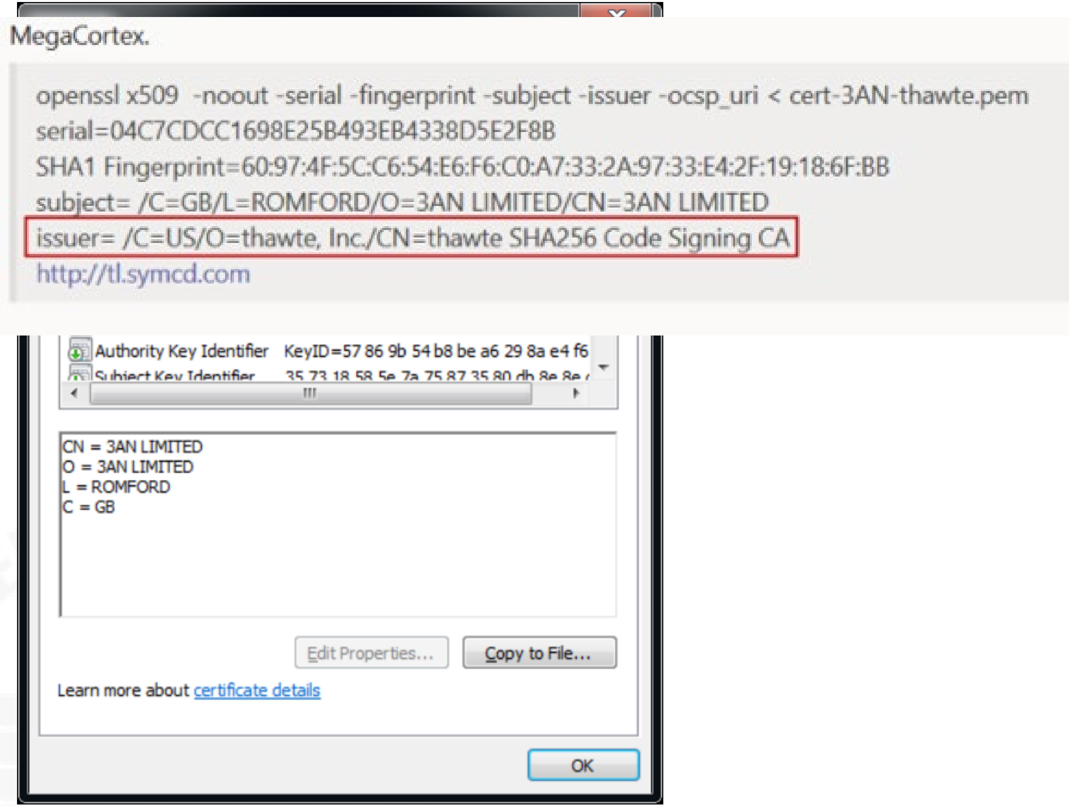
This certificate has been revoked by its certification authority.

Issued to: ALISA LTD

Issued by: Sectigo RSA Code Signing CA

Valid from 2/22/2019 **to** 2/22/2020

Certificate



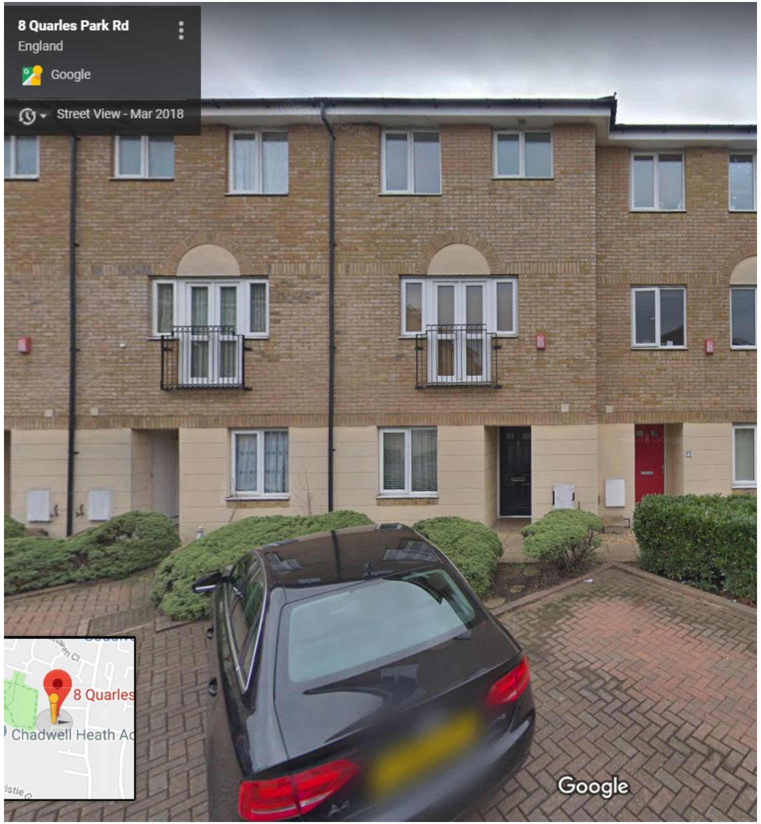
MegaCortex.

```
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 5e 7a 75 87 35 80 db 8e 8e

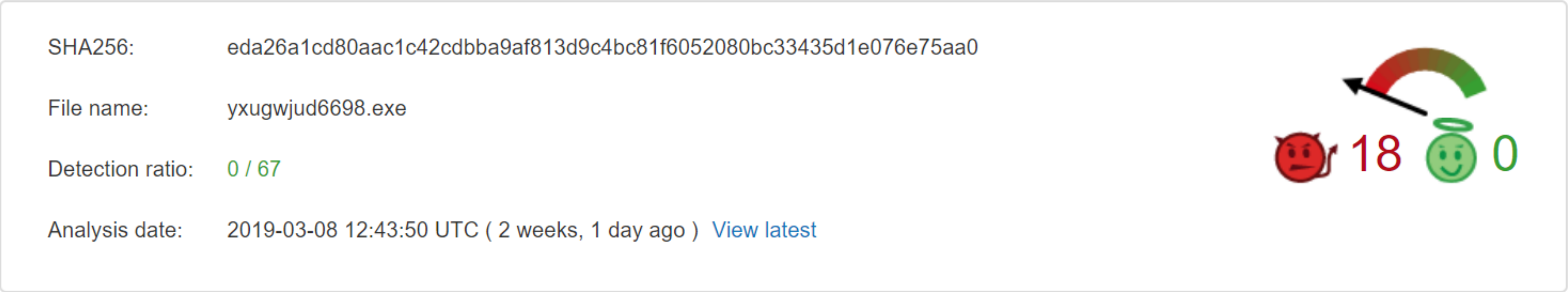
CN = 3AN LIMITED
O = 3AN LIMITED
L = ROMFORD
C = GB

Learn more about certificate details



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

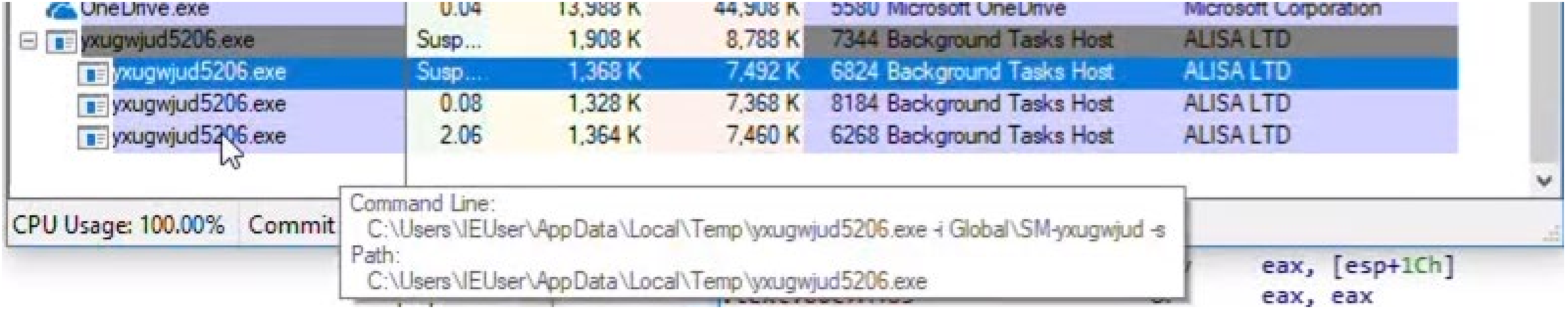
Impact: 0 VT detections of LockerGoga



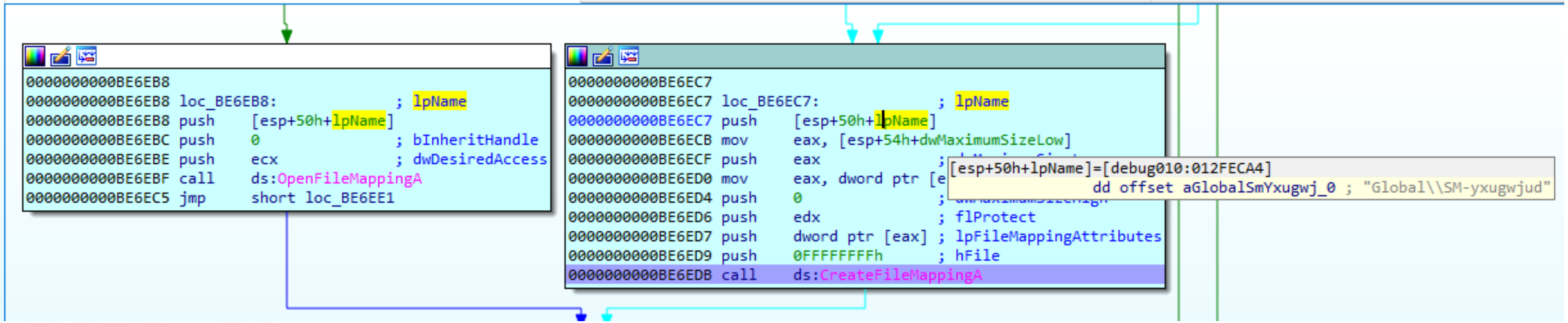
SHA256:	eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0
File name:	yxugwjud6698.exe
Detection ratio:	0 / 67
Analysis date:	2019-03-08 12:43:50 UTC (2 weeks, 1 day ago) View latest

Multiprocess Encryption

LockerGoga



```
OneDrive.exe          0.04    13,988 K   44,908 K   5580 Microsoft OneDrive      Microsoft Corporation
⊟ yxugwjud5206.exe    Susp...  1,908 K    8,788 K   7344 Background Tasks Host   ALISA LTD
    yxugwjud5206.exe  Susp...  1,368 K    7,492 K   6824 Background Tasks Host   ALISA LTD
    yxugwjud5206.exe  0.08     1,328 K    7,368 K   8184 Background Tasks Host   ALISA LTD
    yxugwjud5206.exe  2.06     1,364 K    7,460 K   6268 Background Tasks Host   ALISA LTD

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
```

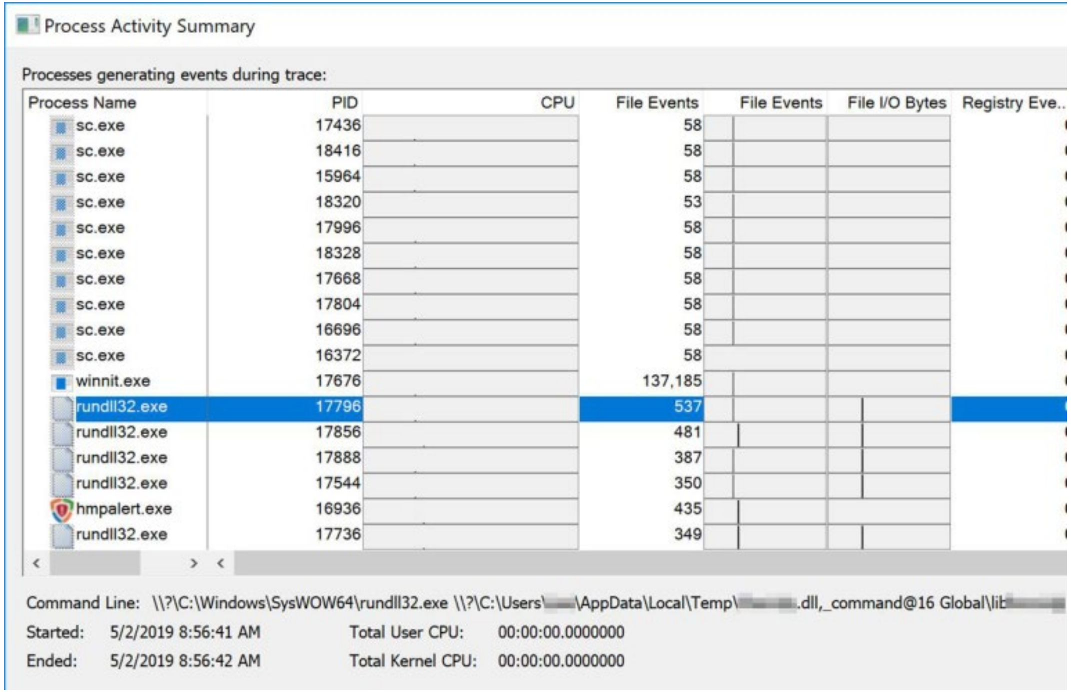


```
0000000000BE6EB8
0000000000BE6EB8 loc_BE6EB8:                 ; lpName
0000000000BE6EB8 push    [esp+50h+lpName]
0000000000BE6EBC push    0                   ; bInheritHandle
0000000000BE6EBE push    ecx                 ; dwDesiredAccess
0000000000BE6EBF call    ds:OpenFileMappingA
0000000000BE6EC5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

```
0000000000BE6EC7
0000000000BE6EC7 loc_BE6EC7:                 ; lpName
0000000000BE6EC7 push    [esp+50h+lpName]
0000000000BE6ECB mov     eax, [esp+54h+dwMaximumSizeLow]
0000000000BE6ECF push    eax                 ;
0000000000BE6ED0 mov     eax, dword ptr [e
0000000000BE6ED4 push    0                   ; dwMaximumSizeHigh
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"
```

MegaCortex



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\[redacted]\AppData\Local\Temp\[redacted].dll,_command@16 Global\lib[redacted]

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

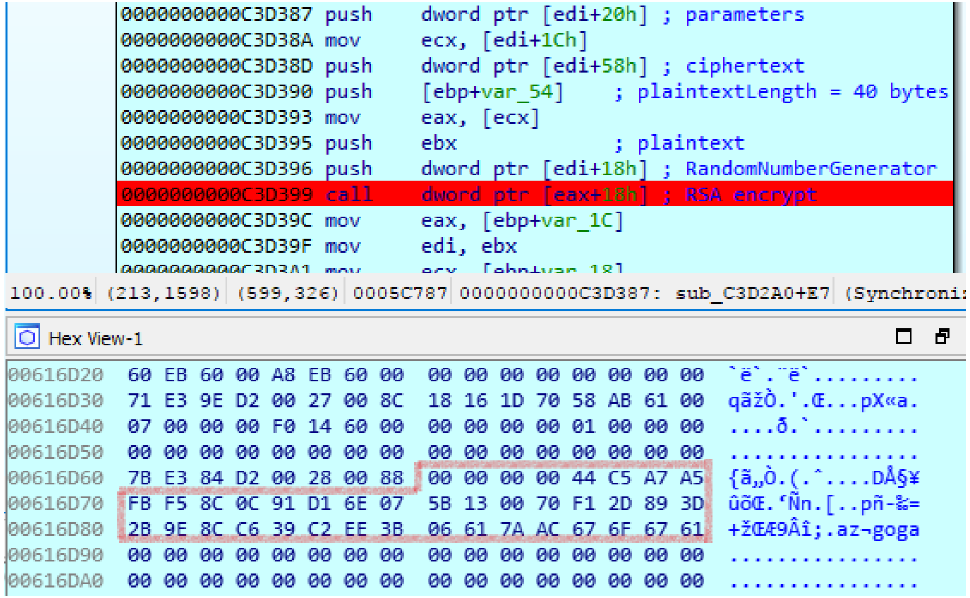
Ended: 5/2/2019 8:56:42 AM   Total Kernel CPU: 00:00:00.0000000

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

Custom Cryptography

LockerGoga encryption

LockerGoga ransomware incorporates statically linked Crypto++ library to implement AES-128-CTR with AES-NI acceleration for file encryption and RSA-1024 with OAEP using the MGF1(SHA-1).

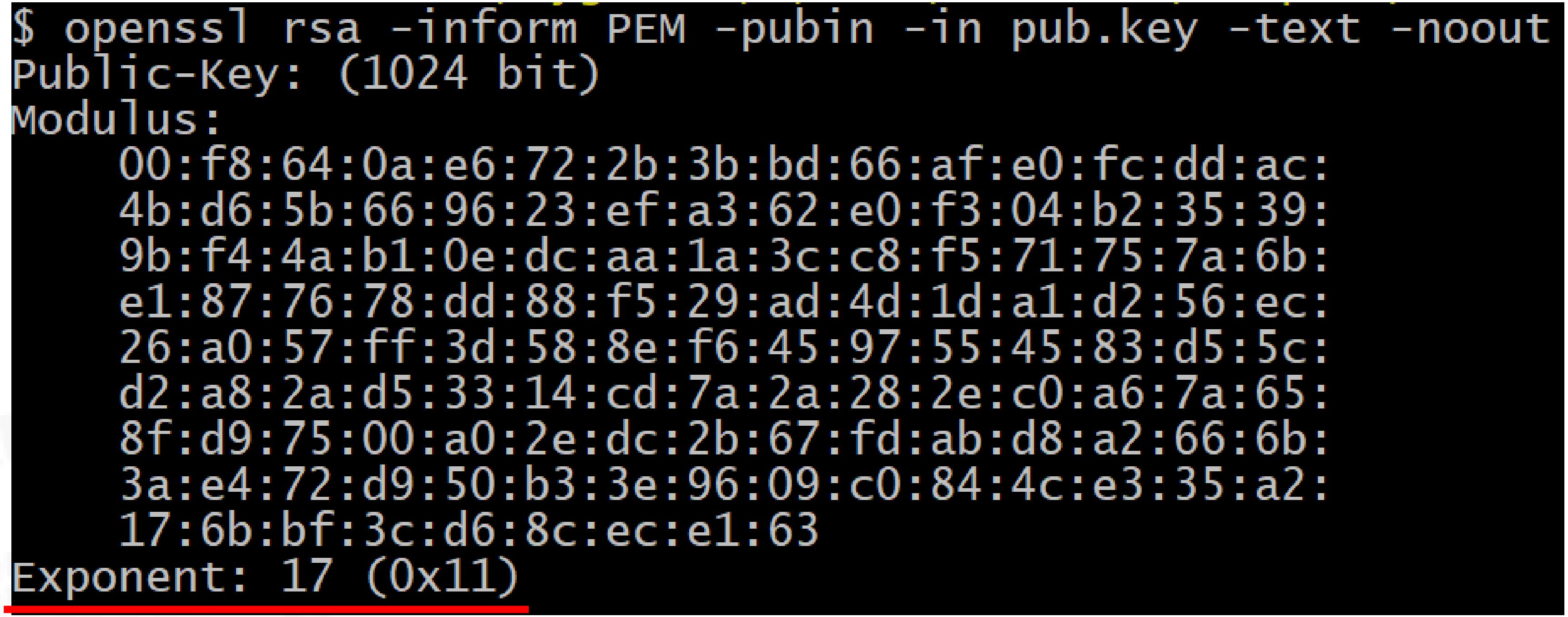


```
0000000000C3D387 push    dword ptr [edi+20h] ; parameters
0000000000C3D38A mov     ecx, [edi+1Ch]
0000000000C3D38D push    dword ptr [edi+58h] ; ciphertext
0000000000C3D390 push    [ebp+var_54]     ; plaintextLength = 40 bytes
0000000000C3D393 mov     eax, [ecx]
0000000000C3D395 push    ebx              ; plaintext
0000000000C3D396 push    dword ptr [edi+18h] ; RandomNumberGenerator
0000000000C3D399 call    dword ptr [eax+18h] ; RSA encrypt
0000000000C3D39C mov     eax, [ebp+var_1C]
0000000000C3D39F mov     edi, ebx
0000000000C3D3A1 mov     ecx, [ebp+var_18]
```

```
100.00% (213,1598) (599,326) 0005C787 0000000000C3D387: sub_C3D2A0+E7 (Synchroni
```

```
00616D20  60 EB 60 00 A8 EB 60 00  00 00 00 00 00 00 00 00  `ë`.¨ë`.........
00616D30  71 E3 9E D2 00 27 00 8C  18 16 1D 70 58 AB 61 00  qãžÒ.'.Œ...pX«a.
00616D40  07 00 00 00 F0 14 60 00  00 00 00 00 01 00 00 00  ....ð.`.........
00616D50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00616D60  7B E3 84 D2 00 28 00 88  00 00 00 00 44 C5 A7 A5  {ã„Ò.(.ˆ....DÅ§¥
00616D70  FB F5 8C 0C 91 D1 6E 07  5B 13 00 70 F1 2D 89 3D  ûõŒ.‘Ñn.[..pñ-‰=
00616D80  2B 9E 8C C6 39 C2 EE 3B  06 61 7A AC 67 6F 67 61  +žŒÆ9Âî;.az¬goga
00616D90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00616DA0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

LockerGoga’s Master Public Key

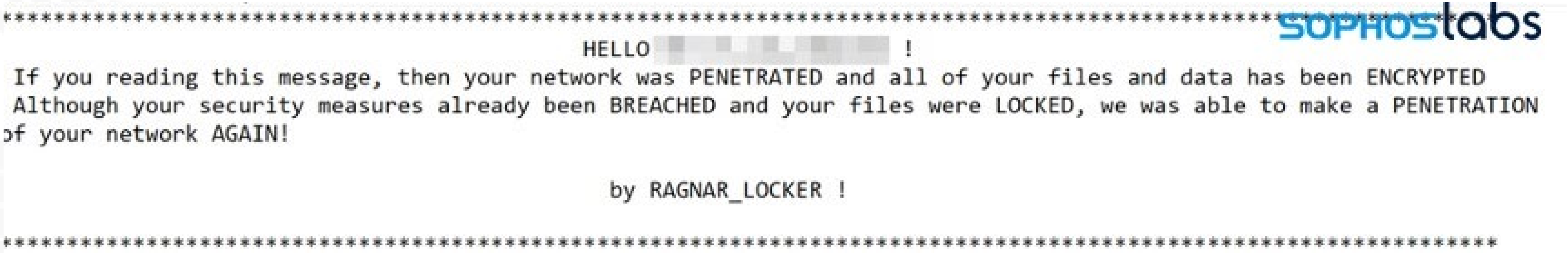


```
$ openssl rsa -inform PEM -pubin -in pub.key -text -noout
Public-Key: (1024 bit)
Modulus:
    00:f8:64:0a:e6:72:2b:3b:bd:66:af:e0:fc:dd:ac:
    4b:d6:5b:66:96:23:ef:a3:62:e0:f3:04:b2:35:39:
    9b:f4:4a:b1:0e:dc:aa:1a:3c:c8:f5:71:75:7a:6b:
    e1:87:76:78:dd:88:f5:29:ad:4d:1d:a1:d2:56:ec:
    26:a0:57:ff:3d:58:8e:f6:45:97:55:45:83:d5:5c:
    d2:a8:2a:d5:33:14:cd:7a:2a:28:2e:c0:a6:7a:65:
    8f:d9:75:00:a0:2e:dc:2b:67:fd:ab:d8:a2:66:6b:
    3a:e4:72:d9:50:b3:3e:96:09:c0:84:4c:e3:35:a2:
    17:6b:bf:3c:d6:8c:ec:e1:63
Exponent: 17 (0x11)
```

Targeted Ransomware Attacks in 2020

Ragnar Locker

- In April, the actors behind Ragnar Locker attacked the network of Energias de Portugal (EDP) and claimed to have stolen 10 terabytes of sensitive company data, demanding a payment of 1,580 Bitcoin (approximately $11 million US) and threatening to release the data if the ransom was not paid.
- Ragnar Locker ransomware was deployed inside an Oracle VirtualBox Windows XP virtual machine. The attack payload was a 122 MB installer with a 282 MB virtual image inside—all to conceal a 49 kB ransomware executable.

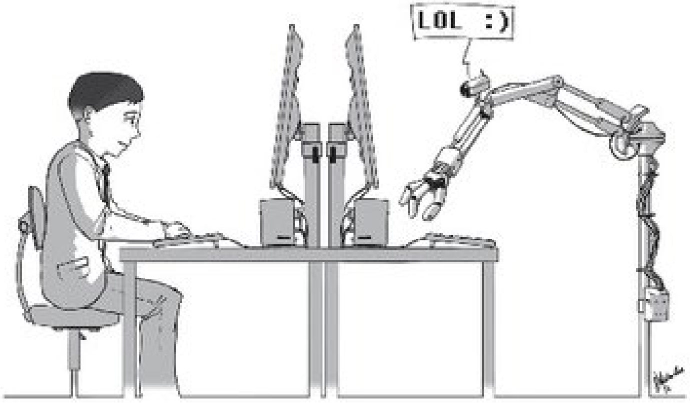


```
****************************************************************************************************
                                    HELLO [redacted] !
 If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED
 Although your security measures already been BREACHED and your files were LOCKED, we was able to make a PENETRATION
of your network AGAIN!

                                    by RAGNAR_LOCKER !

****************************************************************************************************
```

Source: https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/

The Imitation Game

The success factor of many ransomware attacks seen in 2019 is mimicking behavior and appearance of benign applications.
This helped the attackers to bypass cyber defence.



In the next episode

PROMIS (Professional Master in Information Security)

GENERAL FORMAT

Active industrials studying and working at the same time

- *University grade* ***COURSES for professionals****!*
- *Extend current competence in* ***an area ("security")***
- Case-based pedagogy (bring your own problems!)
- Online collaborative didactics
- Distance capability overall incl. lab and tools

Courses under development with input from companies

- Keep relevant and right level (companies advise us)
- DO YOU want to be part of the companies advising on courses?
  - CONTACT: Anna Eriksson aes@bth.se

BALLOU
VI ÄR EXPERTER PÅ DRIFT - ÄR NI?
citynetwork
ERICSSON
CYBERCOM GROUP
Outpost24
PROMESTRA
TRUESEC
telenor
advenica
factor10
more to
MaxKompetens
HELP AT WORK

Courses (3 thus far)

PROMIS (Professional Master in Information Security)

https://promisedu.se/

Security in Software-intensive products and service development (PA2582)
https://www.bth.se/eng/courses/D5818/20202/
Course responsible: Tony Gorschek
tony.gorschek@bth.se

- The ability to understand the technology, operational aspects, and engineering aspects of security - albeit the focus on the course is on "engineering security”
- The ability to plan for "pre-emptive" security in the planning and development of products and services
- The ability to do a risk assessment and take ROI into account
- The ability to develop and use secure architectures that allows for a more stable base for products and services
- The ability to compare and weigh the benefits and costs of non-functional aspects in combination to security
- The ability to estimate how security aspects impact, and are impacted on quality-/non-functional aspects such as usability, performance and maintainability of a product

more to come

Courses (3 thus far)

PROMIS (Professional Master in Information Security)

https://promisedu.se/

Software Security (DV2595)
https://www.bth.se/eng/courses/D5816/20202/
Course responsible: Dragos Ilie dragos.ilie@bth.se

- The ability to understand how attackers exploit risky programming practices
- The ability to detect risky programming practices
- The ability to understand and reason about efficiency and limitations in existing software security mechanisms
- The ability to to compare and weight the benefits and costs associated with binary analysis and instrumentation techniques

more to come

Courses (3 thus far)

PROMIS (Professional Master in Information Security)

https://promisedu.se/

Web System Security (DV2596)

https://www.bth.se/eng/courses/D5816/20202/

Course responsible: Anders Carlsson

anders.carlsson@bth.se

- be able to explain web protocols based on known vulnerabilities and weaknesses
- be able to describe the Common Vulnerability Scoring System (CVSS)
- be able to explain web protocols based on known vulnerabilities and weaknesses
- be able to explain the security aspects when using languages and framework, eg. PHP, JavaScript, and SQL
- be able to explain authentication mechanisms and counter techniques to bypass authentication
- understand Cross-site scripting (XSS) attacks and SQL injections
- be able to explain impacts of one or more combined vulnerabilities that limit or extend the damage given
- be able to install and configure the web server for high security independently
- be able to use and search open vulnerability databases (Common Vulnerability databases CV -DB)

to prevent and find security problems

- be able to use best practice of known design patterns for secure web applications
- be able to utilize OWASP where applicable
- be able to conduct internal and external penetration testing of web applications and related infrastructure)

more to come

PROMIS

HOW TO APPLY

https://promisedu.se/

Spread information about courses @ your company

Entry Requirements

PROMIS courses requires at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).

Even if you don’t have the formal academic merits, you might be qualified for the course through validation (reell kompetens)!

Apply for course:

1. **Create a user account at antagning.se / universityadmission.se**
2. **Search for PROMIS courses by the name Fill in and send in your application**
3. **Upload your required documents (employer’s certificate)**
4. **Reply to any offers of admission**

Questions about the course: contact course responsible
Questions about applying and validation (reell kompetens): : anna.eriksson@bth.se
Visit promisedu.se for more info about courses, application and template for employer’s certificate