UNIT 42
BY PALO ALTO NETWORKS

IR lessons learned

Sebastian Möbius
Consulting Director Pro Active Services
smobius@paloaltonetworks.com

paloalto NETWORKS

UNIT 42
BY PALO ALTO NETWORKS

AGENDA

Sign of EDR Tempering

Options to monitor and check for any tempering activity

OUT OF OFFICE HOURS! / REMOTE TOOLS

Every Ransomware case we had showed that behavior.

CANARY TOKEN

to monitor if admin accounts are tempered with.

HOW TO HUNT AN ACTOR THROUGH AN ENTERPRISE?

Especially without Cloud Connection and Firewalls etc.

DETECTION USE
EDR Tempering

paloalto NETWORKS

UNIT 42
BY PALO ALTO NETWORKS

Always alert for non functioning sensors

ALERT!

non working sensor

should always be closely monitored and react immediately

Hence the sensor is not working no data gets stored or alerted.

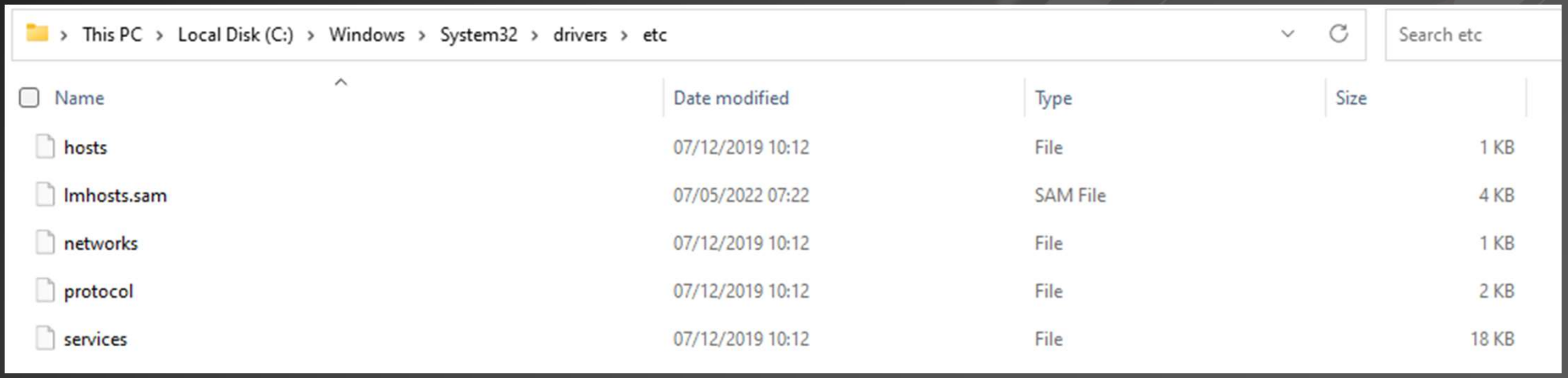
Means there is nothing to follow up on, you need forensics for the logs.

UNIT 42
BY PALO ALTO NETWORKS

Host entry / Firewall change

EDR is collecting that data and storing it accordingly to the storage policy which is in most cases 90 days.

Just change the Update Server of the EDR Vendor and no more updates will be applied.



UNIT 42
BY PALO ALTO NETWORKS

Safe boot to evade detection

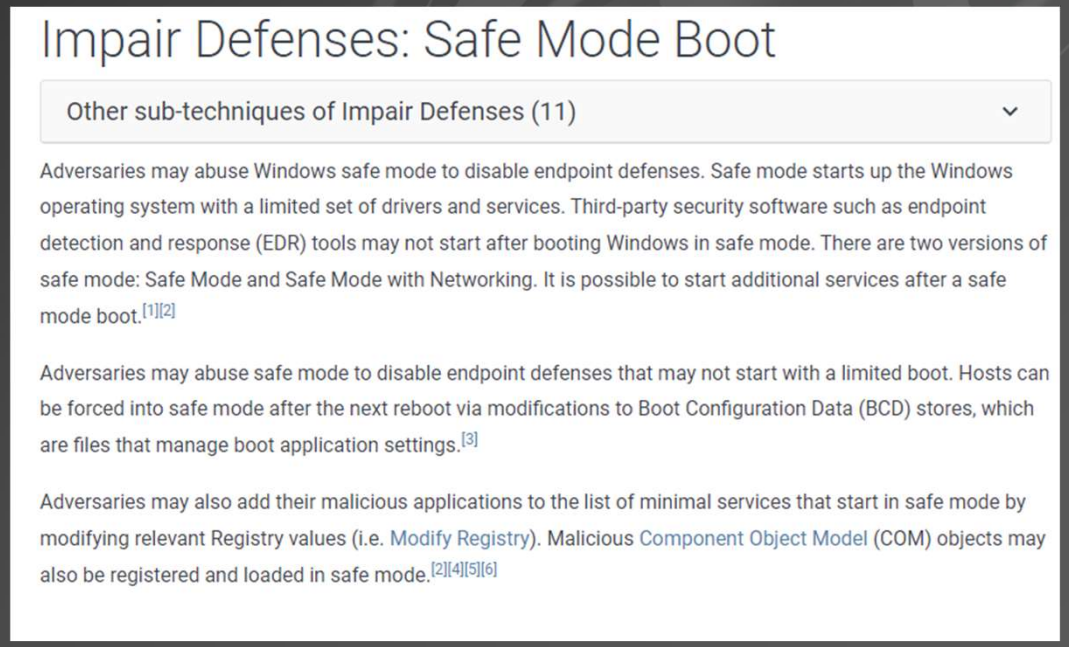
Windows Check for Safe Boot:

eventvwr.exe.
Windows Logs\System

Event ID 12 from source "Kernel-General"

This event's description is
"The operating system started at system time <timestamp>"

"BootMode".
value of 0 indicates normal boot
value of 1 indicates SafeMode



Impair Defenses: Safe Mode Boot

Other sub-techniques of Impair Defenses (11)

Adversaries may abuse Windows safe mode to disable endpoint defenses. Safe mode starts up the Windows operating system with a limited set of drivers and services. Third-party security software such as endpoint detection and response (EDR) tools may not start after booting Windows in safe mode. There are two versions of safe mode: Safe Mode and Safe Mode with Networking. It is possible to start additional services after a safe mode boot.[1][2]

Adversaries may abuse safe mode to disable endpoint defenses that may not start with a limited boot. Hosts can be forced into safe mode after the next reboot via modifications to Boot Configuration Data (BCD) stores, which are files that manage boot application settings.[3]

Adversaries may also add their malicious applications to the list of minimal services that start in safe mode by modifying relevant Registry values (i.e. Modify Registry). Malicious Component Object Model (COM) objects may also be registered and loaded in safe mode.[2][4][5][6]

https://attack.mitre.org/techniques/T1562/009/

UNIT 42
BY PALO ALTO NETWORKS

Cloaked URSA Phishing via HTML Smuggling to obscure ISO

CAR FOR SALE IN KYIV

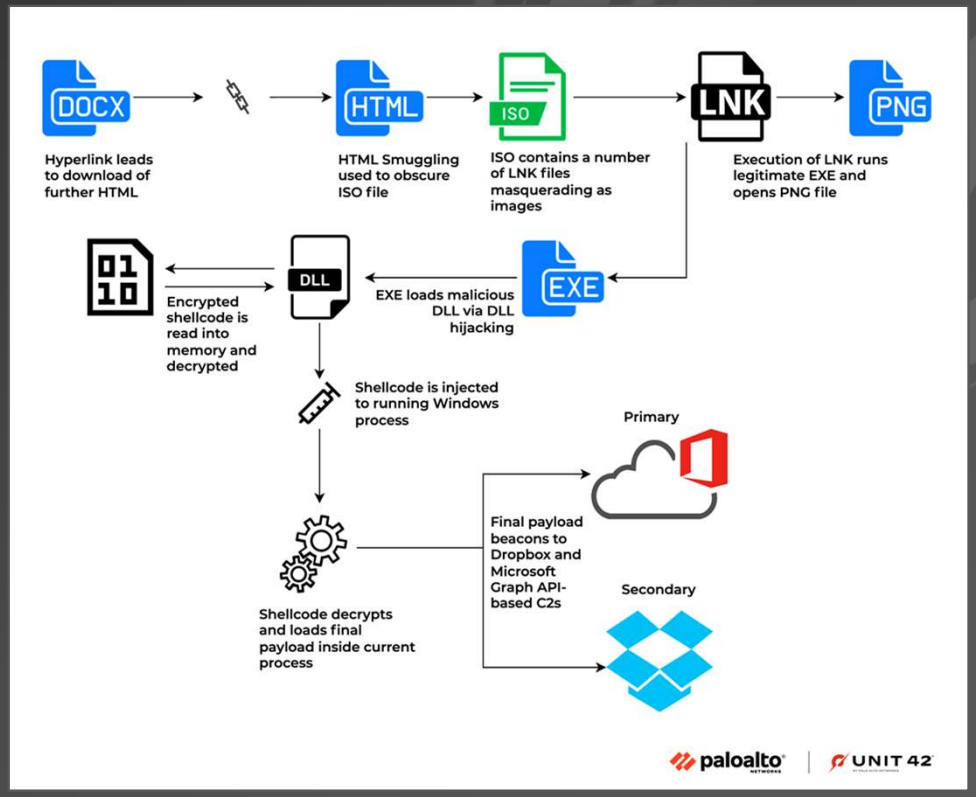
THE PRICE IS REDUCED!!!

BMW 5 (F10) 2.0 TDI, 7,500 Euros!!

Very good condition, low fuel consumption

More high quality photos are here: https://t.ly/

Model	**BMW 5, 2.0 TDI (184 HP)**
Year	April 2011
Mileage	266,000 km
Engine	2.0 Diesel
Transmission	Mechanic
Colour	Black, black leather interior
Package	A/C, set of summer and winter tires, ABS/ESP, led lights, cruise control, multifunction steering wheel, CD, electric seats, electric windows, engine control, rain sensor, electrical hand brake, airbags, start-stop system.
Price	7,500 Euros
Custom	NOT CLEARED
Contact	



UNIT 42
BY PALO ALTO NETWORKS

Use Eventlogs to check for ISO interactions

USER	EVENTLOG_LEVEL	EVENTLOG_PROVIDER	EVENTLOG_MESSAGE
TESTVM-RENZ\User	Information	Microsoft-Windows-VHDMP	VhdFileName=C:\Users\User\Videos\document-130722.9274.iso Status=0
TESTVM-RENZ\User	Information	Microsoft-Windows-VHDMP	Flags=0 AccessMask=851968 WriteDepth=0
TESTVM-RENZ\User	Information	Microsoft-Windows-VHDMP	VirtualDisk=0xffffd0880175f040
TESTVM-RENZ\User	Information	Microsoft-Windows-VHDMP	FileObject=0xffffd087fc118c80
TESTVM-RENZ\User	Information	Microsoft-Windows-VHDMP	FileObject=0xffffd087fc118c80
TESTVM-RENZ\User	Information	Microsoft-Windows-VHDMP	VhdFileName=C:\Users\User\Videos\document-130722.9274.iso DesiredAccess=2148532224
TESTVM-RENZ\User	Information	Microsoft-Windows-VHDMP	FileObject=0xffffd087fc118c80
TESTVM-RENZ\User	Information	Microsoft-Windows-VHDMP	VhdFileName=C:\Users\User\Videos\document-130722.9274.iso Status=0

Powershell command: Get-EventLog -LogName System -Source "Virtual Disk Service"

UNIT 42
BY PALO ALTO NETWORKS

Non protected device

Anything that had not a sensor installed at the moment it was compromised.

EDR is often not rolled out from the beginning on every device.

Some devices may are spared like production, SAP etc.

Some devices may not have any direct external connection

OUT OF OFFICE HOURS! / REMOTE TOOLS

paloalto NETWORKS

UNIT 42
BY PALO ALTO NETWORKS

Out of Office activity

Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	Sun.
08:00 – 17:00 Office Work	08:00 – 17:00 Office Work	08:00 – 17:00 Office Work	08:00 – 17:00 Office Work	08:00 – 17:00 Office Work		
20:30 – 22:00 Persistence		20:00 – 23:00 Exfiltration		22:00 – 00:00 Deploy Malware	00:00 – 00:00 Deploy Malware	00:00 – 00:00 Deploy Malware

UNIT 42
BY PALO ALTO NETWORKS

Example Screen Connect

Why this is so dangerous:

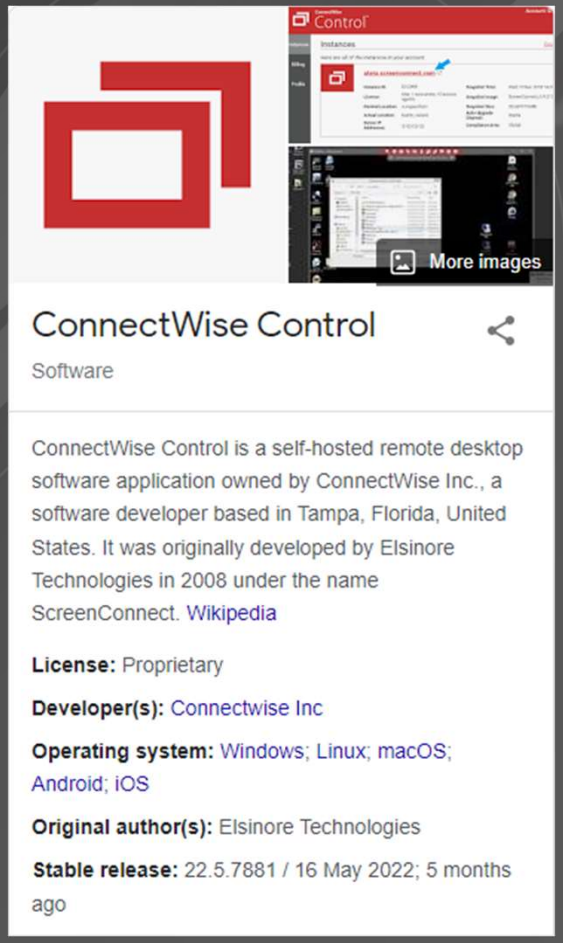
1. Remote tool registered as a service
2. Enables HTTPS tunnel to transfer malware
3. Automatically connects to external
4. Enables the attacker to use reverse shell

Maybe alerted as a PUP or Grayware

- Often no attention was paid to it

Worst part:

- Access will still work even after AD password reset



UNIT 42
BY PALO ALTO NETWORKS

Easy usecase to spot remote tools

Services with an IP in the Parameters are always interesting.

! Be aware: If they start as system account no password reset will help you out

C:\Program Files (x86)\ScreenConnect Client (8ac59e2ad44a3d74)\ScreenConnect.ClientService.exe "?e=Access&y=Guest&h=176.111.173.134&p=443&s=5c7b4980-87f5-4a11-ad48-b465c6ce0668&k=BgIAAACkAABSU0ExAAgAAAEAAQD9zwzarY9sCx5AURKy%2fzPuquO83sK9ubYqo5LoZ6d4JO%2bqCAYNBV9JPYtKXVXtfPBTJZ8EBnnalLLmNOV8ymvz0oKbhS%2fhWMgX%2bOZIXnHlVCTjb5NupPMoI22NcTOH9TVTKxURQZA%2f3%2b2ptS1pPDi%2b%2bb0gmKqVFAfQXqC3NV23W17tdvM04a4ES4k2KU40%2fZJ%2b6FknSRc5w5sZB7LdIsLZivEHnFheN7YlmKwHFQhq%2blI4%2fP1hcrpHvlNVcJJML7qCDJCRNeZEzFe7hw2RBO6fmjIyODhvqScTaez9NulTuQ1ZC%2bVOQu%2fW%2fFBLkv4m0tqlWtMY4BJfe62EDpaEW8iK&t=&c=hipp.de&c=&c=&c=&c=&c=&c=&c="

UNIT 42
BY PALO ALTO NETWORKS

The other big issues

Reverse Shell

Continuous full access to the box

HTTPS Tunnel

Malware and C2 Commands are hidden from Proxy

No Email Gateway or other means are able to spot malware delivery

UNIT 42
BY PALO ALTO NETWORKS

Dont forget to look everywhere!

Amcache	Process Hash
Shimcache	Process Hash
Crash Dump	ProcessName, Memory Information
Registry Keys	Service Name, Path
Event Logs	Service Name, Path
File Changes	File Names, Hashes
Prefetch	File Name
MFT Table	Deleted File

Canary Tokens

paloalto NETWORKS

UNIT 42
BY PALO ALTO NETWORKS

First steps of an attacker

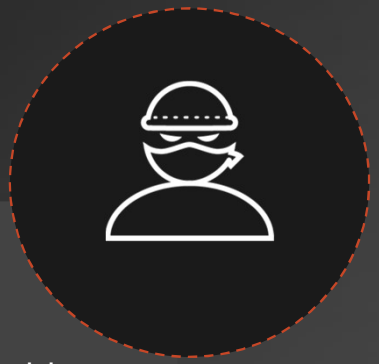
hope of striking easy gold!

Means they check for these things first:

- Locally cached admin credentials
- Locally stored credentials
- Domain Admin Hashes

UNIT 42
BY PALO ALTO NETWORKS

Kerberoasting is super hard to monitor for all accounts!



Create fake domain admin accounts that are never used but still are part of the domain admin.

! Windows event ID 4769 is generated every time the Key Distribution Center (KDC) receives a Kerberos Ticket Granting Service (TGS) ticket request.

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4769

UNIT 42
BY PALO ALTO NETWORKS

Other detection options and fail safe

! Check for
Event ID 4624 and 4625
for the canary tokens.

You do not want your canary to really be abused without noticing it!

UNIT 42
BY PALO ALTO NETWORKS

Password Vault to protect creds

Ransomware searching for higher privileged accounts

Credentials will have a lifetime of 20min.

Nearly impossible to find anything valid, that can be abused.

HOW TO HUNT AN ACTOR THROUGH AN ENTERPRISE?

paloalto NETWORKS

UNIT 42
BY PALO ALTO NETWORKS

What if your IOC is a Pokemon Name and it can be everywhere?

UNIT 42
BY PALO ALTO NETWORKS

Create a short script that searches for something

```
1   $Pokemon = ""
2   $Pokemon = Get-Service -Name "Pikachu"
3   $hostnme = hostname
4
5
6   if ($Pokemon -like "Pikachu") {
7       nslookup $hostname".PokemonService.TestDomaine.de"
8   }
9   else {
10      Write-Host ("nothing found")
11  }
```

UNIT 42
BY PALO ALTO NETWORKS

The DNS Call is forwarded to root

Create failing DNS requests!

Deploy the script in question via GPO to all Endpoints

Requests that can't be handled are always send to the DNS ROOT server.

Collect logs from root DNS Server to find any clients reaching out.