SOPHOS

Shared secret: EDR killers in the kill chain

Gabor Szappanos & Steeve Gaudreault

Steeve Gaudreault:

Senior Threat Researcher @ Sophos

steeve.gaudreault@sophos.com

Gabor Szappanos:

Threat Research Director @ Sophos

gabor.szappanos@sophos.com

SOPHOS


The days before R-Day: ransomware toolsets
Gabor Szappanos
Vikas Singh
Throwback Thursday
SOPHOS
labs
VB2020
localhost
2:18:11 / 4:40:30 • The days before R-Day: ra...

First they came for the

~~JOURNALISTS~~

Your EDR

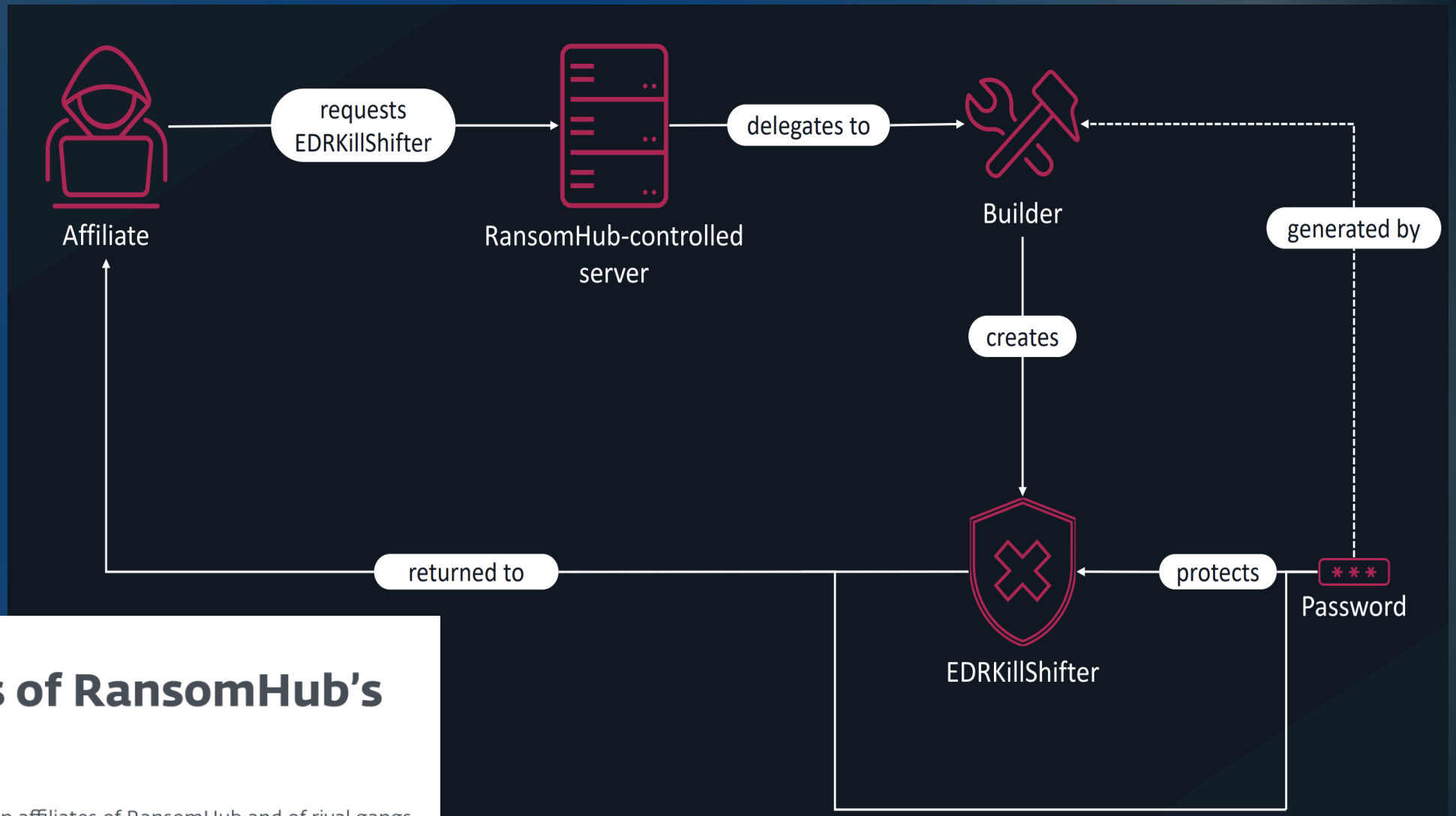
we don’t know

what happened after that

What do we know?

SOPHOS

EDRKillShifter as a Service



ESET Research

Shifting the sands of RansomHub's EDRKillShifter

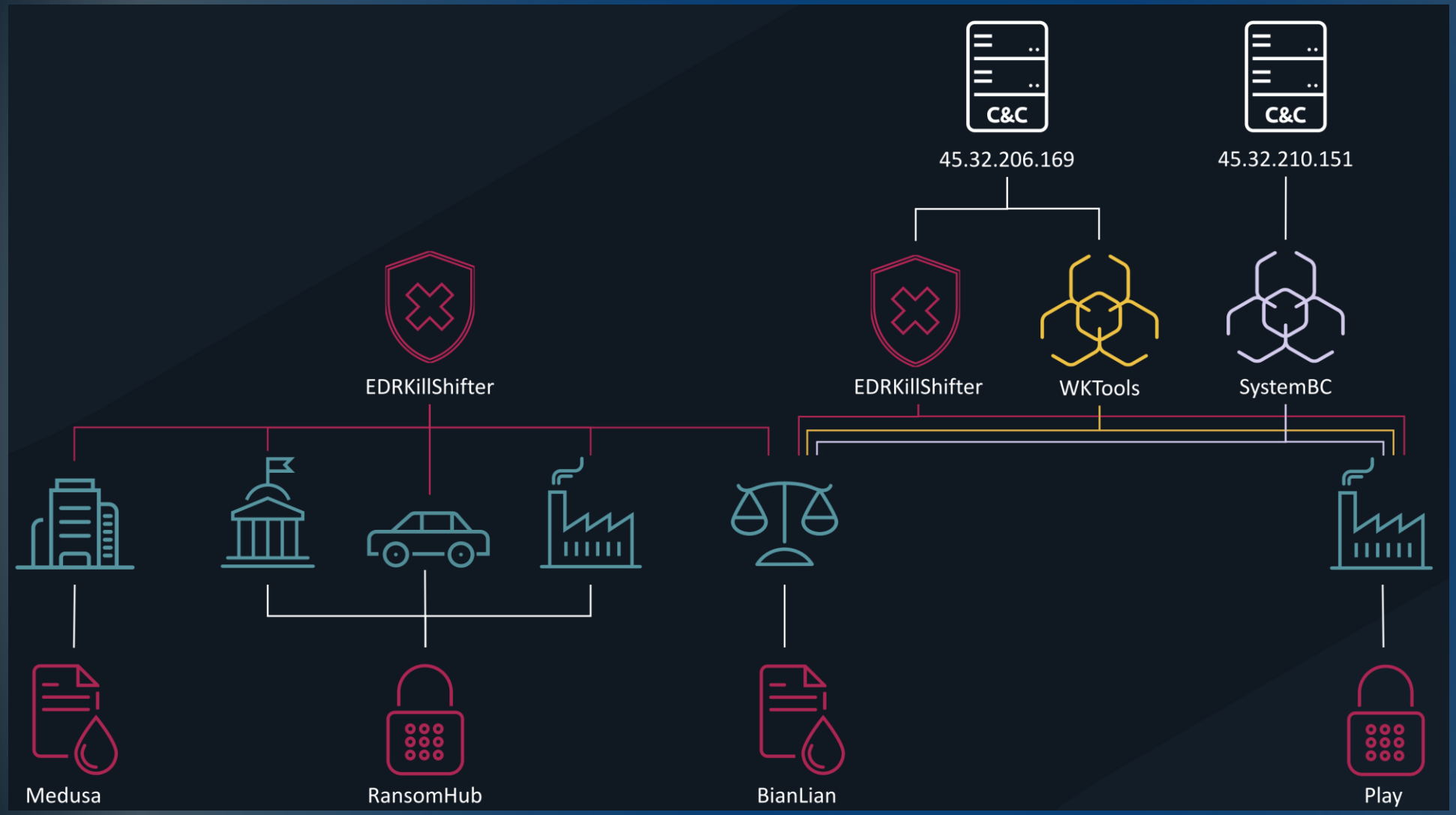
ESET researchers discover new ties between affiliates of RansomHub and of rival gangs Medusa, BianLian, and Play


Jakub Souček


Jan Holman

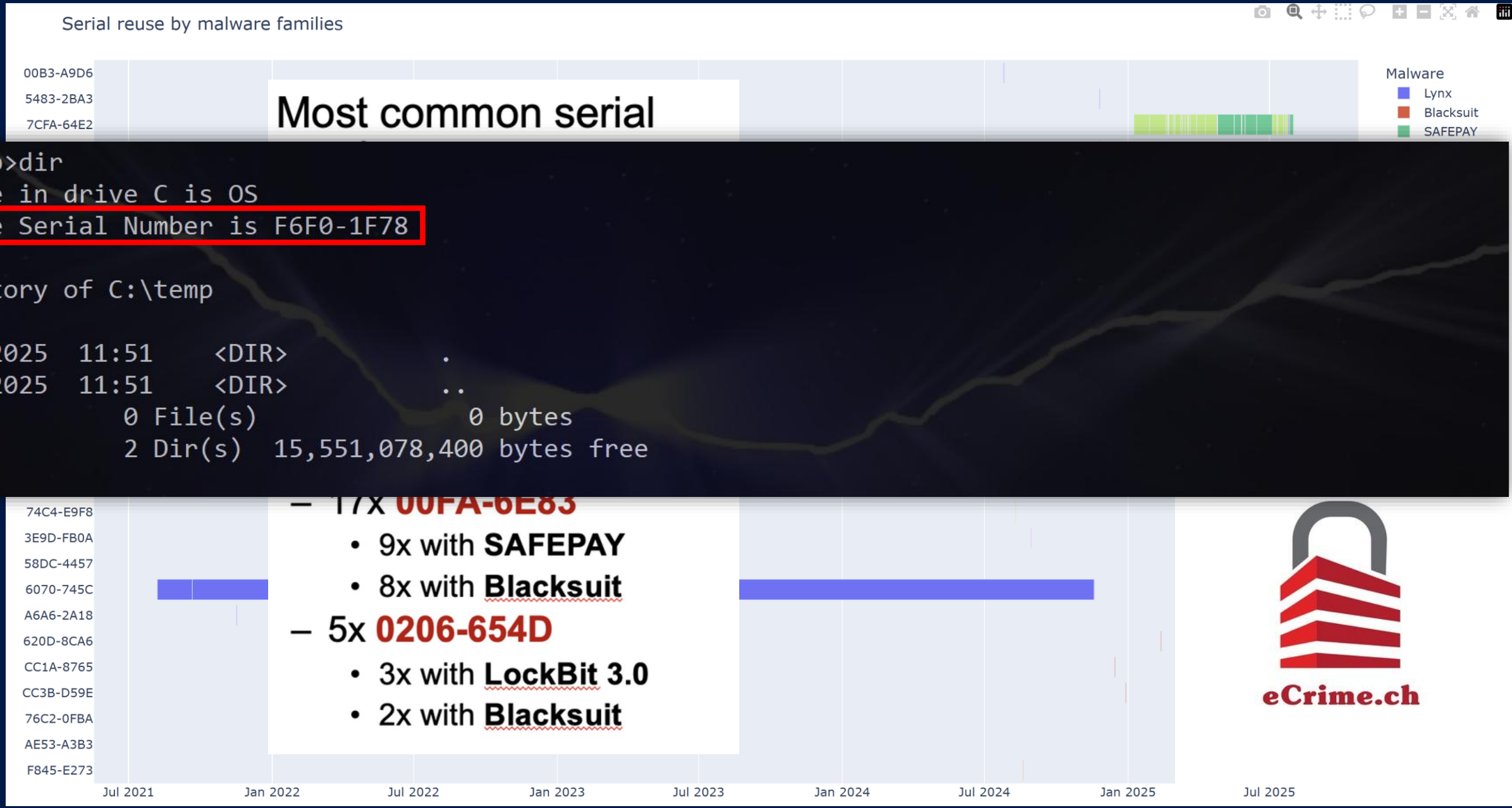
https://www.welivesecurity.com/en/eset-research/shifting-sands-ransomhub-edrkillshifter/

EDRKillShifter running wild



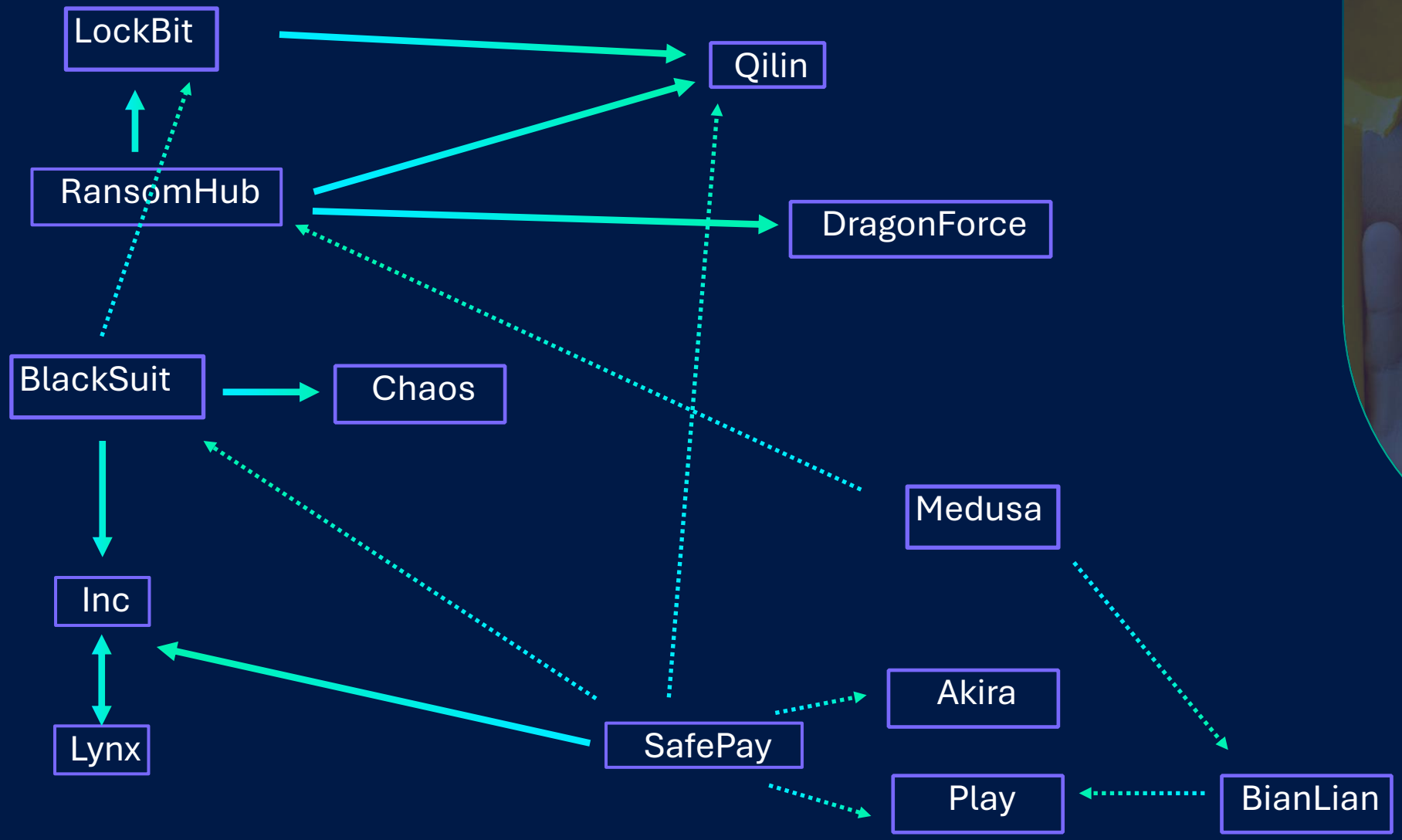
https://www.welivesecurity.com/en/eset-research/shifting-sands-ransomhub-edrkillshifter/

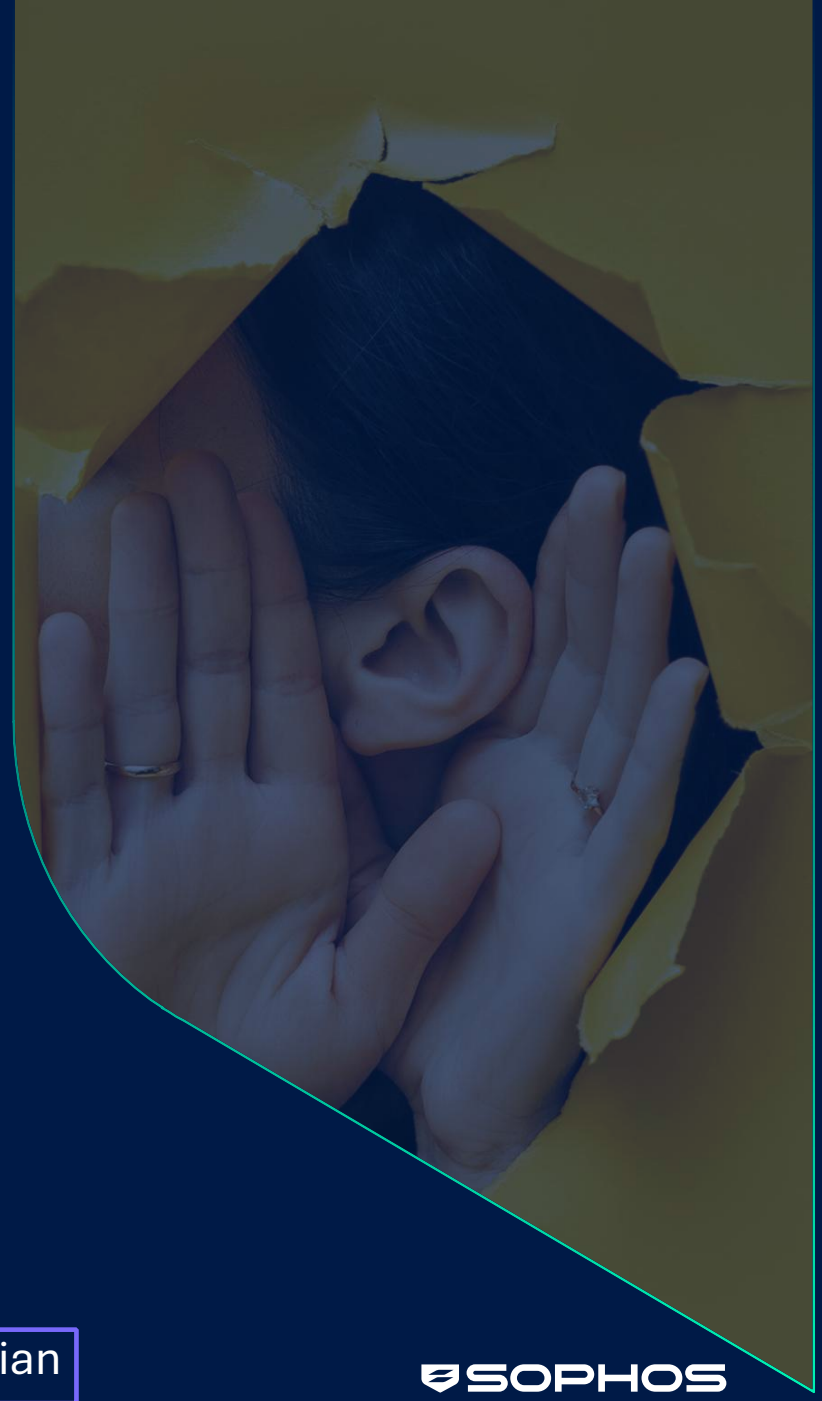
Affiliates are multi-tasking



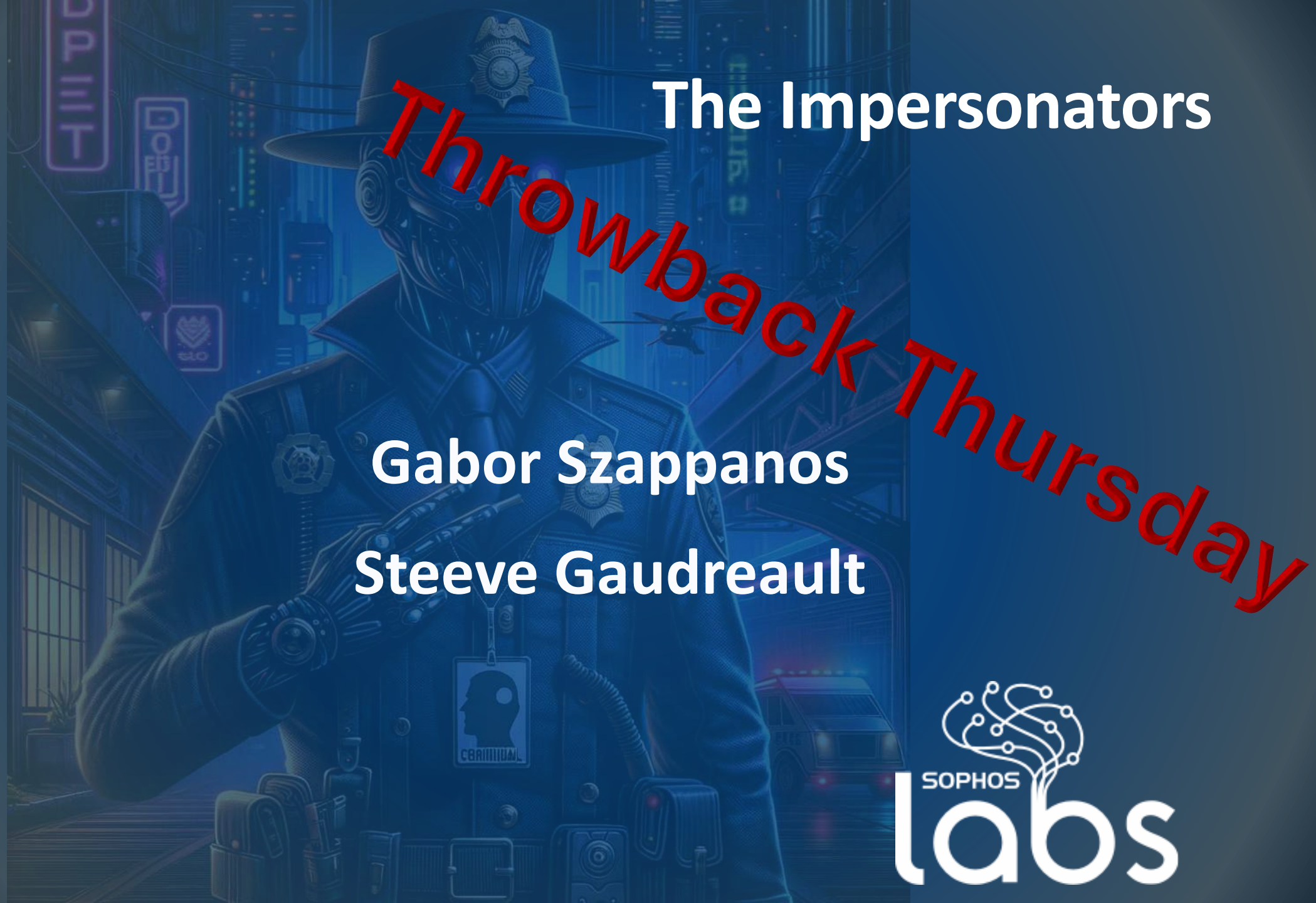

```
C:\temp>dir
 Volume in drive C is OS
 Volume Serial Number is F6F0-1F78

 Directory of C:\temp

22/09/2025  11:51    <DIR>          .
22/09/2025  11:51    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  15,551,078,400 bytes free
```

Known transitions





SOPHOS



The Impersonators

Throwback Thursday

Gabor Szappanos

Steeve Gaudreault

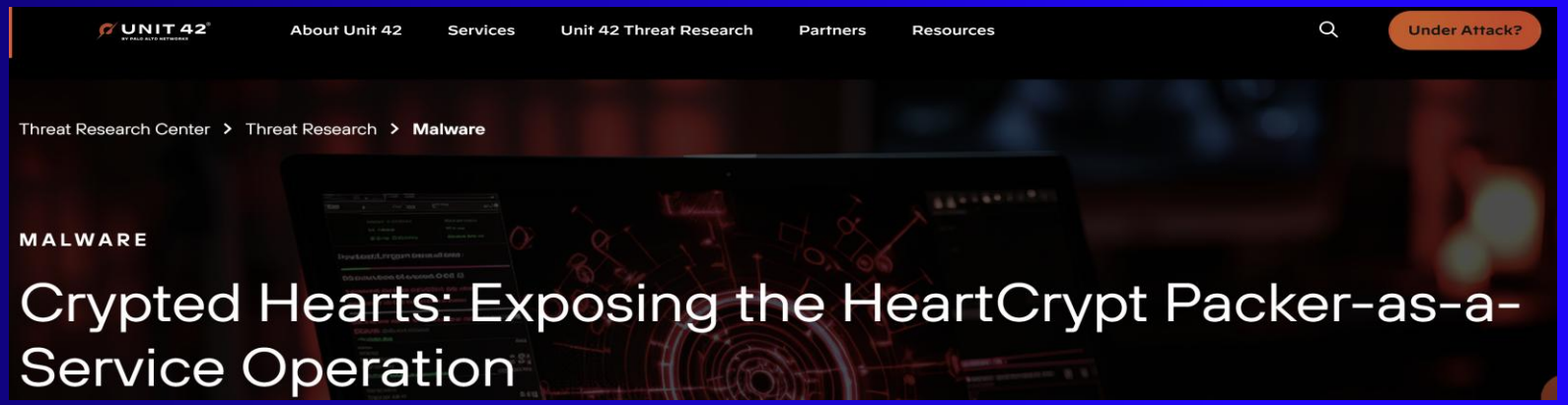
SOPHOS labs

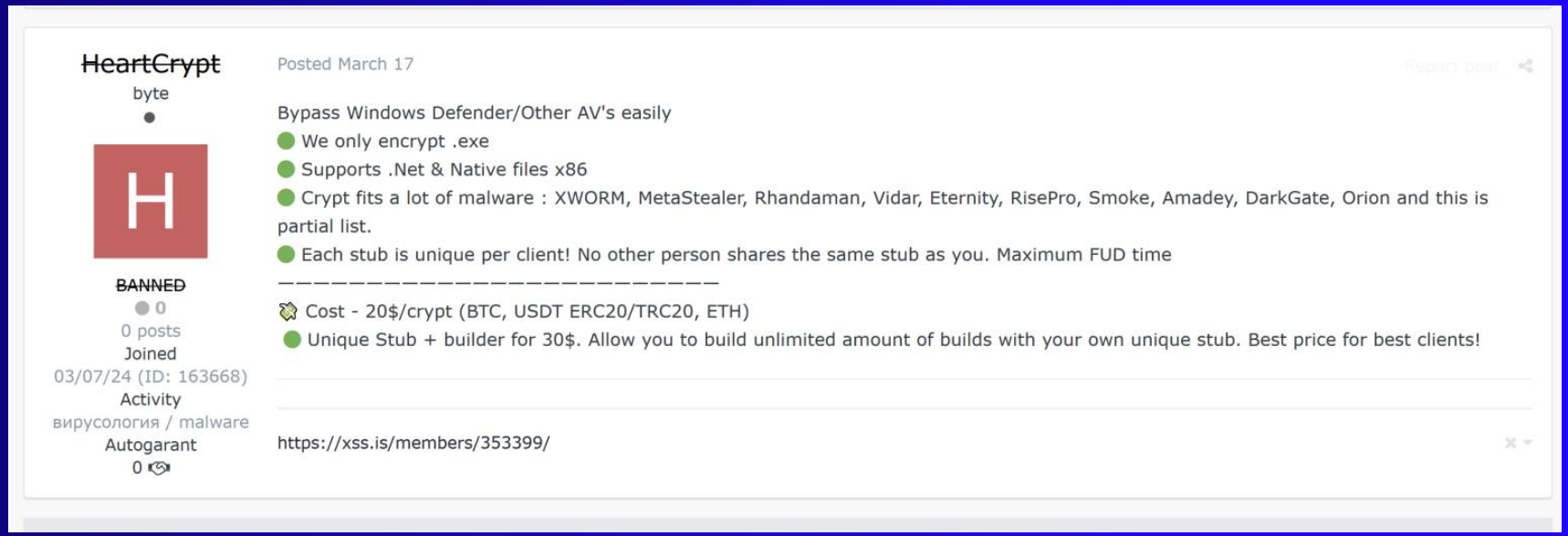
Conclusions

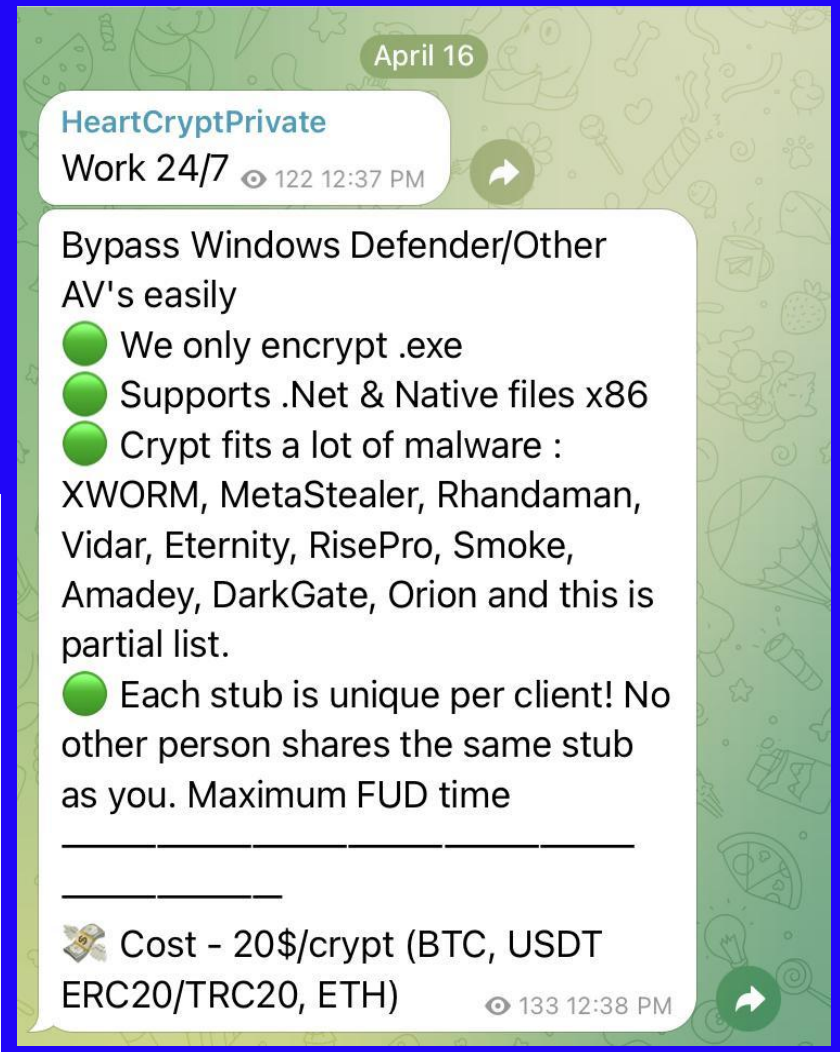
Throwback Thursday

- No, we still don't write viruses
- Just because it looks and smells like it, is not necessarily a legit Sophos program
- None of the affected software vendors were compromised
- Security products are reputable
- Attackers like to abuse this fact
- The threat actor is still active
- Expect similar attacks in the future
  - in fact, we already have (==> AsyncRAT, Redline, Remcos)
- Transparency and detailed disclosure helps to fight against it

HeartCrypt packer as a service







https://unit42.paloaltonetworks.com/packer-as-a-service-heartcrypt-malware/

SOPHOS

Overall stats

2091 modified binaries

first sample: January 2024

last sample: yesterday

230 software vendors

66 hosting URLs

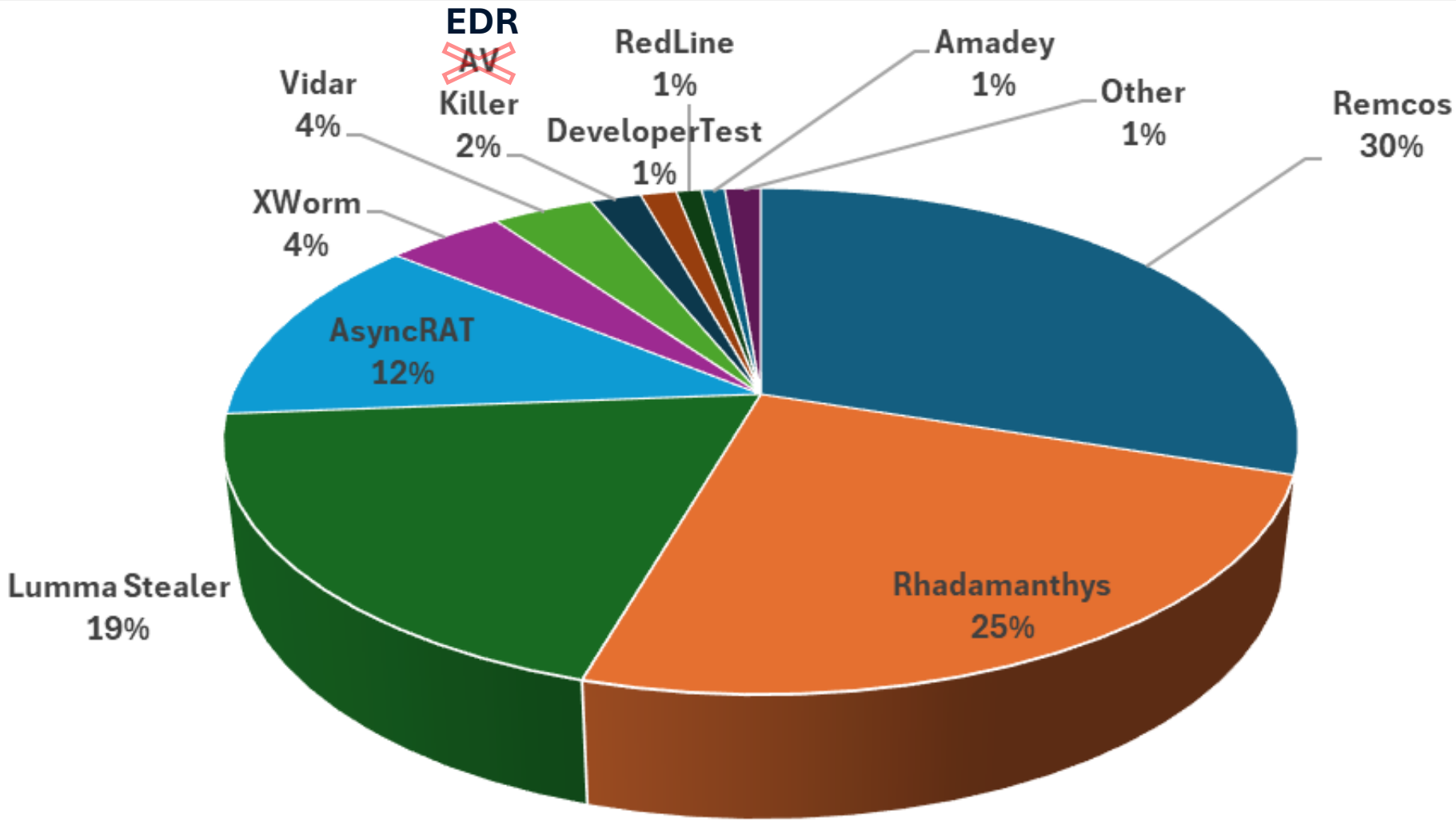
771 C2 servers

2brightsparks
360
3dm
4th_generation
FAST
abacom
abelssoft
acreom
adersoft
adobe
akelsoft
amazon
angus_johnson
apple
ashampoo
asl
asus
atlantis
atto
audacity
autodesk
avanset
avery_lee
bahrani
bandicam
bistone
bittorent
bleeping_computer
blizzard
block_financial
broadcom
burnaware
bytedance
cableguys
caphyon
carebuzz
chaos363
checkpoint
chengdu_chaoyoumao
cholaware
chromium
cisco
citrix
cmclient
code_jelly
codetwo
crashrpt
crow_hill
crypto_pro
crystal_dew
crystal_rich
crystalidea
cubicdesign
curl
cyberlink
cybertron
deepinstinct
deere
dell
destinator
dk1tb
donho
eurotherm
fatih_ramazan_cikan
feiq
free_picture
geomind
girdac
git
github
glarysoft
glenn_delahoy
glib
global_graphics
godot
google
handy
hddguru
hds_hungary
hdtunepro
heaventools
honeygain
hotspot
ibm
identiv
igor_pavlov
indigo_rose
intellution
intuit
iobit
iriun
itruschina
ivan219
kadokawa
kc_softwares
kirikiri
klauncher
ledstatus
lespeed
lucasarts
macromedia
matrin_prikryl
mazov_gosha
mehatronika
merops
microsoft
mirage
mister_group
mkvtoolnix
monero
mserver
myplaycity
nefarius
nero
nhc
nitro
novosoft
nw.js
ok_soft
onesoft
opencv
openssl
opera
oracle
other
parus
pc_software_accounting
piotr_pawlowski
piriform
plants_vs_zombies
plus
pmg_pte
popcap
premiumsoft
projekt_red
proton
qt
qualys
quickheal
razer
roblox
rockhip
rovio
ruiware
sacred
safer_networking
samsung
sap
scooter
se7en
searchinform
seiko
sergey_klochkov
simpli
skyriver
sordum
starlight
stegano
stormcoast
symantec
syncios
sysinternals
teamviewer
tefincom
telegram
tencent
think_cell
tiger_brokers
toby_fox
tonec
tornillo
treesitter
trellix
trendmicro
truecrypt
tuttop
twitch
ubisoft
undertale
unifab.ai
unity
valve
ventoy
veracrypt
videloan
watchguard
wide_angle
wisecleaner
x2game
yandex
yenling
yoyo
zamar
zenproductions
zhorn
zoom

Most common payloads

- *Remcos*
- *Rhadamanthys*
- *Lumma Stealer*
- *AsyncRAT*
- *XWorm*
- *Vidar*
- ***~~AV~~ EDR Killer***
- *DeveloperTest*
- *RedLine*
- *Amadey*
- *DarkGate*
- *Bladabindi*
- *Icarus Stealer*
- *GhostSocks*
- *Venom*
- *Lumar*

- *Phemedrone Stealer*
- *DiscoStealer*
- *DiabloMiner*
- *StormKitty*
- *StealC*



Payload: ~~AV~~ EDR killer

Host	Defense Evasion	Look for unusual service installations, especially of kernel drivers, in windows logs. In this particular case, Cylerian identified a service name containing 5 random characters and the driver signed by "Changsha Hengxiang Information Technology Co., Ltd.".

Threat Intelligence
@threatintel

Multiple new variants of a malicious driver that first surfaced in 2022 are circulating in the wild. The driver is used by attackers to attempt to disable security solutions. #ransomware #threatintelligence (1 of 3)

4:11 PM · Jan 16, 2025 · **2,169** Views

2 5 9 2

Post your reply Reply

Threat Intelligence @threatintel · Jan 16
File hashes
6d8209114aa52d28c18d5789efbb873fc131d56b538c5747d713a2d7a5447e22
77360c4a82229349cb1b9e105b7f5618a10848a8ef9beb5d6d0bd21e86f3527b
20f5e210d87c10eb9deb7b93c29da3bbae8b3c4bbe5bfefd3d2e16e94df0bf20 (2 of 3)

1 2 2 889

Threat Intelligence @threatintel · Jan 16
99a2c5b7224d537c768035ffdf6066330509b6541f750ec3ad0ffd92bfe3199e
3fbe5a1ed857a6736e061a6850706f9e8a7e881f024bff044df1c34795b89bf4 (3 of 3)

https://x.com/threatintel/status/1879909266250932226
https://www.cylerian.com/blog/t_2024_10_24_inside_the_attack/

SOPHOS

ScorchedHeart overview

- Heavily protected code
- Looks for a driver with 5-letter random name
- Driver is signed with compromised certificate
- Multiple security vendors targeted by:
  - Deleting *.EXE files in AV install directory
  - Killing running processes and services
- The list varies with samples

```
aDestroyDriverA:
                text "UTF-16LE", '[*] Destroy driver ability [%ws]:',0Ah,0
                align 4
aDestroyDriverD:
                text "UTF-16LE", '[*] Destroy driver dispatch func [%ws]:',0Ah,0
                align 4
aDestroyDriverA_0:
                text "UTF-16LE", '[*] Destroy driver all system thread [%ws]:',0Ah,0
                db    0
aMramlSys       db 'mraml.sys',0
```

ScorchedHeart targets

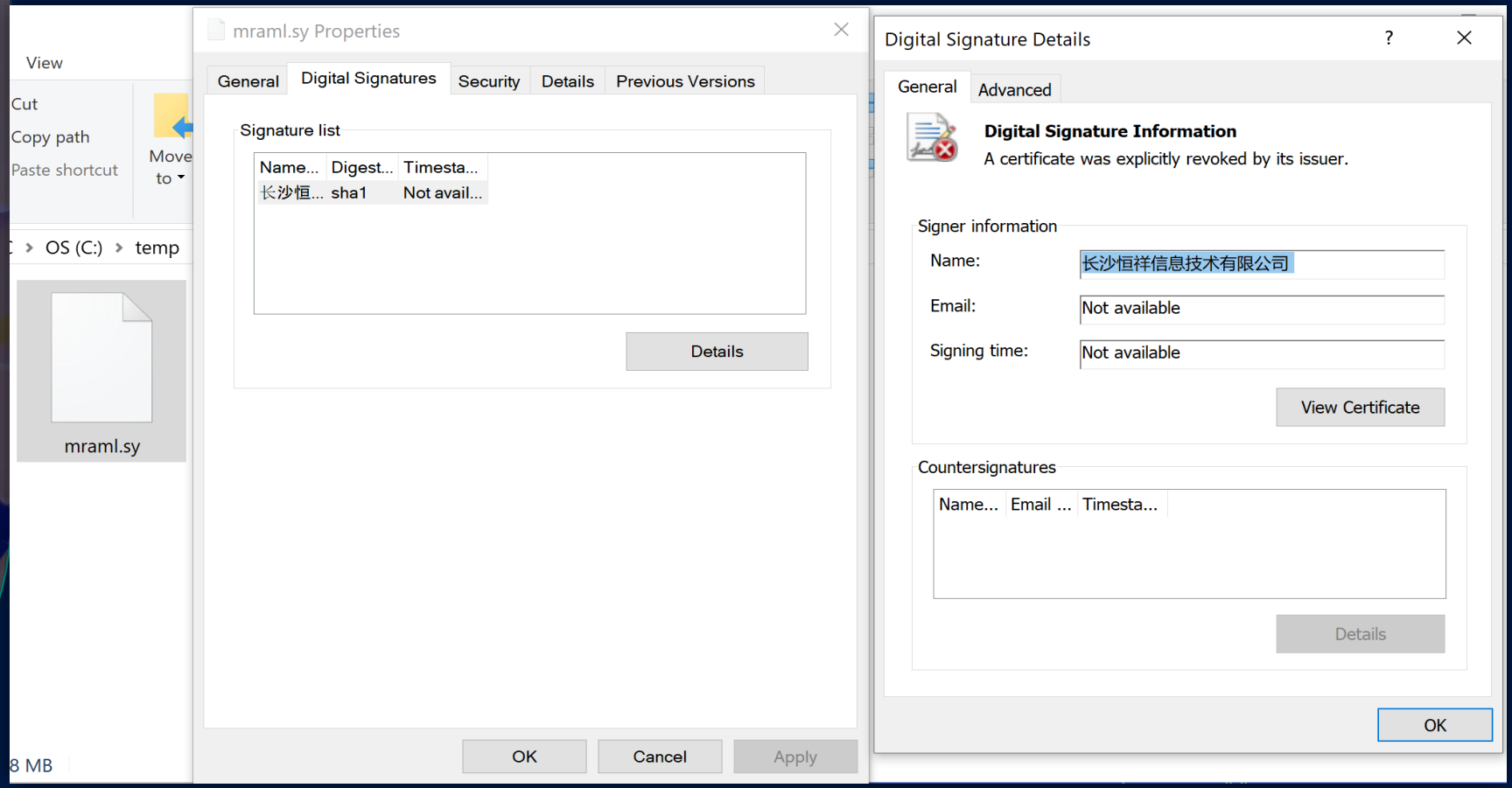
```
aCProgramFilesS:
                text "UTF-16LE",
aCProgramFilesX:
                text "UTF-16LE",
aCProgramFilesX_0:
                text "UTF-16LE",
                align 10h
aCProgramFilesH:
                text "UTF-16LE",
```

```
aCProgramFilesE:
                text "UTF-16LE", 'C:\Program Files\ESET',0
aDll:
                text "UTF-16LE", '.dll',0
                dw 0
aCProgramFilesX:
                text "UTF-16LE", 'C:\Program Files (x86)\Symantec',0
aCProgramFilesS:
                text "UTF-16LE", 'C:\Program Files\Symantec',0
aCProgramFilesS_0:
                text "UTF-16LE", 'C:\Program Files\Sophos',0
aCProgramFilesX_0:
                text "UTF-16LE", 'C:\Program Files (x86)\Sophos',0
aCProgramFilesX_1:
                text "UTF-16LE", 'C:\Program Files (x86)\HitmanPro.alert',0
                dw 0
aCProgramFilesH:
                text "UTF-16LE", 'C:\Program Files\HitmanPro',0
                dw 0
aCProgramFilesW:
                text "UTF-16LE", 'C:\program files\Webroot',0
                dw 0
aCProgramFilesX_2:
                text "UTF-16LE", 'C:\Program Files (x86)\Webroot',0
                dw 0
aCProgramFilesX_3:
                text "UTF-16LE", 'C:\Program Files (x86)\Kaspersky Lab',0
```

ScorchedHeart targets

- Bitdefender
- Cylance
- Eset
- F-Secure
- Fortinet
- HitManPro
- Kaspersky
- McAfee
- Microsoft
- SentinelOne
- Sophos
- Symantec
- Trend Micro
- Webroot

ScorchedHeart driver signature



Name: *Changsha Hengxiang Information Technology Co., Ltd.*
Valid From: *12:00 AM 03/20/2015*
Valid To: *11:59 PM 03/19/2016*
Thumbprint: *7749BE16F266669D505684E9F002C689706C4295*
Serial Number: *75 E8 E7 B9 04 3B 13 DF 60 E7 64 99 66 30 21 C1*

SOPHOS

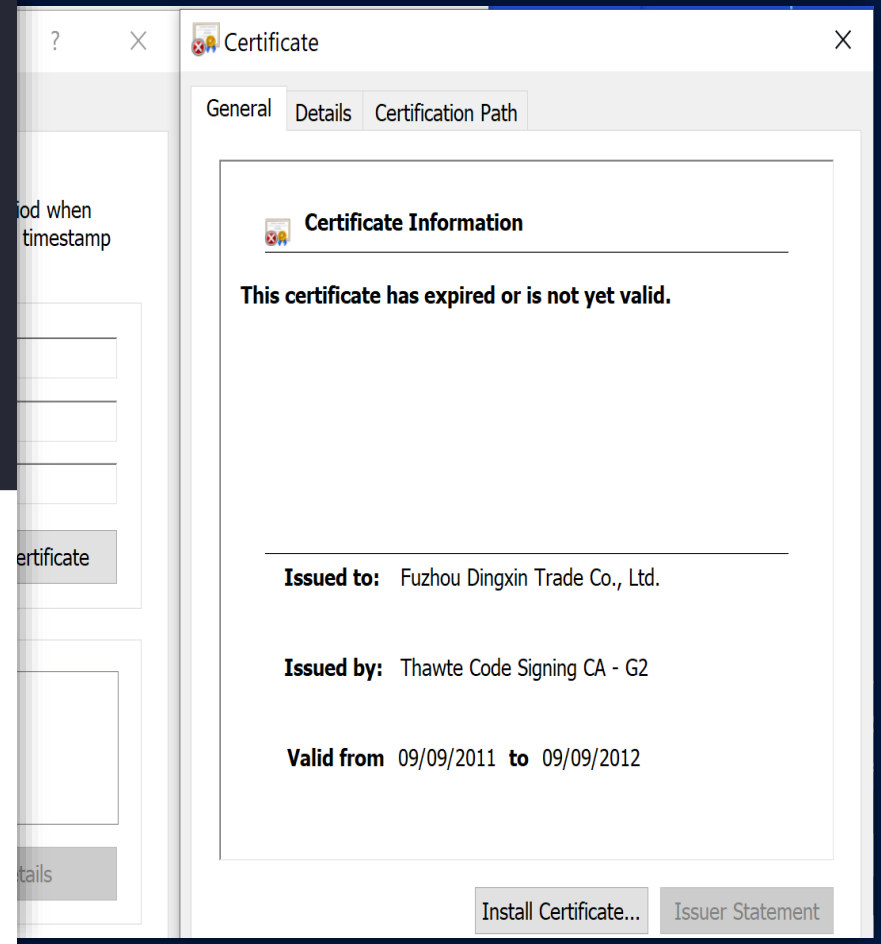
hen a new signature

aon.com/en/insights/cyber-labs/bypassing-edr-through-retrosigned-drivers-and-system-time-manipulation

September 13, 2024 / 9 mins

Bypassing EDR through Retrosigned Drivers and System Time Manipulation

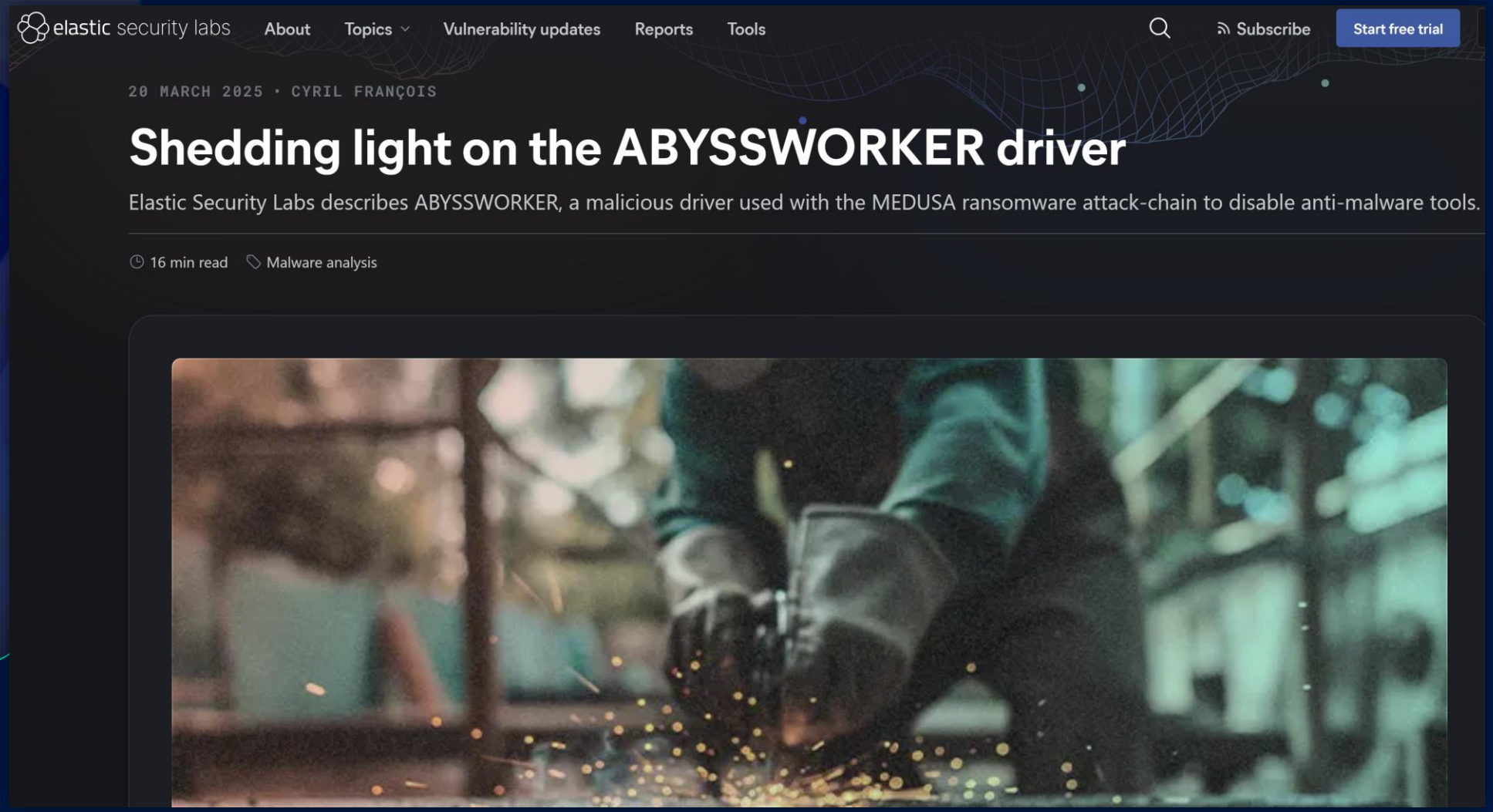
The Retrosigned Driver EDR Bypass is a novel modification of a technique employed by multiple ransomware groups to bypass EDR and limit visibility into malicious actions by abusing expired code signing certificates to load malicious kernel drivers.



Name: *Fuzhou Dingxin Trade Co., Ltd.*
Valid From: *01:00 09/09/2011*
Valid To: *00:59 09/09/2012*
Thumbprint: *D01B544CF4A4F901FA496BEA2B3A8F66F9583CB2*
Serial Number: *72 88 1F 10 CD 24 8A 33 E6 12 43 A9 E1 50 EC 1D*

SOPHOS

ABYSSWORKER/POORTRY/BURNTCIGAR



https://www.elastic.co/security-labs/abyssworker
https://www.linkedin.com/pulse/attackers-leveraging-microsoft-teams-defaults-quick-assist-p1u5c/

SOPHOS

Ransomware connection

ScorchedHeart deployed

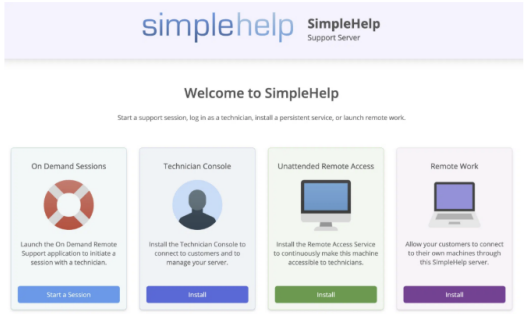
Mitigation DynamicShellcode
Timestamp 2025-01-22T09:53:42
Path: c:\temp\6Vwq.exe
SHA-256: 43cd3f8675e25816619f7

Process Trace
1 C:\temp\6Vwq.exe
2 2 cmd.exe /c start c:\temp\6Vwq.e
3 C:\ProgramData\JWrapper-Remot
complete\bin\Remote Access.exe

Followed by Medusa

Detection: Mal/Medusa-C
Path: <d>/Windows/Temp/MilanoSoft
SHA-256: 3a6d5694eec724726efa332

HORIZON3.ai Solutions Partners Resources Company



Critical Vulnerabilities in SimpleHelp Remote Support Software

Naveen Sunkavally | January 13, 2025 | Attack Blogs, Disclosures

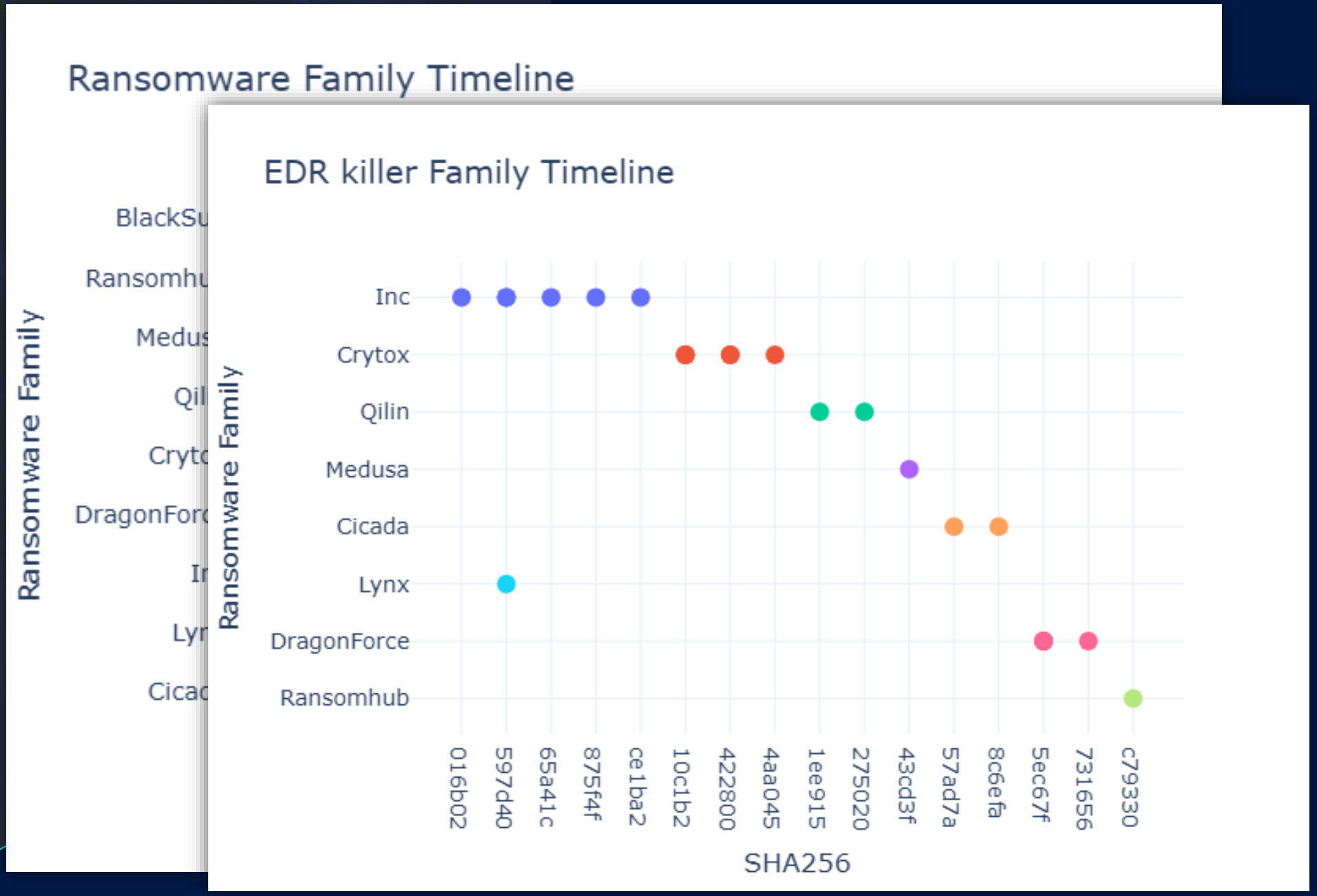
Summary

2024 was bookended by notable zero-day vulnerabilities affecting popular remote support/access software: CVE-2024-1708 and CVE-2024-1709 affecting ConnectWise ScreenConnect and CVE-2024-12356 and CVE-2024-12686 affecting BeyondTrust products. These vulnerabilities were exploited in the wild and are on CISA's list of Known Exploited Vulnerabilities.

We were curious to see what other remote support software was out there and came across a tool called SimpleHelp. While we hadn't heard of it before, we found it being used by a number of our users, and it has a decent presence on the Internet.

SOPHOS

ScorchedHeart and ransomware



- Blacksuit
- RansomHub
- Medusa
- Qilin
- Dragonforce
- Crytox
- Lynx
- INC
- Cicada

First seen:
2024-12-18
Last seen:
2025-08-18

SOPHOS

What comes next?

Why Shanya?

PE64 | Sections | ANSI | Unicode | Null-terminated | Links | 10 | RegExp | Save | Search

Number	Offset	Address		Size	Typ	String
Filter	Filter	Filter	Filter	Filter	F…	Filter
0	00001016	0000000140…	Section(0)…	21	U	-1001_Classes\Applications\%1.exe
1	00001ac4	0000000140…	Section(0)…	44	U	C:\Users\crash0ut\Desktop\cryptor_src\x64\Release\shanya_crypter.exe
2	001c68f0	0000000140…	Section(1)…	0d	U	XmB3g6XQlgfe1
3	001c6910	0000000140…	Section(1)…	1c	U	j36FkY4c bnFOi Vulcanologist
4	001c6950	0000000140…	Section(1)…	0c	U	vulnose Lass

```
;
; Export Address Table for 5h4ny4_fuck4v_0x000735A5BFC229C.dll
;
off_1015D118    dd rva RtwqAddPeriodicCallback, rva RtwqAllocateSerialWorkQueue
                                        ; DATA XREF: .rdata:1015D10C↑o
                dd rva RtwqAllocateWorkQueue, rva RtwqBeginRegisterWorkQueueWithMMCSS ; "\\\\.\\GLOBALROOT\\SystemRoot\\SysWOW64"
                dd rva RtwqBeginUnregisterWorkQueueWithMMCSS, rva RtwqCancelDeadline
                dd rva RtwqCancelMultipleWaitingWorkItem, rva RtwqCancelWorkItem
                dd rva RtwqCreateAsyncResult, rva RtwqEndRegisterWorkQueueWithMMCSS
                dd rva RtwqEndUnregisterWorkQueueWithMMCSS, rva RtwqGetPlatform
                dd rva RtwqGetWorkQueueMMCSSClass, rva RtwqGetWorkQueueMMCSSPriority
                dd rva RtwqGetWorkQueueMMCSSTaskId, rva RtwqInvokeCallback
                dd rva RtwqJoinWorkQueue, rva RtwqLockPlatform, rva RtwqLockSharedWorkQueue
```

DLL names in early samples:

5h4ny4_fuck4v_0x000735A5BFC229C.dll
sh4nya_fuck4v_0x000CFA853F46C84.dll
shanya_fuckav_0x0001DC90D59DCDBE.dll

What is Shanya? – AKA Armillaria Loader

Armillaria Loader

In early May a sample was uploaded to VirusTotal which was detected as BumbleBee malware. Analysis of the sample indicates it is a new loader, which we are calling Armillaria, that was observed loading BumbleBee, ChuChuka Implant, Lumma Stealer, Stealc Stealer, WHT Downloader, and some of threat researcher Hasherezade's open-source tools.

Armillaria employs anti-analysis techniques including the use of junk code to inflate the size of the entry function, which was observed to prevent a decompiler from analyzing the function.

The loader also dynamically resolves APIs using a custom add-polynomial hashing algorithm, where:

- the polynomial varies per sample
- the string is converted to lower-case
- the first character is ignored
- the null-terminator is included

As part of the loading sequence:

- Structures are created which contain information about two (2) buffers, the first including a decryption function and the first portion of the encrypted payload, and the second containing the second portion of the payload.
- Size and take-skip encoding parameters are masked in the structure, and the mask is different per buffer. This information is unmasked during runtime.
- If the flag for take-skip on a buffer is set, the buffer is first take-skip decoded before being combined with the other segment.
    - The take-skip is updated each round using a set of arithmetic operations that vary per sample.
- After being combined, the data is decoded using a series of seeded arithmetic operations that vary per sample, where the seed is updated each round.

The initial payload is a Donut shellcode variant which uses Halo's Gate to check if Windows API's are hooked and has differences in the configuration structure when compared to the base repository and it's various versions.

Payloads:

- *BumbleBee*
- *ChuChuka*
- *Lumma*
- *WHT downloader*
- StealC
- ~~AV~~ EDR Killer
- CastleRAT

https://www.ciphertechsolutions.com/acce-release-notes-v2-9-20250602/

Who is Shanya?

Some of the features:

- ***Non-standard module loading into memory**, wrapper over the system loaderStub uniqueization.*
- *Each customer receives their own **(relatively) unique stub** with a **unique encryption algorithm upon purchase**.*
- ***AMSI bypass for your .NET assemblies**; the payload is not detected in memory.Icons,*

VX Crypt by Shan

ID: 6768dddeb4103b69c
Thread ID: 123986
Created: 2024-10-02T1
Last Post: 2024-12-18
Author: Kernel32dll
Replies: 15 Views: 3K

Контакты:

PM


```
![t.me](/proxy.php?image=https%3A%2F%2Fcdn4.cdn- telegram.org%2Ffile%2FH_WsdJvbDXTbX038LNVxtroaoNG3Hk-_Lkmb8bjinQ263hEJa7vG_JEJDuKwbFHCO_DNppq5co7B_9XRQGVnpwMpCjhocAxmsyg7GOYKKtI70KKGn3vHwq0Ly2IAq_wZR-71fDen6hBpiOAK2kjw3Rdvu6I8Burvc8FuWcJC7AEfy0xkg4ziQSpUyV_1U1tyuZCP2p6AjXMUtoPkS2QTzTHT6JdtZ8V_bVoMMXnlnF-Ta2IdjjJSEUkzSymNUtizyfgyaDyfYYDgYTELhGa1vD-icKfAv8N8rZUwDSv-ircBByRK0Dbb3C57DpzwXoiU6fBTjLic7w2LaY7uhtmz3w.jpg&hash=67f0effccad9ba0c3bce1b3ac23c009a&return_error=1)
```


Shanya

You can contact @shanya0xff right away.

1. Обход SmartScreen не гарантирован. Используйте chk/nta/другие скрипты для обхода, ставьте сертификаты, прогревайте файл, но смартскрин я не смогу обойти, можем попробовать Sideloading
2. Рантайм. В большинстве случаев, если ваш софт обновляется, с рантаймом не должно возникнуть проблем. Можем попробовать решить проблему мем-детектов если ваш файл x32 и нативный, но Mimikatz я вам без детектов в рантайме не запущу :P
3. Обход Chrome. Не надейтесь на то, что с обычным криптом вы сможете грузить файл по Direct-ссылке. Используйте архивацию, доверенные домены, другие методы доставки. Как правило, если файлообменник доверенный и вы не заливаете файл без архива, Chrome пропускает файл
4. Стабы не стучат по СНГ, ex-СНГ (no CIS)

SOPHOS

EDR Killer AKA Shanyageddon

Used in DLL side loading:

- consent.exe (clean Microsoft program)
- msimg32.dll (Shanya packed malicious DLL)

Drops kernel drivers:

- ThrottleStop.sys/rwdrv.sys (vulnerable driver by TechPowerUp)
- hlpdrv.sys (malicious kernel driver)

```
if ( (int)sub_140006490(*(_QWORD *)(v23 + 4088), v24, v25, 10) < 0
  || !(unsigned __int8)write_to_file(
                         (__int64)&throttlestop_embedded,



{
  return 0i64;
}
```

```
if ( (unsigned __int8)write_to_file((__int64)&hlpdrv_embedded, 0x2400u, (__int64)L"KMHLPSVC", (__int64)L"hlpdrv.sys") )
{
  hDevice = CreateFileW(L"\\\\.\\KMHLPDRV", 0x40000000u, 2u, 0i64, 3u, 0x80u, 0i64);
  if ( hDevice )
  {
    v87 = 0i64;
    *(_OWORD *)lpMem = 0i64;
    sub_140003830(lpMem);
    v77 = (__int64 *)lpMem[1];
    v78 = (__int64 *)lpMem[0];
    if ( lpMem[0] != lpMem[1] )
    {
      do
      {
        InBuffer = *v78;
        if ( !DeviceIoControl(hDevice, 0x222008u, &InBuffer, 8u, 0i64, 0, BytesReturned, 0i64) )
```

Shanyageddon

The killer loads the drives and passes the service and process names

```
v6 = driver_list;
v7 = 0i64;
if ( driver_list )
{
  while ( !StrStrIA(v5, v6) )
  {
    v6 = (&driver_list)[++v7];
    if ( !v6 )
      goto LABEL_14;
  }
  LODWORD(v18) = 0;
  memset(v17, 0, 0x10ui64);
  v8 = sub_140005750(a1);
  if ( !v8 )
  {
    MessageBoxA(
      0i64,
      "CRITICAL ERROR!!! TELL CODER IF IT'S APPEARED!",
      "CRITICAL ERROR!!! TELL CODER IF IT'S APPEARED!",
      0);
LABEL_13:
    ((void (__fastcall __noreturn *)(__int64))sub_140009
  }
  v9 = qword_140051008;
  v17[0] = v8;
  v17[1] = qword_140051000;
  v10 = get_PEB();
  if ( !(unsigned int)sub_140001480(
                        (unsigned int)*(_QWORD *)&v10[4]
                        v11,
                        v12,
                        v9,
                        v14,
                        (__int64)v17,
                        16i64,
                        v15,
                        v16,
                        (__int64)&v18) )
```

```
driver_list     dq offset aKlflt        ; DATA XREF: sub_140002310+18↑o
                                        ; sub_140002310+91↑r ...
                                        ; "klflt"
                dq offset aKlhk         ; "klhk"
                dq offset aKlif         ; "klif"
```

```
process_list    dq offset aMpcmdrunExe  ; DATA XREF: sub_140003830+24E↑r
                                        ; sub_140003830+255↑o ...
                                        ; "MpCmdRun.exe"
                dq offset aMsmpengExe   ; "MsMpEng.exe"
                dq offset aMsmpengcpExe ; "MsMpEngCP.exe"
                dq offset aMssenseExe   ; "MsSense.exe"
                dq offset aSecurityhealth ; "SecurityHealthService.exe"
                dq offset aUhssvcExe    ; "uhssvc.exe"
                dq offset aAvpExe       ; "avp.exe"
                dq offset aKlnagentExe  ; "klnagent.exe"
                dq offset aAvpsusExe    ; "avpsus.exe"
                dq offset aAvpuiExe     ; "avpui.exe"
                dq offset aKavfsExe     ; "kavfs.exe"
                dq offset aKavfsgtExe   ; "kavfsgt.exe"
                dq offset aKavfswhExe   ; "kavfswh.exe"
                dq offset aKavfswpExe   ; "kavfswp.exe"
                dq offset aKavtrayExe   ; "kavtray.exe"
                dq offset aEbloaderExe  ; "ebloader.exe"
                dq offset aKlcsldclExe  ; "klcsldcl.exe"
                dq offset aSoyuzExe     ; "soyuz.exe"
                dq offset aProtonExe    ; "proton.exe"
                dq offset aVapmExe      ; "vapm.exe"
                dq offset aSedserviceExe ; "SEDService.exe"
                dq offset aHmpalertExe  ; "hmpalert.exe"
                dq offset aSspserviceExe ; "SSPService.exe"
                dq offset aSophosntpservi ; "SophosNtpService.exe"
                dq offset aSophosnetfilte ; "SophosNetFilter.exe"
                dq offset aMcsagentExe  ; "McsAgent.exe"
                dq offset aMcsclientExe ; "McsClient.exe"
                dq offset aSophosfsExe  ; "SophosFS.exe"
                dq offset aSophosfilescan ; "SophosFileScanner.exe"
                dq offset aSophoshealthEx ; "SophosHealth.exe"
                dq offset aSophosEncrypti ; "Sophos.Encryption.BitLockerService.exe"
```

```
t.KES"
_arkmon"
"
_swmon"
sdk_arkmon"
64"
"
EV"
```

Shanyageddon

Malicious driver kills services and processes

```
  DbgPrint("HandleIoctl: PsLookupProcessByProcessId pid:0x%x\n", *(_QWORD *)&MasterIrp->Type);
  v8 = PsLookupProcessByProcessId(v7, &Process);
  v6 = v8;
  if ( v8 )
  {
LABEL_20:
    DbgPrint("HandleIoctl: PsLookupProcessByProcessId failed with status 0x%x\n", v8);
    goto LABEL_16;
  }
  v9 = CopyProcessImagePath(Process, SourceString, 2048i64);
  v6 = v9;
  if ( v9 )
  {
    DbgPrint("HandleIoctl: GetProcessImagePathByPEProcess failed with status 0x%x\n", v9);
  }
  else
  {
    RtlInitUnicodeString(&DestinationString, SourceString);
    v10 = set_file_DACL(&DestinationString);
    v6 = v10;
    if ( v10 )
    {
      DbgPrint("HandleIoctl: UntrustFile failed with status 0x%x\n", v10);
    }
    else
    {
      v11 = zwterminateprocess(Process);
      v6 = v11;
      if ( v11 )
        DbgPrint("HandleIoctl: TerminateProcessByPID failed with status 0x%x\n", v11);
```

EDR Killer AKA Shanyageddon

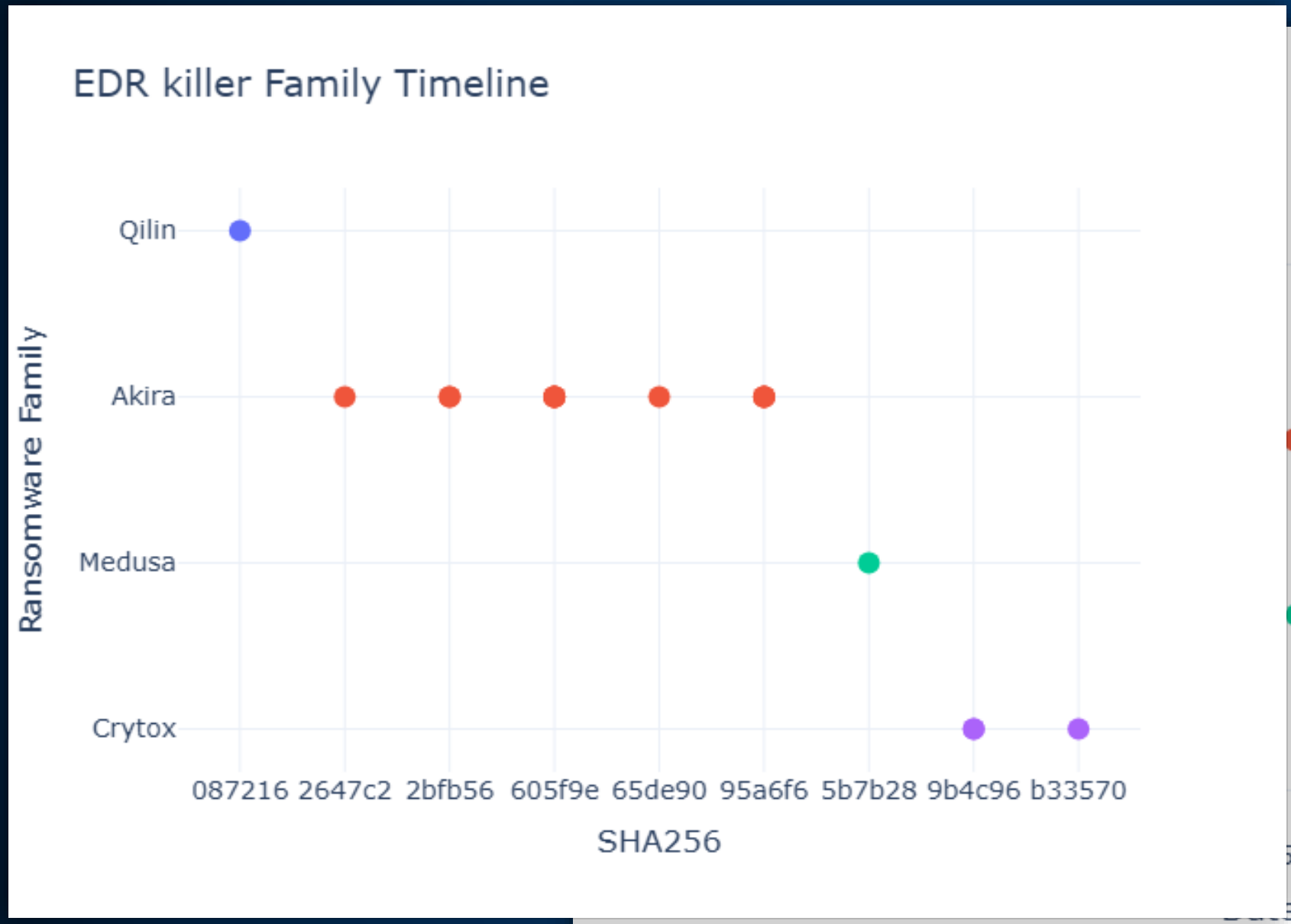
Seen with ransomware families:

- Medusa
- Akira
- Qilin
- Crytox

First seen:
2025-04-29

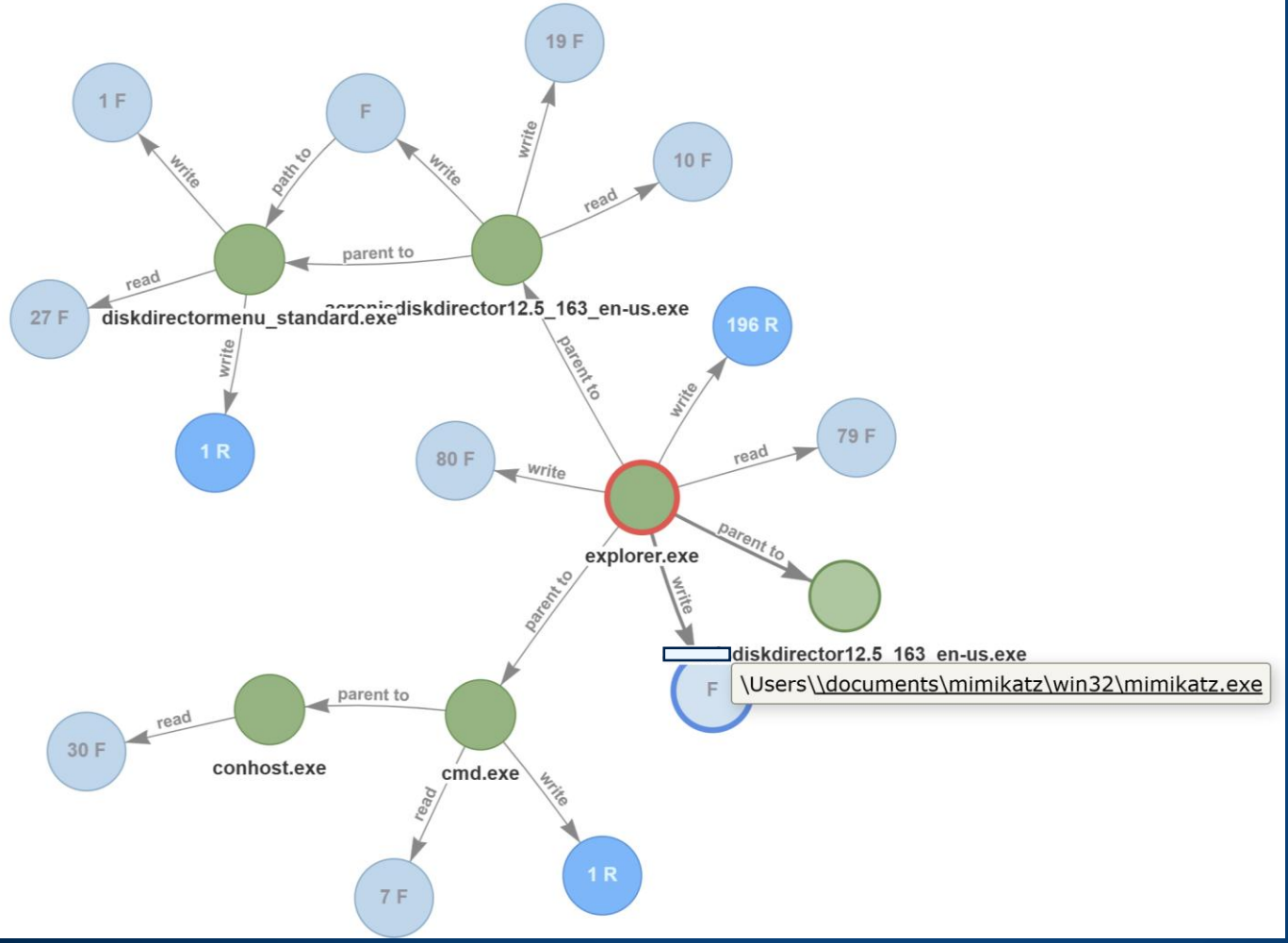
Last seen:
2025-09-09

EDR Killer AKA Shanyageddon



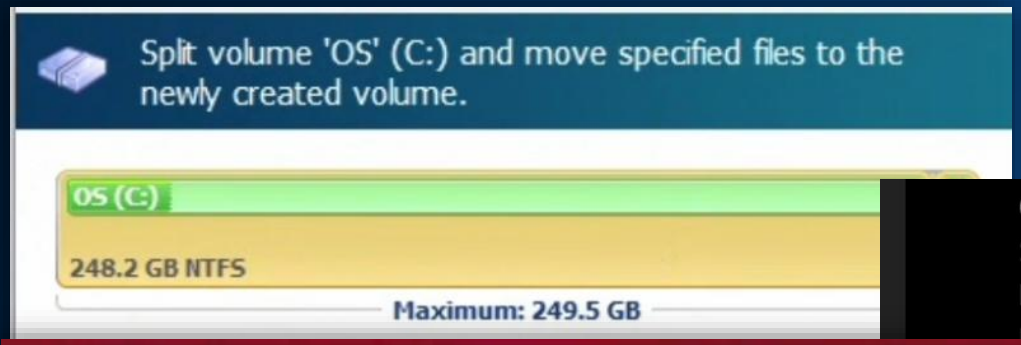
And now for something completely different…

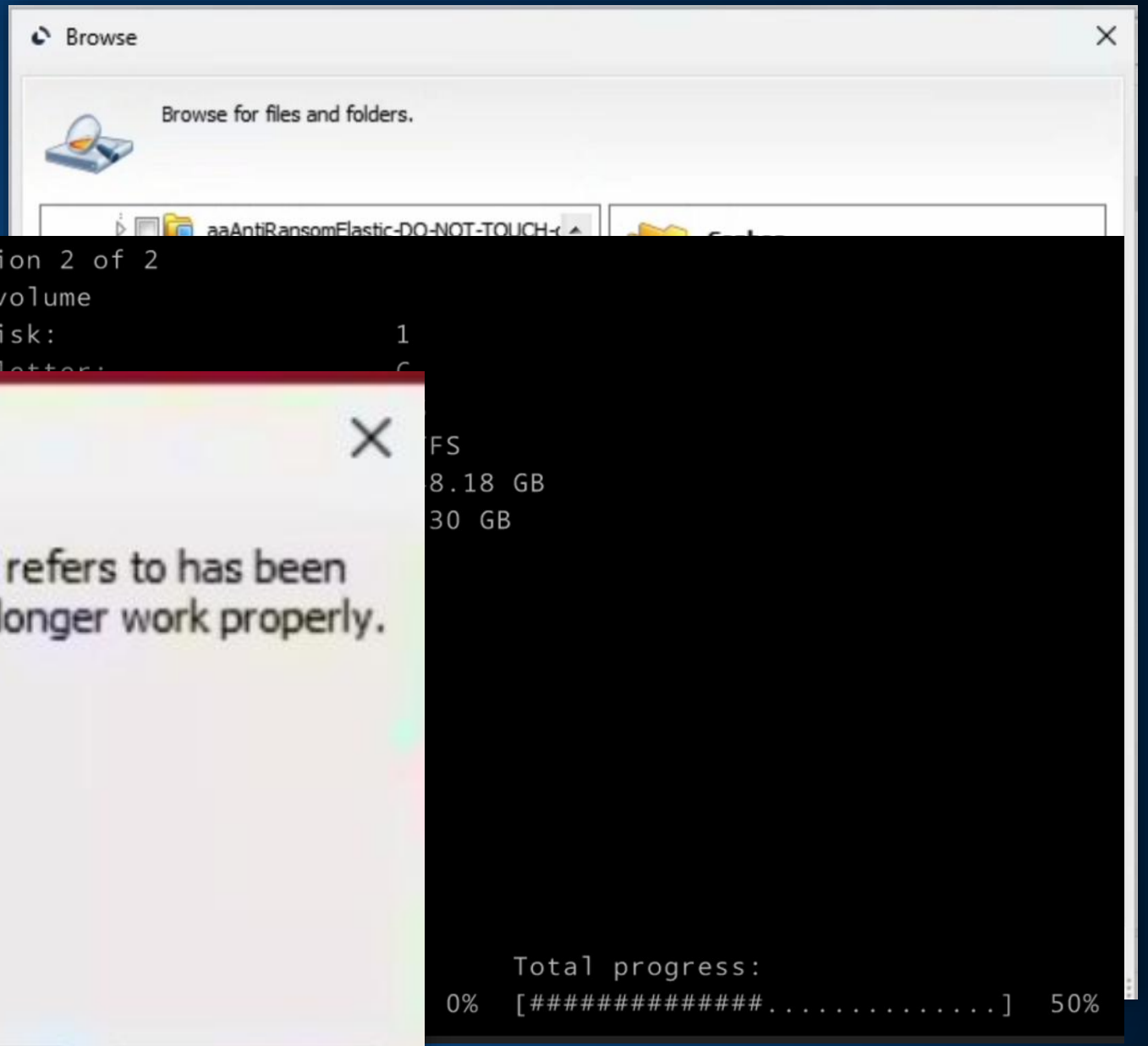
Who needs and EDR killer?

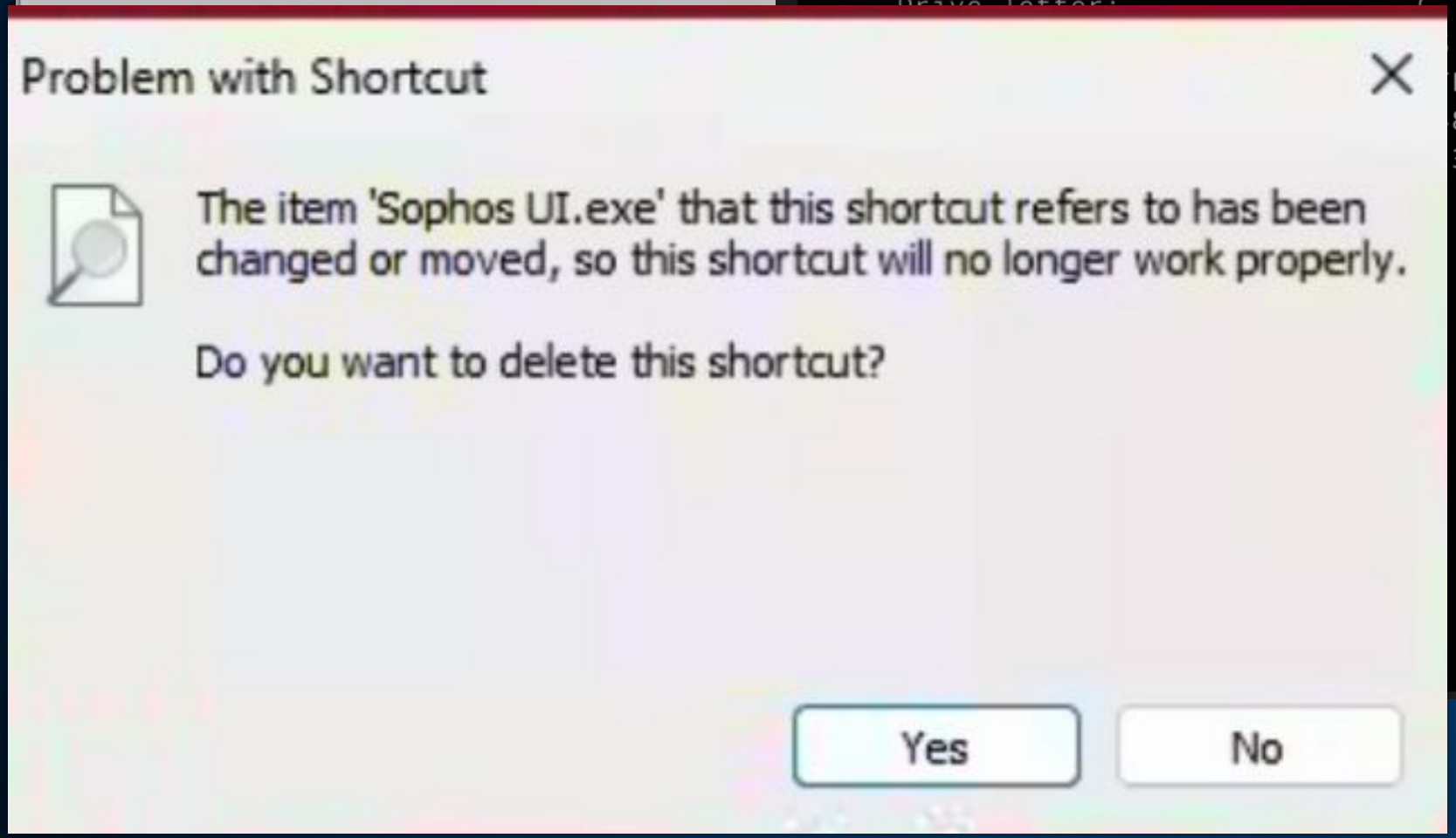


Followed by RansomHub:
C:\vBjgRB.exe -only-local -pass cdd7703d4a4819664e677fdc3378f4418b974165ac849b84a79dd59d5b159516

How does it work?

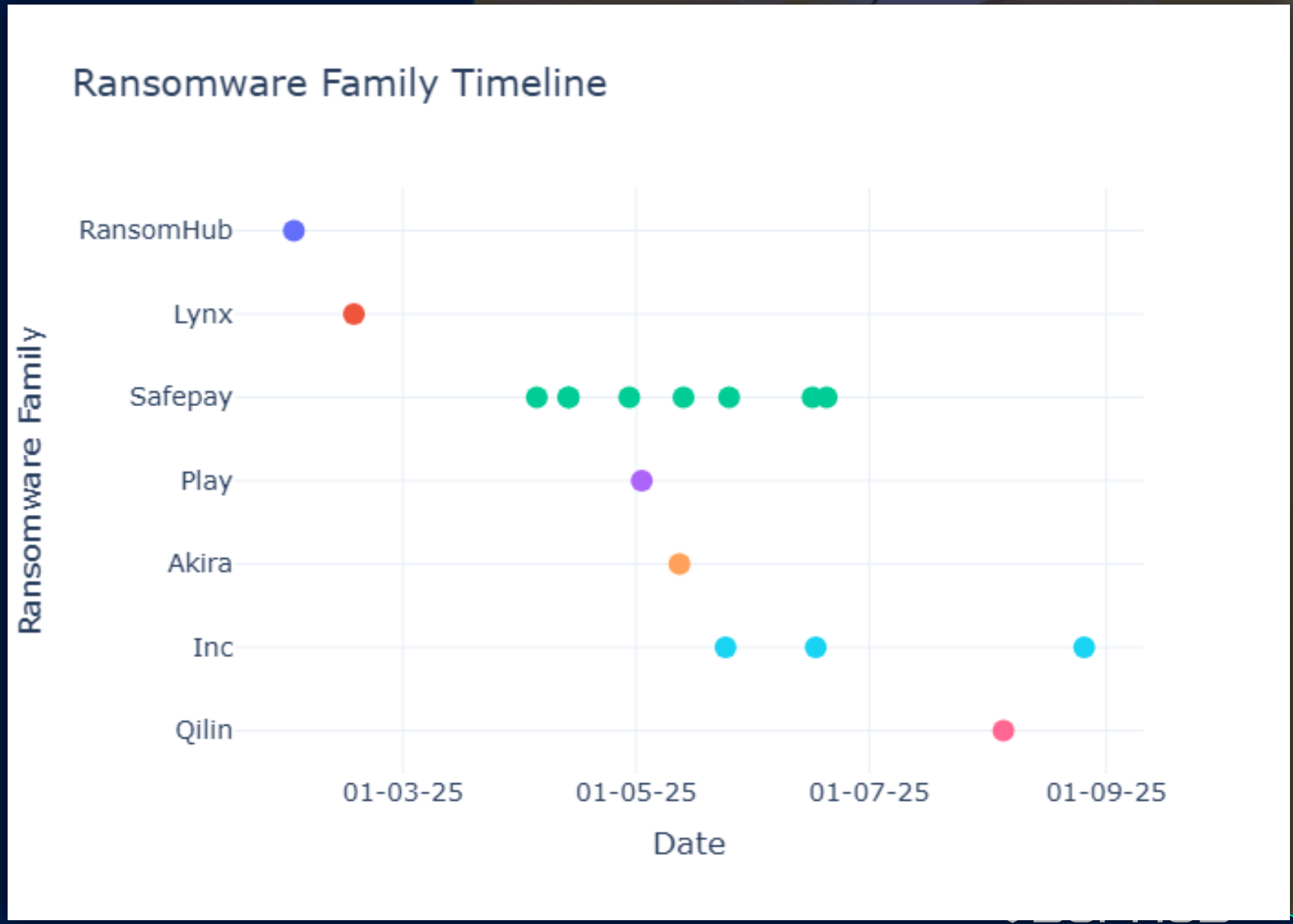






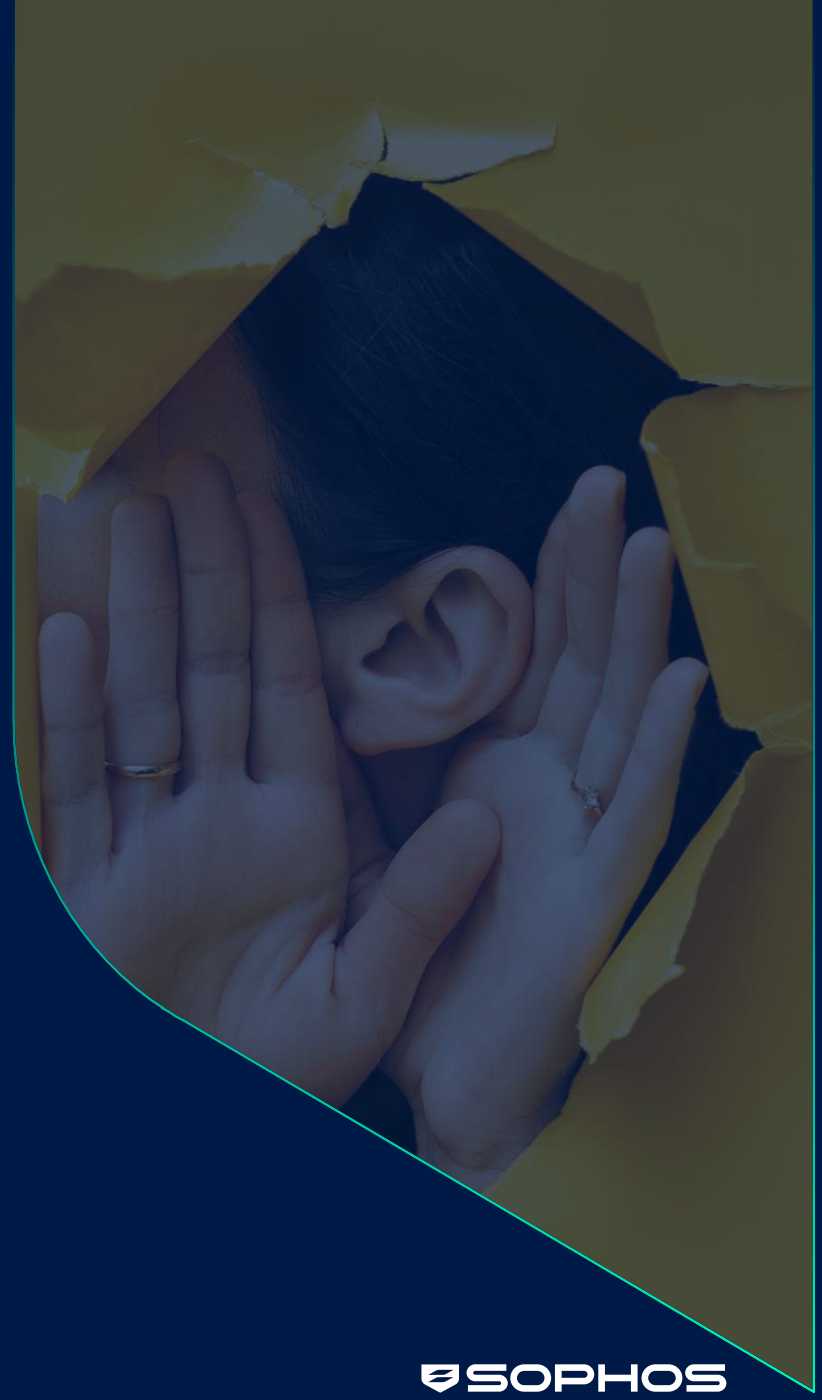
Observed ransomware families

- Ransomhub
- Safepay
- Lynx
- Inc
- Akira
- Play
- Qilin



So, what is happening?

- It could be affiliates are multitasking
- … or migrating to new group
- Or operators doing the same
- But Play, SafePay and BianLian use closed affiliate model
- And what about Qilin?



In other words:

We don’t understand it yet

steeve.gaudreault@sophos.com

gabor.szappanos@sophos.com