GlobeImposter Ransomware Being Distributed with MedusaLocker via RDP - ASEC

By ATCP

Published: 2023-02-27 · Archived: 2026-04-05 13:50:04 UTC

ASEC (AhnLab Security Emergency response Center) has recently discovered the active distribution of the GlobeImposter ransomware. This attack is being carried out by the threat actors behind MedusaLocker. While the specific route could not be ascertained, it is assumed that the ransomware is being distributed through RDP due to the various pieces of evidence gathered from the infection logs.

The threat actor installed various tools alongside GlobeImposter, such as Port Scanner and Mimikatz. Once installed, if these tools are able to confirm that they are within a company's internal network, it is assumed that they will then target that network.

1. Ransomware Installed Using RDP

Threat actors who use RDP (Remote Desktop Protocol) as an attack vector generally scan for systems where RDP is active and allows external access. Systems found during this scanning process are subject to brute force or dictionary attacks. If a user has inappropriate account credentials, then threat actors can easily take those very credentials.

Threat actors can use the obtained account credentials to log in to the system through RDP, allowing them to gain control over the system in question and perform a variety of malicious actions. The threat actors who install GlobeImposter are also assumed to be using RDP as their attack vector. More details about each case will be covered further in this post, but the bases are as follows.

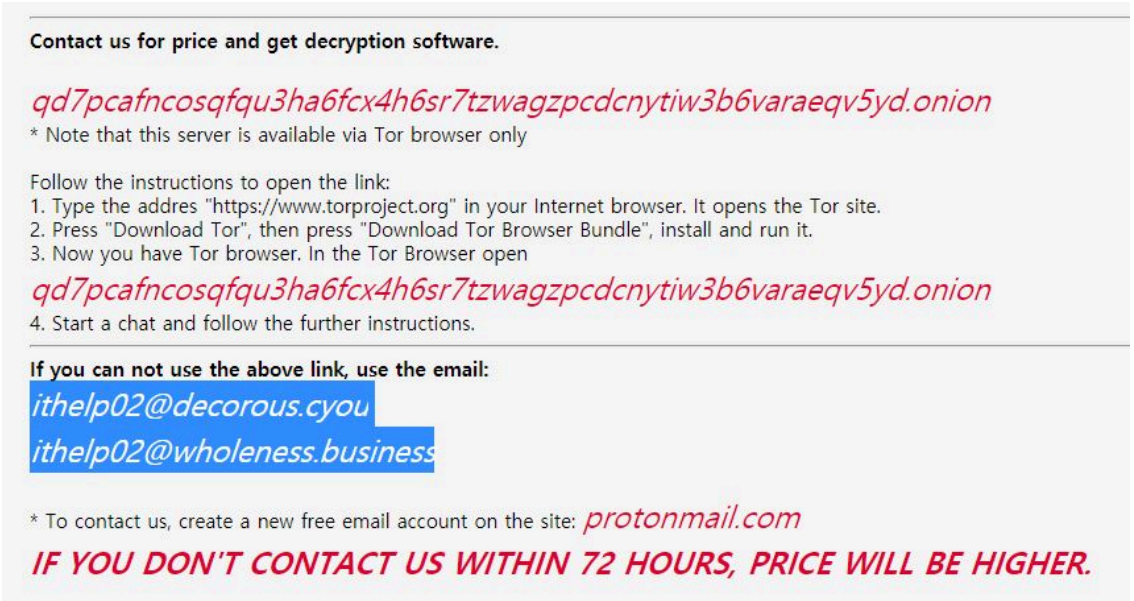
A. Malware created through the explorer process (explorer.exe)
B. RDP-related settings and logs deleted
C. Connection with the MedusaLocker ransomware threat actor who uses RDP as their attack vector

The threat actor usually creates a folder named "skynet work" in the "Music" folder before installing malware in this directory. This ransomware attack has been steadily ongoing since last year, and the fact that the same path is still being used to this day is a characteristic. The following is the log from an attack case by the same threat actor in the past. Through this, we can see that the explorer process, explorer.exe, is creating the malware. As this behavior is often seen when malware is installed on systems through RDP, it serves as reasonable grounds to believe that RDP was used as an attack vector.

CreateFile	%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\music\skynet work\advanced_port_scanner_2.5.3869.exe
CreateFile	%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\music\skynet work\kamikadze new\64.exe
CreateFile	%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\music\skynet work\kamikadze new\86.exe
CreateFile	%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\music\skynet work\kamikadze new\mimidrv.sys
CreateFile	%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\music\skynet work\kamikadze new\mimikatz.dll
CreateFile	%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\music\skynet work\kamikadze new\mimilib.dll
CreateFile	%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\music\skynet work\kamikadze new\mimispool.dll
CreateFile	%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\music\skynet work\miners.exe
CreateFile	%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\music\skynet work\netpass (1).exe
CreateFile	%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\music\skynet work\networkshare_pre2.exe

There are also other connections that tie this with the MedusaLocker threat actor. Recently, the United States Department of Health and Human Services released a report about how the MedusaLocker ransomware threat actors have been using RPD to infect systems with ransomware. **[1]** The MedusaLocker threat group has been using RDP as their attack vector, and relevant information was also released by the United States' Cybersecurity and Infrastructure Security Agency (CISA). **[2]**

A noteworthy thing to point out is that the email and onion addresses found in the ransom note from the recently active GlobeImposter ransomware are included in the list of addresses used by the MedusaLocker group which was released by CISA.



Additionally, the team also discovered during their investigation of multiple logs that some ransomware attack cases used both GlobeImposter and MedusaLocker. Therefore, it can be inferred that the MedusaLocker group is using RDP as their main attack vector and are targeting inappropriately managed systems. Adding to this, they have also been using GlobeImposter instead of MedusaLocker in recent attacks.

2. Malware Used in the Attack Process

As seen in Figure 1, the threat actor installs various pieces of malware in the infected system. Most of the installed m are scanners and account credential stealing tools. It can be assumed through this that the network of the

infected system can also be targeted.

- advanced_port_scanner.exe, advanced_port_scanner_2.5.3869.exe: Port scanners
- Files inside the “kamikadze new” folder: Mimikatz
- netpass (1).exe: Network password recovery tool made by NirSoft
- networkshare_pre2.exe: Shared folder scanner

After the threat actor takes over the system via RDP, the above tools are used to scan the network to check if the infected system is a part of a specific network. If the system is part of a specific network, then the ransomware can perform internal reconnaissance and lateral movement in order to also encrypt the other systems on the network.

The following is a log from AhnLab’s ASD (AhnLab Smart Defense) infrastructure of the Mimikatz command used by a threat actor during their attack. The sekurlsa::logonpasswords command outputs every verifiable account credential currently stored on the system memory. The account credentials obtained in this domain environment can be used for lateral movement.


```
"targetProcess": {
  "imageInfo": {
    "commandLine": "64.exe  \"privilege::debug\" \"sekurlsa::logonpasswords\" \"token::elevate\" \"lsadump::sam full\" exit ",
    "fileObj": {
      "fileName": "64.exe",
      "filePath": "%SystemDrive%\\users\\%ASD%\\music\\skynet work\\kamikadze new\\64.exe",
      "fileSize": 1355680,
    }
  }
```


There are some cases where the threat actor would also install an XMRig CoinMiner alongside the ransomware. This can be seen in Figure 1 as Miners.exe. Thus, not only do the MedusaLocker threat actors encrypt infected systems using their ransomware, but they also mine for coins by installing XMRig.

- **Mining Pool** : pool.supportxmr[.]com:3333
- **User** : 49c2xjofxbxkydovzvfart2ekruhe6wiep55xcjaogaq1dugduyzgxphd1zx6j21nvv5emtupnfr39sulbp1ggczqwfzjmc
- **Password** : x

3. GlobeImposter

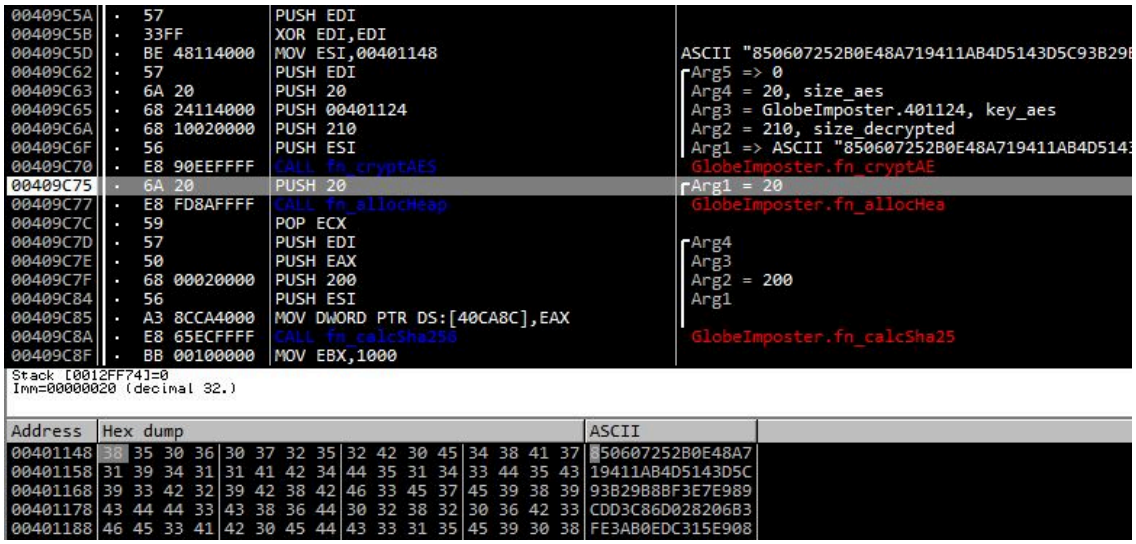
The ols.exe file within the “skynet work” folder is the GlobeImposter ransomware. GlobeImposter is a type of ransomware that uses the AES symmetric key algorithm for file encryption and a public/private RSA key algorithm for key encryption. **[3]**

Overview	Description
Encryption method	AES / RSA-1024
Extension	.onelock
Paths excluded from encryption	Refer to the information further below
Extensions excluded from encryption	Refer to the information further below

Ransom note	how_to_back_files.html
Others	Registers RunOnce key Removes volume shadow service Deletes event logs Deletes RDP logs

Table 1. GlobeImposter ransomware overview

Upon execution, GlobeImposter creates a new public and private RSA-1024 key before using the public RSA key to encrypt the AES key that was used to encrypt files. The generated private RSA key is encrypted with the threat actor's public RSA key. This key exists encrypted in binary. As shown in the figure below, the public RSA key can be decrypted with the hard-coded AES key.



To maintain persistence, GlobeImposter first copies itself into the %LOCALAPPDATA% path before registering itself to the RunOnce key, allowing it to operate even after system reboots. A file that uses the SHA256 hash value of the threat actor's private key as its name is created in the %PUBLIC% path. The key information is then encrypted and saved here.

Afterward, files within the system are encrypted. Configuration data such as the list of paths and file extensions excluded from encryption are encrypted with the AES key. Additionally, the AES key used to decrypt the configuration data is the SHA256 hash value of the threat actor's private key mentioned above. The following is a list of the paths and file extensions excluded from encryption that was obtained during the decryption process.

Paths excluded from encryption
Windows, Microsoft, Microsoft Help, Windows App Certification Kit, Windows Defender, ESET, COMODO, Windows NT, Windows Kits, Windows Mail, Windows Media Player, Windows Multimedia Platform, Windows Phone Kits, Windows Phone Silverlight Kits, Windows Photo Viewer, Windows Portable Devices, Windows Sidebar, WindowsPowerShell, NVIDIA Corporation, Microsoft.NET, Internet Explorer, Kaspersky

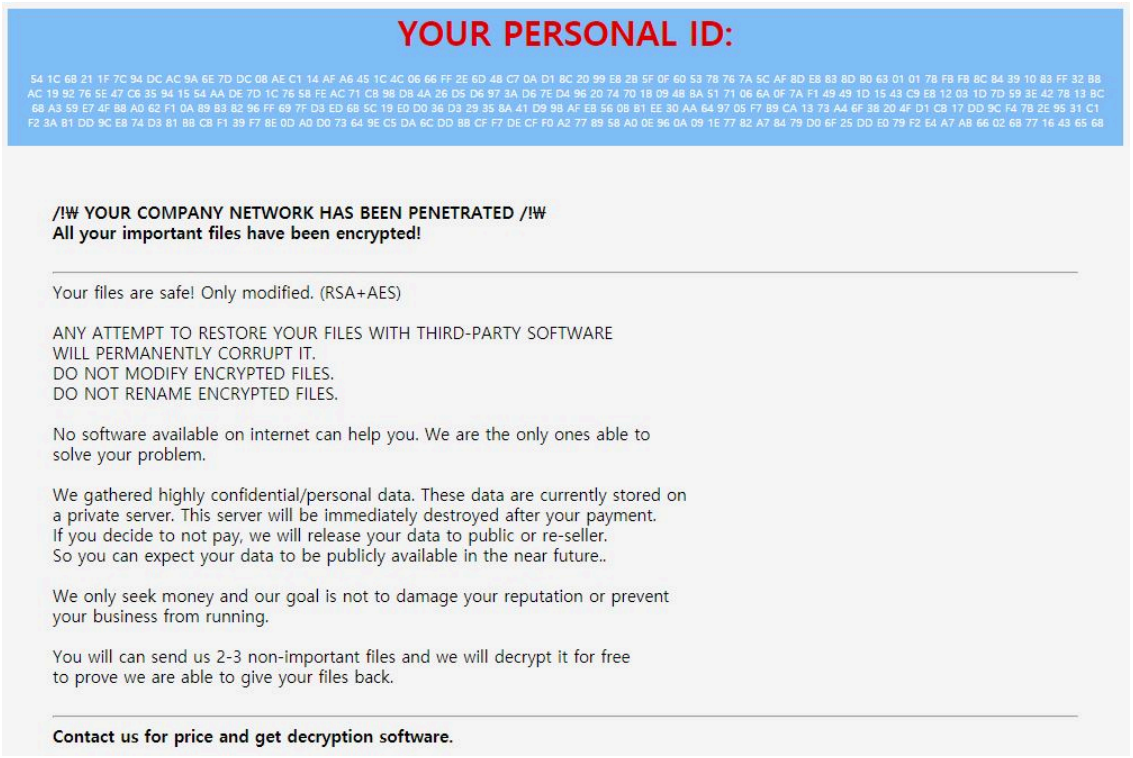
Lab, McAfee, Avira spytech software, sysconfig, Avast, Dr.Web, Symantec, Symantec_Client_Security, system volume information, AVG, Microsoft Shared, Common Files, Outlook Express, Movie Maker, Chrome, Mozilla, Firefox, Opera, YandexBrowser, ntldr, Wsus, ProgramData

Extensions excluded from encryption
.onelock, .dll, .sys, .exe, .rdp, .ini, .revenlock8, .revenlock9, .revenlock10, .locklock, .allock, .allock2, .allock3, .allock4, .allock5, .allock6, .allock7, .allock8, .allock9, .allock10, .netlock1, .allock1, .allock02, .allock03, .allock05, .allock06, .allock07, .allock08, .alloc

When the file encryption is complete, the following batch file is created and executed. The batch file is responsible for deleting volume shadow copies and logs. Event logs and RDP-related logs are the logs that get deleted. Like this, the ransomware attack is performed through RDP. It can be assumed that the threat actor added these kinds of features to the ransomware in order to erase their access history.

```
@echo off
vssadmin.exe Delete Shadows /All /Quiet
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
cd %userprofile%\documents\
attrib Default.rdp -s -h
del Default.rdp
for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
```

The ransom note is created in the folder where the infection occurs under the file name “how_to_back_files.html”. The ransom note also differs from previously known GlobeImposter ransom notes but matches the MedusaLocker ransom note that was previously disclosed in the report published by Carbon Black. **[4]**



4. Conclusion

Threat actors have consistently been using RDP during their initial infiltration and lateral movement processes. These attacks usually occur through brute force and dictionary attacks against systems with inappropriate account credentials. In particular, a large number of ransomware threat actors aside from the MedusaLocker group also use RDP as their main initial attack vector.

Users can deactivate RDP when not in use to decrease the number of attack attempts. If RDP is being used, it is advised to use a complex account password and to change it periodically to prevent brute force and dictionary attacks. Also, V3 should be updated to the latest version so that malware infection can be prevented.

File Detection

– Ransomware/Win.MedusaLocker.R335910 (2022.11.23.00)
– Trojan/Win32.FileCoder.R228072 (2018.05.16.01)
– Trojan/Win32.RL_CoinMiner.C4078402 (2020.04.25.01)
– Trojan/Win32.RL_CoinMiner.C4078402 (2020.04.25.01)
– Trojan/Win32.RL_Mimikatz.R366782 (2021.02.18.01)
– Trojan/Win.Mimikatz.R433236 (2021.07.23.01)
– Trojan/Win.Mimikatz.R434976 (2021.07.31.01)
– HackTool/Win.Scanner.C5310311 (2022.11.21.03)
– HackTool/Win.Scanner.C5310305 (2022.11.21.03)
– Trojan/Win.Mimikatz.R433236 (2021.07.23.01)
– Trojan/RL.Mimikatz.R248084 (2018.12.10.01)
– Unwanted/Win32.Agent.R266440 (2019.04.23.00)
– HackTool/Win.PSWTool.R345815 (2022.09.02.00)

Behavior Detection

– Persistence/MDP.AutoRun.M224

– Ransom/MDP.Event.M4428

MD5

21ea77788aa2649614c9ec739f1dd1b8

4edd26323a12e06568ed69e49a8595a5

4fdabe571b66ceec3448939bfb3ffcd1

597de376b1f80c06d501415dd973dcec

5e1a53a0178c9be598edff8c5170b91c

Additional IOCs are available on AhnLab TIP.

URL

http[:]//46[.]148[.]235[.]114/cmd[.]php

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/48940/