Webworm: Espionage Attackers Testing and Using Older Modified RATs

Symantec, by Broadcom Software, has gained insight into the current activities of a group we call Webworm. The group has developed customized versions of three older remote access Trojans (RATs), including Trochilus, Gh0st RAT, and 9002 RAT. At least one of the indicators of compromise (IOCs) observed by Symantec was used in an attack against an IT service provider operating in multiple Asian countries, while others appear to be in pre-deployment or testing stages.

Webworm

Symantec's Webworm has links to a group dubbed Space Pirates, which was previously documented in a May 2022 report from Positive Technologies. It is likely that the two groups are one and the same.

Active since at least 2017, Webworm has been known to target government agencies and enterprises involved in IT services, aerospace, and electric power industries located in Russia, Georgia, Mongolia, and a number of other Asian countries.

Previous research on the group's activity found that it uses custom loaders hidden behind decoy documents and modified backdoors that have been around for quite some time. This corresponds with recent Webworm activity observed by Symantec.

Malware used by Webworm includes versions of the following threats:

Trochilus RAT

First spotted back in 2015, Trochilus is a RAT implemented in C++ and its source code is available for download on GitHub. The malware has been used in targeted threat operations by multiple groups and has features that can help it evade sandbox analysis and be useful in cyber-espionage operations. The RAT's features include, but are not limited to, the ability to remotely uninstall a file manager, and the ability to download, upload, and execute files.

Trochilus has been previously linked to malware operations from threat actors also using malware such as PlugX and a variant of the 9002 RAT.

9002 RAT

The 9002 RAT appears to have been in use since at least 2009 and has historically been used by state-sponsored actors. The malware provides attackers with extensive data exfiltration capabilities. Some variants of 9002 RAT inject into memory and do not write to the disk, something that also applies to the sample analyzed by Symantec.

The malware has been used in multiple campaigns by a range of actors, including in a hacking operation targeting several large corporations located in South Korea. The RAT was used to deliver additional malware, including the PlugX RAT, onto compromised machines. It has also been involved in attacks making use of zero-day exploits.

Gh0st RAT

While the source code for Gh0st RAT was released online in 2008, the malware has continued to be used by advanced persistent threat (APT) groups.

Gh0st RAT first made headlines back in 2009, when a cyber-espionage group called GhostNet used it to target diplomatic, political, economic, and military targets around the world.

Observed Webworm activity

Symantec observed three malware droppers developed by Webworm:

- 6201c604ac7b6093dc8f6f12a92f40161508af1ddffa171946b876442a66927e (Trochilus dropper)
- b9a0602661013d973bc978d64b7abb6bed20cf0498d0def3acb164f0d303b646 (Trochilus Dropper)
- c71e0979336615e67006e20b24baafb19d600db94f93e3bf64181478dfc056a8 (Trochilus Dropper)

Analysis of one of the droppers revealed that it drops the following files:

- [TEMP]\Logger.exe (28d78e52420906794e4059a603fa9f22d5d6e4479d91e9046a97318c83998679)
- [TEMP]\sc.cfg (a618b3041935ec3ece269effba5569b610da212b1aa3968e5645f3e37d478536)
- [TEMP]\logexts.dat (a6b9975bfe02432e80c7963147c4011a4f7cdb9baaee4ae8d27aaff7dff79c2b)
- [TEMP]\logexts.dll (a73a4c0aa557241a09e137387537e04ce582c989caa10a6644d4391f00a836ef)
- [TEMP]\logger.dat (10456bc3b5cfd2f1b1ab9c3833022ef52f5e9733d002ab237bdebad09b125024)
- [TEMP]\[RANDOM_DIGITS].doc (d295712185de2e5f8811b0ce7384a04915abdf970ef0f087c294bb00e340afad)

The legitimate executable Logger.exe is used to call the “LoadLibraryA” API in order to load the malicious "[TEMP]\logexts.dll" file.

Thelogexts.dll file is a loader. Once run, it checks the process command-line parameters. If the command-line is the single parameter "isdf", it attempts to steal a token from the "WINLOGON.EXE" process. It then starts the following process by calling the CreateProcessAsUserW API:

C:\ProgramData\Logger\Logger.exe mdkv

Otherwise it constructs the pathname of the second stage based on its own running executable, where it replaces the last three characters with hardcoded "dat" (resulting with "Logger.dat"). Then it reads and executes the second stage as shellcode.

The second stage ("Logger.dat") constructs the pathname of the third stage also based on its own running executable, where it combines the directory part with hardcoded "logexts.dat". Finally, it reads and executes the third stage.

Thelogexts.dat file is obfuscated and includes several User Account Control (UAC) bypasses.

It attempts to copy the previously dropped files to the following new locations:

- [Temp]\Logger.exe to C:\ProgramData\Logger\Logger.exe
- [Temp]\Logger.dat to C:\ProgramData\Logger\logger.dat
- [Temp]\logexts.dll to C:\ProgramData\Logger\logexts.dll
- [Temp]\logexts.dat to C:\ProgramData\Logger\logexts.dat
- [Temp]\sc.cfg to C:\ProgramData\Logger\sc.cfg

Then the file unpacks and executes in memory its backdoor payload, a variant of the Trochilus RAT (e69177e58b65dd21e0bbe4f6caf66604f120e0c835f3ee0d16a45858f5fe9d90).

The Trochilus modifications include functionality to load its configuration from a file by checking for any of the following locations (in order of preference):

- C:\ProgramData\Logger\sc.cfg
- C:\ProgramData\resmon.resmoncfg
- C:\ProgramData\appsoft\resmon.resmoncfg

The content of the configuration file is decompressed using the Lempel–Ziv–Welch (LZW) algorithm.

Interestingly, one of the locations described above (“C:\ProgramData\resmon.resmoncfg”) is mentioned in third-party research detailing previous Space Pirates (Webworm) activity.

The malware then injects svchost.exe with the ability to:

- Execute commands
- Download potentially malicious files

Further investigation by Symantec found that droppers that share a similar structure to the one used to deploy the version of Trochilus RAT modified by Webworm were also used to deploy two additional modified versions of Gh0st RAT and 9002 RAT. Some code modifications made to the variant of Trochilus RAT were also present in the two additional retooled RATs. The additional RATs included:

Gh0st RAT:

- 1e725f1fe67d1a596c9677df69ef5b1b2c29903e84d7b08284f0a767aedcc097 (Dropper)
- b0a58c6c859833eb6fb1c7d8cb0c5875ab42be727996bcc20b17dd8ad0058ffa (Shellcode loader)
- 1CC32C7F2C90A558BA5FF6BA191E655B20D7C65C10AF0D5D06820A28C2947EFD (Shellcode loader)

9002 RAT:

- 6e46054aa9fd5992a7398e0feee894d5887e70373ca5987fc56cd4c0d28f26a1 (Dropper)
- 37fa5108db1ae73475911a5558fba423ef6eee2cf3132e35d3918b9073aeecc1 (Packed backdoor)

Changes made by Webworm to this version of 9002 RAT are apparently intended to evade detection. For example, the details of the RAT's communication protocol, such as encryption, have also been modified by the threat actors.

Gh0st RAT (BH_A006) was documented in third-party research detailing previous Webworm (Space Pirates) activity. In that research, the version of Gh0st RAT included features such as layers of obfuscation to bypass security protections and hinder analysis, network service creation, UAC bypassing, and shellcode unpacking and launching in the memory. Some of these features were also present in the version of the RAT being prepared by Webworm.

Conclusion

Webworm's use of customized versions of older, and in some cases open-source, malware, as well as code overlaps with the group known as Space Pirates, suggest that they may be the same threat group. However, the common use of these types of tools and the exchange of tools between groups in this region can obscure the traces of distinct threat groups, which is likely one of the reasons why this approach is adopted, another being cost, as developing sophisticated malware can be expensive in terms of both money and time.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

IOCs

c71e0979336615e67006e20b24baafb19d600db94f93e3bf64181478dfc056a8 - Trochilus dropper

28d78e52420906794e4059a603fa9f22d5d6e4479d91e9046a97318c83998679 – Logger.exe

a6b9975bfe02432e80c7963147c4011a4f7cdb9baaee4ae8d27aaff7dff79c2b – logexts.dat

a73a4c0aa557241a09e137387537e04ce582c989caa10a6644d4391f00a836ef – logexts.dll

10456bc3b5cfd2f1b1ab9c3833022ef52f5e9733d002ab237bdebad09b125024 – logger.dat

d295712185de2e5f8811b0ce7384a04915abdf970ef0f087c294bb00e340afad – [RANDOM_DIGITS].doc

e69177e58b65dd21e0bbe4f6caf66604f120e0c835f3ee0d16a45858f5fe9d90 – Trochilus RAT

a618b3041935ec3ece269effba5569b610da212b1aa3968e5645f3e37d478536 - Backdoor configuration

6201c604ac7b6093dc8f6f12a92f40161508af1ddffa171946b876442a66927e – Trochilus dropper

3629d2ce400ce834b1d4b7764a662757a9dc95c1ef56411a7bf38fb5470efa84 - Backdoor configuration

b9a0602661013d973bc978d64b7abb6bed20cf0498d0def3acb164f0d303b646 - Trochilus dropper

824100a64c64f711b481a6f0e25812332cc70a13c98357dd26fb556683f8a7c7 – Packed backdoor