IronHusky updates the forgotten MysterySnail RAT to target Russia and Mongolia

By GReAT

Published: 2025-04-17 · Archived: 2026-04-05 16:21:19 UTC

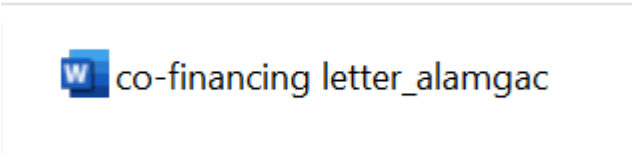
Day after day, threat actors create new malware to use in cyberattacks. Each of these new implants is developed in its own way, and as a result gets its own destiny – while the use of some malware families is reported for decades, information about others disappears after days, months or several years.

We observed the latter situation with an implant that we dubbed MysterySnail RAT. We discovered it back in 2021, when we were investigating the CVE-2021-40449 zero-day vulnerability. At that time, we identified this backdoor as related to the IronHusky APT, a Chinese-speaking threat actor operating since at least 2017. Since we published a blogpost on this implant, there have been no public reports about it, and its whereabouts have remained unknown.

However, recently we managed to spot attempted deployments of a new version of this implant, occurring in government organizations located in Mongolia and Russia. To us, this observed choice of victims wasn't surprising, as back in 2018, we wrote that IronHusky, the actor related to this RAT, has a specific interest in targeting these two countries. It turned out that the implant has been actively used in cyberattacks all these years although not reported.

Infection through a malicious MMC script

One of the recent infections we spotted was delivered through a malicious MMC script, designed to be disguised as a document from the National Land Agency of Mongolia (ALAMGAC):



Malicious MMC script as displayed in Windows Explorer. It has the icon of a Microsoft Word document

When we analyzed the script, we identified that it is designed to:

- Retrieve a ZIP archive with a second-stage malicious payload and a lure DOCX file from the file[.]io public file storage.
- Unzip the downloaded archive and place the legitimate DOCX file into the %AppData%\Cisco\Plugins\X86\bin\etc\Update folder
- Start the CiscoCollabHost.exe file dropped from the ZIP archive.
- Configure persistence for the dropped CiscoCollabHost.exefile by adding an entry to the Run registry key.
- Open the downloaded lure document for the victim.

Having investigated the CiscoCollabHost.exe file, we identified it as a legitimate executable. However, the archive deployed by the attackers also turned out to include a malicious library named CiscoSparkLauncher.dll, designed to be loaded by the legitimate process through the DLL Sideloading technique.

We found out that this DLL represents a previously unknown intermediary backdoor, designed to perform C2 communications by abusing the open-source piping-server project. An interesting fact about this backdoor is that information about Windows API functions used by it is located not in the malicious DLL file, but rather in an external file having the log\MYFC.log relative path. This file is encrypted with a single-byte XOR and is loaded at runtime. It is likely that the attackers introduced this file to the backdoor as an anti-analysis measure – since it is not possible to determine the API functions called without having access to this file, the process of reverse engineering the backdoor essentially turns into guesswork.

By communicating with the legitimate https://ppng.io server powered by the piping-server project, the backdoor is able to request commands from attackers and send back their execution results. It supports the following set of basic malicious commands:

Command name	Command description
RCOMM	Runs command shells.
FSEND	Downloads files from the C2 server.
FRECV	Uploads files to the C2 server.
FSHOW	Lists directory contents.
FDELE	Deletes files.
FEXEC	Creates new processes.
REXIT	Terminates the backdoor.
RSLEE	Performs sleeping.
RESET	Resets the timeout counter for the C2 server connection.

As we found out, attackers used commands implemented in this backdoor to deploy the following files to the victim machine:

- sophosfilesubmitter.exe, a legitimate executable
- fltlib.dll, a malicious library to be sideloaded

In our telemetry, these files turned out to leave footprints of the MysterySnail RAT malware, an implant we described back in 2021.

New version of MysterySnail RAT

In observed infection cases, MysterySnail RAT was configured to persist on compromised machines as a service. Its malicious DLL, which is deployed by the intermediary backdoor, is designed to load a payload encrypted with RC4 and XOR, and stored inside a file named attach.dat. When decrypted, it is reflectively loaded using DLL hollowing with the help of code implemented inside the run_pe library.

Just as the version of MysterySnail RAT we described in 2021, the latest version of this implant uses attacker-created HTTP servers for communication. We have observed communications being performed with the following servers:

- watch-smcsvc[.]com
- leotolstoys[.]com

Having analyzed the set of commands implemented in the latest version of this backdoor, we identified that it is quite similar to the one implemented in the 2021 version of MysterySnail RAT – the newly discovered implant is able to accept about 40 commands, making it possible to:

- Perform file system management (read, write and delete files; list drives and directories).
- Execute commands via the cmd.exe shell.
- Spawn and kill processes.
- Manage services.
- Connect to network resources.

Compared to the samples of MysterySnail RAT we described in our 2021 article, these commands were implemented differently. While the version of MysterySnail from 2021 implements these commands inside a single malicious component, the newly discovered version of the implant relies on five additional DLL modules, downloaded at runtime, for command execution. These modules are as follows:

Internal module ID	Internal module name	Module DLL name	Module description
0	Basic	BasicMod.dll	Allows listing drives, deleting files, and fingerprinting the infected machine.
1	EMode	ExplorerMoudleDll.dll (sic!)	Allows reading files, managing services, and spawning new processes.
2	PMod	process.dll	Allows listing and terminating running processes.
3	CMod	cmd.dll	Allows creating new processes and spawning command shells.
4	TranMod	tcptran.dll	Allows connecting to network resources.

However, this transition to a modular architecture isn't something new – as we have seen modular versions of the MysterySnail RAT deployed as early as 2021. These versions featured the same modules as described above,

including the typo in the ExplorerMoudleDll.dll module name. Back then, we promptly made information about these versions available to subscribers of our APT Intelligence Reporting service.

MysteryMonoSnail – a repurposed version of MysterySnail RAT

Notably, a short time after we blocked the recent intrusions related to MysterySnail RAT, we observed the attackers to continue conducting their attacks, by deploying a repurposed and more lightweight version of MysterySnail RAT. This version consists of a single component, and that's why we dubbed it MysteryMonoSnail. We noted that it performed communications with the same C2 server addresses as found in the full-fledged version of MysterySnail RAT, albeit via a different protocol – WebSocket instead of HTTP.

This version doesn't have as many capabilities as the version of MysterySnail RAT that we described above – it was programmed to have only 13 basic commands, used to list directory contents, write data to files, and launch processes and remote shells.

Obsolete malware families may reappear at any time

Four years, the gap between the publications on MysterySnail RAT, has been quite lengthy. What is notable is that throughout that time, the internals of this backdoor hardly changed. For instance, the typo in the ExplorerMoudleDll.dll that we previously noted was present in the modular version of MysterySnail RAT from 2021. Furthermore, commands implemented in the 2025 version of this RAT were implemented similarly to the 2021 version of the implant. That is why, while conducting threat hunting activities, it's crucial to consider that old malware families, which have not been reported on for years, may continue their activities under the radar. Due to that, signatures designed to detect historical malware families should never be discontinued simply because they are too old.

At Kaspersky's GReAT team, we have been focusing on detecting complex threats since 2008 – and we provide sets of IoCs for both old and new malware to customers of our Threat Intelligence portal. If you wish to get access to these IoCs and other information about historical and emerging threats, please contact us at intelreports@kaspersky.com.
