Rhadamanthys Malware: Swiss Army Knife of Information Stealers Emerges

By The Hacker News

Published: 2023-12-18 · Archived: 2026-04-05 15:09:06 UTC

The developers of the information stealer malware known as Rhadamanthys are actively iterating on its features, broadening its information-gathering capabilities and also incorporating a plugin system to make it more customizable.

This approach not only transforms it into a threat capable of delivering "specific distributor needs," but also makes it more potent, Check Point said in a technical deep dive published last week.

Rhadamanthys, first documented by ThreatMon in October 2022, has been sold under the malware-as-a-service (MaaS) model as early as September 2022 by an actor under the alias "kingcrete2022."

Typically distributed through malicious websites mirroring those of genuine software that are advertised through Google ads, the malware is capable of harvesting a wide range of sensitive information from compromised hosts, including from web browsers, crypto wallets, email clients, VPN, and instant messaging apps.

"Rhadamanthys represents a step in the emerging tradition of malware that tries to do as much as possible, and also a demonstration that in the malware business, having a strong brand is everything," the Israeli cybersecurity firm noted in March 2022.

A subsequent investigation into the off-the-shelf malware in August revealed "design and implementation" overlap with that of the Hidden Bee coin miner.

"The similarity is apparent at many levels: custom executable formats, the use of similar virtual filesystems, identical paths to some of the components, reused functions, similar use of steganography, use of LUA scripts, and overall analogous design," the researchers said, describing the malware's development as "fast-paced and ongoing."

As of writing, the current working version of Rhadamanthys is 0.5.2, per the description on the threat actor's Telegram channel.

Check Point's analysis of versions 0.5.0 and 0.5.1 reveals a new plugin system that effectively makes it more of a Swiss Army knife, indicating a shift towards modularization and customization. This also allows the stealer customers to deploy additional tools tailored to their targets.

The stealer components are both active, capable of opening processes and injecting additional payloads designed to facilitate information theft, and passive, which are designed to search and parse specific files to retrieve saved credentials.

Another noticeable aspect is the use of a Lua script runner that can load up to 100 Lua scripts to pilfer as much information as possible from cryptocurrency wallets, email agents, FTP services, note-taking apps, instant messengers, VPNs, two-factor authentication apps, and password managers.

Version 0.5.1 goes a step further, adding clipper functionality to alter clipboard data matching wallet addresses to divert cryptocurrency payments to an attacker-controlled wallet as well as an option to recover Google Account cookies, following the footsteps of Lumma Stealer.

"The author keeps enriching the set of available features, trying to make it not only a stealer but a multipurpose bot, by enabling it to load multiple extensions created by a distributor," security researcher Aleksandra "Hasherezade" Doniec said.

"The added features, such as a keylogger, and collecting information about the system, are also a step towards making it a general-purpose spyware."

AsyncRAT's Code Injection into aspnet_compiler.exe

The findings come as Trend Micro detailed new AsyncRAT infection chains that leverage a legitimate Microsoft process called aspnet_compiler.exe, which is used for precompiling ASP.NET web applications, to stealthily deploy the remote access trojan (RAT) via phishing attacks.

Similar to how Rhadamanthys carries out code injection into running processes, the multi-stage process culminates in the AsyncRAT payload being injected into a newly spawned aspnet_compiler.exe process to ultimately establish contact with a command-and-control (C2) server.

"The AsyncRAT backdoor has other capabilities depending on the embedded configuration," security researchers Buddy Tancio, Fe Cureg, and Maria Emreen Viray said. "This includes anti-debugging and analysis checks, persistence installation, and keylogging."

It's also designed to scan particular folders within the application directory, browser extensions, and user data to check for the presence of crypto wallets. On top of that, the threat actors have been observed relying on Dynamic DNS (DDNS) to deliberately obfuscate their activities.

"The use of dynamic host servers allows threat actors to seamlessly update their IP addresses, strengthening their ability to remain undetected within the system," the researchers said.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
