Like Father Like Son? New Mars Stealer

By Yaara Shriebman

Published: 2022-02-22 · Archived: 2026-04-05 21:38:29 UTC

Executive Summary

First observed in 2021 and advertised as a standalone version on various cybercriminal forums, Mars is an information stealer mainly targeting Windows victim credentials and cryptocurrency wallets including 2FA plugins and any essential system information. Mars is also capable of loading any type of file by downloading and executing them from a given drop-zone.

Over the past several months, Mars took the place of a solid info stealer. We now see more new threat actors comparing its efficiency to Raccoon stealer, and having a hard time choosing between the two given the simplicity, “noob-friendly” setup, and cheap price.

As some claims suggest, Mars is actually a new version of Oski stealer which we have written about in the past.

Advertising

Mars is currently advertised in over 47 different underground forums, Telegram channels and Darknet onion sites, while the main channel for purchasing the malware is the official Telegram channel (Figure 1), created on August 4, 2021, giving a big boost to the stealer.

Although Mars is a better version than its predecessor, Oski, a leak of the dashboard caused damage to the info stealer’s team. But over the past months, we’ve seen the effort the team put into branding this info stealer with competitive prices, promoting the “MarsTeam” name, pushing new abilities, providing lifetime support, and more.

As mentioned, Mars offers a cheap lifetime subscription for only $160, paid in cryptocurrency of course. In comparison, Raccoon and Redline, the top 2 info stealers at the moment, charge the same price for a two-week subscription, although their business model is Malware-as-a-Service (MaaS).

Another option is to use the leaked panel version that is currently free of charge, but threat actors need to take care of the infrastructure, anonymity, and so on, without any help or support from the MarsTeam.

Command and Control

The C&C setup is fairly easy, whether you buy the panel or use the leaked one. The group provides an all-in-one solution that makes the stealer’s infrastructure very simple to use, but also very easy to detect.

The C&C is comprised of three modules: the dashboard, the drop zone for stealers’ logs, and the downloading source for dependencies.

Although the modules are separate, and the leaked code is easy to understand, it seems that most threat actors do not use more sophisticated techniques such as reverse proxy or segregation of each module in a different host, but rather use them all in the same host.

Structure

The Cyberint Research Team has been tracking Mars for some time now and found several C&Cs that were set up as public, disclosing the structure and files within the C&C (Figure 2).

Other than a campaign overview, the dashboard provides file grabbing statistics and Loader rules, which are used for setting up the files the threat actor would like to load into the infected machine.

It seems that more experienced threat actors will look to use the leaked panel kit given that it comes with full installation and building instructions, and , like more advanced stealers, can be modelized to create Telegram integration, making the campaign less obvious.

Dependencies

The C&C contains the dependencies the stealer needs in order to operate properly when it comes to information gathering.

The files are in fact legitimate third-party Dynamic-link Libraries (DLL) used to support access to data of various applications and/or browsers.

Drop Zone

The drop zone module within the C&C is straightforward and simple with the common gate.php file in which the stealer posting a Zip file containing the stolen data.

Delivery

Lacking an out-of-the-box distribution method, recently observed Mars incidents appear to begin with social engineering techniques commonly used in gaming forums and groups as the threat actors lure the victims to download patching software (Figure 5), cracks and keygens (Figure 6).

Using this technique might be even more effective than malicious documents sent via email given the fact that victims might think that the defense mechanisms alerts these files because of their original purposes, which are pretty sketchy by themselves. This results in excluding these files from the defense systems by the victims and knowingly approves theses files to run in administrator privileges.

In addition to this technique, evidence suggests that malspam campaign delivery is also used in the wild, along with Twitter and Instagram Direct Messaging.

Like most info stealers, the targeting of these campaigns is based more on the hobbies and communities the victims take part in, such as gaming, cryptocurrency, 3D artists and graphic designers, than on a specific geolocation or business sector.

As mentioned, the more traditional and more scalable technique of spreading the stealer will be a combination of social engineering the abusing malspam campaigns – often carried out by delivering malicious documents of any kind to the victim's machine containing malicious macros (Figure 7) that downloads and execute Mars in the machine

There has been a rise in cases where campaigners will abuse the Discord infrastructure and use it as a solid loading module for their malicious content. With Mars Stealer, it's no different.

Post Infection

Mars Stealer's approach is somewhat similar to most other stealer threats. It is obviously focused on the theft of credentials from common applications, browsers and credentials stores, as well as the acquisition of potentially sensitive and valuable data from a victim machine, such as cryptocurrency wallets or other files,

Additionally, Mars Stealer can be used as a 'loader' to download and execute additional payloads from its command and control (C2) infrastructure and, notably, will terminate and delete itself upon the conclusion of its task.

In cases in which the default languages of the victim's machine are from Kazakhstan, Uzbekistan, Azerbaijan, Belarus and Russia, the stealer will not proceed with.

Calling Home

The first step Mars will take once the machine is infected is to communicate with the C&C in order to receive configurations and instructions via HTTP GET request to the gate.php file (Figure 8).

Oski Comparison

Throughout the entire operation process, Mars implements the same methods as Oski: Communication with the C&C, working directory, dependencies use and data exfiltration phase are, all the same. The differences between the two are with the type of content the info stealer will look for by default and the 2FA plugins.

Recommendations

- Employee security awareness training remains an important step in helping them identify and be suspicious of unsolicited emails and phishing campaigns, especially messages with embedded links or file attachments.
- Disable administrative tools and script interpreters, such as PowerShell, to prevent their misuse by malicious payloads.
- Use Group Policy to disable macros from running in Microsoft Office applications (legitimate macros should be digitally signed to allow for an exception to the disable rule),
- Educate users on the common TTP used and reinforce the message that documents encouraging them to 'Enable Editing', 'Enable Content' or disable any other security setting are almost certainly malicious.
- Multi-factor authentication should be implemented wherever possible to limit the effectiveness of stolen credentials.

- Employees should be reminded of the risks associated with credential reuse and weak passwords supported by password policies to encourage best practice.
- Limit user permissions according to the principal of least privilege (POLP).
- Ensure that email security controls are applied to limit the delivery of potentially malicious attachments or links to end-users, as well as implementing protocols and security controls such as DKIM, DMARC and SPF.
- Continuous monitoring of unusual endpoint behaviors such as excessive requests to specific webhosts using unusual user-agent strings, can provide an early indication of compromise.
- Consider applying deep content inspection to ensure that any downloaded content filetype matches the actual file content in addition to blocking dangerous filetypes, such as executables, for standard users.

Recommendations

Indicators of Compromise

File Samples (SHA256)

The following hashes are provided for reference, given the ongoing nature of these campaigns, it is likely that the threat actor will utilize methods to avoid detection such as packing and crypting resulting in differing cryptographic hashes.

Delivery:

- `dc52bd40b95294f98db602df36975e9c5a203a2648dd8ddc6748f2e678cc39a6`
- `2cfdba6fcd48a3047b93b72092061bf1fac2511f74f8c747215a7c3aaf2a9102`
- `ed427feb185f07a51de0194f1165ebaeb002f2b8c9b08d974219be5c6075c6f`

Mars:

- `a4d54f94d70dcb5a029d89dcd3bcda4bb5e3e0b909fbcad04bb5ed4d09459c7d`
- `031ebdaf0189694eec6b83ad26e8252547d843780563f54ec06a170f1c0e40d3`

URLs

The following URLs have been observed as used during the initial downloader phases:

- `hxxps[:]//siasky.net/OAC12bva5mDWqNV5JIvaN4K9ASZmy1rMTXxCg7lUGhUf0A`
- `hxxps[:]//plik.root.gg/file/7Pi2XabIKFrlmvfR/oF2VN0eo1Z0CGt2y/BOINCPortable_7_16_22.log`

Additionally, multiple resources hosted on the Oski Stealer C2 URL have been observed with the directory structure potentially changing between campaigns:

- `anderd2w[.]beget.tech`
- `185[.]4.65.70`
- `a0626884[.]xsph.ru`
- `panel[.]computer`
- `f0623459[.]xsph.rublitzhost.ga`

- `80[.]79.114.182`
- `test[.]akadns9[.]ne`

Source: https://cyberint.com/blog/research/mars-stealer/