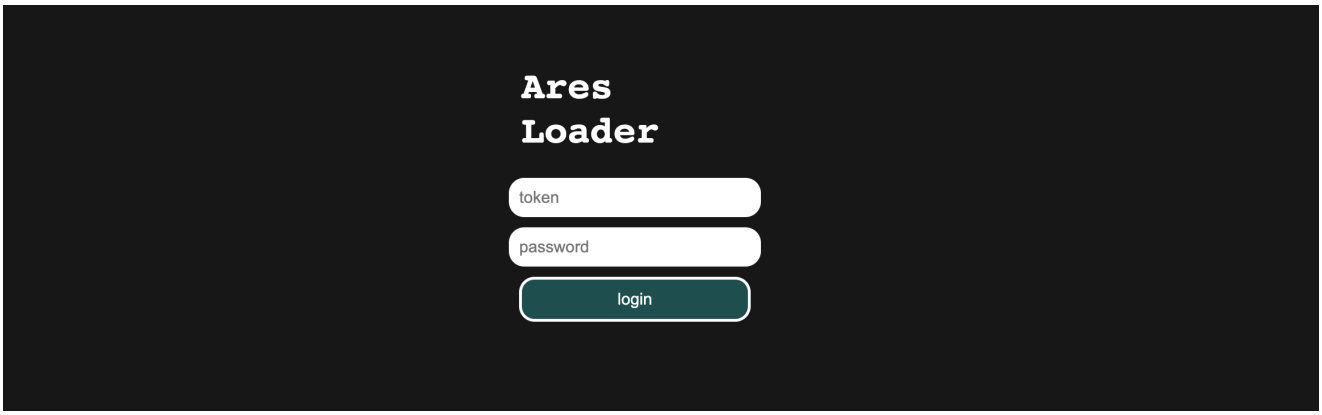
AresLoader

research.openanalysis.net/ares/aresloader/loader/2023/04/02/aresloader.html

OALABS Research April 2, 2023



Overview

AresLoader is a new malware downloader that has been advertised on some underground forums.

References

- New loader on the bloc - AresLoader
- Private Malware for Sale: A Closer Look at AresLoader

Samples

`7572b5b6b1f0ea8e857de568898cf97139c4e5237b835c61fea7d91a6f1155fb` UnpacMe

Panels

The following were live panels at the time of analysis (thanks @lloydlabs)

```
45.80.69[.]193
37.220.87[.]52
```

Note From The Developers

From the the developers themselves!

Dear Customer.
Here will be described the advantages, the rules of using the lowers you are renting.

Product name: AresLoader.

Monthly lease will cost $300. There are no discounts provided. Price includes: 5 rebuilds (including the first one), each with a partial stub cleanup (uniqueization of the binary signature). Any rebuild after that will cost $50, and this may take some time, since this service is manual, but we will not keep you waiting.
In addition, manual morphing code (for each build it is different).

==========
The way AresLoader works is that it presents itself as legitimate software (not a required feature) and then downloads the payload and puts it on the disk wherever you want. Before launching the payload, Ares launches a legitimate file.

AresLoader can ask the user admin rights (until he allows it) on behalf of cmd.exe and afterwards transfer the rights from cmd.exe to the payload.

Ares supports the ability to load encrypted payloads using AES/RSA ciphers (only use your own encoder to avoid decryption problems)

For more details about the work and functionality of the builder - contact the team, we are ready to answer any question. As the builder is in the form of a constructor, they can arise.

Due to the fact that the Lauder will be improved and we will be introducing different updates, they may be free or for a fee. In any case, we will notify you about updates and explain what and where they will be updated/modernized.

==========

There are rules for use. Attempts to change or break them will be treated critically, up to and including blocking the user.

1. Resale of license is FORBIDDEN.
2. We are not responsible for any loss to the renter.
4. It is forbidden to post the Lowder binary file in the public domain.
5. It is forbidden to upload the loeder to Virus Total.

For our part, the Development team is ready to ensure the comfortable use of our product. Soon we will be adding new updates and other additions to the functionality to improve the performance, increasing the potential of using our AresLoader. In case of any questions we are ready to get in touch with you at any convenient time and solve any arising problems. We are looking for long-term cooperation and diligent customers.

```
Sincerely, developers.
```

Analysis

The first stage is "packed" with fake API calls used to obscure a simple shellcode loader. The loader loads the 2nd stage onto the heap and executes it (yes you read the right, the heap).

Stage 2

The 2nd stage uses a custom decryption algorithm to decrypt the final stage which is loaded into a RWX section and executed. The decryption algorithm was previously observed in a malware dubbed BUGHATCH by elastic. The overlap between the two malware families is currently unclear.

Stage 3

The 3rd and final stage is composed of some shellcode and the AresLoader payload PE file. The shellode is used to execute the PE file.

Based on the strings in the payload this sample is .... `AresLdr_v_3`

The 3rd stage appears to have been around since at least 2021 in some form as this analysis report describes a most of the same functionality Anatomy of a simple and popular packer.

The purpose of the loader is to download and launch a final malware payload (technically making this a downloader not a loader). The download URLs are in plain text in the final stage and the payload is executed via `CreateProcessA`.