Negasteal Uses Hastebin for Fileless Delivery of Crysis Ransomware

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/negasteal-uses-hastebin-for-fileless-delivery-of-crysis-ransomware

By Matthew Camacho, Raphael Centeno, and Junestherry Salvador

We recently encountered a Negasteal (also known as Agent Tesla) variant that used hastebin for the fileless delivery of the Crysis (also known as Dharma) ransomware. This is the first time that we have observed Negasteal with a ransomware payload.

Only a few months ago, Deep Instinct published the first reported case of a Negasteal variant that used hastebin[.]com, a paste site for online content. Negasteal is a spyware trojan that was discovered in 2014. It offers its services in the form of paid subscriptions in cybercriminal underground forums, with its developers constantly making changes to improve its evasion tactics and remain relevant in their market.

The Crysis ransomware, meanwhile, is behind several high-profile attacks, with variants that continuously demonstrate different techniques. Similar to Negasteal, Dharma works on a ransomware-as-a-service (RaaS) model that makes it accessible for other cybercriminals to pay for.

Behavior

This is the first time that we have observed these two malware services being used together. According to the sample that we encountered, the variant arrives through a phishing email, as seen in Figure 1.

Figure 1. An image of the phishing email that was used

As part of its evasion tactics, it tries to exclude itself from debugging by Windows Defender, which it can also try to disable as a possible alternative evasion method. These tactics are shown in Figures 2 and 3.

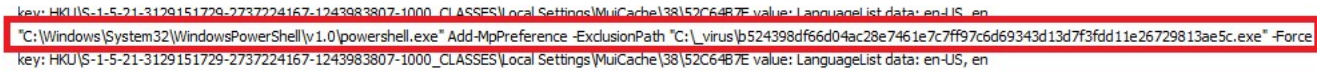

Figure 2. The malware excludes itself from being debugged.

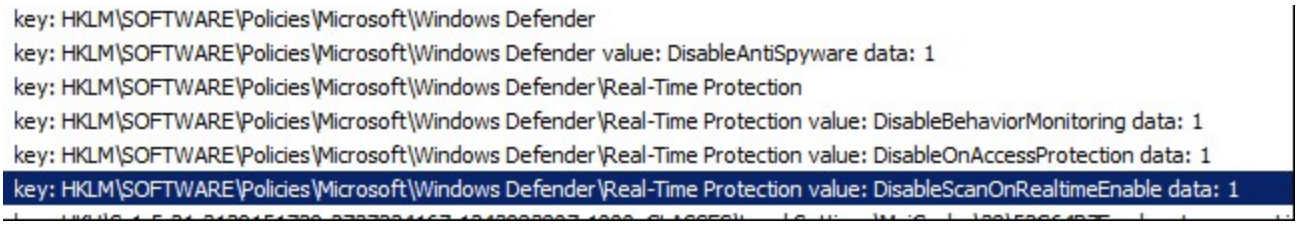

Figure 3. The malware disables Windows Defender.

For persistence, it adds itself to the startup folder and CurrentVersion\Run. Eventually, the loader will connect to “hastebin[.]com” and decode the binary (Crysis) from the command-and-control (C&C) server, thereby allowing fileless delivery of the ransomware.

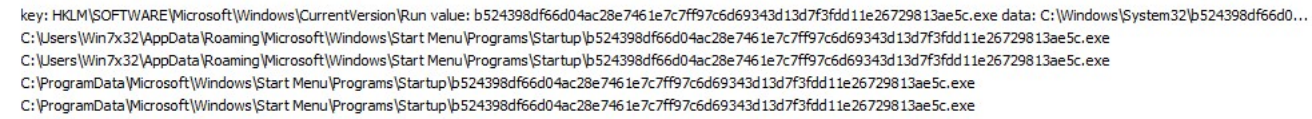

Figure 4. A snippet of the malware adding itself to the startup folder

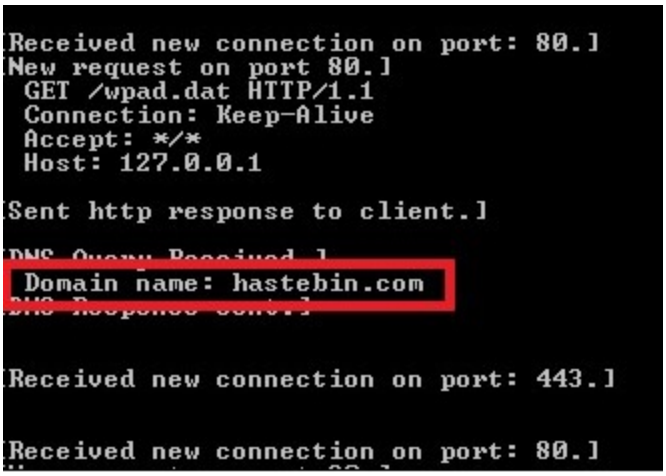

Figure 5. The malware connects to hastebin[.]com

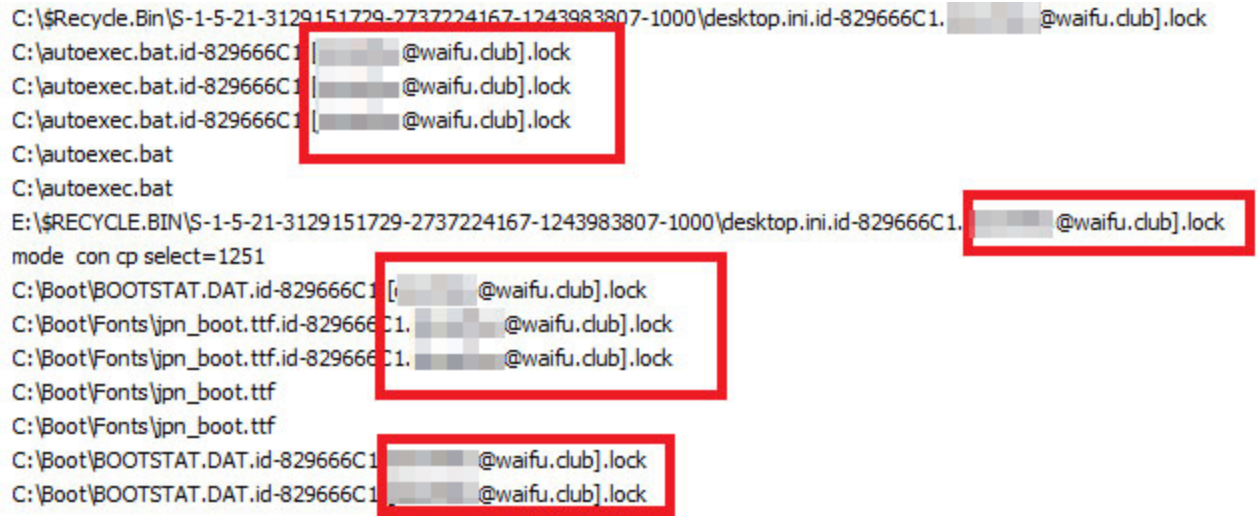

Figure 6. The Crysis ransomware payload

Security Recommendations

This campaign shows the potential of Negasteal to deliver other malware filelessly through its hastebin C&C server. The combination of these two active malware services demonstrates how cybercriminals can cobble together accessible malware in hopes of a successful campaign. Fileless delivery also adds a further challenge in removing this threat, as it leaves no trace after execution.

For organizations, following security best practices will help minimize the success of similar campaigns. As with this campaign, stopping threats from their initial entry can prevent larger problems caused by their payloads. In this case, the campaign has a ransomware payload that can encrypt important files and freeze operations.

Here are some general security practices to implement:

- Secure email gateways. Secured email gateways thwart threats that are delivered via spam and phishing. They also help users to avoid opening suspicious emails and attachments.

- Regularly back up files. This also serves as a good precaution against ransomware attacks.
- Keep systems and applications updated. Use virtual patching for legacy or unpatchable systems and software.
- Enforce the principle of least privilege. Implement network segmentation and data categorization to minimize further exposure of mission-critical data.
- Implement defense in-depth. Additional layers of security like application control and behavior monitoring help prevent the execution of anomalous files.

A multilayered security approach is advised to protect all possible threat entry points. The following solutions can help secure against a variety of threats:

- Trend Micro Apex One™ and Apex One Endpoint Sensor – Employ behavioral analysis that protects against malicious scripts, injection, ransomware, and memory and browser attacks related to fileless threats.
- Trend Micro XDR – Connects email, endpoints, servers, cloud workloads, and networks to detect and respond to threats earlier.
- Trend Micro™ Email Security – Uses enhanced machine learning and dynamic sandbox analysis for file and URL to stop email threats.

Indicators of Compromise (IOCs):

Files

- 2adb3505038e73bc83e5c5d9a60b725645fb65a7b0a781a5aadde50c942d13dc (detected as TrojanSpy.MSIL.NEGASTEAL.DYSHPF)
- b524398df66d04ac28e7461e7c7ff97c6d69343d13d7f3fdd11e26729813ae5c (detected as Trojan.MSIL.NEGASTEAL.BGO)

Payload

f3587884456922ffd42c8189e111c1184d74e12f (detected as Ransom.MSIL.DHARMA.AC)

C&C

- hxxps://hastebin[.]com/raw/avucapadey
- hxxps://hastebin[.]com/raw/molijokewe
- hxxps://hastebin[.]com/raw/sijifewopi
- 199[.]193[.]7.228

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Ransomware