Valak Downloader/InfoStealer Delivers IcedID Banking Trojan

Author: James Barnett

Overview

Between 24 June and 1 July, security researcher Brad Duncan reported four malware campaigns that used the Valak malware loader to deliver the IcedID banking trojan.[1,2,3,4]

Customer Impact

Valak is a sophisticated modular malware that acts as both a malware loader and information stealer (infostealer). It was first observed in late 2019 and quickly evolved, with the creators producing over 30 new versions of the malware in the span of just six months.[5] Valak's modular nature allows the authors to rapidly develop and deploy new malicious code to infected systems in order to expand the malware's capabilities.

IcedID is a banking trojan that uses web injection and redirection attacks to steal banking credentials, credit cards, and other financial information from victims who believe they are entering their information into a secure website.

Campaign Analysis

The reports of these Valak campaigns did not specify how the malware was initially distributed, but based on recent reports about Valak's behavior,[6] it is likely that the reported campaigns used a technique known as a "reply chain attack" to deliver the malware via email.

Unlike malicious spam (malspam) techniques that use arbitrary email accounts to indiscriminately deliver malicious emails to a large number of targets, reply chain attacks use hijacked email accounts to send targeted replies to legitimate emails sent to the hijacked account. This makes the malicious emails much harder to detect, because they appear to be legitimate responses to existing conversations sent by accounts the recipient already knows.

The bodies of emails in reply chain attacks are generally similar to those of typical malspam messages: they entice the recipients to open an attached file, or download and open a file from a provided link. According to recent reports, Valak has used both file attachments and download links in its reply chain attacks.

Attack Chain

The Valak attack chain begins when the victim downloads a password-protected ZIP file from an email attachment or link[7] and extracts it using a password contained in the body of the email. The extracted file is a malicious Microsoft Word document that instructs the victim to enable macros in order to view its contents.

When the victim does so, the macros within the document contact a PHP-based download proxy to retrieve the initial Valak dynamic-link library (DLL) payload. This behavior is similar to certain versions of Ursnif (a.k.a. Gozi) and some security solutions may incorrectly identify it as such. After downloading the Valak DLL payload, the macros use the Windows Register Server (regsrv32.exe) to register and execute it.

Upon execution, the Valak DLL drops a malicious JavaScript file with an arbitrary name and executes it using the Windows Script Host (wscript.exe). This creates registry keys to store configuration data for Valak's other components. It then reaches out to embedded command and control (C2) URLs to download two files. The first is an additional JavaScript payload that Valak saves as text within one of the aforementioned registry keys. The second is an executable that Valak's code refers to as PluginHost.exe, though the name it uses when saving the file varies between campaigns.

After downloading these additional files, the initial Valak JavaScript creates a third JavaScript file that it stores within an Alternative Data Stream (ADS) in an arbitrary file that varies between campaigns. It executes the second JavaScript payload stored in the Windows Registry. The initial JavaScript then creates a scheduled task to execute the third JavaScript, thus establishing persistence on the infected machine.

When Valak's scheduled task launches the second stage JavaScript payload, it executes PluginHost.exe to manage Valak's various plugin modules. It then downloads additional payload(s) from its C2, saves them as ADSs in arbitrary files, then executes them. In these campaigns, the payload it delivered was an installer for the IcedID banking trojan.

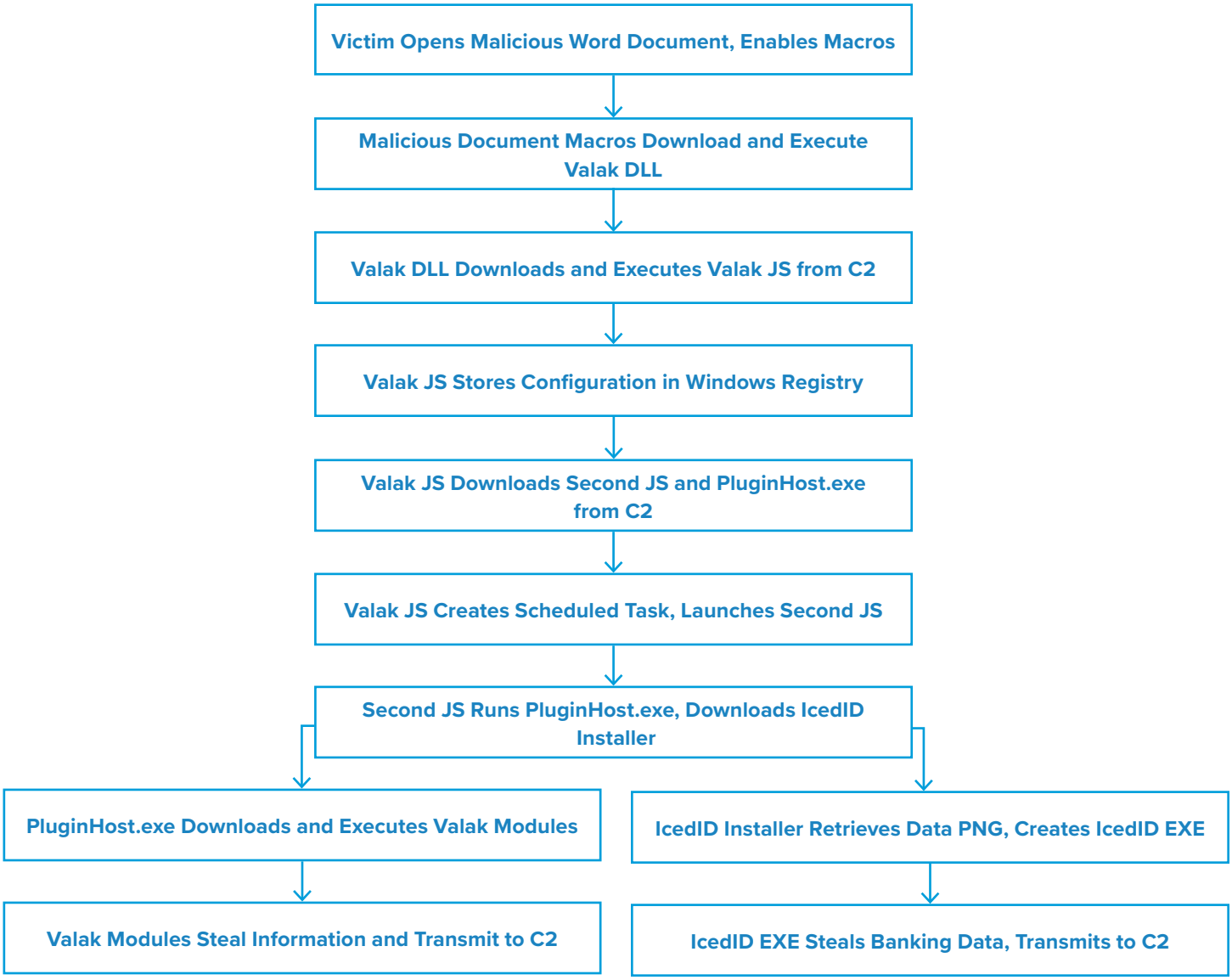
When PluginHost.exe is executed, it contacts the Valak C2 to download and install various plugin modules to expand the malware's capabilities. These modules currently include various types of reconnaissance and information stealers, but Valak may expand to include other types of modules in the future. One of Valak's most notable modules is Exchgrabber, which can steal email credentials from the infected system as well as any internal Microsoft Exchange email servers it is connected to. It then sends this information to its C2, enabling the attacker to execute reply chain attacks using the stolen email credentials.

When the IcedID installer is executed, it retrieves a PNG image with embedded data, then uses it to generate an IcedID EXE. The IcedID EXE generates a second EXE to establish persistence, then steals banking data and transmits it to its C2.

Vulnerabilities & Mitigation

Infoblox recommends the following actions to reduce the risk of this type of infection:

- Be aware of the possibility of reply chain attacks and do not assume that a file attachment or link is safe simply because the sender is familiar.
- Always be suspicious of vague emails, especially if there is a prompt to open an attachment or click on a link.
- If clicking on a link immediately initiates an attempt to download a file, that file is suspicious. Inspect it carefully.
- Never enable macros, and do not configure Microsoft Office to enable macros by default.



Endnotes

1. http://malware-traffic-analysis.net/2020/06/24/index.html
2. http://malware-traffic-analysis.net/2020/06/26/index.html
3. http://malware-traffic-analysis.net/2020/06/30/index.html
4. http://malware-traffic-analysis.net/2020/07/01/index.html
5. https://www.cybereason.com/blog/valak-more-than-meets-the-eye
6. https://labs.sentinelone.com/valak-malware-and-the-connection-to-gozi-loader-confcrew/
7. https://twitter.com/malware_traffic/status/1278481732413657088

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com