Hancitor Downloader Delivers Cobalt Strike and Ficker Stealer

Author: James Barnett

Overview

On 18 March, security researcher Brad Duncan reported a malspam campaign that used DocuSign-themed lures to entice users to download and open Microsoft Word documents with malicious macros that install embedded copies of the Hancitor trojan downloader.[1] These copies of Hancitor delivered additional payloads containing Cobalt Strike and Ficker Stealer.

Customer Impact

Hancitor is a trojan downloader that targets businesses and individuals around the world. It is distributed via malspam sent by compromised servers in many countries, including the United States, Japan and Canada. These malicious emails mimic notifications from legitimate organizations to entice the user to download a weaponized Microsoft Office document.

Infoblox has reported on multiple Hancitor campaigns in the past, most recently in December 2020.[2,3] Hancitor's core characteristics have remained the same since our last report, and this new campaign is notable for how similar it is to the one we previously reported. Both campaigns use a nearly identical lure and deliver the same types of malware payloads. This may indicate that the threat actors behind Hancitor have become comfortable with this pattern of attack. If so, we could see more campaigns with similar lures and payloads in the future.

Campaign Analysis

The emails in these campaigns used a DocuSign lure to entice targets into opening links in the messages. The subject lines of the messages indicated that the target had a pending invoice or notification from DocuSign. Each email contained an embedded link leading to a Google search redirect page.

Attack Chain

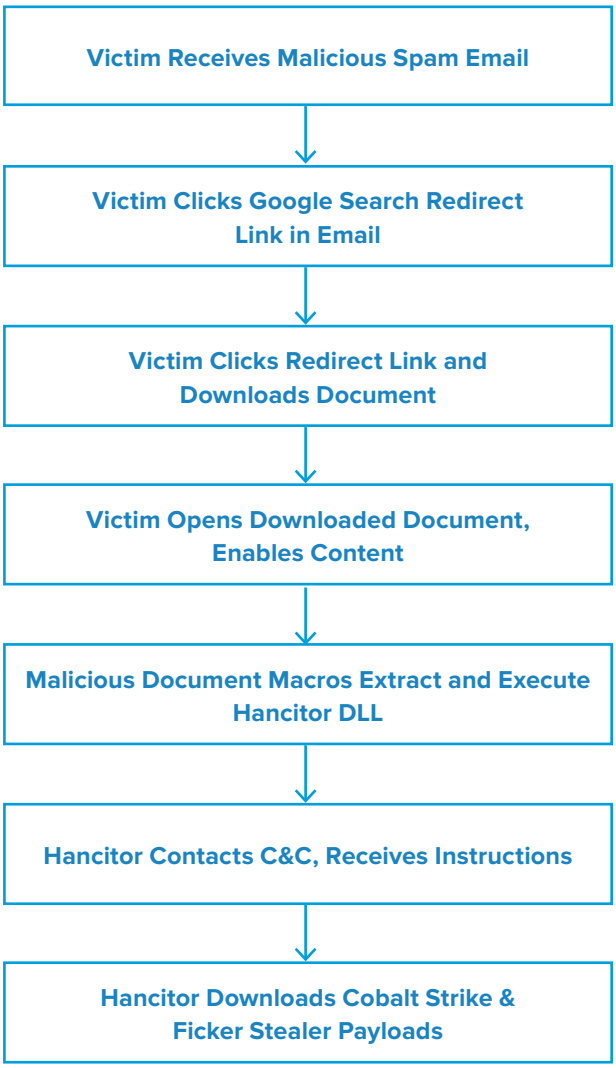
When the victim clicks the link in the initial Hancitor malspam message, they are taken to a generic Google redirect page informing them that they are being redirected to another URL. If the user clicks the redirect link on this page, they will be sent to a page that downloads a Microsoft Word document containing malicious macros. Once this download begins, the page subsequently redirects them to DocuSign's legitimate website to enhance the illusion that the malicious document is actually from DocuSign.

When the victim opens the downloaded Word document, it displays a message instructing the viewer to enable content. If the victim does so, the malicious macros in the document will execute. These macros then extract and execute the Hancitor payload dynamic-link library (DLL) embedded within the Word document, thus establishing the initial Hancitor infection.

Once Hancitor infects the victim's system, it sends some basic information about the system to one of its three hardcoded command and control (C&C) servers. The server responds with further instructions that direct Hancitor to download and execute one or more additional malware payloads. In these campaigns, Hancitor delivered two additional payloads.

The first additional payload was Cobalt Strike, a legitimate penetration testing tool that has become increasingly popular amongst threat actors. Its features include infostealer capabilities such as keylogging, exploits that can leverage system vulnerabilities to facilitate additional attacks, and various methods to help conceal its activity on both the infected system and the victim's network.[4]

The second follow-on payload was Ficker Stealer, a relatively new malware-as-a-service (MaaS) infostealer that was initially identified in August 2020.[5] According to the author of Ficker Stealer, the malware is capable of stealing web browser passwords, cryptocurrency wallets, FTP) client information, credentials stored by Windows Credential Manager and session information from various chat and email clients.[6]



Vulnerabilities & Mitigation

- If a well-known company provides a link, that link should generally point to the company's domain (e.g. "http://fedex[.]com" if the sender is FedEx).
- Be suspicious of links that immediately attempt to download a file when clicked.
- Do not enable macros in a Microsoft Office attachment, especially if the file's only apparent content is a message with instructions to enable macro.

Endnotes

1. https://www.malware-traffic-analysis.net/2021/03/18/index.html
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--69
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--96
4. https://www.cobaltstrike.com/features
5. https://twitter.com/Cyber_Bolo/status/1294576137495023616
6. https://twitter.com/3xp0rtblog/status/1321209656774135810