Final Project Script

Hello to all! We are Mike and Todd from team MET-Amorphic, and today we will walk you through our analysis of a cybersecurity incident that shows how clicking one link can lead to at least 3 pieces of malicious code infecting your computer in under 3 minutes.

Hancitor

It all starts on February 8, 2021 at 10:59 AM. A user, Bill Cook, has downloaded a Microsoft Word document at 'tonmatdoanminh.com/uninviting.php'. This macro-enabled word document contains scripts that start the infection process. Opening the document with macros enabled begins the infection with Hancitor, a malware loader that has existed since 2013 is still used by threat actors today due to its speed and simplicity.

First, the script reaches out to api.ipify.org. On its own, a user contacting ipify.org is not considered a threat-related incident, but the api sub-domain indicates that this is part of an automated process. The script gathers the internet-facing IP address of Bill Cook's machine, and contacts 'satursed.com' with a POST request containing user, and machine information..

Cobalt Strike

With this user and machine information, Bill's machine contacts 'roanokemortgages.com' and starts downloading. It collects two binary files and one shellcode trojan that appears to be a meterpreter backdoor. Cobalt Strike is a commercially available pentesting tool that, due to its malleability, is difficult to design firewall rules for. In this scenario, Cobalt Strike was used to set up a persistent backdoor over HTTPS.

Ficker Stealer

While still in contact with roanokemortgages.com the machine downloads another executable file. This is Ficker, which is a credential-stealing Malware-as-a-service (MaaS) from Russia. Ficker sends encrypted login and password data to a command and control client. This data is exfiltrated from the victim machine's web browsers and other applications like discord and steam.

Remediation

Since Cobalt strike is a persistent backdoor that writes to Windows system hosts, we recommend a containment strategy of removal from the network, followed by a reformatting and clean install of the operating system. Bill should also make sure to change all passwords. Moving forward, a combination of user education and security policy can help prevent incidents like this. Security profiles should be set to disallow macro-enabled files by default and users trained not to enable macros from any unknown source. While Cobalt Strike is difficult to detect with simplified firewall rules, there are rules for malware-detection systems like YARA that can identify and block Ficker traffic.