Infoblox
NEXT LEVEL NETWORKING

Brushaloader Malware

Author: Chris Kim

Overview

During 25 February through 1 March, security researchers on Twitter reported several domains affiliated with a malware loader called Brushaloader.[1] With further research, we found additional information about the campaigns that used the domains. These campaigns distributed Brushaloader via emails containing weaponized files and specifically targeted users in Poland. Brushaloader campaigns have also targeted other European countries including Ukraine, Italy, Germany, and Austria.

Customer Impact

When Talos first discovered Brushaloader in August 2018, the threat actors were primarily targeting Polish victims using Polish language emails.[2] The campaigns often distributed RAR attachments embedded with Visual Basic script (VBScript) that infects devices with Brushaloader, which then downloads and executes other malware such as Danabot.

Danabot is a modular banking trojan that can remotely control victims' computers and harvest passwords from a number of applications such as browsers, file transfer protocol (FTP) clients, virtual private network (VPN) clients, chat services, email systems, or poker programs.[3]

Campaign Analysis

The campaigns that used the domains reported recently on Twitter distributed Brushaloader via spam emails themed around the Polish term "Faktura," meaning invoice. One of the emails in the current campaigns carried a compressed file named faktura022019.tar - in this case a TAR rather than an RAR. When we extracted it, we found a VBScript named deklaracja.vbs. "Deklaracja" is Polish for declaration or statement.

Attack Chain

Once the VBScript executed, it produced a dialog box that printed numeric characters of the Fibonacci sequence. The downloader functionality of the VBScript file did not activate until we clicked on the "ok" button. This is a technique used to evade detection by automated malware systems.

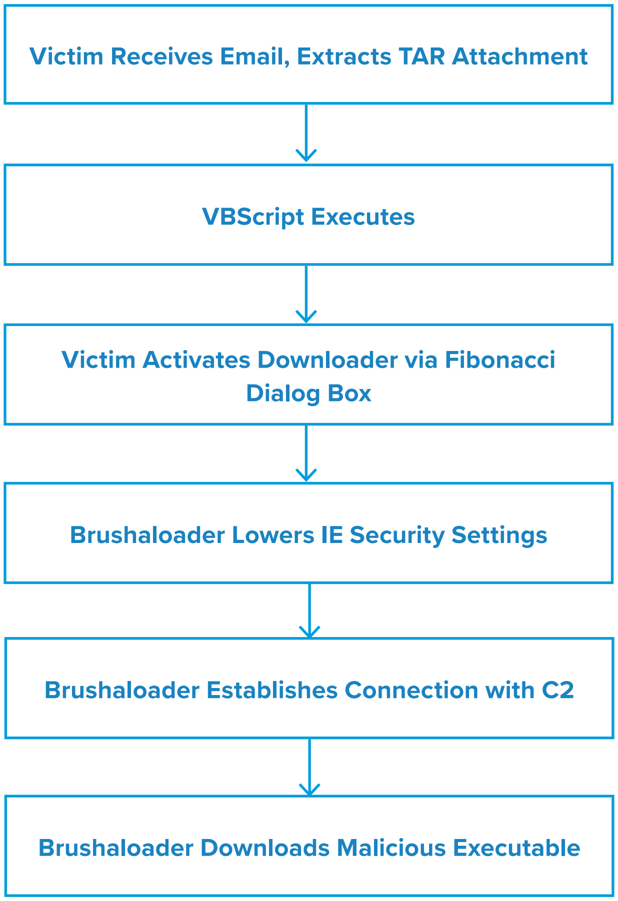
We then saw the VBScript lower the security settings of Internet Explorer (IE) by modifying its registry subkey. The infected machine then made an HTTP POST request to its command and control (C2) at wwebsservice[.]info over port 443, and resolving to IP address 50[.]2[.]39[.]247.

We did not observe further activity in the sandbox. However, normally, infected clients establish interactive sessions with the C2 and receive PowerShell commands. Brushaloader uses the victim's system information to determine what modules need to be delivered so that it can install additional malware - like Danabot - which has a modular design.

Vulnerabilities & Mitigation

Infoblox recommends the following precautions and mitigation strategies:

- Enable strong email security solutions that can detect malicious emails and send them to quarantine.
- Be wary of unfamiliar email senders or emails that contain compressed attachments.
- Be cautious of attachments that are unusually small in size; Brushaloader TAR and RAR files are between 500B and 4KB.
- Use a reputable antivirus program that can prevent malware from activating in the event a user accidentally opens a malicious attachment.
- Enabling PowerShell logging can prove valuable during incident investigation, since Brushaloader and other malware receive PowerShell commands from their C2.



Victim Receives Email, Extracts TAR Attachment

VBScript Executes

Victim Activates Downloader via Fibonacci Dialog Box

Brushaloader Lowers IE Security Settings

Brushaloader Establishes Connection with C2

Brushaloader Downloads Malicious Executable

Endnotes

1. https://twitter.com/search?q=%23brushaloader&src=typd&lang=en
2. https://blog.talosintelligence.com/2019/02/combing-through-brushaloader.html
3. https://www.welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/

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