Trickbot WHO?

Author: James Barnett

Overview

From 21 to 24 March, Infoblox observed another malicious spam (malspam) email campaign that used a fraudulent Coronavirus alert from the World Health Organization (WHO) to deliver Trickbot banking malware.

In the Appendices of our previous two Cyber Campaign Briefs, we included indicators from a campaign impersonating the director of the WHO and delivering the Hawkeye keylogger malware,[1] as well as indicators from a campaign spoofing messages from the WHO to deliver the Formbook infostealer.[2]

Customer Impact

Trickbot is a modular banking trojan that targets customers of major banks. Once Trickbot infects a victim, it will attempt to steal sensitive financial information and exfiltrate that data to a command and control (C2) server. Trickbot also attempts to move laterally across vulnerable networks to infect additional systems.

Trickbot's modular nature allows the authors to rapidly develop and deploy new malicious code to infected systems. One of Trickbot's newest modules allows it to brute force Remote Desktop Protocol (RDP) connections,[3] which gives it an additional way to move laterally within networks.

Campaign Analysis

The Trickbot campaign that Infoblox observed used a Coronavirus theme to lure recipients into opening a malicious Microsoft Word document. Each of the messages we observed had the sender name "World Health Organization" and subject line "Coronavirus: an important information about precautionary measures for the enterprises."

The bodies of the messages informed the recipient that there were recorded Coronavirus cases in their region and encouraged them to open the attached document to receive a list of precautionary measures published by the WHO.

Attack Chain

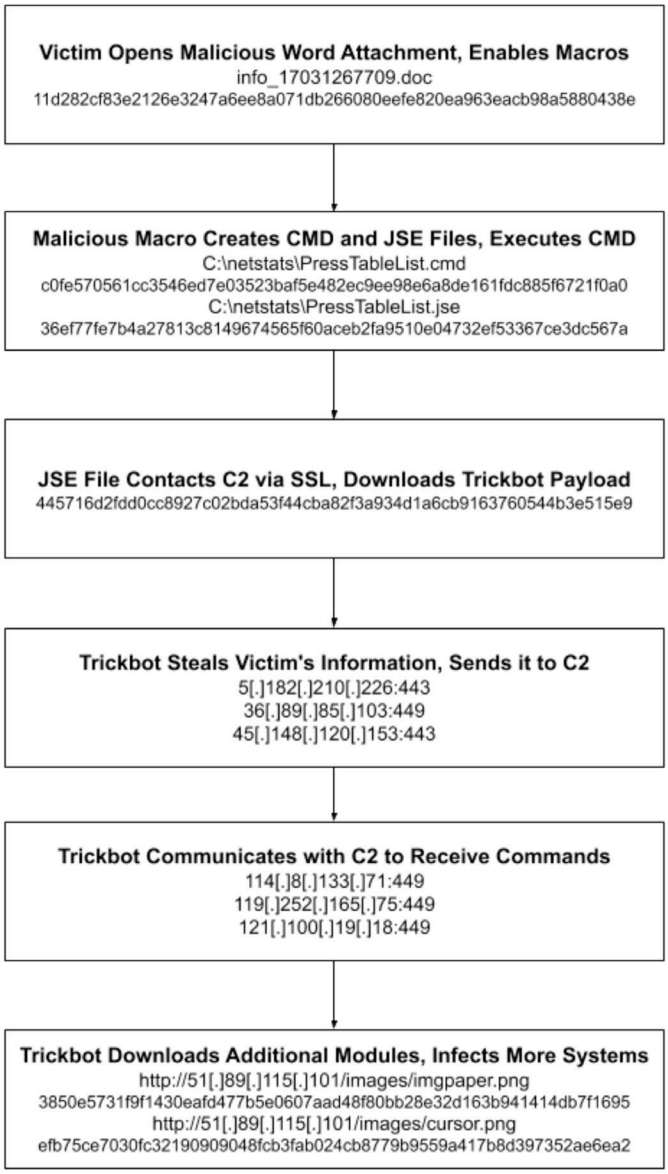
When the recipient opens the malicious Word document and enables macros, the macros within the document create a new directory, *C:\netstats*, and generate two files within it.

The first, *PressTableList.jse*, is a Microsoft JScript file containing the malicious payload. The second is a basic Windows command (CMD) file, PressTableList.cmd, that is used to execute the malicious JScript. Once these files are created, the macro executes the CMD file, which executes the JScript file.

Upon execution, the JScript file generates a fake error notification that the document failed to open properly, and proceeds to download and execute the initial Trickbot payload.

Once Trickbot is installed, it proceeds to steal the victim's information and communicate with its various C2 servers in order to transfer stolen information, receive commands, and download modules that expand the malware's capabilities.

In this campaign, we observed Trickbot downloading two additional modules, both of which were EXE files that used a PNG file extension to avoid suspicion. The settings file produced by the original Trickbot payload identified one of these modules as "pwgrab," which expands Trickbot's credential-stealing capabilities.[4] The second module was not identified.



Vulnerabilities & Mitigation

Threat actors often use current events to lure victims into opening malicious files. Infoblox recommends the following actions to reduce the risk of this type of infection:

- Regularly train users to be aware of potential phishing efforts and how to handle them appropriately.
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Never enable macros and do not configure your settings to enable macros by default. They are a common infection vector that many families of malware use.
- Ensure your system's file sharing and remote desktop capabilities are disabled or protected with a strong password.

Endnotes

1. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--65
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--63
3. https://labs.bitdefender.com/2020/03/new-trickbot-module-bruteforces-rdp-connections-targets-select- telecommunication-services-in-us-and-hong-kong/
4. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/trickbot-s-updated-password-grabbing-module-targets-more-apps-services

Appendix

Representative Indicators of Compromise	Description
Coronavirus: an important information about precautionary measures for the enterprises	Trickbot malspam email subject
info_1599267609.doc info_1599267613.doc info_1599267615.doc info_1599267640.doc info_1599267644.doc info_1599267646.doc info_1599267741.doc info_17031267636.doc info_17031267641.doc info_17031267683.doc info_17031267705.doc info_17031267709.doc info_17031267726.doc info_1703267633.doc info_1703267711.doc info_17033267648.doc info_17033267667.doc Info_181338267627.doc	
0797840b727c56685607c6818ae81a8792c82148303ddeae143e7a028b3e8594 11d282cf83e2126e3247a6ee8a071db266080eefe820ea963eacb98a5880438e 2e83016b063a59a20334df2cd1fdedd876778a477fd050d73d76b0df202170a5 2ffa995eb56877969490ceae4521e3de84183e83f5c67c137e34431431628df0 38ba1134ff906ad39182ee20ab716737ed986f50397c04b7ab445cf8abe456b7 46725bcecf7f03eb8ffa87d3c00e3d71953cf0d0642bc773fd3aa5654df8c946 48abb8aa3a7f30496a46a241e25ab12a6baa57747756d23f44472b5a9cb9a568 67198b0578acffd0e3d1b6025992ff4014c48c38b55534d816bf5a17e2d631d4 6d195f3b7f86d650e305c5090c0e7036b8f77eca07800f078bd6cf6459d03606 6e7ea621d4f0761209fc3d00b13eb576b94e2af17c00b99ff53bcf1d46571bcf 966e5243f2fa2cc6bbb80c09d97b521c93fca10c05a12f288aa2f7ce425b716b 9c36be78c80bca0de229c6678f611f8434d15b0d1ea5b6fa7e45d8e364165738 abc5c6b2de5bf602f72390d7d4ef995dad7c3940cf549585d50fd71512f05043 af7b6b9bd92f0e257e394cfb865cb5249526ed5e62388318ec2ff0bc7dd43e59 dabecd7f330e511d4d578937790519fa41e5844d5f921baa700265e7f4a62985 e78f30be1256c2aba7cbd500cf5fd009916958150de913b0e8a35651a11cc65a edaf28e0395d0d310dcd53dc1f3c263c4323d562e29730c2437c0737ded6e676 f3b086bfc251b108753967d8ced29b6b75b4d573f96634b593c4b5390df7131b	Trickbot malicious document sha256
C:\netstats\PressTableList.cmd c0fe570561cc3546ed7e03523baf5e482ec9ee98e6a8de161fdc885f6721f0a0	Trickbot command script
C:\netstats\PressTableList.jse 36ef77fe7b4a27813c8149674565f60aceb2fa9510e04732ef53367ce3dc567a	Trickbot JScript downloader
445716d2fdd0cc8927c02bda53f44cba82f3a934d1a6cb9163760544b3e515e9	Trickbot payload sha256
http://51.89[.]115.101/images/cursor.png http://51.89[.]115.101/images/imgpaper.png	Trickbot EXE module download URL

3850e5731f9f1430eafd477b5e0607aad48f80bb28e32d163b941414db7f1695 efb75ce7030fc32190909048fcb3fab024cb8779b9559a417b8d397352ae6ea2	Trickbot EXE module sha256
5[.]182[.]210[.]226:443 36[.]89[.]85[.]103:449 45[.]148[.]120[.]153:443 46[.]17[.]107[.]65:443 46[.]174[.]235[.]36:449 51[.]254[.]164[.]244:443 51[.]254[.]164[.]245:443 51[.]89[.]73[.]158:443 114[.]8[.]133[.]71:449 119[.]252[.]165[.]75:449 121[.]100[.]19[.]18:449 131[.]161[.]253[.]190:449 146[.]185[.]253[.]178:443 170[.]84[.]78[.]224:449 171[.]100[.]142[.]238:449 172[.]245[.]156[.]138:443 180[.]180[.]216[.]177:449 181[.]112[.]157[.]42:449 181[.]113[.]28[.]146:449 181[.]129[.]104[.]139:449 181[.]129[.]134[.]18:449 181[.]140[.]173[.]186:449 181[.]196[.]207[.]202:449 185[.]14[.]31[.]252:443 185[.]20[.]185[.]76:443 185[.]203[.]118[.]37:443 185[.]62[.]188[.]159:443 185[.]99[.]2[.]115:443 185[.]99[.]2[.]221:443 186[.]232[.]91[.]240:449 186[.]71[.]150[.]23:449 190[.]214[.]13[.]2:449 192[.]210[.]226[.]106:443 194[.]5[.]250[.]150:443 195[.]123[.]239[.]67:443 200[.]127[.]121[.]99:449 200[.]21[.]51[.]38:449 202[.]29[.]215[.]114:449 217[.]12[.]209[.]200:443	Trickbot C2 IP & port