Group Behind TrickBot Spreads Fileless BazarBackdoor

trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/group-behind-trickbot-spreads-fileless-bazarbackdoor

A new campaign is propagating a new malware named “BazarBackdoor,” a fileless backdoor reportedly created by the same threat actors behind TrickBot, as reported by BleepingComputer. The conclusion is drawn due to similarities in code, crypters, and infrastructure between the two malware variants.

The social engineering attacks that were used to spread the backdoor leverage topics such as customer complaints, Covid-19-themed payroll reports, and employee termination lists for the emails they send out. The messages have links to Google Docs files. Once the users click the links, they will be redirected to a landing page. The pages state that the Word Document, Excel Spreadsheet, or PDF cannot be properly viewed. It then instructs the user to click on a link to open the file.

Clicking on the link downloads an executable that masquerades through icons and names associated with the mentioned file types. For instance, the supposed customer complaint document will be downloaded as Preview.PDF.exe, which uses the PDF icon. Since the file extension is hidden by default, the file will convincingly appear as a PDF file.

The disguised executable serves as the loader for the backdoor. After launching the file, the loader sleeps for some time, then connects to command and control (C&C) servers to check-in and download the payload. The payload will then be injected filelessly into C:\Windows\system32\svchost.exe through process hollowing and process doppelgänging techniques. The backdoor will be installed on the computer.

This sets a scheduled task that launches the loader every time the user logs into Windows, which makes way for new versions of the backdoor to be downloaded and injected into svchost.exe. Security researchers Vitali Kremez and James revealed that this malware was most likely created by the threat actors behind TrickBot trojan. This is because both malware types use the same crypter and email chain deliverables. Both malware also utilize the Emercoin DNS resolution service for C&C server communication.

Defense against fileless threats

Fileless threats are stealthy and difficult to detect because they take advantage of existing applications to infiltrate and attack systems. However, users can still defend against these malware types by adhering to the following best practices:

[Related: Risks Under the Radar: Understanding Fileless Threats]

- Secure possible entry points. Malicious sites, spam, and third-party components like browser plug-ins can all be sources of fileless malware. Be cautious when downloading attachments and other files, and never click links from unfamiliar sources.

- Reboot device and change passwords. In case of infection, users can stop fileless attacks that do not employ persistence techniques by restarting the device. As an extra precaution, users should also change their passwords.
- Utilize behavior monitoring and analysis. These can detect and block malicious behaviors and routines associated with malware, stopping threats before they can reach the system.

To further secure the system, the following security solutions are recommended:

Indicators of Compromise

SHA-256	Detection Name
11b5adaefd04ffdaceb9539f95647b1f51aec2117d71ece061f15a2621f1ece9	Trojan.Win64.TRICKBOT.CFI
1e123a6c5d65084ca6ea78a26ec4bebcfc4800642fec480d1ceeafb1cacaaa83	Trojan.Win64.TRICKBOT.CFJ
37d713860d529cbe4eab958419ffd7ebb3dc53bb6909f8bd360adaa84700faf2	Trojan.Win64.TRICKBOT.CFL
4e4f9a467dd041e6a76e2ea5d57b28fe5a3267b251055bf2172d9ce38bea6b1f	Trojan.Win64.TRICKBOT.CFK
55d95d9486d77df6ac79bb25eb8b8778940bac27021249f779198e05a2e1edae	TrojanSpy.Win64.LOKI.A
5a888d05804d06190f7fc408bede9da0423678c8f6eca37ecce83791de4df83d	Trojan.Win64.TRICKBOT.CFL
5dbe967bb62ffd60d5410709cb4e102ce8d72299cea16f9e8f80fcf2a1ff8536	TrojanSpy.Win32.TRICKBOT.THAOFBO
6cbf7795618fb5472c5277000d1c1de92b77724d77873b88af3819e431251f00	Trojan.Win32.TRICKBOT.TIGOCBAINS
835edf1ec33ff1436d354aa52e2e180e3e8f7500e9d261d1ff26aa6daddffc55	TrojanSpy.Win64.LOKI.A
859fa9acf0b8a989a1634a1eee309355438b9f6b6f73b69f12d53ac534618c6a	Trojan.Win64.TRICKBOT.CFK
a76426e269a2defabcf7aef9486ff521c6110b64952267cfe3b77039d1414a41	Trojan.Win64.TRICKBOT.CFJ
c55f8979995df82555d66f6b197b0fbcb8fe30b431ff9760deae6927a584b9e3	Trojan.Win64.TRICKBOT.CFL
ce478fdbd03573076394ac0275f0f7027f44a62a306e378fe52beb0658d0b273	Trojan.Win64.TRICKBOT.CFM
e90ccb9d51a930f69b78aa0d2612c4af2741311088b9eb7731857579feef89c3	Trojan.Win64.TRICKBOT.CFL

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats