Fileless Botnet Novter Spread Via KovCoreG Campaign

blog.trendmicro.com/trendlabs-security-intelligence/new-fileless-botnet-novter-distributed-by-kovcoreg-malvertising-campaign/

October 1, 2019

Cyber Threats

We found a new modular fileless botnet malware, which we named “Novter,” that the KovCoreG campaign has been distributing. We’ve been actively monitoring this threat since its emergence and early development, and saw it being frequently updated.

By: Jaromir Horejsi, Joseph C Chen, Ecular Xu October 01, 2019 Read time: (words)

We found a new modular fileless botnet malware, which we named “Novter,” (also reported and known as “Nodersok” and “Divergent”) that the KovCoreG campaign has been distributing since March. We’ve been actively monitoring this threat since its emergence and early development, and saw it being frequently updated. KovCoreG, active since 2011, is a long-running campaign known for using the Kovter botnet malware, which was distributed mainly through malvertisements and exploit kits. Kovter has been involved in click fraud operations since 2015, using fraudulent ads that have reportedly cost businesses more than US$29 million. The botnet was taken down at the end of 2018 through concerted efforts by law enforcement and cybersecurity experts, including Trend Micro.

The dismantlement hasn't deterred the cybercriminals. Though the botnet is dead, we noticed that the KovCoreG campaign didn't stop their activities and instead developed another botnet. Working with ProofPoint's threat researcher Kafeine, we were able to uncover a new fileless botnet malware — Novter — being distributed by the operators of KovCoreG.

While the malvertising attacks were originally focused on U.S.-based users, they have since expanded to several European countries starting this summer. Our telemetry also revealed that the malvertising attacks were being distributed through a few of top 100 websites in the U.S., which were also abused by Kovter in their previous activities. Our analysis of Novter, particularly its most notable modules, are detailed in this ***technical brief***.

Figure 1. Infection chain of KovCoreG, Novter, and Nodster

KovCoreG's attack chain

KovCoreG's attacks are socially engineered malvertisments that lure unwitting users into downloading a software package needed to update their supposedly out-of-date Adobe Flash application. However, it instead drops a malicious HTML application (HTA) file named *Player{timestamp}.hta*. When the victim executes the HTA file, it will load additional scripts from a remote server (communication is RC4-encrypted) and run a PowerShell script that appears to take inspiration from the open-source Invoke-PSInject project.

Figure 2. Screenshot showing an example of KovCoreG's malvertisements (captured by ProofPoint)

Figure 3. Snapshot of KovCoreG's malvertisement traffic (captured by ProofPoint)

The PowerShell script, in turn, will disable Windows Defender and Windows Update processes. It runs a shellcode to bypass User Account Control (UAC) via the CMSTPLUA COM interface (related to connection management). The PowerShell script is also embedded with Novter, which will be executed filelessly via the PowerShell reflective injection technique.

Analysis of the Novter malware

Novter is a backdoor in the form of an executable file. Immediately after its execution, it performs the following anti-debugging and anti-analysis checks:

- Searching for blacklisted processes and modules by comparing the CRC32 algorithms of their names with a list of hardcoded CRC32s
- Checking if the number of cores is too small
- Checking if the process is being debugged
- Checking if the Sleep function is being manipulated

If it finds any of aforementioned information, it is then reported to the C&C server. Note that it uses different sets of C&C servers for different purposes. One set, for instance, is solely used for anti-analysis reporting. After the affected machine's environment is double-checked and reported, the malware goes to sleep for a long time.

The backdoor commands that Novter supports are:

- killall — Terminate a process and delete a file (for all modules)
- kill — Terminate a process and delete a file (for a specific module)
- stop — Terminate the process without deleting its file (for a specific module)
- resume — Start a process (for a specific module)
- modules — Download and execute an additional module
- update — Download a new version and install the update
- update_interval — Set an interval between two consecutive update attempts

Novter communicates with its command-and-control (C&C) servers and downloads multiple JavaScript modules for different purposes. We have identified three Novter modules, which include:

- A module that shows a technical support scam page on the victim's machine
- A module that abuses WinDivert (Windows packet divert, a tool that enables network packets sent to and from Windows network stacks to be captured, modified, or dropped) to block the communication from processes like those from antivirus (AV) software
- A module (which we named "Nodster") that is written with NodeJS and io for proxying network traffic. We consider it a module responsible for building the proxy network needed to support the click fraud operations.

Analysis of Novter's module "Nodster"

During our analysis of Novter, we came across three notable modules downloaded by the malware. One of them, which we named "Nodster," is a network proxy module. The module installs NodeJS on the victim's machine and executes a NodeJS script "app.js" in the background. The script will connect to an embedded C&C server address and receive the second C&C server address.

It will then establish a backconnection to the second C&C server with the socket.io protocol. The second C&C server will return commands to instruct the module to make a TCP connection, send a TCP payload, and return the response from the server back to them. This turns the system infected with Novter become a proxy for the attacker to use.

Figure 4. The communication flow between the Nodster proxy and C&C servers

Correlating Nodster's traffic

During the course of our research, we observed lots of encrypted traffic proxied through the Nodster module, but we managed to decrypt some of it, which showed scripts used for web advertising. This indicates that the C&C server instructed the infected machine to open a website with an embedded JavaScript code related to displaying advertisements.

We also noticed that the ad traffic appeared to have been sent from Android devices, since the HTTP(S) requests transferred through the proxy had HTTP User-Agent headers from Android devices. These requests are appended with a "X-Requested-With" header with many Android app names. We inspected those apps on the Google Play store because we initially thought that the traffic could have been generated by these applications. However, we did not find any suspicious code in these applications that would have generated this traffic. We didn't find any similar code shared between these Android applications either.

Figure 5. The HTTPS request header spoofed to be from an Android device

With this finding, we inferred that the ad traffic was not coming from the mobile devices, but was instead being generated by the attacker. The attacker disguised the traffic to appear as if it was being sent from Android devices and mobile applications and proxied them through the Novter/Nodster botnet. After all, KovCoreG's operations involved click fraud.

Defending against Novter

Advertisements are an innocuous online staple, but KovCoreG's campaign demonstrates how they can be intrusive, not to mention how Novter can expose the user's system to other and actual threats. Given how KovCoreG engages in click fraud, it can significantly affect businesses. A single mobile ad fraud incident in 2018, for instance, cost Google and its partners around US$10 million in losses.

Novter also exemplifies fraudsters' maturing techniques with its use of fileless infection methods and obfuscating its C&C connections and fraud-related traffic. Users, for their part, should adopt best practices, especially against socially engineered threats like malvertisements.

Trend Micro endpoint solutions, such as the Smart Protection Suites and Worry-Free Business Security that have behavior monitoring capabilities, can protect users and businesses from threats like Emotet by detecting malicious files, scripts, and messages as well as blocking all related malicious URLs. Trend Micro Apex One™ protection employs a variety of threat detection capabilities such as behavioral analysis, which protect against malicious scripts, injection, ransomware, memory and browser attacks.

The full details of our research on Novter is in this ***technical brief***, while the indicators of compromise (IoCs) are in this ***appendix***.

Hat tip to ProofPoint's researcher Kafeine whom we worked with in this research.