ESET researchers disrupt cryptomining botnet VictoryGate

eset.com/int/about/newsroom/press-releases/research/eset-researchers-disrupt-cryptomining-botnet-victorygate/

23 Apr 2020

Next story

23 Apr 2020

BRATISLAVA, BUENOS AIRES – ESET researchers have recently discovered a previously undocumented botnet named VictoryGate. It has been active since at least May 2019, and is composed mainly of devices in Peru, where over 90% of the infected devices are located. The main activity of the botnet is mining Monero cryptocurrency. The victims include organizations in both public and private sectors, including financial institutions. Thanks to data obtained during this research and shared with the nonprofit Shadowserver Foundation, at least a portion of the botnet operation has been disrupted.

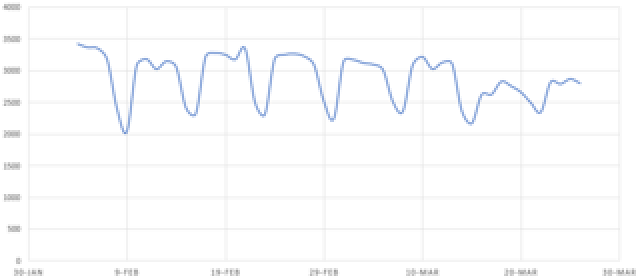
ESET researchers have been “sinkholing” several domain names that control the botnet’s actions, replacing them with machines that do not send the botnet’s slave computers the commands they expect, but simply monitor botnet activity. Based on this data and ESET telemetry, ESET estimates that at least 35,000 devices became infected with VictoryGate at one point or another during this campaign.

The only infection vector used for spreading VictoryGate is via removable devices. “The victim receives a USB drive that at some point was connected to an infected machine. It seemingly has all the files with the same names and icons that it contained before being infected. Because of this, the content will look almost identical at first glance. However, all the original files were replaced by a copy of the malware,” says ESET researcher Alan Warburton, who investigated the botnet. “When an unsuspecting user attempts to open one of these files, the script will open both the file that was intended and the malicious payload.”

Warburton also warns about the impact on victims’ machines: “There is very high resource usage by the botnet, resulting in a constant 90% to 99% CPU load. This slows down the device and can cause overheating and possible damage.”

According to ESET research, VictoryGate has made a much greater effort to avoid detection than in previous, similar campaigns observed in the Latam region. And, given the fact that the botmaster can update functionality of the payloads that are downloaded and executed on the infected devices from cryptomining to any other malicious activities at any given time, this poses a considerable risk. This is particularly true since many of the victims identified were in either the public sector or in financial institutions.

If you suspect your device may have been infected with this malware, you can use our free ESET Online Scanner to clean your machine. The first-stage module is detected by ESET security products as MSIL/VictoryGate.



The peak number of unique IP addresses connecting to the botnet command and control server per day.

For more technical details about the VictoryGate botnet, read the blogpost Following ESET's discovery, a Monero mining botnet is disrupted on WeLiveSecurity. Make sure to follow ESET research on Twitter for the latest news from ESET Research.

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET is the first IT security company to earn 100 Virus Bulletin VB100 awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.