Sly malware author hides cryptomining botnet behind ever-shifting proxy service

By Written by Catalin Cimpanu, ContributorContributor Sept. 13, 2018 at 4:04 p.m. PT

Archived: 2026-04-05 15:32:36 UTC

Security

-
-
-
-

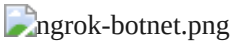
Without a doubt, botnets focused on cryptocurrency mining operations have been one of the most active forms of malware infections in 2018.

New botnets are appearing left and right if we are to believe security researchers from Chinese security firm Qihoo 360, who said this week that they are discovering new instances on a daily basis.

Not all of them may be profitable, as a recent Malwarebytes report has shown, but that doesn't stop cyber-criminals from trying.

Also: Why cryptocurrency mining malware is the new ransomware

Although most botnets are a carbon copy of one another, once in a while researchers spot one that stands out above the crowd. This week, the cryptomining botnet that took the crown in terms of creativity was one discovered by the Netlab team at Qihoo 360.



And according to the Netlab team, the thing that stood out about this botnet was that instead of letting infected bots connect to a remote server via a direct connection, its authors were using the ngrok.com service instead.

Also: 7 tips for SMBs to improve data security TechRepublic

For readers unaware of ngrok, this site is a simple reverse proxy used to let Internet-based users connect to servers located behind firewalls or on local machines that don't have a public IP address.

The service is very popular with enterprises because it allows employees a way to connect to corporate intranets. The service is also used by home users, usually freelance developers, to let customers preview applications that are under development.

In most cases, a user hosts a server on his local machine, registers with ngrok, and gets a public URL in the form of [random_string].ngrok.io that he then shares with a customer or friend to let him preview an ongoing project.

Also: Windows and Linux Kodi users infected with cryptomining malware

According to Netlab researcher Hui Wang, at least one cryptomining botnet operator is also familiar with this service and has been using it to host a command and control (C&C) server behind ngrok's proxy network.

But besides anonymity, the botnet operator also appears to have indirectly gained a resilience against any attempted takedowns of his C&C server.

As Hui explains, this happens because ngrok.io URLs stay online for only around 12 hours, and by the time security researchers identify a new C&C URL, the ngrok.io link changes to a new one, hiding the botnet from researchers once more. This allows the botnet to survive more than other botnets that host C&C servers on popular hosting platforms where security firms can usually intervene via abuse requests.

Also: Best Home Security Devices for 2018 CNET

But that's where the botnet's creativity ends. Besides the nifty C&C trick, this particular botnet uses a somewhat simple make-up for its internal structure.

Hui says the botnet consists of four major components, all which have self-explaining names. The Scanner scans the Internet for applications vulnerable to known exploits; the Reporter takes care of client-server communications; the Loader downloads and infects a host; and the Miner is the actual app installed on the server that generates cryptocurrency for the botnet operator.

Also: New Hakai IoT botnet takes aim at D-Link, Huawei, and Realtek routers

Currently, Hui says the botnet is targeting an assortment of web applications and CMSs, such as Drupal, ModX, Docker, Jenkins, Redis, and CouchDB.

There's also a module to scan for local Ethereum wallets, but this is not active. On the other hand, a module that injects the Coinhive JavaScript library in all of the server's JS files is active, meaning the botnet will also mine Monero inside the browsers of users visiting a site hosted on the infected servers.

This particular botnet is not extremely successful when compared to other botnets that have made millions of US dollars, and according to Hui, its operator made roughly 70 XMR coins, which is around $7,800. In terms of botnet operations, this is only pocket money.

A technical analysis and some indicators of compromise (IOCs) are available in Netlab's report, here.

These are 2018's biggest hacks, leaks, and data breaches

Previous and related coverage:

What is malware? Everything you need to know

Cyber attacks and malware are one of the biggest threats on the internet. Learn about the different types of malware - and how to avoid falling victim to attacks.

Security 101: Here's how to keep your data private, step by step

This simple advice will help to protect you against hackers and government surveillance.

VPN services 2018: The ultimate guide to protecting your data on the internet

Whether you're in the office or on the road, a VPN is still one of the best ways to protect yourself on the big, bad internet.
