MIRAI BEGETS SATORI —

New botnet infects cryptocurrency mining computers, replaces wallet address

Attacker has generated about $2,000 in digital coin so far in a scam that remains active.

DAN GOODIN - 1/17/2018, 3:20 PM

Marco Krohn

Enlarge / A cryptocurrency mining farm.

Satori—the malware family that wrangles routers, security cameras, and other Internet-connected devices into potent botnets—is crashing the cryptocurrency party with a new variant that surreptitiously infects computers dedicated to the mining of digital coins.

A version of Satori that appeared on January 8 exploits one or more weaknesses in the Claymore Miner, researchers from China-based Netlab 360 said in a report published Wednesday. After gaining control of the coin-mining software, the malware replaces the wallet address the computer owner uses to collect newly minted currency with an address controlled by the attacker. From then on, the attacker receives all coins generated, and owners are none the wiser unless they take time to

manually inspect their software configuration.

Records show that the attacker-controlled wallet has already cashed out slightly more than 1 Etherium coin. The coin was valued at as much as $1,300 when the transaction was made. At the time this post was being prepared, the records also showed that the attacker had a current balance of slightly more than 1 Etherium coin and was actively mining more, with a calculation power of about 2,100 million hashes per second. That's roughly equivalent to the output of 85 computers each running a Radeon Rx 480 graphics card or 1,135 computers running a GeForce GTX 560M, based on figures provided here.

Assuming the wallet address continues to generate coins at the same rate, the proceeds after a few months could be well worth the effort, assuming the massive cryptocoin sell-off—which has caused Etherium's value to drop by 42 percent in the past four days—doesn't continue.

Satori: Not just for IoT anymore

Satori is a modified version of the open source Mirai botnet malware. Mirai took control of so-called Internet-of-Things devices and caused them to participate in distributed denial-of-service attacks that paralyzed large swaths of the Internet in 2016. When Satori appeared in December, the underlying code was significantly overhauled. Instead of infecting devices that were secured with easily guessable default passwords, it exploited programming vulnerabilities in the device firmware. In early December, Satori had infected more than 100,000 devices and reportedly grew much bigger in the following weeks.

According to a Netlab 360 researcher who goes by the name RootKiter and wrote in Wednesday's post, the Satori version that appeared on January 8 continues to exploit two IoT vulnerabilities. But, RootKiter continued, the new version also exploits the weakness in the Claymore Mining software.

It's not clear precisely how the new variant is infecting mining computers. At least one vulnerability has been reported in the Claymore Mining software, along with a corresponding vulnerability. Wednesday's post said Satori isn't exploiting it. Instead, Wednesday's post said Satori "works primarily on the Claymore Mining equipment that allows management actions on 3333 ports with no password authentication enabled (which is the default config)."

To prevent further abuse, Netlab 360 said it wasn't providing further details. Developers of the Claymore Mining software didn't respond to an email seeking comment for this post.

Oddly, the developer of the new variant left a message on infected computers that reads:

> Satori dev here, dont be alarmed about this bot it does not currently have any malicious packeting purposes move along. I can be contacted at curtain@riseup.net

The message is demonstrably untrue, since malware that uses other people's computers and electricity to mine cryptocurrency is by definition malicious.

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 46

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

Related Stories

Sponsored Stories

Powered by outbrain

Today on Ars