Satori Author Linked to New Mirai Variant Masuta

By Tom Spring

Published: 2018-01-23 · Archived: 2026-04-02 10:53:41 UTC

Two related Mirai variants called Masuta and PureMasuta have links to a hacker identified as Nexus Zeta.

Researchers at NewSky Security say the hacker behind a Mirai malware variant called Satori, also known as Mirai Okiru, is the same hacker behind two new Mirai variants called Masuta and PureMasuta.

Based on source code for Masuta malware recently found on the dark web, researchers at NewSky Security said they were able to connect the dots between Satori and Masuta. The hacker is identified as Nexus Zeta.

Last month researchers first identified Nexus Zeta as the principle behind a series of attacks against Huawei routers, hijacked to spread the Mirai variant Satori. Originally, Nexus Zeta was considered a novice hacker because of clues the hacker left behind that allowed researchers to identify him as a forum poster to the site HackForums.

“With this code leak, now we know that Nexus Zeta is not just a one-shot wonder or a copy-and-paste script kiddie,” said Ankit Anubhav, principal researcher at NewSky Security. “He has been honing his skills in the form of Masuta.”

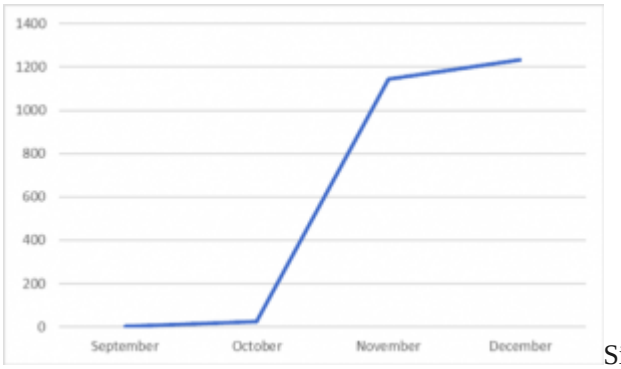
In a research report released Tuesday, NewSky Security researchers also identified a second Masuta variant called PureMasuta. That variant is unique because the malware leverages a “weaponized” D-Link HNAP bug used by attackers to grow its botnet.

The D-Link HNAP flaw takes advantage of a Home Network Administration Protocol (HNAP) injection bug originally identified in D-Link products in 2015. HNAP is a network protocol developed by Pure Networks, later acquired by Cisco Systems. HNAP is based on Simple Object Access Protocol (SOAP) and is used by device admins to manage network devices.

“It is possible to craft a SOAP query which can bypass authentication by using *hxxp://purenetworks.com/HNAP1/GetDeviceSettings.* Also, it is feasible to run system commands (leading to arbitrary code execution) because of improper string handling. When both issues are combined, one can form a SOAP request which first bypasses authentication, and then causes arbitrary code execution,” wrote Anubhav.

Anubhav said an examination of the PureMasuta botnet shell script downloaded from a command-and-control server revealed that both Masuta and PureMasuta shared the same server.

“We noticed that the command and control server is same as used in the original Masuta variants, hence indicating that PureMasuta is an evolved creation of the same Masuta threat actors,” Anubhav said.



Since September, PureMasuta-infected IPs have shot up twelve-fold according to honeypot activities observed by NewSky Security.

Okiku/Satori was first identified by Check Point researchers on November 23. In December, researchers at Qihoo 360 Netlab said Satori infected more than 280,000 IP addresses in a 12 hour period and gained control over 500,000 to 700,000 IoT devices.

“Nexus Zeta is no stranger when it comes to implementing SOAP related exploits. The threat actor has already been observed in implementing two other known SOAP related exploits, CVE-2014–8361 and CVE-2017–17215 in his Satori botnet project. A third SOAP exploit, TR-069 bug has also been observed previously in IoT botnets. This makes EDB 38722 the fourth SOAP related exploit which is discovered in the wild by IoT botnets,” Anubhav said.

Source: https://threatpost.com/satori-author-linked-to-new-mirai-variant-masuta/129640/