Mirai Activity Picks up Once More After Publication of PoC Exploit Code

bleepingcomputer.com/news/security/mirai-activity-picks-up-once-more-after-publication-of-poc-exploit-code/

Catalin Cimpanu

By
Catalin Cimpanu

- November 24, 2017
- 09:23 AM
- 0

The publication of proof-of-concept (PoC) exploit code in a public vulnerabilities database has lead to increased activity from Mirai-based IoT botnets, Li Fengpei, a security researcher with Qihoo 360 Netlab, told Bleeping Computer today.

The exploit code was published online on October 31 but scans using this PoC started on Wednesday, November 22, according to a report Li shared with Bleeping Computer.

PoC exploit targets ZyXEL PK50001Z routers

The PoC is for a vulnerability in the old ZyXEL PK5001Z routers that came to light in January 2016 on the OpenWrt forums.

The vulnerability (CVE-2016-10401) is a hidden su (super-user) password on the affected ZyXEL devices that elevates a user's access to root level. This su password (zyad5001) is useless, as it cannot be used to log into the device.

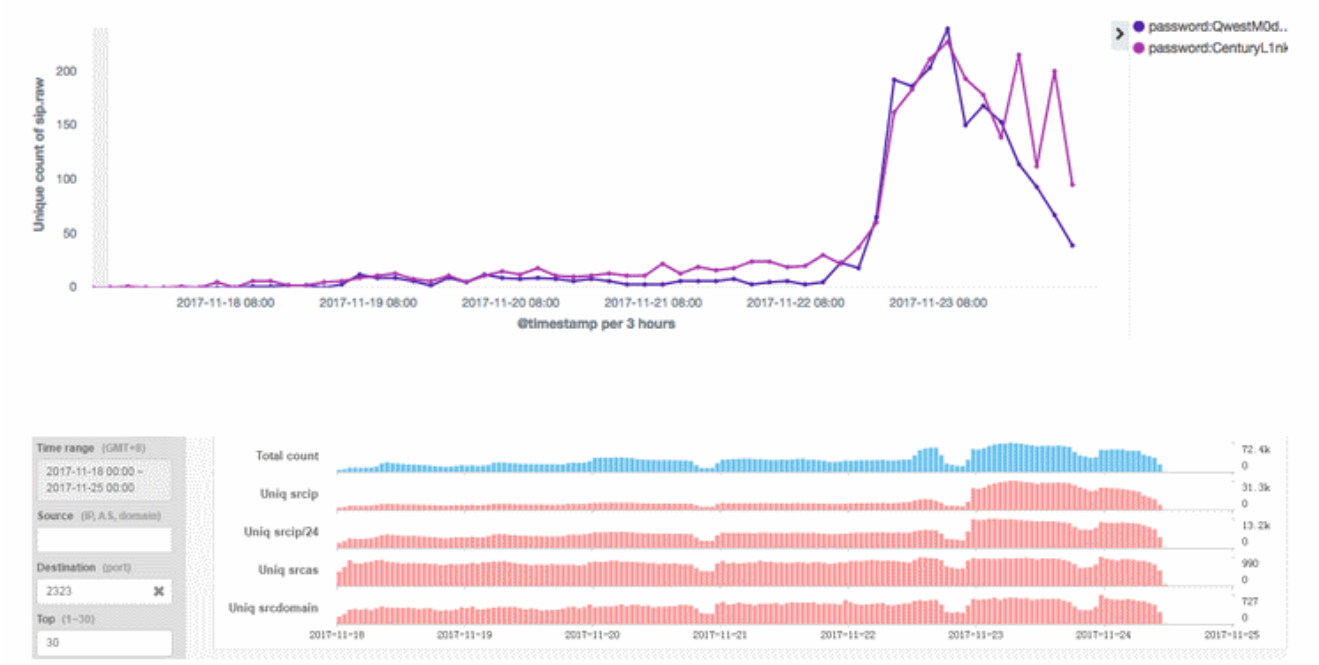
Nonetheless, miscreants have discovered that there's a large amount of ZyXEL devices that have shipped to users that are using admin/CentryL1nk and admin/QwestM0dem as default Telnet credentials.

The PoC published last month automates the process of logging into a remote ZyXEL device using one of the two Telnet passwords, and then uses the hardcoded su password to gain root privileges.

Mirai botnet incorporates recent ZyXEL PoC

The PoC exploit code had Mirai written all over it the moment it was published online. This is because Mirai botnets are built by scanning the Internet for devices with exposed Telnet ports and using a list of default credentials to attempt to log into devices and install the Mirai DDoS malware.

Starting on Wednesday, this is exactly what happened. For the past 60 hours, Li says Netlab has detected a spike of scans on ports 23 and 2323, both used for Telnet authentication. Attackers are using the above PoC to break into exposed devices and infect them with Mirai.



Such a massive scan campaign did not go unnoticed. Independent security researcher Troy Mursch also reported a similar uptick in Mirai activity yesterday.

> 879 new unique IP addresses were found in the #Mirai-like #botnet on 2017-11-22
>
> This is an all-time record for the most new unique IP address that I've seen added to the botnet in one day.
>
> A massive increase of volume from Argentina (@Telefonica) is largely the cause. pic.twitter.com/c8GBUpKNgW
>
> — Bad Packets Report (@bad_packets) November 23, 2017

Most new Mirai bots are located in Argentina

As both Netlab and Mursch have pointed out, most of the infected devices are from Argentina, and more precisely from the network of local ISP Telefonica de Argentina.

Netlab says it detected around 100,000 IPs performing these scans in the past 60 hours. Since Mirai-infected devices perform the IP scanning and exploitation attempt, this is an approximate estimation of the number of bots in this Mirai botnet that's looking for vulnerable ZyXEL devices.

NetLab says that around 65,700 of these bots were located in Argentina, a clear sign that the ISP has shipped devices with the default creds included in the public PoC.

The good news is that Mirai bots do not have a persistence mechanism in place, meaning they are removed when the router reboots. This is why Mirai botnets wildly vary in size from day to day, and why botnet herders need to be constantly scanning the Internet to keep their bot numbers up.

This is also not the first time when a Mirai botnet has exploited flaws in one particular ISP's network to grow to a mammoth size. Similar incidents have happened in Germany and the UK in November and December 2016.

The hacker behind those incidents deployed faulty Mirai malware versions that eventually brought down Internet services for ISP customers. Law enforcement tracked down, arrested, charged, and sentenced the hacker, named BestBuy (also known as Popopret).

There are no reports that Telefonica users are suffering from Internet connectivity outages, meaning users are not aware their devices are infected with the Mirai malware.

Related Articles:

Honeypot experiment reveals what hackers want from IoT devices

New EnemyBot DDoS botnet recruits routers and IoTs into its army

Mirai malware now delivered using Spring4Shell exploits

Beastmode botnet boosts DDoS power with new router exploits

Cisco urges admins to patch IOS XR zero-day exploited in attacks

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.