Hide and Seek IoT Botnet resurfaces with new tricks, persistence

labs.bitdefender.com/2018/05/hide-and-seek-iot-botnet-resurfaces-with-new-tricks-persistence/

Anti-Malware Research
2 min read

Bogdan BOTEZATU
May 07, 2018

On April 30, Bitdefender researchers became aware of a new version of the Hide and Seek bot we documented earlier this year. The botnet, the world's first to communicate via a custom-built peer to peer protocol, has now also become the first to gain persistence (the ability to survive a reboot) with the new version.

Historically, the botnet infected close to 90,000 unique devices from the time of discovery until today, with ups and downs on each update.

The new samples identified in late April don't add functionality, but feature plenty of improvements on the propagation side. For instance, the new binaries now include code to leverage two new vulnerabilities (more about this here and here) to allow the malware to compromise more IPTV camera models. In addition to the vulnerabilities, the bot can also identify two new types of devices and pass their default username and passwords.

Generic attack avenues

The sample discovered also targets several generic devices. Infected victims scan for neighbouring peers for the presence of the telnet service. As soon as the telnet service is found, the infected device attempts to bruteforce acces. If the login succeds, the malware restricts access to port 23 to potentially prevent a competing bot from hijacking the device.

This attack avenue targets a wide range of devices and architecture. Our research shows that the bot has **10 different binaries** compiled for various platforms, including x86, x64, ARM (Little Endian and Big Endian), SuperH, PPC and so on.

Once the infection has been performed successfully, the malware copies itself in the **/etc/init.d/** and adds itself to start with the operating system. In order to achieve persistence, the infection must take place via Telnet, as root privileges are required to copy the binary to the **init.d** directory.

It subsequently opens a random UDP port that is propagated to the neighboring bots. This port will be used by the cyber-criminals to get in touch with the device.

The supported command list has not changed significantly from the previous version of the bot. There is still no support for DDoS attacks (one of the most frequently encountered features of IoT bots), which leaves extremely little room for monetizing the botnet. However, the bot itself can still exfiltrate files using the method described in our last post about HnS.

Based on the evidence at hand, we presume that this botnet is in the growth phase, as operators are trying to seize as many devices as possible before adding weaponized features to the binary.

The samples we used for this piece of research are identified as **9ef7ed8af988d61b18e1f4d8c530249a1ce76d69** and **c6d6df5a69639ba67762ca500327a35b0e3950b0**.

TAGS

anti-malware research

AUTHOR

Bogdan BOTEZATU

Information security professional. Living my second childhood at @Bitdefender as director of threat research.

View all posts