Children of Mirai

Threat Memo - Date: 16/04/2020 - Version: 1.0
TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cybercrime	Botnet, DDoS	World	IoT	A1

Key Points

- New IoT botnets are building on Mirai's success.
- With new features and persistence methods, these new attack tools are formidable threats.
- Most such botnets are created for financial gain and are highly likely available for hire.

Summary

Recently, there has been a resurgence of Internet of things (IoT) botnets. Most of them share some code with Mirai – the first IoT botnet to cause significant damage. In 2016, Mirai was used to conduct the biggest distributed denial of service (DDoS) attack by a botnet, taking down the DNS provider Dyn alongside with its customers, including Amazon, BBC, Fox News, the Guardian, GitHub, Netflix, Paypal, Spotify, and Twitter[1].

Now, a new generation of IoT botnets is building on Mirai's success. Perhaps the most fearsome of them is dubbed **dark_nexus**[2]. The associated malware builds its botnet from home routers, video recorders, monitoring cameras and other network-connected devices. It reuses some Mirai code, but takes the capabilities of an IoT botnet much further.

Dark_nexus is developed to be potent and robust. Its modules are compiled for 12 different CPU architectures, so that it will work on almost any IoT device it will encounter. It also pays close attention to other processes running on the device. If another process is consuming significant computing resources and is not a part of a whitelist that dark_nexus is carrying, it will be killed as a potential existential threat (security software), a competing bot, or simply something that is denying valuable CPU time for the malware. It propagates by using common administrator passwords. Dark_nexus is built to conduct distributed denial of service (DDoS) attacks and is highly likely available for hire.

Another new IoT botnet is called **Mozi**[3]. This too borrows some code from Mirai. It can conduct DDoS attacks, exfiltrate data and execute additional payloads. It builds its peer-to-peer (P2P) network using the distributed has table (DHT) protocol, much like BitTorrent. Mozi compromises IoT devices by guessing weak or default telnet usernames and passwords. It is being actively developed and is also highly likely designed to be a cyber weapon for hire.

Yet another IoT botnet, named **Hoaxcalls**[4], is actively targeting a recently patched SQL injection vulnerability in Grandstream UCM6200 series devices. The UCM6200 is an internet protocol private branch exchange (IP PBX) device. It is used to provide external connectivity to a business's internal telephone and video conferencing network. Hoaxcalls also targets at least one vulnerable home router. Unlike Mirai, dark_nexus, and Mozi, Hoaxcalls is only known to propagate via exploiting certain vulnerabilities in certain devices. The malware communicates with its command and control servers over Internet Relay Chat (IRC).

Comments

When Mirai launched what is still known as the biggest DDoS attack by a botnet, it caught many analysts as a surprise. Mirai was the first botnet to successfully exploit a vast amount of computing devices that was connected to the internet. It propagated using a list of known default and common administrator logon credentials and was frightfully successful at that. One would have hoped that IoT manufacturers and users have learned from Mirai and started practicing better cyber hygiene by moving away from default passwords. The emergence of the "children of Mirai" exemplifies the fact that this is not so. Propagating by guessing passwords is just as successful as four or five years ago.

Most such botnets carry significant firepower in terms of DDoS capability. They are also highly likely available for hire. This means that it does not take much skill to cause denial of service attacks. All it takes is money, which puts cyber attacks against availability well within the reach of rogue countries or criminal actors who otherwise lack access to such expertise.

[1] See CITAR-Flash-2016-013
[2] https://www.bitdefender.com/files/News/CaseStudies/study/319/Bitdefender-PR-Whitepaper-DarkNexus-creat4349-en-EN-interactive.pdf
[3] https://blog.centurylink.com/new-mozi-malware-family-quietly-amasses-iot-bots/
[4] https://www.securityweek.com/botnet-targets-critical-vulnerability-grandstream-appliance

Examples of recent IoT Botnets

date	name	techniques	purpose
04/2020	dark_nexus	Spreads by using default username and password combinations. Will run on most CPU architectures. Kills competing processes.	Distributed denial of service.
12/2019	Mozi	Builds a distributed hash table (DHT) botnet out of IoT devices.	Distributed denial of service.
04/2020	Hoaxcalls	Propagates only on certain devices that have specific vulnerabilities. Uses IRC for command and control.	Distributed denial of service.
05/2020	Lemon Duck	Spreading on IoT devices running Windows 7.	Cryptomining.
12/2019	Dota3	Compromises misconfigured SSH servers by using common username and password combinations.	Cryptomining.