Emerging dark_nexus IoT botnet highlights need for better prevention measures

New botnet presents evolved, damaging capabilities over its predecessors

Omdia view

Summary

Researchers at Bitdefender Labs have discovered a brand-new IoT botnet in the wild. With substantially more advanced functionality over previous IoT botnets such as Mirai or Qbot, dark_nexus has learned from the successes of its predecessors to establish stronger resilience against discovery and mitigation efforts, incorporating numerous threat vector exploitations in order to spread more rapidly.

Botnets born out of insecure IoT practices

Many IoT device Original Equipment Manufacturers (OEMs) engage in the practice of “connect first, secure later”. The rationale behind this idea is that every measure designed to protect information introduces a hurdle that legitimate users must navigate in order to gain access to data. Security measures are rarely cheap and can be seen as obstructions to efficiency when under tight budgetary or time constraints.

Over time, adversaries have learned to take advantage of this insecure practice by infecting vulnerable devices and harnessing their resources to create IoT botnets. Once a device is successfully compromised with malware, it is then used to seek out and infect other vulnerable systems, spreading like a biological infection. This ultimately results in the creation of a zombie network, or botnet, of devices that can be “called up” to participate in more sophisticated attacks.

The evolution of the Qbot and Mirai malware families directly resulted from the weakness of the IoT security ecosystem. Qbot, a banking Trojan first discovered in 2009, was designed to steal user credentials and financial data from its targets. In August 2016, the Mirai malware was discovered after it had successfully exploited vulnerable devices using a dataset of vendor default usernames and passwords. Qbot and Marai have proven to be two of the most effective IoT botnet efforts to date.

While the malware behind the new dark_nexus IoT botnet shares similar code with both Qbot and Mirai, Bitdefender claims that most of the exploit code present within this new iteration are original. For example, the payloads for dark_nexus are compiled for 12 different CPU architectures in order to compensative for unique configurations on victim devices, providing greater resilience through the ability to compromise more targets. Additionally, the malware assigns a scoring system to specific processes, ultimately killing those processes that are not whitelisted and might pose a threat to its overall survival.

Unfortunately, dark_nexus underscores how easy it is for even moderately skilled adversaries to create attack campaigns by compromising IoT devices, as the source code for many of these malware packages remain easily accessible in dark corners of the internet. This ease of access allows malicious hackers to continuously modify their malware as needed to adapt in response to any new security measures they encounter. Even something as simple as changing the default credentials present on a device can place a substantial barrier in front of cyber criminals.

When it comes to addressing the challenges surrounding IoT botnets, the reality is that the responsibility for effective security is shared between device manufacturers and end users alike. Despite diligence from OEMs, device vulnerabilities are discovered with consistent regularity. However, some of the best strategies to mitigate these threats stem from basic security hygiene practices. These can include relegating IoT components to an isolated network, ensuring that all

default credentials are changed using complex passwords, and multifactor authentication is used when available. Ultimately, the security measures taken (or ignored) will determine how quickly botnets like this will continue to flourish in the near term.

Appendix

Further reading

The US makes a good start on IoT security legislation, (August 2017)

Information protection is about more than confidentiality, INT003-000248 (October 2018)

Shared Accountability for IoT Security (May 2019)

New dark nexus IoT Botnet Puts Others to Shame, (April 2020)

Author

Tanner Johnson, Senior Cybersecurity Analyst, Connectivity and IoT

tanner.johnson@omdia.com

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com