NETSCOUT
Guardians of the Connected World | Arbor

The countdown is running: IoT devices hacked in 5 minutes

Users of connected devices only have five minutes to change the factory settings. Otherwise, there is a risk of hackers taking over. These are findings of ASERT, a team of security specialists within NETSCOUT, a provider of business assurance, cyber security and business intelligence solutions. The team has leveraged a global network of honeypots to gain these insights.

Cybercriminals are focusing on IoT devices such as network cameras, thermostats and door opening systems. By using lists of standard user names and passwords which are circulating on the Internet, these devices are quickly compromised without the users even noticing. The takeover allows attackers to bundle the devices in huge botnets and misuse their computing power for criminal activities. Yet, other known, but still not fixed security issues are still pressing: These cannot be closed by the user by simply changing the login information. Cybercriminals gain access to private data via such weak points and can tap microphones and cameras.

- Why IoT devices are dangerous: Most devices such as surveillance and security cameras, routers, smart factory devices, control and door opening systems, sensors and alarm systems are still bursting with security gaps, weak points and unchangeable default settings. Just recently, cooling systems from the Taiwanese manufacturer Resource Data Management were hacked using the pre-set login information.

- Blackmailing made easy: Once hacked, cybercriminals often combine individual IoT devices to form larger and thus powerful botnets. Especially Distributed Denial of Service (DDoS) attacks can be effectively executed via botnets. The aim of the attackers is to slow down, completely paralyze or damage Internet services, IT components or the IT infrastructure of an attacked company. In 2017, companies in Germany had to fend off a total of 392 DDoS attacks per day. The motives range from blackmailing and data theft to competitive damage and state influence.

- In 2019, Mirai successors remain extremely dangerous: The potential danger of botnets remains high. According to IHS Markit, there will be more than 125 billion IoT devices by 2030. Mirai botnet offshoots are particularly damaging because they allow anyone with minimal technical skills to build their own IoT botnet – and perform multiple types of DDoS attacks on both the network and application layers. This can cause significant financial damage to businesses.

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) assures digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility, and insights customers need to accelerate, and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor security solutions protect against DDoS attacks that threaten availability, and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions, powered by service intelligence can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT and @ArborNetworks on Twitter, Facebook, or LinkedIn.

Press contact

Carolin Nillert / Yannik Bartling

Oseon

netscout@oseon.com

+49-69-25 73 80 22 -16 / -15