Corporate IoT – an intrusion path for APT groups

Reference: Memo [190905-1] – Version: 1.0
Keywords: internet of things (IoT), supply chain attacks, APT, Russia, espionage
Sources: Publicly available information

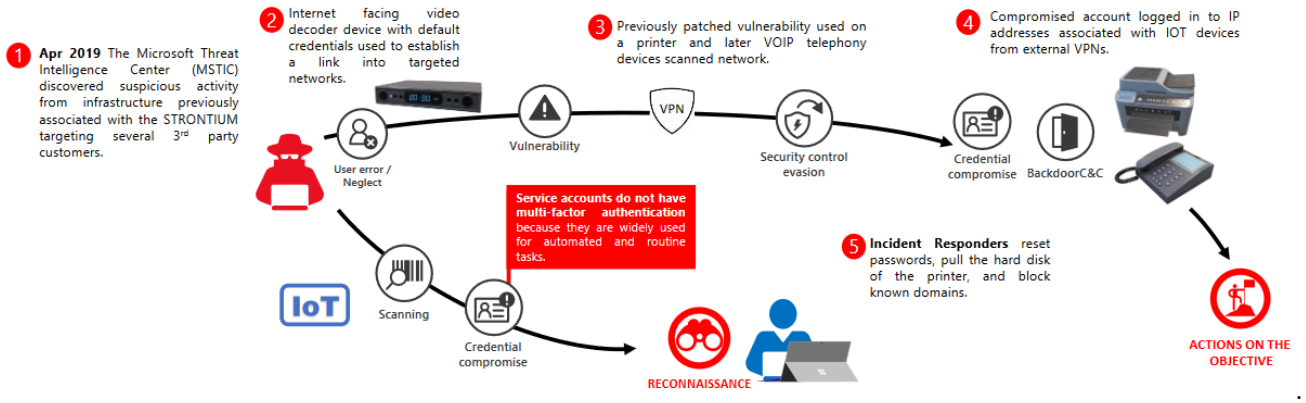
Key Points

- APT28 reportedly attempted to compromise IoT devices to gain initial access to corporate networks.
- Such attacks are likely to expand as more IoT devices are deployed in corporate environments.

Summary

According to Microsoft[1,2], the highly likely Russian APT28 threat actor attempted to compromise Internet of Things (IoT) devices across multiple customer locations to gain initial access to corporate networks.

The targeted IoT devices included a VOIP phone, an office printer, and a video decoder. In two of the cases, the devices were deployed without changing the default manufacturer's passwords and in the third instance the latest security update had not been applied. These devices became points of ingress from which the attackers established a presence on the network and continued looking for further access. The attackers performed simple network scans to look for other insecure devices that would allow them to move across the network in search of higher-privileged accounts that would grant access to higher-value data.



Microsoft slide presented at the Aug 2019' Blackhat conference

Once the attack was discovered, the compromised I0T devices were quarantined and sent for forensic analysis, impacted service account credentials were changed, malicious domains and IPs were blocked on affected networks, and observed techniques, tactics and procedures were shared with IoT vendors.

Comments

APT28 (aka Sofacy, Fancy Bear, Strontium) has targeted various organisations operating in the foreign policy, defence and military sectors. APT28's preferred infection vector is spear-phishing, delivering infected documents. However, it is not the first time that APT28 is suspected to additionally compromise network or infrastructure devices. In May 2018, the VPNFilter malware (attributed to APT28[3] by the FBI) was discovered infecting routers and certain network attached storage devices.

One of the first massive IoT targeting operations was carried out by the Mirai botnet in 2016. This botnet consisted mainly of compromised IP cameras and home routers (due to unchanged default passwords on devices). Since then, many variants of Mirai have been observed targeting additional types of IoT. In October 2016, the Mirai source code was leaked[4], accommodating would-be hackers.

While the compromise of IoT devices has traditionally been associated with their misuse to induce large-scale DDoS attacks, the Microsoft investigation can be seen as a wake-up call for another targeted intrusion method to organisations. The protection of corporate IoT devices should be an integral part of the global defence against targeted attacks. Indeed, the simple attacks described in this case are taking advantage of weak device management. Such attacks are likely to expand as more IoT devices are deployed in corporate environments.

1 https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/
2 https://i.blackhat.com/USA-19/Thursday/us-19-Doerr-The-Enemy-Within-Modern-Supply-Chain-Attacks.pdf
3 https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected
4 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/