technologyreview.com

Russian hackers are infiltrating companies via the office printer

Patrick Howell O'Neill

3–4 minutes

A group of hackers linked to Russian spy agencies are using "internet of things" devices like internet-connected phones and printers to break into corporate networks, Microsoft announced on Monday.

Fancy Bear never hibernates: The Russian hackers, who go by names like Strontium, Fancy Bear, and APT28, are linked to the military intelligence agency GRU.

The group has been active since at least 2007. They are credited with a long list of infamous work including breaking into the Democratic National Committee in 2016, the crippling NotPetya attacks against Ukraine in 2017, and targeting political groups in Europe and North America throughout 2018.

Insecurity of Things: The new campaign from GRU compromised popular internet of things devices including a VOIP (voice over internet protocol) phone, a connected office printer, and a video decoder in order to gain access to corporate networks. Microsoft has some of the best visibility into corporate networks on earth because so many organizations are using Windows machines.

Microsoft's Threat Intelligence Center spotted Fancy Bear's new work starting in April 2019.

The password is password: Although things like smartphones and desktop computers are often top of mind when it comes to security, it's often the printer, camera, or decoder that leaves a door open for a hacker to exploit.

In multiple cases, Microsoft saw Fancy Bear get access to targeted networks because the IoT devices were deployed with default passwords. In another case, the latest security update was not applied. Using those devices as a starting point, the hackers established a beachhead and looked 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," Microsoft warned in a blog post published on Monday.

The hackers moved from one device to another, establishing persistence and mapping the network as they went, communicating with command and control servers all the while.

Global targets: Microsoft has been closely watching this group over the last year.

Of the 1,400 notifications the company delivered to those targeted or compromised by Fancy Bear, 20% have been to global non-governmental organizations, think tanks, or politically affiliated organizations. The remaining 80% have been to various sectors including government, technology, military, medicine, education, and engineering.

“We have also observed and notified STRONTIUM attacks against Olympic organizing committees, anti-doping agencies, and the hospitality industry,” Microsoft’s blog warned.

Last year, the FBI took disruptive action against a Fancy Bear campaign known as “VPNFilter” which targeted routers and network storage devices with malware with destructive capabilities of “bricking” a device by deleting firmware and rendering the device unusable. That campaign especially targeted Ukraine, a favorite target of Fancy Bear.