Can Nanotech Secure Iot Devices from The Inside-Out?

2021-05-26
Work’s being done with uber-lightweight nanoagents on every IoT device to stop malicious behavior, such as a scourge of botnet attacks, among other threats.

Another day, another incident of internet-of-things (IoT) gadgets falling flat on their faces and spilling users’ privacy, if not getting hooked into a botnet, used for cryptomining or opening a network backdoor that allows intruders to move laterally through a network.

It’s only Wednesday, but already reports this week detail IoT devices pressed into service to spread misery. Thanks to an internal server bug, users of Anker’s Eufy home-security cameras found they could view, pan and zoom in on each other’s home-video feeds for about a day, turning them into both unwitting spies and targets to be ogled.

Then too, we saw the debut of a new botnet, Simp, that infects IoT devices in tandem with the prolific Gafgyt botnet. Simp, like its IoT-abusing brethren, uses known security vulnerabilities – only one of the weak spots typical in IoT nodes.

Given the frequency of IoT device takeovers, how easy must it be to pwn these things? And how can organizations fight back?

Pwning IoT Gadgets Is Super-Duper Easy

It’s as easy as hacking an ultrasound machine that’s running on the legacy Windows 2000 operating system, with its known, unpatched vulnerabilities…a device that won’t be patched by the vendor because it’s end-of-life, though it’s still operational and still in use in hospitals.

Check Point's Itzik Feiglevitch and Justin Sowder said at an RSA Conference 2021 session on Tuesday – entitled Into the Mind of an IoT Hacker – that pwning these things is as simple as pie. After all, there are tens of thousands of vulnerable IoT devices to be found with a Shodan search: The researchers pointed to a search that turned up 25,959 printers connected to the internet and 284,092 webcams.

Those devices typically have no, or feeble, built-in security. They often run on legacy, weak OS passwords. They're also a bear to patch, for multiple reasons, such as the case of life-saving IoT medical devices can't be taken offline. That's just one reason why hospitals have been hit by a growing wave of ransomware attacks, for example: According to a report from Forescout, hospitals are struggling to manage a sprawling number of endpoints, ranging from computer systems, surgical equipment, telemedicine platforms, medical sensors and infusion pumps. All told, the report estimated that healthcare-delivery organizations contain an average of 20,000 devices.

Back when these devices were developed, "no one thought of that," Feiglevitch said. "We've seen Windows 95 running on some devices, or Windows 2000 with no security patches. Many use simple passwords, like '1234.' If you connect them, now you have hundreds of devices connected to your network."

How Do You Even Find Them, Internally?

According to Feiglevitch, when Check Point asks new customers if they know how many IoT devices are connected to their network, the answer is always "No, I don't know." Organizations can have diverse types of devices, of course – industrial control systems alongside healthcare IT, for example. Besides this diversity, the devices often use proprietary IoT protocols. This all makes the nodes "unmanaged and invisible," Feiglevitch noted. "If you look for them internally, you will not find those devices."

But attackers know how to find devices that are connected to businesses' networks on one side and to the internet on the other: Shodan is just one tool to do that. Check Point has found that, on average, enterprises with 5,000 employees have about 20,000 IoT devices on

their networks; hospitals with 500 beds have about 10,000 healthcare IoT devices; and a factory with 2,000 workers has about 5,000 industrial IoT devices.

The first thing an organization has to do to defend IoT devices and networks is to inventory them all, Feiglevitch instructed: every smartphone, every tablet, every hematology analyzer, every immunoassay analyzer, every router, every security camera, and on and on, in every smart office, every smart building, every industrial setting, and every medical facility.

That includes granular details about every device: Is it an IP camera? What's the risk score, based on firmware version and known vulnerabilities? What are the device ID details – MAC address, firmware version, connection type, protocols? Who manufactures it, and what's its IP address?

Vendors these days are able to generate a context-aware network security policy out of that intelligence map that gets enforced at the perimeter and inside the network, identifying and blocking malicious traffic with integrated threat prevention engines such as IPS, APPI and Anti-Bot, Sowder said.

Small Compute Power Requires Small Agents

Sowder said that many times, "the challenge with these IoT devices is the limited compute capability that they have on them. An IP camera can't run a full IPS protection suite against traffic to it. It has a job to record video and send it upstream."

He pointed to the potential solution of nanotechnology: Specifically, the concept of a nanoagent on each IoT node that inspects firmware code to determine if it's engaged in malicious behavior, such as memory corruption. If so, the nanoagent can block it in real-time.

The challenge is how to do it with a small footprint, Sowder said: "A lot of devices don't have a lot of compute. Sticking a firewall in front of every IP camera simply isn't feasible. The solution is a very, very slight agent. It phones home to get a device signature, including what

kind of device it is and what can run on it.”

Nanoagents don’t put a lot of overhead on these devices, so the devices’ performance isn’t slowed down, Sowder noted: “There’s no overhead to prevent them from performing their functions.”

Check Point has been working on a lightweight agent that relies on a cloud instance to pull down specific protection details related to that device. “As you can imagine, this is a large task and the ever-changing amount of IoT devices out there complicates that further, and I believe a standard should be in place,” Sowder commented.

Having said that, Sowder has seen signs that the manufacturers themselves are making progress: “We’re starting to see non-default passwords, encryption on device communication, hardening of web interfaces, etc. The challenge here absolutely has to have device manufacturers as part of the solution.”

Read the original article on Threatpost.