portnox™

What Can a Hijacked IoT Device Do to Your Network?

Mar 9,2017

“I don’t know where I’m going, but I’m on my way.” This remark by American writer and poet Carl Sandburg seems to capture what’s going on at the moment with the Internet of Things (IoT). It is growing at such breakneck speed that nobody can pinpoint how extensive this growth will continue to be. Take, for example, a forecast by Gartner, which anticipates 20.8 billion connected IoT devices will be in use for 2020 – and compare it to the significantly higher prediction by IHS forecasts, which anticipates no less than 30.7 billion connected devices in the same period.

Whatever the statistics, one thing is clear: The widespread adoption of IoT is a development that brings with it the promise of value to many organizations. On the other hand, it also creates security challenges by increasing the attack surface for organizational networks.

This reality was starkly illustrated in the Dyn cyber-attack at the end of October last year, notoriously known as the first robot-based digital assault involving millions of IoT devices operating in concert.

HOW CAN YOUR CORPORATE

ORGANIZATION PREPARE FOR THIS NEW KIND OF THREAT?

1. Gain Complete Visibility into Your Network

One aspect of the challenge that CISOs face in the age of IoT involves handling a glaring and somewhat shocking lack of visibility into 100% of devices that access a network.

With the BYOD phenomenon, IT cannot afford to ignore the question of how to securely manage virtually invisible devices that are connecting to corporate networks. Devices that IT cannot see create blind spots, which prevent an organization from successfully maintaining the ongoing vigilance necessary to protect the network.

2. Take Proactive Steps toward Protection

While visibility is an essential prerequisite to security, it's not *only* a question of visibility: it's the ability to control and manage permissions for each device.

Sensible protection from attacks on IoT devices means developing new techniques for network hygiene, and forcing IoT devices to a defined segment of the business network – in order to ensure that the rest of the network remains out of reach.

3. Understand the Mind of a Hacker

Let's take a step back, and talk about why both visibility and network access control are so essential.

Say, for example, a hacker hijacks an employee's IoT device – a device that is connected to your company's network. You might think this is a difficult task, but the reality is that it does not take much sophistication.

The problems start when the hijacked device – which, don't forget, is already connected to the network – is turned into a bot that runs automated tasks over the Internet. If the bot is used for malicious purposes, the hacker can probably do pretty much anything – from creating an APT or DDoS attack, to stealing sensitive data.

4. Change Those Default Settings

As pointed out in Portnox's eBook, *The Top 5 Misconception of IoT Network and Device Security*, IoT devices are possibly the most problematic aspect of a corporate network. This is partly because, generally, they are not set up securely.

Frequently, devices are connected to networks with their default configuration intact. Most users don't know it is important to change the default usernames and passwords. As a result, once IoT devices are connected, it is not hard for hackers to hijack them.

5. Beef Up Your Security Responses

For hackers, there's always the question of avoiding quick exposure.

Experienced hackers won't hijack an employee's PC. That's because PCs are in frequent use and are "owned" by a single individual, so it doesn't take much time for an employee to figure out there's a problem. Normal actions take longer or become difficult to do.

In contrast, if a device such as a printer or IP camera is hijacked, employees might not notice. These devices are not used as intensely and they are generally accessed by multiple individuals, so there's less chance of rapid exposure.

6. Adopt New Strategies for Network Visibility and Access Control Management

The security problems inherent to IoT open up a shocking range of opportunities for cybercriminals. As pointed out by this article on TechCrunch, the threat even touches everyday areas of activity including car safety and medical care.

Meeting the needs of today's cyber threats requires adopting a solution such as Portnox, which offers next-gen network visibility and access control management solutions that allow security teams to:

- Gain 100% actionable visibility of managed devices, BYOD and IoT in real time, using an approach that's agentless, centralized, and vendor agnostic
- Mitigate risk through controlled access, by creating a quarantine or blocking a device to solve a security issue
- Provide automation for certain kinds of reactions, enabling security teams to cut the time and costs associated with a manual response

According to Forbes, global spending on IoT products and services by enterprises is expected to reach $253 billion in 2021, attaining a 16% CAGR. With this degree of IoT technology integrated into corporate environments, the old approaches of maintaining security are no longer relevant.

The Portnox system meets today's growing challenges and protects networks from resulting vulnerabilities, providing a holistic approach to security that works for any user, any device, and any network – anywhere.

Ofer Amitai

CEO

Love what you are reading? Subscribe for more

Subscribe

Categories

IoT

Network Security

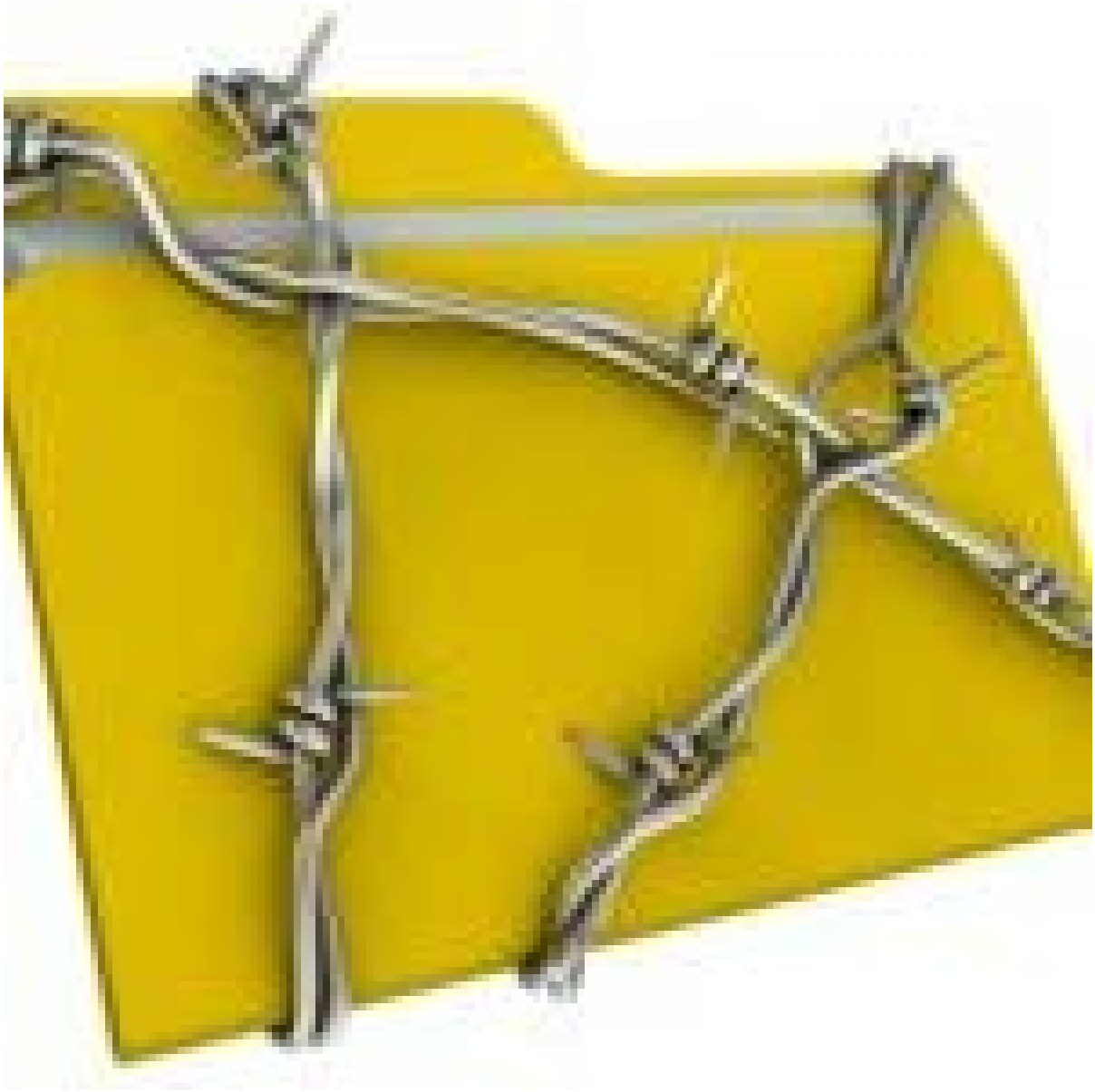
Our Technology

Threat Detection and Response

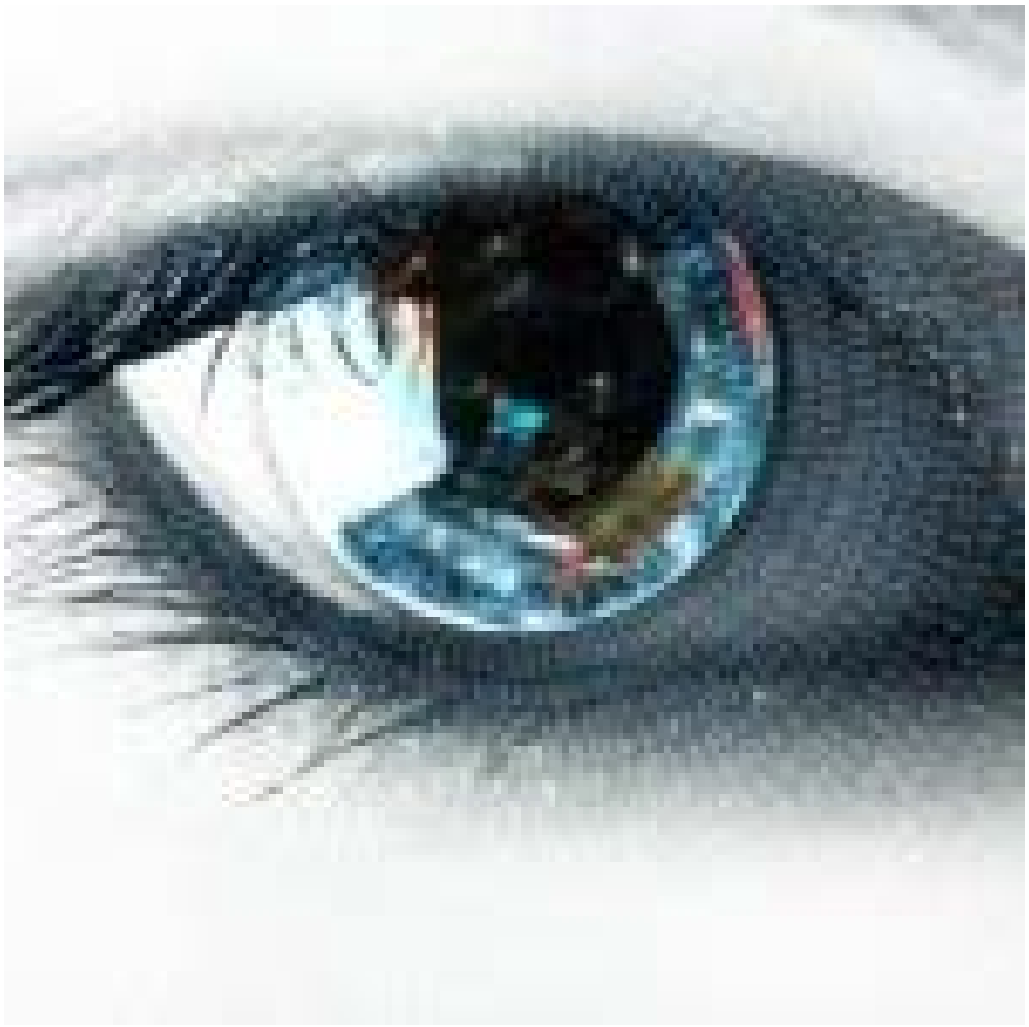
Network Access Management

Related Posts

Portnox Gains Full Visibility to All Devices and Users Across an Enterprise Network



DDoS Attacks are a Loud IoT Wakeup Call for Enterprise Security



Securing VPN remote access with Portnox CLEAR

Find a Reseller
Partner Program
Partner Portal
Contact Us
Leadership
News and Events
Careers