IoT Agenda

MANAGE

Defending the internet of things at machine speed

GUEST CONTRIBUTOR

Anthony Giandomenico
Fortinet

18 May 2018

While the first generation of the internet was primarily focused on connecting people to people via primarily static networks, IoT enables devices to communicate directly with each other across meshed and dynamically expanding networked environments. When combined with increasing levels of device intelligence (rather than relying on human intervention for every decision — resulting in a corresponding lag time), we now have devices connecting to each other and making decisions for us at machine speeds.

Unfortunately, this trend also holds true for malicious actors. According to the findings of Fortinet's Global Threat Landscape Report for Q1 of 2018, cybercriminals are evolving their attack methods to also include automation in order to increase their success rates and to speed infections. And they're targeting these increasingly autonomous exploits at more attack vectors than ever before.

Data indicates that cybercriminals are getting better and more sophisticated in their use of malware, utilizing both newly announced zero-day vulnerabilities and known threats in order to attack at speed and scale. While the number of detections per firm dropped by more than 13% in Q1 of 2018, the number of unique exploit detections still grew by more than 11% during the quarter, while 73% of companies experienced a severe exploit.

Below are key findings of the report, along with recommendations for defeating current threats.

Multiple attack vectors: Although the side-channel attacks dubbed Meltdown and Spectre dominated the news headlines during the quarter, some of the top attacks targeted mobile devices or known exploits on router, web or internet technologies. Twenty-one percent of organizations

reported mobile malware (up 7% from last quarter), demonstrating that IoT devices continue to be a growing target. Cybercriminals also continue to recognize the value of exploiting known vulnerabilities that haven't been patched, as well as exploiting zero-day vulnerabilities. Microsoft continued to be the number one target for exploits, and routers took the number two spot in total attack volume. Content management systems and web-oriented technologies were also heavily targeted.

More than patching is needed: Measuring how long botnet infections persist based on the number of consecutive days in which continued communications are detected reveals that cyber hygiene involves far more than just patching. It is also about cleanup. Data shows that while 58% of

was still appearing prominently in both volume and prevalence.

Operational technology under attack: While OT attacks are a smaller percentage of the overall attack landscape, the trends are concerning. This sector is increasingly becoming connected to the internet, with serious potential ramifications for security. Currently, the vast majority of exploit activity is directed against the two most common industrial communication protocols because they are widely deployed and therefore highly targeted. Data shows that in Asia, industrial control system exploit attempts appear to be somewhat more prevalent when comparing the prevalence of ICS exploit activity across other regions.

Integrated security required: The threat data in this quarter's report reinforces many of the trends predicted by the Fortinet FortiGuard Labs global research team for 2018, demonstrating that the best defense against intelligent and automated threats is an integrated, broad and automated security fabric. A highly aware and proactive security defense system is needed to keep pace with the next generation of automated, AI-based attacks.

A three-pronged approach to protecting IoT

Several exploits targeting IoT devices topped the charts this quarter. Fortinet recommends the "learn, segment and protect" approach to defeat those exploits. This starts with learning more about the devices connected to networks, how they're configured and how they authenticate. Organizations need to understand the capabilities and limitations of each device and network ecosystem they are tying together. To do this, security systems require complete network visibility in order to securely authenticate and classify all IoT devices. OT and ICS/SCADA networks and devices are particularly sensitive to any sort of service interruption. So, it is essential that organizations use a trust-based security framework to automatically discover and classify devices in real time, to build risk profiles and then dynamically assign IoT devices to device groups, and to distribute appropriate policies to security devices and network segments.

When an organization has achieved complete visibility, it's time to dynamically segment IoT devices into secured network zones with customized policies. Organizations need to establish complete visibility and centralized management across their entire trust-based security framework. They can begin by establishing controls to protect the expanding IoT attack surface. An essential component of these controls involves the intelligent and, where possible, automated segmenting of IoT devices and communications technologies into secured network zones that are, in turn, protected by enforcing customized and dynamically updated policies. This allows the network to automatically grant and enforce baseline privileges for each IoT device risk profile, enabling the critical distribution and collection of data without compromising the integrity of critical systems.

Finally, segments can be linked together by using an integrated, intelligent and protective fabric deployed across the network. Combining policy-designated IoT groups with intelligent internal network segmentation enables multilayered monitoring, inspection and enforcement of device policies based on activity anywhere across the distributed enterprise infrastructure. But segmentation alone can lead to fractured visibility. Each group and network segment also needs to be linked together into a holistic security framework that can span the entire distributed network. Such an integrated, fabric-based approach enables the centralized correlation of intelligence between different network and security devices and segments, followed by the automatic application of advanced security functions to IoT devices and traffic located anywhere across the network — especially at access points, cross-segment network traffic locations, and even into multi-cloud environments.

Security at IoT speed

As IoT expands, so does its attack surface. Traditional point defense products and platforms alone are not sufficient to secure today's IoT environments. In many cases, a human response would be too slow — especially if incident data needs to be manually correlated between different device management consoles. Operating at speed and scale requires security tools that are tightly integrated and powered by real-time intelligence. Keep that, along with the key findings listed above, in mind and adjust your security posture as needed in order to protect your evolving and dynamic network environment.

All IoT Agenda network contributors are responsible for the content and accuracy of their posts. Opinions are of the writers and do not necessarily convey the thoughts of IoT Agenda.

Start the conversation

Share your comment

Send me notifications when other members comment.

Create Username and Add My Comment

SearchCIO

5 ways to keep developers happy so they deliver great CX

Companies need to work on ensuring their developers are satisfied with their jobs and how they're treated, otherwise it'll be ...

Link software development to measured business value creation

Companies must balance customer needs against potential risks during software development to ensure they aren't ignoring security...