PROTECT IOT OPPORTUNITY WITH NETWORK-BASED SECURITY

IoT devices, expected to grow 21 percent annually through 2022, represent profound changes for service providers.[1] With great diversity in devices, functional complexity and availability requirements, service providers are challenged to provide the breadth of capabilities required, protect their own networks from IoT-related botnet attacks, and still capture a significant portion of the global market value of the entire value chain, estimated to reach as high as $14.4 trillion by 2022.[2]

Security had been an afterthought in much of the earlier IoT system design. However, in the latter part of 2016, multiple Mirai botnet attacks exposed the lax security of IoT devices and the vulnerability of critical infrastructure to organized attacks from infected devices outside and within the service provider networks. As a result, the industry has been awakened to the critical requirement for multiple levels of protection across the entire IoT value chain.

Palo Alto Networks® Next-Generation Security Platform provides advanced network-based security mechanisms that protect service provider networks, IoT systems, and interconnected networks and infrastructure. The platform identifies infected devices, prevents security attacks targeting IoT systems (controllers and devices), and establishes the basis for adding significant value to the services offered to consumers. With this capability, service providers can grow their market share in the IoT market while providing deep protection for their own infrastructure and interconnected networks.

1. IoT devices in this document are broadly defined to include a range of connected devices, including machine-to-machine (M2M), wide area IoT, short range IoT, and massive and critical IoT. IoT is also recognized as a multi-access edge computing (MEC) device by some analysts.
2. 5G Americas, "LTE and 5G Technologies Enabling the Internet of Things," December 2016 and Oracle Infographic: Energize your Business with IOT-Enabled Applications

Multiple Levels of Protection Required for IoT Opportunity

IoT is a significant opportunity for service providers. With global market value across the entire value chain estimated to reach $14.4 trillion by 2022,[3] most service providers have aggressive plans and initiatives already underway. For mobile network operators (MNOs), success with IoT is critical to reaching business and profitability objectives. Mobile phones, which currently dominate all connected devices in terms of volume, will be surpassed by IoT devices by 2018 and dwindle to only a 3 percent share.[4]

Concerns on security, fundamental to capturing this opportunity, have risen in significance. In the latter part of 2016, multiple Mirai botnet attacks exposed the lax security of IoT devices and the vulnerability of critical infrastructure to organized attacks from infected devices outside and within the service provider networks. Industry research predicts that two-thirds of enterprises will experience an IoT-related security breach by 2018[5] and that many common enterprise IP-connected devices, such as security cameras, climate control, printers and VoIP phones, can be hacked in as few as three minutes, potentially creating disastrous results for critical infrastructure.[6]

Service providers recognize the critical requirement for multiple levels of protection across the entire IoT value chain, shown in Figure 1:

- **IoT Systems:** Protect systems from infection and attack, and prevent them from further infecting endpoints or other elements of the system.
- **Connectivity Networks:** Protect their own networks against attacks from infected IoT devices. Prevent attacks to external networks and public infrastructure (outside the service provider domain) from infected devices operating within the service provider domain.
- **Local Networks and Gateways:** Protection is needed in the local networks (WAN, SCADA, LAN/ICS, Wi-Fi, etc.) that connect the devices to the local controller, or gateway, and to the broader connectivity network.
- **IoT Devices:** Protect endpoint devices from infection and prevent them from engaging in malicious actions, if already infected, under the direction of cybercriminal command-and-control (C2) servers.

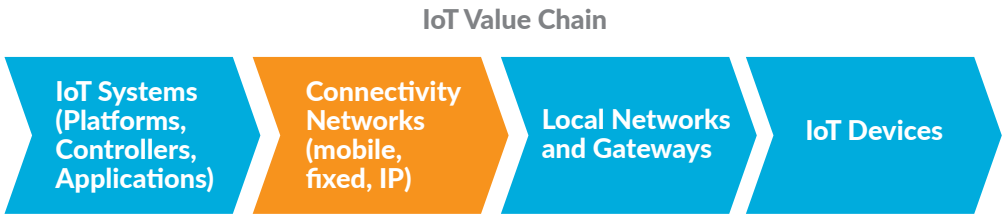

Figure 1: Service providers are in the middle of the IoT value chain

Service providers are faced with a significant challenge: they must provide a breadth of network and security capabilities if they want to capture a significant portion of the global market value, and they must protect their own networks from IoT-related botnet attacks.

Unique Security Risks With IoT

IoT devices pose some unique security challenges to mobile networks operators. This is partly because of the very high volume of devices and also because of the inherent characteristics of IoT devices:

- **Limited Endpoint Protection:** Most IoT devices are low-power, low-complexity and low-cost. Manufacturers have little incentive and few resources to add complex security mechanisms onto the devices themselves. Most devices have limited processing capability and simply do what their software directs, uploading information to a control server. Endpoint protection is not feasible in most cases.
- **Limited Visibility:** Unlike consumer smartphones, functions performed by IoT are usually intended to minimize user interaction, so any misbehavior may go unnoticed for some time. Industrial or enterprise applications are often deployed in remote or inaccessible locations, so they are physically less secure and not under direct observation.
- **Expanded, Dispersed Attack Surface:** Most IoT devices are broadly deployed, expanding beyond the geographic serving area or security perimeter of any individual service provider network. The devices are usually in a different physical location from the controllers with which they interact. The controllers can be in a data center or virtualized into the cloud. The potential threat vectors open for hackers to access things, or even the controllers themselves, are quite extensive and costly to monitor.

3. Oracle Infographic: Energize Your Business with IOT Enabled Applications
4. Source: 5G Americas, "LTE and 5G Technologies Enabling the Internet of Things," December 2016
5. ForeScout IoT Enterprise Risk Report, 2016
6. ZDnet, "IoT devices can be hacked in minutes warn researchers," Oct. 25, 2016

- **Business Value Variance:** Not all IoT services have equal value, but they still require protection. For example, some IoT devices are merely consumer conveniences, while others are critical to public safety or government operations. From a service provider perspective, the lowest value IoT devices can still create signaling or malicious denial-of-service attacks. The ability to cost-efficiently match protection capabilities (costs) to the value of the IoT system is important.
- **Service Availability:** Critical devices may need to be given priority and allowed to maintain service, even if the devices are unwitting accomplices in a malicious botnet. This requires the service provider to apply different security options for different types of IoT services and significantly limits the mitigation options of mobile operators once an attack has been initiated.

Network-Based Protection for IoT Devices and Systems

Palo Alto Networks Next-Generation Security Platform empowers service providers to establish a new security posture and take the lead in IoT protection with advanced, application-layer, network-based security mechanisms.

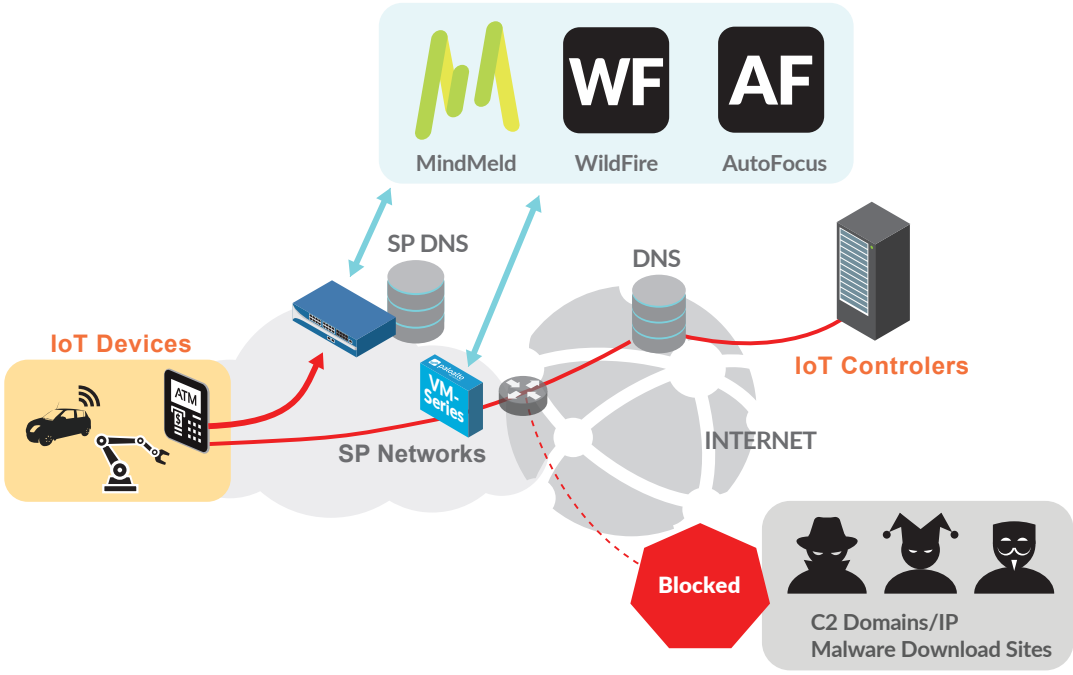

Figure 2: Palo Alto Networks Next-Generation Security Platform protects IoT systems and endpoint devices

With advanced capabilities from Palo Alto Networks, service providers can take a proactive stance on security in the IoT ecosystem while providing added value to their industrial, enterprise and consumer subscribers who have deployed connected "things."

The Palo Alto Networks platform provides protection for IoT systems and networks through the detection of malicious activity and blocking of suspicious traffic (or applying other enforcement), and it prevents further infection through the automated updating of threat mechanisms and continual monitoring of vulnerable devices. These platform capabilities are described next.

First Detect Infected Devices and Malicious Activity

Today, over 400 million IoT devices utilize cellular networks worldwide, most deployed within the last seven years.[7] With this large volume of active devices, deployed when there may have been less awareness of potential risks, identification of any already installed malware on the devices is the first step toward ensuring the protection of IoT systems.

The malware infection cycle, shown in Figure 2, illustrates the delivery and communication steps used. After a device is infected, the malware application must communicate with its remote command-and-control center in order to execute the malicious action, using a service provider transport and DNS infrastructure. By detecting this communication, the malicious communication can be stopped and the infected device, identified.

7. Oracle Infographic: Energize Your Business with IoT-Enabled Applications

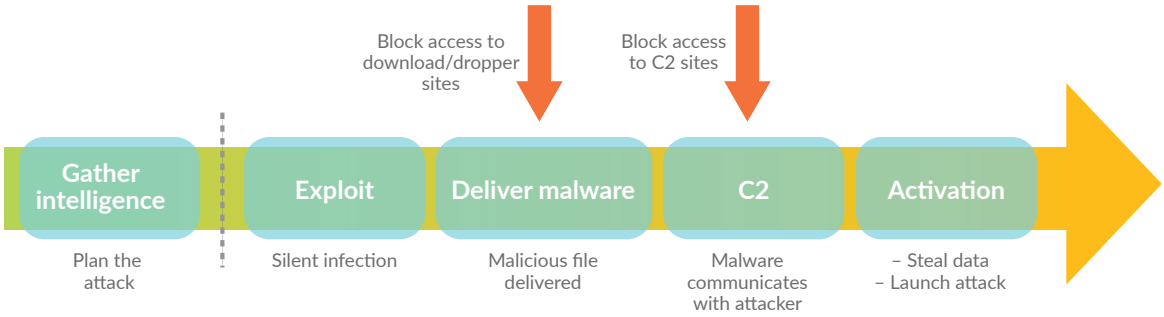

Figure 3: Malware Infection Cycle

The Palo Alto Networks Next-Generation Security Platform continually monitors traffic transiting the service provider network through its DNS infrastructure. The platform utilizes application-layer inspection to identify suspicious domains, attachments or actions. Suspected devices are displayed in the Palo Alto Networks Panorama™ network security management interface and further analysis is conducted.

Premium Prevention for Critical IoT Systems With AppWL

For those critical IoT systems, or where the business value is high, Palo Alto Networks enables the service provider to offer a premium protection layer, customized for each IoT application.

The Palo Alto Networks Next-Generation Security Platform enables service providers to establish specific application rules for IoT systems that permit communications only between authorized devices and controllers and restrict all others within that system. These application-specific "whitelist" rules (AppWL) restrict "things" from any communication with domains other than their authorized controllers, and only using approved dialects. When in place, bad actors can't even access the IoT devices. They must breach the controller to get malware onto the devices, which is a more difficult task.

However, IoT controllers are not totally impervious to potential breach. Once compromised, an IoT controller (which is likely located outside the mobile operator network) can infect all the IoT devices with which it communicates. The Palo Alto Networks platform can also assist in this situation by monitoring the communication of the IoT devices for any unusual activity that does not conform to the application whitelist rules, such as unscheduled upgrades, file downloads or other C2 communication to unlisted servers. Disrupting communications with malicious command-and-control centers and preventing the malware from executing also stops further spread of the malware.

Enforcement: Flag or Block Malicious Traffic

Any unauthorized or known malicious traffic, identified via App-ID™ technology and signatures, is blocked by the DNS servers or at other enforcement points determined by the service provider. In addition to disrupting communications with malicious command-and-control centers preventing the malware from executing as previously described, it also stops further spread of the malware. Any unknown traffic or attachments are flagged for notification and further analysis by the threat intelligence function. Armed with clear insight into which devices are infected, the service provider can enact a number of enforcement options or pursue upsell opportunities with the IoT owner for "premium prevention" against future infections.

Automated Intelligence Updates With Actionable Insight

The Palo Alto Networks Wildfire threat intelligence cloud conducts dynamic analysis of the suspicious (unknown) traffic and, if determined to be malicious, generates a new or modified prevention signature, and automatically updates all Palo Alto Networks Next-Generation Security Platform deployments to prevent malware spread.

Using AutoFocus™ contextual threat intelligence and the MineMeld application, the service provider can incorporate internal network intelligence with the WildFire™ threat analysis service and conduct system analysis for further insight into developing threat protection strategies.

Create a Security-Oriented Value Proposition

The service provider network is the transit method used for malware communications. Since the network is in the path of the attack lifecycle, the network can supply the visibility and application awareness needed to disrupt malicious activity and command-and-control communications between bad actors and compromised IoT devices. When the network can supply the visibility to see malicious activity while still developing – it can prevent the execution of an attack. Therefore, service providers – including MNOs – are in the best position to protect IoT systems.

Protect Network Availability

Recent security incidents have shown that attackers can rapidly infect large numbers of lightly protected IoT devices and leverage them as botnets – threatening the service provider infrastructure and subscribers. Thus, service providers must also take steps to protect their own network infrastructure, as well as offer protection for the IoT systems and devices that use the network.

In October 2016, a botnet of connected things strung together by the Mirai malware launched a distributed denial-of-service attack against the DNS service provider Dyn, causing internet service outages of many high-profile enterprise accounts.[8] About a month later, the same malware took a different, and more evolved, tactic by targeting a specific vulnerability in a management interface present in routers used by almost a million customers of a Tier 1 European mobile operator, with the goal of infecting the devices and making them part of a Mirai botnet. The infection attempts failed; nevertheless, they caused the routers to crash.[9]

These events demonstrate the persistence and rapid adaptability of cybercriminals and the negative impact possible to service provider networks. Attackers will continue to target devices that are largely unprotected, powerful enough, well-connected and largely ignored. IoT devices are perfect candidates.

The Palo Alto Networks Next-Generation Security Platform provides the deepest prevention for all network interfaces against malicious IoT attacks or unintentional signaling storms, with consistent manageability and application visibility across the broadest scalability range and variety of physical and virtual form factors.

Enable a Safe Network Free of Infected IoT Devices

IoT is recognized as a huge opportunity for service providers, but security issues must be addressed in order to realize the potential. Security is now cited as the No. 1 roadblock to consumer IoT adoption,[10] and new regulatory oversight is being explored as a result of several well-publicized botnet attacks on service provider infrastructure.

Palo Alto Networks proposes that service providers offer "safe networking" capabilities for things connected through mobile or other service provider networks, which allows mobile network operator to identify these infected devices, disrupt the malicious communication, and prevent future attacks.

With the Palo Alto Networks Next-Generation Platform, service providers can offer safe networking protection to their IoT customers, while further protecting their own network from IoT-based botnet attacks. Safe networking protection will strengthen the service provider value proposition, enable new monetization opportunities, and provide critical information to fortify security strategies.

8. Source: Threatpost, October 22, 2016
9. Dark Reading, Hacker 2016 To-Do List: Botnet All The Things!, January 5, 2016
10. "Accenture, Igniting Growth in Consumer Technology," 2016

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

protec-IoT-opportunity-with network-based-security-wp-022417