Pulse Secure®

Securing the Changing Landscape of the Enterprise – IoT and Beyond

Table of Contents

Introduction

IT organizations have been undergoing a fundamental shift in the types of devices they have to support that have been connecting to the network in the past decade. The days are long gone when IT staff had to support only desktops and laptops. Mobile BYOD devices represented the first wave of devices to change the status quo in terms of opening up the network beyond corporate owned devices.

IoT devices are the new wave of devices that are connecting to enterprise networks. While these devices bring with them ease of use and management along with monitoring capabilities by virtue of being IP enabled, they also present unique challenges for enterprise security teams. Previously adopted security practices have to be relooked at to mitigate risk and ensure compliance to policies in light of the changing threat landscape.

The increased attack surface is proving to be a new vector of attack that hackers are using to gain access into other parts of the network through lateral movement.

The Evolving Threat Landscape

Last week saw a huge attack on global internet access where many popular websites like Twitter, Paypal, Github, Amazon and Spotify were targeted in a DDOS attack that was launched from a botnet that controlled internet-enabled CCTV cameras. The botnet targeted Dyn who is the DNS provider for these organizations. The malware, dubbed "Mirai" spreads to vulnerable devices by continuously scanning the internet for IoT devices with factory default username and password.

Mirai is capable of launching multiple types of DDoS attacks, including SYN-flooding, UDP flooding, Valve Source Engine (VSE) query-flooding, GRE-flooding, ACK-flooding, HTTP GET attacks, HTTP POST attacks, and HTTP HEAD attacks. While none of the DDoS attack capabilities of Mirai observed to date are new or unique, it is a flexible DDoS attack generation system and can launch high-volume, non-trivial DDoS attacks when wielded by a capable attacker. Mirai features segmented command-and-control, which allows the botnet to launch simultaneous DDoS attacks against multiple, unrelated targets.

Vulnerable IoT devices become part of the Mirai botnet by continuous scanning of well-known hardcoded administrative credentials of IoT systems. The prevalence of automated scanning of the whole IPv4 internet address space means that vulnerable IoT devices can be compromised quickly.

IoT devices have been in enterprise for a while, albeit in the form of specialized devices like medical equipment and industrial control systems. There has been an explosion of cheaper and more accessible IoT devices that are making their way into the enterprise space like internet-enabled cameras, smart TVs, VOIP phones, temperature sensors. More traditional systems like HVAC are also getting internet enabled. A recent Gartner survey estimated that there were 6.4 billion connected devices in use worldwide in 2016 with the number growing to 20.8 billion by 2020. The same survey mentions that while consumer use will account for growth in numbers, enterprise will account for the largest spending on IoT devices.

As the adoption of the connected devices are increasing in the enterprise, the attack surface is also increasing. Stuxnet was the first known instance of malware that attacked industrial systems to cause damage and marked an inflection point in malware development. Since then, there have been many known instances of malware targeted specifically at IoT devices to direct damage of the equipment they control or being used as launch pads for lateral movement attacks or DOS attacks.

If the IoT devices that are in an enterprise are placed in a network segment that is access controlled from the critical data center infrastructure, it will greatly reduce the probability of a compromise. Continuously monitoring of the network so that any possible compromise can be identified and mitigated is an additional counter-measure that should be considered.

With the free availability of the botnet source code, it is only matter of time before these attacks become prevalent and target enterprises in APT style attacks. The development of specialized IoT malware has become mainstream.

Limited resources

Most IOT devices have limited computing resources and are built using embedded OS systems, frequently some favor of embedded Linux, with very little emphasis on security. The explosive interest that IoT has generated has resulted in a rush to get these devices into markets fast to capitalize on the trend. The development of many of these devices are increasing, crowd-funded and delivered by companies who are inexperienced in enterprise security requirements.

Hard to patch devices

Many of the IoT devices are hard to patch if a security vulnerability is discovered and the attack surface increases with new vulnerabilities that are found in those devices.

Employees bring IoT devices

In addition to the IoT devices that an enterprise may have like internet-enabled surveillance cameras, smart Video conferencing systems, HVAC and other control equipment, the employees may bring their own connected devices like smartwatches, Fitbits and other consumer IoT devices into the enterprise network by connecting the onsite Wi-Fi.

Exposed APIs

Some IoT systems expose APIs for integration with other products and if these are not properly secured, it could be an attack vector for malware.

Default passwords

Many IoT systems emphasize ease of setup and use over security and often this means that the factory default password for the management consoles are not changed. To make matters worse, even if the administrator changes the password for an infected system, the attackers may have installed SSH keys to gain password-less access to the device.

Increased attack surface

Due to the increased number of devices connecting to the network, the attack surface available to an attacker has also increased. Insider threat compounds this issue whereby a device can be placed surreptitiously to engage in unauthorized surveillance or to aid in data exfiltration.

Lack of controls

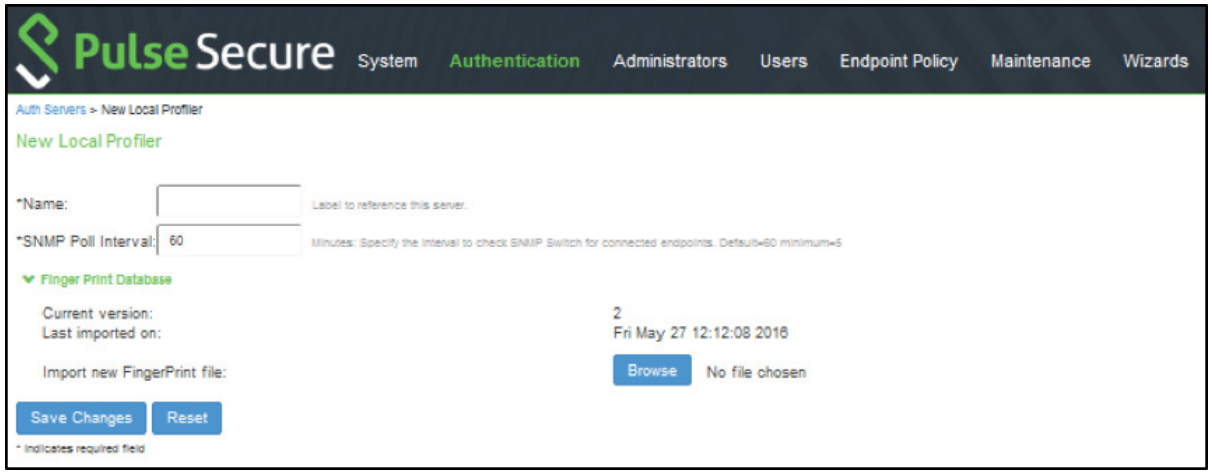
Traditional security systems that were designed to manage and control desktops, laptops and servers are not very effective in detecting IoT devices and mitigating threats originating from them.

Pulse Policy Secure

Pulse Policy Secure (PPS) is a Network Access Control (NAC) which provides complete visibility to users and devices and compliance posture based access.

IoT devices that are connecting to the network will be profiled and classified based on fine-grained attributes including type and category. Access policies based on these attributes allow the administrator to provide segmented network access to devices.

The Profiler in PPS can discover and profile all the devices in the network to provide full visibility using different profiling methods like DHCP, SNMP, Nmap.



Device Discovery Report

+ Add Device | Download Report

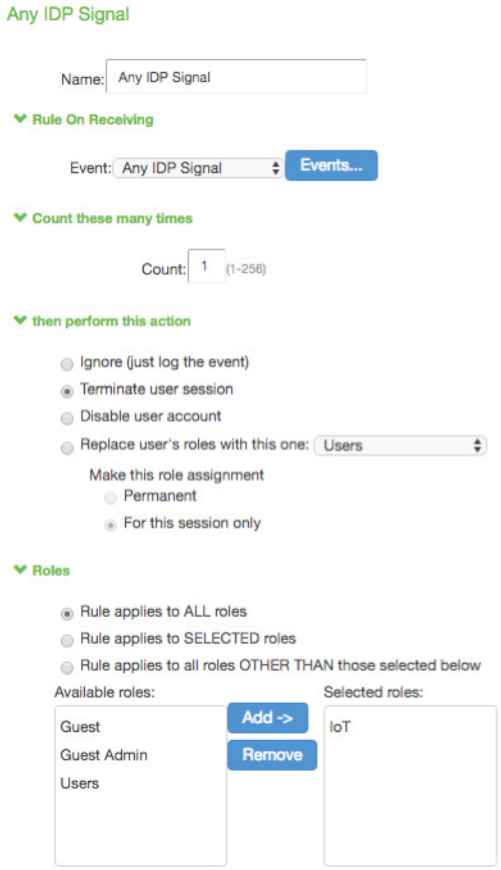
10 records per page | Search:

MAC Address	IP Address	Hostname	Manufacturer	OS	Category	First Seen	Last Seen
00:50:56:b7:0e:b7	0.0.0.0	admin-PC	VMware, Inc.	Microsoft Windows Kernel 6.0	Windows	Fri, 27 May 2016 12:17:04	Fri, 01 Jul 2016 09:50:59
00:07:5f:7a:fc:2d	172.21.3.156	datacenterpassage	VCS Video Communication Systems AG	Netgear Router	Routers and APs	Fri, 27 May 2016 12:12:16	Fri, 01 Jul 2016 09:50:59
00:07:5f:7b:e1:51	172.21.3.157	reception	VCS Video Communication Systems AG	Netgear Router	Routers and APs	Fri, 27 May 2016 12:12:15	Fri, 01 Jul 2016 09:50:58
78:48:59:9d:25:6f	0.0.0.0	HP	Hewlett Packard	HP ProCurve Switches	Switches	Fri, 27 May 2016 12:16:29	Fri, 01 Jul 2016 09:50:58
00:07:5f:7b:e1:50	172.21.3.155	mainpassage	VCS Video Communication Systems AG	Netgear Router	Routers and APs	Fri, 27 May 2016 12:12:15	Fri, 01 Jul 2016 09:50:58

An example of a Nest thermostat being profiled and classified in PPS is shown below.

Once a device is classified as an IoT device, it can be placed into the right network segment based on access control policy definition. An example of this is shown below.

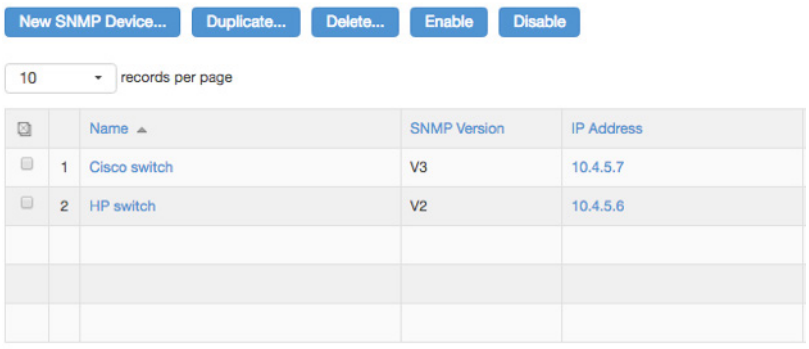
With integration from IDP, a signal from IDP can be used to kick a misbehaving device off the network. An example of this is shown below.



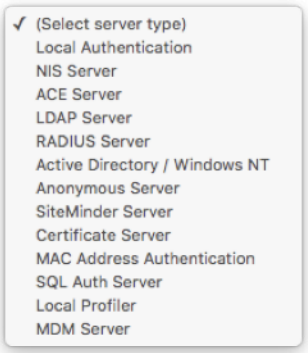
PPS supports admission control for users in addition to devices. Users can be granted differentiated network access based on their roles in the organization.

Role	Enabled settings						
	Session Options	UI Options	UAC Agent	Host Enforcer	TC Access	Pre-config	Agentless Access
Contractor	✔	✔	✔				
Engineering	✔	✔	✔				
Guest System created Guest Users role.	✔	✔					✔
Guest Admin System created Guest Admin role.	✔	✔					✔
HR	✔	✔	✔				
IoT	✔	✔	✔				
Users System created Users role.	✔	✔	✔				

PPS also supports different access methods like RADIUS (802.1x and MAC authentication) or SNMP so that the appropriate methods can be used according an enterprise's needs.



PPS supports authentication with many different authentication servers like AD, LDAP and RADIUS.



Download an evaluation copy to try it out or request a demo

Best Practices for Securing Enterprise Networks

Implementing a security program for IoT devices starts with gaining full visibility into the devices that are connecting to your network and enforcing segmented network access through access policies.

Visibility

The ability to detect IoT devices the instant they connect to your network is key. You cannot control what you cannot see. Devices need to be identified and classified by fine-grained attributes so as to aid in design of effective access policies. Further, this allows investigation efforts where you need to figure out what a device was doing in a given time interval.

Discover devices

Devices that are connecting to your network, both on premise or remotely, need to be discovered and profiled so that appropriate access control policies can be designed. Are all devices that are seen expected? Are there any BYOD or IoT devices? Are there any compromised devices on the network?

Monitor network traffic

Inspecting network traffic can give a good indication of the different types of devices that are connecting on the network. Network traffic like DHCP, SNMP, NetFlow, SPAN traces can be examined to profile the device.

Monitor network infrastructure

Network equipment like Wired switches, Wireless LAN controllers and Routers should be queried to find out all the devices that can connected on the LAN network. Additionally, VPN gateways should be used as a source of identifying which devices are connected remotely.

Identify unmanaged devices

Once visibility is there into all the devices that are connected to the network, special attention should be paid to identify unmanaged devices on the network. Corporate issued devices are usually bound by policies that ensure a higher level security which are generally not adhered by employee owned devices. The unmanaged devices usually are soft targets for an attacker to infiltrate into the network and move laterally.

Control

Once you gain visibility into what is connecting to your network, you can design access control policies based on device type and compliance posture.

Network segregation

Differentiated access should be implemented for devices with differing capabilities. For example, laptops and desktops should be in a different network segment than printers or HVAC systems. Employees in different functions (like Sales, HR, Marketing etc) should have access only to the corporate servers related to their functions. Implementing a fine-grained access strategy is essential to mitigating effects of any breaches that may occur.

Integrate with Identity store

The network access control policy should use mechanisms that integrate with corporate identity stores (like Active Directory or LDAP stores) to authenticate users and/or devices. Strong authentication is essential for security and auditing access.

Implement network controls

Access policy implementation should meet industry standard 802.1x/RADIUS based authentication for users and devices wherever possible so that the right level of access is granted. Network infrastructure access should be driven from the access policy determined after authentication. These are generally done by setting VLANs or ACLs on switches.

Firewall/IDS integration

IoT devices use embedded OS, unique industry-specific protocols, so it is essential to do deep packet inspection to identify malicious payloads for compromised devices. After detecting a compromised device, Firewall/IPS can trigger an alert to the NAC solution to block or isolate specific IoT devices from the network.

Conclusion

IoT devices bring increased efficiencies to an enterprise at the cost of decreased security. The rush to bring these devices into market mean that most effort is put into functionality and usability while almost none into security. The rise of malware targeted specifically at IoT devices continues to increase since they make attractive beachheads to launch targeted attacks.

To effectively support IoT devices, visibility and control of devices is key and is critical to ensuring security to the whole enterprise.

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize the company's Pulse virtual private network (VPN), network access control and mobile security products to enable end user mobility securely and seamlessly in their organizations. Pulse Secure's mission is to enable open, integrated enterprise system solutions that empower business productivity through seamless mobility.

References

1. IOT DDOS attack
   https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault
2. Gartner IOT report
   http://www.gartner.com/newsroom/id/3165317
3. IOT devices under attack
   https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack