CALIFORNIA STATE UNIVERSITY SAN MARCOS

THESIS SIGNATURE PAGE

THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE

MASTER OF SCIENCE

IN

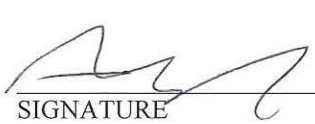
CYBERSECURITY

THESIS TITLE: The Internet of Things – An Engineering Approach to Combating a Potential Skynet

AUTHOR: Lee Chieffalo, Lauren Wright

DATE OF SUCCESSFUL DEFENSE: May 3rd, 2018

THE THESIS HAS BEEN ACCEPTED BY THE THESIS COMMITTEE IN
PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF
SCIENCE IN CYBERSECURITY

Teresa Macklin THESIS COMMITTEE CHAIR	 SIGNATURE	5-3-18 DATE
Charles Renert THESIS COMMITTEE MEMBER	 SIGNATURE	5/3/18 DATE
Ali Ahmadinia THESIS COMMITTEE MEMBER	 SIGNATURE	5/8/18 DATE

The Internet of Things – An Engineering Approach to Combating a Potential Skynet

Authors
Lee Chieffalo
Lauren Wright
Cohort II
May 2018

California State University, San Marcos
College of Science and Mathematics
333 S. Twin Oaks Valley Rd., San Marcos, CA 92096

In partial fulfillment of the requirements
For the Degree of Master of Science, Cybersecurity

Faculty Advisors
Project Chair:
Teresa Macklin, Chief Information Security Officer, CSUSM

Committee Members
Charles Renert, Chief Cybersecurity Strategist, Viasat
Dr. Ali Ahmadinia, Associate Professor, CSUSM

Abstract

Our Semester-in-Residence project was conducted at Viasat, Inc. (“Viasat”) located at the Company’s headquarters in Carlsbad, California. Viasat is a global telecommunications company that provides secure transport services to residential, business, government, and military customers. For our Semester-in-Residence project, we worked with the networking team and the Security Operations Center (SOC) team of Viasat, Inc. to install and configure third party products to detect, identify, and classify device types on the network, group these devices into categories based on the network traffic and behaviors associated with them, and finally, begin to develop security related rules/policies for the identified traffic and related behaviors in order to reduce the risks that Internet of Things (IoT) devices pose.

The ability to positively identify device types was imperative to the project: in a 2017 report, Gartner made the projection that 20.4 billion IoT devices will be in use by the year 2020, and, in a 2018 publication, made the claim that IoT devices introduce a multitude of security challenges to not only the devices themselves, but also to the systems to which they are connected to. As an Internet transport company providing connectivity to customers and forecasting Internet consumption for the near future in a non-infinite bandwidth reality, it is imperative Viasat understand the devices on the network at large and identify ways of categorizing and handling this traffic at scale.

Our project proposal garnered technical and business development leadership interest: the ability to enhance customer experience, decrease network downtime, and decrease wasted bandwidth consumption to improve network security and reputation, brand loyalty and monetary savings was a worthy undertaking.

Installing and configuring vendor hardware into physical Internet Service Provider (ISP) -level network space was the most time consuming and most technically complex piece of the project. The vendors' capabilities introduced the classic "create it or buy it" scenario that technical companies often face; for this project, Viasat opted to pursue utilizing the vendors' capabilities to accomplish detecting and identifying endpoint device types to focus efforts on better classifying and understanding the network and how to most effectively enforce security-centric policies in the future.

With the proliferation of IoT devices, it is imperative that ISPs and security providers implement creative identification and effective enforcement solutions that stymie the risks these devices perpetuate all while being at the distinct disadvantage of not owning or administering the devices at either end of the conversation.

Acknowledgements

The authors would like to thank the individuals whose contributions to this project were invaluable.

We would like to thank Teresa Macklin, the Associate Dean and Chief Information Security Officer of California State University, San Marcos for her unwavering tenacity and willingness to set us up for success. Without her guidance and patience, we would not have been able to get this project off the ground.

We would like to thank Charles Renert, the Chief Cybersecurity Strategist of Viasat, Inc. for believing in this project and for his help not only with creating the project proposal but also with helping us refine strategies and direction along the way. Without his leadership and support, the funding and allocation of resources necessary to make this project a reality would not have been possible.

We would like to express our gratitude of the internal Viasat team, especially Nick Desnoyers, Nick Saunders and McKenzie Velia for assisting us with architectural design, tool installation, configuration validation of networks and tools, interpretation of massive amounts of data, and the valuable recommendations, insights and ideas throughout the project's duration. Without their help, this project would not have been as successful as it was, and it would not be continuing as it is into the summer.

We would like to thank the ForeScout technical and business team, especially Tom Leyland, Burke Adams, Zach Dworak, and Tara Mattmuller for their involvement in getting their company's appliance to align with the use cases of the project.

We would like to thank Charles Renert and Dr. Ali Ahmadinia for serving as valuable committee members to our projects.

Finally, we would like to express our gratitude to our families and friends for their support and encouragement throughout the process of our academic undertaking, especially during the duration of our project research, development, and thesis culmination.

Table of Contents

The Internet of Things – An Engineering Approach to Combating a Potential Skynet

Introduction and Background

IoT devices are the newest scourge to the Cybersecurity industry. Manufacturer's priorities are to be the first to market to beat competition. This strategy makes sense for businesses but is (typically) accomplished at the detrimental cost to device security. The speed at which technology is developing far outpaces any manufacturer's desire or ability to make these devices more secure. Consumers' naiveté of IoT security risks compounds the reality that no government has been capable of legislating (or even meaningfully regulating) this industry to protect consumers, ISPs, or businesses. The consequences have beckoned a new, extremely dangerous present and future: the IoT devices of today and tomorrow can be leveraged to perpetuate malicious intent.

These devices are everywhere: our kitchens, our bodies, our offices, our buildings, the list is expansive. They assist with a multitude of tasks: inventory stock levels, health, entertainment, and security- purposes that are all Internet capable and connected. As IoT devices become more ubiquitous, consumers become reliant on them to the point of absolute dependency. These devices are a security risk due to inherent resource constraints, limited configuration ability, limited manageability of network interfaces, and lack of established methods and standards. IoT devices are frequently and highly vulnerable to compromise and can result in degradation of services, violation of consumer privacy, and the enablement or propagation of criminal activity.

The problem is multi-faceted: average IoT users have little (to no) notion of the dangers, consequences, and security ramifications of these devices, manufacturers lack incentive to delay product releases due to security concerns, and the vast majority of the people capable of securing these devices do not have the necessary access to make security related configuration changes.

Purpose of this Project

The purpose of this project is to develop a security enclave that positively identifies and fingerprints IoT devices within a network to provide an ISP or security provider a means of protecting consumers, ISP infrastructure, and network reputation by classifying devices and endpoints so that performance and security related actions can be proactively implemented on the network. The capability of positively detecting, classifying, and performing actions on types of traffic has the potential to dramatically reduce the risk that IoT devices present not only to consumers, but to ISP infrastructure and service availability as well.

Why the Problem is Worth Solving

There is no single answer to solve the IoT security problem. This project provides the first step in developing the capability to stymie the consequences of IoT security risk pervasiveness- it is a reactive solution to a systemic problem. The end state of the security enclave will empower the ISP to proactively mitigate network risk. As an ISP, we are confined by the following realities:

1. We do not own, manage, or administer our customer's end devices- we cannot affect change or push security configurations to these devices to make them more secure,
2. Customer experience and brand loyalty diminishes significantly when there are traffic delays or any sort of degradation in service availability, and
3. ISP owned infrastructure is adversely impacted when targeted by these attacks perpetuated by IoT devices

As an ISP, only transport is provided to our customers. Our initial assumption before beginning this project was that end users are either unaware of IoT device compromise, or that they are ambivalent to ongoing compromise until such compromise affects them directly,

manifesting typically as data over-consumption on a data-capped internet plan, or as service degradation attributed to malicious traffic. Consumers likely maintain this attitude because of a lack of user education, and the complete absence of manufacturers' commitment to produce hardened, more resilient IoT devices.

ISPs are in a unique, powerful position to eliminate the risk caused by this dilemma: all the network traffic, regardless of source or destination endpoint, must transit ISP systems. This level of visibility provides us with massive insight to detect when large scale attacks involving thousands, hundreds of thousands, or even millions of endpoints begin to conduct attacks or large Internet sweeps looking for vulnerabilities to exploit. Even more valuable is that an ISP is in the position to enforce traffic policies at scale to not only provide better overall service to our consumers but to also make a safer, more secure and more resilient Internet for all who utilize it.

Materials and Methods

Identifying and fingerprinting devices based on traffic analysis has no easy or straightforward solution. We utilized numerous tools to garner a greater understanding of the network:

1. CounterACT, ForeScout - Leveraged by our team to perform detection, identification, fingerprinting, and classification of data based on traffic flows, especially on IoT devices,
2. Kentik - Leveraged for network traffic analysis,
3. Peakflow, Arbor - Distributed denial of service (DDOS) detection and protection,
4. QRadar, IBM - Flow based security analytics
5. Threatstream, Anomoli - Threat intelligence integration platform

Using these highly-specialized tools was imperative: each tool provided perspective based on its respective position in the network and, when the data from these tools was used in conjunction with each other, enabled us to positively achieve our goal of identifying and classifying devices and the associated behaviors. With the combined data and intelligence feeds, we determined the following:

1. Frequency of connection attempts over intervals of time,
2. Traffic directionality,
3. Categories of behavior (normal, benign, suspicious, malicious),
4. Protocol and payload attributes of network flows,
5. Source and destination analysis based on risk calculations (calculations were derived internally by our data science team and other sources), and
6. Border Gateway Protocol (BGP) next-hop and route traversal information

We quickly determined that decoupling classification and enforcement capabilities was desirable: leadership valued the degree of confidence we garnered from these tools and building

many measures to establish a more accurate baseline. We identified malicious traffic from every possible perspective for an ISP: sourced from external endpoints destined to our internal customers, sourced from our internal customers to external endpoints, and laterally, sourced by our internal customers to other internal networked customers' devices.

Threat intelligence feeds kept us abreast of current and ongoing attacks occurring elsewhere in the world, and our internal tools coupled with our security analytics team allowed us to derive our own internal threat intelligence. Using these technologies and data points, we built a set of proactive network policies capable of quickly rate limiting or "black-holing"[1] the traffic associated with either known exploits or malicious activities identified on the network. The ability to rate limit or drop this traffic altogether has immediate monetary, security, and brand benefits: improved security posture of the network, greater control over traffic handling/shaping, and greater bandwidth capacity, availability, and resilience for customer data, which generally sustains higher levels of customer satisfaction.

Phases of Accomplishment

Accomplish Visibility

The first phase of our undertaking was to accomplish visibility into a portion of the network. This was achieved by installing ForeScout's hardware and by configuring a Gigamon network tap[2] within one of the ISP's core nodes. ForeScout software came installed on a server appliance that uses a custom operating system (OS) based on CentOS-7, a distribution of the Linux operation system. The network tap was not configured to enforce any port or protocol

[1] A place on a network where incoming or outgoing traffic is discarded and no response is provided to either endpoint

[2] A network test access point (TAP) is a hardware device inserted into the network that replicates traffic passing between nodes

restrictions for the traffic. Corresponding management and control plane traffic from network services that the ISP hosts (DHCP, DNS, NTP) was also included in the traffic sent to ForeScout. The ForeScout appliance was connected to the network tap using two ten gigabit copper links. The network tap was configured to communicate to the connected switch regarding the subnet range/virtual local area network (VLAN) information to capture. The switches were configured to utilize Juniper's Switch Port Analyzer (SPAN) protocol which meant that no matter which switch the targeted network traffic traversed, all the data sourced or destined to the network range would be sent to the configured VLAN. The switch sent this VLAN traffic to the network tap which replicated the traffic to the ForeScout applicant, guaranteeing that the appliance received all aspects of network traffic involving the targeted network ranges. By configuring the network to send network data in this manner had several benefits:

1. No oversubscription for ForeScout- The ForeScout appliance did not have to spend compute cycles filtering out data packets it was not configured to monitor
2. Viasat-enforced network visibility limitations for third party vendor: ForeScout was configured to monitor only the subnets our team specified to properly scope the tool to a manageable sampling of customer data; however, this was the only data that was sent to the tool anyways. No other traffic was seen by the tool.

The chosen subnet ranges included 3,584 customers on the data plane (and corresponding management plane traffic) and was constituted of residential users and commercial businesses. No government data and no airline data was included in the collected dataset. The subnet ranges, and thus, the subscriber set, were chosen based the following factors: geographic location, non-government customers, non-aircraft customers, and ISP infrastructure limitations. The data set size was large enough to create a diverse set of endpoints while also properly scaling the

customer set size to a manageable quantity for our use cases. Once we had this visibility, our next step was to detect and identify the types of devices communicating on the network.

Detect and Identify Device Types

Phase two of the project was dedicated to detecting and identifying the device types in the network traffic conversation. We utilized ForeScout's CounterACT tool to implement this capability. Using their proprietary methods, devices were detected, identified, and sorted into categories based on vendor, for example: Apple, Inc. devices, Samsung products, Asus, NetGear, etc. Based on this information we moved to the next phase of better understanding the devices.

Device Classification

Phase three of the project was focused on classifying the devices into categories based on their underlying operating system. One of ForeScout's capabilities is to perform the reconnaissance necessary for determining this data. It was at this phase that we could detect the operating systems associated with the devices. It is true that knowing purely the manufacturer or vendor of the device could directly correlate to the underlying operating system (Apple is to iOS as Microsoft is to Windows, etc.); however, detecting this information based on various each of the internet protocol layers increased our confidence in the accuracy of the device fingerprinting, especially when customers could be spoofing information.

Determine Compliance

Our next phase was determining compliance. ForeScout reported the ports and services running on the devices enabling us to answer more definitively which device(s) were responsible for types of network traffic. We created policies based on known malicious attack patterns to determine (based on the device, vendor, operating system, ports, protocols, and underlying traffic

patterns) which devices belonged to certain categories of traffic based on network behavior. We configured custom policies tailored to our network needs using the following attributes:

1. The wireless routers that the clients had ("Customer Premise Equipment", or CPE wireless router),
2. The OS and model number of the router (CPE),
3. Open ports on the router,
4. Media Access Control (MAC) address of the router,
5. Dynamic Host Control Protocol (DHCP) server subscribed to, and
6. DHCP options

Using network metadata, we identified the existence of customer devices behind their home routers, and, subsequently, the device(s) operating system, open ports, and traffic signatures from the received and transmitted traffic. Custom policies did not come pre-configured by the ForeScout tool- it is the responsibility of the ForeScout administrator to build policies for the environment.

The first step of policy writing was based on the initial classification of the traffic that ForeScout was seeing. To classify devices, we utilized the following collected details: network metadata, organizationally unique identifier (OUI) codes of connected devices, Network Mapper (NMAP) results, and DHCP options. After classifying the devices, we created sub-policies that worked in conjunction with the primary policies. Sub-policies enabled us to separate data into logical groupings: distinguish manufacturers from model types and versions, data from voice traffic, etc. Logically grouping devices based on functionality and vendor enabled us to build directed policies for advanced enforcement and management techniques. To create these sub-policies, we clarified and enriched the data originally detected by ForeScout.

Next, to clarify the results, we used DHCP options and NMAP results to more accurately determine the operating systems, open ports, and any other associated device details, if any. This information was aggregated into a profile for each individual primary device (wireless router). Since we do not administer customer devices, we could not utilize the numerous Network Access Control (NAC) mechanisms native to ForeScout's CounterACT tool. To overcome this, we built compliance policies to detect and alert on exploitation or malicious traffic targeting or origination from our customer's devices. We achieved this by tying alerts to specific device vendors and models details detected by underlying policies to identify compromise attempts against highly exploitable devices, for example, routers made by Ubiquiti, Netis, and ReadyNet, or to identify specific traffic patterns or metadata indicative of a compromise such as Mirai, Hajime, Satori, and Jen-X botnet signatures. Finally, we built application metadata polices to correlate threat intelligence, application level Domain Name Service (DNS), and Hyper-Text Transfer Protocol (HTTP) traffic indicative of compromise.

The policies excelled at identifying device types associated with the data traversing the network, categorizing them and making determinations based on network activity. It is at this point that we experienced architectural flaws within ForeScout's implementation for our use cases:

1. **The CounterACT tool was built for an enterprise environment that retains administrative control of its endpoints**, not an ISP with the complete antithesis of this capability (with respect to customer devices). Out of three categories of traffic, we were able to identify and fingerprint one of them: lateral traffic. We attributed this to an underlying ForeScout presumption: each side of the conversation must be an internally managed device. Since lateral traffic flows are within the same managed subnet, the tool

successfully detected the traffic as defined by the policy but also classified threats in the traffic that was not defined by any policy; this gave us the ability to react to known and unknown malicious traffic patterns between endpoints without analyst intervention

2. **We were not fully capable of identifying and classifying suspicious or malicious traffic not pre-defined via custom policy**. Because of this, our ability to discover traffic sourced from the internet or sourced from our clients destined to an unmanaged network that could be classified as malicious or suspicious based on behavioral and statistical anomalies was greatly impacted. After many days of troubleshooting and custom policy development with ForeScout engineers, we determined that ForeScout's CounterACT tool (as currently implemented at the time of this writing) is unable to effectively detect and notify analysts of any inbound or outbound threat not specifically tied to policy due to database resource limitations, licensing restrictions, and programming process limitations.

To conclude, we successfully utilized ForeScout's extensive detection capabilities to fingerprint devices traversing our network, but we are unable to recommend its further development outside of device typing within our security enclave based on the aforementioned limitations. Because of this, we must revise future goals and strategies; however, we will likely continue leveraging information from our shaping and acceleration ecosystems to obtain and maintain the visibility necessary to make security determinations of every packet that traverses the network. Future iterations to security enclave development will enable these capabilities to function at scale across the enterprise and be autonomous for classifying malicious traffic and notifying an analyst when suspicious traffic is found.

Discussion

There is a constant barrage of threats primarily involving IoT botnets (Mirai, Satori, JenX, Hajime)[3]. We successfully measured the volume of compromised logon attempts targeting IoT devices and wireless routers: they are numerous, constant, and are typically sourced from the following countries: China, Russia, the Netherlands & France[4], Brazil[5].

The top IoT devices being exploited and their associated manufacturers are the following:

1. Cameras: Huewai, TRENDnet
2. Routers: Ubiquiti, Netis, Zyxel, Mikrotik & ReadyNet
3. TVs: Samsung
4. Phones: Huewai
5. OS: Android, BusyBox
6. DVR: XiongMai Technology components

The network traffic supported prior findings regarding malware exploit propagation behavior: once a machine is compromised, malware code targets the network information of the devices (IP, subnet mask, default gateway) and performs enumeration activities to find neighboring devices to attempt further exploitation. Out of our customer subset in one of the core nodes, 325 customers, or approximately 10% of the traffic, constituted this behavior.

[3] The four names listed are (at the time of this writing) recent, prominent malware campaigns that turn devices (usually IoT devices) into botnets

[4] Traditionally and extremely popular due to European Union privacy policies that prevent the cloud providing from shutting down outbound attacks, making it a popular haven for hosting or routing attacks (also known as bulletproof hosting)

[5] Large population of antiquated, low-cost, and/or pirated devices, making them highly susceptible to exploit

The most targeted IoT exploit ports are 22 (SSH[6]) and 23 (Telnet[7]) for general remote management, 2222, 2323, & 23231 for the original Mirai strain, 5555 and 7547 for the Satori and Gen-X strain of Mirai, and most recently 2000 and 8291 for the Hajime/Slingshot malware.

In addition to running network enumeration scans, the infected devices also perform numerous extremely network intensive credential brute force attacks and distributed denial of service (DDoS) attacks against neighboring targets and towards the Internet. During this project, our team discovered that the devices are being leveraged for their network and routing capabilities to act as (extremely effective) proxies[8] or as virtual private network (VPN) termination points could be attributed to IoT devices. Infected IoT devices operating in this manner can be leveraged for data exfiltration through our customer's routers, traffic anonymization purposes, circumventing government or geographic content restrictions for various services by making the attacker appear to originate from the United States while really streaming data to the true origin location, and many more uses. The impact of these attacks are severe: it would make the origin of an attack virtually impossible to identify, the attack would force the client to go over data caps, and the company risks significant reputation damage.

During this project, we identified, correlated, and quantified attack traffic that was detected and black holed during March 2018. We developed dynamic mitigations to proactively our Internet drains. The first attack pattern we developed correlation for are DDoS attacks targeting our customers. This attack traffic is prevalent across out entire customer base and far exceeds the amount of data we could reasonable push to CounterACT via the network tap.

[6] The Secure Shell protocol, used for securely managing remote devices on an unsecured network
[7] The Terminal Network protocol, also used for managing remote devices. This protocol does not provide cryptographic support. All data is transmitted unencrypted
[8] Technological capability of routing traffic directly through a system to anonymize the source of the originator. Malicious attackers typically utilize this technology to increase the overall separation between origin and the target

During March 2018, our customers were targeted by 110 attacks that each measured over 100 megabits per second. To put this in perspective, the average customer operated with a downlink bandwidth of 20 Mbps. All of these attacks were capable of knocking a single client offline for the duration of the attack. Out of the 110 attacks we were able to completely detect and mitigate 67 of them. Out of the remaining 43 we were able to partially mitigate these attacks. These attacks were categorized as Fast Flood attacks that basically hit you with a mass of traffic at the front of the attack and due to convergence times and protections built into our detection algorithms to prevent false positives we were prevented from mitigation 100% of these attacks. However, in most of these cases due to the high volume of connection attempts created by these attacks they are still dropped by our shapers before getting to the client.

The most common type of DDoS attack is fragmentation based. This is a protocol exploit built into User Datagram Protocol (UDP) that leverages the fragmentation capabilities within UDP to create millions of garbage packets over UDP port 0. Since most appliances only see port 0 as an overhead port it will allow it through until the entire datagram can be rebuilt and the actual port defined. However, in this case there is not an original header, so the effect is bandwidth consumption by useless traffic. This constitutes around 65% of our DDoS traffic. The remaining DDoS traffic falls into either the amplification or flooding subtypes. The 110 attacks consumed 50.8 TB’s of total volume, 47.3 of which was mitigated by the enclave. Most of these attacks came from compromised IoT devices with networking functionality being leveraged to conduct these operations. In most cases, the owners of these systems are completely unaware that their devices are being used to perpetuate these attacks.

The other traffic blackholed throughout the month of March 2018 is categorized into two types. The tier 1 classification consists of horizontal and vertical scanning and brute force exploit

attempts detected through automated mechanisms while tier 2 classifications correspond to decisions by analysts deeming the traffic malicious. This traffic is mitigated through the implementation of a dynamic Access Control List (ACL). This list currently consists of an estimated three million internet addresses that represent a large degree of compromised internet exposed hosts used to conduct reconnaissance or perform specific attacks on certain targets or actual Command and Control (C2) nodes controlling armies of bots.

During March 2018, this ACL detected an average rate of 13.62 MBps which would translate into 36.5 TBps of traffic that was black holed. This brings the total to 87.4 TBps of traffic that was offloaded from clients during the month of March. This represents only the inbound traffic that is sourced from the Internet and destined to one of our clients. At the internet drain before data traverses the satellite we have detailed visibility of traffic coming in and we can easily build filters to blackhole malicious traffic. Conversely, we do not have the same visibility for traffic originating from our consumers. Because of this lack of visibility, we have only been able to convict on and block outbound attack traffic sourced from 2091 customers infected with malware. Since integrating with CounterACT we have the appropriate network visibility (within a portion of the network) to determine accurate measurements of customers infected with malware. If we implemented CounterACT at scale across our enterprise this measurement is expected to scale as well and be approximately 20,000 customers.

Because the filters placed in customers modems restrict the traffic to their Local Area Network (LAN) we cannot measure the amount of bandwidth conserved from going over the return link of the satellite. However, before the filters were put into place, each infected customer was producing an average of 50 GB’s of traffic per 24 hours. This volume of traffic consumed

the customer's entire upload bandwidth speed and counted negatively toward their data consumption limits for any given pay period.

The results provide evidence that the traffic believed to have been already blocked at the edge was still being allowed into the network, indicative of a configuration error somewhere in the network. The tool appropriately highlighted a configuration believed to be no longer a problem. In the future, we would like to:

1. Extract currently attacking IPs and dynamically block them for the duration of the attack,
2. Determine service level attacks against our clients and fingerprint some of the types of attacks, worms, botnets, etc. that are attacking our customers

Next Steps

The next phases of the enclave are to expand the integrations with our threat intelligence, traffic shaping and monitoring utilities. By expanding these capabilities, our visibility of the management, control and data planes will increase substantially. Once these integrations are developed, we can begin orchestrating security mitigation strategies and providing a tiered response to traffic being classified as malicious by the enclave.

Tier 1 classifications tentatively include general scanning, brute force, known exploit traffic, and DDoS attacks originated from the internet and by our customers. Once detected, the attack traffic will be fingerprinted based on the N-tuple of information needed to fingerprint the attack and a mitigation will be crafted and sent to either the Internet drains or the modems based on the origin of the traffic.

Tier 2 classifications tentatively consist of anomalous or suspicious traffic that strays outside of the baseline heuristics known for that client and can also consist of traffic identified by threat hunting activities. Once detected, this traffic will cause a Security Operations Center analyst to be alerted and the associated traffic will be tapped to capture the flows. Once a mitigation is crafted, it will be applied to Tier 1 detection facilities to ensure inline mitigation of the threat at scale, for the duration and every occurrence afterword of the attack.

All data regarding attacker origin will be collected and sent to our big data analytics team. With the involvement of the Data Science team, we will build and disseminate real-time active threat intelligence to all the sensors and interdiction tools in the network as STIX or TAXII feeds. This intelligence sharing capability will enable us to protect our enterprise regardless of the attack type targeting our network. This intelligence can also be shared with partners and Viasat external consumers. By sharing this data, we foster information sharing

within our community with the intention to build a more secure internet that is difficult for attackers to exploit and malware to perpetuate.

References

Bamiduro, Wunmi. Meulen, Rob van der. (2018). *Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018*. Gartner. Retrieved from https://www.gartner.com/newsroom/id/3869181

Meulen, Rob van der. (2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*. Gartner. Retrieved from https://www.gartner.com/newsroom/id/3598917

Tool Versions

- Arbor, version 8.2
- ForeScout, version 7
- QRadar version 7.3.0, patch 7

Acronyms

Acronym	Meaning
ACL	Access Control List
BGP	Border Gateway Protocol
C2	Command and Control
CPE	Customer Premise Equipment
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
HTTP	Hypertext Transfer Protocol
IoT	“Internet of Things”
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
NAT	Network Address Translation
NMAP	Network Mapper
MAC	Media Access Control
MBps	Megabytes per second
OS	Operating System
OUI	Organizationally Unique Identifier
SOC	Security Operations Center
SSH	Secure Shell
SPAN	Switched Port Analyzer

Acronym	Meaning
STIX	Structured Threat Information Expression
TAP	Test Access Point
TAXII	Trusted Automated Exchange of Indicator Information
TB	Terabyte
TBps	Terabytes per second
UDP	User Datagram Protocol
VoIP	Voice over IP
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

THE INTERNET OF THINGS

AN ENGINEERING APPROACH TO COMBATING A POTENTIAL SKYNET

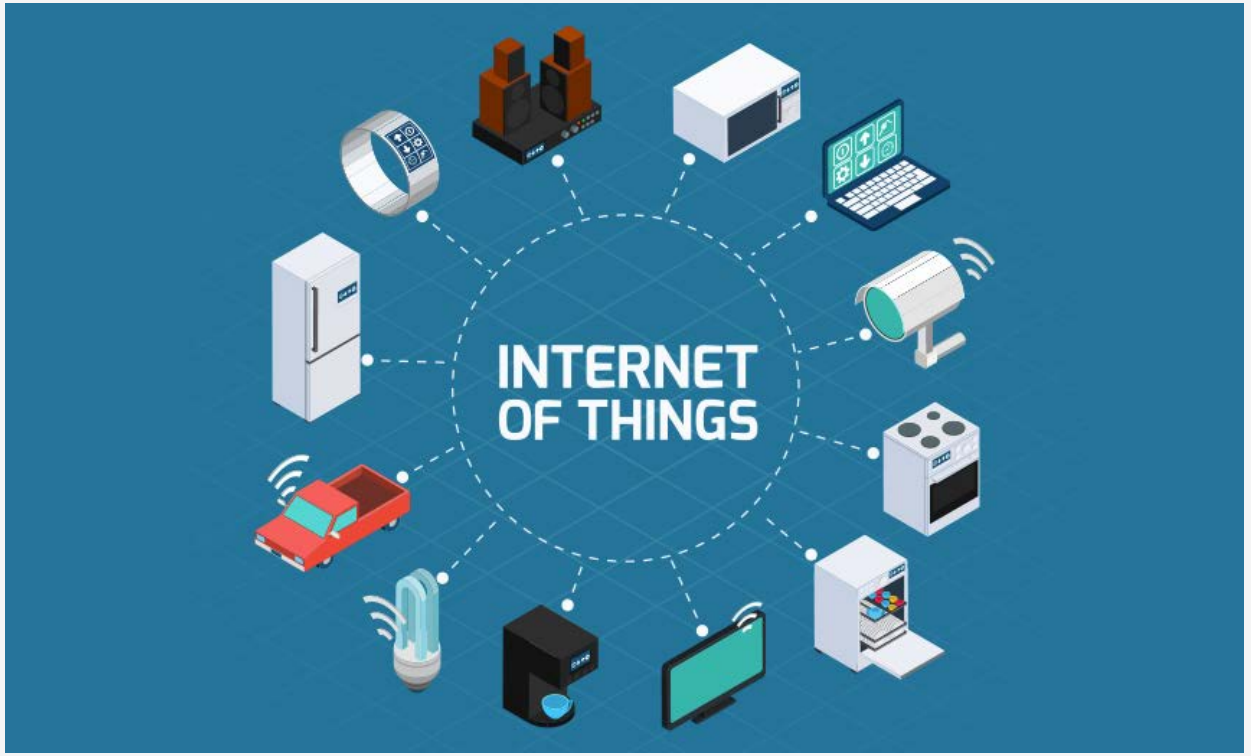
Lee Chieffalo, Lauren Wright

California State University, San Marcos
Master of Science, Cybersecurity Program

What is IoT?

A system of interconnected computing devices, machines, and objects that have unique identifiers and utilities that are network connected and capable of transferring data over a network

Without requiring human-to-human or human-to-computer interaction!



~~*What is IoT?*~~

Who can feasibly temper the repercussions of lacking IoT device security?

Nebulous Project Inception

“Wouldn’t it be cool if…”

“… as a network security administrator:”

1. I knew what device types were on my network,
2. I could conserve available bandwidth by limiting or eliminating malicious traffic,
3. I could enforce device compliance on the network

“... as an Internet Service Provider:”

1. I could sell specialized security services to the risk-prone customers,
2. I could protect my infrastructure by handling certain types of traffic *differently*

Formulated Project Proposal

- Identify device types on the network
  - Classify the IoT device quantities project to increase rapidly.
  - More devices → More Traffic → More bandwidth necessary; Problem! Bandwidth is not unlimited
- Categorize devices into categories and learn about them
  - Traffic patterns: Suspicious, Known-malicious
  - Most vulnerable devices, most vulnerable categories of devices?
  - Most prevalent devices
  - Top talkers
- Do something with these traffic patterns
  - Alert?
  - Rate limit? Shape?
  - Black-hole? Alt-route?
  - Sell services?
  - Nothing?
- Enforce device compliance
- Establish foundation to provide the means of protecting customers, ISP infrastructure, and network reputation
- Identify path forward for taking performance and security related actions based on device type, network traffic, historical baseline, enriched intelligence, etc. data points

Initial Realities

- Endpoint administrators are authorized to only protect themselves, defensively
  - Residential Customers
  - Government/Military organizations
  - Businesses
- [Most] Endpoint administrators do not have knowledge, time, money, resources to protect endpoint devices
- End users are either unaware or ambivalent of IoT device compromise (until such compromise affects them directly)
- ISP have full visibility of all conversations going to and from the Internet and the technical expertise to act

Why Accomplish This Goal?

- Unique offering for an ISP
- Competitive differentiator
- Customer experience enhancement
- Resource savings on multiple systems RF & Data
- Empower ISP to proactively mitigate network risk
- **Improved network reputation**
- **Improve the overall availability and reliability of satellite and network resources**

Phases for Accomplishment

Phase 1 - Visibility

- Install and configure tools

Phase 2 - Detect and Identify Device Types

- Identify client devices on the network at their network edge (Wireless Router)
- Identify and tag suspicious/malicious traffic
- Determine technological gap for capabilities to be applied at scale for ISP

Phase 3 - Device Classification

- Underlying Operating System

Phase 4 - Determine Compliance

- Ports and Services

Phase 5 - (Future) [Automate] Malicious Traffic Mitigations

- Automate the enforcement and/or mitigation actions

Installing ForeScout

- Installed in production core node servicing ~200,000 clients
- Tied to Gigamon TAP in order to span traffic tied to specific networks for analysis.
  - x.x.x.x/21 - residential users
  - x.x.x.x/22 - business clients
  - 2x x.x.x.x/24’s corresponding management plane traffic

Technologies Utilized

- Network

- Big Data Analytics

- Threat Intelligence/Enrichment

- Future

With the Technologies We Determined

- Frequency of connection attempts over intervals of time
- Traffic directionality
- Categories of behavior (normal, benign, suspicious, malicious)
- Protocol and payload attributes of network flows
- Source and destination analysis based on risk calculations
- Border Gateway Protocol (BGP) next-hop and route traversal information

Tiers of Malicious Traffic Classification

- Tier 1
  - Distributed Denial of Service
  - Horizontal and Vertical IP/Port Scanning
  - Brute Force Attacks
  - Known malware signature exploits
- Tier 2
  - Proxy Attacks
  - Targeted exploits against a specific vendor or application
  - Social Engineering/Phishing Attacks
- Tier 3
  - APT related threats
  - Zero Day

Tier 1 Classification & Remediation

- Identification based on directionality and traffic classification
  - Inbound & Outbound
    - Sourced from internet
    - Based on connection & payload measurements or traffic fingerprint
- Remediation
  - Inbound traffic blackholed at internet drain via ACL or BGP Flowspec
  - Outbound traffic dropped at SPE modem via IP Table

Tier 2 Classification & Remediation

- Identification based on fingerprint detection, intelligence match, or threshold trip.
  - Information enriched and pushed to analyst for further review.
- Remediation
  - Analyst determination on what, why, and how the traffic can be blocked without interfering with legitimate traffic.
  - If malicious can it be fingerprinted and sent to Tier 1
  - Generate Threat Intelligence on all aspects of the 5-tuple

Tier 3 Classification & Remediation

- Identification through Intelligence TTP’s and Threat Hunting
- Remediation
  - Threat Hunter determination on what, why, and how the traffic can be blocked without interfering with legitimate traffic.
  - If malicious can it be fingerprinted and sent to Tier 1
  - Generate Threat Intelligence on all aspects of the 5-tuple

Project Outcomes

- The Good
  - We were able to detect an average of 10% of our customer base that was compromised.
  - We were able to successfully able to fingerprint exploitable router types and tie malicious traffic to them.
  - Multiple mitigations put in place in order to protect the end user
- The Bad
  - ForeScout unable to adapt to an ISP environment based on internal database limitations and licensing models
  - Due to current infrastructure limitations we are unable to get into the home to determine which device was compromised
- The Ugly
  - Lack of available technology that can exist in the ISP space and operate at this scale
  - Overwhelming difficulty for developing a process in which we can bring in the residential client to protect his own network
  - How bad it really is when you are exposed to the internet :(

Research and Implementation Methods

- Need was derived from Cyber Security need to reclaim bandwidth on satellite network
- Led to investigation of device typing technology (build/buy) strategy. Led to multiple discussions with technology partners
- Design, implementation, and engineering of all technology and transport. The classification and categorization of traffic and hardware types and the implementation of policy that will be used for the expansion to design remediation chain.

Research and Implementation Methods

- This represents traffic blackholed for our sample set of clients that matches our malware fingerprints

Discussion – Most Exploited IoT Devices

222.73.254.215	other	Multiple (3,325)	Multiple (2)	Multiple (41)	Multiple (2)
99.198.129.157	other	Multiple (2,800)	23	Multiple (15)	RemoteAccess.Telnet
50.5.135.150	other	Multiple (2,767)	Multiple (2)	Multiple (44)	Multiple (2)
185.44.76.133	other	Multiple (2,280)	23	Multiple (42)	RemoteAccess.Telnet
64.188.53.254	other	Multiple (2,108)	23	Multiple (41)	RemoteAccess.Telnet
206.189.47.157	other	Multiple (1,714)	Multiple (2)	Multiple (42)	Multiple (2)
41.226.0.96	other	Multiple (1,608)	Multiple (2)	Multiple (42)	Multiple (2)
131.213.114.47	other	Multiple (1,481)	23	Multiple (41)	RemoteAccess.Telnet
208.100.26.228	other	Multiple (1,394)	23	Multiple (43)	RemoteAccess.Telnet
167.142.248.97	other	Multiple (1,329)	Multiple (2)	Multiple (38)	Multiple (2)
191.96.249.112	other	Multiple (1,322)	23	Multiple (41)	RemoteAccess.Telnet
206.189.21.201	other	Multiple (1,303)	23	Multiple (41)	RemoteAccess.Telnet
96.8.28.31	other	Multiple (1,253)	Multiple (2)	Multiple (43)	Multiple (2)
5.128.135.58	other	Multiple (1,219)	Multiple (2)	Multiple (40)	Multiple (2)
5.188.11.93	other	Multiple (1,205)	23231	Multiple (43)	Other
118.163.16.3	other	Multiple (1,189)	23	Multiple (39)	RemoteAccess.Telnet
173.82.152.188	other	Multiple (1,165)	23	Multiple (39)	RemoteAccess.Telnet
185.244.25.202	other	Multiple (1,139)	2222	Multiple (43)	Other
103.79.74.9	other	Multiple (1,088)	Multiple (2)	Multiple (39)	Multiple (2)
185.141.26.181	other	Multiple (1,051)	Multiple (2)	Multiple (41)	Multiple (2)
222.96.190.71	other	Multiple (1,032)	23	Multiple (38)	RemoteAccess.Telnet
185.156.177.77	other	Multiple (1,002)	2222	Multiple (43)	Other
199.195.254.118	other	Multiple (994)	Multiple (2)	Multiple (43)	Multiple (2)
222.161.223.54	other	Multiple (965)	Multiple (2)	Multiple (39)	Multiple (2)
5.188.11.71	other	Multiple (964)	2222	Multiple (42)	Other
123.147.190.217	other	Multiple (962)	Multiple (2)	Multiple (39)	Multiple (2)
37.187.244.195	other	Multiple (934)	23	Multiple (40)	RemoteAccess.Telnet
195.68.111.242	other	Multiple (912)	Multiple (2)	Multiple (42)	Multiple (2)
168.167.141.76	other	Multiple (889)	Multiple (2)	Multiple (44)	Multiple (2)
200.7.101.13	other	Multiple (834)	23	Multiple (41)	RemoteAccess.Telnet

Inbound Mirai (and derivative) scanning and exploit attempts

Proxy exploit attempts against target group

139.162.70.53	other	Multiple (1,338)	1080	Multiple (43)	Other
180.97.106.39	other	Multiple (398)	1080	Multiple (34)	Other
181.214.87.227	other	Multiple (268)	1080	Multiple (31)	Other
180.97.106.163	other	Multiple (228)	1080	Multiple (34)	Other
180.97.106.164	other	Multiple (216)	1080	Multiple (34)	Other
60.191.38.77	other	Multiple (113)	1080	Multiple (30)	Other
78.106.218.44	other	Multiple (98)	1080	Multiple (13)	Other
109.200.24.7	other	Multiple (66)	1080	Multiple (15)	Other
191.187.161.177	other	Multiple (65)	1080	Multiple (17)	Other
108.58.125.2	other	Multiple (63)	1080	Multiple (13)	Other
93.174.93.218	other	Multiple (56)	1080	Multiple (14)	Other
172.104.98.231	other	Multiple (52)	1080	Multiple (18)	Other
140.82.55.198	other	Multiple (49)	1080	Multiple (23)	Other
45.32.243.178	other	Multiple (45)	1080	Multiple (21)	Other
191.101.167.252	other	Multiple (45)	1080	Multiple (15)	Other
123.206.225.251	other	Multiple (41)	1080	Multiple (20)	Other
123.206.191.189	other	Multiple (40)	1080	Multiple (17)	Other
177.132.42.115	other	Multiple (39)	1080	Multiple (9)	Other
14.134.19.1	other	Multiple (38)	1080	Multiple (18)	Other

Discussion - Malicious Traffic Identified

222.73.254.215	other	Multiple (3,325)	Multiple (2)	Multiple (41)	Multiple (2)
99.198.129.157	other	Multiple (2,800)	23	Multiple (15)	RemoteAccess.Telnet
50.5.135.150	other	Multiple (2,767)	Multiple (2)	Multiple (44)	Multiple (2)
185.44.76.133	other	Multiple (2,280)	23	Multiple (42)	RemoteAccess.Telnet
64.188.53.254	other	Multiple (2,108)	23	Multiple (41)	RemoteAccess.Telnet
206.189.47.157	other	Multiple (1,714)	Multiple (2)	Multiple (42)	Multiple (2)
41.226.0.96	other	Multiple (1,608)	Multiple (2)	Multiple (42)	Multiple (2)
131.213.114.47	other	Multiple (1,481)	23	Multiple (41)	RemoteAccess.Telnet
208.100.26.228	other	Multiple (1,394)	23	Multiple (43)	RemoteAccess.Telnet
167.142.248.97	other	Multiple (1,329)	Multiple (2)	Multiple (38)	Multiple (2)
191.96.249.112	other	Multiple (1,322)	23	Multiple (41)	RemoteAccess.Telnet
206.189.21.201	other	Multiple (1,303)	23	Multiple (41)	RemoteAccess.Telnet
96.8.28.31	other	Multiple (1,253)	Multiple (2)	Multiple (43)	Multiple (2)
5.128.135.58	other	Multiple (1,219)	Multiple (2)	Multiple (40)	Multiple (2)
5.188.11.93	other	Multiple (1,205)	23231	Multiple (43)	Other
118.163.16.3	other	Multiple (1,189)	23	Multiple (39)	RemoteAccess.Telnet
173.82.152.188	other	Multiple (1,165)	23	Multiple (39)	RemoteAccess.Telnet
185.244.25.202	other	Multiple (1,139)	2222	Multiple (43)	Other
103.79.74.9	other	Multiple (1,088)	Multiple (2)	Multiple (39)	Multiple (2)
185.141.26.181	other	Multiple (1,051)	Multiple (2)	Multiple (41)	Multiple (2)
222.96.190.71	other	Multiple (1,032)	23	Multiple (38)	RemoteAccess.Telnet
185.156.177.77	other	Multiple (1,002)	2222	Multiple (43)	Other
199.195.254.118	other	Multiple (994)	Multiple (2)	Multiple (43)	Multiple (2)
222.161.223.54	other	Multiple (965)	Multiple (2)	Multiple (39)	Multiple (2)
5.188.11.71	other	Multiple (964)	2222	Multiple (42)	Other
123.147.190.217	other	Multiple (962)	Multiple (2)	Multiple (39)	Multiple (2)
37.187.244.195	other	Multiple (934)	23	Multiple (40)	RemoteAccess.Telnet
195.68.111.242	other	Multiple (912)	Multiple (2)	Multiple (42)	Multiple (2)
168.167.141.76	other	Multiple (889)	Multiple (2)	Multiple (44)	Multiple (2)
200.7.101.13	other	Multiple (834)	23	Multiple (41)	RemoteAccess.Telnet

Inbound Mirai (and derivative) scanning and exploit attempts.

Proxy exploit attempts against target group

139.162.70.53	other	Multiple (1,338)	1080	Multiple (43)	Other
180.97.106.39	other	Multiple (398)	1080	Multiple (34)	Other
81.214.87.227	other	Multiple (268)	1080	Multiple (31)	Other
180.97.106.163	other	Multiple (228)	1080	Multiple (34)	Other
180.97.106.164	other	Multiple (216)	1080	Multiple (34)	Other
60.191.38.77	other	Multiple (113)	1080	Multiple (30)	Other
78.106.218.44	other	Multiple (98)	1080	Multiple (13)	Other
109.200.24.7	other	Multiple (66)	1080	Multiple (15)	Other
191.187.161.177	other	Multiple (65)	1080	Multiple (17)	Other
108.58.125.2	other	Multiple (63)	1080	Multiple (13)	Other
93.174.93.218	other	Multiple (56)	1080	Multiple (14)	Other
172.104.98.231	other	Multiple (52)	1080	Multiple (18)	Other
140.82.55.198	other	Multiple (49)	1080	Multiple (23)	Other
45.32.243.178	other	Multiple (45)	1080	Multiple (21)	Other
191.101.167.252	other	Multiple (45)	1080	Multiple (15)	Other
123.206.225.251	other	Multiple (41)	1080	Multiple (20)	Other
123.206.191.189	other	Multiple (40)	1080	Multiple (17)	Other
177.132.42.115	other	Multiple (39)	1080	Multiple (9)	Other
14.134.19.1	other	Multiple (38)	1080	Multiple (18)	Other

Device Typing - Triumphs and Pitfalls

Triumphs

- Successfully identified all of the wireless routers used by our client pool as well as some of the devices and operating systems of the devices behind them
- Successfully fingerprinted inbound and lateral attacks within the client pool
- Successfully identified all assets on Management and Control planes, then determined their security posture on the network

Pitfalls

- Licensing and resource issues drastically hindered our data plane detection capabilities
- ForeScout’s CounterACT Java UI was clunky and restrictive
  - Prevented us from getting outbound traffic visibility, ongoing attacks
- Custom IOC ingestion was limited and the categories built into the platform to define attack types were outdated and limited.

Thesis Project Research and Development Conclusion

- Successfully achieved:
  - Positively identifying and fingerprinting device types from a customer subset
  - Classifying device types (emphasis on IoT devices) into categories to group suspicious and malicious traffic
  - Enriching the data
  - Establishing foundation to provide the means of protecting customers, ISP infrastructure, and network reputation
    - Tools installed, policies configured
- Future development in this space:
  - The path forward to make performance and security related actions:
    - Based on categories of behaviors determined by tools, dynamically
      - Shape “categories” of traffic
      - Apply traffic filters/rules to edge network devices
    - Share derived internal intelligence across the company, maybe externally as well

Acknowledgements

Teresa Macklin for her dedication, unwavering tenacity, and willingness to set us up for success

Chief Cybersecurity Strategist, Company X for his help refining, believing in, and strategizing this project since its inception

Internal Company X Team for assisting with design, tool installation and data analytics

ForeScout team: Tom Leyland, Burke Adams, Zach Dworak, and Tara Mattmuller

Committee Members: Chief Cybersecurity Strategist of Company X and Dr. Ali Ahmadinia for serving as valuable committee members to our project

Our friends and families for their support and encouragement throughout the process of our academic undertaking, especially during the duration of our project research, development, and thesis culmination

References

Internet of Things Image Credit

Image Credit