Global Information Assurance Certification Paper

Invaders of the internet connected home

GIAC (GCIH) Gold Certification

Author: Jay Yaneza, jay_yaneza@trendmicro.com
Advisor: Hamed Khiabani, Ph.D.
Accepted: September 23rd, 2020

Abstract

With this rising need of network connectivity to the average home, the role called the "administrator-of-things" exists in which there would be responsible individual/s worrying about some aspects of the home networked environment: uptime, updates, connectivity, troubleshooting … and security. In the not-so-distant-past, these aspects were just a worry of an enterprise systems/network administrator where the stakes were uptime and business continuity, and now these tasks have silently creeped in the household within the last few years. This paper would look into network-based threats that would attempt to break in and, in the process, explore the dangers that may befall the budding "administrator-of-things".

1. Introduction

A recent interconnected device survey assessed that the average household has 11 connected devices, and that twenty-eight percent of consumers would have a variety of smart home devices. This report also mentioned that home owners who had multiple smart home devices tend to spend more on internet bandwidth (Build it and they will embrace it | Deloitte, 2019) as all of these smart home devices may contend for internet bandwidth. This steady trend in saturating the average home with internet connected things was an expected effect of the internet of things (IoT) or, right now, the internet of everything (IoE) – equivocally leading to the fact that every piece of device that can be connected to the internet will be connected to the internet.

With this, the average home unintentionally needs "administrator-of-things", a mixed role of a handyman and a multi-user IT Administrator, whose responsibility would be to worry about some aspects of the home networked environment (TrendLabs Security Intelligence Blog, 2014). For example, a slight internet outage for an internet connected home would be immediately felt by various aspects of the household – ranging from the loss of control for temperature (thermostat), visibility (camera), lighting automation, and screens that rely on streaming content. Aside from worrying about connectivity and uptime, this role would need to worry about keeping these devices updated – if not for newer features that may be offered by the vendor, then probably to ensure that patches are applied to the device for increased security. Sounds familiar? Indeed, all of these factors play very much in the day to day operations of a business that requires internet connectivity to provide services.

At the time of writing, there is also a wider acceptance of companies for working from home. With this, the boundaries of a secure working environment is blurred: how can an organization ensure that remote workers are not opening up doors for remote attacks when a home network is beyond the mandate and scope of the enterprise IT organization?

It should be noted that this paper also includes an initial effort to profile threats to an internet connected home. With the initial research was conducted around July 2016, and would differentiate what observed activities 4 years after.

Jay Yaneza, jay_yaneza@trendmicro.com

1.1 TCP/IP based devices – hardwired or wireless

A research into classifications of devices within a Smart Home ("Classification of functions in smart home," 2012), there are generally four classifications of devices within a Smart Home:

- Electro – this includes touch panels, control appliances, kitchen appliances, garage openers, or irrigation (sprinkler) systems. These aspects of a home that were usually utilized through manual operations that has been introduced to the internet-connected world.
- Audio/Video – includes home theatre, music, and games. Most commonly experienced through Smart TVs, smart speakers, gaming consoles and streaming sticks.
- Security – this would generally include systems that provide safety, more commonly found in homes. Web-enabled IP cameras, baby monitors, motion detections and alarms are part of this group.
- Environment, energy and health – almost all devices that comfortable living conditions fall in this group: heating ventilation and air conditioning (HVAC) systems, shutters, lighting, or even internet connected weighing scales and exercise trackers.

Aside from these devices that may be permanent fixtures within a Smart Home, let us not forget that there are other "productivity-related" devices that are also connected, which includes computers, laptops, tablets, printers and the like.

1.2 Smart Home Hubs

Having a few internet connected (a.k.a., "smart") device would mostly work with various apps cluttered in your personal device (i.e., phone, tablet). However, as these devices grow in number, having a Smart Home (Automation) Hub. In general, a Smart Home Automation Hub "*serves as the nerve center of your home automation system and ties all of your devices together*" ("What is a smart home hub (And do you need one)?" 2014). Depending on the vendor of your Smart Home Hub, it can support multiple protocols including:

- Bluetooth

- Wi-Fi (mostly through web-based APIs)
- Z-Wave radio (908.4 MHz)
- ZigBee radio (2.4 GHz)

There are also support for vendor-specific protocols such as Apple HomeKit, Lutron Clear Connect (lighting), and Kidde (smoke and CO alarm) wireless protocols. Most of them also integrate with "smart assistants" like Amazon Alexa and Google Assistant, and often integration with *If This then That* (IFTTT) web services.

2. Normal outbound network traffic flow within the observed home network

For most configurations, home networks are largely controlled by the home network's firewall/router devices and such devices are designed to 1) allow all outbound network access and 2) deny inbound connection connections. There are, however, certain conditions wherein a home network's firewall/router device may be configured to allow incoming traffic:

a) Universal Plug and Play (UPnP) or Network Address Translation Port Mapping Protocol (NAT-PMP)

The term UPnP may be a little bit more popular than NAT-PMP as it is a ubiquitous term utilized by a lot of devices, while NAT-PMP is commonly found in Apple devices and programs. Both of these functionality though function the say way: if the home router/firewall device supports it, these devices/programs that utilize either UPnP or NAT-PMP can dynamically add port forwards and firewall entries. Most common of these devices would be a gaming console, and programs such as BitTorrent would utilize the same as well.

b) Manually configured by the home owner

In some configurations that UPnP doesn't natively work on the home network, a home owner may configure the firewall functionality to allow certain ports inbound to a destination device. There are several configurations of this: either setting the device up in the DMZ location of a home network, 1-to-1 mapping for port forwarding or even port triggering features. Such terminologies may be straightforward for a firewall

administrator for a business setting, but not so much for the regular home user. It may, however, come into discussion if one of the members of the household would be playing online games that require "hosting" a game on a Microsoft Windows PC located within the home network. Another possible instance of configuring such inbound access would be if the home owner would like to take advantage of certain functionalities of the home router, such as "*offering a locally attached USB storage to be accessible anywhere*".

The next few sections would discuss observations on a home network with mostly outbound connectivity, with only one section having a port-forwarding rule found in the second example for 2.5 Productivity for a particular Microsoft Windows game. Both UPnP and NAT-PMP is disabled within the observed network environment, and the observation was performed for the entire July 2020.

2.1 Electro

A Wi-Fi enabled sprinkler was observed during this time, and it turns out that the traffic is rather simplistic:

nf_dst_address_country_code	nf_proto_name	nf_dst_port	count()	avg(nf_bytes)
US	TCP	31314	1	833

Figure 1: Wi-Fi enabled Sprinkler traffic profile

The vendor also listed these ports on their support site, with the following information:

- TCP/31314 – Used for earlier generation of the device, and TCP/8883 was used for future models.
- TCP/80 – Used for firmware updates
- UDP/53 and UDP/123 - for Domain Name Server (DNS) lookup queries and time synchronization via Network Time Protocol (NTP)

During the time of observation, the TCP/31314 traffic was consistently communicating with a well-known web hosting provider (Amazon AWS).

2.2 Audio / Video

Analysis of traffic coming from two video devices (a popular streaming stick and a Smart TV) share the following characteristics:

- All of the devices tested were physically located within the United States, so it's expected that the traffic mostly were reaching out to destinations that are within the United States.
- Heavy utilization of ports TCP/80 and TCP/443 for both devices, which is the primary medium of delivering streaming content.
- There was also significant use of UDP/53 and UDP/123, for Domain Name Server (DNS) lookup queries and time synchronization via Network Time Protocol (NTP).
- Intermittent and low utilization of UDP/55623, UDP/55625, UDP/58899, UDP/65432. Very little is known about this network access, but was observed in both devices.
- Not surprisingly, these two devices that are used to consume streaming content do not communicate directly at all with devices within the same Wi-Fi network.

nf_dst_address_country_code	nf_proto_name	nf_dst_port	count()	avg(nf_bytes)
US	TCP	443	38945	37302.18153806651
		80	3789	6487.709685932964
		53	420	216.123809523809 5
		2350	99	3168.6464646464647
	UDP	53	1334	125.36281859070465
		55623	1	696
		55625	1	348
		58899	1	1392
		65432	1	1392
IE	TCP	443	40	1791.575
CA	TCP	443	27	2439.8518518518517
		80	1	1343
NL	TCP	443	8	1899.5
GB	TCP	443	3	1604.6666666666667
N/A	TCP	443	2	3298.5

nf_dst_address_country_code	nf_proto_name	nf_dst_port	count()	avg(nf_bytes)
US	UDP	443	45750	3069.073442622951
		53	4509	840.1182080283877
		123	2562	76
		55623	44	543
		55625	4	543
		65432	4	543
		58899	1	543
	TCP	443	20658	33485.13186174847
		80	1295	43503.95521235521
		5228	36	66698.77777777778
	ICMP	2048	396	43196.36363636364
		771	349	826.2750716332379
IE	TCP	443	13	1532.1538461538462
CA	TCP	443	8	2720.25
GB	TCP	443	3	2330
N/A	TCP	443	2	1643.5
		5228	1	48632

Figure 2: Streaming stick (left), Smart TV (right)

After these similarities, there are some port ranges that seem to be very specific to each device:

- Aside from the TCP traffic for both TCP/80 and TCP/443, UDP/80 and UDP/443 was also observed for the Smart TV.
- The Smart TV also had ICMP requests (2048/Echo Request and 771/Port Unreachable), which was not present in the streaming stick.

Jay Yaneza, jay_yaneza@trendmicro.com

- 4 digit destination ports for both the streaming stick and the Smart TV:
    - TCP/2350 – accordingly used specifically by the streaming stick, and is consistently communicating with a well-known web hosting provider (Amazon AWS).
    - TCP/5228 – used by the tested Smart TV, and is consistently communicating with a well-known web hosting provider (Google Cloud)

To make another comparison, traffic profile of a Smart Speaker was also observed with the following findings:

nf_dst_address_country_code	nf_proto_name	nf_dst_port	count()	avg(nf_bytes)
US	UDP	53	152634	69.71869308279938
		123	2573	76
	TCP	443	21843	15359.024172503778
		80	1363	26886.481291269258
		5228	81	63111.432098765436
	ICMP	2048	663	7400.868778280543
		771	5	124.4
N/A	TCP	5228	2	140050.5

Figure 3: Smart Speaker traffic profile

The characteristics of this Smart Speaker is almost the same as the two video devices (a popular streaming stick and a Smart TV):

- TCP traffic for both TCP/80 and TCP/443 was heavily utilized
- TCP/5228 is consistently communicating with a well-known web hosting provider (Google Cloud) hosted within the United States.
- There was also significant use of UDP/53 and UDP/123, for Domain Name Server (DNS) lookup queries and time synchronization via Network Time Protocol (NTP).
- The Smart Speaker also had ICMP requests (2048/Echo Request and 771/Port Unreachable), towards a well-known web hosting provider (Google Cloud) hosted within the United States.

It should be noted that the devices did not use any local streaming traffic (e.g., DLNA), both devices were utilize personalized devices (i.e., phone and tablet) to stream content to the

device, and the traffic characterized above does not include traffic analysis similar to multicast DNS (mDNS) implemented by software packages like Apple Bonjour or Avahi.

2.3 Security

Home security panels that aspects of the dwelling (e.g., doors, windows, gates, heat, smoke, freeze) during certain states (e.g., armed, disarmed, stay or away) usually communicate with sensors that could either be a combination of hardwired or wireless methods. These wireless methods aren't necessarily Wi-Fi, and operate in a specific range of signals (e.g., 345 MHz, 900 MHz), depending on the vendor of such device. Further, while Wi-Fi-only home security control panels exists, most of these home security panels would have a battery backup and communicate through cellular radio modules. That being said, another device that was put into consideration was a home security control panel, through its "*IP communicator*" add-on device, which is usually offered as an option for "backup communications" to the monitoring service's Central Station in case network coverage of cellular services are poor.

nf_dst_address_country_code	nf_proto_name	nf_dst_port	count()	avg(nf_bytes)
US	UDP	1121	378	10059.351851851852

Figure 4: Home Security IP communicator traffic profile

Traffic analysis of such device reveals that its communication protocol was only for UDP/1121 that was for the monitoring service's Central Station. No other ports or hosts were observed.

Next, a home security suite that provided video recording (including Wi-Fi-enabled doorbells) were observed during the same time period. While there were numerous ports observed, some of which not documented by the vendor, we will go through the top common ports observed:

nf_dst_address_country_code	nf_proto_name	nf_dst_port	count()	avg(nf_bytes)
US	TCP	443	38745	71371.23510130339
		15064	590	4439.794915254237
		5201	72	6482187.888888889
		9999	63	475743.9365079365
		9998	53	333593.2641509434
		6190	3	4858716.666666667
		5301	2	7350210.5
		5334	2	6838736
		5464	2	6985745.5
		5506	2	7211486.5
		5598	2	7272969.5
		5674	2	6916735.5
		5743	2	7388486.5
		5760	2	7255038.5
		5841	2	7170236

Figure 5: Wi-Fi enabled video/doorbell traffic profile (TCP ports)

The top TCP ports being in used were the following:

- TCP/443 – HTTPS, the main communications protocol to the cloud-based service, which enables this home security suite to provide its service.
- TCP/15064 – Session Initiated Protocol (SIP), a signaling protocol used real-time sessions with a devices that provide voice, video or messaging.
- TCP/5201 – observed in actual use and several end-user reports, but no public documentation (from the vendor) on its function. Confirmed that the communication goes to a well-known web hosting provider (Amazon AWS).
- TCP/9999 and TCP/9998 – device-specific ports that is used to maintain communication path to the mobile device (which has the home security device app).

On the other hand, while UDP ports have very small amount of traffic, it does show that this home security suite utilizes UDP ports only for the mostly for the important services:

- UDP/123 – time synchronization via Network Time Protocol (NTP)
- UDP/53 – Domain Name Server (DNS) lookup queries

Jay Yaneza, jay_yaneza@trendmicro.com

- UDP/5001 – observed in actual use and several end-user reports, but no public documentation (from the vendor) on its function. Confirmed that the communication goes to a well-known web hosting provider (Amazon AWS).

	UDP	123	3176	121.9206549118388
		53	2505	220.18562874251498
		5001	300	3804479.08
		6238	2	1919410
		17778	2	615200
		20584	2	19214910
		34254	2	17104654
		36956	2	18366593
		39620	2	10164361
		40656	2	19381003.5
		43956	2	605600
		44468	2	7827638
		57328	2	18844279.5
		63052	2	9947567
		5254	1	2557970

Figure 6: Wi-Fi enabled video/doorbell traffic profile (UDP ports)

Finally, there are other observations for this home security suite, as observed below:

- The home security suite had ICMP requests (2048/Echo Request and 771/Port Unreachable), towards a well-known web hosting provider (Amazon AWS) hosted within the United States.
- The other non-US based traffic, it was seen that it was mostly for UDP/123 time synchronization via Network Time Protocol (NTP)

	ICMP	2048	512	11031.6796875
		771	1	1152
DE	UDP	123	49	145.79591836734693
GB	UDP	123	31	144.6451612903226
FR	UDP	123	25	142.88
NL	UDP	123	19	140
CH	UDP	123	16	152
UA	UDP	123	12	133
CA	UDP	123	11	145.0909090909091
HU	UDP	123	11	152
RU	UDP	123	11	131.27272727272728
CZ	UDP	123	9	143.55555555555554
SE	UDP	123	9	135.11111111111111
DK	UDP	123	7	141.14285714285714
PL	UDP	123	6	139.33333333333334
AU	UDP	123	4	133

Figure 7: Wi-Fi enabled video/doorbell traffic profile (UDP ports)

2.4 Environment, energy and health

Unfortunately, no Wi-Fi enabled device was put in observation during this time that can be included in this section. The employed devices were utilizing other wireless protocols (Z-Wave) that would be covered in section 2.6 Smart Hub.

2.5 Productivity

For the observed productivity devices, three devices has been put into observation: 1) a Wi-Fi enabled scanner/printer, 2) a Microsoft Windows 10 PC that was primarily used for personal use (e.g., gaming) and 3) a Microsoft Windows 10 PC that was used for remotely working from home

First, the Wi-Fi enabled scanner/printer has a rather simplistic network traffic profile as seen below:

nf_dst_address_country_code	nf_proto_name	nf_dst_port	count()	avg(nf_bytes)
US	TCP	443	12	4300.583333333333
		5222	2	3760

Figure 8: Wi-Fi enabled printer/scanner traffic profile (TCP ports only)

- Traffic directed at TCP/443 was seen for fetching web-based (cloud) print services (e.g., Google Cloud Print).
- TCP/5222 was observed communicating to two well-known web hosting provider (Google and Akamai).

All other network traffic was local to the environment, namely traffic between TCP/9100 – TCP/9102, TCP/443, and TCP/631. It should also be noted that IGMP, SMB and NetBIOS traffic was observed when printing as well.

Second, the Microsoft Windows 10 PC that was primarily used for personal use can readily be observed through the number of non-standard ports that have been observed:

nf_proto_name	nf_dst_port	count()	avg(nf_bytes)
TCP	443	173240	14525.290521819441
	80	29703	22239.056761943237
	5223	172	48673.24418604651
	2099	152	43786.41447368421
	5228	93	14793.075268817205
	27020	54	59202.166666666664
	27021	40	20671.075
	27035	27	50697.444444444445
	6667	21	67644.09523809524
	27036	21	22587.333333333332
	25565	20	9835541.95
	27030	19	3309.1052631578946
	27032	19	9453
	27028	18	38149.11111111111
	27029	18	9126.111111111111

Figure 9: Microsoft Windows 10 PC (for personal use) traffic profile, TCP ports only

- Traffic directed at TCP/443 was seen for normal internet browsing
- TCP/80 traffic was again seen for internet browsing
- TCP/5223 was observed for Apple Push Notification Service (APNS)
- TCP/6667 traffic, which is related to Internet Relay Chat (IRC)
- Other TCP ports (i.e., 25147, 27015-27030, 27036-27037) seen above are for game hosting.

UDP ports observed for this Microsoft Windows 10 host shows a traffic profile that is very much expected for a modern Windows 10 Operating System:

UDP	443	27698	85797.56249548704
	1900	11869	868.0774285955009
	3478	8468	206.26735947094946
	19302	8049	198.84010436079015
	5355	5951	98.11561082171063
	27015	5473	3048.971679152202
	8181	2160	64
	137	1284	1230.5327102803737
	8092	1093	395.6806953339433
	5353	946	1076.0084566596195
	27017	945	2612.361904761905
	27018	860	1882.2697674418605
	27019	832	5677.947115384615
	27025	736	189.91440217391303
	53	563	166.5595026642984

Figure 10: Microsoft Windows 10 PC (for personal use) traffic profile, UDP ports only

- Traffic directed at UDP/443 was because of the browser used (Google Chrome), which utilizes QUIC. This protocol (QUIC) is defined as "*a new transport which reduces latency compared to that of TCP*" ("QUIC, a multiplexed stream transport over UDP," n.d.), and is being implemented on an experimental basis on some web sites when utilizing a browser that supports it (e.g., Google Chrome).
- UDP/1900, which is associated to the Simple Service Discovery Protocol (SSDP), is related to the Universal Plug and Play (UPnP) service. Microsoft Windows 10 natively includes an SSDP Discovery service.
- UDP/5355 is similarly observed, which is related to Link-Local Multicast Name Resolution (LLMNR).
- UDP/5353 was observed as the host utilized multicast DNS (mDNS), as well as IGMP (not shown here). Microsoft Windows 10 supports mDNS/Zeroconf, as well as IGMP natively.

- UDP/3478 and UDP/19302 is associated to webRTC and VoIP Session Traversal Utilities for NAT (STUN) traffic, commonly used for various in-game (voice) communications.
- Other UDP ports (i.e., 27000-27031) seen above are for game hosting.
- Similar to other hosts, there is the existence of UDP/53 for Domain Name Server (DNS) lookup queries and UDP/123 time synchronization via Network Time Protocol (NTP).

Third, and last, for the Microsoft Windows 10 PC that was used for remotely working from home, the traffic profile is a little bit varied, as seen below:

nf_proto_name	nf_dst_port	count()	avg(nf_bytes)
TCP	443	202296	29458.336561276545
	80	18980	4239.010063224447
	389	721	258.55755894590845
	5228	151	6940.721854304636
	3389	83	1431368.8915662651
	22	48	79612.29166666667
	1022	23	79799.73913043478
	445	18	260
	3010	16	1867.5
	3478	15	721.2
	139	13	260
	902	2	509106
	33067	1	1697
	33207	1	553261
	35051	1	653875

Figure 11: Microsoft Windows 10 PC (for work from home use) traffic profile, TCP ports only

- Traffic directed at TCP/443 was a mix of normal internet browsing and the SSL VPN traffic to the VPN gateway of the corporate network.
- TCP/80 traffic was again a mix of normal internet browsing and internal resources within the corporate network.
- Noticeable in this network traffic profile that several ports that are normally found within the corporate network are observed: TCP/389 (LDAP), TCP/3389 (Microsoft RDP), TCP/22 (SSH), TCP/139 (NetBIOS) and TCP/445 (SMB).

For the UDP ports, the characteristics mimic that of a Microsoft Windows 10 host that was used for personal user, with just small irregularities observed:

UDP	1900	10279	855.4107403443915
	5355	5689	94.89470908771312
	443	3281	5081.26973483694
	137	2368	927.8665540540541
	138	1832	506.06004366812226
	5353	765	2483.0300653594772
	53	738	95.23983739837398
	3702	532	19081.40037593985
	8801	301	20147420.172757477
	123	283	76.26855123674912
	389	208	472.1394230769231
	5050	105	2925.2
	3289	57	183.73684210526315
	3478	43	6161.302325581395
	3481	2	98048576

Figure 12: Microsoft Windows 10 PC (for work from home use) traffic profile, UDP ports only

- The highest traffic observed here is UDP/1900, which is associated to the Simple Service Discovery Protocol (SSDP), is related to the Universal Plug and Play (UPnP) service. Microsoft Windows 10 natively includes an SSDP Discovery service.
- UDP/5355 is similarly observed, which is related to Link-Local Multicast Name Resolution (LLMNR).
- After analysis, it was found out that the utilization of UDP/443 was because of the browser used (Google Chrome), which utilizes QUIC. This protocol (QUIC) is defined as "*a new transport which reduces latency compared to that of TCP*" ("QUIC, a multiplexed stream transport over UDP," n.d.), and is being implemented on an experimental basis on some web sites when utilizing a browser that supports it (e.g., Google Chrome).
- UDP/5353 was observed as the host utilized multicast DNS (mDNS), as well as IGMP (not shown here). Microsoft Windows 10 supports mDNS/Zeroconf, as well as IGMP natively.
- Again, we see the existence of ports that are normally found within the corporate network: both UDP/137 and UDP/138 for NetBIOS and UDP/389 for LDAP.
- Similar to other hosts, there is the existence of UDP/53 for Domain Name Server (DNS) lookup queries and UDP/123 time synchronization via Network Time Protocol (NTP).

With this, the most traffic observed for productivity hosts were has the following similarities and differences:

Traffic Profile	Wi-Fi enabled printer/scanner	Microsoft Windows 10, for personal use	Microsoft Windows 10, for work from home
Web-related traffic (e.g., TCP/443, TCP/80)	✓	✓	✓
Printer-related traffic (e.g., TCP/910?, TCP/631)	✓	✓ (when printing)	✓ (when printing)
SMB/NetBIOS	✓	✓	✓
mDNS/IGMP	✓	✓	✓
DNS/NTP	×	✓	✓
QUIC (UDP/443)	×	✓	✓
SSDP (UDP/1900)	×	✓	✓
LLMNR (UDP/5355)	×	✓	✓
Enterprise-related traffic (LDAP, RDP, SSH)	×	×	✓
Other traffic (e.g., TCP/5223)	×	✓	×
IRC traffic (e.g., TCP/6667)	×	✓	×
webRTC / STUN (e.g., UDP/3478, UDP/19302)	×	✓	×
Game Hosting	×	✓	×

2.6 Smart Home Hub

The Smart Home Hub observed had rather a simple network traffic profile:

nf_dst_address_country_code	nf_proto_name	nf_dst_port	count()	avg(nf_bytes)
US	TCP	443	43147	3122.9052773078083
	UDP	9	137	46

Figure 13: Smart Home Hub traffic profile

During the time of observation, the TCP/443 traffic was consistently communicating with a well-known web hosting provider (Amazon AWS).

It should also be noted that, while the Smart Home Hub utilized in this paper was observed to communicate via HTTP (TCP/443) traffic, Z-Wave communication was observed as well, as seen below:

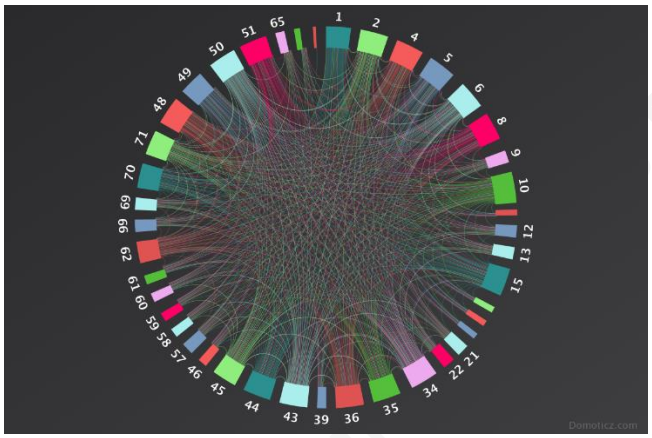

Figure 14: Smart Home Hub Z-Wave wireless mesh network

Z-Wave is based on a wireless mesh network topology and each device that is joined to a Z-Wave wireless network can either be battery operated or non-battery (continuous power) device. Usually, a non-battery operated Z-wave device acts as a signal repeater ("Z-wave smart home products are the #1 choice for smart homes," n.d.), and battery operated Z-wave devices disables the repeater functionality to preserve battery consumption. Each Z-Wave device (also called node) becomes linked together to form a low communication latency and interoperable network within a smart home.

Finally, there are several API-level integrations that were done on the Smart Home Hub in this paper:

- Smart Home Hub to the Smart Speaker
- Smart Home Hub to Home Security service
- Smart Home Hub to the Wi-Fi enabled sprinkler
- Smart Home Hub to the Wi-Fi enabled video/doorbell
- Smart Speaker to the Smart TV
- Smart Speaker to the Home Security Service

These integrations were not observed in the local traffic within the Smart Home, and is implicitly known that the integrations happened between the backend cloud services of each device.

Jay Yaneza, jay_yaneza@trendmicro.com

3. Observing an attack: initial methodology and findings

In July 2016, the author had performed an initial effort to profile internet-connected threats, choosing to analyze network-based threats by implementing honeypots. Honeypots are great since there are a lot of free and open-source options and gathers a great deal of data to analyze. The voluminous amount of data may be a challenge to analyze, but the approach that was chosen was to separate mass-scanning activities of the internet and differentiate that with traffic that is dedicated to an internet home. As such, it was decided to setup honeypot nodes that are hosted in a virtual private server (VPS) and a dedicated one at home. A separate observation was done on the traffic directed at the VPS servers, comparing it with the traffic directed specifically at our home network. Immediately, we did see some traffic that was specific to our monitored home network – and we decided to observe the traffic for the entire month of July 2016, and both the VPS server and the home are located within the United States.

Also, note that we classify one probe as a unique combination of: source IP address, source port and destination port, thereby one probe equates to one attempt. For example, one IP address that probed, say, the existence of both HTTP and SMTP ports (port 80 and 25, respectively) would be two entries in our list as one attempt would have a different source port and destination port. Here are the initial numbers:

- Out of the 33,197 probes to our VPS server, we counted only 686 probes to our home network of which only 337 probes (49.12%) were specific to our home network, while the other 349 probes were shared between our home network and our VPS server. This tells us that around 50% of the time, our monitored home network received unique traffic that is not seen at our VPS server. These 337 probes that are specific to our home network would be the object of interest.

- There were only 209 unique IP addresses doing all 337 probes to our home network - some hosts were scanning the home network multiple times and, at one point, across multiple protocols:

- Out of the 209 unique IP addresses, we counted 42 hosts that had repeated probes on the same destination port, but one host out of the 42 had probed our home network twice for different ports.

- The rest of the 167 hosts just probed one specific port, and moved on.

- The top two ports that was sought out were 1433 (Microsoft SQL Server) and 3389 (Microsoft Remote Desktop), with 27.59% and 27.29% respectively.

These initial results show that majority of the hosts that are external to our home network were seeking something very specific, with just a handful of ports (and, thereby, services) being of their interest. For now, we have looked into the connection attempts and captured data of the 209 unique hosts to our home network. After that, we created potential malicious profiles based on the attempts to introduce threats to our home network – particularly looking into the entry attempts, methods of entry and other suspicious activities. We came up with four possible profiles:

- Hosts that are engaged with other suspicious activities
- Homes that are spreading known worms
- Homes exploiting other homes through network exploits

4. Are nature of attacks the same 4 years after?

Similar observations were ran for July 2020, and here is a summary of the data:

Year	Protocol	Home	VPS	Overlap	Unique (Home)	Unique (VPS)
2016	**TCP**	686	33,197	349	337 (49.12%)	32,848 (98.94%)
2020	**TCP**	21,716	45,256	10,990	10,726 (49.39%)	34,266 (75.71%)
	UDP	2,373	2,712	1,038	1,335 (56.25%)	1,674 (61.72%)

Here are some observations:

- Out of the 10,726 unique hosts that scanned TCP ports, 1,106 hosts had scanned more than 1 port and the other 9,620 hosts only scanned 1 port.

Jay Yaneza, jay_yaneza@trendmicro.com

- Out of the 1,335 unique hosts that scanned UDP ports, 248 hosts had scanned more than 1 port and the other 1,087 hosts had scanned only 1 port.
- Cross-referencing the hosts that had scanned TCP ports and UDP ports, there are 81 unique hosts that had scanned both protocols.

Looking at the top 5 unique ports that were scanned that were clearly only affecting the home location, we have the following:

TCP	General Use
23	Telnet Server
1433	Microsoft SQL Server
5555	Several services claim this port (e.g., SoftEther VPN)
80	World Wide Web (HTTP) Server
22	Secure Shell (SSH) Server

UDP	General Use
1900	Simple Service Discovery Protocol (SSDP)
53	Domain Name Server (DNS)
5060	Session Initiation Protocol (SIP)
30366	(unknown)
56681	(unknown)

With the main interest in being able to determine TCP ports, and to make sense of the changes in the landscape, honeypots were again deployed to determine what are attacking these ports:

- TCP ports 23, 1433, 5555 and 22 are mostly being targeted with the MIRAI botnet ("Mirai widens distribution with new Trojan," 2017), which was first seen around August of 2016 ("MMD-0056-2016 - Linux/Mirai, how an old ELF malcode is recycled.," 2016). There are various version and iterations of MIRAI, but is mainly targeting Linux Servers and IoT devices running Linux-based firmware called Busybox, which is common in DVRs, CCTVs and IP-based cameras. Not surprisingly, the TCP port 5555 is for the Android Debug Port (ADB) that was reportedly left open in some Android-based phones ("Open ADB ports used to spread possible satori variant," 2018). This is also the same

entry point for various MIRAI variants, such as Satori, Okiru, Masuta, and Tsunami/Fbot to name a few. Several attempts were also attributed to a Perl-based backdoor ("Outlaw's Botnet spreads miner, Perl-based Backdoor," 2019), with the objective of cryptocurrency mining. Successful logins to either telnet (TCP 23) or ssh (TCP 22) also a sequence of commands that would download additional payload that would effectively make the afflicted device as part of the botnet, often communicating with other devices to perform malicious activities. Devices that may be compromised from would be communicating with other devices through TCP port 80, 8088, 7001, and higher ephemeral ports.

- On the other hand, TCP 80 attempts varied, such as :
    - Fingerprinting HTTP GET commands just looking for .env variable. There are various uses of the .env file (e.g., projects that involve Docker, Node.js, Python, etc.) but basically it describes working environment variables for a project.
    - Another HTTP get command that is very common is the attempt to access a subdirectory called /phpmyadmin/, a free and open source administration tool written in PHP.
    - Access to /hudson/ has been observed as well, which is usually related to the Hudson continuous integration (CI) that usually runs within the Apache Tomcat or Glassfish application server.
    - Access to the Solr admin URL (/solr/admin/info/system?wt=json) was performed as well, in attempt to determine if the Solr server was running. Solr is an open-source enterprise-search platform, which is part of the Apache Lucene project.
    - ThinkCMF framework vulnerability exploit attempts, with the associated ThinkPHP vulnerability scanning (related to CVE-2018-20062), also being abused by a MIRAI variant called Miori ("ThinkPHP remote code execution vulnerability used to deploy variety of malware (CVE-2018-20062)," 2019).
    - ZeroShell vulnerability exploit attempts, related to CVE-2009-0545, being abused by ECHOBOT, another MIRAI variant ("Mirai variant ECHOBOT resurfaces with 13 previously unexploited vulnerabilities," 2019).
    - Attempts to exploit Telerik UI for ASP.NET AJAX. There has been several CVEs related to this application, such as CVE-2017-9248, CVE-2017-11317, and CVE-2017-11357, with sightings of active exploitation ("Canadian centre for cyber

security," 2018), and the most recent one would be CVE-2019-18935 (Gross, 2019).

- JSON WEB Services Invoker (/api/jsonws/invoke) exploit attempts, related to CVE-2020-7961, which is fairly recent ("How to exploit Liferay CVE-2020-7961 : Quick journey to PoC | Synacktiv," 2020).
- Exploit attempts against Grandstream and DrayTek devices, which was recently discovered as CVE-2020-8515, related to a botnet called “Hoaxcalls” ("Grandstream and DrayTek devices exploited to power new Hoaxcalls DDoS Botnet," 2020).
- Netlink GPON Router 1.0.11 - Remote Code Execution (Shellord, 2020), with access to “boaform/admin/”. This is again being related to the aforementioned botnet called “Hoaxcalls” ("New Mirai variant expands, exploits CVE-2020-1017," 2020)

Clearly, home based attacks has changed 4 years after, with the current threat landscape being awash with various IoT-based threats.

5. Why apply Network Micro-segmentation when working from home?

Whether working from home is a norm that a company allows, or have just been recently allowed due to certain conditions, one of the perceived benefits of working from home is that it can allow workers to minimize distractions and increase the time they spend focused on a project. However, the IT security risks for such arrangements are well known, such as:

a) Physical security and the boundaries of work data vs personal data, where personal information may co-mingle with corporate data. This not only applies to data stored on a company owned and provisioned asset (e.g., laptop), but on USB disks or flash drives.
b) Network security. In a corporate environment, network devices are often scanned for, patched updated to protect against vulnerabilities. Suspicious network usage (e.g., unusual outbound network requests, network scanning) may also be recognized if traffic within a corporate environment should this be monitored. In a home network setting, a

compromise of a home based router, or any IOT device, which may be stepping stone to the corporate asset owned by the remote worker would not be visible, or even recognized, by an IT administrator.

c) Host security. Similar to network security, regular patching may be part of the regular monthly maintenance, with patches being pushed out through enterprise means of patch management. Alongside this, the deployment of host-based security software (antimalware software, host based intrusion prevention/detection systems, data loss prevention, etc.) would not extend to other personal devices within the home network.

On the other hand, micro-segmentation is the concept of creating very granular segments within an IT infrastructure, to which the objective is to effectively limit the size of the network's attack surface by ensuring unrelated network segments are "walled-off". It has been previously established that network micro-segmentation does provide additional security ("Does Network Micro-segmentation Provide Additional Security?" Jaworski, 2017), and that the basis of this security model is from the "Zero Trust Model" introduced by Forrester Research (Kindervag & Ferrara, 2013). So not to be confused by the two terms, it is important to bear in mind that micro-segmentation is an implementation of the Zero Trust Model. Most importantly, Zero Trust Model advocates that security professionals must eliminate the idea of a "trusted network", otherwise known as the internal network, and the "untrusted network", which is usually the external network. There are three fundamental concepts in the Zero Trust Model:

- Concept No. 1: Ensure that all resources are accessed securely regardless of location
- Concept No. 2: Adopt a least privilege strategy and strictly enforce access control
- Concept No. 3: Inspect and log all traffic

A working example of the Zero Trust Model includes the implementation of micro-segmentation, wherein the end-result of this is trying to protect hosts that reside within the same security zone. The usual approach would be to segment an entire network according to the functional subnet, VLAN or broadcast domain, after which only the necessary resources are exposed between the separations (east-west traffic) and further complemented with the use of host-based solutions such as a host intrusion/prevention system (HID/PS) to extend the implementation up to the most atomic component of a corporate network. These approaches have

been present in most enterprise networks through physical switches or routers and, in today's world of virtual switches and software define networks (SDNs), such implementation may be widely accepted within an enterprise network. The integration of host intrusion/prevention system (HID/PS) within antimalware security suites has also been quite common.

So how can this be implemented in a home network? Over the past few years, the author had tried multiple methods of implementing VLANs within a home network and, unless the home owner would introduce costly enterprise-grade hardware within a home network, found it overly complex for most end-users to implement using commodity hardware. However, two features stands out to be consistent in ensuring that a Wi-Fi connect host would be isolated within a home network:

- Utilization of the Guest Network, and
- Access Point (AP) Isolation

First, the Guest Network essentially shares bandwidth of a single internet connection within the home, and is commonly advertised to "limit of guest users connectivity to local resources". However, most implementations of this would also be inversely true as some implementations of the guest network also limit hosts on the home network from accessing those on the guest network.

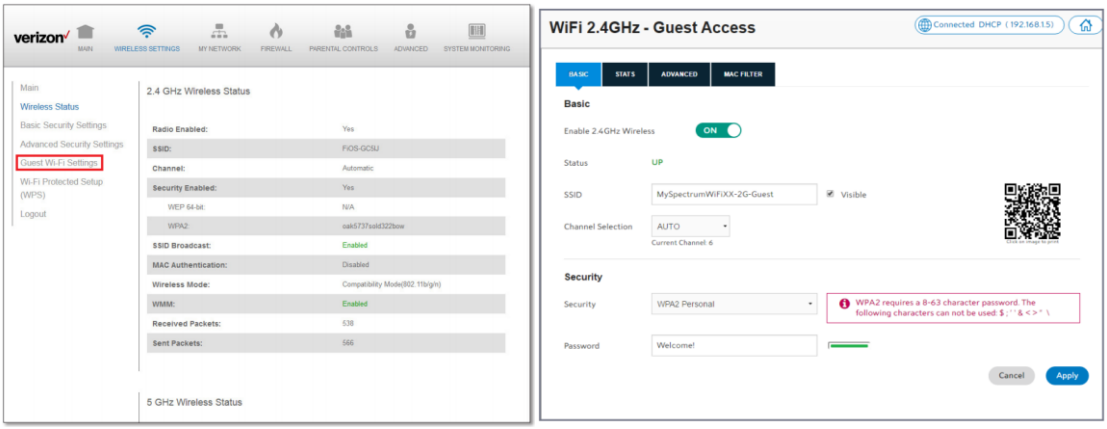

Figure 15: Guest Network configuration settings for some home-based wireless devices in North America

Jay Yaneza, jay_yaneza@trendmicro.com

Second, Access Point (AP) Isolation is another option that home users can also implement, and is usually hidden in under the advanced configuration of a wireless access point. The effect of this option would largely affect the home access point's wireless radio wherein all wireless devices connecting to wireless network name (SSID) would be unable to communicate amongst one another.

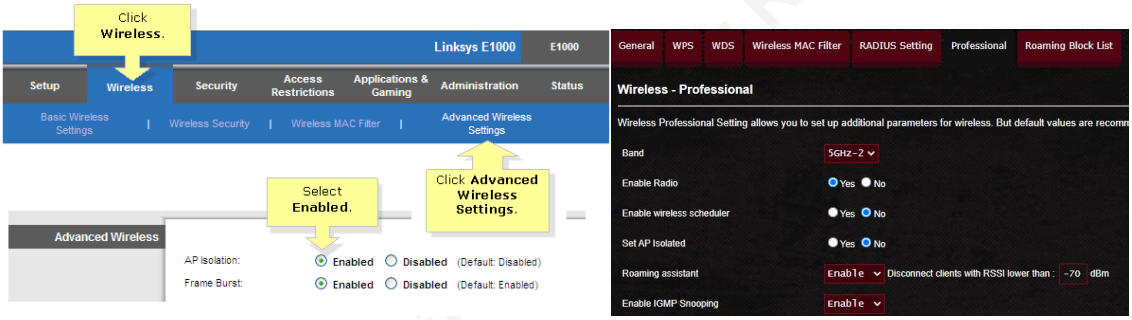

Figure 16: Access Point Isolation configuration settings for some home-based wireless sold within North America

In testing both features, it was found out that Access Point (AP) Isolation works more consistently than Guest Network implementations across different home based wireless devices vendor's interpretation and implementation of "Guest Network" still allows some communication between hosts. With majority of hosts observed relatively very low to inexistent intra-host communication within a home network, there may be an opportunity to set these hosts to communicate with a wireless AP that offers either of these two restrictions, with preference on the Access Point (AP) Isolation. This feature would work well in conjunction with host-based settings, such as network discoverability:

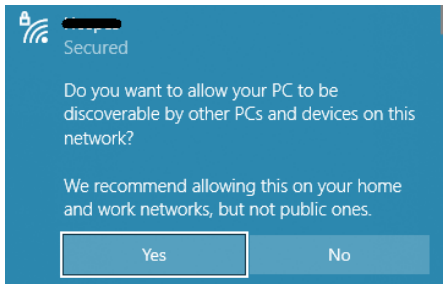

Figure 17: Network discoverability option in Microsoft Windows 10

Jay Yaneza, jay_yaneza@trendmicro.com

Commonly, such prompts will let the end-user know that the recommendation is to allow the endpoint to be discoverable on the home network. The common practice is to select “Yes” for home or work networks, and “No” if you are connecting to an unknown and untrusted location such as a coffee-shop or an internet cafe. However, there is practically no reason to keep the corporate laptop accessing company resources to remain visible on a home network, so hiding the host’s visibility from the rest of the home network may be appropriate.

6. Recommendations

The management of home networks definitely looks like enterprise networks and the recent wide acceptance of remote work, or working from home, makes it clear that threats that may affect the home would open the possibility of compromising the enterprise network. At this point, here are a few challenges that we think the "administrator-of-things" has to heavily consider:

- Make sure all your internal devices are up-to-date to cover known issues and vulnerabilities. In most cases, the prolonged use of old technology opens your family members to the possibility of being either the victim or the attacker, or maybe both. Ensure that the device that you’re picking up has a stable history of providing patches for their software and ensure that the device is still within maintenance of the vendor. Once a device is out of date, heavily consider replacing it *even though it still works*. Patch management is critical in enterprise network, and a similar approach in keeping software up-to-date applies, for all the devices, in your home network as well.

- Look into possible security options of your devices, and take advantage of them when possible. The main purpose of a cable modem is to connect your home to your cable company/ISP and bring wired/wireless connectivity options. It may take a while for ISP-provided home routers to have better security options, and so it may cost a little extra. There is very little (if any) offering in that device for any type of security - mostly a just basic firewall and access control, maybe parental options for time restraints and keyword filtering. In fact, most documentation would just mention maintaining your endpoint like keeping your patches and anti-virus up to date - and scant information about "security",

mostly talking about the wireless security options. Not that these fundamentals are not important, but it does not help the "administrator-of-things" who may need to secure multiple devices. Consider a home security software that encompasses all your devices, one that offers visibility for all your home network devices

- Think before opening ports at your home router / gateway, as you might accidently share more than you'd want. Most home router configurations would offer a DMZ host configuration, where a single device on the network would be fully exposed to the internet for special purposes like internet gaming.

- Consider and implement network segmentation. A lot of your devices would like to hop on to your network. If it is absolutely necessary for that device to connect through your wireless network, it would be ideal if you can identify it, and separate it from the rest of your important assets – like your corporate laptop/device. If not for the IOT devices, do it for your corporate-issued laptop or work device. Having separate (and isolated) network devices would go a long way of ensuring that vulnerabilities and threats affecting a compromised device would not cross over from the home network to the corporate-issued laptop, and vice versa.

- Similar to the enterprise, make sure that you have enabled two factor authentication (2FA) for your online accounts for the vendor-provided portals, especially those that would allow access to APIs, as they allow direct access to data that is being gathered, collected and uploaded.

7. Conclusion

Without a doubt, the role called the "administrator-of-things" is a necessity for today's smart home. Long gone are the simple days wherein an internet connection to the home is solely used for a student trying to submit homework, a professional completing some last minute research for a big business presentation the next day, a child playing online games or streaming internet content to watch videos or catch-up with social media. Today's internet connected home consists of a combination of devices that gives access, control and visibility on multiple aspects of a

Jay Yaneza, jay_yaneza@trendmicro.com

regular household, with the internet of everything (IoE) changing how we interact with the smart home.

An enterprise IT organization may have different staff to manage firewalls, network traffic, patch management and troubleshooting but today's home would most likely be run by limited staff - the home owner. While such job function would be satisfying for hobbyists or technology-oriented individuals, the responsibility of configuration, management, maintaining connectivity, patching and troubleshooting of a smart home may be daunting for some home owners. Every day devices that would've been operated simply by a flip of a switch have added complexity of "getting online" as these devices now exist within a connected ecosystem of home network and, in effect, the internet. However, if we were to summarize the top three priorities of the "administrator-of-things", it would boil down to three functions:

- Secure configuration and management of these devices. The recommendation of regular patching and updating of the device may be difficult to keep up for the most part, so the least that can be done would be changing the default passwords of these devices. Besides, the vendor may be slow to respond to a vulnerability, or choose not to update the device at all.
- Implementing network segregation across all devices. Most of the traffic that is observed for most home networks would generally be outbound to the internet, rarely is it seen that devices "talk" to each other. If at all, devices that regularly communicate for some administrative means should be grouped and made to communicate to each other only.
- For devices that synchronizes any information in the cloud, make sure to secure it. From small businesses to large enterprises, nothing is worse than a data breach. The same would apply to the smart home: a vendor-provided portal that is poorly secured may allow unauthorized users to acquire personal information, or even spy on you or your family members.

A differential comparison between 2016 and 2020 showed that there is approximately 49% unique traffic directed at an internet connected home, but the scale of it has been massive: a contrast of TCP attacks between 4 years (2016: 337 vs 2020: 10,726) had increased over 3,182.78%. The nature of the threats that are a cause of these attacks, the

invaders of the internet connected home, have also shifted between opportunistic threats to target the internet of things (IoT) that have gained popularity with home owners in the recent years.

Most of these threats directly compromise the home router, the main and most important device within a home network. A smart home, and other possible vulnerable devices hosted therein, may therefore be enslaved in a larger pool of infected devices. But as damaging as it may sound for the regular home owner, the effects on the remote worker should also be put into consideration. Going beyond malicious software, malicious threat actors may have their cross-hairs on the remote worker as an entry point to the larger organization. Thus, companies who allow remote work should also put guidelines for their employees surrounding how to secure home networks if and when they allow remote work, extending beyond simple recommendations of "using the device for office work, and go through the corporate VPN". While the corporate laptop or the work device may only be what the larger enterprise can control, that device is now a member of another network that has recently become complex. Fortunately, the "administrator-of-things" may help in this endeavor.

Jay Yaneza, jay_yaneza@trendmicro.com

References

Canadian centre for cyber security. (2018, August 15). Canadian Centre for Cyber Security. https://cyber.gc.ca/en/alerts/active-exploitation-telerik-ui-aspnet-ajax

Connectivity and Mobile Trends Survey | Build it and they will embrace it | Deloitte (2019) Retrieved from https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html

Classification of functions in smart home. (2012, April 1). ResearchGate. https://www.researchgate.net/publication/275156028_Classification_of_Functions_in_Smart_Home

Does network micro-segmentation provide additional security? (2017, September 15). Information Security Training | SANS Cyber Security Certifications & Research. https://www.sans.org/reading-room/whitepapers/networksecurity/network-micro-segmentation-provide-additional-security-38030

Grandstream and DrayTek devices exploited to power new Hoaxcalls DDoS Botnet. (2020, April 6). Unit42. https://unit42.paloaltonetworks.com/new-hoaxcalls-ddos-botnet/

Gross, C. (2019, December 12). CVE-2019-18935: Remote code execution via insecure Deserialization in Telerik UI. Bishop Fox Labs. https://labs.bishopfox.com/tech-blog/cve-2019-18935-remote-code-execution-in-telerik-ui

How to exploit Liferay CVE-2020-7961 : Quick journey to PoC | Synacktiv. (2020, March 30). Pentest, Reverse, Développement l Synacktiv. https://www.synacktiv.com/en/publications/how-to-exploit-liferay-cve-2020-7961-quick-journey-to-poc.html

Kindervag, J., & Ferrara, E. (2013, April 8). Developing a Framework to Improve Critical Infrastructure Cybersecurity. Retrieved April 30, 2017, from NIST: http://csrc.nist.gov/cyberframework/rfi_comments/040813_forrester_research.pdf

Mirai widens distribution with new Trojan. (2017, February 13). Trend Micro. https://www.trendmicro.com/en_us/research/17/b/mirai-widens-distribution-new-trojan-scans-ports.html

Jay Yaneza, jay_yaneza@trendmicro.com

Mirai variant ECHOBOT resurfaces with 13 previously unexploited vulnerabilities. (2019, December 17). Unit42. https://unit42.paloaltonetworks.com/mirai-variant-echobot-resurfaces-with-13-previously-unexploited-vulnerabilities/

MMD-0056-2016 - Linux/Mirai, how an old ELF malcode is recycled.. (2016, September 1). Malware Must Die!. https://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html

New Mirai variant expands, exploits CVE-2020-1017. (n.d.). Trend Micro. https://www.trendmicro.com/en_us/research/20/g/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173.html

Open ADB ports used to spread possible satori variant. (2018, July 23). Trend Micro. https://www.trendmicro.com/en_us/research/18/g/open-adb-ports-being-exploited-to-spread-possible-satori-variant-in-android-devices.html

Outlaw's Botnet spreads miner, Perl-based Backdoor. (2019, June 13). Trend Micro. https://www.trendmicro.com/en_us/research/19/f/outlaw-hacking-groups-botnet-observed-spreading-miner-perl-based-backdoor.html

QUIC, a multiplexed stream transport over UDP. (n.d.). The Chromium Projects. https://www.chromium.org/quic

Shellord. (2020, March 18). Offensive security's exploit database archive. Exploit Database. https://www.exploit-db.com/exploits/48225

ThinkPHP remote code execution vulnerability used to deploy variety of malware (CVE-2018-20062). (2019, February 26). Tenable®. https://www.tenable.com/blog/thinkphp-remote-code-execution-vulnerability-used-to-deploy-variety-of-malware-cve-2018-20062

TrendLabs Security Intelligence Blog | The Administrator of Things (AoT) – A Side Effect of Smartification - TrendLabs Security Intelligence Blog. (2014, August). Retrieved from https://blog.trendmicro.com/trendlabs-security-intelligence/the-administrator-of-things-aot-a-side-effect-of-smartification/

What is a smart home hub (And do you need one)? (2014, September 17). PCMAG. https://www.pcmag.com/news/what-is-a-smart-home-hub-and-do-you-need-one

Z-wave smart home products are the #1 choice for smart homes. (n.d.). Z-Wave. https://www.z-wave.com/learn

Jay Yaneza, jay_yaneza@trendmicro.com