Disposable botnet infrastructure: examining the anatomy of IoT botnets

Under the skin of the Bashlite, Mirai, Hajime and Tsunami botnets

YING TIE, Yokohama National University
RYOICHI ISAWA, National Institute of Information and Communications Technology
TATSUYA TAMAI, Yokohama National University
CARLOS GAÑÁN, Delft University of Technology
MICHEL VAN EETEN, Delft University of Technology
KATSUSNARI YOSHIOKA, Yokohama National University
TSUTOMU MATSUMOTO, Yokohama National University

The rise of the Internet-of-Things (IoT) has also brought us new threats. It has enabled attackers to compromise a sheer number of Internet-connected devices with malware. That IoT malware has been recognized as one of the significant security threats on the Internet. We used IoT honeypot to collect IoT malware and obtain infrastructure information such as C&C servers and download servers. We focused on four major IoT malware families: Bashlite, Mirai, Tsunami, and Hajime and found out that malware download servers of Bashlite and Tsunami family are much more active than the others with high update frequency of their binar

Additional Key Words and Phrases: Internet of things, malware, botnets

ACM Reference Format:
Ying Tie, Ryoichi Isawa, Tatsuya Tamai, Carlos Gañán, Michel van Eeten, Katsusnari Yoshioka, and Tsutomu Matsumoto. 2023. Disposable botnet infrastructure: examining the anatomy of IoT botnets: Under the skin of the Bashlite, Mirai, Hajime and Tsunami botnets. *Digit. Threat. Res. Pract.* 1, 1 (July 2023), 15 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The rise of the Internet-of-Things (IoT) is causing dramatic changes in the Internet ecosystem. Billions of heterogeneous devices are being connected, a trend that is accelerating by the many sectors that are deploying Internet-connected devices to maintain, control and monitor all kinds of processes. Online sensors such as smart meters have been rolled out, automated homes can be controlled remotely, entire manufacturing plants are monitored over the Internet, traffic management is enhanced with road sensors and smart traffic lights, homes are increasingly populated with devices with IP connectivity, like fridges, washing machines, and security cameras –the list goes on and on. However, the IoT security measures have not kept up with these developments.

Authors' addresses: Ying TieYokohama National University; Ryoichi IsawaNational Institute of Information and Communications Technology; Tatsuya TamaiYokohama National University; Carlos GañánDelft University of Technology; Michel van EetenDelft University of Technology; Katsusnari YoshiokaYokohama National University; Tsutomu MatsumotoYokohama National University.

2576-5337/2023/7-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

IoT malware, such as Bashlite [Spring et al. 2016], Mirai [Antonakakis et al. 2017] and its variants [Trend Micro 2017], which targets IoT devices, is raging on the Internet.

They were able to quickly compromise millions of devices by guessing weak login credentials of Telnet- or SSH-enabled services. Denial-of-service (DoS) attacks launched from the compromised IoT devices were of an unprecedented scale. "Krebs on Security" [Krebs 2016] and Dyn [Hilton 2016] were under DDoS attack by IoT malware in 2016. Also, in 2017, Satori, a Mirai variant, exploited the `CVE-2014=8361` vulnerability infecting millions IoT devices that were then misused to launch DDoS attacks [360 netlab 2018]. Unfortunately, these were not isolated cases and current trends seem to indicate that IoT botnets will continue emerging and growing.

While previous research reveal xxx and xxx of IoT botnets, there is little study on the characteristics of their infrastructures such as C2 and DL servers. Understanding botnet infrastructure is essential when taking practical actions such as take-down.

Therefore, in this paper we analyze botnet infrastructure and their operation of binary distribution. Namely, we analyzed xxx malware binaries captured by honeypot [cite iotpot] from x days of operation, executed them in IoT malware sandboxes, extracted xxxx and XXXX IP addresses of C2 and DL servers, respectively and analyzed their relationships. Following is our main findings:

- Some IoT botnets are very dynamic, frequently updating binaries and changing their corresponding C2 and DL servers. In other words, many C2, DL servers, and binaries are short-lived. They only appear for a few days and are never observed in our measurement after that.
- Each binary does not necessarily have robust connectivity to its infrastructure, containing only one or few C2/DL addresses as if they are treated as "disposable". This may be related to the fact that IoT malware infection is indeed not persistant (i.e. rebooting infected devices would erase the malware process).
- The same infrastructures use multiple botnet families, like Bashlite and Mirai, probably due to the fact that the source codes of these bot are leaked and shared among the malware authors.
- C2/DL are mostly located in hosting and cloud services, which are quite common in traditional botnets. Only Hajime, which is a P2P botnet, has widely distributed infra as they are indeed composed of infected devices over the world.

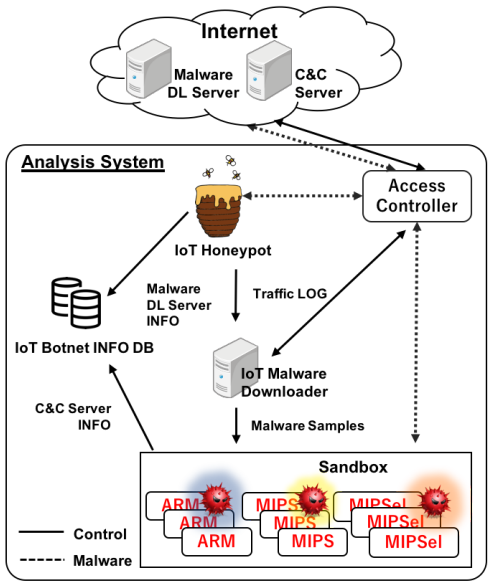
2 RELATED WORK

Since 2005, security researchers have been working on understanding, detecting and disrupting botnets [Cooke et al. 2005]. Rossow et al. [Rossow et al. 2012] did a long-time study of windows botnets infrastructure. They observed many servers as botnet infrastructure had been actively operating for more than a year. And, Zand et al. proposed a detection method based on identifying C&C(Command and Control) communication signatures. After the emergence of IoT devices, security researchers have shed light on IoT security flaws [Angrishi 2017; Schneier 2014]. In [Antonakakis et al. 2017], authors have done a comprehensive study that has analyzed the MiraiâĂŹs emergence and evolution of the Mirai botnet ecosystem. Kishore Angrishi [Angrishi 2017] also pointed that most IoT botnets launch DDoS attacks, and provide remedies and recommendations to mitigate IoT related cyber risks. Besides, several honeypots aim to collect malware that spread via IoT-related protocols [Luo et al. 2017; Oosterhof 2017; Pa et al. 2015; Tamminen 2013]. Pa et al. [Pa et al. 2015] provided preliminary analysis results of the infrastructural roles of IoT malware purely based on honeypot data. We have extended one of them with new capabilities and added bare-metal systems to the honeypot. Moreover, we dynamically analyzed malware collected by honeypot in semi-real-time (within 15 minutes after its capture) and traced C&C server detected.

While there have been studies on IoT botnets in the past [Angrishi 2017; Antonakakis et al. 2017; Bertino and Islam 2017; Kolias et al. 2017], to the best of our knowledge, we are the first to study IoT botnet infrastructure in depth.

3 DISCOVERING IOT BOTNETS

To understand the infrastructure used by different IoT botnets, we started by observing IoT-related attacks as captured by a hybrid honeypot scheme that combines low and high interaction [Pa et al. 2015], then we used a sandbox environment for dynamically analyzing malware collected by the honeypot; and, finally, we conducted a static analysis of these samples.



SPECIFICATION				
	OS	CPU	Memory	HD
Analysis System	Ubuntu 14.04	Intel®CPU E3-1240 V2@3.40GHz*4	16G	2T
ARM/MIPS/MIPSel	Debian 7.3	QEMU	124MB	24GB

Fig. 1. Structure of Analysis System.

3.1 Analysis System

Figure 1 illustrates the overview of our analysis system. The proposed system consists of five components, as follows:

- **IoT Honeypot** emulates Telnet, known abused HTTP front-ends, the CPE WAN Management Protocol (CWMP) [Bernstein and Spets 2004], a backdoor of the Netis router, and the remote access setup service of several IP cameras. Moreover, we use bare-metal IoT devices (see Table 2) as high-interaction honeypots. Once an attacker logs into the honeypot and obtains a privileged system shell, we recorded the system interactions, including shell commands. We deployed the IoT Honeypot at 808 IP addresses distributed across three countries, as shown in Table 1. One sensor was located in the Netherlands within a /24 network, 5 sensors were deployed in Taiwan within /26 network and 2 additional sensors in Japan in different /24 networks.

Table 1. IoT Honeypot Sensors

Sensor Name	Location	#IP addresses	Observation Period
NL 01	Netherlands	253	Dec,16 - Dec,17
TW01-05	Taiwan	5 * 63	Dec,16 - May,17
JP01	Japan	140	Oct,16 - Dec,17
JP02	Japan	130	Nov,16 - Dec,17

Table 2. Bare-metal devices characteristics

Device Type	CPU Architecture
Wi-Fi Storage 1	MIPSEL
Wi-Fi Storage 2	MIPSEL
Router	MIPS
IP Camera	ARM

- **IoT Malware Downloader** extracts malware download command from shell command sequence which was observed by IoT Honeypot. We download IoT malware samples as soon as the download command is observed.
- **Sandbox** is composed of VMs (see SPECIFICATION in Figure 1) and bare-metal devices (Table 1). The VM sandbox uses QEMU for emulating devices with the three most prevalent CPU architectures of the collected samples: ARM, MIPS, and MIPSel, on which a Linux OS (Debian) is running. The bare-metal sandbox uses four types of physical devices: 2 Wi-Fi Storages, 1 Router, and 1 IP Camera. These devices are chosen as they have indeed been identified as infected devices by our honeypot and are typical off-the-shelf, low-cost hardware. Note that bare-metal sandboxes run the risk of malfunctioning, as they run untrusted malware binaries. Therefore, we reboot the devices after each malware execution and compare files and processes in the devices to see if any changes made by the malware remain after the reboot. Authors in [Kazuki et al. 2017] reported that existing IoT malware is non-persistent and thus can be easily removed by rebooting the infected device.
- **Access Controller** controls the traffic between the Internet and the IoT Honeypot, Malware Downloader, and Sandbox. It also forwards inbound traffic such as Telnet, to honeypot for passive monitoring. On the other hand, it filters out dangerous outbound attacks.
- **IoT Botnet INFO DB** is a database where every information such as hash codes of IoT malware binaries, DL servers, C&C servers and the relationship of them. we obtained regarding IoT botnets are stored.

3.2 Data

From 2016/10/02 to 2017/12/02, we collected 50, 026 IoT malware samples and observed 23, 341 malware downloader and 1, 131 C&C servers.

3.2.1 IoT malware samples. As shown in Table 3, collected IoT malware has a great diversity in CPU architecture. Main parts are ARM (22.87%), Intel 80386(15.72%), MIPS (12.38%) and MIPSel (11.07%). The reason may be that the attackers attempt to infect as many IoT devices as possible. In many cases, malware binaries for multiple CPU architectures were downloaded and executed. We also found attacks that check device information. They use command "`/bin/busybox dd if =/bin/busybox bs = 22`" to get the top 22 bytes of busybox and obtain ELF format information. Finally, the corresponding binary is downloaded.

3.2.2 Infrastructure (Downloader and C&C servers). From Oct 2016 - Dec 2017, 23,341 unique IP addresses associated with download servers distributed across 145 countries and 1,405 ASes, are identified. Table 4 shows the Top 15 of DL servers' AS information of each malware family and AS types. ASes are colored according to their types, such as Data Center/Web hosting/Transit, Mobile, Government. We used Anti-virus software Dr.WEB's [Daniloff 2018] to label the binaries. For ASes, we used IP2Location [IP2Location.com 2018] "Usage Type" information. Although there is some

Table 3. Number of binaries per CPU architecture

CPU Arch.	# Binaries	
ARM	11,439	(22.87%)
Intel 80386	7,364	(14.72%)
MIPS	6,195	(12.38%)
MIPSel	5,536	(11.07%)
PowerPC or cisco 4500	4,069	(8.13%)
Renesas SH	3,933	(7.86%)
x86-64	3,847	(7.69%)
SPARC version 1 (SYSV)	3,824	(7.64%)
Motorola 68020	3,725	(7.45%)
MIPS(64bit)	76	(0.15%)
Others	18	(0.04%)

variance in ranking, the main locations of DL servers of Bashlite, Mirai and Tsunami are US and European countries. Most DL servers are using "Data Center/Web Hosting/Transit" services. In case of Hajime, which is a P2P botnet, malware binaries are downloaded not from particular servers but from other members of the botnet. Thus the source of malware download is mostly end users of ISP service. We illustrate the monthly AS types transition of TOP 10 Hajime DL servers(see Figure 2). Interestingly, we can observe the ratio of Top 10 countries is dramatically varied. For example, DL servers in AS34400 start from May 2017 and disappear at Aug 2017. The results indicate that Hajime's targets are continuously changing.

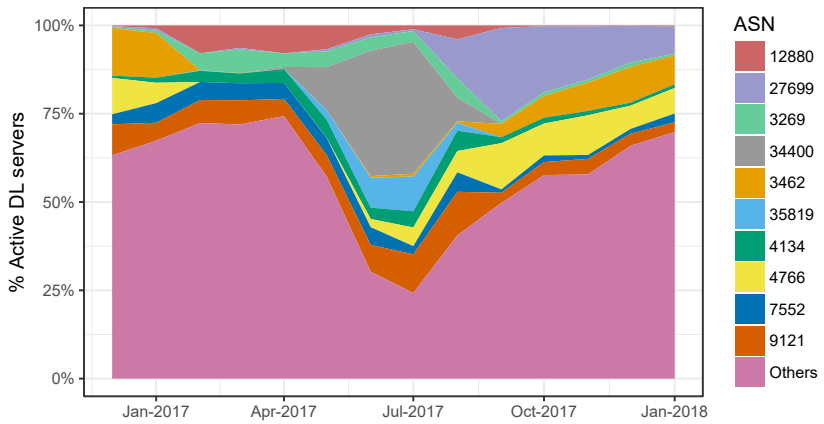


Fig. 2. AS Transition of TOP 10 Hajime DL Servers

In the same period as for download servers, we identified 1,131 unique IP addresses associated with C&C servers distributed across 38 countries and 157 ASes. We observed C&C servers corresponding to 3 different malware families: 1,011 Bashlite, 58 Mirai, and 32 Tsunami. The P2P botnet Hajime did not contribute to these statistics due to its server-less nature. Table 5 shows the country information.

It is the same trend as the DL servers, most C&C servers are located in US and European countries. Also, the most number of AS type of C&C servers is "Data Center/Web Hosting/Transit".

Table 4. Top15 downloader servers per malware family

	Bashlite			Mirai			Tsunami			Hajime		
	ASN	**CC**	**#DL**	**ASN**	**CC**	**#DL**	**ASN**	**CC**	**#DL**	**ASN**	**CC**	**#DL**
1	23033	US	167	12876	FR	50	20473	US	7	34400	SA	2611
2	20473	US	117	31034	IT	31	12876	FR	5	9121	TR	1305
3	31034	IT	108	20473	US	29	60781	NL	4	7552	VN	922
4	36352	US	97	43350	NL	20	31034	IT	4	12880	IR	776
5	33387	US	53	36352	US	16	23033	US	4	3462	TW	736
6	53755	US	52	29073	SC	10	44812	RU	3	4134	CN	705
7	393406	US	46	393406	US	9	43350	NL	3	4766	KR	679
8	200039	GB	40	49981	NL	8	36352	US	2	3269	IT	674
9	43350	NL	38	4766	KR	7	33387	US	2	35819	SA	628
10	49349	NL	27	47381	HU	7	62282	LT	1	27699	BR	612
11	60781	NL	25	56934	ES	6	60392	DE	1	45899	VN	565
12	32097	US	22	51167	DE	6	57043	NL	1	48159	IR	542
13	12876	FR	22	197226	PL	6	51167	DE	1	12389	RU	382
14	18978	US	21	60781	NL	5	49349	NL	1	45595	PK	376
15	16276	FR	21	44812	RU	5	46664	US	1	8386	TR	248
Total	**856 (61.6%)**			**215 (51.9%)**			**40 (75.5%)**			**11,761 (55.1%)**		

Data Center/Hosting/Transit | Mobile ISP | Broadband ISP | Fixed-line ISP

4 MALWARE ANALYSIS

4.1 Infrastructure characterization

Through a dynamic analysis, we identify the C&C and downloader servers used by the different malware families. This analysis is conducted right after a new malware sample is capture by the honeypot. Each new sample is executed it for five minutes in the sandbox environment to observe its behavior. During the analysis period, we obtained 4, 513 from 8, 827 malware samples that belonged to Bashlite, Mirai, Tsunami families. By using C&C server identification method as in [T. Yang et al. 2018], 1, 083 IP addresses and 28 domains were identified as C&C servers. 4, 511 (99.9%) out of the 4, 513 samples connected only to one C&C server. Contrary to traditional Windows malware which often contains multiple C&C server information for their robust control, the observed IoT malware did not seem to have such robustness in C&C connection.

We have drawn some examples of correspondence between the malware samples and C&C Domain/IP in Figure 4. We observed some patterns including multiple C&C domains corresponding

Table 5. Top15 C&C per malware family

	Bashlite			Mirai			Tsunami		
	AS	**CC**	**# C&C**	**AS**	**CC**	**# C&C**	**AS**	**CC**	**# C&C**
1	23033	US	128	31034	IT	7	31034	IT	5
2	31034	IT	100	12876	FR	6	20473	US	5
3	20473	US	84	49981	NL	2	43350	NL	3
4	36352	US	68	44812	RU	2	12876	FR	3
5	393406	US	38	43350	NL	2	60781	NL	2
6	43350	NL	35	29073	SC	2	44812	RU	2
7	53755	US	30	200019	MD	2	36352	US	2
8	200039	GB	30	197226	PL	2	62282	LT	1
9	33387	US	25	9605	JP	1	60392	CH	1
10	60781	NL	21	8896	NO	1	51167	DE	1
TOTAL	**559 (55.2%)**			**27 (45.8%)**			**25 (75.8%)**		

Data Center/Hosting/Transit | Mobile ISP | Government

Table 6. Summary statistics of the botnet infrastructure

Family	#Binaries	#C&C	#DL	#C&C and DL
Bashlite	6,222	52	387	971
Mirai	19,46	26	383	57
Tsunami	72	4	20	32
Total	8,240	82	790	1,060

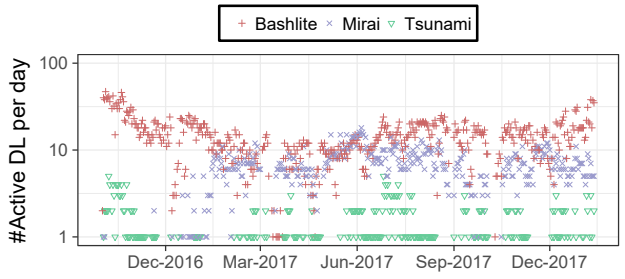


Fig. 3. Number of active downloader servers per day per family

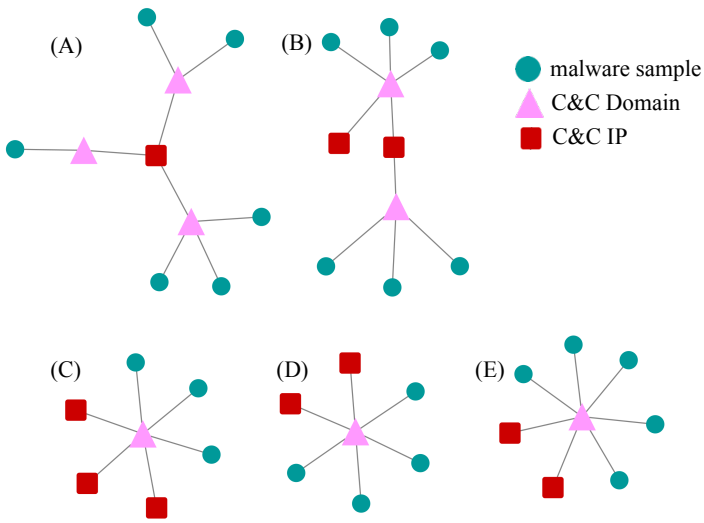


Fig. 4. Examples of C&C Domain, IP and Malware SamplesâĂŹ Relation

to a single IP address ((A), (B) in Figure 4) and one domain corresponding to multiple IP addresses ((C), (D), (E) in Figure 4) In any pattern, each malware sample contained only a single C&C domain.

4.2 IoT malware active period

Analyzing the active period of IoT malware and knowing the update frequency of malware binaries is useful for countering malware. The more frequent the update is, the harder it is to catch up with the countermeasure response.

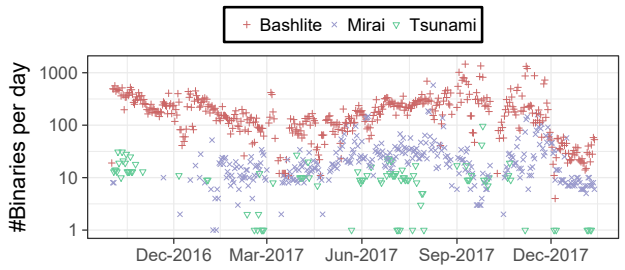
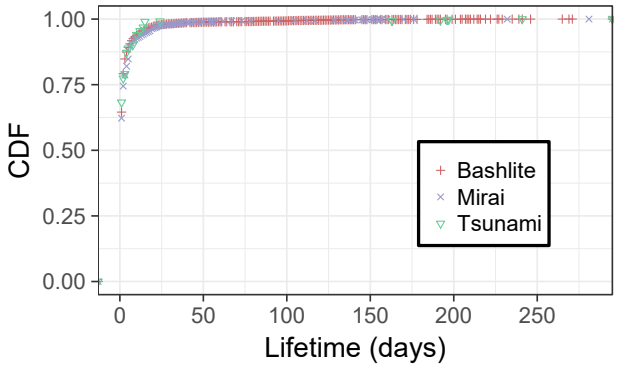


Fig. 5. Number of binaries per day per family

Firstly, we estimated the lifetime of a malware binary. We define the lifetime of a binary as the amount of days from the first time it was seen until the last time it is seen. Figure 6 shows the empircal CDF of the lifetime of the different bianries per malware familys. The lifetime of the binaries belonging to Bashlite, Mirai, Tsunami family is short, and about 80% of these are only seen for less than 3 days. More than 90% of do not survive one week.

Fig. 6. CDF of the binaries' lifetime per malware family



The facts that the DL periods of these binaries are very short and that each binary only contains a single C&C domain/IP as shown in previous subsection suggest that these binaries are treated as âĂIJdisposableâĂİ. This may be related to the fact that these binaries are non-persistent and can be removed by rebooting the infected devices. We now focus on malware binaries downloaded from the same DL server with a case study of DL server "XXX.239.72.250". In Figure 7, gray points are malware samples downloaded from the DL server. Pink squares are download dates. Samples linking to the square means they are downloaded in that date. In this case, among 1,202 samples downloaded in 2017-09-09, only 199 samples were downloaded in 2017-09-10. The figure shows that malware binaries are indeed frequently updated within a single download server.

Moreover, we shed light on 2,012 DL servers that we could collected malware from for two or more consecutive days. For one DL server(Y), the malware could be downloaded during the period TT which counted by day unit, newly downloaded malware of a certain date t (t ∈ T) is defined as $newmalware(t)$. Calculate the update speed frequency (means average number of malware updated per day) of the DL server Y (average number of malware updated per day) by the following formula.

$$UpdateFrequency(Y) = \frac{\sum_{t=1}^{T} newmalware(t)}{T-1}$$

Figure 8 shows the distribution chart of the update speed frequency of each DL server. The vertical axis is the update frequencyspeed. Each point is a DL server, and the family of IoT malware samples obtained from the DL server is displayed as gray for Bashlite, orange for Mirai, green for Tsunami, and blue for Hajime. If downloaded malware samples are belonging to multiple families, it will be paint color of the most obtained malware familyâĂŹs color. As the average update frequency of each malware family speed shown in Table 7, Bashlite is 10.8 near to TsunamiâĂŹs 10.86. That means each DL server updates about 10 malware samples binaries per day on average. On the other hand, Mirai is 3.92. Hajime is the lowest, only 1. That may be Hajime is a P2P type malware family, have different malware distribution measures.

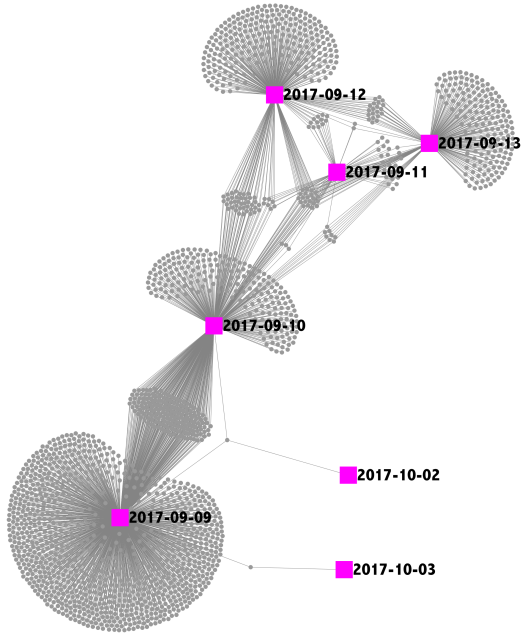


Fig. 7. Relationship of Malware Binaries and Download Dates

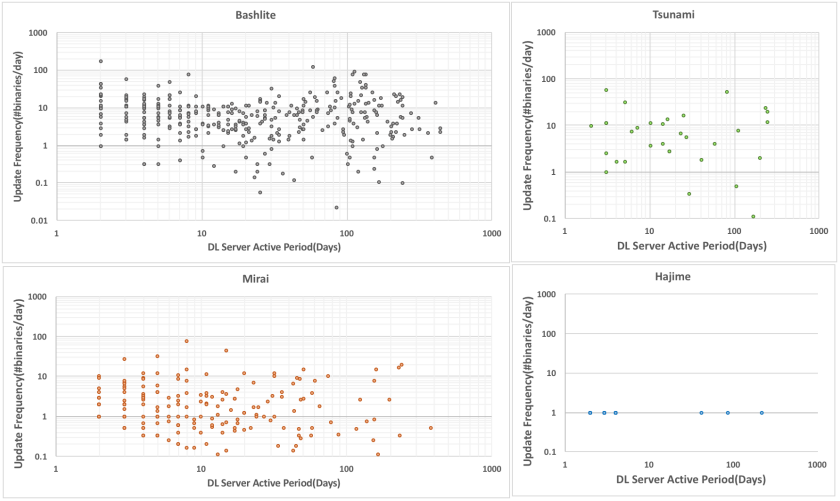


Fig. 8. Update Frequency

4.3 Relationship of Malware, DL and C&C

In the IoT honeypot observation, we could obtain malware binaries and the DL servers, C&C servers identified by dynamic analysis. We now investigate the relationship between DL servers and C&C

servers and the binaries which belong to Bashlite, Mirai, Tsunami families.

Figure 9 illustrates the relationship between the binaries, DL servers, and C&C servers. The pink triangles are the C&C server IPs, the red triangles are the DL server IPs, and the blue points are IPs working as both C&C server and DL server. The gray points are Bashlite binaries, the orange is Mirai, and the green is Tsunami. A binary and server are connected with an edge if the binary is indeed downloaded by the DL server or controlled by the C&C server. In Figure 9, there are 21 groups of Mirai, 92 Bashlite, and 3 Tsunami. Among the Mirai groups, the largest one contains 445 binaries and 226 servers. Among 445 samples, 391 were detected as Mirai, 42 as Bashlite and 12 as Tsunami. The 226 servers include 13 C&C servers, 187 DL servers, and 26 servers have both roles of C&C and DL server. Compared to other groups, the number of infrastructure servers is quite large, especially the number of DL servers. The number of Tsunami malware is insufficient, and the trend is similar to the Bashlite groups. In the Bashlite groups, servers work as both C&C and DL server, and the number of the servers is little compared with Mirai case mentioned above. We note that different groups depicted in Fig 6 may belong to the same botnet. As some of the DL servers and C&C servers are indeed located in the same IP range [T. Yang et al. 2018]. Deeper analysis of these servers is our future work.

5 DISCUSSION

As we have shown, IoT botnet infrastructure is mainly located in the hosting services, which is not different from many traditional Windows botnets. We have not seen clear indication of infected IoT devices being misused as botnet infrastructure except that Hajime downloads its binaries and transmit commands through its own P2P network of infected devices.

We found that the update frequency of Bashlite and Tsunami malware is very high and each binary seems to be treated as âĂIJdisposableâĂİ only containing single or very few C&C domains/IPs. It seems that the botnet operators are not keen about constructing long-lasting robust botnets, which may be due to the fact that the IoT malware infection is indeed non-persistent.

6 CONCLUSION

At first, we designed an analysis system for observation of IoT attacks and collection of IoT malware infrastructure serversâĂŹ information. From the observation continued for more than one year, we obtained 50,026 malware binaries, 23,341 DL servers, 1,131 C&C servers information. We then analyze the botnet infrastructure, except P2P type malware Hajime, the infrastructure of Bashlite, Mirai, Tsunmai are mostly using hosting services. We also found that the Bashlite and Tsunami malware update frequency is very high, updating about 10 malware samples per day. At last, we analyzed the relationship of malware, DL and C&C servers. We found large infrastructure of Mirai. However, for Bashlite and Tsunami we could not link the binaries and servers clearly due to the âĂIJdisposableâĂİ nature of their binaries. We will take deeper look at the relationship in our future work.

7 ACKNOWLEDGMENTS

Part of this research was conducted with the support of the National University Reform Improvement Promotion Project of Ministry of Education, Culture, Sports, Science and Technology. A part of this research result was obtained by contract research of National Institute of Information and

Communications Technology (NICT): Research and development for practical application of web mediation attack countermeasure technology.

REFERENCES

360 netlab. 2018. Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869. http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/

Kishore Angrishi. 2017. *Turning internet of things (IOT) into internet of vulnerabilities (IoV): IoT botnets.* preprint. arXiv. arXiv:1702.03681

Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the Mirai Botnet. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 1093–1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

Jeff Bernstein and Tim Spets. 2004. CPE WAN management protocol. In *DSL Forum, Tech. Rep. TR-069.*

Elisa Bertino and Nayeem Islam. 2017. Botnets and internet of things security. *Computer* 50, 2 (2017), 76–79.

Evan Cooke, Farnam Jahanian, and Danny McPherson. 2005. The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets. *SRUTI* 5 (2005), 6–6.

Igor Daniloff. 2018. Doctor Web. https://www.drweb.com

Scott Hilton. 2016. Dyn Analysis Summary Of Friday October 21 Attack. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack

IP2Location.com. 2018. IP2Location. https://www.ip2location.com/

Tamiya Kazuki, Nakayama Atsushi, Erizawa Yuta, Katsunari Yoshioka, and Tsutomu Matsumoto. 2017. Removal and prevention of IoT malware using real devices. In *Symposium on Cryptography and Information Security.*

Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IoT: Mirai and other botnets. *Computer* 50, 7 (2017), 80–84.

Bryan Krebs. 2016. KrebsOnSecurity Hit With Record DDoS. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Tongbo Luo et al. 2017. Iotcandyjar: towards an intelligent-interaction honeypot for iot devices. *Black Hat* (2017).

Michel Oosterhof. 2017. Cowrie Telnet/SSH Honeypot. https://github.com/micheloosterhof/cowrie

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, and Christian Rossow. 2015. IoTPOT: Analysing the Rise of IoT Compromises. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*. USENIX Association, Washington, D.C. https://www.usenix.org/conference/woot15/workshop-program/presentation/pa

Christian Rossow, Christian Dietrich, and Herbert Bos. 2012. Large-scale analysis of malware downloaders. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.* Springer, 42–61.

Bruce Schneier. 2014. The Internet of Things is wildly insecure-and often unpatchable. https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

Tom Spring, K Carpenter, and M Mimoso. 2016. BASHLITE family of Malware Infects 1 Million IoT devices. *Threat Post* (2016).

D. Yang T. Yang, S. Nakayama T. Hoizumi, and T. Matsumoto K. Yoshioka. 2018. Observation of DDoS attacks from IoT malware using sandbox analysis. *Information Processing Society of Japan Journal* 59 (2018), 5.

U Tamminen. 2013. Kippo SSH honeypot. *Retrieved* 9 (2013), 2013.

Trend Micro. 2017. New Mirai variant found spreading like wildfire. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/new-mirai-variant-found-spreading-like-wildfire