AN EXTENDED ANALYSIS OF AN IOT MALWARE FROM A BLACKHOLE NETWORK

Alexandre Dulaunoy, Gérard Wagener

CIRCL-Computer Incident Response Center
41, av. de la Gare, L-1611 Luxembourg
Luxembourg
{alexandre.dulaunoy, gerard.wagener}@circl.lu

Sami Mokaddem

Université catholique de Louvain
1, Place de l'Université, B-1348 Louvain-la-Neuve
Belgium
sami.mokaddem@student.uclouvain.be

Cynthia Wagner

Fondation RESTENA, CSIRT
2, avenue de l'Université, L-4365 Esch-sur-Alzette
Luxembourg
{cynthia.wagner}@restena.lu

Paper type

Research paper/Case Study

Keywords

IP-blackhole monitoring, Internet of Things (IoT), Mirai analysis and network security

Abstract

The Internet of Things becomes more and more ubiquitous and new impacts in the landscape of classical network activities can be observed due to the fact of pervasive computing. This new kind of devices needs permanent connectivity, ranging from surveillance cameras to connected mattresses. This has also become a main trigger for a new threat landscape. Weak to no security features at all build a good starting point for attacking these kinds of devices.

In this paper, we present some recent observations from a practical analysis of Internet of Things malware by inspecting traffic from a blackhole. We reviewed some old infections and assume that the clean-up of compromised machines is a long lasting process.

1. Introduction

Referring to the Oxford dictionary the Internet of Things (IoT) is defined as "the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data". IoT devices have become very popular in the last few years. Almost everyone has at least one IoT device in its close surroundings. The idea to stay connected to devices and to track and collect data about daily activities, such as adjusting temperature at home, collecting actual health status information or simply using a surveillance camera, has become very tempting. Referring to latest statistics from Cisco [CiscoStats15], it is estimated that in 2020, the number of connected IoT devices will easily exceed the number 50 billion.

The IoT grows permanently and gains on popularity daily, and with this, also the related threat landscape. In general, IoT devices were designed by applying the "any"-paradigm [Any], as represented in Figure 1, which means that devices should to be available and communicating at any time, from anywhere, on any path with any service and so on, and at the same time be fast and cheap.

To top these arguments for smart devices, additional requirements are that they should be easy to handle and provide collections of fancy services to the user. A major issue that faces these devices is the plethora of security problems, since security does not flow in-line with the "any"-paradigm.

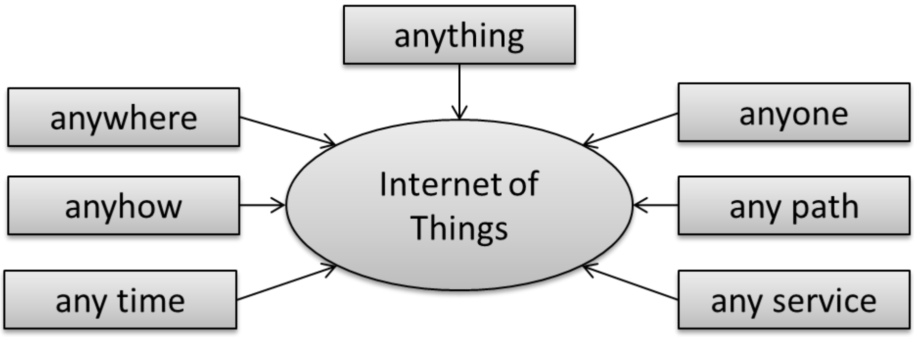


Figure 1: The "any"-paradigm in IoT [Any]

Securing connected devices becomes more and more important due to the fact that actual devices have only weak or completely lack of integrated security features by design. Known security vulnerabilities range from weakly secured devices, for example default password (“admin/1234”) to weakly implemented C code. These basic vulnerabilities expose IoT devices to the most unsophisticated attacks such as spoofing, jamming and simple intrusion attacks.

The attractiveness for attacking IoT devices is simple, the devices are permanently online (even if there is no need to); have no anti-virus protection or malware scanners and only weak protection mechanisms, if any at all. Another major flaw is that there are even devices which do not have the capability to be patched, which means that in case of a vulnerability disclosure it cannot be fixed.

In recent past, a large increase of telnet-based attacks targeting IoT devices can be observed [IoTpot15]. One example is the recent Mirai attack that faced large services as DNS[1]-providers, GitHub, Amazon, etc. In this paper, we present results of an extended analysis on IoT malware from our operated blackhole network sensor.

This paper is organised as follows: Chapter 2 presents a short state of the art that introduces to blackhole monitoring, presents briefly some IoT malware and explains some relevant features that were used in this case study paper. Chapter 3 presents the analysis of IoT malware, such as the evaluation and evolution of the Mirai malware that had recently gained popularity. Chapter 4 presents other types of malware and the related observations in the blackhole. Chapter 5 gives some future intentions and concludes the paper.

2. State of the Art

The buzzword "Internet of Things" (IoT) was first introduced in 1999 by Kevin Ashton, a technology pioneer, in the framework of a project for RFID[2] standards [Ashton]. Since a few years only, this topic has become a hot research topic. Recent simulations show that more than 20 billion devices are estimated to be active in 2020 [CiscoStats15]. One research domain in IoT focuses on securing IoT devices. In [Bhattasali13], a study on how to secure IoT devices in general is presented. Other research topics focus on the detection of vulnerable devices in IoT such as [Markowsky15], or present challenges in order to increase security within IoT as presented in [He2016, Kumar16, Bertino16].

A blackhole can be described as temporarily unused routed IP address space of a network, also called dark address space, that is announced globally on the Internet but not running any services on it. In general, traffic ending in blackholes is unidirectional and unwanted. Bailey et al. [Bailey05-2] introduced the definition of black-hole monitoring in 2005, by collecting measurements of the Internet noise.

[1] DNS: Domain Name System

[2] RFID: radio-frequency identification

A common observation is that blackhole information contains not only local erratic traffic, such as reflecting misconfiguration of devices [Dulaunoy14], but also information about events occurred on the Internet as a whole [Zseby12, Zseby13, Wustrow10, Bertino16,…], such as backscatter traffic or malware traffic. Beside these misconfigurations or erroneous events, another observation is that these logs also present some interesting patterns or strange attractors [Zalweski01]. For example in [Medeiros10], strange attractors were used to set up a method to fingerprint operating systems by analysing TCP ISN (Initial sequence number) by means of chaotic dynamics theory and neural networks.

Blackholes and honeypots not only represent an interesting source for extracting information on botnets and malware [Shimoda10, IoTpot15, Agrishi17, Duy15, Spitzner03, Darknet, Furutani15] from IP networks in general, but also from IoT devices. In [Duy15], Bayesian game models were applied to honeypot-enabled industrial control systems (ICS) networks in order to detect malicious behaviours and to set up protection mechanisms. [Perakovic15] analyses the effect of increasing the number of IoT devices in a network and its direct impact on the number and volume of DDoS attacks. On the other hand, [Farina15] introduces SlowBot Net, a prototype botnet for executing DDoS attacks by using only low bandwidth rate techniques.

In this paper, we focus on malware and botnet traffic that is related to IoT malware and more specifically, on the observations on our blackhole. Different works focussed on the analysis of Mirai shortly after the main attacks, as presented in [MapMirai16, OP-Mirai16]. The source code of the Mirai malware [jgamblin] was also shortly leaked after the attacks [SouceMirai]. A complete explanation of the source code in detail is provided in [Web16] for example

3. IoT Malware and Analysis

Malware of all kind has been a daily threat to classical networks over the last decade. With the rising of the IoT and connected devices, threats have shifted to this new domain as well.

The first time that the name Mirai in relation with malware showed up was in 2016. The strongest attack in the short history of the IoT ever took place in September 2016. The Mirai malware was used to perform a strong DDOS attack against a significant DNS-provider called Dyn. This attack also had significant impact and side effects on other large sites such as OVH, GitHub, Amazon and others, which were temporarily unavailable. In [MiraiDesc], it was estimated that the overall throughput of the attack reached about 1.2 Terabits per second, involving more than 100 000 compromised devices by guess, which were mostly DVR players and digital cameras. A few weeks earlier already a less strong attack occurred on the security blog “Krebs on Security”[3]. This attack reached approximately a throughput of about 665 Gigabits per second.

In the following paragraphs an extended case study on the evolution of Mirai and similar IoT malware will be presented. The main point that differentiates Mirai from other botnets is that the attacks were, first executed by compromised easy-to-hack IoT devices and second, on a very large scale. By digging deeper into the data from the blackhole it can be observed that Mirai was not only a “one time headliner”, but is still an active threat.

3.1 **The Mirai case study**

This paper refers to two data sources for this case study. The first data source is a blackhole network, which has an address space close to the private address space as in RFC1918 and it did not change over time since August 2011. This blackhole network includes 6140 public IP addresses. The observation period on the blackhole for data described in this paper reaches until April 1st 2017. The second data source is a mid-interaction honeypot called MTPot[4]. This honeypot was operated from December 11th 2016 until February 27th 2017 in order to gain further insights and understanding of the Mirai variant described in this paper.

All observations and graphs represented in this paper are by default from the blackhole network unless explicitly mentioned. Privacy issues related to IoT such as the ex-filtration of personal data is out of scope for this paper.

[3] Krebs on Security, link to source: https://krebsonsecurity.com/

[4] MTPot: https://github.com/Cymmetria/MTPot

3.1.1 Fingerprinting Mirai

The source code of Mirai was shortly leaked after the attacks on GitHub [jgamblin]. This source code serves as a reference for defining Mirai in this paper, although there are many other variants available, but will not be considered here.

The source code of [jgamblin] called Mirai-Source-Code includes a file called `scanner.c` (sha1sum hash c561be28156cf45c83641fd9190165d8b25a392b). This code is responsible for searching new victims to compromise and to convert them into bots. It reaches out for machines exposing telnet services on port 23 (TCP) and 2323 (TCP). Once it receives a prompt for user name and password, it starts to brute force a list of passwords. A particularity of this piece of malware is that it uses a totally unsophisticated method to attack, by bruteforcing telnet servers. For this, it applies a small predefined list with 63 default passwords only. This number is quite small compared to the Morris Worm in 1988 for example, that used a bruteforcing list of 432 passwords [MorrisW88].

Once the bot successfully logs in the probed telnet server, it sends the discovered credentials to a randomly chosen machine, called loader, on a port whose encrypted value is defined at the offset `TABLE_SCAN_CB_PORT` in the lookup table. The discovery of the loader can be explained as follows: The ciphered domain name of the loader domain is hard coded in `table.c`. This domain is resolved from the name server of Google that is `8.8.8.8` on port UDP 53. The bots wait for multiple IPs and one is chosen randomly. The decryption key is defined in the file `table.c`.

In order to find vulnerable telnet servers, it generates random IPv4 addresses (32 bit integers). Then it checks the generated IP address with a blacklist, including RFC 1819, public IP addresses of the department of defense, US Postal service, Hewlett-Packard ….

It uses raw sockets, which means that it manages the TCP sessions in the user space with its own code. As initial TCP sequence number, it uses the same 32 bit integer as for the randomly generated destination IP address. By referring to this technique, the conventional TCP connection table for all probed servers can be decreases and limits itself to manage connections to responding telnet servers.

At the point the Mirai bot receives an answer; it checks the IP protocol, the port (23 or 2323), the flags and expects a TCP sequence number corresponding to the victim's IP address minus 1. Once these conditions are met, it puts it in a connection table, if the TCP connection state is not closed and if there is still room in the connection table, which is limited to 128 by default.

On the other hand, the setting of the initial number to the destination IP address provides the following possibilities to honeypot operators:

- Identify potential IP packets from this kind of bots. Hence, the fact of setting the initial sequence number to the destination port is defined as *Mirai fingerprint* in this paper. For a honeypot or black hole operators the destination IP addresses are known and it can be searched in the initial fingerprint.

- Tarpitting bots. This means to keep them busy brute forcing a controlled set of (128) IP addresses, which corresponds to the maximal size of the connection table. Although, the Mirai bot forks for doing brute forcing against telnet servers in parallel with its core activities, it could be slowed down by preventing it reporting the harvested credentials.

Since the Mirai malware bruteforces telnet services on port 23 and port 2323 services, a first general observation was a large increase of this kind of traffic over time. On the following page, Figure 2 shows the distribution of port 23 and port 2323 over the last 28 months. It can be observed that shortly before the attack a significant peak can be observed in both figures and that after the attacks these activities cease again slowly.

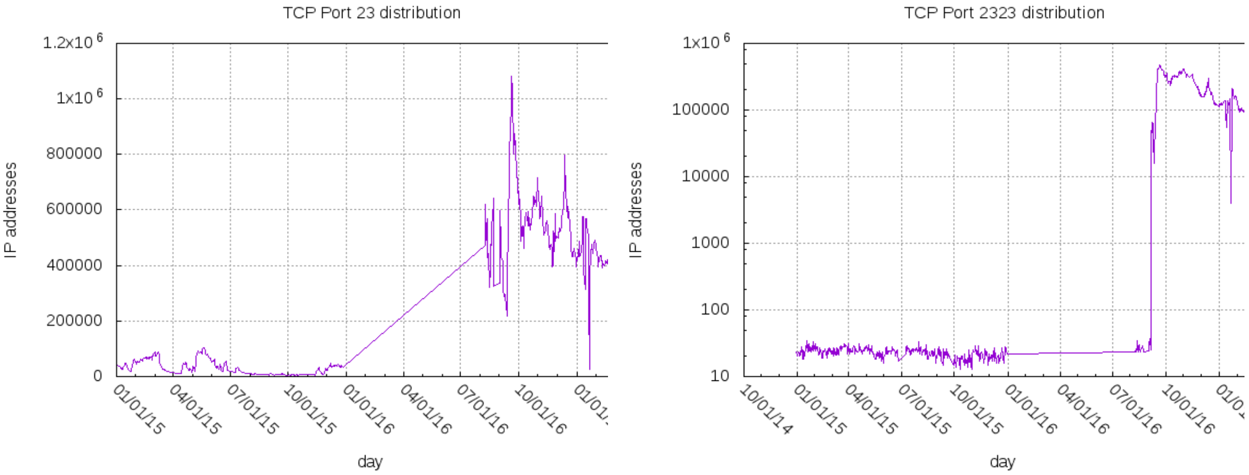


Figure 2: Significant increase of telnet traffic on port 23 and 2323

The scanning activities of Mirai using as ISN the destination IP address decreased over time, as can be observed in Figure 3 and 4. Figure 3 shows the scanning activity of Mirai for the period in the surroundings of the attack in September 2016, where shortly after the attack, the overall activity drops. This can be explained by the patching of source code, as well as to the reboot of devices since Mirai is not persistent. Over the last few months the number of observed unique IP addresses dropped significantly, compared to the period of September to November, but overall it can be seen that it continuously exists. The through in Figure 4 for March 2017 can be explained by a technical breakdown of the blackhole.

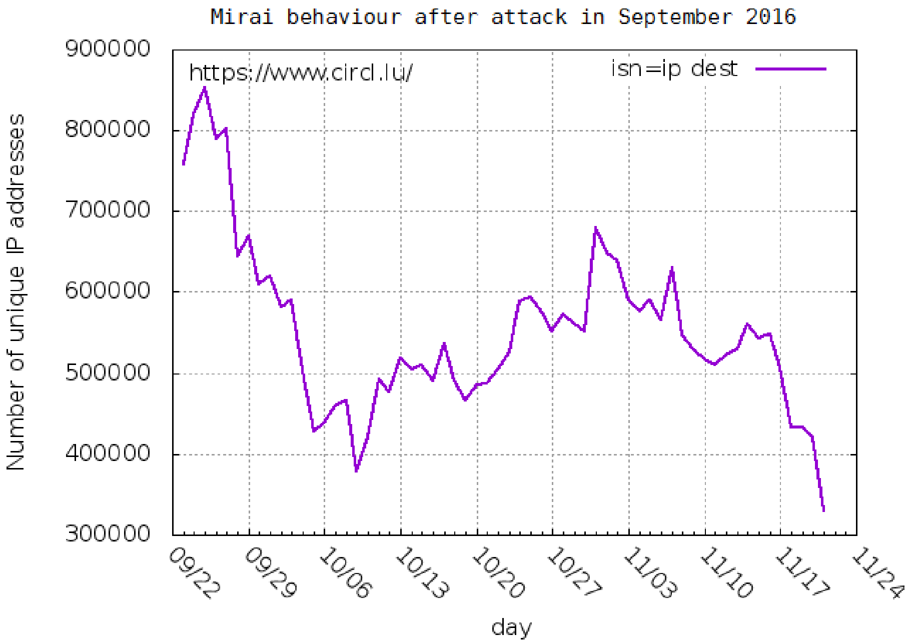


Figure 3: Activities of Mirai from September to November 2016

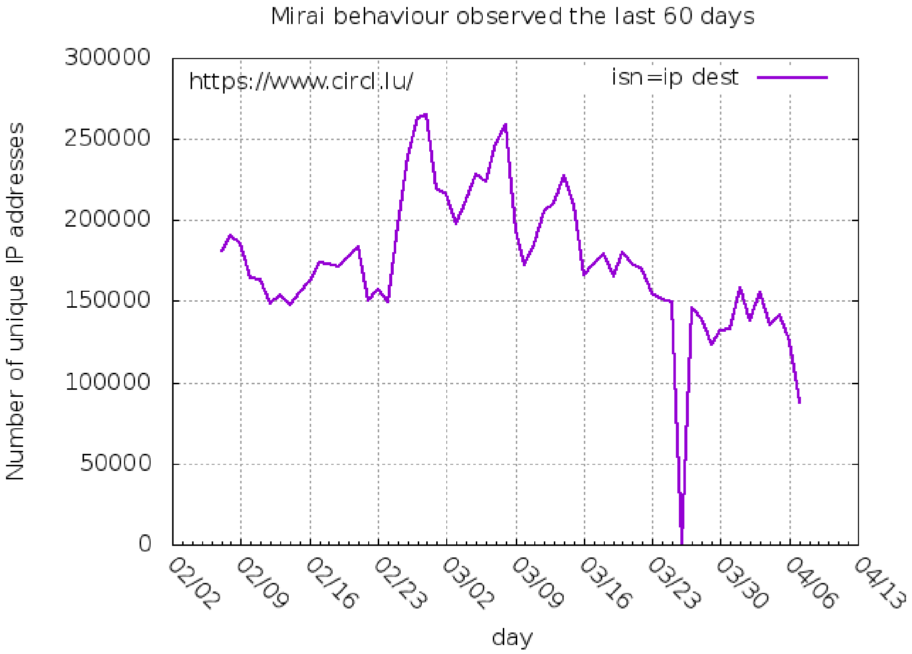


Figure 4: Activity of Mirai from February to April 2017

3.1.2 Evolution of Mirai

In Figure 5, the unique IP addresses having set the initial sequence number (ISN) to the destination IP address for the ports 23 TCP and 2323 TCP are represented. On this plot, the unique IP addresses probing port 23 TCP and port 2323 TCP are also represented. The focus was set on the period where the ISN is destination IP was observed. In the blackhole network this behaviour was observed on 2016-08-09. The last week of August this behaviour dropped due to an outage of the blackhole capturing system.

The number of unique IP addresses hitting the blackhole including ISN=destination IP on port 23 and 2323 is almost the same than the traffic dedicated for port 23. Around December 1st 2016, this behaviour changed. One hypothesis for this divergence is that new variants of Mirai emerged, which changed the initial TCP sequence setting. In order to validate this hypothesis telnet honeypot data from this period should be evaluated.

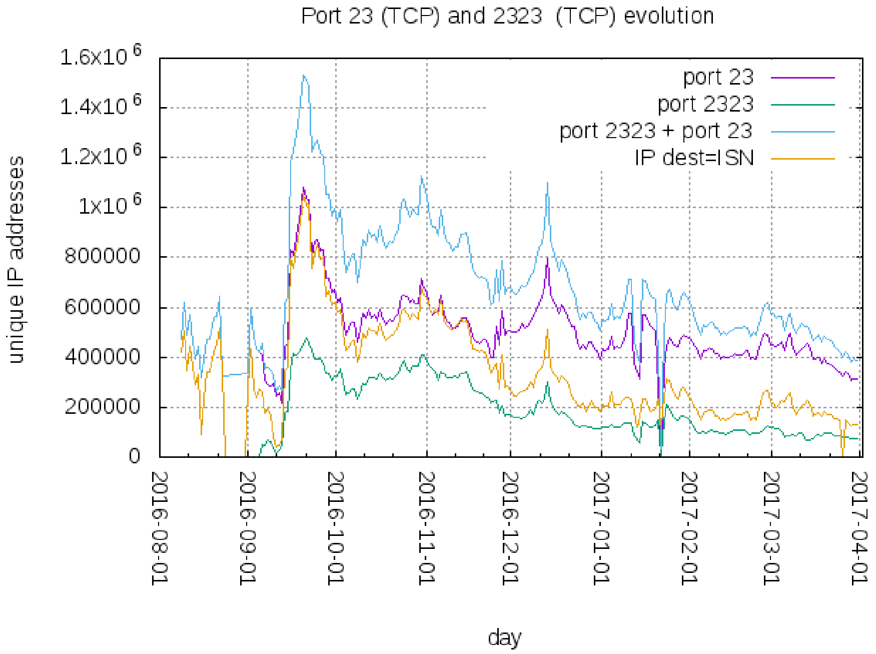


Figure 5: Mirai behaviour observation

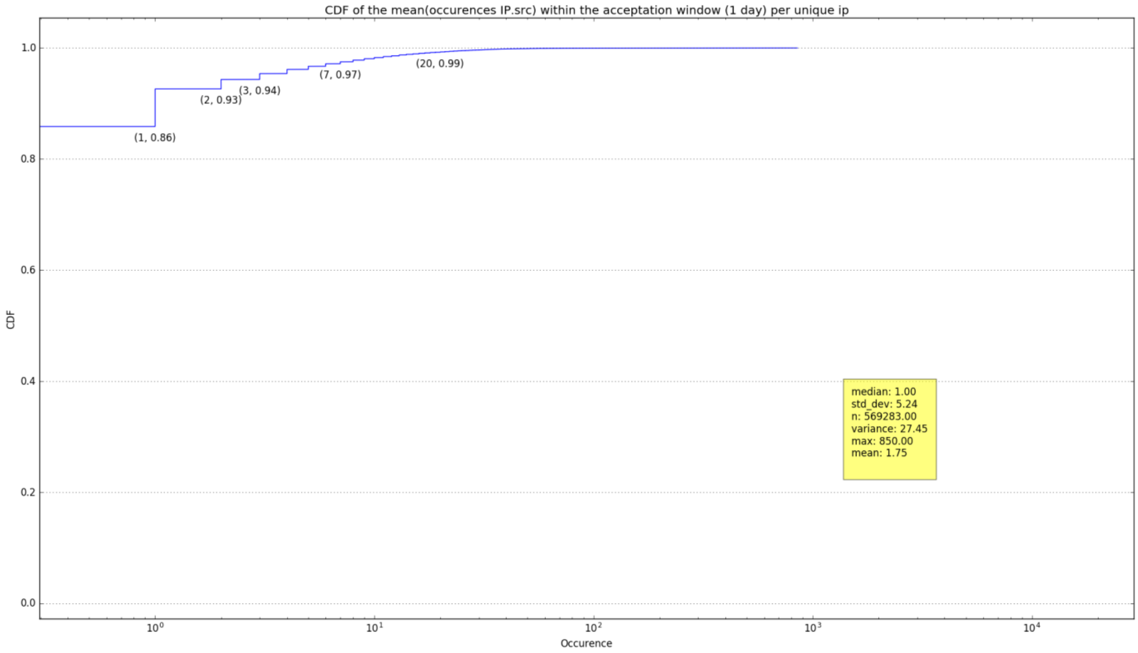


Figure 6: Distribution of unique IP addresses per day

In the Mirai source code, the target IP addresses that are brute-forced, are randomly generated and filtered with a blacklist, as described previously. In Figure 6, derived from the honeypot, the cumulative distribution function (CDF) of the occurrences of probes per day is represented. It is shown that approximately 85% of the unique IP addresses probe the honeypot less than 10 times.

In another experiment, the unique IP addresses are grouped together in daily sets. The first set included IP addresses from March 21st 2017. The intersection of the set corresponds to the day d and the previous day d-1. The elements of this intersection are stored in the set i0. The intersection between the sets i0 and d-2 results in set i1. This was repeated until the resulting intersection set, labelled iN, was empty and with N being the number of days. The cardinality of each intersection set is given in Figure 7.

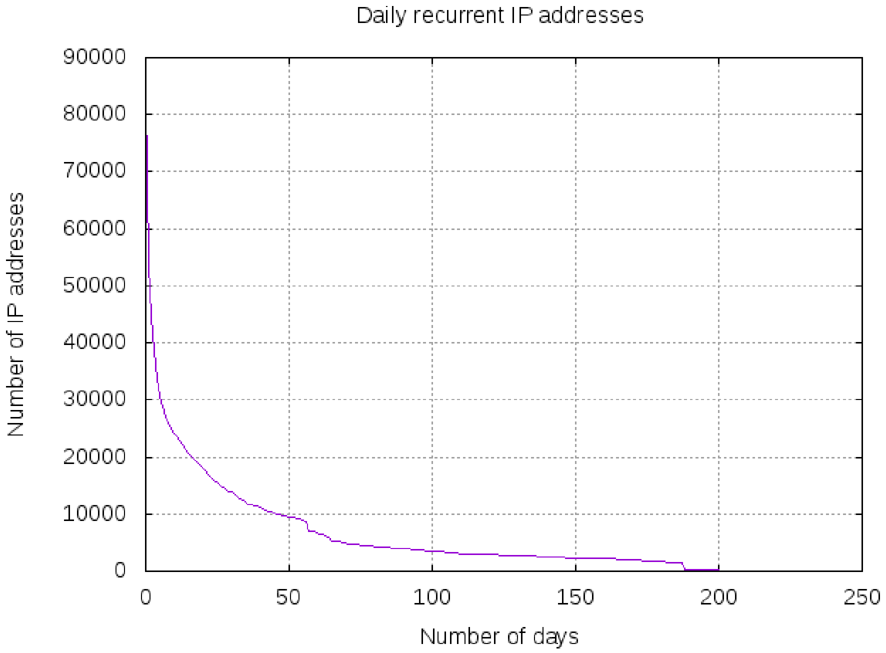


Figure 7: Distribution of daily occurrences of IP addresses

From Figure 7 on the previous page, it can be derived that at least 260 IP addresses probed minimum one time our blackhole network during 260 days. Hence, we defined these IP addresses as stable IP addresses. After 187 days the cardinality dropped by a factor 4, which shows that the younger botnets (less old than 187 days) are more stable than those observed in the past.

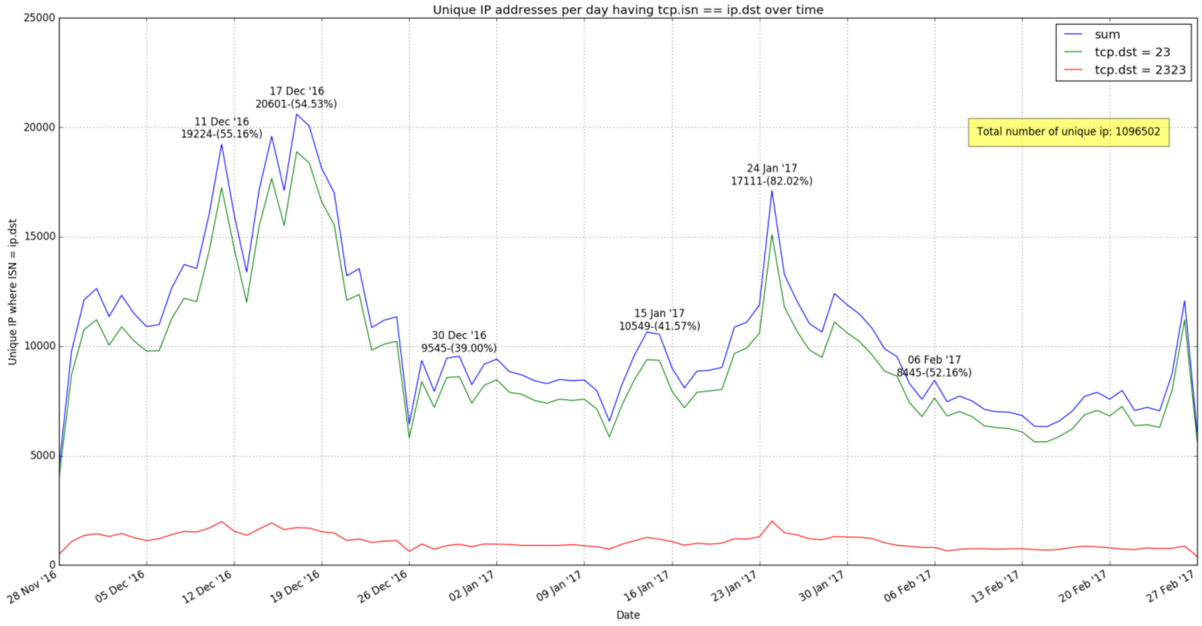


Figure 8: Evolution of probes of port 23 and 2323 on the honeypot

Figure 8 depicts the number of unique IP per day having set the tcp.isn = ip.dst property over time. This represents the amount of Mirai compromised devices contacting the blackhole.

We can observe that on December 17th 2016, the number of compromised IP addresses contacting the blackhole rose at 20 601, representing 54.53% of the total unique IP addresses contacting our server on this particular date. Also, on January 24th 2017, the number of IP drastically increased again to a peak of 17 111 before falling back onto its normal level. We should note that on this date, 82.02% of IP addresses have the Mirai property set to tcp.isn = ip.dst. Unfortunately we do not have any information why these peaks occur.

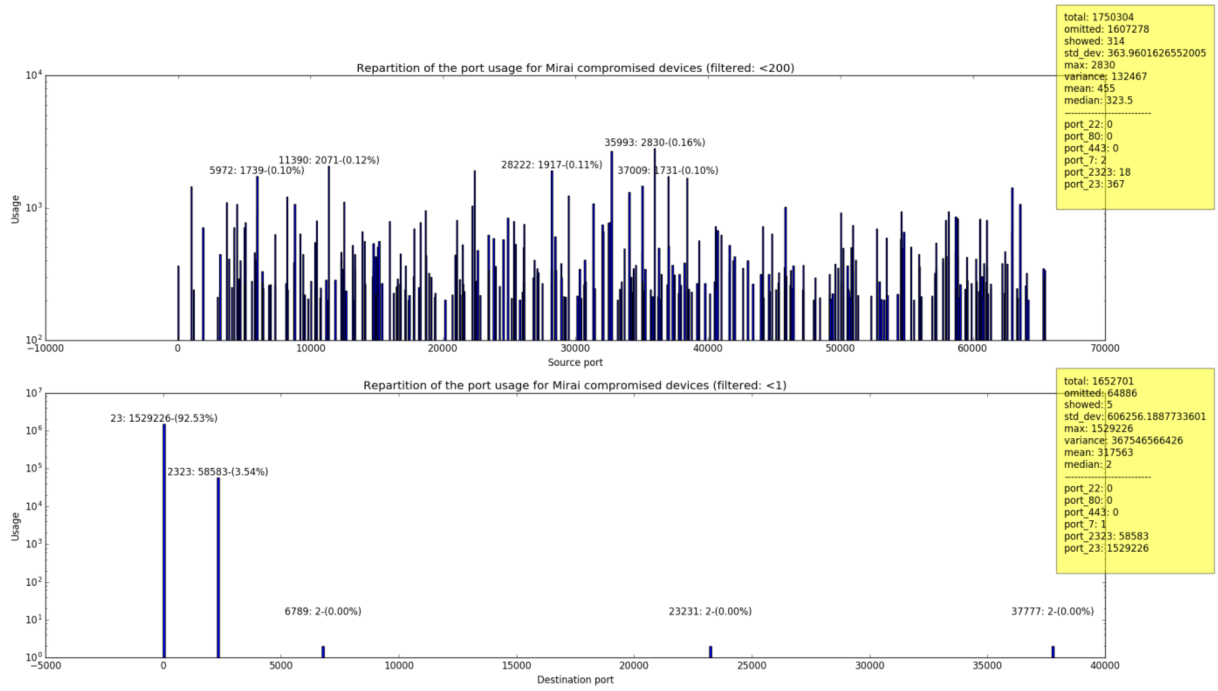


Figure 9: Ports targeted on the honeypot

In Figure 9, the first (upper) bar chart represents the use of the source port for Mirai compromised devices (isn = ip.dst). It can be observed that this usage is rather uniform. All ports seem to be used randomly without any preferences.

However, by observing the second (lower) chart it can be said differently. It can immediately be seen that a huge amount of traffic targets the port 23 (92.53%) and port 2323 (3.54%). This confirms that Mirai targets specifically telnet services running on IoT devices and using the ports 23 and 2323. It can also be observed that the ports 6789 and 23231 are also targeted. These ports were put in direct relation with Mirai by the authors of [miraiscanner]. The port 23231 is also linked to Mirai according the authors of [MiraiPort].

3.1.3 Telnet sessions

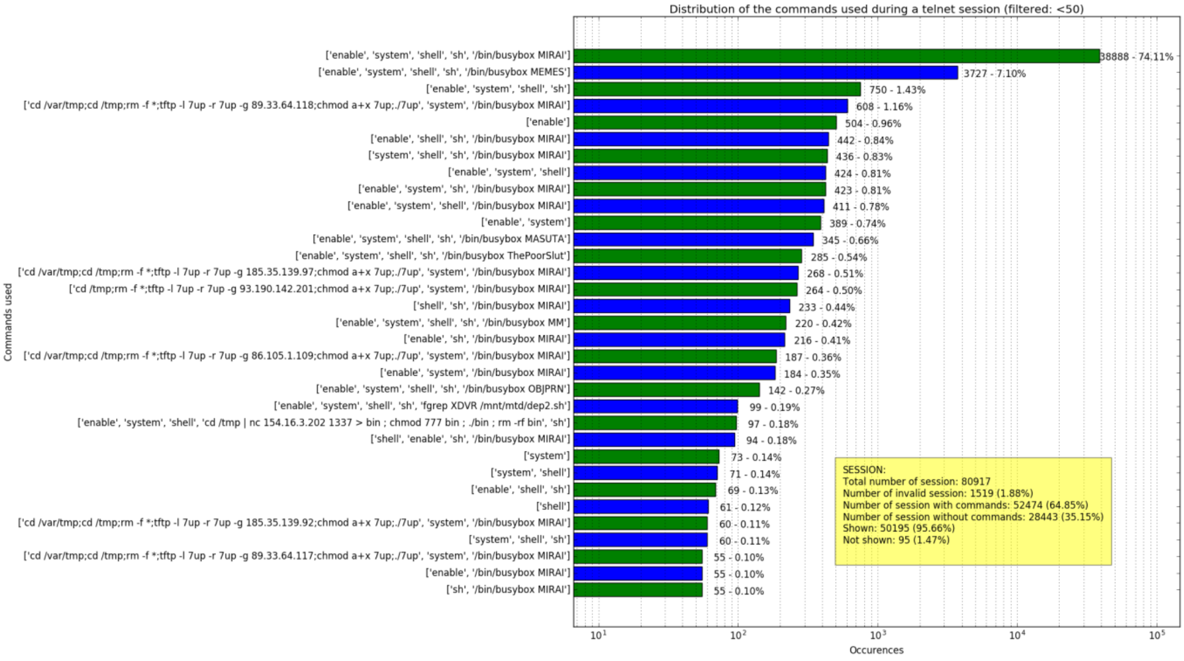
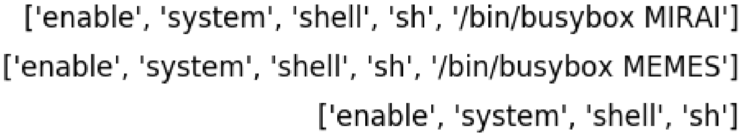


Figure 10: Executed commands on the honeypot

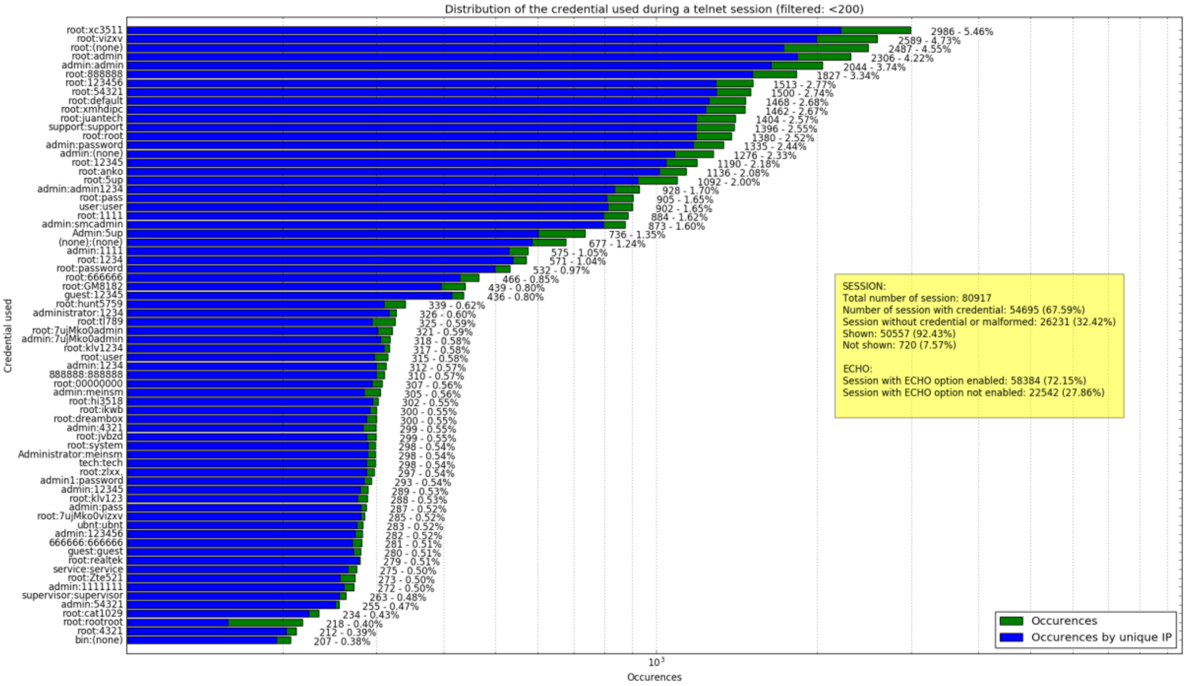
Figure 10 shows the distribution of the most used commands by the remote devices right after it has logged in the honeypot. First of all, it can be observed that one set of commands is particularly predominant as can be seen in the top 3 commands:



```
['enable', 'system', 'shell', 'sh', '/bin/busybox MIRAI']
['enable', 'system', 'shell', 'sh', '/bin/busybox MEMES']
['enable', 'system', 'shell', 'sh']
```

The large majority of the sent commands are used to launch a malware (e.g. MIRAI or MEMES) on the busybox application. But others are used to fetch a malware from distribution points.

Another interesting fact is that a large proportion (35%) of session successfully logged-in but do not sent any commands at all.



SESSION:
Total number of session: 80917
Number of session with credential: 54695 (67.59%)
Session without credential or malformed: 26231 (32.42%)
Shown: 50557 (92.43%)
Not shown: 720 (7.57%)

ECHO:
Session with ECHO option enabled: 58384 (72.15%)
Session with ECHO option not enabled: 22542 (27.86%)

Figure 11: Probed credentials

Figure 12 is derived from the honeypot. This bar chart depicts the distribution of the credentials used to connect through a telnet session. First of all, it can be observed that some credentials are way more used that others.
Secondly, the graph shows that remote devices do not try too often to execute the same credentials on the blackhole. Except for the `'root:rootroot'` (218 times), where nearly half of the tests are done multiple times by the same set of IP(s) during the time spanned over the dataset. Thirdly, it can be seen that a huge proportion (32.42%) of the sessions are malformed or do not have completed the log-in operation. A small list with the top 5 credentials is given below:

```
root:xc3511
root:vizxv
root:(none)
root:admin
admin:admin
```

The keyword '`xc3511`' encoded in the Snort rule by the authors of [kliarsky17] is leading the ranking in Figure 11. Finally, a third of the sessions have the DO ECHO telnet option not enabled. This can tell that different versions of the telnet client are used by the remote device.

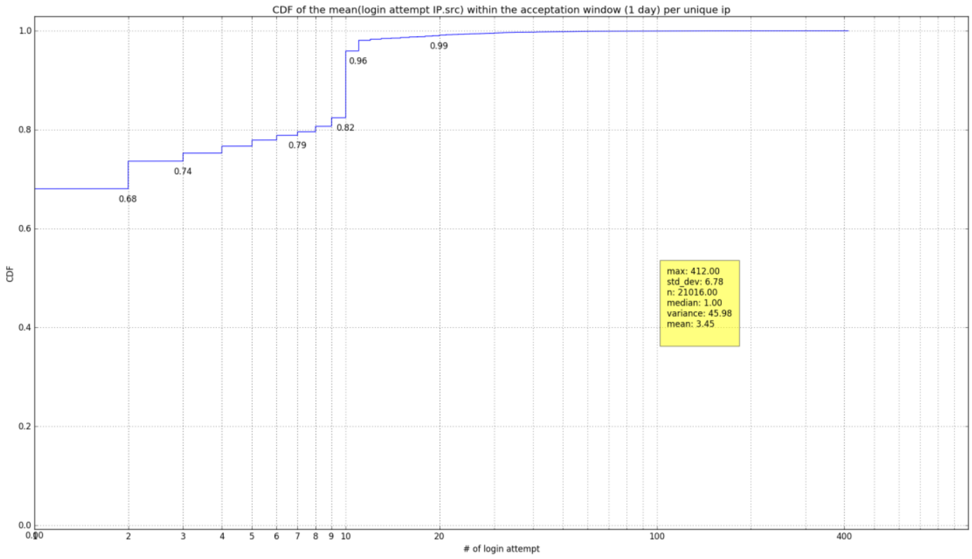


Figure 12: Distribution of mean login attempts

In Figure 12, the cumulative distribution function is represented, that shows the average amount of telnet log-in attempts per unique IP within a timeframe of 1 day. It can be seen that 68% of the IPs only try 1 time per day, while 74% of the IPs tries maximally 2 times per day to log in. An interesting observation is that there is a gap of about 14% between the 9th and the 10th attempts.

3.2 **Other malware observations**

The following paragraphs regroup some general observations that appeared while analysing the data sets.

3.2.1 Observations on Netis and Asus routers vulnerability

Table 1 shows the observed target ports from January 1st, 2014 until December 31st, 2016. Destination port 53413 and 9999 also often occur commonly. By digging deeper and after some general searches on the Internet, an explanation for the occurrence of the ports are the vulnerabilities detected in the Netis [port53413] and Asus [port9999] routers.

Frequency	**Port numbers**
17 040 164	**53413**
252 652	**9999**
11 087	534
7 188	54544
2 666	32764
1 810	5900
1 046	22
782	43413
200	29172
69	3074
25	23
22	53418

Table 1: Port distribution

In January 2015, a backdoor in Asus routers were detected, where a service listens on port 9999 for new device detection, but had the flaw that unauthenticated users were given root privileges.

A similar case is the observation of UDP packets for the port 53413. In the blackhole, UDP packets were extracted having in the payload the keywords ‘`wget`’ and ‘`http`’. These keywords are often used in the exploit code of Netis routers. The results are represented in Figure 13.

The y-axis uses a logarithmic scale and represents the unique number of IP addresses per day. Hence, the residual noise over the years is also visualized. The first packets were observed the first September 2014 which is very close to the disclosure date of the vulnerability in Netis routers. A typical assumption is that the infections will disappear over time expecting low residual noise such as it is observed close to the end 2015. However, on the 26th November 2015, the number of unique IP addresses exploded by a factor of 86. A similar event can be observed for April 14th 2016. Although, UDP packets can be easily spoofed, therefore we assume that vulnerabilities of network devices are attractive to attackers, even years after their announcements.

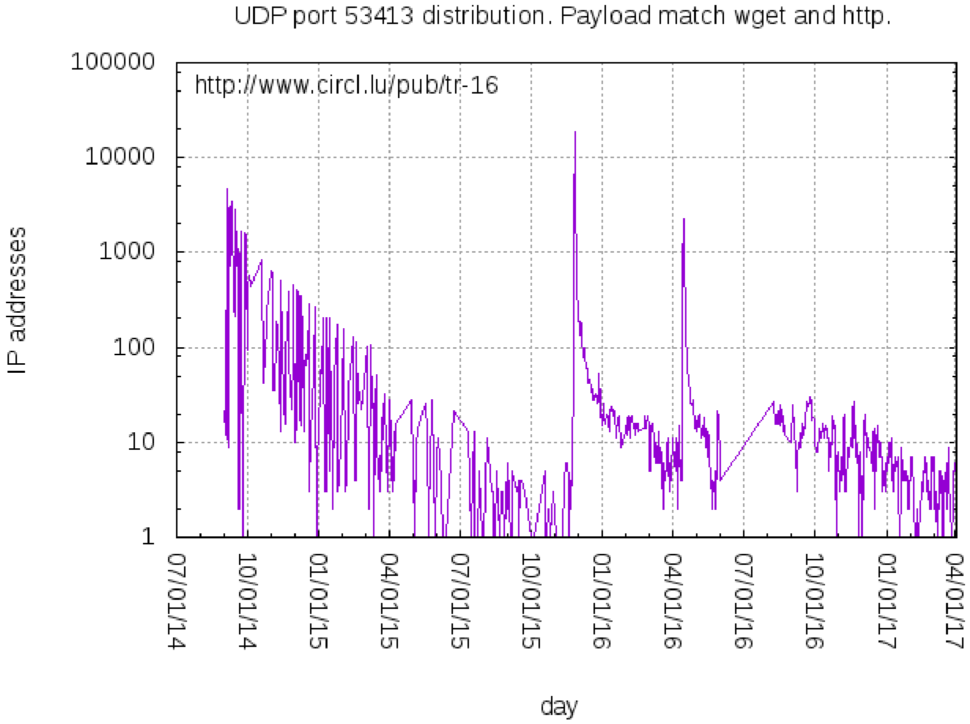


Figure 13: UDP Port 53413 distribution

3.2.2 Recent Mirai evolutions

In this paper we have shown that the overall activities of Mirai have not ceased, as can also be seen for example on the site of [MapMirai16], after the disclosure of its source code last year. Recently, new variants respectively evolutions of Mirai can be observed too. In February 2017, a new Mirai version was detected that referred to a Windows Trojan in order to spread [McMillen]. A particularity of this new version is that it has a built-in bitcoin mining module that enables attackers not only to perform DDoS attacks via the compromised devices, but also to improve their revenue by mining for bitcoins.

Another version of Mirai that appeared recently in April 2017 is the new Brickerbot [Brickerbot]. A particularity of this version is that it not only compromises devices but destroys them by performing permanent DoS (PDoS).

4. Conclusion

In this paper, it has been shown that by digging deeper into the blackhole traffic a lot of observations can be made on the behaviour of IoT malware types. As a future work it would interesting to perform a long-term analysis of these kinds of malware types in order to observe trends in the evolution. To this extend an analysis on all known Mirai bots/variants would be interesting, respectively to reverse, fingerprint them and set up a model to reproduce the historical attacks. To conclude this paper, Iot devices per se are devices that in most cases are installed once and then forgotten, since they perform their duty and do not ask for any maintenance next to the user.

A lot of users have IoT devices but do not know how to handle them adequately, respectively are naive on that point by estimating that the producer of such devices has integrated enough security to protect their privacy. These points ease the task of attackers to misuse the devices for their purposes. By design, IoT devices should be fast and cheap. This has as a major drawback on security.

Tackling security issues in IoT devices is not a straightforward task, since the origin of vulnerabilities are diversified, ranging from weakly implemented C code in the device itself to unsecured devices by with default passwords, as shown in the recent Mirai attacks.

In order to reduce impact on IoT devices respectively to inform about these threats in future, malware samples or reports should be shared within the cybersecurity, as for example by using MISP [Dulaunoy16], a threat intel sharing platform, that for example allows to import Mirai bot feeds and to share them within the security community.

Besides the technical aspects of security in IoT, more effort should also be put into user awareness, because users lack of most basis information about the devices they use. More effort should be put on user education on using their devices correctly and develop some basic reflexes for security.

Security in IoT devices should be implemented by default since the devices build the bridge between the physical and connected world for a user.

References

[Angrishi17]. Angrishi K. Turning Internet of Things into Internet of vulnerabilities: IoT Botnets. published on arXiv. Link: https://arxiv.org/abs/1702.03681. Last visited 03/01/2017.

[Any]. The Internet of Things 2012 New Horizons pdf file, page. Link: http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf, page 13.

[Ashton]. Ashton K. Link: https://en.wikipedia.org/wiki/Kevin_Ashton

[Bailey05-2]. Bailey M., Cooke E., Jahanian F., Nazario J. and Watson D., 2005. The Internet Motion Sensor - A Distributed Blackhole Monitoring System. In Proceedings of Network and Distributed System Security Symposium (NDSS ’05), pp. 167-179.

[Bhattasali13]. Bhattasali T., Chaki R. and Chaki N. 2013. Study of security issues in pervasive environment of next generation Internet of Things. IFIP CISIM 2013, LNCS 8104, pp.206-217.

[Bertino16]. Bertino E., 2016. Data security and privacy in the IoT. In Proceedings of the 19th International conference on Extending Database Technology (EDBT), Bordeaux, France, ISBN 978-3-89318-070-7.

[Brickerbot]. Radware ERT Threat Alert. April 2017. "Brickerbot results in Permanent Denial-of-Service". Link: https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/. Last visited: 04/11/2017.

[CiscoStats15]. Cisco Internet of Things. 2015. Last visited: 11/22/16, link: http://www.slideshare.net/Panduit/cisco-internet-of-things

[Dulaunoy14]. Dulaunoy A., Wagener G., Wagner C. and Stiefer M. 2014. The void - An interesting place for network security monitoring. In Proceedings of the 30th TERENA networking conference (TNC'14). Dublin, Ireland. ISBN 978-90-77559-24-6.

[Dulaunoy16]. Dulaunoy A., Wagner C., Wagener G. and Iklody A. 2016. MISP: The design and implementation of a collaborative threat intelligence sharing platform. ACM WISCS'16, Austria, pp.49-56.

[Duy15]. Duy Q., Quek T.Q.S., Lee J., Jin S. and Zhu H. 2015. Deceptive Attack and Defense Game in Honeypot-enabled Networks for the Internet of Things. IEEE Internet of Things Journal. DOI10.1109/JOIT.2016.2547994.

[Farina15]. Farina P., Cabmiaso E., Papaleo G. and Aiello M. 2015. Understanding DDoS attacks from mobile devices. 3rd International Conference on Future Internet of Things and Cloud.

[Furutani15]. Furutani N., Kitazono J., Ozawa S., Ban T., Nakazato J. and Shimamura J. 2015. Adaptive DDoS-Event Detection from Big Darknet Traffic Data. ICONIP 2015, Part IV, LNCS 9492, pp.376-383.

[Kliarksy17]. Kliarsky A. 2017. Detecting attacks against the "Internet of Things. SANS Institute InfoSec reading Room. Link: https://www.sans.org/reading-room/whitepapers/internet/detecting-attacks-039-internet-things-039-37712.

[He2016]. He H., Maple C., Watson T., Tiwari A., Mehnen J., Yaochu J. and Gabrys B. 2016. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. 2016 WCCI. IEEE Congress on evolutionary computation, Canada.

[IoTpot15]. Pa Pa Y. M., Suzuki S., Yoshioka K., Matsumoto T., Kasama T. and Rossow C. 2015. IoTPOT: analysing the rise of IoT compromises. In Proceedings of the 9th USENIX Conference on Offensive Technologies (WOOT'15). USENIX Association. Berkeley, CA, USA. 9-9.

[Jgamblin]. Mirai Source code. 2016. Link: https://github.com/jgamblin/Mirai-Source-Code/commit/43a57c77140d67e64f0b5a312a53ea1950f0a105. Last visited:03/30/2017.

[Kumar16]: P. Kumar, R.S. Kunwar, A. Sachan. 2016. A survey on: Security and Challenges in Internet of Things. IJRSD- National Conference on ICT and IoT.

[MorrisW88]. Litterio F. The Internet Worm of 1988. 1988. Last visited: 21/11/2016. Link: http://www.cs.unc.edu/~jeffay/courses/nidsS05/attacks/seely-RTMworm-89.html.

[MapMirai16]. Mapping Mirai, A botnet Case Study. Published on Malwaretech. October 3rd, 2016. Last visited: 11/21/2016, link: https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html.

[MiraiPort]. SANS ISC InfoSec Forum. Link: https://isc.sans.edu/forums/diary/UPDATED+x1+Mirai+Scanning+for+Port+6789+Looking+for+New+Victims+Now+Hitting+tcp23231/21833/

[MiraiScanner]. Mirai Scanner from Netlab 360.com. Link: http://data.netlab.360.com/mirai-scanner/

[MiraiDesc]. DDoS attack that disrupted internet was largest of his kind in history, experts say. Link: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet. Last visited: 04/11/2017.

[MiraiMap]. Mirai Map. Link: https://intel.malwaretech.com/botnet/mirai. Last visited: 04/11/2017.

[McMillen]. McMillen D., Alvarez M. 2017. Link: https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/ . Last visited: 04/13/2017.

[Markowsky15]. Markowsky L. and Markowsky G. 2015. Scanning for vulnerable devices in the Internet of Things. 8th IEEE International conference on Intelligent Data Aquisition and Advanced Computing Systems: Technology and Application, Poland.

[Medeiros10]. Medeiros J.P.S., Brito A.M.Jr. and Pires P.S.M. 2009. An effective TCP/IP fingerprinting technique based on strange attractors classification. DPM 2009 and SETOP 2009, LNCS 5939, pp.208-221.

[OP-Mirai16]. Nixon A., Costello J. and Wilson Z. 2016. An after-action analysis of the Mirai Botnet Attacks on Dyn. October 25, 2016. Last visited 11/21/2016, link: https://www.flashpoint-intel.com/action-analysis-mirai-botnet-attacks-dyn/.

[Perakovic15]. Perakovic D., Perisa M. and Cvitiv I. 2015. Analysis of the IoT impact on volume of DDoS attacks. XXXIII Simpozijum o novim tehnoloijama u postankom i telekomunikacionom soabracaju - PosTel2015. Beograd. 2015.

[port9999]. Asus vulnerability. Links: https://www.exploit-db.com/exploits/35688/ and https://github.com/jduck/asus-cmd . Last visited: 04/04/2017.

[port53414]. Netis vulnerability. Links: https://isc.sans.edu/forums/diary/Surge+in+Exploit+Attempts+for+Netis+Router+Backdoor+UDP53413/21337/ and http://www.securityweek.com/easily-exploitable-vulnerability-found-netis-routers . Last visited: 04/04/2017.

[Spitzner03]. Spitzner L. 2003. The honeynet project.: trapping the hackers. IEEE Security & Privacy, vol.1, no.2., pp. 15-23.

[Shimoda10]. Shimoda A., Tatsuya M. and Shigeki G. 2010. Sensor in the dark: Untraceable large-scale honeypots using virtualization technologies. 10th annual international symposium on applications and the Internet. SAINT, Korea.

[SouceMirai]. Source code of Mirai. 2016. Link: https://github.com/jgamblin/Mirai-Source-Code.

[Darknet]. The Darknet Project. Link: http://www.cymru.com/Darknet.

[Web16]. Dr. Web. Investigation of Linux.Mirai. Trojan family. 2016. Link: https://st.drweb.com/static/new-www/news/2016/september/Investigation_of_Linux.Mirai_Trojan_family_en.pdf . Last visited: 03/08/017.

[Wustrow10]. Wustrow E., Karir M., Bailey M., Jahanian F. and Huston G. 2010. Internet Background Radiation Revisited. In Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement (IMC '10), ACM, pp. 62-74.

[Zalweski01]. Zalweksi M. 2001. Strange attractors and TCP/IP sequence number analysis. Link: http://lcamtuf.coredump.cx/newtcp/ . Last visited: 03/01/2017.

[Zseby12]. Zseby T. and Claffy K. 2012. Workshop report: darkspace and unsolicited traffic analysis (DUST 2012). SIGCOMM Computer Communication Review 42, ACM, pp. 49-53.

[Zseby13]. Zseby T. 2013. IP Darkspace Analysis. Advances in IT early warning, Frauenhofer IRB Verlag, pp. 21-29.

Biographies

Alexandre Dulaunoy encountered his first computer in the eighties, and he disassembled it to know how the thing worked. While pursuing his logical path towards information security and free software, he worked as senior security network consultant at different places (e.g. Ubizen, now Cybertrust). He co-founded a startup called Conostix specialized in information security management, and the past 6 years, he was the manager of global information security at SES, a leading international satellite operator. He is now working at the national Luxembourgian Computer Security Incident Response Team (CSIRT) in the research and operational fields. He is also lecturer in information security at Paul-Verlaine University in Metz and the University of Luxembourg.

Sami Mokaddem is currently a second year Master student as Civil Engineer with specialization in Networking and Security at Louvain-La-Neuve University. He is going to finish his Master degree in June 2017. His research interests are network and system security.

Gérard Wagener holds a bi-national Ph.D. in computer science by the University of Luxembourg and INPL Nancy, France since 2011. He was working for 4 years in the global information security team at SES, a leading international satellite operator. He is currently working for the Computer Incident Response Center Luxembourg since 5 years. His doctoral research focuses on adaptive decoying systems to improve intelligence gathering on attackers in computer networks. Gérard comes from the malware research community, where he worked on projects such as sandboxes for monitoring and analyzing malicious software. In addition to these hands-down activities, his scientific work has investigated malware classification using phylogenetic trees and intelligent high-interaction honeypots driven by game theory. At CIRCL he is doing incident response and evidence analysis.

Cynthia Wagner holds a PhD in computer science from the University of Luxembourg, where she studied the effects on network monitoring and security by applying different kind of flow measurements. She actually is the representative for the Computer Security Incident Response Team (CSIRT) of the RESTENA Foundation, the national research and education network in Luxembourg. Besides this, she works in the team of the registry DNS-LU for the top-level domain .lu, where she is actively involved in research and development for security. Recently, she joined the Interdisciplinary Centre for Security, Reliability and Trust Center (SnT) Luxembourg as a research fellow in the SEDAN (Services and Data Management) group. In her spare time she likes to spend time in her garden and loves traveling.