IoT Botnet from 2008 to 2021

The following content is adopted from the PhD thesis of K.O. Chee [1].

We identified 55 IoT botnets from various sources (e.g., journals, conferences, forums, security white papers, security websites, etc.) ranging from 2008 to 2021. After carefully reviewing the information, we rearranged it according to when the malware was first discovered and briefly described their features and behaviours in the following. Figure 1 shows the timeline of botnets that appeared from 2008 to 2021.

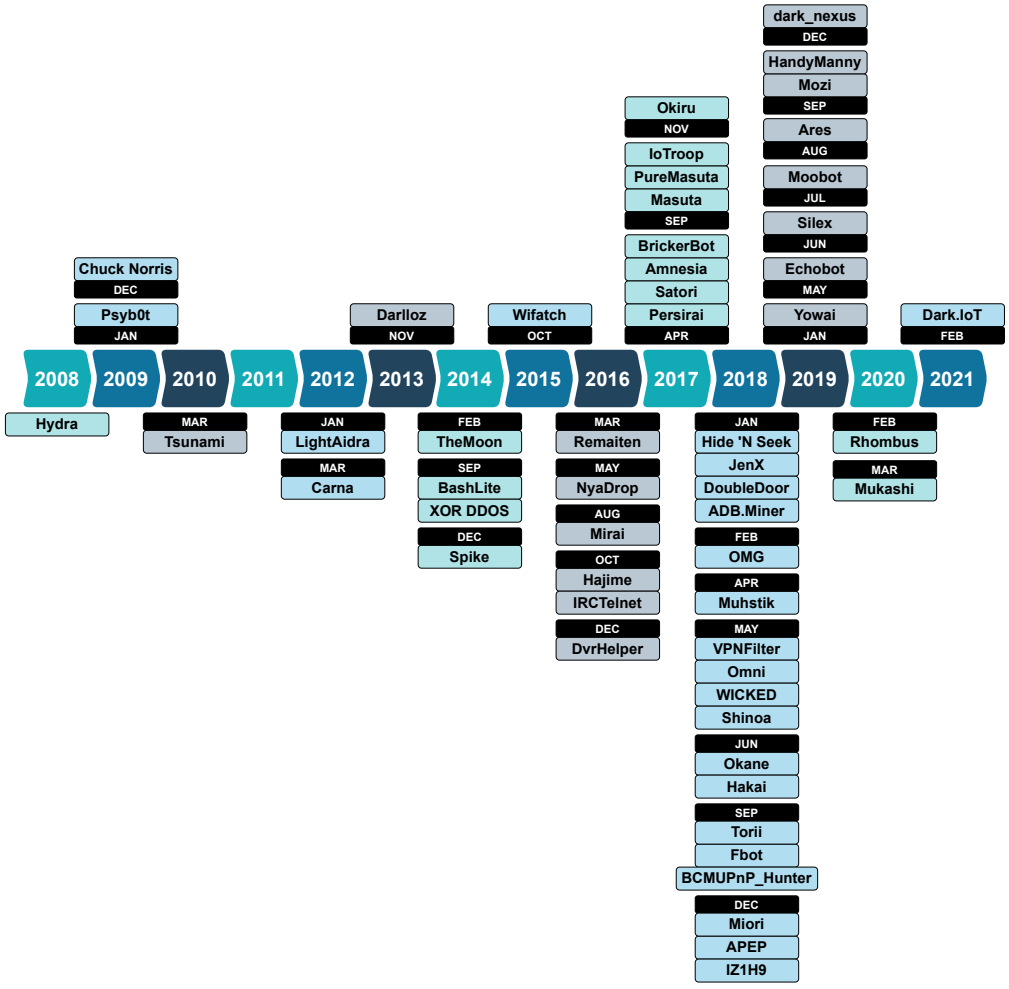

Figure 1: IoT Botnets spanning from 2008 to 2021.

1. *Hydra* [2, 3, 4]
   It was first seen in 2008 and is also known as Linux.Hydra. It is an IRC-based botnet framework that is publicly available to download. It was designed to utilise a list of default credentials to brute-force attack routers and spread like a computer worm. Also, it can bypass the D-Link router's authentication. Moreover, Hydra can launch a DDoS attack (e.g., SYN flood). It is targeting x86 and MIPSEL device architectures.

2. *Psyb0t* [5, 2, 3]
   Terry Baume first discovered it in January 2009, also known as Network BluePill. It is an IRC-based botnet and was considered the first IoT botnet in the wild. It utilises default credentials or authentication bypass techniques to compromise routers or modems. After gaining unauthorised access to the device, it uses the device shell to download the malware binary. The binary file is deleted after it is executed to run in the device memory. Also, this malware can set up the iptables rule to block access on multiple ports (i.e., 22, 23, 80). It employs several techniques to evade detection (e.g., single instance). The botmaster used this botnet to launch a DDoS attack (e.g., SYN flood, UDP flood, and ICMP flood) on the DroneBL website. After gaining public attention, the botmaster eventually shut the botnet down on 22 March 2009.
3. *Chuck Norris* [6, 2, 3]
   It was first discovered in December 2009. It is an IRC-based botnet and strongly resembles Psyb0t malware in the binary file. It utilises dictionary attacks with default credentials and can bypass authentication on D-Link routers. This botnet can launch several types of DDoS attacks (e.g., SYN flood, ACK flood, and UDP flood). It can block access on telnet (23) and HTTP (80) ports using the iptables rule. However, this malware does not persist with a device reboot.
4. *Tsunami* [2, 3, 7]
   It was first discovered in March 2010 and is also known as Kaiten. Tsunami is deemed as one of the variants of Hydra and also inherited some code from Chuck Norris and DDoS-Kaiten Trojan. It is an IRC-based botnet and can launch several types of DDoS attacks (e.g., SYN flood, PSH-ACK flood, UDP flood, HTTP flood, and XMAS flood). It utilises dictionary attacks with default credentials. Also, this malware can set up iptables rules to block access on multiple ports from 22 to 80.
5. *LightAidra* [8, 9, 3]
   It was first discovered in January 2012 and is also known as Aidra and Linux Aidra. It is an IRC-based botnet and is publicly available on GitHub. It utilises dictionary attacks with credential pair and can exploit a configuration reset bug on D-Link devices. This botnet can launch several types of DDoS attacks (e.g., SYN flood and ACK flood). However, this malware can be removed by a device reboot. LightAidra can search and remove Chuck Norris malware.
6. *Carna* [10, 11, 12]
   It was first discovered in March 2012. It was created by an anonymous hacker for the IPv4 address census. It utilises dictionary attacks with default credentials. This botnet does not launch any malicious attack and was set to terminate itself sometime later. During the propagation, the hacker found that some vulnerable devices were infected by Aidra malware and decided to set up an iptables rule to block telnet access to stop Aidra from compromising other devices. Carna can be removed by a device reboot.
7. *Darlloz* [13, 14, 15]
   It was first discovered in November 2013 and is also known as Linux.Darlloz. It can utilise dictionary attacks with credential pairs and exploit a PHP vulnerability (CVE-2012-1823) on unpatched devices. Also, Darlloz searches and removes LightAidra from the compromised device and blocks the telnet port to prevent LightAidra's reinfection. Later, in March 2014, a new version of Darlloz could mine crypto-currency using the compromised devices.
8. *TheMoon* [16, 17, 18, 19, 20, 21]
   Johannes B. Ullrich first discovered it in February 2014. It is a P2P-based botnet that targets Linksys routers by exploiting an unauthenticated remote code execution vulnerability. It then

uses a shell script to download the malware binary to the compromised device. Later, the botnet evolved to attack modems and routers from manufacturers (Asus, MicroTik, and D-Link) and GPON routers. TheMoon uses hardcoded IPs for C&C servers. Compromised devices are used as proxy servers. iptables rules were implemented to prevent other malware infections.

9. *BashLite* [22, 23, 24]
   Trend Micro first discovered it in September 2014. It is also known as Gafgyt, Lizkebab, Torlus, Qbot, and LizardStresser. It is an IRC-based botnet that utilises brute force attacks and exploits Shellshock vulnerability to gain unauthorised access. It can launch DDoS attacks (e.g., SYN and UDP floods). Later, a new variant was found, and devices running on BusyBox were exploited. Its source code was exposed in 2015.
10. *XOR DDOS* [25, 12]
    MalwareMustDie first discovered it in September 2014. It can utilise brute force attacks to gain unauthorised access. This malware can survive a device reboot by installing a trojan in the cron and init folders. Encryption and obfuscation techniques are used to avoid detection. This botnet can launch several types of DDoS attacks (e.g., SYN flood and UDP flood).
11. *Spike* [26, 27, 28]
    Akamai first discovered it in December 2014. It is also known as MrBlack, Dafloo, Wrkatk, Sotdas, and AES.DDoS. It is an IRC-based botnet that can launch several types of DDoS attacks (e.g., SYN flood, UDP flood, and HTTP GET flood). This botnet can survive device reboot by tampering */etc/rc.local*. Also, the bots can collect device data and send it to the C&C server.
12. *Wifatch* [29, 11, 12]
    It was first seen in October 2015 and is also known as Linux.Wifatch, Ifwatch, and REINCARNA. It is an open-source P2P-based botnet developed by a white hat with no malicious intent. Only the binaries are available in their GitLab repository to prevent any malicious utilisation of the source code. It can utilise dictionary attacks with default credentials.
13. *Remaiten* [30, 11, 12]
    ESET researchers first discovered it in March 2016. It is also known as KTN-RM, KTN-Remastered, and Linux/Remaiten. It is an IRC-based botnet that inherited the code from Tsunami and BashLite. It can utilise dictionary attacks with credential pairs. Remaiten has a slightly different propagation life cycle if compared with other botnets. Instead of downloading all binary executables for different architectures from C&C to the target device and trying to install them one by one to determine the correct architecture, Remaiten's bot determines the target device's architecture after accessing it successfully and transfers a suitable ELF executable to download the correct binary to the target device. The botnet has hardcoded the C&C server's IP address. Remaiten can kill other bots based on the blacklisted name. A shell script is used in a later version to download the bot binaries.
14. *NyaDrop* [31, 32]
    It was first discovered in May 2016. NyaDrop uses brute force attacks with default credential pairs to attack only MIPS-based IoT devices. After successful login to the target device, a small executable is dropped to the target device to install a backdoor. Via the backdoor, the malware can connect with the C&C server to download the Nya trojan only if the IoT device is MIPS-based. Otherwise, the real malware binary is not installed on an incompatible device.
15. *Mirai* [33, 34, 35, 36]
    MalwareMustDie first discovered it in August 2016. At first, Mirai malware scans pseudorandom

IPv4 addresses with open ports on 23 and 2323. Once the target device is detected, it utilises brute force attacks with default credential pairs to gain unauthorised access to the target device. Each time, ten credential pairs are selected to try for the login phase from a list of 62 pairs of default credentials. Once login is successful, Mirai malware sends a report consisting of the IP address, port number, and credential pair to a report server. Then, a loader server is responsible for establishing a connection and logging in to the target device using the information received earlier. After checking the system environment and architecture, a compatible malware binary is downloaded and installed on the target device. To evade detection, the malware binary is removed after execution, and its process name is changed to a pseudorandom string. Due to the malware only existing in the device memory, the malware is deleted when the device reboots. However, a reboot does not prevent the device from being reinfected by Mirai. Also, Mirai finds and removes processes from competitors (e.g., other Mirai variants, .anime, and Qbot). Moreover, Mirai fortifies itself by closing port 23 and port 2323 to prevent competitors from entering the compromised device via the same ports. Mirai is capable of launching ten types of DDoS attacks (e.g., SYN flood and UDP flood, HTTP flood, UDP-PLAIN flood, ACK flood, GRE-IP flood, GRE-ETH flood, ACK-STOMP flood, VSE flood, and DNS flood). Multiple damaging DDoS attacks were launched against targets such as OVH, Krebs on Security, Dyn, Liberia's Lonestar Cell, and Deutsche Telekom in the first four months since its discovery. After the author released Mirai's source code in a forum, countless new botnets based on Mirai emerged and competed with each other to harvest IoT devices globally.

16. *Hajime* [37, 38, 39]
    RapidityNetworks first discovered it in October 2016. It is a P2P-based botnet. It was claimed to be benevolent by its developer. Hajime's propagation life cycle contains three stages. The first stage is scanning and accessing; the second stage is downloading the first binary; the third stage is downloading the second binary and establishing a connection with its P2P network. After the third stage, it will repeat the life cycle to compromise other targets.
17. *IRCTelnet* [40, 41, 11]
    It was first discovered in October 2016 and is known as NewAidra and LinuxIRCTelnet. It is an IRC-based botnet that inherited the code from Tsunami, LightAidra, BashLite, and Mirai. It can launch DDoS attacks (e.g., SYN and UDP floods). Moreover, IRCTelnet can scan and attack devices with IPv6 addresses. It utilises Mirai's credential list in dictionary attacks on vulnerable IoT devices.
18. *DvrHelper* [19, 42]
    Security Artwork first discovered it in December 2016. It is a variant of Mirai malware and can launch DDoS attacks with at least eight different modules. The author has added two methods to bypass DDoS mitigation. The first method can defeat the challenge-response authentication by generating the answer in the C&C server using embedded JavaScript code. The second method is utilising a shared "Google reCAPTCHA response" token to bypass the DDoS protection on the target server.
19. *Persirai* [19, 43, 12]
    It was first discovered by Trend Micro in April 2017. Although Persirai is a variant of Mirai malware and inherited most of the codes, several key differences are found in Persirai. First, Persirai gains unauthorised access by exploiting software vulnerabilities (e.g., authentication bypass and CVE-2014-8361) on IP cameras instead of brute force attacks. After that, it will connect with a website to download the shell script. Multiple binaries of different architectures

are downloaded and executed using the shell script. Binaries are deleted after execution. Then, it will patch the vulnerability on the device to prevent others from exploiting it. Persirai is capable of launching DDoS attacks (e.g., UDP flood).

20. *Satori* [44, 45, 46, 47, 48, 49, 50, 51, 52, 53]
    It was first discovered by Unit 42 in April 2017. Satori is a variant of Mirai malware. It was developed by *NexusZeta* and has six different versions. Each version contains different modifications and additions from the author. Additional exploits are added to the later variants. The first version is similar to Mirai, using brute force attacks to gain unauthorised access to vulnerable devices and installing malware binary afterwards. The second version utilises the packer technique to mask its malicious code to evade detection and added a new password ("aquario") to target vulnerable routers in South America. Okiru is considered the third version of Satori. This version has added software vulnerability exploitation methods targeting CVE-2017-17215 and CVE-2014-8361. The fourth version is dubbed Satori.Coin.Robber because it hacks into Claymore Miner hosts and replaces the mining wallet address with its address to steal the crypto-currency. The fifth version was found in May 2018 for exploiting GPON vulnerability (i.e., CVE-2018-10561 and CVE-2018-10562). The sixth version exploits the vulnerability of XiongMai uc-httpd 1.0.0 (CVE-2018-10088) and the D-Link DSL-2750B device. Also, this version of Satori carries four DDoS attack methods (e.g., UDP flood, SYN flood, ACK flood, and GRE flood).
21. *Amnesia* [54, 12]
    It was first discovered by Unit 42 in April 2017. It is an IRC-based botnet that inherited the code from Tsunami. This malware exploits a remote code execution (RCE) vulnerability in IoT devices. It can launch two types of DDoS attacks (e.g., UDP flood and HTTP flood). Moreover, Unit 42 researchers claimed that this malware is the first Linux malware to evade analysis in a virtual machine environment by deleting its binary when detected in a virtual machine. This malware can survive a device reboot by implanting files in multiple locations during installation. In addition, this malware would remove any process that runs on telnet and SSH ports.
22. *BrickerBot* [55, 56, 57]
    It was first discovered by Radware in April 2017. It is a unique botnet that aims to brick vulnerable IoT devices susceptible to Mirai malware attacks using permanent denial-of-service (PDoS) attacks. Like Mirai, it uses brute force attacks with default credentials to gain unauthorised access to vulnerable IoT devices. After successful access, it does not download its binary but quickly performs a series of commands to destroy the vulnerable device's firmware, storage, settings, and network configurations. After that, it forces the device to reboot into a brick state. The malware's author, The janit0r, claimed that he wanted to reduce the bots being utilised for DDoS attacks and create awareness to show that the insecurity in IoT devices is fatal and worrying.
23. *Masuta & PureMasuta* [58]
    Masuta was first discovered in September 2017, and it is a variant of Mirai malware. It was developed by *NexusZeta*, which is also the author of Satori. It utilises dictionary attacks with several credential pairs. PureMasuta is the evolved version of Masuta. Like its previous version, PureMasuta also utilises dictionary attacks with several credential pairs. However, PureMasuta can exploit a software vulnerability (EDB 38722 D-Link HNAP) and bypass authentication. Moreover, PureMasuta utilises a shell script to download malware binary from the C&C server to the target device.

24. *IoTroop* [59, 60, 61, 62]
    It was first discovered in September 2017 and is also known as IoT_reaper, IoTrooper, and Reaper. It is a variant of Mirai malware. However, IoTroop contains several differences if compared with Mirai. IoTroop does not utilise brute force attacks but exploits nine software vulnerabilities. There is no DDoS attack command in IoTroop. Moreover, it employs multiple ways to evade detection, such as hiding the process name, maintaining a single instance, and obfuscation. Also, it can prevent the device from rebooting for persistence. Furthermore, it can find and kill any process that uses port 23 and any process that contains specific strings on the process name.
25. *Okiru* [53, 63, 64, 46, 44, 65]
    It was first discovered in November 2017 and can be considered the third version of Satori. It is a variant of Mirai malware. It has two different versions. The first version exploits Huawei HG532 home routers and Realtek devices, and the second version targets ARC CPU (Argonaut RISC Core central processing unit).
26. *Hide 'N Seek* [66, 67, 68, 69]
    Bitdefender first discovered it in January 2018 and is also known as HNS. It is a P2P-based botnet that utilises a custom P2P protocol. At the beginning of the accessing phase, this bot tries to find a specific banner ("buildroot login:") on the target device and uses specific credential pairs to log in if found before utilising dictionary attacks with other credential pairs. Once a successful login is made, the bot uses different methods to download the malware binary based on the device location. In the early version, this malware is terminated if the device reboots. Later, in May 2018, the malware was upgraded and could copy itself to the init and rc folders to survive a device reboot. It can remove other competitors during setup and fortify the new bot with iptables rules on specific ports. HNS does not perform any DDoS attack, but can retrieve and transfer files from the compromised device for data exfiltration. Crypto-mining is another objective of HNS. Also, FortiGuard Labs found that HNS has added multiple exploits for software vulnerability from January to July 2018 in different malware versions.
27. *JenX* [70, 71, 72, 7]
    Radware first discovered it in January 2018, and it is also known as Jennifer and Jen-X. It is based on the BrickerBot source code. JenX prefers to exploit software vulnerabilities (e.g., CVE-2014-8361 and CVE-2017-17215). Unlike other botnets, JenX utilises servers instead of bots to scan and access vulnerable devices. Centralised scanning brings several benefits to this malware, although the growth of the botnet is significantly limited. First, bots create less noise and consume fewer resources because they no longer perform the scan and access tasks. The bot binary is less complicated and easy to deliver. The scan and access function code is easier to develop and implement when it resides in the C&C server. Also, it is harder for security researchers to detect, analyse, and estimate the botnet. The main objective of JenX is to provide the DDoS attack as a service.
28. *DoubleDoor* [73, 74, 75]
    NewSky Security first discovered it in January 2018. It utilises two known software exploits (CVE-2015-7755 and CVE-2016-10401) to bypass firewall authentication and gain control of the target device. This malware uses polymorphism in a scanning phase by using a randomised string. The purpose of this malware is not discussed in the report.
29. *ADB.Miner* [76, 77]
    It was first discovered by 360Netlab in January 2018. It uses Mirai's scanning module to target

Android-based IoT devices with an open port 5555 for Android Debug Bridge (ADB) service. It propagates like a worm by cloning its binary from a compromised device to a new target device. This malware is used for crypto-mining and does not have a C&C server. It installs files in multiple directories in the compromised device to ensure its persistence against reboot.

30. *OMG* [78, 79]
    It was first discovered by FortiGuard Labs in February 2018, and it is a variant of Mirai malware. OMG has all the basic functionalities of Mirai malware, including scanner, attack, and killer modules. Moreover, OMG can turn the compromised device into a proxy server by utilising 3proxy.
31. *Muhstik* [80, 81, 82, 83]
    It was first discovered by 360Netlab in April 2018. It is an IRC-based botnet which is also one of the Tsunami's variants. It can perform DDoS attacks and crypto-mining. Initially, it is exploiting a Drupal vulnerability (CVE-2018-7600). Later, multiple exploits are added to this malware, including those that target GPON (CVE-2018-10561 and CVE-2018-10562), JBOSS (CVE-2007-1036) and DD-WRT (Web Authentication Brute Forcing). In December 2019, Unit 42 researchers reported that a new Muhstik version targeted routers that used Tomato firmware. In November 2021, Sysdig Security researchers discovered that the Muhstik botnet harvested Kubernetes Pod to mine cryptocurrency. It can survive a device reboot by adding malware binary into multiple directories in the compromised device.
32. *VPNFilter* [84, 85, 12]
    Talos first reported it in May 2018. VPNFilter is a unique malware with multi-stages of modules and modular design. It has the objective to exfiltrate data or sabotage the compromised device. The exploitation method is not available in the report. The stage 1 module is tasked to download the stage 2 module and maintain the persistence of the stage 1 module. Stage 2 module runs predefined functions, including sabotaging the device, collecting and transferring data to the C&C server, rebooting the device, setting up proxy URL and port, etc. Stage 3 can use plugin modules on the malware to enhance its functionalities, such as packet sniffer, Tor communication tool, etc.
33. *Omni* [86, 87, 51]
    NewSky Security first discovered it in May 2018 and it is a variant of Mirai malware. It is closely related to several botnets (i.e., Owari, Sora, WICKED). Initially, Omni exploits two software vulnerabilities, CVE-2018-10561 (authentication bypass) and CVE-2018-10562 (command injection), on Dasan GPON routers. Later, in July 2018, 11 exploits were added to Omni malware. Omni does not use dictionary attacks like the Mirai botnet. Omni can set up multiple iptables rules to block access on specific ports on the compromised device.
34. *WICKED* [88, 79]
    It was first discovered by FortiGuard Labs in May 2018, and it is a variant of Mirai malware. WICKED uses four known software vulnerability exploits to compromise IoT devices instead of utilising dictionary attacks. Moreover, this malware is closely related to Omni, Owari, and Sora botnets.
35. *Shinoa* [89]
    It was first discovered by FortiGuard Labs in May 2018, and it is a variant of Mirai malware. It is closely related to the Miori botnet. Three DDoS attack methods (i.e., DNS resolver flood, TCP Stomp flood, and HTTP flood) are removed, and two new methods (i.e., XMAS flood and LYNX flood) are added if compared with Mirai botnet.

36. *Okane* [87]
    It was first reported by Unit 42 in June 2018, and it is a variant of Mirai malware. It can utilise brute force attacks with credential pairs and 11 software vulnerability exploits to compromise IoT devices. It can launch several types of DDoS attacks (e.g., UDP-GAME flood, STD flood, XMAS flood, ASYN flood, TCP Frag flood, TCP All flood, and TCP USYN flood).
37. *Hakai* [87, 90, 91, 92, 93]
    NewSky Security first discovered it in June 2018 and it is a variant of the BashLite malware but also contains some code from the Mirai botnet. It utilises software vulnerability exploits and brute force attacks to compromise IoT devices. It can launch several types of DDoS attacks (e.g., TCP flood, UDP flood, HTTP flood, and STD flood). Later, Intezer's researchers found that two variants (Kenjiro and Izuku) were spawned from the Hakai botnet.
38. *Torii* [94, 95]
    Avast first discovered it in September 2018. It utilises dictionary attacks with credential pairs. Torii is a unique and complex malware. It utilises a shell script to determine the target device architecture and download the suitable payload. However, there are two payload stages: a dropper and the real binary. Obfuscation is used on the dropper. The main function of the dropper is to download the real binary and install it in a pseudo-random location. Also, six ways are used to ensure the malware binary can survive the device reboot. The second payload, which is the real binary, has multiple features (e.g., anti-analysis methods, data exfiltration, multi-level encryption of communication, etc.) other than the basic botnet functionalities. Moreover, Torii does not perform DDoS attacks.
39. *Fbot* [96, 97, 98]
    It was first discovered by 360Netlab in September 2018, and it is a variant of Mirai malware. However, Fbot is utilising an exploit that targets ADB service to compromise the device. Also, it uses a shell script to download malware binary. Moreover, this malware specifically searches and removes com.ufo.miner, a variant of ADB.Miner intended for crypto-mining. Also, it finds and kills processes that contain specific strings on their name. It has the DDoS attack modules from the Mirai botnet. The author of this malware is *NexusZeta*. In February 2019, a new zero-day exploit was added to this malware to attack HiSilicon DVR/NVR devices. In February 2021, a new exploit (CVE-2020-9020) was used by this malware to compromise IoT devices from Iteris.
40. *BCMUPnP_Hunter* [99]
    It was first discovered by 360Netlab in September 2018. This botnet begins the infection by sending a TCP SYN scan to port 5431. Once the target responds, the bot checks for UDP port 1900 on the target device. Then, the bot uses a vulnerability scan to approach the target device for Broadcom UPnP vulnerability and sends the target device information to the loader server once the information is retrieved. The loader server picks the correct exploit and shell code to access the target device. Once it successfully accesses the device, the shellcode is executed to download the malware binary. The infection is completed once the malware is installed on the target device. According to the report, the botmaster utilises the botnet as a proxy network service to send spam, simulate clicks, etc.
41. *Miori* [100, 101, 102]
    Trend Micro first discovered it in December 2018, and it is a variant of Mirai malware. Besides dictionary attacks with credential pairs, Miori also spreads by exploiting a remote code execution (RCE) vulnerability in the ThinkPHP framework. Also, it can prevent the device from rebooting

for persistence.

42. *APEP* [100]
    Trend Micro first reported it in December 2018, and it is a variant of Mirai malware. Besides dictionary attacks with credential pairs, APEP also spreads by exploiting CVE-2017-17215 on Huawei HG532 routers. There is not much information related to this malware.
43. *IZ1H9* [100]
    Trend Micro first reported it in December 2018, and it is a variant of Mirai malware. It utilises dictionary attacks with several credential pairs. There is not much information related to this malware.
44. *Yowai* [91]
    Trend Micro first discovered it in January 2019, and it is a variant of Mirai malware. It can perform dictionary attacks with several credential pairs and exploit software vulnerabilities to compromise IoT devices. The vulnerabilities exploited by this botnet include ThinkPHP vulnerability, CVE-2014-8361, Linksys RCE, CVE-2018-10561, and CCTV-DVR RCE. Yowai malware has a long blacklist to search and terminate other competing botnets.
45. *Echobot* [103, 104, 105, 106, 107]
    It was first discovered by Unit 42 in May 2019, and it is a variant of Mirai malware. At the beginning of this malware discovery, this Echobot malware carried 18 exploits (8 were new additions and could not be found in Mirai at that time). Moreover, this malware can utilise dictionary attacks with credential pairs like Mirai (including several new credential pairs not found in Mirai's credential list). In June 2019, a newer version of Echobot was found to utilise 26 different exploits to compromise IoT devices and target the Oracle WebLogic server and VMware SD-WAN (networking software). After that, another new version of Echobot was detected in August 2019, which could carry 61 exploits. In December 2019, Echobot was upgraded again to carry 71 exploits and be able to target SCADA systems. Echobot downloads and executes a bash script (dropper) named "Richard" once it accesses the target device successfully. The bash script downloads and executes 13 malware binaries for different architectures. Echobot can launch 11 types of DDoS attacks (e.g., SYN flood, XMAS flood, ACK flood, TCP-STOMP flood, UDP-GENERIC flood, UDP-PLAIN flood, UDP-DNS flood, VSE flood, GRE-ETH flood, GRE-IP flood and STD flood).
46. *Silex* [108]
    It was first discovered by Akamai in June 2019. Like BrickerBot, Silex malware is intended to PDoS the compromised device by corrupting the compromised device's storage, dropping the iptables rules, removing all network settings, and rebooting the device into an unusable state. The author of this malware does not seek financial benefits when attacking IoT devices. Silex malware utilises dictionary attacks with default credential pairs to gain unauthorised access to vulnerable devices. This malware does not perform DDoS attacks.
47. *Moobot* [109, 110, 111]
    It was first discovered by 360Netlab in July 2019, and it is a variant of Mirai malware. Moobot malware utilises Mirai's scanning module to identify and access target devices. Then, the credential information of the target device is reported to the report server. The loader server accesses the target device and downloads the malware binary. The binary is executed to complete the infection. Unlike Mirai malware, Moobot scans many ports, which include 34567 (DVRIP), 5555 (ADB), 80 (HTTP) and 23 (telnet). According to the report, the bots share the scan results after scanning different ports simultaneously. For DVRIP vulnerability, Moobot can gain access

using default credentials and upload a fake upgrade file via the DVRIP upgrade interface. The fake upgrade file contains a shell command to open a backdoor on the vulnerable IoT device. The loader server then downloads and installs the malware binary via the backdoor. Later, in December 2021, a new version of Moobot was found to be exploiting Hikvision products via a command injection attack. Moobot can launch several types of DDoS attacks (e.g., SYN flood, UDP flood, ACK flood, and ACK-PUSH flood).

48. *Ares* [112, 113]
    WootCloud Threat Research Labs first discovered it in August 2019, and it is a variant of Mirai malware. Ares botnet is another malware that exploits ADB service on Android-based IoT devices. Ares malware scans for TCP port 5555 to identify the IoT device that runs the ADB service. Once the vulnerable device is detected, the Ares bot can send a copy of the malware binary to the vulnerable device via ADB service. Moreover, Ares malware can utilise brute force attacks with credential pairs to compromise other IoT devices without the ADB service. Ares bot is disguised as an ADB binary in the compromised device.
49. *Mozi* [114, 115, 116]
    It was first discovered by 360Netlab in September 2019. It is a P2P-based botnet that utilises DHT protocol with ECDSA384 and xor algorithm. Mozi can compromise IoT devices via brute force attacks or software vulnerability exploitation. Mozi can launch DDoS attacks (e.g., HTTP flood, SYN flood, UDP flood, etc.) and retrieve bot information. Mozi reused some code from the BashLite botnet to gain some evasion and suppression functionalities, such as remaining as a single instance, changing the process name, and modifying the access control list (ACL).
50. *HandyManny* [109]
    It was first discovered by 360Netlab in September 2019. HandyManny malware is identical to BrickerBot and Silex, which aims to sabotage the vulnerable device with a PDoS attack.
51. *dark_nexus* [117]
    Bitdefender first discovered it in December 2019. dark_nexus malware contains some code from BashLite malware and Mirai malware. The author of this malware updated the malware frequently during the active period of 3 months. dark_nexus malware uses two styles of propagation (synchronous and asynchronous). The bot utilises brute force attacks with credential pairs or software vulnerability exploits to gain unauthorised access to the target device. In synchronous style, the bot can send the retrieved information (credential data and IP address of the target device) to the report server and send the malware binary to the target device directly (similar to worm behaviour). On the contrary, in the asynchronous style, the bot sends the information to the report server. The loader server or C&C server accesses the target device with the credential information and installs the malware binary. dark_nexus utilises a single instance and changes the process name to evade detection. Also, it prevents the compromised device from rebooting by disabling the watchdog or stopping the cron service. dark_nexus can launch several types of DDoS attacks (e.g., UDP flood, HTTP flood, SYN flood, browser_http_req flood, etc.). This malware makes its DDoS attack traffic look like benign browser traffic when launching a DDoS attack on the target server. Moreover, dark_nexus utilises a weighting score system to determine which process to terminate, and this competing malware process removal function is executed periodically.
52. *Rhombus* [118, 119, 120, 121]
    It was first discovered by 0xrb and reported by MalwareMustDie in February 2020. It is a variant of Mirai malware. Like Mirai, Rhombus uses brute force attacks with credential pairs to

compromise vulnerable IoT devices. A dropper is implanted into the target device as the stage 1 payload. This dropper can modify the crontab and add a shell script to ensure its persistence by executing the script every hour. The script downloads another shell script and executes it. The second script creates a backdoor for the botmaster and downloads a stage 2 payload, the malware binary. Rhombus can launch several types of DDoS attacks (e.g., UDP flood, SYN flood, GRE flood, and HTTP flood).

53. *Mukashi* [122, 123]
    It was first discovered by Unit 42 in March 2020, and it is a variant of Mirai malware, which also inherited code from the DvrHelper botnet. Initially, Mukashi uses dictionary attacks with credential pairs to compromise IoT devices. After CVE-2020-9054 was exposed to the public, the author of Mukashi quickly equipped the malware with the software exploit and used it to harvest vulnerable Zyxel network-attached storage (NAS) devices. Like Mirai, Mukashi reports the credential information to its C&C server once the login is successful. However, a shell script is downloaded to the target device to determine and download the correct binary. After the infection is completed, Mukashi ensures that only a single instance is running and changes its process name to "dvrhelper". Obfuscation is used to encrypt commands and credential lists stored in the binary. Like Mirai malware, Mukashi can launch several types of DDoS attacks (e.g., UDP flood, SYN flood, UDP bypass, and TCP bypass). Also, Mukashi inherited the anti-DDoS defence techniques from DvrHelper too.
54. *Dark.IoT* [124, 125, 126]
    It was first discovered by Unit 42 in February 2021, and it is a variant of Mirai malware. Dark.IoT can utilise dictionary attacks with credential pairs stored in a text file or software exploits to compromise IoT devices. Similar to Rhombus, there are two shell scripts for two stages. However, the scripts work a little bit differently here. The first script can download malware binaries once it removes several key folders from the target device. Only the suitable binary can be executed on the target device. Then, the script creates a new scheduled job and runs every hour to maintain persistence. iptables rules are created to block access on SSH, HTTP and telnet ports. The second script is downloaded to install a binary for brute force attacks and a text file that contains a credential list. In a later version, the brute force attack binary is removed. Dark.IoT has a long blacklist of competitor malware to terminate. Dark.IoT can launch several types of DDoS attacks (e.g., UDP-GENERIC flood, UDP-PLAIN flood, UDP-GAME flood, UDP-DNS flood, TCP-ALL flood, TCP-FRAG flood, SYN flood, ACK flood, TCP-USYN flood, A-SYN flood, GRE-IP flood, STD flood, and HTTP flood).

References

[1] K. O. Chee, Security modelling and analysis of internet of things against evolving attacks, PhD Thesis (2024). doi:10.14264/39c3456.

[2] M. Janus, Heads of the Hydra. Malware for Network Devices, accessed on 23 September 2022 (2011).
URL https://securelist.com/heads-of-the-hydra-malware-for-network-devices/36396/

[3] M. De Donno, N. Dragoni, A. Giaretta, A. Spognardi, Ddos-capable iot malwares: Comparative analysis and mirai investigation, Security and Communication Networks 2018 (2018) 1–30.

[4] P. Mcgregor, Hydra IRC bot, the 25 minute overview of the kit., accessed on 23 September 2022 (2018).
URL http://insecurety.net/hydra-irc-bot-the-25-minute-overview-of-the-kit/

[5] Nenolod, Network Bluepill - stealth router-based botnet has been DDoSing dronebl for the last couple of weeks, accessed on 23 September 2022 (2009).
URL https://www.dronebl.org/blog/8

[6] P. Čeleda, R. Krejčí, J. Vykopal, M. Drašar, Embedded Malware - An Analysis of the Chuck Norris Botnet, in: 2010 European Conference on Computer Network Defense, 2010, pp. 3–10. doi:10.1109/EC2ND.2010.15.

[7] S. Hilt, F. Mercês, M. Rosario, D. Sancho, Worm War: The Botnet Battle for IoT Territory, accessed on 3 October 2022 (2020).
URL https://documents.trendmicro.com/assets/white_papers/wp-worm-war-the-botnet-battle-for-iot-territory.pdf

[8] F. Fazzi, K. Kirsche, Lightaidra, online; Accessed on 3 October 2022 (2015).
URL https://github.com/ociredefz/lightaidra

[9] New Jersey Cybersecurity & Communications Integration Cell (NJCCIC, Aidra Botnet - NJCCIC Threat Profile, accessed on 3 October 2022 (2016).
URL https://www.cyber.nj.gov/threat-center/threat-profiles/botnet-variants/aidra-botnet

[10] Carna Botnet, Internet Census 2012 - Port scanning /0 using insecure embedded devices, accessed on 3 October 2022 (2012).
URL https://census2012.sourceforge.net/paper.html

[11] K. Angrishi, Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets, arXiv preprint arXiv:1702.03681 (2017). doi:10.48550/arXiv.1702.03681.

[12] B. Vignau, R. Khoury, S. Hallé, A. Hamou-Lhadj, The evolution of IoT Malwares, from 2008 to 2019: Survey, taxonomy, process simulator and perspectives, Journal of Systems Architecture 116 (2021) 102143. doi:10.1016/j.sysarc.2021.102143.

[13] Broadcom, Linux Worm Targeting Hidden Devices, accessed on 4 October 2022 (2013).
URL https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=6cc8a697-5c01-45ba-ad5c-599eee0a4678&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[14] Broadcom, The Internet of Things: New Threats Emerge in a Connected World, accessed on 4 October 2022 (2014).
URL https://community.broadcom.com/symantecenterprise/communities/community-

home/librarydocuments/viewdocument?DocumentKey=8f00b02f-e843-4156-af87-bfa817249ec8&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[15] Broadcom, IoT Worm Used to Mine Cryptocurrency, accessed on 4 October 2022 (2014).
URL https://community.broadcom.com/symantecenterprise/viewdocument/iot-worm-used-to-mine-cryptocurrenc?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[16] Ullrich, J. B., Linksys Worm ("TheMoon") Captured, accessed on 4 October 2022 (2014).
URL https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Captured/17630

[17] Ullrich, J. B., Linksys Worm "TheMoon" Summary: What we know so far, accessed on 4 October 2022 (2014).
URL https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Summary+What+we+know+so+far/17633

[18] Liu, B., TheMoon - A P2P botnet targeting Home Routers, accessed on 4 October 2022 (2016).
URL https://www.fortinet.com/blog/threat-research/themoon-a-p2p-botnet-targeting-home-routers

[19] K. Lu, T. Yeh, D. Chiu, The Reigning King of IP Camera Botnets and its Challengers, accessed on 28 Aug 2019 (2017).
URL https://blog.trendmicro.com/trendlabs-security-intelligence/reigning-king-ip-camera-botnets-challengers/

[20] H. Wang, Rootkiter, G. Ye, GPON Exploit in the Wild (IV) - TheMoon Botnet Join in with a 0day(?), accessed on 4 October 2022 (2018).
URL https://blog.netlab.360.com/gpon-exploit-in-the-wild-iv-themoon-botnet-join-in-with-a-0day/

[21] Black Lotus Labs, A New Phase of TheMoon, accessed on 4 October 2022 (2019).
URL https://blog.lumen.com/a-new-phase-of-themoon/

[22] Trend Micro, ELF_BASHLITE.A, accessed on 4 October 2022 (2014).
URL https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/elf_bashlite.a

[23] Trend Micro, ELF_BASHLITE.SMB, accessed on 4 October 2022 (2014).
URL https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ELF_BASHLITE.SMB

[24] Paganini, P., A new variant of the BASHLITE malware exploiting the ShellShock vulnerability was used by cyber criminals to infect devices that use BusyBox software, accessed on 4 October 2022 (2014).
URL https://securityaffairs.co/wordpress/30225/cyber-crime/bashlite-exploits-shellshock.html

[25] unixfreaxjp, MMD-0028-2014 - Linux/XOR.DDoS : Fuzzy reversing a new China ELF, accessed on 4 October 2022 (2014).
URL https://blog.malwaremustdie.org/2014/09/mmd-0028-2014-fuzzy-reversing-new-china.html

[26] Paganini, P., Spike botnet runs DDoS attacks from IoT devices, accessed on 4 October 2022 (2014).
URL https://securityaffairs.co/wordpress/28642/cyber-crime/spike-botnet-runs-ddos.html

[27] Bohio, M. J., Analyzing a Backdoor/Bot for the MIPS Platform, accessed on 4 October 2022 (2015).
URL https://www.sans.org/white-papers/35902/

[28] I. Zeifman, R. Atias, O. Gayer, Lax Security Opens the Door for Mass-Scale Abuse of SOHO Routers, accessed on 4 October 2022 (2015).
URL https://www.imperva.com/blog/ddos-botnet-soho-router/

[29] The White Team, linux.wifatch, online; Accessed on 4 October 2022 (2015).
URL https://gitlab.com/rav7teif/linux.wifatch/

[30] M. Malik, M. M. Léveillé, Meet Remaiten – a Linux bot on steroids targeting routers and potentially other IoT devices, accessed on 4 October 2022 (2016).
URL https://www.welivesecurity.com/2016/03/30/meet-remaiten-a-linux-bot-on-steroids-targeting-routers-and-potentially-other-iot-devices/

[31] unixfreaxjp, MMD-0058-2016 - Linux/NyaDrop - a linux MIPS IoT bad news, accessed on 4 October 2022 (2016).
URL https://blog.malwaremustdie.org/2016/10/mmd-0058-2016-elf-linuxnyadrop.html

[32] Paganini, P., Exclusive – ELF Linux/NyaDrop, a new IoT threat in the wild, accessed on 4 October 2022 (2016).
URL http://securityaffairs.co/wordpress/52273/malware/elf-linux-nyadrop-iot.html

[33] unixfreaxjp, MMD-0056-2016 - Linux/Mirai, how an old ELF malcode is recycled.. , accessed on 1 April 2019 (2016).
URL http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html

[34] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, Y. Zhou, Understanding the mirai botnet, in: 26th USENIX Security Symposium (USENIX Security 17), 2017, pp. 1093–1110.

[35] B. Krebs, KrebsOnSecurity Hit With Record DDoS, accessed on 1 April 2019 (2016).
URL https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[36] B. Krebs, Source Code for IoT Botnet 'Mirai' Released, accessed on 13 June 2019 (2016).
URL https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

[37] S. Edwards, I. Profetis, Hajime: Analysis of a decentralized internet worm for IoT devices, accessed on 4 October 2022 (2016).
URL https://www.cs.umd.edu/class/fall2017/cmsc818O/papers/hajime-rapidity.pdf

[38] Radware, Hajime – Friend or Foe?, accessed on 4 October 2022 (2017).
URL https://www.radware.com/security/ddos-threats-attacks/hajime-iot-botnet/

[39] S. Herwig, K. Harvey, G. Hughey, R. Roberts, D. Levin, Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet, Network and Distributed Systems Security (NDSS) Symposium 2019 (2019). doi:10.14722/ndss.2019.23488.

[40] unixfreaxjp, MMD-0059-2016 - Linux/IRCTelnet (new Aidra) - A DDoS botnet aims IoT w/ IPv6 ready, accessed on 4 October 2022 (2016).
URL https://blog.malwaremustdie.org/2016/10/mmd-0059-2016-linuxirctelnet-new-ddos.html

[41] Goodin, D., New, more-powerful IoT botnet infects 3,500 devices in 5 days, accessed on 4 October 2022 (2016).
URL https://arstechnica.com/information-technology/2016/11/new-iot-botnet-that-borrows-from-notorious-mirai-infects-3500-devices/

[42] J. Soriano, Linux.Mirai: Attacking video surveillance systems, accessed on 5 October 2022 (2016).
URL https://www.securityartwork.es/2016/12/05/linux-mirai-attacking-video-surveillance-systems/

[43] T. Yeh, D. Chiu, K. Lu, Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras, accessed on 30 July 2019 (2017).
URL https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

[44] C. Zheng, C.and Xiao, Y. Jia, IoT Malware Evolves to Harvest Bots by Exploiting a Zero-day Home Router Vulnerability, accessed on 31 July 2019 (2018).
URL https://unit42.paloaltonetworks.com/unit42-iot-malware-evolves-harvest-bots-exploiting-zero-day-home-router-vulnerability/

[45] B. Krebs, 'Satori' IoT Botnet Operator Pleads Guilty, accessed on 5 Sep 2019 (2019).
URL https://krebsonsecurity.com/2019/09/satori-iot-botnet-operator-pleads-guilty/

[46] F. Li, Warning: Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869, accessed on 31 July 2019 (2017).
URL https://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/

[47] P. Paganini, Mirai botnet evolution since its source code is available online, accessed on 24 July 2019 (2018).
URL https://resources.infosecinstitute.com/mirai-botnet-evolution-since-its-source-code-is-available-online/

[48] P. Paganini, Satori Botnet is targeting exposed Ethereum mining pools running the Claymore mining software, accessed on 1 August 2019 (2018).
URL https://securityaffairs.co/wordpress/72651/cyber-crime/satori-botnet-mass-scanning.html

[49] RootKiter, Art of Steal: Satori Variant is Robbing ETH BitCoin by Replacing Wallet Address, accessed on 6 Aug 2019 (2018).
URL https://blog.netlab.360.com/art-of-steal-satori-variant-is-robbing-eth-bitcoin-by-replacing-wallet-address-en/

[50] RootKiter, Botnets never Die, Satori REFUSES to Fade Away, accessed on 7 Aug 2019 (2018).
URL https://blog.netlab.360.com/botnets-never-die-satori-refuses-to-fade-away-en/

[51] RootKiter, H. Wang, G. Ye, GPON exploit in the wild (ii) - satori botnet, accessed on 1 August 2019 (2018).
URL https://blog.netlab.360.com/gpon-exploit-in-the-wild-ii-satori-botnet-en/

[52] unixfreaxjp, Quick notes for Okiru & Satori variant of Mirai, accessed on 15 July 2019 (2018).
URL https://www.reddit.com/r/LinuxMalware/comments/7p00i3/quick_notes_for_okiru_satori_variant_of_mirai/

[53] Check Point Research, Huawei Home Routers in Botnet Recruitment, accessed on 1 August 2019 (2017).
URL https://research.checkpoint.com/good-zero-day-skiddie/

[54] C. Xiao, C. Zheng, New IoT/Linux Malware Targets DVRs, Forms Botnet, accessed on 5 October 2022 (2017).
URL https://unit42.paloaltonetworks.com/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/

[55] Radware, "BrickerBot" Results In Permanent Denial-of-Service, accessed on 5 October 2022 (2017).
URL https://www.radware.com/security/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/

[56] C. Cimpanu, BrickerBot Author Retires Claiming to Have Bricked over 10 Million IoT Devices, accessed on 5 October 2022 (2017).
URL https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/

[57] C. Cimpanu, BrickerBot Author Claims He Bricked Two Million Devices, accessed on 5 October 2022 (2017).
URL https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/

[58] A. Anubhav, Masuta : Satori Creators' Second Botnet Weaponizes A New Router Exploit, accessed on 19 Aug 2019 (2018).
URL https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7

[59] P. Geenens, Why the World is Under the Spell of IoT_Reaper, accessed on 29 Aug 2019 (2017).
URL https://blog.radware.com/security/2017/10/iot_reaper-botnet/

[60] G. Ye, IoT_reaper: A Rappid Spreading New IoT Botnet, accessed on 6 Aug 2019 (2017).
URL https://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

[61] Check Point Research, IoTroop Botnet: The Full Investigation, accessed on 17 June 2019 (2017).
URL https://research.checkpoint.com/iotroop-botnet-full-investigation/

[62] Radware, Reaper Botnet, accessed on 4 October 2022 (2017).
URL https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/reaper-botnet/

[63] D. Maciejak, Rise of One More Mirai Worm Variant, accessed on 5 October 2022 (2017).
URL https://www.fortinet.com/blog/threat-research/rise-of-one-more-mirai-worm-variant

[64] Trend Micro, Source Code of IoT Botnet Satori Publicly Released on Pastebin, accessed on 20 Aug 2019 (2018).
URL https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/source-code-of-iot-botnet-satori-publicly-released-on-pastebin?_ga=2.130140943.1805011413.1566193152-1053516337.1564462058

[65] P. Paganini, Mirai Okiru botnet targets for first time ever in the history ARC-based IoT devices, accessed on 1 Aug 2019 (2018).
URL http://securityaffairs.co/wordpress/67742/malware/mirai-okiru-botnet.html

[66] B. Botezatu, New Hide 'N Seek IoT Botnet using custom-built Peer-to-Peer communication spotted in the wild, accessed on 5 October 2022 (2018).
URL https://www.bitdefender.com/blog/labs/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/

[67] R. Joven, K. Yang, D. Maciejak, Hide 'N Seek: From Home Routers to Smart Home Insecurities, accessed on 5 October 2022 (2018).
URL https://www.fortinet.com/blog/threat-research/hide--n-seek--from-home-routers-to-smart-home-insecurities

[68] Threat Intelligence Team, Let's play Hide 'N Seek with a botnet., accessed on 5 October 2022 (2018).
URL https://blog.avast.com/hide-n-seek-botnet-continues

[69] A. Şendroiu, V. Diaconescu, Hide'n'seek: an adaptive peer-to-peer iot botnet, architecture 3 (2018) 5.

[70] P. Geenens, JenX – Los Calvos de San Calvicie, accessed on 31 July 2019 (2018).
URL https://blog.radware.com/security/2018/02/jenx-los-calvos-de-san-calvicie/

[71] Radware, JenX: A New Botnet Threatening All, accessed on 5 October 2022 (2018).
URL https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/jenx/

[72] M. Smii, JenX, New IoT Botnet, accessed on 5 October 2022 (2018).
URL https://medium.com/secjuice/jenx-new-iot-botnet-c412d5a446ee

[73] A. Anubhav, DoubleDoor: IoT Botnet bypasses firewall as well as modem security using two backdoor exploits, accessed on 5 October 2022 (2018).
URL https://blog.newskysecurity.com/doubledoor-iot-botnet-bypasses-firewall-as-well-as-modem-security-using-two-backdoor-exploits-88457627306d

[74] C. Cimpanu, DoubleDoor Botnet Chains Exploits to Bypass Firewalls, accessed on 5 October 2022 (2018).
URL https://www.bleepingcomputer.com/news/security/doubledoor-botnet-chains-exploits-to-bypass-firewalls/

[75] P. Paganini, DoubleDoor, a new IoT Botnet bypasses firewall using two backdoor exploits, accessed on 5 October 2022 (2018).
URL https://securityaffairs.co/wordpress/69063/malware/doubledoor-iot-botney.html

[76] Wang, H. and RootKiter, Early Warning: ADB.Miner A Mining Botnet Utilizing Android ADB Is Now Rapidly Spreading, accessed on 5 October 2022 (2018).
URL https://blog.netlab.360.com/early-warning-adb-miner-a-mining-botnet-utilizing-android-adb-is-now-rapidly-spreading-en/

[77] RootKiter, ADB.Miner: More Information, accessed on 5 October 2022 (2018).
URL https://blog.netlab.360.com/adb-miner-more-information-en/

[78] J. Manuel, R. Joven, D. Durando, OMG: Mirai-based Bot Turns IoT Devices into Proxy Servers, accessed on 15 July 2019 (2018).
URL https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers.html

[79] ASERT Team, OMG - Mirai Minions are Wicked, accessed on 15 July 2019 (2018).
URL https://www.netscout.com/blog/asert/omg-mirai-minions-are-wicked

[80] G. Ye, botnet muhstik is actively exploiting drupal cve-2018-7600 in a worm-style, accessed on 5 October 2022 (2018).
URL https://blog.netlab.360.com/botnet-muhstik-is-actively-exploiting-drupal-cve-2018-7600-in-a-worm-style/

[81] G. Ye, GPON Exploit in the Wild (I) - Muhstik Botnet Among Others, accessed on 5 October 2022 (2018).
URL https://blog.netlab.360.com/gpon-exploit-in-the-wild-i-muhstik-botnet-among-others-en/

[82] C. Zheng, Y. Ji, A. Davila, Muhstik Botnet Attacks Tomato Routers to Harvest New IoT Devices, accessed on 5 October 2022 (2020).
URL https://unit42.paloaltonetworks.com/muhstik-botnet-attacks-tomato-routers-to-harvest-new-iot-devices/

[83] S. Chierici, Hands-On Muhstik Botnet: crypto-mining attacks targeting Kubernetes, accessed on 5 October 2022 (2021).
URL https://sysdig.com/blog/muhstik-malware-botnet-analysis/

[84] W. Largent, New VPNFilter malware targets at least 500K networking devices worldwide, accessed on 5 October 2022 (2018).
URL https://blog.talosintelligence.com/2018/05/VPNFilter.html

[85] D. Goodin, Hackers infect 500,000 consumer routers all over the world with malware, accessed on 5 October 2022 (2018).
URL https://arstechnica.com/information-technology/2018/05/hackers-infect-500000-consumer-routers-all-over-the-world-with-malware/

[86] A. Anubhav, CVE-2018–10561 Dasan GPON exploit weaponized in Omni and Muhstik botnets, accessed on 6 Aug 2019 (2018).
URL https://blog.newskysecurity.com/cve-2018-10561-dasan-gpon-exploit-weaponized-in-omni-and-muhstik-botnets-ad7b1f89cff3

[87] R. Nigam, Unit 42 Finds New Mirai and Gafgyt IoT/Linux Botnet Campaigns, accessed on 6 Aug 2019 (2018).
URL https://unit42.paloaltonetworks.com/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/

[88] R. Joven, K. Yang, A Wicked Family of Bots, accessed on 2 Aug 2019 (2018).
URL https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html

[89] M. Tran, Shinoa, Owari, Mirai: What's with All the Anime References?, accessed on 20 Aug 2019 (2018).
URL https://www.fortinet.com/blog/threat-research/shinoa--owari--mirai--what-s-with-all-the-anime-references-.html

[90] C. Cimpanu, New Hakai IoT botnet takes aim at D-Link, Huawei, and Realtek routers, accessed on 5 October 2022 (2018).

URL https://www.zdnet.com/article/new-hakai-iot-botnet-takes-aim-at-d-link-huawei-and-realtek-routers/

[91] A. Remillano II, ThinkPHP Vulnerability Abused by Botnets, accessed on 5 October 2022 (2019).
URL https://www.trendmicro.com/en_au/research/19/a/thinkphp-vulnerability-abused-by-botnets-hakai-and-yowai.html

[92] J. Ahmed, Hakai :New Linux IoT Botnet, accessed on 5 October 2022 (2018).
URL https://medium.com/@ahmedjouini99/hakai-new-linux-iot-botnet-832d19377395

[93] J. Rosenberg, I. Sanmillan, Intezer Analyze™ ELF Support Release: Hakai Variant Case Study, accessed on 5 October 2022 (2018).
URL https://www.intezer.com/blog/malware-analysis/elf-support-released-hakai-malware/

[94] Kroustek, J. and Iliushin, V. and Shirokova, A. and Neduchal, J. and Hron, M., Torii botnet - Not another Mirai variant, accessed on 5 October 2022 (2018).
URL https://blog.avast.com/new-torii-botnet-threat-research

[95] Ilascu, I., New Iot Botnet Torii Uses Six Methods for Persistence, Has No Clear Purpose, accessed on 5 October 2022 (2018).
URL https://www.bleepingcomputer.com/news/security/new-iot-botnet-torii-uses-six-methods-for-persistence-has-no-clear-purpose/

[96] H. Wang, Fbot, A Satori Related Botnet Using Block-chain DNS System, accessed on 5 October 2022 (2018).
URL https://blog.netlab.360.com/threat-alert-a-new-worm-fbot-cleaning-adbminer-is-using-a-blockchain-based-dns-en/

[97] Ye, G. and Wang, H. and RootKiter, The new developments Of the FBot, accessed on 5 October 2022 (2019).
URL https://blog.netlab.360.com/the-new-developments-of-the-fbot-en/

[98] G. Ye, A. Turing, Fbot is now riding the traffic and transportation smart devices, accessed on 5 October 2022 (2021).
URL https://blog.netlab.360.com/fbot-is-now-riding-the-traffic-and-transportation-smart-devices-en/

[99] Wang, H. and RootKiter, BCMPUPnP_Hunter: A 100k Botnet Turns Home Routers to Email Spammers, accessed on 5 October 2022 (2018).
URL https://blog.netlab.360.com/bcmpupnp_hunter-a-100k-botnet-turns-home-routers-to-email-spammers-en/

[100] A. Remillano II, M. Vicente, Miori IoT Botnet Delivered via ThinkPHP Exploit, accessed on 5 October 2022 (2018).
URL https://www.trendmicro.com/en_us/research/18/l/with-mirai-comes-miori-iot-botnet-delivered-via-thinkphp-remote-code-execution-exploit.html?_ga=2.109430976.470075851.1651629382-575581362.1647321519

[101] P. Paganini, New Miori botnet has a unique protocol for C2 communication, accessed on 5 October 2022 (2019).
URL https://securityaffairs.co/wordpress/88303/malware/miori-botnet-new-c2-protocol.html

[102] Trend Micro, Into the Battlefield: A Security Guide to IoT Botnets, accessed on 5 October 2022 (2019).
URL https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/into-the-battlefield-a-security-guide-to-iot-botnets

[103] R. Nigam, New Mirai Variant Adds 8 New Exploits, Targets Additional IoT Devices, accessed on 22 Aug 2019 (2019).
URL https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/

[104] L. Cashdollar, Latest ECHOBOT: 26 Infection Vectors, accessed on 26 Aug 2019 (2019).
URL https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html

[105] I. Ilascu, Echobot Botnet Spreads via 26 Exploits, Targets Oracle, VMware Apps, accessed on 26 Aug 2019 (2019).
URL https://www.bleepingcomputer.com/news/security/echobot-botnet-spreads-via-26-exploits-targets-oracle-vmware-apps/

[106] I. Ilascu, New Echobot Botnet Variant Uses Over 50 Exploits to Propagate, accessed on 26 Aug 2019 (2019).
URL https://www.bleepingcomputer.com/news/security/new-echobot-botnet-variant-uses-over-50-exploits-to-propagate/

[107] E. Kreminchuker, M. Zavodchik, R. Pompon, Echobot Malware Now up to 71 Exploits, Targeting SCADA, accessed on 5 October 2022 (2019).
URL https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada

[108] P. Paganini, Silex malware bricks thousands of IoT devices in a few hours, accessed on 5 October 2022 (2019).
URL https://securityaffairs.co/wordpress/87609/iot/silex-malware-bricks-iot-devices.html

[109] H. Wang, A. Turing, L. Ya, G. Ye, The Botnet Cluster on the 185.244.25.0/24, accessed on 5 October 2022 (2019).
URL https://blog.netlab.360.com/the-botnet-cluster-on-185-244-25-0-24-en/

[110] P. Paganini, Moobot botnet spreads by exploiting CVE-2021-36260 flaw in Hikvision products, accessed on 5 October 2022 (2021).
URL https://securityaffairs.co/wordpress/125409/malware/moobot-botnet-hikvision.html

[111] C. Lin, Mirai-based Botnet - Moobot Targets Hikvision Vulnerability, accessed on 5 October 2022 (2021).
URL https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability

[112] P. Paganini, ARES ADB IOT Botnet targets Android Set Top Boxes (STB) and TVs, accessed on 5 October 2022 (2019).
URL https://securityaffairs.co/wordpress/90624/malware/ares-iot-botnet.html

[113] WootCloud Research, WootCloud Discovers ARES ADB IOT Botnet Targeting Android Devices especially STBs/ TVs, accessed on 5 October 2022 (2019).
URL https://wootcloud.com/wp-content/uploads/2019/10/WootCloud-Discovers-ARES-ADB-IOT-Botnet-Targeting-Android-Devices-especially-STBs_-TVs-1.pdf

[114] A. Turing, H. Wang, Mozi, Another Botnet Using DHT, accessed on 5 October 2022 (2019).
URL https://blog.netlab.360.com/mozi-another-botnet-using-dht/

[115] D. McMillen, W. Gao, C. DeBeck, A New Botnet Attack Just Mozied Into Town, accessed on 5 October 2022 (2020).
URL https://securityintelligence.com/posts/botnet-attack-mozi-mozied-into-town/

[116] T. F. Tu, J. W. Qin, H. Zhang, M. Chen, T. Xu, Y. Huang, A comprehensive study of Mozi botnet, International Journal of Intelligent Systems 37 (10) (2022) 6877–6908. doi:10.1002/int.22866.

[117] Bitdefender Investigations and Forensics Unit, New dark_nexus IoT Botnet Puts Others to Shame, accessed on 5 October 2022 (2020).
URL https://www.bitdefender.com/files/News/CaseStudies/study/319/Bitdefender-PR-Whitepaper-DarkNexus-creat4349-en-EN-interactive.pdf

[118] MalwareMustDie, Twitter's post, accessed on 5 October 2022 (2020).
URL https://twitter.com/malwaremustd1e/status/1233027817123667968

[119] L. Ya, The Gafgyt variant vbot seen in its 31 campaigns, accessed on 5 October 2022 (2020).
URL https://blog.netlab.360.com/the-gafgyt-variant-vbot-and-its-31-campaigns/

[120] L. Ubiedo, RHOMBUS: a new IoT Malware, accessed on 5 October 2022 (2020).
URL https://www.stratosphereips.org/blog/2020/4/29/rhombus-a-new-iot-malware

[121] MalwareMustDie, Reddit's post, accessed on 5 October 2022 (2020).
URL https://www.reddit.com/r/LinuxMalware/comments/fh3zar/memo_rhombus_an_elf_bot_installerdropper/

[122] K. Hsu, Z. Zhang, R. Nigam, New Mirai Variant Targets Zyxel Network-Attached Storage Devices, accessed on 5 October 2022 (2020).
URL https://unit42.paloaltonetworks.com/new-mirai-variant-mukashi/

[123] D. Palmer, This new variant of Mirai botnet malware is targeting network-attached storage devices, accessed on 5 October 2022 (2020).
URL https://www.zdnet.com/article/this-new-variant-of-mirai-botnet-malware-is-targeting-network-attached-storage-devices/

[124] V. Singhal, R. Nigam, Z. Zhang, A. Davila, New Mirai Variant Targeting Network Security Devices, accessed on 5 October 2022 (2021).
URL https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/

[125] Radware, Dark.IoT Botnet, accessed on 5 October 2022 (2021).
URL https://www.radware.com/security/threat-advisories-and-attack-reports/dark-iot-botnet/

[126] Radware, Dark.IoT Botnet, accessed on 5 October 2022 (2021).
URL https://www.radware.com/getmedia/18d24c2d-c092-4a61-9ad6-ebb92b7a49b8/Alert_Realtek_SDK.aspx