An investigation into the Bashlite botnet

Boluwarin Oladipo

I. EXECUTIVE SUMMARY

This paper seeks to investigate:

- the Bashlite botnet,
- details of its malware binary,
- its size and damage caused by it
- target devices for the malware
- the botnet architecture
- the botnet behaviour
- takedown attempts
- the evolution of the botnet malware

The Bashlite botnet malware is also identified by the names Gafgyt, LizardStresser and Torlus. It is spread through malware targeting mainly Linux-based and Internet of Things devices [1]. It was first discovered in 2014 and was responsible for the largest recorded distributed denial of service attack in 2016 against krebsonsecurity.com, recording 620 gigabits per second of traffic on average. The Bashlite source code was leaked in 2015 [2], evolving into other variants most notably Mirai causing further havoc. Due to the danger these botnets pose, recommendations to combat the spread as well as protect against distributed denial-of-service attacks will also be discussed in this paper.

II. METHODOLOGY

This report seeks to investigate the Bashlite botnet, identify infected bots by its behaviour, its architecture, how resilient it is, attempted takedowns of the botnet and iterations of the botnet after its first discovery. This will be done mainly through literature review of relevant papers related to analysis of Bashlite's attributes. Peer reviewed papers from reputable industry journals as well as detailed analysis of the botnet from cybersecurity researchers will be considered to investigate the botnet.

The NCI library EBSCO service [3], IEEE Xplore [4] as well as Google Scholar [5] will be used for searching and selecting relevant research papers. Relevant references within these papers will also be explored further for details relevant to the investigation.

III. BOTNET INVESTIGATION AND FINDINGS

A. Bots Identification

- File Type: The Bashlite malware is an Executable and Linkable Format Linux file (ELF).
- File Name: i686; zbetcheckin_tracker_i686 [6]
- File Size: 111.81 Kilobytes
- Hashes: 0689c812b0e267315832ac7d823c77e5 (MD5); d9f0bcb4545200c699d8c8733e701c1fd2489722 (SHA-1); 80e66807631cac8a5414bd6de6cc06f672b872dc040725a9ccbb092437f7e22c (SHA-256) [6]
- Malware Names: The malware is detected by major anti-virus engines under the following names: ELF:DDoS-Y [Trj] (Avast); Linux.Gafgyt!gen2 (Symantec); Backdoor:Linux/Gafgyt.AX!xp (Microsoft) [6]
- Anti-Virus Detection Capabilities: It is currently detected by 47 of 68 anti-virus engines on VirusTotal.[6]
- First created: 1st July 2024.[6]

B. Botnet Size and Damage

The Bashlite botnet in its most recent estimate is said to have about a million devices [7], [8]. Over two hundred command and control servers were discovered acting as bot herders with the average server having control of 74 bots and the largest server controlling as many as 120,000 bots and the IP addresses of the command-and-control server hardcoded into the malware. Most attacks carried out by this botnet lasted for five minutes or less with the average attack lasting only two minutes. [9]

Security journalist Brian Krebs' website krebsonsecurity.com was subject to an unsuccessful denial of service attack attempt in September 2016. The size of the attack was reported at about 620 gigabits per second of traffic, double the record at the time for the previous record attack of 363 gigabits per second [10]. According to estimates provided to Brian Krebs by security firm Akamai who were responsible for protection of the website, it would have cost up to 200,000 US dollars annually to mitigate the traffic that was sent to the website.

A Kaspersky report on denial of service attacks estimated the cost of an average distributed denial of service attack at 106,000 US dollars for small to medium sized businesses and as up to 1.6 million US dollars for larger enterprises [11]. This is the estimated cost of potential revenue loss that comes through the online assets that are being held to ransom, mitigation and recovery costs of the attack, regulatory and legal fines, brand and reputational damage, and equipment costs.

C. Target Devices

The Bashlite botnet is reported to have as many as one million devices, 96% of which are reported to be Internet of Things (IoT) devices. It was further reported that 95% of these IoT devices were cameras and Digital Video Recorders (DVR). The remaining 4 percent consisted of compromised home routers and Linux servers [9].

A large percentage of the devices sent traffic to targets possess unique IP addresses attributed to Taiwan, Brazil and Colombia. This is due to the presence of generic devices labelled as H.264 DVR as well as DVRs manufactured by Dahua Technology. These devices were targeted mainly due to their ability to process large bandwidths of network traffic being a requirement of maintaining video streams over a network as well as the presence of the Linux operating system that is run on them [9].

IoT devices also generally possess access methods such as telnet and unsecured web interfaces for management enabled and insecure by default. These access methods utilize default credentials which are present on word lists available on the public internet. These factors combined make these devices particularly vulnerable to brute force attacks which pave the way for the malware to be installed. Once access has been gained, the attackers run commands to retrieve their bot payloads and attempt to run multiple versions of the malware for different architectures until one executes [9].

D. Botnet Architecture

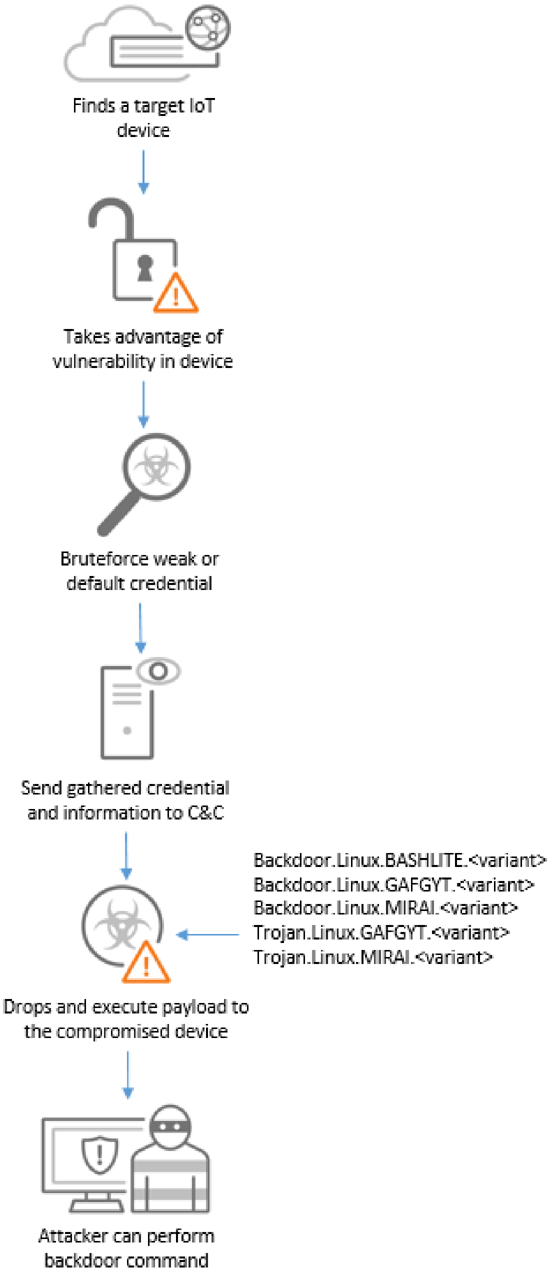
Finds a target IoT device
Takes advantage of vulnerability in device
Bruteforce weak or default credential
Send gathered credential and information to C&C
Backdoor.Linux.BASHLITE.<variant>
Backdoor.Linux.GAFGYT.<variant>
Backdoor.Linux.MIRAI.<variant>
Trojan.Linux.GAFGYT.<variant>
Trojan.Linux.MIRAI.<variant>
Drops and execute payload to the compromised device
Attacker can perform backdoor command

Fig. 1. Bashlite infection kill chain [12]

There are over two hundred command and control servers that have been tracked for the Bashlite malware family with the IP addresses of the servers hard coded into the malware. Fig. 1 above shows the infection chain of the Bashlite malware from reconnaissance of targets to actions on objectives for infection of a target.

The command-and-control servers communicate commands primarily through a custom protocol based on Internet Relay Chat, establishing TCP sessions with each bot and sending commands via clear text [9]. This botnet utilizes a centralized command and control architecture with each bot receiving commands from their assigned command-and-control server to execute denial of service attacks. Fig. 2 shows a probable architecture of the botnet as described while Fig. 3 shows an overview of a typical botnet.

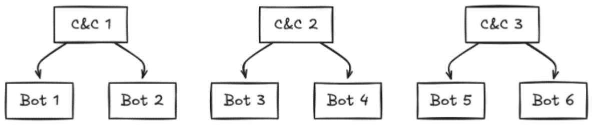

Fig. 2. Bashlite architecture

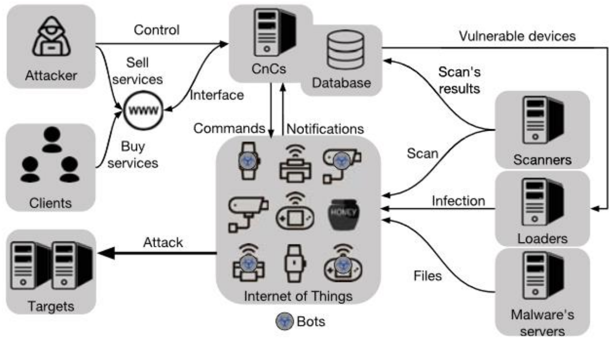

Fig. 3. Overview of an IoT botnet [13]

E. Botnet Behaviour

The Bashlite malware targets devices that have been identified as vulnerable and conducts a brute-force attack using default credentials widely utilized by the management interfaces of these targets. Once the malware has been installed and the attacker is in control, the communication protocol initiates a keep-alive message between the bot and its designated command-and-control server at one-minute intervals. Fig. 3 shows the protocol for communication between bot and server. The botnet is primarily used for conducting distributed denial of service (DDoS) attacks against specified targets. Many attacks consist of bots being directed to flood the target with multiple TCP and UDP packets, with TCP being preferred for high packets-per-second attacks and UDP being preferred for high bandwidth attacks. Some variants of the malware also support HTTP attacks which establish complete connections to the target web servers.

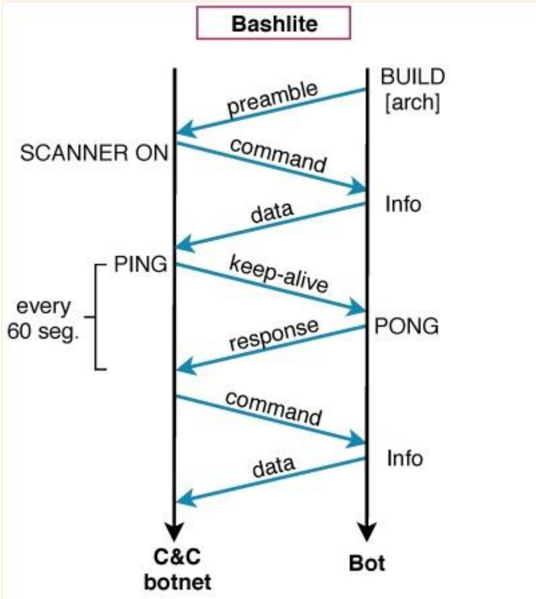

Fig. 4. Bashlite communication protocol [14]

Commands that can be sent to a bot from a command-and-control server include:

- `SCANNER` to perform TCP scans to find other vulnerable devices to infect via Telnet.
- `UDP` to perform UDP flooding attacks.
- `TCP` to deploy TCP attacks.
- `HOLD` to hold a specified number of TCP connections for a specific period or delay attack for a specified duration.
- `GETLOCALIP` to identify the local IP address of the bot.
- `HTTP` to deploy a HTTP flood attack.
- `UPDATE` to deploy updates to the malware binary.
- `KILLATTK` to stop any ongoing attacks. [9], [13] [12]

F. Botnet Resilience

The presence of multiple vulnerable IoT devices combined with the fact that most devices are in use by end users who have little to no concern for anything other than functionality means a steady supply of vulnerable devices for infection by this botnet. While the malware can be eradicated by a factory reset of the affected device, a large percentage of the devices may never be discovered as infected for as long as they are in service due to the limited interaction with the operating system. The Bashlite malware can scan for other vulnerable devices and propagate itself. This is done using the `SCAN` command as mentioned in the above section.

The command-and-control servers utilized in this botnet are distributed, making a takedown harder by bringing down a single server. While the malware is relatively unsophisticated when compared to other malware in its class, the ease of replacing a command-and-control server mitigates this risk. Since the IP address of its assigned command-and-control server is hardcoded into the malware, an update to the malware binary is required for changing the IP address and is issued through running the `UPDATE` command.

G. Botnet Takedown

There have not been any documented takedown attempts by law enforcement or government agencies of the Bashlite botnet. However, attempts against similar botnets such as Mirai included domain seizure, sinkholing of traffic and analysis of traffic data from previous attacks. This was evident in the mitigation of the attack on krebsonsecurity.com where all the traffic was sinkholed to the localhost IP due to the load on Akamai's services [15].

H. Botnet Evolution

The Bashlite malware was first discovered in 2014 and spread through deliberate targeting of vulnerable IoT devices and then spreading through scanning the networks of infected machines to find other vulnerable machines for infection. It exploited the Shellshock vulnerability (CVE-2014-7169) [16] to gain access to these devices and other vulnerabilities in Huawei, [17] Zyxel [18] and Realtek [19] devices to infect bots. The malware at a basic level, provided a backdoor to send commands from the command-and-control server to bots to conduct denial of service attacks against specified targets, download additional payloads, perform scans on the bot's network, run arbitrary shell commands and perform brute force attacks using a dictionary of username and password pairs.

Recent variants of the malware showcased added functionality such as utilization of the TOR (The Onion Router) network to hide its command-and-control server traffic as well as encryption of strings related to commands to be used to conduct attacks. Other versions of the malware also exploit remote code execution vulnerabilities [20], [21], [22] as well as incorporating modules such as HTTP flooding, UDP flooding and Telnet brute force derived from the Mirai malware code.

IV. RECOMMENDATIONS

A large percentage of these vulnerable devices are infected due to the presence of insecure management interfaces and hard-coded credentials enabled by the manufacturer implemented due to the ease and cost as opposed to implementing more secure interfaces. This combined with the fact that a significant number [23] of these IoT devices including but not limited to wearable technology and smart home devices used by consumers who may not be as security-conscious as enterprise users, creates a large pool of potential bots to be used for nefarious purposes.

. The below recommendations will ensure that the risk of infection of machines and the impact of the botnet is reduced to a minimum:

- Strengthening IoT device security: Manufacturers of these devices can mitigate the vulnerabilities before they are even discovered and exploited by installing relatively secure access mechanisms that are enabled by default. They should also avoid hard-coding credentials into the devices to enable the end-users change the default to other values which prevents brute-force attack methods employed by the Bashlite malware [9]. This is in line with the NIST SP 800-160 guidelines on secure systems engineering [24].

- Anti-DDoS protection: Companies such as Cloudflare [25] and Akamai [26] offering anti-DDoS protection can mitigate the effects of denial of service attacks due to the large network capacity possessed by these networks. This can be seen to be effective in the case of the attack on krebsonsecurity.com totalling 620Gbps that was mitigated by Akamai. Internet Service Providers can also prevent amplification attacks at the lower layers of the network stack by implementation of traffic filtering policies such as the BCP38 standard on their network edge devices [2], [27]
- Information sharing: Manufacturers, law enforcement agencies, cybersecurity research companies can collaborate to share information such as firewall rules via threat intelligence feed for distribution to organizations, so they stay up to date with current and emerging signature related to all variants of malware. This will be useful in ensuring that tactics, techniques and procedures utilized as well as Bashlite malware signatures are well defended against.
- Network security measures: Segmentation of the network will ensure that malware cannot spread to other parts of the network easily, stopping an attack in its earlier stages. Network security devices such as firewalls, intrusion detection systems and load balancers, updated with the latest rules from robust threat intelligence feeds could also be deployed to ensure the security of the internal network and prevent attacks from progressing.
- Awareness: Efforts should be made to educate consumers of IoT devices on the implications of purchasing and using insecure devices in their homes. This is due to many devices that are vulnerable to Bashlite being consumer IoT devices, used by end users who have a preference for functionality and cost over all other attributes of these devices. [2]

V. CONCLUSIONS

This report investigated the Bashlite botnet using authoritative academy and industry sources. The botnet malware binary was researched and detailed, its estimated size as well as reported damage caused by it, devices targeted by the malware, its architecture, its main purpose, its resilience, documented takedown attempts and its evolution. The investigation has revealed the massive scale at which Bashlite has affected IoT devices and the potential to infect many more with relative ease, posing a significant threat to web security due to the low cost of accessing and using the Bashlite botnet and similar botnets. Recommendations for mitigating the effects of these botnets were also discussed with responsibilities of end users, network providers and device manufacturers in securing the vulnerable devices.

If there was more time to investigate the malware and botnet, the below steps will be taken:

- The experiment conducted by Marzano et al. [13] where a number of low-interactivity devices were deployed to mimic infected devices and receive commands to be logged on a server, will be reproduced within Europe as the devices were deployed only in Brazil.
- Further investigation into the major variants of Bashlite within the parameters of the investigation conducted in this paper will be conducted to predict future trends and determine the best ways to combat subsequent variants.
- An investigation into the economic incentives of denial-of-service attacks will be conducted to provide valuable insights for device manufacturers as well as law enforcement agencies to shore up defences against the malware.

Overall, this investigation has provided insights into how easily common devices can be utilized for malicious purposes and the importance of basic cyber hygiene for all networked devices. The recommendations provided will assist individuals and organizations in ensuring their devices do not fall victim to infections or attacks by malicious actors.

REFERENCES

[1] "Gafgyt Malware Analysis, Overview by ANY.RUN." Accessed: Jul. 31, 2024. [Online]. Available: https://any.run/malware-trends/gafgyt

[2] J. Scott and D. Spaniel, "Rise of the Machines," 2016.

[3] NCI, "EBSCO Discovery Service." Accessed: Aug. 09, 2024. [Online]. Available: https://research.ebsco.com/c/x47ol5/search

[4] IEEE, "IEEE Xplore." Accessed: Aug. 09, 2024. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp

[5] Google, "Google Scholar." Accessed: Aug. 09, 2024. [Online]. Available: https://scholar.google.com/

[6] "VirusTotal - File - 80e66807631cac8a5414bd6de6cc06f672b872dc040725a9ccbb092437f7e22c." Accessed: Jul. 31, 2024. [Online]. Available: https://www.virustotal.com/gui/file/80e66807631cac8a5414bd6de6cc06f672b872dc040725a9ccbb092437f7e22c/detection

[7] T. Spring, "BASHLITE Family Of Malware Infects 1 Million IoT Devices | Threatpost." Accessed: Aug. 01, 2024. [Online]. Available: https://threatpost.com/bashlite-family-of-malware-infects-1-million-iot-devices/120230/

[8] E. Chickowski, "Another IoT-Dominated Botnet Rises With Almost 1M Infected Devices." Accessed: Aug. 01, 2024. [Online]. Available: https://www.darkreading.com/endpoint-security/another-iot-dominated-botnet-rises-with-almost-1m-infected-devices

[9] Black Lotus Labs, "Attack of Things! - Lumen." Accessed: Aug. 06, 2024. [Online]. Available: https://blog.lumen.com/attack-of-things/

[10] B. Krebs, "KrebsOnSecurity Hit With Record DDoS – Krebs on Security." Accessed: Aug. 06, 2024. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[11] E. Eliseeva, "Protecting your business against financial and reputational losses with Kaspersky DDoS Protection".

[12] "GAFGYT - Threat Encyclopedia | Trend Micro (US)." Accessed: Jul. 31, 2024. [Online]. Available: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/GAFGYT

[13] A. Marzano *et al.*, "The Evolution of Bashlite and Mirai IoT Botnets," in *2018 IEEE Symposium on Computers and Communications (ISCC)*, Natal: IEEE, Jun. 2018, pp. 00813–00818. doi: 10.1109/ISCC.2018.8538636.

[14] J. M. Ceron, K. Steding-Jessen, C. Hoepers, L. Z. Granville, and C. B. Margi, “Improving IoT Botnet Investigation Using an Adaptive Network Layer,” *Sensors*, vol. 19, no. 3, p. 727, Feb. 2019, doi: 10.3390/s19030727.

[15] B. Krebs, “The Democratization of Censorship – Krebs on Security.” Accessed: Aug. 08, 2024. [Online]. Available: https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/

[16] MITRE, “NVD - CVE-2014-7169.” Accessed: Aug. 08, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2014-7169

[17] Huawei Technologies, “NVD - cve-2017-17215.” Accessed: Aug. 08, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2017-17215?ref=blog.netlab.360.com

[18] MITRE, “NVD - CVE-2017-18368.” Accessed: Aug. 08, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-18368

[19] MITRE, “NVD - CVE-2014-8361.” Accessed: Aug. 08, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2014-8361

[20] MITRE, “NVD - CVE-2019-16920.” Accessed: Aug. 08, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-16920

[21] MITRE, “NVD - CVE-2019-19781.” Accessed: Aug. 08, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-19781

[22] MITRE, “NVD - CVE-2020-7961.” Accessed: Aug. 08, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-7961

[23] Statista Research Department, “Europe: Internet of Things segment revenue 2023 | Statista.” Accessed: Aug. 08, 2024. [Online]. Available: https://www.statista.com/forecasts/1283717/revenue-from-internet-of-things-in-europe-segment

[24] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, “Developing cyber-resilient systems : a systems security engineering approach,” National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST SP 800-160v2r1, Dec. 2021. doi: 10.6028/NIST.SP.800-160v2r1.

[25] “DDoS Protection & Mitigation Solutions | Cloudflare.” Accessed: Aug. 08, 2024. [Online]. Available: https://www.cloudflare.com/ddos/

[26] “DDoS (Distributed Denial-of-Service) Attack Protection | Akamai.” Accessed: Aug. 08, 2024. [Online]. Available: https://www.akamai.com/solutions/security/ddos-protection

[27] Ferguson and Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,” Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Accessed: Aug. 08, 2024. [Online]. Available: https://www.ietf.org/rfc/bcp/bcp38.html