Bashlite Updated with Mining and Backdoor Commands

By Mark Vicente, Byron Gelera, Augusto Remillano II, Chizuru Toyama, Jakub Urbanec (words)

Published: 2019-04-03 · Archived: 2026-04-10 03:10:43 UTC

We uncovered an updated Bashlite malware designed to add infected internet-of-things devices to a distributed-denial-of-service (DDoS) botnet. Trend Micro detects this malware as Backdoor.Linux.BASHLITE.SMJC4, Backdoor.Linux.BASHLITE.AMF, Troj.ELF.TRX.XXELFC1DFF002, and Trojan.SH.BASHDLOD.AMF. Based on the Metasploit module it exploits, the malware targets devices with the WeMo Universal Plug and Play (UPnP) application programming interface (API).

Bashlite (also known as Gafgyt, Lizkebab, Qbot, Torlus, and LizardStresser) gained notoriety for its use in large-scale DDoS attacks in 2014, but it has since crossed overnews article to infecting IoT devices. In its previous iterations, Bashlite exploited Shellshock to gain a foothold into the vulnerable devices. An attacker can then remotely issue commands — particularly, to launch DDoS attacks similar to the way it was used in 2016 — and download other files to the compromised devices.

This updated iteration of Bashlite is notable. For one, its arrival method is unique in that it doesn't rely on specific vulnerabilities (e.g., security flaws assigned with CVEs). It instead abuses a publicly available remote-code-execution (RCE) Metasploit module. It now also sports additional DDoS-related commands, and added new ones that gave the malware cryptocurrency miningnews- cybercrime-and-digital-threats and backdoor capabilities. It can also deliver malware that removes competing botnet malware.

The exploit used doesn't have a list of targeted WeMo devices. It only needs to check if the device is enabled with the WeMo UPnP API. The impact could be significant. WeMo's home automation productsproducts, for instance, range from internet-connected cameras, electrical plugs, and light switches and bulbs to motion sensors. It has a mobile application that uses the Wi-Fi network to wirelessly control IoT devices.

While we have not seen significant detections for these versions of Bashlite, it's worth noting that it's already in the wild, based on feedback from Trend Micro™ Smart Protection Network™. The detections, seen last March 21, were observed in Taiwan, United States, Thailand, Malaysia, Japan, and Canada.

We disclosed our findings to Belkin. The company has since released an official statement regarding the vulnerabilities that the malware targets. "Belkin is committed to product and customer security. The vulnerability described in this article was detected and remediated in 2015 for all affected devices.We strongly encourage customers to update their devices and mobile apps to obtain the latest security fixes."

intelFigure 1. Bashlite infection chain

intel

intel

Figure 2. Snapshot of code showing a network indicator (via Trend Micro™ Deep Discovery Inspectorproducts™) of the attack targeting devices with WeMo API (top), which is also in the Metasploit module (bottom)

Infection chain

Some of the Bashlite samples we analyzed appear to differ depending on the architectures they infect. These recent Bashlite iterations use a Telnet scanner and brute force the device with these usernames and passwords: *root, 9615-cdp, admin, admin123, huigu309, xc3511, vizxv,* and *Dvrdvs.*

Bashlite uses the scanner to find possible machines to infect. It will then send a dropper binary (XORred, with key=0x54) to the vulnerable machine. Of note here is the way the binary dropper is supposed to retrieve and drop the Hakai botnet malware, whose code is based on Bashlite and was seen targeting routers last year. However, the URL from which Hakai is supposed to be downloaded is no longer accessible. There are multiple dropper binaries embedded in Bashlite, designed for different architectures. Figure 3 shows how the embedded binaries are retrieved and dumped.

As part of its command-and-control (C&C) communication, the binary dropper connects to 178[.]128[.]185[.]250/hakai[.]x86. It also connects to 185[.]244[.]25[.]213:3437 for Bashlite's backdoor routines.

intel

Figure 3. Screenshot showing how the Hakai malware is also supposed to be downloaded and executed on another device

intel

intel

Figure 4. Snapshots of code showing functions responsible for retrieving (top) and dumping (bottom) the embedded binaries

Backdoor and DDoS capabilities

The most notable of Bashlite's backdoor commands include simultaneously launching multiple types of DDoS floods to a target as well as downloading and executing cryptocurrency-mining and bricking malware. It also has code designed to circumvent a DDoS mitigation service.

Here are some of Bashlite's backdoor commands:

- PINGING: Similar to an internet relay chat (IRC) message; the malware replies with PONGING.
- ECHOSCAN: Toggles the Telnet scanner.
- OELINUX: Similar to ECHOSCAN but targets embedded systems.
- CFBYPASS: Used to bypass a DDoS mitigation service

intel

intel

Figure 5. Snapshots of code showing the backdoor commands PINGING, ECHOSCAN (top), OELINUX, and CFBYPASS (bottom)

Bashlite can launch several types of DDoS attacks using these commands:

- HOLD: Connects to an IP address and port, and sustained for a specified time.
- JUNK: Same as HOLD but also sends a randomly generated string to the IP address.
- UDP: Flood target with user datagram protocol (UDP) packets.
- ACK: Send acknowledgment (ACK) signals to disrupt network activity.
- VSE: An amplification attack used to consume the resources of a target (e.g., server).
- TCP: Send numerous transmission control protocol-based (TCP) requests.
- OVH: DDoS attack designed to bypass a DDoS mitigation service
- STD: Similar to UDP (flooding the target with UDP packets)
- GRENADE: Launch all the DDoS commands.

Bashlite has other notable commands. For example, *BRICKER* downloads and executes a bricker malware from a specified URL to presumably eliminate competing bots. *MINER* downloads and executes a cryptocurrency-mining malware on the infected machine, while *PKILL* terminates a specified process.

Figure 6. Snapshot of code showing different DDoS-related commands

IoT security shouldn't be an afterthought

While connected devices — from those used in smart homesnews article to complex IoT environmentsnews article — provide convenience and efficiency, they can also come with risks if improperly configured or left unsecured. Bashlite is just one of the many threats that could threaten the privacy, security, and even safety of users. We've seen some of these threats, for example, take advantage of exposed UPnP-enabled devices that don't have patches for known vulnerabilities. Equipment designers and manufacturers must integrate security into the development life cycle of their products. Organizations that adopt BYOD policiesnews- cybercrime-and-digital-threats for IoT device use in the workplace must balancenews article the advantages of mobility and the need for security. Users should also adopt best practicesnews article.

Trend Micro Home Network Security™products protects users from this threat via this intrusion prevention rule:

- 1135463 – WEB Belkin Wemo UPnP Remote Code Execution

The Trend Micro™ Deep Discovery Inspector™products solution protects customers from related attacks via this DDI rule:

- 2860 – Belkin Wemo UPnP Remote Code Execution

Indicators of compromise (IoCs)

Related hashes (SHA-256):

- 81cbb253ef6ad4803e3918883eed3ec6306ef12e7933c5723bd720d55d13a46a — Backdoor.Linux.BASHLITE.SMJC4
- 01570ee09d63579afc77a44295aeb06c1cc826ae6f0aa9423915ea4ecfd9899f — Trojan.SH.BASHDLOD.AMF

Detected as Backdoor.Linux.BASHLITE.AMF (SHA-256):

- 2d896a7e4db137024b947ca5be79fd0497f50f3a0ad2edf07455d3b35a40735b
- fe887192440d1a7c6199593dfab52362a22e187d80879c89eba72f1659e82d0b
- 506e4824beb216a33ed7cb1fe98637091f603b93df789f3819c624f5e3e19b80
- 9ce735506f6cb663d4a4617da99b75262dc937c62c2afda0509adc49745c1554
- d9faa3e129a72a9908eafc25d4ecc54aca77da2714471db45d191520bc6075f4
- 323b4260e8fbfb46461ff017882832ed195821e855a473a0b0e15ace5ad8b2ef
- 8da4b0d63aa6824e454ec3786093d2fb18d1ba89ddc5510221b076058db0bb19
- bcb19d156b089cabc2b89f31e36b577be700ea489dd8c1ef69cbcb95585ef05c
- 21c740671cad8dc67b5504e0d5e6cf0a92864ea87c075f1ebdff419e95263077
- ba47ec0a9f2dedb169590f607f96cc889f4b9e465ce9334502a09997e74c4334
- 31607153ce9edec754027b3ea2ddc3b6c3f13532c2e78b54a89dbeb09b4efd43
- d2aeb3beadbdfe9d44521551ce44661595a51ce9bb9e1c317b74e173ab65c6fa

Related malicious URLs:

- hxxp://185[.]244[.]25[.]213/ECHOBOT[.]mips
- hxxp://185[.]244[.]25[.]213/UqHDZbqr9S[.]sh
