

Linux-Targeted Malware Increases by 35% in 2021

crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/

Mihai Maganu

January 13, 2022



- Malware targeting Linux systems increased by 35% in 2021 compared to 2020
- XorDDoS, Mirai and Mozi malware families accounted for over 22% of Linux-targeted threats observed by CrowdStrike in 2021
- Ten times more Mozi malware samples were observed in 2021 compared to 2020

Malware targeting Linux-based operating systems, commonly deployed in Internet of Things (IoT) devices, have increased by 35% in 2021 compared to 2020, according to current CrowdStrike threat telemetry, with the top three malware families accounting for 22% of all Linux-based IoT malware in 2021.

XorDDoS, Mirai and Mozi are the most prevalent Linux-based malware families observed in 2021, with Mozi registering a significant tenfold increase in the number of in-the-wild samples in 2021 compared to 2020. The primary purpose of these malware families is to compromise vulnerable internet-connected devices, amass them into botnets, and use them to perform distributed denial of service (DDoS) attacks.

Linux-based Malware and IoT

Linux powers most of today's cloud infrastructure and web servers, yet it also powers mobile and IoT devices. It's popular because it offers scalability, security features and a wide range of distributions to support multiple hardware designs and great performance on any hardware requirements.

With various Linux builds and distributions at the heart of cloud infrastructures, mobile and IoT, it presents a massive opportunity for threat actors. For example, whether using hardcoded credentials, open ports or unpatched vulnerabilities, Linux-running IoT devices are a low-hanging fruit for threat actors — and their en masse compromise can threaten the integrity of critical internet services. More than 30 billion IoT devices are projected to be connected to the internet by the end of 2025, creating a potentially very large attack surface for threats and cybercriminals to create massive botnets.

A botnet is a network of compromised devices connected to a remote command-and-control (C2) center. It functions as a small cog in the larger network, and can infect other devices. Botnets are often used for DDoS attacks, spamming targets, gaining remote control and performing CPU-intensive activities like cryptomining. DDoS attacks use multiple internet-connected devices to access a specific service or gateway, preventing legitimate traffic from passing through by consuming the entire bandwidth, causing it to crash.

The 2016 Mirai botnet incident serves as a reminder that a large number of seemingly benign devices performing a DDoS attack can disrupt critical internet services, affecting both organizations and average users.

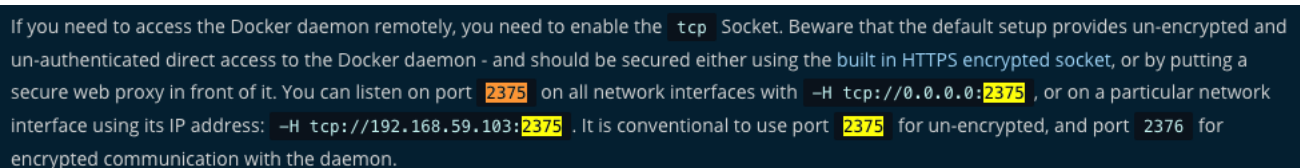
Top Linux Threats in Today's Landscape

Analyzing the current Linux threat landscape, the XorDDoS, Mirai and Mozi malware families and variants have emerged as the most prolific in 2021, accounting for over 22% of all IoT Linux-targeting malware.

XorDDoS: 123% Increase in Malware Samples

XorDDoS is a Linux trojan compiled for multiple Linux architectures, ranging from ARM to x86 and x64. Its name is derived from using XOR encryption in malware and network communication to the C2 infrastructure.

When targeting IoT devices, the trojan is known to use SSH brute-forcing attacks to gain remote control on vulnerable devices.



```
If you need to access the Docker daemon remotely, you need to enable the tcp Socket. Beware that the default setup provides un-encrypted and un-authenticated direct access to the Docker daemon - and should be secured either using the built in HTTPS encrypted socket, or by putting a secure web proxy in front of it. You can listen on port 2375 on all network interfaces with -H tcp://0.0.0.0:2375, or on a particular network interface using its IP address: -H tcp://192.168.59.103:2375. It is conventional to use port 2375 for un-encrypted, and port 2376 for encrypted communication with the daemon.
```

Fig. 1- Docker's official documentation (Click to enlarge)

On Linux machines, some variants of XorDDoS show that its operators scan and search for Docker servers with the 2375 port open. This port offers an unencrypted Docker socket and remote root passwordless access to the host, which attackers can abuse to get root access to the machine.

CrowdStrike researchers have found that the number of XorDDoS malware samples throughout 2021 has increased by almost 123% compared to 2020.

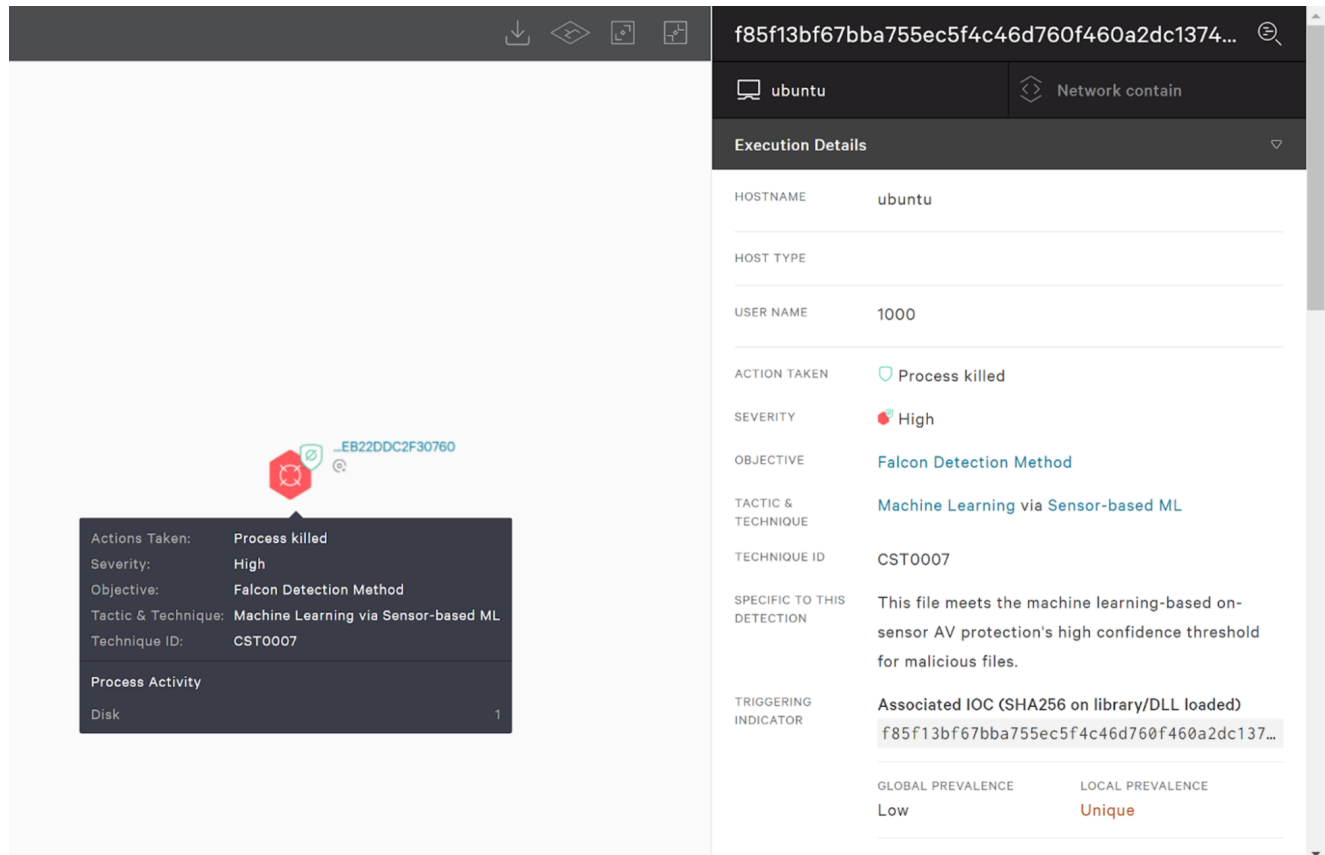


Fig. 2 – Falcon detection for Linux XorDDoS malware sample (Click to enlarge)

Mozi: 10 Times More Prevalent in 2021

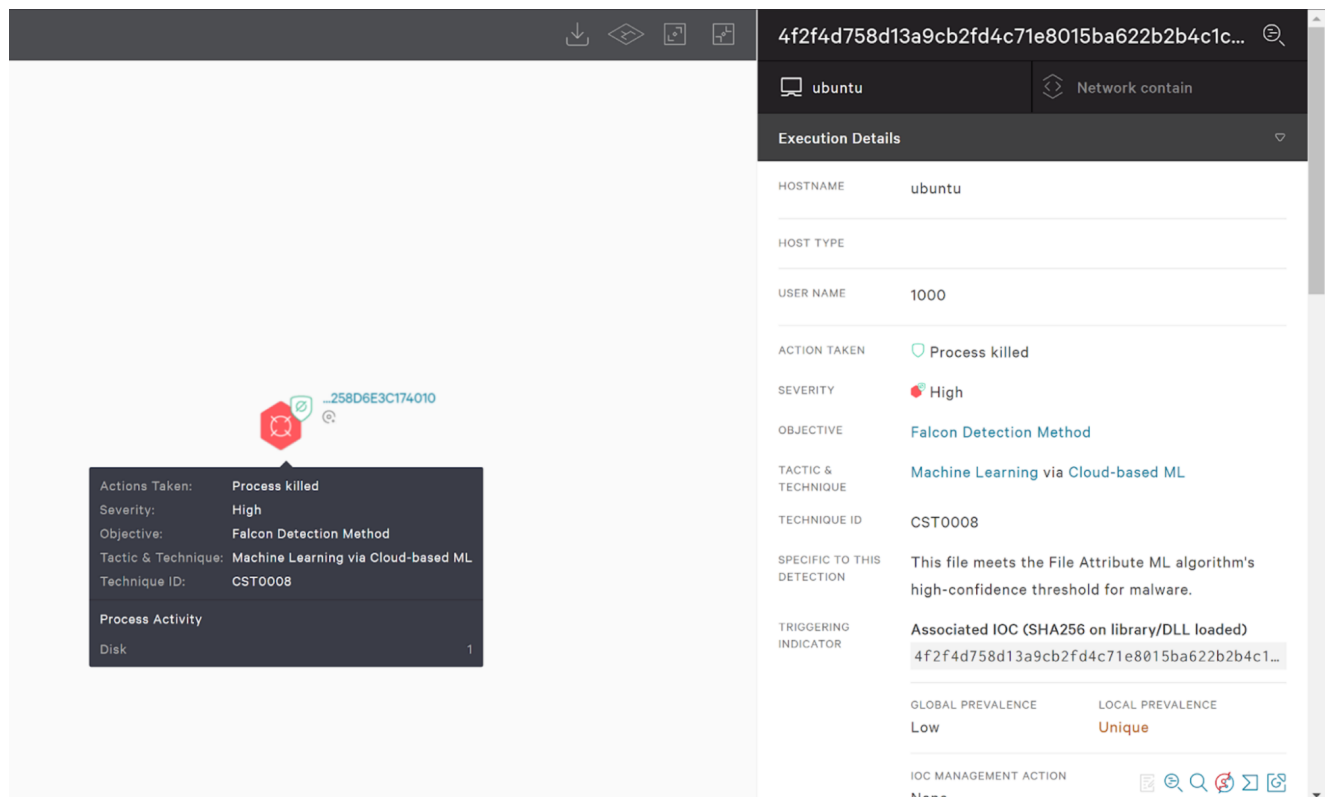
Mozi is a peer-to-peer (P2P) botnet network that utilizes the distributed hash table (DHT) system, implementing its own extended DHT. The distributed and decentralized lookup mechanism provided by DHT enables Mozi to hide C2 communication behind a large amount of legitimate DHT traffic.

Mirai: The Common Ancestor

Mirai malware has made a name for itself in the last few years, especially after its developer published Mirai's [source code](#). Similar to Mozi, Mirai abuses weak protocols and weak passwords, such as Telnet, to compromise devices using brute-forcing attacks.

With multiple Mirai variants emerging since its source code became public, the Linux trojan can be considered the common ancestor to many of today's Linux DDoS malware. While most variants add onto existing Mirai features or implement different communication protocols, at their core they share the same Mirai DNA.

Some of the most prevalent variants tracked by CrowdStrike researchers involve Sora, IZIH9 and Reikai. Compared to 2020, the numbers of identified samples for all three variants have increased by 33%, 39% and 83% respectively in 2021.



The screenshot displays the CrowdStrike Falcon console interface. On the left, a dark overlay shows a summary of the detection: Actions Taken: Process killed; Severity: High; Objective: Falcon Detection Method; Tactic & Technique: Machine Learning via Cloud-based ML; Technique ID: CST0008; Process Activity: Disk. The main panel on the right shows 'Execution Details' for a file with SHA256 hash 4f2f4d758d13a9cb2fd4c71e8015ba622b2b4c1c... on an ubuntu host. The details include: Hostname: ubuntu; Host Type: Network contain; User Name: 1000; Action Taken: Process killed; Severity: High; Objective: Falcon Detection Method; Tactic & Technique: Machine Learning via Cloud-based ML; Technique ID: CST0008; Specific to this Detection: This file meets the File Attribute ML algorithm's high-confidence threshold for malware; Triggering Indicator: Associated IOC (SHA256 on library/DLL loaded) 4f2f4d758d13a9cb2fd4c71e8015ba622b2b4c1c...; Global Prevalence: Low; Local Prevalence: Unique; IOC Management Action: None.

Fig. 5 – Falcon detection for Linux Mirai malware sample (Click to enlarge)

CrowdStrike Protection for Linux

Linux is one of the primary operating systems for many business-critical applications. As Linux servers can be found on premises and in private and public clouds, protecting them requires a solution that provides runtime protection and visibility for all Linux hosts, regardless of location.

The CrowdStrike Falcon® platform protects Linux workloads, including containers, running in all environments, from public and private clouds to on-premises and hybrid data centers. Using machine learning, artificial intelligence, behavior-based indicators of attack (IOAs) and custom hash blocking to defend Linux workloads against malware and sophisticated threats, the Falcon platform delivers complete visibility and context into any attack on Linux workloads.

Indicators of Compromise (IOCs)

File	SHA256
Mozi	<u>4790754ccd895626c67f0d63736577d363de7e7684b624d584615d83532d1414</u>
XorDDoS	<u>f85f13bf67bba755ec5f4c46d760f460a2dc137494d7edf64aeb22ddc2f30760</u>
Mirai	<u>4f2f4d758d13a9cb2fd4c71e8015ba622b2b4c1c26ceb1114b258d6e3c174010</u>

Additional Resources

- *Learn more about how the Falcon platform protects Linux systems in this solution brief.*
- *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.*