Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

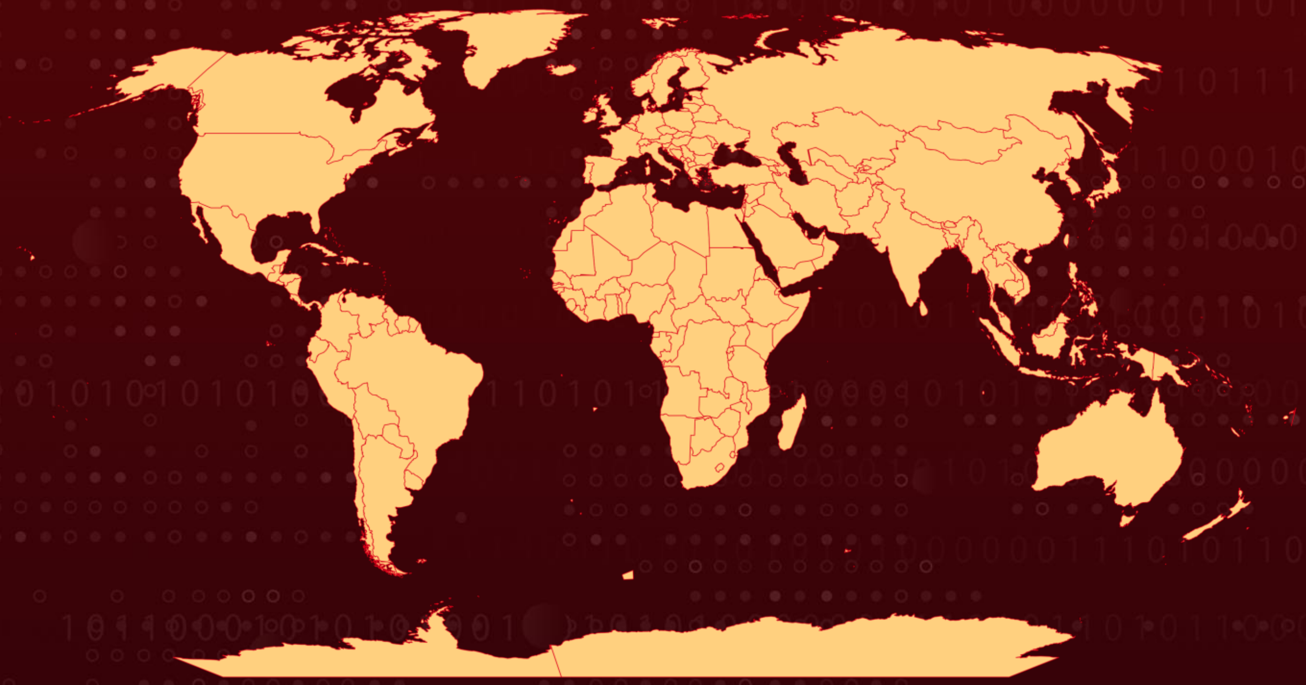
A New XorDDoS Linux Trojan That Launches Powerful DDoS Attacks

Date of Publication	Admiralty Code	TA Number
October 17, 2023	A1	TA2023418

Summary

First Appearance: July 28, 2023
Attack Region: Worldwide
Affected Platforms: Linux
Targeted Industries: Semiconductor, Telecom, Transportation, Finance, Insurance, Retail
Malware: XorDDoS Trojan
Attack: The XorDDoS Trojan, a Linux-based malware, orchestrates DDoS attacks through infected devices, with a recent campaign detected in 2023. Attackers employ scanning, persistence, and C2 infrastructure changes, requiring advanced detection to counter the evolving threat.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

The XorDDoS Trojan is a Linux-based malware that infects devices, turning them into zombies for launching DDoS attacks. A recent campaign involving XorDDoS Trojan was identified in July and August 2023, with a surge of activity starting on July 28, 2023.

#2

This campaign included multiple unique malware variants. Before infecting devices, the attackers conducted a scanning process to identify potential vulnerabilities, particularly focusing on an HTTP vulnerability related to directory traversal. They accessed the /etc/passwd file to obtain usernames, then used SSH brute-force attacks to gain initial access to the devices.

#3

The XorDDoS Trojan encrypts its data using an XOR encryption key. It collects essential information about the compromised device, including its identifier, OS version, malware version, memory status, and CPU information. The Trojan uses CRC codes for error detection during network communication.

#4

The malware communicates with C2 domains and can execute various commands, including stopping, launching DDoS attacks, downloading files, uploading files, sending system information, and obtaining configuration files. The malware employs multiple persistence mechanisms, including autorun tasks and services, to maintain its presence on infected devices.

#5

It also self-replicates, generating a large number of similar malware samples. The attackers have been using C2 domains for several years, and their network infrastructure is connected to previous campaigns in 2022. They have recently changed the IP addresses for their C2 domains, complicating detection efforts. Due to the shared web hosting infrastructure used by the attackers, detection of isolated connections as malicious or benign is challenging.

#6

Multiple connections to C2 IP addresses within a short timeframe are proposed as a better indicator of C2 traffic. The XorDDoS Trojan remains a global threat targeting Linux devices for DDoS attacks. The attackers have relocated their C2 servers to new IP addresses from public hosting services.

Recommendations

Implement Robust Security Measures: Ensure that robust security measures are in place, especially for Linux-based systems. Employ intrusion detection systems (IDS), intrusion prevention systems (IPS), and firewalls to safeguard your network.

Regular Software Updates and Patch Management: Keep all software and operating systems up-to-date with the latest security patches. Vulnerabilities are often exploited by malware, and timely updates can help prevent these attacks.

Enhance Password Security: Implement strong password policies, multi-factor authentication (MFA), and rate limiting for login attempts to protect against brute-force attacks. Regularly audit and change passwords, especially for critical systems.

Network Segmentation: Segment your network to limit lateral movement for attackers. Isolate sensitive systems from the rest of the network and implement strict access controls.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0001 Initial Access	TA0011 Command and Control	TA0040 Impact
TA0005 Defense Evasion	TA0010 Exfiltration	TA0003 Persistence	T1190 Exploit Public-Facing Application
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1584 Compromise Infrastructure	T1021.004 SSH
T1021 Remote Services	T1110 Brute Force	T1560.003 Archive via Custom Method	T1560 Archive Collected Data
T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1498 Network Denial of Service	T1053.005 Scheduled Task
T1053 Scheduled Task/Job			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	23.252.167[.]35 34.98.99[.]30 66.102.253[.]30 98.126.8[.]114 103.25.9[.]245 103.233.83[.]245 103.240.141[.]50 104.247.217[.]167 113.10.246[.]145 119.147.145[.]198 142.0.138[.]41 142.0.138[.]42 142.0.138[.]43 142.0.138[.]44 142.4.106[.]73 142.4.106[.]74 142.4.106[.]75 142.4.106[.]76 162.251.95[.]209 174.139.217[.]145 183.56.173[.]144 183.56.173[.]156 183.60.202[.]2 183.136.213[.]96 192.74.236[.]33 192.74.236[.]34 192.74.236[.]35 192.74.236[.]36 203.12.202[.]137
Domains	0o557[.]com 604418589[.]xyz www.98syn[.]com aldz[.]xyz syn.aldz[.]xyz p.assword[.]xyz linux.bc5j[.]com cdn.netflix2cdn[.]com dddgata789[.]com b12.dddgata789[.]com d14.dddgata789[.]com ddd.dddgata789[.]com p5.dddgata789[.]com ww.dnstells[.]com ndns.dsaj2a[.]com ndns.dsaj2a[.]org

TYPE	VALUE
Domains	gh.dsaj2a1[.]org ndns.dsaj2a1[.]org www.enoan2107[.]com a381422.f3322[.]net 1107791273.f3322[.]org aa369369.f3322[.]org shaoqian.f3322[.]org xlxl.f3322[.]org cdn.finance1num[.]com baidu.gddos[.]com soft8.gddos[.]com gggatat456[.]com aaa.gggatat456[.]com b12.gggatat456[.]com g14.gggatat456[.]com ppp.gggatat456[.]com www.ppp.gggatat456[.]com www1.gggatat456[.]com 8uc.gwd58[.]com ww.gzcfr5axf6[.]com www.gzcfr5axf6[.]com ww.gzcfr5axf7[.]com ndns.hcxiaoao[.]com ns1.hostasa[.]org ns2.hostasa[.]org ns3.hostasa[.]org ns4.hostasa[.]org linux.jum2[.]com lpjulidny7[.]com p0.lpjulidny7[.]com p2.lpjulidny7[.]com p3.lpjulidny7[.]com p4.lpjulidny7[.]com p5.lpjulidny7[.]com 2w5.mc150[.]cn ww.myserv012[.]com nishabud[.]com aaaaaaaaaa.re67das[.]com ww.s9xk32a[.]com ww.s9xk32b[.]com ww.s9xk32c[.]com ww.search2c[.]com ssh.upx[.]wang www.wangzongfacai[.]com bb.wordpressau[.]com bbb.wordpressau[.]com xran[.]xyz xxxatat456[.]com

TYPE	VALUE
Domains	aaa.xxxatat456[.]com b12.xxxatat456[.]com ppp.xxxatat456[.]com www.ppp.xxxatat456[.]com www.xxxatat456[.]com x14.xxxatat456[.]com zryl[.]online
SHA256	b8c4d68755d09e9ad47e0fa14737b3d2d5ad1246de5ef1b3c794b1339d8fe9f8 265a38c6dee58f912ff82a4e7ce3a32b2a3216bffd8c971a7414432c5f66ef11 1e823ae1e8d2689f1090b09dc15dc1953fa0d3f703aec682214750b9ef8795f1 989a371948b2c50b1d45dac9b3375cbbf832623b30e41d2e04d13d2bcf76e56b 20f202d4a42096588c6a498ddb1e92f5b7531cb108fca45498ac7cd9d46b6448 9c5fc75a453276dcd479601d13593420fc53c80ad6bd911aaeb57d8da693da43 ce0268e14b9095e186d5d4fe0b3d7ced0c1cc5bd9c4823b3dfa89853ba83c94f aeb29dc28699b899a89c990eab32c7697679f764f9f33de7d2e2dc28ea8300f5

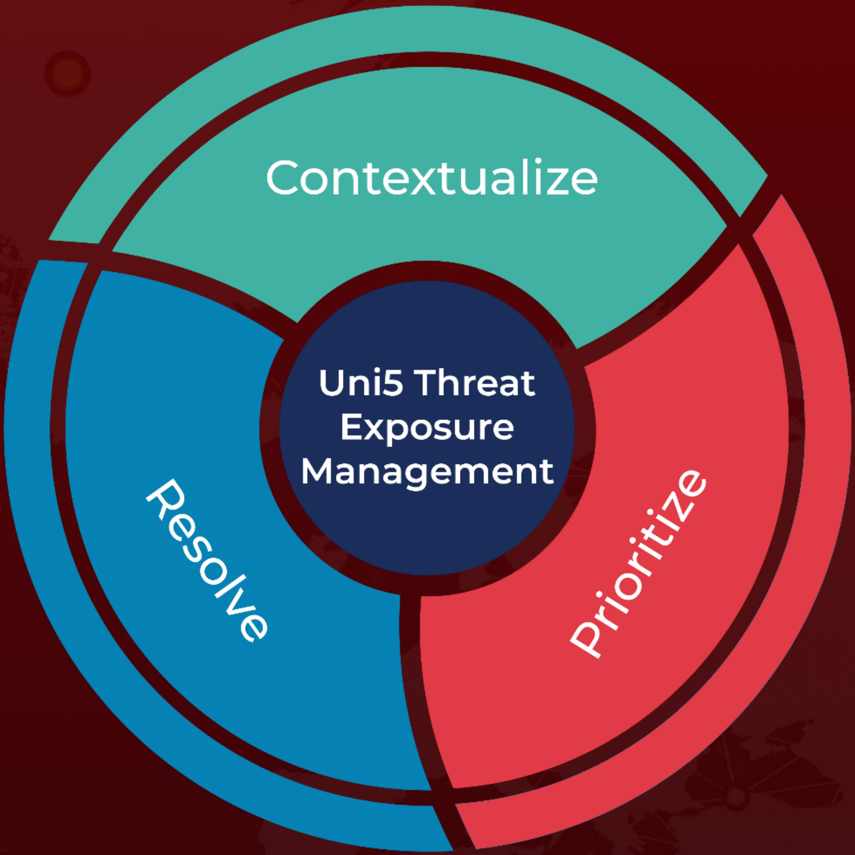
References

https://unit42.paloaltonetworks.com/new-linux-xorddos-trojan-campaign-delivers-malware/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 17, 2023 • 5:30 AM

More at www.hivepro.com