Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

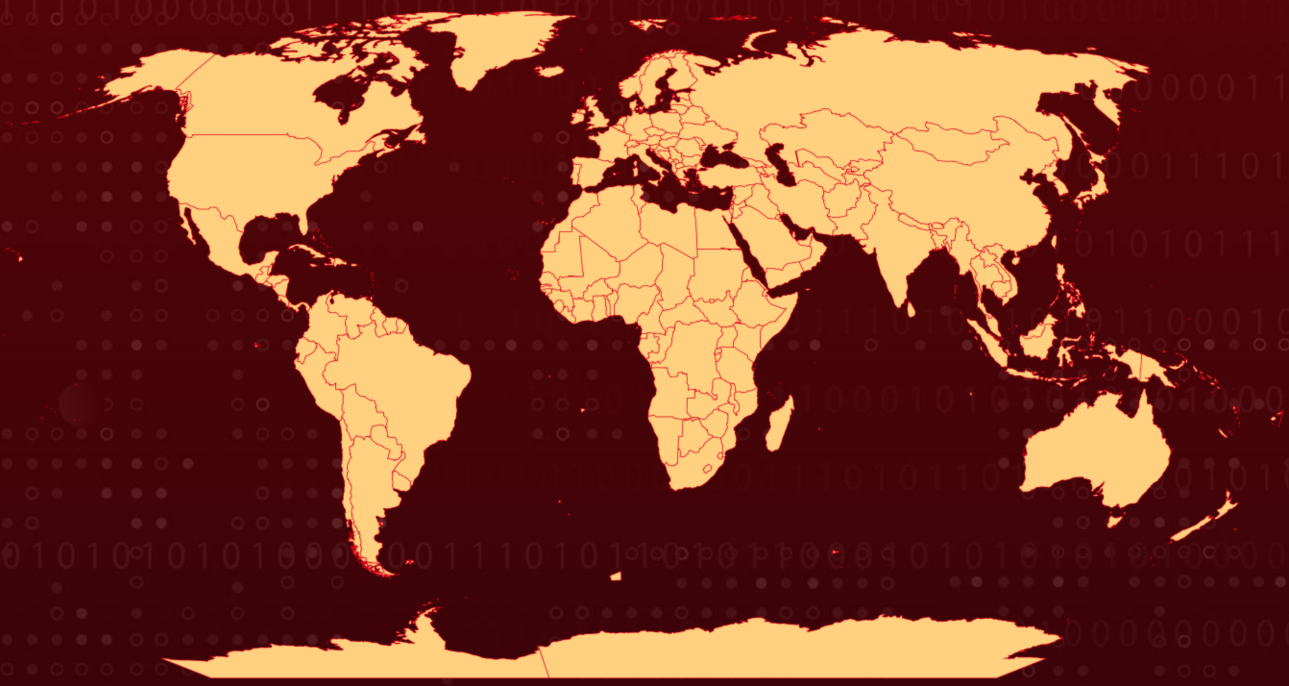
A New Cross-Platform ‘P2PInfect’ Worm Threatening Cloud Environments

Date of Publication	Admiralty Code	TA Number
July 20, 2023	A1	TA2023306

Summary

First Appearance: July 11, 2023
Attack Region: Worldwide
Affected Platform: Windows and Linux
Malware: P2PInfect
Targeted Industries: Cloud Technology
Attack: P2PInfect, a new cross-platform worm written in Rust, targets vulnerable Redis instances in cloud environments via the CVE-2022-0543 vulnerability, potentially posing a significant threat to over 307,000 systems.

Attack Regions



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

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2022-0543	Debian-specific Redis Server Lua Sandbox Escape Vulnerability	Debian-specific Redis Server	✗	✓	✓

Attack Details

#1

A new peer-to-peer (P2P) worm called P2PInfect, written in the Rust programming language making it highly scalable and potent, targets Redis, a widely used open-source database application within cloud environments. The worm exploits the CVE-2022-0543 vulnerability, allowing it to infect both Linux and Windows-based Redis instances.

#2

It’s identified over 307,000 unique Redis systems publicly communicating in the last two weeks, of which 934 may be vulnerable to the P2PInfect worm. Although not all 307,000 instances will be vulnerable, the worm will still attempt to compromise them.

#3

P2PInfect establishes initial access by exploiting the Lua sandbox escape vulnerability (CVE-2022-0543) and then establishes a P2P network to distribute additional malicious payloads, such as OS-specific scripts and scanning software, to newly infected Redis instances.

#4

The worm's cross-platform capabilities and use of a P2P network make it potent and scalable. This campaign is believed to be just the first stage of a potentially more sophisticated attack leveraging the robust P2P command and control (C2) network.

#5

The P2PInfect worm is designed to operate effectively in cloud container environments, where it can exploit Redis vulnerabilities. The worm exhibits multiple C2 features, including auto-updating, which allows attackers to enhance its performance by pushing new payloads into the network.

Recommendations

Regularly Update and Patch: Ensure that all software and applications, including Redis instances, are up-to-date with the latest security patches and updates. Vulnerabilities like CVE-2022-0543 can be mitigated through timely patching.

Monitor Redis Instances: Continuously monitor Redis instances, both on-premises and within cloud environments, to detect any suspicious activities or potential vulnerabilities. Implement monitoring tools that can alert administrators of any unusual behaviors.

Deploy Advanced Security Solutions: Invest in advanced security solutions, like intrusion detection systems (IDS), endpoint protection platforms (EPP), and cloud-delivered security services. These tools can help detect and block sophisticated threats like P2PInfect, providing an additional layer of defense for your organization.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0042 Resource Development
TA0007 Discovery	TA0005 Defense Evasion	TA0009 Collection	TA0011 Command and Control
T1190 Exploit Public-Facing Application	T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1021 Remote Services
T1005 Data from Local System	T1588 Obtain Capabilities	T1588.005 Exploits	T1588.006 Vulnerabilities
T1562 Impair Defenses	T1018 Remote System Discovery	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information
T1046 Network Service Discovery	T1095 Non-Application Layer Protocol	T1584 Compromise Infrastructure	T1021.004 SSH

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	35.183.81[.]182, 66.154.127[.]38, 66.154.127[.]39, 8.218.44[.]75, 97.107.96[.]14
SHA256	88601359222a47671ea6f010a670a35347214d8592bceaf9d2e8d1b303fe26d7, b1fab9d92a29ca7e8c0b0c4c45f759adf69b7387da9aebb1d1e90ea9ab7de76c, 68eaccf15a96fdc9a4961daffec5e42878b5924c3c72d6e7d7a9b143ba2bbfa9, 89be7d1d2526c22f127c9351c0b9eafccd811e617939e029b757db66dadc8f93

Patch Link

https://security-tracker.debian.org/tracker/CVE-2022-0543

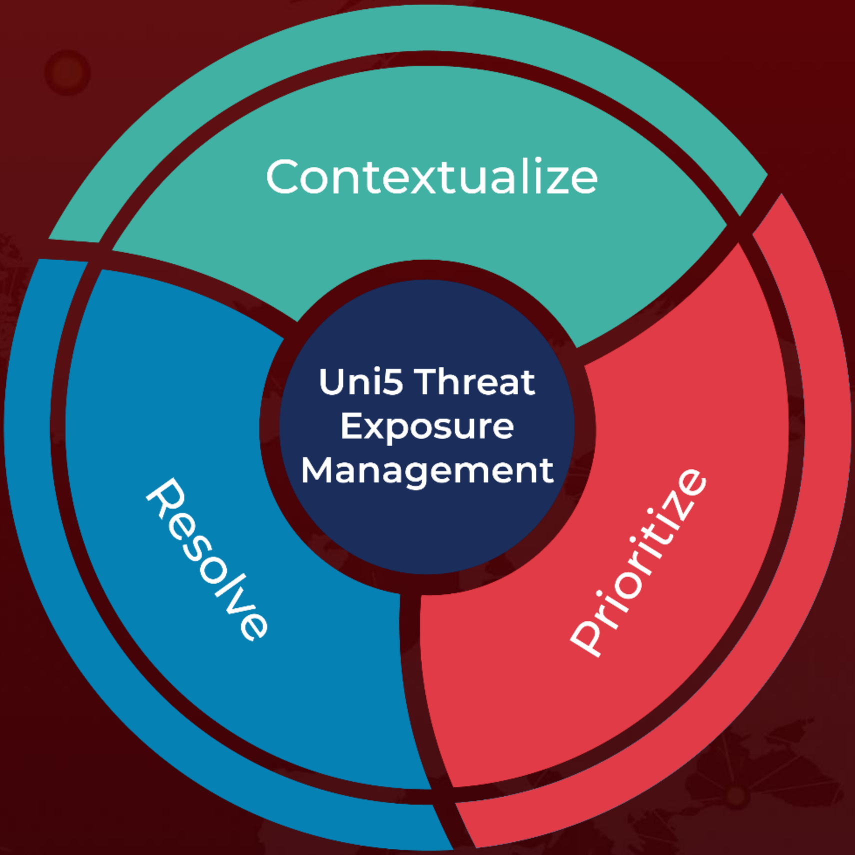
References

https://unit42.paloaltonetworks.com/peer-to-peer-worm-p2pinfect/

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

July 20, 2023 • 6:30 AM

More at www.hivepro.com