Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

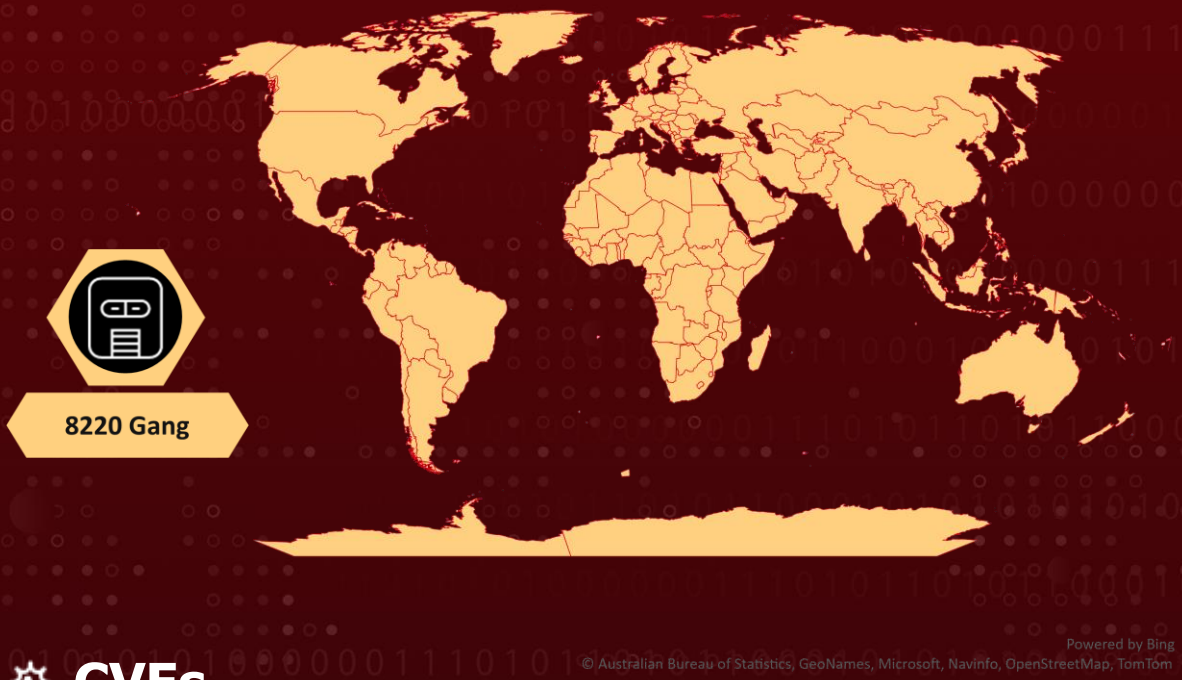
8220 Gang's Heist: Exploiting Oracle WebLogic for Cryptomining

Date of Publication	Admiralty Code	TA Number
July 4, 2024	A1	TA2024257

Summary

Threat Actor: 8220 Gang (aka Water Sigbin)
Malware: XMRig Cryptominer, PureCrypter loader
Attack Regions: Worldwide
Attack: The 8220 Gang, also known as Water Sigbin, has been aggressively targeting Oracle WebLogic servers to install cryptocurrency miners. Their sophisticated multi-stage loading technique efficiently deploys the PureCrypter loader and the XMRig crypto miner.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2017-3506	Oracle WebLogic Server OS Command Injection Vulnerability	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2	✗	✓	✓
CVE-2023-21839	Oracle WebLogic Server Unauthenticated RCE Vulnerability	Oracle WebLogic Server 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	✗	✓	✓

Attack Details

#1 The **8220 Gang**, also known as Water Sigbin, has been actively targeting Oracle WebLogic servers to deploy cryptocurrency miners as their final payload. They establish a foothold in the targeted environment by exploiting vulnerabilities in the Oracle WebLogic Server, notably CVE-2017-3506 and CVE-2023-21839, using PowerShell scripts to deploy the miners.

#2 All payloads in this campaign are protected using .Net Reactor, a .NET code protection software designed to prevent reverse engineering. This software obfuscates the code and incorporates anti-debugging techniques.

#3 The 8220 Gang employs fileless execution techniques, utilizing DLL reflective loading and process injection, which allows the malware to run solely in memory, evading disk-based detection mechanisms. The gang also uses a multi-stage loading technique to deliver the PureCrypter loader.

#4 This loader generates a unique identifier based on the victim's hardware information and communicates with the malware's command-and-control (C&C) server. It then downloads the final payload, which includes the XMRig cryptocurrency miner, a popular open-source mining software compatible with multiple operating systems.

Recommendations

Patch and Update Systems: Ensure that operating systems, applications, and system firmware are kept up to date with the latest security patches. Regularly update Oracle WebLogic servers to address known vulnerabilities like CVE-2017-3506 and CVE-2023-21839.

Enable Multi-Factor Authentication (MFA): Enforce MFA for all administrative access to Oracle WebLogic servers and critical systems. Implement MFA for remote access to strengthen authentication mechanisms.

Implement Network Segmentation: Isolate Oracle WebLogic servers from other critical systems and user networks to limit the impact of potential breaches. Use VLANs, firewalls, and access controls to create secure zones.

Integrate File Integrity Monitoring (FIM): Implement FIM solutions to detect unauthorized changes to critical files and configurations on Oracle WebLogic servers. Monitor for indicators of compromise (IoCs) and respond promptly to potential security breaches.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0040 Impact	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1047 Windows Management Instrumentation	**T1036** Masquerading	**T1036.005** Match Legitimate Name or Location	**T1140** Deobfuscate/Decode Files or Information
T1112 Modify Registry	**T1562.001** Disable or Modify Tools	**T1620** Reflective Code Loading	**T1055** Process Injection
T1055.012 Process Hollowing	**T1053.005** Scheduled Task	**T1057** Process Discovery	**T1012** Query Registry
T1518.001 Security Software Discovery	**T1082** System Information Discovery	**T1071** Application Layer Protocol	**T1001** Data Obfuscation
T1571 Non-Standard Port	**T1095** Non-Application Layer Protocol	**T1496** Resource Hijacking	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e6e69e85962a402a35cbc5b75571dab3739c0b2f3861ba5853dbd140bae4e4da, f4d11b36a844a68bf9718cf720984468583efa6664fc99966115a44b9a20aa33, 0bf87b0e65713bf35c8cf54c9fa0015fa629624fd590cb4ba941cd7cdeda8050, b380b771c7f5c2c26750e281101873772e10c8c1a0d2a2ff0aff1912b569ab93, 2e32c5cea00f8e4c808eae806b14585e8672385df7449d2f6575927537ce8884
IPv4	89[.]169[.]52[.]37
URLs	hxxp[:]//87[.]121[.]105[.]232/bin[.]ps1, hxxp[:]//79[.]110[.]49[.]232/plugin3[.]dll

Patch Links

https://www.oracle.com/security-alerts/cpuapr2017.html

https://www.oracle.com/security-alerts/cpujan2023.html

References

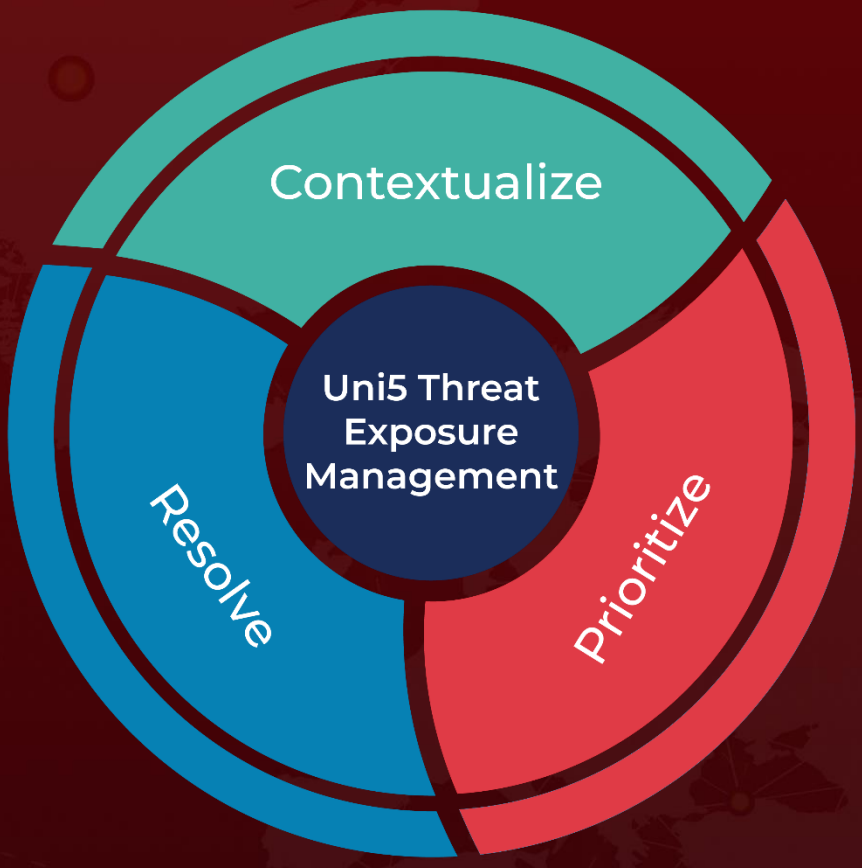
https://www.trendmicro.com/en_in/research/24/f/water-sigbin-xmrig.html

https://www.hivepro.com/threat-advisory/8220-gang-exploiting-vulnerabilities-in-cloud-environments-for-cryptocurrency-mining/

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 4, 2024 • 6:30 AM

More at www.hivepro.com