Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

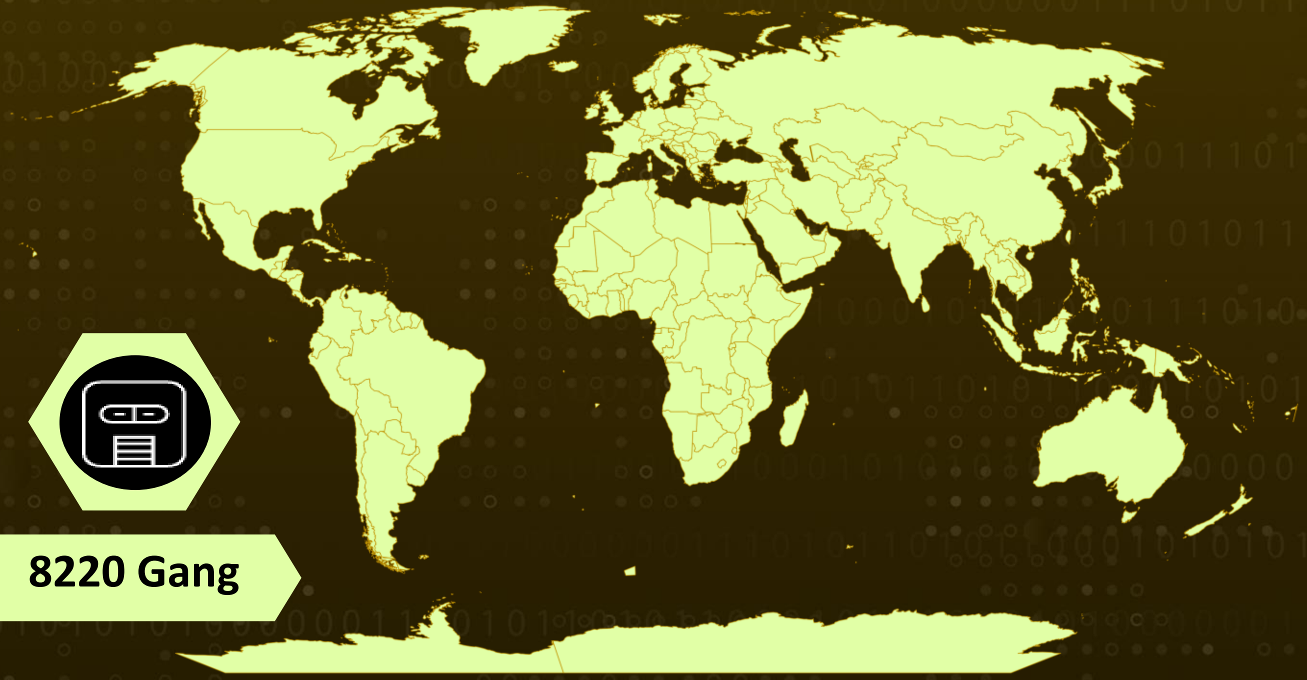
8220 Gang Exploiting Vulnerabilities in Cloud Environments for Cryptocurrency Mining

Date of Publication	Admiralty Code	TA Number
May 17, 2023	A1	TA2023233

Summary

First Appearance: 2017
Actor Name: 8220 Gang (8220 Mining Group)
Targeted Region: Worldwide
Affected Platform: Windows, Linux
Malware: Tsunami malware, XMRIG cryptominer
Targeted Industries: Technology, Cloud Services

Actor Map



8220 Gang

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

CVEs

CVE	NAME	AFFECTED PRODUCT	CISA	ZERO DAY	PATCH
CVE-2017-3506	Denial of service Vulnerability in Oracle WebLogic Server	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2	✗	✗	✓

Actor Details

#1

The 8220 Gang is an active threat group known for scanning and exploiting vulnerabilities in cloud and container environments. They specifically target applications such as Oracle WebLogic, Apache Log4j, Atlassian Confluence, and misconfigured Docker containers. Their objective is to exploit these vulnerabilities and deploy cryptocurrency mining software on compromised systems.

#2

To carry out their attacks, the gang uses various tools including Tsunami malware, XMRIG cryptominer, masscan, and spirit. These tools assist them in identifying and exploiting weaknesses in the targeted applications.

#3

One of their recent attacks involved exploiting a vulnerability known as CVE-2017-3506 in Oracle WebLogic. This vulnerability allows them to execute arbitrary commands remotely and gain unauthorized access to sensitive data or take control of the entire system. They leverage a specific entry point, the "wls-wsat/CoordinatorPortType" HTTP URI, to target Oracle WebLogic servers.

#4

In their attack payload, the gang employs a PowerShell script that is responsible for downloading and creating additional files needed for the attack. It exploits the CVE-2017-3506 vulnerability, which is a six-year-old security gap. Surprisingly, despite its age, the vulnerability still exists in some systems, making it a valuable target for the gang.

#5

Their ultimate goal is to install and execute a cryptocurrency miner on the compromised systems. They achieve this by injecting an encrypted resource file into the MS Build process and communicating with their command-and-control (C&C) servers. The C&C servers provide instructions and deliver the necessary files for the cryptocurrency mining operation.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
8220 Gang (8220 Mining Group)	China	Worldwide	Technology, Cloud Services
	MOTIVE		
	Financial gain		

Recommendations

Keep software and applications up to date: Regularly apply patches and updates to vulnerable applications such as Oracle WebLogic, Apache Log4j, and Atlassian Confluence. This helps to address known vulnerabilities and protect against exploitation by the 8220 Gang.

Implement strong security measures: Employ secure configurations, strong passwords, and appropriate access controls for your cloud and container environments. Use network segmentation to isolate critical systems and deploy intrusion detection and prevention systems (IDPS) to monitor network traffic for any malicious activity.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0003 Persistence	TA0011 Command and Control
TA0010 Exfiltration	TA0001 Initial Access	TA0006 Credential Access	TA0004 Privilege Escalation
T1140 Deobfuscate/Decode Files or Information	T1105 Ingress Tool Transfer	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1071 Application Layer Protocol	T1204.002 Malicious File	T1071.001 Web Protocols	T1566 Phishing
T1204 User Execution	T1190 Exploit Public-Facing Application	T1525 Implant Internal Image	T1132 Data Encoding
T1055 Process Injection	T1132.001 Standard Encoding	T1027 Obfuscated Files or Information	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1027.010 Command Obfuscation	T1055.002 Portable Executable Injection	T1620 Reflective Code Loading

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	http[:]//79[.]137[.]203[.]156/Ebvjmba.dat http[:]//185[.]17[.]0[.]19/bypass.ps1 http[:]//185[.]17[.]0[.]19/Nmfwg.png
IPV4	185[.]17[.]0[.]19 194[.]38[.]23[.]170 201[.]71[.]165[.]153 179[.]43[.]155[.]202
Domains	Work[.]letmaker[.]top su-94[.]letmaker[.]top

Patch Link

http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html

References

https://www.trendmicro.com/en_us/research/23/e/8220-gang-evolution-new-strategies-adapted.html

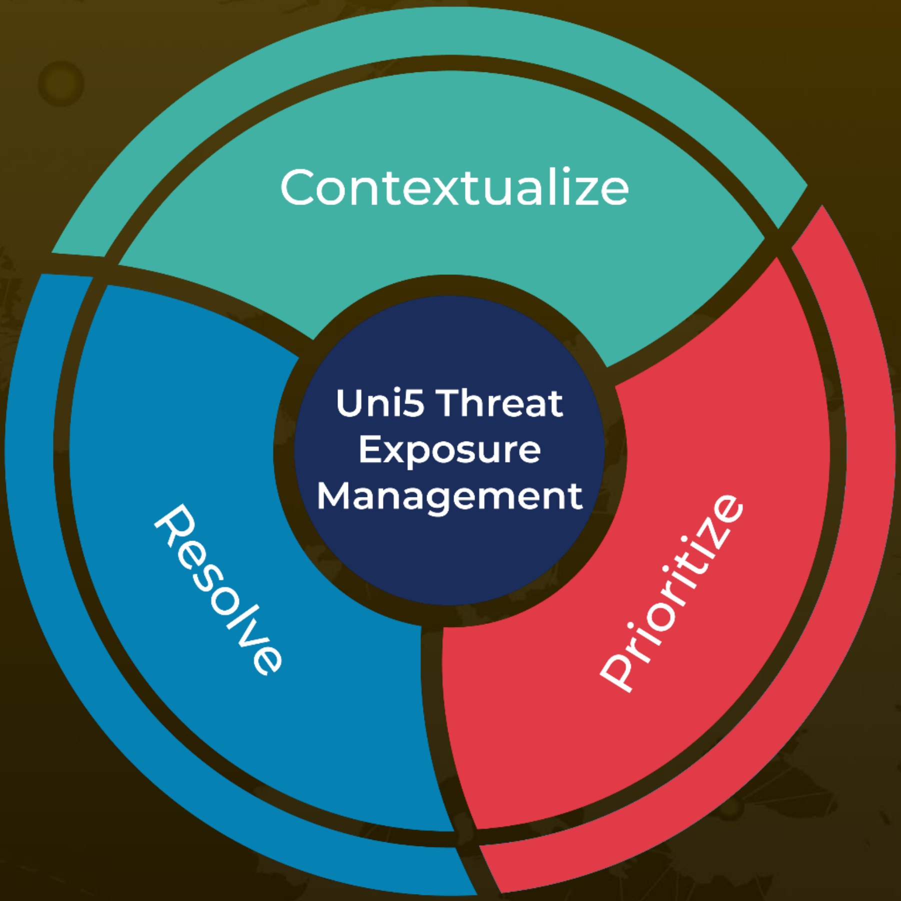
https://www.hivepro.com/8220-gang-leverages-scrubcrypt-in-cryptojacking-attacks/

https://www.hivepro.com/the-8220-cryptomining-gang-massively-expands-cloud-botnets/

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

May 17, 2023 • 3:30 PM

More at www.hivepro.com