

HiveForce Labs

THREAT ADVISORY

**ATTACK REPORT**

CRYSTALRAY Threat Actor Employs OSS to Strike 1,500 Targets

Date of Publication

July 12, 2024

Admiralty Code

A1

TA Number

TA2024271

Summary

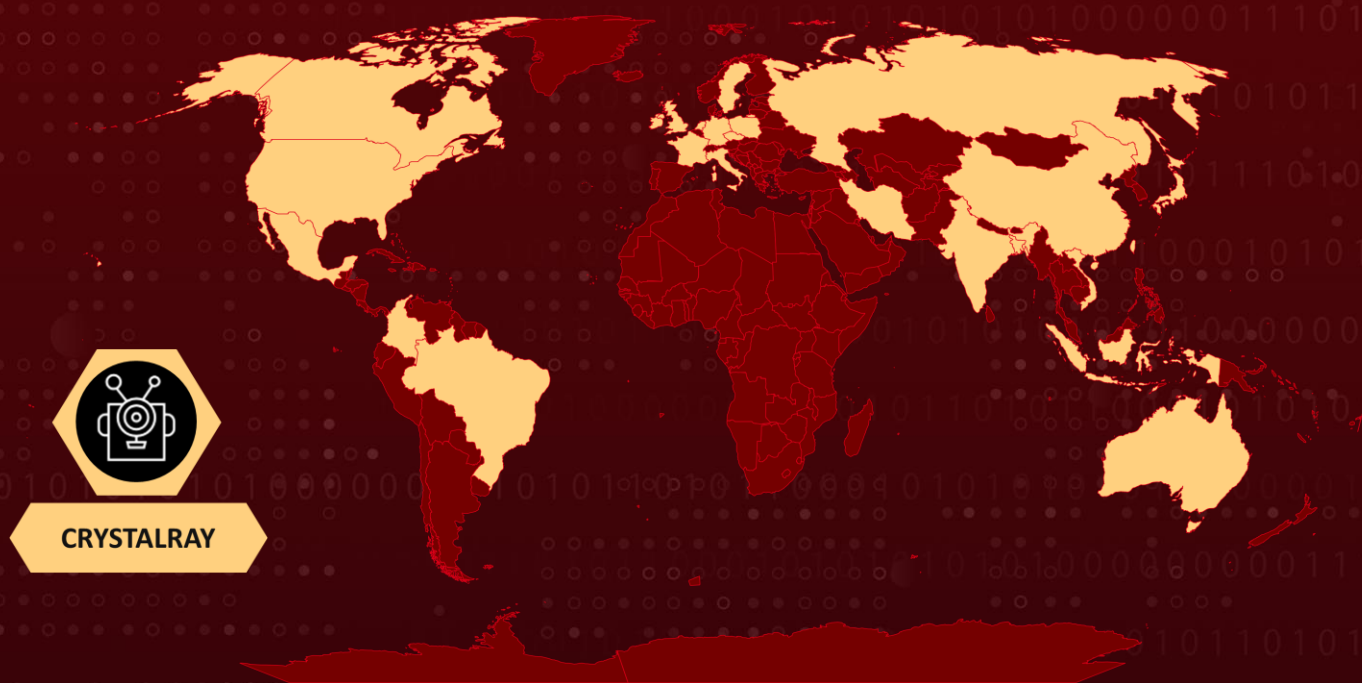
Threat Actor: CRYSTALRAY

OSS Tools: zmap, asn, httpx, nuclei, platypus, and SSH-Snake

Targeted Countries: Australia, Bangladesh, Brazil, Canada, China, Colombia, Czechia, France, Germany, India, Indonesia, Iran, Ireland, Italy, Japan, Korea, Mexico, Netherlands, Northern Ireland, Poland, Russia, Singapore, Sweden, Taiwan, UK, USA, Vietnam










Attack: CRYSTALRAY, a newly emerged cyber threat actor, has dramatically expanded its operations, employing advanced tactics and tools to steal credentials and deploy cryptocurrency miners. This cybercrime group's activities have surged tenfold, now affecting over 1,500 victims globally.

🗡️ Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-44877	CWP Control Web Panel OS Command Injection Vulnerability	CWP Control Web Panel			
CVE-2021-3129	Laravel Ignition File Upload Vulnerability	Laravel Ignition			
CVE-2019-18394	Ignite Realtime Openfire Server-Side Request Forgery (SSRF) vulnerability	Ignite Realtime Openfire through 4.4.2			

Attack Details

#1

A newly emerged threat actor, CRYSTALRAY, has significantly expanded its attack portfolio with sophisticated tactics and exploits, resulting in credential theft and the deployment of crypto miners. Leveraging the SSH-Snake tool and various open-source software (OSS) utilities such as zmap, asn, httpx, nuclei, and Platypus, CRYSTALRAY has orchestrated a wide-ranging campaign. Many of these tools originate from the reputable ProjectDiscovery OSS organization.

#2

CRYSTALRAY's operations have escalated tenfold, now impacting over 1,500 victims through extensive mass scanning, multi-vulnerability exploitation, and backdoor placements. The actor has targeted services like Activemq, Confluence, Metabase, Weblogic, Solr, Openfire, Rocketmq, and Laravel, exploiting vulnerabilities such as [CVE-2022-44877](#), [CVE-2021-3129](#), and CVE-2019-18394.

#3

To infiltrate their targets, CRYSTALRAY often adapts existing vulnerability proof-of-concepts to suit their payload needs. The Platypus web-based manager is employed to manage multiple reverse shell sessions on compromised systems. Concurrently, SSH-Snake remains the principal tool for propagating through breached networks.

#4

SSH-Snake not only facilitates the spread of infections but also exfiltrates captured keys and bash histories to CRYSTALRAY's command and control (C2) server, enhancing attack flexibility. Furthermore, CRYSTALRAY deploys crypto-miners to monetize breached systems by hijacking their processing power, using scripts to eliminate existing crypto-miners and maximize profits.

Recommendations



Enhance Detection and Prevention Measures: CRYSTALRAY's operations highlight the effectiveness of open source and penetration testing tools in maintaining persistent access to victim networks. Implement robust detection and prevention mechanisms to combat such tactics effectively.



Adopt Zero Trust Architecture: Embrace a Zero Trust security model where every user and device, both inside and outside the network perimeter, is verified before granting access. This approach reduces the risk of unauthorized access, even if perimeter defenses are breached



Implement Network Segmentation: Segment your network to limit the lateral movement of attackers and protect sensitive data. Deploy Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) solutions to monitor and respond to suspicious activities.



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

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0004</u> Privilege Escalation
<u>TA0005</u> Defense Evasion	<u>TA0006</u> Credential Access	<u>TA0007</u> Discovery	<u>TA0008</u> Lateral Movement
<u>TA0009</u> Collection	<u>TA0010</u> Exfiltration	<u>TA0011</u> Command and Control	<u>TA0040</u> Impact
<u>TA0043</u> Reconnaissance	<u>TA0042</u> Resource Development	<u>T1595</u> Active Scanning	<u>T1595.002</u> Vulnerability Scanning

<u>T1592</u> Gather Victim Host Information	<u>T1590</u> Gather Victim Network Information	<u>T1588</u> Obtain Capabilities	<u>T1588.002</u> Tool
<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	<u>T1190</u> Exploit Public-Facing Application	<u>T1059</u> Command and Scripting Interpreter
<u>T1555</u> Credentials from Password Stores	<u>T1496</u> Resource Hijacking	<u>T1041</u> Exfiltration Over C2 Channel	<u>T1657</u> Financial Theft
<u>T1071</u> Application Layer Protocol	<u>T1070</u> Indicator Removal	<u>T1010</u> Application Window Discovery	<u>T1005</u> Data from Local System
<u>T1053</u> Scheduled Task/Job	<u>T1053.003</u> Cron		

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	82[.]153[.]138[.]25, 157[.]245[.]193[.]241, 45[.]61[.]143[.]47
Domain	aextg[.]us[.]to, linux[.]kyun[.]li, ww-1[.]us[.]to
SHA256	a22b0b20052e65ad713f5c3a7427b514ee4f2388f6fda0510e3f5c9eb c78859e, c98d1d7686b5ff56e50264442ac27d4fb443425539de98458b7cfbf61 31b606f, da2bd678a49f428353cb570671aa04cddce239ecb98b825220af6d2a cf85abe9, 06bdd9a6753fba54f2772c1576f31db36f3b2b4e673be7e1ec9af3b18 0144eb9, da2bd678a49f428353cb570671aa04cddce239ecb98b825220af6d2a cf85abe9, 6a7b06ed7b15339327983dcd7102e27caf72b218bdaeb5b47d11698 1df093c52, db029555a58199fa6d02cbc0a7d3f810ab837f1e73eb77ec63d5367fa 772298b,

TYPE	VALUE
SHA256	f037d0cc0a1dc30e92b292024ba531bd0385081716cb0acd9e140944de8d3089, 1da7479af017ec0dacbada52029584a318aa19ff4b945f1bb9a51472d01284ec, b04db92036547d08d1a8b40e45fb25f65329fef01cf854caa1b57e0bf5faa605, fdced57d370ba188380e681351c888a31b384020dff7e029bd868f5dce732a90, 673a399699ce8dad00fa2dffee2aab413948408e807977451ccd0ceaa8b00b04, 364a7f8e3701a340400d77795512c18f680ee67e178880e1bb1fcda36ddbc12c, 8cbec5881e770ecea451b248e7393dfcfc52f8fbb91d20c6e34392054490d039, 908d7443875f3e043e84504568263ec9c39c207ff398285e849a7b5f20304c21, 2b945609b5be1171ff9ea8d1ffdca7d7ba4907a68c6f91d409dd41a06bb70154, a544d0ffd75918a4e46108db0ba112b7e95a88054ec628468876c7cf22c203a3, 04fec439f2f08ec1ad8352859c46f865a6353a445410208a50aa638d93f49451, 5a35b7708846f96b3fb5876f7510357c602da67417e726c702ddf1ad2e71f813, 7d003d3f5de5044c2c5d41a083837529641bd6bed13769d635c4e7f1b9147295, 7be2b15b56da32dc5bdb6228c2ed5c3bf3d8fc6236b337f625e3aff73a5c11d3, 08aaf6a45c17fa38958dd0ed1d9b25126315c6e0d93e7800472d0853ad696a87, 4f20eb19c627239aaf91c662da51ca7f298526df8e0eadccb6bbd7fc1b bcf0b3, 0841a190e50c6022100c4c56c233108aa01e5da60ba5a57c9778135f42def544, b04db92036547d08d1a8b40e45fb25f65329fef01cf854caa1b57e0bf5faa605, 4dc790ef83397af9d9337d10d2e926d263654772a6584354865194a1b06ce305, F2aef4c5f95664e88c2dd21436aa2bee4d2e7f8d32231c238e1aa407120705e4

Patch Details

Implement updates by transitioning to the most recent releases. CWP users are advised to update their versions to 0.9.8.1147 or higher.

Links:

<https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/master/cves/2021/CVE-2021-3129.yaml>

<https://github.com/igniterealtime/Openfire/pull/1497>

References

<https://sysdig.com/blog/crystalray-rising-threat-actor-exploiting-oss-tools/>

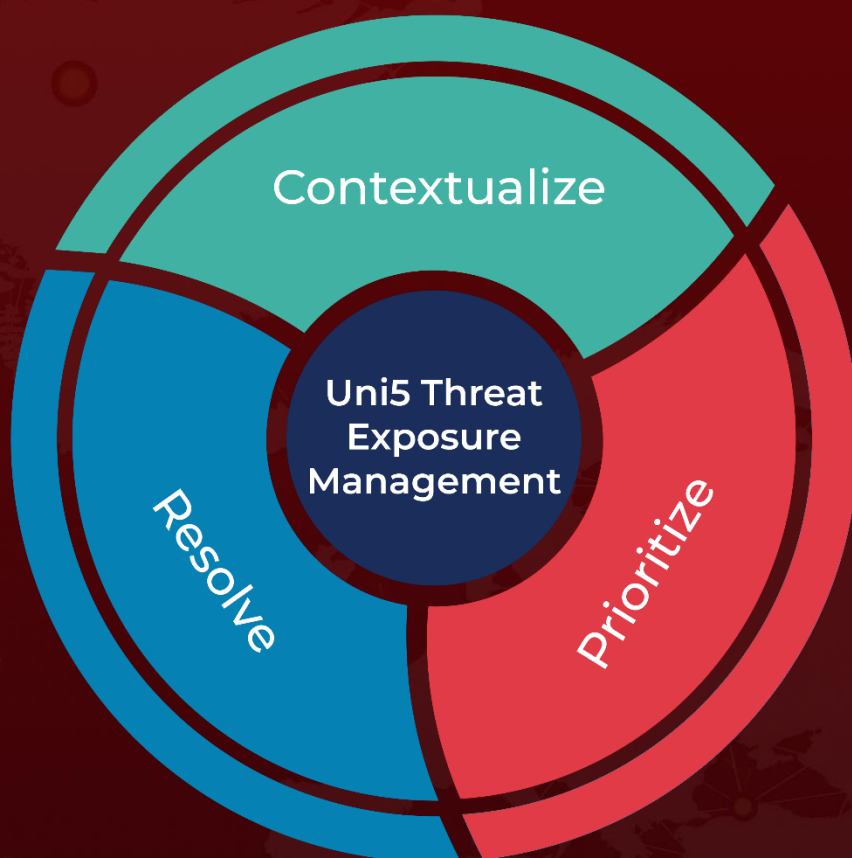
<https://hivepro.com/threat-advisory/control-web-panel-os-command-injection-exploitation-increases-after-poc-release/>

<https://hivepro.com/threat-advisory/llmjacking-an-attack-method-for-stealing-cloud-credentials/>

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 12, 2024 • 6:00 AM

© 2024 All Rights are Reserved by HivePro



More at www.hivepro.com