Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

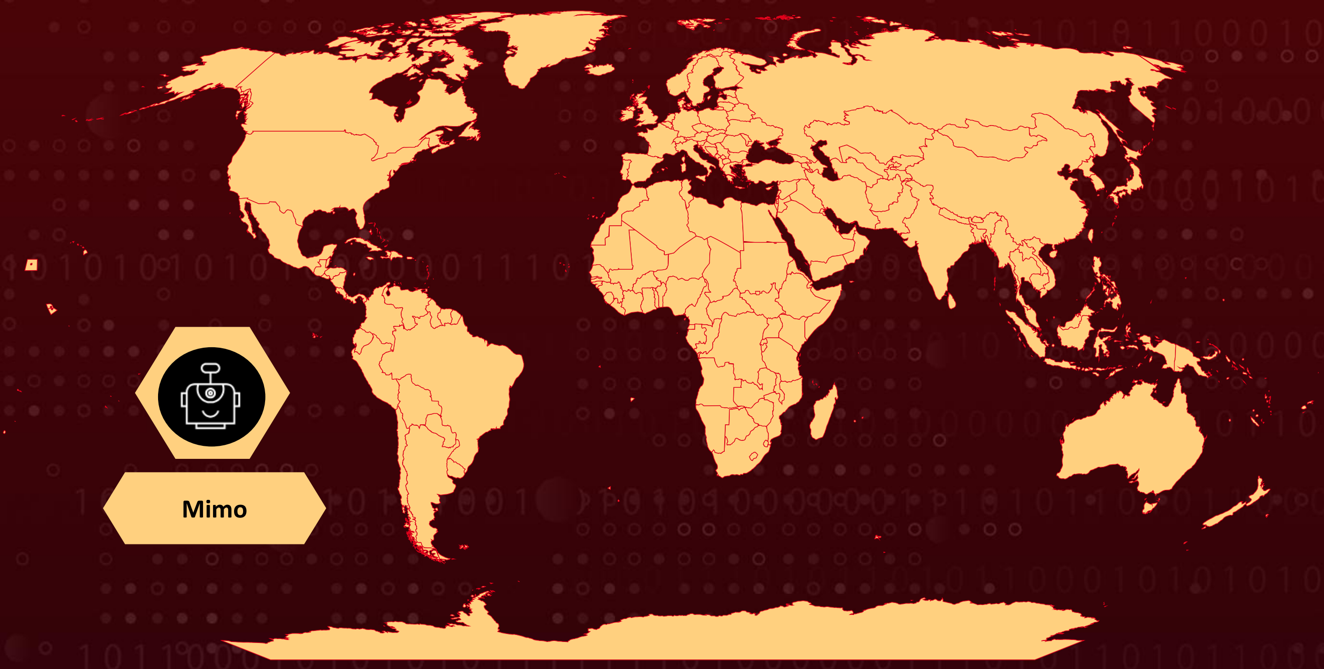
Mimo Threat Actor Exploits Critical RCE Vulnerability in Craft CMS

Date of Publication	Admiralty Code	TA Number
May 29, 2025	A1	TA2025167

Summary

First Seen: February 2025
Targeted Countries: Worldwide
Malware: XMRig
Targeted Industries: Finance
Threat Actor: Mimo (aka Hezb)
Attack: Mimo, a financially motivated threat actor, exploited a critical remote code execution vulnerability (CVE-2025-32432) in Craft CMS shortly after its disclosure in April 2025. The group used the flaw to deploy web shells, execute malicious scripts, and install payloads like XMRig (a crypto miner) and residential proxyware for monetization. They also chained this with another Yii framework vulnerability (CVE-2024-58136) to escalate privileges and maintain persistence. Organizations using Craft CMS are strongly urged to act quickly and apply patches immediately.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-32432	Craft CMS Remote Code Execution Vulnerability	Craft CMS	✓	✗	✓
CVE-2024-58136	Yiiframework Yii Improper Protection of Alternate Path Vulnerability	Yiiframework Yii	✓	✓	✓

Attack Details

#1

A financially motivated threat actor known as Mimo has been exploiting a critical remote code execution (RCE) vulnerability in Craft CMS, identified as CVE-2025-32432. This vulnerability, stemming from insecure deserialization in the image transformation feature, allows unauthenticated attackers to execute arbitrary code on affected servers. The flaw discovered in February 2025 and publicly disclosed in April, Mimo swiftly weaponized the flaw, launching a widespread campaign to compromise vulnerable systems.

#2

The attack chain begins with the exploitation of Craft CMS's image transformation feature. Attackers send specially crafted POST requests to manipulate the server and upload a PHP web shell. Once the web shell is in place, it downloads and executes a shell script named "4l4md4r.sh," which deploys additional malware. The primary payloads observed include a cryptocurrency miner (XMRig) and residential proxyware, both used to monetize the compromised systems by mining cryptocurrency and selling bandwidth to third parties.

#3

A notable aspect of this campaign is the chaining of CVE-2025-32432 with another critical vulnerability in the Yii framework (CVE-2024-58136), which Craft CMS relies on. This combination allows attackers to escalate their access and maintain persistent control over the targeted servers.

#4

The Mimo intrusion set, active since at least 2022, has previously exploited vulnerabilities in Apache Log4j, Atlassian Confluence, and Apache ActiveMQ. Their swift adaptation to newly disclosed vulnerabilities, such as CVE-2025-32432, highlights their technical agility and the evolving threat landscape. The Mimo campaign serves as a stark reminder of the importance of rapid vulnerability management and proactive threat detection in the face of increasingly sophisticated cyber threats

Recommendations

Immediately Apply Security Patches: Upgrade Craft CMS to the latest patched versions (3.9.15, 4.14.15, or 5.6.17) that address CVE-2025-32432. Ensure all dependencies, especially the Yii framework, are also updated to eliminate the risk of chaining vulnerabilities (e.g., CVE-2024-58136).

Audit and Harden Server Configurations: Disable or restrict access to unnecessary features like image transformation endpoints if not in use. Limit public exposure of the admin panel and sensitive CMS functionalities by using IP whitelisting, VPNs, or access control lists (ACLs). Run the CMS with the minimum required privileges and avoid root-level execution of web services.

Implement Endpoint and Network Detection: Use endpoint detection and response (EDR) tools capable of identifying LD_PRELOAD abuse and dynamic library injections. Deploy web application firewalls (WAFs) to inspect and block suspicious payloads, especially on Craft CMS endpoints. Employ DNS filtering and network segmentation to prevent C2 communication and lateral movement.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
TA0003 Persistence	**TA0011** Command and Control	**TA0005** Defense Evasion	**TA0040** Impact
T1588 Obtain Capabilities	**T1588.005** Exploits	**T1543** Create or Modify System Process	**T1588.006** Vulnerabilities
T1204 User Execution	**T1190** Exploit Public-Facing Application	**T1068** Exploitation for Privilege Escalation	**T1564** Hide Artifacts

T1070 Indicator Removal	T1071 Application Layer Protocol	T1496 Resource Hijacking	T1059 Command and Scripting Interpreter
T1486 Data Encrypted for Impact	T1505.003 Web Shell	T1505 Server Software Component	T1059.006 Python
T1584 Compromise Infrastructure			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1aa4d88a38f5a27a60cfc6d6995f065da074ee340789ed00ddc29abc29ea671e, 2e46816450ad1b4baa85e2a279031f37608657be93e1095238e2b6c36bbb3fd5, 3a71680ffb4264e07da4aaca16a3f8831b9a30d444215268e82b2125a98b94aa, 7868cb82440632cc4fd7a451a351c137a39e1495c84172a17894daf1d108ee9a, fc04f1ef05847607bce3b0ac3710c80c5ae238dcc7fd842cd15e252c18dd7a62, 0aa7571d06532fea194a62091a812557a8f8b8d616ffd923df766a4871f4a918
SHA1	2b76bc5457143d069676587401cad105bfbd53f3, 43df852fc522d1b2ea1d6a888ad2e77e42eb5c31, 984c30f0bc39ae78152a66808c4bf9ae4b0c51d9, f7f2ef6f65d301e78a1cc855c22dd9395ed5e507
MD5	03471b7a82e2001714b355aaab10c532, af2596fb1309272902006eebe07c93eb, d8fa6e6c7bc700baef9ad24ca471612c, e11365871cc409651fb216d2f5253a6c

TYPE	VALUE
Bitcoin Address	15Jz1fmreZx9wG93DKjTXMhuLpPpCgvEQk, 1CSfam568zRscwyiYXMwhha9MDmZLo1Ewm, 1JdgXqDpmBSqMjAb3zHia8o8ppQf8pGsac, 3BhtK1j8EBvpFsMpPAiVtZL2WXgjH75Erw
URLs	hxxp[://]mail[.]n1tr0[.]online/, hxxp[://]windows[.]n1tro[.]cyou:4544, hxxp[://]windows[.]n1tro[.]cyou:4544/api/keys/add, hxxp[://]dos[.]n1tro[.]cyou, hxxp[://]dos[.]n1tro[.]cyou/, hxxp[://]windows[.]n1tro[.]cyou, hxxp[://]windows[.]n1tro[.]cyou/, hxxp[://]dos[.]n1tro[.]cyou, hxxp[://]dos[.]n1tro[.]cyou/, hxxp[://]windows[.]n1tro[.]cyou, hxxp[://]windows[.]n1tro[.]cyou/
Host Name	windows[.]n1tro[.]cyou, dos[.]n1tro[.]cyou
Domain	n1tr0[.]online, n1tro[.]cyou
IPv4	85[.]106[.]113[.]168
Email Address	4l4md4r[@]proton[.]me

Patch Details

CVE-2025-32432: Upgrade Craft CMS to versions 3.9.15, 4.14.15, and 5.6.17 or later versions.

CVE-2024-58136: Upgrade Yii to 2.0.52 or later versions.

Links:
https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47

https://github.com/yiisoft/yii2/pull/20232

References

https://blog.sekoia.io/the-sharp-taste-of-mimolette-analyzing-mimos-latest-campaign-targeting-craft-cms/

https://sensepost.com/blog/2025/investigating-an-in-the-wild-campaign-using-rce-in-craftcms/

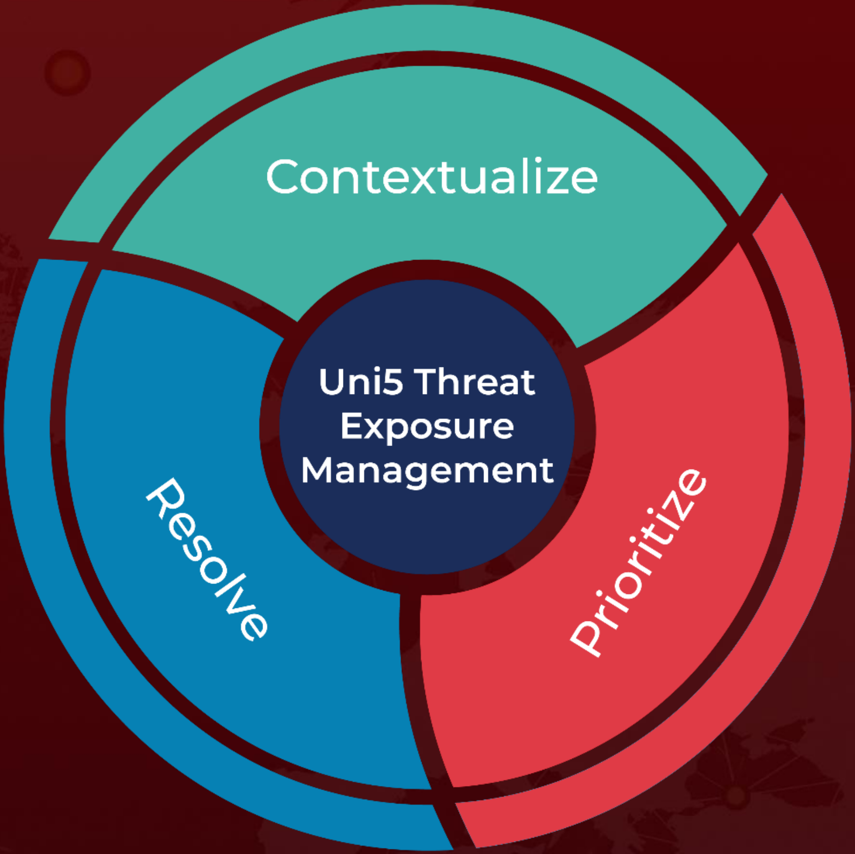
https://asec.ahnlab.com/en/60440/

https://www.esecurityplanet.com/cybersecurity/craft-cms-flaws-exploited/

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 29, 2025 • 8:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com