

Date of Publication  
June 2, 2025



HiveForce Labs  
WEEKLY  
**THREAT DIGEST**

**Attacks, Vulnerabilities, and Actors**

26 MAY to 1 JUNE 2025

# Table Of Contents

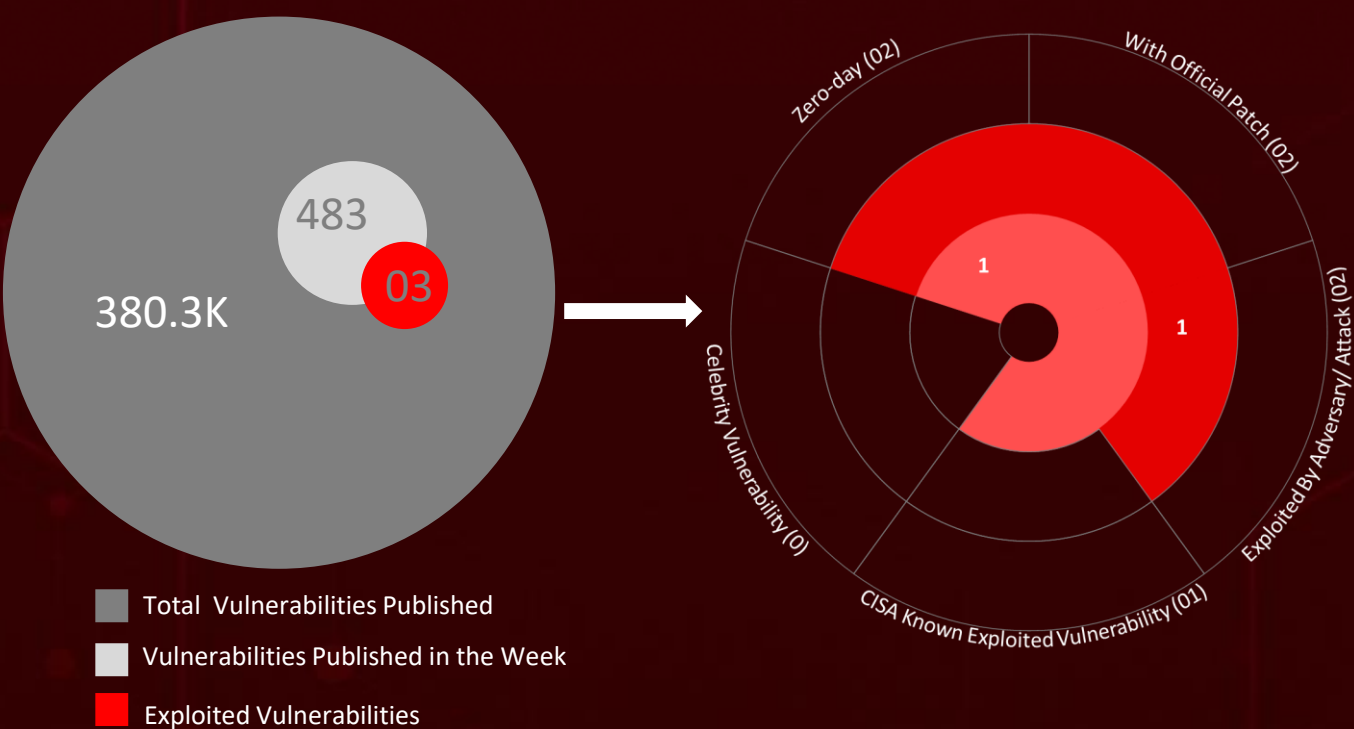
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	13
<u>Recommendations</u>	16
<u>Threat Advisories</u>	17
<u>Appendix</u>	18
<u>What Next?</u>	19

# Summary

HiveForce Labs has observed a significant surge in cybersecurity threats, underscoring the growing complexity and frequency of cyber incidents. Over the past week, **five** major attacks were detected, **three** critical vulnerabilities were actively exploited, and **three** threat actor groups were closely monitored, reflecting an alarming escalation in malicious activities.

Among the notable incidents, a sophisticated malware campaign is leveraging **AI-generated TikTok videos** to lure victims into executing malicious PowerShell commands, cleverly disguised as software activation instructions. Meanwhile, a new **Dero cryptocurrency mining** operation targets exposed Docker APIs, hijacking containers and transforming them into zombie nodes to silently spread the infection across environments.

In the world of zero-day exploits, **Mimo**, a financially driven hacking group, rapidly weaponized a critical remote code execution flaw (**CVE-2025-32432**) in Craft CMS just days after its disclosure in April 2025. Additionally, a severe vulnerability (**CVE-2025-47577**) in the TI WooCommerce Wishlist WordPress plugin is placing over 100,000 active websites at immediate risk. With **no official patch available**, we are advising security experts to disable the plugin to mitigate exposure. These escalating threats highlight the increasing sophistication of cyber adversaries and reinforce the urgent need for proactive, resilient cybersecurity measures to combat the rapidly evolving global threat landscape.



# High Level Statistics

5

Attacks  
Executed

- [Vidar](#)
- [StealC](#)
- [Dero](#)
- [XMRig](#)
- [TOUGHPROGRESS](#)

3

Vulnerabilities  
Exploited

- [CVE-2025-32432](#)
- [CVE-2024-58136](#)
- [CVE-2025-47577](#)

3

Adversaries in  
Action

- [Void Blizzard](#)
- [Mimo](#)
- [APT41](#)



# Insights

## Dero Campaign

Turns Unsecured Docker Environments into Crypto Mining Hubs

## Craft CMS at Risk:

**Mimo** Exploits New Vulnerability for Crypto Mining and Web Shells

**Void Blizzard's** Rising Cyberattacks put Aviation, Defense, and Government at Risk

**APT41** Uses Google Calendar for Covert Cyberattacks: A New Era of Cloud-Based Threats

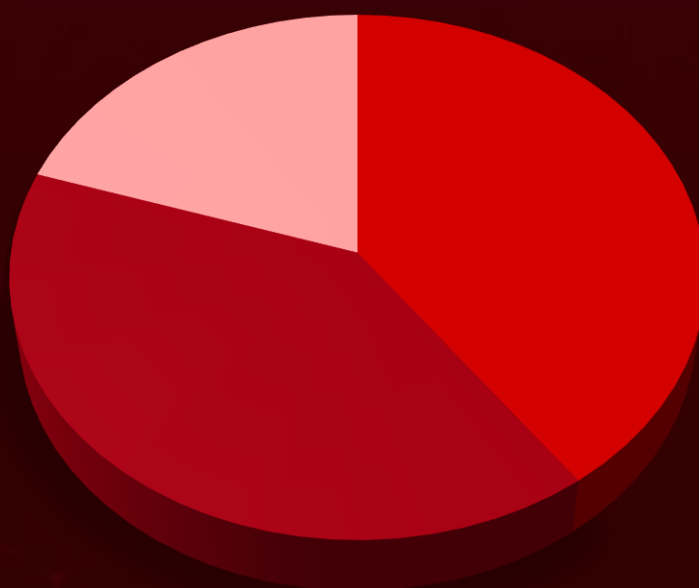
## No Patch Yet: CVE-2025-

**47577** Flaw in WooCommerce Plugin Threatens Over **100K** WordPress Sites

## AI-Driven TikTok Malware Campaign:

PowerShell Commands Deliver StealC and Vidar Malware

## Threat Distribution



■ Cryptominer

■ Stealer

■ Framework

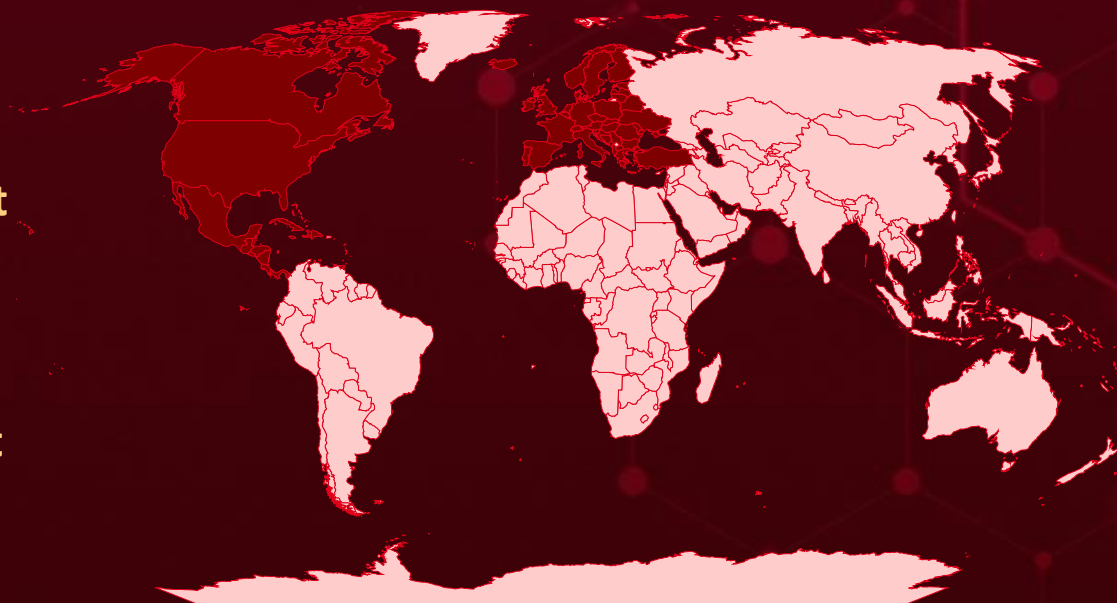


# Targeted Countries

Most



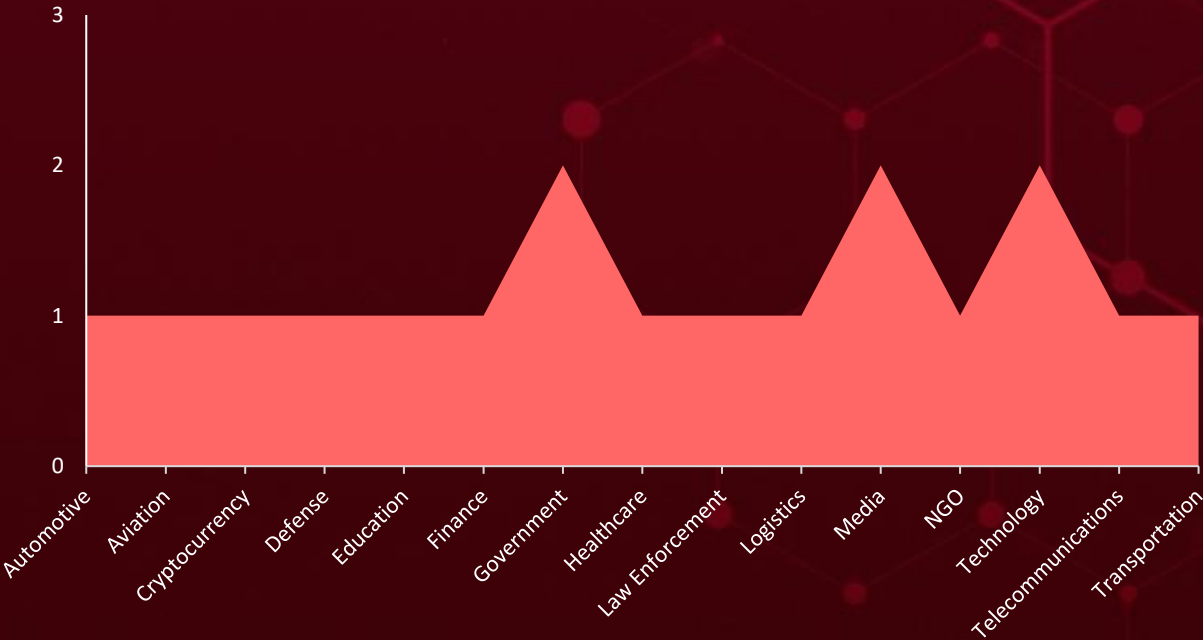
Least



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

Countries	Countries	Countries	Countries
United States	Switzerland	Sweden	Brazil
Turkey	Croatia	Holy See	Cyprus
Canada	Cuba	Trinidad and Tobago	Guadeloupe
United Kingdom	Italy	Honduras	Djibouti
Ukraine	Czech Republic	Hungary	Guinea
France	Liechtenstein	Iceland	South Africa
Albania	Denmark	Latvia	Guinea-Bissau
Serbia	Luxembourg	Norway	Suriname
Andorra	Dominica	Malta	Guyana
Jamaica	Mexico	Montenegro	Togo
Antigua and Barbuda	Dominican Republic	Austria	Brunei
Bahamas	Monaco	Romania	Angola
Barbados	El Salvador	Eswatini	Bolivia
Ireland	Netherlands	Paraguay	Burkina Faso
Belarus	Estonia	Gabon	Bahrain
Lithuania	North Macedonia	Sri Lanka	Burundi
Belgium	Finland	Gambia	Bangladesh
Moldova	Panama	North Korea	Cabo Verde
Belize	Portugal	Georgia	Philippines
Nicaragua	Germany	Russia	India
Bosnia and Herzegovina	Saint Kitts & Nevis	Australia	Qatar
Poland	Greece	DR Congo	Indonesia
Bulgaria	San Marino	Ghana	Iran
Saint Lucia	Grenada	Tajikistan	Samoa
Slovenia	Slovakia	Botswana	Iraq
Costa Rica	Guatemala	Fiji	Senegal
	Spain	Greenland	Cambodia
	Haiti	Pakistan	Singapore

# Targeted Industries



## TOP MITRE ATT&CK TTPs

<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1036</u></b> Masquerading	<b><u>T1041</u></b> Exfiltration Over C2 Channel
<b><u>T1204</u></b> User Execution	<b><u>T1566</u></b> Phishing	<b><u>T1140</u></b> Deobfuscate/Decode Files or Information	<b><u>T1102</u></b> Web Service	<b><u>T1027</u></b> Obfuscated Files or Information
<b><u>T1543</u></b> Create or Modify System Process	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1566.001</u></b> Spearphishing Attachment	<b><u>T1496</u></b> Resource Hijacking	<b><u>T1588.005</u></b> Exploits
<b><u>T1505</u></b> Server Software Component	<b><u>T1505.003</u></b> Web Shell	<b><u>T1204.002</u></b> Malicious File	<b><u>T1564</u></b> Hide Artifacts	<b><u>T1072</u></b> Software Deployment Tools

# Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Vidar</u>	Vidar is a variant of the Arkei malware, designed to exploit legitimate platforms like Steam and Telegram as Dead Drop Resolvers (DDR) to hide its command-and-control (C&C) server details. It harvests sensitive data from web browsers and digital wallets, making it a serious threat by enabling the theft of personal information and cryptocurrency.	Social Engineering via AI-generated TikTok videos	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft, C&C Obfuscation	TikTok
Stealer			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	3bb81c977bb34fadb3bdeac7e61193dd009725783fb2cf453e15ced70fc39e9b, b8d9821a478f1a377095867aeb2038c464cc59ed31a4c7413ff768f2e14d3886		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>StealC</u>	Stealc is developed in C and leverages WinAPI functions. It primarily targets data from web browsers, browser extensions, desktop cryptocurrency wallets, and other applications.	Social Engineering via AI-generated TikTok videos	-
		IMPACT	AFFECTED PLATFORM
		Credential Theft, Data Exposure	TikTok
			PATCH LINK
TYPE			
Stealer			
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	afc72f0d8f24657d0090566ebda910a3be89d4bdd68b029a99a19d146d63adc5		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<b><u>Dero</u></b>	The Dero cryptocurrency miner, developed in Golang and packed with UPX, is part of an ongoing mining campaign that targets exposed Docker APIs. It hijacks vulnerable environments, converting containers into botnet nodes to propagate the infection and mine cryptocurrency.	Exploit Public-Facing Application	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
		Resource Drain, Infrastructure Hijacking, Reputation Damage	Windows, Linux
			<b>PATCH LINK</b>
			-
<b>TYPE</b>			
Cryptominer			
<b>ASSOCIATED ACTOR</b>			
-			
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	e4aa649015b19a3c3350b0d897e23377d0487f9ea265fe94e7161fed09f283cf		
Domains	d[.]windowsupdatesupport[.]link, h[.]wiNdowsupdatesupport[.]link		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>XMRig</u>	XMRig is an open-source cryptocurrency miner commonly used to mine Monero (XMR). Cybercriminals frequently leverage it in cryptojacking attacks, covertly exploiting victims’ computing resources to generate cryptocurrency.	Exploiting Software Vulnerabilities	CVE-2025-32432 CVE-2024-58136
		IMPACT	AFFECTED PRODUCTS
Operational Disruption, Financial Loss		Craft CMS, Yiiframework Yii	
		PATCH LINK	
		<a href="https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47">https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47</a> , <a href="https://github.com/yiisoft/yii2/pull/20232">https://github.com/yiisoft/yii2/pull/20232</a>	
TYPE			
Cryptominer			
ASSOCIATED ACTOR			
Mimo			
IOC TYPE	VALUE		
SHA256	3a71680ffb4264e07da4aaca16a3f8831b9a30d444215268e82b2125a98b94aa		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE	
<u>TOUGHPROGRESS</u>	TOUGHPROGRESS is an advanced malware framework focused on stealth, persistence, and control. It uniquely uses Google Calendar as a command-and-control (C2) channel by embedding encrypted payloads in event descriptions. With a modular design, it deploys three sequential payloads, each performing specific functions and employing evasion techniques like memory-resident execution, encryption, compression, process hollowing, and control flow obfuscation.	Spear-phishing Attachment	-	
		IMPACT	AFFECTED PRODUCT	
		Persistent System Compromise, Data Theft and Espionage	-	
TYPE	Framework		PATCH LINK	
ASSOCIATED ACTOR				
APT41			-	
IOC TYPE	VALUE			
SHA256	3b88b3efbdc86383ee9738c92026b8931ce1c13cd75cd1cda2fa302791c2c4fb			





The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.




# Vulnerabilities Exploited


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-32432</u>		Craft CMS	Mimo (aka Hezb)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:craftcms:craft_cms :*:*:*:*:*:*:*	XMRig
Craft CMS Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	<a href="https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47">https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47</a>


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-58136</u>		Yiiframework Yii	Mimo (aka Hezb)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:yiiframework:yii:*:*:*:*:*:*	XMRig
Yiiframework Yii Improper Protection of Alternate Path Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-424	T1068: Exploitation for Privilege Escalation	<a href="https://github.com/yiisoft/yii2/pull/20232">https://github.com/yiisoft/yii2/pull/20232</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-47577</u>		TemplateInvaders TI WooCommerce Wishlist Plugin versions upto 2.9.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:templateinvaders:ti_woocommerce_wishlist_plugin:*:*:*:*:*:*	-
TemplateInvaders TI WooCommerce Wishlist Plugin Unrestricted File Type Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-434	T1059: Command and Scripting Interpreter, T1485: Data Destruction, T1190: Exploit Public-Facing Application	

# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Void Blizzard (aka Laundry Bear)</u>	Russia	Aviation, Defense, Education, Government, Healthcare, IT, Law Enforcement, Media, NGO, Telecommunications, Transportation	North America, Europe, NATO Members
	MOTIVE		
	Information theft, Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1557: Adversary-in-the-Middle; T1204: User Execution; T1204.002: Malicious File; T1586: Compromise Accounts; T1586.003: Cloud Accounts; T1588: Obtain Capabilities; T1588.002: Tool; T1110.003: Password Spraying; T1550.004: Web Session Cookie; T1552.001: Credentials In Files; T1087: Account Discovery; T1087.004: Cloud Account; T1018: Remote System Discovery; T1082: System Information Discovery; T1114: Email Collection; T1114.002: Remote Email Collection; T1530: Data from Cloud Storage; T1119: Automated Collection; T1071.001: Web Protocols			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Mimo (aka Hezb)</u>	-	Finance	Worldwide
	MOTIVE		
	Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-32432 CVE-2024-58136	XMRig	Craft CMS, Yiiframework Yii
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			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
<div></div> <div><u>APT41 (aka HOODOO, WICKED PANDA, Winnti, Group 72, BARIUM, LEAD, GREF, Earth Baku, Brass Typhoon)</u></div>	China	Governments, Shipping, Logistics, Media, Technology, Automotive	Worldwide
	<b>MOTIVE</b>		
	Financial crime, Information theft and espionage		
	<b>TARGETED CVE</b>	<b>ASSOCIATED ATTACKS/RANSOM WARE</b>	<b>AFFECTED PRODUCT</b>
	-	TOUGHPROGRESS	-
<b>TTPs</b>			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1036: Masquerading; T1036.008: Masquerade File Type; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1005: Data from Local System; T1027.005: Indicator Removal from Tools; T1620: Reflective Code Loading; T1055: Process Injection; T1055.012: Process Hollowing; T1102: Web Service; T1001: Data Obfuscation; T1041: Exfiltration Over C2 Channel			

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerabilities** and block the indicators related to the threat actors **Void Blizzard**, **Mimo**, **APT41**, and malware **Vidar**, **StealC**, **Dero**, **XMRig**, **TOUGHPROGRESS**.

## Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Run a Scan to discover the assets impacted by the **three exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Void Blizzard**, **Mimo**, **APT41**, and malware **Vidar**, **StealC**, **Dero**, **TOUGHPROGRESS** in Breach and Attack Simulation(BAS).

# Threat Advisories

[From Likes to Leaks: TikTok Campaign Lures Users into Installing Info-Stealers](#)

[Docker Under Siege: Zombie Containers Fuel Dero Crypto Heist](#)

[Void Blizzard Isn't Knocking, It's Already Inside 20+ NGO Networks](#)

[Mimo Threat Actor Exploits Critical RCE Vulnerability in Craft CMS](#)

[APT41 Leverages Google Calendar for Command and Control](#)

[Critical Unpatched Flaw Found in TI WooCommerce Wishlist Plugin](#)

# Appendix

**Known Exploited Vulnerabilities (KEV):** Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

**Celebrity Vulnerabilities:** Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

## ✂ Indicators of Compromise (IOCs)

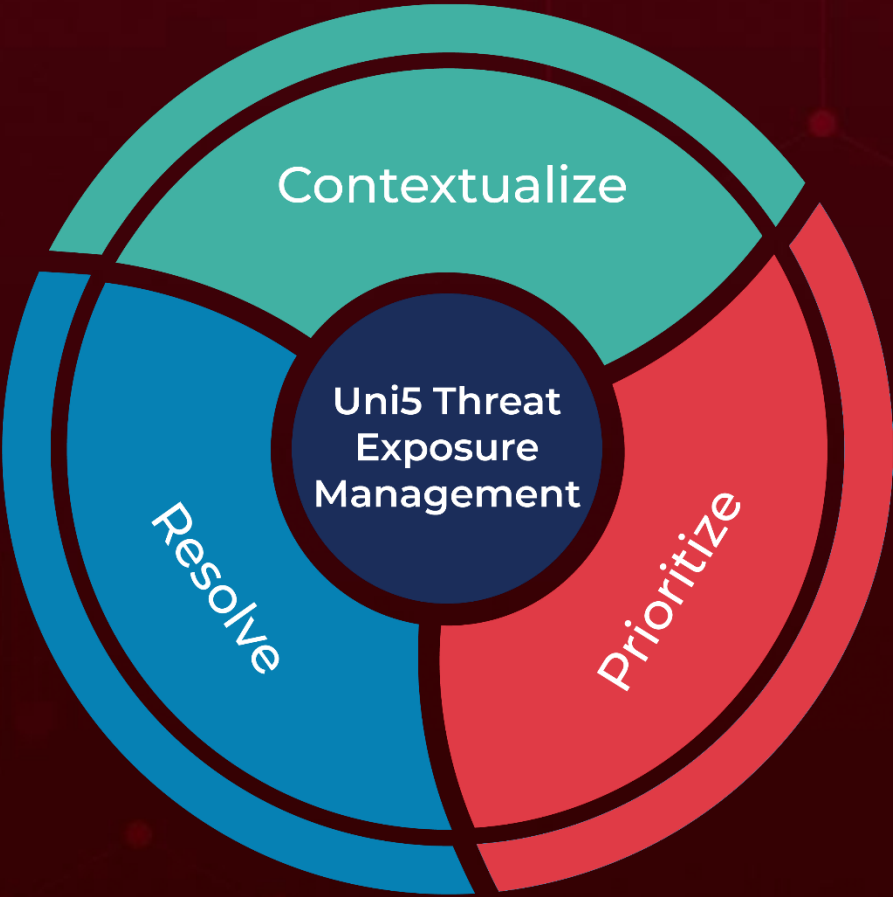
Attack Name	TYPE	VALUE
<u>Vidar</u>	SHA256	3bb81c977bb34fadb3bdeac7e61193dd009725783fb2cf453e15ced70fc39e9b, b8d9821a478f1a377095867aeb2038c464cc59ed31a4c7413ff768f2e14d3886
<u>StealC</u>	SHA256	afc72f0d8f24657d0090566ebda910a3be89d4bdd68b029a99a19d146d63adc5
<u>Dero</u>	SHA256	e4aa649015b19a3c3350b0d897e23377d0487f9ea265fe94e7161fed09f283cf
	Wallet Address	dero1qyy8xjrdjcn2dvr6pwe40jrl3evv9vam6tpx537vux60xxkx6hs7zqgde993y
	Domains	d[.]windowsupdatesupport[.]link, h[.]wiNdowsupdatesupport[.]link
<u>XMRig</u>	SHA256	3a71680ffb4264e07da4aaca16a3f8831b9a30d444215268e82b2125a98b94aa
<u>TOUGHPROGRESS</u>	SHA256	3b88b3efbdc86383ee9738c92026b8931ce1c13cd75cd1cda2fa302791c2c4fb

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

# 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  
**June 2, 2025 • 5:00 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)