Date of Publication
July 4, 2023

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

26 JUNE to 2 JULY 2023

Table Of Contents

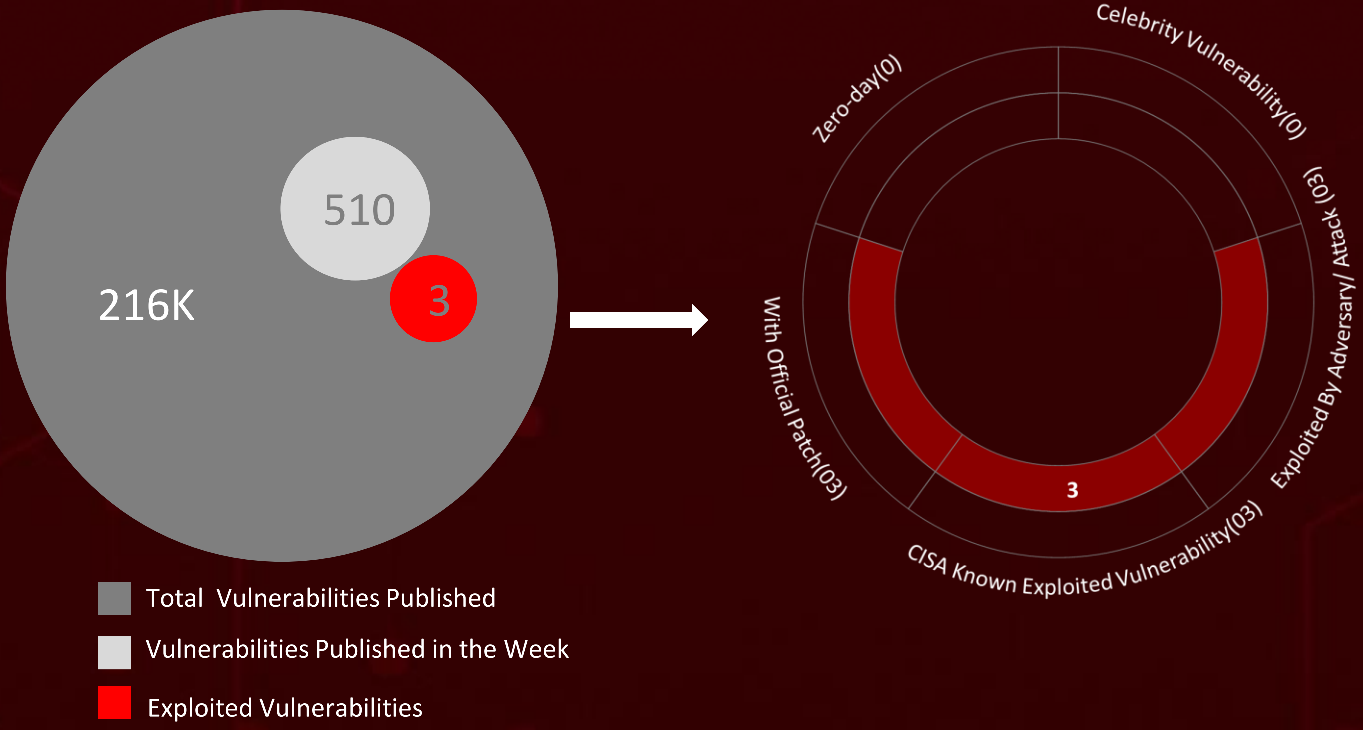
Summary

HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of **four** attacks executed, taking advantage of **three** different vulnerabilities in various systems, and involving **two** different adversaries highlights the ever-present danger of cyber attacks.

HiveForce Labs also highlighted repojacking vulnerabilities possible with millions of github repositories, notably no of these repos are related with big tech giant. A critical Remote Code Execution vulnerability with CVSS score of 9.6 was also discovered in FortiNAC.

Moreover, HiveForce Labs also discovered that APT28 exploited **three** old vulnerabilities related to Roundcube Mailing platform. And Threat Actor Andariel bolsters their arsenal with a newly developed lightweight EarlyRat malware.

Meanwhile, A new malware PindOS was found to be deploying Ransomware related malwares. Also, A new attack campaign MULTI#STORM strikes USA and India. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

4
Attacks Executed

3
Vulnerabilities Exploited

2
Adversaries in Action

- JokerSpy
- PindOS
- EarlyRat
- Warzone

- CVE-2020-35730
- CVE-2021-44026
- CVE-2020-12641

- APT28
- Andariel

Insights

Three

Roundcube Vulnerabilities Exploited by APT28

Millions of Github repository are found to be susceptible to RepoJacking. Vulnerable repositories were found to be from big tech giants.

Andariel

Latest Creation: EarlyRat Malware, have simplistic design for limited functionality for C2 activities.

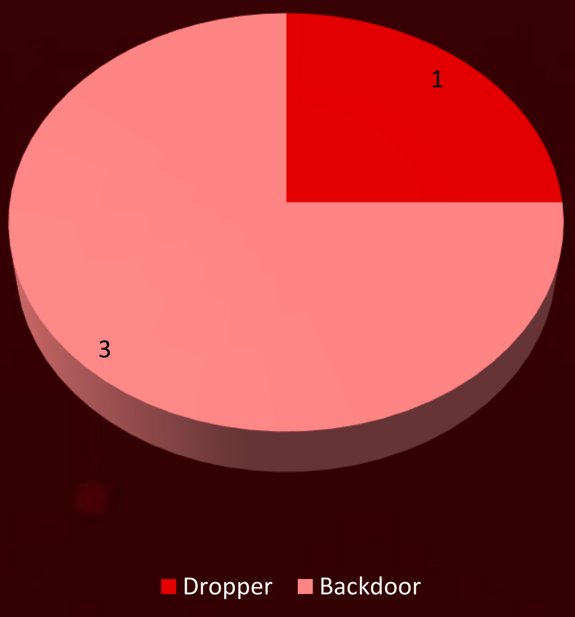
JockerSpy a Mac OS backdoor used in assault of Japanese cryptocurrency exchange market and Mac TCC was tampered for permission evasion.

Countries Under Cyber Siege

United States, South Korea, Japan, Ukraine and India Face Intense Targeting in Recent Cyber Attacks

MULTI#STORM new attack campaign delivering Warzone RAT via phishing mails.

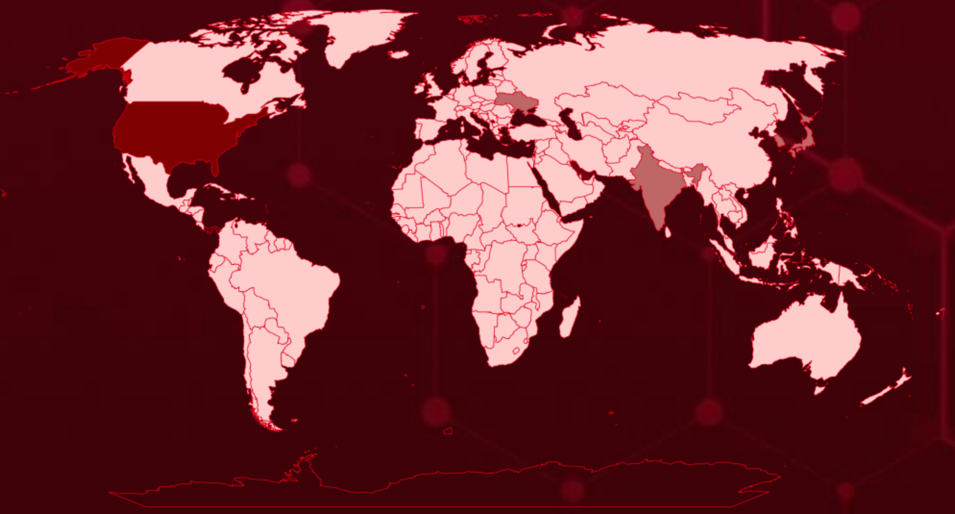
Threat Distribution



Targeted Countries

Most

Least



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom, Zenrin

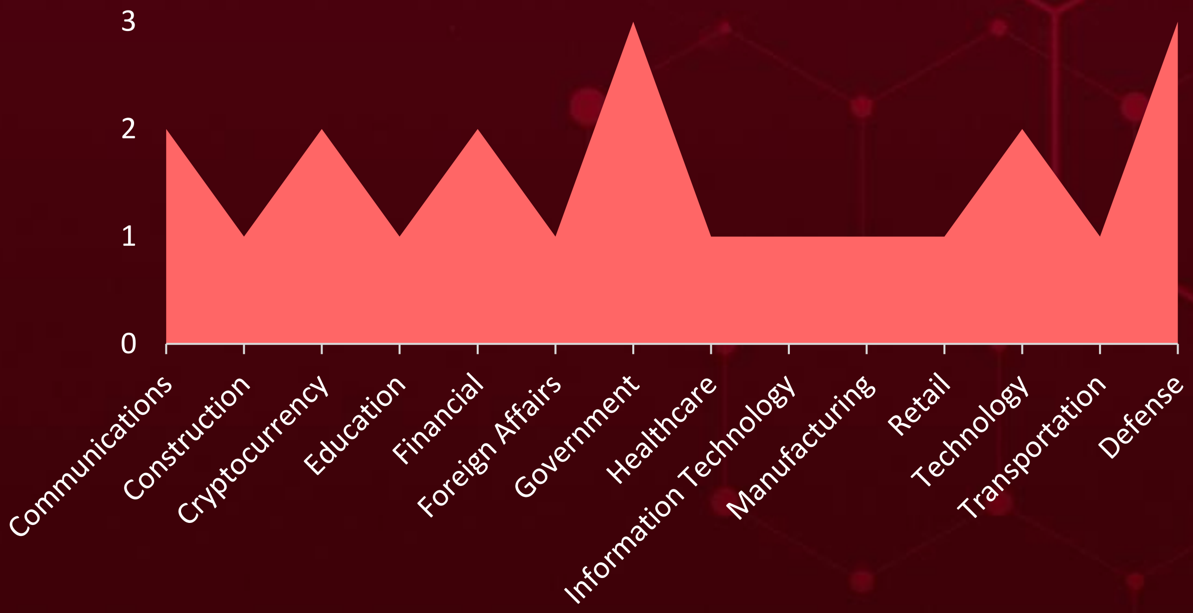
	Countries
🟥	United States
▨	South Korea
▨	Ukraine
▨	India
▨	Japan
□	Peru
□	Malaysia
□	Taiwan
□	Austria
□	Netherlands
□	Azerbaijan
□	Serbia
□	Belarus
□	Vietnam
□	Belgium
□	Monaco
□	Bolivia
□	Norway
□	Bosnia and Herzegovina
□	Puerto Rico
□	Brazil
□	Armenia
□	Brunei
□	Turkey
□	Bulgaria
□	Lithuania

	Countries
□	Cambodia
□	Mexico
□	Chile
□	Myanmar
□	China
□	Nicaragua
□	Colombia
□	Papua New Guinea
□	Costa Rica
□	Poland
□	Croatia
□	Russia
□	Cuba
□	Slovakia
□	Cyprus
□	Sweden
□	Czechia
□	Thailand
□	Denmark
□	Vatican City
□	Dominican Republic
□	Liechtenstein
□	Ecuador
□	Luxembourg
□	El Salvador
□	Malta

	Countries
□	Estonia
□	Moldova
□	Fiji
□	Montenegro
□	Finland
□	Nepal
□	France
□	New Zealand
□	Georgia
□	North Macedonia
□	Germany
□	Panama
□	Greece
□	Paraguay
□	Guatemala
□	Philippines
□	Haiti
□	Portugal
□	Honduras
□	Romania
□	Hungary
□	San Marino
□	Iceland
□	Singapore
□	Andorra
□	Slovenia

	Countries
□	Indonesia
□	Spain
□	Ireland
□	Switzerland
□	Italy
□	Tajikistan
□	Turkmenistan
□	Timor-Leste
□	Argentina
□	Australia
□	Uruguay
□	Albania
□	United Kingdom
□	Kazakhstan
□	Uzbekistan
□	Kyrgyzstan
□	Venezuela
□	Laos
□	Afghanistan
□	Latvia
□	Pakistan
□	Bhutan

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059
Command and Scripting Interpreter

T1027
Obfuscated Files or Information

T1566
Phishing

T1059.007
Javascript

T1566.001
Spearphishing Attachment

T1547
Boot or Logon Autostart Execution

T1113
Screencapture

T1005
Data from Local System

T1132
Data Encoding

T1608
Stage Capabilities

T1204
User Execution

T1608.004
Drive-by Target

T1204.002
Malicious File

T1190
Exploit Public-Facing Application

T1571
Non-Standard Port

T1593.003
Code Repositories

T1068
Exploitation for Privilege Escalation

T1553
Subvert Trust Controls

T1071
Application Layer Protocol

T1574.004
Dylib Hijacking

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JokerSpy	JokerSpy is an advanced toolkit meticulously crafted to infiltrate macOS machines. It utilizes a combination of Python and Swift programs to gather data and execute arbitrary commands.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Disruption, Information Theft, and Financial Loss	Mac OS
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA1	370a0bb4177eeebb2a75651a8addb0477b7d610b, 1ed2c5ee95ab77f8e1c1f5e2bd246589526c6362, 76b790eb3bed4a625250b961a5dda86ca5cd3a11
SHA256	d895075057e491b34b0f8c0392b44e43ade425d19eaaacea6ef8c5c9bd3487d8
Domain	app.influmarket[.]org

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
EarlyRat	EarlyRat is similar to MagicRat and have a simple design. It executes given command and sends details to C2 site.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
backdoor		System Disruption, Information Theft, and Financial Loss	Windows
ASSOCIATED ACTOR			PATCH LINK
Andariel			-

IOC TYPE	VALUE
IPv4	226.132.219[.]125 74.124.228[.]148

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
PindOS	PindOS is a sleek JavaScript dropper designed to discreetly retrieve and deploy next stage payloads, such as Bumblebee and IcedID.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
dropper		System Disruption, Information Theft, and Financial Loss	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	bcd9b7d4ca83e96704e00e378728db06291e8e2b50d68db22efd1f8974d1ca91, 07d2cb0dc0cd353fb210b065733743078e79c4a27c42872cd516a6b1fb1f00d1, 00ec8f3900336c7aeb31fef4d111ee6e33f12ad451bc5119d3e50ad80b2212b0, 15da5b0a65dd8135273124da0c6e52e017e3b54642f87571e82d2314aae97eec, 180a935383b39501c7bdf2745b3a334841f01a7df9d063fecca587b5cc3f5e7a, 92506fe773db7472e7782dbb5403548323e65a9eb2e4c15f9ac65ee6c4bd908b

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
WarZone	Warzone is a remote access tool (RAT) and operates as malware as-a-service. It has no of features to harvest sensitive data and download additional malware.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
backdoor		System Disruption, Information Theft, and Financial Loss	Widnows
ASSOCIATED ACTOR			PATCH LINK
Confucius			-

IOC TYPE	VALUE
URL	134.19.179[.]147:38046/dominion46.ddns[.]net
SHA256	0E799B2F64CD9D10A4DFED1109394AC7B4CCC317A3C17A95D4B3565943213257 B452A2BA481E881D10A9741A452A3F092DFB87BA42D530484D7C3B475E04DA11

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
CVE-2021-44026	✗	Roundcube: 1.3.0 - 1.4.11	APT28 (aka Fancy Bear)
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
Roundcube Webmail SQL Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter, T1005: Data from Local System, T1505: Server Software Component, T1505.003: Web Shell, T1136: Create Account, T1190: Exploit Public-Facing Application, T1565.001: Data Manipulation	https://roundcube.net/news/2021/11/12/security-updates-1.4.12-and-1.3.17-released

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-12641	✗	Roundcube: 1.2.0 - 1.4.3	APT28 (aka Fancy Bear)
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
Roundcube Webmail Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://roundcube.net/news/2020/04/29/security-updates-1.4.4-1.3.11-and-1.2.10

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2020-35730</td><td>✗</td><td rowspan="2">Roundcube: 1.2.0 - 1.4.9</td><td rowspan="2">APT28 (aka Fancy Bear)</td></tr>
<tr><th>ZERO-DAY</th></tr>
<tr><td>✗</td><th>AFFECTED CPE</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th></tr>
<tr><th>NAME</th><th>CISA KEV</th><td rowspan="2">cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Roundcube Webmail CrossSite Scripting (XSS) Vulnerability</td><td>✓</td></tr>
<tr><th>CWE ID</th><th>ASSOCIATED TTPs</th><th>PATCH LINK</th></tr>
<tr><td>CWE-79</td><td>T1059: Command and Scripting Interpreter, T1059.007: JavaScript/JScript, T1557: Man-in-the-Browser, T1189: Drive-by Compromise, T1204: User Execution, T1204.001: Malicious Link</td><td>https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRY
APT28	Russia	Government Institutions, Military, and Media	Ukraine
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2020-35730, CVE-2021-44026, CVE-2020-12641	-	Roundcube: 1.2.0 - 1.4.11
TTPs			
T1005: Data from Local System, T1021: Remote Services, T1027: Obfuscated Files or Information, T1048: Exfiltration Over Alternative Protocol, T1059: Command and Scripting Interpreter, T1071: Application Layer Protocol, T1078: Valid Accounts, T1114: Email Collection, T1119: Automated Collection, T1133: External Remote Services, T1203: Exploitation for Client Execution, T1204: User Execution, T1213: Data from Information Repositories, T1566: Phishing, T1567: Exfiltration Over Web Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRY
Andariel	North-Korea	Government Agencies, Military Organizations, Financial Services	South Korea
	MOTIVE		
	Information Theft, Espionage and Monetary Gains		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	EarlyRat	Windows
TTPs			
TA0042: Resource Development, T1587: Develop Capabilities, T1566: Phishing, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1547: Boot or Logon Autostart Execution, T1132: Data Encoding			

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 actor - **APT28** & **Andariel** and malware - **JokerSpy, PindOS, EarlyRat** & **WarZone**.

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

- Running 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 actor - **APT28** & **Andariel** and malwares in **JokerSpy, PindOS, EarlyRat** & **WarZone** Breach and Attack Simulation(BAS).

Threat Advisories

APT28 Leveraged Three Roundcube Exploits in Espionage Campaign

Millions of Github Repository susceptible to Repojacking

Fortinet Addressed Critical RCE FortiNAC Vulnerability

MULTI#STORM Campaign Sets Sights on India and U.S. with RAT

PindOS malware deploying Bumblebee and IcedID

JokerSpy macOS Backdoor Attacks Japanese Cryptocurrency Exchange

Andariel Group unleashes New EarlyRAT malware

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 been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
JockerSpy Backdoor	Domain	app.influmarket[.]org hXXps://www.git-hub[.]me/view.php
	SHA1	937a9811b3e5482eb8f96832454723d59229f945 c7d6ede0f6ac9f060ae53bb1db40a4fbe96f9ceb bd8626420ecfd1ab5f4576d83be35edecd8fa70e 370a0bb4177eeebb2a75651a8addb0477b7d610b 1ed2c5ee95ab77f8e1c1f5e2bd246589526c6362 76b790eb3bed4a625250b961a5dda86ca5cd3a11
	SHA256	d895075057e491b34b0f8c0392b44e43ade425d19eaaacea6ef8c5c9bd3487d8, 8ca86f78f0c73a46f31be366538423ea0ec58089f3880e041543d08ce11fa626, aa951c053baf011d08f3a60a10c1d09bbac32f332413db5b38b8737558a08dc1
PindOS dropper	URL	hxxps://qaswrahc.com/wp-content/out/mn[.]php hxxp://tusaceitesesenciales.com/mn[.]php hxxp://carwashdenham.com/mn[.]php hxxps://intellectproactive.com/dist/out/mn[.]php hxxps://masar-alulaedu.com/wp-content/woocommerce/out/berr[.]php hxxps://egyfruitcorner.com/wp-content/tareq/out/berr[.]php hxxps://tech21africa.com/wp-content/uploads/out/berr[.]php hxxps://www.posao-austrija.at/images/out/lim[.]php hxxps://logisticavirtual.org/wp-content/out/lim[.]php hxxps://adecoco.us/wp-content/out/lim[.]php hxxps://acsdxb.net/wp-content/out/lim[.]php

Attack Name	TYPE	VALUE
PindOS dropper	SHA256	bcd9b7d4ca83e96704e00e378728db06291e8e2b50d68db22efd1f8974d1ca91, 07d2cb0dc0cd353fb210b065733743078e79c4a27c42872cd516a6b1fb1f00d1, 00ec8f3900336c7aeb31fef4d111ee6e33f12ad451bc5119d3e50ad80b2212b0, 15da5b0a65dd8135273124da0c6e52e017e3b54642f87571e82d2314aae97eec, 180a935383b39501c7bdf2745b3a334841f01a7df9d063fecca587b5cc3f5e7a, 24dd5c33b8a5136bdf29d0c07cf56ef0e33a285bb12696a8ff65e4065cb18359, 76c9780256e195901e1c09cb8a37fb5967f9f5b36564e380e7cf2558652f875b, 28c87170f2525fdecc4092fb347acd9b8350ed65e0fd584ce9fc001fd237d523, ac261ac26221505798c65c61a207f3951cc7dce2e1014409d8a765d85bfd91d4, 92506fe773db7472e7782dbb5403548323e65a9eb2e4c15f9ac65ee6c4bd908b, c84c84387f0b9e7bc575a008f36919448b4e6645e1f5d054e20b59be726ee814, 7355656f894ae26215f979b953c8fa237dc39af857a6b27754a93adb1823f3b6, 8f40ff286419eb4b0c4d15710dc552afb2c2a227a180f4b4f520d09b05724151, 9101975f7aca998da796fc15a63b36ab8aa0fe0aed0b186aaed06a3383d5f226, 4f0c9c6fc1287ef16f4683db90dd677054a1f834594494d61d765fa3f2e1352c, cb307d7fa6eaac6a975ad64ff966ff6b0b0fdd59109246c2f6f5e8d50a33e93c, 361b0157ef63d362fdd4399288f5f6a0e1536633dfb49c808a3590718c4d8f10, e71c9ac9ddd55b485e636840da150db5cd2791d0681123457bd40623acd8311c, 8ae3be9f09f5fc64ec898a4d6467b2f6e50eaaa26fc460a4f1a9b9566e97a9a7
EarlyRat Backdoor	IPv4	226.132.219[.]125 74.124.228[.]148

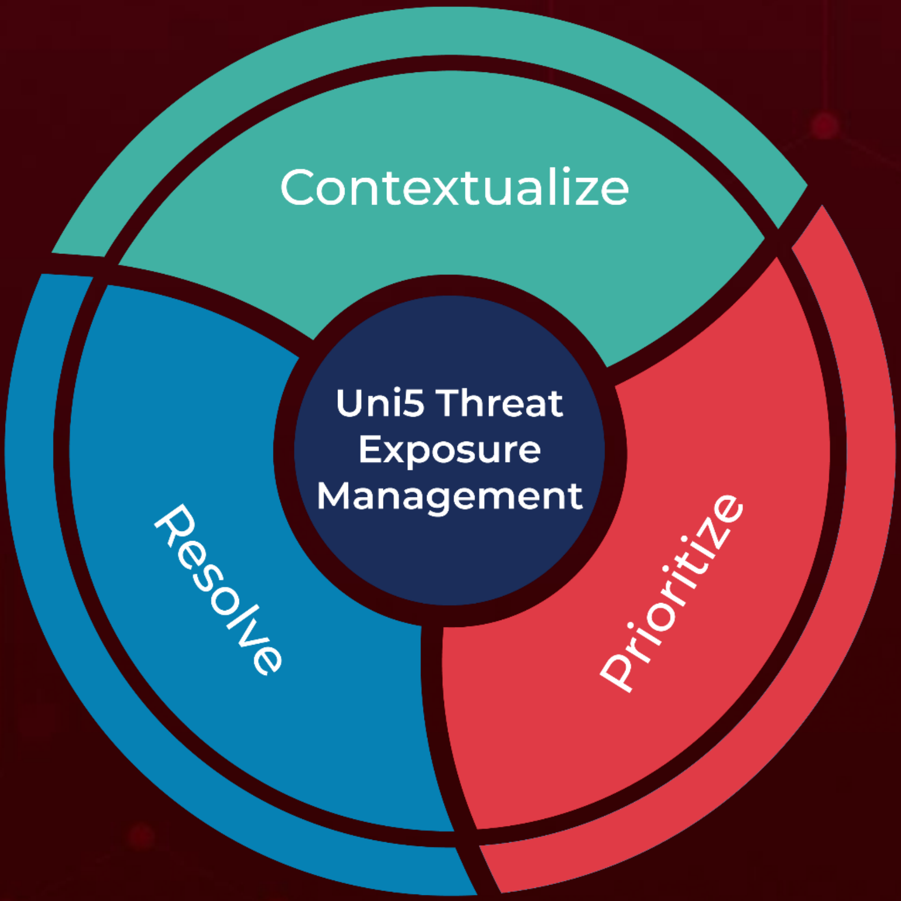
Attack Name	TYPE	VALUE
WarZone backdoor	URL	hxxps://lo3kcg.bl.files.1drv[.]com/y4mtafF_tQM7vAFHxOASpTWOq0M5qmXCnd8FhdFvHvKOxYaA1h-ocJsybIp-r0iMVcK8UH6WP-fFspS6l-aP6uTlpsy11crZ_p_HfMxTI4yymzBqVkLX-v4nQLrn2Ty0-illRzICAbtwbooanM9U97qPmTgUNxhC9ab_4VfNvcmiWFeami9lwl35D8Eb7UiF7TCJTo_0XyAatlemjaXw9zAlw/REQUEST.zip?download&psid=1 -- redirects to -- hxxps://onedrive.live[.]com/download?cid=D09BFD4EBDA21A3D&resid=D09BFD4EBDA21A3D!152&authkey=AErksvWpjzpD_Ag hxxps://onedrive.live[.]com/download?cid=D09BFD4EBDA21A3D&resid=D09BFD4EBDA21A3D%21151&authkey=AGCMruhQJESxca4 hxxps://onedrive.live[.]com/download?cid=D09BFD4EBDA21A3D&resid=D09BFD4EBDA21A3D%21148&authkey=ADY1aqOba7HnNZs&em=2 hxxps://onedrive.live[.]com/download?cid=4A89E2A4EA0448C0&resid=4A89E2A4EA0448C0%21130&authkey=ABwx94zEGC3SmxA 134[.]19.179.147:38046/dominion46.ddns[.]net 134[.]19.179.147:29185/dominion46.ddns[.]net
	SHA256	8674817912be90a09c5a0840cd2dff2606027fe8843eb868929fc33935f5511e, 3783acc6600b0555dec5ee8d3cc4d59e07b5078dd33082c5da279a240e7c0e79, 18C876A24913EE8FC89A146EC6A6350CDC4F081AC93C0477FF8FC054CC507B75, 31960A45B069D62E951729E519E14DE9D7AF29CB4BB4FB8FEAD627174A07B425, 02212f763b2d19e96651613d88338c933ddfd18be4cb7e721b2fb57f55887d64, 5A11C5641C476891AA30E7ECFA57C2639F6827D8640061F73E9AFEC0ADBBD7D2, 30951DB8BFC21640645AA9144CFEAA294BB7C6980EF236D28552B6F4F3F92A96, 37C59C8398279916CFCE45F8C5E3431058248F5E3BEF4D9F5C0F44A7D564F82E, F9130B4FC7052138A0E4DBAAEC385EF5FAE57522B5D61CB887B0327965CCC02A, 0E799B2F64CD9D10A4DFED1109394AC7B4CCC317A3C17A95D4B3565943213257, 455ED920D79F9270E8E236F14B13ED4E8DB8DD493D4DABB05756C867547D8BC7, 9C14375FBBCE08BCF3DC7F2F1100316B2FB745FA2C510F5503E07DB57499BFC8

Attack Name	TYPE	VALUE
WarZone backdoor	SHA256	B452A2BA481E881D10A9741A452A3F092DFB87BA42D530484D7C3B475E04DA11, AB0212F8790678E3F76ED90FBA5A455AC23FBB935CF99CABC2515A1D7277676F, 4A834B03E7FAFFEF929A2932D8E5A1839190DF4D5282CEF35DA4019FE84B19A5, 11408368F4C25509C24017B9B68B19CE5278681F6F12CE7DB992D3C6124B0A23

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, 2023 • 08:30 AM

More at www.hivepro.com