

Date of Publication
October 30, 2023



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

23 to 29 OCTOBER 2023

Table Of Contents

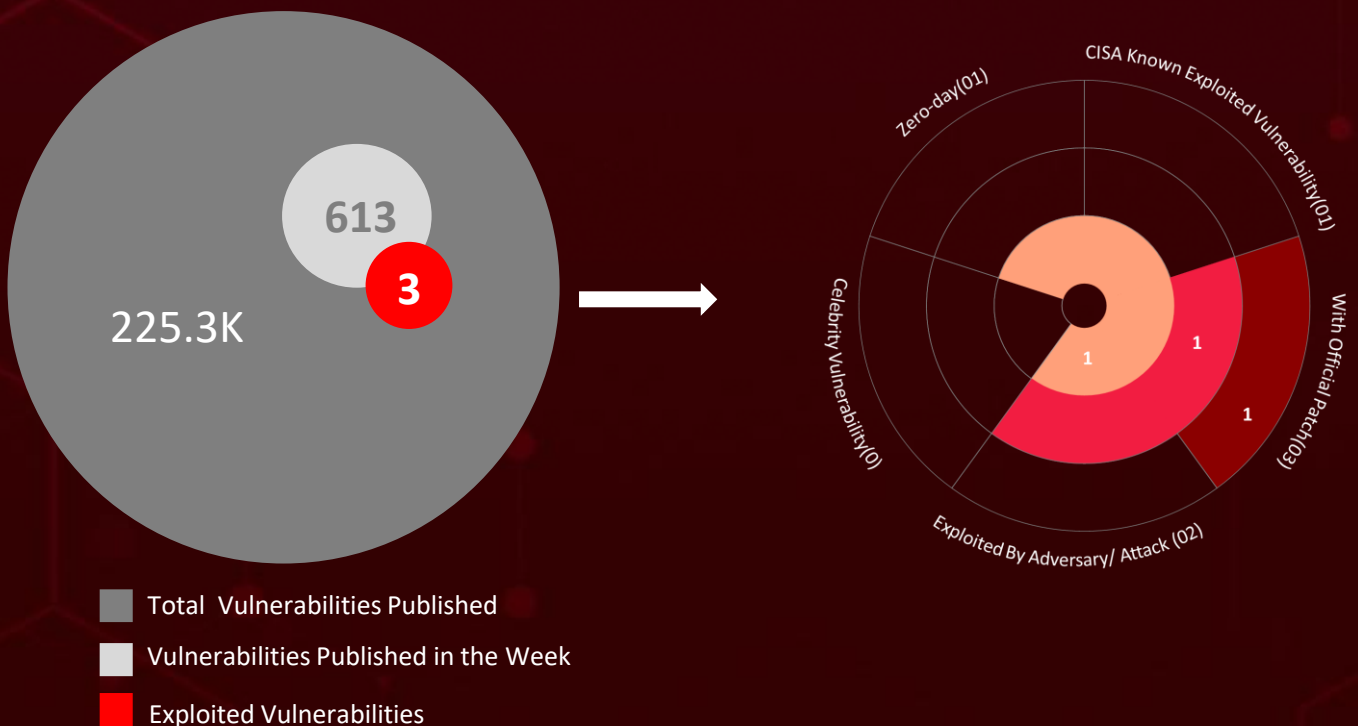
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	16
<u>Threat Advisories</u>	17
<u>Appendix</u>	18
<u>What Next?</u>	20

Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **seven** executed attacks, **two** instances of adversary activity, and **three** exploited vulnerability, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs uncovered a Malware Framework named **StripedFly**, establish network persistence, gain a comprehensive insight into network activities, and exfiltrate credentials from approximately one million Windows and Linux systems.

Meanwhile, A critical zero-day flaw, **CVE-2023-5631**, affecting Roundcube instances is being actively exploited. Also, the Roundcube flaws, exploited by **Winter Vivern**. These observed attacks have been on the rise, posing a significant threat worldwide.



High Level Statistics

7

Attacks
Executed

3

Vulnerabilities
Exploited

2

Adversaries in
Action

- [Quasar RAT](#)
- [Netrunner](#)
- [Dmcserv](#)
- [ExelaStealer](#)
- [GoPIX](#)
- [StripedFly](#)
- [ThunderCrypt](#)

- [CVE-2023-34051](#)
- [CVE-2023-5631](#)
- [CVE-2023-34048](#)

- [YoroTrooper](#)
- [Winter Vivern](#)



Insights

ExelaStealer

New InfoStealer malware an open-source tool, customizable for a fee

StripedFly

An intricate cross-platform malware framework exfiltrate credentials from approximately one million Windows and Linux systems

GoPIX

A typical clipboard stealer malware steals PIX transactions

VMware Aria Operations for Logs

a critical authentication bypass vulnerability (CVE-2023-34051) in VMware allows RCE with root privileges under certain conditions, raising concerns for compromised networks

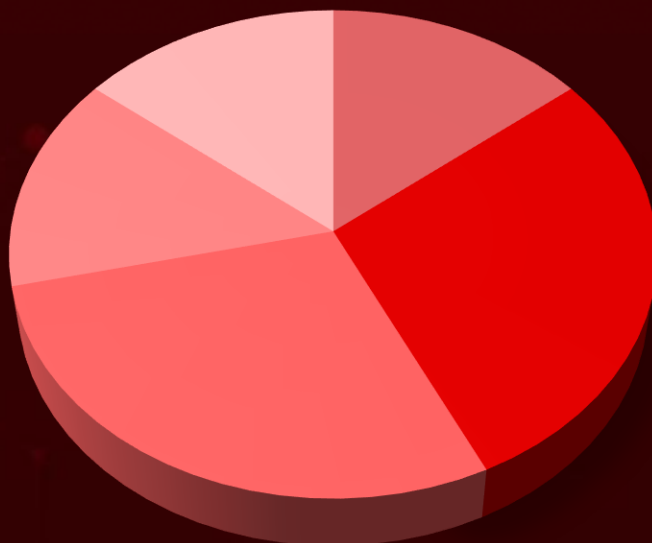
Roundcube 0-day

A zero-day vulnerability, CVE-2023-5631 in the Roundcube webmail exploited by Winter Vivern

Quasar RAT

An open-source remote access trojan uses DLL side-loading to avoid detection

Threat Distribution



■ RAT ■ Backdoor ■ InfoStealer ■ Ransomware ■ Modular

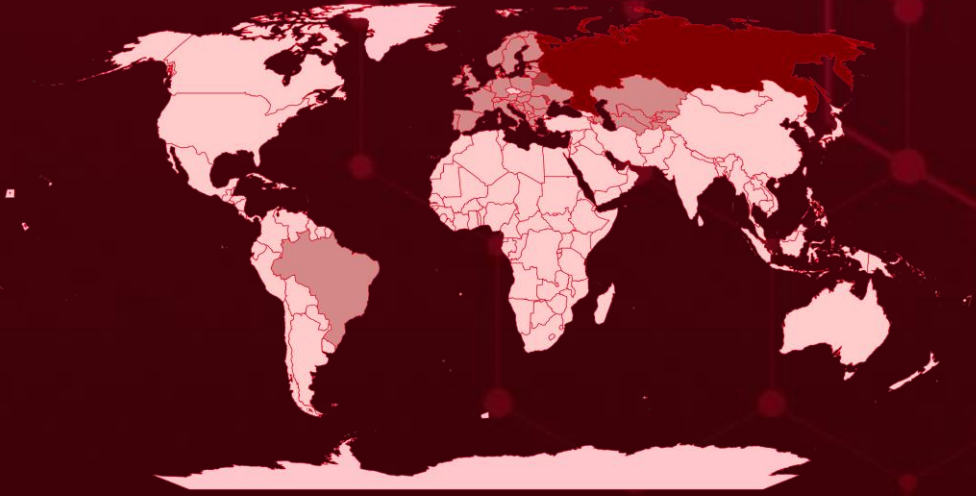


Targeted Countries

Most



Least



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

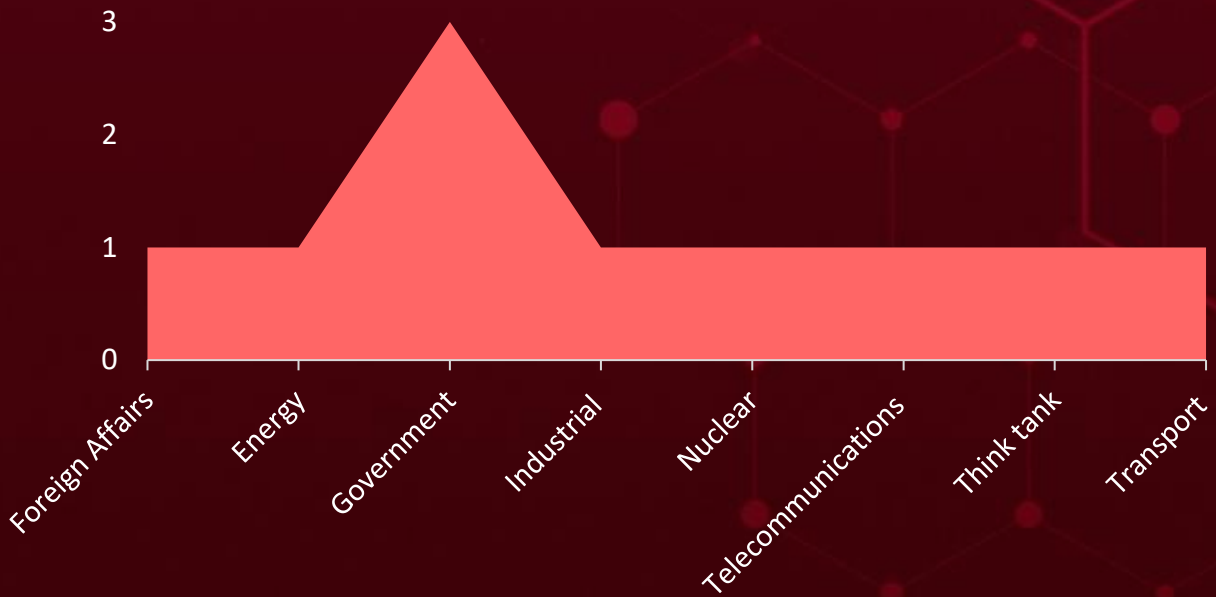
Countries
Russia
Belarus
Moldova
Norway
Uzbekistan
Spain
Austria
Armenia
Azerbaijan
San Marino
Andorra
Turkmenistan
Belgium
Lithuania
Bosnia and Herzegovina
Netherlands
Brazil
Portugal
Bulgaria
Slovakia
Croatia

Countries
Switzerland
Czech Republic (Czechia)
United Kingdom
Denmark
Liechtenstein
Estonia
Luxembourg
Malta
Monaco
Finland
Montenegro
France
North Macedonia
Germany
Poland
Greece
Albania
Romania
Holy See
Serbia
Hungary
Slovenia
Iceland

Countries
Sweden
Ireland
Tajikistan
Italy
Ukraine
Kazakhstan
Kyrgyzstan
Latvia
Turkey
Bahamas
Pakistan
Equatorial Guinea
Sri Lanka
Eritrea
New Zealand
Barbados
Congo
Eswatini
Cyprus
Ethiopia
Dominican Republic
Fiji
Uruguay
Argentina

Countries
North Korea
Algeria
Paraguay
Gabon
Rwanda
Gambia
Cuba
Georgia
South Africa
Belize
Suriname
Ghana
Togo
Benin
Ecuador
Grenada
Nepal
Guatemala
Niger
Guinea
Colombia
Guinea-Bissau
Panama
Guyana
Philippines

Targeted Industries



TOP MITRE ATT&CK TTPS

T1027

Obfuscated Files or Information

T1059

Command and Scripting Interpreter

T1041

Exfiltration Over C2 Channel

T1588.006

Vulnerabilities

T1566

Phishing

T1190

Exploit Public-Facing Application

T1036

Masquerading

T1071.001

Web Protocols

T1583

Acquire Infrastructure

T1140

Deobfuscate/Decode Files or Information

T1547.001

Registry Run Keys / Startup Folder

T1056

Input Capture

T1574

Hijack Execution Flow

T1203

Exploitation for Client Execution

T1588

Obtain Capabilities

T1497

Virtualization/Sandbox Evasion

T1518.001

Security Software Discovery

T1005

Data from Local System

T1055.012

Process Hollowing

T1583.004

Server

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Quasar RAT (aka xRAT, CinaRAT, Yggdrasil)</u>	<p>Quasar RAT is an open-source remote administration tool developed in C#. It comes with a variety of features, including the ability to gather system information, list running applications, retrieve files, log keystrokes, capture screenshots, and execute arbitrary shell commands on the compromised host.</p>	DLL side-loading	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Deploying and executing malicious payloads	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	5e3e65909b68d631913056a90e3da3e86c5378719f6d910d55989600d2a36cd1, 17ef487d5567c1fa318ae31b821746d6071dc21490de778359095e014127dff5, 8bd0ac703bd20a29a588599e2a3ee59d21e53cb356eea4a624ae859eaa23a381, f5e916891cb6585fb06e655518a64223aae96691f77e768398b32bfd7d9a90e0, b55588176b3531a9ecf8ba0e5b5a979df21046c46a63fb0e4ae225095a18b558		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Netrunner</u>	<p>Netrunner is a custom Go-based backdoor that performs data theft, likely aiding espionage operations. The backdoor is distinguished primarily by its command-and-control server configurations.</p>	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
MD5	6086673A65B85B3463B551BA611EE6E6		

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>Dmcserv</u>	Dmcserv is a custom Go-based backdoor that performs data theft, likely aiding espionage operations. The backdoor is distinguished primarily by its command-and-control server configurations.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR			PATCH LINK
-		-	
IOC TYPE	VALUE		
MD5	16074C7518B2E5A3335CCF5AAA469470		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>ExelaStealer</u>	Exela Stealer is a Python-based tool designed to discreetly extract sensitive data, including credentials, tokens, sessions, cookies, and more. It accomplishes this covert data exfiltration solely through Discord webhook URLs.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
InfoStealer			-
ASSOCIATED ACTOR			PATCH LINK
-		-	
IOC TYPE	VALUE		
SHA256	b9bc445af6729a95599f1a39e37f559f3ca18dbbc8ae4e60263af565ef4f4db3, 882484b56ad4418786852f401b1b81f31030bec8566b6b07c9798d4ea3033516, ccb1337383351bb6889eb8478c18c0142cb99cbb523acc85d0d626d323f5d7ad, d8488f93b8c096838b3d9b335091216667ce4ffc7ae2cf3c8925271f0f190c11, b6ca47065e68aebb007657ff0e6b0dfa0fc4e19823f336ab73f42b25dd5cfc22		

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>GoPIX</u>	GoPIX is a typical clipboard stealer malware that steals PIX “transactions” used to identify payment requests and replaces them with a malicious one which is retrieved from the C2. The malware also supports substituting Bitcoin and Ethereum wallet addresses.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer			-
ASSOCIATED ACTOR		Steal PIX transactions, financial and personal information.	PATCH LINK
-			-
IOC TYPE	VALUE		
MD5	EB0B4E35A2BA442821E28D617DD2DAA2, 6BA5539762A71E542ECAC7CF59BDDF79, 333A34BD2A7C6AAF298888F3EF02C186		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>StripedFly</u>	StripedFly is a complex modular malware, enabling attackers to establish network persistence, gain a comprehensive insight into network activities, and exfiltrate credentials. It boasts advanced features such as TOR-based traffic obscuring methods for communication with command servers, automated update and delivery capabilities.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Modular			-
ASSOCIATED ACTOR		Inject Shellcode	PATCH LINK
-			-
IOC TYPE	VALUE		
MD5	b28c6d00855be3b60e220c32bfad2535, 18f5ccdd9efb9c41aa63efbe0c65d3db, 2cdc600185901cf045af027289c4429c, 54dd5c70f67df5dc8d750f19eceed797, d32fa257cd6fb1b0c6df80f673865581		




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
ThunderCrypt	ThunderCrypt is a ransomware-type virus distributed via fake Adobe Flash Player updates. Once infiltrated, ThunderCrypt encrypts various data using RSA-2048 cryptography. It opens a pop-up window containing a ransom-demand message	-	-
		IMPACT	AFFECTED PRODUCTS
		Demand Ransom	-
			PATCH LINK
TYPE			
Ransomware			
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
MD5	120f62e78b97cd748170b2779d8c0c67, d64361802515cf32bd34f98312dfd40d, 3281b2d95e7123a429001400c10ebe28		
SHA256	8258c53a44012f6911281a6331c3ecbd834b6698b7d2dbf4b1828540793340d1		
SHA1	b97308ea9f9c410188d43c34a867fa42c9e9128e		

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-2023-34051		Vmware Aria Operations for Logs (formerly vRealize Log Insight): 8.0.0 - 8.12	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:vmware:vrealize_log_insight:8.12:*.~*.~*.~*.~*.~*.~*	-
VMware Aria Operations for Logs Authentication Bypass Vulnerability			ASSOCIATED TTPs
	CWE ID	T1190: Exploit Public-Facing Application	https://www.vmware.com/security/advisories/VMSA-2023-0021.html
	CWE-287		


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR	
CVE-2023-5631		Roundcube: 1.0.0 - 1.6.3	Winter Vivern	
	ZERO-DAY			
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE	
NAME	CISA KEY	cpe:2.3:a:roundcube:webmail:~*.~*.~*.~*.~*.~*.~*	-	
Roundcube Cross Site Scripting Vulnerability			ASSOCIATED TTPs	PATCH LINK
	CWE ID		T1190: Exploit Public-Facing Application	https://roundcube.net/download/
	CWE-79			

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-34048</u>		vCenter Server: 7.0-7.0U3n 8.0- 8.0U1c, VMware Cloud Foundation 5.x, 4.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWA RE
NAME	CISA KEV	cpe:2.3:a:vmware:vcenter- server:8.0:U1c:*:*:*:*:*	-
			
VMware vCenter Out-of-Bounds Write Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter	https://customerconnect.vmware.com/downloads/details?downloadGroup=VC80U2&productId=1345&rPId=110105 , https://customerconnect.vmware.com/downloads/details?downloadGroup=VC80U1D&productId=1345&rPId=112378 , https://customerconnect.vmware.com/downloads/details?downloadGroup=VC70U30&productId=974&rPId=110262 , https://kb.vmware.com/s/article/88287



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>YoroTrooper</u>	Unknown	Energy and Government	Azerbaijan, Kyrgyzstan, Tajikistan, Turkey, Turkmenistan and Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	-	-
TTPs			
T1595: Active Scanning; T1590: Gather Victim Network Information; T1588.006: Vulnerabilities; T1190: Exploit Public-Facing Application; T1566: Phishing; T1059: Command and Scripting Interpreter; T1548: Abuse Elevation Control Mechanism; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1046: Network Service Discovery; T1105: Ingress Tool Transfer; T1041 Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Winter Vivern (aka UAC-0114, TA473)</u></p>	Unknown	Defense and Government	India, Lithuania, Poland, Slovakia, Ukraine, USA and Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2023-5631	-	Roundcube
TTPs			
T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1587: Develop Capabilities; T1587.004: Exploits; T1190: Exploit Public-Facing Application; T1566: Phishing; T1203: Exploitation for Client Execution; T1087: Account Discovery; T1087.003: Email Account; T1114: Email Collection; T1114.002: Remote Email Collection; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2			

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 **YoroTrooper, Winter Vivern** and malware **Quasar RAT, Netrunner, Dmcserv, ExelaStealer, GoPIX, StripedFly, ThunderCrypt**.

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 **YoroTrooper, Winter Vivern** and malware **Quasar RAT, Netrunner, Dmcserv, ExelaStealer, GoPIX, StripedFly, ThunderCrypt** in Breach and Attack Simulation(BAS).



Threat Advisories

[Quasar RAT Utilizes DLL Side-Loading to Evade Detection](#)

[Hackers Infiltrate Russian Government and Industrial Entities](#)

[ExelaStealer: A New Entrant in the InfoStealer Landscape](#)

[Attackers Exploit VMware's Aria Operations for Logs Vulnerability](#)

[Attackers Exploit Brazil's PIX System with GoPIX Malware Campaign](#)

[YoroTrooper Covert Cyber Espionage Masters of Kazakhstan](#)

[Winter Vivern Capitalizes on Zero-Day Flaw in Roundcube](#)

[VMware vCenter Flaws Leading to RCE Attacks](#)

[Redefining the StripedFly Malware Framework](#)

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)

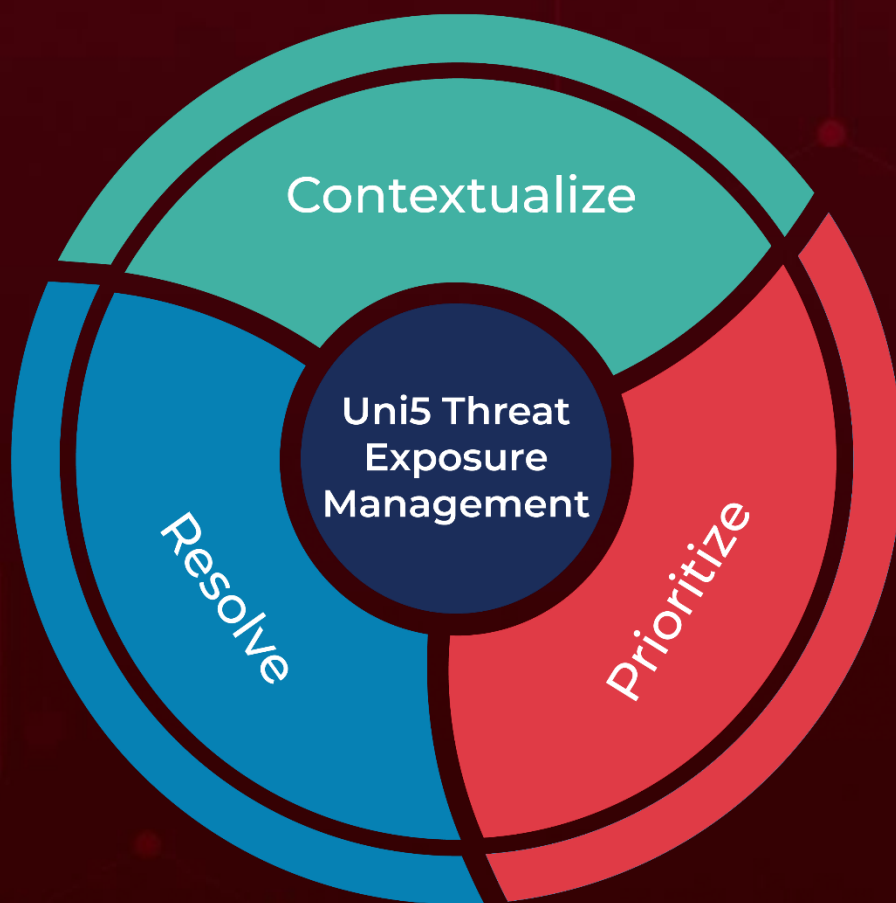
Attack Name	TYPE	VALUE
<u>Quasar RAT</u>	SHA256	5e3e65909b68d631913056a90e3da3e86c5378719f6d910d55989600d2a36cd1, 17ef487d5567c1fa318ae31b821746d6071dc21490de778359095e014127dff5, 8bd0ac703bd20a29a588599e2a3ee59d21e53cb356eea4a624ae859eaa23a381, f5e916891cb6585fb06e655518a64223aae96691f77e768398b32bfd7d9a90e0, b55588176b3531a9ecf8ba0e5b5a979df21046c46a63fb0e4ae225095a18b558, 7aa071e2184478eb932bd815a0eb393fb5efd7b322e3d333b908a9d7d33a4186, b55588176b3531a9ecf8ba0e5b5a979df21046c46a63fb0e4ae225095a18b558, 6dfe949ce3664c802ecd34968f18f0e9fc15f6fab58b35272ed7e83ab2442f2b, d64ec3e1fd63333c0d31d524027260e3d61c27921ab3d922a5a47588942ea051, c7550dc220b264239f7250607d6af8a0123107be4c377a3c94e5f8e63984b17d, 6ed6ea86dae39ff40a2b03781c2bbf13f5c7bc022d5419ef82d1d5f61535358c, d40f6568584ba4a9bda4e27dd7ef8f86620b648df32aee2eeb9c900de1b89f7d, 6cf1314c130a41c977aafce4585a144762d3fb65f8fe493e836796b989b002cb, ec8188e4e07aceea9afd588332ffb08549cc610364d8cd4695200f29b70da153, 6ff6f0407f18ac2a5cf56dd333998e5319f769f16d37b8f3cbf56e0f97e7b3d2,

Attack Name	TYPE	VALUE
<u>Netrunner</u>	MD5	6086673A65B85B3463B551BA611EE6E6
<u>Dmcserv</u>	MD5	16074C7518B2E5A3335CCF5AAA469470
<u>ExelaStealer</u>	SHA256	b9bc445af6729a95599f1a39e37f559f3ca18dbbc8ae4e60263af565ef4f4db3, 882484b56ad4418786852f401b1b81f31030bec8566b6b07c9798d4ea3033516, ccb1337383351bb6889eb8478c18c0142cb99cbb523acc85d0d626d323f5d7ad, d8488f93b8c096838b3d9b335091216667ce4ffc7ae2cf3c8925271f0f190c11, b6ca47065e68aebb007657ff0e6b0dfa0fc4e19823f336ab73f42b25dd5cfc22, 206278545b897a7e2ebb1ec4687e6ec31d7ca8f1828792a34f4fca745db8e3d4, 53b1b3c6f73312cdae7be69d16a42d298fae0cb3721c7fc11252f65b10f5a323, 2db54628a877ab40463a128496cb94523ccea6186d1648c6f372c719f6ed8152
<u>GoPIX</u>	MD5	EB0B4E35A2BA442821E28D617DD2DAA2, 6BA5539762A71E542ECAC7CF59BDDF79, 333A34BD2A7C6AAF298888F3EF02C186
<u>StripedFly</u>	MD5	b28c6d00855be3b60e220c32bfad2535, 18f5ccdd9efb9c41aa63efbe0c65d3db, 2cdc600185901cf045af027289c4429c, 54dd5c70f67df5dc8d750f19eeced797, d32fa257cd6fb1b0c6df80f673865581, c04868dabd6b9ce132a790fdc02acc14, c7e3df6455738fb080d741dcbb620b89, d684de2c5cfb38917c5d99c04c21769a, a5d3abe7feb56f49fa33dc49fea11f85, 35fadceca0bae2cdcfdaac0f188ba7e0, 00c9fd9371791e9160a3adaade0b4aa2, 41b326df0d21d0a8fad6ed01fec1389f, 506599fe3aecdfb1acc846ea52adc09f, 6ace7d5115a1c63b674b736ae760423b, 2e2ef6e074bd683b477a2a2e581386f0, 04df1280798594965d6fdfeb4c257f6c, abe845285510079229d83bb117ab8ed6, 090059c1786075591dec7ddc6f9ee3eb
<u>ThunderCrypt</u>	MD5	120f62e78b97cd748170b2779d8c0c67, d64361802515cf32bd34f98312dfd40d, 3281b2d95e7123a429001400c10ebe28
	SHA256	8258c53a44012f6911281a6331c3ecbd834b6698b7d2dbf4b1828540793340d1
	SHA1	b97308ea9f9c410188d43c34a867fa42c9e9128e

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

October 30, 2023 • 7:30 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com