

Date of Publication  
October 9, 2023



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

02 OCTOBER to 08 OCTOBER 2023

# Table Of Contents

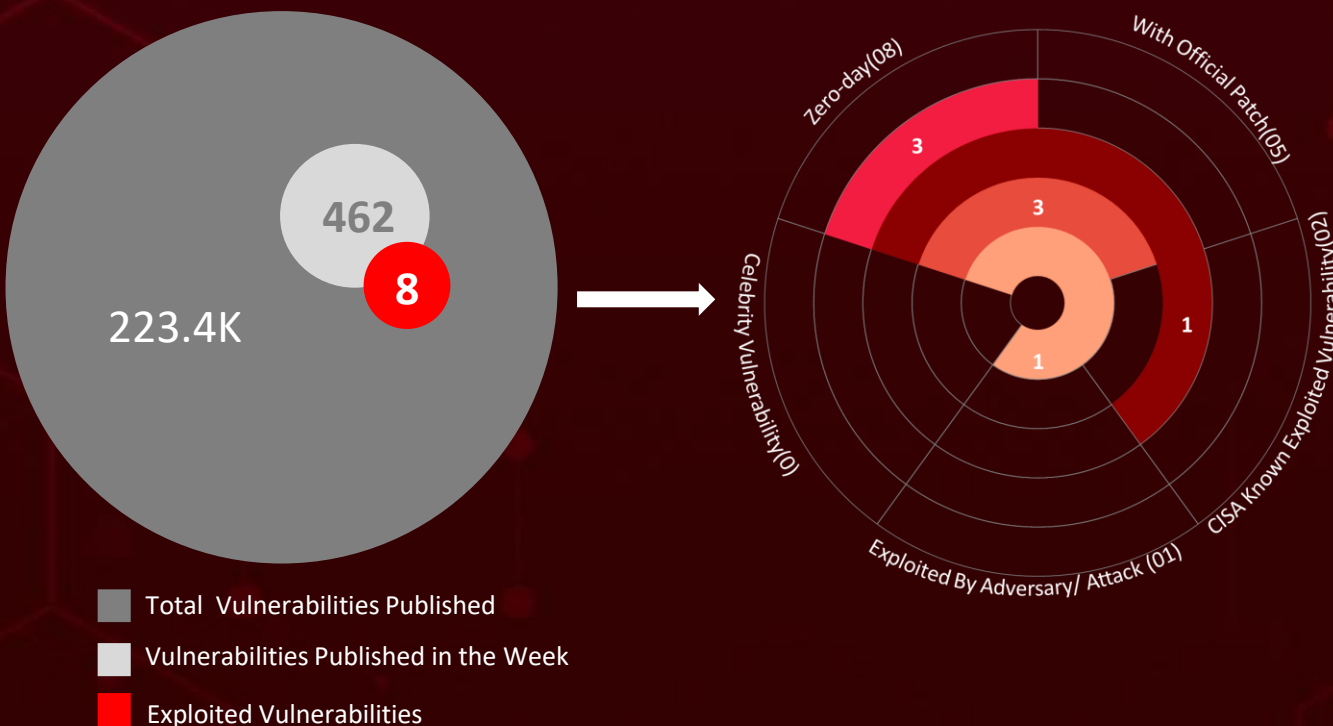
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	14
<u>Adversaries in Action</u>	18
<u>Recommendations</u>	18
<u>Threat Advisories</u>	19
<u>Appendix</u>	20
<u>What Next?</u>	23

# 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, **zero** instances of adversary activity, and **eight** zero-day vulnerabilities, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs uncovered a Malware-as-a-Service named **BunnyLoader**, which is being sold on various forums. BunnyLoader is a malicious software loader written in C/C++ and is sold for \$250.

Meanwhile, A critical zero-day flaw, **CVE-2023-22515**, affecting Confluence Data Center and Server instances is being actively exploited. Also, the MOVEit Transfer product, exploited by **Clop ransomware**. These observed attacks have been on the rise, posing a significant threat worldwide.



# High Level Statistics

7

Attacks  
Executed

8

Vulnerabilities  
Exploited

0

Adversaries in  
Action

- [EvilProxy](#)
- [BunnyLoader](#)
- [DinodasRAT](#)
- [Qakbot](#)
- [Ransom Knight ransomware](#)
- [Remcos backdoor](#)
- [Clop Ransomware](#)
- [CVE-2023-42114](#)
- [CVE-2023-42115](#)
- [CVE-2023-42116](#)
- [CVE-2023-42117](#)
- [CVE-2023-42118](#)
- [CVE-2023-42119](#)
- [CVE-2023-22515](#)
- [CVE-2023-34362](#)



# Insights

## Qakbot

Distributing Ransom Knight ransomware and the Remcos backdoor via phishing emails

## BunnyLoader

Malware-as-a-Service (MaaS) being sold on various forums.

## MOVEit

Flaws in Progress MOVEit Transfer exploited by Clop ransomware

## EvilProxy

The campaign used a sophisticated phishing kit called 'EvilProxy' which acts as a reverse proxy intercepting the requests between the client and the legitimate site

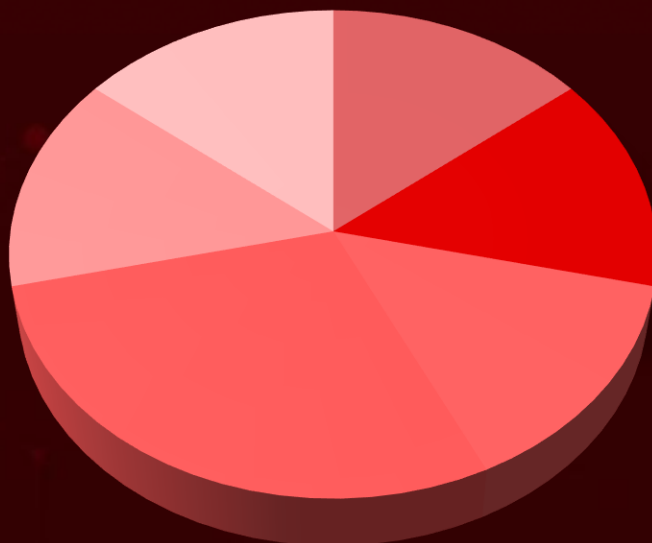
## Atlassian Confluence 0-day

A critical zero-day affecting Confluence Data Center and Server enables external attackers to create unauthorized Confluence administrator accounts

## Looney Tunables

A buffer overflow vulnerability in the glibc's dynamic loader (ld.so)

## Threat Distribution



■ Loader ■ RAT ■ Trojan ■ Ransomware ■ Backdoor ■ Phishing-as-a-service kit

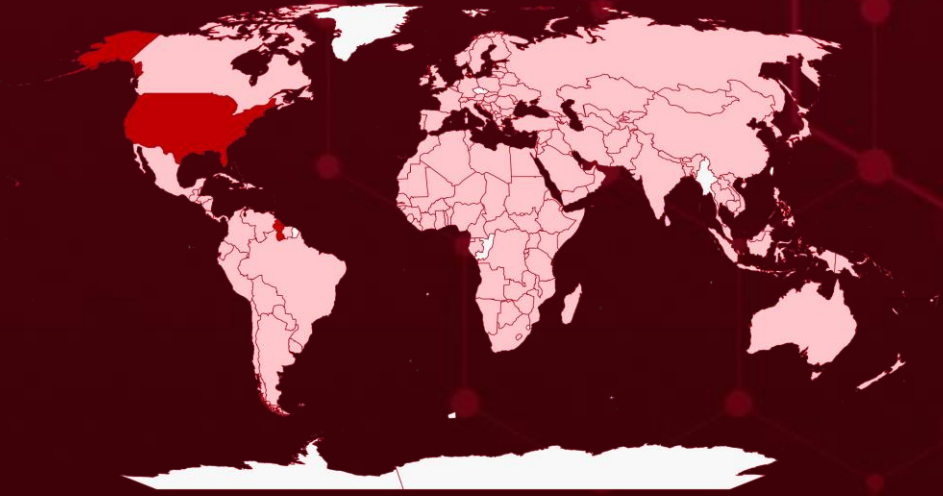


# Targeted Countries

Most



Least



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

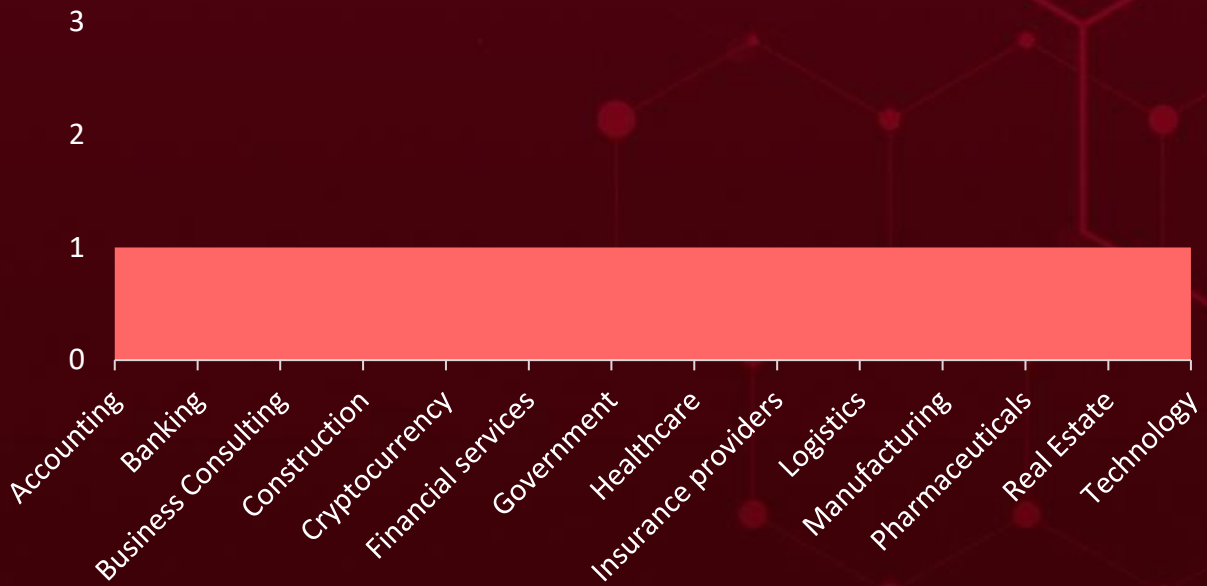
Countries
Guyana
United States
Norway
Afghanistan
South Africa
Andorra
Monaco
Angola
Saint Kitts and Nevis
Antigua and Barbuda
Trinidad and Tobago
Argentina
Mali
Armenia
Nepal
Australia
Peru
Austria
Serbia
Azerbaijan

Countries
Switzerland
Bahamas
Algeria
Bahrain
Madagascar
Bangladesh
Mauritius
Barbados
Mozambique
Belarus
Niger
Belgium
Palestine State
Belize
Qatar
Benin
San Marino
Bhutan
Slovakia
Bolivia
Sri Lanka
Bosnia and Herzegovina
Thailand

Countries
Botswana
Tuvalu
Brazil
Vietnam
Brunei
Lithuania
Bulgaria
Malaysia
Burkina Faso
Marshall Islands
Burundi
Micronesia
Cabo Verde
Montenegro
Cambodia
Namibia
Cameroon
New Zealand
Canada
North Korea
Central African Republic
Papua New Guinea

Countries
Chile
Poland
China
Russia
Colombia
Saint Vincent and the Grenadines
Comoros
Saudi Arabia
Congo (Congo-Brazzaville)
Sierra Leone
Costa Rica
Solomon Islands
Côte d'Ivoire
South Sudan
Croatia
Suriname
Cuba
Tajikistan
Cyprus
Togo
Czechia (Czech Republic)
Turkey

# Targeted Industries



## TOP MITRE ATT&CK TTPS

### T1055

Process Injection

### T1588

Obtain Capabilities

### T1059

Command and Scripting Interpreter

### T1105

Ingress Tool Transfer

### T1566

Phishing

### T1588.006

Vulnerabilities

### T1588.001

Malware

### T1083

File and Directory Discovery

### T1203

Exploitation for Client Execution

### T1036

Masquerading

### T1113

Screen Capture

### T1041

Exfiltration Over C2 Channel

### T1190

Exploit Public-Facing Application

### T1053

Scheduled Task/Job

### T1497

Virtualization/Sandbox Evasion

### T1059.001

PowerShell

### T1090

Proxy

### T1068

Exploitation for Privilege Escalation

### T1115

Clipboard Data

### T1140

Deobfuscate/Decode Files or Information

# ⚔ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>EvilProxy</u>	EvilProxy is a phishing-as-a-service platform that employs reverse proxies to simplify communication and transfer user information between the target, and the malicious actors orchestrating the phishing campaign.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Phishing-as-a-service kit		Unauthorised Access	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			-
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>Domains</b>	lmo[.]roxylvfuco[.]com[.]au, lmo[.]bartmfil[.]com, lmo[.]triperlid[.]com, roxylvfuco[.]com[.]au, earthscigrovp[.]com[.]au		

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>BunnyLoader</u>	<p>BunnyLoader is a type of malware that is openly available for purchase on various online forums. This malicious software provides cybercriminals with a wide range of features and functionalities, including the ability to download and execute a second-stage payload, as well as harvest browser credentials and system information from infected machines. It is often marketed at a price of \$250.</p>	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Loader			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		Information Disclosure	-
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>MD5</b>	Dbf727e1effc3631ae634d95a0d88bf3, Bbf53c2f20ac95a3bc18ea7575f2344b, 59ac3eacd67228850d5478fd3f18df78		
<b>IPv4</b>	37[.]139[.]129[.]145		

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>DinodasRAT</u>	DinodasRAT is a remote access trojan developed in C++ with various capabilities that allow an attacker to spy on and collect sensitive information from a victim's computer.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Remote access trojan (RAT)		Exfiltrate files, manipulate Windows registry keys, and execute commands	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			-
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>SHA1</b>	599EA9B26581EBC7B4BDFC02E6C792B6588B751E, 8BDC8FA3E398733F50F8572D04172CD4B9765BBC, 9C660AC9E32AD853CAAA995F5FC112E281D8520A, 6022383243927CAFC74D8DC937423DBED2A170B8, B2B86DDA48A109EDD932B460649F60F505D5D71C		

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><a href="#">Qakbot (aka QBot, QuackBot, and Pinkslipbot)</a></u>	Qakbot is a modular second-stage malware with backdoor capabilities, initially purposed as a credential stealer. Qakbot steals sensitive data and attempts to self-propagate to other systems on the network. Qakbot also provides RCE capabilities, allowing attackers to perform manual attacks to achieve secondary objectives such as scanning the compromised network or injecting ransomware.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
		Deliver payloads, including ransomware	-
			<b>PATCH LINK</b>
<b>ASSOCIATED ACTOR</b>	-		
<b>TYPE</b>	Trojan		
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>SHA256</b>	006e0b5f47462c4d755b3f84e22b90f09fb6b369032a3ca72f39180e5395ed17, 25cc64a072861840df9dfa7b2449165e4c37d57c542da8ec4ea4fffa10f1be39, 6e0062ccdfa7a117a8b76d4056ac144fdf91f3a2811b32d5a3b7f31ac326181b		

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
<a href="#"><u>Ransom Knight ransomware (aka Cyclops)</u></a>	Knight ransomware is the rebrand of Cyclops. It is designed to encrypt files and demand ransoms for their decryption.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
		Information stealing	-
			<b>PATCH LINK</b>
<b>TYPE</b>			
Ransomware			
<b>ASSOCIATED ACTOR</b>			
-			-
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>SHA256</b>	7b4d227fddcc4e93ea0cdf017026ff2dad6efd6bc7de71b689dc0595a2a4fb4d, a2c654357d790d7c4cec619de951649db31ecdb63935f38b11bb37f983ff58de, C42ad519510936f14ab46fbad53606db8132ea52a11e3fc8d111fbccc7d9ab5a		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>Remcos backdoor</u></a>	Remcos is a sophisticated remote access Trojan (RAT) that can be used to fully control and monitor any Windows computer from XP and onwards.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
		Information Theft	-
			<b>PATCH LINK</b>
<b>TYPE</b>			
Backdoor			
<b>ASSOCIATED ACTOR</b>			
-			-
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>SHA256</b>	34ea4cad8558fcab75631a44eae492a54e1cf9ae2f52e7d5fa712686acd06437, 597541041b49043bd2abd482b3bf4dd233a0dbb47d5ef704ea9ee28705d2764b, 86e96d3d22ead8f41f6a29f7bfe4b35c0d4ae5bd8da046ff0d01d9c6ea678dc2		




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>Clop Ransomware</u>	<p>Clop is a type of ransomware that is known for encrypting a victim's files and appending the ".clop" extension to them. One distinctive feature of Clop ransomware is the string "Dont Worry C OP" that is often included in the ransom notes left behind for the victim. Clop is known to attempt to disable Windows Defender and remove Microsoft Security Essentials from the infected system, aiming to evade detection by security software running in the user space.</p>	Phishing	CVE-2023-34362 CVE-2023-35036 CVE-2023-35708 CVE-2023-36934 CVE-2023-36932 CVE-2023-36933
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware		Unauthorized access and data breaches	Progress MOVEit Transfer
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			<a href="https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023">https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023</a> , <a href="https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-2023-35036-June-9-2023">https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-2023-35036-June-9-2023</a> , <a href="https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023">https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023</a> , <a href="https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023">https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023</a>
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>SHA256</b>	c73388f2ae31cab1a62b18006c634a06e34d42cdd9129efc3de2d095700810d2, ac978f6aaf36d1d90c35e6dc7ae010a19082794d3391ea0111112aed7507f708, 198d3affc04ac9e18cd6fb84f06f809a53ea7b96ad61fd622188abaa11e9328d		




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
<a href="#">CVE-2023-42114</a>		Exim: 4.96 or earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:exim:exim:4.96.*:*:*:*:*:*	-
Exim Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1082: System Information Discovery	<a href="https://exim.org/">https://exim.org/</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-42115</a>		Exim: 4.96 or earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:exim:exim:4.96.*:*:*:*:*:*	-
Exim Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	<a href="https://exim.org/">https://exim.org/</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-42116</a>		Exim: 4.96 or earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*	-
Exim Buffer Overflow Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	<a href="https://exim.org/">https://exim.org/</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-42117</a>		Exim: 4.96 or earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*	-
Exim Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	<a href="https://exim.org/">https://exim.org/</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2023-42118</u></a>		Exim: 4.96 or earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	BAS ATTACKS	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*	-
Exim Remote Code Execution Vulnerability			
	CWE ID		
	CWE-191	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	<a href="https://exim.org/">https://exim.org/</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2023-42119</u></a>		Exim: 4.96 or earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	BAS ATTACKS	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*	-
Exim Information Disclosure Vulnerability			
	CWE ID		
	CWE-125	T1082: System Information Discovery	<a href="https://exim.org/">https://exim.org/</a>



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2023-22515</u></a>		Confluence Data Center and Confluence Server Versions- 8.0.x, 8.1.x, 8.2.x, 8.3.0, 8.3.1, 8.3.2, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.5.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:atlassian:confluence_server_and_data_center:*:*:*:*:*.*.*	-
Atlassian Confluence Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-269	T1068: Exploitation for Privilege Escalation	<a href="https://www.atlassian.com/software/confluence/download-archives">https://www.atlassian.com/software/confluence/download-archives</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2023-34362</u></a>		Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:progress:moveit_cloud:*:*:*:*:*.*.*	Clop Ransomware
Progress MOVEit Transfer SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-89	T1055: Process Injection	<a href="https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023">https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023</a>

# Adversaries in Action

No actionable intelligence observed on adversary activities for the week.

## Recommendations

### Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eight exploited vulnerabilities** and block the indicators related to the **EvilProxy, BunnyLoader, DinodasRAT, Qakbot (aka QBot, QuackBot, and Pinkslipbot), Ransom Knight ransomware (aka Cyclops), Remcos backdoor, Clop Ransomware** malware.

### 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 **eight exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the the **EvilProxy, BunnyLoader, DinodasRAT, Qakbot (aka QBot, QuackBot, and Pinkslipbot), Ransom Knight ransomware (aka Cyclops), Remcos backdoor, Clop Ransomware** in Breach and Attack Simulation(BAS).

# Threat Advisories

[Exim Vulnerable to Zero-Day Remote Code Execution Attacks](#)

[EvilProxy Phishing Attack Targets Indeed Job Platform](#)

['Looney Tunables' Flaw Enables Local Privilege Escalation in Glibc](#)

[Atlassian Confluence Zero-Day Actively Exploited in the Wild](#)

[BunnyLoader: The New Malware-as-a-Service Threat](#)

[Cracking ShellTorch Vulnerabilities: Exposing TorchServe to RCE](#)

[Unveiling Operation Jacana: Targeting the Guyana Government with DinodasRAT](#)

[QakBot Resurges Latest Strikes with Ransom Knight and Remcos RAT](#)

[MOVEit Vulnerabilities Expose Organizations to Cyberattacks](#)

# 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>EvilProxy</u>	Domains	lmo[.]roxylvfuco[.]com[.]au, lmo[.]bartmfil[.]com, lmo[.]triperlid[.]com, roxylvfuco[.]com[.]au, earthscigrovp[.]com[.]au, mscr.earthscigrovp[.]com[.]au, vfuco.com[.]au, catalogsumut[.]com, ivonnesart[.]com, sheridanwyolibrary[.]org
	IPv4	199.204.248[.]121, 193.239.85[.]29, 212.224.107[.]74, 206.189.190[.]128, 116.90.49[.]27, 85.187.128[.]19, 202.139.238[.]230
<u>BunnyLoader</u>	MD5	Dbf727e1effc3631ae634d95a0d88bf3, Bbf53c2f20ac95a3bc18ea7575f2344b, 59ac3eacd67228850d5478fd3f18df78
	IPv4	37[.]139[.]129[.]145

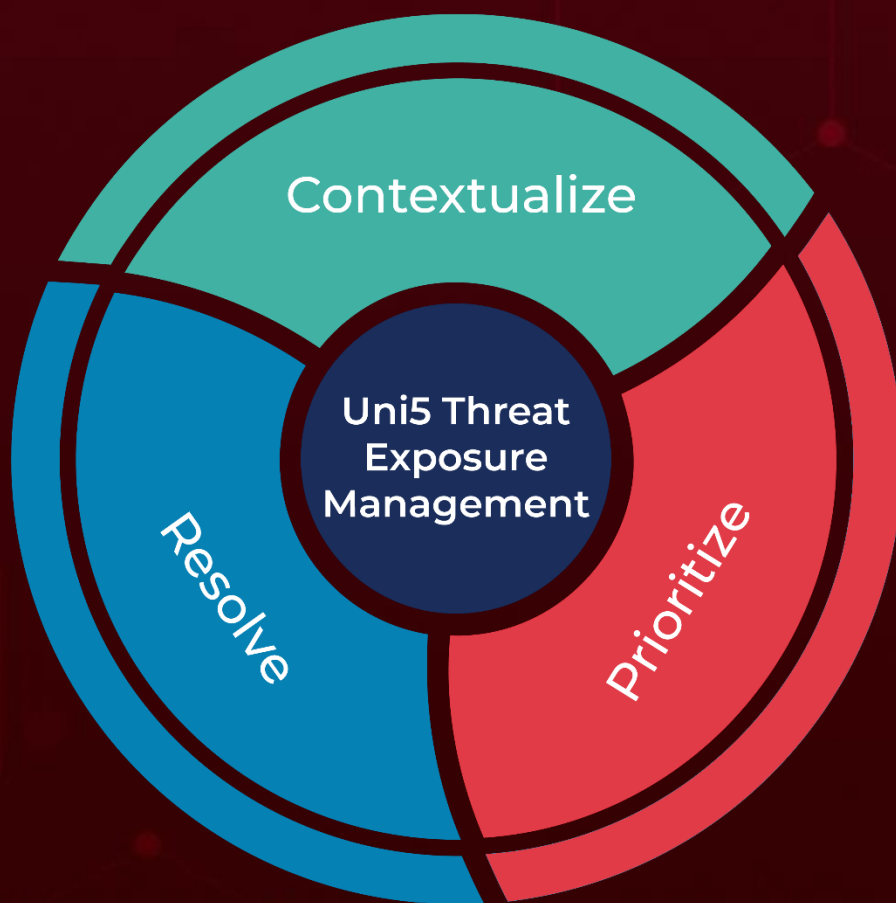
Attack Name	TYPE	VALUE
<u>DinodasRAT</u>	SHA1	599EA9B26581EBC7B4BDFC02E6C792B6588B751E, 8BDC8FA3E398733F50F8572D04172CD4B9765BBC, 9C660AC9E32AD853CAA995F5FC112E281D8520A, 6022383243927CAFC74D8DC937423DBED2A170B8, B2B86DDA48A109EDD932B460649F60F505D5D71C, EFD1387BB272FFE75EC9BF5C1DD614356B6D40B5, 9343E9716933382DA172124803F5463A8454E347, C92DAC928D70EDED7D52CB1347850AA422CEA817, FFBA119D86688AFC098109E08811F67A6E5DECDA, 9A6E803A28D27462D2DF47B52E34120FB2CF814B, 33065850B30A7C797A9F1E5B219388C6991674DB, 6129E37412AFEAFEE47ECEB4C52094EE185E6768, 010451191D8556DCF65C7187BE9579E99323F74D
	IPv4	23.106.122[.]5, 23.106.122[.]46, 23.106.123[.]166, 42.119.111[.]97, 115.126.98[.]204, 118.99.6[.]202, 199.231.211[.]19
	Filenames	President Mohamed Irfaan Ali's Official Visit to Nassau, The Bahamas.doc.exe, client.exe, tools.exe, Client.exe, windowsupdate.exe, people.zip, lass.exe, 2.dll, 1.dll, President Mohamed Irfaan Ali's Official Visit to Nassau, The Bahamas.exe, 114.exe, hh.hsnx, COTED_Att. I to Sav. 230 (Draft Agenda).docx.exe
	Domains	`fta.moit.gov[.]vn, update.microsoft-settings[.]com
<u>Qakbot</u>	SHA256	006e0b5f47462c4d755b3f84e22b90f09fb6b369032a3ca72f39180 e5395ed17, 25cc64a072861840df9dfa7b2449165e4c37d57c542da8ec4ea4ffa 10f1be39, 6e0062ccdfa7a117a8b76d4056ac144fdf91f3a2811b32d5a3b7f31a c326181b

Attack Name	TYPE	VALUE
<u><a href="#">Ransom Knight ransomware (aka Cyclops)</a></u>	SHA256	7b4d227fddcc4e93ea0cdf017026ff2dad6efd6bc7de71b689dc0595a2a4fb4d, a2c654357d790d7c4cec619de951649db31ecdb63935f38b11bb37f983ff58de, C42ad519510936f14ab46fbad53606db8132ea52a11e3fc8d111fbc cc7d9ab5a
<u><a href="#">Remcos Backdoor</a></u>	SHA256	34ea4cad8558fcab75631a44eae492a54e1cf9ae2f52e7d5fa712686acd06437, 597541041b49043bd2abd482b3bf4dd233a0dbb47d5ef704ea9ee28705d2764b, 86e96d3d22ead8f41f6a29f7bfe4b35c0d4ae5bd8da046ff0d01d9c6ea678dc2
<u><a href="#">Clop Ransomware</a></u>	SHA256	c73388f2ae31cab1a62b18006c634a06e34d42cdd9129efc3de2d095700810d2, ac978f6aaf36d1d90c35e6dc7ae010a19082794d3391ea0111112aed7507f708, 198d3affc04ac9e18cd6fb84f06f809a53ea7b96ad61fd622188abaa11e9328d

# 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 9, 2023 • 9:25 AM**

© 2023 All Rights are Reserved by Hive Pro®



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