

Date of Publication
December 26, 2023



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

18 to 24 DECEMBER 2023

Table Of Contents

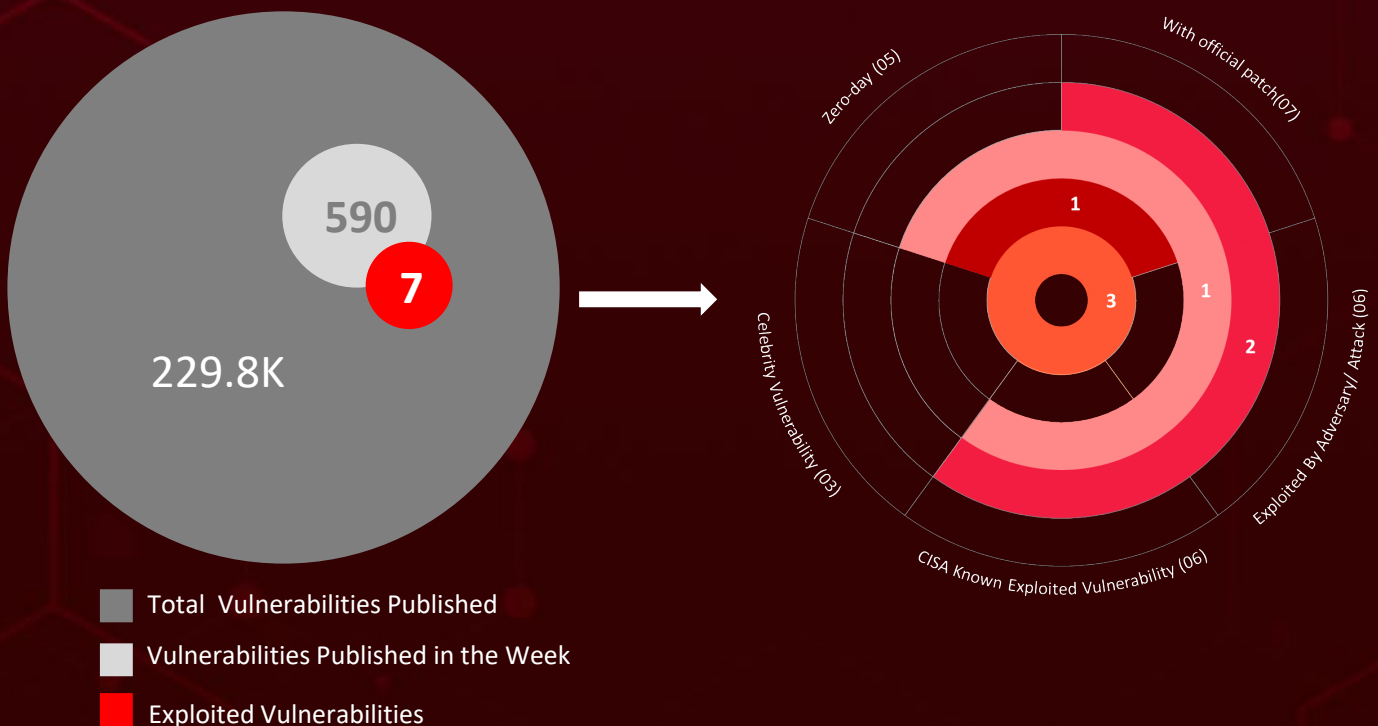
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	16
<u>Adversaries in Action</u>	20
<u>Recommendations</u>	23
<u>Threat Advisories</u>	24
<u>Appendix</u>	25
<u>What Next?</u>	31

Summary

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

Furthermore, HiveForce Labs uncovered Iranian espionage group **Muddywater**, targeted telecommunications companies in Egypt, Sudan, and Tanzania as part of their espionage efforts.

Meanwhile, a high severity zero-day vulnerability (**CVE-2023-7024**), in Google Chrome that can lead to program crashes or enable arbitrary code execution. These observed attacks have been on the rise, posing a significant threat worldwide.



High Level Statistics

15

Attacks
Executed

7

Vulnerabilities
Exploited

4

Adversaries in
Action

- [NKAbuse](#)
 - [Pierogi++](#)
 - [Micropsia](#)
 - [BarbWire](#)
 - [Play Ransomware](#)
 - [ODAgent](#)
 - [OilCheck](#)
 - [OilBooster](#)
 - [SC5k downloader](#)
 - [Kuiper ransomware](#)
 - [Pikabot](#)
 - [JaskaGO](#)
 - [Mallox ransomware](#)
 - [MuddyC2Go](#)
 - [Bandook RAT](#)
- [CVE-2017-5638](#)
 - [CVE-2018-13379](#)
 - [CVE-2020-12812](#)
 - [CVE-2022-41040](#)
 - [CVE-2022-41082](#)
 - [CVE-2021-26855](#)
 - [CVE-2023-7024](#)
- [Gaza Cybergang](#)
 - [OilRig](#)
 - [TA577](#)
 - [MuddyWater](#)



Insights

Zero-Day

Google Chrome fixes CVE-2023-7024, that can lead to program crashes or enable arbitrary code execution

OilRig

Threat group introduced three new downloaders ODAgent, OilCheck, and OilBooster targeting multiple sectors in Israel

JaskaGO

A new infostealer designed to target both Windows and macOS platforms

Zero Click

Two vulnerabilities (CVE-2023-35384 and CVE-2023-36710) in Microsoft Windows can be chained to achieve RCE on vulnerable Outlook clients.

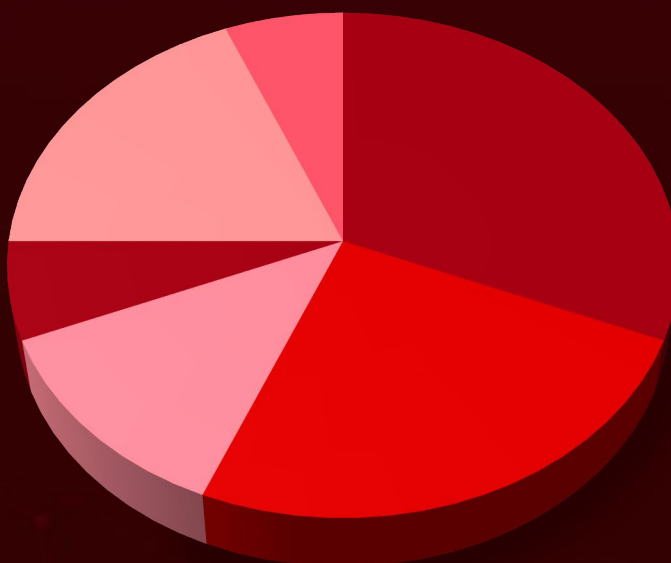
Gaza Cybergang

Threat actors are targeting the Middle East by intensifying their attacks, deploying an advanced version of the Pierogi backdoor malware

Mallox Ransomware

Recent variant, "Mallox.Resurrection," exploiting MS-SQL vulnerabilities and employing brute force attacks

Threat Distribution



■ Backdoor ■ Downloader ■ Infostealer ■ Loader ■ Ransomware ■ RAT

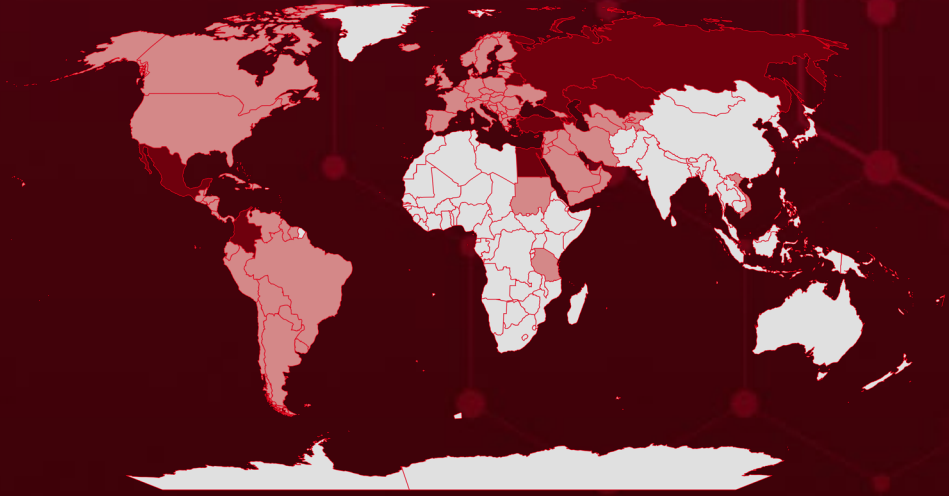


Targeted Countries

Most



Least



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

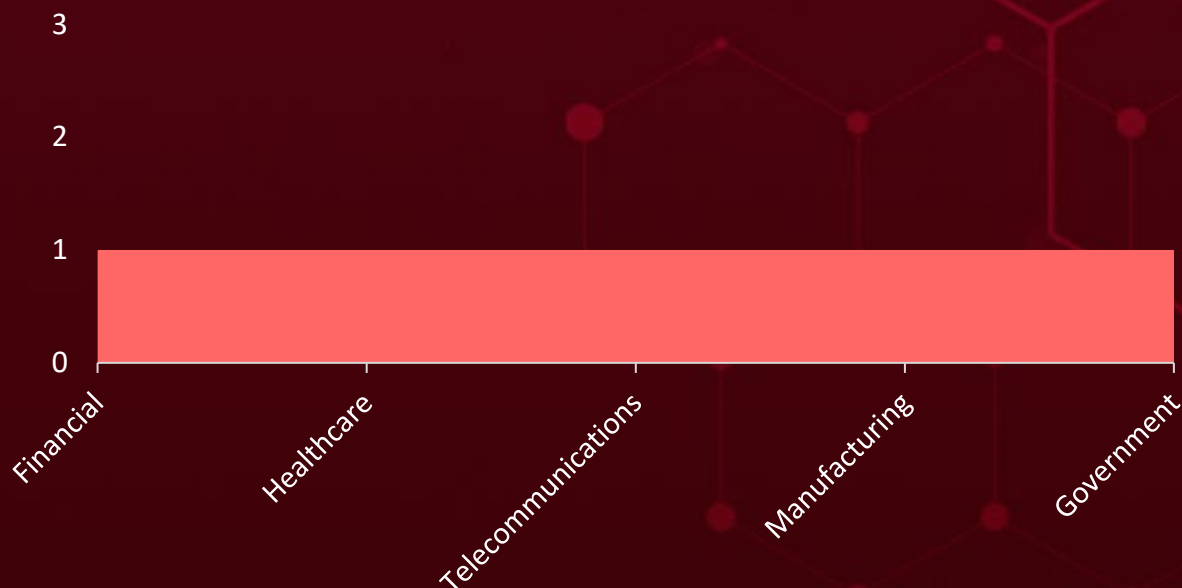
Countries
Israel
Turkey
Moldova
Armenia
Egypt
Azerbaijan
Mexico
Belarus
Russia
Colombia
Cyprus
Kazakhstan
Qatar
Malta
Syria
Bosnia and Herzegovina
Norway
Brazil
Serbia
Bulgaria
United Arab Emirates
Canada

Countries
Montenegro
Chile
Paraguay
Andorra
Saint Lucia
Costa Rica
Sudan
Croatia
Trinidad and Tobago
Cuba
Lithuania
Austria
Argentina
Czech Republic
Nicaragua
Denmark
Palestine
Dominica
Poland
Dominican Republic

Countries
Belgium
Ecuador
San Marino
Antigua and Barbuda
Slovenia
El Salvador
Sweden
Estonia
Tanzania
Finland
Turkmenistan
France
United States
Georgia
Luxembourg
Germany
Barbados
Greece
Monaco
Grenada
Netherlands
Guatemala
North Macedonia

Countries
Iraq
Saint Vincent and the Grenadines
Ireland
Saudi Arabia
Bahrain
Slovakia
Italy
Spain
Jamaica
Suriname
Jordan
Switzerland
Uruguay
Tajikistan
Uzbekistan
The Bahamas
Venezuela
Belize
Yemen
Ukraine
Latvia
United Kingdom
Lebanon

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1082

System Information Discovery

T1083

File and Directory Discovery

T1041

Exfiltration Over C2 Channel

T1057

Process Discovery

T1105

Ingress Tool Transfer

T1204

User Execution

T1053

Scheduled Task/Job

T1055

Process Injection

T1204.002

Malicious File

T1027

Obfuscated Files or Information

T1543

Create or Modify System Process

T1071

Application Layer Protocol

T1059.001

PowerShell

T1190

Exploit Public-Facing Application

T1566

Phishing

T1659

Content Injection

T1071.001

Web Protocols

T1036

Masquerading

T1574

Hijack Execution Flow

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>NKAbuse</u>	NKAbuse is a multiplatform malware that hides in blockchain networks, acts as a backdoor and flooder, and targets Linux systems and IoT devices. It infects through vulnerabilities and uses NKN to communicate with its command-and-control server.	Exploiting vulnerability	CVE-2017-5638
		IMPACT	AFFECTED PRODUCTS
		Data Theft, Launching DDoS attacks	Apache Struts Remote Code Execution Vulnerability
			PATCH LINK
		https://struts.apache.org/download.cgi#struts-ga	
IOC TYPE	VALUE		
-	-		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Pierogi++</u>	Pierogi++ is a backdoor malware targeting Palestinians, developed by Gaza Cyber Gang. It spies, executes commands, and uploads files. It's written in C++ for stealth and lacks Ukrainian clues.	-	-
		IMPACT	AFFECTED PRODUCTS
		Espionage, Disruption, Data exfiltration	-
			PATCH LINK
		-	
IOC TYPE	VALUE		
SHA1	32d0073b8297cc8350969fd4b844d80620e2273a, 3ae41f7a84ca750a774f77766ccf4fd38f7725a, 42cb16fc35cfc30995e5c6a63e32e2f9522c2a77, 5128d0af7d700241f227dd3f546b4af0ee420bbc, 5e46151df994b7b71f58556c84eeb90de0776609		

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>Micropsia</u>	Micropsia is stealthy Windows malware that steals passwords, credit card info, documents, records keystrokes, takes screenshots, spies on browsing, and sends data to attackers.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Data Theft	-
			PATCH LINK
			-
TYPE			
Infostealer			
ASSOCIATED ACTOR			
Gaza Cybergang			
IOC TYPE	VALUE		
SHA1	003bb055758a7d687f12b65fc802bac07368335e, 19026b6eb5c1c272d33bda3eab8197bec692abab, 2a45843cab0241cce3541781e4e19428dcf9d949, 5619e476392c195ba318a5ff20e40212528729ba, 745657b4902a451c72b4aab6cf00d05895bbc02f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>BarbWire</u>	BarbWire, a potent malware developed by the APT-C-23 hacking group, has emerged as a significant threat to Israeli national security and private citizens alike.	-	-
		IMPACT	AFFECTED PRODUCTS
		Data Theft, Launching DDoS attacks	-
			PATCH LINK
			-
TYPE			
Backdoor			
ASSOCIATED ACTOR			
Gaza Cybergang			
IOC TYPE	VALUE		
SHA1	4dcdcb7095da34b3cef73ad721d27002c5f65f47b, 694fa6436302d55c544cfb4bc9f853d3b29888ef		
Domain	wanda-bell[.]website		

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>Play Ransomware</u>	The Play ransomware group, active since June 2022, employs a double-extortion model, impacting businesses globally. Utilizing legitimate tools for malicious activities, the group has affected approximately 300 entities.	Exploiting vulnerabilities	CVE-2018-13379 CVE-2020-12812 CVE-2022-41040 CVE-2022-41082
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	Fortinet FortiOS, Microsoft Exchange Server
Ransomware			PATCH LINK
ASSOCIATED ACTOR			https://fortiguard.com/advisory/FG-IR-18-384 ; http://www.fortiguard.com/psirt/FG-IR-20-233 ; https://fortiguard.com/psirt/FG-IR-19-283 ; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040 ; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082
-			
IOC TYPE	VALUE		
SHA256	453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10522465deb, 47c7cee3d76106279c4c28ad1de3c833c1ba0a2ec56b0150586c7e8480ccae57, 75404543de25513b376f097ceb383e8efb9c9b95da8945fd4aa37c7b2f226212, 7a42f96599df8090cf89d6e3ce4316d24c6c00e499c8557a2e09d61c00c11986, 7a6df63d883bbccb315986c2cfb76570335abf84fafbefce047d126b32234af8		

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>ODAgent</u>	<p>ODAgent, an Iran-linked OilRig downloader, hides in cloud APIs to infect systems and fetch more malware. It targets Israel, especially healthcare, manufacturing, and government.</p>	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Downloader		Data Theft, Disruption	-
ASSOCIATED ACTOR			PATCH LINK
OilRig			-
IOC TYPE	VALUE		
SHA1	7E498B3366F54E936CB0AF767BFC3D1F92D80687		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>OilCheck</u>	<p>OilCheck, an OilRig reconnaissance malware, gathers system info and helps launch future attacks. It hides as Windows processes and targets Israel's government, military, and critical infrastructure.</p>	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Downloader		Data Theft, Disruption	-
ASSOCIATED ACTOR			PATCH LINK
OilRig			-
IOC TYPE	VALUE		
SHA1	8D84D32DF5768B0D4D2AB8B1327C43F17F182001, DDF0B7B509B240AAB6D4AB096284A21D9A3CB910		

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>OilBooster</u>	OilBooster, linked to OilRig group, is a downloader that silently grabs more malware onto your system. It hides in cloud APIs, targets Israel.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Downloader			
ASSOCIATED ACTOR			
OilRig		Data Theft, Disruption	PATCH LINK
			-
IOC TYPE	VALUE		
SHA1	1B2FEDD5F2A37A0152231AE4099A13C8D4B73C9E		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>SC5k</u>	SC5k, an Iran-linked OilRig downloader, grabs and runs hidden malware on your system. It hides in cloud APIs, targets Israel.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Downloader			
ASSOCIATED ACTOR			
OilRig		Data Theft, Disruption	PATCH 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>Kuiper ransomware</u>	The Kuiper ransomware, developed in Golang, is compatible with Windows, Linux, and OSX systems, and is associated with a suspected intrusion at a government financial department in Africa.	Exploiting vulnerability	CVE-2021-26855	
TYPE		IMPACT	AFFECTED PRODUCTS	
Ransomware				Microsoft Exchange Server
ASSOCIATED ACTOR				PATCH LINK
-				https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855
IOC TYPE	VALUE			
SHA1	90dd8718560a23faddf99e64b52175d1d765397c			
MD5	84820f3eb491a2fde1f52435cd29646c			
IPv4	91.92.251[.]25			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs		
<u>PikaBot</u>	PikaBot, a versatile malware, downloads other threats like ransomware, gives attackers remote control, and hides on Windows systems.	Malvertising	-		
TYPE		IMPACT	AFFECTED PRODUCTS		
Loader and backdoor				-	
ASSOCIATED ACTOR				Data Theft, Downloading other malware	PATCH LINK
TA577					-
IOC TYPE	VALUE				
SHA256	0e81a36141d196401c46f6ce293a370e8f21c5e074db5442ff2ba6f223c435f5, da81259f341b83842bf52325a22db28af0bc752e703a93f1027fa8d38d3495ff, 69281eea10f5bfcfd8bc0481f0da9e648d1bd4d519fe57da82f2a9a452d60320				

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
JaskaGO	JaskaGO is a new cross-platform information stealer malware. This malware is designed to target and compromise systems running both Windows and macOS operating systems.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Data Theft, Data exfiltration	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	7bc872896748f346fdb2426c774477c4f6dcedc9789a44bd9d3c889f778d5c4b, f38a29d96eee9655b537fee8663d78b0c410521e1b88885650a695aad89dbe3f, 6efa29a0f9d112cfbb982f7d9c0ddfe395b0b0edb885c2d5409b33ad60ce1435, f2809656e675e9025f4845016f539b88c6887fa247113ff60642bd802e8a15d2, 85bffa4587801b863de62b8ab4b048714c5303a1129d621ce97750d2a9a989f9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mallox Ransomware	Mallox is a resilient Ransomware-as-a-Service (RaaS) threat, utilizing tactics like exploiting MS-SQL vulnerabilities and employing brute force attacks. Operating with a prolonged presence, Mallox's recent variant, "Mallox.Resurrection," exhibits consistent functionalities.	Exploiting vulnerabilities	CVE-2019-1068 CVE-2020-0618
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data Theft	Microsoft SQL Server
ASSOCIATED ACTOR			PATCH LINK
-			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1068 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618
IOC TYPE	VALUE		
SHA256	60784ab7fec3f23066a996f3347b721a09eb677b63dbc5e1bb2bfc920fa3f13d, 9b24ee3dd5f50e65ea15aaa3946e76281c4f9d519524dc659f2bcdfb62241316, 142f2b232fa96e71379894d1bb6cb242c0f33886c1802922163901e70fdc3320, 0901a9920c9f0c74fb2170524477693d62c8493715520ae95143abd8055e7a39, 634043ca72cd2b6a4d7a1cfe2aa12b7cd8c8348055fbc38c7d8006602ac66b87		




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>MuddyC2Go</u>	MuddyC2Go, employed by the Iranian nation-state actor identified as MuddyWater, functions as a backdoor for carrying out cyber espionage attacks on the telecommunications sectors of Egypt, Sudan, and Tanzania.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Theft, data breaches, and financial losses	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
IPv4	94.131.109[.]65, 95.164.38[.]99, 45.67.230[.]91, 45.150.64(.)39 , 95.164.46[.]199		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Bandook RAT</u>	The Bandook malware is a persistent remote access trojan (RAT) that surfaced in 2007. Programmed in Delphi and C++, it has evolved through various iterations over the years and has historical associations with Dark Caracal. It featured prominently in a campaign dubbed 'Operation Manul'.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Remote access trojan		Data exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	8904ce99827280e447cb19cf226f814b24b0b4eec18dd758e7fb93476b7bf8b8, d3e7b5be903eb9a596b9b2b78e5dd28390c6aad8b8dd4ea1ba3d896d99fa0057, 3169171e671315e18949b2ff334db83f81a3962b8389253561c813f01974670b, e87c338d926cc32c966fce2e968cf6a20c088dc6aedf0467224725ce36c9a525, 2e7998a8df9491dad978dee76c63cb1493945b9cf198d856a395ba0fae5c265a		



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-2017-5638		Apache Struts: 2.3.5 - 2.5.10	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:struts:*:*:*:*:*	NKAbuse
Apache Struts Remote Code Execution Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://struts.apache.org/download.cgi#struts-ga
	CWE-20		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-13379		FortiOS: 5.6.3 - 6.0.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*	Play Ransomware
Fortinet FortiOS SSL VPN Path Traversal Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://fortiguard.com/advisory/FG-IR-18-384 http://www.fortiguard.com/psirt/FG-IR-20-233
	CWE-22		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2020-12812</u>		FortiOS: 6.0.0 - 6.4.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:fortinet:fortios:*: *.*.*.*.*.*	Play Ransomware
Fortinet FortiOS SSL VPN Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-178	T1082: System Information Discovery	https://fortiguard.com/psirt/FG-IR-19-283

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-41040</u>	ProxyNotShell	Microsoft Exchange Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:*.*.*.*.*	Play Ransomware
Microsoft Exchange Server Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1552.005: Cloud Instance Metadata API	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-41082	ProxyNotShell	Microsoft Exchange Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*	Play Ransomware
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082
	CWE-502		


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*	Kuiper ransomware
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855
	CWE-918		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-7024</u>		Google Chrome: 100.0.4896.60 - 120.0.6099.110	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:google:chrome:*:*:*:*:*:*	-
Google Chrome Heap buffer overflow in WebRTC Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://www.google.com/intl/en/chrome/?standalone=1




Adversaries in Action


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Gaza Cybergang (aka TA402, Extreme Jackal, Molerats, Gaza Hackers Team, Aluminum Saratoga, ATK 89, TAG-CT5)</u>	Gaza	Manufacturing, Agricultural and Physical security companies	Middle East
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	Pierogi++, Micropsia, and BarbWire	-	
TTPs			
TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1059: Command and Scripting Interpreter; T1083: File and Directory Discovery; T1082: System Information Discovery; T1204: User Execution; T1598: Phishing for Information; T1566.001: Spearphishing Attachment; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1543: Create or Modify System Process; T1587: Develop Capabilities; T1587.001: Malware			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>OilRig (aka APT 34, Helix Kitten, Twisted Kitten, Crambus, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13, DEV-0861, EUROPIUM, Hazel Sandstorm, Scarred Manticore)</u></p>	Iran	Healthcare sector, Manufacturing company, Local government	Israel
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	ODAgent, OilCheck, OilBooster, SC5k downloader	-	

TTPs

TA0042: Resource Development; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1583.006: Web Services; T1587: Develop Capabilities; T1587.001: Malware; T1585: Establish Accounts; T1585.003: Cloud Accounts; T1585.002: Email Accounts; T1608: Stage Capabilities; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1106: Native API; T1140: Deobfuscate/Decode Files or Information; T1480: Execution Guardrails; T1564: Hide Artifacts; T1564.003: Hidden Window; T1070: Indicator Removal; T1070.004: File Deletion; T1202: Indirect Command: Execution; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1027: Obfuscated Files or Information; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1560: Archive Collected Data; T1560.003 : Archive via Custom Method; T1074: Data Staged; T1074.001: Local Data Staging; T1132: Data Encoding; T1132.001: Standard Encoding; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1008: Fallback Channels; T1105: Ingress Tool Transfer; T1102: Web Service; T1102.002: Bidirectional Communication; T1020: Automated Exfiltration; T1041: Exfiltration Over C2 Channel; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>TA577</u>	Unknown	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	PikaBot	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0042: Resource Development; T1583: Acquire Infrastructure; T1583.008: Malvertising; T1566: Phishing; T1566.002: Spearphishing Link; T1204.002: Malicious File; T1204: User Execution; T1036: Masquerading; T1059.007: JavaScript; T1059: Command and Scripting Interpreter ; T1218.011: Rundll32; T1218: System Binary Proxy Execution; T1218.007: Msiexec			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm)</u>	Iran	Telecommunications	Egypt, Sudan, and Tanzania
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	MuddyC2Go, Venom Proxy, SimpleHelp	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1047: Windows Management Instrumentation; T1189: Drive-by Compromise; T1105: Ingress Tool Transfer; T1056: Input Capture; T1566: Phishing; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1027: Obfuscated Files or Information; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seven exploited vulnerability** and block the indicators related to the threat actor **Gaza Cybergang , OilRig, TA577, MuddyWater** and malware **NKAbuse, Pierogi++, Play Ransomware, Kuiper ransomware, Pikabot, Bandoor RAT**.

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 **seven exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Gaza Cybergang, OilRig, TA577, MuddyWater** and malware **NKAbuse, Pierogi++, Play Ransomware, Kuiper ransomware, Pikabot, Bandoor RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

[NKAbuse: A New Multiplatform Threat Exploiting the Blockchain Protocol](#)

[Gaza Cybergang's Pierogi++ Upgrade Takes Center Stage](#)

[Play Ransomware A Global Threat Impacting Businesses](#)

[OilRig Group Unleashes Three New Malware Strains](#)

[The Kuiper Ransomware Surge and Its Dark Origins](#)

[PikaBot Malware Unleashes Threat via Malvertising](#)

[Novel Go-Based Malware Unleashes Coordinated Strikes on macOS and Windows](#)

[Mallox Ransomware A Resurgent Threat Exploiting MS-SQL Flaws](#)

[Google's Battle Against Zero-Day Vulnerability Continues](#)

[Muddywater Utilizes Custom Tools to Target Telecom Companies](#)

[Zero-Click Outlook RCE Exploitation Chain in Windows](#)

[Bandook a 2007 Legacy Still Thriving in the Threat Landscape](#)

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.

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>Pierogi++</u>	SHA1	32d0073b8297cc8350969fd4b844d80620e2273a, 3ae41f7a84ca750a774f777766ccf4fd38f7725a, 42cb16fc35cfc30995e5c6a63e32e2f9522c2a77, 5128d0af7d700241f227dd3f546b4af0ee420bbc, 5e46151df994b7b71f58556c84eeb90de0776609, 60480323f0e6efa3ec08282650106820b1f35d2f, 75a63321938463b8416d500b34a73ce543a9d54d, aeeeee47becaa646789c5ee6df2a6e18f1d25228, da96a8c04edf8c39d9f9a98381d0d549d1a887e8, f3e99ec389e6108e8fda6896fa28a4d7237995be
	Domians	aracaravan[.]com, beatricewarner[.]com, swsan-lina-soso[.]info, zakaria-chotzen[.]info
<u>Micropsia</u>	SHA1	003bb055758a7d687f12b65fc802bac07368335e, 19026b6eb5c1c272d33bda3eab8197bec692abab, 2a45843cab0241cce3541781e4e19428dcf9d949, 5619e476392c195ba318a5ff20e40212528729ba, 745657b4902a451c72b4aab6cf00d05895bbc02f, 95fc3fb692874f7415203a819543b1e0dd495a57, c3038d7b01813b365fd9c5fd98cd67053ed22371
	Domains	bruce-ess[.]com, claire-conway[.]com, delooy[.]com, izocraft[.]com, jane-chapman[.]com, porthopeminorhockey[.]net, wayne-lashley[.]com

Attack Name	TYPE	VALUE
<u>BarbWire</u>	SHA1	4dcdb7095da34b3cef73ad721d27002c5f65f47b, 694fa6436302d55c544cfb4bc9f853d3b29888ef
	Domain	wanda-bell[.]website
<u>Kuiper Ransomware</u>	SHA1	90dd8718560a23faddf99e64b52175d1d765397c
	MD5	84820f3eb491a2fde1f52435cd29646c
	IPv4	91.92.251[.]25
<u>Play Ransomware</u>	MD5	09f341874f72a5cfcedbca707bfd1b3b, 57bcb8cfad510109f7ddedf045e86a70
	SHA256	453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10 522465deb, 47c7cee3d76106279c4c28ad1de3c833c1ba0a2ec56b0150586c7e8 480ccae57, 75404543de25513b376f097ceb383e8efb9c9b95da8945fd4aa37c7 b2f226212, 7a42f96599df8090cf89d6e3ce4316d24c6c00e499c8557a2e09d61c 00c11986, 7a6df63d883bbccb315986c2cfb76570335abf84fafbefce047d126b3 2234af8, 7dea671be77a2ca5772b86cf8831b02bff0567bce6a3ae023825aa40 354f8aca, c59f3c8d61d940b56436c14bc148c1fe98862921b8f7bad97fbc96b3 1d71193c, e652051fe47d784f6f85dc00adca1c15a8c7a40f1e5772e6a95281d8 bf3d5c74, e8d5ad0bf292c42a9185bb1251c7e763d16614c180071b01da74297 2999b95da
	SHA1	6e8582faeaf34f63fbe0083a811bcce1aa6c31de, e6c381859f53d0c0db9fcd30fa601ecb935b93e0
	IPv4	85.203.44[.]5, 85.203.44[.]8

Attack Name	TYPE	VALUE
<u>MuddyC2Go</u>	SHA256	1a0827082d4b517b643c86ee678eaa53f85f1b33ad409a23c50164c3909fdaca, 25b985ce5d7bf15015553e30927691e7673a68ad071693bf6d0284b069ca6d6a
	IPv4	94.131.109[.]65, 95.164.38[.]99, 45.67.230[.]91, 45.150.64[.]39, 95.164.46[.]199, 94.131.98[.]14
<u>ODAgent</u>	SHA1	7E498B3366F54E936CB0AF767BFC3D1F92D80687
<u>OilCheck</u>	SHA1	8D84D32DF5768B0D4D2AB8B1327C43F17F182001, DDF0B7B509B240AAB6D4AB096284A21D9A3CB910
<u>OilBooster</u>	SHA1	1B2FEDD5F2A37A0152231AE4099A13C8D4B73C9E
<u>PikaBot</u>	SHA256	0e81a36141d196401c46f6ce293a370e8f21c5e074db5442ff2ba6f223c435f5, da81259f341b83842bf52325a22db28af0bc752e703a93f1027fa8d38d3495ff, 69281eea10f5bfcfd8bc0481f0da9e648d1bd4d519fe57da82f2a9a452d60320
	Domains	anadesky[.]ovmv[.]net, cxtensones[.]top
	IPv4	172[.]232[.]186[.]251, 57[.]128[.]83[.]129, 57[.]128[.]164[.]11, 57[.]128[.]108[.]132, 139[.]99[.]222[.]29, 172[.]232[.]164[.]77, 54[.]37[.]79[.]82, 172[.]232[.]162[.]198, 57[.]128[.]109[.]221
<u>JaskaGO</u>	SHA256	7bc872896748f346fdb2426c774477c4f6dcedc9789a44bd9d3c889f778d5c4b, f38a29d96eee9655b537fee8663d78b0c410521e1b88885650a695aad89dbe3f, 6efa29a0f9d112cfbb982f7d9c0ddfe395b0b0edb885c2d5409b33ad60ce1435

Attack Name	TYPE	VALUE
<u>JaskaGO</u>	SHA256	f2809656e675e9025f4845016f539b88c6887fa247113ff60642bd802e8a15d2, 85bffa4587801b863de62b8ab4b048714c5303a1129d621ce97750d2a9a989f9, 37f07cc207160109b94693f6e095780bea23e163f788882cc0263cbddac37320, e347d1833f82dc88e28b1baaa2657fe7ecbfe41b265c769cce25f1c0e181d7e0, c714f3985668865594784dba3aeda1d961acc4ea7f59a178851e609966ca5fa6, 9b23091e5e0bd973822da1ce9bf1f081987daa3ad8d2924ddc87eee6d1b4570d, 1c0e66e2ea354c745aebda07c116f869c6f17d205940bf4f19e0fdf78d5dec26, e69017e410aa185b34e713b658a5aa64bff9992ec1dbd274327a5d4173f6e559, 6cdda60ffbc0e767596eb27dc4597ad31b5f5b4ade066f727012de9e510fc186, 44d2d0e47071b96a2bd160aeed12239d4114b7ec6c15fd451501c008d53783cf, 8ad4f7e14b36ffa6eb7ab4834268a7c4651b1b44c2fc5b940246a7382897c98e, 888623644d722f35e4dcc6df83693eab38c1af88ae03e68fd30a96d4f8cbcc01, 3f139c3fcad8bd15a714a17d22895389b92852118687f62d7b4c9e57763a8867, 207b5ee9d8cbff6db8282bc89c63f85e0ccc164a6229c882ccdf6143ccfeffc
<u>Mallox Ransomware</u>	SHA1	3d434b7cc9589c43d986bf0e1cadb956391b5f9a, 9295a02c49aa50475aa7876ca80b3081a361ff7d, 3fa79012dfdac626a19017ed6974316df13bc6ff, 7e7957d7e7fd7c27b9fb903a0828b09cbb44c196, 08a236455490d5246a880821ba33108c4ef00047, 0d2711c5f8eb84bd9915a4191999afd46abca67a, 0e45e8a5b25c756f743445f0317c6352d3c8040a, 11d7779e77531eb27831e65c32798405746ccea1, 246e7f798c3bfba81639384a58fa94174a08be80, 273e40d0925af9ad6ca6d1c6a9d8e669a3bdc376, 2a6f632ab771e7da8c551111e2df786979fd895d, 2c49fa21b0a8415994412fe30e023907f8a7b46e, 33c24486f41c3948fbd761e6f55210807af59a1f, 4c863df8ea7446cb7fba6e582959bc3097f92b5c, 4fcfb65cb757c83ed91bc01b3f663072a52da54b, 5229a5d56836c3d3fc7fb12a43a431b5c90f771d,

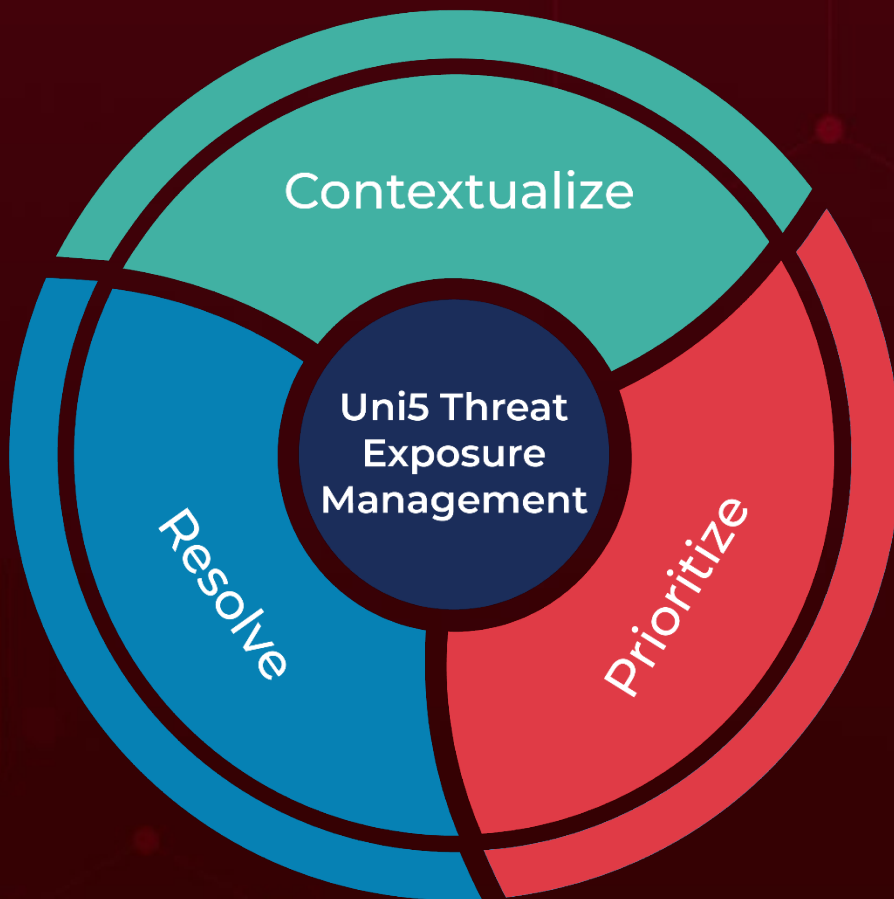
Attack Name	TYPE	VALUE
<u>Mallox ransomware</u>	SHA1	552862af77b204ac1f69b9e25937cc60e30e6c0f, 5d0b9521cca0c911d49162e7f416a1463fbaefae, 5d9cc0bc652b1d21858d2e4ddd35303cd9aeb2a3, 63408c84c5d642cf1c5b643a97b84e22e18323c0, 643918830b87691422d6d7bd669c408679411303, 65d7cb5f1770b77b047baf376bd6b4cf86c5d42c, 88eef50d85157f2e0552aab07cac7e7ec21680f5, 88f8629423efe84e2935eb71d292e194be951a16, 9d182e17f88e26cb0928e8d07d6544c2d17e99f5, a8886c9417b648944d2afd6b6c4941588d670e3c, db3fd39fc826e87fa70840e86d5c12eef0fe0566, ee15c76e07051c10059a14e03d18a6358966e290, fb05a6fadc28194d011a909d946b3efa64cdb4cf,
	IPv4	104[.]21.76.77, 104[.]237.62.211, 172[.]67.191.103, 64[.]185.227.155, 80[.]66.75.37
<u>MuddyC2 Go</u>	SHA256	1a0827082d4b517b643c86ee678eaa53f85f1b33ad409a23c50164c3909fdaca, 25b985ce5d7bf15015553e30927691e7673a68ad071693bf6d0284b069ca6d6a
	IPv4	94.131.109[.]65, 95.164.38[.]99, 45.67.230[.]91, 45.150.64(.)39 , 95.164.46[.]199, 94.131.98[.]14
<u>Bandook RAT</u>	SHA256	8904ce99827280e447cb19cf226f814b24b0b4eec18dd758e7fb93476b7bf8b8, d3e7b5be903eb9a596b9b2b78e5dd28390c6aadb8bdd4ea1ba3d896d99fa0057, 3169171e671315e18949b2ff334db83f81a3962b8389253561c813f01974670b, e87c338d926cc32c966fce2e968cf6a20c088dc6aedf0467224725ce36c9a525, 2e7998a8df9491dad978dee76c63cb1493945b9cf198d856a395ba0fae5c265a,

Attack Name	TYPE	VALUE
<u>Bandook</u> <u>RAT</u>	SHA256	430b9e91a0936978757eb8c493d06cbd2869f4e332ae00be0b759f2f229ca8ce, cd78f0f4869d986cf129a6c108264a3517dbcf16ecfc7c88ff3654a6c9be2bca
	IPv4	77.91.100[.]237, 45.67.34[.]219

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

December 26, 2023 • 6:30 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com