Date of Publication
May 29, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

22 to 28 MAY 2023

Table Of Contents

Summary

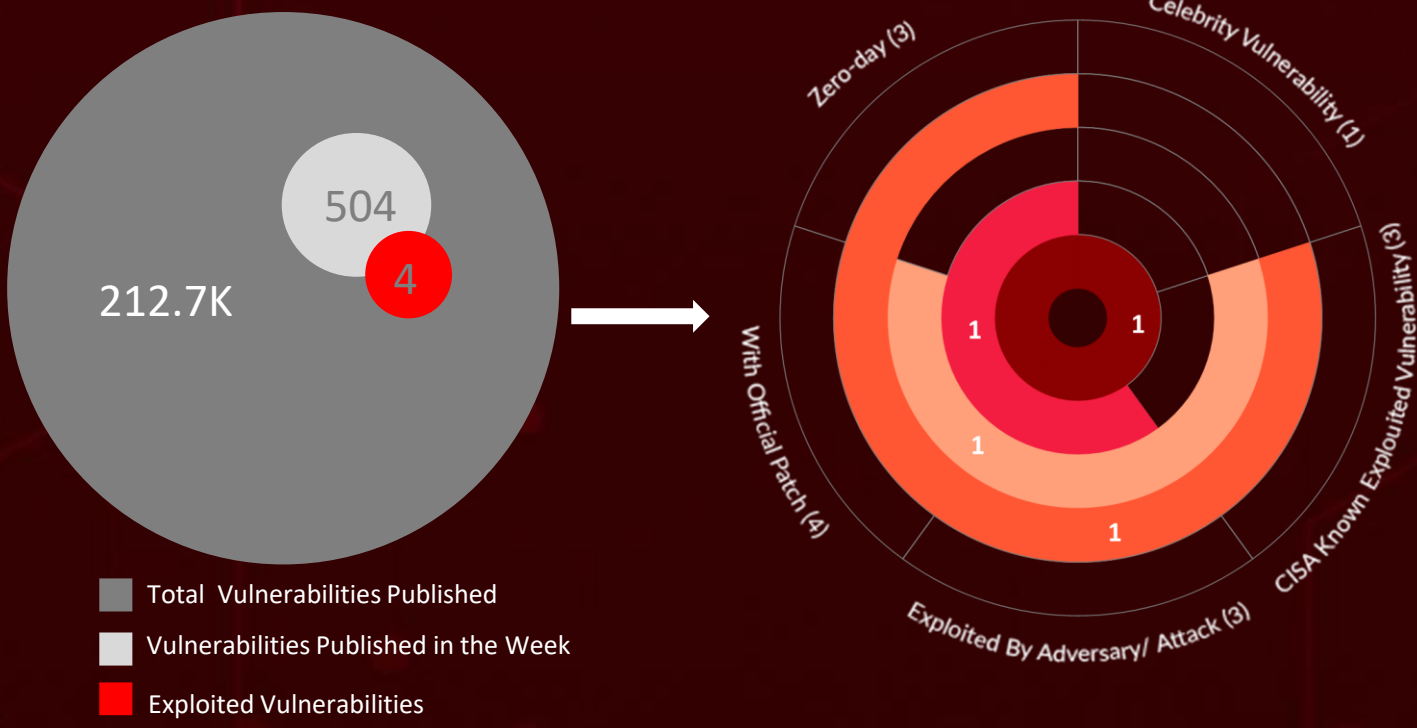
HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of **ten** attacks executed, taking advantage of **four** different vulnerabilities in various systems, and involving **three** different adversaries highlights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

Interestingly, out of these **three** vulnerabilities are part of the known exploited vulnerability catalog by CISA.

Moreover, HiveForce Labs also found that **GoldenJackal APT** was exploiting a one-year-old Follina vulnerability (**CVE-2022-30190**).

Furthermore, we identified a new powershell-based backdoor malware **PowerExchange** that is being distributed through phishing emails targeting Microsoft Exchange servers.

Apart from these threats, there was also a new ransomware strain named **MichaelKors**, has been targeting Linux and Vmware ESXi systems using tactic of "**hypervisor jackpotting**". All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

10
Attacks Executed

4
Vulnerabilities Exploited

3
Adversaries in Action

- MichaelKors
- BlackCat
- Donut
- JackalControl
- JackalSteal
- JackalWorm
- JackalPerInfo
- JackalScreenWatcher
- Pikabot
- PowerExchange

- CVE-2023-2868
- CVE-2023-23397
- CVE-2022-30190
- CVE-2021-22205

- APT28
- GUI-vil
- GoldenJackal

Insights

WINTAPIX driver

Targeting Middle Eastern countries

GoldenJackal APT

Targeting Government and Diplomatic entities in Middle East and South Asia

One 0-day

Found in Barracuda's Email Security Gateway (ESG)

BlackCat

Ransomware utilizes a signed kernel driver for defense evasion

APT28

Targeting the Ukrainian civic community by the help of Russian GRU

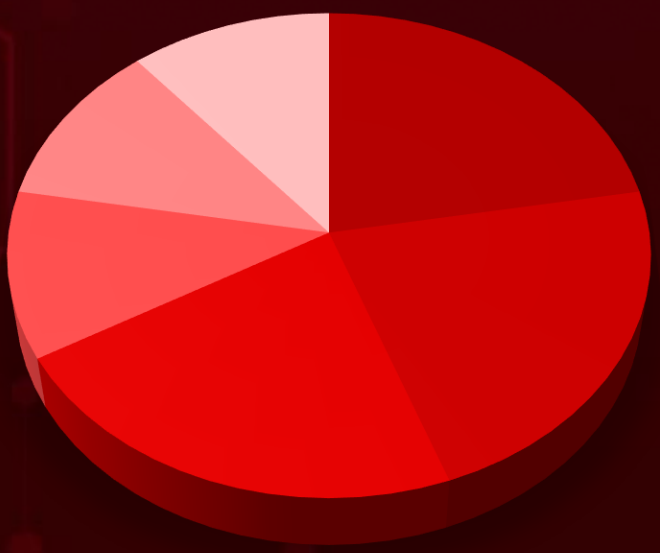
Pikabot

Employs anti-analysis measures like the "sleep" function

GUI-vil

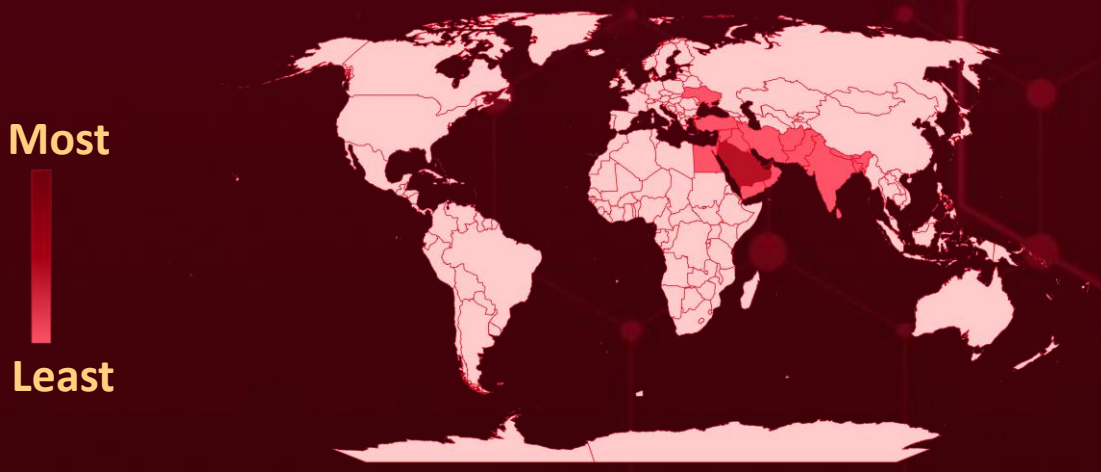
Indonesian Threat Group Exploits AWS for Crypto Mining

Threat Distribution



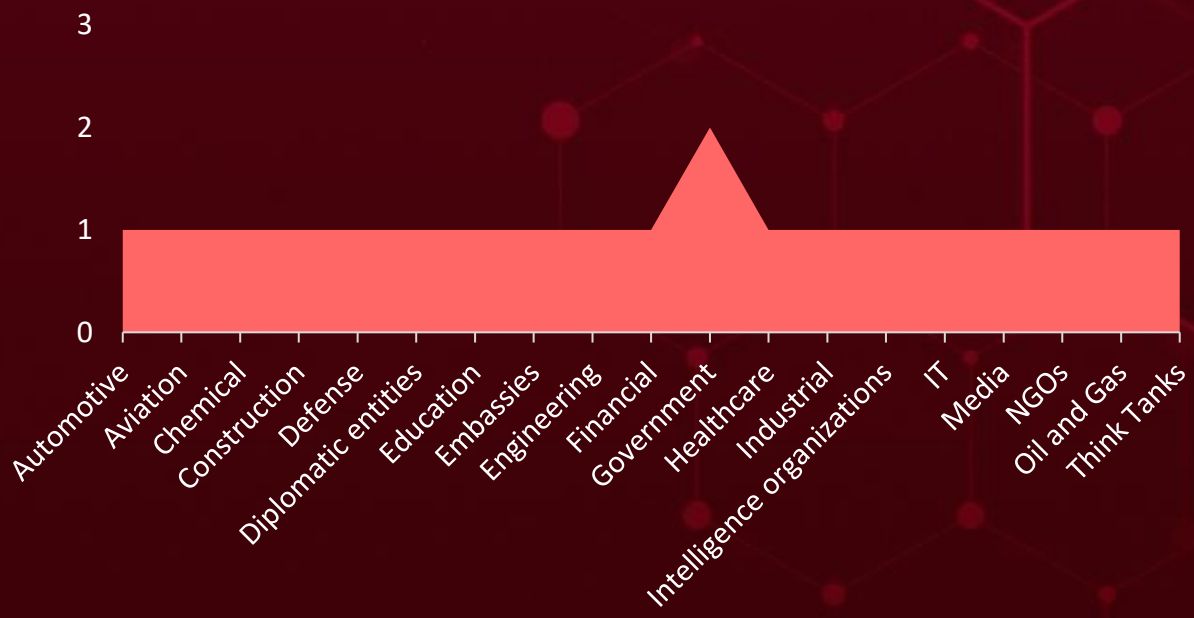
Ransomware Backdoor InfoStealer Loader Spyware Trojan

Targeted Countries



	Countries
	United Arab Emirates
	Qatar
	Saudi Arabia
	Jordan
	Bhutan
	Oman
	Maldives
	Egypt
	Palestine
	India
	Cyprus
	Iran
	Nepal
	Iraq
	Pakistan
	Israel
	Bangladesh
	Syria
	Sri Lanka
	Turkey
	Yemen
	Bahrain
	Ukraine
	Kuwait
	Afghanistan
	Lebanon

Targeted Industries



TOP MITRE ATT&CK TTPS

T1027 Obfuscated Files or Information

T1041 Exfiltration Over C2 Channel

T1021 Remote Services

T1068 Exploitation for Privilege Escalation

T1569 System Services

T1505 Server Software Component

T1566 Phishing

T1036 Masquerading

T1078 Valid Accounts

T1059 Command and Scripting Interpreter

T1190 Exploit Public-Facing Application

T1083 File and Directory Discovery

T1518 Software Discovery

T1057 Process Discovery

T1564 Hide Artifacts

T1071 Application Layer Protocol

T1588 Obtain Capabilities

T1055 Process Injection

T1095 Non-Application Layer Protocol

T1056 Input Capture

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MichaelKors	MichaelKors ransomware, a new RaaS operation, has been targeting Linux and VMware ESXi systems since April 2023, utilizing the tactic of "hypervisor jackpotting" to gain unrestricted access and encrypt files, posing a significant threat to organizations' virtualization infrastructure.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial and data losses	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5 cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849 a32b7e40fc353fd2f13307d8bfe1c7c634c8c897b80e72a9872baa9a1da08c46 855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcdd956e0808 7095beafff5837070a89407c1bf3c6acf8221ed786e0697f6c578d4c3de0efd6		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlackCat (aka ALPHV, AlphaV, AlphaVM, ALPHV-ng, or Noberus)	BlackCat ransomware is a sophisticated threat targeting corporate environments. It employs advanced encryption, spreading capabilities, and triple extortion tactics. It now uses a signed kernel driver for defense evasion.	Phishing Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial and data losses	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	52d5c35325ce701516f8b04380c9fbdb78ec6bcc13b444f758fdb03d545b0677 c8f9e1ad7b8cce62fba349a00bc168c849d42cfb2ca5b2c6cc4b51d054e0c497		
SHA1	17bd8fda268cbb009508c014b7c0ff9d8284f850 78cd4dfb251b21b53592322570cc32c6678aa468 c2387833f4d2fbb1b54c8f8ec8b5b34f1e8e2d91		

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
Donut	Donut is a position-independent shellcode that runs .NET Assemblies, PE files, and other Windows payloads from memory with customizable parameters.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		System compromise, data loss, and unauthorized access	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	f6c316e2385f2694d47e936boac4bc9b55e279d530dd5e805f0d963cb47c3c0d 8578bff36e3b02cc71495b647db88c67c3c5ca710b5a2bd539148550595d0330 aae9c8bd9db4e0d48e35d9ab3b1a8c7933284dcbeb344809fed18349a9ec7407 27a6c3f5c50c8813ca34ab3b0791c08817c8038776657749548908848429 73ed 1485cOed3e875cbdfc6786a5bd26d18ea9d31727deb8df290a1cOOc780419a4e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JackalControl	Jackal Control is a Trojan that enables remote control of a target machine through predefined commands. It uses an HTTPS communication channel to receive instructions, allowing attackers to execute programs, download files, and upload files.	Unknown	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		System compromise, data loss, and unauthorized access	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190
IOC TYPE	**VALUE**		
MD5	5ed498f9ad6e74442b9b6fe289d9feb3 a5ad15a9115a60f15b7796bc717a471d c6e5c8bd7c066008178bc1fb19437763 4f041937da7748ebf6d0bbc44f1373c9 eab4f3a69b2d30b16df3d780d689794c		

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
JackalSteal	JackalSteal is a file exfiltration implant used to locate and extract targeted files from compromised machines, monitoring USB drives, remote shares, and logical drives, while requiring installation by another component as it lacks persistence.	Unknown	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		System compromise, data loss, and unauthorized access	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

IOC TYPE	VALUE
MD5	c05999b9390a3d8f4086f6074a592bc2
URLs	hxxps://tahaherbal[.]ir/wp-includes/class-wp-http-iwr-client.php hxxps://winoptimum[.]com/wp-includes/customize/class-wp-customize-sidebar-refresh.php

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JackalWorm	The Jackal Worm is a self-propagating malware that spreads through USB drives, hiding and replacing directories with copies of itself to infect systems with different types of malware.	USB drives	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Worm		Unauthorized execution of malicious code, data loss, system instability	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

IOC TYPE	VALUE
MD5	5de309466b2163958c2e12c7b02d8384

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
JackalPerInfo	Jackal Perinfo is a malware that gathers system information and targeted files containing stored credentials and web activities, using predefined directories and files for its operations.	Unknown	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		Data theft	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190
IOC TYPE	**VALUE**		
MD5	a491aefb659d2952002ef20ae98d7465		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JackalScreenWatcher	JackalScreenWatcher is a malware tool that captures screenshots of the victim's desktop and sends them to a remote server using encryption and compression techniques, sharing similarities with the JackalSteal component.	USB drives	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Spyware		Data loss	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190
IOC TYPE	**VALUE**		
MD5	1072bfeee89e369a9355819ffa39ad20		
URLs	hxxps://tahaherbal[.]ir/wp-includes/class-wp-http-iwr-client.php hxxps://winoptimum[.]com/wp-includes/customize/class-wp-customize-sidebar-refresh.php		

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
Pikabot	Pikabot is an advanced backdoor that has been active since 2023, utilizing anti-analysis techniques, including the "sleep" function and language-based execution cessation, while also showing associations with the Qakbot trojan.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Unauthorized access and control over compromised systems.	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	92153e88db63016334625514802d0d1019363989d7b3f6863947ce0e490c1006 a48c39cc45efea110a7c8edadcb6719f5d1ebbeebb570b345f47172d393c0821 8ee9141074b48784c89aa5d3cd4010fcf4e6d467b618c8719970f78fcc24a365 a9db5aca01499f6ce404db22fb4ba3e4e0dc4b94a41c805c520bd39262df1ddc 347e2f0d8332dd2d9294d06544c051a302a2436da453b2ccfa2d7829e3a79944		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PowerExchange	PowerExchange is a PowerShell-based backdoor malware for Microsoft Exchange servers, enabling credential theft, command execution, and file exfiltration, while evading detection by utilizing the Exchange Web Services API for communication.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	f18575065970ef36e613ffa046f381fe9b01b3e9 2ba23d9115fb1c1d4c5899d34dc4772631d77eda 2b995ce4656db7257451080111705d5b98b45df3 68299DF5D8CE52845A8FC10598F138840094181C d82aad3222664ec9fb112808dfabbb56de9aa770		

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-2023-2868	ZERO-DAY	Barracuda Networks Email Security Gateway (ESG): 5.1.3 - 9.2	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:barracuda_networks:esg:9.2:*:*:*:*:*:*:*	-
Barracuda Networks ESG Appliance Improper Input Validation Vulnerability		CWE ID	ASSOCIATED TTPs	PATCH LINK
		CWE-20	T1059: Command and Scripting Interpreter	https://status.barracuda.com/incidents/34kx82j5n4q9

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-23397	ZERO-DAY	Microsoft Windows	APT28
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:365_apps::*:*:*:enterprise:*:*:*	-
Microsoft Office Outlook Privilege Escalation Vulnerability		CWE ID	ASSOCIATED TTPs	PATCH LINK
		CWE-294	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	Follina	Microsoft Windows	GoldenJackal
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*	JackalControl, JackalWorm, JackalSteal, JackalPerInfo and JackalScreenWatcher
Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22205		Community and Enterprise Editions From 11.9	GUI-vil
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:*	-
GitLab Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1203: Exploitation for Client Execution	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
APT28 (aka FANCY BEAR, STRONTIUM, Sofacy, Zebrocy, Sednit, Pawn Storm, TG-4127, Tsar-Team, Iron Twilight, Swallowtail, SNAKEMACKEREL, Frozen Lake)	Russia	Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and Gas, Think Tanks, and Intelligence organizations	Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-23397	-	Microsoft Windows
TTPs			
T1176:Browser Extensions; T1014:Rootkit; T1114:Email Collection; T1566:Phishing; T1056:Input Capture; T1134:Access Token Manipulation; T1204:User Execution			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
GUI-vil (aka p0-LUCR-1)	Indonesia	Cloud computing and technology services	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-22205	-	Community and Enterprise Editions From 11.9
TTPs			
T1596:Search Open Technical Databases; T1098:Account Manipulation; T1078:Valid Accounts; T1068:Exploitation for Privilege Escalation; T1496:Resource Hijacking; T1021:Remote Services; T1021.004:SSH; T1211:Exploitation for Defense Evasion; T1538:Cloud Service Dashboard			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 GoldenJackal APT	Unknown	Government and Diplomatic entities	Middle East and South Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-30190	JackalControl, JackalWorm, JackalSteal, JackalPerInfo and JackalScreenWatcher	Microsoft Windows
TTPs			
T1027:Obfuscated Files orInformation; T1219:Remote Access Software; T1059:Command and ScriptingInterpreter; T1112:Modify Registry; T1021:Remote Services; T1003:OS Credential Dumping; T1056:Input Capture; T1574:Hijack Execution Flow; T1055:Process Injection; T1090:Proxy; T1566:Phishing; T1218:System Binary Proxy Execution; T1566.001:Spearphishing Attachment; T1190:Exploit Public-Facing Application; T1021:Remote Services; T1041:Exfiltration Over C2 Channel; T1555:Credentials from Password Stores; T1005:Data from Local System; T1102:Web Service; T1113:Screen Capture; T1204:User Execution; T1204.002:Malicious File; T1036:Masquerading; T1221:Template Injection; T1588:Obtain Capabilities; T1588.005:Exploits; T1092:Communication Through Removable Media; T1053:Scheduled Task/Job			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actor **APT28, GUI-vil, GoldenJackal** and malware **MichaelKors , BlackCat , Donut , JackalControl , JackalSteal, JackalWorm, JackalPerInfo, JackalScreenWatcher , Pikabot, and PowerExchange.**

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 **four exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT28, GUI-vil, GoldenJackal** and malware **MichaelKors , BlackCat , Donut , JackalControl , JackalSteal, JackalWorm, JackalPerInfo, JackalScreenWatcher , Pikabot, and PowerExchange** in Breach and Attack Simulation(BAS).

Threat Advisories

MichaelKors Ransomware Targets Linux and VMware ESXi Systems with Hypervisor Jackpotting

APT28's Cyber Espionage Campaigns Targeting Ukraine

Advanced BlackCat Ransomware Using Triple Extortion Tactics and Signed Kernel Driver

WINTAPIX Kernel Driver Targeting Middle Eastern Nations

Unveiling the Stealthy Operations of GoldenJackal APT Group

GUI-Vil Threat Group Exploits AWS for Crypto Mining

A Zero-Day Vulnerability Found in Barracuda Email Security Gateway

Pikabot A Stealthy Backdoor with Ingenious Evasion Tactics

PowerExchange Backdoor and Web Shells Breach at UAE Government Agency

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
MichaelKors Ransomware	SHA256	da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5 cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849 a32b7e40fc353fd2f13307d8bfe1c7c634c8c897b80e72a9872baa9a1da08c46 855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcdd956e0808 7095beafff5837070a89407c1bf3c6acf8221ed786e0697f6c578d4c3de0efd6 3339ba53e1f05f91dbe907d187489dbaba6c801f7af6fd06521f3ba8c484ec6c
	SHA1	c7fcbaedf6b077b3d9bfc4720c3860a5d848bcb4 c7b28fe059e944f883058450d5c77b03076b0ea1 b033a146de147d97db6f8dadbe2141df2f0192be 91ad089f5259845141dfb10145271553aa711a2b 228239d1bf7020ecdc4021f3c20a14041b210d78 0f5457b123e60636623f585cc2bf2729f13a95d6
	MD5	c159afb7d2111690326cad610776db34 b0fd45162c2219e14bdccab76f33946e aa1ddf0c8312349be614ff43e80a262f 99549bcea63af5f81b01decf427519af 546af2069c28f794dc918958a80ac17b 40c9dc2897b6b348da88b23deb0d3952
Blackcat Ransomware	SHA256	52d5c35325ce701516f8b04380c9fbdb78ec6bcc13b444f758fdb03d545b0677 c8f9e1ad7b8cce62fba349a00bc168c849d42cfb2ca5b2c6cc4b51d054e0c497

Attack Name	TYPE	VALUE
BlackCat Ransomware	MD5	909f3fc221acbe999483c87d9ead024a a837302307dace2a00d07202b661bce2
	SHA1	17bd8fda268cbb009508c014b7c0ff9d8284f850 78cd4dfb251b21b53592322570cc32c6678aa468 c2387833f4d2fbb1b54c8f8ec8b5b34f1e8e2d91 91568d7a82cc7677f6b13f11bea5c40cf12d281b 0bec69c1b22603e9a385495fbe94700ac36b28e5 5ed22c0033aed380aa154e672e8db3a2d4c195c4 cb25a5125fb353496b59b910263209f273f3552d 994e3f5dd082f5d82f9cc84108a60d359910ba79 f6793243ad20359d8be40d3accac168a15a327fb b2f955b3e6107f831ebe67997f8586d4fe9f3e98
Donut	SHA256	f6c316e2385f2694d47e936boac4bc9b55e279d530dd5e805f 0d963cb47c3c0d 8578bff36e3b02cc71495b647db88c67c3c5ca710b5a2bd5391 48550595d0330 aae9c8bd9db4e0d48e35d9ab3b1a8c7933284dcbeb344809fe d18349a9ec7407 27a6c3f5c50c8813ca34ab3b0791c08817c803877665774954 890884842973ed 1485cOed3e875cbdfc6786a5bd26d18ea9d31727deb8df290a 1cOOc780419a4e
JackalControl	MD5	5ed498f9ad6e74442b9b6fe289d9feb3 a5ad15a9115a60f15b7796bc717a471d c6e5c8bd7c066008178bc1fb19437763 4f041937da7748ebf6d0bbc44f1373c9 eab4f3a69b2d30b16df3d780d689794c 8c1070f188ae87fba1148a3d791f2523
	URLs	hxxp://abert-online[.]de/meeting/plugins[.]php hxxp://acehigh[.]host/robotx[.]php hxxp://assistance[.]uz/admin/plugins[.]php hxxp://cnom[.]sante[.]gov[.]ml/components/com_avreloaded/views/popup/tmpl/header[.]php hxxp://info[.]merysof[.]am/plugins/search/content/plugins[.]php hxxp://invest[.]zyrardow[.]pl/admin/model/setting/plugins[.]php hxxp://weblines[.]gr/gallery/gallery_input[.]php hxxp://www[.]wetter-bild[.]de/plugins[.]php hxxps://ajapnyakmc[.]com/wp-content/cache/index[.]php hxxps://asusiran[.]com/wp-content/plugins/persian-woocommerce/include/class-cache[.]php hxxps://asusiran[.]com/wp-content/themes/woodmart/inc/modules/cache[.]php

Attack Name	TYPE	VALUE
JackalControl	URLs	hxxps://croma[.]vn/wp-content/themes/croma/template-parts/footer[.]php hxxps://den-photomaster[.]kz/wp-track[.]php hxxps://eyetelligence[.]ai/wp-content/themes/cms/inc/template-parts/footer[.]php hxxps://finasteridehair[.]com/wp-includes/class-wp-network-statistics[.]php hxxps://gradaran[.]be/wp-content/themes/tb-sound/inc/footer[.]php hxxps://mehrganhospital[.]com/wp-includes/class-wp-tax-system[.]php hxxps://meukowcognac[.]com/wp-content/themes/astra/page-flags[.]php hxxps://nassiraq[.]iq/wp-includes/class-wp-header-styles[.]php hxxps://new[.]jmcashback[.]com/wp-track[.]php hxxps://news[.]lmond[.]com/wp-content/themes/newsbook/inc/footer[.]php hxxps://pabalochistan[.]gov[.]pk/new/wp-content/cache/functions[.]php hxxps://pabalochistan[.]gov[.]pk/new/wp-content/themes/dt-the7/inc/cache[.]php hxxps://pabalochistan[.]gov[.]pk/new/wp-content/themes/twentyfifteen/content-manager[.]php hxxps://sbj-i[.]com/wp-content/plugins/wp-persian/includes/class-wp-cache[.]php hxxps://sbj-i[.]com/wp-content/themes/hamyarwp-spacious/cache[.]php hxxps://sokerpower[.]com/wp-includes/class-wp-header-styles[.]php hxxps://technocometsolutions[.]com/wp-content/themes/seofy/templates-sample[.]php hxxps://www[.]djstuff[.]fr/wp-content/themes/twentyfourteen/inc/footer[.]php hxxps://www[.]perlesoie[.]com/wp-content/plugins/contact-form-7/includes/cache[.]php hxxps://www[.]perlesoie[.]com/wp-content/themes/flatsome/inc/classes/class-flatsome-cache[.]php
JackalSteal	URLs	hxxps://tahaherbal[.]ir/wp-includes/class-wp-http-iwr-client.php hxxps://winoptimum[.]com/wp-includes/customize/class-wp-customize-sidebar-refresh.php
	MD5	C05999b9390a3d8f4086f6074a592bc2

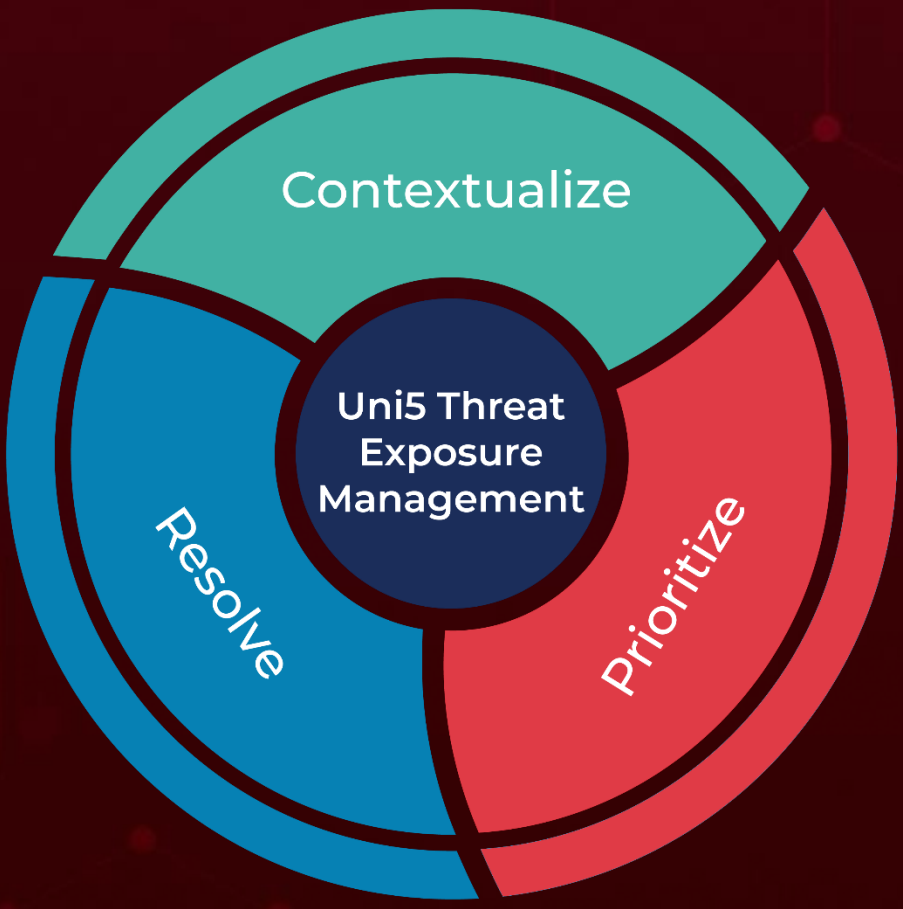
Attack Name	TYPE	VALUE
JackalWorm	MD5	5de309466b2163958c2e12c7b02d8384
JackalPerInfo	MD5	a491aefb659d2952002ef20ae98d7465
JackalScreenWatcher	MD5	1072bfeee89e369a9355819ffa39ad20
Pikabot	SHA256	92153e88db63016334625514802d0d1019363989d7b3f6863947ce0e490c1006 a48c39cc45efea110a7c8edadcb6719f5d1ebbeebb570b345f47172d393c0821 8ee9141074b48784c89aa5d3cd4010fcf4e6d467b618c8719970f78fcc24a365 a9db5aca01499f6ce404db22fb4ba3e4e0dc4b94a41c805c520bd39262df1ddc 347e2f0d8332dd2d9294d06544c051a302a2436da453b2ccfa2d7829e3a79944
	URLs	hxxps://129.153[.]135.83:2078 hxxps://132.148.79[.]222:2222 hxxps://45.154.24[.]57:2078 hxxps://45.85.235[.]39:2078 hxxps://94.199.173[.]6:2222
PowerExchange	MD5	f18575065970ef36e613ffa046f381fe9b01b3e9 2ba23d9115fb1c1d4c5899d34dc4772631d77eda 2b995ce4656db72574510801117O5d5b98b45df3 68299DF5D8CE52845A8FC10598F138840094181C d82aad3222664ec9fb112808dfabbb56de9aa770 70aaa46784a2abd8af5628cb94f876d57fe8d154 fd3750d809f6ff9cf2b49d7a63f8f3fa0a457f61
	URL	hxxps://enmckkb0t0v3[.]x[.]pipedream[.]net?n=my
	File Names	Brochure[.]zip Brochure[.]exe MicrosoftEdgeUpdateService
	File Paths	C:\Users\Public\MicrosoftEdge\autosave[.]exe C:\Users\Public\MicrosoftEdge\wsdl[.]ps1 C:\Users\Public\MicrosoftEdge\Microsoft[.]Exchange[.]WebServices[.]dll C:\Users\Public\MicrosoftEdge\config[.]conf

Attack Name	TYPE	VALUE
PowerExchange	File Paths	C:\Windows\Microsoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]Handler\v4[.]0_1[.]0[.]0[.]0__9cbc39238c01012f\System[.]Web[.]Handler[.]dll C:\Windows\Microsoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]Roles\v4[.]0_1[.]0[.]0[.]0_9cbc39238c01012f\System[.]Web[.]Roles[.]dll C:\Users\Public\System[.]Web[.]Handler[.]dll C:\Windows\temp\temp[.]ps1 C:\Users\Public\temp[.]ps1 C:\Windows\System32\System[.]Web[.]TransportClient[.]dll C:\Windows\System32\inetsrv\System[.]Web[.]TransportClient[.]dll C:\Windows\Mirosoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]TransportClient\v4[.]0_1[.]0[.]0[.]0__9cbc39238c01012f\System[.]Web[.]TransportClient[.]dll C:\Windows\Microsoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]ServiceAuthentication\ v4[.]0_1[.]0[.]0[.]0__ff08ceb7abd6adf3\System[.]Web[.]ServiceAuthentication[.]dll

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

May 29, 2023 . 7:00 AM

More at www.hivepro.com