Date of Publication
April 17, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

10 APRIL to 16 APRIL 2023

Table Of Contents

Summary

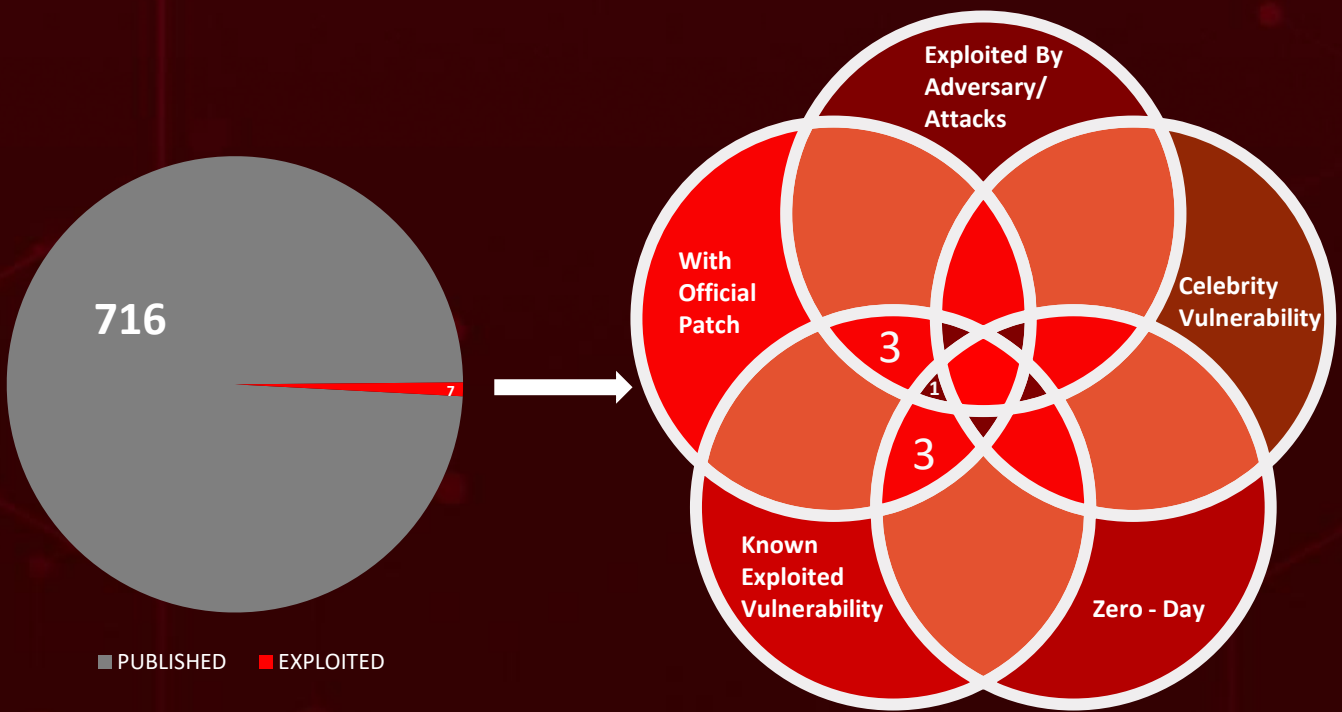
HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, they identified a total of **nine** attacks that were executed. These attacks were taking advantage of **seven** different vulnerabilities in various systems. Additionally, HiveForce Labs identified **five** different adversaries that were actively carrying out these attacks.

Interestingly, all the seven vulnerabilities are part of the known exploited vulnerability catalog by CISA.

Moreover, HiveForce Labs also found that **UNC4466** was exploiting a group of **three** old vulnerabilities to deploy **Blackcat ransomware** to carry out attacks.

Furthermore, they identified new actor called **DEV-1084** building partnership with an old actor **MERCURY** to perform destructive attacks.

Apart from these threats, there was also an increase in the ransomware attacks over the past week. These attacks included **Blackcat**, **Nokoyawa**, **Trigona** and **Cylance**. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

9
Attacks Executed

7
Vulnerabilities Exploited

5
Adversaries in Action

- BlackCat
- Cylance
- Micropsia
- Arid Gopher
- Nokoyawa
- CHM
- Trigona
- Havoc Demon
- Rilide
- CVE-2021-27876
- CVE-2021-27877
- CVE-2021-27878
- CVE-2023-28205
- CVE-2023-28206
- CVE-2023-28252
- CVE-2013-3900
- UNC4466
- Desert Falcons
- MERCURY
- DEV-1084
- Bitter APT

Insights

2 Zero-day vulnerabilities were discovered in macOS

Mercury & DEV-1084

carried out Destructive Attacks

Desert Falcon

Upgraded its arsenal

UNC4466

targeted vulnerabilities in Veritas Backup exec to deploy **BlackCat ransomware**

Nokoyawa Ransomware

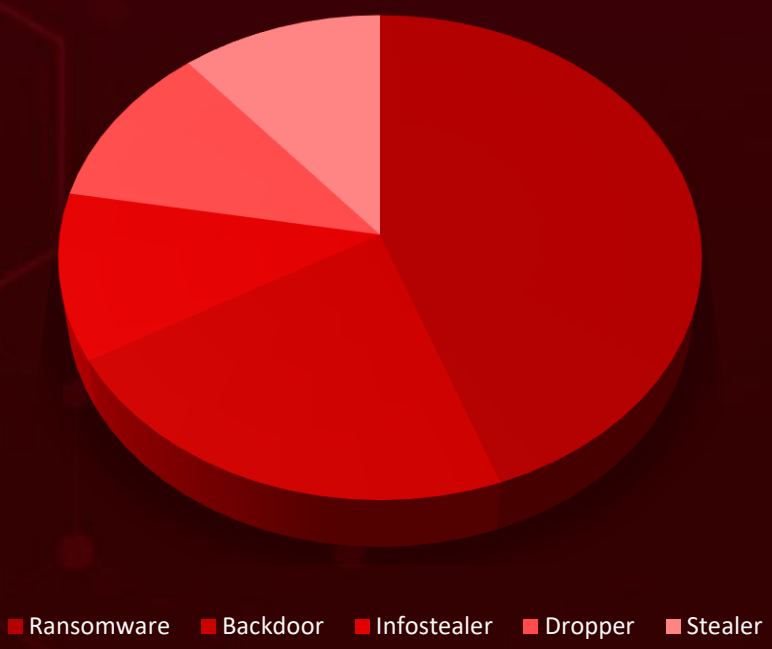
Exploited a vulnerability in Microsoft Windows

10 year old vulnerability was addressed by Microsoft in April Patch Tuesday

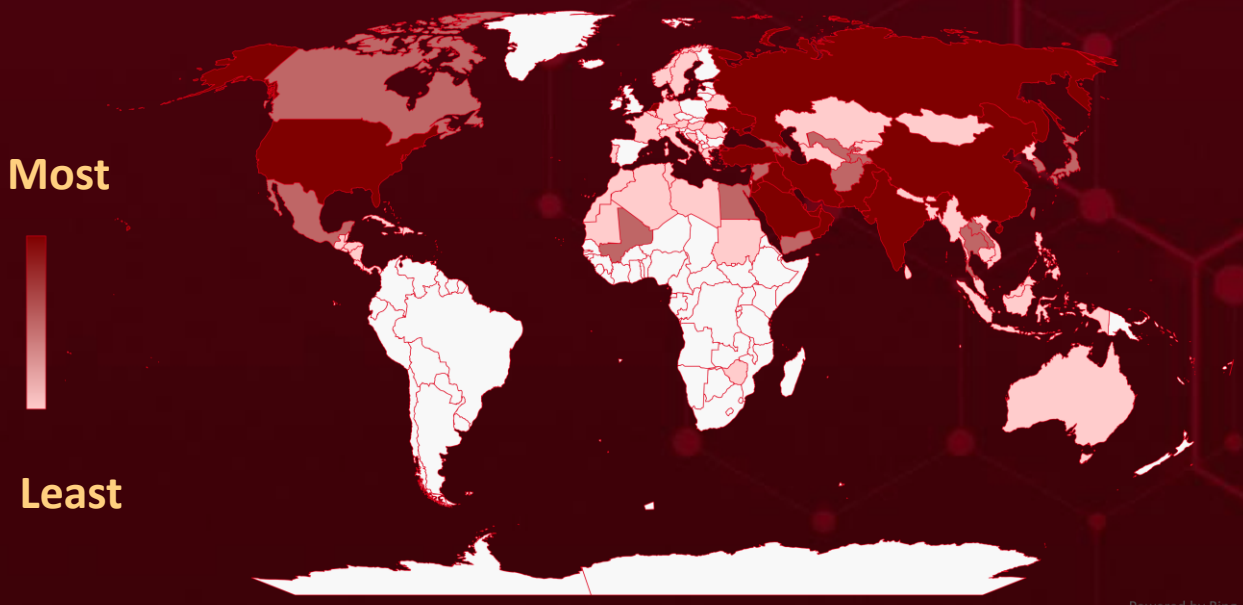
Trigona Ransomware

targets improperly managed MS-SQL Servers

Threat Distribution



Targeted Countries



Countries
Turkey
Pakistan
Netherlands
Bahrain
Russia
China
Ukraine
India
Oman
Iran
Qatar
Iraq
Saudi Arabia
Israel
UAE
Jordan
USA
Lebanon
Kuwait
Taiwan
Yemen

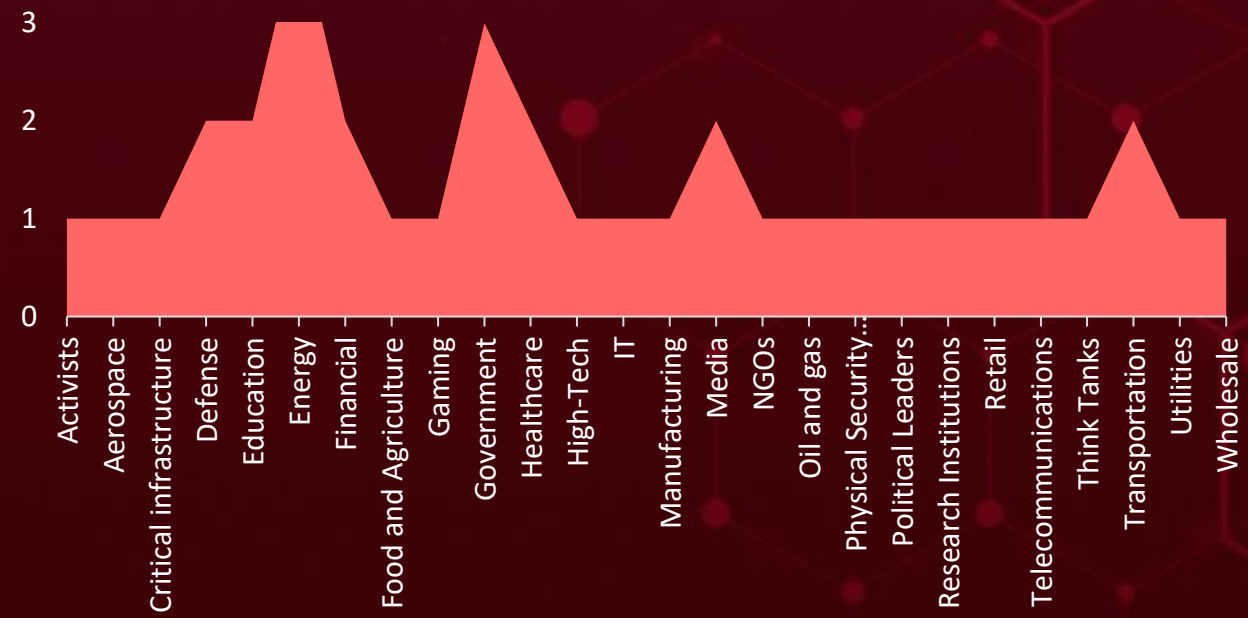
Countries
Azerbaijan
Canada
South Korea
Cyprus
Thailand
Egypt
Mali
Georgia
Palestine
Armenia
Syria
Japan
Tajikistan
Afghanistan
Uzbekistan
Laos
Mexico
Mauritania
Singapore
France
Sweden

Countries
Cuba
Greece
Saint Lucia
Algeria
Turkmenistan
Indonesia
Barbados
Antigua and Barbuda
Germany
Albania
Timor-Leste
Australia
Honduras
Italy
Philippines
Jamaica
Belarus
Denmark
Belgium
Austria
Sudan

Countries
Kazakhstan
Guatemala
Zimbabwe
Tunisia
Dominica
Bosnia and Herzegovina
Dominican Republic
Hungary
Costa Rica
Panama
Libya
Portugal
Malaysia
Romania
Maldives
Saint Kitts and Nevis
El Salvador
Saint Vincent and the Grenadines
Cambodia

Countries
Sri Lanka
Cambodia
Sweden
Morocco
Grenada
Myanmar
Haiti
Nepal
Trinidad and Tobago
Bahamas
Belize
Nicaragua
Bhutan
North Korea
Brunei
Norway
Vietnam
Akrotiri and Dhekelia
Bangladesh
Mongolia
Kyrgyzstan
Sri Lanka

Targeted Industries



TOP MITRE ATT&CK TTPS

T1486
Data Encrypted for Impact

T1059
Command and Scripting Interpreter

T1053
Scheduled Task/Job

T1027
Obfuscated Files or Information

T1082
System Information Discovery

T1574
Hijack Execution Flow

T1566
Phishing

T1057
Process Discovery

T1070
Indicator Removal

T1055
Process Injection

T1190
Exploit Public-Facing Application

T1083
File and Directory Discovery

T1543
Create or Modify System Process

T1047
Windows Management Instrumentation

T1564
Hide Artifacts

T1547
Boot or Logon Autostart Execution

T1204
User Execution

T1036
Masquerading

T1068
Exploitation for Privilege Escalation

T1210
Exploitation of Remote Services

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlackCat (aka ALPHV and Noberus) ransomware	BlackCat ransomware is known for being based on the Rust programming language and for its use of evasion techniques to avoid detection by security software.	Internet-exposed Windows server, running Veritas Backup Exec version 21.0	CVE-2021-27876 CVE-2021-27877 CVE-2021-27878
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data loss, unauthorized access, and infrastructure damage	Veritas Backup Exec
ASSOCIATED ACTOR			**PATCH LINK**
UNC4466			https://www.veritas.com/support/en_US/security/VTS21-001

IOC TYPE	VALUE
MD5	da202cc4b3679fdb47003d603a93c90d 5fe66b2835511f9d4d3703b6c639b866
URLs	45[.]61[.]138[.]109 185[.]141[.]62[.]123 5[.]199[.]169[.]209

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
Cylance	Cylance ransomware is a new malware that can adjust to customized encryption tactics and can accept different command-line parameters.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	ec8952dc14bac73174cef02a489539e244b378b7de76c771126a8ba7ce532efd D1ba6260e2c6bf82be1d6815e19a1128aa0880f162a0691f667061c8fe8f1b2c		
SHA1	933ad0a7d9db57b92144840d838f7b10356c7e51 663081e2767df7083f765a3a8a994982959d4cbe		
MD5	521666a43aeb19e91e7df9a3f9fe76ba 4601076b807ed013844ac7e8a394eb33		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Micropsia	Micropsia is a backdoor used by attackers to run secondary payloads and perform various functions, such as keylogging and data exfiltration.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Gain unauthorized access to a system or network	-
ASSOCIATED ACTOR			PATCH LINK
Desert Falcons			-
IOC TYPE	VALUE		
SHA256	0a6247759679c92e1d2d2907ce374e4d6112a79fe764a6254baff4d14ac55038 1d1a0f39f339d1ddd506a3c5a69a9bc1e411e057fe9115352482a20b63f609aa 211f04160aa40c11637782973859f44fd623cb5e9f9c83df704cc21c4e18857d		
Domains	chloe-boreman[.]com criston-cole[.]com		

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
Arid Gopher	Arid Gopher is a Go-written malware used in cyber campaigns that contain embedded components and is regularly updated and rewritten by attackers to evade detection	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Credential theft and exfiltration of stolen data	-
ASSOCIATED ACTOR			**PATCH LINK**
Desert Falcons			-
IOC TYPE	**VALUE**		
SHA256	0fb4d09a29b9ca50bc98cb1f0d23bfc21cb1ab602050ce786c86bd2bb6050311 3d649b84df687da1429c2214d6f271cc9c026eb4a248254b9bfd438f4973e529 82f734f2b1ccc44a93b8f787f5c9b4eca09efd9e8dcd90c80ab355a496208fe4		
Domains	jumpstartmail[.]com paydayloansnew[.]com		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Nokoyawa	Nokoyawa ransomware is a new threat that exploits vulnerability to infiltrate and encrypt victims' files, demanding a ransom for their release.	Through CVE-2023-28252	CVE-2023-28252
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data loss, unauthorized access, and infrastructure damage	Windows & Windows Server
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252
IOC TYPE	**VALUE**		
MD5	46168ed7dbe33ffc4179974f8bf401aa 1e4dd35b16ddc59c1ecf240c22b8a4c4 f23be19024fcc7c8f885dfa16634e6e7		
Domains	vnssinc[.]com qooqle[.]top		

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
CHM	The CHM dropper is distributed via CHM files, which have the capability to gather user data, establish persistence, and perform various malicious actions according to the attacker's command	Via Email attachments	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Bitter APT			-
IOC TYPE	**VALUE**		
SHA256	cd3effd25629ab9c440ed8bedb9bfb312c73a022cad5078684784ea07eff2c68 43c8ada7cb7c046893dd96aef195856ec94f62823ca1a2987adf31899788c92d		
SHA1	365203360046573682932 69d72dfc535f30fd8a6 19875ccc639e103e9045bbc71f4a5ce44433d1c0		
MD5	a7e8d75eae4f1cb343745d9dd394a154		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Trigona	Trigona ransomware is installed on vulnerable MS-SQL servers that are not properly managed, allowing attackers to execute malicious commands and encrypt files without distinguishing file extensions.	Improperly managed MS-SQL servers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	1cece45e368656d322b68467ad1b8c02 530967fb3b7d9427552e4ac181a37b9a 1e71a0bb69803a2ca902397e08269302 46b639d59fea86c21e5c4b05b3e29617 5db23a2c723cbceabec8d5e545302dc4		

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
Havoc Demon	Havoc Demon Backdoor malware attack targets Windows users through a spoofed document from Energoatom, a state-owned enterprise that operates Ukraine's nuclear power plants.	Via Email attachments	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Gain control over the compromised machines	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	b773fa65bb375e6fe6d387f301f6bf33219189ea1d4a06762e965a9eba7de4e8 17637fac7f989549acd248ca9e5293d2b9a1a2e4bb0f7e4edf5571df35129f0c 9f797d705facebd1687b7765cbf65231e71821eb3c38dcc171a3fc88b9f52328 b6cb8a7cdce0bfd3a7402d22fb0014dedb259d6c91c1538ac74097b8ca22ca5c		
URLs	hxxps://ukrtatnafta[.]org		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rilide	The Rilide Stealer Extension is a sophisticated malware that disguises itself as a benign Google Drive extension and targets Chromium-based browsers, carrying out various malicious activities such as injecting scripts and exfiltrating sensitive information.	By mimicking Google Drive extensions	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal data and exfiltrate URLs and screenshots.	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	d54fa225b07298ec34be872cd4ebf4ae baee9ba0b94ea1e2b2e566fc8a615554 99dc4073f2fe91f48fd16bc65e7dcbc2 2cc204564b68c5a98b1ff68d861b66c5 646b9404a29febe9f3741797b79e300c		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-27876	ZERO-DAY	Veritas Backup Exec before 21.2	UNC4466
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veritas:backup_exec:*:*:*:*:*:*:*:*	BlackCat ransomware
Veritas Backup Exec Agent File Access Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1090: Proxy; T1134: Access Token Manipulation; T1185: Browser Session Hijacking; T1505: Server Software Component	https://www.veritas.com/support/en_US/security/VTS21-001

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-27877	ZERO-DAY	Veritas Backup Exec before 21.2	UNC4466
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veritas:backup_exec:*:*:*:*:*:*:*:*	BlackCat ransomware
Veritas Backup Exec Agent Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1090: Proxy; T1134: Access Token Manipulation; T1185: Browser Session Hijacking; T1505: Server Software Component	https://www.veritas.com/support/en_US/security/VTS21-001

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-27878	✗	Veritas Backup Exec before 21.2	UNC4466
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veritas:backup_exec:*:*:*:*:*:*:*:*	BlackCat ransomware
Veritas Backup Exec Agent Command Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1090: Proxy; T1134: Access Token Manipulation; T1185: Browser Session Hijacking; T1505: Server Software Component	https://www.veritas.com/support/en_US/security/VTS21-001

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28205	✗	Apple Safari in macOS Big Sur and macOS Monterey: 16.0 - 16.4 macOS Ventura: 13.0 22A380 - 13.3 22E252	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:apple_safari:*:*:*:*:*:*:*:*, cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple WebKit Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1189: Drive-by Compromise; T1190: Exploit Public-Facing Application; T1102: Web Service; T1005: Data from Local System; T1048: Exfiltration Over Alternative Protocol	https://support.apple.com/en-us/HT213722 https://support.apple.com/en-us/HT213721

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28206	✗ ZERO-DAY	macOS Ventura: 13.0 22A380 - 13.3 22E252	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple macOS IOSurfaceAccelerator Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1189: Drive-by Compromise; T1190: Exploit Public-Facing Application; T1547: Boot or Logon Autostart Execution; T1547.006: Kernel Modules and Extensions; T1014: Rootkit	https://support.apple.com/en-us/HT213721

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28252	✗ ZERO-DAY	Windows: 10 - 11 22H2 & Windows Server: 2008 - 2022 20H2	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	Nokoyawa ransomware
Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28252

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2013-3900</td><td>  </td><td rowspan="2">Windows: Vista, XP, 7, 8, 8.1;
Windows Server: 2003 - 2012</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*;
cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td>Microsoft WinVerifyTrust function Remote Code Execution</td><td>  </td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-20
CWE-310</td><td>T1027: Obfuscated Files or Information; T1562: Impair Defenses</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC4466	Unknown	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-27876 CVE-2021-27877 CVE-2021-27878	BlackCat Ransomware	Veritas Backup Exec

TTPs

T1486: Data Encrypted for Impact; T1489: Service Stop; T1490: Inhibit System Recovery; T1529: System Shutdown/Reboot; T1047: Windows Management Instrumentation; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.006: Python; T1569: System Services; T1569.002: Service Execution; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1027.009: Embedded Payloads; T1055: Process Injection; T1070: Indicator Removal; T1070.001: Clear Windows Event Logs; T1070.004: File Deletion; T1112: Modify Registry; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1222: File and Directory Permissions Modification: T1497: Virtualization/Sandbox Evasion; T1497.001: System Checks; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1564: Hide Artifacts; T1564.010: Process Argument Spoofing; T1574: Hijack Execution Flow; T1574.011: Services Registry Permissions Weakness; T1620: Reflective Code Loading; T1622: Debugger Evasion; T1484: Domain Policy Modification; T1484.001: Group Policy Modification; T1007: System Service Discovery; T1012: Query Registry; T1016: System Network Configuration Discovery; T1033: System Owner/User Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1087: Account Discovery; T1135: Network Share Discovery; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder; T1095: Non-Application Layer Protocol; T1105: Ingress Tool Transfer; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1213: Data from Information Repositories; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 

Desert Falcons (Mantis, APT-C-23, Two-tailed Scorpion, Arid Viper, ATK 66, TAG-CT1)</td><td>Gaza</td><td rowspan="3">Government, Media, Financial, Research Institutions, Education, Activists, Political Leaders, Energy Firms, Physical Security Companies, Critical infrastructure, Defense, Transportation, Utilities, Aerospace, Think Tanks</td><td rowspan="3">Akrotiri and Dhekelia, Albania, Algeria, Australia, Bahrain, Belgium, Bosnia and Herzegovina, Canada, China, Cyprus, Denmark, Egypt, France, Germany, Greece, Hungary, India, Iran, Iraq, Israel, Italy, Japan, Jordan, Kuwait, Lebanon, Libya, Mali, Mauritania, Mexico, Morocco, Netherland, Netherlands, Norway, Oman, Pakistan, Palestine, Portugal, Qatar, Romania, Russia, Saudi Arabia, South Korea, Sudan, Sweden, Syria, Taiwan, Turkey, UAE, Ukraine, USA, Uzbekistan, Yemen, Zimbabwe</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Micropsia backdoor and Arid Gopher info-stealer</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1190: Exploit Public-Facing Application; T1566: Phishing; T1059: Command and Scripting Interpreter; T1053: Scheduled Task/Job; T1204: User Execution; T1047: Windows Management Instrumentation; T1543: Create or Modify System Process; T1574: Hijack Execution Flow; T1548: Abuse Elevation Control Mechanism; T1055: Process Injection; T1564: Hide Artifacts; T1562: Impair Defenses; T1070: Indicator Removal; T1036: Masquerading; T1212: Exploitation for Credential Access; T1056: Input Capture; T1083: File and Directory Discovery; T1046: Network Service Discovery; T1057: Process Discovery; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1001: Data Obfuscation; T1105: Ingress Tool Transfer; T1571: Non-Standard Port; T1047: Windows Management Instrumentation; T1566.002: Spearphishing Link</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 MERCURY (MuddyWater, Seedworm, TEMP.Zagros, Static Kitten, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17)	Iran	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation	Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Qatar, Pakistan, Russia, Saudi Arabia, Tajikistan, Thailand, Tunisia, Turkey, UAE, Ukraine, USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs
T1083: File and Directory Discovery; T1190: Exploit Public-Facing Application; T1505: Server Software Component; T1505.003: Web Shell; T1546: Event Triggered Execution; T1546.013: PowerShell Profile; T1518: Software Discovery; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1589: Gather Victim Identity Information; T1589.001: Credentials; T1590: Gather Victim Network Information; T1484: Domain Policy Modification; T1484.001: Group Policy Modification; T1047: Windows Management Instrumentation; T1136: Create Account; T1136.001: Local Account; T1548: Abuse Elevation Control Mechanism; T1548.004: Elevated Execution with Prompt; T1070: Indicator Removal; T1070.004: File Deletion; T1578: Modify Cloud Compute Infrastructure; T1578.003: Delete Cloud Instance; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1572: Protocol Tunneling; T1210: Exploitation of Remote Services; T1003: OS Credential Dumping; T1078: Valid Accounts; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1059: Command and Scripting Interpreter; T1046: Network Service Discovery; T1069: Permission Groups Discovery; T1018: Remote System: Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1027: Obfuscated Files or Information; T1569: System Services; T1569.002: Service Execution; T1573: Encrypted Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 DEV-1084	Unknown	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation	Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Qatar, Pakistan, Russia, Saudi Arabia, Tajikistan, Thailand, Tunisia, Turkey, UAE, Ukraine, USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs
T1083: File and Directory Discovery; T1190: Exploit Public-Facing Application; T1505: Server Software Component; T1505.003: Web Shell; T1546: Event Triggered Execution; T1546.013: PowerShell Profile; T1518: Software Discovery; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1589: Gather Victim Identity Information; T1589.001: Credentials; T1590: Gather Victim Network Information; T1484: Domain Policy Modification; T1484.001: Group Policy Modification; T1047: Windows Management Instrumentation; T1136: Create Account; T1136.001: Local Account; T1548: Abuse Elevation Control Mechanism; T1548.004: Elevated Execution with Prompt; T1070: Indicator Removal; T1070.004: File Deletion; T1578: Modify Cloud Compute Infrastructure; T1578.003: Delete Cloud Instance; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1572: Protocol Tunneling; T1210: Exploitation of Remote Services; T1003: OS Credential Dumping; T1078: Valid Accounts; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1059: Command and Scripting Interpreter; T1046: Network Service Discovery; T1069: Permission Groups Discovery; T1018: Remote System: Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1027: Obfuscated Files or Information; T1569: System Services; T1569.002: Service Execution; T1573: Encrypted Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Bitter APT(T-APT-17, APT-C-08, Orange Yali)	South Asia	Government	China
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	CHM	-
TTPs			
T1007: System Service Discovery; T1204: User Execution; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1218: System Binary Proxy Execution; T1218.007: Msiexec; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1053: Scheduled Task/Job; T1083: File and Directory Discovery			

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 **UNC4466, Desert Falcons, MERCURY, DEV-1084, Bitter APT** and malware **BlackCat, Cylance, Micropsia, Arid Gopher, Nokoyawa, CHM, Trigona , Havoc Demon and Rilide.**

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 **7 exploited vulnerability.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **UNC4466, Desert Falcons, MERCURY, DEV-1084, Bitter APT** and malware **BlackCat, Cylance, Micropsia, Arid Gopher, Nokoyawa, CHM, Trigona , Havoc Demon and Rilide** in Breach and Attack Simulation(BAS).

Threat Advisories

UNC4466 Attack Campaign Targets Veritas Backup Exec and Deploys ALPHV Ransomware

80K QNAP Devices Vulnerable to Cyberattack

Apple Addresses Zero-Day Vulnerabilities in macOS and Safari

New Cylance Ransomware Targets Linux and Windows Operating Systems

Desert Falcon Strikes with an Upgraded Arsenal

Cybercrime group exploits zero-day on Windows servers to deploy Nokoyawa ransomware

Microsoft Addresses Zero-Day and Wormable Vulnerabilities

Nation-State Actors MERCURY and Partner DEV-1084 Carry Out Destructive Attack

The Bitter Group Targets Chinese Agencies with CHM Malware via Email Attachments

Trigona Ransomware Targets Improperly Managed MS-SQL Servers

Malware Attack Targets Windows Users with Spoofed Energoatom Document

Rilide Stealer Extension Targets Chromium-Based Browsers

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
BlackCat	IPV4	45[.]61[.]138[.]109 185[.]141[.]62[.]123 5[.]199[.]169[.]209
	URL	hxxp://185[.]141[.]62[.]123:10228/update[.]exe
	MD5	da202cc4b3679fdb47003d603a93c90d 5fe66b2835511f9d4d3703b6c639b866 1f437347917f0a4ced71fb7df53b1a05 b41dc7bef82ef384bc884973f3d0e8ca c590a84b8c72cf18f35ae166f815c9df 24b0f58f014bd259b57f346fb5aed2ea e31270e4a6f215f45abad65916da9db4 4fdabe571b66ceec3448939bfb3ffcd1 68d3bf2c363144ec6874ab360fdda00a ee6e0cb1b3b7601696e9a05ce66e7f37 f66e1d717b54b95cf32154b770e10ba4 17424a22f01b7b996810ba1274f7b8e9
	IPV4:PORT	45[.]61[.]138[.]109:45815 45[.]61[.]138[.]109:43937 45[.]61[.]138[.]109:36931 5[.]199[.]169[.]209:31600 45[.]61[.]138[.]109:41703 185[.]99[.]135[.]115:39839 185[.]99[.]135[.]115:41773 45[.]61[.]138[.]109:33971 185[.]141[.]62[.]123:50810 185[.]99[.]135[.]115:49196

Attack Name	TYPE	VALUE
Cylance	SHA256	ec8952dc14bac73174cef02a489539e244b378b7de76c771126a8ba7ce532efd D1ba6260e2c6bf82be1d6815e19a1128aa0880f162a0691f667061c8fe8f1b2c
	SHA1	933ad0a7d9db57b92144840d838f7b10356c7e51 663081e2767df7083f765a3a8a994982959d4cbe
	MD5	521666a43aeb19e91e7df9a3f9fe76ba 4601076b807ed013844ac7e8a394eb33
Micropsia	SHA256	0a6247759679c92e1d2d2907ce374e4d6112a79fe764a6254baff4d14ac55038 1d1a0f39f339d1ddd506a3c5a69a9bc1e411e057fe9115352482a20b63f609aa 211f04160aa40c11637782973859f44fd623cb5e9f9c83df704cc21c4e18857d D10a2dda29dbf669a32e4198657216698f3e0e3832411e53bd59f067298a9798 c4b9ad35b92408fa85b92b110fe355b3b996782ceaafce7feca44977c037556b
	Domains	criston-cole[.]com chloe-boreman[.]com
Arid Gopher	SHA256	0fb4d09a29b9ca50bc98cb1f0d23bfc21cb1ab602050ce786c86bd2bb6050311 3d649b84df687da1429c2214d6f271cc9c026eb4a248254b9bfd438f4973e529 82f734f2b1ccc44a93b8f787f5c9b4eca09efd9e8dcd90c80ab355a496208fe4 85b083b431c6dab2dd4d6484fe0749ab4acba50842591292fdb40e14ce19d097 cb765467dd9948aa0bfff18214ddec9e993a141a5fdd8750b451fd5b37b16341 f2168eca27fbee69f0c683d07c2c5051c8f3214f8841c05d48897a1a9e2b31f8 21708cea44e38d0ef3c608b25933349d54c35e392f7c668c28f3cf253f6f9db8 5405ff84473abccc5526310903fcc4f7ad79a03af9f509b6bca61f1db8793ee4
	Domains	jumpstartmail[.]com paydayloansnew[.]com picture-world[.]info salimafia[.]net seomoi[.]net

Attack Name	TYPE	VALUE
Nokoyawa	MD5	46168ed7dbe33ffc4179974f8bf401aa 1e4dd35b16ddc59c1ecf240c22b8a4c4 f23be19024fcc7c8f885dfa16634e6e7 A2313d7fdb2f8f5e5c1962e22b504a17 8800e6f1501f69a0a04ce709e9fa251c
	Domains	vnssinc[.]com qooqle[.]top vsexec[.]com devsetgroup[.]com
CHM	Hostname	msdata[.]ddns[.]net bluelotus[.]mail-gdrive[.]com
	URLs	hXXps://coauthcn[.]com/hbz[.]php?id=%computername% hXXps://bluelotus[.]mail-gdrive[.]com/Services[.]msi hXXp://msdata[.]ddns[.]net:443
	SHA256	cd3effd25629ab9c440ed8bedb9bfb312c73a022cad5078684784ea07eff2c68 43c8ada7cb7c046893dd96aef195856ec94f62823ca1a2987adf31899788c92d
	SHA1	365203360046573682932 69d72dfc535f30fd8a619875ccc639e103e9045bbc71f4a5ce44433d1c0
	MD5	a7e8d75eae4f1cb343745d9dd394a154
Trigona	MD5	1cece45e368656d322b68467ad1b8c02 530967fb3b7d9427552e4ac181a37b9a 1e71a0bb69803a2ca902397e08269302 46b639d59fea86c21e5c4b05b3e29617 5db23a2c723cbceabec8d5e545302dc4
	Website	hxxp://3x55o3u2b7cjs54eifja5m3ottxntlubhjzt6k6htp5nrocjmsxxh7ad[.]onion/
Havoc Demon	SHA256	b773fa65bb375e6fe6d387f301f6bf33219189ea1d4a06762e965a9eba7de4e8 17637fac7f989549acd248ca9e5293d2b9a1a2e4bb0f7e4edf5571df35129f0c 9f797d705facebd1687b7765cbf65231e71821eb3c38dcc171a3fc88b9f52328 b6cb8a7cdce0bfd3a7402d22fb0014dedb259d6c91c1538ac74097b8ca22ca5c

Attack Name	TYPE	VALUE
Havoc Demon	URLs	hxxps://ukrtatnafta[.]org hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/avias.js hxxps://ukrtatnafta[.]org/wpcontent/themes/pressa/js/mobile_menu.js hxxps://ukrtatnafta[.]org/wp-content/plugins/contact-form-7/includes/js/scripts.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/bootstrap.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/hovermenu.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/retina1.1.0.js hxxps://ukrtatnafta[.]org/wpcontent/plugins/js_composer/assets/lib/bower/isotope/dist/isotope.pkgd.min.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/custom-script.js hxxps://ukrtatnafta[.]org/wp-includes/js/wp-emoji-release.min.js hxxps://ukrtatnafta[.]org/maps-api-v3/api/js/52/1/intl/uk_ALL/util.js hxxps://ukrtatnafta[.]org/wp-includes/js/wp-embed.min.js
Rilide	Domains	nvidia-graphics[.]top nch-software[.]info 45[.]15[.]156[.]210 vceilinichego[.]ru ashgrrwt[.]click
	Wallet Address	bc1qkczacyp5jq29s5kaphth4asu8cv2y4u4gdgj7q bc1qsjg8dqx6ga30h6szjd8dv2wg50ch50qrey4t7j 0xDBc1330056E2F5e2FB11FB3C96dE2c44B313eA8d 1KqequymujeNJuyB4gH7oJSFTB3En3Hf5n LRYpzmnqBVozkbzJhTWndzYDPfjmNPyaLv rUPTadzFN6LS662Z2d2AvNyqU1xwg2japJ THiD8hFLiEyULVKLp3DSbBXQSbR3MQxm4X D5asYfjtbTtFmFkrEwqVgbJKYv9YT7Tgjh
	MD5	558104b26ccadec3d3eb2925113387a6 c28a180de1f80c8c98d0904e64142bef 1baaeedd1a26edf4fa79ded370e3d19a 0a4f321c903a7fbc59566918c12aca09 561797d7e5cf956e33735180d93be5b6 766d020e902b6470d0510e5c6cfcd6e8 d9cca3dd5bdaeb0466d52821b584602b 9e5f43b2dc1606e27fa0cfdfb4e363d2 740606987f4d588c89d0a5b68648e31e 1c54dd00bc7cc52b60ad4a46e2fb3a77

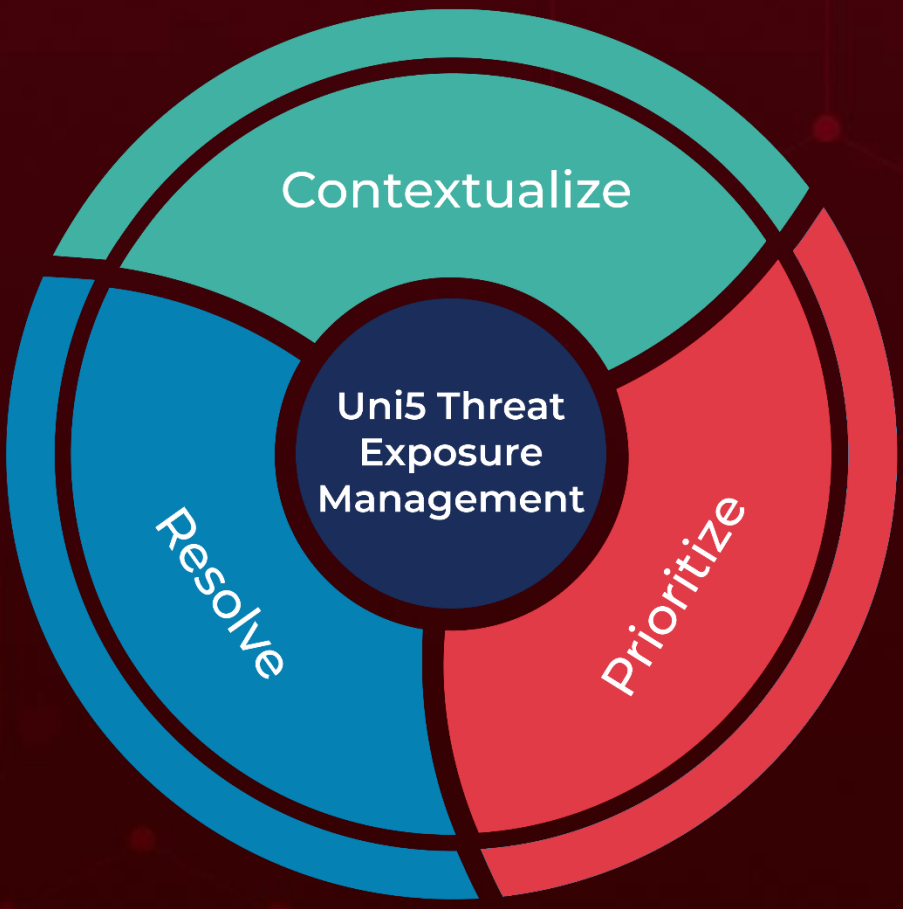
Attack Name	TYPE	VALUE
Rilide	MD5	d54fa225b07298ec34be872cd4ebf4ae baee9ba0b94ea1e2b2e566fc8a615554 99dc4073f2fe91f48fd16bc65e7dcbc2 2cc204564b68c5a98b1ff68d861b66c5 646b9404a29febe9f3741797b79e300c 253f4319673673d2bf5285558a6903df 50e363409ba77b20fb6f0bce4eff7b1 c1f40584e4ac391d97218ce137a63fb3 ebce63fdc8ef245f117f06ada3ba0f6d 4abe60d2c3506f4767e163d135f89f92 b85c5659e946b5d7ad78410356288928 ff4e2df1a46d49862ab2a0af830a007e c0e120778853f0a4865e006a07cd728a
	SHA1	add0d61399c8c47f8ac73dc83cc83dfa31cddeca 415d790b54ca8e374f37fdbb00090110b823ba18 ec6de82efa93e59da148f4d696efcfca851e051e 2449e4b27d778f6a4ffc00bb7b73926ac2c54e8a 0ead1d32ce6b15c4a90373fce58d1554035cd40f 39f546a4ec94e63e603e3c2481fecab2b5e8a475 61acdad59223a9eb0b392ccd085db1e49700d65 28ae2440c56350f65b607e4e99b67a2632db873b 05536aa80f8280ddc31be5c0ac3ca995f2190a0a f689396c73055e99a06e002c39e3a74d3d402607 84db08e3dcbe40c7cbc998a77788f7303d4a2905 0cb1d9c2a3c8b776ef1e3ec1316fbf595ced7863 eafdc35b233600ef552b87e684faa3ab3396eae9 5012e783b2ee29cb40b04a10d1a40d0bfda683d9 a46586bfe22f4d84cd9174238740af275bf50c69 ffebf78a9692293a23f9a477ea8a79f7f6ef5aa2 a39d252e7927ae1adf518e6a3dd08f37e7ee7c26 70167e7e5d71fba7d92796324b488c0fb9727712 25f3fb6d2dab206a5e9b2c0ef26ec6d6a56c5767 b4b918a5898463dad1c7d823e0b3f828bac15aad abaaa2644b1e84e8b39119988dd711572377c839 b1c100d5a99ae34ccb3654c7b7f8573376a44fd9 e049f56198c23d86e9083142bfe80042e21d4b8e
	SHA256	0e31ff6406b03982581246b7dd60f3b96edcf0bd007b31766954df001fd68f69 e623984143e0dc6e35c79869ab1521c6714e588e8e648606496f8372ca0d8416 ebd72806abd354f3162eec0991d127f993a5dde1a0c719b47087c9ee0edefeaf 0f11aeecbde1f355d26c9d406dad80cb0ae8536aea31fdddaf915d4afd434f3f

Attack Name	TYPE	VALUE
Rilide	SHA256	8342b134cddeaf34ce05bafa9e860dacf6cd01b85fd00147d90a350516c055e5 4cc83be0fa496855d244050616ee2e86b044a9bc87bc5ca70b305986c1ba3bb8 55251c725e9f6f51b8db7a631b54dd85b1b59d644c3219e03ceffb0c49cd00a4 1b01c3e554700e1282c7fdd2dcb54314516ee1f0c5eef3560cdbabc1ba776293 a28c623d120a76dcfeef9504eaeefabac9d33f292576ccf012fa458b8d7bc6ef 8989f4244667626728c6c0083422ff714cb622c92c35a53f9cb1e9891f4528ff 170a13a7a8757336babe857804fa24b6cb20aaa9593b32546d7151f23095a510 bb57a504e0b821552344cecb3da9ecdd0d61817264617a4917d6f5e64a1df7e5 d70e933e10e667ae7ef6e68a625c447be8aabe9b29affdad999c969bd8769003 c8939f8d6237fcc17d486981a800b1e7e9974377de21d7e76677babe8ed536af 2e310391d77022bcc708c354140319718777ca35efdfb76d6c80cb9de8c8091e 4bbb0584eed0c082b5c43d3f259f37cf1a0b64eabb485e85090951a6566d98d4 9dca66f52f31dca921fb238bd36bfc1b1a59d3e4af7b071da9bc4c6bf294e402 4df0f18a7e05518bbe93758e751f1f462fef212cdc786c7217d50ddbda14efb5 ef20c929f5204b223b6e53dc406ea0bcd76d9e98c9ae4942037902883d4bb22a e1ad66cc0244fc075e0aabe0fd19502d4c9617829b90aa210e74be1d915275d2 a7f0fdfdfdf1ef65799fd2114bf5c1e133a8b7635b498b334553fbb64b218a05 68278b40b59b1b0db2f814d2d864f0b9c2b4285f5795d22cabf60715f922989c 2f947644c7752ba014eae7971b247be60249a6088923c66ffe9886a7f5c5fe1c

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

April 17, 2023 . 7:00 AM

More at www.hivepro.com