Date of Publication
March 4, 2024

Hive Pro®

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

26 FEBRUARY to 3 MARCH 2024

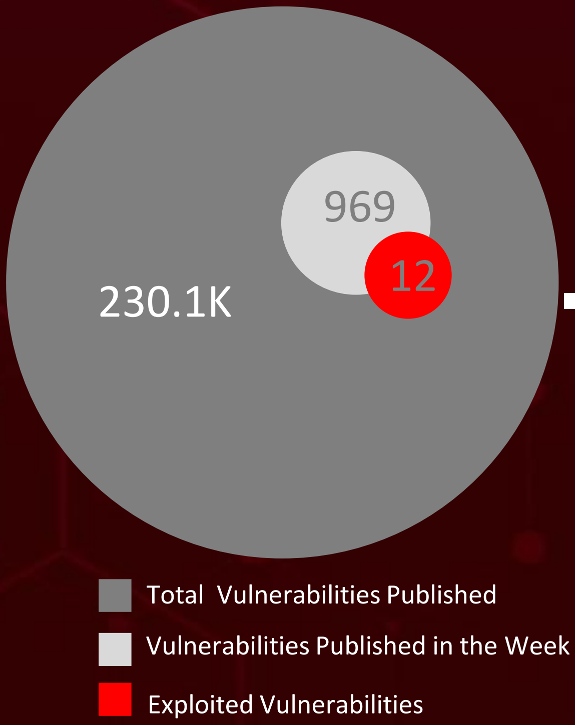
Table Of Contents

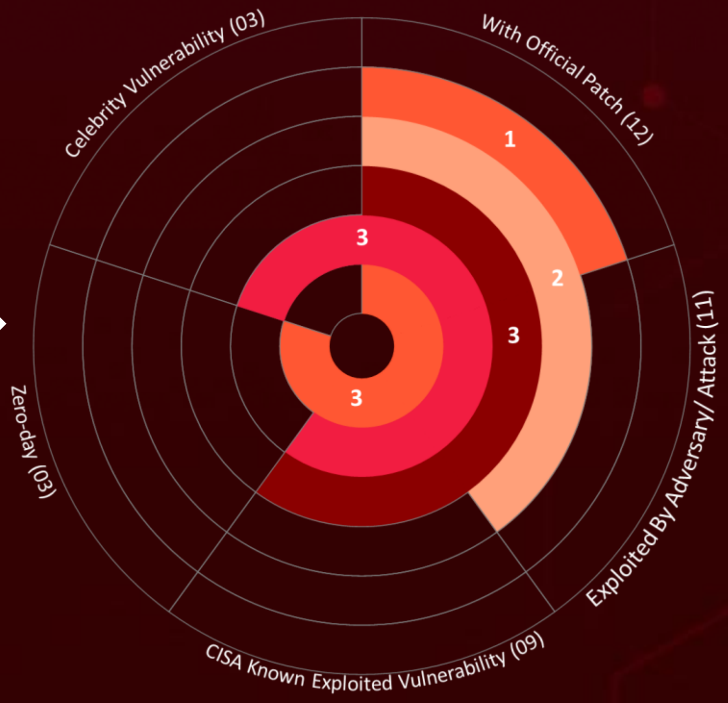
Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **eight** attacks were executed, **twelve** vulnerabilities were uncovered, and **six** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs revealed **three zero-day** vulnerabilities in Ivanti. Cyber threat actors, tagged as **UTA0178**, have been exploiting these vulnerabilities to bypass authentication and execute arbitrary commands with elevated privileges. The hacking group **UNC1549**, potentially connected to Tortoiseshell (aka Imperial Kitten), has deployed distinct backdoors known as **MiniBike** and **MiniBus**. Their primary focus lies in targeting defense-related entities in the Middle East.

Despite a recent takedown named **Operation Cronos**, by global law enforcement, **LockBit** ransomware remains a significant threat. It reemerged within four days, and its affiliates were found exploiting vulnerabilities in ScreenConnect. These attacks are on the rise, posing a significant threat to users worldwide.





High Level Statistics

8

Attacks Executed

- LockBit
- Abyss Locker
- Xeno RAT
- Blackcat
- WINELOADER
- MINIBIKE
- MINIBUS
- LIGHTRAIL

12

Vulnerabilities Exploited

- CVE-2024-23204
- CVE-2016-0099
- CVE-2019-7481
- CVE-2021-31207
- CVE-2021-34473
- CVE-2021-34523
- CVE-2024-1709
- CVE-2023-46805
- CVE-2024-21887
- CVE-2024-21893
- CVE-2024-22024
- CVE-2024-21888

6

Adversaries in Action

- LockBit Gang
- Doppelgänger
- Blackcat
- SPIKEDWINE
- UTA0178
- UNC1549

Insights

Whispers of Deceit: **Doppelgänger's** Sophisticated Tactics Targeting German Voters

Defying Defeat: **LockBit's** Rapid Revival and Affiliates' Tactical Strikes

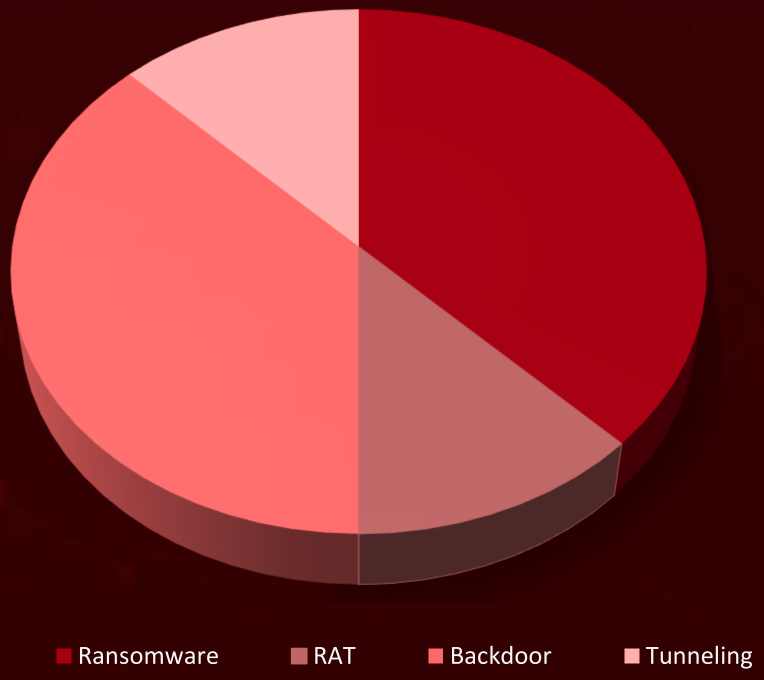
Pouring Trouble: **SPIKEDWINE's** Cyber Operation Shaking **EU-India** Relations

Triple Threat: Blackcat's Comeback with Triple Extortion Tactics Sparks Chaos in U.S Pharmacies.

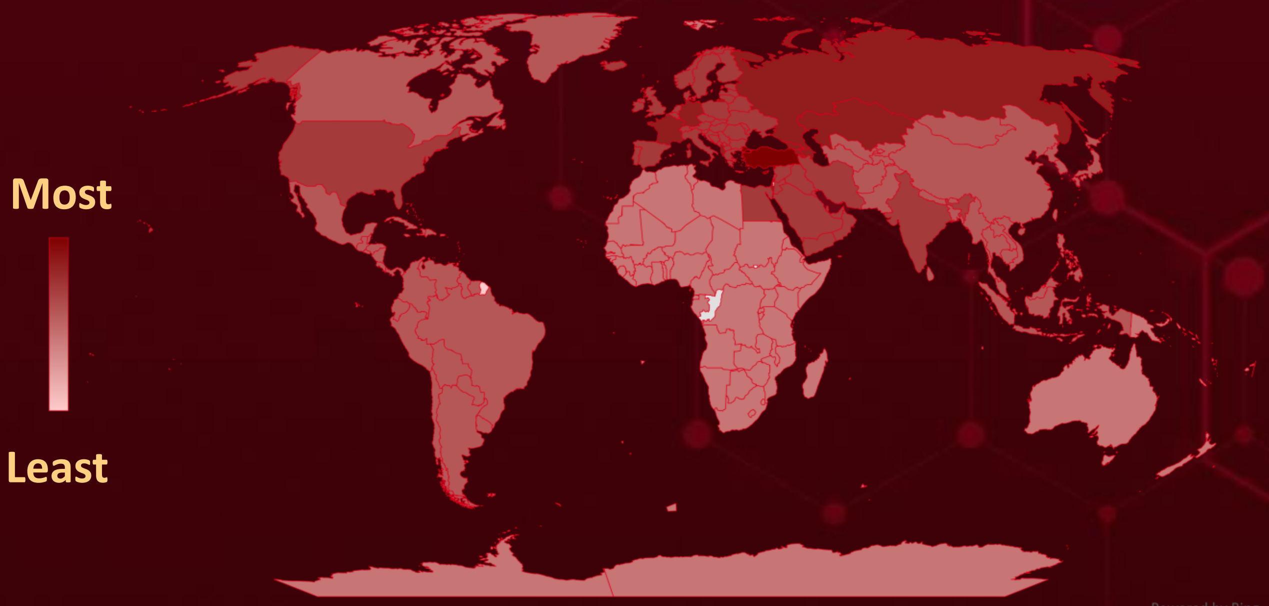
Unlocking the Origins: Abyss Locker Emerges from the Shadow of HelloKitty

Device Data at Stake: **Apple's** Shortcuts Vulnerability Raises Red Flags

Threat Distribution



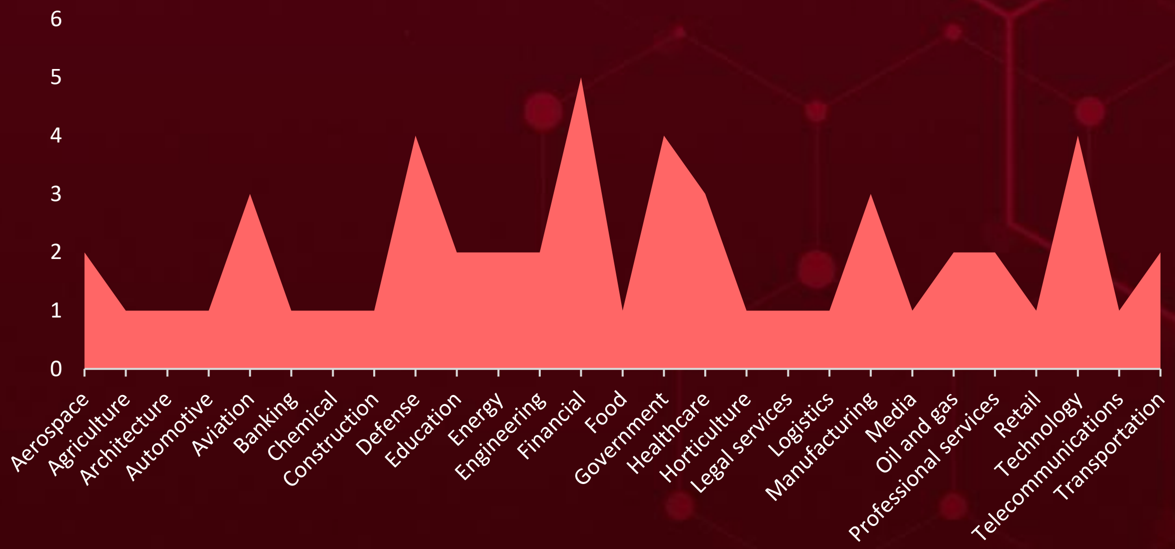
Targeted Countries



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

Countries
Turkey
Cyprus
Albania
Germany
Georgia
Azerbaijan
Israel
Russia
Armenia
France
Kazakhstan
Montenegro
Slovenia
Portugal
Austria
Luxembourg
Czech Republic
Norway
Denmark
San Marino
Egypt
Switzerland
Estonia
Moldova
Finland
North Macedonia
Andorra
Palestine
Bahrain
Romania
Belarus
Serbia
Greece
Spain
Hungary
Croatia
Iceland
Malta
India
Monaco
Iran
Netherlands
Iraq
Northern Cyprus
Ireland
Oman
Belgium
Poland
Italy
Qatar
Jordan
Bulgaria
Transnistria
Saudi Arabia
Bosnia and Herzegovina
Slovakia
United Arab Emirates
South Ossetia
United States
Sweden
Yemen
Syria
Liechtenstein
Lithuania
Ukraine
Abkhazia
United Kingdom
Kuwait
Vatican City
Latvia
Lebanon
Kosovo
Anguilla
Puerto Rico
Cambodia
East Timor
Saint Vincent and the Grenadines
Ecuador
Turks and Caicos Islands
El Salvador
Paraguay
Aruba
Saint Kitts and Nevis
Falkland Islands
South Korea
Bahamas
Cuba
Greenland
Uzbekistan
Grenada
Pakistan
Guatemala
Philippines
Guyana
China
Haiti
Saint Martin
Honduras
Sint Maarten
Hong Kong
Suriname
Afghanistan
Tajikistan
Bangladesh
Curaçao
Barbados
Argentina
Indonesia

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1562
Impair Defenses

T1027
Obfuscated Files or Information

T1041
Exfiltration Over C2 Channel

T1036
Masquerading

T1219
Remote Access Software

T1083
File and Directory Discovery

T1078
Valid Accounts

T1046
Network Service Discovery

T1204.001
Malicious Link

T1055
Process Injection

T1486
Data Encrypted for Impact

T1057
Process Discovery

T1574.002
DLL Side-Loading

T1588
Obtain Capabilities

T1071.001
Web Protocols

T1204.002
Malicious File

T1555
Credentials from Password Stores

T1001
Data Obfuscation

T1569
System Services

Attacks Executed

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>LockBit Ransomware (aka ABCD)</td><td rowspan="5">LockBit ransomware is malicious software designed to block user access to computer systems in exchange for a ransom payment. LockBit will automatically vet for valuable targets, spread the infection, and encrypt all accessible computer systems on a network.</td><td>Exploiting Vulnerabilities</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>Ransomware</td><td rowspan="3">Encrypts files, System Compromise</td><td>Windows, Linux, MacOS and VMware Exsi</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">a340d3ddacb9a9890f94c995510611099a682cf482323b6fd9922c2311c93782,
d4f150a8b26e9edccae4987433fb5b8a105970db143ba196f13652730c635668,
2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46,
6fcee00c908b40aac5a7e50007f485fc35ebfbdc2ae6a6d5e0a1f37636caca75</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>Abyss Locker ransomware (aka AbyssLocker)</td><td rowspan="5">Abyss Locker ransomware surfaced in July 2023, deriving from the HelloKitty ransomware source code. The Abyss Locker threat actor steals victims' data before deploying and running its ransomware malware for file encryption. The ransomware is also capable of deleting Volume Shadow Copies and system backups.</td><td>SSH brute force attacks</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>Ransomware</td><td rowspan="3">Encrypt files, System Compromise</td><td>Windows, Linux</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">72310e31280b7e90ebc9a32cb33674060a3587663c0334daef76c2ae2cc2a462,
3fd080ef4cc5fbf8bf0e8736af00af973d5e41c105b4cd69522a0a3c34c96b6d,
9243bdcbe30fbd430a841a623e9e1bcc894e4fdc136d46e702a94dad4b10dfdc,</td></tr>
</table>

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
Xeno RAT	Xeno-RAT is an open-source RAT developed in C#, and has been made available on GitHub. It has a SOCKS5 reverse proxy and real-time audio recording capability, as well as a Hidden Virtual Network Computing (HVNC) module.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
-			

IOC TYPE	VALUE
MD5	13b1d354ac2649b309b0d9229def8091, 6f9e84087cabbb9aaa7d8aba43a84dcf
SHA256	848020d2e8bacd35c71b78e1a81c669c9dc63c78dd3db5a97200fc87aeb44c3c, 4d0d8c2696588ff74fe7d9f8c2097fddd665308fccf16ffea23b9741a261b1c0

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
WINELOADER	New modular backdoor WINELOADER has a modular design, with encrypted modules downloaded from the C2 server. The backdoor employs techniques, including re-encryption and zeroing out memory buffers, to guard sensitive data in memory and evade memory forensics solutions.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Encrypt data	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
SPIKEDWINE			

IOC TYPE	VALUE
SHA256	72b92683052e0c813890caf7b4f8bfd331a8b2afc324dd545d46138f677178c4, ad43bbb21e2524a71bad5312a7b74af223090a8375f586d65ff239410bbd81a7, 3739b2eae11c8367b576869b68d502b97676fb68d18cc0045f661fbe354afcb9,

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="3">Blackcat Ransomware</td><td rowspan="7">BlackCat is the first prominent malware written in the Rust programming language. It is operated as a ransomware-as-a-service (RaaS). Its campaigns often employ a triple-extortion tactic: making individual ransom demands for the decryption of infected files; for not publishing stolen data; and for not launching denial of service (DoS) attacks.</td><td>Social Engineering and Remote Access Tools</td><td>CVE-2016-0099
CVE-2019-7481
CVE-2021-31207
CVE-2021-34473
CVE-2021-34523
CVE-2024-1709</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td rowspan="5">Encrypt data, System Compromise</td><td rowspan="3">Windows, Linux, and VMware ESXi, ConnectWise ScreenConnect</td></tr>
<tr><th>TYPE</th></tr>
<tr><td>Ransomware</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>Blackcat</td><td>https://learn.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-032, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0016, https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523, https://screenconnect.connectwise.com/download</td></tr>
</table>

IOC TYPE	VALUE
SHA256	1f5e4e2c78451623cfbf32cf517a92253b7abfe0243297c5ddf7dd1448e460d5, 3670dd4663adca40f168f3450fa9e7e84bc1a612d78830004020b73bd40fcd71,
IPv4	5.199.168[.]24, 91.92.254[.]193

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
MINIBIKE	MINIBIKE, a custom C++ backdoor first identified in June 2022, facilitates file exfiltration, command execution, and more, communicating through Azure cloud infrastructure.	Spear phishing and watering-hole attacks	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Espionage	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UNC1549			-
IOC TYPE	VALUE		
MD5	01cbaddd7a269521bf7b80f4a9a1982f, 054c67236a86d9ab5ec80e16b884f733, 1d8a1756b882a19d98632bc6c1f1f8cd		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MINIBUS	MINIBUS, documented in August 2023, offers a more versatile code-execution interface and enhanced reconnaissance features compared to MINIBIKE.	Spear phishing and watering-hole attacks	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Espionage	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UNC1549			-
IOC TYPE	VALUE		
MD5	ef262f571cd429d88f629789616365e4, 816af741c3d6be1397d306841d12e206, c5dc2c75459dc99a42400f6d8b455250		

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">LIGHTRAIL</td><td rowspan="6">A tunneler first seen in November 2022, likely based on an open-source Socks4a proxy, that communicates using Azure cloud infrastructure</td><td>Spear phishing and watering-hole attacks</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><th>TYPE</th><td rowspan="4">Espionage</td><td rowspan="2">-</td></tr>
<tr><td>Tunneling</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>UNC1549</td><td>-</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>MD5</td><td colspan="3">0a739dbdbcf9a5d8389511732371ecb4,
36e2d9ce19ed045a9840313439d6f18d,
aaef98be8e58be6b96566268c163b6aa</td></tr>
</table>

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-2024-23204	☒	macOS and iOS devices	-
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*	-
Apple Security features bypass Vulnerability	☒		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1588.006: Vulnerabilities, T1204: User Execution, T1083: File and Directory Discovery	https://support.apple.com/en-us/HT214061 , https://support.apple.com/en-us/HT214060 , https://support.apple.com/en-us/HT214059

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-0099	✗	Microsoft Windows	Blackcat
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	Blackcat Ransomware
Microsoft Windows Secondary Logon Service Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-264	T1068: Exploitation for Privilege Escalation	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-032

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-7481	✗	SonicWall SMA100	Blackcat
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:sonicwall:sma_100_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:sonicwall:sma_100:-:*:*:*:*:*:*:*	Blackcat Ransomware
SonicWall SMA100 SQL Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1055: Process Injection, T1190 : Exploit Public-Facing Application	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0016

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-31207	✓	Microsoft Exchange Server	Blackcat
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_:*:*:*:*:*:*	Blackcat Ransomware
PROXYSHELL (Microsoft Exchange Server Security Feature Bypass Vulnerability)	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-434	T1588.006: Vulnerabilities	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34473	✓	Microsoft Exchange Server	Blackcat
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_:*:*:*:*:*:*	Blackcat Ransomware
PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-918	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34523	✓	Microsoft Exchange Server	Blackcat
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_:*:*:*:*:*:*	Blackcat Ransomware
PROXYSHELL (Microsoft Exchange Server Privilege Escalation Vulnerability)	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-1709	✗	ScreenConnect 23.9.7 and prior	Blackcat
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*:*	Blackcat Ransomware
ConnectWise ScreenConnect Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities, T1068: Exploitation for Privilege Escalation	https://screenconnect.connectwise.com/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-46805	✗	Ivanti Connect Secure and Policy Secure	UTA0178
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:-:*:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21887	✗	Ivanti Connect Secure and Policy Secure	UTA0178
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:-:*:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21893	✗	Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA	UTA0178
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:-:*:*:*:*:*:*:*	-
Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1090: Proxy, T1135: Network Share Discovery, T1005: Data from Local System	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-22024	✗	Ivanti Connect Secure, Ivanti Policy Secure and ZTA gateways	UTA0178
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:-:*:*:*:*:*:*:*	-
Ivanti Connect Secure, Policy Secure, and ZTA XML external entity or XXE Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1059: Command and Scripting Interpreter, T1005: Data from Local System, T1046: Network Service Discovery	https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21888	⊗	Ivanti Connect Secure and Ivanti Policy Secure	UTA0178
	ZERO-DAY		
	⊗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:ivanti:connect_secure:-:*:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Privilege Escalation Vulnerability	⊗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-264	T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
LockBit Gang	Unknown	Government, Food and Agriculture, Education, Technology, Manufacturing, Aviation, Defense, Energy, Financial, Healthcare, Transportation	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	LockBit Ransomware	Windows, Linux, MacOS and VMware Exsi
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1219: Remote Access Software; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1482: Domain Trust Discovery; T1072: Software Deployment Tools; T1003: OS Credential Dumping; T1095: Non-Application Layer Protocol; T1003.001: LSASS Memory; T1555.003: Credentials from Web Browsers; T1555: Credentials from Password Stores; T1572: Protocol Tunneling; T1082: System Information Discovery; T1219: Remote Access Software; T1046: Network Service Discovery; T1021.001: Remote Desktop Protocol; T1021: Remote Services; T1219: Remote Access Software; T1071.001: Web Protocols; T1048: Exfiltration Over Alternative Protocol; T1189: Drive-by Compromise; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1566: Phishing; T1078: Valid Accounts; T1059.003: Windows Command Shell; T1059: Command and Scripting Interpreter; T1072: Software Deployment Tools; T1569.002: Service Execution; T1569: System Services; T1547: Boot or Logon Autostart Execution; T1548: Abuse Elevation Control Mechanism; T1484: Domain Policy Modification; T1484.001: Group Policy Modification; T1480.001: Environmental Keying; T1480: Execution Guardrails; T1070.004: File Deletion; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1562: Impair Defenses; T1046: Network Service Discovery; T1486: Data Encrypted for Impact; T1588: Obtain Capabilities; T1588.005: Exploits; T1588.006: Vulnerabilities			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Doppelgänger	Russia-aligned	Government, Media	Germany, the United States, Israel, and France
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
TA0003: Persistence; TA0002: Execution; TA0040: Impact; TA0005: Defense Evasion; TA0011: Command and Control; TA0043: Reconnaissance; TA0042: Resource Development; T1140: Deobfuscate/Decode Files or Information; T1593: Search Open Websites/Domains; T1491.002: External Defacement; T1491: Defacement; T1104: Multi-Stage Channels; T1583.001: Domains; T1583: Acquire Infrastructure; T1585: Establish Accounts; T1593.001: Social Media; T1059.007: JavaScript; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1585.001: Social Media Accounts			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
SPIKEDWINE	Unknown	Diplomats	Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	WINELOADER	-
TTPs			
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1204.002: Malicious File; T1656: Impersonation; T1204.001: Malicious Link; T1574.002: DLL Side-Loading; T1055.001: Dynamic-link Library Injection; T1573.001: Symmetric Cryptography; T1041: Exfiltration Over C2 Channel; T1584: Compromise Infrastructure; T1053.005: Scheduled Task; T1547.001: Registry Run Keys / Startup Folder; T1140: Deobfuscate/Decode Files or Information; T1036.001: Invalid Code Signature; T1036.004: Masquerade Task or Service; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1218.005: Mshta; T1033: System Owner/User Discovery; T1071.001: Web Protocols; T1001.001: Junk Data; T1598.002: Spearphishing Attachment			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Blackcat (aka ALPHV, ALPHVM, UNC4466)	Unknown	Healthcare, Oil and gas, Education, Petroleum, Chemical, Energy, Logistics, Finance, Manufacturing, Legal services, Technology, Transport, Engineering, Professional services, Construction and Retail	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2016-0099 CVE-2019-7481 CVE-2021-31207 CVE-2021-34473 CVE-2021-34523 CVE-2024-1709	Blackcat Ransomware	-
TTPs			
TA0003: Persistence; TA0002: Execution; TA0008: Lateral Movement; TA0004: Privilege Escalation; TA0011: Command and Control; TA0042: Resource Development; TA0005: Defense Evasion; TA0040: Impact; TA0001: Initial Access; TA0006: Credential Access; T1569: System Services; T1027: Obfuscated Files or Information; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1110: Brute Force; T1562: Impair Defenses; T1588: Obtain Capabilities; T1564: Hide Artifacts; T1486: Data Encrypted for Impact; T1210: Exploitation of Remote Services; T1078: Valid Accounts; T1505: Server Software Component; T1021: Remote Services; T1068: Exploitation for Privilege Escalation; T1040: Network Sniffing; T1041: Exfiltration Over C2 Channel; T1046: Network Service Scanning; T1047: Windows Management Instrumentation; T1106: Native API; T1119: Automated Collection; T1553: Subvert Trust Controls; T1105: Ingress Tool Transfer; T1598: Phishing for Information; T1555: Credentials from Password Stores; T1558: Steal or Forge Kerberos Tickets; T1557: Adversary-in-the-Middle; T1562.001: Disable or Modify Tools; T1562.009: Safe Mode Boot; T1489: Service Stop; T1057: Process Discovery; T1649: Steal or Forge Authentication Certificates; T1588.003: Code Signing Certificates; T1529: System Shutdown/Reboot; T1566: Phishing			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
UTA0178	-	Government, Military, Telecommunications, Defense, Technology, Banking, Finance, Accounting, Aerospace, Aviation, Engineering	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-46805 CVE-2024-21887 CVE-2024-21893 CVE-2024-22024 CVE-2024-21888	-	Ivanti Connect Secure and Ivanti Policy Secure
TTPs			
TA0008: Lateral Movement; TA0003: Persistence; TA0006: Credential Access; TA0002: Execution; TA0001: Initial Access; TA0042: Resource Development; TA0004: Privilege Escalation; T1505: Server Software Component; T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution; T1068: Exploitation for Privilege Escalation; T1059.001: PowerShell; T1588: Obtain Capabilities; T1588.005: Exploits; T1588.006: Vulnerabilities; T1190: Exploit Public-Facing Application; T1078: Valid Accounts; T1505.003: Web Shell			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
UNC1549	Affiliated to Iran	Aerospace, Aviation, and Defense	Akrotiri and Dhekelia, Albania, Bahrain, Cyprus, Egypt, India, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	MINIBIKE, MINIBUS, LIGHTRAIL	-

TTPs
TA0043: Reconnaissance; TA0042: Resource: Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and: Control; TA0040: Impact; T1055: Process Injection; T1204.002: Malicious File; T1562: Impair Defenses; T1059: Command and: Scripting Interpreter; T1057: Process Discovery; T1083: File and Directory: Discovery; T1027: Obfuscated Files or: Information; T1598.002: Spearphishing: Attachment; T1070: Indicator Removal; T1574.002: DLL Side-Loading; T1041: Exfiltration Over C2: Channel; T1036: Masquerading; T1001: Data Obfuscation; T1027.010: Command: Obfuscation; T1555.003: Credentials from Web: Browsers; T1578: Modify Cloud: Compute: Infrastructure

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **twelve exploited vulnerabilities** and block the indicators related to the threat actors **LockBit Gang, Doppelgänger, Blackcat, SPIKEDWINE, UTA0178, UNC1549,** and malware **LockBit, Abyss Locker, Xeno RAT, Blackcat, WINELOADER, MINIBIKE, MINIBUS, LIGHTRAIL**.

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 **twelve exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Blackcat,** and malware **LockBit, Abyss Locker, Xeno RAT, Blackcat, WINELOADER, Minibike, Minibus, LIGHTRAIL** in Breach and Attack Simulation(BAS).

Threat Advisories

Apple Shortcuts’ Secret Threat to Your Data

LockBit’s Resurgence After Operation Cronos

Abyss Locker’s Substantial Threat Explored

Unmasking Doppelgänger: Russia’s Disinformation Campaign Revealed

Xeno RAT Open-Source Trojan Sparks Alarm

BlackCat’s Resurgence Despite Law Enforcement Disruptions

SPIKEDWINE Ploy to Infiltrate EU Diplomatic Circles

Ivanti Gateways Under Attack by Cybercriminals Patch Now

Iranian hackers soar into the defense sectors of the Middle East

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. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
LockBit	SHA256	a340d3ddacb9a9890f94c995510611099a682cf482323b6fd9922c2311c93782, d4f150a8b26e9edccae4987433fb5b8a105970db143ba196f13652730c635668, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 6fcee00c908b40aac5a7e50007f485fc35ebfbdc2ae6a6d5e0a1f37636caca75, e32dc551a721b43da44a068f38928d3e363435ce0e4d2e0479c0dfdb27563c82, 73406e0e7882addf0f810d3bc0e386fd5fd2dd441c895095f4125bb236ae7345, f0db0d23b83b54d8a565f8e9bd66b4ae7be8b2f8efffc471b6e5ef95298376e8, b65b65c3ccf923af7be7db31b3919120e47849cc3e870afdac1bc555fc25b200, b14a55a5dbc52dc58ee5447ced1caaac304e77aca7b5805a25456e2c2338309f, e51155ce803bd9b96b91c822e41969c89e0c9e162aebc7643c23ed9489eb75b4, 4cd8104440fb28afb5cadcfbdc529f57f62db479b679117c0c461fdae5796997, 954d1ef6afce8843a96769f710d52f407777a6c294ecb3539da592f3f72a560c, b8c53972ca8e7c683183a34b5a4e17f04d9bca80d8d2e156e99fb8973d41f6b9,

Attack Name	TYPE	VALUE
LockBit	SHA256	b2c3beda4b000a3d9af0a457d6d942ec81696f3ed485f7cf723b18008a5f3d10, 9b5f1ec1ca04344582d1eca400b4a21dfff89bc650aba4715edd7efb089d8141, 8b6946cca11e9507df8234e0c68567f19a893c3f08b1d384b88808846d67d7eb, 0447c931bb8efc6dc531f69a891f2a0f28a85a18b25e04366fdb59bf827b2eb1, c431cd8702361f700751745a64802a177c8db6bf58d5a428948cdc7bd0def7e7, 110372c328433649abf49f1079ea0c6610770cf9b22e7f9dfd55144dffa21aa4, 2da975fee507060baa1042fb45e8467579abf3f348f1fd37b86bb742db63438a, a50d9954c0a50e5804065a8165b18571048160200249766bfa2f75d03c8cb6d0, 707bb3b958fbf4728d8a39b043e8df083e0fce1178dac60c0d984604ec23c881, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, 32cf89ca7cccc410ca4ad9bc58e22fe8920131687ef2a0d9f61d215c9d50d661, fc073ee5e385a148e0f4d0fd9c1af696d16bd6c8d3507a98d409c2eda858ce23, f01909eee3dec5474a5a845deea3f8fb5502ac006f65060a7e945f91c966e266, 655f0d2974bf6da082463a2e1c5cf9ae87dcc873058e5e33cb47ca9490e158c2, 77a41f2ea91e559f5f1b0a24e0eedf28c4c74a1983641cff434be417f7ac20f7, 492ac25608dda01b3f776b46a7631bb8cd91a0ce0168931ec5bb9a846e702e39, 91c614d4868abe9c71d77aa77e881851dec34524afff8cad20bdb2087e58433d, 853ed24a495d866d64a922922e5d5329ed165fe102cef00007095ee92ba3746d, 2fcad226b17131da4274e1b9f8f31359bdd325c9568665f08fd1f6c5d06a23ce, 74c8269a9ec642c0fd432fc9e0d7506a079b6d32c2c3e5313d96205726629233, 6dd44d852226fd9e7fc914c6edbaf185bfcaacdc7a4dcdb7268440e6fc811618, 71895d170c7578dc8d5dba7e3136e514d8c42f502e5dc88aff532f11dac01f32, ea0094eec469916f81aa039d87700c88c89f7e10b9c90243127de1c7ad2cfbc0, 63b9637406042b4a9ab162e581c935e7f2c20b64ca504c4ae4e947aa43565b52

Attack Name	TYPE	VALUE
Abyss Locker	SHA256	72310e31280b7e90ebc9a32cb33674060a3587663c0334daef76c2ae2cc2a462, 3fd080ef4cc5fbf8bf0e8736af00af973d5e41c105b4cd69522a0a3c34c96b6d, 9243bdcbe30fbd430a841a623e9e1bcc894e4fdc136d46e702a94dad4b10dfdc, 0763e887924f6c7afad58e7675ecfe34ab615f4bd8f569759b1c33f0b6d08c64, dee2af08e1f5bb89e7bad79fae5c39c71ff089083d65da1c03c7a4c051fabae0, e6537d30d66727c5a306dc291f02ceb9d2b48bffe89dd5eff7aa2d22e28b6d7c, 1d04d9a8eeed0e1371afed06dcc7300c7b8ca341fe2d4d777191a26dabac3596, 1a31b8e23ccc7933c442d88523210c89cebd2c199d9ebb88b3d16eacbefe4120, 25ce2fec4cd164a93dee5d00ab547ebe47a4b713cced567ab9aca4a7080afcb7, b524773160f3cb3bfb96e7704ef31a986a179395d40a578edce8257862cafe5f, 362a16c5e86f13700bdf2d58f6c0ab26e289b6a5c10ad2769f3412ec0b2da711, e5417c7a24aa6f952170e9dfcfdf044c2a7259a03a7683c3ddb72512ad0cd5c7, 056220ff4204783d8cc8e596b3fc463a2e6b130db08ec923f17c9a78aa2032da, 877c8a1c391e21727b2cdb2f87c7b0b37fb7be1d8dd2d941f5c20b30eb65ee97, 2e42b9ded573e97c095e45dad0bdd2a2d6a0a99e4f7242695054217e2bba6829
Xeno RAT	MD5	13b1d354ac2649b309b0d9229def8091, 6f9e84087cabbb9aaa7d8aba43a84dcf, 7704241dd8770b11b50b1448647197a5, 0aa5930aa736636fd95907328d47ea45
	SHA256	848020d2e8bacd35c71b78e1a81c669c9dc63c78dd3db5a97200fc87aeb44c3c, 4d0d8c2696588ff74fe7d9f8c2097fddd665308fccf16ffea23b9741a261b1c0, 1762536a663879d5fb8a94c1d145331e1d001fb27f787d79691f9f8208fc68f2, 96b091ce5d06afd11ee5ad911566645dbe32bfe1da2269a3d3ef8d3fa0014689
Blackcat	SHA256	1f5e4e2c78451623cfbf32cf517a92253b7abfe0243297c5ddf7dd1448e460d5, 3670dd4663adca40f168f3450fa9e7e84bc1a612d78830004020b73bd40fcd71, af28b78c64a9effe3de0e5ccc778527428953837948d913d64dbd0fa45942021,

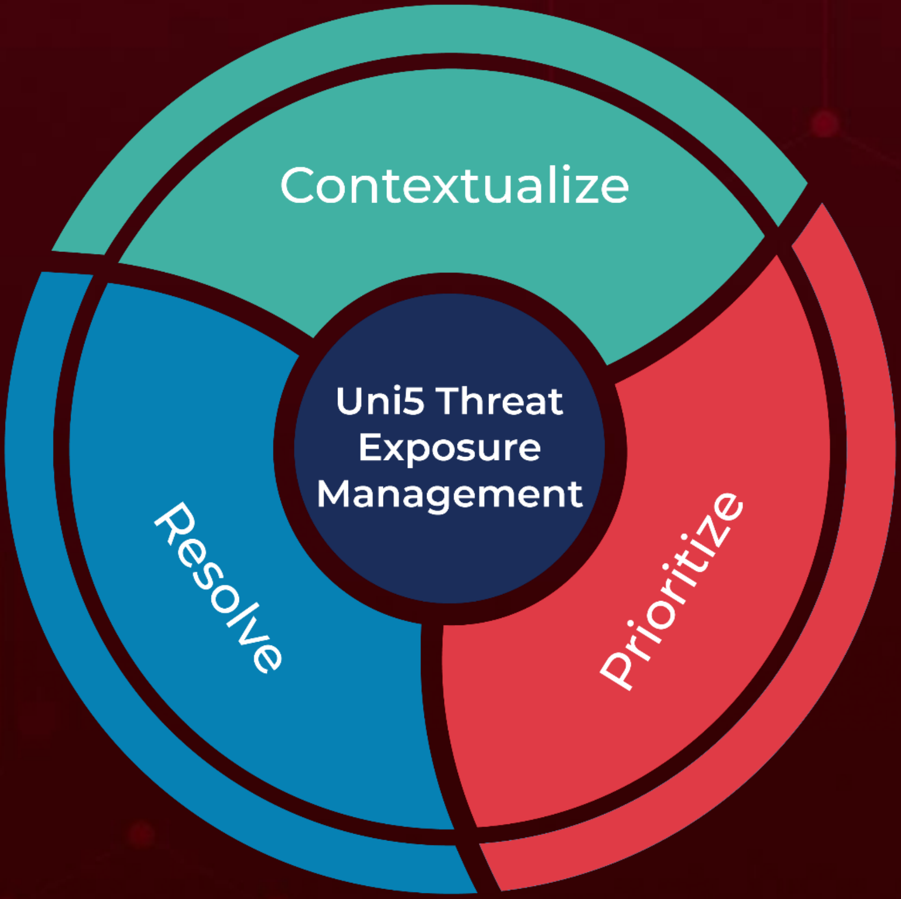
Attack Name	TYPE	VALUE
Blackcat	SHA256	bbfe7289de6ab1f374d0bcbeecf31cad2333b0928ea883ca13b9e733b58e27b1, 5d1df950b238825a36fa6204d1a2935a5fbcfe2a5991a7fc69c74f476df67905, bd9edc3bf3d45e3cdf5236e8f8cd57a95ca3b41f61e4cd5c6c0404a83519058e, 732e24cb5d7ab558effc6dc88854f756016352c923ff5155dcb2eece35c19bc0
	SHA1	3dd0f674526f30729bced4271e6b7eb0bb890c52, d6d442e8b3b0aef856ac86391e4a57bcb93c19ad, 6b52543e4097f7c39cc913d55c0044fcf673f6fc, 004ba0454feb2c4033ff0bdb2ff67388af0c41b6, 430bd437162d4c60227288fa6a82cde8a5f87100, 1376ac8b5a126bb163423948bd1c7f861b4bfe32, 380f941f8047904607210add4c6da2da8f8cd398
	IPv4	5.199.168[.]24, 91.92.254[.]193
	Domains	resources.docusong[.]com, Fisa99.screenconnect[.]com
WINELOADER	SHA256	72b92683052e0c813890caf7b4f8bfd331a8b2afc324dd545d46138f677178c4, ad43bbb21e2524a71bad5312a7b74af223090a8375f586d65ff239410bbd81a7, 3739b2eae11c8367b576869b68d502b97676fb68d18cc0045f661fbe354afcb9, 1c7593078f69f642b3442dc558cddff4347334ed7c96cd096367afd08dca67bc, e477f52a5f67830d81cf417434991fe088bfec21984514a5ee22c1bcffe1f2bc, f61cee951b7024fca048175ca0606bfd550437f5ba2824c50d10bef8fb54ca45, c1223aa67a72e6c4a9a61bf3733b68bfbe08add41b73ad133a7c640ba265a19e, b014cdff3ac877bdd329ca0c02bdd604817e7af36ad82f912132c50355af0920, 7600d4bb4e159b38408cb4f3a4fa19a5526eec0051c8c508ef1045f75b0f6083
	URLs	hxxps://castechtools[.]com/api.php, hxxps://seeceafcleaners[.]co[.]uk/cert.php, hxxps://seeceafcleaners[.]co[.]uk/wine.php, hxxps://passatempobasico[.]com[.]br/wine.php
MINIBIKE	MD5	01cbaddd7a269521bf7b80f4a9a1982f, 054c67236a86d9ab5ec80e16b884f733, 1d8a1756b882a19d98632bc6c1f1f8cd, 2c4cdc0e78ef57b44f11f7ec2f6164cd, 3b658afa91ce3327dbfa1cf665529a6d, 409c2ac789015e76f9886f1203a73bc0,

Attack Name	TYPE	VALUE
MINIBIKE	MD5	601eb396c339a69e7d8c2a3de3b0296d, 664cfda4ada6f8b7bb25a5f50cccf984, 68f6810f248d032bbb65b391cdb1d5e0, 691d0143c0642ff783909f983ccb8ffd, 710d1a8b2fc17c381a7f20da5d2d70fc, 75d2c686d410ec1f880a6fd7a9800055, 909a235ac0349041b38d84e9aab3f3a1, a5e64f196175c5f068e1352aa04bc5fa, adef679c6aa6860aa89b775dceb6958b, bfd024e64867e6ca44738dd03d4f87b5, c12ff86d32bd10c6c764b71728a51bce, cf32d73c501d5924b3c98383f53fda51, d94ffe668751935b19eaeb93fed1cdbe, e3dc8810da71812b860fc59aeadcc350, e9ed595b24a7eeb34ac52f57eeec6e2b, eadbaabe3b8133426bcf09f7102088d4
MINIBUS	MD5	ef262f571cd429d88f629789616365e4, 816af741c3d6be1397d306841d12e206, c5dc2c75459dc99a42400f6d8b455250, 05fcace605b525f1bece1813bb18a56c, 4ed5d74a746461d3faa9f96995a1eec8, f58e0dfb8f915fa5ce1b7ca50c46b51b
LIGHTRAIL	MD5	0a739dbdbcf9a5d8389511732371ecb4, 36e2d9ce19ed045a9840313439d6f18d, aaef98be8e58be6b96566268c163b6aa, c3830b1381d95aa6f97a58fd8ff3524e, c51bc86beb9e16d1c905160e96d9fa29, a5fdf55c1c50be471946de937f1e46dd

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

March 4, 2024 • 9:00 PM

More at www.hivepro.com