Date of Publication
June 19, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

12 to 18 JUNE 2023

Table Of Contents

Summary

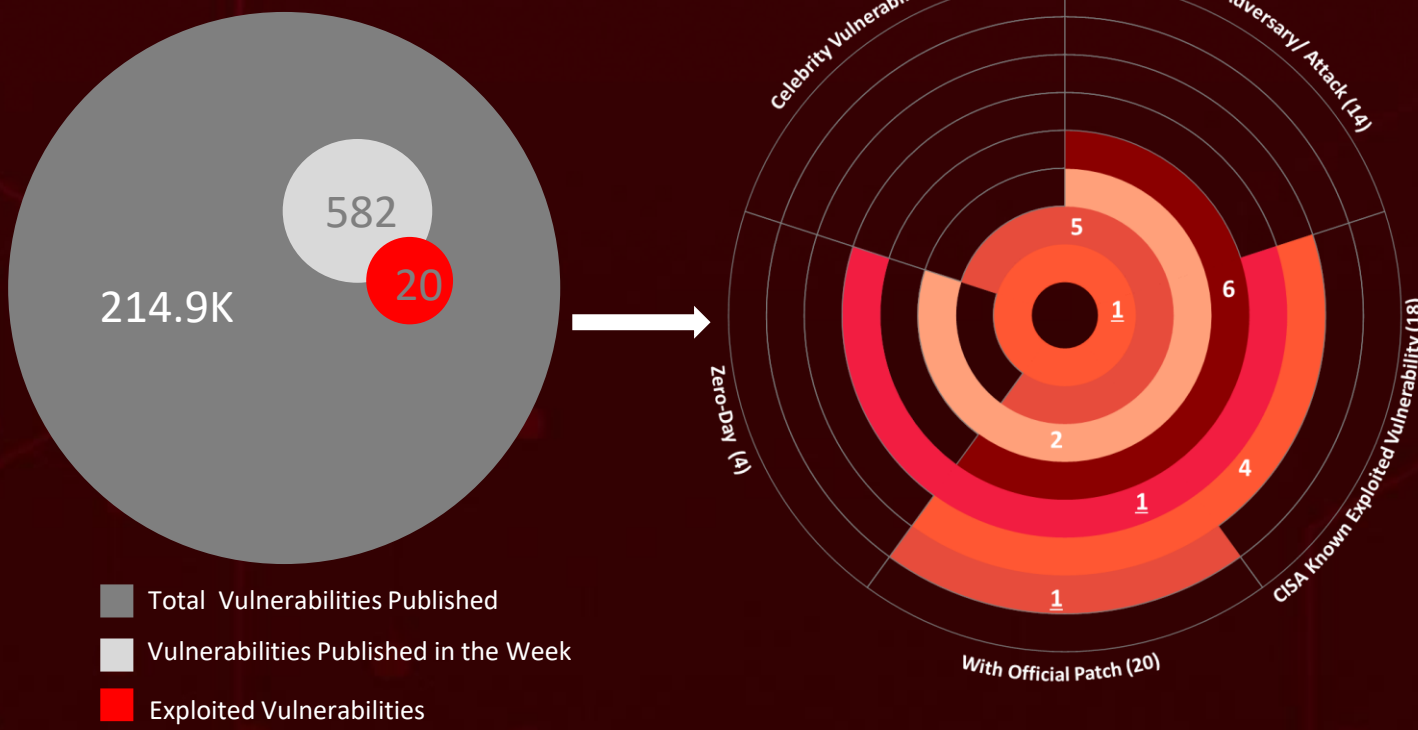
HiveForceLabs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of **seven** attacks executed, taking advantage of **twenty** different vulnerabilities in various systems, and involving **three** different adversaries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

Interestingly, **eighteen** vulnerabilities are part of the known exploited vulnerability catalog by CISA, with **four** being zero-day vulnerabilities and **six** classified as celebrity vulnerabilities.

Moreover, HiveForceLabs also discovered that Cadet Blizzard exploited **six** vulnerabilities, while **ChamelGang** exploited **four**.

Furthermore, we identified **LockBit Ransomware** exploiting **seven** vulnerabilities and **WhisperGate** wiper exploiting **six** vulnerabilities.

Meanwhile, the Chinese-sponsored hacking group **UNC3886** has been actively exploiting the **CVE-2023-20867** vulnerability and employing advanced backdoors such as VirtualPita and VirtualPie to carry out malicious activities across organizations in the US and APJ regions. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

7
Attacks Executed

20
Vulnerabilities Exploited

3
Adversaries in Action

- DoubleFinger loader
- GreetingGhoul stealer
- VirtualPita backdoor
- VirtualPie backdoor
- LockBit Ransomware
- WhisperGate
- ChamelDoH

- CVE-2023-27997
- CVE-2023-28299
- CVE-2023-20867
- CVE-2023-0669
- CVE-2023-27350
- CVE-2021-44228
- CVE-2021-22986
- CVE-2019-0708
- CVE-2018-13379
- CVE-2021-26084
- CVE-2020-1472
- CVE-2021-4034
- CVE-2021-34523
- CVE-2017-12149
- CVE-2021-34473
- CVE-2021-31207
- CVE-2019-18935
- CVE-2017-9248
- CVE-2017-11357
- CVE-2017-11317

- UNC3886
- Cadet Blizzard
- ChamelGang

Insights

Total of **Six** Vulnerabilities Exploited by Cadet Blizzard Actor

$91 Million The US alone has paid the ransom, highlighting the impact of LockBit Ransomware, a global Ransomware-as-a-Service (RaaS) threat targeting critical sectors

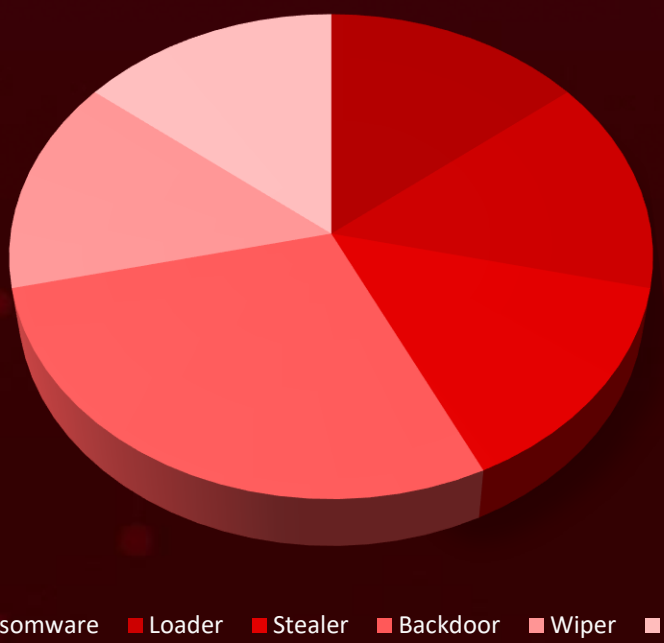
ChamelGang's Latest Creation: ChamelDoH Linux Malware Employs Encrypted Communication

250,000 Internet-Accessible Fortigate Firewalls Vulnerable to Exploitation Due to a Specific Bug

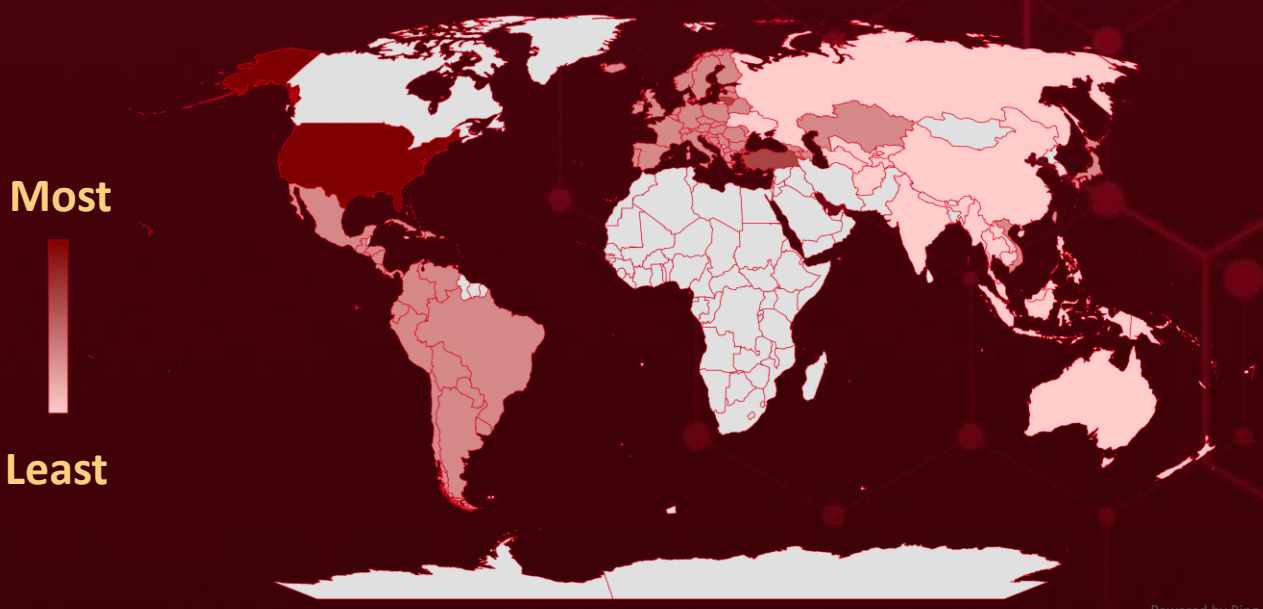
7 Flaws: LockBit Ransomware Exploits a Mix of Old and New Vulnerabilities

Trio Under Siege United States, Lithuania, and Turkey Face Intense Targeting in Recent Cyber Attacks

Threat Distribution



Targeted Countries



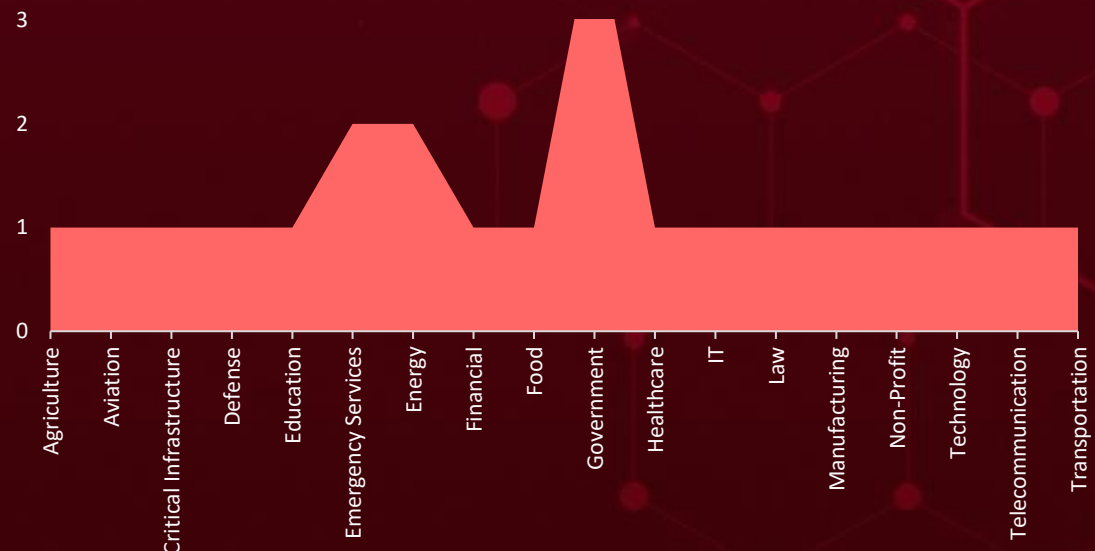
Countries
United States
Lithuania
Turkey
Italy
Paraguay
Moldova
Armenia
Slovakia
Austria
Andorra
Azerbaijan
Nicaragua
Belarus
Puerto Rico
Belgium
Argentina
Bolivia
Kazakhstan
Bosnia and Herzegovina
Malta
Brazil
Montenegro
Bulgaria
Norway
Chile
Poland

Countries
Colombia
San Marino
Costa Rica
Spain
Switzerland
Uruguay
Croatia
Venezuela
Cuba
Japan
Cyprus
Latvia
Czechia
Luxembourg
Denmark
Mexico
Dominican Republic
Monaco
Ecuador
Netherlands
El Salvador
North Macedonia
Estonia
Panama
Finland
Peru

Countries
France
Portugal
Georgia
Romania
Germany
Serbia
Greece
Slovenia
Guatemala
Sweden
Haiti
Taiwan
Honduras
Albania
United Kingdom
Hungary
Vatican City
Iceland
Vietnam
Ireland
Liechtenstein
Papua New Guinea
Cambodia
China
Russia
Thailand

Countries
Myanmar
Ukraine
Nepal
Uzbekistan
Singapore
Kyrgyzstan
Laos
Timor-Leste
New Zealand
Turkmenistan
South Korea
Malaysia
Fiji
Philippines
Afghanistan
Australia
India
Brunei
Indonesia
Tajikistan

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059
Command and Scripting Interpreter

T1105
Ingress Tool Transfer

T1055
Process Injection

T1082
System Information Discovery

T1071
Application Layer Protocol

T1027
Obfuscated Files or Information

T1036
Masquerading

T1095
Non-Application Layer Protocol

T1566
Phishing

T1562
Impair Defenses

T1070.004
File Deletion

T1572
Protocol Tunneling

T1562.001
Disable or Modify Tools

T1190
Exploit Public-Facing Application

T1566.001
Spearphishing Attachment

T1203
Exploitation for Client Execution

T1560
Archive Collected Data

T1005
Data from Local System

T1573
Encrypted Channel

T1543
Create or Modify System Process

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DoubleFinger loader	An advanced campaign utilizes a multi-stage DoubleFinger loader to deploy GreetingGhoul malware, specially crafted for pilfering cryptocurrency credentials.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	a500d9518bfe0b0d1c7f77343cac68d8 dbd0cf87c085150eb0e4a40539390a9a 56acd988653c0e7c4a5f1302e6c3b1c0 16203abd150a709c0629a366393994ea d9130cb36f23edf90848ffd73bd4e0e0		
Domain	cryptohedgefund[.]us		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GreetingGhoul stealer	GreetingGhoul is a stealer designed to steal cryptocurrency-related credentials. It essentially consists of two major components that work together	DoubleFinger loader	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	642f192372a4bd4fb3bfa5bae4f8644c a9a5f529bf530d0425e6f04cbe508f1e		
Domain	cryptohedgefund[.]us		

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
VirtualPita backdoor	VIRTUALPITA is a 64-bit passive backdoor that creates a listener on a hardcoded port number on a VMware ESXi server. The backdoor often utilizes VMware service names and ports to masquerade as a legitimate service.	Utilizing a zero-day vulnerability (CVE-2023-20867)	CVE-2023-20867
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft and Financial Loss	VMware Tools: 10.0.0 - 12.2.0
ASSOCIATED ACTOR			**PATCH LINK**
UNC3886			https://www.vmware.com/security/advisories/VMSA-2023-0013.html

IOC TYPE	VALUE
MD5	8e80b40b1298f022c7f3a96599806c43
SHA1	e9cbac1f64587ce1dc5b92cde9637affb3b58577
SHA256	4a6f559426493abc0d056665f23457e2779abd3482434623e1f61f4cd5b41843

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
VirtualPie backdoor	VIRTUALPIE is a lightweight backdoor written in Python that spawns a daemonized IPv6 listener on a hardcoded port on a VMware ESXi server. It supports arbitrary command line execution, file transfer capabilities, and reverse shell capabilities.	Utilizing a zero-day vulnerability (CVE-2023-20867)	CVE-2023-20867
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft, and Financial Loss	VMware Tools: 10.0.0 - 12.2.0
ASSOCIATED ACTOR			**PATCH LINK**
UNC3886			https://www.vmware.com/security/advisories/VMSA-2023-0013.html

IOC TYPE	VALUE
MD5	61ab3f6401d60ec36cd3ac980a8deb75
SHA1	93d5c4ebec2aa45dcbd6ddbaad5d80614af82f84
SHA256	4cf3e0b60e880e6a6ba9f45187ac5454813ae8c2031966d8b264ae0d1e15e70d

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
LockBit Ransomware	LockBit ransomware has been one of the most widespread and active variants in the world, with affiliates targeting organizations across various critical infrastructure sectors. LockBit has undergone several evolutions, introducing new versions with expanded capabilities and incorporating source code from other ransomware variants.	Phishing	CVE-2023-0669 CVE-2023-27350 CVE-2021-44228 CVE-2021-22986 CVE-2020-1472 CVE-2019-0708 CVE-2018-13379
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Espionage, Information Theft, and Financial Loss	Fortra GoAnywhere MFT,PaperCut MF/NG,Apache Log4j2,F5 BIG-IP and BIG-IQ Centralized Management, Microsoft Netlogon, Microsoft Remote Desktop Services, and Fortinet FortiOS
ASSOCIATED ACTOR			**PATCH LINK**
-			https://github.com/rapid7/metasploitframework/pull/17607 https://www.papercut.com/kb/Main/PO-1216-and-PO-1219 https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/ https://support.f5.com/csp/article/K03009991 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708 http://www.fortiguard.com/psirt/FG-IR-20-233
IOC TYPE	**VALUE**		
SHA256	0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194498e3b7a867d41b5a3af3910d2aa6231612c787ce8a4bc14ab03f800caab130f		

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
WhisperGate	In the WhisperGate operation in January 2022, Cadet Blizzard is known to deploy destructive malware to select target environments to delete data and render systems inoperable.	By exploiting web servers	CVE-2021-26084 CVE-2020-1472 CVE-2021-4034 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Wiper		Data destruction and Financial Loss	Atlassian Confluence Server and Data Center, Microsoft Netlogon, Red Hat Polkit, and Microsoft Exchange Server
ASSOCIATED ACTOR			**PATCH LINK**
Cadet Blizzard (aka DEV-0586, Ruinous Ursa)			https://jira.atlassian.com/browse/CONFSERVER-67940 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472 https://bugzilla.redhat.com/show_bug.cgi?id=2025869 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34473 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34523 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

IOC TYPE	VALUE
MD5	3a2a2de20daa74d8f6921230416ed4e6

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
ChamelDoH	A new Linux malware called 'ChamelDoH' infects Linux devices and establishes communication with the attackers' servers using DNS-over-HTTPS (DoH). The use of DoH allows the malware's communication to be encrypted and disguised as regular HTTPS traffic, making it difficult to detect.	Unknown	CVE-2017-12149 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Information Theft and Financial Loss	Red Hat JBoss Application Server and Microsoft Exchange Server
ASSOCIATED ACTOR			**PATCH LINK**
ChamelGang			https://access.redhat.com/security/cve/CVE-2017-12149 https://bugzilla.redhat.com/show_bug.cgi?id=1486220 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

IOC TYPE	VALUE
SHA256	34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7 4fd1515bfb5cf7a928acfacabe9d6b5272c036def898d1de3de7659f174475e0 6a26367b905fb1a8534732746fa968e3282d065e13267d459770fe0ec9f101fe 70e845163ee46100f93633e135a7ca4361a0d7bc21030bc200d45bb14756f007 92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b a0bd3b9a008089903c8653d0fcbc16e502da08eb2e77211473d0dfdec2cce67c b893445ae388af7a5c8b398edf98cfb7acd191fb7c2e12c7d3b2d82ee8611b1a de2c8264c0378f651f607ef5d0b93aca5760d370d5fed562e784ce5404bbc1a9 e41a5e84d19f9e45972f497270133167669052ad6f11e7a16e832cf1de59da7d fe68af66cd9bc02de1221765d793637d27856fcaa632fabb81e805d2a2862b72

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-2023-27997	✗ ZERO-DAY	FortiOS and FortiProxy SSL-VPN	-
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*	-
Fortinet heap-based buffer overflow Pre-Auth Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-122	T1574: Hijack Execution Flow,T1499: Endpoint Denial of Service, T1499.004:Application or System Exploitation, T1005:Data from Local System	https://www.fortiguard.com/psirt/FG-IR-23-097

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28299	✗	Visual Studio: 2017 version 15.9; 2022 version 17.4, 17.4, 17.2, 17.0; 2019 version 16.11	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:visual_studio_2017:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:-:*:* cpe:2.3:a:microsoft:visual_studio_2019:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:-:*:* cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:-:*:*	-
Visual Studio Spoofing Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-451	T1059: Command and Scripting Interpreter, T1005: Data from Local System,T1046: Network Service Scanning	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28299

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20867		VMware Tools: 10.0.0 - 12.2.0	UNC3886
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:tools:*:*:*:*:*:*:*:*	VirtualPita and VirtualPie backdoors
VMware Tools authentication bypass			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing, T1078: Valid Accounts	https://www.vmware.com/security/advisories/VMSA-2023-0013.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-0669		Fortra GoAnywhere MFT	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortra:goanywhere_managed_file_transfer:*:*:*:*:*:*:*:*	LockBit Ransomware
Fortra GoAnywhere MFT Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059:Command and Scripting Interpreter	https://github.com/rapid7/metasploit-framework/pull/17607

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27350	✗	PaperCut MF/NG	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*:*:* cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*:*:*	LockBit Ransomware
PaperCut MF/NG Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1478: Install Insecure or Malicious Configuration, T1136: Create Account, T1078: Valid Accounts, T1562: Impair Defenses, T1529: System Shutdown/Reboot	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228	LOG4J	Apache Log4j2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	LockBit Ransomware
Apache Log4j2 Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917 CWE-20 CWE-400 CWE-502	T1059:Command and Scripting Interpreter	https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22986	✗	F5 BIG-IP and BIG-IQ Centralized Management	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*	LockBit Ransomware
F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1059:Command and Scripting Interpreter	https://support.f5.com/csp/article/K03009991

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-0708	BlueKeep	Microsoft Remote Desktop Services	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_:-:*:*:*:*:*:*:*	LockBit Ransomware
Microsoft Remote Desktop Services Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059:Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-13379	✗ ZERO-DAY	Fortinet FortiOS	-
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	LockBit Ransomware
Fortinet FortiOS SSL VPN Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1574:Hijack Execution Flow	https://fortiguard.com/advisory/FG-IR-18-384

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26084	✗ ZERO-DAY	Atlassian Confluence Server and Data Center	Cadet Blizzard (aka DEV-0586, Ruinous Ursa)
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*	WhisperGate
Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1190: Exploit Public-Facing Application, T1040: Network Sniffing, T1078: Valid Accounts	https://jira.atlassian.com/browse/CONFSERVER-67940

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-1472	ZEROLOGON	Microsoft Netlogon	Cadet Blizzard (aka DEV-0586, Ruinous Ursa)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	WhisperGate & LockBit Ransomware
Microsoft Netlogon Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-330	T1068: Exploitation for Privilege Escalation, T1204: User Execution	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-4034	PWNKIT	Red Hat Polkit	Cadet Blizzard (aka DEV-0586, Ruinous Ursa)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:polkit_project:polkit:*:*:*:*:*:*:*:*	WhisperGate
Red Hat Polkit Out-of-Bounds Read and Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787 CWE-125	T1005: Data from Local System, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	https://bugzilla.redhat.com/show_bug.cgi?id=2025869

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34523	PROXYSHELL	Microsoft Exchange Server	Cadet Blizzard (aka DEV-0586, Ruinous Ursa) & ChamelGang
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	WhisperGate & ChamelDoH
Microsoft Exchange Server Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation, T1204: User Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-12149		Red Hat JBoss Application Server Remote Code Execution Vulnerability	ChamelGang
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:redhat:jboss_enterprise_application_platform:-:*:*:*:*:*:*:*	ChamelDoH
Red Hat JBoss Application Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059:Command and Scripting Interpreter	https://access.redhat.com/security/cve/CVE-2017-12149

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34473	PROXYSHELL ZERO-DAY	Microsoft Exchange Server	ChamelGang & Cadet Blizzard (aka DEV-0586, Ruinous Ursa)
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	ChamelDoH & WhisperGate
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1059:Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-31207	PROXYSHELL ZERO-DAY	Microsoft Exchange Server	ChamelGang & Cadet Blizzard (aka DEV-0586, Ruinous Ursa)
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	ChamelDoH & WhisperGate
Microsoft Exchange Server Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190:Exploit Public-Facing Application	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-18935	✗	Telerik UI for ASP.NET AJAX	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:telerik:ui_for_asp.net_ajax:*:*:*:*:*:*:*:*	-
Progress Telerik UI for ASP.NET AJAX Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059:Command and Scripting Interpreter	https://www.telerik.com/support/kb/aspnet-ajax/details/allows-javascriptserializer-deserialization

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-9248	✗	ASP.NET AJAX and Sitefinity	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:telerik:sitefinity_cms:*:*:*:*:*:*:*:* cpe:2.3:a:telerik:ui_for_asp.net_ajax:*:*:*:*:*:*:*:*	-
Progress Telerik UI for ASP.NET AJAX and Sitefinity Cryptographic Weakness Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-522	T1078:Valid Accounts, T1557:Man-in-the-Middle, T1040:Network Sniffing	http://www.telerik.com/support/kb/aspnet-ajax/details/cryptographic-weakness

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11357	✗	Telerik User Interface (UI) for ASP.NET AJAX	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:telerik:ui_for_asp.net_ajax:*:*:*:*:*:*:*:*	-
Telerik UI for ASP.NET AJAX Insecure Direct Object Reference Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1005: Data from Local System, T1046: Network Service Scanning	http://www.telerik.com/support/kb/aspnet-ajax/upload-%28async%29/details/insecure-direct-object-reference

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11317	✗	Telerik User Interface (UI) for ASP.NET AJAX	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:telerik:ui_for_asp.net_ajax:*:*:*:*:*:*:*:*	-
Telerik UI for ASP.NET AJAX Unrestricted File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-326	T1505.003:Server Software Component: Web Shell, T1059: (Command and Scripting Interpreter	http://www.telerik.com/support/kb/aspnet-ajax/upload-%28async%29/details/unrestricted-file-upload

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC3886	China	Defense, Technology, and Telecommunicati on.	The US and APJ regions.
	MOTIVE		
	Financial Crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RAN SOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-20867	VirtualPita and VirtualPie backdoors	VMware Tools: 10.0.0 - 12.2.0
TTPs			
T1560:Archive Collected Data, T1059:Command and Scripting Interpreter, T1203:Exploitation for Client:Execution, T1569:System Services, T1098:Account Manipulation, T1136:Create Account, T1543:Create or Modify System Process, T1548:Abuse Elevation Control Mechanism, T1068:Exploitation for Privilege Escalation, T1055:Process Injection, T1211:Exploitation for Defense:Evasion, T1212:Exploitation for:Credential Access, T1087:Account Discovery, T1105:Ingress Tool Transfer			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 ChamelGang	China	Energy, aviation, and government organizations	Russia, the United States, Japan, Turkey, Taiwan, Vietnam, India, Afghanistan, Lithuania, and Nepal
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RAN SOMWARE**	**AFFECTED PRODUCTS**
	CVE-2017-12149 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	ChamelDoH	Red Hat JBoss Application Server and Microsoft Exchange Server
TTPs			
T1105: Ingress Tool Transfer, T1071: Application Layer Protocol, T1189: Drive-by Compromise, T1071.004: DNS, T1059: Command and Scripting Interpreter, T1564.001: Hidden Files and Directories, T1564: Hide Artifacts, T1027: Obfuscated Files or Information, T1082: System Information Discovery, T1005: Data from Local System, T1041: Exfiltration Over C2 Channel, T1572: Protocol Tunneling			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Cadet Blizzard (aka DEV-0586, Ruinous Ursa)	Russia	Government services, Law enforcement, Non-profit/non-governmental organizations, IT service providers/consulting, and Emergency services.	Europe, Central Asia, and Latin America
	MOTIVE		
	Financial Crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-26084 CVE-2020-1472 CVE-2021-4034 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	WhisperGate	Atlassian Confluence Server and Data Center, Microsoft Netlogon, Red Hat Polkit, and Microsoft Exchange Server
TTPs			
T1059:Command and Scripting Interpreter, T1059.001:PowerShell, T1059.005:Visual Basic, T1055:Process Injection, T1055.012:Process Hollowing, T1562:Impair Defenses, T1562.001:Disable or Modify Tools, T1132:Data Encoding, T1132.001:Standard Encoding, T1102:Web Service, T1071:Application Layer Protocol, T1071.001:Web Protocols, T1105:Ingress Tool Transfer, T1561:Disk Wipe, T1561.002:Disk Structure Wipe, T1486:Data Encrypted for Impact			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **twenty exploited vulnerabilities** and block the indicators related to the threat actor **UNC3886**, **Cadet Blizzard**, **ChamelGang** and **DoubleFinger loader**, **GreetingGhoul stealer**, **VirtualPita backdoor**, **VirtualPie backdoor**, **LockBit Ransomware**, **WhisperGate**, and **ChamelDoH** malware.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **twenty exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **UNC3886**, **Cadet Blizzard**, **ChamelGang** and **DoubleFinger loader**, **GreetingGhoul stealer**, **VirtualPita backdoor**, **VirtualPie backdoor**, **LockBit Ransomware**, **WhisperGate**, and **ChamelDoH** in Breach and Attack Simulation(BAS).

Threat Advisories

Fortinet Releases Patch for Pre-announced Critical Vulnerability

A Flaw in Microsoft Visual Studio Installer Enables Malicious Extension Distribution

DoubleFinger A Sneaky Loader Targets Cryptocurrency

Chinese Espionage Hackers Exploit ESXi Zero-Day

LockBit Ransomware Evolving Tactics and Pervasive Impact in 2023

Unveiling Cadet Blizzard APT's Wiper Attacks Targeting Ukraine

ChamelGang Strikes Again With ChamelDoH Malware XDNS-over-HTTPS

Cybercriminals Exploit Old Telerik Bug for Data Theft

Microsoft's June 2023 Patch Tuesday Addresses 78 Vulnerabilities

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
DoubleFinger loader	Domain	cryptohedgefund[.]us
	MD5	a500d9518bfe0b0d1c7f77343cac68d8 dbd0cf87c085150eb0e4a40539390a9a 56acd988653c0e7c4a5f1302e6c3b1c0 16203abd150a709c0629a366393994ea d9130cb36f23edf90848ffd73bd4e0e0
GreetingGhoul stealer	MD5	642f192372a4bd4fb3bfa5bae4f8644c a9a5f529bf530d0425e6f04cbe508f1e
VirtualPita backdoor	MD5	8e80b40b1298f022c7f3a96599806c43 61ab3f6401d60ec36cd3ac980a8deb75 2c28ec2d541f555b2838099ca849f965 744e2a4c1da48869776827d461c2b2ec 93d50025b81d3dbcb2e25d15cae03428 fe34b7c071d96dac498b72a4a07cb246
	SHA1	e9cbac1f64587ce1dc5b92cde9637affb3b58577 93d5c4ebec2aa45dcbd6ddbaad5d80614af82f84 e35733db8061b57b8fcdb83ab51a90d0a8ba618c a3cc666e0764e856e65275bd4f32a56d76e51420 abff003edf67e77667f56bbcfc391e2175cb0f8a 0962e10dc34256c6b31509a5ced498f8f6a3d6b6
	FullPath	/bin/rdt /usr/lib/vmware/weasel/consoleui/rhttpproxy-io /usr/libexec/setconf/ksmd /usr/bin/ksmd

Attack Name	TYPE	VALUE
VirtualPita backdoor	SHA256	c2ef08af063f6d416233a4b2b2e991c177fc72d70a76c24bca9080521d41040f 4cf3e0b60e880e6a6ba9f45187ac5454813ae8c2031966d8b264ae0d1e15e70d 505eb3b90cd107cf7e2c20189889afdff813b2fbb98bbdeab65cde520893b168 4a6f559426493abc0d056665f23457e2779abd3482434623e1f61f4cd5b41843 13f11c81331bdce711139f985e6c525915a72dc5443fbbfe99c8ec1dd7ad2209 5731d988781c9a1d2941f7333615f6292fb359f6d48498f32c29878b5bedf00f
VirtualPie backdoor	MD5	61ab3f6401d60ec36cd3ac980a8deb75
	SHA1	93d5c4ebec2aa45dcbd6ddbaad5d80614af82f84
	SHA256	4cf3e0b60e880e6a6ba9f45187ac5454813ae8c2031966d8b264ae0d1e15e70d
LockBit Ransomware	SHA256	0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194 498e3b7a867d41b5a3af3910d2aa6231612c787ce8a4bc14ab03f800caab130f af4c28fb1c65ebe93181b67d279733e864cafab5919a7aa7eced93fc8113df16 984d96730ae19d4532325c6fcbd34580fb02fbe454781b589d2eea6090ea2b6d 2cee882bd0dc4267bacf099ac4571c319ac547be12b955f7ccb2f0144ae40876 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db

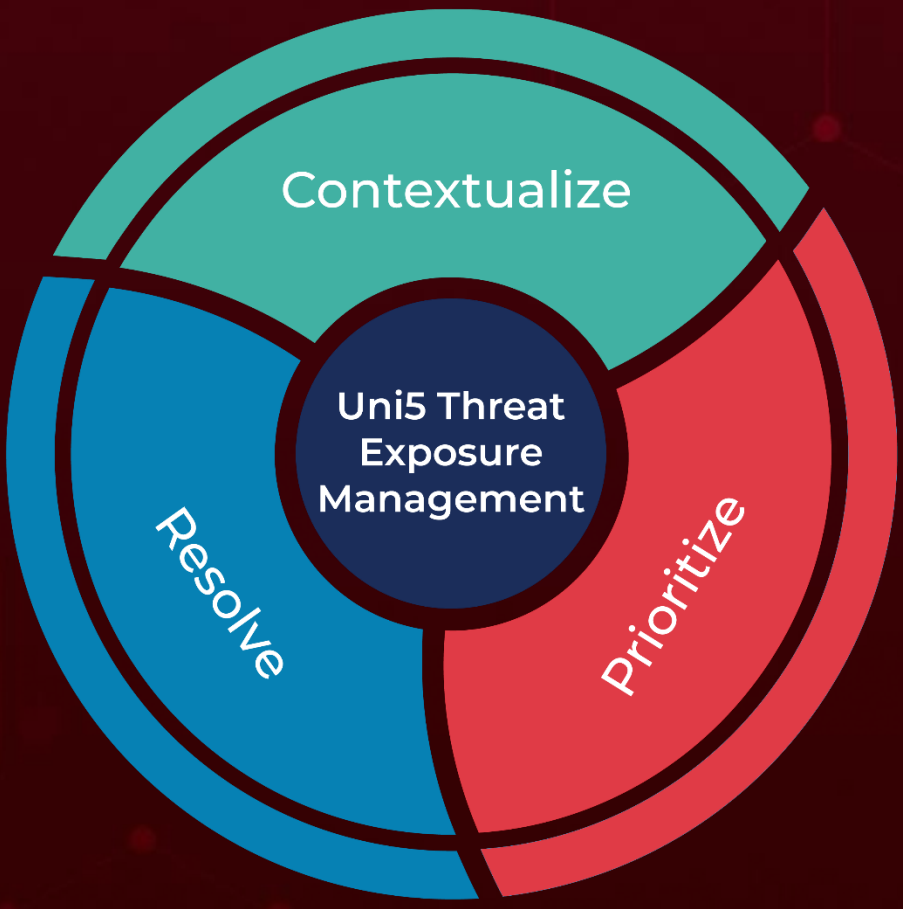
Attack Name	TYPE	VALUE
LockBit Ransomware	SHA256	9aa5bcee06109d52fade97ad21317ff951abc656ba4c800441bacfec00328fd8 379c4620d6f482e153d7033bba21da5d8027387c0e60e3497b63d778dcafd888 0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194 a439c5093801d3b12e2f79b64c0b65bdf148eb6eca8c1e3d179af5ab4995034d 54ac7ac6db6fcec5234454430513d1d2787ee8a48aa60fbf95c1af27534fdb4a a9abab8ab44ccec6321da83d9960a1f30ba783e02b6e0ba3f2e9d19cee76b39b 286726ecca68f8c2752116258aba0cd35c051a6342043ee1add84b890654276f 239c9969fd07e1701a129cfd033a11a93ee9e88e4df4f79b7c5c0dd5bba86390 b964a5253c25465633ef8c2e7f77703d27227bfc0b13a7ca49d187dadc4d38ae ba0eefdfbd1421d37d47f3feaae8e768a4679d6b544bb97f5237319e8ab0b122 f9dbdb825067616070c64565b6b27dc872c4a7219856eb5f8eb3eb1eb1463423 2e218735fa53e036659ea721bfd7b97e2af67b7eda648e9e2579356eb20899d9 1f0e4cbc1a4b52b6d7e4188e4a835a904cf783c75db9a066df4201452bd9647d de7f501e4a17898e85229b962e2f43b9a20d995c8a9fe0cad4536adc8fbd9f48 8989a9aec8d2c4d61fa399a97807f8e62814b1a55fecbd38d11d4d35fdf4a7d1 01bf78841b63bcdd8280157c486b45ad74811c0251140a054de81a925ce7f716 ab4d20b73c7358f1e3a60145d5debc791a17416e2a88eb39f80ec1f53985fad5 9366a5b8021d0283156986bbf020c99ae5e2a3dcbbaa03db934e94bfa7088b86 4bdda7dd3bbe1f9cb0a7d42f6947ba0f6442e52758bd2638541f9409b573d5c9 6b4502d8ba3cff1a3139f72cdad863d53551b65b8c38d7b838d64212822e4630 4d0f95028bb6a04e64550872ddeef6b0c6fa4a5bd368736da47401420df2bee7 cfc45c36b4c731f2308e19a087c3dc3fb7b12eef93e171e8e86e2134ead325ee 4134d5d8f7b038e23e7887db56bb3ad295341a1aaf0bebe6be21d901d06dd662

Attack Name	TYPE	VALUE
LockBit Ransomware	SHA256	149d691411f10f8ec7af43f0237ccfab5b65a9ae73718acf1e0cc0dbdea36ebd cb83eb6f5fd42f59b1c1a34826df48e5a5882c45e4a7f34c80c0830c26cb30dd 4d4bc9d78db93c25548a679de06e267363a31a400e2e37caf9d1fce91b65fe8d b9872ad6ec82d3f2f9a8c6af7e5838f91712e52ece265cd04f4452378bd5bcfd a8939a43feb8cc258507ffd0be564d56a2874c220729e00da8ad204c3b4012c5 fef1f9664fde9b23754c691b15a05fdc35a51a0ceb8a18fb9a5a0166e6377c69 fef1f9664fde9b23754c691b15a05fdc35a51a0ceb8a18fb9a5a0166e6377c69 734955fdb84b29fa1aa87aa0af2ebf155125917a6b61ffe4b4dc7030dd212309 E47b928d0fc16348b828abeb3c2106a6d752512f60ef4583d6532cc0dbebebbf 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c 5a13ac97ce91d5b095c7154fe756615fa0730c17ddf432ae4af6c42d2c29946d
WhisperGate	MD5	3a2a2de20daa74d8f6921230416ed4e6
ChamelDoH	SHA256	34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7 4fd1515bfb5cf7a928acfacabe9d6b5272c036def898d1de3de7659f174475e0 6a26367b905fb1a8534732746fa968e3282d065e13267d459770fe0ec9f101fe 70e845163ee46100f93633e135a7ca4361a0d7bc21030bc200d45bb14756f007 92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b a0bd3b9a008089903c8653d0fcbc16e502da08eb2e77211473d0dfdec2cce67c b893445ae388af7a5c8b398edf98cfb7acd191fb7c2e12c7d3b2d82ee8611b1a de2c8264c0378f651f607ef5d0b93aca5760d370d5fed562e784ce5404bbc1a9 e41a5e84d19f9e45972f497270133167669052ad6f11e7a16e832cf1de59da7d fe68af66cd9bc02de1221765d793637d27856fcaa632fabb81e805d2a2862b72

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

June 19, 2023 • 11:11 AM

More at www.hivepro.com