

Date of Publication
June 3, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

27 MAY to 02 JUNE 2024

Table Of Contents

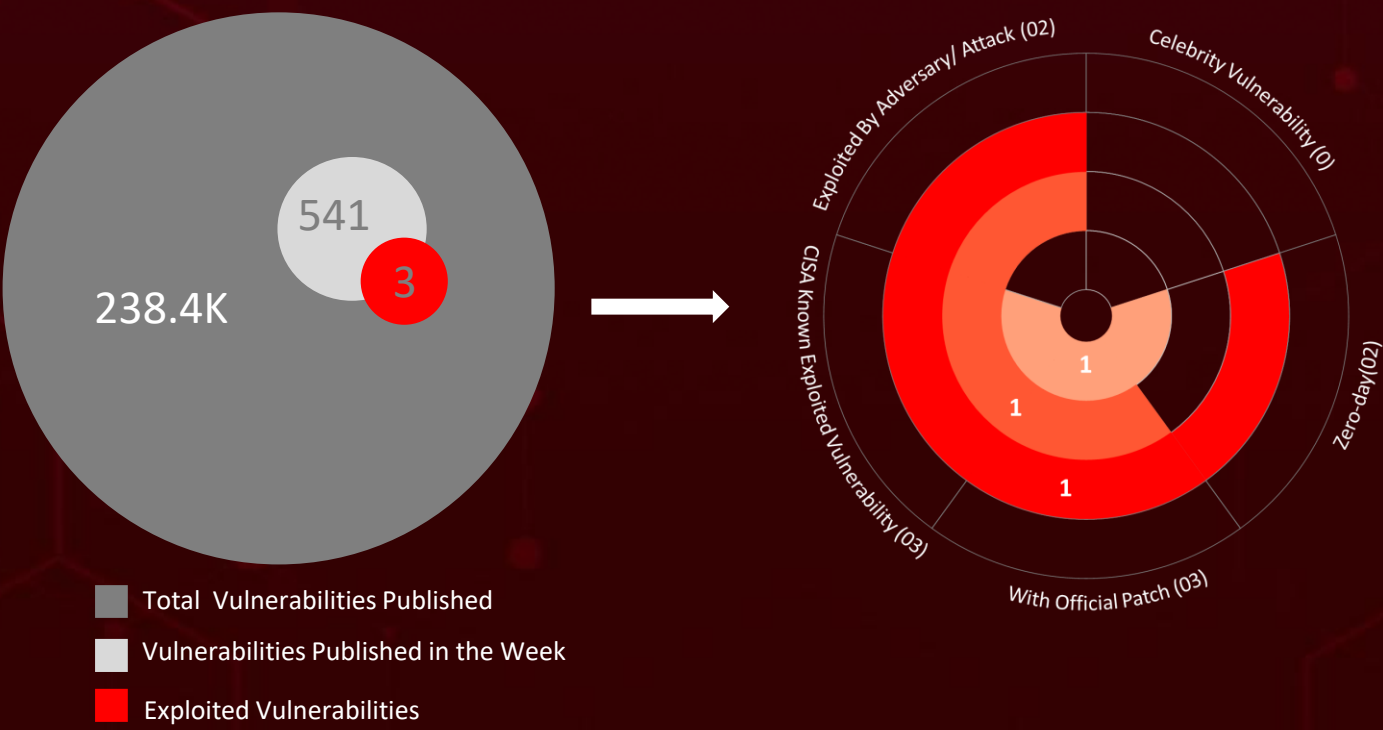
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	10
<u>Adversaries in Action</u>	12
<u>Recommendations</u>	14
<u>Threat Advisories</u>	15
<u>Appendix</u>	16
<u>What Next?</u>	19

Summary

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

Furthermore, HiveForce Labs uncovered that the North Korean hacking group **Moonstone Sleet** has been creating fake companies and job opportunities, deploying trojanized tools, developing a malicious game and utilized a new custom ransomware called **FakePenny**.

Furthermore, Google has addressed **CVE-2024-5274**, fourth Chrome zero-day vulnerability in the month of May. This vulnerability pertains to a type confusion bug in the V8 JavaScript and WebAssembly engine that can lead to code execution. These rising attacks present a significant and immediate threat to users globally.



High Level Statistics

4

Attacks
Executed

3

Vulnerabilities
Exploited

2

Adversaries in
Action

- [ShrinkLocker Ransomware](#)
- [RustDoor](#)
- [GateDoor](#)
- [FakePenny Ransomware](#)

- [CVE-2024-5274](#)
- [CVE-2024-4978](#)
- [CVE-2024-24919](#)

- [Moonstone Sleet](#)
- [UNC5537](#)



Insights

UNC5537

targets Snowflake instances, for data theft and extortion

CVE-2024-5274, The Persistence of

Google Zero Day Google's fourth zero-day in May, affecting the V8 JavaScript and WebAssembly engine in Chrome browser, that can lead to code execution

Moonstone Sleet

group targets companies for financial gain employing tactics like trojanized software, and custom ransomware

ShrinkLocker Exploits BitLocker

Shrinklocker encrypts discs and creates new boot volumes using Microsoft BitLocker. To make discovery more difficult, it alters registry settings for encryption and disables Remote Desktop Protocol

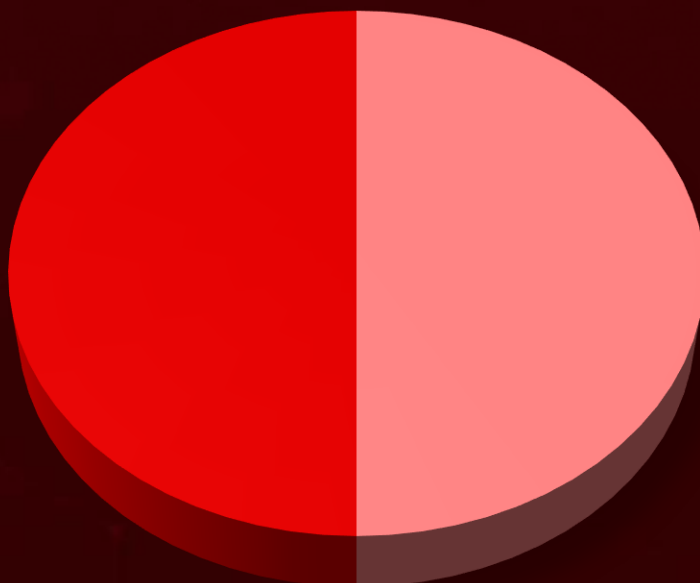
CVE-2024-4978

critical supply chain attack, Adversaries have backdoored the installer for the widely used JAVS courtroom video recording software with RustDoor and GateDoor malware, enabling them to take control of compromised systems

CVE-2024-24919

zero-day flaw in Check Point Security Gateways allows attackers to read sensitive information

Threat Distribution



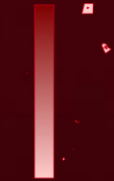
■ Backdoor

■ Ransomware

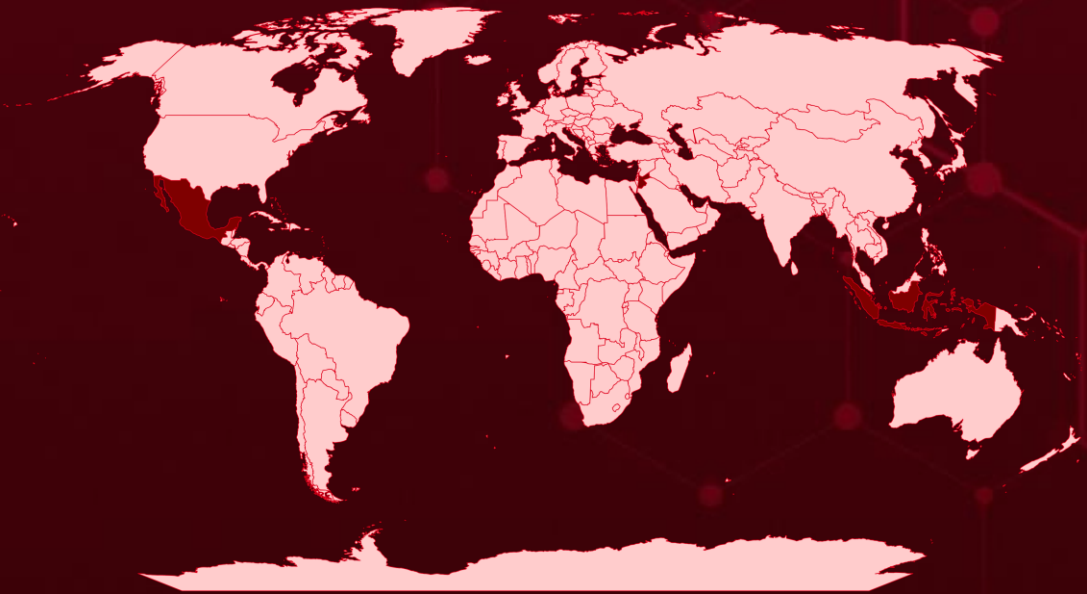


Targeted Countries

Most



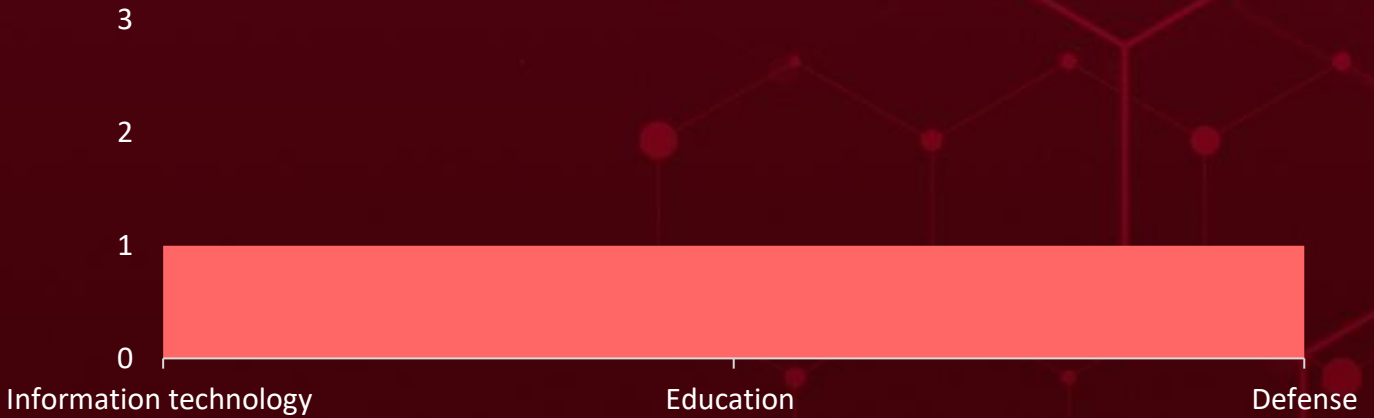
Least



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

Countries	Countries	Countries	Countries
Indonesia	New Zealand	Saudi Arabia	Timor-Leste
Mexico	Gambia	Hungary	Thailand
Jordan	Niger	Serbia	Togo
Oman	Georgia	Iceland	Trinidad and Tobago
Liechtenstein	North Korea	Sierra Leone	Tonga
Spain	Germany	India	Kazakhstan
Angola	Norway	Slovakia	Tunisia
Mongolia	Ghana	Albania	Kenya
Antigua and Barbuda	Pakistan	Solomon Islands	Turkmenistan
Samoa	Greece	Iran	Kiribati
Argentina	Panama	South Africa	Uganda
Tuvalu	Grenada	Iraq	Kuwait
Armenia	Paraguay	South Sudan	United Arab Emirates
Malta	Guatemala	Ireland	Kyrgyzstan
Australia	Philippines	Sri Lanka	United States
Netherlands	Guinea	Israel	Laos
Austria	Portugal	State of Palestine	Uzbekistan
Poland	Guinea-Bissau	Italy	Latvia
Azerbaijan	Romania	Suriname	Venezuela
Singapore	Guyana	Jamaica	Lebanon
Bahamas	Rwanda	Switzerland	Yemen
Syria	Haiti	Japan	Lesotho
Bahrain	Saint Lucia	Tajikistan	Zimbabwe
	Holy See		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1212

Exploitation for Credential Access

T1588.006

Vulnerabilities

T1486

Data Encrypted for Impact

T1059

Command and Scripting Interpreter

T1584

Compromise Infrastructure

T1036

Masquerading

T1588

Obtain Capabilities

T1059.001

PowerShell

T1657

Financial Theft

T1204.002

Malicious File

T1204

User Execution

T1567

Exfiltration Over Web Service

T1027.009

Embedded Payloads

T1055

Process Injection

T1059.005

Visual Basic

T1547.001

Registry Run Keys / Startup Folder

T1059.006

Python

T1586.003

Cloud Accounts

T1059.007

JavaScript

T1619

Cloud Storage Object Discovery

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ShrinkLocker Ransomware	ShrinkLocker is a new ransomware strain that exploits Microsoft's BitLocker to encrypt entire drives, using a VBScript to shrink partitions and create new boot volumes. It disables Remote Desktop Protocol (RDP) and modifies registry settings to enforce encryption, making detection difficult.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	e5471fb4827cb570e65c2ebdff5da38e64b6a9fe47a81d11dab2f0937315be30		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RustDoor	Rustdoor facilitates unauthorized remote access, collects data from the host computer, and downloads additional malicious payloads, enabling them to take control of compromised systems. RustDoor was initially identified in December 2023, and uses Apple-related keywords such as Mac, iCloud, and Apple as the address of the C&C server.	Exploiting Vulnerability	CVE-2024-4978
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	JAVS Viewer software
ASSOCIATED ACTOR			PATCH LINK
-			https://www.javs.com/downloads/
IOC TYPE	VALUE		
SHA256	238b546e2a1afc230f88b98dce1be6bf442b0b807e364106c0b28fe18db2ce66, 2acd053b854545d381866d471a711d860e84a38cb9f2e13983a74c4044080dc2, e86963c94f3c1de1ccfffaa4d192d39881a24df8b175c00fd64a4e076826b76b		




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
GateDoor	GateDoor is a Windows malware written in Golang. It functions as a backdoor with loader capabilities and is signed with a valid certificate.	Exploiting Vulnerability	CVE-2024-4978
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	JAVS Viewer software
ASSOCIATED ACTOR			PATCH LINK
-			https://www.javs.com/downloads/
IOC TYPE	VALUE		
SHA256	9dd66e5692e496c9cfcc647edf593c323404424cad61276725efb934b64b96e9		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FakePenny Ransomware	FakePenny is a new custom ransomware used by Moonstone Sleet in its operations. FakePenny comprises an encryptor and a loader, with its ransomware note resembling that of NotPetya.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			PATCH LINK
Moonstone Sleet			-
IOC TYPE	VALUE		
SHA256	f59035192098e44b86c4648a0de4078edbe80352260276f4755d15d354f5fc58, cb97ec024c04150ad419d1af2d1eb66b5c48ab5f345409d9d791db574981a3fb, 39d7407e76080ec5d838c8ebca5182f3ac4a5f416ff7bda9cbc4efffd78b4ff5		

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-2024-5274		Google Chrome	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*	-
Google Chrome Type Confusion in V8 Vulnerability			
	CWE ID		
	CWE-843	T1059.007: JavaScript, T1203: Exploitation for Client Execution	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4978		JAVS Viewer software	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:justice_av_solutions:viewer:*:*:*:*:*	RustDoor, GateDoor
JAVS Arbitrary code Execution Vulnerability			
	CWE ID		
	CWE-506	T1059: Command and Scripting Interpreter, T1027.009: Embedded Payloads	https://www.javs.com/downloads/


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR		
<u>CVE-2024-24919</u>		Check Point Security Gateway	-		
	ZERO-DAY				
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE		
NAME	CISA KEV	cpe:2.3:a:checkpoint:quantum_gateway:*:*:*:*.*	-		
Check Point Security Gateway Information Disclosure Vulnerability				ASSOCIATED TTPs	PATCH LINK
	CWE ID			T1133: External Remote Services, T1212: Exploitation for Credential Access	https://support.checkpoint.com/results/sk/sk182336
	CWE-200				

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Moonstone Sleet (aka Storm-1789)</u>	North Korea	Information technology, Education, and Defense	Worldwide
	MOTIVE Financial gain and stealing information		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	FakePenny Ransomware	-

TTPs

TA0002: Execution; TA0005: Defense Evasion; TA0003: Persistence; TA0011: Command and Control; TA0007: Discovery; TA0040: Impact; TA0001: Initial Access; TA0009: Collection; T1566: Phishing; T1204: User Execution; T1204.002: Malicious File; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1547.001: Registry Run Keys /Startup Folder; T1547: Boot or Logon Autostart Execution; T1055.001: Dynamic-link Library Injection; T1055: Process Injection; T1033: System Owner/User Discovery; T1016: System Network Configuration; T1584: Compromise Infrastructure; T1657: Financial Theft; T1486: Data Encrypted for Impact; T1656: Impersonation

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC5537	-	All	Worldwide
	MOTIVE		
	Data theft and extortion		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	-	-	-
TTPs			
TA0002: Execution; TA0040: Impact; TA0001: Initial Access; TA0009: Collection; TA0007: Discovery; TA0010: Exfiltration; TA0006: Credential Access; T1657: Financial Theft; T1619: Cloud Storage Object Discovery; T1586.003: Cloud Accounts; T1586: Compromise Accounts; T1530: Data from Cloud Storage; T1486: Data Encrypted for Impact; T1212: Exploitation for Credential Access; T1621: Multi-Factor Authentication Request Generation			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerabilities** and block the indicators related to the threat actors **Moonstone Sleet, UNC5537** and malware **ShrinkLocker Ransomware, RustDoor, GateDoor, FakePenny Ransomware**.

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 **three exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Moonstone Sleet, UNC5537** and malware **RustDoor, GateDoor** in Breach and Attack Simulation(BAS).

Threat Advisories

[Google Fends Off Fourth Zero-Day in May](#)

[ShrinkLocker: Ransomware Exploits BitLocker for Drive Encryption](#)

[JAVS Courtroom Recording Software Hit by Supply Chain Attack](#)

[Moonstone Sleet: A New North Korean Cyber Threat](#)

[Check Point Fixes Zero-Day CVE-2024-24919 Exploited in the Wild](#)

[UNC5537 Targeting Snowflake Users for Data Theft and Extortion](#)

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
<u>ShrinkLocker Ransomware</u>	SHA256	e5471fb4827cb570e65c2ebdff5da38e64b6a9fe47a81d11dab2f0937315be30
	MD5	842f7b1c425c5cf41aed9df63888e768
<u>RustDoor</u>	SHA256	238b546e2a1afc230f88b98dce1be6bf442b0b807e364106c0b28fe18db2ce66, 2acd053b854545d381866d471a711d860e84a38cb9f2e13983a74c4044080dc2, e86963c94f3c1de1ccfffaa4d192d39881a24df8b175c00fd64a4e076826b76b, f11b0f67f76b7d49511a6212921901afae5b7ecd2bbc718a3d70f6ccb524903a, b0665afbd99baf586899abae457f702962503afb855f4bda58cf070ca1c69956, bd1b0c5e48f4aa7595ef3e7dd125d0b95d39d647e480bd3c0c6ff7229d52f800, 00b66c1e7e483da6cbcc0d94f01b9fca245fb052ef8e958e21abcb0880aff37f, 996921573bc8d2618eaf4b7532fc1b46074fe5cdc317f5a751fc70b5371362a3, b4991bc670ba62c77ffec0a2fe3c445085de822ce8b282265cb24cfbae951ae0, f9a4f04d7222afbbadb2cb417ee9e70733e1dcc2af94ec3cc9b6308a3216f93, 20b986b24d86d9a06746bdb0c25e21a24cb477acb36e7427a8c465c08d51c1e4, c93feb701e04cac4c6ed805d529378351e500ca1178958862d9e24c9f8723518,

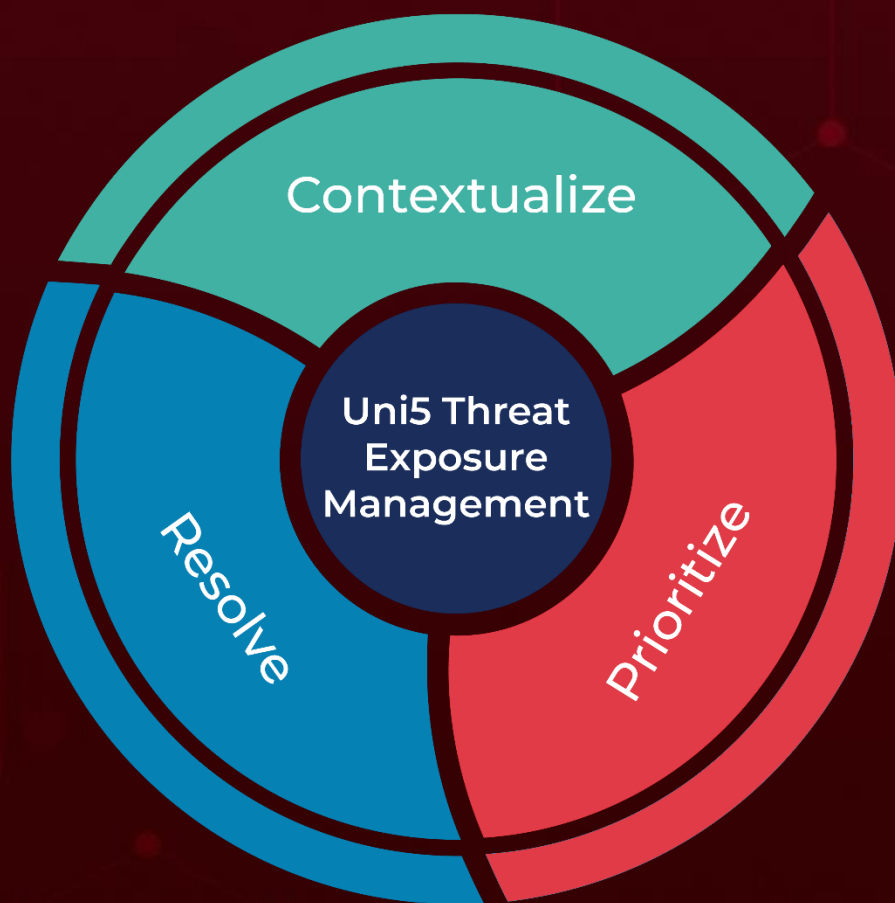
Attack Name	TYPE	VALUE
<u>RustDoor</u>	SHA256	e96c13667bccd6c6c38d9797b15642bfea19080f9bc90d944e7ae6abfb4c64be, 4a59e2fe11ed9136d96a985448b34957ee5861adc9c1a52de4ad65880875dfdb, f59fcbb11a66b6596c2cca926c54e0a4114687769e726c39f2a918dc9e332eff, 449cc50caf2f4b85c6425fea809aa662b80f17821a8f3dc47fe8586ee56bd1dc, 5763ab1ccadc2724d6ec728926eb4dc574a6005a8456a65035dee5edb3cc2a0a, 481a279e15f808d695da233f690a0e3eb15d9b90fce42b9edb1ee296af6289d7, a69d91cf565e717662d0470183cced3350ba0bb4f91d2ced3f089af3a707c5c3, a9d299edf6b3bc1c98185e1c22ba7326f3ad6cba73ca00565330d5c3da50e02c, 6ea00e7d945e78f28d6043bb5d304e0f56d22ab104c9c74e77d1f8572dc17809, 01534a1849b197c03eb23c27d16ace7fc99778eeaa24953154e4f41afc712032, 11c998005bcce297b6a0595b97281aca7a587b6bc1e6aa414609812108b3328c, fe565f4296570a89893828cdd61c6421cf745bab220e21cebce226863d5772a0, c30f634f56000e87c9c4258174ec09ee5bd67d29eca4e78f63c34f976b0272d8, 43609c813c3084532073a22f24e931f24c04e118dcd972c6c8f0428637d9c0ff
<u>GateDoor</u>	SHA256	9dd66e5692e496c9cfcc647edf593c323404424cad61276725efb934b64b96e9
<u>FakePenny Ransomware</u>	Domain	bestonlinefilmstudio[.]org, blockchain-newtech[.]com, ccwaterfall[.]com, chaingrown[.]com, defitankzone[.]com, detankwar[.]com, freenet-zhilly[.]org, matrixane[.]com, pointdnt[.]com, starglowventures[.]com, mingeloem[.]com
	MD5	1d5ad4a60ec9be32c11ad99f234bfe8f, 14af3f039f2398b454bbb64c7fdf4a22,

Attack Name	TYPE	VALUE
<p><u>FakePenny Ransomware</u></p>	MD5	<p>66c45a736e165cf78cee7970bbc74ead, 330fff5b3c54a03fd59a64981e96814d, b8e1fe2955282a58fa3042b25f2ce19d, 608fb305734364e63513ef36da787f2b, c0bb453d00bf3d8acde09b691ca9b5f2, 6c76f795c4b3ff2e478766dee7c738d6, 08f8353101fb2f11a1036a947f8fce83, 39898007146d7b436d013924db58ebc6</p>
	SHA256	<p>f59035192098e44b86c4648a0de4078edbe80352260276f4755d15d 354f5fc58, cb97ec024c04150ad419d1af2d1eb66b5c48ab5f345409d9d791db57 4981a3fb, 39d7407e76080ec5d838c8ebca5182f3ac4a5f416ff7bda9cbc4efffd78 b4ff5, 70c5b64589277ace59db86d19d846a9236214b48aacabbaf880f2b63 55ab5260, cafaa7bc3277711509dc0800ed53b82f645e86c195e85fbf34430bbc7 5c39c24, 9863173e0a45318f776e36b1a8529380362af8f3e73a2b4875e30d31 ad7bd3c1, f66122a3e1eaa7dcb7c13838037573dace4e5a1c474a23006417274c 0c8608be, 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccb6f143 13ead8c, ecce739b556f26de07adbfc660a958ba2dca432f70a8c4dd01466141a 6551146, 09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5e8 4a6cc38</p>
	SHA1	<p>be6909ba6e0b4d228da5b9dacc83f7082c06cf2, f1f75da17e8c125b87fdafd76386f90213362bcf, b0479c5d4de5541a60923b5627ed62e6391efe2f, 550bdf367fba63a81276465a65dcb64280240dda, dd91678f1d023607430d53b5ff5f1d6533a98469, bda08d55f14827abf21abb79384039660f2fa198, 2ebfcfb2deb09e9af046ae765797a654b49645c2, e99d44e93069001129c8f88f7a5259fb21bb6b68, 853d256bafd39426fad9bf5f7fad2971b7978c06, dd8b8c4de92d9b6d1d04f0e995f4cc7e746d0a64</p>

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 3, 2024 • 7:00 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com