Date of Publication
July 24 , 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

17 to 23 JULY 2023

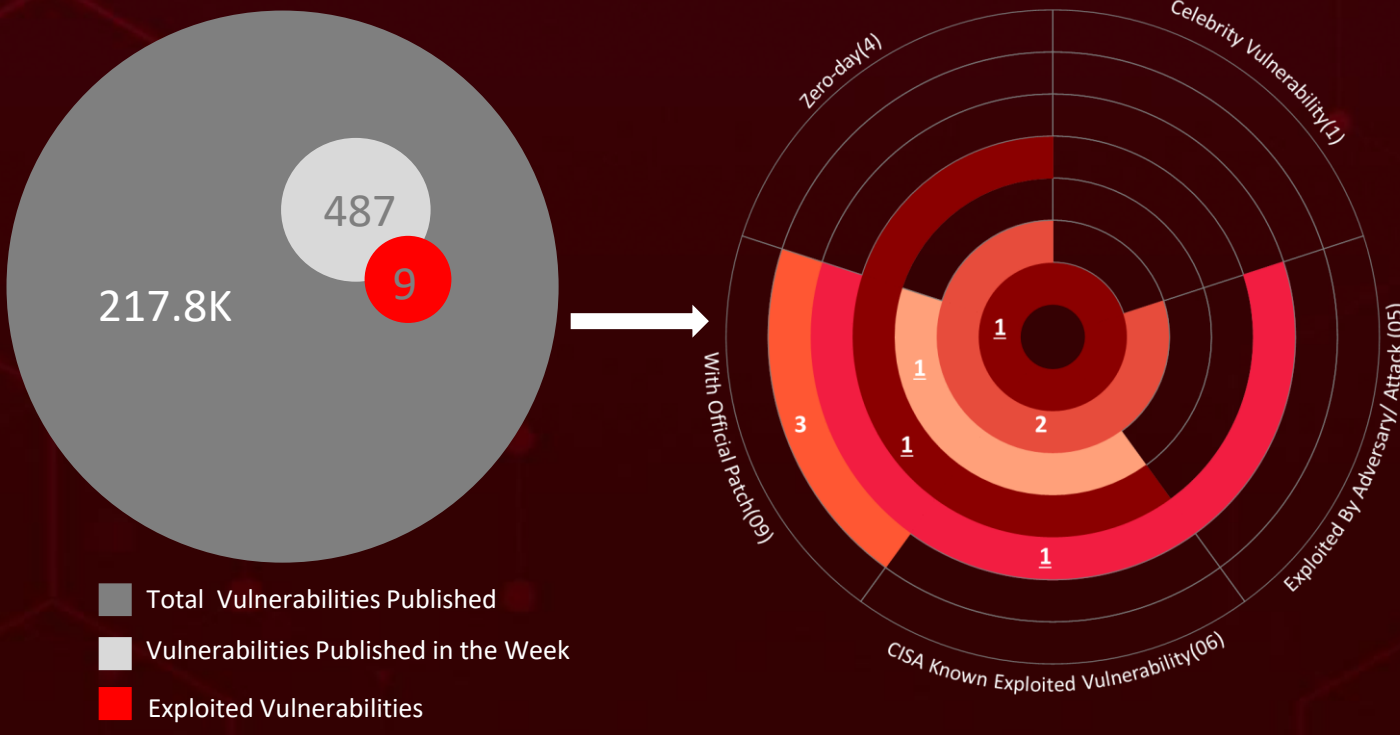
Table Of Contents

Summary

HiveForceLabs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of **eleven** attacks executed, **nine** vulnerabilities, and **three** different adversaries highlights the ever-present danger of cyber attacks.

Moreover, HiveForceLabs also discovered that **Turla** employed two malware strains, while **Space Pirates** deployed four malware in their recent attack. Furthermore, we identified **LokiBot** leveraging **two** Zero-days to acquire confidential data.

Meanwhile, Cybercriminals are orchestrating a widespread campaign to exploit a pivotal **WooCommerce Payments plugin**, with a staggering 1.3 million assault attempts recorded against 157,000 websites. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

11
Attacks Executed

9
Vulnerabilities Exploited

3
Adversaries in Action

- LokiBot
- Sardonic backdoor
- Noberus ransomware
- P2PInfect
- Deed RAT
- Voidoor
- ShadowPad
- PlugX
- Kanti ransomware
- DeliveryCheck
- KAZUAR

- CVE-2021-40444
- CVE-2022-30190
- CVE-2023-29298
- CVE-2023-38203
- CVE-2023-29300
- CVE-2023-28121
- CVE-2023-3519
- CVE-2022-0543
- CVE-2017-0213

- FIN8
- Space Pirates
- Turla

Insights

LokiBot: Harnessing **2 Zero-Days** to Siphon Your Data!

FIN8 Strikes: Unleashing a Reinvented Sardonic Backdoor to deploy **Noberus** Ransomware!

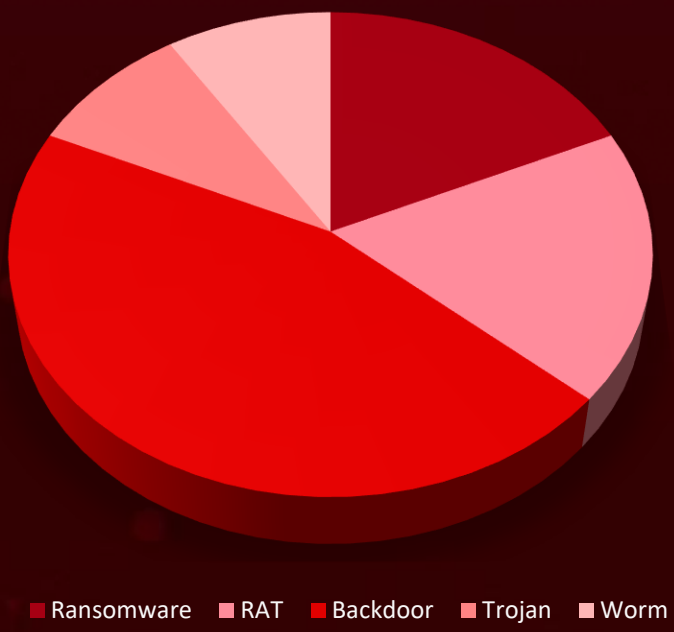
Cloud Alert: **P2PInfect** Worm Strikes, Posing a Significant Threat to **307,000 Systems!**

Space Pirates Infamous Group Targets 16 Russian Organizations in Intensified Cyber Assaults

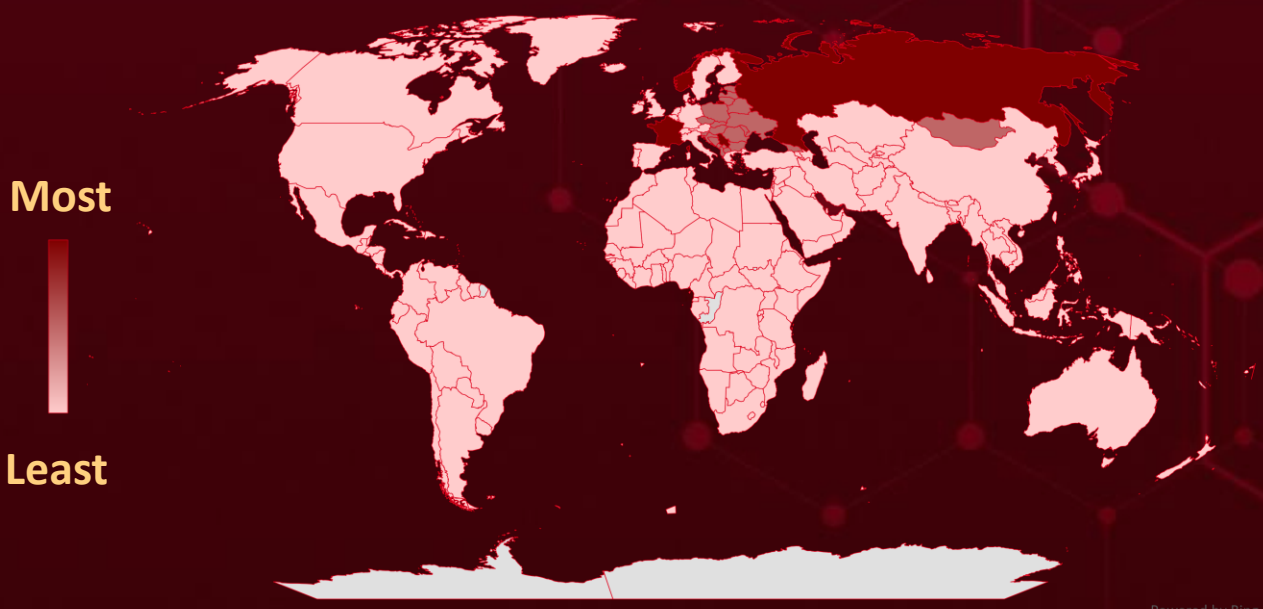
Ukraine's Defense Sector Under Siege: **Turla** Strikes with **DeliveryCheck** Backdoor's Signature

Kanti Ransomware: Targeting Crypto Users, Adeptly Tailored for Bitcoin Wallets

Threat Distribution



Targeted Countries



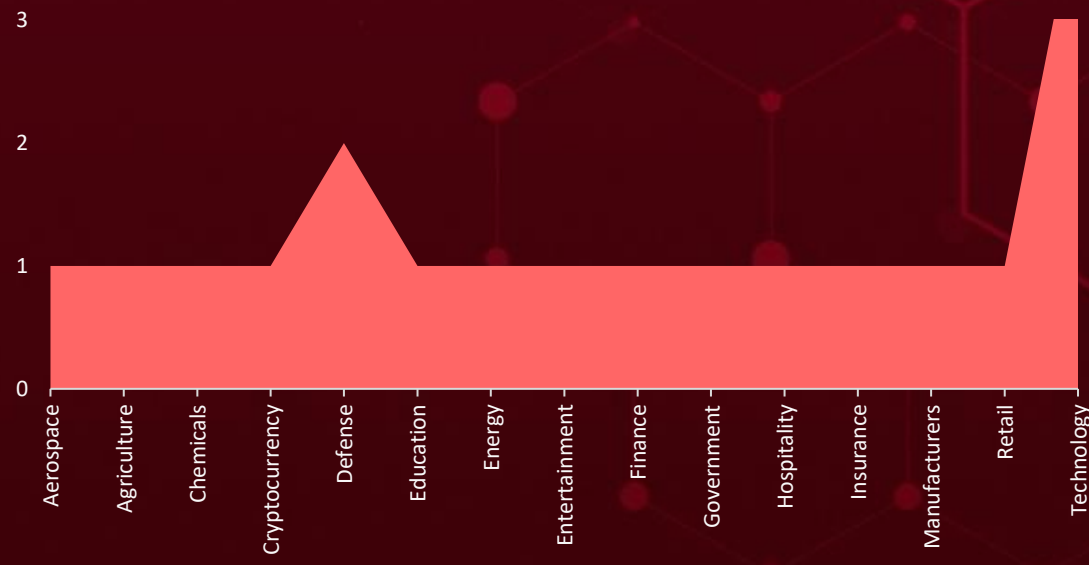
Countries
Norway
Serbia
France
Russia
Bulgaria
Montenegro
Moldova
Croatia
Bosnia and Herzegovina
Czech Republic
Lithuania
Estonia
Mongolia
Albania
North Macedonia
Romania
Poland
Belarus
Slovenia
Georgia
Slovakia
Hungary
Ukraine
Kosovo
Latvia

Countries
Aruba
Azerbaijan
Benin
United States
Bermuda
Norfolk Island
Bhutan
San Marino
Bir Tawil
Thailand
Bolivia
Malta
Bonaire
Nepal
Åland
Palau
Botswana
Saint Barthélemy
Bouvet Island
Sint Eustatius
Brazil
Suriname
British Indian Ocean Territory
Turkmenistan
British Virgin Islands

Countries
Brunei
Mexico
Afghanistan
Mozambique
Burkina Faso
Nicaragua
Burundi
Cambodia
Paraguay
Cameroon
Bahamas
Canada
Saint Martin
Bangladesh
Central African Republic
Spain
Chad
Syria
Chile
Transnistria
China
Uganda
Vanuatu
Clipperton Island
Zimbabwe

Countries
Colombia
Australia
Saudi Arabia
United Arab Emirates
Finland
Germany
North Korea
Qatar
Bahrain
Iceland
India
Iran
Iraq
Ireland
Israel
South Africa
South Korea
Japan
Kenya
Switzerland
Kuwait
United Kingdom
Vietnam
Malaysia
Maldives

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1588.006** Vulnerabilities	**T1082** System Information Discovery	**T1588** Obtain Capabilities
T1059.001 PowerShell	**T1588.005** Exploits	**T1083** File and Directory Discovery	**T1566** Phishing	**T1203** Exploitation for Client Execution
T1068 Exploitation for Privilege Escalation	**T1027** Obfuscated Files or Information	**T1095** Non-Application Layer Protocol	**T1057** Process Discovery	**T1566.001** Spearphishing Attachment
T1547 Boot or Logon Autostart Execution	**T1036** Masquerading	**T1573** Encrypted Channel	**T1010** Application Window Discovery	**T1546** Event Triggered Execution

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LokiBot	LokiBot, alternatively recognised as Loki PWS, has been operating since 2015. By leveraging the remote code execution vulnerabilities CVE-2021-40444 and CVE-2022-30190, the attackers used the ability to implant malicious macros within Microsoft documents, diligently striving to acquire confidential data from compromised machines.	Unknown	CVE-2021-40444 CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		System Disruption and Loss of Confidential Data	Windows Server & Microsoft Internet Explorer
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40444 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

IOC TYPE	VALUE
SHA256	17d95ec93678b0a73e984354f55312dda9e6ae4b57a54e6d57eb59bcbbe3c382, 23982d2d2501cfe1eb931aa83a4d8dfe922bce06e9c327a9936a54a2c6d409ae, 9eaf7231579ab0cb65794043affb10ae8e4ad8f79ec108b5302da2f363b77c93, da18e6dcefe5e3dac076517ac2ba3fd449b6a768d9ce120fe5fc8d6050e09c55, 2e3e5642106ffbde1596a2335eda84e1c48de0bf4a5872f94ae5ee4f7bffda39, 80f4803c1ae286005a64ad790ae2d9f7e8294c6e436b7c686bd91257efbaa1e5, 21675edce1fdabfee96407ac2683bcad0064c3117ef14a4333e564be6adf0539, 4a23054c2241e20aec97c9b0937a37f63c30e321be01398977e13228fa980f29
IPv4	95[.]164[.]23[.]2

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
Sardonic backdoor	The financially motivated threat actor FIN8 has been detected employing a revised variant of the backdoor known as Sardonic to deliver the Noberus ransomware. Sardonic, which enables the collection of information, execution of commands, and deployment of malicious DLL plugins.	Spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft, and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
FIN8 (aka Syssphinx, ATK 113)			-
IOC TYPE	**VALUE**		
SHA256	1d3e573d432ef094fba33f615aa0564feffa99853af77e10367f54dc6df95509, 5b8b732d0bb708aa51ac7f8a4ff5ca5ea99a84112b8b22d13674da7a8ca18c28,		
IPv4	37.10.71[.]215		
Domains	api-cdn[.]net, git-api[.]com, api-cdnw5[.]net, 104-168-237-21.sslip[.]io		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Noberus ransomware	The FIN8 group deployed the Noberus (aka ALPHV, BlackCat) ransomware via a reworked Sardonic backdoor in attacks as the final payload.	Sardonic backdoor	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Information Theft, and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
FIN8 (aka Syssphinx, ATK 113)			-
IOC TYPE	**VALUE**		
SHA256	0c6f444c6940a3688ffc6f8b9d5774c032e3551ebbccb64e4280ae7fc1fac479, 13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31, 15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed, 1af1ca666e48afc933e2eda0ae1d6e88ebd23d27c54fd1d882161fd8c70b678e, 2587001d6599f0ec03534ea823aab0febb75e83f657fadc3a662338cc08646b0, 28d7e6fe31dc00f82cb032ba29aad6429837ba5efb83c2ce4d31d565896e1169, 2cf54942e8cf0ef6296deaa7975618dadff0c32535295d3f0d5f577552229ffc, 38834b796ed025563774167716a477e9217d45e47def20facb027325f2a790d1		

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
P2PInfect	A new peer-to-peer (P2P) worm called P2PInfect, written in the Rust programming language making it highly scalable and potent, targets Redis, a widely used open-source database applications within cloud environments.	Exploits the CVE-2022-0543 vulnerability	CVE-2022-0543
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Worm		System Disruption and Information Theft	Debian-specific Redis Server
ASSOCIATED ACTOR			**PATCH LINK**
-			https://security-tracker.debian.org/tracker/CVE-2022-0543
IOC TYPE	**VALUE**		
SHA256	88601359222a47671ea6f010a670a35347214d8592bceaf9d2e8d1b303fe26d7, b1fab9d92a29ca7e8c0b0c4c45f759adf69b7387da9aebb1d1e90ea9ab7de76c, 68eaccf15a96fdc9a4961daffec5e42878b5924c3c72d6e7d7a9b143ba2bbfa9, 89be7d1d2526c22f127c9351c0b9eafccd811e617939e029b757db66dadC8f93		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Deed RAT	Deed RAT saves all its data, including configuration and plugins, in the registry. Through network sniffing, it gathers information about active proxies. It obtains the linguistic code identifier during system information gathering. Deed RAT could encapsulate its protocol in DNS and identifies and connect to its C&C using proxies.	Spear-phishing	CVE-2017-0213
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Disruption, Information Theft, and Financial Loss	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
Space Pirates (aka Webworm)			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0213
IOC TYPE	**VALUE**		
SHA256	b6860214fcc1ef17937e82b1333672afa5fcf1c1b394a0c7c0447357477fe7c9, 212f750a1d38921b83e68e142ee4ae1c7b612bf11c99210da60775f17c85a83e		
SHA1	3f8ee1e875cbb01e145a09db7d857b6be22bdd92, f99f5f397fe1abb3fc25cc99fe95952fe24b6123		

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
Voidoor	Voidoor is a 32-bit EXE file that contains the PDB path. It takes advantage of the victim identifier, which is kept in the %TEMP%/ids file. The Voidoor starts the Preparatory phase by trying to connect to port 27015. If this attempt fails, the process is immediately suspended.	Delivered by Deed RAT	CVE-2017-0213
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Disruption, Information Theft, and Financial Loss	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
Space Pirates (aka Webworm)			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0213
IOC TYPE	**VALUE**		
SHA256	86c17c549433223f3b59f5ee3e4f2694ebf4e6aabd66508a9a6fec1bdf830c61		
SHA1	1749f99443b345860dd037940505421c45156950		
MD5	48097e614cdf1f9c908b7449cd1119c5		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ShadowPad	ShadowPad is a modular RAT with features comparable to PlugX, and it is frequently referred to as the malware's successor, which is constantly developed and maintained. ShadowPad implements many features that can be used to obtain and retain unauthorised access to a system.	Spear-phishing	CVE-2017-0213
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Disruption, Information Theft, and Financial Loss	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
Space Pirates (aka Webworm)			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0213
IOC TYPE	**VALUE**		
SHA256	3ce38a2fc896b75c2f605c135297c4e0cddc9d93fc5b53fe0b92360781b5b94e, 210934a2cc59e1f5af39aa5a18aae1d8c5da95d1a8f34c9cfc3ab42ecd37ac92		

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
PlugX	PlugX is used to access and control infected devices remotely. It enables attackers to access a system, steal sensitive data, and exploit the compromised machine.	Spear-phishing	CVE-2017-0213
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Disruption, Information Theft, and Financial Loss	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
Space Pirates (aka Webworm)			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0213

IOC TYPE	VALUE
SHA256	22c6d07b64d40811ef31113faac7293348845ab6a06f7319a653ca694c26e94a, 8c8f9fd17d1c28b471bcc4c870ab53a3b4b260ae2fd123b0ef2a2a819ce1cc78
SHA1	a8808089c37faacebc19bafd2677ba011afffc49, 154da55173f97c50e41e48157bc94515cc6146ec
MD5	3cf999dd950af82cad3f8c6eb5430bd5, 6d3ce5d4003ce4c9af3048826638ab82

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Kanti ransomware	Kanti is sophisticated NIM-Based ransomware that is cunningly crafted to infiltrate systems and encrypt files, particularly those related to crypto wallets, with a particular focus on BTC (Bitcoin) users.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Information Theft and Financial Loss	Windows and Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	ce61f7dad5a1bb7ef8dedb6938b3e6f4fbd4bf991fdd62212578a92c9ae6dec1
SHA1	3775db152fdf754105ae0b5ced67897209d6203d
MD5	d8b6fe900e0a446d3ff44e967d358700

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
DeliveryCheck	DeliveryCheck (aka CAPIBAR, GAMEDAY), a .NET-based backdoor, targets Ukraine's defense sector, attributed to Russian actor Turla; it aims to exfiltrate Signal app data. Notably, it breaches Microsoft Exchange servers using PowerShell DSC for malicious activity.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Turla			-
IOC TYPE	**VALUE**		
MD5	cdf7fa901701ea1ef642aeb271c70361, 153b713b3c6e642f39993d65ab33c5f0, 9ececb4acbf692c2a8ea411f2e7dd006, 5c7466a177fcaad2ebab131a54c28fab		
SHA256	1c97f92a144ac17e35c0e40dc89e12211ef5a7d5eb8db57ab093987ae6f3b9dc, 5cf64f37fac74dc8f3dcb58831c3f2ce2b3cf522db448b40acdab254dd46cb3e, 07f9b090172535089eb62a175e5deaf95853fdfd4bcabf099619c60057d38c57, bd7dbaf91ba162b6623292ebcdd2768c5d87e518240fe8ca200a81e9c7f01d76		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
KAZUAR	A complicated multipurpose KAZUAR backdoor with over 40 features is loaded. The assaults involve the spread of a known Turla implant known as Kazuar, which is capable of stealing data from web browsers, application configuration files, and event logs.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Turla			-
IOC TYPE	**VALUE**		
MD5	11a289347b95aab157aa0efe4a59bf24		
SHA256	91dc8593ee573f3a07e9356e65e06aed58d8e74258313e3414a7de278b3b5233		

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-2021-40444	✗	Windows Server & Microsoft Internet Explorer	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	LokiBot (aka Loki PWS)
Microsoft MSHTML Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40444

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	Follina	Microsoft Windows	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	LokiBot (aka Loki PWS)
Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-78	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29298	✗	Adobe ColdFusion	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:coldfusion:-:*:*:*:*:*:*:*	-
Adobe ColdFusion Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-284	T1562: Impair Defenses, T1005: Data from Local System	https://helpx.adobe.com/security/products/coldfusion/apsb23-40.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38203	✗	Adobe ColdFusion	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:coldfusion:-:*:*:*:*:*:*:*	-
Adobe ColdFusion Arbitrary Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-502	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://helpx.adobe.com/security/products/coldfusion/apsb23-41.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29300		Adobe ColdFusion	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:coldfusion:-:*:*:*:*:*:*:*	-
Adobe ColdFusion Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-502	T1059: Command and Scripting Interpreter, T1574: Hijack Execution Flow	https://helpx.adobe.com/security/products/coldfusion/apsb23-40.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28121		WordPress WooCommerce Payments plugin version: 4.8.0 - 5.6.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:automattic:woocommerce_payments:*:*:*:*:*:*:wordpress:*:*	-
WordPress Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://www.wordfence.com/wordpress-plugins/woocommerce-payments/woocommerce-payments-561

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3519		Citrix NetScaler ADC and NetScaler Gateway	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:adc:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:gateway:*:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-0543		Debian-specific Redis Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:redis:redis:-:*:*:*:*:*:*:*	P2PInfect
Debian-specific Redis Server Lua Sandbox Escape Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://security-tracker.debian.org/tracker/CVE-2022-0543

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2017-0213</td><td>  </td><td rowspan="2">Microsoft Windows</td><td rowspan="2">Space Pirates (aka Webworm)</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*</td><td rowspan="2">Deed RAT, Voidoor, ShadowPad, and PlugX</td></tr>
<tr><td rowspan="2">Microsoft Windows Privilege Escalation Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-264</td><td>T1068: Exploitation for Privilege Escalation, T1204.001: Malicious Link,</td><td>https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0213</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
FIN8 (aka Syssphinx, ATK 113)	Unknown	Hospitality, Retail, Entertainment, Insurance, Technology, Chemicals, and Finance Sectors.	Worldwide
	MOTIVE		
	Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Sardonic backdoor and Noberus ransomware (aka BlackCat, ALPHV)	-

TTPs
T1055-Process Injection;T1070-Indicator Removal; T1070.004-File Deletion; T1497-Virtualization/Sandbox Evasion; T1010-Application Window Discovery; T1057-Process Discovery; T1082-System Information Discovery; T1083-File and Directory Discovery; T1518-Software Discovery; T1518.001-Security Software Discovery; T1573-Encrypted Channel; T1598-Phishing for Information; T1598.002-Spearphishing Attachment; T1059.001-PowerShell

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Turla(aka UAC-0003, IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear)	Russia	Defense	Ukraine and Eastern Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	DeliveryCheck (aka CAPIBAR, GAMEDAY), KAZUAR	Windows

TTPs
T1190:Exploit Public-Facing Application;T1059.001: PowerShell;T1059: Command and Scripting Interpreter;T1220: XSL Script Processing;T1005: Data from Local System;T1027: Obfuscated Files or Information;T1027.009: Embedded Payloads; T1567:Exfiltration Over Web Service;T1105:Ingress Tool Transfer;T1053:Scheduled Task/Job;T1053.005:Scheduled Task;T1546:Event Triggered Execution;T1566.001: Spearphishing Attachment;T1041:Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Space Pirates (aka Webworm)	China	Government, Educational Institutions, Private Security Companies, Aerospace Manufacturers, Agricultural Producers, Defense, Energy, and Infosec Companies	Georgia, Mongolia, Russia, Serbia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2017-0213	Deed RAT, Voidoor, ShadowPad, and PlugX	Microsoft Windows

TTPs

T1595:Active Scanning; T1595.002:Vulnerability Scanning; T1566.001:Spearphishing Attachment; T1566.002:Spearphishing Link; T1059.003:Windows Command Shell; T1059.005:Visual Basic; T1053.002:At; T1053.005:Scheduled Task; T1106:Native API; T1036.004:Masquerade Task or Service; T1036.005:Match Legitimate Name or Location; T1197:BITS Jobs; T1569:System Services; T1569.002:Service Execution; T1543:Create or Modify System Process; T1543.003:Windows Service; T1546:Event Triggered Execution; T1546.015:Component Object Model Hijacking; T1547:Boot or Logon Autostart Execution; T1547.001:Registry Run Keys /Startup Folder; T1548:Abuse Elevation Control Mechanism; T1548.002:Bypass User Account Control; T1068:Exploitation for Privilege Escalation; T1027:Obfuscated Files or Information; T1027.001:Binary Padding; T1027.002:Software Packing; T1036:Masquerading; T1055:Process Injection; T1055.001:Dynamic-link Library Injection; T1078:Valid Accounts; T1078.002:Domain Accounts; T1112:Modify Registry; T1140:Deobfuscate/Decode Files or Information; T1218:System Binary Proxy Execution; T1218.011:Rundll32; T1553:Subvert Trust Controls; T1553.002:Code Signing; T1572:Protocol Tunneling; T1571:Non-Standard Port; T1090.001:Internal Proxy; T1105:Ingress Tool Transfer; T1564.001:Hidden Files and:Directories; T1574:Hijack Execution Flow; T1574.002:DLL Side-Loading; T1620:Reflective Code:Loading; T1555:Credentials from Password Stores; T1555.003:Credentials from Web Browsers; T1095:Non-Application Layer Protocol; T1003.001:LSASS Memory; T1040:Network Sniffing; T1102.002:Bidirectional Communication; T1087.001:Local Account; T1087.002:Domain Account; T1082:System Information Discovery; T1614.001:System Language Discovery; T1016:System Network:Configuration Discovery; T1069.002:Domain Groups; T1083:File and Directory Discovery; T1033:System Owner/User Discovery; T1057:Process Discovery; T1021.002:SMB/Windows Admin Shares; T1119:Automated Collection; T1560.001:Archive via Utility; T1056.001:Keylogging; T1071.001:Web Protocols; T1071.004:DNS; T1132.001:Standard Encoding; T1573.001:Symmetric Cryptography; T1008:Fallback Channels

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actor **FIN8, Space Pirates, Turla** and **LokiBot, Sardonic backdoor, Noberus ransomware, P2PInfect, Deed RAT, Voidoor, ShadowPad, PlugX, Kanti ransomware, DeliveryCheck,** and **KAZUAR** 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 **nine exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **FIN8, Space Pirates, Turla** and **LokiBot, Sardonic backdoor, Noberus ransomware, P2PInfect, Deed RAT, Voidoor, ShadowPad, PlugX, Kanti ransomware, DeliveryCheck,** and **KAZUAR** in Breach and Attack Simulation(BAS).

Threat Advisories

LokiBot Data Exfiltrating Trojan Targets Windows Systems

Active Exploitation of Adobe ColdFusion Critical Vulnerabilities

Hackers Target WooCommerce Payments Plugin to Hijack Websites

FIN8 Strikes with Noberus Ransomware via Altered Sardonic Backdoor

Citrix Netscaler ADC and Gateway Vulnerabilities Exploited in the Wild

A New Cross-Platform ‘P2PInfect’ Worm Threatening Cloud Environments

A Deep Dive into Space Pirates' Unconventional Cyber Arsenal

Kanti Ransomware Strikes Cryptocurrency Users

Turla Exploits Ukraine's Defense Sector with DeliveryCheck Backdoor

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
LokiBot	SHA256	127c29b65ebf2143b66e5c60fcdbae43c4789c836e273e4f996efd0e56040e8f, 30c51845ddd526bf0472c52af64b591baee970f2ab39bec2d6bea1a64b5c7f9b, 7559e6ca8b77400f88bf4e67208a1c32570a670068eccae9e3d226cc5471bd47, 9346d441c3136edb70bc96afd06717fbb96074592bcb4896741ede01be7925ed, 61868e99c4fff04df6ba82cbd4eb414c132c5932acd762f379b4c0fe852968bf, 73ca91a52ed319db604f0951f4b95ebd4a93eabc6f410e3d7f7ffd33efa29982, cabcb0bfd5b86be43f98e9ea8dcb92e8ef87d1c98e326b2effa2d39482bb882a, b0504206461bb3a04bc80d299501c2d2765f097bc621a0e86e5b9e889f383287, 42ed620528c450c61185a065b7e73c5d8207c731acb7bf965df2a49c030de497, 42ed620528c450c61185a065b7e73c5d8207c731acb7bf965df2a49c030de497, 73ca91a52ed319db604f0951f4b95ebd4a93eabc6f410e3d7f7ffd33efa29982, a65903f3968b96768cd2ca31af342c23b7f8c8b0d928b6a7f9119c80f105b3ee, 24e91c3b0d477625a70c71ea05ad7e6ce3dd9582567bb7c33ed6ff537915490c, 24e91c3b0d477625a70c71ea05ad7e6ce3dd9582567bb7c33ed6ff537915490c,

Attack Name	TYPE	VALUE
LokiBot	SHA256	3d87812ab5871d3d39ee5989e5ea9f531061bb2366197b929c42889e4377a87f, a452e58b0a7862c490e028e3a9cab9d5b33a6bd34b4e86e1385333e60717fa02, 0d31edaf7d6a20a6a50e9b8b66592d6a18f23466ed54a9b63768afbbb84140ff, 647a55bbed92a840ad9b1b6b1fa8898927310dc81d39e5ca9f223c3f7f315cb6, ddf9208f37a6707462c99f48495752554a13df724120887df88fbc9d2bf75ba0, 578153b3c97aeb8bee7d4c75e6fadc389575385968df4fd4f39f71871f7ed1f8, 4e51f0616df48153ae9a76dec9a194ba7710d13a419e3eb7b8e845832a41540d, f03390fa3307e28389f6581e930065b810892ddb2cd0b12f59ccf896e1852681, f03390fa3307e28389f6581e930065b810892ddb2cd0b12f59ccf896e1852681, 3f2261e0d78987287c17b70aee3541edf714bcca93bea5f66872bea7d872f790, 3b492c5191fbeeff74cbaa092bca97936135c165ac2919b506004eabfcf92e150, d5275100a4f01bfdc9c99ea76177b80b5257185a255c762bd98665e243620d12, ac176f2b29fb8ee6af988681a8fd5a6eecbef64c7e6a301a00ce925b4f1e431b, 96a5aac25dc29322b45abee014e3dbfcb30e4b14150c1c4e13872904d4739ed0, ff36e05a76e31b8c32297d4e98f745a3e5d1d9beba9fdb455935e4302e0f2e57, 75ea332096b6ae8eabc2c398d2cd97f3f119591b39b16ce7c96953d4ebfcc63b, 099b16630e07d02d34a717dd001cdfac0023c7847cc3e5aab9933b4861138395, 2c8b9e7e30951113a55140552f9c3aaebb7c7e4a11624b5c948d5a64d9a89f3b, 121bea26acd46a7ce020d48ea79216f4119474fb6dd9895baf1d9dfdf6dc8fcd, 121bea26acd46a7ce020d48ea79216f4119474fb6dd9895baf1d9dfdf6dc8fcd, 7704a4a10e786469680636e849feffba29379edf93a1feabf0798e6683e2eb60, cdc818a75fd935601dc318e97046858d96fd92e2b1547794450a35541540aee3, d04b4aee3b062e68e9c35402495cf1d40ded53c7dadcdb35590640342932170c, 567e8970d27c1e43b55c0156c957f71fb553282709237cc73bbeb6bd518edbc7,

Attack Name	TYPE	VALUE
LokiBot	SHA256	ea5a585a8b9e9223d5d6d66c78615c795bab186c681b04f11e7901dae8d79bfd, f15f539c0ae209595dc2256318091681aa7852d4f88b2c6ab8e0d1f1dc1f1e91, ea87aab944e82b6711433894358556b563fa27e0d99b06febdba8d1a5c7dde0e, 827555c608d1e12973d7c28d45b4ca8d5342d1dc77b12a5d403a32d83e591fb8, 5a7a9170adc2fe2a4167392be4532c945faef7a2d0f9a18d79cf9d9cb459d61a, bd32a9cbb3ed1a616bf91d7121386a78cf6bb2b8c904088d1daa3982edb4fb8b, bd32a9cbb3ed1a616bf91d7121386a78cf6bb2b8c904088d1daa3982edb4fb8b, c98512ee509dca89b8f6073faf337cda879e39f669add3632011590411878c9a, 2af1bb0bba5a26df1520604cbf7e84bf8bd19d4f9f23167b3408c78b545b7190, 4e49637ce52ae9105d53e9de9994e680ba5894f25ffffbc2272e9d95c0adfbf1, 9f54a66ad8152ec7b3923d98a8261ba15d643dc241cdf995e5332bcf4b91eb0a, 59bfe87a4f70ad80b96e5d135d9688324b18009f800b7001c6efa116fb780d2f,
Noberus ransomware	SHA256	029dde7c2ec880fb3d3e95e6a8376739b4bc46a0ce24012e064b904e6ecb672c, 72f0981f18b969db2781e874d249d8003c07f99786e217f84cf54a148de259cc
Deed RAT	SHA256	b6860214fcc1ef17937e82b1333672afa5fcf1c1b394a0c7c0447357477fe7c9, 212f750a1d38921b83e68e142ee4ae1c7b612bf11c99210da60775f17c85a83e, 6cfa8ce876c09f7e24af17bbe9baa97f089e9bf478a47d18417e399e64a18d40, b7bb9b41298420d681d1a79765d7afb7ecf05d6f0baf0b29a07b8b1af20a8c97, f554ff7eb069f0ea5ebc49e015bde1e88d4cf83f6df21e4de2056716e83fedc6, 7ee776272f7c51e41e10f5ffbd55c8c24ddb332e8c376e132e5a8cb72abd7397, ece771ab5ae8372078c378fa0cf0a1ac055ea5cbe6091f890185c02caf0edc19, 5c7f727c852819ae60182c4406c233f5b86962c1da3b933953058985d9f90722,

Attack Name	TYPE	VALUE
Deed RAT	SHA256	ceca49486dd7e5cf8af7b8f297d87efe65aba69124a3b61255c6f4a099c4a2ab, 4f84f4333dc9c42ae4ed55c4550ebb14c8079235ae7de9fef4191251537454fc, 8c3e0fdddc2c53cf7961f770080e96332592c847839ccf84c280da555456baf0, 85d190304accb34422d3e1d603c33b86b6b8c4e88cc4713b0e0c6d4fdee9d93e, a3df5eb54f0a77cb52beccf1b2aa2caa427f80fcd047fc6be4c7aa849649e1b5, f9e97776826f83278c63cda59910c49920b7316433d9d95570dd187e154fed0b, 74ac74ea85118fe3686f9d6774de2d63db7870dadb4f0ba0d119a77d6c11323a, 057a16008ce50c3d02c910eac697748eb157afb8a6e8573adefa4b75b495a778, 66bca22ba5fbd01758fde8e57e1e251191cd1c7bb599f0beb8dd0ffd661464ac, 10d122833af8b8fec97ebdd843942bfc2bf237e3b8c01ae9f852eaca2e9cddc7, f0b8bf55a3e23379aefd9a95c556430e073ad206b4c39e0086f0a17d00ae64fe, 8a3aefd75501137f601d4b802959fb50b7cba2b135ce2ab2f1f5fa65b1a86159, 3a1e67006fb1e761e0188a04361cb7a57329346e7d0a78ef909fbc5469e3c08b, e88c7dd128c456a34804a36459f32cdf97fe30a5642caa3072ff31cda07f29e2, a2d7255cf7c8710cdec62c01b3e2c9d22600441b20914d73eb8f8af3245a9806, bfa3c91767c333a97d6849a3f885f4ed2205f24882bffbbfc916624b2601a9b7, 241d1ab6a0da9dfcbc9c565d1ff948743cd7673ed334e5906a1428055cab6c82, c8c3b639c6e880d7e01cba8cb019087f0c4d2cf4dcdfa712a18054b78e525a47, 5e712e78736bde2d3ed507fb730be3a9d55d2b4ee3f7ff827f961fcada4e4e0b, ef17d44cde003c17c28137c6d4692eb4a1b42f86e5d6995f2f06a05e363f044a, 42ef77391f20ffc1751ded79da25376bc20a007d03e501049fff37f781df5403, cae7622a5f1ed791d317db0b3bc791a8ab71a9c68837282435f5db6bab540615, 2707602481a025da29438d01e894cfc9742389d419a5b08aa96ddc76bde38cba,

Attack Name	TYPE	VALUE
Deed RAT	SHA256	5311e4fd3329945496962c6417b74da919f5e50ae20ba7ab0d5983012c956f4b, dc3c1df20d73a62e8219ed6193ecf1229845dd0a6e42d32eb11cbaee04cfa7df, 70e43da5c5b6a8cfea8fcad768a2e5cfdf532b49b5ac87ec8ca9d05d83e0e915, 1473fcf2297376a819b6cccd50dc709fb61f48f70dc9a0eaff741c893b33d670, 67f7faf0161fdac7ebb619a2aa0c73a4a08def05d7752dfdd698d24410d9989e, 7c11eecc2fef6a2ad2e5d80156946d7bdcb9c345d542781c3116141f10eb490f, e2735841dd8ae66a825182d6d06629821c49aca44357e5980c3bfb97ace7ebf0, 374fff9a48949254d72bfe34b9b62129da1cfafb74623d187791ada09d976e7d, c4e023110216481d0ccb09787ccc5ea46879fdf331f5d2fda2b1f33719a35104
	MD5	972a1a6f17756da29d55a84d7f3f23a4, 51ca39e3700e9ed16d90302dd31f3a1d, b0b438bcb2a71233721a2ddcdb765a68, 0fa4a2b8210500427bb23d2d92502964, 804824203f31ebfb56e580e73e932d26, 38c43e589e3dc65258322d91b58e2e15, ef6264abe296357100e2db48820b13f6, 24ec73b4e1845088a28dde0007c2d6bd, d217fe96c7737ac318321deafc4cd261, 633ccb76bd17281d5288f3a5e03277a0, 77ef4bc2f23ef97add7ec0ad229396a4, 8002cd74e579a44a78b2c8e66f8f08a4, d4e51120c368ee4ef5f5571756803fd3, 66e8f82a418923b92bef57ad61bcebf3, fb23fc47484150250cfd7b1260e23524, 99b86ad9bf6193b044076df373534fad, 4db33e5390bfebd84e38cbb85b75c006, dbb5995037745e04d03dc7f2985f017f, a94277fad94ca6fbdb2b8eeb716bac90, 7aa890406a74a44f17fe665653bd92e2, 9faf04fc6e522050527e71dea5918d01, 1a04af6c3abe8f67bf98adc588c46736, 6d52d0e7f49817c6315b308cb973d405, 8e3217391e11cabf6f9a62a35c636835, 97c00cee887279f12f309a86e7bc3638, 5d0aa944ce19e0a70adad562ce0e7880,

Attack Name	TYPE	VALUE
Deed RAT	MD5	1d07e53969cd1cb34db944bfdfa5bf6f, 81a93165b338dd5ebb59841e199e0460, a2221a72d42b978c0f295557a100d574, c1be341ffc0f58bafdf4e5210b881106, 9a6b1bd3b7f13d30d1595b874f513744, ab6a57e40ba74135de9fc6b8f37efa7b, 7949b560ecf60644e2b537199589d67b, 81de205ac5e44e1167c0c01c7207c6c4, 4fdb78de4da91c06e5778feb560750f4, 2ec55245fbe57cae1a045f9106ca709a, ffc18496b2b1563e081beefc9e884769, ef4d35b1780cb1799eadb648f4e7b5b5, 01b596051d1fa4785ef4e73dc3f08ec0, 54c7f04fc5418553812910db8adc6995, 824fbfa8b35f19152a834a1bfff9ef54
	SHA1	3f8ee1e875cbb01e145a09db7d857b6be22bdd92, f99f5f397fe1abb3fc25cc99fe95952fe24b6123, 1fb924ec4f0ab73a952f2a3cb624b94933275d1b, 2910415d483972cc17c76548e2b2aa5afd5bc59a, 067ca2d961b913cb2e6d6aaa92595345125d6683, 1a6e675d82e67cc41493ff991f99da70316848c4, c055f30523028037f51cc62d25ce6d38334a531e, 2404ac00114cd2481099c52b879e1776dedb2d24, ced02716f59a9a70c37eaf373c42796e6f3e93b0, e986b238cb5fe037718172d965a41c12c85bbdd0, 59239f73996a3f5a6260228cf7ca3c01e3a00822, 84ca568879ca62448d035d56bec816a11188b831, ac499c86012858f40eb78ecf3bcefae779527d73, 99cc3349b64188aae1c986afbcee7e776aa4b349, 30ad2f4a758ab2c526b6439772c7cd7cee66ffc4, 0d0c026a1661923cd184b6d0fde647128be75488, 20c83bcfd9fb45a8ba5922dbefb74d47cb361db7, e50dc750e7697ba5e28d6dde12e9a4d370076c0c, 491248fdf1141e81d5ff23eb1e44d58b50339fe2, c58d5d36201cee88a01c9913d771723edde302e4, 0912822548e5983f8a2b6d77848994f6d929ffed, af71956b59b9c05acdcd7badecc232ca6237cc8d, bfe05003730d79f0004cc41e09f48944df6f68fe, 19da36d73e0a72f65c8a9f6fc2e2504ed599b57d, 6e0c406d07206b588652729a271e054c416b5c90, 338881ff10434b523feb63a8a66370f444378cc7, f4a5778b74b73745a533f22d33a65880f2968705, 57792f875625fec78bea22af46010bd34dff863a,

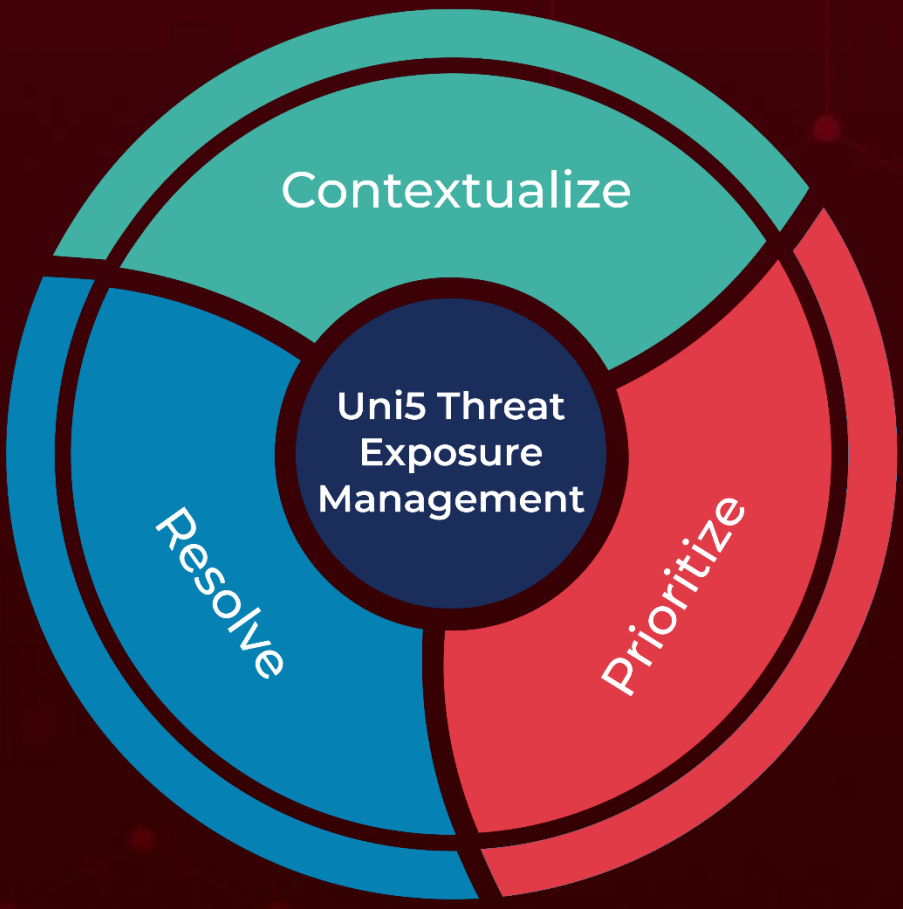
Attack Name	TYPE	VALUE
Deed RAT	SHA1	a7de9de3774ad507e7d1ddfcce4924625a600434, 493e89a70c4176dcec50f34b79eaa4f910e50800, ab64d32da52a1e516b0c874aad006db404f9c21e, a3225a0bbb66b5babf52466ae23a1538407f0cef, c5c844582c0590cdc901c253a121568251154c61, e49d21f1e66268715efc6003c4e2d3b98cee666a, 28ed17b046e0bed3d1cde67eccf241ecf01fe3c4, aa42f3758dc599e6184894a2911e774c2e16b92d, 57b138f2bb4731b1c50a034aff3013bce735267c, f95deea8d824ee681341f9457e0a86129ec4eb91, a24d306d0ed0061485cb05901cf9fc9d5f07c097, c321233155af13a53ecd746eaab84cc6ac69d510, 6f8cc7abbf3185a085aa43186c5da332b04c3156,
Voidoor	SHA256	86c17c549433223f3b59f5ee3e4f2694ebf4e6aabd66508a9a6fec1bdf830c61
	SHA1	1749f99443b345860dd037940505421c45156950
	MD5	48097e614cdf1f9c908b7449cd1119c5
PlugX	SHA256	22c6d07b64d40811ef31113faac7293348845ab6a06f7319a653ca694c26e94a, 8c8f9fd17d1c28b471bcc4c870ab53a3b4b260ae2fd123b0ef2a2a819ce1cc78
	SHA1	A8808089c37faacebc19bafd2677ba011afffc49, 154da55173f97c50e41e48157bc94515cc6146ec
	MD5	3cf999dd950af82cad3f8c6eb5430bd5, 6d3ce5d4003ce4c9af3048826638ab82
Kanti Ransomware	SHA256	ce61f7dad5a1bb7ef8dedb6938b3e6f4fbd4bf991fdd62212578a92c9ae6dec1
	SHA1	5db152fdf754105ae0b5ced67897209d6203d
	MD5	8b6fe900e0a446d3ff44e967d358700
Sardonic backdoor	SHA256	1d3e573d432ef094fba33f615aa0564feffa99853af77e10367f54dc6df95509, 5b8b732d0bb708aa51ac7f8a4ff5ca5ea99a84112b8b22d13674da7a8ca18c28
	IPv4	37.10.71[.]215
	Domains	api-cdn[.]net, git-api[.]com, api-cdnw5[.]net, 104-168-237-21.sslip[.]io

Attack Name	TYPE	VALUE
P2PInfect	SHA256	88601359222a47671ea6f010a670a35347214d8592bceaf9d2e8d1b303fe26d7, b1fab9d92a29ca7e8c0b0c4c45f759adf69b7387da9aebb1d1e90ea9ab7de76c, 68eaccf15a96fdc9a4961daffec5e42878b5924c3c72d6e7d7a9b143ba2bbfa9, 89be7d1d2526c22f127c9351c0b9eafccd811e617939e029b757db66dadC8f93
ShadowPad	SHA256	3ce38a2fc896b75c2f605c135297c4e0cddc9d93fc5b53fe0b92360781b5b94e, 210934a2cc59e1f5af39aa5a18aae1d8c5da95d1a8f34c9cfc3ab42ecd37ac92
DeliveryCheck	MD5	cdf7fa901701ea1ef642aeb271c70361, 153b713b3c6e642f39993d65ab33c5f0, 9ececb4acbf692c2a8ea411f2e7dd006, 5c7466a177fcaad2ebab131a54c28fab
	SHA256	1c97f92a144ac17e35c0e40dc89e12211ef5a7d5eb8db57ab093987ae6f3b9dc, 5cf64f37fac74dc8f3dcb58831c3f2ce2b3cf522db448b40acdab254dd46cb3e, 07f9b090172535089eb62a175e5deaf95853fdfd4bcabf099619c60057d38c57, bd7dbaf91ba162b6623292ebcdd2768c5d87e518240fe8ca200a81e9c7f01d76
KAZUAR	SHA256	ce61f7dad5a1bb7ef8dedb6938b3e6f4fbd4bf991fdd62212578a92c9ae6dec1
	SHA1	3775db152fdf754105ae0b5ced67897209d6203d
	MD5	d8b6fe900e0a446d3ff44e967d358700

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

July 24, 2023 • 9:00 AM

More at www.hivepro.com