Date of Publication
September 25, 2023

Hive Pro®

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

18 to 24 SEPTEMBER 2023

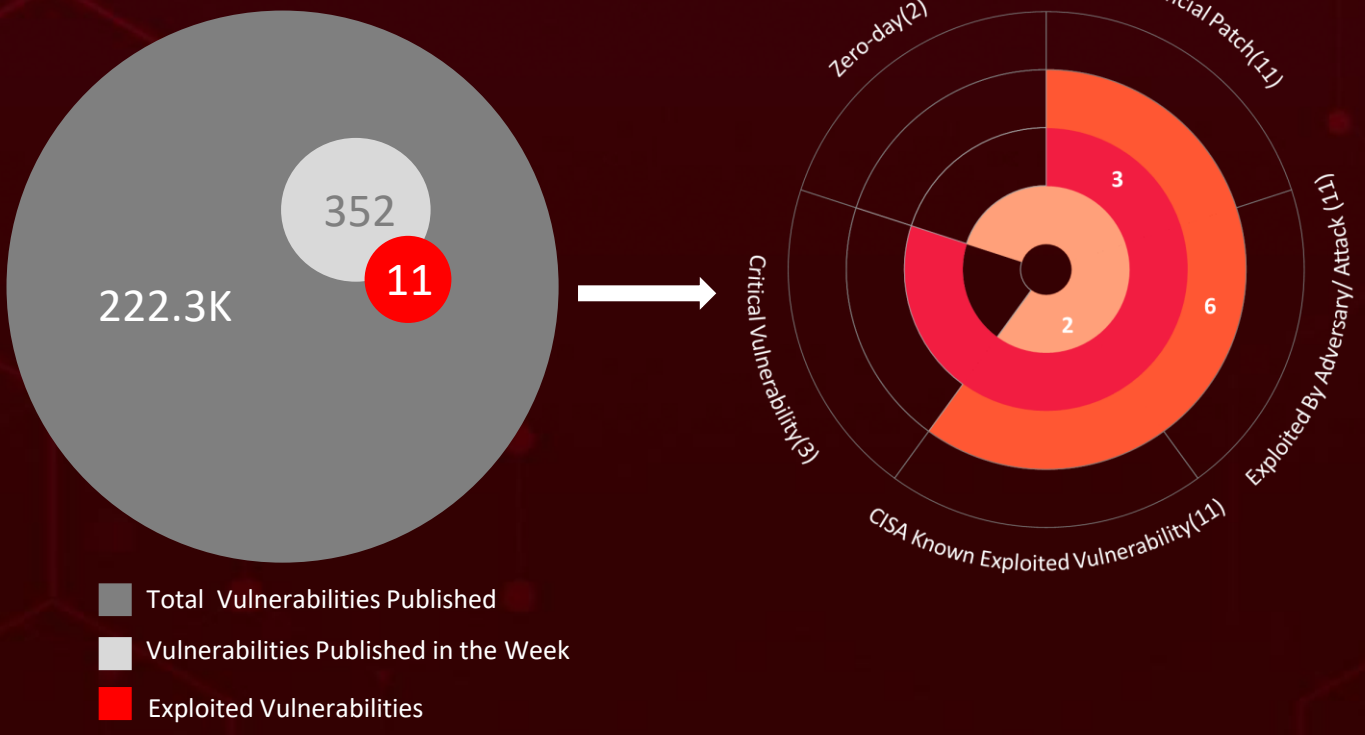
Table Of Contents

Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **eight** executed attacks, **five** instance of adversary activity, and **eleven** vulnerabilities including two zero-day vulnerabilities highlighting the ever-present danger of cyber attacks.

Furthermore, HiveForce Labs uncovered a modular RAT **ShadowPad** targeting critical infrastructure in Asia, successfully compromising a national grid for a duration of six months.

Meanwhile, **Earth Lusca** is a China-based threat actor, is back in action in 2023. They use the SprySOCKS backdoor to target government departments in foreign affairs, technology, and telecommunications. These observed attacks have been on the rise, posing a significant threat to users worldwide.



High Level Statistics

8
Attacks Executed

11
Vulnerabilities Exploited

5
Adversaries in Action

- ShadowPad
- Packerloader
- HTTPSnoop
- PipeSnoop
- SprySOCKS backdoor
- VenomRAT
- Snatch ransomware
- LuaDream

- CVE-2022-47966
- CVE-2022-26134
- CVE-2023-41179
- CVE-2022-40684
- CVE-2021-22205
- CVE-2019-18935
- CVE-2019-9670
- CVE-2021-34473
- CVE-2021-34523
- CVE-2021-31207
- CVE-2023-3932

- APT33
- Redfly
- ShroudedSnooper
- Earth Lusca
- Sandman APT

Insights

APT 33

Using Password Spray Campaigns to Infiltrate Organizations

Redfly

An espionage group, targets critical infrastructure in Asia with ShadowPad trojan

Nagios XI

Multiple Critical Security Vulnerabilities Uncovered in Nagios XI monitoring software

Snatch ransomware

A RaaS variant is known for its ability to reboot devices into Safe Mode, where many security protections are disabled, before encrypting files.

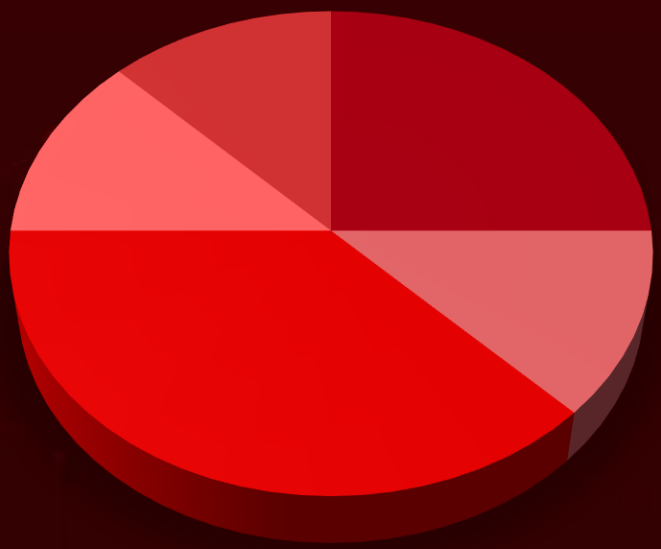
Sandman APT

An espionage group of unknown origins targeting the Telecommunication sector with the LuaDream backdoor

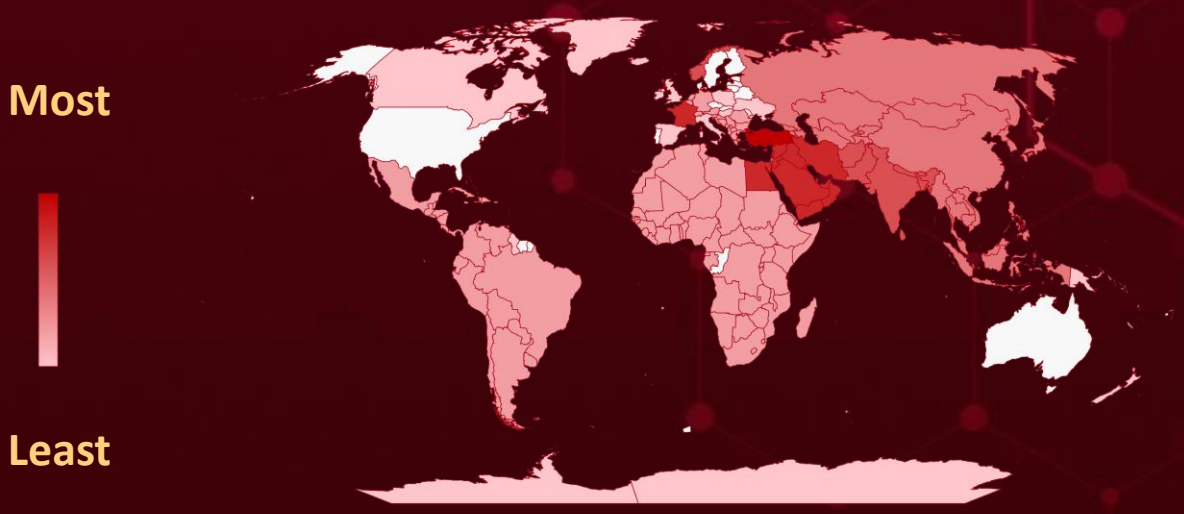
Trend Micro Zero Day Exploited

CVE-2023-41179 identified in the third-party AV uninstaller module

Threat Distribution



Targeted Countries



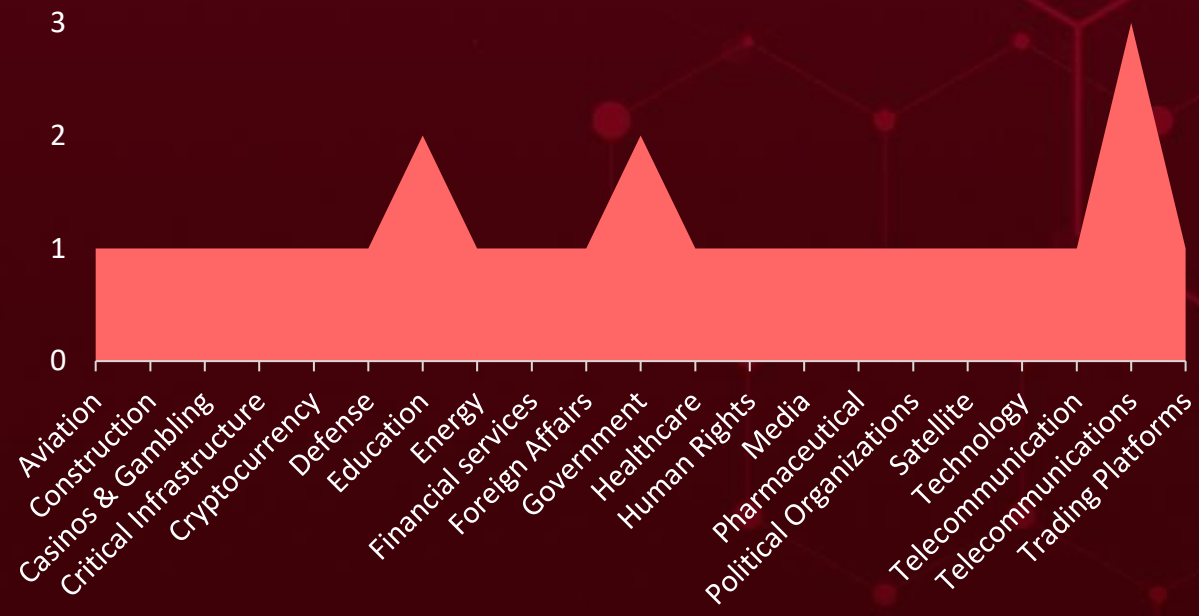
Countries
Turkey
United Arab Emirates
Palestine
Yemen
Cyprus
Saudi Arabia
Egypt
Kuwait
France
Oman
Iran
Qatar
Iraq
Bahrain
Syria
Israel
Jordan
Lebanon
Sri Lanka
Nepal
Maldives
Afghanistan

Countries
Pakistan
Bangladesh
India
Bhutan
Norway
Azerbaijan
Hong Kong
Georgia
Macao
China
Malaysia
South Korea
Japan
Tajikistan
Mongolia
Kyrgyzstan
Myanmar
Russia
Brunei
Singapore
North Korea
Cambodia
Vietnam
Taiwan
Indonesia
Thailand

Countries
Kazakhstan
Turkmenistan
East Timor
Uzbekistan
Philippines
Armenia
Akrotiri and Dhekelia
Seychelles
Djibouti
Togo
Haiti
Ecuador
Honduras
Eswatini
Bosnia and Herzegovina
Venezuela
Botswana
Paraguay
Brazil
São Tomé and Príncipe
Austria

Countries
Bulgaria
Albania
Burkina Faso
Somalia
Uganda
Ivory Coast
Zambia
Burundi
DR Congo
Algeria
Belgium
Cameroon
Benin
Kenya
Senegal
Kosovo
Equatorial Guinea
Cape Verde
Eritrea
Central African Republic
Switzerland
Zimbabwe
Tanzania
Chad

Targeted Industries



TOP MITRE ATT&CK TTPS

T1083 File and Directory Discovery	**T1059** Command and Scripting Interpreter	**T1057** Process Discovery	**T1027** Obfuscated Files or Information	**T1566** Phishing
T1203 Exploitation for Client Execution	**T1110** Brute Force	**T1573** Encrypted Channel	**T1497** Virtualization/ Sandbox Evasion	**T1588** Obtain Capabilities
T1053 Scheduled Task/Job	**T1012** Query Registry	**T1070.004** File Deletion	**T1486** Data Encrypted for Impact	**T1105** Ingress Tool Transfer
T1005 Data from Local System	**T1059.001** PowerShell	**T1588.005** Exploits	**T1140** Deobfuscate/ Decode Files or Information	**T1574.002** DLL Side-Loading

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ShadowPad	ShadowPad is a sophisticated modular trojan malware that has been used for cyber espionage campaigns since at least 2015. It is believed to be the successor to the PlugX malware platform, and is known to be used by a number of Chinese state-sponsored threat groups, including Redfly.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Modular RAT		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Redfly			-
IOC TYPE	**VALUE**		
SHA256	656582bf82205ac3e10b46cbbcf8abb56dd67092459093f35ce8daa64f379a2c ac6938e03f2a076152ee4ce23a39a0bfcd676e4f0b031574d442b6e2df532646 231d21ceefd5c70aa952e8a21523dfe6b5aae9ae6e2b71a0cdbe4e5430b4f5b3 d9438cd2cdc83e8efad7b0c9a825466efea709335b63d6181dfdc57fb1f4a4e3		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Packerloader	Packerloader is a sophisticated malware loader that evades detection by decrypting and executing a payload file, often running it directly from memory for added stealth.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	32d709d8d41e4ede6861ce27c9e2bb86d83be8336b45a17f567bab1869c6600a		

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
HTTPSnoop	HTTPSnoop malware is a backdoor that enables threat actors to listen to incoming requests for specific URLs and execute that content on the infected endpoint. HTTPSnoop uses low-level Windows APIs to monitor HTTP(S) traffic on an infected device for specific URLs	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft, Disruption of operations	-
ASSOCIATED ACTOR			**PATCH LINK**
ShroudedSnooper			-
IOC TYPE	**VALUE**		
SHA256	1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb, 7495c1ea421063845eb8f4599a1c17c105f700ca0671ca874c5aa5aef3764c1c, 3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7, 04cf425e57e7d511f03189749c8c0a95483eeeb4c423e9ee1a6a766d2fe0094c, c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PipeSnoop	PipeSnoop malware is a backdoor that enables threat actors to execute arbitrary shellcode on an infected endpoint through Windows IPC (Inter-Process Communication) pipes. It was first discovered in 2023 and has been used to target telecommunications service providers in the Middle East.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft, Disruption of operations	Windows
ASSOCIATED ACTOR			**PATCH LINK**
ShroudedSnooper			-
IOC TYPE	**VALUE**		
SHA256	e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d, 9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0ceb		

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>SprySOCKS Backdoor</td><td rowspan="6">SprySOCKS is a Linux-targeted backdoor malware that was first observed in September 2023. It is believed to be the work of the China-linked threat actor group Earth Lusca, which has been targeting government agencies and other organizations around the world since at least 2021.</td><td>Exploiting CVEs</td><td>CVE-2022-40684
CVE-2021-22205
CVE-2019-18935
CVE-2019-9670
CVE-2021-34473
CVE-2021-34523
CVE-2021-31207</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Backdoor</td><td rowspan="3">Data Steal and compromised systems</td><td>FortiOS, FortiProxy, FortiSwitchManager, GitLab CE/EE, TELERIK.WEB.UI.DLL, Zimbra Collaboration Suite, Microsoft Exchange Server, Confluence Server and Confluence Data Center</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Earth Lusca</td><td>https://fortiguard.com/psirt/FG-IR-22-377; https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json; https://www.telerik.com/support/kb/aspnet-ajax/details/allows-javascriptserializer-deserialization; https://wiki.zimbra.com/wiki/Security_Center; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">6f84b54c81d29cb6ff52ce66426b180ad0a3b907e2ef1117a30e95f2dc9959fc, f8ba9179d8f34e2643ee4f8bc51c8af046e3762508a005a2d961154f639b2912, eebd75ae0cb2b52b71890f84e92405ac30407c7a3fe37334c272fd2ab03dff58</td></tr>
<tr><td>Domains</td><td colspan="3">lt76ux.confenos[.]shop, 2e6veme8xs.bmssystemg188[.]us</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
VenomRAT	VenomRAT is a remote access trojan (RAT) malware that is used to steal data and take control of infected devices. It is a highly sophisticated malware that is difficult to detect and remove.	Phishing emails	CVE-2023-25157 CVE-2023-40477
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://github.com/geoserver/geoserver/commit/145a8af798590288d270b240235e89c8f0b62e1d; https://www.winrar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa
IOC TYPE	**VALUE**		
SHA256	79b87d7accc9cbd1414b72ca13c48a385be9cb06c1bb53d845e94107b579bf62, 4b84283c40560991da34ef2b465a4724facd0932acebff60466d8d5ff1916bd5, 75c12ccacd764101736b213981355b39056227929214c8963e9bf3ea5a60f6ef, 1648bea3c1c3b00e7f9c9bf7f65be833fa7f291f0e05a342382e9e36f0350c60, b23e4ea87917a517565de8471a101ab55c2a31186c8a23e9e8af71b359d35aa9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Snatch ransomware	Snatch ransomware is a ransomware-as-a-service (RaaS) variant that was first discovered in 2018. It is known for its ability to reboot devices into Safe Mode, where many security protections are disabled, before encrypting files.	Ransomware-as-a-service	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f, 1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d, 5950b4e27554585123d7fca44e83169375c6001201e3bf26e57d079437e70bd, 7018240d67fd11847c7f9737eaaae45794b37a5c27ffd02beaacaf6ae13352b3, 28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd76b8c4acff7c		

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>LuaDream</td><td rowspan="5">LuaDream is a sophisticated malware that is difficult to detect and remove. It is written in Lua, a lightweight programming language that is not commonly used for malware development.</td><td>Phishing emails</td><td>-</td></tr>
<tr><td>TYPE</td><td rowspan="3">IMPACT</td><td rowspan="2">AFFECTED PRODUCTS</td></tr>
<tr><td>Infostealer</td></tr>
<tr><td rowspan="2">ASSOCIATED ACTOR</td><td rowspan="3">Data Theft and Financial loss</td><td>-</td></tr>
<tr><td>Sandman APT</td><td rowspan="2">PATCH LINK</td></tr>
<tr><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA1</td><td colspan="3">1cd0a3dd6354a3d4a29226f5580f8a51ec3837d4,
27894955aaf082a606337ebe29d263263be52154,
5302c39764922f17e4bc14f589fa45408f8a5089,
77e00e3067f23df10196412f231e80cec41c5253,
b9ea189e2420a29978e4dc73d8d2fd801f6a0db2</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-2022-47966	✗	Multiple products of Zoho ManageEngine	APT 33
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_access_manager_plus:*:*:*:*:*:*:*:*	-
Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-26134	✗	Confluence Server and Confluence Data Center	APT 33
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*	-
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-917	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.atlassian.com/software/confluence/download-archives

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41179	✗	Trend Micro Apex One OnPremise (2019) Trend Micro Apex One as a Service Worry-Free Business Security 10.0 SP1 Worry-Free Business Security Services (SaaS)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:trend_micro:apex_one:CP_12033:*:*:*:*:*:*:*	-
Trend Micro Arbitrary Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-78	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://success.trendmicro.com/dcx/s/solution/000294994/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-40684	✗	FortiOS, FortiProxy, and FortiSwitchManager	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*	SprySOCKS Backdoor
Fortinet Multiple Products Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1556: Modify Authentication Process	https://fortiguard.com/psirt/FG-IR-22-377

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22205		GitLab CE/EE	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:*	SprySOCKS Backdoor
GitLab Community and Enterprise Editions Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-18935		TELERIK.WEB.UI.DL	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:telerik:ui_for_asp.net_ajax:*:*:*:*:*:*:*:*	SprySOCKS Backdoor
Progress Telerik UI for ASP.NET AJAX Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	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-2019-9670		Zimbra Collaboration Suite v8.5 to v8.7.11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*:*:*	SprySOCKS Backdoor
Synacor Zimbra Collaboration (ZCS) Improper Restriction of XML External Entity Reference			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-611	T1068: Exploitation for Privilege Escalation	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34473		Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*	SprySOCKS Backdoor
Microsoft Exchange Server Remote Code Execution Vulnerability (PROXYSHELL)			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34523		Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*	SprySOCKS Backdoor
Microsoft Exchange Server Privilege Escalation Vulnerability (PROXYSHELL)			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1068: Exploitation for Privilege Escalation	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-31207		Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2019 Cumulative Update 9 15.02.0858.005	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*	SprySOCKS Backdoor
Microsoft Exchange Server Security Feature Bypass Vulnerability (PROXYSHELL)			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-787	T1556: Modify Authentication Process	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-3932</td><td>✗</td><td rowspan="2">GitLab Enterprise Edition (EE) starting from 13.12 and prior to 16.2.7 as well as from 16.3 and before 16.3.4</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">GitLab Pipeline Execution Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-862</td><td>T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution</td><td>https://about.gitlab.com/releases/2023/09/18/security-release-gitlab-16-3-4-released/#attacker-can-abuse-scan-execution-policies-to-run-pipelines-as-another-user</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT 33 (aka Peach Sandstorm, Elfin, Magnallium, Holmium, ATK 35, Refined Kitten, TA451, Cobalt Trinity)	Iran	Aviation, construction, defense, education, energy, financial services, healthcare, government, satellite, pharmaceutical sector, and telecommunications sectors	Worldwide
	MOTIVE		
	Information theft and espionage, Sabotage and destruction		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022- 47966 CVE-2022- 26134	-	-
TTPs			
TA0001 Initial Access; TA0003 Persistence; TA0008 Lateral Movement; TA0011 Command and Control; TA0043 Reconnaissance; TA0002 Execution; TA0006 Credential Access; TA0004 Privilege Escalation; TA0042 Resource Development; T1589 Gather Victim Identity Information; T1589.001 Credentials; T1078 Valid Accounts; T1572 Protocol Tunneling; T1651 Cloud Administration Command; T1098 Account Manipulation; T1203 Exploitation for Client Execution; T1021 Remote Services; T1110 Brute Force; T1110.003 Password Spraying; T1574 Hijack Execution Flow; T1574.002 DLL Side-Loading; T1072 Software Deployment Tools; T1574.001 DLL Search Order Hijacking; T1105 Ingress Tool Transfer; T1588 Obtain Capabilities; T1588.006 Vulnerabilities; T1588.005 Exploits			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Redfly	China	Critical Infrastructure	Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	ShadowPad, Packerloader	-

TTPs
TA0001 Initial Access; TA0003 Persistence; TA0008 Lateral Movement; TA0011 Command and Control; TA0043 Reconnaissance; TA0002 Execution; TA0006 Credential Access; TA0004 Privilege Escalation; TA0042 Resource Development; T1584: Compromise Infrastructure; T1036: Masquerading ; T1027: Obfuscated Files or Information; T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter; T1486: Data Encrypted for Impact; T1140: Deobfuscate/Decode Files or Information; T1012: Query Registry; T1573.001: Symmetric Cryptography ; T1573: Encrypted Channel ; T1055.001: Dynamic-link Library Injection ; T1055: Process Injection; T1056.001: Keylogging ; T1056: Input Capture ; T1574.002: DLL Side-Loading ; T1574: Hijack Execution Flow; T1059.001: PowerShell

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 ShroudedSnooper	Unknown	Telecommunications	Middle East
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	HTTPSnoop and PipeSnoop	-

TTPs
TA0001: Initial Access, TA0042: Resource Development, TA0005: Defense Evasion, TA0002: Execution, TA0004: Privilege Escalation, TA0011: Command and Control , T1059: Command and Scripting Interpreter, T1584: Compromise Infrastructure, T1036: Masquerading, T1574.001: DLL Search Order Hijacking, T1190: Exploit Public-Facing Application, T1106: Native API, T1140: Deobfuscate/Decode Files or Information, T1027: Obfuscated Files or Information,

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Earth Lusca (aka Bronze University, Charcoal Typhoon, Red Scylla)</td><td>China</td><td rowspan="2">Asia, the Balkans, and a few scattered regions in Latin</td><td rowspan="2">Casinos And Gambling, Technology, Education, Government, Media, Telecommunications, Foreign Affairs, Human Rights, Political Organizations and Cryptocurrency Trading Platforms</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Financial gain</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TARGETED CVEs</td><td>SprySOCKS Backdoor</td><td>FortiOS, FortiProxy, FortiSwitchManager, GitLab CE/EE, TELERIK.WEB.UI.DLL, Zimbra Collaboration Suite, Microsoft Exchange Server, Confluence Server and Confluence Data Center</td></tr>
<tr><td>CVE-2022-40684
CVE-2021-22205
CVE-2019-18935
CVE-2019-9670
CVE-2021-34473
CVE-2021-34523
CVE-2021-31207</td><td></td><td></td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0043: Reconnaissance, TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0005: Defense Evasion, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, T1190: Exploit Public-Facing Application, T1595.002: Vulnerability Scanning, T1584.004: Server, T1543: Create or Modify: System Process, T1055: Process Injection, T1570: Lateral Tool Transfer, T1112: Modify Registry, T1588.001: Malware, T1007: System Service Discovery, T1560: Archive Collected Data</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Sandman APT	China	Critical Infrastructure	Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	ShadowPad, Packerloader	-

TTPs
TA0001 Initial Access; TA0003 Persistence; TA0008 Lateral Movement; TA0011 Command and Control; TA0043 Reconnaissance; TA0002 Execution; TA0006 Credential Access; TA0004 Privilege Escalation; TA0042 Resource Development; T1584: Compromise Infrastructure; T1036: Masquerading ; T1027: Obfuscated Files or Information; T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter; T1486: Data Encrypted for Impact; T1140: Deobfuscate/Decode Files or Information; T1012: Query Registry; T1573.001: Symmetric Cryptography ; T1573: Encrypted Channel ; T1055.001: Dynamic-link Library Injection ; T1055: Process Injection; T1056.001: Keylogging ; T1056: Input Capture ; T1574.002: DLL Side-Loading ; T1574: Hijack Execution Flow; T1059.001: PowerShell

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eleven exploited vulnerabilities** and block the indicators related to the threat actor **APT33, Redfly, ShroudedSnooper, Earth Lusca , Sandman APT** and **PipeSnoop, SprySOCKSBackdoor, VenomRAT, Snatchransomware, LuaDream** 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 **eleven exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT33, Redfly, ShroudedSnooper, Earth Lusca , Sandman APT** and **PipeSnoop, SprySOCKSBackdoor, VenomRAT, Snatchransomware, LuaDream** in Breach and Attack Simulation(BAS).

Threat Advisories

APT 33 Uses Password Spray Campaigns to Infiltrate Organizations

Redfly Targets Critical Infrastructure in Asia with ShadowPad Trojan

Trend Micro Addresses Zero-Day Flaws Exploited in the Wild

HTTPSnoop and PipeSnoop Malware Target Telecoms in the Middle East

Earth Lusca's Sneaky Moves Unleashes New Linux Backdoor

GitLab Releases Critical Patch to Address Pipeline Execution Vulnerability

Deceptive WinRAR PoC Released on GitHub Drops VenomRAT

Snatch Ransomware: Evolving Threat and Defense Strategies

Critical Security Vulnerabilities Uncovered in Nagios XI

Sandman APT Strikes the Telecom Sector with the LuaDream 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
ShadowPad	SHA256	656582bf82205ac3e10b46cbbcf8abb56dd67092459093f35ce8daa64f379a2c, ac6938e03f2a076152ee4ce23a39a0bfcd676e4f0b031574d442b6e2df532646, 231d21ceefd5c70aa952e8a21523dfe6b5aae9ae6e2b71a0cdbe4e5430b4f5b3, d9438cd2cdc83e8efad7b0c9a825466efea709335b63d6181dfdc57fb1f4a4e3
Packerloader	SHA256	32d709d8d41e4ede6861ce27c9e2bb86d83be8336b45a17f567bab1869c6600a
SprySOCKS Backdoor	SHA256	6f84b54c81d29cb6ff52ce66426b180ad0a3b907e2ef1117a30e95f2dc9959fc, f8ba9179d8f34e2643ee4f8bc51c8af046e3762508a005a2d961154f639b2912, eebd75ae0cb2b52b71890f84e92405ac30407c7a3fe37334c272fd2ab03dff58
	Domains	lt76ux.confenos[.]shop, 2e6veme8xs.bmssystemg188[.]us
VenomRAT	SHA256	61dd71441a2b4955467243e986c38f1ea543bae7b1546f003c4a30074dd6c04e, cabc45f1dab04be3fc63192d98324d2665599a6d6ea2f0277ecd27a62fb694f3,

Attack Name	TYPE	VALUE
VenomRAT	SHA256	79b87d7accc9cbd1414b72ca13c48a385be9cb06c1bb53d845e94107b579bf62, 4b84283c40560991da34ef2b465a4724facd0932acebff60466d8d5ff1916bd5, 75c12ccacd764101736b213981355b39056227929214c8963e9bf3ea5a60f6ef, 1648bea3c1c3b00e7f9c9bf7f65be833fa7f291f0e05a342382e9e36f0350c60, b23e4ea87917a517565de8471a101ab55c2a31186c8a23e9e8af71b359d35aa9, 65235e5bd2f9b30e2b272602a83a8f3805cfca50252da8a79e279f232a6d3990, ecc3971af558300b451a87b51d0324737174ea1993d8aa7424078fb1bd97ffb3, f9497f07d69b043501cc52bf2db7828abad35a14bd95bb05e6b5ab9e4408de4e, 48f61821feeaa45c53daaeb567e142ce9614d131dcf886506a31bf0ba2d75c45, f6ad1568aa318f7d27c41ce47b5b3a1a2aceb0fb470d7528117364b67463501e, f6ad1568aa318f7d27c41ce47b5b3a1a2aceb0fb470d7528117364b67463501e, d0e7f2c67877f06c0e8854b1a37f6f04d181537d77e242f46401415da17f9b03, 8ef5c7eaa352e547c2e0de266844122ab471cd2ac73a9388b4f1416b2ac8c840, d845bc06b40c5810390a226e0608090aa7ea67f603af8bbd4f00318102bb8b7d, d845bc06b40c5810390a226e0608090aa7ea67f603af8bbd4f00318102bb8b7d, b9b75fe8ce464a4ae9c0578741718777da09646ea89f42ac3663cbf365681b3d, b9b75fe8ce464a4ae9c0578741718777da09646ea89f42ac3663cbf365681b3d, a9e8b6b187c3bbfccfec6266b95c079bf27752d22bcd04c97df8a62f4a6dcd59, 4c69911de167a507a1c6effb9724ab72ca0026d1fdfa9c747f70800abdbcbbe5, 9e8f792af1587b867f477863e2c19d7443f2926ba1e933cf073dcdc68a748dad, 78a11a10e8d26f98221c9981f1d35b91ce67714a044400fe9933756435b4b690, 997a1ea14695bc0275446cd35e362ae48a4f3a6f108d91fea49ba1c83803edd1, 997a1ea14695bc0275446cd35e362ae48a4f3a6f108d91fea49ba1c83803edd1, 997a1ea14695bc0275446cd35e362ae48a4f3a6f108d91fea49ba1c83803edd1,

Attack Name	TYPE	VALUE
VenomRAT	SHA256	4694bd08ad1446ae0deb2ea6db86658930422cbef632e88ef7ab2218ff75e509, 35afd46abb89d050971ffc41a372e2f64046404783e33d896cb77a3b3855d2e0, 45c95edaadc2c82c1ce03f7e9d9a60be0361f6f964e845ac74fecf0403c1bfa3, 45c95edaadc2c82c1ce03f7e9d9a60be0361f6f964e845ac74fecf0403c1bfa3, e8c6798610293bad3d42472fcc5df23ce3498d91eb2f05cec76a9cd7c5248d29, d0bd2f3e2c91bd604ed1d4604d65deff63d443c8abac736873edc085cfca002e, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 9f917ff3160a74ffe217d5941530753fbd1292a31141a0bc6d4e889bb58cb883, 9f917ff3160a74ffe217d5941530753fbd1292a31141a0bc6d4e889bb58cb883, e2ba06f64e174ff0daa92c39e13ca9a4b735c005d01b65a43a20b6af81f0068b, 0ea528ae0f3931379941f569ae55f0ec2c0714ccd1c2c36cc39e20ba58e11113, 96e560ca4abd5f6309f52eabdaffb87399aa91e70cc9f548c35753f8526206f3, a99b925b26f753b0da74d16c53161ada4f2048ceb28b81e2b532c8c840efd31b, bd5244f5beeb1ca343da306f4f2cf40a4d7aee3e60d75eda37823d61124b24d0, ac12768102db5b194391395525873722232c85e2237afe093f2cd7f75f876f155, ac12768102db5b194391395525873722232c85e2237afe093f2cd7f75f876f155, 8283f5942a09cefc09ede83ec97cea26ae094c41b4df2036844a7a5e51bdc4ae, e0b3ea9079e7606ef7575bedd5fc648c63b6d0e12b27d6c9dcbdc17d8a758e33, e0b3ea9079e7606ef7575bedd5fc648c63b6d0e12b27d6c9dcbdc17d8a758e33, bb593c07ee6598e8ba0f941809a93be8c42051b03aecd2356ded08f35630871a

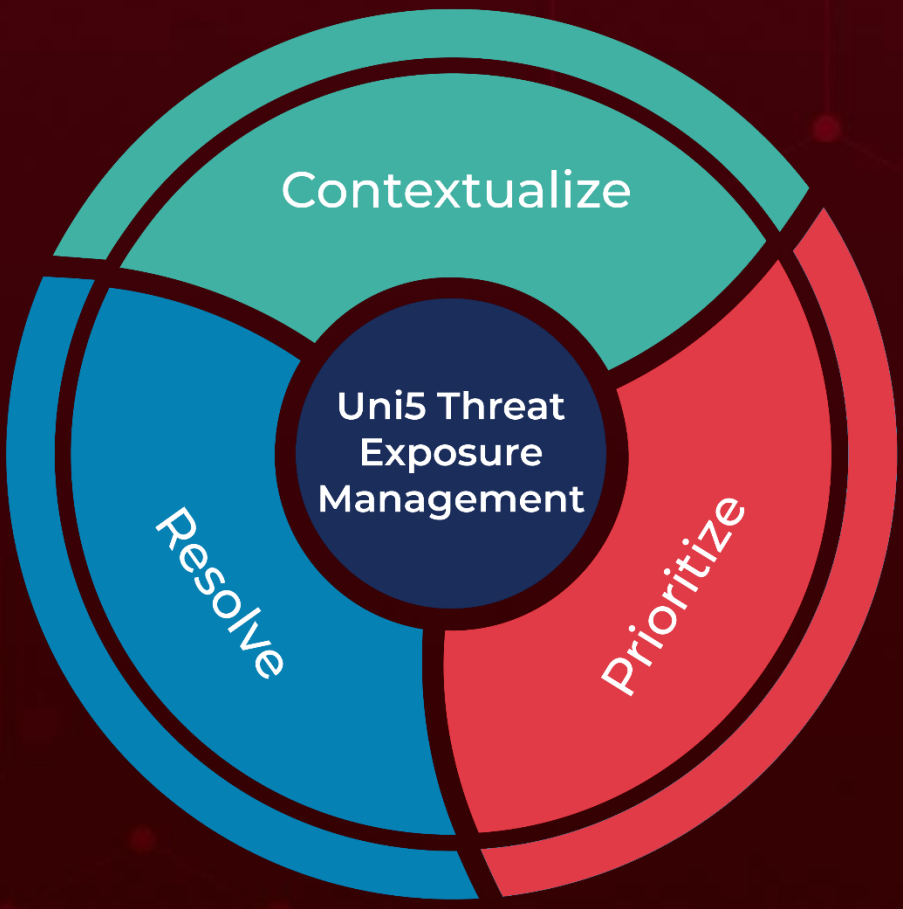
Attack Name	TYPE	VALUE
Snatch ransomware	SHA256	0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f, 1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d, 5950b4e27554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcd, 7018240d67fd11847c7f9737eaaae45794b37a5c27ffd02beaacaf6ae13352b3, 28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd76b8c4acff7c, fc31043b5f079ce88385883668eeebba76a62f77954a960fb03bf46f47dbb066, a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae, 6992aaad3c47b938309fc1e6f37179eb51f028536f8afc02e4986312e29220c0, 510e9fa38a08d446189c34fe6125295f410b36f00aceb65e7b4508e9d7c4e1d1, ed0fd61bf82660a69f5bfe0e66457cfe56d66dd2b310e9e97657c37779aef65d, 2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57, 251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d, 3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924, 6c9d8c577dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7, 84e1476c6b21531de62bbac67e52ab2ac14aa7a30f504ecf33e6b62aa33d1fe5, a80c7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84, b998a8c15cc19c8c31c89b30f692a40b14d7a6c09233eb976c07f19a84eccb40, 1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d, 0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f
	Emails	sn.tchnews.top@protonmail[.]me, funny385@swisscows[.]email, funny385@proton[.]me, russellrspeck@seznam[.]cz, russellrspeck@protonmail[.]com, Mailz13MoraleS@proton[.]me, datasto100@tutanota[.]com, snatch.vip@protonmail[.]com
	Domains	tutanota[.]com / tutamail[.]com / tuta[.]io, mail[.]fr, keemail[.]me, protonmail[.]com / proton[.]me,

Attack Name	TYPE	VALUE
Snatch ransomware	Domains	swisscows[.]email, sn.tchnews.top@protonmail[.]me
LuaDream	SHA1	1cd0a3dd6354a3d4a29226f5580f8a51ec3837d4, 27894955aaf082a606337ebe29d263263be52154, 5302c39764922f17e4bc14f589fa45408f8a5089, 77e00e3067f23df10196412f231e80cec41c5253, b9ea189e2420a29978e4dc73d8d2fd801f6a0db2, fb1c6a23e8e0693194a365619b388b09155c2183, ff2802cdbc40d2ef3585357b7e6947d42b875884
	File Paths	%ProgramData%\FaxConfig, %ProgramData%\FaxLib
	Domains	mode.encagil[.]com, ssl.explorecell[.]com
HTTPSnoop	SHA256	1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb, 7495c1ea421063845eb8f4599a1c17c105f700ca0671ca874c5aa5aef3764c1c, 3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7, 04cf425e57e7d511f03189749c8c0a95483eeeb4c423e9ee1a6a766d2fe0094c, c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0
PipeSnoop	SHA256	e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d, 9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0ceb

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

September 25, 2023 . 10:30 AM

More at www.hivepro.com