

Date of Publication
December 15, 2023



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

8 to 14 JANUARY 2024

Table Of Contents

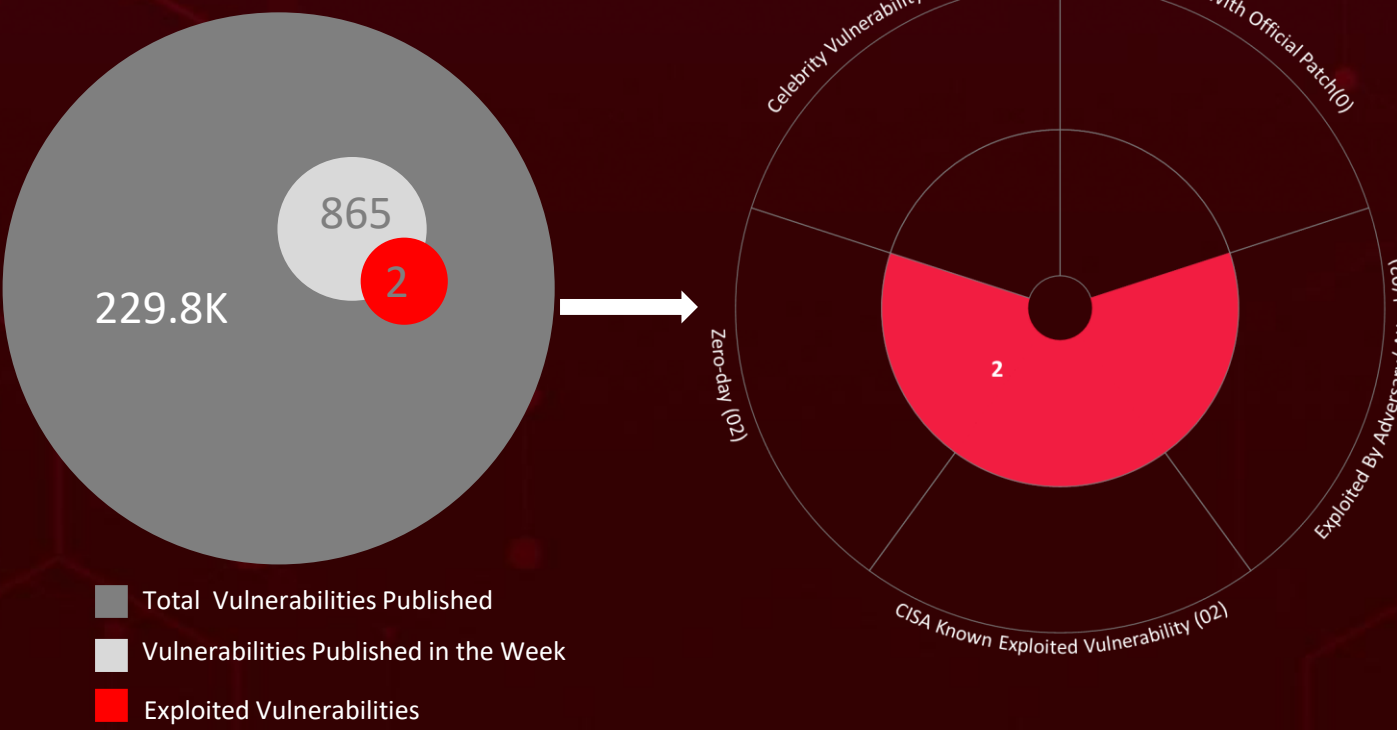
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	17
<u>Threat Advisories</u>	18
<u>Appendix</u>	19
<u>What Next?</u>	24

Summary

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

Furthermore, HiveForce Labs revealed that there are **two zero-day** vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways. These vulnerabilities pose a significant risk, as they enable unauthorized remote code execution. The entity identified as UTA0178, a Chinese nation-state-level actor, utilized these exploits to compromise systems.

Silver RAT, developed by the group **Anonymous Arabic**, showcases advanced features such as antivirus evasion and ransomware encryption. **Sea Turtle**, a Turkish APT, specializes in information theft and DNS hijacking, using a reverse TCP shell called **SnappyTCP** to compromise repositories holding valuable and sensitive data. These attacks are on the rise, posing a significant threat to users worldwide.



High Level Statistics

7

Attacks
Executed

2

Vulnerabilities
Exploited

3

Adversaries in
Action

- [PikaBot](#)
- [Black Basta](#)
- [Silver RAT](#)
- [SnappyTCP](#)
- [Fbot](#)
- [Lumma](#)
- [Medusa](#)

- [CVE-2023-46805](#)
- [CVE-2024-21887](#)

- [Water Curupira](#)
- [Anonymous Arabic](#)
- [Sea Turtle](#)



Insights

January Shield:

Microsoft's Patch Tuesday for January 2024, addressed a total of 49 vulnerabilities across a spectrum of products.

Cryptic Craftsmanship Unveiled:

Behind the intricate creation of Silver RAT in C# lurk the masterminds known as 'Anonymous Arabic,' skillfully exposing the group's direct association with this formidable Remote Access Trojan.

Mastering Multi-Extortion:

Medusa unleashes a multi-extortion approach, leveraging its Medusa Blog to disclose victim data.

Mysterious Maritime Menace:

Unveiling Sea Turtle, an Advanced Persistent Threat (APT) actor based in Turkey, notorious for its enigmatic tactics involving information theft and DNS hijacking.

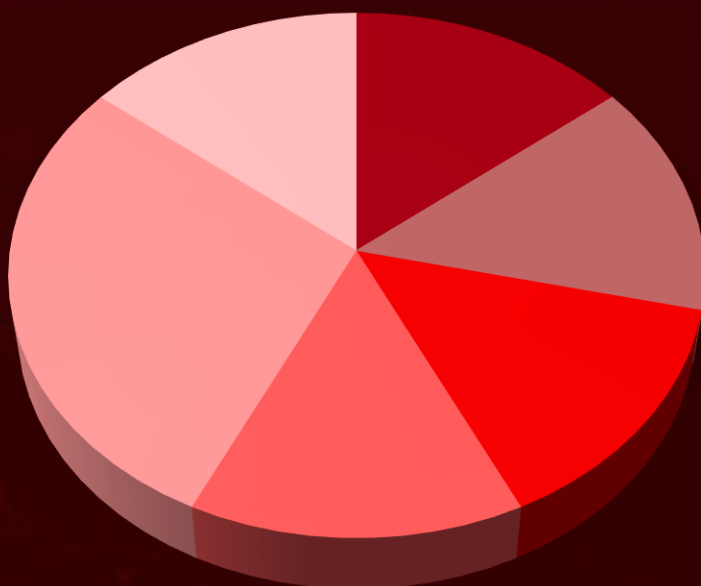
Unveiling the Zero-Day Symphony:

UTA0178, a Chinese nation-state-level entity, is the orchestrator behind the exploitation of zero-day vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways. This underscores the imperative to promptly apply mitigations, thwarting the potential for compromise.

Lumma's Shape-Shifting Tactics:

Lumma Stealer is adapting to the ever-evolving landscape by exploiting users' interests in cracked software via YouTube.

Threat Distribution



■ Exploit tool ■ Loader ■ RAT ■ WebShell ■ Ransomware ■ Stealer

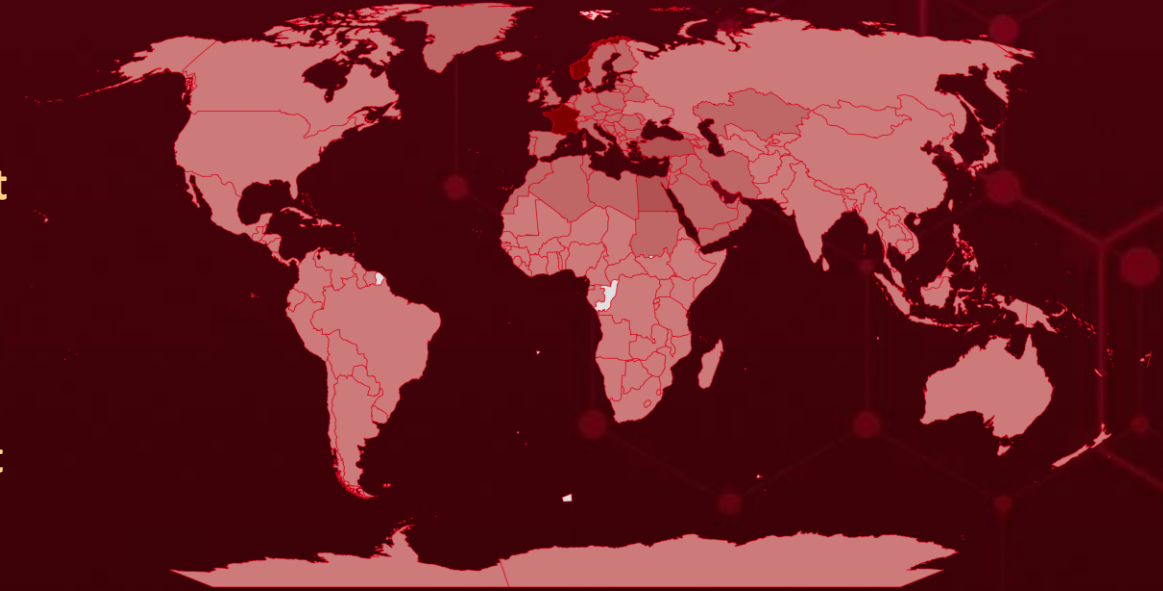


Targeted Countries

Most



Least

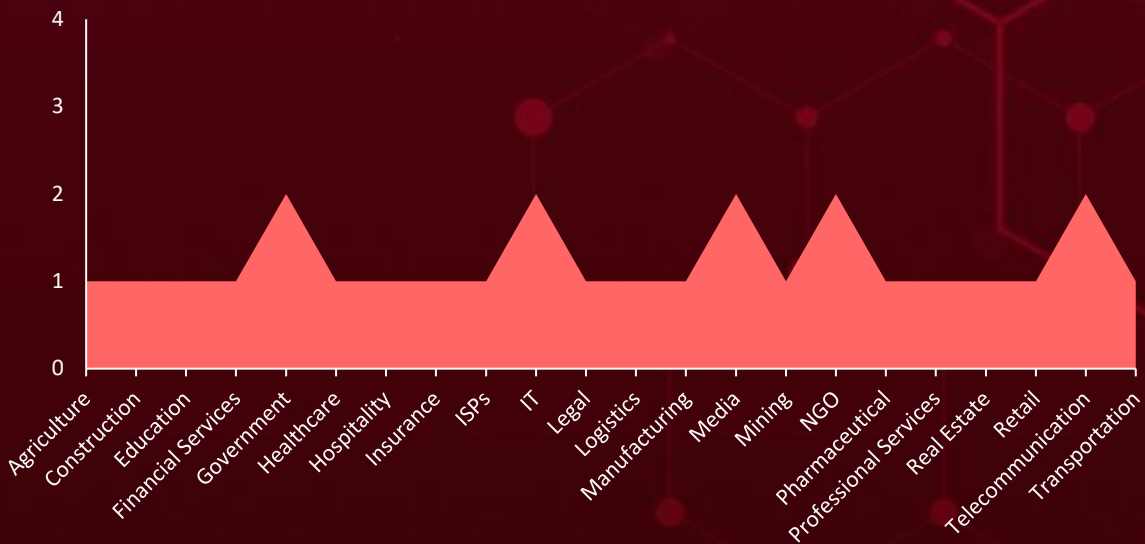


Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Countries	Countries	Countries	Countries
Norway	Serbia	United Kingdom	Rwanda
France	Bulgaria	Netherlands	New Zealand
Cyprus	Saudi Arabia	Czech Republic	Puerto Rico
Turkey	Bahrain	Morocco	New Caledonia
Egypt	San Marino	Croatia	Cameroon
Albania	Andorra	Montenegro	Uruguay
Germany	Romania	Bosnia and Herzegovina	Bangladesh
Israel	Akrotiri and Dhekelia	Monaco	Nepal
Tunisia	Qatar	Belarus	Afghanistan
Belgium	Kuwait	Moldova	Nauru
Transnistria	Portugal	Azerbaijan	Russia
Kosovo	Kazakhstan	Malta	Namibia
Syria	Poland	Armenia	Dominica
Iceland	Italy	Luxembourg	Myanmar
Switzerland	Palestine	Algeria	Togo
Faroe Islands	Ireland	Lithuania	Mozambique
Sweden	Oman	Åland	Central African Republic
Austria	Iran	Liechtenstein	United States
Sudan	Vatican City	Abkhazia	Philippines
Latvia	Hungary	Libya	Mongolia
Spain	Northern Cyprus	Lebanon	Belize
Jordan	Greece	Antigua and Barbuda	Suriname
South Ossetia	North Macedonia	Colombia	Palau
Iraq	Georgia	Trinidad and Tobago	Western Sahara
Slovenia	Estonia	Niger	Tajikistan
Greenland	Finland	Peru	Micronesia
Slovakia	Denmark	Nicaragua	Saint Kitts and Nevis
United Arab Emirates	Yemen		Mexico

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1588

Obtain Capabilities

T1588.006

Vulnerabilities

T1027

Obfuscated Files or Information

T1036

Masquerading

T1082

System Information Discovery

T1588.005

Exploits

T1059.001

PowerShell

T1059.007

JavaScript

T1056

Input Capture

T1566

Phishing

T1070

Indicator Removal

T1041

Exfiltration Over C2 Channel

T1567

Exfiltration Over Web Service

T1190

Exploit Public-Facing Application

T1057

Process Discovery

T1203

Exploitation for Client Execution

T1204

User Execution

T1659

Content Injection

T1218.011

Rundll32

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PikaBot</u>	Pikabot is a sophisticated piece of multi-stage malware with a loader and core module within the same file. Pikabot, downloads other threats like ransomware, gives attackers remote control, and hides on Windows systems.	Malvertising and phishing campaigns	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader			
ASSOCIATED ACTOR		Data Theft, Downloading other malware	PATCH LINK
Water Curupira			
IOC TYPE	VALUE		
SHA256	4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b, fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de, 29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8		
IPv4:Port	15[.]235[.]202[.]109:2226, 15[.]235[.]44[.]231:5938, 15[.]235[.]45[.]155:2221		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Black Basta</u>	Black Basta ransomware has been actively using Pikabot a loader malware in spam campaigns throughout 2023. Black Basta deploys a range of second-stage tactics to acquire Windows Domain credentials and penetrate a target's network laterally	Pikabot	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			
ASSOCIATED ACTOR		Steal credentials, data theft and Financial Loss	PATCH LINK
Water Curupira			
IOC TYPE	VALUE		
Domains	lindacolor[.]com, withclier[.]com, unough[.]com		

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
<u>Silver RAT</u>	Silver RAT, a Windows-based RAT written in C# and developed by a group known as "Anonymous Arabic," exhibits advanced capabilities, including antivirus evasion and ransomware encryption.	Social engineering tactics	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Executes custom commands, data encryption, and system restore point deletion.	Windows and Android
ASSOCIATED ACTOR			PATCH LINK
Anonymous Arabic			-
IOC TYPE	VALUE		
SHA256	79a4605d24d32f992d8e144202e980bb6b52bf8c9925b1498a1da59e50ac51f9, a9fa8e14080792b67a12f682a336c0ea9ff463bbcb27955644c6fcfa80023641, 7a9aeea5e65a0966894710c1d9191ba4cbd6415cba5b10b3b75091237a70a5b8		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>SnappyTCP</u>	A reverse TCP shell named SnappyTCP for Linux/Unix with basic command-and-control capabilities has been used to establish persistence on systems.	Compromised cPanel account	-
TYPE		IMPACT	AFFECTED PRODUCTS
WebShell		Man-in-the-middle attacks to harvest credentials	-
ASSOCIATED ACTOR			PATCH LINK
Sea Turtle			-
IOC TYPE	VALUE		
MD5	102d8524f21d1b6b0380c817a435e9a7, 80aa20453ca295467bff3f8708a06280,		
SHA256	1ac0b2e91ba3d33ed6b8cd90f5c1f63454bdf7aad7dbf4f239445f31dfc6eb5, f8cb77919f411db6eaeaa8f0c8394239ad38222fe15abc024362771f611c360f, aea947f06ac36c07ae37884abc5b6659d91d52aa99fd7d26bd0e233fd0fe7ad4		

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
<u>Fbot</u>	<p>FBot, a Python-based exploit tool, has systematically targeted critical infrastructures. Its primary objective is to infiltrate these services, acquiring credentials to subsequently monetize unauthorized access by selling it to other malicious entities.</p>	Credential harvesting	-
TYPE		IMPACT	AFFECTED PRODUCTS
Exploit tool		<p>Data loss, Hijack cloud, SaaS, and web services</p>	<p>AWS, Office365, PayPal, Sendgrid, and Twilio.</p>
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA1	<p>1ad78e99918fd66ed43d42a93d2f910a2173b3c5, 2becd32162b2b0cb1afc541e33ace3a29dad96f1, 8ba3fca4deada6dbdc94b17a0c3c55a0b785331e</p>		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Lumma</u>	<p>Lumma Stealer, developed in C Language, is designed to target browsers, cryptocurrency wallets, system data. It employs various obfuscation techniques and is actively promoted on dark web forums.</p>	Disguised as cracked software	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		<p>Stealing sensitive information</p>	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	<p>01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f</p>		




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	
Medusa	<p>Medusa ransomware employs a multi-extortion approach via its Medusa Blog, disclosing victim data and pressuring non-compliant organizations. Operating as a ransomware-as-a-service approach involves a multi-extortion strategy, offering victims options like time extensions, data deletion, or full data download, each with associated costs.</p>	Exploiting vulnerable services	-	
TYPE		IMPACT	AFFECTED PRODUCTS	
Ransomware			Windows	
ASSOCIATED ACTOR		-	Data exfiltration, information theft, and financial loss	PATCH LINK
			-	
IOC TYPE	VALUE			
SHA256	4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6, 657c0cce98d6e73e53b4001eeee51ed91fdcf3d47a18712b6ba9c66d59677980, 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95, 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669, 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd27 0			


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
<u>CVE-2023-46805</u>		Ivanti Pulse Connect Secure: 9.x and 22.x Ivanti Pulse Policy Secure: 9.x and 22.x	UTA0178
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	MITIGATION
	CWE-287	T1588: Obtain Capabilities, T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1040: Network Sniffing	Import the mitigation.release.20240107.1.xml file via the download portal to address the vulnerabilities temporarily. https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21887</u>		Ivanti Pulse Connect Secure: 9.x and 22.x Ivanti Pulse Policy Secure: 9.x and 22.x	UTA0178
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*	
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability			-
	CWE ID	ASSOCIATED TTPs	MITIGATION
	CWE-78	T1059: Command and Scripting Interpreter	Import the mitigation.release.20240107.1.xml file via the download portal to address the vulnerabilities temporarily. https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Water Curupira</u>	-	-	Worldwide
	MOTIVE Financial gain, Information Theft and Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	PikaBot, Black Basta	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0042: Resource Development; TA0007: Discovery; TA0011: Command and Control; TA0009: Collection; TA0010: Exfiltration; TA0040: Impact; T1082: System Information Discovery; T1057: Process Discovery; T1219: Remote Access Software; T1583: Acquire Infrastructure; T1583.008: Malvertising; T1566: Phishing; T1566.002: Spearphishing Link; T1204.002: Malicious File; T1204: User Execution; T1036: Masquerading; T1059.007: JavaScript; T1059: Command and Scripting Interpreter; T1218.011: Rundll32; T1218: System Binary Proxy Execution; T1218.007: Msiexec; T1041: Exfiltration Over C2 Channel; T1140: Deobfuscate/Decode Files or Information; T1560: Archive Collected Data; T1102: Web Service; T1574: Hijack Execution Flow			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Anonymous Arabic</u>	-	-	Worldwide
	MOTIVE		
	Hacktivist and Financial gain	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	TARGETED CVEs		
	-		
TTPs			
TA0007: Discovery; TA0002: Execution; TA0005: Defense Evasion; TA0009: Collection; TA0006: Credential Access; TA0010: Exfiltration; TA0003: Persistence; TA0004: Privilege Escalation; T1027: Obfuscated Files or Information; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1059: Command and Scripting Interpreter; T1055: Process Injection; T1112: Modify Registry; T1497: Virtualization/Sandbox Evasion; T1056: Input Capture; T1539: Steal Web Session Cookie; T1552: Unsecured Credentials; T1528: Steal Application Access Token; T1057: Process Discovery; T1083: File and Directory Discovery; T1082: System Information Discovery; T1041: Exfiltration Over C2 Channel; T1567: Exfiltration Over Web Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Sea Turtle (aka Teal Kurma, Marbled Dust, SILICON, and Cosmic Wolf)</u></p>	Turkey	Government entities, political groups, telecommunication, ISPs, IT-service providers (including security companies), NGO and Media & Entertainment sectors	Europe, Middle East and North Africa
	MOTIVE		
	Information theft and espionage	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	SnappyTCP	-

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1588: Obtain Capabilities; T1588.001: Malware; T1133: External Remote Services; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1505: Server Software Component; T1505.003: Web Shell; T1070: Indicator Removal; T1070.003: Clear Command History; T1070.002: Clear Linux or Mac System Logs; T1114: Email Collection; T1114.001: Local Email Collection; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1567: Exfiltration Over Web Service

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploited vulnerabilities** and block the indicators related to the threat actors **Water Curupira, Anonymous Arabic, Sea Turtle**, and malware **PikaBot, Black Basta, Silver RAT, SnappyTCP, Fbot, Lumma, Medusa**.

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 **two exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Water Curupira, Anonymous Arabic, Sea Turtle**, and malware **PikaBot, Black Basta, Silver RAT, SnappyTCP, Fbot, Lumma, Medusa** in Breach and Attack Simulation(BAS).

Threat Advisories

[PikaBot Malware Unleashes Threat via Malvertising](#)

[Anonymous Arabic Hactivist Group Orchestrating Silver RAT](#)

[Unveiling the Sea Turtle Cyber Espionage Campaign](#)

[Microsoft's January 2024 Patch Tuesday Addresses 49 Vulnerabilities](#)

[Two Zero-Day Flaws Found in Ivanti Connect Secure and Policy Secure](#)

[FBot's Arsenal against the SaaS Giants](#)

[Maliciously Crafted Cracked Software Propagates Lumma Stealer via YouTube](#)

[Medusa Ransomware Unleashed A Growing Cybersecurity Menace](#)

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 malicious 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
PikaBot	SHA256	4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b, fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de, 29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8, 6c13985e067cfad583bb1f5751821e649a61a41171a5f95ee9dfd254c04f71a8, ed4bba5e886871527fa56beb280f222ef0fde97686db00a74ee02c1a44a0094d, 1d365a8a2e72a81a6ffbc6c0c32b28e580872e57df184c270b4fa47ac8b8bf2b, b436380d62babc42fa6b3adc592e1b6b0bd05c5cb1b0c08aa5c55eae738729e7, 980e2dccc3b83bab32b13f82091f37a2ffc302c7fb7e87532c7c618f68c0753, 6f9b2fdac415c7eb7fcc31c5ff9aac7e6347ddf4747985b7bac4f76a6f9da193, 3b13380f7dfd615707887f3e8904f432aacdbb111822dd596a44366cb5526624, 8045ea8720b66291e3c00f6fd1925de11241410421851b7cab e4a707875a1004, 4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b, 7808be7f2b92c775f6ef047ffc857d8731e75bf486a45fec1c4d199b43c5a6c2, 1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8f5fc5443a,

Attack Name	TYPE	VALUE
<u>PikaBot</u>	SHA256	ea63ac688aec3ab8920d83617f214922c16aedee341edbe3a18469 179555fb21, 07279c93f0532a4f5bc4617ab3cb30b7c336f71f587e934a5a0e35ce 88fbf632, 2dad1218d4950ba3a84cfce17af2d8d4ece92f623338d49b357ec9d 973ecf8a8, 33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a 254255c34, 1a12028a0e0ecc32160e5372a45d95e3045421906f2c807b7c4c8f4 a85d47469, 1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8 f5fc5443a, 33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a 254255c34, 6e18eb1884d2a1a20a0d6a4dcdaf1b7ab342271b2de0d0327848f3 7eb45e785e, 7094f89bf955dfbdcc4de8943af2328aa7475c2fb6af305c76a6df73a ff8b1c3, 2c49ff53d0cf0ea36f34148598b8eacca12a1a654bfc09c4e00d6b60 a8ad57fe, 8514b9d2fe185989d996a2669788910405af5e8fd7102ab3decdd4d 727af35df, 79b1ac4dc5cae6d03548c2ab570e98f9cfb7e4da24480ce3d513b1a bdd13bf21, 1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8 f5fc5443a, eead7f5b6f1282ad988238cc8c39292fa99ea416f7793038a20e5caa be93112a, 7e85b9d1d09301d8b3f48df44159347d89cb3c798d0436b5e9b060 df4072b8c7, 46e0fe3a942bb1f9aa9cd1b460ca7efa9acddb3c5b2d2bc3b42a87d 8463f1c66
	URLs	hxxps://sindicaturadetecate[.]gob[.]mx/pe/?IDbHJCMofpElzDQjrcw NcDqHoiQRnSKZQcA, hxxps://lsn[.]edu[.]dz/pqis/?aWDzZBatBsyv, hxxp:188[.]34[.]192[.]184/76DKN6/Wheez, hxxps://brouweres[.]com:443/vvs49/0.6515179055030298.dat, hxxps://brouweres[.]com:443/vvs49/0.8450027286577588.dat, hxxps://brouweres[.]com:443/vvs49/0.15313287608559223.dat, hxxps://brouweres[.]com:443/vvs49/0.9900618798908114.dat
	IPv4:Port	15[.]235[.]202[.]109:2226, 15[.]235[.]44[.]231:5938, 15[.]235[.]45[.]155:2221, 15[.]235[.]47[.]206:13783, 15[.]235[.]47[.]80:23399, 154[.]221[.]30[.]136:13724, 154[.]61[.]75[.]156:2078, 154[.]92[.]19[.]139:2222, 188[.]26[.]127[.]4:13785,

Attack Name	TYPE	VALUE
<u>PikaBot</u>	IPv4:Port	210[.]243[.]8[.]247:23399, 51[.]195[.]232[.]97:13782, 51[.]68[.]147[.]114:2083, 51[.]79[.]143[.]215:13783, 64[.]176[.]5[.]228:13783, 154[.]221[.]30[.]136:13724, 137[.]220[.]55[.]190:2223, 210[.]243[.]8[.]247:23399, 65[.]20[.]78[.]68:13721, 139[.]180[.]216[.]25:2967, 70[.]34[.]209[.]101:13720, 154[.]92[.]19[.]139:2222, 172[.]233[.]156[.]100:13721, 154[.]61[.]75[.]156:2078, 64[.]176[.]67[.]194:2967, 158[.]247[.]253[.]155:2225, 139[.]180[.]216[.]25:2967, 70[.]34[.]209[.]101:13720, 172[.]233[.]156[.]100:13721, 154[.]92[.]19[.]139:2222, 154[.]61[.]75[.]156:2078, 137[.]220[.]55[.]190:2223
<u>Black Basta</u>	Domains	lindacolor[.]com, withclier[.]com, unoughn[.]com, bluenetworking[.]net, getfnewsolutions[.]com, conitroid[.]com, allcompanycenter[.]com, sandelias[.]com, getfnewssolutions[.]com, erihudeg[.]com, reganter[.]com, masterunis[.]net, masterunis[.]net, taskthebox[.]net, taskthebox[.]net, settingfir[.]com, magementfair[.]com, businesforhome[.]com, ruggioil[.]com, gertefin[.]com, gartenlofti[.]com, garbagemoval[.]com, constrtionfirst[.]com, animalsfast[.]net, schumacherbar[.]com, maluisepaul[.]com, masterunix[.]net, wardeli[.]com,

Attack Name	TYPE	VALUE
<u>Black Basta</u>	Domains	nutiense[.]com, jessvisser[.]com, caspercan[.]com, kolinileas[.]com, unitedfrom[.]com, brendonline[.]com, septcntr[.]com, auiditoe[.]com, conectmeto[.]net, startupbusiness24[.]net, seohomee[.]com, softradar[.]net, investsystemus[.]net, blocknowtech[.]net, mytrailinvest[.]net, realeinvestment[.]net, cloudwebstart[.]net, monitor-websystem[.]net, karmafisker[.]com, airbusco[.]net, trailgroup[.]net, monitorsystem[.]net, cloudworldst[.]net, neobeelab[.]net, stockinvestlab[.]net, prettyanimals[.]net, gift4animals[.]com, ionoslaba[.]com, buyadvisershop[.]net, blockcentersys[.]net, startuptechnologyw[.]net, investmentrealtyhp[.]net, mynewbee[.]net, buzzybeet[.]net, wellsystemte[.]net, investmendvisor[.]net, reelsysmoona[.]net, startupbizaud[.]net, building4business[.]net, steamteamdev[.]net, audsystemecll[.]net, welausystem[.]net, treeauwin[.]net, clearsystemwo[.]net
<u>Silver RAT</u>	SHA256	79a4605d24d32f992d8e144202e980bb6b52bf8c9925b1498a1da59e50ac51f9, a9fa8e14080792b67a12f682a336c0ea9ff463bbcb27955644c6fcfa80023641, 7a9aeea5e65a0966894710c1d9191ba4cbd6415cba5b10b3b75091237a70a5b8,

Attack Name	TYPE	VALUE
<u>Silver RAT</u>	SHA256	0ace7ae35b7b44a3ec64667983ff9106df688c24b52f8fcb25729c70a00cc319, 3b06b4aab7f6f590aeac5afb33bbe2c36191aeec724ec82e2a9661e34679af0a, 27b781269be3b0d2f16689a17245d82210f39531e3bcb88684b03ae620ac5007
<u>SnappyTCP</u>	MD5	102d8524f21d1b6b0380c817a435e9a7, 80aa20453ca295467bff3f8708a06280, 2a684c83401ec4706f81bf4a3503e096, 19021c37d8adda5fa509dd242629cd50, 8640f22e5a859ea2216d0e9dacef4f50
	SHA256	1ac0b2e91ba3d33ed6b8cd90f5c1f63454bdfd7aad7dbf4f239445f31dfc6eb5, f8cb77919f411db6eaeaa8f0c8394239ad38222fe15abc024362771f611c360f, aea947f06ac36c07ae37884abc5b6659d91d52aa99fd7d26bd0e233fd0fe7ad4
<u>Fbot</u>	SHA1	1ad78e99918fd66ed43d42a93d2f910a2173b3c5, 2becd32162b2b0cb1afc541e33ace3a29dad96f1, 8ba3fca4deada6dbdc94b17a0c3c55a0b785331e
<u>Lumma</u>	SHA256	01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f
<u>Medusa</u>	SHA256	4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6, 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980, 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95, 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669, 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270

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

January 15, 2024 • 1:00 AM

© 2024 All Rights are Reserved by Hive Pro®



More at www.hivepro.com