Date of Publication
August 1, 2023

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Actors, and Attacks

JULY 2023

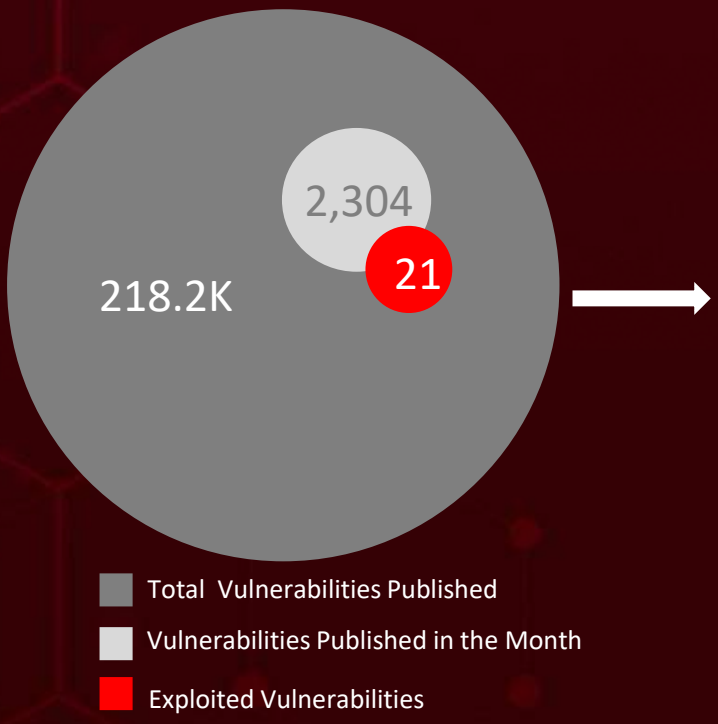
Table Of Contents

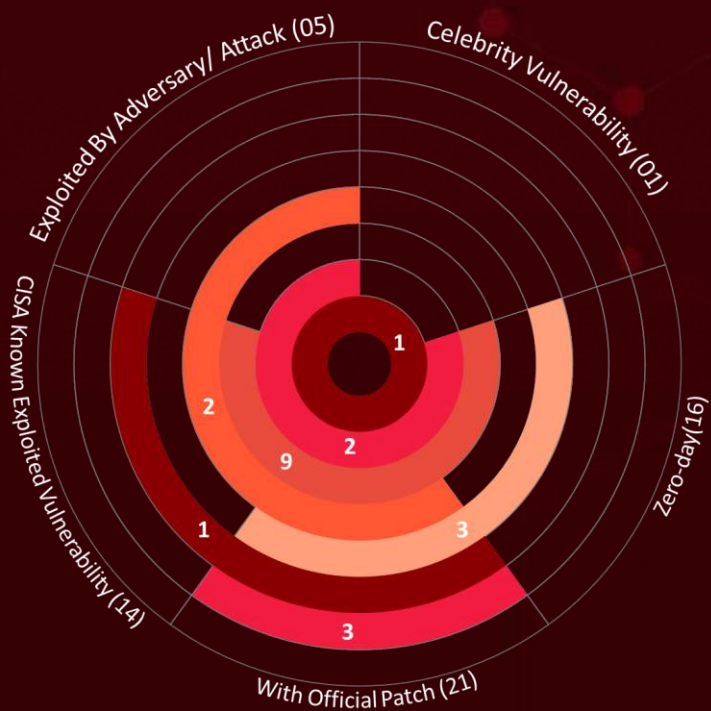
Summary

In **July**, the cybersecurity community witnessed significant attention drawn to the discovery of **sixteen zero-day** vulnerabilities. Among them was the **Celebrity Vulnerability**, exploited by **LokiBot** Data Exfiltrating Trojan Targets Windows Systems, which heightened the sense of urgency among security teams to patch their systems.

The month of July saw a rise in **ransomware** attacks, with various strains such as **Crysis**, **Venus**, **Big Head**, **Noberus**, and **Kanti** actively targeting victims. As ransomware continues to evolve and grow in sophistication, organizations must take steps to protect themselves by implementing comprehensive backup and disaster recovery strategies and training employees on how to recognize and avoid phishing attacks.

Finally, the **Zero-day** vulnerability, **CVE-2023-36884**, was exploited by the **Storm-0978** threat actor to deploy **RomCom Backdoor**.





Insights

TA445

Conducts ongoing campaigns targeting government entities, military, and civilians in Ukraine and Poland

$70 million

was demanded by the **LockBit** ransomware gang, striking **TSMC IT supplier**

200K Installs

Ultimate Member WordPress Plugin Vulnerable to Zero-Day Exploit

MS Patch Tuesday

Addressed **5 zero-day** vulnerabilities as part of July 2023

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

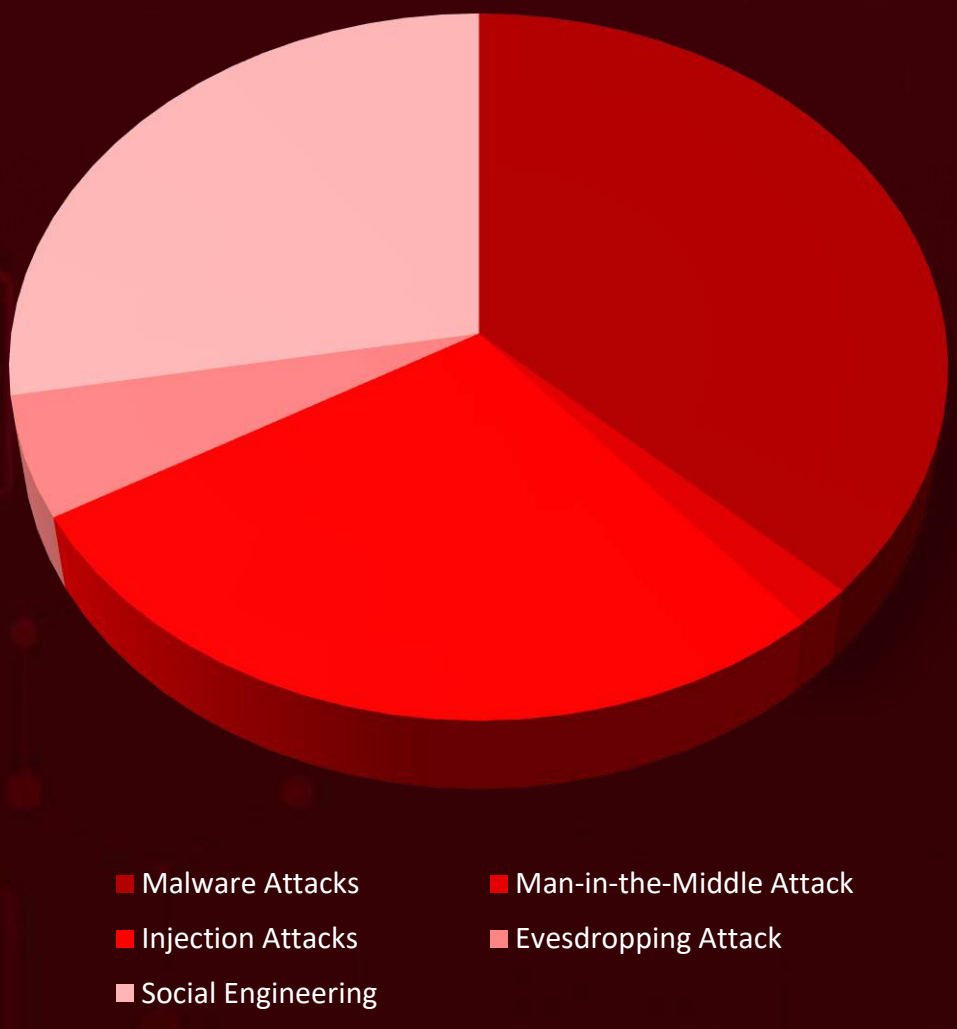
Storm-0978

Threat Actor is actively exploiting unpatched office zero-day vulnerability

Ukraine, Turkey, Cyprus, Poland, Georgia, and **Moldova** were the most targeted countries

Ivanti Addressed **CVE-2023-35078**, Zero-day Authentication Bypass Vulnerability in **EPMM**

Threat Landscape



Celebrity Vulnerabilities

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

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-3460	WordPress unauthenticated Privilege Escalation Vulnerability	WordPress Ultimate Member Plugin <= 2.6.6	✓	✗	✓
CVE-2023-37450	Apple WebKit Remote Code Execution Vulnerability	Apple Safari up to 16.5.2, Apple iOS and iPadOS up to 16.5.1, Apple macOS up to 13.4.1.	✓	✓	✓
CVE-2023-36874	Microsoft Windows Error Reporting Service Privilege Escalation Vulnerability	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	✓	✓	✓
CVE-2023-32049	Microsoft Windows Defender SmartScreen Security Feature Bypass Vulnerability	Windows: 10 - 11 22H2, Windows Server: 2016 -2022 20H2	✓	✓	✓
CVE-2023-32046	Microsoft Windows MSHTML Platform Privilege Escalation Vulnerability	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2 Microsoft Internet Explorer: 11 - 11.1790.17763.0	✓	✓	✓
CVE-2023-36884	Office and Windows HTML Remote Code Execution Vulnerability	Windows: 10 - 11 22H2, Windows Server: 2008 -2022 20H2 , Microsoft Office: 2013 -2019 Microsoft Word: 2013, Service Pack1 - 2019	✓	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-35311	Microsoft Outlook Security Feature Bypass Vulnerability	Microsoft Office:2013 -2019 Microsoft Outlook: 2013 -2016 Microsoft 365 Apps forEnterprise: 32-bit Systems- 64-bit Systems	✓	✓	✓
CVE-2021-40444	Microsoft MSHTML Remote Code Execution Vulnerability	Windows Server & Microsoft Internet Explorer	✓	✓	✓
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2023-29298	Adobe ColdFusion Improper Access Control Vulnerability	Adobe ColdFusion	✗	✓	✓
CVE-2023-38203	Adobe ColdFusion Arbitrary Code Execution Vulnerability	Adobe ColdFusion	✗	✗	✓
CVE-2023-29300	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	Adobe ColdFusion	✗	✗	✓
CVE-2023-28121	WordPress Authentication Bypass Vulnerability	WordPress WooCommerce Payments plugin version: 4.8.0 - 5.6.1	✗	✗	✓
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2022-0543	Debian-specific Redis Server Lua Sandbox Escape Vulnerability	Debian-specific Redis Server	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2017-0213	Microsoft Windows Privilege Escalation Vulnerability	Microsoft Windows	✗	✓	✓
CVE-2023-38606	Apple Multiple Products Kernel Unspecified Vulnerability	iOS version before: 15.7.1. macOS version: 13.0 22A380 - 13.4.1 22F82, watchOS, tvOS	✓	✓	✓
CVE-2023-26077	Atera Agent Windows Privilege Escalation	Atera Agent versions 1.8.3.6 and before	✓	✗	✓
CVE-2023-26078	Atera Agent Windows Privilege Escalation	Atera Agent versions 1.8.3.6 and before	✓	✗	✓
CVE-2023-35078	Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	Ivanti Endpoint Manager Mobile	✓	✓	✓
CVE-2023-37580	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	Zimbra Collaboration: 8.8.15 - 8.8.15 Patch 40	✓	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Lockbit Ransomware	Ransomware	-	-	-	Unknown
PlugX variant	RAT	-	-	-	Spear-Phishing Emails
RUSTBUCKET	Backdoor	-	-	-	Unknown
Crysis Ransomware	Ransomware	-	-	-	Externally Exposed RDP
Venus Ransomware	Ransomware	-	-	-	Externally Exposed RDP
GorjolEcho	Backdoor	-	-	-	Phishing
CharmPower (aka GhostEcho or POWERSTAR)	Backdoor	-	-	-	Phishing
NokNok	Backdoor	-	-	-	Phishing
Big Head Ransomware	Ransomware	-	-	-	Spear-Phishing Emails
TOITOIN Trojan	Trojan	-	-	-	Spear-Phishing Emails
PyLoose	Fileless	-	-	-	Exploitation
RomCom	Backdoor	CVE-2023-36884	Office and Windows	✓	Phishing
PicassoLoader	Loader	-	-	-	Malicious Microsoft Office documents
CustomerLoader	Loader	-	-	-	Phishing
LokiBot	Trojan	CVE-2021-40444 CVE-2022-30190	Windows Server & Microsoft Internet Explorer	✓	Unknown

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Sardonic backdoor	Backdoor	-	-	-	Spear-phishing
Noberus ransomware	Ransomware	-	-	-	Sardonic backdoor
P2PInfect	Worm	CVE-2022-0543	Debian-specific Redis Server	✓	Exploits the CVE-2022-0543 vulnerability
Deed RAT	RAT	CVE-2017-0213	Microsoft Windows	✓	Spear-phishing
Voidoor	Backdoor	CVE-2017-0213	Microsoft Windows	✓	Delivered by Deed RAT
ShadowPad	Backdoor	CVE-2017-0213	Microsoft Windows	✓	Spear-phishing
PlugX	RAT	CVE-2017-0213	Microsoft Windows	✓	Spear-phishing
Kanti ransomware	Ransomware	-	-	-	Phishing
DeliveryCheck	Backdoor	-	-	-	Phishing
KAZUAR	Backdoor	-	-	-	Phishing
Cigril	Trojan	-	-	-	Spam emails
Realst	InfoStealer	-	MacOS	-	Malicious websites
Fenix	Botnet	-	-	-	Phishing emails
Decoy Dog	RAT	-	-	-	Phishing
Pupy	RAT	-	-	-	Phishing emails

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Lazarus	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	-	RUSTBUCKET	macOS
8Base	Monetary Gains	-	-	-	-
Charming Kitten	Information theft and espionage	Iran	-	GorjolEcho, NokNok, CharmPower, and BellaCiao	macOS, Windows
Storm-0978	Espionage	Russia	CVE-2023-36884	RomCom Backdoor	Office and Windows
TA445	Information theft and espionage, Sabotage and destruction	Belarus	-	PicassoLoader, AgentTesla, Cobalt Strike Beacon and njRAT	-
FIN8	Financial crime	Unknown	-	Sardonic backdoor and Noberus ransomware (aka BlackCat, ALPHV)	-
Turla	Information theft and espionage	Russia	-	DeliveryCheck , KAZUAR	Windows

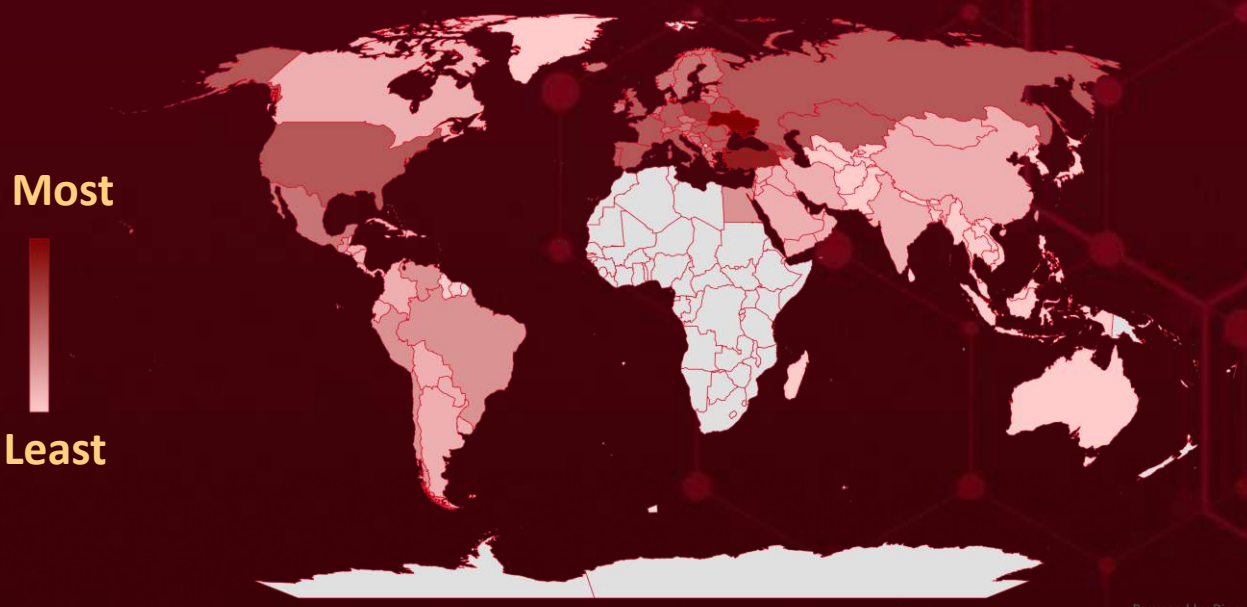
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Space Pirates	Information theft and espionage	China	CVE-2017-0213	Deed RAT, Voidoor, ShadowPad, and PlugX	Microsoft Windows
Storm-0558	Information theft and espionage	China	-	Cigril	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
WordPress	Plugin	WordPress Ultimate Member Plugin <= 2.6.6, WordPress WooCommerce Payments plugin version: 4.8.0 - 5.6.1
	Operating System	Apple Safari up to 16.5.2 Apple iOS and iPadOS up to 16.5.1, Apple macOS up to 13.4.1., iOS version before: 15.7.1. macOS version: 13.0 22A380 - 13.4.1 22F82, watchOS, tvOS
vmware	Application	VMware Aria Operations for Logs: before 8.12
Microsoft	Operating System, Application	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2 Microsoft Internet Explorer: 11 - 11.1790.17763.0, Microsoft Office: 2013 - 2019, Microsoft Outlook: 2013 -2016, and Microsoft SharePoint Enterprise Server: 2016 -2016
Adobe	Application	Adobe ColdFusion 2018: Update 17 and earlier versions Adobe ColdFusion 2021: Update 7 and earlier versions Adobe ColdFusion 2023: Update 1 and earlier versions
citrix	Application	Citrix NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13; Citrix NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13; Citrix NetScaler ADC 13.1-FIPS before 13.1-37.159; Citrix NetScaler ADC 12.1-FIPS before 12.1-55.297; Citrix NetScaler ADC 12.1-NDcPP before 12.1-55.297
redis	Application	redis (Debian package): 5.0.3-4+deb10u1 - 5:6.0.16-1+deb11u1
ATERA	Application	Atera Agent versions 1.8.3.6 and before

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
ivanti	Endpoint Manager Application	Ivanti Endpoint Manager Mobile
zimbra	Application	Zimbra Collaboration: 8.8.15 - 8.8.15 Patch 40

Targeted Countries



Color	Countries
	Ukraine
	Turkey
	Cyprus
	Poland
	Georgia
	Moldova
	Bulgaria
	Portugal
	Belarus
	United States
	France
	Belgium
	Russia
	Romania
	Serbia
	Azerbaijan
	Slovakia
	Spain
	Armenia
	Germany
	United Kingdom
	Hungary
	Kazakhstan

Color	Countries
	Italy
	Montenegro
	Sweden
	Austria
	Estonia
	Denmark
	Finland
	North Macedonia
	Albania
	Slovenia
	Greece
	Andorra
	Iceland
	Vatican City
	Ireland
	Netherlands
	Bosnia and Herzegovina
	Norway
	Latvia
	San Marino
	Liechtenstein
	Croatia

Color	Countries
	Lithuania
	Switzerland
	Luxembourg
	Czechia
	Malta
	Mexico
	Monaco
	Venezuela
	Chile
	Guatemala
	Brazil
	Taiwan
	Egypt
	Peru
	Colombia
	Nicaragua
	El Salvador
	Iraq
	Yemen
	Bahrain
	Jordan
	Oman
	Syria

Color	Countries
	Palestine
	China
	Panama
	Saudi Arabia
	Paraguay
	Costa Rica
	Cuba
	Argentina
	Ecuador
	Lebanon
	Bolivia
	Iran
	Uruguay
	India
	United Arab Emirates
	Israel
	Haiti
	Canada
	Honduras
	Qatar
	Dominican Republic
	Mongolia
	Kuwait

Color	Countries
	Suriname
	Uyghur
	Malaysia
	Myanmar
	Australia
	Nepal
	Madagascar
	Hong Kong
	Martinique
	Akrotiri and Dhekelia
	Vietnam
	North Korea
	Belize
	Bahamas
	Greenland
	Dominica
	Thailand
	Indonesia
	Maldives
	Pakistan
	Bhutan
	British Virgin Islands

Targeted Industries

Most

Least

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1566** Phishing	**T1027** Obfuscated Files or Information	**T1588** Obtain Capabilities	**T1190** Exploit Public-Facing Application
T1588.005 Exploits	**T1588.006** Vulnerabilities	**T1082** System Information Discovery	**T1203** Exploitation for Client Execution	**T1068** Exploitation for Privilege Escalation
T1547 Boot or Logon Autostart Execution	**T1059.001** PowerShell	**T1140** Deobfuscate/ Decode Files or Information	**T1071** Application Layer Protocol	**T1036** Masqueradin g
T1562 Impair Defenses	**T1055** Process Injection	**T1083** File and Directory Discovery	**T1547.001** Registry Run Keys / Startup Folder	**T1204** User Execution
T1070 Indicator Removal	**T1071.001** Web Protocols	**T1486** Data Encrypted for Impact	**T1573** Encrypted Channel	**T1574** Hijack Execution Flow

Top Indicators of Compromise (IOCs)

Attack	TYPE	VALUE
Lockbit Ransomware	SHA256	0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194, 498e3b7a867d41b5a3af3910d2aa6231612c787ce8a4bc14ab03f800caab130f, af4c28fb1c65ebe93181b67d279733e864cafab5919a7aa7eced93fc8113df16, 984d96730ae19d4532325c6fcbd34580fb02fbe454781b589d2eea6090ea2b6d, 2cee882bd0dc4267bacf099ac4571c319ac547be12b955f7ccb2f0144ae4876, 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75, 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75, 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c, 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c, 5a13ac97ce91d5b095c7154fe756615fa0730c17ddf432ae4af6c42d2c29946d, 9aa5bcee06109d52fade97ad21317ff951abc656ba4c800441bacfec00328fd8, 379c4620d6f482e153d7033bba21da5d8027387c0e60e3497b63d778dcafd888, 0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194, b964a5253c25465633ef8c2e7f77703d27227bfc0b13a7ca49d187dadc4d38ae, ba0eefdfbd1421d37d47f3feaae8e768a4679d6b544bb97f5237319e8ab0b122, f9dbdb825067616070c64565b6b27dc872c4a7219856eb5f8eb3eb1eb1463423,

Attack	TYPE	VALUE
RUSTBUCKET	SHA256	788261d948177acfcfeb1f839053c8ee9f325bd6fb3f07637a7465acdbbef76a, 1031871a8bb920033af87078e4a418ebd30a5d06152cd3c2c257aecdf8203ce6, 9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747, 7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387, ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41, de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500, 4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16, fe8c0e881593cc3dfa7a66e314b12b322053c67cbc9b606d5a2c0a12f097ef69, 7887638bcafd57e2896c7c16698e927ce92fd7d409aae698d33cdca3ce8d25b8
	Domains	webhostwatto.work[.]gd, crypto.hondchain[.]com, starbucls[.]xyz, jaicvc[.]com, docsend.linkpc[.]net, companydeck[.]online
	IPv4	104.168.167[.]88, 64.44.141[.]15
GorjolEcho	Domain	library-store.camdvr[.]org, fuschia-rhinestone.cleverapps[.]io, filemanager.theworkpc[.]com
	IPv4	144.217.129[.]176
CharmPower	SHA256	b79d28fe5e3c988bb5aadb12ce442d53291dbb9ede0c7d9d64eec078beba5585, 9777f106ac62829cd3cfdbc156100fe892cfc4038f4c29a076e623dc40a60872, 977cf5cc1d0c61b7364edcf397e5c67d910fac628c6c9a41cf9c73b3720ce67f, 823ffbcc62bd3296957a47fbf8c238949584996911e71d5140a25d0a8f6abd80
RomCom	SHA1	fb4ad5d21f0d8c6755eb4addba0ac288bd2574b6
	MD5	059175be5681a633190cd9631e2975f6

Attack	TYPE	VALUE
RomCom	SHA256	d4a847fa9c4c7130a852a2e197b205493170a8b44426d9ec481fc4b285a92666, a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f, e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539, d3263cc3eff826431c2016aee674c7e3e5329bebfb7a145907de39a279859f4a, 3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97
LokiBot	SHA256	127c29b65ebf2143b66e5c60fcdbae43c4789c836e273e4f996efd0e56040e8f, 30c51845ddd526bf0472c52af64b591baee970f2ab39bec2d6bea1a64b5c7f9b, 827555c608d1e12973d7c28d45b4ca8d5342d1dc77b12a5d403a32d83e591fb8, 5a7a9170adc2fe2a4167392be4532c945faef7a2d0f9a18d79cf9d9cb459d61a, bd32a9cbb3ed1a616bf91d7121386a78cf6bb2b8c904088d1daa3982edb4fb8b, bd32a9cbb3ed1a616bf91d7121386a78cf6bb2b8c904088d1daa3982edb4fb8b, c98512ee509dca89b8f6073faf337cda879e39f669add3632011590411878c9a, 2af1bb0bba5a26df1520604cbf7e84bf8bd19d4f9f23167b3408c78b545b7190, 4e49637ce52ae9105d53e9de9994e680ba5894f25ffffbc2272e9d95c0adfbf1, 9f54a66ad8152ec7b3923d98a8261ba15d643dc241cdf995e5332bcf4b91eb0a, 59bfe87a4f70ad80b96e5d135d9688324b18009f800b7001c6efa116fb780d2f, 7559e6ca8b77400f88bf4e67208a1c32570a670068eccae9e3d226cc5471bd47, 9346d441c3136edb70bc96afd06717fbb96074592bcb4896741ede01be7925ed, 61868e99c4fff04df6ba82cbd4eb414c132c5932acd762f379b4c0fe852968bf, 73ca91a52ed319db604f0951f4b95ebd4a93eabc6f410e3d7f7ffd33efa29982, cabcb0bfd5b86be43f98e9ea8dcb92e8ef87d1c98e326b2effa2d39482bb882a, b0504206461bb3a04bc80d299501c2d2765f097bc621a0e86e5b9e889f383287, 42ed620528c450c61185a065b7e73c5d8207c731acb7bf965df2a49c030de497

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3460		WordPress Ultimate Member Plugin <= 2.6.6	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ultimatemember:ultimate-member:2.6.5:*:*:*:*:wordpress:*:*	-
WordPress unauthenticated Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-269	T1595- Active Scanning, T1595.002- Vulnerability Scanning, T1068- Exploitation for Privilege- Escalation, T1190- Exploit Public-Facing- Application, T1136- Create Account, T1078- Valid Accounts	Update the plugin to version 2.6.7 or higher. You can update the plugin version to the required version through the WordPress Admin dashboard.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-37450		Apple Safari up to 16.5.2 Apple iOS and iPadOS up to 16.5.1 Apple macOS up to 13.4.1.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:safari:16.5.0:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:16.5.1:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:16.5.2:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:16.5.0:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:16.5.1:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:16.5.0:*:*:*:*:*:*:* cpe:2.3:o:apple:mac_os:13.4.0:*:*:*:*:*:*:* cpe:2.3:o:apple:mac_os:13.4.1:*:*:*:*:*:*:*	-
Apple WebKit Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1595- Active Scanning, T1595.002- Vulnerability Scanning, T1068- Exploitation for Privilege- Escalation, T1190- Exploit Public-Facing- Application, T1136- Create Account, T1078- Valid Accounts	https://support.apple.com/en-gb/HT213826; https://support.apple.com/en-gb/HT213823; https://support.apple.com/en-gb/HT213825

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36874	✗	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Microsoft Windows Error Reporting Service Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1404: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36874

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32049	✗	Windows: 10 - 11 22H2 Windows Server: 2016 - 2022 20H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Microsoft Windows Defender SmartScreen Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-254	T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32046		Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2 Microsoft Internet Explorer: 11 - 11.1790.17763.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Microsoft Windows MSHTML Platform Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1404: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36884		Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2 Microsoft Office: 2013 - 2019 Microsoft Word: 2013 Service Pack 1 - 2019	Storm-0978 (aka DEV-0978, RomCom)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	RomCom Backdoor
Office and Windows HTML Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-20	T1203: Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35311		Microsoft Office: 2013 - 2019 Microsoft Outlook: 2013 -2016 Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:microsoft_office:2019:*:*:*:*:*:*:*	-
Microsoft Outlook Security Feature Bypass Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH DETAILS**
	CWE-254	T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311

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-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

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-26078		Atera Agent versions 1.8.3.6 and before	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atera:agent:1.8.4.x:*:*:*:*:*:*:*	-
Atera Agent Windows Privilege Escalation			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-648	T1211: Exploitation for Defense Evasion	The vulnerability fixed in ATERA AGENT version 1.8.4.9

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38606		iOS version before: 15.7.1. macOS version: 13.0 22A380 - 13.4.1 22F82, watchOS, tvOS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:-:*:*:*:*:*:*:*	-
Apple Multiple Products Kernel Unspecified Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter; T1068:Exploitation for Privilege Escalation	https://support.apple.com/en-us/HT213841; https://support.apple.com/en-us/HT213842; https://support.apple.com/en-us/HT213843; https://support.apple.com/en-us/HT213844; https://support.apple.com/en-us/HT213845; https://support.apple.com/en-us/HT213846; https://support.apple.com/en-us/HT213848

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-26077		Atera Agent versions 1.8.3.6 and before	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atera:agent:1.8.3.x:*:*:*:*:*:*:*	-
Atera Agent Windows Privilege Escalation			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-379	T1404: Exploitation for Privilege Escalation	The vulnerability fixed in ATERA AGENT version 1.8.3.7

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-37580		Zimbra Collaboration: 8.8.15 - 8.8.15 Patch 40	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:synacor:zimbra_collaboration:8.8.15:Patch 40:*:*:*:*:*:*	-
Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-79	T1190: Exploit Public-Facing Application	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P41; https://wiki.zimbra.com/wiki/Security_Center

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35078		Ivanti Endpoint Manager Mobile	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1404: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	The vulnerability was fixed in Ivanti EPMM versions 11.8.1.1, 11.9.1.1, 11.10.0.2

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Lockbit Ransomware	The Lockbit Ransomware group, National Hazard Agency, has claimed of targeting TSMC and is demanding a 70-million-dollar Ransom, Attackers are claiming to be in possession of sensitive information and threaten to release data in the public domain	Unkown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Exfiltration, Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PlugX variant	A Chinese nation-state group has been persistently conducting a SmugX campaign targeting Foreign Affairs ministries and embassies in Europe. They employ HTML smuggling techniques to distribute a new variant of the PlugX remote access trojan.	Spear-Phishing Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Information Theft and Espionage.	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RUSTBUCKET	The RUSTBUCKET malware family is undergoing active development, incorporating new persistence capabilities and focusing on reducing its signature detection. This variant of RUSTBUCKET specifically targets macOS systems.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

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
Crysis Ransomware	The CrySIS aka Dharma ransomware family is operating as ransomware-as-a-service (RaaS) model. Crysis ransomware scoured the internet using brute force or dictionary attacks, searching for vulnerable RDP endpoints.	Externally Exposed RDP	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Venus Ransomware	The threat actors behind the Crysis ransomware are currently utilizing the Venus ransomware as a component of their attack strategy, with a primary focus on targeting vulnerable systems through active RDP.	Externally Exposed RDP	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GorjolEcho	A new PowerShell backdoor called GorjolEcho establishes persistence on compromised systems. GorjolEcho enables the threat actor to conduct intrusive activities such as information exfiltration and potential module downloads for espionage purposes.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-

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
CharmPower (aka GhostEcho or POWERSTAR)	The new modular PowerShell-based framework dubbed CharmPower, is used to establish persistence, gather information, and execute commands.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft, and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
NokNok	Charming Kitten ported its malware and attempted to launch an Apple-flavored infection chain dubbed NokNok.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft, and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Big Head Ransomware	Big Head ransomware is a new ransomware, and its variants suggest a shared source, distributed through deceptive Windows updates and Word installer disguises.	Spear-Phishing Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Exfiltration, Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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
TOITOIN Trojan	TOITOIN malware campaign, targeting businesses in the LATAM region, employs sophisticated techniques and multi-stage infection chains with numerous malware samples disguised as compressed ZIP archives hosted on Amazon EC2.	Spear-Phishing Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Information Theft and System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PyLoose	A new fileless malware called PyLoose targets cloud workloads by loading an XMRig Miner directly into memory using Python code and the memfd technique.	Exploitation	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Fileless		Cryptomining	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RomCom	The RomCom backdoor is a notorious malware, that is distributed through phishing campaigns and disguised as well-known software, allowing unauthorized access to compromised systems.	Phishing	CVE-2023-36884
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage and Unauthorized access	Office and Windows
ASSOCIATED ACTOR			**Mitigation LINK**
Storm-0978			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

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
PicassoLoader	PicassoLoader is a downloader malware identified in ongoing cyberattacks targeting Ukraine and Poland. It serves as a conduit for deploying subsequent payloads like Cobalt Strike beacons and njRAT, aimed at stealing information and establishing remote access.	Malicious Microsoft Office documents	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Stealing information and establishing remote access	-
ASSOCIATED ACTOR			PATCH LINK
TA445			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CustomerLoader	A covert .NET loader, known as CustomerLoader, was specifically designed to facilitate the retrieval, deciphering, and activation of subsequent payloads.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Malware propagation	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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)			-

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
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

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)			-

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

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

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

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

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

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**
-			-

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			-

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			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cigril	Cigril is a Trojan horse malware that steals sensitive information from infected devices. It can be spread through malicious attachments or links in spam emails.	Spam emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Theft, Fraud	-
ASSOCIATED ACTOR			**PATCH LINK**
Storm-0558			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Realst	Realst Infostealer is a macOS malware that steals sensitive information, such as passwords, credit card numbers, and cryptocurrency wallets. It is distributed via malicious websites advertising fake blockchain games.	Malicious websites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		Information Theft and System Compromise	MacOS
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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
Fenix	Fenix Botnet is a modular botnet that targets users in Mexico and Chile. It can be used to perform a variety of malicious tasks, such as DDoS attacks, credential theft, and data exfiltration. It is spread through malicious websites and phishing emails.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		DDoS attacks, credential theft, and data exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Decoy Dog	Decoy Dog, a sophisticated malware toolkit uses DNS for C2 communication, evading detection with its wildcard-type behavior and encryption methods. Its origin remains mysterious, and the malware's capabilities surpass traditional RATs like Pupy, making it highly elusive.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Pupy	Pupy RAT is an open-source Remote Access Trojan (RAT) written in Python that is designed to steal sensitive information from infected devices. Pupy RAT is a modular malware, which means that it can be customized to perform a variety of malicious tasks.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Information Theft and Data exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten (APT35)			-

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Lazarus (aka Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, Diamond Sleet)	North Korea	Aerospace, Defense, Energy, Engineering, Financial, Government, Healthcare, Media, Shipping and Logistics, Technology, and Cryptocurrency	Worldwide
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	RUSTBUCKET	macOS
TTPs			
T1071.001- Web Protocols, T1071- Application Layer Protocol, T1106- Native API, T1059- Command and Scripting Interpreter, T1647- Plist File Modification, T1547- Boot or Logon Autostart Execution, T1082- System Information Discovery, T1218- System Binary Proxy Execution, T1102- Web Service, T1566- Phishing, T1036- Masquerading, T1105-Ingress Tool Transfer, T1204- User Execution			

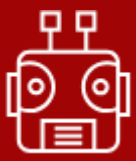
NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 8Base	-	United States, Brazil, Australia, Germany, United Kingdom, Mexico, Portugal, Belgium, Egypt, China, Spain, Madagascar, France, Peru, Canada, Turkey, Guatemala, Venezuela, India, Italy	Business Services, Finance, Manufacturing, Technology, Healthcare, Real Estate, Construction, Hospitality, Non-Profit, Automotive, Engineering, Food
	MOTIVE		
	Monetary Gains		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
T1588- Obtain Capabilities, T1588.001- Malware, T1547- Boot or Logon Autostart Execution, T1547.001- Registry Run Keys/Startup Folder, T1134- Access Token Manipulation, T1134.001- Token Impersonation/ Theft, T1562- Impair Defenses, T1562.001- Disable or Modify Tools, T1027- Obfuscated Files or Information, T1027.002- Software Packing, T1135- Network Share Discovery, T1486- Data Encrypted for Impact, T1490- Inhibit System Recovery, T1561- Disk Wipe			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, TarhAndishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm)	Iran	Foreign affairs, Think Tanks, and Nuclear security	Middle East, United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	GorjolEcho, NokNok, CharmPower, and BellaCiao	macOS, Windows
TTPs			
T1071- Application Layer Protocol, T1041- Exfiltration Over C2 Channel, T1059-Command and Scripting Interpreter, T1590-Gather Victim Network Information, T1547-Boot or Logon Autostart Execution, T1082- System Information Discovery, T1218- System Binary Proxy Execution, T1102- Web Service, T1566- Phishing, T1036- Masquerading, T1204- User Execution, T1059.005- Visual Basic, T1204.001- Malicious Link, T1059.001- PowerShell, T1055- Process Injection			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Storm-0978 (aka DEV-0978, RomCom)	Russia	Finance, Telecommunications, Political, Defense, and Government	Europe, North America, and Ukraine
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-36884	RomCom Backdoor	Office and Windows
TTPs			
T1566: Phishing; T1204: User Execution; T1082: System Information Discovery; T1217: Browser Information Discovery; T1083: File and Directory Discovery; T1070: Indicator Removal; T1534: Internal Spearphishing; T1550: Use Alternate Authentication Material; T1486: Data Encrypted for Impact; T1490: Inhibit System Recovery; T1071: Application Layer Protocol; T1005: Data from Local System			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 TA445 (Operation Ghostwriter, UNC1151, UAC-0051, PUSHCHA, DEV-0257, Storm-0257)	Belarus	Government, Military, Business, Civilian	Ukraine and Poland
	MOTIVE		
	Information theft and espionage, Sabotage and destruction		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PicassoLoader, AgentTesla, Cobalt Strike Beacon and njRAT	-
TTPs			
T1574: Hijack Execution Flow; T1140: Deobfuscate/Decode Files or Information; T1574.001: DLL Search Order Hijacking; T1566: Phishing; T1204: User Execution; T1204.002: Malicious File; T1059.005: Visual Basic; T1059: Command and Scripting Interpreter; T1564: Hide Artifacts; T1036: Masquerading; T1027: Obfuscated Files or Information; T1218.010: Regsvr32; T1218: System Binary Proxy Execution; T1218.011: Rundll32			

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

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Storm-0558	China	Government, Diplomatic entities, Media companies, Think tanks, and Telecommunications	US, Europe, Taiwan, and Uyghur
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Cigril	-
TTPs			
T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1589.001: Credentials Token , T1134.001: Token Impersonation/Theft, T1134: Access Token Manipulation , T1589: Gather Victim Identity Information, T1059.006: Python , T1505.003: Web Shell, T1505: Server Software Component, T1574.001: DLL Search Order Hijacking, T1574: Hijack Execution Flow, T1003.001: LSASS Memory, T1003: OS Credential Dumping, T1003.002: Security Account Manager, T1078: Valid Accounts , T1102: Web Service, T1567: Exfiltration Over Web Service, T1566: Phishing, T1090: Proxy, T1543.001: Launch Agent , T1543: Create or Modify System Process , T1106: Native API, T1190: Exploit Public-Facing Application			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	T1589.001: Credentials
	T1590: Gather Victim Network Information	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1598: Phishing for Information	T1598.002: Spearphishing Attachment
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1584: Compromise Infrastructure	
	T1588: Obtain Capabilities	T1588.001: Malware
		T1588.005: Exploits
		T1588.006: Vulnerabilities
TA0001: Initial Access	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.002: At
		T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
	T1106: Native API	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution
TA0003: Persistence	T1037: Boot or Logon Initialization Scripts	
	T1053: Scheduled Task/Job	T1053.002: At
		T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1136: Create Account	
	T1137: Office Application Startup	T1137.001: Office Template Macros
	T1176: Browser Extensions	
	T1197: BITS Jobs	
	T1505: Server Software Component	T1505.003: Web Shell

Tactic	Technique	Sub-technique
TA0003: Persistence	T1543: Create or Modify System Process	T1543.001: Launch Agent
		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
		T1547.009: Shortcut Modification
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
TA0004: Privilege Escalation	T1037: Boot or Logon Initialization Scripts	
	T1053: Scheduled Task/Job	T1053.002: At
		T1053.005: Scheduled Task
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.012: Process Hollowing
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/ Theft
	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.009: Shortcut Modification
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.001: Binary Padding
		T1027.002: Software Packing
		T1027.005: Indicator Removal from Tools
		T1027.007: Dynamic API Resolution
		T1027.009: Embedded Payloads
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
		T1036.008: Masquerade File Type
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.012: Process Hollowing
	T1070: Indicator Removal	T1070.004: File Deletion
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1112: Modify Registry	
	T1127: Trusted Developer Utilities Proxy Execution	
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/ Theft

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1197: BITS Jobs	
	T1218: System Binary Proxy Execution	T1218.010: Regsvr32
		T1218.011: Rundll32
	T1220: XSL Script Processing	
	T1480: Execution Guardrails	T1480.001: Environmental Keying
	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
	T1497: Virtualization/Sandbox Evasion	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1550: Use Alternate Authentication Material	
	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
	T1620: Reflective Code Loading	
	T1647: Plist File Modification	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
	T1040: Network Sniffing	
	T1056: Input Capture	T1056.001: Keylogging
	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
	T1557: Adversary-in-the-Middle	
TA0007: Discovery	T1007: System Service Discovery	
	T1010: Application Window Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1040: Network Sniffing	
	T1046: Network Service Discovery	
	T1057: Process Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.001: Local Account
		T1087.002: Domain Account
	T1135: Network Share Discovery	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1217: Browser Information Discovery	
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1614: System Location Discovery	T1614.001: System Language Discovery
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
		T1021.004: SSH
	T1534: Internal Spearphishing	
	T1550: Use Alternate Authentication Material	
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
	T1113: Screen Capture	
	T1119: Automated Collection	
	T1557: Adversary-in-the-Middle	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0011: Command and Control	T1001: Data Obfuscation	
	T1008: Fallback Channels	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1090: Proxy	T1090.001: Internal Proxy
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol
	T1567: Exfiltration Over Web Service	
TA0040: Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1496: Resource Hijacking	
	T1561: Disk Wipe	T1561.001: Disk Content Wipe

Top 5 Takeaways

#1 In **July**, there were **sixteen zero-day** vulnerabilities. Among these is a **Celebrity Vulnerability**, exploited by **LokiBot** Data Exfiltrating Trojan Targeting Windows Systems.

#2 Throughout the month, various ransomware strains including **Crysis**, **Venus**, **Big Head**, **Noberus**, and **Kanti** actively targeted victims.

#3 Numerous malware families have been observed targeting victims in the wild. These include **RomCom, PyLoose, PlugX, TOITOIN, P2PInfect, DecoyDog and CustomerLoader.**

#4 There were a total of **9** active **adversaries** identified across multiple campaigns. Their focus was directed toward the following key industries: **Technology**, **Government**, **Financial**, **Defense**, and **Cryptocurrency**.

#5 Finally, the **Zero-day** vulnerability, **CVE-2023-36884**, was exploited by the **Storm-0978** threat actor to deploy **RomCom Backdoor** and **P2PInfect** Worm Strikes, Posing a Significant Threat to **307,000 Systems.**

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **21 significant vulnerabilities** and block the indicators related to the **9 active threat actors, 30 active malware,** and **168 potential MITRE TTPs.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, who can get comprehensive insights into their threat exposure and take action easily through the HivePro Uni5 dashboard by:

- Running a scan to discover the assets impacted by the **significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to **active threat actors, active malware**, and **potential MITRE TTPs** in Breach and Attack Simulation(BAS).

Hive Pro Threat Advisories (JULY 2023)

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY	SUNDAY
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Click on any of the icons to get directed to the advisory

	Red Vulnerability Report		Amber Attack Report
	Amber Vulnerability Report		Red Actor Report
	Green Vulnerability Report		Amber Actor Report
	Red Attack Report		

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.

Social engineering: is an attack that relies on human interaction to persuade people into compromising security. It involves various strategies aimed at extracting specific information or performing illicit activities from a target.

Supply chain attack: Also known as a value-chain or third-party attack, occurs when an outside partner or provider with access to your systems and data infiltrates your system. The purpose is to gain access to source codes, development processes, or update mechanisms in order to distribute malware by infecting legitimate programs.

Eavesdropping: Often known as sniffing or spying, is a significant risk in cybersecurity. Passwords, credit card information, and other sensitive data are easily stolen during these attacks as they are transmitted from one device to another. This type of network attack often occurs when unsecured networks, such as public Wi-Fi connections or shared electronic devices, are used.

Glossary:
CISA KEV - Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities
CVE - Common Vulnerabilities and Exposures
CPE - Common Platform Enumeration
CWE - Common Weakness Enumeration

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Lockbit Ransomware	SHA256	0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194, 498e3b7a867d41b5a3af3910d2aa6231612c787ce8a4bc14ab03f800caab130f, af4c28fb1c65ebe93181b67d279733e864cafab5919a7aa7eced93fc8113df16, 984d96730ae19d4532325c6fcbd34580fb02fbe454781b589d2eea6090ea2b6d, 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75, 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75, 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c, 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c, 5a13ac97ce91d5b095c7154fe756615fa0730c17ddf432ae4af6c42d2c29946d, 9aa5bcee06109d52fade97ad21317ff951abc656ba4c800441bacfec00328fd8, 379c4620d6f482e153d7033bba21da5d8027387c0e60e3497b63d778dcafd888, 0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194, b964a5253c25465633ef8c2e7f77703d27227bfc0b13a7ca49d187dadc4d38ae, ba0eefdfbd1421d37d47f3feaae8e768a4679d6b544bb97f5237319e8ab0b122, f9dbdb825067616070c64565b6b27dc872c4a7219856eb5f8eb3eb1eb1463423, 2e218735fa53e036659ea721bfd7b97e2af67b7eda648e9e2579356eb20899d9, 286726ecca68f8c2752116258aba0cd35c051a6342043ee1add84b890654276f,

Attack Name	TYPE	VALUE
Lockbit Ransomware	SHA256	1f0e4cbc1a4b52b6d7e4188e4a835a904cf783c75db9a066df4201452bd9647d, de7f501e4a17898e85229b962e2f43b9a20d995c8a9fe0cad4536adc8fbd9f48, 8989a9aec8d2c4d61fa399a97807f8e62814b1a55fecbd38d11d4d35fdf4a7d1, 01bf78841b63bcdd8280157c486b45ad74811c0251140a054de81a925ce7f716, ab4d20b73c7358f1e3a60145d5debc791a17416e2a88eb39f80ec1f53985fad5, 9366a5b8021d0283156986bbf020c99ae5e2a3dcbbaa03db934e94bfa7088b86, 4bdda7dd3bbe1f9cb0a7d42f6947ba0f6442e52758bd2638541f9409b573d5c9, 6b4502d8ba3cff1a3139f72cdad863d53551b65b8c38d7b838d64212822e4630, 4d0f95028bb6a04e64550872ddeef6b0c6fa4a5bd368736da47401420df2bee7, cfc45c36b4c731f2308e19a087c3dc3fb7b12eef93e171e8e86e2134ead325ee, 4134d5d8f7b038e23e7887db56bb3ad295341a1aaf0bebe6be21d901d06dd662, 153fc9e90b955e2cfaf91b86888a29fdd8685144a3802f5e90b95b64116cdd33, 00accc2c186201607d3e36c1b013872ac51d4f805f23e625dc70154fb58fd4f4, 734955fdb84b29fa1aa87aa0af2ebf155125917a6b61ffe4b4dc7030dd212309, e47b928d0fc16348b828abeb3c2106a6d752512f60ef4583d6532cc0dbebebbf, 239c9969fd07e1701a129cfd033a11a93ee9e88e4df4f79b7c5c0dd5bba86390, a439c5093801d3b12e2f79b64c0b65bdf148eb6eca8c1e3d179af5ab4995034d, 54ac7ac6db6fcec5234454430513d1d2787ee8a48aa60fbf95c1af27534fdb4a, A9abab8ab44ccec6321da83d9960a1f30ba783e02b6e0ba3f2e9d19cee76b39b
PlugX variant	SHA256	edb5d4b454b6c7d3abecd6de7099e05575b8f28bb09dfc364e45ce8c16a34fcd, 736451c2593bc1601c52b45c16ad8fd1aec56f868eb3bba333183723dea805af, 0e4b81e04ca77762be2afb8bd451abb2ff46d2831028cde1c5d0ec45199f01a1,

Attack Name	TYPE	VALUE
PlugX variant	SHA256	989ede1df02e4d9620f6caf75a88a11791d156f62fdea4258e12d972df76bc05, 10cad59ea2a566597d933b1e8ba929af0b4c7af85481eacaab708ef4ddf6e0ee, 324bfb2f414be221e24aaa9fb22cb49e4d4c0904bd7c203afdff158ba63fe35b, c96723a68fc939c835578ff746f7d4c5371cb82a9c0dffe360bb656acea4d6e1, 9ce5abd02d397689d99f62dfbd2a6a396876c6629cb5db453f1dcbbc3465ac9a, 5f751fb287db51f79bb6df2e330a53b6d80ef3d2af93f09bb786b62e613514db, baca1159acc715545a787d522950117eae5b7dc65efacfe86383f62e6b9b59d3, 720a70ca6ee1fbaf06c7cb60d14e27391130407e34e13a092d19f1df2c9c6d05, 460c459db77c5625ed1c029b2dd6c6eae5e631b81a169494fb0182d550769f76, 277390cc50e00f52e76a6562e6e699b0345497bd1df26c7c41bd56da5b6d1347, 3c6ace055527877778d989f469a5a70eb5ef7700375b850f0b1b8414151105ee, 27a61653ce4e503334413cf80809647ce5dca02ff4aea63fb3a39bc62c9c258c, ce308b538ff3a0be0dbcee753db7e556a54b4aeddbddd0c03db7126b08911fe2, fd0711a50c8af1dbc5c7ba42b894b2af8a2b03dd7544d20f5a887c93b9834429, 3489955d23e66d6f34b3ada70b4d228547dbb3ccb0f6c7282553cbbdeaf168cb, 04b99518502774deb4a9d9cf6b54d43ff8f333d8ec5b4b230c0e995542bb2c61, bd3881964e351a7691bfc7e997e8a2c8ce4a8e26b79e3712d0cbdc484a5646b6, ea2869424df2ffbb113017d95ae48ae8ed9897280fd21b26e046c75b3e43b25a, b00c252a60171f33e32e64891ffe826b8a45f8816acf778838d788897213a405, 2bc30ced135acd6a506cfb557734407f21b70fecd2f645c5b938e14199b24f1e, 0d13a503d86a6450f71408eb82a196718324465744bf6b8c4e0a780fd5be40c0, 0bdfb922a39103658195d1d37ff584d24f7bd88464e7a119e86d6e3579958cc1, a0879dd439c7f1ed520aad0c309fe1dbf1a2fc41e2468f4174489a0ec56c47c7, bddbc529f23ab6b865bc750508403ef57c8cf77284d613d030949bd37078d880,

Attack Name	TYPE	VALUE
PlugX variant	SHA256	4547914e17c127d9b53bbc9d44de0e5b867f1a86d2e5ede828cd3188ed7fe838, 0032d5430f1b5fcfb6a380b4f1d226b6b919f2677340503f04df04235409b2d0, 62c2e246855d589eb1ec37a9f3bcc0b6f3ba9946532aff8a39a4dc9d3a93f42c, f7d35cb95256513c07c262d4b03603e073e58eb4cd5fa9aac1e04ecc6e870d42, bf4f8a5f75e9e5ecd752baa73abddd37b014728722ac3d74b82bffa625bf09b5, 8a6ef9aa3f0762b03f983a1e53e8c731247273aafa410ed884ecd4c4e02c7db8, ec3e491a831b4057fc0e2ebe9f43c32f1f07959b6430b323d35d6d409d2b31e4, bf8e512921522e49d16c638dc8d01bd0a2803a4ef019afbfc2f0941875019ea1, ba55542c6fa12865633d6d24f4a81bffd512791a6e0a9b77f6b17a53e2216659, 8ea34b85dd4fb64f7e6591e4f1c24763fc3421caa7c0f0d8350c67b9bafa4d32, 8cac6dfb2a894ff3f530c29e79dcd37810b4628279b9570a34f7e22bd4d416b3, ea5825fa1f39587a88882e87064caae9dd3b79f02438dc3a229c5b775b530c7d, 1acb061ce63ee8ee172fbdf518bd261ef2c46d818ffd4b1614db6ce3daa5a885, 08661f40f40371fc8a49380ad3d57521f9d0c2aa322ae4b0a684b27e637aed12
	Domains	jcswcd[.]com, newsmailnet[.]com
	IPv4	45[.]90[.]58[.]69, 62[.]233[.]57[.]136, 217[.]12[.]207[.]164, 152[.]152[.]12[.]12
	Paths	C:\Users\<username>\VirtualFile, C:\Users\Public\VirtualFile, C:\Users\<username>\SamsungDriver, C:\Users\Public\SamsungDriver, C:\Users\Public\SecurityScan
RUSTBUCKET	SHA256	788261d948177acfcfeb1f839053c8ee9f325bd6fb3f07637a7465acdbbef76a, 1031871a8bb920033af87078e4a418ebd30a5d06152cd3c2c257aecdf8203ce6, 9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747,

Attack Name	TYPE	VALUE
RUSTBUCKET	SHA256	7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387, ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41, de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500, 4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16, fe8c0e881593cc3dfa7a66e314b12b322053c67cbc9b606d5a2c0a12f097ef69, 7887638bcafd57e2896c7c16698e927ce92fd7d409aae698d33cdca3ce8d25b8
	Domains	webhostwatto.work[.]gd, crypto.hondchain[.]com, starbucls[.]xyz, jaicvc[.]com, docsend.linkpc[.]net, companydeck[.]online
	IPv4	104.168.167[.]88, 64.44.141[.]15
Crysis Ransomware	FilePath	bild.exe_
	MD5	786ce74458720ec55b824586d2e5666d
	SHA256	419bc8196013d7d8c72b060da1a02d202d7e3eb441101f7bcb6d7667871a5c16, 5c2fb1c42f007093be5e463f70ee7e7192990b3385a3cbcc71043980efa312e0, 6a0017262def9565b504d04318c59f55bea136ac3dd48862d1ae90ff6b963811, b557bf11d82d3d64d028a87584657d25dba0480295ed08447f10c7a579dee048, b3984a2de76eee3ad20c4b13e0c0cbbab2dd6db65e3f6ca34418e79c21cf5c39, E9253218e30b30c8bb690b2ab02eef47b8b5c8991629d814b2af6664151e9a2f
Venus Ransomware	FilePath	1.exe_
	MD5	67b1a741e020284593a05bc4b1a3d218
	SHA1	026ce3bceb3a82452f0fc38c0b9abfa90f2c9d87, 06757be6174bdc9ef8fe899bcbe5e6e5547dc059, 0d0bbcecc80ea3b1712678b24ba925ac2903531f, 102b8625e5662c89efe4547dc2cb173be8b08851, 10f2ed474a9e0065fed2afebbfe81dc596f46542, 13315ee0ba756ac3e7edf2b9a4028b7649ece754, 1482e7fdbab29c3e8a2f3ccd1c6ddd48a54c06b0,

Attack Name	TYPE	VALUE
Venus Ransomware	SHA1	14d031138fb0aad2432cadf2e0d241ca75b2dfbb, 1970f6c17567d56c3e7840fe33a6959dd887fca2, 1992336a5d752187c979e24a95a871d8932ade6d, 1cb7e2ab7012990bd5051120c3ef8a438035aa88, 1fb9b8115d74cf38d6a90b9049c73ea6eb743643, 326dc3ca63d10968054153305a9564fac2a37ba3, 5166d17d8e9a91a3a36b5edaf168699b03bb13de, 5d1229ece791a55823f60298cb7dcf9c0494f3ee, 62383813a6ca85fc9c70051c361e0273e135593d, 6bf35f44a2267755c2646c89c836bd618c4e964c, 6e530c9a3eddabc29c2f8f6aca6c6f786ae052d6
GorjolEcho	Domain	library-store.camdvr[.]org, fuschia-rhinestone.cleverapps[.]io, filemanager.theworkpc[.]com
	IPv4	144.217.129[.]176
CharmPower	SHA256	b79d28fe5e3c988bb5aadb12ce442d53291dbb9ede0c7d9d64eec078beba5585, 9777f106ac62829cd3cfdbc156100fe892cfc4038f4c29a076e623dc40a60872, 977cf5cc1d0c61b7364edcf397e5c67d910fac628c6c9a41cf9c73b3720ce67f, 823ffbcc62bd3296957a47fbf8c238949584996911e71d5140a25d0a8f6abd80
NokNok	SHA256	1fb7f1bf97b72379494ea140c42d6ddd53f0a78ce22e9192cfba3bae58251da4, e98afa8550f81196e456c0cd4397120469212e190027e33a1131f602892b5f79, 5dc7e84813f0dae2e72508d178aed241f8508796e59e33da63bd6b481f507026, b6916b5980e79a2d20b4c433ad8e5e34fe9683ee61a42b0730effc6f056191eb, acfa8a5306b702d610620a07040262538dd59820d5a42cf01fd9094ce5c3487c
	Domain	library-store[.]camdvr[.]org
	IPv4	144.217.129[.]176
Big Head Ransomware	SHA256	6d27c1b457a34ce9edfb4060d9e04eb44d021a7b03223ee72ca569c8c4215438, 2a36d1be9330a77f0bc0f7fdc0e903ddd99fcee0b9c93cb69d2f0773f0afd254, 39caec2f2e9fda6e6a7ce8f22e29e1c77c8f1b4bde80c91f6f78cc819f031756, b8e456861a5fb452bcf08d7b37277972a4a06b0a928d57c5ec30afa101d77ead,

Attack Name	TYPE	VALUE
Big Head Ransomware	SHA256	ff900b9224fde97889d37b81855a976cddf64be50af280e04ce53c587d978840, 980bac6c9afe8efc9c6fe459a5f77213b0d8524eb00de82437288eb96138b9a2, f354148b5f0eab5af22e8152438468ae8976db84c65415d3f4a469b35e31710f, f59c45b71eb62326d74e83a87f821603bf277465863bfc9c1dcb38a97b0b359d, 40e5050b894cb70c93260645bf9804f50580050eb131e24f30cb91eec9ad1a6e, 64aac04ffb290a23ab9f537b1143a4556e6893d9ff7685a11c2c0931d978a931, 64246b9455d76a094376b04a2584d16771cd6164db72287492078719a0c749ab, 627b920845683bd7303d33946ff52fb2ea595208452285457aa5ccd9c01c3b0a, 037f9434e83919506544aa04fecd7f56446a7cc65ee03ac0a11570cf4f607853, 0dbfd3479cfaf0856eb8a75f0ad4fccb5fd6bd17164bcfa6a5a386ed7378958d, 159fbb0d04c1a77d434ce3810d1e2c659fda0a5703c9d06f89ee8dc556783614, 1942aac761bc2e21cf303e987ef2a7740a33c388af28ba57787f10b1804ea38e, 1ada91cb860cd3318adbb4b6fd097d31ad39c2718b16c136c16407762251c5db, 1c8bc3890f3f202e459fb87acec4602955697eef3b08c93c15ebb0facb019845, 226bec8acd653ea9f4b7ea4eaa75703696863841853f488b0b7d892a6be3832a, 40d11a20bd5ca039a15a0de0b1cb83814fa9b1d102585db114bba4c5895a8a44, 603fcc53fd7848cd300dad85bef9a6b80acaa7984aa9cb9217cdd012ff1ce5f0, 6698f8ffb7ba04c2496634ff69b0a3de9537716cfc8f76d1cfea419dbd880c94, 66bb57338bec9110839dc9a83f85b05362ab53686ff7b864d302a217cafb7531, 6b3bf710cf4a0806b2c5eaa26d2d91ca57575248ff0298f6dee7180456f37d2e, 6b771983142c7fa72ce209df8423460189c14ec635d6235bf60386317357428a, 806f64fda529d92c16fac02e9ddaf468a8cc6cbc710dc0f3be55aec01ed65235, 9a7889147fa53311ba7ec8166c785f7a935c35eba4a877c1313a8d2e80e3230d,

Attack Name	TYPE	VALUE
Big Head Ransomware	SHA256	9aa38796e0ce4866cff8763b026272eb568fa79d8a147f7d61824752ad6d8f09, 9c1c527a826d16419009a1b7797ed20990b9a04344da9c32deea00378a6eeee2, bcf8464d042171d7ecaada848b5403b6a810a91f7fd8f298b611e94fa7250463, be6416218e2b1a879e33e0517bcacaefccab6ad2f511de07eebd88821027f92d, cf9410565f8a06af92d65e118bd2dbaeb146d7e51de2c35ba84b47cfa8e4f53b, dcfa0fca8c1dd710b4f40784d286c39e5d07b87700bdc87a48659c0426ec6cb6,
TOITOIN Trojan	MD5	8fc3c83b88a3c65a749b27f8439a8416, 2fa7c647c626901321f5decde4273633, b7bc67f2ef833212f25ef58887d5035a, 690bfd65c2738e7c1c42ca8050634166, e6c7d8d5683f338ca5c40aad462263a6, c35d55b8b0ddd01aa4796d1616c09a46, 7871f9a0b4b9c413a8c7085983ec9a72
	URLs	ec2-3-89-143-150[.]compute-1[.]amazonaws[.]com/storage[.]php?e=Desktop-PC, ec2-3-82-104-156[.]compute-1[.]amazonaws[.]com/storage.php?e=Desktop-PC, http[:]//alemaoautopecas[.]com, http[:]//contatosclientes[.]services, http[:]//cartolabrasil[.]com, http[:]//bragancasbrasil[.]com, http[:]//afroblack[.]shop/CasaMoveis\ClienteD.php
	Domains	atendimento-arquivos[.]com, arquivosclientes[.]online, fantasiacinematica[.]online
	IPv4	91[.]252[.]203[.]222, 179[.]188[.]38[.]7
PyLoose	SHA1	d422493b47e4798717f2b05a482c97ef9e6b74b9, eba82ed21b329b0955ab87b2397a949628349b3f
	SHA256	25232290fa9fa5529240a4e893ce206dfdcfc28d0b3a1b89389f7270f1046822, 935ee206846223e6d2db3f62d05101c0bea741e7b43e1b73c1eb008f947d5ff1
	MD5	059f83f8969b09c29c95b17452718ea3, fec5b820594579f1088db47583d2c62d
	IPv4:PORT	51[.]75[.]64[.]249[:]20128

Attack Name	TYPE	VALUE
PyLoose	DNS	gulf[.]moneroocean[.]stream, Pool[.]sabu-sabu[.]ml, pool[.]xiao[.]my[.]id
	Monero wallet address	85DS3ShGZwtFffeQUrDK8Db12qwCcaCHofNcZdjMkjTCfWiRv9WLe4cR2W97eGnRXwBxDhTK7BbbE2Z7t4gjXRz1VLPmhn7
RomCom	SHA256	d4a847fa9c4c7130a852a2e197b205493170a8b44426d9ec481fc4b285a92666, a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f, e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539, d3263cc3eff826431c2016aee674c7e3e5329bebfb7a145907de39a279859f4a, 3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97
	SHA1	fb4ad5d21f0d8c6755eb4addba0ac288bd2574b6
	MD5	059175be5681a633190cd9631e2975f6
PicassoLoader	SHA256	f11310f075171f8502bcd32dcb2fe5894808b17a37f6fd960fb26653871e7b7d, 6b310bd23806272f6c69b84a0381915f16d705e79ce423f19de940247543c76a, a7b7691baa21ad118348661a035b69605a6efd1cd1fa0fd52e5645c64f5f61e6, 1a0e930fbdab2266e14dc501abdbb5623b5762d687df3670d86bb05f252509ac, 0397c586fa56e672db7f14afa8c19992b6e08ab0c1d282c960df1af26371bd72, ce96fe99ebe30ae44e74c22c0b2a055005d0da131e0082a1c290ddeb79dd1114, 5039d76e697f242c36c5a0ebf7dec127757bc34ddaf33c58251c2798da3ce03e, a58da0e6a20fed03364a0cbae18008eb4f8d6bee7c9f5e8ffcdac34fb823d363, 7e35ce60d80c85e050133de142a3b261160259846c9c967c7b2bb84923328f8c, 27a061daee3ec9cff928b8152159a472797821834a3aa7639749489b90f703c3, c7ec4570524ad59d5bd7a3e8f0d23c8cf05cc0e8a98dcdbec00c9dc075084558, aea76f905b0169e4289895a8d85980896f802fd18fe246a27d601310bfa5905e, 7a9a5317a88afb53b44f6cfed59c48907f63aaa7ef63b1587f990951c423c211,

Attack Name	TYPE	VALUE
PicassoLoader	SHA256	0f189246247c51a701d5a88a06e1fc4932f333d24d7ff40dc8152ad6224f6ca4, 41f050f3d003edd67ec02710c60a7b4022685465cb61ae37fc0b3193c1dab5cb, 1c118d8fb0be904b129e4552f86cd0b3e239ecd25f4d599c54cc96c1096747af, e41b3bdbfb816d5cfd4b235d2b985894153c41da6726ebfa83e45f3b5b4a1945, 6e6f5bebd6bf0fd0b626d6521cdb4faa06275f558bacd419c76702e2728f734c, dd61887d5cdf361a335fec917cd6d1bb186aad56b1f9f5d09b66355ff7f41751, 40b87c5444e03b6b4f3d38315c1525cedfafc20355fff84502cc594799dc41df, d3f012662c44293ae07d8c763914db18fc9795673da7c1cdc4d862b1a7c887b9, f00939201f7e77221e94e917a8e34c3d2143324e02fdf35058526d870a0023a0, 71c0881d35f769fe58c084883d2aaee9ec284fcdc04500e5e5272973dfc78944, 00030b0db567afa524eb68faf6f194f25bc5361c380599668a82dbae12af088e, a7a7c4062ced46275638719c100ea2397c673148e8473e56a3ec4313ca7dc5f9, 4d9cca1d75d4691e794dfe9efb9eef6e9e64b4e978ad17831b459d4bb6722829, 4da99f963c26bcc4537ba0437c9cc1445be8bea64067d34308dda6c2e49c8c65, 4cedec3e1a2f72a917ad9a59ebe116ed50c3268567946d1e493c8163486b888b, df33b1187c20582560ffaa1c3e86b92003c4a7c8a61acbbe886ab195531c5c89, bec98a8a5e6786ef415a7a7bf7e60cbd384d43ede4e882aa560fdcb24865ac55, 00fdb03518c238dc649a39e94f0bcc95dacf3b832979d14d0ed5194b9b482b87, 991a19fb00cda372dd1ce4a42580dc40872da5c5bfbb34301615f3870ea3fb58, 2c5ba56a41f40bac2f21065fb9883545ef8d359883cb7bc351c481cb9542e104, 44fd895174a7c1c0019fc95bb04201106dc165704c70e902e3de58db98f03c7e, 30d46a740e2677c8fee383c2a4762561a10c66c5b99215262e42bfabf6bfb1aa, 924d3589d642e8fd65746dc156ff9f104d43114a04ea9509f51ee6a439d1915b,

Attack Name	TYPE	VALUE
PicassoLoader	SHA256	ecafe10f0f7d6a9ae94d9735b45f88492b6ea11ff58f37e62fbf7070778af20a, bc92a5b1c4205ea1fbfec9144b8aab485e095142c7105c9d616b089ec668f198, ea5a8f1052e40cb6bcebf384fe67a6920b3651fbd8f3a34a844f39789ebc4d5f, ad8e3ebd496fb4d97e5075adb4f2f1b91195cca059800d0acd182a07698c13b6, 3670115fa5fac918ad0dafe399568788690f0f205dd0bebe4f55180fd70d36e9, 5969180b072703709764d1ca40be3eeb40f2eb0090859b3743cc21b884fa2106, a5fb6b9417e50bd2260afdcdb5a9eed33e48a283a51408344a4caa2b1025b9a7, c0c455cd3e18be14d2e34cf4e3fb98e7ab0a75ef04b6049ff9f7b306d62704b8, 0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32, 35d1e819d2ac2535f0aa9e2294570135f37519386872c415e326146e931b8fb9, 5a4bd78a4d3d1a772e9e9b14983646a4c1c6a25cc983b804e4522774ebfa1c14, c40e6b176ad3fd7332cd217191e557352ef4b82bf91f29939121267598737990, e9bbe7c6705a6f5a78c2a9b8060a7e32374b81058f7c2f24851c4d1ea38d7411, 73a21c1492996794688d9751edd1e5c287da645fa7a960e945bb4ea69855424a, 7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152
	Host Name	everything-everywhere.at.ply[.]gg
	IPv4	94.131.108[.]109
	URLs	hxxps[://]wuzhenfestival[.]site/5109c46d40f801a862c96e628f83faca[.]png, hxxps[://]onyangdol[.]site/thumb_d_F3D14F4982A256B5CDAE9BD579429AE7[.]jpg, hxxps[://]kebhana[.]site/Believe-Me-Lyrics[.]jpg, hxxps[://]wordrow[.]website/pictures-91[.]jpg, hxxps[://]ellechina[.]online/01_logo_HLW-300x168[.]jpg, hxxps[://]sellmyhousequickly[.]website/dangjiansigeyishibiaoyuxuanchuanguahua[.]jpg, hxxps[://]frivol[.]space/memnet-profiles/A10818[.]jpg, hxxps[://]wordrow[.]website/pictures-91[.]jpg, hxxps[://]simplifymedia[.]pw/images/bnd/news/23908t5[.]png,

Attack Name	TYPE	VALUE
PicassoLoader	URLs	hxxps[://]hssenglish[.]pw/fonini/pundit/leaf_background[.]jpg, hxxps[://]mingxing[.]pw/content/_processed_/f/a/_742fa0bbd1[.]jpg, hxxps[://]mingxing[.]pw/datastream/thumb_b/43950sec[.]jpg, hxxps[://]carpetmarker[.]pw/images/Carpet_Shop_3b09adf[.]jpg, hxxps[://]bourns[.]space/p/covers/assets/images/lee-leopard[.]jpg
CustomerLoader	URLs	hxxp://smartmaster.com[.]my/48E003A01/48E003A01.7z, hxxp://5.42.94[.]169/customer/735, hxxps://telegra[.]ph/Full-Version-06-03-2, hxxps://tinyurl[.]com/bdz2uchr, hxxps://www.mediafire[.]com/file/nnamjnckj7h80xz/v2.4_2023.rar/file, hxxps://www.mediafire[.]com/file/lgoql94feiic0x7/v2.5_2023.rar/file, hxxp://5.42.94[.]169/customer/770, hxxps://slackmessenger[.]site/, hxxps://slackmessenger[.]pw/slack.zip, hxxp://5.42.94[.]169/customer/798
	SHA256	d40af29bbc4ff1ea1827871711e5bfa3470d59723dd8ea29d2b19f5239e509e9, 3fb66e93d12abd992e94244ac7464474d0ff9156811a76a29a76dec0aa910f82, 65e3b326ace2ec3121f17da6f94291fdaf13fa3900dc8d997fbbf05365dd518f, 7ff5a77d6f6b5f1801277d941047757fa6fec7070d7d4a8813173476e9965ffc, c05c7ec4570bfc44e87f6e6efc83643b47a378bb088c53da4c5ecf7b93194dc6, 695f138dd517ded4dd6fcd57761902a5bcc9dd1da53482e94d70ceb720092ae6, b8f5519f7d66e7940e92f49c9f5f0cac0ae12cc9c9072c5308475bd5d093cdca
	IPv4	45.9.74[.]99, 5.42.65[.]69
	C2	missunno[.]com:80
LokiBot	SHA256	127c29b65ebf2143b66e5c60fcdbae43c4789c836e273e4f996efd0e56040e8f, 30c51845ddd526bf0472c52af64b591baee970f2ab39bec2d6bea1a64b5c7f9b,

Attack Name	TYPE	VALUE
LokiBot	SHA256	7559e6ca8b77400f88bf4e67208a1c32570a670068eccae9e3d226cc5471bd47, 9346d441c3136edb70bc96afd06717fbb96074592bcb4896741ede01be7925ed, 61868e99c4fff04df6ba82cbd4eb414c132c5932acd762f379b4c0fe852968bf, 73ca91a52ed319db604f0951f4b95ebd4a93eabc6f410e3d7f7ffd33efa29982, cabcb0bfd5b86be43f98e9ea8dcb92e8ef87d1c98e326b2effa2d39482bb882a, b0504206461bb3a04bc80d299501c2d2765f097bc621a0e86e5b9e889f383287, 42ed620528c450c61185a065b7e73c5d8207c731acb7bf965df2a49c030de497, 42ed620528c450c61185a065b7e73c5d8207c731acb7bf965df2a49c030de497, 73ca91a52ed319db604f0951f4b95ebd4a93eabc6f410e3d7f7ffd33efa29982, a65903f3968b96768cd2ca31af342c23b7f8c8b0d928b6a7f9119c80f105b3ee, 24e91c3b0d477625a70c71ea05ad7e6ce3dd9582567bb7c33ed6ff537915490c, 24e91c3b0d477625a70c71ea05ad7e6ce3dd9582567bb7c33ed6ff537915490c, 3d87812ab5871d3d39ee5989e5ea9f531061bb2366197b929c42889e4377a87f, a452e58b0a7862c490e028e3a9cab9d5b33a6bd34b4e86e1385333e60717fa02, 0d31edaf7d6a20a6a50e9b8b66592d6a18f23466ed54a9b63768afbbb84140ff, 647a55bbed92a840ad9b1b6b1fa8898927310dc81d39e5ca9f223c3f7f315cb6, ddf9208f37a6707462c99f48495752554a13df724120887df88fbc9d2bf75ba0, 578153b3c97aeb8bee7d4c75e6fadc389575385968df4fd4f39f71871f7ed1f8, 4e51f0616df48153ae9a76dec9a194ba7710d13a419e3eb7b8e845832a41540d, f03390fa3307e28389f6581e930065b810892ddb2cd0b12f59ccf896e1852681, f03390fa3307e28389f6581e930065b810892ddb2cd0b12f59ccf896e1852681, 3f2261e0d78987287c17b70aee3541edf714bcca93bea5f66872bea7d872f790, 3b492c5191fbeeff74cbaa092bca97936135c165ac2919b50604eabfcf92e150,

Attack Name	TYPE	VALUE
LokiBot	SHA256	d5275100a4f01bfdc9c99ea76177b80b5257185a255c762bd98665e243620d12, ac176f2b29fb8ee6af988681a8fd5a6eecbef64c7e6a301a00ce925b4f1e431b, 96a5aac25dc29322b45abee014e3dbfcb30e4b14150c1c4e13872904d4739ed0, ff36e05a76e31b8c32297d4e98f745a3e5d1d9beba9fdb455935e4302e0f2e57, 75ea332096b6ae8eabc2c398d2cd97f3f119591b39b16ce7c96953d4ebfcc63b, 099b16630e07d02d34a717dd001cdfac0023c7847cc3e5aab9933b4861138395, 2c8b9e7e30951113a55140552f9c3aaebb7c7e4a11624b5c948d5a64d9a89f3b, 121bea26acd46a7ce020d48ea79216f4119474fb6dd9895baf1d9dfdf6dc8fcd, 121bea26acd46a7ce020d48ea79216f4119474fb6dd9895baf1d9dfdf6dc8fcd, 7704a4a10e786469680636e849feffba29379edf93a1feabf0798e6683e2eb60, cdc818a75fd935601dc318e97046858d96fd92e2b1547794450a35541540aee3, d04b4aee3b062e68e9c35402495cf1d40ded53c7dadcdb355906640342932170c, 567e8970d27c1e43b55c0156c957f71fb553282709237cc73bbeb6bd518edbc7, ea5a585a8b9e9223d5d6d66c78615c795bab186c681b04f11e7901dae8d79bfd, f15f539c0ae209595dc2256318091681aa7852d4f88b2c6ab8e0d1f1dc1f1e91, ea87aab944e82b6711433894358556b563fa27e0d99b06febdba8d1a5c7dde0e, 827555c608d1e12973d7c28d45b4ca8d5342d1dc77b12a5d403a32d83e591fb8, 5a7a9170adc2fe2a4167392be4532c945faef7a2d0f9a18d79cf9d9cb459d61a, bd32a9cbb3ed1a616bf91d7121386a78cf6bb2b8c904088d1daa3982edb4fb8b, bd32a9cbb3ed1a616bf91d7121386a78cf6bb2b8c904088d1daa3982edb4fb8b, c98512ee509dca89b8f6073faf337cda879e39f669add3632011590411878c9a, 2af1bb0bba5a26df1520604cbf7e84bf8bd19d4f9f23167b3408c78b545b7190, 4e49637ce52ae9105d53e9de9994e680ba5894f25ffffbc2272e9d95c0adfbf1,

Attack Name	TYPE	VALUE
LokiBot	SHA256	9f54a66ad8152ec7b3923d98a8261ba15d643dc241cdf995e5332bcf4b91eb0a, 59bfe87a4f70ad80b96e5d135d9688324b18009f800b7001c6efa116fb780d2f
Noberus ransomware	SHA256	029dde7c2ec880fb3d3e95e6a8376739b4bc46a0ce24012e064b904e6ecb672c, 72f0981f18b969db2781e874d249d8003c07f99786e217f84cf54a148de259cc
Deed RAT	SHA256	b6860214fcc1ef17937e82b1333672afa5fcf1c1b394a0c7c0447357477fe7c9, 212f750a1d38921b83e68e142ee4ae1c7b612bf11c99210da60775f17c85a83e, 6cfa8ce876c09f7e24af17bbe9baa97f089e9bf478a47d18417e399e64a18d40, b7bb9b41298420d681d1a79765d7afb7ecf05d6f0baf0b29a07b8b1af20a8c97, f554ff7eb069f0ea5ebc49e015bde1e88d4cf83f6df21e4de2056716e83fedc6, 7ee776272f7c51e41e10f5ffbd55c8c24ddb332e8c376e132e5a8cb72abd7397, ece771ab5ae8372078c378fa0cf0a1ac055ea5cbe6091f890185c02caf0edc19, 5c7f727c852819ae60182c4406c233f5b86962c1da3b933953058985d9f90722, ceca49486dd7e5cf8af7b8f297d87efe65aba69124a3b61255c6f4a099c4a2ab, 4f84f4333dc9c42ae4ed55c4550ebb14c8079235ae7de9fef4191251537454fc, 8c3e0fdddc2c53cf7961f770080e96332592c847839ccf84c280da555456baf0, 85d190304accb34422d3e1d603c33b86b6b8c4e88cc4713b0e0c6d4fdee9d93e, a3df5eb54f0a77cb52beccf1b2aa2caa427f80fcd047fc6be4c7aa849649e1b5, f9e97776826f83278c63cda59910c49920b7316433d9d95570dd187e154fed0b, 74ac74ea85118fe3686f9d6774de2d63db7870dadb4f0ba0d119a77d6c11323a, 057a16008ce50c3d02c910eac697748eb157afb8a6e8573adefa4b75b495a778, 66bca22ba5fbd01758fde8e57e1e251191cd1c7bb599f0beb8dd0ffd661464ac, 10d122833af8b8fec97ebdd843942bfc2bf237e3b8c01ae9f852eaca2e9cddc7, f0b8bf55a3e23379aefd9a95c556430e073ad206b4c39e0086f0a17d00ae64fe,

Attack Name	TYPE	VALUE
Deed RAT	SHA256	8a3aefd75501137f601d4b802959fb50b7cba2b135ce2ab2f1f5fa65b1a86159, 3a1e67006fb1e761e0188a04361cb7a57329346e7d0a78ef909fbc5469e3c08b, e88c7dd128c456a34804a36459f32cdf97fe30a5642caa3072ff31cda07f29e2, a2d7255cf7c8710cdec62c01b3e2c9d22600441b20914d73eb8f8af3245a9806, bfa3c91767c333a97d6849a3f885f4ed2205f24882bffbbfc916624b2601a9b7, 241d1ab6a0da9dfcbc9c565d1ff948743cd7673ed334e5906a1428055cab6c82, c8c3b639c6e880d7e01cba8cb019087f0c4d2cf4dcdfa712a18054b78e525a47, 5e712e78736bde2d3ed507fb730be3a9d55d2b4ee3f7ff827f961fcada4e4e0b, ef17d44cde003c17c28137c6d4692eb4a1b42f86e5d6995f2f06a05e363f044a, 42ef77391f20ffc1751ded79da25376bc20a007d03e501049fff37f781df5403, cae7622a5f1ed791d317db0b3bc791a8ab71a9c68837282435f5db6bab540615, 2707602481a025da29438d01e894cfc9742389d419a5b08aa96ddc76bde38cba, 5311e4fd3329945496962c6417b74da919f5e50ae20ba7ab0d5983012c956f4b, dc3c1df20d73a62e8219ed6193ecf1229845dd0a6e42d32eb11cbaee04cfa7df, 70e43da5c5b6a8cfea8fcad768a2e5cfdf532b49b5ac87ec8ca9d05d83e0e915, 1473fcf2297376a819b6cccd50dc709fb61f48f70dc9a0eaff741c893b33d670, 67f7faf0161fdac7ebb619a2aa0c73a4a08def05d7752dfdd698d24410d9989e, 7c11eecc2fef6a2ad2e5d80156946d7bdcb9c345d542781c3116141f10eb490f, e2735841dd8ae66a825182d6d06629821c49aca44357e5980c3bfb97ace7ebf0, 374fff9a48949254d72bfe34b9b62129da1cfafb74623d187791ada09d976e7d, c4e023110216481d0ccb09787ccc5ea46879fdf331f5d2fda2b1f33719a35104
	MD5	972a1a6f17756da29d55a84d7f3f23a4, 51ca39e3700e9ed16d90302dd31f3a1d, b0b438bcb2a71233721a2ddcdb765a68, 0fa4a2b8210500427bb23d2d92502964,

Attack Name	TYPE	VALUE
Deed RAT	MD5	804824203f31ebfb56e580e73e932d26, 38c43e589e3dc65258322d91b58e2e15, ef6264abe296357100e2db48820b13f6, 24ec73b4e1845088a28dde0007c2d6bd, d217fe96c7737ac318321deafc4cd261, 633ccb76bd17281d5288f3a5e03277a0, 77ef4bc2f23ef97add7ec0ad229396a4, 8002cd74e579a44a78b2c8e66f8f08a4, d4e51120c368ee4ef5f5571756803fd3, 66e8f82a418923b92bef57ad61bcebf3, fb23fc47484150250cfd7b1260e23524, 99b86ad9bf6193b044076df373534fad, 4db33e5390bfebd84e38cbb85b75c006, dbb5995037745e04d03dc7f2985f017f, a94277fad94ca6fbdb2b8eeb716bac90, 7aa890406a74a44f17fe665653bd92e2, 9faf04fc6e522050527e71dea5918d01, 1a04af6c3abe8f67bf98adc588c46736, 6d52d0e7f49817c6315b308cb973d405, 8e3217391e11cabf6f9a62a35c636835, 97c00cee887279f12f309a86e7bc3638, 5d0aa944ce19e0a70adad562ce0e7880, 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,

Attack Name	TYPE	VALUE
Deed RAT	SHA1	e986b238cb5fe037718172d965a41c12c85bbdd0, 59239f73996a3f5a6260228cf7ca3c01e3a00822, 84ca568879ca62448d035d56bec816a11188b831, ac499c86012858f40eb78ecf3bcefae779527d73, 99cc3349b64188aae1c986afbcee7e776aa4b349, 30ad2f4a758ab2c526b6439772c7cd7cee66ffc4, 0d0c026a1661923cd184b6d0fde647128be75488, 20c83bcfd9fb45a8ba5922dbefb74d47cb361db7, e50dc750e7697ba5e28d6dde12e9a4d370076c0c, 491248fdf1141e81d5ff23eb1e44d58b50339fe2, c58d5d36201cee88a01c9913d771723edde302e4, 0912822548e5983f8a2b6d77848994f6d929ffed, af71956b59b9c05acdcd7badecc232ca6237cc8d, bfe05003730d79f0004cc41e09f48944df6f68fe, 19da36d73e0a72f65c8a9f6fc2e2504ed599b57d, 6e0c406d07206b588652729a271e054c416b5c90, 338881ff10434b523feb63a8a66370f444378cc7, f4a5778b74b73745a533f22d33a65880f2968705, 57792f875625fec78bea22af46010bd34dff863a, 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

Attack Name	TYPE	VALUE
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
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

Attack Name	TYPE	VALUE
Realst Infostealer	SHA1	0eeb66a08ca067f168779be8b22da25f90fe4f51, 88880772b0f8723020e0feb2bb179dc71e482072, 6ee0d99e3a56a72c60f3da790268286cd1e7a3ab, 60a747b3e8a25b885ccd16945ba1a238a66e4439, 8054b51a51c8c8f21fe4c51322ef36a9fa02b570, b8ac89eed011c0a4e5f4973acbee888323ec80f0, efccafe8cf2a7d63f82c69882195a565fbd60720, 39060bb82061c5d426d4a7bad66e07888b05b354, b1aac3888403f4597d9cf14b505f572b2fe7d485, d890822af137df48a91f4ba47a27272dcacc9920, 630b23a57d2d8e6d8e25c346173191af6273c3ab, 087b3bf372928279d547fb6bb0ab656717fa8c4b, 0a2a853251fe28333761cc6f9c4518807354dd27, 13bdb3823b8555d846f17bdf381f9568b9a81d26, 29a7eefff22156a72577ed920eaf9b903e9f164a, 2d89ffbadddd62483bc2be33e296ce4e6036c45b, 4e5a59a515981fb97bdb272e3e4acb7118e4e6b2, 9719fd9415d438722f94877c55c9495708c64fee, c205d4ba044f2d69500f10a46c31aaf068e32c44, c716a02e3bc8603fcf0bb8d63fc4f7e3afab471d, dadfbd13b7bd0e9b6d87ebae30bc48c2eeae0eb3, 09e8672af5e18ce99ad8ae608cdc0fa229f121f0, 112b5637c8cbb7d2e216d89f969515809e1dc66d, 154909cdd261130b0ed6d603d4727cb9f15ddc36, 247c50d19e7ad18f466558f9c1785ef29962ab7c, 32f06e3e9d8899f5224f3d5538724d132bda0921, 68dc1f80064f6c261e587cdbb2f01677c8f2e14a, 8b4cdd02330cf25f4e1d338b91ffd1c1dd87021a, ce42d202446cc6b316f668a072c17df87dcd495c, 2f61ddd391d23a6665fa326629e004cb380c4f85, 38ae4fa8f4fec9ab98c0003c455016464b62acce, 65c175f5fad31ea1c938a96a9cdc9987413fd1f2, 80483c5c95ed92da6f086e9497cd08cf7d3b7658, c4296e1a67545e50f44c3776adb674ea1d4d4c0e, d436de35164a045e3c0f7b51cf41fcefedf7e77d, f097123a1999a656a368114abbd848b68d523ee0, 158cf7a0c89544ce1c3294453be2a8c8ced9c9b0, 294392bcf166953c552443fe95ba1e8f15487f74, 294bfc9b97092904bb5e216531b184e38fb2c11f, 3685fdd3d14b500fd73f0a3d16dafcc028035204, 4053e0ecf5f59b6f7afc06750551d77e131ebd2d, 410e4e24f6f6c4f29c8a75723f84bf60ff96c2d5, ada7a47b7fecb142ff532c6e0f01a89bcb47afc9, bfac1b17ad79719c4602a2142435f02c529ec4ab, db9fe7ba9ff8771d28a2fa504d84059faab6be5b

Attack Name	TYPE	VALUE
Fenix Botnet	IPV4	207.210.228[.]67, 139.162.73[.]58, 80.66.64[.]154
	File Names	SII_Seguro_XXXXXX.zip, Herramienta Seguridad SII.url, AT_herramienta_XXXXXX.zip, SAT_Herramienta_Seguridad.jse, 7684jasdtg.xls, ot.crypt, proxy.crypt, steal.crypt, pay.txt
	MD5	b10b9f1f286f7ae29d9e87c5391d3653, 500b1c312163009fefec3f8fe7861258, 594804aa21887ee9d7b1b888f482d60c, 1c50c6d0aeaf8071f528b76b1ab242fe, d80f1780bb24e7ecdab8a262744bccb7, 1be0606640d645ddbfb2fbdff53ca918, 7631660bdcf74b95b5806328a7668cab, eaff13d6c89ce0e2a7632bd811045c35, ea68e0cc90a88315526704bae1ca8b4a, b262b36c3b09ebeab66c95e121be4c73, 6f0b4018da4aa0887b5aa879ce315543, 7fe97d4e29e17f39e343a9ef5fde03ca
	URLs	file[:]\\139[.]162[.]73[.]58@80\SuECWRPQ\SAT_Herramienta_Seguridad[.]jse, file[:]\\139[.]162[.]73[.]58@80\YtmpEoBw\Herramienta_de_Seguridad_SII[.]jse, hxxps[:]//fja[.]com[.]mx/wp-contents/execution[.]php?tag=russian, hxxps[:]//fja[.]com[.]mx/wp-contents/init[.]php?id=1, hxxps[:]//www[.]grafoce[.]com/scripts/index[.]php?id=2, hxxps[:]//www[.]grafoce[.]com/wp-contents/execution[.]php?tag=russian, hxxps[:]//russiancl[.]top/bramx/7684jasdtg[.]xls, hxxps[:]//russiancl[.]top/bramx/post[.]php, hxxps[:]//russiancl[.]top/bramx/ot[.]crypt, hxxps[:]//russiancl[.]top/bramx/proxy[.]crypt, hxxps[:]//russiancl[.]top/bramx/steal[.]crypt
	Domains	2repuvegobmx[.]com.mx, annydesk.website, citasatmx2023[.]lat, citas-sat2023[.]com.mx, citas-satmx[.]com,

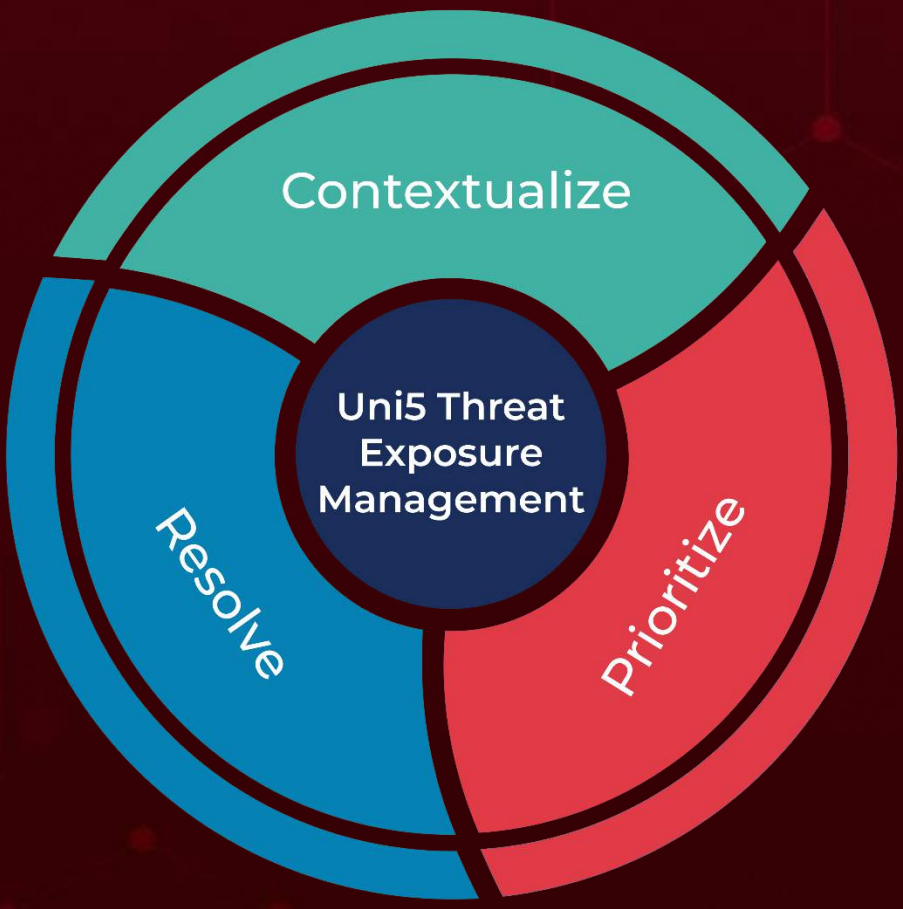
Attack Name	TYPE	VALUE
Fenix Botnet	Domains	citas-sregob-mexico[.]com, consultacurp-gobmx[.]com.mx, consultacurp-gobmx[.]com[.]mx, fja[.]com[.]mx, grafoce[.]com, lbci-seguro[.]com, mexico-curp[.]com, russiancl[.]top, siii-chile[.]com, sre-curpmexico[.]com, tramites-sat[.]com.mx, whatsapp.website
Pupy	MD5	D069812AA63B631897498621DE353519, 42A5798608F196CE7376CE196F4452FE, F365A8BDFD9B39C4F8B9D99613818207
	IPV4	103[.]79[.]76[.]40
Decoy Dog	Domains	ads-tm-glb[.]click, allowlisted[.]net, atlas-upd[.]com, cbox4[.]ignorelist[.]com, claudfront[.]net, hsdps[.]cc, j2update[.]cc, maxpatrol[.]net, nsdps[.]cc, rcmsf100[.]net
	IPV4	13[.]248[.]169[.]48, 156[.]154[.]132[.]200, 194[.]31[.]55[.]85, 5[.]199[.]173[.]4, 5[.]252[.]176[.]63, 5[.]252[.]176[.]22, 5[.]252[.]179[.]18, 67[.]220[.]81[.]190, 69[.]65[.]50[.]194, 69[.]65[.]50[.]223, 70[.]39[.]97[.]253, 83[.]166[.]240[.]52
	SHA256	4996180b2fa1045aab5d36f46983e91dadeebfd4f765d69fa50eba4edf310acf, ab8e333ef9bc5c5a7d1ed4cab08335861e150b0639d3d0ca4c30b7def5cdccde, ad186df91282cf78394ef3bd60f04d859bcacccbcdcbfb620cc73f19ec0cec64,

Attack Name	TYPE	VALUE
Decoy Dog	SHA256	6c8f413111f1abfee788dad4ee7cca37e0c2597cca66d155af958c535faf55cc, 0375f4b3fe011b35e6575133539441009d015ebecbee78b578c3ed04e0f22568, 6c8f413111f1abfee788dad4ee7cca37e0c2597cca66d155af958c535faf55cc
	Telfhash	t1fde0f101c9395f39ecd16430b41041a59107c73c904087309fb8d0e8d87e0077129f3f

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

August 01, 2023 . 11:00 AM

More at www.hivepro.com