Date of Publication
June 4, 2024

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

MAY 2024

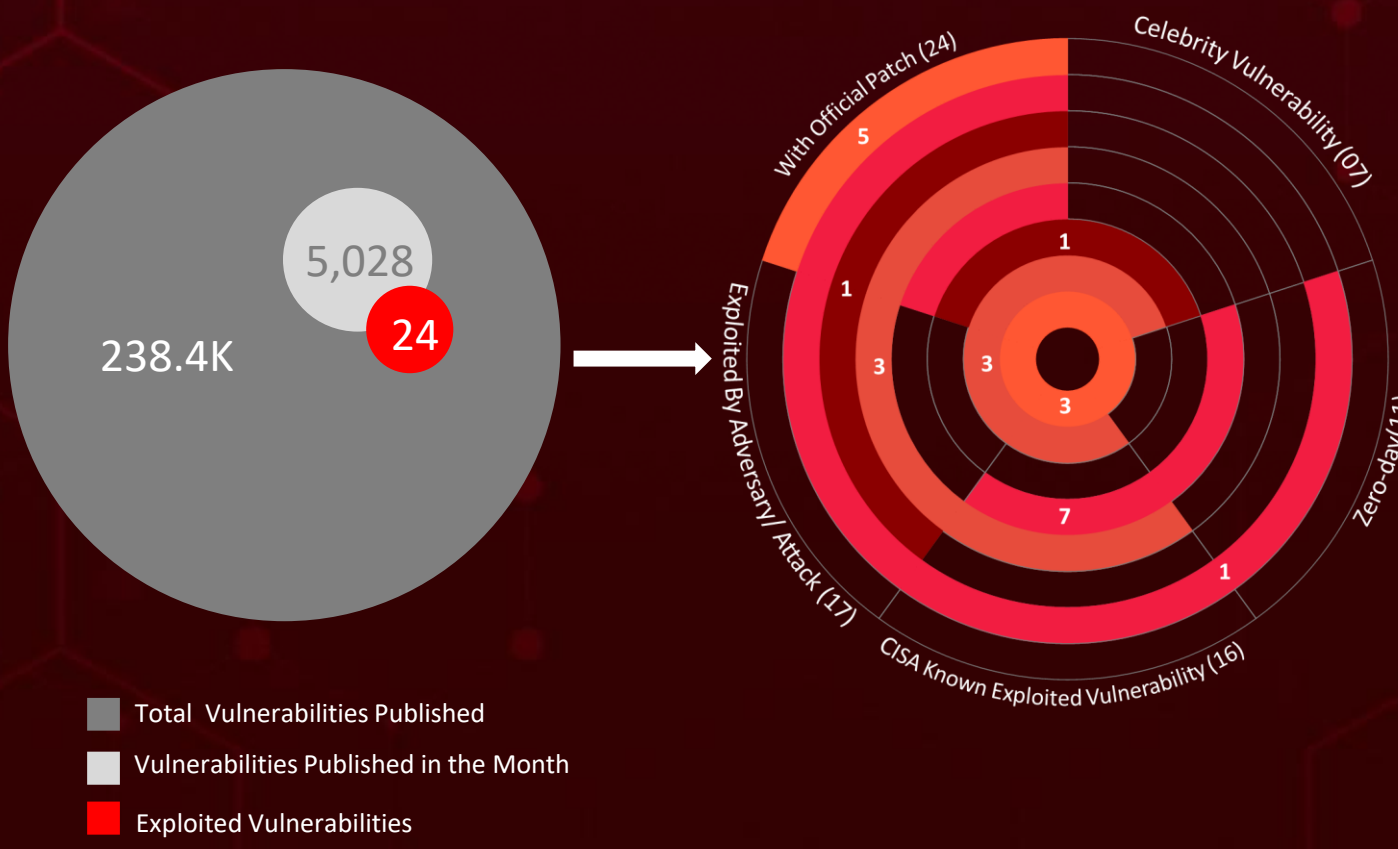
Table Of Contents

Summary

In May, the cybersecurity arena garnered significant attention following the identification of **eleven zero-day** vulnerabilities. The Chief 'Seven Celebrity Vulnerabilities,' which included critical flaws like **ZeroLogon**, **NoPac**, **PrintNightmare**, and **Follina**, all of which were leveraged to deploy the **Black Basta Ransomware and Qakbot**. Additionally, the **Dirty COW** vulnerability was exploited to distribute the **Ebury Botnet**, while the novel **Linguistic Lumberjack** vulnerability was discovered within **Fluent Bit**.

During this same timeframe, there was a marked increase in ransomware attacks, with variants such as **Trinity**, **ShrinkLocker**, and **FakePenny** aggressively targeting victims. As ransomware tactics become increasingly sophisticated, it is imperative for organizations to bolster their defenses by implementing comprehensive backup and disaster recovery strategies. Furthermore, training employees to detect and prevent phishing attacks remains essential.

Concurrently, **eleven** threat actors were engaged in various campaigns. **APT28**, a notorious threat group, utilized compromised EdgeRouters to conduct covert cyber operations, repurposing **Ubiquiti EdgeRouter** devices for a spectrum of malicious activities. This group, associated with the **GRU**, also orchestrated a sophisticated **email campaign** aimed at **Polish government institutions**. As the cybersecurity landscape continues to evolve, it is crucial for organizations to stay vigilant and proactively address emerging threats.



Insights

In May 2024, a geopolitical cybersecurity landscape unfolds, revealing **Jamaica**, **Cuba**, **Mexico**, **Belize**, and **Poland** as the top-targeted countries

Highlighted in **May 2024** is a cyber battleground encompassing the **Defence**, **Education**, **Government**, **NGOs**, and **Technology** sectors, designating them as the top industries

Decade-old Flaw Weaponized

The nearly-decade old flaw, **CVE-2015-2051**, in **D-Link** devices leveraged by **Goldoon Botnet** in a global attack

LLMJacking Leasing AI Power:

Novel intrusion set compromising cloud LLM infrastructure to steer AI rental businesses

Spooky Chrome Zero-Day on the Loose:

May brought **four** zero-days for **Google Chrome**, three of them originating from the **V8 engine**

CLOUD#REVERSER

is a campaign using Google Drive and Dropbox for malicious operations by threat actors

Checkpoint Flaw Leaks Passwords:

An information disclosure vulnerability in Checkpoint Gateways was exploited to dump local passwords, leading to an Active Directory breach.

Grandoreiro Upgraded, Spreads via Outlook

Grandoreiro wings out of **Latin America** evolved to infect Outlook clients for a wider attack

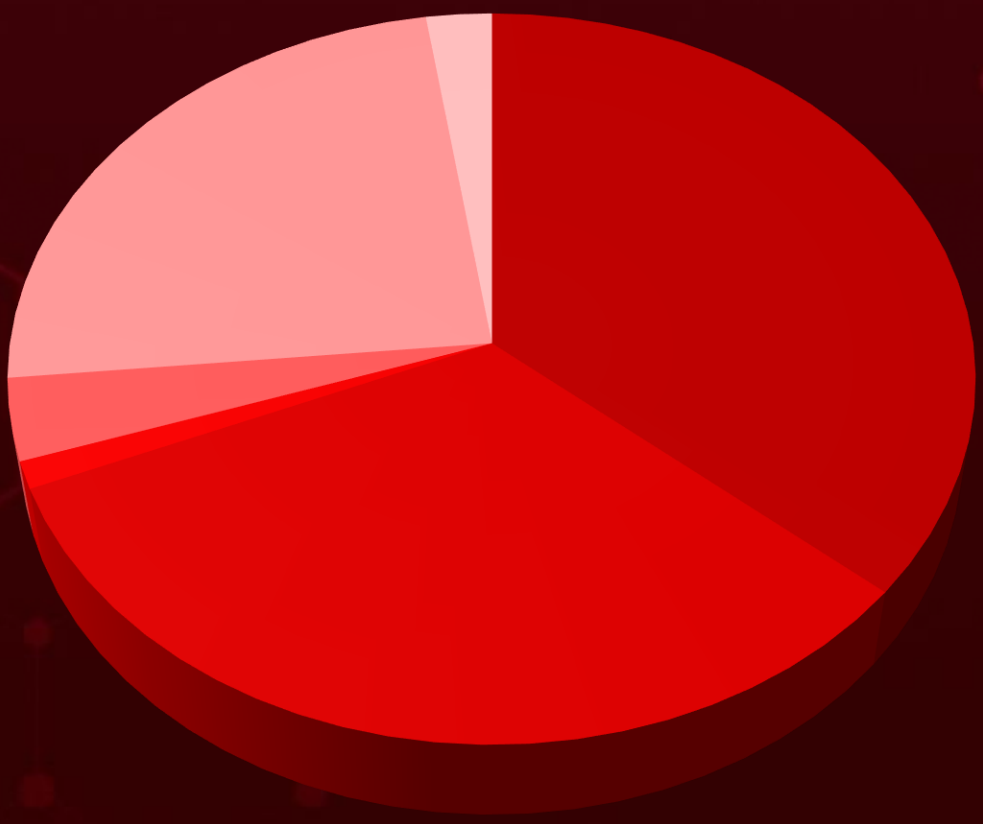
Malware Infiltrates Justice AV Solutions:

Courtroom recording software, Justice AV Solutions, **backdoored** with **Rustdoor** and **Gatedoor** malware

Over 500 Organizations Held Hostage: Black Basta

Ransomware on the Rampage

Threat Landscape



Celebrity Vulnerabilities

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-1472	✗	Microsoft Netlogon	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
ZeroLogon (Microsoft Netlogon Privilege Escalation Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-330	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-42278	✗	Microsoft Active Directory Domain Services	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
NoPac (Microsoft Active Directory Domain Services Privilege Escalation Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-42278

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-42287		Microsoft Active Directory Domain Services	-
	CISA KEV		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
NoPac (Microsoft Active Directory Domain Services Privilege Escalation Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-269	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-42287

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34527		Windows Print Spooler	-
	CISA KEV		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
PrintNightmare (Windows Print Spooler Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-269	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34527

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	✓	Microsoft Windows Support Diagnostic Tool (MSDT)	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
Follina (Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-610	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-30190

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-5195	✓	Linux Kernel	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:canonical:ubuntu_linux:*:*:*:-:*:*:*	Ebury Botnet
Dirty COW (Linux Kernel Race Condition Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-362	T1068: Exploitation for Privilege Escalation	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=19be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4323	✗	Fluent Bit versions 2.0.7 through 3.0.3	-
	CISA KEV		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:fluent_bit:fluent_bit:*:*:*:*:*:*:*:*	-
Linguistic Lumberjack (Fluent Bit Memory Corruption Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-122	T1190 : Exploit Public-Facing Application, T1082 : System Information Discovery	https://github.com/fluent/fluent-bit/releases/tag/v3.0.4

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2015-2051	D-Link DIR-645 Router Remote Code Execution Vulnerability	Dir-645: All versions	✗	✓	✓
CVE-2023-49606	Tinyproxy HTTP Connection Headers Use-After-Free Vulnerability	Tinyproxy	✗	✗	✓
CVE-2023-40000	WordPress LiteSpeed Cache Plugin Cross-Site Scripting Vulnerability	WordPress LiteSpeed Cache Plugin	✗	✗	✓
CVE-2024-4671	Google Chromium Visuals Use After Free Vulnerability	Google Chromium	✓	✓	✓
CVE-2021-3129	Laravel Ignition File Upload Vulnerability	Laravel Ignition	✗	✓	✓
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect	✗	✓	✓
CVE-2020-1472	ZeroLogon (Microsoft Netlogon Privilege Escalation Vulnerability)	Microsoft Netlogon	✗	✓	✓
CVE-2021-42278	NoPac (Microsoft Active Directory Domain Services Privilege Escalation Vulnerability)	Microsoft Active Directory Domain Services	✗	✓	✓
CVE-2021-42287	NoPac (Microsoft Active Directory Domain Services Privilege Escalation Vulnerability)	Microsoft Active Directory Domain Services	✗	✓	✓
CVE-2021-34527	PrintNightmare (Windows Print Spooler Remote Code Execution Vulnerability)	Windows Print Spooler	✓	✓	✓
CVE-2022-30190	Follina (Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability)	Microsoft Windows Support Diagnostic Tool (MSDT)	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-4761	Google Chrome Out of bounds write in V8 Vulnerability	Google Chrome	✓	✓	✓
CVE-2024-4947	Google Chrome Type Confusion in V8 Vulnerability	Google Chrome	✓	✓	✓
CVE-2024-30040	Microsoft Windows MSHTML Platform Security Feature Bypass Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-30051	Microsoft Windows DWM Core Library Elevation of Privilege Vulnerability	Microsoft Windows DWM Core Library	✓	✓	✓
CVE-2021-45467	CentOS Web Panel Pre-Authentication File Inclusion Vulnerability	CentOS Web Panel	✗	✗	✓
CVE-2016-5195	Dirty COW (Linux Kernel Race Condition Vulnerability)	Linux Kernel	✓	✓	✓
CVE-2024-4323	Linguistic Lumberjack (Fluent Bit Memory Corruption Vulnerability)	Fluent Bit	✗	✗	✓
CVE-2024-27130	QNAP QTS/QuTS hero Buffer Overflow Vulnerability	QTS and QuTS hero	✗	✗	✓
CVE-2024-4985	GitHub Enterprise Server Authentication Bypass Vulnerability	GitHub Enterprise Server (GHES)	✗	✗	✓
CVE-2023-0669	Fortra GoAnywhere MFT Remote Code Execution Vulnerability	Fortra GoAnywhere MFT	✓	✓	✓
CVE-2024-5274	Google Chrome Type Confusion in V8 Vulnerability	Google Chrome	✓	✓	✓
CVE-2024-4978	JAVS Arbitrary code Execution Vulnerability	JAVS Viewer software	✗	✓	✓
CVE-2024-24919	Check Point Security Gateway Information Disclosure Vulnerability	Check Point Security Gateway	✓	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Goldoon	Botnet	CVE-2015-2051	D-Link DIR-645 Router	✓	Exploiting Vulnerability
Cuckoo	Infostealer and Spyware	-	macOS	-	-
Nicecurl	Backdoor	-	-	-	Spear phishing
Tamecat	Backdoor	-	-	-	Spear phishing
Cuttlefish	Infostealer	-	-	-	-
HijackLoader	Loader	-	-	-	-
zEus	Infostealer	-	Microsoft Windows	-	Social Engineering
RokRAT	RAT	-	-	-	-
DiceLoader	Loader	-	-	-	Social Engineering
Black Basta Rasnomware	Ransomware	CVE-2021-34527 CVE-2022-30190	Windows, Linux, macOS, and Vmware ESXi	✓	Phishing
Qakbot	Trojan	CVE-2021-34527 CVE-2022-30190	Windows, Linux, macOS, and Vmware ESXi	✓	Phishing
Trinity Ransomware	Ransomware	-	-	-	-
Cobalt Strike Beacon	Hack Tool	-	-	-	Social Engineering
Ebury Botnet	Botnet	CVE-2021-45467 CVE-2016-5195	Linux	-	-

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
LunarLoader	Loader	-	-	-	-
LunarWeb	Backdoor	-	-	-	-
LunarMail	Backdoor	-	-	-	-
Gomir	Backdoor	-	Linux	-	Social Engineering
Troll Stealer	Infostealer	-	-	-	Social Engineering
GoBear	Backdoor	-	-	-	Social Engineering
SugarGh0st RAT	RAT	-	-	-	Phishing
DarkGate	Loader	-	-	-	Phishing
Metamorfo	Trojan	-	-	-	Malspam campaigns
Grandoreiro	Trojan	-	-	-	Phishing
Dora RAT	RAT	-	-	-	Phishing
Nestdoor	RAT	-	-	-	Phishing
D3F@ck	Loader	-	Windows	-	Google Ads
GhostEngine	Crypto Miner	-	-	-	Phishing
XMRig	Crypto Miner	-	-	-	Phishing
Acrid	Infostealer	-	-	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
ScarletStealer	Infostealer	-	-	-	Phishing
Sys01	Infostealer	-	-	-	Phishing
5.t Downloader	Downloader	CVE-2023-0669	Fortra GoAnywhere MFT		-
Tiny backdoor	Backdoor	-	-	-	Phishing
ShrinkLocker Ransomware	Ransomware	-	Windows	-	-
RustDoor	Backdoor	CVE-2024-4978	JAVS Viewer software		Exploiting Vulnerability
GateDoor	Backdoor	CVE-2024-4978	JAVS Viewer software		Exploiting Vulnerability
FakePenny Ransomware	Ransomware	-	-	-	Phishing

Adversaries Summary

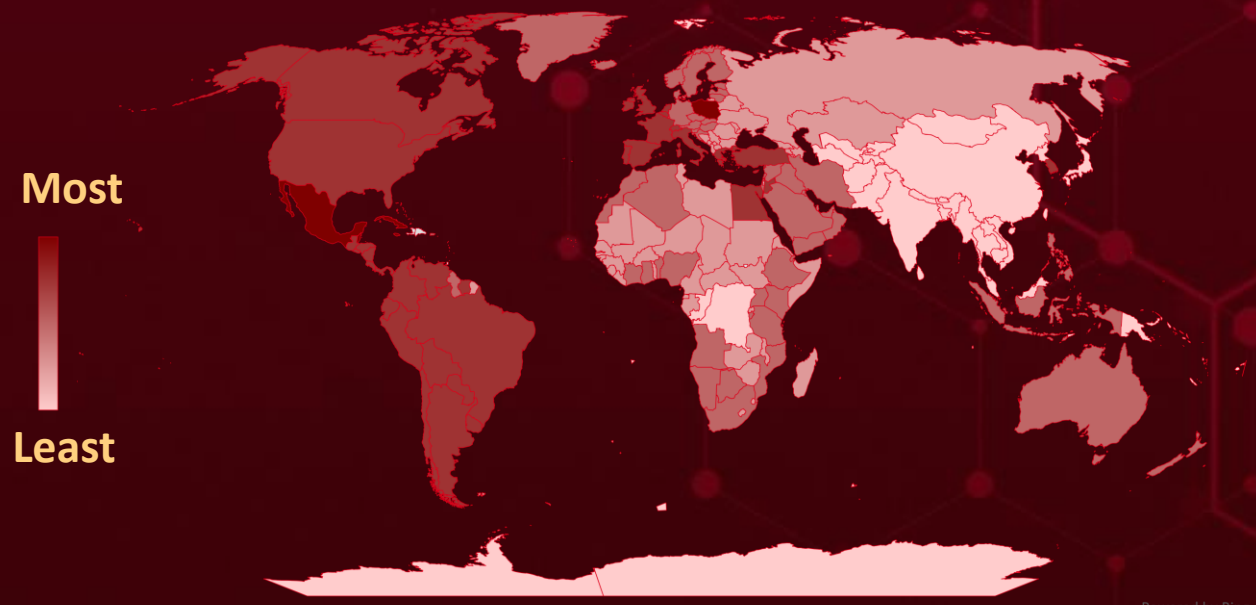
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
APT28	Information theft and espionage	Russia	-	-	-
APT42	Information theft and espionage	Iran	-	Nicecurl, Tamecat	-
FIN7	Financial crime	Russia	-	DiceLoader	-
Turla	Information theft and espionage	Russia	-	LunarLoader, LunarWeb, LunarMail	-
Kimsuky	Information theft and espionage	North Korea	-	Gomir, Troll Stealer, GoBear	-
UNK_SweetSpecter	Espionage	-	-	SugarGh0st RAT	-
Andariel	Espionage, Monetary Gains	North Korea	-	Dora RAT, Nestdoor	-
Sharp Dragon	Information theft and espionage	China	CVE-2023-0669	5.t Downloader	Fortra GoAnywhere MFT
Turla	Information theft and espionage	Russia	-	Tiny backdoor	Windows
Moonstone Sleet	Information theft, Financial Gains	North Korea	-	FakePenny Ransomware	-
UNC5537	Information theft, extortion	-	-	-	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
D-Link	Router	D-Link Dir-645: All versions
F5	Application	BIG-IP Next Central Manager Versions 20.0.1 - 20.1.0
WordPress	Plugin	WordPress LiteSpeed Cache Plugin versions prior 5.7.0.1
Chrome	Browser	Google Chrome prior to 124.0.6367.201, Google Chrome prior to 124.0.6367.207, Google Chrome prior to 125.0.6422.60, Google Chrome prior to 125.0.6422.112
Laravel	Application	Laravel Ignition: 1.16.0 - 1.16.4
ConnectWise	Application	ConnectWise ScreenConnect 23.9.7 and prior
Microsoft	Application	Windows Server: 2008 R2 - 2019 2004, Windows Server: 2008 - 2019 2004, Microsoft Active Directory, Windows Print Spooler, Microsoft Windows Support Diagnostic Tool, Windows: 10 - 11 23H2, Windows Server: 2016 - 2022 23H2, Windows Server: 2008 R2 SP1 - 2022 23H2, Microsoft SharePoint Server: 2019, Microsoft SharePoint Server Subscription Edition: All versions, Microsoft SharePoint Enterprise Server: 2016
CentOS	Application	CentOS Web Panel before 0.9.8.1107
Linux	OS	Linux kernel 2.x through 4.x before 4.8.3

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
fluentbit	Telemetry Agent	Fluent Bit version 2.0.7 through 3.0.3
QNAP	Application	QNAP QTS Prior to 5.1.7 and QuTS hero Prior to h5.1.7
	Application	All versions of GitHub Enterprise Server prior to 3.13.0
FORTRA	Application	Fortra GoAnywhere MFT
	Application	GitLab versions 15.11 prior to 16.10.6, 16.11 prior to 16.11.3, and 17.0 prior to 17.0.1.
JAVS JUSTICE AV SOLUTIONS	Application	JAVS Viewer Software Version 8.3.7
CHECK POINT	Security Gateway Appliance	Check Point CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, Quantum Spark Appliances versions: R77.20 (EOL), R77.30 (EOL), R80.10 (EOL), R80.20 (EOL), R80.20.x, R80.20SP (EOL), R80.30 (EOL), R80.30SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, R81.20

Targeted Countries



Color	Countries
	Jamaica
	Cuba
	Mexico
	Belize
	Poland
	Ireland
	Paraguay
	Argentina
	Brazil
	United Kingdom
	Canada
	Belgium
	Chile
	Nicaragua
	Colombia
	Switzerland
	Costa Rica
	Uruguay
	Bahamas
	Venezuela
	Cyprus
	Jordan

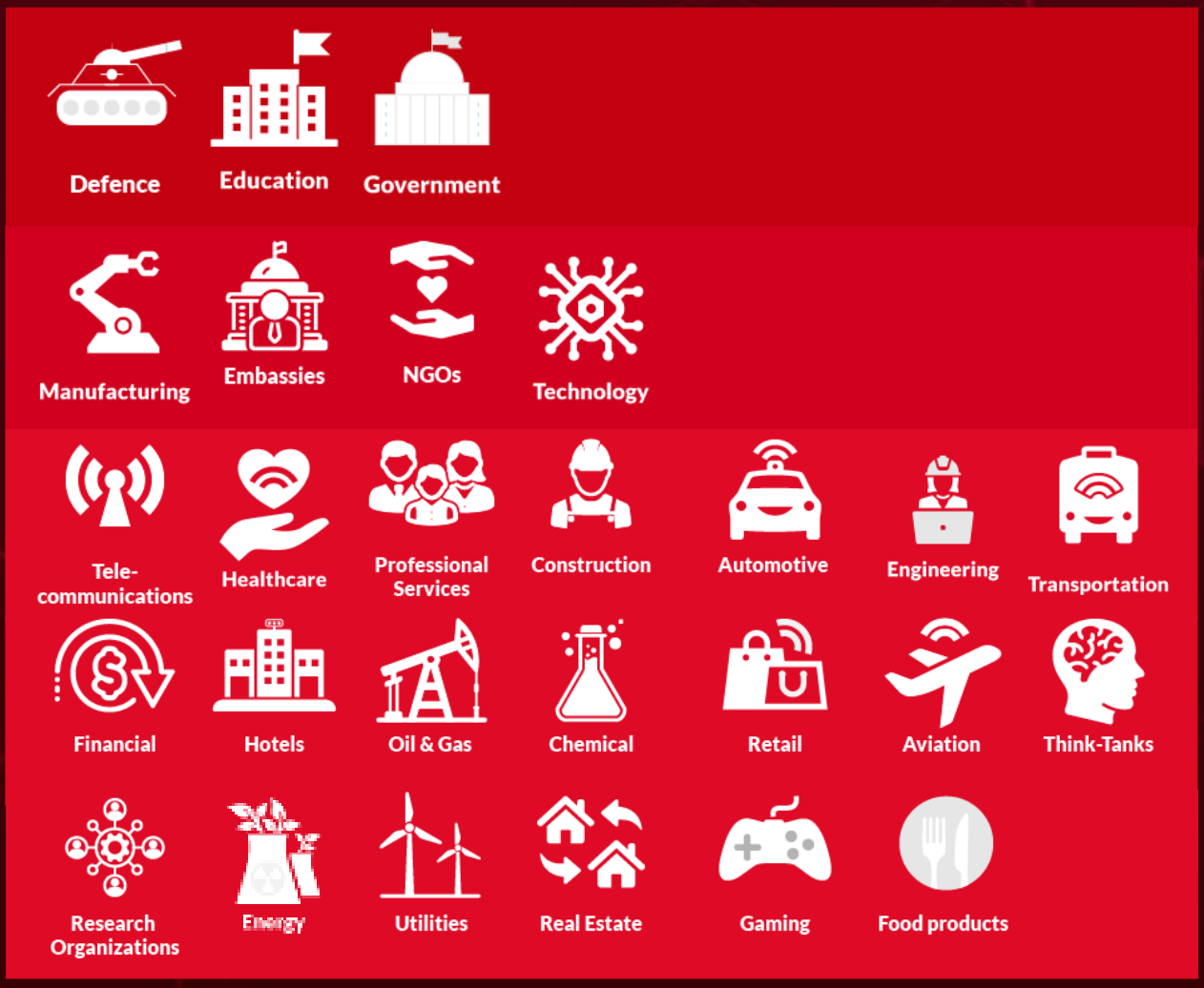
Color	Countries
	Ecuador
	Netherlands
	Peru
	Panama
	Portugal
	Bolivia
	Spain
	Egypt
	South Korea
	El Salvador
	Suriname
	France
	Turkey
	Greece
	United States
	Guatemala
	Honduras
	Italy
	Turks and Caicos Islands
	Saint Barthélemy
	Curaçao

Color	Countries
	British Virgin Islands
	Benin
	Greenland
	Nigeria
	Guadeloupe
	Denmark
	Burundi
	Sint Maarten
	Guyana
	Estonia
	Australia
	Aruba
	Hungary
	Oman
	Iceland
	Czech Republic
	Indonesia
	Puerto Rico
	Iran
	San Marino
	Iraq
	Slovenia
	Caribbean Netherlands
	Botswana
	Israel

Color	Countries
	Tanzania
	Cayman Islands
	United Arab Emirates
	Yemen
	Vatican City
	Austria
	Norway
	Andorra
	Palestine
	Kenya
	Anguilla
	Latvia
	Philippines
	Lebanon
	Djibouti
	Liechtenstein
	Qatar
	Lithuania
	Saint Martin
	Luxembourg
	Saudi Arabia
	Malta

Color	Countries
	Slovakia
	Martinique
	South Africa
	Bahrain
	Algeria
	Monaco
	Sweden
	Montserrat
	Syria
	Morocco
	Ethiopia
	Mozambique
	Uganda
	Namibia
	Finland
	Croatia
	Germany
	New Zealand
	Ghana
	Angola
	Ivory Coast
	Kuwait
	Equatorial Guinea

Targeted Industries



TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1588** Obtain Capabilities	**T1204** User Execution	**T1036** Masquerading	**T1082** System Information Discovery
T1588.006 Vulnerabilities	**T1566** Phishing	**T1041** Exfiltration Over C2 Channel	**T1027** Obfuscated Files or Information	**T1055** Process Injection
T1140 Deobfuscate/ Decode Files or Information	**T1059.001** PowerShell	**T1204.002** Malicious File	**T1057** Process Discovery	**T1190** Exploit Public-Facing Application
T1068 Exploitation for Privilege Escalation	**T1056** Input Capture	**T1071** Application Layer Protocol	**T1212** Exploitation for Credential Access	**T1547** Boot or Logon Autostart Execution
T1562 Impair Defenses	**T1070** Indicator Removal	**T1053** Scheduled Task/Job	**T1588.005** Exploits	**T1005** Data from Local System

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Goldoon	SHA256	66f21251d7f8c58316f149fec104723beb979a1215ad4e788d83f0ee6fd34696, 712d9abe8fbdff71642a4d377ef920d66338d73388bfee542f657f2e916e219c, d7367d41d19baa4f1022f8eb47f7ff1e13f583265c7c26ab96d5f716fa0d61ee, fdf6dae772f7003d0b7cdc55e047434dbd089e0dc7664a3fae8ccfd9d10ece8c, aa9e6006bce7d0b4554165dba76e67c4a44d98090c9e6ac9f3dca726f6e9adbf, fc44018b7432d9e6a1e98f723b0402101fa6e7483d098b10133aac142c0a4a0b, e7b78f16d0dfc91b4c7e8fd50fc31eba1eb22ec7030af9bf7c551b6019c79333, 0e6eb17664943756cab434af5d94fcd341f154cb36fc6f1ef5eb5cfdce68975f, 9af8720766c5f3978718c026c2263801b08634443c93bd67022c56c6ef531ef3, df71219ba6f5835309479b6e3eaca73b187f509b915420656bfe9a9cc32596c2, 48130a7c09a5c92e15b3fc0d2e1eb655e0bd8f759e01ba849f7734e32dbc2652, 8eb9c1eaecd0dcdd242e1bc8c62a1052915b627abe2de8ce147635fb7da3bfcc, b050a1ff0d205f392195179233493ff5b6f44adc93fe0dba1f78c4fe90ebcc46, ffd2d3888b6b1289e380fa040247db6a4fbd2555db3e01fadd2fe41a0fa2debc, 88cea61218bdeea94537b74c67873e75b8ada6d050a30d311569c3118d161c46, 115e15fbee077a9e126cc0eb349445df34cc9404245520c702fadc5f75b6f859, b10e47db989e29ace6c23ed15e29f313993f95e5e6157110608 81dfa84618071, 037331ab84a841b9d3cfb6f8797c1695e2dc0a2cdcc3f8f3c794dfaa50bcf0df, 5631980fab33525f4de1b47be606cd518403f54fa71b81186f02dbf7e9ed0004, 246142a5e3f3d3f84d8b38f98ff6897b03628e06e31016b8fafc9eb8c2b6201d

Attack Name	TYPE	VALUE
zEus	SHA256	aabfbef31ab073d99c01ecae697f66bbf6f14aa5d9c295c7a6a548879381fb24, c9687714cf799e5ce9083c9afa3e622c978136d339fc9c15e272b0df9cd7e21c, d9d394cc2a743c0147f7c536cbb11d6ea070f2618a12e7cc0b15816307808b8a, c2c8a7050b28d86143f4d606a6d245b53c588bc547a639094fce857962246da4, be9ea302bcfb52fbfdf006b2df8357388cd4c078059aabc5b5928676c3361e50, 9d3409852348caa65d28e674008dd6bb986eed4fb507957c7a8b73a41e00be70, b6e8b612e99c54dd98af1756f7c9b8a8c19e31ed9b2836878c2a5144563ff1b2, 8a2f6d5f6cf7d1a7534454e3c3007337b71d7da470e86f7636eb02d68b2db8cc, df6156fdbbcc7b6f8c9cb4c5c1b0018fc3f1e1ca7d949b5538ec27dc86d026a4, 5840f3e43a0c635be94b5fbf2e300d727545371b582361a52682b4a9e08bcebd, 51ede75315d858209f9aa60d791c097c18d38f44b9d050b555ff1f4de0ae672d, d1865d2aaf11e3f8bccefe9c4847510234f14aaa5378ce9e8e97553537cf2ca1, 9ba19d614af029c3c198b576ccdf1de87d80ac14b12103e8a15376229a2a7860, 6063c8285e13d10eabbe363e2ab0d8748bcd595b470698e0cffee31ba255a566, d1a18b436f947611914ced09e4465b49807cec4f3a62b0973c9017b6d82c9f70, 1cdd580176eeb4342a0333b50454da061e473358274e6e543df1411186c12042, ed59a797521db06abdf4c88dad7b1666e5978aaa6670a5952a55b7e11f7b790e, 2ceae724f0e96e2d8c47296dd1e73ac592e22ee3288eabf11c8d039c6d6d4f8b, 03983b56d8b1a6cc43109f6cd67a13666367595a2ea07766127cb1fe4d4bb1a5, 9940da9d02d29489c3e26d27feb15b6f4bbf49547b962592125441917c952f12, fbf967295dac00f1e9cb67e9a40b6729b003dd12cf022eb15d626df09716442d, 4e0a96ab28570936d095ac3910dcd239c7ceeb2b38a070468404584f8b902dd1, 20009fd157a898ad6d50fae6b8127056c5b1f50e31f90f01d2e6c13e6b4c38f8

Attack Name	TYPE	VALUE
Black Basta Rasnomware	MD5	2642ec377c0cee3235571832cb472870, 4c897334e6391e7a2fa3cbcbf773d5a4, B3fe23dd4701ed00d79c03043b0b952e
Trinity Ransomware	MD5	949c438e4ed541877dce02b38bf593ad
	SHA1	4c58d2d624d9bdf6b14a6f8563788785074947a7
	SHA256	36696ba25bdc8df0612b638430a70e5ff6c5f9e75517ad401727be03b26d8ec4
Cobalt Strike Beacon	Domain	limitedtoday[.]com, thetrailbig[.]net
Ebury Botnet	IPv4	135[.]181[.]148[.]230, 141[.]164[.]52[.]243, 141[.]255[.]166[.]187, 146[.]70[.]124[.]102, 185[.]145[.]245[.]167, 185[.]59[.]103[.]8, 195[.]123[.]225[.]83, 213[.]232[.]235[.]104, 45[.]59[.]120[.]146
	Domain	a1hcy1xendd[.]net, a1k8h2xendd[.]info, a1t9y1xendd[.]info, a1z1h2xendd[.]biz, abo0u6ach9k3w[.]net, b2z6m9k1zaf3v[.]net, b8dfs5ecw9p3o[.]info, c0dbq5vcj9o3e[.]info, c1b1jfi2pdi8w1f[.]net, c1jczbhcpdi8w1f[.]biz, c1m8k5q0hfi8w1f[.]net, c1v9j2pahfi8w1f[.]biz, c1v9l8s6yei8w1f[.]info, c9xfb8u1cad3m[.]net, checklicence[.]net, f2y1j8v1saa3t[.]biz, f8wda5yck9i3h[.]net, fas1k9i1jap3u[.]biz, h0nct5rca9y3f[.]biz, h9g0q8a1hat3s[.]net, hdm5o8e1tas3n[.]net, idkff7m1lac3g[.]biz, k2qai2yeodm[.]net, k2rdz1yeodm[.]biz, k2t6i2yeodm[.]biz, k2zbz1yeodm[.]info, larfj7g1vaz3y[.]net,

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-2051	✗	Dir-645: All versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:dir-645_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:dlink:dir-645:a1:*:*:*:*:*:*:*	Goldoon Botnet
D-Link DIR-645 Router Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190 : Exploit Public-Facing Application, 1505 : Server Software Component	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-49606	✗	Tinyproxy 1.11.1 and Tinyproxy 1.10.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:tinyproxy:tinyproxy:1.10.0:*:*:*:*:*:*:* cpe:2.3:a:tinyproxy:tinyproxy:1.11.1:*:*:*:*:*:*:*	-
Tinyproxy HTTP Connection Headers Use-After-Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://github.com/tinyproxy/tinyproxy/releases/tag/1.11.2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-40000		WordPress LiteSpeed Cache Plugin versions prior 5.7.0.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:litespeed_technologies:litespeed_cache_plugin:*:*:*:*:*:*:*:*	-
WordPress LiteSpeed Cache Plugin Cross Site Scripting Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter; T1189: Drive-by Compromise	https://wpscan.com/vulnerability/dd9054cc-1259-427d-a4ad-1875b7b2b3b4/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4671		Google Chrome prior to 124.0.6367.201	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Visuals Use After Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1189: Drive-by Compromise; T1203: Exploitation for Client Execution	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-3129		Laravel Ignition	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:facade:ignition:*:*:*:*:*:laravel:*:* cpe:2.3:a:laravel:laravel:*:*:*:*:*:*:*:*	-
Laravel Ignition File Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter	https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/master/cves/2021/CVE-2021-3129.yaml

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-1709		ConnectWise ScreenConnect	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
ConnectWise ScreenConnect Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application	https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4761		Google Chrome	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Out of bounds write in V8 Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059.007: JavaScript T1189: Drive by Compromise	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4947		Google Chrome	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Type Confusion in V8 Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1059.007: JavaScript T1189: Drive-by Compromise	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-30040	✗	Microsoft Windows	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows MSHTML Platform Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30040

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-30051	✗	Microsoft Windows DWM Core Library	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows DWM Core Library Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-45467	✗	CentOS Web Panel	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:control-webpanel:webpanel:*:*:*:*:*:*:*:*	Ebury Botnet
CentOS Web Panel Pre-Authentication File Inclusion Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1068: Exploitation for Privilege Escalation	https://control-webpanel.com/changelog

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-27130	✗	QTS Prior to 5.1.7 and QuTS hero Prior to h5.1.7	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:qnap:qts:*:*:*:*:*:*:*:* cpe:2.3:a:qnap:quts_hero:*:*:*:*:*:*:*:*	-
QNAP QTS/QuTS hero Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1068 : Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://www.qnap.com/en-in/download

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-4985</td><td>✗</td><td rowspan="2">All versions of GitHub Enterprise Server prior to 3.13.0</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:github:enterprise_server:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">GitHub Enterprise Server Authentication Bypass Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-303</td><td>T1190 : Exploit Public-Facing Application, T1556 : Modify Authentication Process</td><td>https://docs.github.com/en/enterprise-server@3.12/admin/release-notes#3.12.4; https://docs.github.com/en/enterprise-server@3.11/admin/release-notes#3.11.10; https://docs.github.com/en/enterprise-server@3.10/admin/release-notes#3.10.12; https://docs.github.com/en/enterprise-server@3.9/admin/release-notes#3.9.15</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-0669	✗ ZERO-DAY	Fortra GoAnywhere MFT version prior to 7.1.2	Sharp Dragon
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:fortra:goanywhere_managed_file_transfer:*:*:*:*:*:*:*:*	5.t Downloader
Fortra GoAnywhere MFT Remote Code Execution Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-502	T1059 : Command and Scripting Interpreter, T1203 : Exploitation for Client Execution	https://my.goanywhere.com/webclient/Login.xhtml

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-5274	✗ ZERO-DAY	Google Chrome version prior to 125.0.6422.112	-
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Type Confusion in V8 Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-843	T1059.007: JavaScript T1189: Drive-by Compromise	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4978		JAVS Viewer Software Version 8.3.7	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:justice_av_solutions:viewer:*:*:*:*:*:*:*:*	RustDoor, GateDoor
JAVS Arbitrary code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1059: Command and Scripting Interpreter, T1195: Supply Chain Compromise	https://www.javs.com/downloads/

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

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Goldoon	The Goldoon botnet is a recent malware threat targeting a critical vulnerability in D-Link DIR-645 routers. This decade-old flaw (CVE-2015-2051) allows attackers to remotely take control of the router. Once infected, the Goldoon malware can steal information about the network, establish a persistent presence, and even launch denial-of-service	Exploiting vulnerability	CVE-2015-2051
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Data theft and launch denial-of-service	Dir-645: All versions
ASSOCIATED ACTOR			**PATCH LINK**
-			https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cuckoo	Cuckoo malware, named after the parasitic bird, targets macOS systems as a dual infostealer and spyware, clandestinely gathering sensitive data and monitoring user activities for malicious purposes	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer and Spyware		Data theft	macOS
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Nicecurl	NICECURL is a backdoor coded in VBScript, skilled at obtaining extra modules for execution. These modules include data mining and executing commands as needed. NICECURL communicates securely over HTTPS.	Spear phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft, Espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
APT42 (aka UNC2448)			-

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
Tamecat	TAMECAT serves as a PowerShell entry point capable of running custom PowerShell or C# code. It initiates its operations through a compact VBScript downloader, which utilizes Windows Management Instrumentation (WMI) to assess the antivirus solutions active on the target system.	Spear phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft, Espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
APT42 (aka UNC2448)			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cuttlefish	Cuttlefish malware has been detected penetrating enterprise-grade as well as small office/home office (SOHO) routers with the intent of covertly monitoring data transmissions and pilfering authentication credentials. Employing a zero-click method, Cuttlefish seamlessly siphons data from users and devices situated within the confines of the targeted network's perimeter.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Credential Theft, Espionage, Information Theft	-
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
HijackLoader (aka IDAT Loader)	The modular malware loader known as HijackLoader has undergone notable evolution, marked by the adoption of innovative evasion tactics. A fresh variant of this loader utilizes a PNG image to distribute subsequent malware stages. This advanced iteration is outfitted with numerous modules dedicated to injecting and executing code, thus amplifying both its efficacy and stealth capabilities.	Unknown	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft and compromised systems	-
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
zEus	zEus stealer has adeptly infiltrated both a source pack distributed on YouTube and a Minecraft pack concealed within a WinRAR file, cleverly posing as a Windows screensaver. Its ability to gather diverse data effectively poses a significant threat, enhancing the potential for future attacks.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft, Espionage	Microsoft Windows
Information Stealer			
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
RokRAT	The RokRAT malware spreads through LNK files hidden within seemingly genuine documents. Upon activation, this malicious software triggers PowerShell commands, which in turn initiate the execution of additional files. This process enables the extraction of user data, which is subsequently sent to the perpetrators' command and control (C2) servers.	Unknown	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft, Espionage	-
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DiceLoader	DiceLoader is a compact malware component in the FIN7 arsenal. It is deployed using a PowerShell script with specific obfuscation techniques and is often accompanied by other malware from their toolset.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		System Compromise	-
ASSOCIATED ACTOR			
FIN7			**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
Black Basta Rasnomware	Black Basta is a ransomware-as-a-service (RaaS) variant that was first identified in April 2022. They employ a double-extortion model, where they not only encrypt the victim's systems but also exfiltrate data. This dual approach increases the pressure on victims to pay the ransom, as they face the threat of data leaks in addition to system inaccessibility.	Phishing	CVE-2021-34527 CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	Windows, Linux, macOS, and Vmware ESXi
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-30190

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Qakbot	Classified as a banking trojan, Qakbot is designed to steal sensitive data and attempts to self-propagate to other systems within the network. Qakbot also provides remote code execution (RCE) capabilities, enabling attackers to perform manual attacks to achieve secondary objectives, such as scanning the compromised network or deploying ransomware.	Phishing	CVE-2021-34527 CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Steal data	Windows, Linux, macOS, and Vmware ESXi
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-30190

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
Trinity Ransomware	Trinity is a newly identified ransomware variant, believed to be an updated version of the "2023Lock" ransomware. This malware encrypts user files and appends the ".trinitylock" extension to them.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cobalt Strike Beacon	Cobalt Strike is a paid penetration testing tool that allows attackers to deploy an agent called 'Beacon' on a victim's machine. Beacon offers a range of functionalities, including command execution, key logging, file transfer, SOCKS proxying, privilege escalation, mimikatz integration, port scanning, and lateral movement.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Hack Tool		Execute Commands	-
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
Ebury Botnet	Ebury is a Linux malware botnet that has been infecting Linux servers for over a decade. It uses various tactics such as exploiting software vulnerabilities, using stolen credentials, and hiding behind fake identities. Once inside a server, Ebury can steal login information, act as a backdoor for further attacks, and deploy additional tools to steal credit card details and reroute traffic.	-	CVE-2021-45467 CVE-2016-5195
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Steal data	Linux
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LunarLoader	LunarLoader utilizes the RC4 symmetric key cipher. It allocates memory for the PE image and decrypts the name of an exported function within the PE file, which is then executed in a new thread.	-	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		System Compromise	-
Loader			
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
LunarWeb	The LunarWeb backdoor, deployed on servers, leverages HTTP(S) for its command and control (C&C) communications, emulating legitimate requests. During initialization, LunarWeb attempts to locate or generate its state file, which contains entries related to its execution.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
Turla			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LunarMail	The LunarMail backdoor, installed on workstations, is embedded as an Outlook add-in and uses email messages for its command and control (C&C) communications. It employs steganography to hide commands within images, thereby evading detection.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
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
Gomir	Gomir shares many similarities with GoBear, featuring direct C2 communication, persistence mechanisms, and support for executing a wide range of commands. Upon installation, the malware checks the group ID value to determine if it runs with root privileges on the Linux machine. If it has root privileges, it copies itself to /var/log/syslogd for persistence.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Exfiltrate data	Linux
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Troll Stealer	Troll Stealer is an information-stealing malware written in the Go language. It exfiltrates various types of data, including SSH credentials, FileZilla information, browser data, system information, and screen captures. The malware is distributed via droppers disguised as Korean security software installers and is signed with a stolen certificate.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Steal data	-
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky			-

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
GoBear	GoBear is a backdoor malware crafted in the Go language and authenticated with a legitimate D2innovation Co., LTD certificate. This insidious threat operates by executing malicious commands received from a C&C server. GoBear establishes persistent access to the infected system, enabling attackers to control and manipulate the device remotely.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Execute Commands, Steal data	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SugarGh0st RAT	SugarGh0st RAT is a remote access trojan, which is a customized variant of Gh0stRAT. During the infection process, it utilizes Windows Shortcut files containing malicious JavaScript to deploy DLL loaders and execute SugarGh0st binaries. This malware is capable of gathering system details, executing various file operations, enabling remote control by attackers, initiating reverse shells, and executing arbitrary commands sent by the attackers.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Execute Commands	-
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
UNK_SweetSpecter			-

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
DarkGate	DarkGate malware is a potent and adaptable threat that infiltrates computer systems, compromising security. It has infostealer functionality, enabling attackers to control compromised systems and extract valuable information. DarkGate has been implicated in various malicious activities, including data exfiltration, credential phishing, and ransomware deployment.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft	
Loader			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Metamorfo	Metamorfo, also referred to as Mekotio or Casbaneiro, is an advanced banking Trojan disseminated through malspam campaigns, primarily targeting users in North and South America. Active since 2018, this malware is designed to pilfer financial information and banking credentials.	Malspam campaigns	-
TYPE		IMPACT	AFFECTED PRODUCTS
Trojan		Data theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Grandoreiro	The Grandoreiro banking Trojan, initially targeting Latin America, has evolved to attack financial institutions globally, now targeting over 1500 banks in 60 countries. The latest variant can harvest email addresses from infected Outlook clients to send further phishing emails.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Trojan		Data theft and Manipulate transactions	-
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
Dora RAT	The attackers introduced a new malware, Dora RAT, developed in the Go language. Dora RAT is relatively simple, supporting reverse shell and file download/upload functions. It exists in two variants: one as a standalone executable and another injected into the explorer.exe process.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Andariel group			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Nestdoor	Nestdoor is a RAT malware that has been active since at least May 2022. It enables attackers to control infected systems by receiving commands remotely. The Andariel group has been consistently linked to attack cases involving this malware.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Andariel group			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
D3F@ck	D3F@ck Loader is a new malware loader that leverages Google Ads and EV certificates to bypass security measures. It can download other malware, including Raccoon Stealer and Danabot. It impersonates legitimate applications to trick users into downloading it.	Google ads	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Malware Deployment and System Compromise	Windows
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
GhostEngine	GhostEngine is a sophisticated malware that disables security measures and uses advanced techniques to install and maintain a persistent crypto-miner on infected systems. It employs methods like leveraging vulnerable drivers and PowerShell scripts to deploy the XMRig Monero miner.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Crypto Miner		Cryptomining	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XMRig	XMRig is an open-source cryptocurrency mining software commonly used to mine Monero (XMR). While it can be used legitimately, it is often exploited by cybercriminals in malware campaigns to secretly mine cryptocurrency on infected systems, draining system resources and reducing performance	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Crypto Miner		Cryptomining	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Acrid	Acrid malware is a type of information stealer that spreads primarily through malicious email attachments and websites, targeting login credentials, cookies, and other sensitive data from browsers. Acrid is written in C++ for the 32-bit system.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data theft	-
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
ScarletStealer	ScarletStealer is a sophisticated information-stealing malware that often disguises itself as legitimate software to trick users. It targets a wide range of data, including cryptocurrency wallets, gaming accounts, and social media credentials.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Sys01	SYS01, also known as "Album Stealer" or "S1deload Stealer," is a relatively unknown malware active since at least 2022. It has evolved from a C# stealer to a PHP-based variant, with recent versions combining both C# and PHP payloads.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
5.t Downloader	The 5.t downloader is a malicious program specialized in downloading and installing additional malware on infected systems. It spreads via phishing emails, malicious websites, or bundled software, establishing connections to remote servers to fetch and deploy harmful payloads, facilitating multi-stage cyberattacks.	-	CVE-2023-0669
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Downloads other malware	Fortra GoAnywhere MFT
ASSOCIATED ACTOR			**PATCH LINK**
Sharp Dragon			https://my.goanywhere.com/webclient/Login.xhtml

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
Tiny backdoor	A sophisticated campaign by the Turla APT group, is employing a Tiny backdoor. It uses malicious .LNK files disguised as legitimate documents to target individuals and leverages MSBuild to evade detection.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Turla			-

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

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

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GateDoor	GateDoor is a Windows malware written in Golang. It functions as a backdoor with loader capabilities and is signed with a valid certificate.	Exploiting Vulnerability	CVE-2024-4978
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Infrastructure compromise, Data theft, Loss of Confidentiality	JAVS Viewer software
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.javs.com/downloads/

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FakePenny Ransomware	FakePenny is a new custom ransomware used by Moonstone Sleet in its operations. FakePenny comprises an encryptor and a loader, with its ransomware note resembling that of NotPetya.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Moonstone Sleet (aka Storm-1789)			-

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
APT28 (aka Sofacy , Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Forest Blizzard,BlueDelta,TA422, Fighting Ursa,Blue Athena)	Russia	Aerospace, Defense, Education, Energy, Utilities, Governments, Hospitality, Manufacturing, Oil & Gas, Retail, Technology, Transportation	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0006: Credential Access; TA0011: Command and Control; TA0042: Resource Development; T1562: Impair Defenses; T1556: Modify Authentication Process; T1055: Process Injection; T1587: Develop Capabilities; T1584: Compromise Infrastructure; T1203: Exploitation for Client Execution; T1082: System Information: Discovery; T1546: Event Triggered Execution; T1557; Adversary-in-the-Middle; T1059: Command and Scripting Interpreter; T1219: Remote Access Software; T1018: Remote System Discovery; T1041: Exfiltration Over C2 Channel; T1562.001: Disable or Modify Tools; T1588: Obtain Capabilities

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
APT42 (aka UNC2448)</td><td>Iran</td><td rowspan="3">NGOs, media organizations, academia, legal services, researchers, journalists, defense, foreign affairs</td><td rowspan="3">Western and Middle Eastern</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Nicecurl, Tamecat</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1598: Phishing for Information; T1190: Exploit Public-Facing Application; T1059: Command and: Scripting Interpreter; T1059.007: JavaScript; T1059.005: Visual Basic; T1059.001: PowerShell; T1566: Phishing; T1566.002: Spearphishing Link; T1027: Obfuscated Files or Information; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1047: Windows Management Instrumentation; T1204: User Execution; T1204.001: Malicious Link; T1036: Masquerading; T1056: Input Capture; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1537: Transfer Data to Cloud Account; T1140: Deobfuscate/Decode Files or Information; T1555: Credentials from Password Stores</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
FIN7 (aka Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, ITG14, TAG-CR1)</td><td>Russia</td><td rowspan="3">Casinos and Gambling, Construction, Education, Energy, Financial, Government, High-Tech, Hospitality, Retail, Technology, Telecommunications, Transportation</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial crime</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>DiceLoader</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.006: Python; T1204: User Execution; T1204.001: Malicious Link; T1547: Boot or Logon Autostart Execution; T1033: System Owner/User Discovery; T1176: Browser Extensions; T1199: Trusted Relationship; T1056: Input Capture; T1036: Masquerading; T1053: Scheduled Task/Job; T1140: Deobfuscate/Decode Files or Information; T1055: Process Injection; T1588: Obtain Capabilities; T1588.003: Code Signing Certificates; T1518: Software Discovery; T1518.001: Security Software Discovery; T1592: Gather Victim Host Information; T1082: System Information Discovery; T1219: Remote Access Software; T1104: Multi-Stage Channels; T1132: Data Encoding; T1132.001: Standard Encoding</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 

Turla (aka Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Secret Blizzard, Pensive Ursa, Blue Python, Snake)</td><td>Russia</td><td rowspan="3">Foreign Affairs, Diplomats, Aerospace, Defense, Education, Embassies, Energy, Government, High-Tech, IT, Media, NGOs, Pharmaceutical, Research, Retail</td><td rowspan="3">Afghanistan, Algeria, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bolivia, Botswana, Brazil, China, Chile, Denmark, Ecuador, Estonia, Finland, France, Georgia, Germany, Hong Kong, Hungary, India, Indonesia, Iran, Iraq, Italy, Jamaica, Jordan, Kazakhstan, Kyrgyzstan, Kuwait, Latvia, Mexico, Netherlands, Pakistan, Paraguay, Poland, Qatar, Romania, Russia, Serbia, Spain, Saudi Arabia, South Africa, Sweden, Switzerland, Syria, Tajikistan, Thailand, Tunisia, Turkmenistan, UK, Ukraine, Uruguay, USA, Uzbekistan, Venezuela, Vietnam, Yemen</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>LunarLoader, LunarWeb, LunarMail</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0042: Resource Development; TA0043: Reconnaissance; T1591: Gather Victim Org Information; T1583.002: DNS Server; T1583.003: Virtual Private Server; T1584.003: Virtual Private Server; T1586.002: Email Accounts; T1587.001: Malware; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1059.005: Visual Basic; T1106: Native API; T1204.002: Malicious File; T1137.006: Add-ins; T1547: Boot or Logon Autostart Execution; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1027.003: Steganography; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1036.005: Match Legitimate Name or Location; T1070.004: File Deletion; T1070.008: Clear Mailbox Data; T1140: Deobfuscate/Decode Files or Information; T1480.001: Environmental Keying; T1620: Reflective Code Loading; T1007: System Service Discovery; T1016: System Network Configuration Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1518.001: Security Software Discovery;</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Kimsuky (aka Velvet Chollima, Springtail, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082)</td><td>North Korea</td><td rowspan="3">Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks and Ministry of Unification, Sejong Institute and Korea Institute for Defense Analyses.</td><td rowspan="3">Japan, South Korea, Thailand, USA, Vietnam and Europe</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><th>TARGETED CVEs</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>-</td><td>Gomir, Troll Stealer, GoBear</td><td>-</td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1217: Browser Information Discovery; T1036: Masquerading; T1059: Command and Scripting Interpreter; T1057: Process Discovery; T1056: Input Capture; T1082: System Information Discovery; T1543: Create or Modify System Process; T1543.002: Systemd Service; T1053: Scheduled Task/Job; T1053.003: Cron; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1005: Data from Local System; T1588: Obtain Capabilities; T1588.003: Code Signing Certificates; T1204: User Execution; T1204.002: Malicious File; T1189: Drive-by Compromise; T1070: Indicator Removal; T1070.004: File Deletion; T1529: System Shutdown/Reboot; T1546: Event Triggered Execution; T1546.016: Installer Packages</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
UNK_SweetSpecter</td><td>-</td><td rowspan="3">Technology, Government, Education</td><td rowspan="3">USA</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>SugarGh0st RAT</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1083: File and Directory Discovery; T1570: Lateral Tool Transfer; T1071.001: Web Protocols; T1566.001: Spearphishing Attachment; T1566: Phishing; T1490: Inhibit System Recovery; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1574: Hijack Execution Flow; T1057: Process Discovery; T1105: Ingress Tool Transfer; T1204.002: Malicious File; T1204: User Execution</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Andariel (aka Silent Chollima, Stonefly, Plutonium, Onyx Sleet)</td><td>North Korea</td><td rowspan="3">Government Agencies, Military Organizations, Financial Services</td><td rowspan="3">South Korea</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage, Monetary Gains</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Dora RAT, Nestdoor</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1113: Screen Capture; T1056.001: Keylogging; T1584: Compromise Infrastructure; T1584.004: Server; T1566: Phishing; T1204: User Execution; T1055: Process Injection; T1027: Obfuscated Files or Information; T1049: System Network Connections: Discovery; T1082: System Information Discovery; T1057: Process Discovery; T1560: Archive Collected Data; T1005: Data from Local System; T1056: Input Capture; T1115: Clipboard Data; T1657: Financial Theft; T1053.005: Scheduled Task; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Sharp Dragon	China	Government	Africa and the Caribbean
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-0669	5.t Downloader	Fortra GoAnywhere MFT
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0043: Reconnaissance, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1036: Masquerading, T1012: Query Registry, T1018: Remote System Discovery, T1057: Process Discovery, T1082: System Information Discovery, T1083: File and Directory Discovery, T1001: Data Obfuscation, T1071: Application Layer Protocol, T1095: Non-Application Layer Protocol, T1105: Ingress Tool Transfer, T1573: Encrypted Channel, T1053: Scheduled Task/Job, T1588.001: Malware, T1588.002: Tool, T1588.006: Vulnerabilities, T1566: Phishing, T1203: Exploitation for Client Execution, T1566.001: Spearphishing Attachment, T1204: User Execution, T1204.002: Malicious File:			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Turla (aka Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23 , Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton , Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Secret Blizzard , Pensive Ursa)	Russia	NGOs	Philippines
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Tiny backdoor	Windows

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0010: Exfiltration; TA0005: Defense Evasion; TA0011: Command and Control; T1036: Masquerading, T1573: Encrypted Channel, T1053: Scheduled Task/Job, T1566: Phishing, T1566.001: Spearphishing Attachment, T1204: User Execution, T1204.002: Malicious File, T1059.001: PowerShell, T1059: Command and Scripting Interpreter, T1140: Deobfuscate/Decode Files or Information, T1127: Trusted Developer Utilities Proxy Execution, T1127.001: MSBuild, T1071: Application Layer Protocol, T1041: Exfiltration Over C2 Channel, T1027: Obfuscated Files or Information

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Moonstone Sleet (aka Storm-1789)	North Korea	Information technology, Education, and Defense	Worldwide
	MOTIVE		
	Information theft, Financial Gains		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	FakePenny Ransomware	-

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

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
UNC5537</td><td>-</td><td rowspan="2">All</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft, extortion</td><td rowspan="2">ASSOCIATED ATTACKS/RANSOMWARE</td><td rowspan="2">AFFECTED PRODUCTS</td></tr>
<tr><td>TARGETED CVEs</td></tr>
<tr><td>-</td><td>-</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0002: Execution; TA0040: Impact; TA0001: Initial Access; TA0009: Collection; TA0007: Discovery; TA0010:Exfiltration; TA0006: Credential Access; T1657: Financial Theft; T1619: Cloud Storage Object Discovery; T1586.003: Cloud Accounts; T1586: Compromise Accounts; T1530: Data from Cloud Storage; T1486: Data Encrypted for Impact; T1212: Exploitation for Credential Access; T1621: Multi-Factor Authentication Request Generation</td></tr>
</table>

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1598: Phishing for Information	T1598.002: Spearphishing Attachment
	T1592: Gather Victim Host Information	
	T1593: Search Open Websites/Domains	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1590: Gather Victim Network Information	T1590.004: Network Topology
	T1592: Gather Victim Host Information	T1592.002: Software
	T1590: Gather Victim Network Information	
	T1595: Active Scanning	T1595.003: Wordlist Scanning
	T1589: Gather Victim Identity Information	T1589.002: Email Addresses
TA0042: Resource Development	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.005: Link Target
	T1584: Compromise Infrastructure	T1584.004: Server
	T1585: Establish Accounts	T1585.001: Social Media Accounts
		T1585.003: Cloud Accounts
		T1585.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.002: DNS Server
		T1583.005: Botnet
		T1583.008: Malvertising
		T1583.004: Server
		T1583.006: Web Services
	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits
		T1588.002: Tool
		T1588.001: Malware
	T1586: Compromise Accounts	T1586.002: Email Accounts
TA0001: Initial Access	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1659: Content Injection	
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
TA0002: Execution	T1106: Native API	
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic
		T1059.007: JavaScript
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task

Tactic	Technique	Sub-technique
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1203: Exploitation for Client Execution	
	T1129: Shared Modules	
	T1569: System Services	T1569.002: Service Execution
	T1204: User Execution	T1204.002: Malicious File
		T1204.001: Malicious Link
	T1559: Inter-Process Communication	T1559.001: Component Object Model
		T1559.002: Dynamic Data Exchange
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1098: Account Manipulation	
	T1176: Browser Extensions	
	T1133: External Remote Services	
	T1136.002: Create Account	T1136.002: Domain Account
	T1505: Server Software Component	T1505.003: Web Shell
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1137: Office Application Startup	T1137.001: Office Template Macros
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1543.001: Launch Agent
		T1543.004: Launch Daemon
TA0004: Privilege Escalation	T1098: Account Manipulation	
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1543.001: Launch Agent
		T1543.004: Launch Daemon
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	
	T1134: Access Token Manipulation	
	T1068: Exploitation for Privilege Escalation	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
TA0005: Defense Evasion	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
	T1036: Masquerading	T1036.007: Double File Extension
		T1036.008: Masquerade File Type
		T1036.005: Match Legitimate Name or Location
	T1070: Indicator Removal	T1070.004: File Deletion
	T1218: System Binary Proxy Execution	T1218.011: Rundll32
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1027: Obfuscated Files or Information	T1027.009: Embedded Payloads

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
	T1562: Impair Defenses	
	T1221: Template Injection	
	T1202: Indirect Command Execution	
	T1480: Execution Guardrails	
	T1218: System Binary Proxy Execution	T1218.007: Msiexec
		T1218.005: Mshta
	T1070: Indicator Removal	T1070.006: Timestomp
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1600: Weaken Encryption	
	T1564: Hide Artifacts	T1564.002: Hidden Users
	T1622: Debugger Evasion	
	T1550: Use Alternate Authentication Material	
	T1014: Rootkit	
	T1134: Access Token Manipulation	
	T1220: XSL Script Processing	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
	T1110: Brute Force	
	T1552: Unsecured Credentials	
	T1539: Steal Web Session Cookie	
	T1040: Network Sniffing	
	T1056: Input Capture	T1056.001: Keylogging
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
		T1555.004: Windows Credential Manager
	T1558: Steal or Forge Kerberos Tickets	T1558.001: Golden Ticket
	T1606: Forge Web Credentials	
	T1557: Adversary-in-the-Middle	
TA0007: Discovery	T1018: Remote System Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1057: Process Discovery	
	T1046: Network Service Discovery	
	T1087: Account Discovery	
	T1016: System Network Configuration Discovery	
	T1482: Domain Trust Discovery	
	T1518: Software Discovery	
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1622: Debugger Evasion	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1007: System Service Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1040: Network Sniffing	
	T1518: Software Discovery	T1518.001: Security Software Discovery
TA0008: Lateral Movement	T1021: Remote Services	T1021.006: Windows Remote Management
		T1021.002: SMB/Windows Admin Shares
	T1570: Lateral Tool Transfer	
	T1210: Exploitation of Remote Services	
	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
TA0009: Collection	T1056: Input Capture	T1056.001: Keylogging
	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1074: Data Staged	T1074.001: Local Data Staging
	T1114: Email Collection	T1114.002: Remote Email Collection
		T1114.003: Email Forwarding Rule
	T1005: Data from Local System	
	T1119: Automated Collection	
	T1557: Adversary-in-the-Middle	
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.002: File Transfer Protocols
		T1071.004: DNS
	T1659: Content Injection	
	T1105: Ingress Tool Transfer	
	T1104: Multi-Stage Channels	
	T1572: Protocol Tunneling	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1568: Dynamic Resolution	
	T1008: Fallback Channels	
	T1571: Non-Standard Port	
TA0010: Exfiltration	T1030: Data Transfer Size Limits	
	T1041: Exfiltration Over C2 Channel	
	T1020: Automated Exfiltration	
	T1029: Scheduled Transfer	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
	T1048: Exfiltration Over Alternative Protocol	
TA0040: Impact	T1657: Financial Theft	
	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1498: Network Denial of Service	
	T1565: Data Manipulation	T1565.002: Transmitted Data Manipulation
	T1489: Service Stop	

Top 5 Takeaways

#1 In **May**, there were **eleven zero-day** vulnerabilities, with the '**Seven** Celebrity Vulnerabilities' taking center stage. These featured flaws such as **ZeroLogon**, **NoPac**, **PrintNightmare**, **Follina**, **Dirty COW** and, **Linguistic Lumberjack**.

#2 Over the course of the month, a variety of ransomware variants, including the well-known **Trinity** strain, have been actively targeting victims on a global scale. **ShrinkLocker**, another malicious program, has focused its attacks on a more specific geographical range, primarily targeting victims in **Mexico**, **Indonesia**, and **Jordan**. Furthermore, a recently discovered North Korean hacking group, **Moonstone Sleet**, has emerged as a threat, employing custom ransomware known as **FakePenny** to target companies for financial gain through data exfiltration and extortion.

#3 A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These malicious actors include the Goldoon botnet, the Ebury botnet, the SugarGh0st Remote Access Trojan (RAT), the Nestdoor RAT, the Nicecurl backdoor, the Tamecat backdoor, Metamorfo, the Grandoreiro Trojan, and the ScarletStealer and Sys01 infostealers.

#4 **Eleven** active adversaries were identified across multiple campaigns, targeting the following key industries: **defense**, **education**, **government**, **NGOs**, and **technology**.

#5 Multiple campaigns leveraging sophisticated, previously unseen malware and ransomware variants orchestrated a total of 38 attacks targeting the following nations: **Jamaica**, **Cuba**, **Mexico**, **Belize**, and **Poland**.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **24 significant vulnerabilities** and block the indicators related to the **11 active threat actors, 38 active malware,** and **233 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 **24 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 (MAY 2024)

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 have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

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
Goldoon	SHA256	66f21251d7f8c58316f149fec104723beb979a1215ad4e788d83f0ee6fd34696, 712d9abe8fbdff71642a4d377ef920d66338d73388bfee542f657f2e916e219c, d7367d41d19baa4f1022f8eb47f7ff1e13f583265c7c26ab96d5f716fa0d61ee, fdf6dae772f7003d0b7cdc55e047434dbd089e0dc7664a3fae8ccfd9d10ece8c, aa9e6006bce7d0b4554165dba76e67c4a44d98090c9e6ac9f3dca726f6e9adbf, fc44018b7432d9e6a1e98f723b0402101fa6e7483d098b10133aac142c0a4a0b, e7b78f16d0dfc91b4c7e8fd50fc31eba1eb22ec7030af9bf7c551b6019c79333, 0e6eb17664943756cab434af5d94fcd341f154cb36fc6f1ef5eb5cfdce68975f, 9af8720766c5f3978718c026c2263801b08634443c93bd67022c56c6ef531ef3, df71219ba6f5835309479b6e3eaca73b187f509b915420656bfe9a9cc32596c2, 48130a7c09a5c92e15b3fc0d2e1eb655e0bd8f759e01ba849f7734e32dbc2652, 8eb9c1eaecd0dcdd242e1bc8c62a1052915b627abe2de8ce147635fb7da3bfcc, b050a1ff0d205f392195179233493ff5b6f44adc93fe0dba1f78c4fe90ebcc46, ffd2d3888b6b1289e380fa040247db6a4fbd2555db3e01fadd2fe41a0fa2debc, 88cea61218bdeea94537b74c67873e75b8ada6d050a30d311569c3118d161c46, 115e15fbee077a9e126cc0eb349445df34cc9404245520c702fadc5f75b6f859, b10e47db989e29ace6c23ed15e29f313993f95e5e615711060881dfa84618071, 037331ab84a841b9d3cfb6f8797c1695e2dc0a2cdcc3f8f3c794dfaa50bcf0df, 5631980fab33525f4de1b47be606cd518403f54fa71b81186f02dbf7e9ed0004, 246142a5e3f3d3f84d8b38f98ff6897b03628e06e31016b8fafc9eb8c2b6201d, 3123a458a6346fd14c5bd7d41cda6c9c9bdabc786366a9ab3d5e7c00132ff835,

Attack Name	TYPE	VALUE
Goldoon	SHA256	45bf2c9c6628d87a3cb85ee78ae3e92a09949185e6da11c41e2df04a53bb1274, C81cfe4d3b98d0b28d3c3e7812beda005279bc6c67821b27571240eba440fa49
Nicecurl	MD5	d5a05212f5931d50bb024567a2873642, 347b273df245f5e1fcbef32f5b836f1d, 2f6bf8586ed0a87ef3d156124de32757, 13aa118181ac6a202f0a64c0c7a61ce7, c23663ebdfbc340457201dbec7469386, 853687659483d215309941dae391a68f
	Domain	drive-file-share[.]site, prism-west-candy[.]glitch[.]me
Tamecat	MD5	d7bf138d1aa2b70d6204a2f3c3bc72a7, 081419a484bbf99f278ce636d445b9d8, c3b9191f3a3c139ae886c0840709865e, dd2653a2543fa44eaeeff3ca82fe3513, 9c5337e0b1aef2657948fd5e82bdb4c3
	Domain	tnt200[.]mywire[.]org, accurate-sprout-porpoise[.]glitch[.]me
Cuttlefish	URL	hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/arm, hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/i386, hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/i386_i686, hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/i386_x64, hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/misp32, hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/misp64, hxxp://209[.]141[.]49[.]178/r/arm_sniff, hxxp://209[.]141[.]49[.]178/r/i386_i686_sniff, hxxp://209[.]141[.]49[.]178/r/i386_sniff, hxxp://209[.]141[.]49[.]178/r/i386_x64_sniff, hxxp://209[.]141[.]49[.]178/r/mips32_sniff, hxxp://209[.]141[.]49[.]178/r/mips64_sniff, hxxp://209[.]141[.]49[.]178/r/s[.]sh, hxxp://209[.]141[.]49[.]178/s, hxxps://107[.]189[.]28[.]251:443/rules, hxxps://198[.]98[.]56[.]93:443/rules, hxxps://198[.]98[.]56[.]93:443/rulesinit, hxxps://198[.]98[.]56[.]93:443/upload, hxxps://205[.]185[.]122[.]121/rules, hxxps://205[.]185[.]122[.]121/rulesinit, hxxps://205[.]185[.]122[.]121/upload, hxxps://kkthreas[.]com, hxxps://kkthreas[.]com/upload, hxxps://pp[.]kkthreas[.]com
	SHA256	07df37d8168e911b189bbe0912b4842fa1fe48d5264e99738ad3247f9c818478, 10a4edbbb852a1b01fc6fbf0aa1407bc8589432bddb2001ae62702f18d919e89,

Attack Name	TYPE	VALUE
Cuttlefish	SHA256	1168e97ccf61600536e93e9c371ee7671bae4198d4bf566550328b241ec52e89, 23c2e7ff2602e5f76b3f2c354761ef39966facb3b12ed05551816f482d4d5608, 2ed174523bd80a93b7d09940d375f9c0d71e1ce8ecffb2320e02a78f4b601408, 2f0911fb892d448910c36a37c9fbdec8c73ccfecc274854b1fa053fb1cc2369b, 3d9ee05c0841ad65547c0cc8516d092cff48dad5e7bbf97c99ddd44ee94a24bc, 44b769be0c2a807082a9bfd2f33fdc744552c5c7ca88a812ef4bd0393a50f132, 4aa23fbdc27d317c6e54481b6d884b962adf6e691a4731c859ddaf9af09822c6, 6295d5cb21c441066d2da81a76440bcac9bd5a7830fc9faea9668bd0b2015046, 70693211cd0b14a7463b39b2fa801ce1fdefc85c7f3e003772d1b4deeb78efde, 73cf20675639c18c04381b5efd7d628736d149734280988f55358e301c1d9bb8, 94812d391160e4fce821701b944cfd8f5fd9454b3cbb8e8974d1dc259310e500, 99d5cf32f8198e99c530be4f5e05487e280bacdb8ef26aaf38dc20e301aad75f, Eb7a7ab952080f66c82fe8350da131ce0d7766f203bd4d97b0798b4f59283a27
HijackLoader	SHA256	7a8db5d75ca30164236d2474a4719046a7814a4411cf703ffb702bf6319939d7, d95e82392d720911f7eb5d8856b8ccd2427e51645975cdf8081560c2f6967ffb, fcadcee5388fa2e6d4061c7621bf268cb3d156cb879314fa2f518d15f5fa2aa2, f37b158b3b3c6ef9f6fe08d0056915fc7e5a220d1dabb6a2b62364ae54dca0f1, e0a4f1c878f20e70143b358ddaa28242bac56be709b5702f3ad656341c54fb76, cf42af2bdcec387df84ba7f8467bbcdad9719df2c524b6c9b7fffa55cfdc8844, c215c0838b1f8081a11ff3050d12fcfe67f14442ed2e18398f0c26c47931df44, 9b15cb2782f953090caf76efe974c4ef8a5f28df3dbb3eff135d44306d80c29c, 56fd2541a36680249ec670d07a5682d2ef5a343d1feccbcf2c3da86bd546af85, 1fbf01b3cb97fda61a065891f03dca7ed9187a4c1d0e8c5f24ef0001884a54da

Attack Name	TYPE	VALUE
zEus	SHA256	aabfbef31ab073d99c01ecae697f66bbf6f14aa5d9c295c7a6a548879381fb24, c9687714cf799e5ce9083c9afa3e622c978136d339fc9c15e272b0df9cd7e21c, d9d394cc2a743c0147f7c536cbb11d6ea070f2618a12e7cc0b15816307808b8a, c2c8a7050b28d86143f4d606a6d245b53c588bc547a639094fce857962246da4, be9ea302bcfb52fbfdf006b2df8357388cd4c078059aabc5b5928676c3361e50, 9d3409852348caa65d28e674008dd6bb986eed4fb507957c7a8b73a41e00be70, b6e8b612e99c54dd98af1756f7c9b8a8c19e31ed9b2836878c2a5144563ff1b2, 8a2f6d5f6cf7d1a7534454e3c3007337b71d7da470e86f7636eb02d68b2db8cc, df6156fdbbcc7b6f8c9cb4c5c1b0018fc3f1e1ca7d949b5538ec27dc86d026a4, 5840f3e43a0c635be94b5fbf2e300d727545371b582361a52682b4a9e08bcebd, 51ede75315d858209f9aa60d791c097c18d38f44b9d050b555ff1f4de0ae672d, d1865d2aaf11e3f8bccefe9c4847510234f14aaa5378ce9e8e97553537cf2ca1, 9ba19d614af029c3c198b576ccdf1de87d80ac14b12103e8a15376229a2a7860, 6063c8285e13d10eabbe363e2ab0d8748bcd595b470698e0cffee31ba255a566, d1a18b436f947611914ced09e4465b49807cec4f3a62b0973c9017b6d82c9f70, 1cdd580176eeb4342a0333b50454da061e473358274e6e543df1411186c12042, ed59a797521db06abdf4c88dad7b1666e5978aaa6670a5952a55b7e11f7b790e, 2ceae724f0e96e2d8c47296dd1e73ac592e22ee3288eabf11c8d039c6d6d4f8b, 03983b56d8b1a6cc43109f6cd67a13666367595a2ea07766127cb1fe4d4bb1a5, 9940da9d02d29489c3e26d27feb15b6f4bbf49547b962592125441917c952f12, fbf967295dac00f1e9cb67e9a40b6729b003dd12cf022eb15d626df09716442d, 4e0a96ab28570936d095ac3910dcd239c7ceeb2b38a070468404584f8b902dd1, 20009fd157a898ad6d50fae6b8127056c5b1f50e31f90f01d2e6c13e6b4c38f8

Attack Name	TYPE	VALUE
RokRAT	MD5	b85a6b1eb7418aa5da108bc0df824fc0, 358122718ba11b3e8bb56340dbe94f51, 35441efd293d9c9fb4788a3f0b4f2e6b, 68386fa9933b2dc5711dffcee0748115, bd07b927bb765ccfc94fadbc912b0226, 6e5e5ec38454ecf94e723897a42450ea, 3114a3d092e269128f72cfd34812ddc8, bd98fe95107ed54df3c809d7925f2d2c
DiceLoader	IPv4: Port	193[.]124[.]24[.]51:443, 38[.]135[.]52[.]151:273
	MD5	bb0a503a83b1f9833c3d3d08784b78a8
Black Basta Rasnomware	File path	C:\Program Files\MonitorIT\GWT.ps1,C:\Users\All Users\{redacted}\GWT.ps1,C:\Users\Public\7z.dll,C:\Users\Public\7zG.exe,C:\Users\Public\Audio\7z.dll,C:\Users\Public\Audio\7zG.exe,C:\Users\Public\Audio\db_Usr.sql,C:\Users\Public\Audio\esx.zip,C:\Users\Public\Audio\hv2.ps1,C:\Users\Public\Audio\Jun.exe,C:\Users\Public\BitData.exe,C:\Users\Public\BitLogic.dll,C:\Users\Public\DataSoft.exe,C:\Users\Public\db_Usr.sql,C:\Users\Public\DigitalText.dll,C:\Users\Public\eucr.exe,C:\Users\Public\GeniusMesh.exe,C:\Users\Public\NetApp.exe,C:\Users\Public\socksps.ps1,C:\Users\Public\Thief.exe,C:\Windows\DS_c1.dll,\Device\Mup\{redacted}\C$\Users\Public\Music\DumpNParse86.exe,\Device\Mup\{redacted}\C$\Users\Public\Music\DumpNParse.exe,\Device\Mup\{redacted}\C$\Users\Public\Music\POSTDump.exe,\Device\Mup\{redacted}\C$\Users\Public\Music\PROCEXP.sys,*\instructions_read_me.txt
	Domain	airbusco[.]net, allcompanycenter[.]com, animalsfast[.]net, artspathgroupe[.]net, artspathgroup[.]net, artstrailman[.]com, artstrailreviews[.]com, audsystemecll[.]net, auuditoe[.]com, bluenetworking[.]net, brendonline[.]com, businesforhome[.]com, businessprofessionalllc[.]com, buyblocknow[.]com, buygreenstudio[.]com, caspercan[.]com, childrensdolls[.]com, clearsystemwo[.]net, cloudworldst[.]net, constrtionfirst[.]com, consulheartinc[.]com, currentbee[.]net, erihudeg[.]com, garbagemoval[.]com,

Attack Name	TYPE	VALUE
Black Basta Rasnomware	Domain	gartenlofti[.]com, getfnewsolutions[.]com, getfnewssolutions[.]com, investmendvisor[.]net, investmentgblog[.]net, investmentrealtyhp[.]net, investrealtydom[.]net, ionoslaba[.]com, jenshol[.]com, jessvisser[.]com, karmafisker[.]com, kekeoamigo[.]com, kolinileas[.]com, limitedtoday[.]com, magentoengineers[.]com, maluisepaul[.]com, masterunix[.]net, modernbeem[.]net, monitorsystem[.]net, monitor-websystem[.]net, myfinancialexperts[.]com, mytrailinvest[.]net, nebraska-lawyers[.]com, oneblackwood[.]com, onedogsclub[.]com, ontexcare[.]com, otxcarecosmetics[.]com, otxcosmeticscare[.]com, prettyanimals[.]net, protectionek[.]com, rasapool[.]net, realbumblebee[.]net, recentbeelive[.]com, recentbee[.]net, reelsysmoona[.]net, securecloudmanage[.]com, seohomee[.]com, septcntr[.]com, simorten[.]com, softradar[.]net, specialdrills[.]com, startupbizaud[.]net, startupbusiness24[.]net, startupbuss[.]com, startupmartec[.]net,

Attack Name	TYPE	VALUE
Black Basta Rasnomware	Domain	startuptechnologyw[.]net, steamteamdev[.]net, stockinvestlab[.]net, taskthebox[.]net, technologgies[.]com, thesmartcloudusa[.]com, thetrailbig[.]net, tomlawcenter[.]com, topglobaltv[.]com, trackgroup[.]net, trailcocompany[.]com, trailcosolutions[.]com, trailgroupl[.]net, trailshop[.]net, treeauwin[.]net, unitedfrom[.]com, unougn[.]com, usaglobalnews[.]com, wardeli[.]com, webnubee[.]com, welausystem[.]net, wellsystemte[.]net, wipresolutions[.]com, withclier[.]com
	IPv4	104[.]21[.]26[.]145, 104[.]21[.]40[.]72, 107[.]189[.]30[.]69, 116[.]203[.]186[.]178, 151[.]101[.]130[.]159, 155[.]138[.]246[.]122, 183[.]181[.]86[.]147, 185[.]219[.]221[.]136, 185[.]220[.]100[.]240, 185[.]220[.]101[.]149, 185[.]7[.]214[.]79, 188[.]130[.]137[.]181, 188[.]130[.]218[.]39, 207[.]126[.]152[.]242, 34[.]120[.]190[.]48, 34[.]149[.]120[.]3, 34[.]149[.]36[.]179, 34[.]160[.]17[.]71, 34[.]160[.]81[.]203, 34[.]250[.]161[.]149, 34[.]251[.]163[.]236,

Attack Name	TYPE	VALUE
Black Basta Rasnomware	IPv4	35[.]190[.]31[.]54, 35[.]212[.]86[.]55, 35[.]227[.]194[.]51, 35[.]244[.]153[.]44, 46[.]161[.]27[.]151, 46[.]8[.]10[.]134, 46[.]8[.]16[.]77, 5[.]183[.]130[.]92, 5[.]78[.]115[.]67, 64[.]176[.]219[.]106, 66[.]249[.]66[.]18, 72[.]14[.]196[.]192, 72[.]14[.]196[.]2, 72[.]14[.]196[.]226, 72[.]14[.]196[.]50, 80[.]239[.]207[.]200, 83[.]243[.]40[.]10, 88[.]198[.]198[.]90, 95[.]181[.]173[.]227
	SHA256	0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298, 034b5fe047920b2ae9493451623633b14a85176f5eea0c7aadc110ea1730ee79, 0554eb2ffa3582b000d558b6950ec60e876f1259c41acff2eac47ab78a53e94a, 05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431, 07117c02a09410f47a326b52c7f17407e63ba5e6ff97277446efc75b862d2799, 0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e, 17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90, 17879ed48c2a2e324d4f5175112f51b75f4a8ab100b8833c82e6ddb7cd817f20, 1c1b2d7f790750d60a14bd661dae5c5565f00c6ca7d03d062adcecda807e1779, 3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35, 3337a7a9ccdd06acdd6e3cf4af40d871172d0a0e96fc48787b574ac93689622a, 350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd, 360c9c8f0a62010d455f35588ef27817ad35c715a5f291e43449ce6cb1986b98,

Attack Name	TYPE	VALUE
Black Basta Rasnomware	SHA256	37a5cd265f7f555f2fe320a68d70553b7aa9601981212921d1ac2c114e662004, 39939eacfbc20a2607064994497e3e886c90cd97b25926478434f46c95bd8ead, 3a8fc07cadc08eeb8be342452636a754158403c3d4ebff379a4ae66f8298d9a6, 3c50f6369f0938f42d47db29a1f398e754acb2a8d96fd4b366246ac2ccbe250a, 3c65da7f7bfdaf9acc6445abbedd9c4e927d37bb9e3629f34afc338058680407, 42f05f5d4a2617b7ae0bc601dd6c053bf974f9a337a8fcc51f9338b108811b78, 462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7, 4ac69411ed124da06ad66ee8bfbcea2f593b5b199a2c38496e1ee24f9d04f34a, 51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e, 58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd, 5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43, 5b2178c7a0fd69ab00cef041f446e04098bbb397946eda3f6755f9d94d53c221, 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa, 62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087, 69192821f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944, 723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224, 7ad4324ea241782ea859af12094f89f9a182236542627e95b6416c8fb9757c59, 808c96cb90b7de7792a827c6946ff48123802959635a23bf9d98478ae6a259f9, 819cb9bcf62be7666db5666a693524070b0df589c58309b067191b30480b0c3a, 8501e14ee6ee142122746333b936c9ab0fc541328f37b5612b6804e6cdc2c2c6, 86a4dd6be867846b251460d2a0874e6413589878d27f2c4482b54cec134cc737, 882019d1024778e13841db975d5e60aaae1482fcf86ba669e819a68ce980d7d3,

Attack Name	TYPE	VALUE
Black Basta Rasnomware	SHA256	88c8b472108e0d79d16a1634499c1b45048a10a38ee799054414613cc9dccccc, 8C68B2A794BA3D148CAE91BDF9C8D357289752A94118B5558418A36D95A5A45F, 90ba27750a04d1308115fa6a90f36503398a8f528c974c5adc07ae8a6cd630e7, 96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be, 9a55f55886285eef7ffabdd55c0232d1458175b1d868c03d3e304ce7d98980bc, a7b36482ba5bca7a143a795074c432ed627d6afa5bc64de97fa660faa852f1a6, acb60f0dd19a9a26aaaefd3326db8c28f546b6b0182ed2dcc23170bcb0af6d8f, ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e, b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9, b6a4f4097367d9c124f51154d8750ea036a812d5badde0baf9c5f183bb53dd24, c26a5cb62a78c467cc6b6867c7093fbb7b1a96d92121d4d6c3f0557ef9c881e0, d15bfbc181aac8ce9faa05c2063ef4695c09b718596f43edc81ca02ef03110d1, d3683beca3a40574e5fd68d30451137e4a8bbaca8c428ebb781d565d6a70385e, D503090431fdd99c9df3451d9b73c5737c79eda6eb80c148b8dc71e84623401f, d73f6e240766ddd6c3c16eff8db50794ab8ab95c6a616d4ab2bc96780f13464d, df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415, e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757, f039eaaced72618eaba699d2985f9e10d252ac5fe85d609c217b45bc8c3614f4, f21240e0bf9f0a391d514e34d4fa24ecb997d939379d2260ebce7c693e55f061, fafaff3d665b26b5c057e64b4238980589deb0dff0501497ac50be1bc91b3e08, Fff35c2da67eef6f1a10c585b427ac32e7f06f4e4460542207abcd62264e435f

Attack Name	TYPE	VALUE
Black Basta Rasnomware	MD5	2642ec377c0cee3235571832cb472870, 4c897334e6391e7a2fa3cbcbf773d5a4, B3fe23dd4701ed00d79c03043b0b952e
Trinity Ransomware	MD5	949c438e4ed541877dce02b38bf593ad
	SHA1	4c58d2d624d9bdf6b14a6f8563788785074947a7
	SHA256	36696ba25bdc8df0612b638430a70e5ff6c5f9e75517ad401727be03b26d8ec4
Cobalt Strike Beacon	Domain	limitedtoday[.]com, thetrailbig[.]net
Ebury Botnet	IPv4	135[.]181[.]148[.]230, 141[.]164[.]52[.]243, 141[.]255[.]166[.]187, 146[.]70[.]124[.]102, 185[.]145[.]245[.]167, 185[.]59[.]103[.]8, 195[.]123[.]225[.]83, 213[.]232[.]235[.]104, 45[.]59[.]120[.]146
	Domain	a1hcy1xendd[.]net, a1k8h2xendd[.]info, a1t9y1xendd[.]info, a1z1h2xendd[.]biz, abo0u6ach9k3w[.]net, b2z6m9k1zaf3v[.]net, b8dfs5ecw9p3o[.]info, c0dbq5vcj9o3e[.]info, c1b1jfi2pdi8w1f[.]net, c1jczbhcpdi8w1f[.]biz, c1m8k5q0hfi8w1f[.]net, c1v9j2pahfi8w1f[.]biz, c1v9l8s6yei8w1f[.]info, c9xfb8u1cad3m[.]net, checklicence[.]net, f2y1j8v1saa3t[.]biz, f8wda5yck9i3h[.]net, fas1k9i1jap3u[.]biz, h0nct5rca9y3f[.]biz, h9g0q8a1hat3s[.]net, hdm5o8e1tas3n[.]net, idkff7m1lac3g[.]biz, k2qai2yeodm[.]net, k2rdz1yeodm[.]biz, k2t6i2yeodm[.]biz, k2zbz1yeodm[.]info, larfj7g1vaz3y[.]net,

Attack Name	TYPE	VALUE
Ebury Botnet	Domain	m2d4berdzej8x1o[.]info, m2kcjcj2ifj8x1o[.]biz, m2lfk2jfqdj8x1o[.]info, m2w9c4qaqdj8x1o[.]net, m7lea5yck9i3l[.]biz, mae2d2tejdt[.]info, maefu1tejdt[.]net, mag8u1tejdt[.]biz, map9u1tejdt[.]net, maved2tejdt[.]info, o5dec1berdn[.]info, o5e4l2berdn[.]net, o5lcl2berdn[.]biz, o5o8c1berdn[.]net, o5tac1berdn[.]biz, o8rad5ccx9f3r[.]net, o9f3v8r1oaj3p[.]biz, oafcffg8uee8s1v[.]net, oah5w1w4uee8s1v[.]biz, oap3p6f5lde8s1v[.]biz, oaxey7m0lde8s1v[.]info, oay4vbx7dfe8s1v[.]net, odrbz8i1jap3e[.]biz, op3f1libgh[.]biz, pbarsec[.]com, q5ncv0dekcm8a1p[.]biz, q5o2uad1cem8a1p[.]net, q5w0f4n5lfm8a1p[.]info, q5w0g7cbcem8a1p[.]biz, q5y6vdf7tdm8a1p[.]info, qimpj6kkofzf[.]biz, raj2p8z1aae3b[.]net, tav4h8n1baw3r[.]info, u2s0k8d1ial3r[.]info, uajdm8w1kax3j[.]info, ubjcl5ucn9g3m[.]info, v2a7q8a1hat3u[.]biz, x7sbu5hcg9b3f[.]net, xdc1h8n1baw3m[.]info, y2fad8b1gak3f[.]net, z9w8l8k1zaf3g[.]info, zbqaf5zcv9s3x[.]biz, zdm3u9x1fag3i[.]info, ibz[.]so, iptables-multi,

Attack Name	TYPE	VALUE
Ebury Botnet	Domain	iptables-multi-1[.]4[.]7, libcurl[.]so[.]4[.]4[.]0, libcurl[.]so[.]4[.]5[.]0, libcurl[.]so[.]4[.]6[.]0, libkeystats[.]so, libkeyutils[.]so, libkeyutils[.]so[.]1[.]5, Libllz564, libns2[.]so, libns5[.]so, libpw3[.]so, libpw5[.]so, librwctl[.]so, libsbr[.]so, libslr[.]so, libstz[.]so, mod_auth_basic[.]so, mod_authn_file[.]so, mod_authz_host[.]so, mod_authz_user[.]so, mod_dir[.]so, mod_env[.]so, nf_conntrack6[.]ko
	File path	/bin/hostname, /bin/sync, /dev/event-E4LgEFWIcy, /dev/event/loop0, /dev/stats-MxPAxNpy3x, /proc/udevd, /proc/ulog, /run/systemd/journal/dlog, /run/systemd/journal-YAjXO8luqOa, /run/systemd/log, /run/systemd/log-90zMvYX7uL, /run/systemd/log-wuO3nuFBHN, /sbin/auditd, /sbin/rsyslogd, /sbin/udevd, /tmp/dbus-0m9eDQpdXZ, /tmp/dbus-9XZXkmdfpN, /tmp/dbus-kZ8VEtJDOJ, /tmp/dbus-luzG4UqDt8, /tmp/dbus-n3UUkeqEZG, /tmp/dbus-vBWUDhHCHp, /tmp/dbus-VdyGBaqZws,

Attack Name	TYPE	VALUE
Ebury Botnet	File Path	/tmp/dbus-Xrga2cOewg, /tmp/dbus-ZP7tFO4xsL, /usr/lib/systemd/systemd-udevd, /usr/sbin/acpid, /usr/sbin/anacron, /usr/sbin/arpd, /usr/sbin/atd, /usr/sbin/crond
	SHA1	0004b44d110ad9bc48864da3aea9d80edfceed3f, 013647E5AD347539EEF6C5933B16AD01B1806C3C, 035327b42f6e910b652bbdde5d9c270cfbaa9669, 03592b8147e2c84233da47f6e957acd192b3796a, 04FF6202534A394586D826B320645AEC24CE7AA5, 051a89a7a335062829a8e938b8d4e3e2b532f6ff, 070F85BF02AD3FB0978785B3272D7B08F5C47A1A, 09c8af3be4327c83d4a7124a678bbc81e12a1de4, 0B91C3C2627F9948B8F3446822F99FAF88081267, 0daa51519797cefedd52864be0da7fa1a93ca30b, 0eb1108a9d2c9fe1af4f031c84e30dcb43610302, 10c6ce8ee3e5a7cb5eccf3dffd8f580e4fb49089, 10F94157365E6A1BBB101B3222EE3C3C675B9829, 12666F2FBEFC55F1DDB4BA86B5D85DB733889162, 12EA4595C6F38E60C23F09B2F08D78BA6EB0C1B3, 149cf77d2c6db226e172390a9b80bc949149e1dc, 15560B44286122FA0679C6C2368817CE2DC747E6, 16EE09926A2109262686D58974079ADC25E31AA1, 17c40a5858a960afd19cc02e07d3a5e47b2ab97a, 1918E40580291D0299A78DDFB9123923F832CEB3, 1972616a731c9e8a3dbda8ece1072bd16c44aa35, 1a9aff1c382a3b139b33eeccae954c2d65b64b90, 1d3aafce8cd33cf51b70558f33ec93c431a982ef, 1dd7a18125353d426b5314c4ba04d60674ffa837, 20467521bfd58e9ed388ce83467d73e8fd0293a7, 20599D89E4F648CF0F6EB46DEE67DB63984A8C36, 22BB2E0D1E1B0B009464E2919A381C4951D7D90D, 24e3ebc0c5a28ba433dfa69c169a8dd90e05c429, 25a819d658d02548b2e5bdb52d2002df2f65b03a, 267d010201c9ff53f8dc3fb0a48145dc49f9de1e, 27ed035556abeeb98bc305930403a977b3cc2909, 2DBF91347FA987E6199DAE5141641D04D0C963FF, 2e571993e30742ee04500fbe4a40ee1b14fa64d7, 2f382e31f9ef3d418d31653ee124c0831b6c2273, 2fc132440bafdbc72f4d4e8dcb2563cc0a6e096b, 3137DCA3F6FBD566F4ED2F49076A63D84869E13C, 32BB38D7D6B03DB4779E7A7183E7FA42DFBAFFC2,

Attack Name	TYPE	VALUE
Ebury Botnet	SHA1	3988D1A743E83D532130BC8090A7BC7001FE1BB0, 39ec9e03edb25f1c316822605fe4df7a7b1ad94a, 3c5ec2ab2c34ab57cba69bb2dee70c980f26b1bf, 42123cbf9d51fb3dea312290920b57bd5646cefb, 429A81BBD18A35C3C4D1DCB8BC76F5A7D9724A79, 44B04CFC095F93D17B1BD4F8820C16843FCBAC3E, 44b340e90edba5b9f8cf7c2c01cb4d45dd25189e, 471ee431030332dd636b8af24a428556ee72df37, 4A7303DD8E7BBBF063463B3852245ABDD343F5B6, 4d12f98fd49e58e0635c6adce292cc56a31da2a2, 4f40bb464526964ba49ed3a3b2b2b74491ea89a4, 4F92498FB8C1BFED97F18CFB7B36AF899F70F582, 5196a8a034611aaa112232767aafd74b8ef71279, 535C5588ED2EF9A4E960882C23E3104E81F2C079, 53829463A7DE8C4BACE97B1F6925728F3421DF53, 575bb6e681b5f1e1b774fee0fa5c4fe538308814, 580E6075C65D867667D507E2B00C8EEF79C907A1, 58f185c3fe9ce0fb7cac9e433fb881effad31421, 59F238DA1FD822AAD6FA7DF78D823854EAF8762E, 5b87807b4a1796cfb1843df03b3dca7b17995d20, 5bdf483279a4a816ed4f8a235e799d5068d14f64, 5c796dc566647dd0db74d5934e768f4dfafec0e5, 5d3ec6c11c6b5e241df1cc19aa16d50652d6fac0, 615c6b022b0fac1ff55c25b0b16eb734aed02734, 6180d8c1c6967d15a0abb0895103ccc817e43362, 62c4b65e0c4f52c744b498b555c20f0e76363147, 6369AD38D39562DD9D6D3E2612496A5357FFC09B, 67C1905EF4D0422DBDFAC41DC80F9C4D5C69E288, 6BEE8F88F3F145170CEF58D9F790DDD99CDFA547, 6FF132E50EFA5ABF534A005CB58C9C5B5FC39BEC, 71CA9B7C418264C2C856D47483666D123861D476, 72048DEABE7F37BBECBFDA1570E1AB6B366B72BD, 7248e6eada8c70e7a468c0b6df2b50cf8c562bc9, 7314eadbdf18da424c4d8510afcc9fe5fcb56b39, 74aa801c89d07fa5a9692f8b41cb8dd07e77e407, 74cd5ae9f6bbdf27b4eaf45c4a22c6aae07345a2, 75E8A197B6A9A7903CA43782BDD77CD9611FEFE0, 787A93F86E7F5FCF922E996B577DF532270C7184, 78c63e9111a6701a8308ad7db193c6abb17c65c4, 7adb38bf14e6bf0d5b24fa3f3c9abed78c061ad1, 858c612fe020fd5089a05a3ec24a6577cbeaf7eb, 899b860ef9d23095edb6b941866ea841d64d1b26, 8daad0a043237c5e3c760133754528b97efad459, 8f75993437c7983ac35759fe9c5245295d411d35,

Attack Name	TYPE	VALUE
Ebury Botnet	SHA1	9018377c0190392cc95631170efb7d688c4fd393, 907822012D6A970D676B634903F099587ED9C335, 9209D757770AAFCA0B84B9F63B8769DF8CAC3F1A, 94532111459E024BCB7E2025A6C145876A46F829, 947EEE633E9347F72625FB652F94488A4B2B37F0, 9569A8411477305FACA78E1C944D479EFA028DFB, 96FD9B3064F04EE3063B2B103F856BB729B58749, 98cdbf1e0d202f5948552cebaa9f0315b7a3731d, 98FBD545B5C1B1FE185730BA9B1CD4BEBFAE4476, 9bb6a2157c6a3df16c8d2ad107f957153cba4236, 9e2af0910676ec2d92a1cad1ab89029bc036f599, a0f18b5ee2d347961b7109a22ea06cca962693d2, a51b1835abee79959e1f8e9293a9dcd8d8e18977, a53a30f8cdf116de1b41224763c243dae16417e4, a559ee8c2662ee8f3c73428eaf07d4359958cae1, A64D6C7444FC2404A589ED7F8527E698682A3E68, a7b8d06e2c0124e6a0f9021c911b36166a8b62c5, AA0EC27C26E5484B4EB23D8424B2412221D5C7FC, ac96adbe1b4e73c95c28d87fa46dcf55d4f8eea2, AD350D7DA4BF1F7080026B683F93401CD735E974, adfcd3e591330b8d84ab2ab1f7814d36e7b7e89f, b58725399531d38ca11d8651213b4483130c98e2, b8508fc2090ddee19a19659ea794f60f0c2c23ff, bbce62fb1fc8bbed9b40cfb998822c266b95d148, bCC3B83CFADBD58256FC41AF9F0BFF50AC1F148B, bd867907a5059ab1850918d24b4b9bbe33c16b76, bf1466936e3bd882b47210c12bf06cb63f7624c0, c4c28d0372aee7001c44a1659097c948df91985d, CD9A5B823906CC620B28D69DBDB11BD9FE6B3E03, CFB48909B978E91CFC6FFCAF2E4B04F27F503B34, D392022D8B72BCDDB849A94829C87731874E94AC, D39959356283DB4B3184BDB15E890E74CF1EA65C, D3D6567862B4B7811BEA76BE117E901B2B6B8399, d4eeada3d10e76a5755c6913267135a925e195c6, d552cbadee27423772a37c59cb830703b757f35e, D8647E825EFE74BF1726C0C494E3C2588FFF2262, D901D65F7A7A49296A501420F6D32BBF968F5BDE, dd7846b3ec2e88083cae353c02c559e79124a745, DDAE9417470F832DB550EFB716B5BAEAAAA35372, ddb9a74cd91217cfcf8d4ecb77ae2ae11b707cd7, DFAECF7EBFC169CDF923AF421EDD537CCE536A64, e14da493d70ea4dd43e772117a61f9dbcff2c41c, e2a204636bda486c43d7929880eba6cb8e9de068, E39667AA137E315BC26EAEF791CCAB52938FD809, E7DEBD6E453192AD8376DB5BAB03ED0D87566591, E8d392ae654f62c6d44c00da517f6f4f33fe7fed,

Attack Name	TYPE	VALUE
Ebury Botnet	SHA1	e8d3c369a231552081b14076cf3eaa8901e6a1cd, eb352686d1050b4ab289fe8f5b78f39e9c85fb55, ebc45dd1723178f50b6d6f1abfb0b5a728c01968, EC4941BDD9FFB241968FD59A28B70BCE288ED261, ED5662F3CF80B8108D2172FBCA6119E403205EAA, EDD2DE0FAFE84EA51029FFDE38ACBB5918108DF5, ee679661829405d4a57dbea7f39efeb526681a7f, f1ada064941f77929c49c8d773cbad9c15eba322, f634f305a655b06f2647b82b58f7d3920546ac89, fa6707c7ef12ce9b0f7152ca300ebb2bc026ce0b, fc39009542c62a93d472c32891b3811a4900628a, FD6709AF6A8DC384B101A8E9ED36C1092533C404 Fdf91a8c0ff72c9d02467881b7f3c44a8a3c707a
LunarLoader	SHA1	795c4127d42fe8dfaf4510b406b52ba5bede8d3a, 19d86cf2ed82eae23e019706fae8dafc60552e85, 00006b30806f915911349d82beeb1aeb9025adb4, 94a4ce9c75bc847e7be59b96c4133d677d909414, f09e36553e48ebd42e60d9b25a390c0f57ff8de0, 2ed792e39f7d56de52bdf4aed96afc898478bfdf
LunarWeb	SHA1	754fb657156643fd09a68ec9fc124528578cab0c, 4c84110f1b10df5fdd612759e210e44b0f0505ef, 5d3975e57bdcb630a00febe5d405eefb6d119d86, 5ef771afc96c24371d367448627609cfacb34a57, 512e4fa7d6119270ff44a3b2a2359ee8825392ef
	IPv4	45[.]33[.]24[.]145, 45[.]79[.]93[.]87, 65[.]109[.]179[.]67, 74[.]50[.]80[.]35, 82[.]165[.]158[.]86, 82[.]223[.]55[.]220, 139[.]162[.]23[.]113, 158[.]220[.]102[.]80, 161[.]97[.]74[.]237, 176[.]57[.]150[.]252, 212[.]57[.]35[.]174, 212[.]57[.]35[.]176
LunarMail	File path	%LOCALAPPDATA%\Microsoft\Outlook\outlk.share
	SHA1	fcae66f6d95c78dc829688cc0f4c39bb5a57828b, 67c6aec8d129e610378ef52f8bf934886587932f, 9cec3972fa35c88de87bd66950e18b3e0a6df77c, 2ed792e39f7d56de52bdf4aed96afc898478bfdf, f09e36553e48ebd42e60d9b25a390c0f57ff8de0

Attack Name	TYPE	VALUE
Gomir	SHA256	30584f13c0a9d0c86562c803de350432d5a0607a06b24481ad4d92cdf7288213
Troll Stealer	SHA256	d7f3ecd8939ae8b170b641448ff12ade2163baad05ca6595547f8794b5ad013b, 36ea1b317b46c55ed01dd860131a7f6a216de71958520d7d558711e13693c9dc, 8e45daace21f135b54c515dbd5cf6e0bd28ae2515b9d724ad2d01a4bf10f93bd, 6c2a8e2bbe4ebf1fb6967a34211281959484032af1d620cbab390e89f739c339, 47d084e54d15d5d313f09f5b5fcdea0c9273dcddd9a564e154e222343f697822, 8a80b6bd452547650b3e61b2cc301d525de139a740aac9b0da2150ffac986be4, 380ec7396cc67cf1134f8e8cda906b67c70aa5c818273b1db758f0757b955d81, ff945b3565f63cef7bb214a93c623688759ee2805a8c574f00237660b1c4d3fd, cc7a123d08a3558370a32427c8a5d15a4be98fb1b754349d1e0e48f0f4cb6bfc, 8898b6b3e2b7551edcceffbef2557b99bdf4d99533411cc90390eeb278d11ac8, ecab00f86a6c3adb5f4d5b16da56e16f8e742adfb82235c505d3976c06c74e20, d05c50067bd88dae4389e96d7e88b589027f75427104fdb46f8608bbcf89edb4, a98c017d1b9a18195411d22b44dbe65d5f4a9e181c81ea2168794950dc4cbd3c, 831f27eb18caf672d43a5a80590df130b0d3d9e7d08e333b0f710b95f2cde0e0, bc4c1c869a03045e0b594a258ec3801369b0dcabac193e90f0a684900e9a582d, 5068ead78c226893df638a188fbe7222b99618b7889759e0725d85497f533e98
GoBear	SHA256	7bd723b5e4f7b3c645ac04e763dfc913060eaf6e136eecc4ee0653ad2056f3a0
SugarGh0st	Domain	account.gommask[.]online
	IPv4	43[.]242[.]203[.]115
	SHA256	351418c41f1abf7b4c8692188069fb38f1f5ce13bdea2ea7a59918cc52ee4719, 1e2413dcd36060144917e72bb862ec890ad81f2b51eaaeacee6418c2379d5704,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	696533c07a78b8f4b3231f0a22502c1c85fefcf798c3272cdc2b05a4e8b86727, 8b9e0e9ac7c8d61252f2edd6104197ad2e2476fda86583aeef7f5994bcf85b08, ee5982a71268c84a5c062095ce135780b8c2ffb1f266c2799173fb0f7bfdd33e, fbf1038e32d41fa28286e6726f7e39c518cee67edd688615bccfe61a74dcaa86
DarkGate	URL	hxxp[:]//afarm[.]net/uvz2q, hxxp[:]//affixio[.]com/emh0c, hxxp[:]//affiliatebash[.]com/myu0f, hxxp[:]//afcmanager[.]net/jxk6m, hxxp[:]//adventsales[.]co[.]uk/iuw8a, hxxp[:]//amikamobile[.]com/ayu4d, hxxp[:]//adztrk[.]com/ixi7r, hxxp[:]//aerospaceavenue[.]com/cnz8g, hxxp[:]//amishwoods[.]com/jwa4v, hxxp[:]//smbeckwithlaw[.]com/1[.]zip, hxxp[:]//kindupdates[.]com
Qakbot	SHA256	b3781927bcf7932c336630f636f47cbdba47e2f5aa94039f87fbb15797455535, 767bfbc1a25997de2d6203b7ec79afe012f1049eda612efb5c51e4da68972b58, 8b08e73ad310f5e7e06c78b453ff8bc00851d0b9f86fa00c64a3dd42ec1632ce, 71c099ed2857f660b8431eb79cdd49300428cbf97c2cb6f98efa6e1cf30d1414, 9e2864977d0e2bf7e8def198db7d3022188cd764519c2f385797a7ca394c2283, e366c18e2f2389d4e90386f01876174074019a021b6eacfceb187aaa53560078, f3e3d35760f655af5a57029b73c2cc2f42d09de1a694b2eb22366a3e6c49a068, de29782abe28a8fcdc95dd4b031e86653c32d1497e36cdf2f6fbb9cbc48f40e4, b991ef2d58b3246bf5f313e2be71ea961fae1376ec88435173f7fb15a48b6fe2, 60b290310f67adb0ae186b4b938ca466a6b55653b2519261fa425127f5500a1f, 100805c582954d2c13b233229c9f7fe3f4b911ef16dad7aaec5b4616405f7d38, 6787a0800be339b8b6db63fe4b0cbbd68b69c736aecd45c4a85b2f02eb3e57d3,

Attack Name	TYPE	VALUE
Qakbot	SHA256	798e44b2af6329ac38f144d816096b72889009f44c9d74aefa36c11dbdc5522a, 5cfbe018afa45304fb2d7775f635101ee4226ba594bb30cc0e5c017fd1d30da1, f1bbcc5c678d174d858ae089f4494e3ea8bcfc418098d61804a15e437f08aff7, 37d5f69a7b2718386a0c65fbfe65a16c0392428ac4915c41ccd32d7af7c373e8, c14b93f3949b9cc4ba3163a23b5cfeb1d4bea17db91703c3cdccccbb57d2058, d2e6d3c058dd54b354e701633be148e14d96f40df7e7d3fe8778db69bbce0529, c6482951d520c93684161390507d695b8d6a90d8e1ac14e01626adf1989ab731, 8d8e136551e5ae8b82d3a25147f4291c1f0cf6b82dd3a8df89e6f866247ef83a, b7a00ad06ccceff1cf5fe5c7fed8e0d43b456662721ec668f91681196a1cb3ba, b66b7bfcdc8d6fb55fe600c20302405a22e1e7b60a0bb1e48a0ccf4e5daf8e50, fd1e4ecef5aed84a1e9cf04271111c5041d6c50c850b75959932927cf875293a, dec2d24131b54bda92b59c49acc410da4af20a730b3113c0472479ac168e3a81, e49e5a9c12fa92485943517ecba2721387a7ec8942ef92ba02b4c2e35a9dd84d, 2d7a014145e89956cd0ed6997e7efd12e5570864a12359a11e70a30c724d8b0a, 146a74dfa467bb299b8e6719526f224e7643fb4c9da53d8adc1149471184f9d0, 66d36ffbcdd8919b6527110a03fe917c1e47dac123778945305b3baa395631f0, 52321edc0c5a3fcb824d591c730e7783194ec5e1c0f617b40ffe760a876924eb, e4c669aaa5e441eb95dc6baed3e93cc4bd018dd1a03013719283f12cf4322ed8, 06d60d2e4f630514526ac63ab10360a1405899f4dac32888d231f5fcf9abb2d1, a6155313935b355ed814c0df0f423e6a662ea4259dcdcc0ffbcc1e9dad715b6f, 07dc705da27544ca4d232515c665dff2bbbf6b0ab49fd07c602e20d6a512b4af, f93b8b6aedc9c13590c7eb2247c920e376ab33354e9ca4003834ab9f043006f0,

Attack Name	TYPE	VALUE
Qakbot	SHA256	d832c8f49706ff93871a111be8fb280caedbad5b368f801dd720c7786f872e86, 1aa8e55ceec841c7ca088da6fc3e018ebc265bfd3ce85cae0339106143800186, af6a9b7e7aefeb903c76417ed2b8399b73657440ad5f8b48a25cfe5e97ff868f, 59559e97962e40a15adb2237c4d01cfead03623aff1725616caeaa5a8d273a35, f407120d5118eb9f93c290461e19bfb20a456a85919c80cc47b4229716131732, f1cd2d2c9e774735e5e80040a279ca86da78bc901ecc6b92096a5a019a6d04e3, b8a97d0b236d84fd7f9406b9d341add7cb5ec4ed0f4267a2ff5c8eac21503dcc, Ac256fdb6fc028a9c0cfe930535a23842d3e5c50dc720a4186750ae289245e63
Metamorfo	SHA256	71908b731b9bd2c6e5430f35eea2ded9041c272d61dd676a4456201e31e07444, 8c27321c5bc40131cf7873a52907433ae736e8e2801ec8aadc350c17852b55af, c3d85c05121900c93f667ff65073ef331d37e65eea9bd4c60252dba9764056a3, 690ada1acafbbffbb68f52e981ef1d98cbb781627dfa7b3d5653aba2feaf5d79
	SHA1	45f8c91f0299012a8dcb40d9a2fb5ce7962b887a, a9e9df6762418bbed030e825099282da59278db0, 2bd4acea5c3bf107cc6615af65d1617c847814cc, 4b5b7cf403ac7d6e3dd787104e3e6bd088743815
Grandoreiro	SHA256	97f3c0beef87b993be321b5af3bf748cc8e003e6e90cf5febf69dfd81e85f58, afd53240a591daf50f556ca952278cf098dbc5b6c2b16c3e46ab5a0b167afb40, f8f2c7020b2d38c806b5911acb373578cbd69612cbe7f21f172550f4b5d02fdb, 10b498562aef754156e2b540754bf1ccf9a9cb62c732bf9b661746dd08c67bd1, 55426bb348977496189cc6a61b711a3aadde155772a650ef17fba1f653431965, bfcd71a4095c2e81e2681aaf0239436368bc2ebddae7fdc8bb486ffc1040602c, 3f920619470488b8c1fda4bb82803f72205b18b1ea31402b461a0b8fe737d6bd, 84572c0de71bce332eb9fa03fd342433263ad0c4f95dd3acd86d1207fa7d23f0,

Attack Name	TYPE	VALUE
Grandoreiro	SHA256	29f19d9cd8fe38081a2fde66fb2e1eff33c4d4b5714ef5cada5cc76ec09bf2fa, 2ab8c3a1a7fe14a49084fbf42bbdd04d6379e6ae2c74d801616e2b9cf8c8519c, 70f22917ec1fa3a764e21f16d68af80b697fb9d0eb4f9cd6537393b622906908, fb3d843d35c66f76b1b1b88260ad20096e118ef44fd94137dbe394f53c1b8a46, 6772d2425b5a169aca824de3ff2aac400fa64c3edd93faaabd17d9c721d996c1
	URLs	hxxps[:]//onwfacttasunslahf[.]norwayeast[.]cloudapp[.]azure[.]com?_task=mail&_action=get&_mbox=INBOX&_uid=19101&_token=rbrJMXNUOQvrlaWOOxGAyj7vcufaFN3r&_part=1.2.3&_embed=1&_mimeclass=image, hxxps[:]//pjohconstruccionescpaz[.]com?docs/xml/WCA161006TN9/15540f02-d006-4e3b-b2de-6873baff3b2a, hxxps[:]//servicerevenueza[.]southeastasia[.]cloudapp.azure[.]com/?PDF-XML-71348793, hxxps[:]//officebusinessaccount[.]eastus[.]cloudapp[.]azure[.]com/?PDF-XML-<eight digit number>, hxxps[:]//servicerevenueza[.]southeastasia[.]cloudapp[.]azure[.]com/?PDF-XML-<eight digit number>, hxxps[:]//hilcfacdigitaelpichipt[.]norwayeast[.]cloudapp.azure[.]com/?docs/pdf/15540f02-d006-4e3b-b2de-6873baff3b2a, hxxps[:]//pjohconstruccionescpaz[.]com/?8205-23069071&tokenValue=92b768ccface4e96cee662517800b208f88ff796
	Emails	gruposat[@]gob[.]mx, root[[@]]zpmbnoxf[.]crazydocuments[.]com, marcasat[@]gob[.]mx , assistance[@]gov[.]za , ^root[@]yhsp\d{2}\[.]rufnag\[.]com$
	Domains	Rufnag[.]com, pjohconstruccionescpaz[.]com
	IPv4	18[.]231[.]181[.]227, 18[.]231[.]158[.]159, 15[.]229[.]211[.]175, 15[.]228[.]245[.]103
Dora RAT	MD5	4bc571925a80d4ae4aab1e8900bf753c, 951e9fcd048b919516693b25c13a9ef2, fee610058c417b6c4b3054935b7e2730, afc5a07d6e438880cea63920277ed270, d92a317ef4d60dc491082a2fe6eb7a70,

Attack Name	TYPE	VALUE
Dora RAT	MD5	5df3c3e1f423f1cce5bf75f067d1d05c, 094f9a757c6dbd6030bc6dae3f8feab3
	Domain	kmobile[.]bestunif[.]com
	IPv4:PORT	206[.]72[.]205[.]117[:]443
Nestdoor	MD5	7416ea48102e2715c87edd49ddbd1526, a2aefb7ab6c644aa8eeb482e27b2dbc4, e7fd7f48fbf5635a04e302af50dfb651, 33b2b5b7c830c34c688cf6ced287e5be
	IPv4:PORT	45[.]58[.]159[.]237[:]443, 4[.]246[.]149[.]227[:]1443, 209[.]127[.]19[.]223[:]443
GhostEngine	SHA256	2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59ecbd25753, 6f3e913c93887a58e64da5070d96dc34d3265f456034446be89167584a0b347e, 7c242a08ee2dfd5da8a4c6bc86231985e2c26c7b9931ad0b3ea4723e49ceb1c1, cc4384510576131c126db3caca027c5d159d032d33ef90ef30db0daa2a0c4104
XMRig	SHA256	23924cb27039491348cfa9a78c65ab3f6af5d0fa1efe61c90b6d7541c6de896f, c184a73f45c5b340409258c3a9c38e459a6aef8307f710f0eb967a7ff547858b, e875c8c9ee9962f28684d9090a96e6a0112cd4d875c802686de158ee64f0925f, 1afdadf62ec8d374f9c601bf77660f1816998e773c040631c0bbcd28e479b1aa, fe854f6d0ab457d19c354d227ace5edcd43c13194a058671403d42556b103eb3, 1d9876889cfdd7a19e0e847f87f069fd9152cb55d63ad2b1a4ee8e7abd373e59, 265945c6b195c7d80665414a6f8789ddcd087c8804847b67662a780c7bcdd748, 0c0fe53264eb7d9c50651ceaf3cafda42d765c13e6b2b7d845ad5e1f301c6d1f, 2f135bcca75cf029452fd95ebe7f14a56ac0745c08f1a47d1218443a4e85a9b7, df99a6272dd4098f15e779047507f4bf95ba8350d8911382fab6fca66dc0a58a, 37aca4a08a53e90247b03a0da697b0cb47e566bf64ef58698f09f6509c09111f,

Attack Name	TYPE	VALUE
XMRig	SHA256	2d6fac4d3df78fed33d0e0e63dc49bc28657d92dc03379b79aafbc3bda791503, d0271cf08762e9abf52a8d7c1601686bdcd93b0ee32efb12987268049813a7ec, 9dad543968781b6c0af82369e57acf1f52938d77a6bb0fe5d0e8563588f43a95, c6207f7a4f92ad987e43dd3a65a0b50e1778ec8dccf63313d1a6df7d223ddf33, f829a7b5ab31ac6a37035b282e83d55da7d313c70d1ec11f8b6999d78294695e, 08f3805606e1d457ed9e80b975bee0320651e3d5626e9e7cb896fd45e8fd0f7b, cdbeebbb4af40a2cea1aaf41db75f51d5bb511c328e8726256cb4fe7bacab2c8, 674f21780c32078f45bc05baeb308e16e841c4262d5aab352f3596669736b13b, 42fbdcb34832ff79d85b0c7c0cc7779fa3705dd28ba2119ef8e7e7a411afe467, 5f56885a9ac4593449b028b38341b16aabec3adb10702c0f498bc0feb9a2ecbe, 92da2571e11a7109bfbc842dc2859df90feb518302e82d5ddebcde0192fc5b63, fde1de57feca954ba860096e3d209b247d7e498c4210eef1bf1f57f6658e361e, a37dfed9e6f606b7bac6f7aff22b4624e4f670c00a8abc2b229dca8477271bcc, b92736e9915aa13e805583eb82ef68d3de6c2869dd82fe774d013c92365f65ba, 38d6aab4e818507641c0eb76d6448299099823ae7d13bc2bb3be088ae3e24573, 8a73d77a47d29d0e94b3a0de81d626d625b36397ab308f2af2860febe9e465bf, 3b16767f4702e0eedb9461f53bb7794cc188627484efe72f80c4db492e0217d0, d44227d8241bd1ad48cc76771969f96152728d25916dc07b8b15290b9ba767a9, 29d73b2aed43aba1cf0b90278b0cf4d402c3e5e22b0ade679df88bd9e0142ba4, 5d7fc3917f5c5c77543305a2a5185e11755aadac4464937fea223c6e6520a5f3, 87903c2711c047be5ef295419311bc2a4712e0ab10cd4afe2ee01af6145995d0, e0dc29cd9f9fb36a67782abf6231073d54365fa1a4ddade12cf47984a6113b45,

Attack Name	TYPE	VALUE
XMRig	SHA256	cd493e0109f708ba1ccd380f1efaeb6e7533baedf041ed055c621405cdf907b8, 209e301207a4695fa9d1642dd949f270298a82446e027ab8dd78a0d4e1ab2c35, 0d61b6eed0b001f11ed885a2223b39fdc461c2fe0f3338b81c22e11a4f1e9e52, b84cef08f737a9ad878e3ed98e4f3b61cc2e7440e7e0fc325a994e99f8c0cd2e, f241db8dea553a2add84eb7f7818a01bffcd5764e498953cd5a06e54ec8f5599, 8acc667814a5415b89bfaa445609dd68657359f78e6fe50013b436ff5506019e, e0ac7a9fa5503c78d75afbae370f4931aff9d7a18ff80c9c14060cd47045dcb5, be7ae8b05042920a137d990556062ad14b13607a222b8998f93d44dbd48bfda3, d68a529120da32c9e66410a0420f65b98752372bd321c7ff6f58ee3e0cf7af34, 065f21780636063a7b405e6d163b4db90960b84f99df884fbb1c616402ef0ff4, f7257f0645fb84a67c5a5b2dd12104cec156916f64aa7dadb1e354063f9a47a8, 507c455463c8222b988a2d988e742835e42ccc1ec45c3118039441c7e7242d95, 7ff80e19b49a455bd9facded8d476e79379514d78e6ada6087ae33a73cdfbc0c, 65321478bb2725e8c6285bf2b8aaa798034953a8b76f9cdf61a664066cee8444,
Acrid	MD5	abceb35cf20f22fd8a6569a876e702cb, 2b71c81c48625099b18922ff7bebbf51, b9b83de1998ebadc101ed90a6c312da8
ScarletStealer	MD5	1d3c3869d682fbd0ae3151b419984771, c0cf3d6d40a3038966f2a4f5bfe2b7a7, f8b2b941cffb9709ce8f422f193696a0
Sys01	MD5	6e2b16cc41de627eb7ddcd468a037761, 21df3a69540c6618cfbdaf84fc71031c, 23ae473bc44fa49b1b221150e0166199
5.t Downloader	SHA256	21f173a347ed111ce67e4c0f2c0bd4ee34bb7ca765da03635ca5c0df394cd7e6, 7575ebdd90aa0ab66c4eeaecd628c475e406ac9bcc54de5e01a3d372a050aec7, b952a459dac430d006a4d573612ca8474a410310792ea8141f9ab339214f4e57,

Attack Name	TYPE	VALUE
5.t Downloader	SHA256	42095521622c055db8d79441317952c0899c34d7b776f6f45855581fb86522dc, 941e52ce5ce89b7307bdfe1b88657dfd76892b475971b86683cfc6fbca23e209, e848355359de1e59901aa387f2d208889c368663438909fd3bb0a97566de2b2d, cc805511e106a9b5302a4db4bfbb98609aca3dcbd2f709aee8ae316f479dfd49, ea72011929dece4684a2dcb5b76f34cef437dbe50306f19c531d632bf26e7f32, 7b21b95c4256308e8089bff38d5d20845f2dc28fa9e536de979ceab9b7962afa, e6faf05234ceaaba3bdcca60285a7ba83eea229a0ca241e94fb314a73ad98d87, 20a4256443957fbae69c7c666ae025522533b849e01680287177110603a83a41, 1c2a10f282f1a24d88c74d8d324fb59b172cee4ee2e3e3996d9a62ba979812a6
Tiny backdoor	SHA256	b4db8e598741193ea9e04c2111d0c15ba79b2fa098efc3680a63ef457e60dbd9, 6829ab9c4c8a9a0212740f46bf93b1cbe5d4256fb4ff66d65a3a6eb6c55758a1, 8c97df4ca1a5995e22c2c4887bea2945269d6f5f158def98d5ebdd5311bb20c4, 76629afb86bd9024c3ea6759eeea197ba6c8c780e0041d1f8182d206cf3bd1b4, c2618fb013135485f9f9aa27983df3371dfdcb7beecde86d02cee0c258d5ed7f, cac4d4364d20fa343bf681f6544b31995a57d8f69ee606c4675db60be5ae8775
D3F@ck	MD5	44b14057ff868e25ad444fac098d89f0, 87cb408a03daa827f9cc10698ba69a90, 56f2d534631400ef294d321f8dbdfea, 5cf2e80ac2a7f7fa24f74966d3ec904f, 815b3c88950fd572bb4bfef96d2ca23d, be9989c6c218b0e99671a5bde240341e
	IPv4	194[.]147[.]35[.]251, 116[.]202[.]188[.]155, 195[.]20[.]16[.]155

Attack Name	TYPE	VALUE
ShrinkLocker Ransomware	MD5	842f7b1c425c5cf41aed9df63888e768
	SHA1	d96ddc136a68cf669238647c55ba88ea30bf0778
	SHA256	e5471fb4827cb570e65c2ebdff5da38e64b6a9fe47a81d11dab2f0937315be30
RustDoor	SHA256	238b546e2a1afc230f88b98dce1be6bf442b0b807e364106c0b28fe18db2ce66, 2acd053b854545d381866d471a711d860e84a38cb9f2e13983a74c4044080dc2, e86963c94f3c1de1ccfffaa4d192d39881a24df8b175c00fd64a4e076826b76b, f11b0f67f76b7d49511a6212921901afae5b7ecd2bbc718a3d70f6ccb524903a, b0665afbd99baf586899abae457f702962503afb855f4bda58cf070ca1c69956, bd1b0c5e48f4aa7595ef3e7dd125d0b95d39d647e480bd3c0c6ff7229d52f800, 00b66c1e7e483da6cbcc0d94f01b9fca245fb052ef8e958e21abcb0880aff37f, 996921573bc8d2618eaf4b7532fc1b46074fe5cdc317f5a751fc70b5371362a3, b4991bc670ba62c77ffec0a2fe3c445085de822ce8b282265cb24cfbae951ae0, f9a4f04d7222afbbadbf2cb417ee9e70733e1dcc2af94ec3cc9b6308a3216f93, 20b986b24d86d9a06746bdb0c25e21a24cb477acb36e7427a8c465c08d51c1e4, c93feb701e04cac4c6ed805d529378351e500ca1178958862d9e24c9f8723518, e96c13667bccd6c6c38d9797b15642bfea19080f9bc90d944e7ae6abfb4c64be, 4a59e2fe11ed9136d96a985448b34957ee5861adc9c1a52de4ad65880875dfdb, f59fcbb11a66b6596c2cca926c54e0a4114687769e726c39f2a918dc9e332eff, 449cc50caf2f4b85c6425fea809aa662b80f17821a8f3dc47fe8586ee56bd1dc, 5763ab1ccadc2724d6ec728926eb4dc574a6005a8456a65035dee5edb3cc2a0a, 481a279e15f808d695da233f690a0e3eb15d9b90fce42b9edb1ee296af6289d7, a69d91cf565e717662d0470183cced3350ba0bb4f91d2ced3f089af3a707c5c3 a9d299edf6b3bc1c98185e1c22ba7326f3ad6cba73ca00565330d5c3da50e02c,

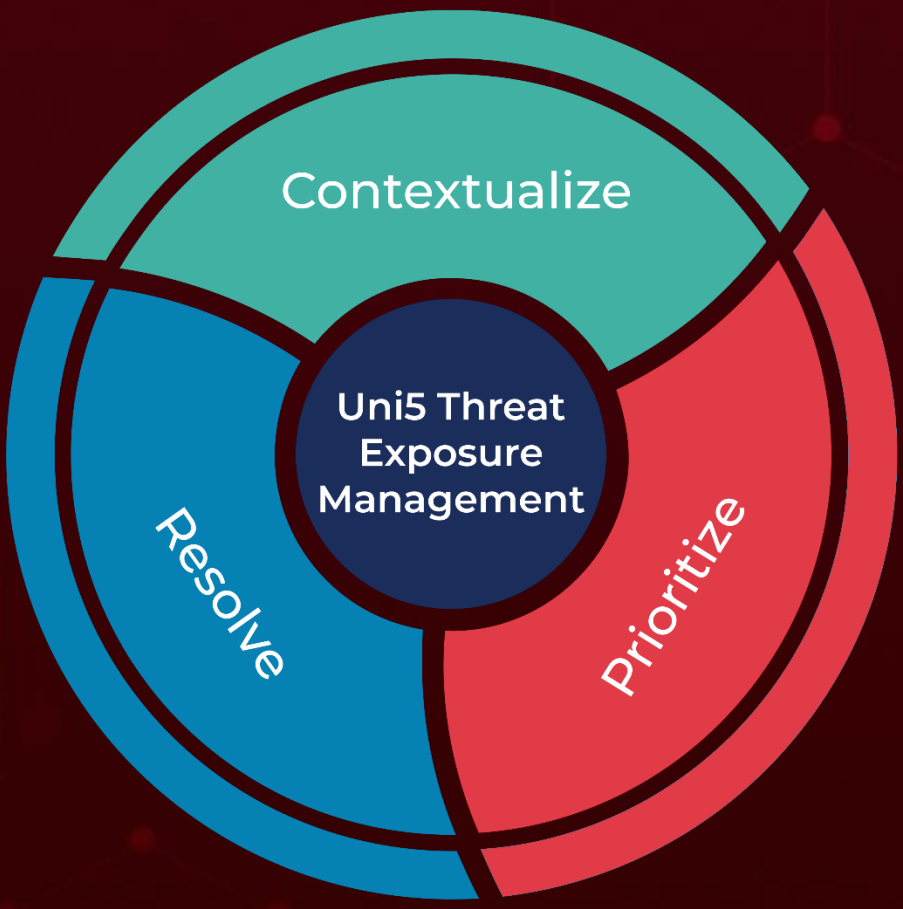
Attack Name	TYPE	VALUE
RustDoor	SHA256	6ea00e7d945e78f28d6043bb5d304e0f56d22ab104c9c74e77d1f8572dc17809, 01534a1849b197c03eb23c27d16ace7fc99778eeaa24953154e4f41afc712032, 11c998005bcce297b6a0595b97281aca7a587b6bc1e6aa414609812108b3328c, fe565f4296570a89893828cdd61c6421cf745bab220e21cebce226863d5772a0, c30f634f56000e87c9c4258174ec09ee5bd67d29eca4e78f63c34f976b0272d8, 43609c813c3084532073a22f24e931f24c04e118dcd972c6c8f0428637d9c0ff
GateDoor	SHA256	9dd66e5692e496c9cfcc647edf593c323404424cad61276725efb934b64b96e9
FakePenny Ransomware	Domain	bestonlinefilmstudio[.]org, blockchain-newtech[.]com, ccwaterfall[.]com, chaingrown[.]com, defitankzone[.]com, detankwar[.]com, freenet-zhilly[.]org, matrixane[.]com, pointdnt[.]com, starglowventures[.]com, mingeloem[.]com
	MD5	1d5ad4a60ec9be32c11ad99f234bfe8f, 14af3f039f2398b454bbb64c7fdf4a22, 66c45a736e165cf78cee7970bbc74ead, 330fff5b3c54a03fd59a64981e96814d, b8e1fe2955282a58fa3042b25f2ce19d, 608fb305734364e63513ef36da787f2b, c0bb453d00bf3d8acde09b691ca9b5f2, 6c76f795c4b3ff2e478766dee7c738d6, 08f8353101fb2f11a1036a947f8fce83, 39898007146d7b436d013924db58ebc6
	SHA256	f59035192098e44b86c4648a0de4078edbe80352260276f4755d15d354f5fc58, cb97ec024c04150ad419d1af2d1eb66b5c48ab5f345409d9d791db574981a3fb, 39d7407e76080ec5d838c8ebca5182f3ac4a5f416ff7bda9cbc4efffd78b4ff5,

Attack Name	TYPE	VALUE
FakePenny Ransomware	SHA256	70c5b64589277ace59db86d19d846a9236214b48aacabbaf880f2b6355ab5260, cafaa7bc3277711509dc0800ed53b82f645e86c195e85fbf34430bbc75c39c24, 9863173e0a45318f776e36b1a8529380362af8f3e73a2b4875e30d31ad7bd3c1, f66122a3e1eaa7dcb7c13838037573dace4e5a1c474a23006417274c0c8608be, 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c, ecce739b556f26de07adbfc660a958ba2dca432f70a8c4dd01466141a6551146, 09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5e84a6cc38
	SHA1	be6909ba6e0b4d228da5b9daccc83f7082c06cf2, f1f75da17e8c125b87fdafd76386f90213362bcf, b0479c5d4de5541a60923b5627ed62e6391efe2f, 550bdf367fba63a81276465a65dcb64280240dda, dd91678f1d023607430d53b5ff5f1d6533a98469, bda08d55f14827abf21abb79384039660f2fa198, 2ebfcbf2deb09e9af046ae765797a654b49645c2, e99d44e93069001129c8f88f7a5259fb21bb6b68, 853d256bafd39426fad9bf5f7fad2971b7978c06, dd8b8c4de92d9b6d1d04f0e995f4cc7e746d0a64

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 4, 2024 . 2:00 AM

More at www.hivepro.com