Date of Publication
December 4, 2023

Hive Pro®

HiveForce Labs

MONTHLY
THREAT DIGEST

Vulnerabilities, Actors, and Attacks

NOVEMBER 2023

Table Of Contents

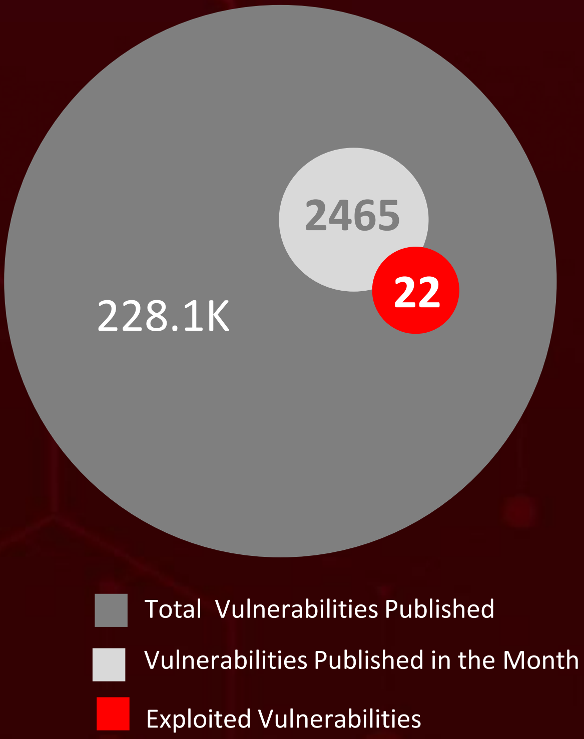
Summary

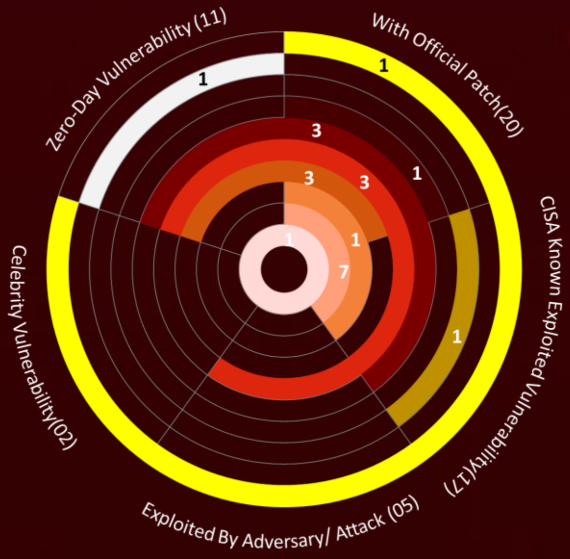
In **November**, the discovery of **eleven zero-day** vulnerabilities drew significant attention from the cybersecurity community. One of these vulnerabilities was exploited by the **Lace Tempest group**, leading to a sense of urgency among security teams to patch their systems.

November saw a rise in ransomware attacks, with various strains such as **LockBit ransomware**, **HelloKitty ransomware**, **TellYouThePass ransomware**, **Clop ransomware** and **NoEscape Ransomware** actively targeting victims. As ransomware continues to evolve and grow in sophistication, organizations must take steps to protect themselves by implementing comprehensive backup and disaster recovery strategies and training employees on how to recognize and avoid phishing attacks.

Furthermore, nineteen adversaries were active and involved in various campaigns. **SideCopy** exploited a vulnerability (**CVE-2023-38831**) in WinRAR, targeting Indian government agencies.

Lastly, the **CVE-2023-4966**, a critical zero-day vulnerability was exploited since August potentially to allowing attackers to steal authentication sessions and hijack accounts.





Insights

farnetwork

The Russian Speaking actor behind five Ransomware strains

Ransom of $980

Demanded by DJVU ransomware for decryption

Citrix Bleed

Flaw has been targeted since August to steal authentication sessions and hijack

NoEscape Ransomware

Operating as Ransomware-as-a-
Service, it encrypts files, changes wallpapers, and demands ransom

Government, Education, Technology Financial Services were the most targeted sectors

63

vulnerabilities were patched during November Microsoft Patch Tuesday, out of which 5 were Zero-Day

CVE-2023-38831

SideCopy is capitalizing on WinRAR's flaw to target Indian government agencies

Mustang Panda

Targets Philippines Government Using Legitimate Software

United States, Israel, United Arab Emirates and **Iraq** were the most targeted countries

BlazeStealer

PyPI repository infiltrated with malicious packages masquerading as Obfuscation utility targeting developer community

Threat Landscape

22 Vulnerabilities

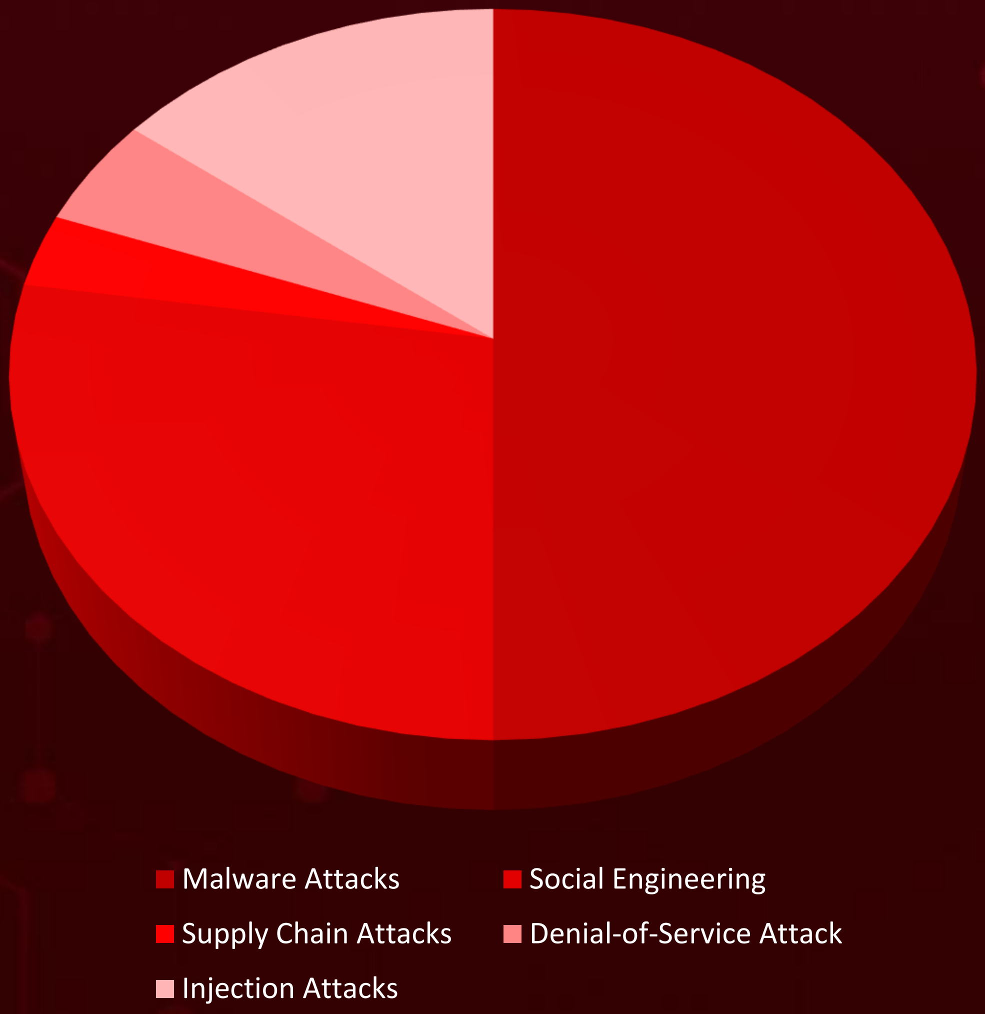
204 MITRE ATT&CK TTPs

33 Industries

20 Adversaries

223 Countries

52 Attacks



Celebrity Vulnerabilities

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4966	✓	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50, 13.1 before 13.1-49.15 & 13.0 before 13.0-92.19, NetScaler ADC 13.1-FIPS before 13.1-37.164 & 12.1-FIPS before 12.1-55.300, NetScaler ADC 12.1-NDcPP before 12.1-55.300	-
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**ZERO-DAY**	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	LockBit ransomware
Citrix Bleed (Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability)	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-119	T1574: Hijack Execution Flow; T1499.004: Application or System Exploitation; T1563: Remote Service Session Hijacking; T1548.002: Bypass User Account Control; T1210: Exploitation of Remote Services	https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4911	✓	All systems running glibc 2.34 to 2.37	Kinsing
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:gnu:c_library:*:*:*:*:*:*:*:*	-
Looney Tunables (Glibc Buffer Overflow Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1574: Hijack Execution Flow	Upgrade glibc to 2.38 or later versions

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability (Citrix Bleed)	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2023-4967	Citrix NetScaler ADC and NetScaler Gateway Denial of Service Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✗	✗	✓
CVE-2023-22518	Atlassian Confluence Improper Authorization Vulnerability	Confluence Data Center, Confluence Server	✗	✓	✓
CVE-2023-46604	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	Apache ActiveMQ	✗	✓	✓
CVE-2023-4911	Glibc Buffer Overflow Vulnerability	GNU C Library (glibc)	✗	✓	✓
CVE-2017-9841	PHPUnit Command Injection Vulnerability	Oracle Communications Diameter Signaling Router	✗	✓	✓
CVE-2023-38831	RARLAB WinRAR Code Execution Vulnerability	WinRAR	✓	✓	✓
CVE-2023-47246	SysAid path traversal vulnerability	SysAid	✓	✗	✓
CVE-2023-36844	Juniper Junos OS EX Series PHP External Variable Modification Vulnerability	Juniper Junos OS	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-36845	Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability	Juniper Junos OS	✗	✓	✓
CVE-2023-36846	Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability	Juniper Junos OS	✗	✓	✓
CVE-2023-36847	Juniper Junos OS EX Series Missing Authentication for Critical Function Vulnerability	Juniper Junos OS	✗	✓	✓
CVE-2023-36851	Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability	Juniper Junos OS	✗	✓	✗
CVE-2023-36033	Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2023-36025	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2023-36036	Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2023-36038	ASP.NET Core Denial of Service Vulnerability	Microsoft ASP.NET	✓	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-36413	Microsoft Office Security Feature Bypass Vulnerability	Microsoft Office	✓	✗	✓
CVE-2023-34060	VMware Cloud Director Authentication Bypass Vulnerability	VMware Cloud Director Appliance (VCD Appliance)	✓	✗	✗
CVE-2023-37580	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	Zimbra Collaboration (ZCS)	✓	✓	✓
CVE-2023-6345	Google Chrome Skia Integer Overflow Vulnerability	Google Chrome	✓	✓	✓
CVE-2023-49103	ownCloud graphapi app Information Disclosure Vulnerability	ownCloud	✗	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
LockBit ransomware	Ransomware	CVE-2023-4966, CVE-2023-4967	Citrix NetScaler ADC and NetScaler Gateway	✓	Exploiting vulnerabilities
LIONTAIL	Passive loader	-	-	-	Phishing
HelloKitty ransomware	Ransomware	CVE-2023-46604	Apache ActiveMQ	✓	Exploiting vulnerabilities
TellYouThePass ransomware	Ransomware	CVE-2023-46604	Apache ActiveMQ	✓	Exploiting vulnerabilities
SparkRAT	RAT	CVE-2023-46604	Apache ActiveMQ	✓	Exploiting vulnerabilities
Socks5Systemz	Proxy botnet	-	-	-	Phishing, exploit kits, malvertising, trojanized executables
PrivateLoader	Loader	-	-	-	Phishing, exploit kits, malvertising, trojanized executables
Amadey	Loader	-	-	-	Phishing, exploit kits, malvertising, trojanized executables
Jupyter Infostealer	Infostealer	-	-	-	Phishing
MultiLayer	Wiper	-	-	-	Exploiting vulnerable internet facing web servers

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
PartialWasher	Wiper	-	-	-	-
BFG Agonizer	Wiper	-	-	-	Exploiting vulnerable internet facing web servers
sqlextractor	Infostealer	-	-	-	Exploiting vulnerable internet facing web servers
ObjCShellz	Backdoor	-	-	-	-
RustBucket	Backdoor	-	-	-	-
AllaKore RAT	RAT	CVE-2023-38831	WinRAR	✓	Exploiting Vulnerability
Ares RAT	RAT	CVE-2023-38831	WinRAR	✓	Phishing
DRat	RAT	CVE-2023-38831	WinRAR	✓	Exploiting Vulnerability
Key RAT	RAT	CVE-2023-38831	WinRAR	✓	Exploiting Vulnerability
Millenium RAT	RAT	-	-	-	-
BlazeStealer	Stealer	-	-	-	-
Nokoyawa	Ransomware	-	-	-	-
JSWORM	Ransomware	-	-	-	-
Nefilim	Ransomware	-	-	-	-
Karma	Ransomware	-	-	-	-
Nemty	Ransomware	-	-	-	-
FakeBat	Loader	-	-	-	Google Ads
Redline stealer	Infostealer	-	-	-	-

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Clop ransomware	Ransomware	CVE-2023-47246	SysAid	✓	-
Gracewire	RAT	CVE-2023-47246	SysAid	✓	-
Ducktail	Infostealer	-	-	-	Spear-phishing emails
IronWind	Downloader	-	-	-	Social Engineering
SharpSploit	Toolkit	-	-	-	Spear phishing and IronWind
NoEscape Ransomware	Ransomware	-	Windows, Linux, and ESXi	-	Phishing
GhostLocker	Modular	-	-	-	Phishing, Affiliate Programs, Darkweb Marketplace
BlackCat/ALPHV Ransomware	Ransomware	-	-	-	Social engineering, phishing, and SIM swap attacks
AveMaria	RAT	-	-	-	Social engineering, phishing, and SIM swap attacks
Raccoon Stealer	Infostealer	-	-	-	Social engineering, phishing, and SIM swap attacks
VIDAR Stealer	Infostealer	-	-	-	Social engineering, phishing, and SIM swap attacks
LitterDrifter	Worm	-	-	-	USB drives

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Kinsing	Cryptocurrency miner	CVE-2023-46604	ActiveMQ	✓	Exploiting vulnerability
NetSupport RAT	RAT	-	-	-	Phishing
Nim backdoor	Backdoor	-	-	-	Phishing
DarkGate	Loader	-	-	-	Phishing
Atomic Stealer	Infostealer	-	Mac OS	-	Legitimate AnyDesk remote desktop software
LambLoad	Downloader	-	-	-	Supply chain attacks, Phishing
InfectedSlurs	Botnet	-	-	-	Exploiting vulnerabilities
SwiftLoader	Loader	-	Mac OS	-	-
KandyKorn	RAT	-	Mac OS	-	-
ParaSiteSnatcher	Malicious Extension	-	-	-	Through a VBScript downloader
Djvu	Ransomware	-	-	-	Disguise of cracked software
Cerber ransomware	Raas	CVE-2023-22518	Confluence Data Center, Confluence Server	✓	Exploiting vulnerabilities

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Scarred Manticore	Information theft and espionage	Iran	-	LIONTAIL	Windows
MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm)	Information theft and espionage	Iran	-	-	-
Kinsing (aka Money Libra)	Information Theft	-	CVE-2023 4911, CVE-2017-9841	-	GNU C Library (glibc), Oracle Communications Diameter Signaling Router
Agrius (aka Agonizing Serpens, DEV-0227, BlackShadow, SharpBoys, AMERICIUM, Pink Sandstorm)	Information theft and espionage, Sabotage and destruction	Iran	-	MultiLayer, PartialWasher, BFG Agonizer, sqlextractor	-
BlueNorOff (APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet, TAG-71)	Financial crime	North Korea	-	ObjCShellz, RustBucket	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
SideCopy	Information theft and espionage	Pakistan	CVE-2023-38831	AllaKore RAT, Ares RAT, DRat, Key RAT	WinRAR
farnetwork (aka farnetworkl, jingo, jsworm, razvrat, piparkuka, and farnetworkit)	Develop ransomware	-	-	Nokoyawa, JSWORM, Nefilim, Karma, and Nemty	-
Lace Tempest (aka DEV-0950, FIN11)	Financial crime, Financial gain	-	CVE-2023-47246	Clop ransomwar, Gracewire (FlawedGrace)	SysAid servers
TA402 (aka Extreme Jackal, Molerats, Gaza Cybergang, Gaza Hackers Team, Aluminum Saratoga, ATK 89, TAG-CT5)	Information theft and espionage	Palestine	-	IronWind, SharpSploit	-
Winter Vivern	Information theft and espionage	-	CVE-2023-37580	-	Zimbra Collaboratio n (ZCS)
GhostSec (aka Ghost Security)	Information theft, espionage and Financial crime	-	-	GhostLocker	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Scattered Spider (Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, and Muddled Libra)	Financial gain	-	-	BlackCat/ALPHV Ransomware, AveMaria, Raccoon Stealer, and VIDAR Stealer	-
Gamaredon (aka Primitive Bear, Winterflounder, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Shuckworm, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard)	Information theft and espionage	Russia	-	LitterDrifter	-
TA569	Information theft and espionage	-	-	NetSupport RAT	-
SideWinder (aka Razor Tiger, Rattlesnake, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21)	Information theft and espionage	India	-	Nim backdoor	-
Mustang Panda (aka Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Earth Preta, Camaro Dragon, Stately Taurus)	Information theft and espionage	China	-	-	-
RastaFarEye	Information theft and espionage	-	-	DarkGate	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Lazarus Group	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	-	LambLoad	-
Andariel	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	-	LambLoad	-
DarkCasino	Economic motivations	-	CVE-2023-38831	-	RARLAB WinRAR

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
CITRIX	Applications	NetScaler ADC and NetScaler Gateway 14.1 before 14.1- 8.50, 13.1 before 13.1- 49.15 & 13.0 before 13.0-92.19, NetScaler ADC 13.1-FIPS before 13.1-37.164 & 12.1- FIPS before 12.1-55.300, NetScaler ADC 12.1-NDcPP before 12.1-55.300
ATLASSIAN	Data Center and Server	Confluence Data Center and Server 6.0.1 - 8.6.0
	Application	Apache ActiveMQ 5.18.0 before 5.18.3, Apache ActiveMQ 5.17.0 before 5.17.6, Apache ActiveMQ 5.16.0 before 5.16.7, Apache ActiveMQ before 5.15.16, Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3, Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6, Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7, Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16
	Library	All systems running glibc 2.34 to 2.37
ORACLE	Router	Oracle Communications Diameter Signaling Router
	Application	WinRAR version 6.22 and older versions

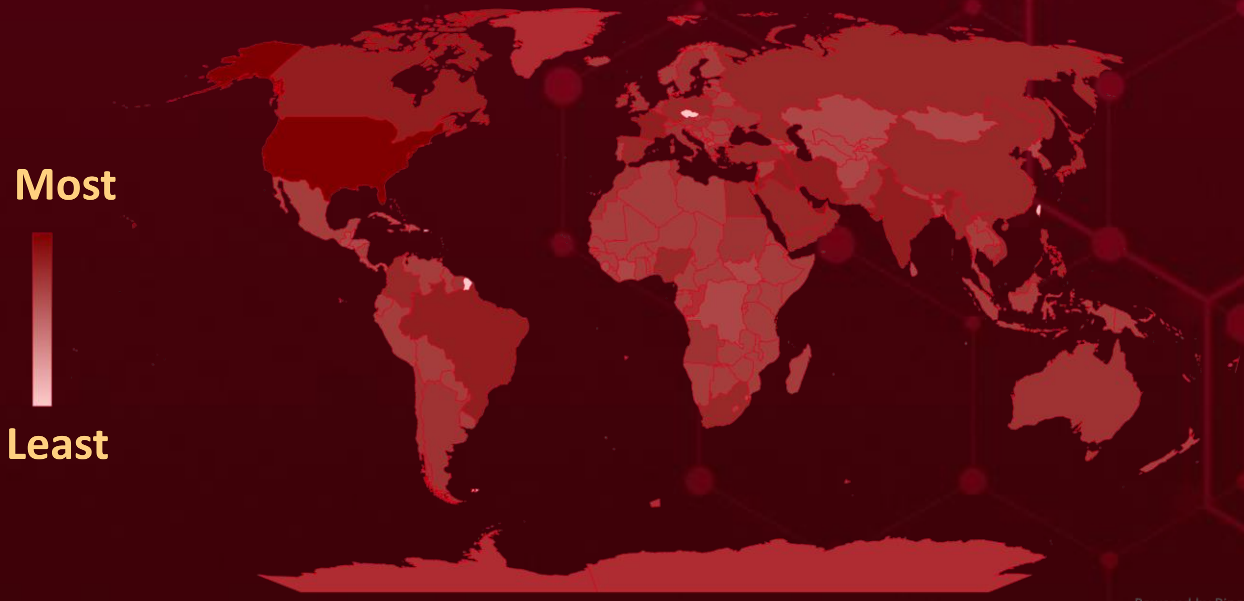
VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
SysAid	Server	SysAid: 21.4.45 - 23.3.35

JUNIPER NETWORKS	Operating System	All versions prior to 20.4R3-S9; 21.1 version 21.1R1 and later versions;
		21.2 versions prior to 21.2R3-S7;
		21.3 versions prior to 21.3R3-S5;
		21.4 versions prior to 21.4R3-S5;
		22.1 versions prior to 22.1R3-S4;
		22.2 versions prior to 22.2R3-S2;
		22.3 versions prior to 22.3R2-S2, 22.3R3-S1;
		22.4 versions prior to 22.4R2-S1, 22.4R3;
		23.2 versions prior to 23.2R1- S1, 23.2R2
		15.0.4

Microsoft	Operating System	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2
	Application	Visual Studio: 2022 version 17.2 – 2022 version 17.7 ASP.NET Core: 8.0 .NET: 8.0.0
	Application	Microsoft Office: 2016 -2019 Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
	Server	Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018
	Cloud Platform	az webapp configappsettings set & delete: All versions; az staticwebappappsettings set & delete: All versions; az logicapp configappsettings set & delete: All versions; az functionapp configappsettings set & delete:All versions

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
vmware	Cloud Service Platform	VMware Cloud Director: 10.5.0
zimbra A SYNACOR PRODUCT	Software	Zimbra Collaboration: 8.8.15 - 8.8.15 Patch 40
Google	Browser	Google Chrome 100.0.4896.60 – 119.0.6045.160
ownCloud	Software	ownCloud graphapi 0.2.0 – 0.3.0

Targeted Countries



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Color	Countries
🟥	United States
🟥	Israel
🟥	United Arab Emirates
🟥	Iraq
🟥	Canada
🟥	Brazil
🟥	Lebanon
🟥	France
🟥	Iran
🟥	India
🟥	Jordan
🟥	Saudi Arabia
🟥	Philippines
🟥	China
🟥	Cyprus
🟥	Qatar
🟥	Egypt
🟥	Spain
🟥	Japan
🟥	Oman
🟥	Bahrain
🟥	Poland
🟥	Kuwait

Color	Countries
🟥	Russia
🟥	Germany
🟥	South Africa
🟥	Yemen
🟥	Turkey
🟥	Myanmar
🟥	Colombia
🟥	Nigeria
🟥	Vietnam
🟥	Pakistan
🟥	Switzerland
🟥	Angola
🟥	Austria
🟥	Morocco
🟥	Greece
🟥	Chile
🟥	Hungary
🟥	Suriname
🟥	Belgium
🟥	Argentina
🟥	Ireland
🟥	Netherlands
🟥	Italy
🟥	Cambodia
🟥	Lithuania

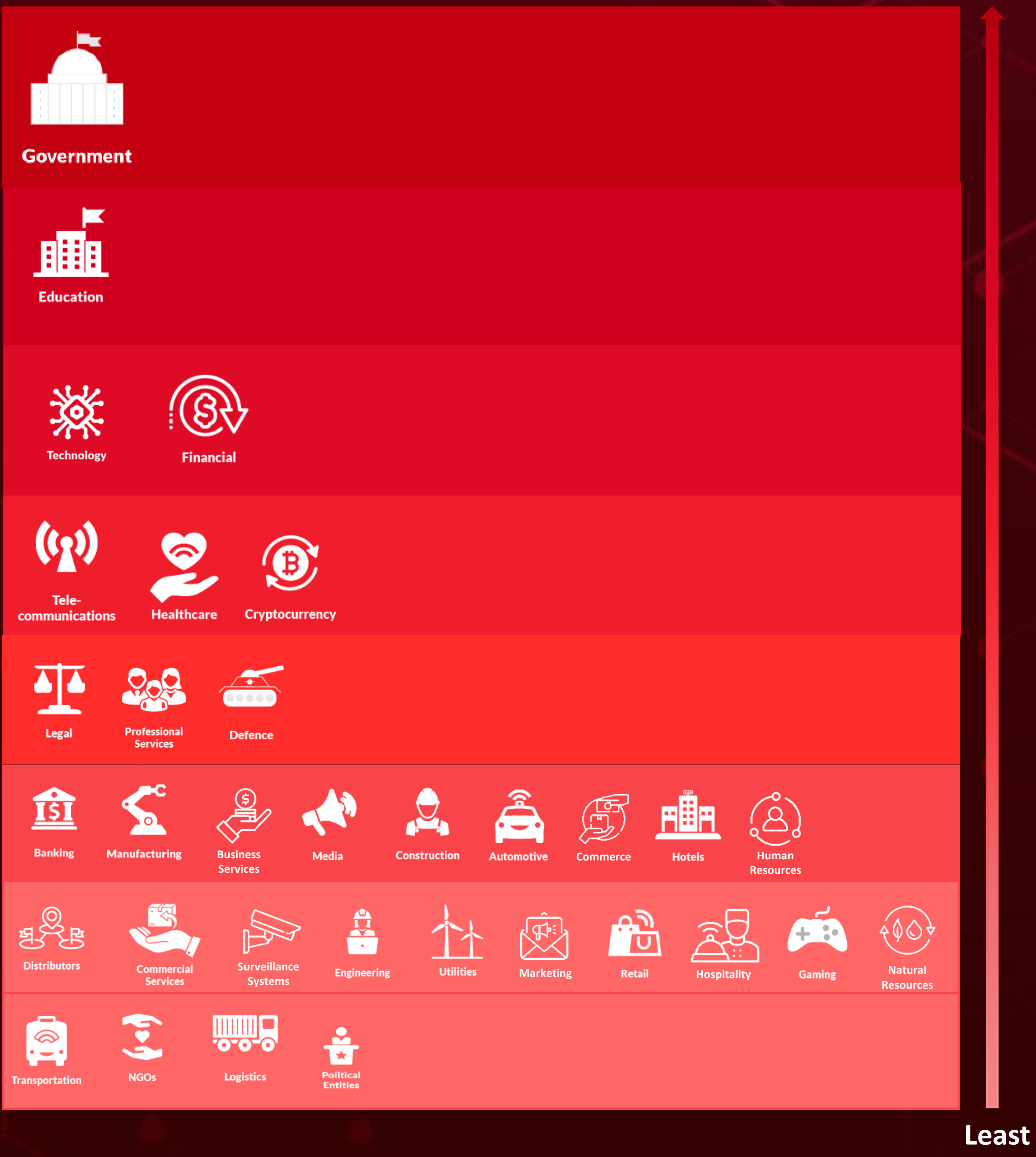
Color	Countries
🟥	South Korea
🟥	Malaysia
🟥	Sudan
🟥	Mauritius
🟥	Sweden
🟥	United Kingdom
🟥	Tunisia
🟥	Croatia
🟥	Ukraine
🟥	Australia
🟥	Moldova
🟥	Iceland
🟥	Central African Republic
🟥	Papua New Guinea
🟥	Bhutan
🟥	Slovakia
🟥	Eritrea
🟥	Denmark
🟥	Bolivia
🟥	Cameroon
🟥	Bosnia and Herzegovina
🟥	Chad
🟥	Kenya

Color	Countries
🟥	Guinea
🟥	Botswana
🟥	Thailand
🟥	Laos
🟥	Equatorial Guinea
🟥	Algeria
🟥	Peru
🟥	Venezuela
🟥	Andorra
🟥	Brunei
🟥	San Marino
🟥	Zimbabwe
🟥	Serbia
🟥	Liechtenstein
🟥	Somalia
🟥	Estonia
🟥	Guyana
🟥	Luxembourg
🟥	Syria
🟥	Madagascar
🟥	Togo

Color	Countries
🟥	Malawi
🟥	Benin
🟥	Ethiopia
🟥	Bangladesh
🟥	Mali
🟥	Paraguay
🟥	Malta
🟥	Ghana
🟥	Mauritania
🟥	Portugal
🟥	Fiji
🟥	Romania
🟥	Mexico
🟥	Rwanda
🟥	Finland
🟥	Sao Tome & Principe
🟥	Albania
🟥	Senegal
🟥	Gabon
🟥	Singapore
🟥	Gambia
🟥	Slovenia
🟥	Mozambique
🟥	Djibouti

Targeted Industries

Most



Government

Education

Technology

Financial

Telecommunications

Healthcare

Cryptocurrency

Legal

Professional Services

Defence

Banking

Manufacturing

Business Services

Media

Construction

Automotive

Commerce

Hotels

Human Resources

Distributors

Commercial Services

Surveillance Systems

Engineering

Utilities

Marketing

Retail

Hospitality

Gaming

Natural Resources

Transportation

NGOs

Logistics

Political Entities

Least

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter

T1204 User Execution

T1588 Obtain Capabilities

T1105 Ingress Tool Transfer

T1027 Obfuscated Files or Information

T1588.006 Vulnerabilities

T1204.002 Malicious File

T1566 Phishing

T1041 Exfiltration Over C2 Channel

T1083 File and Directory Discovery

T1036 Masquerading

T1059.001 PowerShell

T1543 Create or Modify System Process

T1190 Exploit Public-Facing Application

T1574 Hijack Execution Flow

T1082 System Information Discovery

T1140 Deobfuscate/Decode Files or Information

T1071 Application Layer Protocol

T1071.001 Web Protocols

T1055 Process Injection

T1005 Data from Local System

T1547 Boot or Logon Autostart Execution

T1203 Exploitation for Client Execution

T1588.005 Exploits

T1057 Process Discovery

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
LockBit ransomware	SHA256	27389c160ceee51ca1f2b111ca8b221dc75b71cc699789da65802dce082dfbb4, a5e6df754a4d3bb72f4d5c91d6b582e7e2c2f87ca838f5d976bc82384a5ad2d1, 67b05e96f47db0447da53beddbf9aff265cd02562c12428d787fdab0278ded2e, a2db758f099d8a6dec5fd500d033ce2fcd89b58b53d938fdb9d9cba2d91dba01, 2daa5fa152b627f5ae23d2e8fa4e3e399d4899729ad32f184e32d59fd4dd20ef
HelloKitty	SHA256	c3c0cf25d682e981c7ce1cc0a00fa2b8b46cce2fa49abe38bb412da21da99cb7, 8c226e1f640b570a4a542078a7db59bb1f1a55cf143782d93514e3bd86dc07a, 8177455ab89cc96f0c26bc42907da1a4f0b21fdc96a0cc96650843fd616551f4
	Email	service@hellokittycat[.]online
	IPv4	172.245.16[.]125
	URL	hxxp://172.245.16[.]125/m4.png, hxxp://172.245.16[.]125/m2.png
BlazeStealer	SHA256	77e183e63c70a44e87277be35b63817e185efcf1b8ab46937626904923251bbe, fb58f3f04e149b97a01c16a3bfedcb0ff33dc476dbab469fe011e3a379f2b00a, 87fda7a9d8156a9b3ca3ea92173c9c5c5abbd4a7e9f17c1b81e8921914cd5306, ccec28cfab447c153bc82993857b2ae865eab73c996d4db705ab1df6f1f29c40, b6c51f8700c067604354dc3f41cafb76ac7e3235fa7983c7407e18729dd94187, 9c3637d925b3bb46ad68e7667e5958cc6e0926d9b12f022c6e0e990d63f45a9d, a0422225d67779574006c04bd95bb19c02c5dd94f0af009606d58cf0b3854d6d, 14288b82c089fd1edd66feef6b0ff656d723f2e893b8c2574495b64c48b762a5, 51d5f41603a4a311c63e3db5d1cf8d5ddba28aa5cdabff62cad9f646fce8b5da, 716df8c14081570de5489c54a6e1d87d28f5d9d6848ab2b11654a5a3fbb29880

Attack Name	TYPE	VALUE
NoEscape	SHA256	0073414c5a03b20f6f255f400291de67f2a7268c461f90ea6ff0355ca31af07a, 2020cae5115b6980d6423d59492b99e6aaa945a2230b7379c2f8ae3f54e1efd5, 4175dae9b268fe5b4f96055ea0376417b5ddc2518d3bd11e20f0f8255bb4621e, 4d7da1654f9047b6c6a9d32564a66684407ed587cbaffa54ec1185fd73293d3e, 5300d7456183c470a40267da9cd1771d6147445b203d8eb02437348bf3169e0d, 53f5c2f70374696ff12adcaaf1bbbe0e5dd1b1995d98f2e876b0671888b43128, 62205bf0a23e56524f2f1c44897f809457ad26bc70810008ec5486e17c7e64e2, 68bce3a400721d758560273ae024f61603b8a4986440a8ec9e28305d7e6d02b0, 68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccd2bc0d8, 73c19eab8d2ae58db3968dd7de0e745db2d7709859305b113b748bb02494465e, 831a2409d45d0c7f15b7f31eddbbdfe7d58414499e81b3da7d9fdee28fafe646, 8dd64ea7f226d3eb1e857b0086c0668542652cb37f8142dc000272dbd9569e31, 91c515d55fae6d21b106c8c55067ce53d42bef256bd5a385cadd104cf68f64ff,
Clop ransomware	MD5	31e0439e6ef1dd29c0db6d96bac59446, 4431b6302b7d5b1098a61469bdfca982, 5e52f75d17c80dd104ce0da05fdfc362, 8bd774fbc6f846992abda69ddabc3fb7, afe7f87478ba6dfca15839f958e9b2ef, dd5cee48cdd586045c5fb059a1120e15, f59d2a3c925f331aae7437dd7ac1a7c8
	SHA1	40b7b386c2c6944a6571c6dcfb23aaae026e8e82, 46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5, 4fa2b95b7cde72ff81554cfbddc31bbf77530d4d, 77ea0fd635a37194efc1f3e0f5012a4704992b0e, a1a628cca993f9455d22ca2c248ddca7e743683e, a6e940b1bd92864b742fbd5ed9b2ef763d788ea7, ac71b646b0237b487c08478736b58f208a98eebf, ba5c5b5cbd6abdf64131722240703fb585ee8b56

Attack Name	TYPE	VALUE
Gracewire	MD5	88695dbddd4fc57025b523f4fca268d7, 80a20106ced1a5d9f350b1401dbe7d14
	SHA1	57ab5d9b5302644e91e3953062b40c5346b236e3, 753561bf6da3cbb75711d109ed0e38b7abb28db8
	SHA256	f92dbf7943590c2c4011f911ba9ba445010c9d5895b5c8b57a5da9c8708c221d, 6d15a0807858dce0be652e480fa7f298482c7bbf2c1e116e6cf0a3d3df95180f
NoEscape	SHA256	0073414c5a03b20f6f255f400291de67f2a7268c461f90ea6ff0355ca31af07a, 2020cae5115b6980d6423d59492b99e6aaa945a2230b7379c2f8ae3f54e1efd5, 4175dae9b268fe5b4f96055ea0376417b5ddc2518d3bd11e20f0f8255bb4621e, 4d7da1654f9047b6c6a9d32564a66684407ed587cbaffa54ec1185fd73293d3e, 5300d7456183c470a40267da9cd1771d6147445b203d8eb02437348bf3169e0d, 53f5c2f70374696ff12adcaaf1bbbe0e5dd1b1995d98f2e876b0671888b43128, 62205bf0a23e56524f2f1c44897f809457ad26bc70810008ec5486e17c7e64e2, 68bce3a400721d758560273ae024f61603b8a4986440a8ec9e28305d7e6d02b0, 68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccd2bc0d8, 73c19eab8d2ae58db3968dd7de0e745db2d7709859305b113b748bb02494465e, 831a2409d45d0c7f15b7f31eddbbdfe7d58414499e81b3da7d9fdee28fafe646, 8dd64ea7f226d3eb1e857b0086c0668542652cb37f8142dc000272dbd9569e31, 91c515d55fae6d21b106c8c55067ce53d42bef256bd5a385cadd104cf68f64ff, 9d346518330eeefbf288aeca7b2b6243bc158415c7fee3f2c19694f0e5f7d51c, 10d2b5f7d8966d5baeb06971dd154dc378496f4e5faf6d33e4861cd7a26c91d7, 21162bbd796ad2bf9954265276bfebea8741596e8fe9d86070245d9b5f9db6da, 46f1a4c77896f38a387f785b2af535f8c29d40a105b63a259d295cb14d36a561, c34c5dd4a58048d7fd164e500c014d16befa956c0bce7cae559081d57f63a243

Attack Name	TYPE	VALUE
NoEscape	SHA1	ea1f7940271fc80d06b2f222506020b650ad41bc, 30f71a24c15dd81965b12996a79d914acf4f169e, 12dc0a2de3ad30201107bfcb679de5acacf31e5c, 30c60f18279ed5fd36e3ac2d3ba5ddbdc5d1f624, 9cbc7417fa5ce2f6d87026337fc7892e4f485819, d38c613020cb4616783c8535380e28404f7eaebf, b17403e7dcb992ba8d2b56dd843406264d3910e5, 317f296131b37a73c9a5d253015821dfdc8b1190
	MD5	204f028c983f654be32b97e849edeaab, 47ae17d89c2d9b6acdc7458f5df1c6f7, 5779cec690b5bbc61687381ae8a8d518, 58b4a4eed74fbfbf104d0ffd92207018, a106c1236357c315722ddbd985c5613c, c850f6816459e3364b2a54239642101b

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4966	✓	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50, 13.1 before 13.1-49.15 & 13.0 before 13.0-92.19, NetScaler ADC 13.1-FIPS before 13.1-37.164 & 12.1-FIPS before 12.1-55.300, NetScaler ADC 12.1-NDcPP before 12.1-55.300	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	LockBit ransomware
Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1574: Hijack Execution Flow; T1499.004: Application or System Exploitation; T1563: Remote Service Session Hijacking; T1548.002: Bypass User Account Control; T1210: Exploitation of Remote Services	https://support.citrix.com/article/CTX579459/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4967	✗	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50, 13.1 before 13.1-49.15 & 13.0 before 13.0-92.19, NetScaler ADC 13.1-FIPS before 13.1-37.164 & 12.1-FIPS before 12.1-55.300, NetScaler ADC 12.1-NDcPP before 12.1-55.300	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	LockBit ransomware
Citrix NetScaler ADC and NetScaler Gateway Denial of Service Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1499: Endpoint Denial of Service, T1574: Hijack Execution Flow	https://support.citrix.com/article/CTX579459/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-22518	✗	Confluence Data Center and Server 6.0.1 - 8.6.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_server_and_data_center:8.6.0:*:*:*:*:*:*:*	Cerber ransomware
Atlassian Confluence Improper Authorization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-285	T1588.006: Vulnerabilities	https://www.atlassian.com/software/confluence/download-archives

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-46604	✗	Apache ActiveMQ 5.18.0 before 5.18.3, Apache ActiveMQ 5.17.0 before 5.17.6, Apache ActiveMQ 5.16.0 before 5.16.7, Apache ActiveMQ before 5.15.16, Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3, Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6, Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7, Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:activemq:*:*:*:*:*:*:* cpe:2.3:a:apache:activemq_legacy_openwire_module:*:*:*:*:*:*:*	HelloKitty ransomware
Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://activemq.apache.org/security-advisories.data/CVE-2023-46604

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4911	☒	All systems running glibc 2.34 to 2.37	Kinsing
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gnu:c_library:*:*:*:*:*:*:*:*	-
Glibc Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1574: Hijack Execution Flow	Upgrade glibc to 2.38 or later versions

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-9841	☒	Oracle Communications Diameter Signaling Router	Kinsing
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:phpunit_project:phpunit:*:*:*:*:*:*:*:*	-
PHPUnit Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1055: Process Injection	https://www.oracle.com/security-alerts/cpuoct2021.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831	✗	WinRAR version 6.22 and older versions	SideCopy
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*:*	AllaKore RAT, Ares RAT, DRat, Key RAT
RARLAB WinRAR Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	Update WinRAR version to 6.23 or later versions

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-47246	✗	SysAid: 21.4.45 - 23.3.35	Lace Tempest
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sysaid:sysaid:-:*:*:*:*:*:*:*	Clop ransomware, Gracewire
SysAid path traversal vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1588.006: Vulnerabilities	https://documentation.sysaid.com/docs/latest-version-installation-files

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36844	✗	Juniper Junos OS: 20.4 - 22.4R2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*	-
Juniper Junos OS EX Series PHP External Variable Modification Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-473	T1005: Data from Local System, T1499.004: Application or System Exploitation, T1211: Exploitation for Defense Evasion	https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2023-36845](CVE-2023-36845)	☒	Juniper Junos OS: 20.4 - 22.4R2	-
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*	-
Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-473	T1005: Data from Local System, T1499.004: Application or System Exploitation, T1211: Exploitation for Defense Evasion	https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36846	✗	Juniper Junos OS: 20.4 - 22.4R2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*	-
Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36847	✗	Juniper Junos OS: 20.4 - 22.4R2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*	-
Juniper Junos OS EX Series Missing Authentication for Critical Function Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36851	✗	Juniper Junos OS: 20.4 - 22.4R2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*	-
Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	WORKAROUND
	CWE-306	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-36033</td><td>✗</td><td rowspan="2">Windows: 10 - 11 23H2, Windows Server: 2019 - 2022 23H2</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:o:microsoft:windows:10:1809:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-119</td><td>T1068: Exploitation for Privilege Escalation, T1204.001: Malicious Link</td><td>https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36033</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-36025</td><td>✗</td><td rowspan="2">Windows: 10 - 11 23H2, Windows Server: 2008 - 2022 23H2</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:o:microsoft:windows:10:1809:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft Windows SmartScreen Security Feature Bypass Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-254</td><td>T1190: Exploit Public-Facing Application, T1040: Network Sniffing</td><td>https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36025</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36036	✗	Windows: 10 - 11 23H2, Windows Server: 2008 - 2022 23H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36036

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36038	✗	Visual Studio: 2022 version 17.2 – 2022, version 17.7, ASP.NET Core: 8.0 .NET: 8.0.0	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:visual_studio:2022:version17.7:*:*:*:*:*:*	-
ASP.NET Core Denial of Service Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1574: Hijack Execution Flow	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36038

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36413	✗	Microsoft Office: 2016 – 2019, Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions, Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:microsoft_office:2019:*:*:*:*:*:*:*	-
Microsoft Office Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36413

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-34060	✗	VMware Cloud Director: 10.5.0	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:vCloud_Director:10.5.0:*:*:*:*:*:*:*	-
VMware Cloud Director Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	WORKAROUND
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://kb.vmware.com/s/article/95534

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-37580	✗	Zimbra Collaboration (ZCS): 8.8.15 - 8.8.15	Winter Vivern
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zimbra:zimbra:*:*:*:*:*:*:*:*	-
Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1189: Drive-by Compromise, T1204: User Execution, T1059.007: JavaScript	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P41 https://wiki.zimbra.com/wiki/Security_Center

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-6345	✗	Google Chrome 100.0.4896.60 – 119.0.6045.160	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Skia Integer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1059: Command and Scripting Interpreter	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-49103	✗	ownCloud graphapi 0.2.0 – 0.3.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:owncloud:graphapi:*:*:*:*:*:*:*	-
ownCloud graphapi app Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1598: Phishing for Information	https://marketplace.owncloud.com/apps/graphapi , https://marketplace.owncloud.com/apps/oauth2 , https://owncloud.com/download-server

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LockBit ransomware	LockBit ransomware is malicious software designed to block user access to computer systems in exchange for a ransom payment. LockBit will automatically vet for valuable targets, spread the infection, and encrypt all accessible computer systems on a network. This ransomware is used for highly targeted attacks against enterprises and other organizations.	Exploiting Vulnerability	CVE-2023-4966 CVE-2023-4967
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware-as-a-Service		Block User Access, Encrypt data	Citrix NetScaler ADC and NetScaler Gateway
ASSOCIATED ACTOR			**PATCH LINK**
-			https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LIONTAIL	LIONTAIL is a passive loader that uses undocumented functionalities of the HTTP.sys driver to load incoming payloads. It is highly customizable and allows attackers to evade detection.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Passive loader		Data theft and Financial Losses	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Scarred Manticore			-

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
HelloKitty	HelloKitty emerged as a ransomware variant in late 2020, focusing mainly on Windows systems and gaining a reputation for its agility in adopting new Tactics, Techniques, and Procedures (TTPs). It utilized a Golang-based packer to enhance its ability to evade detection. By early 2021, a Linux version of HelloKitty had been spotted operating in the wild.	-	CVE-2023-46604
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft and Financial Losses	Apache ActiveMQ
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
-			https://activemq.apache.org/securityadvisories.data/CVE-2023-46604

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TellYouThePass ransomware	Tellyouthepass is one of many ransomware-type programs used to block access to files by encryption and keep them in this state unless a ransom is paid. The program renames all encrypted files by adding the ".locked" extension and creates a ransom message in a text file called "README.html".	Exploiting Vulnerability	CVE-2023-46604
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt data	Apache ActiveMQ
ASSOCIATED ACTOR			PATCH LINK
-			https://activemq.apache.org/security-advisories.data/CVE-2023-46604

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
SparkRAT	SparkRAT is an open-source RAT malware that is publicly available on GitHub. Notable for being developed with GoLang, SparkRAT provides basic features commonly found in RAT malware, such as executing commands, stealing information, and controlling processes and files.	Exploiting Vulnerability	CVE-2023-46604
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Execute commands, steal data	Apache ActiveMQ
ASSOCIATED ACTOR			**PATCH LINK**
-			https://activemq.apache.org/security-advisories.data/CVE-2023-46604

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Socks5Systemz	It is written in C++ and primarily sets up SOCKS5 proxies on victim computers that can then be used by threat actors to tunnel/hide the malicious traffic associated with other malware.	Phishing, exploit kits, malvertising, trojanized executables	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Retrieve data from the C2 servers	-
Proxy botnet			
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
PrivateLoader	PrivateLoader is a modular malware whose main capability is to download and execute one or several payloads. The loader implements anti-analysis techniques, fingerprints the compromised host and reports statistics to its C2 server.	Phishing, exploit kits, malvertising, trojanized executables	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Download and execute payloads	-
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Amadey	Amadey is being sold for about $500 on Russian-speaking hacking forums. It periodically sends information about the system and installed AV software to its C2 server and polls to receive orders from it. Its main functionality is that it can load other payloads for targeted computers compromised by the malware.	Phishing, exploit kits, malvertising, trojanized executables	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Deliver multiple malwares, update copies of itself	-
Loader			
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.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="3">Jupyter Infostealer</td><td rowspan="7">Jupyter Infostealer is a malware variant that changing its delivery method to evade detection, use SEO poisoning to encourage malicious file downloads. The malware has demonstrated credential harvesting and encrypted C2 communication capabilities used to exfiltrate sensitive data.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td rowspan="5">Data Theft</td><td rowspan="3">-</td></tr>
<tr><td><b>TYPE</b></td></tr>
<tr><td>Infostealer</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">MultiLayer</td><td rowspan="6">Multilayer is .NET based wiper, it can destroy local as well as network files; utilizes timestomping technique and delete system logs to cover its track.</td><td>Exploiting vulnerable internet facing web servers</td><td>-</td></tr>
<tr><td rowspan="2"><b>IMPACT</b></td><td rowspan="2"><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td><b>TYPE</b></td></tr>
<tr><td>Wiper</td><td rowspan="3">Wipes system data</td><td>-</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Agrius</td><td>-</td></tr>
</table>

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PartialWasher	PartialWasher is a data-wiping tool which is coded in C++. It supports command-line arguments	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Wiper		Wipes data	-
ASSOCIATED ACTOR			**PATCH LINK**
Agrius			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BFG Agonizer	BFG Agonizeris an wiper. It has code similarities with CRYLINE-v5.0. It circumvent security measures by employing anti-hooking techniques.	Exploiting vulnerable internet facing web servers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Wiper		Destroys system	-
ASSOCIATED ACTOR			**PATCH LINK**
Agrius			-

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
Sqlextractor	It is a custom tool to extract information from database servers. Its purpose is to query SQL databases and extract sensitive PII data, such as ID numbers, Passport scans, Emails, Full addresses.	Exploiting vulnerable internet facing web servers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Obtains sensitive data	-
ASSOCIATED ACTOR			**PATCH LINK**
Agrius			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ObjCShellz	The malware, written in Objective-C, operates as a remote shell, enabling attackers to execute commands on compromised systems. It communicates with its C2 server using a POST request, providing information about the victim's macOS version.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Executes custom commands	-
ASSOCIATED ACTOR			**PATCH LINK**
BlueNorOff			-

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
RustBucket	RustBucket is a new malware family that targets macOS systems. RustBucket is a multi-stage malware that uses a variety of techniques to infect its victims, including phishing emails, malicious websites, and drive-by downloads.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal sensitive information and install other malware	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			
BlueNorOff			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AllaKore RAT	AllaKore RAT is an open-source remote access tool which has been modified for the purposes of SideCopy operations and is commonly observed in their intrusions.	Exploiting Vulnerability	CVE-2023-38831
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Keylogging, screenshotting, and gain remote access	WinRAR
ASSOCIATED ACTOR			PATCH LINK
SideCopy			Update WinRAR to latest version 6.23 and later.

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
Ares RAT	Its is type of malicious software that allows an attacker to remotely control and monitor a victim’s computer.	Phishing	CVE-2023-38831
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal data	WinRAR
RAT			PATCH LINK
ASSOCIATED ACTOR			Update WinRAR to latest version 6.23 and later.
SideCopy			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DRat	DRat is capable of parsing as many as 13 commands from the C2 server to gather system data, download and execute additional payloads, and perform other file operations.	Exploiting Vulnerability	CVE-2023-38831
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Download and execute payload	WinRAR
ASSOCIATED ACTOR			PATCH LINK
SideCopy			Update WinRAR to latest version 6.23 and later.

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
Key RAT	Key RAT is a Windows based Remote Access Trojan, used by Threat Actor SideCopy in a campaign along side Ares RAT.	Exploiting Vulnerability	CVE-2023-38831
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Steal data	WinRAR
RAT			**PATCH LINK**
ASSOCIATED ACTOR			Update WinRAR to latest version 6.23 and later.
SideCopy			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Millenium RAT	The Millenium RAT, a Win32 executable built on .NET, specifically version 2.4, can be found on GitHub and is available for purchase for $30, granting lifetime access.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Collect user data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlazeStealer	The BlazeStealer payload can extract a malicious script from an external source, giving attackers complete control over the victim's computer. BlazeStealer runs a bot carried via the Discord messaging service using a unique identifier.	-	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Download files, deactivate Windows Defender and Task Manager, and lock a computer by overloading the CPU	-
Stealer			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

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
Nokoyawa	Nokoyawa Ransomware, first discovered in February 2022, is written in Rust making it cross-platform and found to be sharing code with Karma ransomware family. It employs double-extortion technique.	-	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Encrypts data	-
Ransomware			**PATCH LINK**
ASSOCIATED ACTOR			-
farnetwork			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JSWORM	JSWORM is a malicious program classified as ransomware: a program designed to encrypt data and deliver a ransom-demand message. When a computer is infected with a virus of this type, the victim loses access to stored data.	-	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Encrypts data	-
Ransomware			**PATCH LINK**
ASSOCIATED ACTOR			-
farnetwork			

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
Nefilim	Nefilim is a Ransomware as a Service(RaaS) operation first discovered in March 2020. Nefilim ransomware replaces the original files with encrypted versions.	-	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Encrypt Data	-
Ransomware			**PATCH LINK**
ASSOCIATED ACTOR			-
farnetwork			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Karma	Karma is a type of malware that encrypts your files and demands a ransom payment to decrypt them. This ransomware is particularly dangerous because it uses strong encryption algorithms that make it very difficult to recover your files without paying the ransom.	-	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Encrypt Data	-
Ransomware			**PATCH LINK**
ASSOCIATED ACTOR			-
farnetwork			

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
Nemty	Nemty is ransomware with an unusually complex encryption algorithm. This malware encrypts user files and demands money so that they can be unlocked again.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Encrypt data	-
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
farnetwork			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FakeBat	It is a malicious software loader and dropper that associated with malvertising campaigns.	Google Ads	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Distribute infostealers	-
Loader			PATCH LINK
ASSOCIATED ACTOR			-
-			

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="3">Redline stealer</td><td rowspan="7">Redline is a potent information-stealing malware designed to harvest sensitive data, including passwords, cookies, and cryptocurrency-related information.</td><td>-</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td rowspan="5">Harvest information</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td rowspan="2"><b>PATCH LINK</b></td></tr>
<tr><td>Infostealer</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td rowspan="2">-</td></tr>
<tr><td>-</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="3">Clop ransomware</td><td rowspan="7">Clop Ransomware is a dangerous file encrypting virus which actively avoids the security unprotected system and encrypts the saved files by planting the .Clop extension. It exploits AES cipher to encrypt pictures, videos, music, databases papers.</td><td>-</td><td>CVE-2023-47246</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td rowspan="5">Encrypt data</td><td>SysAid</td></tr>
<tr><td><b>TYPE</b></td><td rowspan="2"><b>PATCH LINK</b></td></tr>
<tr><td>Ransomware</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td rowspan="2">https://documentation.sysaid.com/docs/latest-version-installation-files</td></tr>
<tr><td>Lace Tempest</td></tr>
</table>

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Gracewire (aka FlawedGrace)	It is written in C++. It seems to have been developed in the second half of 2017. GraceWire infections can result in financial loss, serious privacy issues and identity theft.	-	CVE-2023-47246
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data theft	SysAid
ASSOCIATED ACTOR			**PATCH LINK**
Lace Tempest			https://documentation.sysaid.com/docs/latest-version-installation-files

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Ducktail	Ducktail info stealer propagated by masquerading as documents related to projects and products of well-known companies and brands. A distinctive feature of this campaign was the use of Delphi as the programming language, deviating from the previous approach that relied on .NET applications.	Spear-phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Extortion of data	-
ASSOCIATED ACTOR			**PATH 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
IronWind	TA402 orchestrated a phishing campaign, deploying a file named PPAM. Within this file were three distinct components, facilitating the deployment of a novel initial access downloader known as IronWind. The infiltration of IronWind occurred through the use of timeout.exe. Subsequently, IronWind initiated communication with a C2 domain via an HTTP GET request.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Denial of Service, Data Theft, and compromised systems	-
ASSOCIATED ACTOR			**PATCH LINK**
TA402			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SharpSploit	The IronWind downloader is designed to establish a connection with a server controlled by the attacker for the retrieval of additional payloads. Among these payloads is a post-exploitation toolkit called SharpSploit, a .NET post-exploitation library written in C#. This process unfolds in a multi-stage sequence	Spear phishing and IronWind	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Toolkit		Denial of Service, Data Theft, and compromised systems	-
ASSOCIATED ACTOR			**PATCH LINKS**
TA402			-

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
NoEscape	The NoEscape ransomware, suspected to be a rebrand of Avaddon, targets enterprises globally through multi-extortion attacks. Operating as Ransomware-as-a-Service, it encrypts files, changes wallpapers, and demands ransom, emphasizing financial motives via a TOR negotiation site.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft and Espionage	Windows, Linux, and ESXi
ASSOCIATED ACTOR			**PATCH LINKS**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GhostLocker	GhostSec, a hacktivist group, has introduced GhostLocker, an advanced Ransomware-as-a-Service (RaaS) framework. GhostSec used Python to develop their encryptor, utilizing PyInstaller to package Python code into standalone executable applications compatible with various operating systems. Recent versions of GhostLocker are compiled using Nuitka, a tool that translates Python programs into C binaries.	Phishing, Affiliate Programs, Darkweb Marketplace	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Modular		Data Theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINKS**
GhostSec			-

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
BlackCat (aka AlphaV, AlphaVM, ALPHV-ng, Noberus)	The BlackCat ransomware gained attention for its utilization of the Rust programming language and its adoption of a Ransomware-as-a-Service (RaaS) business model. BlackCat is highly customizable, allowing it to be tailored for the creation of targeted executables.	Social engineering expertise, phishing, and SIM swap attacks,	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, compromised systems and Espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
Scattered Spider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AveMaria (aka AVE_MARIA, AveMariaRAT, Warzone RAT, WarzoneRAT)	The AveMaria RAT is a remote access trojan written in C++, offered as malware-as-a-service. It possesses a diverse set of capabilities, ranging from stealing victims' files and passwords to capturing desktop activities. The RAT receives regular updates from its command and control (C2) server.	Social engineering expertise, phishing, and SIM swap attacks,	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft, compromised systems and Espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
Scattered Spider			-

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
Raccoon (aka Mohazo, Racealer)	Raccoon is an information-stealing malware available as a Malware-as-a-Service (MaaS). It can be acquired through a subscription, costing $200 per month. The Raccoon malware has already infected over 100,000 devices, making it one of the most discussed viruses on underground forums in 2019.	Social engineering expertise, phishing, and SIM swap attacks,	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Data Theft, compromised systems and Espionage	-
ASSOCIATED ACTOR			PATCH LINK
Scattered Spider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
VIDAR	Vidar is a dangerous malware that steals information and cryptocurrency from infected users. It derives its name from the ancient Scandinavian god of Vengeance. This stealer has been terrorizing the internet since 2018	Social engineering expertise, phishing, and SIM swap attacks,	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Data Theft, compromised systems and Espionage	-
ASSOCIATED ACTOR			PATCH LINK
Scattered Spider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LitterDrifter	LitterDrifter is a self-propagating worm written in VBScript that spreads through removable USB drives. It is believed to be developed by the Gamaredon APT group, which is linked to the Russian government.	USB drives	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal data, Disrupt operations	-
Worm			
ASSOCIATED ACTOR			PATCH LINK
Gamaredon			-

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
Kinsing (aka h2miner)	Kinsing malware is a type of Linux malware that has been around for several years. It is known for targeting containerized environments, such as Docker and Kubernetes, and for its ability to spread to other hosts. Kinsing is typically used to mine cryptocurrency, but it can also be used to steal data or launch other attacks.	Exploiting vulnerability	CVE-2023-46604
		IMPACT	AFFECTED PRODUCTS
TYPE		Performance degradation, Data breach, Denial-of-service attacks	ActiveMQ
Cryptocurrency miner			
ASSOCIATED ACTOR			PATCH LINK
-			https://activemq.apache.org/securityadvisories.data/CVE-2023-46604

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
NetSupport	NetSupport RAT is a that is based on a legitimate remote administration tool called NetSupport Manager. NetSupport Manager is a legitimate tool that is used by IT professionals to remotely control and manage computers. However, cybercriminals have been known to use modified versions of NetSupport Manager as RATs to gain unauthorized access to computers and steal data.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft, Installing malware	-
RAT			
ASSOCIATED ACTOR			PATCH LINK
TA569			-

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
Nim backdoor	Nim backdoor is actually a variant of the C++ backdoor and is written in the Nim programming language . A backdoor is a hidden way to access a system or application that is not intended for public use.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft, Spying on victims	-
ASSOCIATED ACTOR			**PATCH LINK**
SideWinder			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkGate	DarkGate is a commodity malware that is used in a variety of cyber attacks, including targeted attacks and mass attacks. DarkGate is a versatile malware that can be used to steal data, install additional malware, launch denial-of-service attacks, and take control of infected systems.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Launch DDoS attacks And Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
RastaFarEye			-

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
Atomic Stealer	Atomic, or AMOS, macOS information-stealing malware. It is currently being delivered to targets through a deceptive web browser update chain known as ClearFake. ClearFake is a recent malware campaign that exploits compromised websites to distribute fake browser updates.	Legitimate AnyDesk remote desktop software	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data theft	Mac OS
Infostealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LambLoad	LambLoad is a malware family that has been active since at least 2017. It is a downloader that is used in supply chain attacks. Supply chain attacks are attacks that target third-party suppliers to gain access to their customers' systems.	Supply chain attacks, Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Launch DDoS attacks And Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus Group			-

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
InfectedSlurs	InfectedSlurs is a new Mirai-based malware botnet, and is actively conducting a sophisticated campaign by exploiting two zero-day remote code execution (RCE) vulnerabilities in routers and video recorder (NVR) devices. These vulnerabilities, currently being exploited in the wild, facilitate the creation of a distributed denial-of-service (DDoS) botnet.	Exploiting vulnerabilities	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Launch DDoS attacks And Data Theft	-
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SwiftLoader	SwiftLoader is a backdoored PDF reader app, it secretly retrieves and executes secondary malware.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		steal cryptocurrency	macOS
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
KandyKorn	KandyKorn primarily targets macOS and is an Remote Access Trojan written in C++.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		steal cryptocurrency	macOS
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ParaSiteSnatcher	ParaSiteSnatcher is a malicious browser extension with ability to intercept HTTP requests enabling Threat Actors to manipulate and exfiltrate HTTP data.	Through a VBScript downloader	-
TYPE		IMPACT	AFFECTED PRODUCTS
Malicious Extension		Extract highly sensitive information	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Djvu	Djvu is a ransomware family initially identified in 2018 and linked to the STOP ransomware, utilizes various file extensions for naming encrypted files.	Disguise of cracked software	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data exfiltration and information theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cerber ransomware	Cerber Ransomware employs a ransomware-as-a-service model, enabling affiliates to purchase and operate. The latest variant encrypts data with the .L0CK3D extension.	Exploiting Vulnerability	CVE-2023-22518
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware-as-a-service		Encrypt data	Confluence Data Center, Confluence Server
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.

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5">Scarred Manticore</td><td>Iran</td><td rowspan="3">Government, Military, IT Service Providers, Financial Organizations, NGOs, and Telecommunications Sectors</td><td rowspan="3">Middle East</td></tr>
<tr><td><b>MOTIVE</b></td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td><b>TARGETED CVEs</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>-</td><td>LIONTAIL</td><td>Windows</td></tr>
<tr><td colspan="4"><b>TTPs</b></td></tr>
<tr><td colspan="4">TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1574: Hijack Execution Flow, T1078: Valid Accounts, T1543: Create or Modify System Process, T1003: OS Credential Dumping, T1082: System Information Discovery, T1005: Data from Local System, T1041: Exfiltration Over C2 Channel, T1490: Inhibit System Recovery, T1036: Masquerading, T1083: File and Directory Discovery, T1105: Ingress Tool Transfer</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm)	Iran	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation, Aerospace	Middle East, Asia, Africa, Europe, and North America
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	-	-

TTPs
TA0043: Reconnaissance, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0010: Exfiltration, TA0011: Command and Control, T1566: Phishing, T1566.002: Spearphishing Link, T1547: Boot or Logon Autostart: Execution, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1105: Ingress Tool Transfer, T1204: User Execution, T1204.002: Malicious File

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Kinsing (aka Money Libra)	-	Cryptocurrency	Worldwide
	MOTIVE		
	Information Theft		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-4911 CVE-2017-9841	-	GNU C Library (glibc), Oracle Communications Diameter Signaling Router
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0040: Impact; T1059: Command and Scripting Interpreter; T1059.006: Python; T1059.007: JavaScript; T1505: Server Software Component; T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1027: Obfuscated Files or Information; T1003: OS Credential Dumping; T1082: System Information; Discovery; T1083: File and Directory Discovery; T1140: Deobfuscate/Decode Files or Information; T1496: Resource Hijacking			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Agrius (aka Agonizing Serpens, DEV-0227, BlackShadow, SharpBoys, AMERICIUM, Pink Sandstorm)	Iran	Education, Technology	Hong Kong, Israel, South Africa
	MOTIVE		
	Information theft and espionage, Sabotage and destruction		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	MultiLayer, PartialWasher, BFG Agonizer, sqlextractor	-
TTPs			
TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0040:Impact; T1595: Active Scanning; T1190:Exploit Public-Facing Application; T1003: OS Credential Dumping; T1560: Archive CollectedData; T1490: Inhibit System Recovery; T1574: Hijack Execution Flow; T1059: Command and Scripting Interpreter; T1110: Brute Force; T1005: Data from Local System; T1041: Exfiltration Over C2 Channel; T1485: Data Destruction; T1561: Disk Wipe;			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
BlueNorOff (APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet, TAG-71)	North Korea	Cryptocurrency, Financial	-
	MOTIVE		
	Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	ObjCShellz, RustBucket	-

TTPs
TA0005: Defense Evasion; TA0010: Exfiltration; TA0011: Command and Control; TA0002: Execution; TA0040: Impact; TA0042: Resource Development; T1583: Acquire Infrastructure; T1583.001: Domains; T1059: Command and Scripting Interpreter; T1204: User Execution; T1204.001: Malicious Link; T1588.001: Malware; T1588: Obtain Capabilities; T1020: Automated Exfiltration; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
SideCopy	Pakistan	Government	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-38831	AllaKore RAT, Ares RAT, DRat, Key RAT	WinRAR
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583: Acquire Infrastructure; T1583.001: Domains; T1584: Compromise Infrastructure; T1584.001: Domains;T1588: Obtain Capabilities; T1588.001: Malware; T1588.002: Tool; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.005: Link Target; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1106: Native API; T1129: Shared Modules; T1059: Command and Scripting Interpreter; T1047: Windows Management Instrumentation;T1203: Exploitation for Client Execution; T1204: User Execution;T1204.001: Malicious Link;T1204.002: Malicious File; T1053: Scheduled Task/Job;T1053.003: Cron;T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder;T1547.013: XDG Autostart Entries; T1036: Masquerading;T1036.005: Match Legitimate Name or Location; T1140: Deobfuscate/Decode Files or Information;T1218: System Binary Proxy Execution;T1218.005: Mshta; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading;T1222: File and Directory Permissions Modification; T1222.002: Linux and Mac File and Directory Permissions Modification;T1027: Obfuscated Files or Information; T1027.009: Embedded Payloads;T1027.010: Command Obfuscation; T1012: Query Registry;T1033: System Owner/User Discovery; T1057: Process Discovery;T1082: System Information Discovery; T1083: File and Directory Discovery;T1016: System Network Configuration Discovery; T1016.001: Internet Connection Discovery;T1518: Software Discovery; T1518.001: Security Software Discovery;T1005: Data from Local System; T1056: Input Capture;T1056.001: Keylogging; T1074: Data Staged;T1074.001: Local Data Staging; T1119: Automated Collection; T1113: Screen Capture;T1125: Video Capture; T1105: Ingress Tool Transfer;T1571: Non-Standard Port; T1573: Encrypted Channel;T1071: Application Layer Protocol; T1071.001: Web Protocols;T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
farnetwork (aka farnetworkl, jingo, jsworm, razvrat, piparkuka, and farnetworkit)	-	Utilities, Construction, Engineering, Trading Companies, Healthcare, Hotels, Restaurants & leisure, Distributors, Road & rail, Media, Education Services, and Automotive	United States, Korea, Canada, Morocco, Saint Kitts and Nevis
	MOTIVE		
	Develop ransomware		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Nokoyawa, JSWORM, Nefilim, Karma, and Nemty	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059.001: PowerShell; T1027: Obfuscated Files or Information; T1083: File and Directory Discovery; T1113: Screen Capture; T1114: Email Collection; T1005: Data from Local System; T1490: Inhibit System Recovery; T1048: Exfiltration Over Alternative Protocol: T1486: Data Encrypted for Impact; T1491: Defacement; T1555: Credentials from Password Stores; T1059: Command and Scripting Interpreter

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Lace Tempest (aka DEV-0950, FIN11)	-	Defense, Education, Energy, Financial, Hospitality, Retail, Telecommunications, Technology, Transportation	Worldwide
	MOTIVE		
	Financial crime, Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-47246	Clop ransomware, Gracewire	SysAid servers

TTPs
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1059.001: PowerShell; T1543: Create or Modify System Process; T1505: Server Software Component; T1564: Hide Artifacts; T1059: Command and Scripting Interpreter; T1083: File and Directory Discovery; T1046: Network Service Discovery; T1057: Process Discovery; T1070: Indicator Removal; T1570: Lateral Tool Transfer; T1213: Data from Information Repositories; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TA402 (aka Extreme Jackal, Molerats, Gaza Cybergang, Gaza Hackers Team, Aluminum Saratoga, ATK 89, TAG-CT5)	Palestine	Government, Foreign Affairs	Middle East
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	IronWind, SharpSploit	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and: Control; T1059: Command and: Scripting Interpreter; T1072: Software Deployment: Tools; T1083: File and Directory: Discovery; T1082: System Information: Discovery; T1047: Windows Management Instrumentation; T1560: Archive Collected Data; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1543: Create or Modify System Process; T1204: User Execution

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Winter Vivern (aka UAC-0114, TA473)	Unknown	Government	Greece, Moldova, Tunisia, Vietnam, Pakistan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-37580	-	Zimbra Collaboration (ZCS)

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1588.005: Exploits; T1566: Phishing; T1059: Command and Scripting Interpreter; T1134: Access Token Manipulation; T1190: Exploit Public-Facing Application

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
GhostSec (aka Ghost Security)	Unknown	Telecommunications Companies, Surveillance Systems, and Internet Of Things (IoT) Devices.	Russia, Israel, Columbia, Iran, South Africa, Nigeria, Pakistan, Iraq, United Arab Emirates, Lebanon, France, Brazil, Sudan, Myanmar, Nicaragua, Philippines, Canada
	MOTIVE		
	Information theft, espionage and Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	GhostLocker	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1087.001: Local Account; T1659: Content Injection; T1543: Create or Modify System Process; T1560: Archive Collected Data; T1574: Hijack Execution Flow; T1057: Process Discovery; T1211: Exploitation for Defense Evasion; T1071.001: Web Protocols; T1059.006: Python; T1486: Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Scattered Spider (aka Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, and Muddled Libra)	Unknown	Commercial facilities, Telecommunications, Technology, and Business-Process Outsourcing (BPO)	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	BlackCat/ALPHV Ransomware, AveMaria, Raccoon Stealer, and VIDAR Stealer	-

TTPs

TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; TA0040: Impact; T1657: Financial Theft; T1567: Exfiltration Over Web Service; T1585.001: Social Media Accounts; T1585: Establish Accounts; T1566: Phishing; T1660: Phishing; T1566.004: Spearphishing Voice; T1199: Trusted Relationship; T1078.002: Domain Accounts; T1078: Valid Accounts; T1648: Serverless Execution; T1204: User Execution; T1136: Create Account; T1556.006: Multi-Factor Authentication; T1556: Modify Authentication Process; T1484.002: Domain Trust Modification; T1484: Domain Policy Modification; T1578.002: Create Cloud Instance; T1578: Modify Cloud Compute Infrastructure; T1656: Impersonation; T1606: Forge Web Credentials; T1621: Multi-Factor Authentication Request Generation; T1552.001: Credentials In Files; T1552.004: Private Keys; T1552: Unsecured Credentials; T1217: Browser Bookmark Discovery; T1538: Cloud Service Dashboard; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1539: Steal Web Session Cookie; T1021: Remote Services; T1021.007: Cloud Services; T1213.003: Code Repositories; T1213.002: Sharepoint; T1213: Data from Information Repositories; T1074: Data Staged; T1114:Email Collection; T1530: Data from Cloud Storage; T1219: Remote Access Software; T1486: Data Encrypted for Impact; T1567.002: Exfiltration to Cloud Storage

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Gamaredon (aka Primitive Bear, Winterflounder, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Shuckworm, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard)	Russia	Defense, Government, Law enforcement, NGOs and diplomats and journalists	Ukraine, USA, Vietnam, Chile, Poland, Germany, Hong Kong
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	LitterDrifter	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0011: Command and Control; T1140: Deobfuscate/Decode: Files or Information; T1027: Obfuscated Files or: Information; T1102: Web Service; T1008: Fallback Channels; T1053: Scheduled Task/Job; T1047: Windows Management: Instrumentation; T1071: Application Layer: Protocol; T1091: Replication Through: Removable Media			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TA569	Unknown	Education, Government, and Business Services	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	NetSupport RAT	-
TTPs			
T1204.002: User Execution: Malicious File; T1059.001: Command and Scripting Interpreter: PowerShell; T1055: Process Injection; T1027: Obfuscated Files or Information; T1041: Exfiltration Over C2 Channel; T1074.001: Data Staged: Local Data Staging; T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder; T1057: Process Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
SideWinder (aka Razor Tiger, Rattlesnake, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21)	India	Government	Bhutan, Nepal, and Myanmar
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	Nim backdoor	-
TTPs			
TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; TA0010: Exfiltration; T1598: Phishing for: Information; T1566.001: Spearphishing: Attachment; T1059: Command and: Scripting Interpreter; T1083: File and Directory: Discovery; T1057: Process Discovery; T1056: Input Capture; T1053: Scheduled Task/Job; T1204: User Execution; T1547: Boot or Logon: Autostart Execution; T1543: Create or Modify: System Process; T1211: Exploitation for: Defense Evasion; T1132: Data Encoding; T1041: Exfiltration Over C2: Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Mustang Panda (aka Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Earth Preta, Camaro Dragon, Stately Taurus)	China	Government	Philippines
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	-	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and: Control; T1566: Phishing; T1204: User Execution; T1204.002: Malicious File; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1036: Masquerading; T1547: Boot or Logon: Autostart Execution; T1547.001: Registry Run Keys /: Startup Folder			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
RastaFarEye	Unknown	-	United States, Europe, Regions in Asia, South America, and Africa
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	DarkGate	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; TA0010: Exfiltration; TA0040: Impact; T1566.001: Spearphishing: Attachment: T1566.002: Spearphishing Link; T1204.002: Malicious File; T1059.001: PowerShell; T1059.003: Windows Command: Shell; T1547.001: Registry Run Keys /: Startup Folder; T1055.012: Process Hollowing; T1543.003: Windows Service; T1027.002: Software Packing; T1027.007: Dynamic API: Resolution; T1027.009: Embedded Payloads; T1055.002: Portable Executable: Injection; T1574.002: DLL Side-Loading; T1622: Debugger Evasion; T1036.008: Masquerade File Type; T1555.003: Credentials from Web: Browsers; T1056.001: Keylogging; T1528: Steal Application: Access Token; T1010: Application Window: Discovery; T1217: Browser Bookmark: Discovery; T1083: File and Directory: Discovery; T1497.001: System Checks; T1614.001: System Language: Discovery; T1518.001: Security Software: Discovery; T1005: Data from Local: System; T1113: Screen Capture; T1115: Clipboard Data; T1071.001: Web Protocols; T1132.002: Non-Standard: Encoding; T1573.001: Symmetric: Cryptography; T1219: Remote Access: Software; T1041: Exfiltration Over C2: Channel; T1489: Service Stop

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
DarkCasino	Unknown	Cryptocurrency trading platforms, online casinos and network banks worldwide	Worldwide
	MOTIVE		
	Economic benefits		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-38831	-	RARLAB WinRAR
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0011:Command and Control; T1027: Obfuscated Files or Information; T1055: Process Injection; T1566: Phishing; T1140: Deobfuscate/Decode Files or Information; T1056: Input Capture; T1059: Command and Scripting Interpreter; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1105: Ingress Tool Transfer; T1204: User Execution; T1204.002: Malicious File; T1203: Exploitation for Client Execution			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)	North Korea	Media, Defense, Information Technology	Japan, Taiwan, Canada, and the United States
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	LambLoad	-
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1071.001: Web Protocols;T1059: Command and Scripting Interpreter;T1573.001: Symmetric Cryptography;T1098: Account Manipulation;T1566: Phishing; T1204: User Execution;T1047: Windows Management Instrumentation;T1543: Create or Modify System Process;T1574.002: DLL Side-Loading;T1070: Indicator Removal;T1573: Encrypted Channel;T1105: Ingress Tool Transfer; T1003: OS Credential Dumping; T1195.002: Compromise Software Supply Chain; T1195: Supply Chain Compromise; T1036: Masquerading			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Andariel (aka Silent Chollima, Stonefly, Plutonium, Onyx Sleet)	North Korea	Media, Defense, Information Technology	Japan, Taiwan, Canada, and the United States
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	LambLoad	-

TTPs
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1071.001: Web Protocols;T1059: Command and Scripting Interpreter;T1573.001: Symmetric Cryptography;T1098: Account Manipulation;T1566: Phishing; T1204: User Execution;T1047: Windows Management Instrumentation;T1543: Create or Modify System Process;T1574.002: DLL Side-Loading;T1070: Indicator Removal;T1573: Encrypted Channel;T1105: Ingress Tool Transfer; T1003: OS Credential Dumping; T1195.002: Compromise Software Supply Chain; T1195: Supply Chain Compromise; T1036: Masquerading

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1598: Phishing for Information	T1598.002: Spearphishing Attachment
		T1589.001: Information: Credentials
	T1589: Gather Victim Identity Information	
	T1595: Active Scanning	
TA0001: Initial Access	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits
		T1588.001: Malware
		T1588.002: Tool
		T1588.003: Code Signing Certificates
	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.005: Botnet
	T1584: Compromise Infrastructure	T1584.005: Botnet
		T1584.001: Domains
	T1585: Establish Accounts	T1585.001: Social Media Accounts
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.005: Link Target
		T1584.001: Domains
TA0002: Execution	T1059: Command and Scripting Interpreter	T1059.006: Python
		T1059.003: Windows Command Shell
		T1059.001: PowerShell
		T1059.007: JavaScript
		T1059.005: Visual Basic
		T1059.002: AppleScript
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1203: Exploitation for Client Execution	
	T1047: Windows Management Instrumentation	
	T1129: Shared Modules	
	T1106: Native API	
	T1072: Software Deployment Tools	
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1648: Serverless Execution	
	T1569: System Services	

Tactic	Technique	Sub-technique
TA0003: Persistence	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1505: Server Software Component	
	T1133: External Remote Services	
	T1098: Account Manipulation	
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.013: XDG Autostart Entries
		T1547.009: Shortcut Modification
	T1176: Browser Extensions	
	T1136: Create Account	
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
TA0004: Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1098: Account Manipulation	
	T1055: Process Injection	T1055.012: Process Hollowing
		T1055.002: Portable Executable Injection
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.009: Shortcut Modification
		T1547.013: XDG Autostart Entries
	T1068: Exploitation for Privilege Escalation	
	T1134: Access Token Manipulation	
	T1484: Domain Policy Modification	T1484.002: Domain Trust Modification
TA0005: Defense Evasion	T1620: Reflective Code Loading	
	T1202: Indirect Command Execution	
	T1140: Deobfuscate/Decode Files or Information	
	T1112: Modify Registry	
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1055: Process Injection	T1055.012: Process Hollowing
		T1055.002: Portable Executable Injection
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.008: Masquerade File Type
		T1036.003: Rename System Utilities
	T1622: Debugger Evasion	
	T1014: Rootkit	
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1564: Hide Artifacts	T1564.003: Hidden Window
	T1222: File and Directory Permissions Modification	T1222.002: Linux and Mac File and Directory Permissions Modification

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.011: Fileless Storage
		T1027.010: Command Obfuscation
		T1027.009: Embedded Payloads
		T1027.007: Dynamic API Resolution
	T1070: Indicator Removal	T1070.006: Timestomp
		T1070.004: File Deletion
		T1070.001: Clear Windows Event Logs
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1556: Modify Authentication Process	T1556.006: Multi-Factor Authentication
	T1134: Access Token Manipulation	
	T1211: Exploitation for Defense Evasion	
	T1484: Domain Policy Modification	T1484.002: Domain Trust Modification
	T1218: System Binary Proxy Execution	T1218.005: Mshta
		T1218.007: Msiexec
	T1578.002: Modify Cloud Compute Infrastructure: Create Cloud Instance	
TA0006: Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1040: Network Sniffing	
	T1003: OS Credential Dumping	T1003.001: LSASS Memory
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
		T1552.004: Unsecured Credentials: Private Keys
	T1110: Brute Force	
	T1056: Input Capture	T1056.001: Input Capture: Keylogging
	T1539: Steal Web Session Cookie	
	T1556: Modify Authentication Process	T1556.006: Multi-Factor Authentication
	T1528: Steal Application Access Token	
	T1212: Exploitation for Credential Access	
TA0007: Discovery	T1482: Domain Trust Discovery	
	T1135: Network Share Discovery	
	T1082: System Information Discovery	
	T1040: Network Sniffing	
	T1007: System Service Discovery	
	T1083: File and Directory Discovery	
	T1057: Process Discovery	
	T1033: System Owner/User Discovery	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1012: Query Registry	
	T1046: Network Service Discovery	
	T1049: System Network Connections Discovery	
	T1069: Permission Groups Discovery	
	T1010: Application Window Discovery	
	T1622: Debugger Evasion	
	T1018: Remote System Discovery	
	T1538: Cloud Service Dashboard	
	T1087: Account Discovery	T1087.001: Local Account
	T1217: Browser Information Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1016: System Network Configuration Discovery	T1016.001: Internet Connection Discovery
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1614.001: System Location Discovery: System Language Discovery	
TA0008: Lateral Movement	T1563: Remote Service Session Hijacking	
	T1210: Exploitation of Remote Services	
	T1091: Replication Through Removable Media	
	T1021: Remote Services	T1021.007: Cloud Services
		T1021.001: Remote Desktop Protocol
	T1570: Lateral Tool Transfer	
	T1072: Software Deployment Tools	
TA0009: Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1115: Clipboard Data	
	T1005: Data from Local System	
	T1125: Video Capture	
	T1119: Automated Collection	
	T1113: Screen Capture	
	T1074: Data Staged	T1074.001: Local Data Staging
	T1056: Input Capture	T1056.001: Keylogging
	T1123: Audio Capture	
	T1114: Email Collection	
	T1213: Data from Information Repositories	T1213.003: Code Repositories
		T1213.002: Sharepoint
	T1530: Data from Cloud Storage	
	T1185: Browser Session Hijacking	
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1020: Automated Exfiltration	
	T1048: Exfiltration Over Alternative Protocol	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage

Tactic	Technique	Sub-technique
TA0011: Command and Control	T1102: Web Service	
	T1095: Non-Application Layer Protocol	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.002: Non-Standard Encoding
		T1132.001: Standard Encoding
	T1071: Application Layer Protocol	T1071.004: DNS
		T1071.001: Web Protocols
	T1571: Non-Standard Port	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1659: Content Injection	
	T1219: Remote Access Software	
	T1008: Fallback Channels	
	T1001: Data Obfuscation	
TA0040: Impact	T1489: Service Stop	
	T1485: Data Destruction	
	T1490: Inhibit System Recovery	
	T1486: Data Encrypted for Impact	
	T1496: Resource Hijacking	
	T1561: Disk Wipe	
	T1498: Network Denial of Service	
	T1529: System Shutdown/Reboot	
	T1491: Defacement	
	T1657: Financial Theft	
	T1499: Endpoint Denial of Service	

Top 5 Takeaways

#1

In November, there were **eleven zero-day** vulnerabilities, and two were celebrity vulnerability. One of these vulnerabilities "Citrix Bleed" was exploited since August 2023.

#2

Throughout the month, various ransomware strains including LockBit ransomware, HelloKitty ransomware, TellYouThePass ransomware, Clop ransomware, NoEscape Ransomware, BlackCat/ALPHV Ransomware, actively targeting victims.

#3

There were a total of 20 active adversaries identified across multiple campaigns. Their focus was directed toward the following key industries: Government, Technology, Financial, Manufacturing, and Defence.

#4

Numerous malware families have been observed targeting victims worldwide. These include **AveMaria, Raccoon Stealer, VIDAR Stealer, GhostLocker, Ducktail, Atomic Stealer and LambLoad.**

#5

Finally, the critical zero-day vulnerability identified as **CVE-2023-38831** exploited by **DarkCasino** in phishing attacks, launching the final malicious payload, **DarkMe**.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **22 significant vulnerabilities** and block the indicators related to the **20 active threat actors, 52 active malware,** and **204 potential MITRE TTPs.**

Uni5 Users

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

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

Hive Pro Threat Advisories (NOVEMBER 2023)

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

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. This is also known as Celebrity Publicized Software Flaws.

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

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

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

Glossary:

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

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
LockBit ransomware	SHA256	27389c160ceee51ca1f2b111ca8b221dc75b71cc699789da65802dce082dfbb4, a5e6df754a4d3bb72f4d5c91d6b582e7e2c2f87ca838f5d976bc82384a5ad2d1, 67b05e96f47db0447da53beddbf9aff265cd02562c12428d787fdab0278ded2e, a2db758f099d8a6dec5fd500d033ce2fcd89b58b53d938fdb9d9cba2d91dba01, 2daa5fa152b627f5ae23d2e8fa4e3e399d4899729ad32f184e32d59fd4dd20ef
LIONTAIL	SHA256	daa362f070ba121b9a2fa3567abc345edcde33c54cabefa71dd2faad78c10c33, f4639c63fb01875946a4272c3515f005d558823311d0ee4c34896c2b6612259, 2097320e71990865f04b9484858d279875cf5c66a5f6d12c819a34e2385da88, 67560e05383e38b2fcc30df84f0792ad095d5594838087076b214d849cde954, 4f6351b8fb3f49ff0061ee6f338cd1af88893ed20e71e211e8adb6b90e50a3b8, f6c316e2385f2694d47e936b0ac4bc9b55e279d530dd5e805f0d963cb47c3c0d, 1485c0ed3e875cbdfc6786a5bd26d18ea9d31727deb8df290a1c00c780419a4, 8578bff36e3b02cc71495b647db88c67c3c5ca710b5a2bd539148550595d033, c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0, 9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0cb, e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d, a2598161e1efff623de6128ad8aafba9da0300b6f86e8c951e616bd19f0a572b, 7495c1ea421063845eb8f4599a1c17c105f700ca0671ca874c5aa5aef3764c1c, 6f0a38c9eb9171cd323b0f599b74ee571620bc3f34aa07435e7c5822663de60, 3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7, 1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb, b71aa5f27611a2089a5bbe34fd1aafb45bd71824b4f8c2465cf4754db746aa79, da450c639c9a50377233c0f195c3f6162beb253f320ed57d5c9bb9c7f0e83999

Attack Name	TYPE	VALUE
HelloKitty	SHA256	c3c0cf25d682e981c7ce1cc0a00fa2b8b46cce2fa49abe38bb412da21da99cb7, 8c226e1f640b570a4a542078a7db59bb1f1a55cf143782d93514e3bd86dc07a, 8177455ab89cc96f0c26bc42907da1a4f0b21fdc96a0cc96650843fd616551f4
	Email	service@hellokittycat[.]online
	IPv4	172.245.16[.]125
	URL	hxxp://172.245.16[.]125/m4.png, hxxp://172.245.16[.]125/m2.png
TellYouThePass ransomware	SHA256	460b096aaf535b0b8f0224da0f04c7f7997c62bf715839a8012c1e1154a38984, 7d6877eb8a3e2da1e8b06e2ed41604c6c3d5ced8293f7cc7e760ba972303bd0e, 2fc2d747847eb04561a435e65954f0103101e2190458eb3c125deda49326c597, 533abb3f876c5ffc7e3a76874b0c4a3b4995848fa9a278c8a988af90945ecdac, dedeb1640850a6ef21cc0efb5f1f96309f62dc10308c6b6c35a9cdadaaeffa13, 463ee4cee193b4e1eeee91df5c343658fb708ff2795146226dd779eb11580f58, 5c8710638fad8eeac382b0323461892a3e1a8865da3625403769a4378622077e, 7af5c37cc308a222f910d6a7b0759837f37e3270e22ce242a8b59ed4d7ec7ceb, 3e65437f910f1f4e93809b81c19942ef74aa250ae228caca0b278fc523ad47c5
SparkRAT	SHA256	e0b0fe364fe6118e0246d65eeb32a4b3d37c44737dd2aa8d2291af1482cbc99b, d5f2cefc53e8355fe26e8c87f6212abf3a345cd1b82af97ac0bc540fd9dd1ed7, bc140d13eb3190d51c46ad5855f32f908b7617ab5b40d38b4e64914733beff85, 51635f8a613a1d7823318453db03d64990bc4d1bbc98cdc2d0fa70f1c70ee1c0
Socks5Systemz	SHA256	fee88318e738b160cae22f6c0f16c634fd16dbf11b9fb93df5d380b6427ac18f
PrivateLoader	MD5	6cc7d9664c1a89c58549e57b5959bb38
	SHA1	85b665c501b9ab38710050e9a5c1b6d2e96acccc
	SHA256	27c1ed01c767f504642801a7e7a7de8d87dbc87dee88fbc5f6adb99f069afde4

Attack Name	TYPE	VALUE
Amadey	SHA256	68cf6c33c3a11405e8f66b1cd769ac4b9ed53fa702d06323d737f86bb238f0aa, 31fcc145a7951bdb76f7635a0b7bb4ca6649fd8b2e6d5a166dfac138a71200bc, 2260d1b05abe62e94794dfc3d91d34d4751c6ccbdd450c2d3bbf01cb1aa31eec, e865cb5fbed88a0ef8d09376530d4fd855358dba91fa3f3d1296fb03085e8e06, 3141087bc31d396d4151e1bf8b61254374b503faefe444f17316ac40ba5c845b, 39a5de74cb6a87c849ac4d30e9902368f6638f27b98149b13ee8c6e6c4dd646f, d6780e515a8143aa9d8097deae4cba874790690f6743c51f8e03a1af4cf7c0b8, 8a9dda4423be29f85da1210beb83aab506609b9c03fcefd7bf022bd97823a808, a6bd53b43ef7820cb928829288276a9dc67c2746b8e07f0e83413cfacd2edfea, 4b4e85691ca2565dff2b966ff4ad72d617bf65cf02b541add5c66fb8a6747385, b8df7f85014ca1cd332cb971f07e4f78356e9d8c55cfcda3d88ea3c82806c555, 8543412d724c9c2353dc04e956e594341ae71a8aa4cb65778cd77d117014a94d, 25fdb52a6c215c2d3f797ffd349a0d30526f2d5a2d3a6309ff257591f1cf8f00, d721fb8b3424db73480e0f470438275fdea19ec670d7b0107f40571d44612f9f, d3f2db4b59bc69967a1f9206c6f79420247c72bac298c840bbfedd75937bc6b2, 371c1e62cbc18626b2cc6ba6893b71e9a9d945fc5391b5b85ee4ff2b7500f11e, 61afafb954376565e69f6a48e335320c00d529bf0677fe150f1217bf1a7efce3, 1fb2e848188b19f262e131fe524d450413b8e739c50c252a40291e6434bf396b, 06fcfe784a220b6515b8db1471567625bd8150878b404c8c96954e37c556488e, 931008fbe82fffa6412e9539e6a32e309032e76bba0b112ef730a9551df80110

Attack Name	TYPE	VALUE
Jupyter Infostealer	SHA256	c03ff646f732bf3a13b52e4786828af05a211ad69674cc2c11089681bc67ece9, e7ded7fb9f1aa432a3eb598d00157afb67b201647da234f785397a117f046e34, 1d322817bea6534d8b55282eb227a1fcca076b9d60b8b2fa0d3f756f4e38085c, d7f8a922f22d105d5190e91efb592335d5ccdee0fe3615dc3863cdef90a97738, 6738651649eedf22d352fcb5bb3942125487d63c26d7243fee8a25d295187996, df3bba9d570e70caa2f7eb716d9c2c371b535171fee4320af359a85662c45af7, 31cff99a12e1f7b8ae8966021b305d9bf2e2b7276b5c6857bfc45e8d833868f7, 67ddf04e5f8d7668ce666d00af3b3d7212bff8ded5999d36d131a77a4d5bd890, 8dae48b2f3cb1a57d4aff42417bbeace09e7329e0e06c525140a8f65755075df, 23e725d71caa459c745bdad9267d6164096223a4f5f2df03a92d9b49b195386f, 631685a0368e3b2dccea434258beb18dddb47532c17144b455f4218215ba8ceb, cc3d26f0938038eaa113e22640f330275c791e997ff7e822101c174cb693cba0, 1d944510c663c8c452c1784920172d16af4fa1db8a47aba9a5af973665a02a5a, 4f97380eaf66818246136a840df90424e06d6a931a630a42581c0ef5d9825736, 3f55947c29d8b3c50038dd7756e4bb1edb3908318df6f0df082d311582cc7df9
MultiLayer	SHA256	38e406b17715b1b52ed8d8e4defdb5b79a4ddea9a3381a9f2276b00449ec8835, f65880ef9fec17da4142850e5e7d40ebfc58671f5d66395809977dd5027a6a3e
PartialWasher	SHA256	ec7dc5bfadce28b8a8944fb267642c6f713e5b19a9983d7c6f011ebe0f663097
BFG Agonizer	SHA256	c52525cd7d05bddb3ee17eb1ad6b5d6670254252b28b18a1451f604dfff932a4
sqlextractor	SHA256	a8e63550b56178ae5198c9cc5b704a8be4c8505fea887792b6d911e488592a7c

Attack Name	TYPE	VALUE
ObjCShellz	SHA256	ca6d8b8a84e40adb8949f37eef65315d1d25283583c0a65921414611e615b27d, cde067b700e5f39e276a104497bc3ae0a5677977376a1b4c87de3d03730000bf, 462f4ccc290b3cc87cdce2a82aa3f0cb48140a88b590ee175ef9c24180b545c7, fe31f8cba8fc3832da136778aa28c406bf8ef04b448cba076ff7f5f3b8be7683, 1219c2c14afd2db469b0ae479236ab45abd20f6092592b539e04ba7aceec25e2
RustBucket	SHA256	812c795908f38bdb5cc20487569e53e04dfda8ad87ebe7156f3fb2fed1ab0b9b, 9fb57fca174506e96e2eda8db31a193b7476ce076557ff10617cdcae4d5716aa, a43c3097adb0d82eceb867957b54cc29e863d983daa547102361c59c0ac2a804, 070b2723a925d0788ddc3e5e4a214b7c64c61d44e5d01ca5bbe589f45256aa56, aa109f4fe27ed1f69e78a5aeba5356618ba24d8188077f0361c25a2e0d88874c
AllaKore RAT	IP	38.242.149[.]89:61101
	SHA256	877dd8f41c3ba0172907fa90734fce8bcd39919bd24162788b47770da9b99a1b, afe63fb7f4841748dc56f20a2eb6a313eac613c22cdf23694af172c77af88a2d, 1c12c0c62642ebbab1fabc7bd56ffc9c1450e622f6d7ddba08b36ac3ad8b04e6, aad714bbff3546d3352baa53324c2f3e6be6ca61d5d397cc33b09ed470b4dda5, 58d88fd112acdf7161a83a29f4b74f6e697bb520c49e4ec740e9d46cacd33e8b, faa422583f5a7e7d7c02be9a26babe2554412caa46135069f5ebb8673e9ef87b, 4896f8e0166fd0a313727ee94a65fe3a641e2feed3055523e2330fb0028b2c16, c6e59cefdff4dfc83aebf8e4a7a054f6a0820f7f52ceb03566a837823d29a7c7, c1ef58bc181bd3175d8b2f023299d261d40642bced2692251eb254cf5fdc3182
Ares RAT	IP	38.242.220[.]166:9012, 161.97.151[.]220:7015
	SHA256	b88db92adab9bd72ef9a959de450aa1d4cad32415d0364832393820b355a238e,

Attack Name	TYPE	VALUE
Ares RAT	SHA256	6d911bfb01daa6f3acafd3ccb33b432d806c82b2b35c0c3408d822bf8c6b4c00, e93a7924bde0c145485edfa6307bdcbbba80972390f4fba35e57c215c20e8c43, 7cc6d203daa31ee9296848c85cfbd6f6e1b90126d9b02ab8b916922842b316a2, 8581920c2ddbce49fde6c18eab3853fc6ea30983215ab785fbd399d89c7bba7a, 1a763a883378ba1b4a22706267612ca7a19ff30217266622d2f094d7846c654f, 23ef884798a128d49ac864e9cfe49047d3d10e845ec330ab22f059f0d4e35436, f5dddb1cd616f63a21d85d5970b5826c803069ca83b21e9751d28579ee6ebfec, e750e151e11eba9d0ab2f814dd24b2d1551eaf9cb95ab99e951d66619159219e, bf399563930b4af267c2d415b5d5cb208c2eeb9a37536437c993a311e0211e95
DRat	IP	38.242.149[.]89:9828
	SHA256	a216a8fd3f38baaca464642c733148d158256ef5e8156fb70b61e1993fb2abb7, 3dbb8941df5873feafec4b679522a8c237ba16fa045b8332a77b965c5a9ba167, 81259df59d29c22b1c29f178041396605ad2cacd696afe10cd3ba5ffc08278a3, 2f908408f0584fc2f529620c1ac492e766f603ca90618f1d4943ec214018d86b, ff7ca2e01237a0eaaed1f4523069f4c167cf84029dc766157ab10304e9d8c315, 20b4d856ee4b11e2a859bd83d2cd0e0a8c92c739a9753b5c98ee36af27b017e3, 612a094dc4324cb185b17ec8ce76404768b5c620059b2d7fc99a2fdc43e3a182, ee26deb66c5dbcf66c0bcc6334826d203373fcd59a8db4ce0173ece660506267, 64937789f8faba1ef5eba05ba2c2ffaaf8bbc80c016efac1b377ffadf8677da9, 5d42a118f2f693c04e46ca7c89d4d10e8d2cf46ab2841d283d66c17859c0ee57, ec5f5674c3172d59252dac023e52f99f530c89c35bd2a03197a868fbf58d40f3
Key RAT	IP	207.180.192[.]77:6023

Attack Name	TYPE	VALUE
Key RAT	SHA256	df2426f378c8440ee906e3353513f57bd5e531b813e3d944ed85f995da1771e6, 28d45335ac6d45d1d7fbe9297f993dafce3dbc894c1719ca3f7f2ca458ec2c4d, 4a6e7e12ae447b26cc9f490a324ba1795444987e7a5a602a167ba0716ad8d911, 22b366c6bd4e5d8669f01a806eaf2a3aedcc77fb018ada01c31c5c7867b6be35, 6104be5bb34e14ebbeaa330085cd08dfca0782a2cca7099594cc85cf87dd6abc, c7b70220ffa115b777b782698bd435dedf7e4d5aaebabc2230b85b26b55d189c, 68597413352459cb460a08d9fcacfd7650c36223bd0bc3eaa42a1c2f9c2dd939, 9d34900d4d58aa60f09f6d428be018ac9d2850b05a432d371d1c236ae3e204b2, 7dcdc9d0722b6e103bd80394e8eee19d8201a67f387a1e24a9d0b6c260ecf5ec, 7636f7f8f573b806bd473e89a82d404fa692085b8ebd3d03238f69e61e20aa14
Millenium RAT	MD5	eba4be8ed0e9282976f8ee0b04fb2474
	SHA1	f4d698ece0ff6af36c1a2e9108ea475518df0aa7
	SHA256	6d207c1e954f9d60f693e17e63df73fb8e954d02544b5d52b8b18c4ab86a267e
BlazeStealer	SHA256	77e183e63c70a44e87277be35b63817e185efcf1b8ab46937626904923251bbe, fb58f3f04e149b97a01c16a3bfedcb0ff33dc476dbab469fe011e3a379f2b00a, 87fda7a9d8156a9b3ca3ea92173c9c5c5abbd4a7e9f17c1b81e8921914cd5306, ccec28cfab447c153bc82993857b2ae865eab73c996d4db705ab1df6f1f29c40, b6c51f8700c067604354dc3f41cafb76ac7e3235fa7983c7407e18729dd94187, 9c3637d925b3bb46ad68e7667e5958cc6e0926d9b12f022c6e0e990d63f45a9d, a0422225d67779574006c04bd95bb19c02c5dd94f0af009606d58cf0b3854d6d, 14288b82c089fd1edd66feef6b0ff656d723f2e893b8c2574495b64c48b762a5, 51d5f41603a4a311c63e3db5d1cf8d5ddba28aa5cdabff62cad9f646fce8b5da, 716df8c14081570de5489c54a6e1d87d28f5d9d6848ab2b11654a5a3fbb29880

Attack Name	TYPE	VALUE
Nokoyawa	MD5	8800e6f1501f69a0a04ce709e9fa251c, 1e4dd35b16ddc59c1ecf240c22b8a4c4, f23be19024fcc7c8f885dfa16634e6e7, a2313d7fdb2f8f5e5c1962e22b504a17, 46168ed7dbe33ffc4179974f8bf401aa, 2e936942613b9ef1a90b5216ef830fbf, feb7b1e0161df136c3d385bfd2d4b247, c159afb7d2111690326cad610776db34
JSWORM	SHA256	46761b8b727f3002d1c73fa6c8568ebcf2ec0066666251f66dcda9d4268e03e8
Nefilim	SHA256	08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641, 205ddcd3469193139e4b93c8f76ed6bdbbf5108e7bcd51b48753c22ee620276, 5da71f76b9caea411658b43370af339ca20d419670c755b9c1bfc263b78f07f1, 7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599, eacbf729bb96cf2eddac62806a555309d08a705f6084dd98c7cf93503927c34f, ee9ea85d37aa3a6bdc49a6edf39403d041f2155d724bd0659e6884746ea3a250, f51f128bca4dc6b0aa2355907998758a2e3ac808f14c30eb0b0902f71b04e3d5, fdaefa45c8679a161c6590b8f5bb735c12c9768172f81c930bb68c93a53002f7, 24ada19b269279612370bdf16f2becc1d5b7e0f69821050e2d9b48cfc874dca0, b8066b7ec376bc5928d78693d236dbf47414571df05f818a43fb5f52136e8f2e, 7de8ca88e240fb905fc2e8fd5db6c5af82d8e21556f0ae36d055f623128c3377, 7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599, 5da71f76b9caea411658b43370af339ca20d419670c755b9c1bfc263b78f07f1, 24f1b3b9562ffa9b87b1497397c3da9dffa9f872f96b77d2643b18f9846aafaa, b227fa0485e34511627a8a4a7d3f1abb6231517be62d022916273b7a51b80a17, 0125e74c95d3e2762f7e29dc833592f33d5ded892ba4708e2b519eb5f400c2ee, 08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641,

Attack Name	TYPE	VALUE
Nefilim	SHA256	fdaefa45c8679a161c6590b8f5bb735c12c9768172f81c930bb68c93a53002f7, 35a0bced28fd345f3ebfb37b6f9a20cc3ab36ab168e079498f3adb25b41e156f, 5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6, 3080b45bab3f804a297ec6d8f407ae762782fa092164f8ed4e106b1ee7e24953, ea6ced3730495e2231c1a755fcc1aefac7622ac4bd5e269b2a5996572acb42f9, 2e25bdd600695cfed0d4ee3aca4f121bfebf0de889593e6ba06282845cf39ea, d4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3, 5104b8abb22cca1b078dd5b86e61f515a73404b0269fe7e6765ec818fbdf830b, 2b4b2a707662973236ae9b2fc732533b5d7236b279a2fccb2874da07e09af4b3, 7d7c44f9c577c0af913d905b51797f17399d650de0331885abc8828c2696d37f, 8b35aa930dd7260060f12ff92f1447850fc1a6bd79a28ba05a2d4e54a3aad504, fd3c8be2d1ead92101e8909a85695a0a40c2576c87eefeef6d32376a7fe22f1c, fcc2921020690a58c60eba35df885e575669e9803212f7791d7e1956f9bf8020, 3bac058dbea51f52ce154fed0325fd835f35c1cd521462ce048b41c9b099e1e5, 8be1c54a1a4d07c84b7454e789a26f04a30ca09933b41475423167e232abea2b, 353ee5805bc5c7a98fb5d522b15743055484dc47144535628d102a4098532cd5
Karma	SHA256	a63937d94b4d0576c083398497f35abc2ed116138bd22fad4aec5714f83371b0, 3ff1b90dbad5d78397fdc731c3a3c080d91fc488ac9152793b538b74a1e2d8f3, 4dec9a9044631caef283c7f39a576e4e5c1cc1e6a97ce5c60936a3a3d0097818, 124f3a5caf6eb464027f2865225a6a1238c3639e5b4a399f0f7f2dda7bd75aec, 0d037ee0252e4f26800bcf7c750f61d0c549b7ba0a522c75e8d96dcf4f689e27, 1c41acdc2e9d8b89522ebb51d65b4c41d7fd130a14ce9d449edb05f53bbb8d59, ad841882052c3f9d856ad9a393232e0a59d28e17c240d23258f1dac62f903ab8, 19417c0a38a1206007a0cc82c0fc2e19db897214d27d0998bc4dbac53cc2788d,

Attack Name	TYPE	VALUE
Karma	SHA256	a63937d94b4d0576c083398497f35abc2ed116138bd22fad4aec5714f83371b0, 34629751d8202be456dcf149b516afefc980a9128dd6096fd6286fee530a0d20, 0d037ee0252e4f26800bcf7c750f61d0c549b7ba0a522c75e8d96dcf4f689e27, 6c98d424ab1b9bfba683eda340fef6540ffe4ec4634f4b95cf9c70fe4ab2de90
Nemty	SHA256	267a9dcf77c33a1af362e2080aaacc01a7ca075658beb002ab41e0712ffe066e, 064debda941fb6b1ac7de62e4990f658ded67870f55f48757ab72a772c640995, 17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae, c41f14cf5a0c8d407b70cf07f552a5ba26db3b23bfdbfae7b24e7ff8de7ec1a7, dd228f63f0ef02749759ef6d75f9f84d5ba8b0787dadef0d41b390176ea5d6a1, 4cf87dd16d57582719a8fe6a144360f3dfa5d21196711dc140ce1a738ab9816e, abf148370f7cc9c16e20c30590a08f85208f4e594062c8a9e59c0c89cd8ff43f, ddadfcc43e4576de65f5844396a08fec47410663a6b6921991206b7a0df32ada, 57e25a37d8279fe563415d636b1983d447b5521ec6c024e18fd4d578840d2e20, 9913afe01dc4094bd3c5ff90ca27cc9e9ef7d77b6a7bdbf5f3042a8251b96325, 1d828a6c85bd5896ea27eeb17483dfe3bef81e0bf31521c91bcdf2559a03da1f, 31ee05823a66851cf6965f32d02e767206785d0bf0c9fa65e7dcf1ffed32c18e, 12da8dee83df90880d7d9cb4b0a7b608950bb57e9bc59c8b96f68c364350447c, d809ab5906fe6dba964cb30a21753213f5b077e28abb67680b2f28d65cbfc83b, a7558decb9516122781243e791c982977660152813817fb7ed00359365fcb0d3, e410854d9c8afe6e691c0ae638dfd04d792c3745dbb9e335f6f949e7a6b298d8, 5439452012a052851fdd0625abc4559302b9d4f4580e2ec98680e9947841d75d, a9f6d5ad40d5b073be92fc46666ce1f96e30c50494a018d472cfee56ff2b8c65, a5590a987d125a8ca6629e33e3ff1f3eb7d5f41f62133025d3476e1a6e4c6130,

Attack Name	TYPE	VALUE
Nemty	SHA256	3a061909a2631041b16d1d57212c1f44baca897efce50d095a141f8b7563db0b, 17864c4e21c0ebaf30cca1f35d67f46d3c3c33a5b8ea87d4c331e9d86d805965, a127323192abed93aed53648d03ca84de3b5b006b641033eb46a520b7a3c16fc, 2c41b93add9ac5080a12bf93966470f8ab3bde003001492a10f63758867f2a88, b227fa0485e34511627a8a4a7d3f1abb6231517be62d022916273b7a51b80a17, b8066b7ec376bc5928d78693d236dbf47414571df05f818a43fb5f52136e8f2e, 7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599, fcc2921020690a58c60eba35df885e575669e9803212f7791d7e1956f9bf8020, 8be1c54a1a4d07c84b7454e789a26f04a30ca09933b41475423167e232abea2b, 3080b45bab3f804a297ec6d8f407ae762782fa092164f8ed4e106b1ee7e24953, 5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6, d4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3, 35a0bced28fd345f3ebfb37b6f9a20cc3ab36ab168e079498f3adb25b41e156f, 08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641, 3bac058dbea51f52ce154fed0325fd835f35c1cd521462ce048b41c9b099e1e5, 353ee5805bc5c7a98fb5d522b15743055484dc47144535628d102a4098532cd5, 52e25bdd600695cfed0d4ee3aca4f121bfebf0de889593e6ba06282845cf39ea, 7de8ca88e240fb905fc2e8fd5db6c5af82d8e21556f0ae36d055f623128c3377
FakeBat	SHA256	a80846156595af47a977182395583d0b981e091d1281258e81860a0edfdd0159, a1f64f609b0d28707f2132e54d3a19d80f36806557a6031cd8f3154fb8a559be, a80846156595af47a977182395583d0b981e091d1281258e81860a0edfdd0159, 37620313dd1e5277a53e3dcef980e29b2315f4fafe7376fc1a2b941432c0de39, d9c62b110e0049f7ca3f0ccaa7d0058adad9cfdca27b8ab240ec0db70a8a2193

Attack Name	TYPE	VALUE
Redline stealer	SHA256	9f9b6cf7810c6aaadde785a65dd4c7f941c14ec4de7f68ecc6964353fa02e01e, 80af7bf074366eb628c1b08f30f3a8ec1ce44546cf119b7111b546acedec7059, 5d50717f5a866456842ee76543682f0f500619c4f7b12c548be9ea1c0e9c981b, 78dd1b88bea0150d68adb20296c9d819cabb3c587448e046558f97851655b262, 7b867d7b59955eaf09166f3c519b468661dcce3fc54ad63e24db14a26265a080
Clop ransomware	MD5	31e0439e6ef1dd29c0db6d96bac59446, 4431b6302b7d5b1098a61469bdfca982, 5e52f75d17c80dd104ce0da05fdfc362, 8bd774fbc6f846992abda69ddabc3fb7, afe7f87478ba6dfca15839f958e9b2ef, dd5cee48cdd586045c5fb059a1120e15, f59d2a3c925f331aae7437dd7ac1a7c8
	SHA1	40b7b386c2c6944a6571c6dcfb23aaae026e8e82, 46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5, 4fa2b95b7cde72ff81554cfbddc31bbf77530d4d, 77ea0fd635a37194efc1f3e0f5012a4704992b0e, a1a628cca993f9455d22ca2c248ddca7e743683e, a6e940b1bd92864b742fbd5ed9b2ef763d788ea7, ac71b646b0237b487c08478736b58f208a98eebf, ba5c5b5cbd6abdf64131722240703fb585ee8b56
Gracewire	MD5	88695dbddd4fc57025b523f4fca268d7, 80a20106ced1a5d9f350b1401dbe7d14
	SHA1	57ab5d9b5302644e91e3953062b40c5346b236e3, 753561bf6da3cbb75711d109ed0e38b7abb28db8
	SHA256	f92dbf7943590c2c4011f911ba9ba445010c9d5895b5c8b57a5da9c8708c221d, 6d15a0807858dce0be652e480fa7f298482c7bbf2c1e116e6cf0a3d3df95180f
Ducktail	SHA256	8eafccab8c6a80356c84c9ae3bd3603262069748be59a8d5aee4dfa3cf4a00a3, 9cf88cfd198e0070bb24868ce56f260f55a4b227e266ebcb37fdb83183299ae5, c2e8bc6389ba6ba32a350312f4fdda33628c806587ade0836f3886e2ffcaf9b2, 3097d80d4aa3abf2599058bf58d85aa8cec6ca6894c13c6d360dce162a5dd626, 1663d092935809dd5f3f0049463f4367ded67f2253b039d9b0c05510b2e4c94e

Attack Name	TYPE	VALUE
IronWind	SHA256	9b2a16cbe5af12b486d31b68ef397d6bc48b2736e6b388ad8895b588f1831f47, 4018b462f2fcf1b0452ecd88ab64ddc5647d1857481f50fa915070f5f1858115, e2ba2d3d2c1f0b5143d1cd291f6a09abe1c53e570800d8ae43622426c1c4343c
SharpSploit	SHA256	26cb6055be1ee503f87d040c84c0a7cacb245b4182445e3eee47ed6e073eca47, ac227dd5c97a36f54e4fa02df4e4c0339b513e4f8049616e2a815a108e34552f, 6ab5a0b7080e783bba9b3ec53889e82ca4f2d304e67bd139aa267c22c281a368, 81fc4a5b1d22efba961baa695aa53201397505e2a6024743ed58da7bf0b4a97f, 3b2a6c7a39f49e790286185f2d078e17844df1349b713f278ecef1defb4d6b04, 7bddde9708118f709b063da526640a4132718d3d638505aafce5a20d404b2761
NoEscape	SHA256	0073414c5a03b20f6f255f400291de67f2a7268c461f90ea6ff0355ca31af07a, 2020cae5115b6980d6423d59492b99e6aaa945a2230b7379c2f8ae3f54e1efd5, 4175dae9b268fe5b4f96055ea0376417b5ddc2518d3bd11e20f0f8255bb4621e, 4d7da1654f9047b6c6a9d32564a66684407ed587cbaffa54ec1185fd73293d3e, 5300d7456183c470a40267da9cd1771d6147445b203d8eb02437348bf3169e0d, 53f5c2f70374696ff12adcaaf1bbbe0e5dd1b1995d98f2e876b0671888b43128, 62205bf0a23e56524f2f1c44897f809457ad26bc70810008ec5486e17c7e64e2, 68bce3a400721d758560273ae024f61603b8a4986440a8ec9e28305d7e6d02b0, 68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccd2bc0d8, 73c19eab8d2ae58db3968dd7de0e745db2d7709859305b113b748bb02494465e, 831a2409d45d0c7f15b7f31eddbbdfe7d58414499e81b3da7d9fdee28fafe646, 8dd64ea7f226d3eb1e857b0086c0668542652cb37f8142dc000272dbd9569e31, 91c515d55fae6d21b106c8c55067ce53d42bef256bd5a385cadd104cf68f64ff,

Attack Name	TYPE	VALUE
NoEscape	SHA256	9d346518330eeefbf288aeca7b2b6243bc158415c7fee3f2c19694f0e5f7d51c, 10d2b5f7d8966d5baeb06971dd154dc378496f4e5faf6d33e4861cd7a26c91d7, 21162bbd796ad2bf9954265276bfebea8741596e8fe9d86070245d9b5f9db6da, 46f1a4c77896f38a387f785b2af535f8c29d40a105b63a259d295cb14d36a561, c34c5dd4a58048d7fd164e500c014d16befa956c0bce7cae559081d57f63a243
	SHA1	ea1f7940271fc80d06b2f222506020b650ad41bc, 30f71a24c15dd81965b12996a79d914acf4f169e, 12dc0a2de3ad30201107bfcb679de5acacf31e5c, 30c60f18279ed5fd36e3ac2d3ba5ddbdc5d1f624, 9cbc7417fa5ce2f6d87026337fc7892e4f485819, d38c613020cb4616783c8535380e28404f7eaebf, b17403e7dcb992ba8d2b56dd843406264d3910e5, 317f296131b37a73c9a5d253015821dfdc8b1190
	MD5	204f028c983f654be32b97e849edeaab, 47ae17d89c2d9b6acdc7458f5df1c6f7, 5779cec690b5bbc61687381ae8a8d518, 58b4a4eed74fbfbf104d0ffd92207018, a106c1236357c315722ddbd985c5613c, c850f6816459e3364b2a54239642101b
GhostLocker	SHA256	7e14d88f60fe80f8fa27076566fd77e51c7d04674973a564202b4a7cbfaf2778, ee227cdOef308287bc536a3955fd8138&16a0228ac42140e9M308ae6343a3f, Oe484560a909fc06b9987db73346eaoca6750d523f2334913c23e061695f5cc, abac31b5527803a89c941cf24280a9653oee898a7a338424bd3e9b15d792972, 663ac2d887df18e6da97dd358ebd2bca55404fd4a1C8CIC51215834fc6d11b33, 9b6be74c2c144f8bcb92c8350855d35C14bb7f2b727551C3dd5C8054c4136e3f, ee227cdOef308287bc536a3955fd81388a16a0228ac42140e9cf308ae6343a3f, 0e484560a909fc06b9987db73346efaOca6750d5232334913c23e061695f5cc, abac31b5527803a89c941cf24280a9653cdee898a7a338424bd3e9b15d792972, 663ac2d887df18e6da97dd358ebd2bca55404fd4a1c8c1c51215834fc6d11b33, Oe484560a909fc06b9987db73346efaOca6750d5232334913c23e061695f5cc, 15d874e24caf162bc58597ac5f22716694b5d43cf433bee6a78a0314280f2c80,

Attack Name	TYPE	VALUE
GhostLocker	SHA256	0e484560a909fc06b9987db73346efa0ca6750d523f2334913c23e061695f5cc, 4844f44c9de364377f574e4d6a8a77dc0b4d6a67f21ccbf693ac366e52eaa8cb, 65d3a922754af96d8d722859ac31f3de96522d50659c67607021f2ac728f9630, a98f8468d70426ba255469a92d983d653f937d954e936e0ff5d9a0f44f1bdf70, ee227cd0ef308287bc536a3955fd81388a16a0228ac42140e9cf308ae6343a3f, 7d37eddf0b101ff2b633b2ffe33580bdb993a97fecc06874d7b5b07119b9ec99, 4c09a012efff318b01a72199051815c5a7b920634fb6c76082673681f54f2ec3
BlackCat	SHA256	17fd1b0bda42ee4fd6c0444e22ee566c582efb51d72f7382dc089cfbfb705042, 82efdfd29b22cad8e80ef90940086986410d00ec4c42c547069612c7b0f33eb1, a9c37c4caedf09aebcad23be27b6db636d54e94e0f9b86c1bb61da0784269936, 1124a6eea74d6e128ac275ce462f2807cd900d49c87382db81f901e60c8e7758, 76f99fbf8f91556c98848cabfb3fd85892939e410903e03da67e517102745102, 76f99fbf8f91556c98848cabfb3fd85892939e410903e03da67e517102745102
AveMaria	SHA256	33b1fec8b20ebd775dbe037a652b5002124a317b434208c400d5cf933b0e68ef, fd770dfea61dde4dde009e95f4a4ea966ff588ee181a8afb1bb730803912dd73, c4f2e2bf5071a42ee6ca811a253e55adf09b1982bacf5f9b90149ff0393950e0, 62de5582c8c8dad5e6ae1e6008e3883c72b59de0b17cec54be78a888d4097dc2, 40052b060229a0b036bdf73aa09ea1ecc6e73555f448dc092340ccb342ec1669, c925c6fb78be7a4b617be38e6cf80e94cf30198a48689c94d78d42cef12f8223, 568e609adc8d405cb059b471c7f99a2dbc2969642721cc4ce51e869a6af35dca, f0b92472c6a95a379f7235c22460fdb3602d625a662141e7baecc48c049ad715, a230a63b3011b2ebe1fb667cb661835fe34fb93bb6a1cbd4f132996b437e947c, 7bcdc2e607abc65ef93afd009c3048970d9e8d1c2a18fc571562396b13ebb301, 4fd7411cc681154e27eede4332a010641db743700099c602f5ac1e61968c3264, e6df4f343401f5c3c79228940acc0dcadcd655e1e0e8010f9f67eb946d67e94a,

Attack Name	TYPE	VALUE
AveMaria	SHA256	3c4d55297278d1e2d4393d4b65f6ed5a4d88ebf590677521e95f084bab83b6bb, 2a11c5bca51d510efec348abaa05617f21e5b4ab08b67e6261d9830b4729e649
Raccoon	SHA256	184e98107496e5859dd0f09c42deffffaf0cc9362cc192f0e89bf2c4b20d82fd, fd3f9ee2a7b4e35be97140818562dc4470f90705cbd959e87c07ed983692e33d, abcbbdb2a2eb219a82c3f446f74ac6ef93a3deb11e4c277dee8c106792d7b783, 5ff52ab9349cd6d7a7fc0d2596c3423cdfb5df668b363fb93bd686f9ab198910, 1e5c7dcfbe4a1e9da06229b4512229c463b0268832b9cb6cdb35a1153963be37, 43f48b33734f2b7ab20e3798845f8411723f643a15c9833b86942ab6beb9d4fe, 5566d651067c35b90b47039ec1384432ec89fcdc946188274fb5127a8874b194, 35efa67d11c826f739cedc44c759bf9f12b12deab0af24bd8a402eccb7157d97, 334f1cfbe30bc002491e179ac48e228e142e78f13a2fa5eaeb44bcf4cf2bf946, 61431a0d94e6995e43fa174b18ca64052374c5d2ff1743631e13154ca1cf0fab, 89b8c862587864fe60e46ee4f4e8cbba2d8c32081a04ad5df072c6f99f06f4e2, 529c26f60ac5ebc31836486d9fa29f3b139437f06b160ca7f2887d13126c937e, 0ea39ba88fb2afb12f328a24d8b0441c6c6d2220c8ceac1a1c0640c7d6b43ae4, 8352d5041c2baf4613361108ef86b62ce3814bfa543a52662d40ddfc5dbf045a, 1e5b1cee1779ab2659fbaf465da3dfda327fdc83e78b73c4cebc241356ff00d9, 302886dba2ea9783a67247110cfabea3f94d1f78343b55f66edd58fc4be926f1, eeb5ee631e4e3dea3a6faf8fc70bf52d1814db8f5c6a6ebe729ae23df71879e5, 5320425988b0670455042dbd99d0c30b96ddf4710932dbe61b95711b185536b6, 0c1226d05d81a2f2f9ed910fff598bd00a0cb7ae43b3793735d45de1f35b838f, 31b6fba02c5c0d97a7ae7436a7e30793fe86f36ddf289e8eb53702dcd0ef06b9
	URLs	hxxp://51.195.166.184/, hxxp://31.192.237.23:80/, hxxp://45.61.138.198:80/, hxxp://91.92.246.197:80/, hxxp://91.103.252.11

Attack Name	TYPE	VALUE
Raccoon	IPv4	193.222.96[.]7, 185.193.125[.]199, 194.87.31[.]58, 5.78.80[.]43, 5.78.81[.]39, 94.142.138[.]147, 157.90.161[.]111, 89.23.107[.]183
VIDAR	SHA256	3dae32e22775721f2f9de5fec79dbcd8d62adaeb057b47c4524e02d130a43b25, ffaed8dcf0282df833b74faf419729dc20951ee7edbb58103fa5c582e93d5f3a, 9a58dd63b51866541d91a5bae6260c27aeec7a4135cd67a6fb686f549d3646a6, 13e384c54054a094b8045928c8ec9d3697372e551e4887b4ea9e18e319f0f40b, 48b7d39b9c19b0e6131928830add88e9c43e01e8218db17877abca9a65d14a5d, 1eda38c94d7896c350c73e5ac87cf2cd65e96ba7d03cddc7f1302c5d1b65ca88, c1f234ee29062e05c71fbb29d43b75e4a73aeccc95201dea7956fc6e6a5949cf, 726855dc870ed0224d91891b898e542393149b0eaef7817aa332b71c13b22ae0, 6ecf9fda65dc1a4a9c7610510ac9f78a6663e75d736a8444c72e11a0cc8d8d46, fc5336b039a9cc8e14d515f338c90a5a404249adab200032324c65f055904255, 0e9783330259b925379f44dfdc9e8f86b545ad43e8b747a8214a7d7e7617940e
	URLs	hxxp://5.75.246[.]163/, hxxp://5.75.246.163/vcruntime140[.]dll, hxxp://5.75.246.163/softokn3[.]dll, hxxp://5.75.246.163/nss3[.]dll, hxxp://5.75.246.163/msvcp140[.]dll, hxxp://5.75.246.163/mozglue[.]dll, hxxp://5.75.246.163/freebl3[.]dll, hxxp://5.75.246.163/sqlite3[.]dll, hxxp://168.119.173.77[:]2087/, hxxp://168.119.173.77:2087/vcruntime140[.]dll, hxxp://168.119.173.77:2087/softokn3[.]dll
Kinsing	SHA256	7f9f8209dc619d686b32d408fed0beb3a802aa600ddceb5c8d2a9555cdb3b5e0, 8c9b621ba8911350253efc15ab3c761b06f70f503096279f2a173c006a393ee1, 511de8dd7f3cb4c5d88cd5a62150e6826cb2f825fa60607a201a8542524442e2,

Attack Name	TYPE	VALUE
Kinsing	SHA256	4b0138c12e3209d8f9250c591fcc825ee6bff5f57f87ed9c661df6d14500e993, 999e4ebacda24b9431863e4cb1fd3e2d8e568ebb118b4a8e215a28dac8d8da32, 1015a16078b826a0a52bf746016fedf2c758dca4a2033a48a9da20ee0b439eca
NetSupport RAT	SHA256	213af995d4142854b81af3cf73dee7ffe9d8ad6e84fda6386029101dbf3df897, 28208baa507b260c2df6637427de82ad0423c20e2bceceb92ba5d76074dcd347, 2d6c6200508c0797e6542b195c999f3485c4ef76551aa3c65016587788ba1703, 2e4bd5557aedd1743da5fab1b6995fbc447d6e9491d9ec59fa93ab889d8bccd1, 38684adb2183bf320eb308a96cdbde8d1d56740166c3e2596161f42a40fa32d5
Nim backdoor	MD5	7bea8ea83d5b4fe5985172dbb4fa1468, 04e9ce276b3cd75fc2b20b9b33080f7e, 92612dc223e8f0656512cd882d66f78b, c2184d8fd3dd3df9fd6cf7ff8e32a3a4, b2ab01d392d7d20a9261870e709b18d7, 30ddd9ebe00f34f131efcd8124462fe3
DarkGate	SHA256	ad36b909721d64a3c32678f4c2ca758d81661088ba1ed57bec50ef0ac4d4a871, 00985db874d9177de4a18999f7a420260b3a4665ba2b5b32aa39433ef79819df, 0f1545a7176c45b0e7f9198cac8972167e5846e8b84cd40926f7edf338eeace2, 10bfaeb0c00425c4749140d5c7d9f3d88537cf2f621ba7af5322b15cf205b896, 2b24c4c883a562d0326846ee1c92840144d1d755cdb721b24a35038ea92aa0e4, 6750f31ef5e1fe74c1121b0ab1308f93e09505a63322b6ce16fe04099ce8993e, 73c0d0f220a30b541e0855e8039b8050d1332ff03c3e0c8a35671bd5eb9d30be, 74729d4569691daf72e23849e91461471411f551639663e11e1091a48790611e, 74f21cf5ab72aad0f7f3cf3274a167c20e787f9513019510561f39d4230f3c4b, bc5ad215876055a8a6a097579e16d24e233a323a6157afbb6db49705ac12a1f1, bec37877e3bffa222efb5c5680c7defd2d917317293d7fa70e0882ad45290a40, e7b76e11101e35c46a7199851f82c69e819a3d856f6f68fa3af0636c3efde0ca

Attack Name	TYPE	VALUE
Atomic Stealer	SHA256	4cb531bd83a1ebf4061c98f799cdc2922059aff1a49939d427054a556e89f464, be634e786d5d01b91f46efd63e8d71f79b423bfb2d23459e5060a9532b4dcc7b, 5b5ffb0d2fb1f2de5147ec270d60a3ac3f02c36153c943fbfe2a3427ce39d13d
	IPv4	194.169.175[.]117
	Domain	wifi-ber[.]com
LambLoad	SHA256	166d1a6ddcde4e859a89c2c825cd3c8c953a86bfa92b343de7e5bfbfb5afb8be
InfectedSlurs	SHA256	dabdd4b5a3a70c64c031126fad36a4c45feb69a45e1028d79da6b443291addb8, 3f3c2e779f8e3d7f2cc81536ef72d96dd1c7b7691b6e613f5f76c3d02909edd8, 75ef686859010d6164bcd6a4d6cf8a590754ccc3ea45c47ace420b02649ec380, f8abf9fb17f59cbd7381aa9f5f2e1952628897cee368defd6baa6885d74f3ecc, 8777f9af3564b109b43cbcf1fd1a24180f5cf424965050594ce73d754a4e1099, ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1, a4975366f0c5b5b52fb371ff2cb034006955b3e3ae064e5700cc5365f27a1d26, cd93264637cd3bf19b706afc19944dfb88cd27969aaf0077559e56842d9a0f87, 8e64de3ac6818b4271d3de5d8e4a5d166d13d12804da01ce1cdb7510d8922cc6, 35fcc2058ae3a0af68c5ed7452e57ff286abe6ded68bf59078abd9e7b11ea90a, 7cc62a1bb2db82e76183eb06e4ca84e07a78cfb71241f21212afd1e01cb308b2, 29f11b5d4dbd6d06d4906b9035f5787e16f9e23134a2cc43dfc1165127c89bff, cfbcbb876064c2cf671bdae61544649fa13debbbe58b72cf8c630b5bfc0649f9, a3b78818bbef4fd55f704c96c203765b5ab37723bc87aac6aa7ebfcc76dfa06d, ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1
SwiftLoader	SHA256	47b8b4d55d75505d617e53afcb6c32dd817024be209116f98cbbc3d88e57b4d1

Attack Name	TYPE	VALUE
KandyKorn	SHA1	62267b88fa6393bc1f1eeb778e4da6b564b7011e, 8f6c52d7e82fbfdead3d66ad8c52b372cc9e8b18, ac336c5082c2606ab8c3fb023949dfc0db2064d5, 26ec4630b4d1116e131c8e2002e9a3ec7494a5cf, 46ac6dc34fc164525e6f7886c8ed5a79654f3fd3, 8d5d214c490eae8f61325839fcc17277e514301e, 9f97edbc1454ef66d6095f979502d17067215a9d, c45f514a252632cb3851fe45bed34b175370d594, ce3705baf097cd95f8f696f330372dd00996d29a, e244ff1d8e66558a443610200476f98f653b8519, e77270ac0ea05496dd5a2fbccba3e24eb9b863d9, e68bfa72a4b4289a4cc688e81f9282b1f78ebc1f, 26ec4630b4d1116e131c8e2002e9a3ec7494a5cf, 46ac6dc34fc164525e6f7886c8ed5a79654f3fd3, 62267b88fa6393bc1f1eeb778e4da6b564b7011e, 8d5d214c490eae8f61325839fcc17277e514301e, 8f6c52d7e82fbfdead3d66ad8c52b372cc9e8b18, 9f97edbc1454ef66d6095f979502d17067215a9d, ac336c5082c2606ab8c3fb023949dfc0db2064d5, c45f514a252632cb3851fe45bed34b175370d594, ce3705baf097cd95f8f696f330372dd00996d29a, e244ff1d8e66558a443610200476f98f653b8519, e68bfa72a4b4289a4cc688e81f9282b1f78ebc1f, e77270ac0ea05496dd5a2fbccba3e24eb9b863d9
ParaSiteSnatcher	SHA256	0e7fb784a10d8cc942029477fee4c1b8907612e3f667970d5ca9fce885cac1d4, e06e25a13adce5c1889c613f12c269b4926f4900da155f4de5fedd46e45c5807, 96309a0654110f4c9c20869b9f139c7aceea0d1f7f698892cdfd821f9463e04f, b9f8ead09e78645f4a52290b88feafc899d3acf9db776259892058877bd9d250, 6d0a9cf9a80db3f228d51a8f078a6949bf96684cfb5f78f42a0941d070bc15e4, 9e882594b497f6bc99f6da26211c54d5005064423b1f93059406332e36ae3eba, 1ebfe73932122e898c30098be4384a0fc9150565c3a340750b37b121ea7a55fa, 8915b71a1c7a4da5c1cf73cdfa1d24c5546ed203e2a2d17f997ec31398bf85cc, 8603b20b548270423fb03c2138c16f5f863ead4c48eb0999167df869e2eef8a6, bcba29cd571b58e7f0bbf9d72105e50f1eddf915207e9147c554b18922c5adf7, ec22d946dc9538100875b86d2f6035f3541f5e3f08698304b9591efeea7d09a2, 1a3c5f97e7915b70c1371dd9a0265565fe86f7f347e303e7a6d8eaad573d339b, 3f033626d5f4b0cb69e4e902d80d1c3c4de647562e359a0d8904485799483e3b,

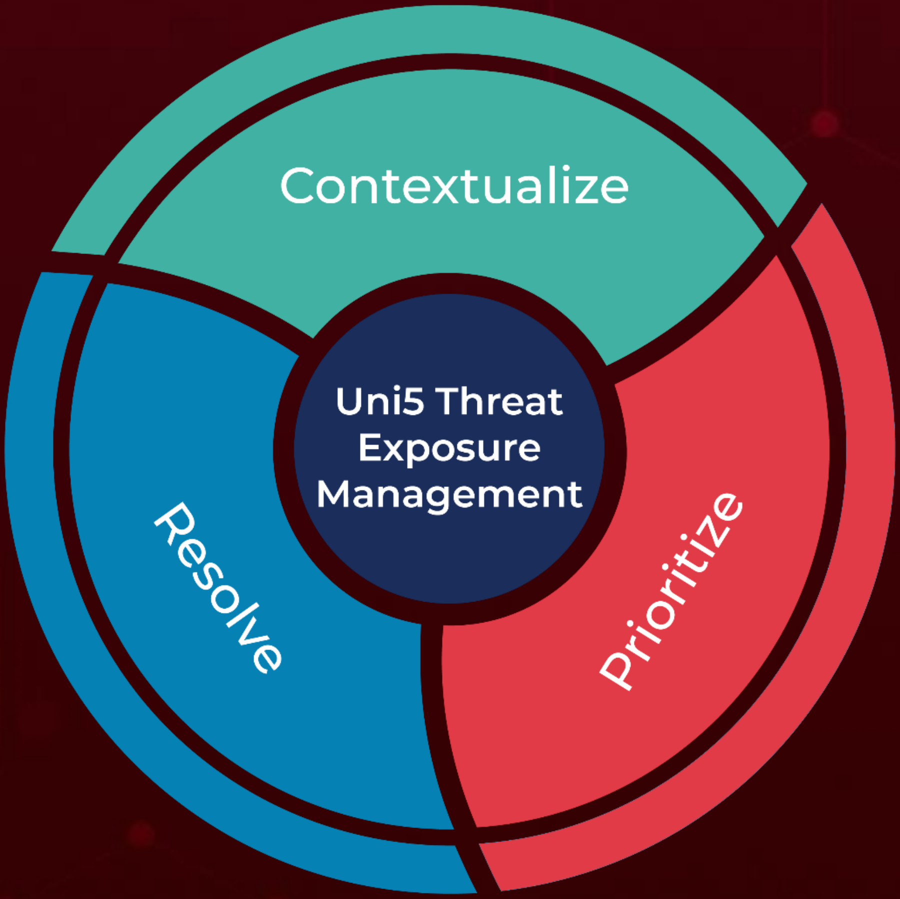
Attack Name	TYPE	VALUE
ParaSiteSnatcher	SHA256	71b9d8721defee1f8f1694ce4e2ae8b1a99b78baa8e7fc9dd11364e97c390ff8, 21f4b82b120d84a2b21f95d75a583f36d7116cc3768785a3d0f213b50e86b240, c08a6db547b833244dd93aca9441059efe65428c588f0db591bcc8157fe4b43f, 5d813c849a79c60440ae2a36117e29da1da6c7649c00156b5cfe6222322e4cd6, 049a80a962618d9b89fb0a2cf03ef2c3ee00975c5b424e209f073e3c7a491f2c, b5e07008f50ff56ffd0389340a037da43b6398d57bf345dda3e0661098bf5ae4, e59e36d652f454aab543722501ac23258d295ef0f1ecf7c97cad7720ceee6123, a21356a2294036d2b573e3f6350a198cd0c4e98d5c2e7ecc9d37089250a6c0c0, 260b650de3977580a86c63c7f13b0aaee606fe16feff552936eed8e3ad652627, e195d0548c52a7cdb142c6c5acda2af40e350bd9d606ae4e1c03c6aa246572b3, 77e314975b4d26998a6384c9cb0deda88b8fa5ea059e3fe7b48edd8a541f2315, 72f327f62710f60f43569741c2cb391b833b44c4dafe1f5d5c085a39c485b5df
Djvu	SHA256	61cbdd06eb0034a51074b1bcaeed4d2d7aff85f7e1fe61903481b1fb63508db4, ce00b1cb3ac152e4c3d6688e595146c2382616cb83139bac6ee798f0e2e99c19, 864f2a472db2e654cd2f2925be768a442d167c6d15c2a678ec81f713ff897b1d, c18b111c047ba4e0aa30ca19634ffd9f131aecb5dec7645c78a666e85e469b03, d0644b5e3e7dcad31d5918e4688e31d6fc691ce2e709e6033263774baf37c50e, f6f2310f44da2c4c97832cff60fb3f60719491f5971cf7fe22062d4ada705e32, 0c8969456b94f05ca3ee3f6b0518bd151fe0547150086980282f4ad1fc8a7bd6, 84161c7097bc5a675ed250ed222f1f4d0aea4c2dc48d623aecd9f7fc44a7119c, 23c672f232c10ed80e8a361da94c54d07ecb2673d21bf663f75ab5dba43b2ae0, 91c21cadd1249480ace996ae3d3e1a0370976d9c4bd17bdade97b1bb92fc59e0, 895593614cf395846b5cdd2c8c4bc7adb87de14cc849e28632f1ab6ff49b43fb, 72a9bb670dc192dae57c0238afdb706bea501f8e0bf06b4fa4b8669741c93547,

Attack Name	TYPE	VALUE
Djvu	SHA256	40fff8c4d316ae5de858fdd429d684a96426ce701582d133718be7bea7ea5ac5, f9b5765e9f494c0c485774a401904ed83092fbd6e19184a4ff48c74f6aed02e6
Cerber ransomwar	SHA256	5bd70163b5ee71238d37ffa0ff179e6a42fc28ff5e218c11502e8341b031b951, ff2ae546f2cb4f72aad3d330f3fd1b7231940c4a1b6d9df10a3870e1d7b7698e, d460a39b8a903a1d6a559515723fd55c7ed0a4c06fbce1635fc8e21662250f9e, f344b2556ca35b3cf957d4284dd00c26404795dff5790258dba2f70a916b2e51, 3ba6b2ddf2c9d3256993bb6a78e40b109176e6f4dd02c99916cc6ff9748f789c, 9377fe5800a21343f76d8067721ba3efa2fbff71f1d4feaf8980f7375f15eb39, a67dc54bb3c0185711abc873346b6d7410e07f9cbe22e620b586e1d63594d806, 7f48304f3484aa9549ca5f6ad4220fd0469563cb0eb6ce06bfa4a27e7db4d2ec, 594b4e3d6f60d8fdddb8d6de5593ed38df821aad47d6255b6af16207f091212b

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

December 04, 2023 • 2:00 AM

More at www.hivepro.com