Date of Publication
November 7, 2024

Hive Pro

HiveForce Labs

MONTHLY
THREAT DIGEST

Vulnerabilities, Attacks, and Actors

OCTOBER 2024

Table Of Contents

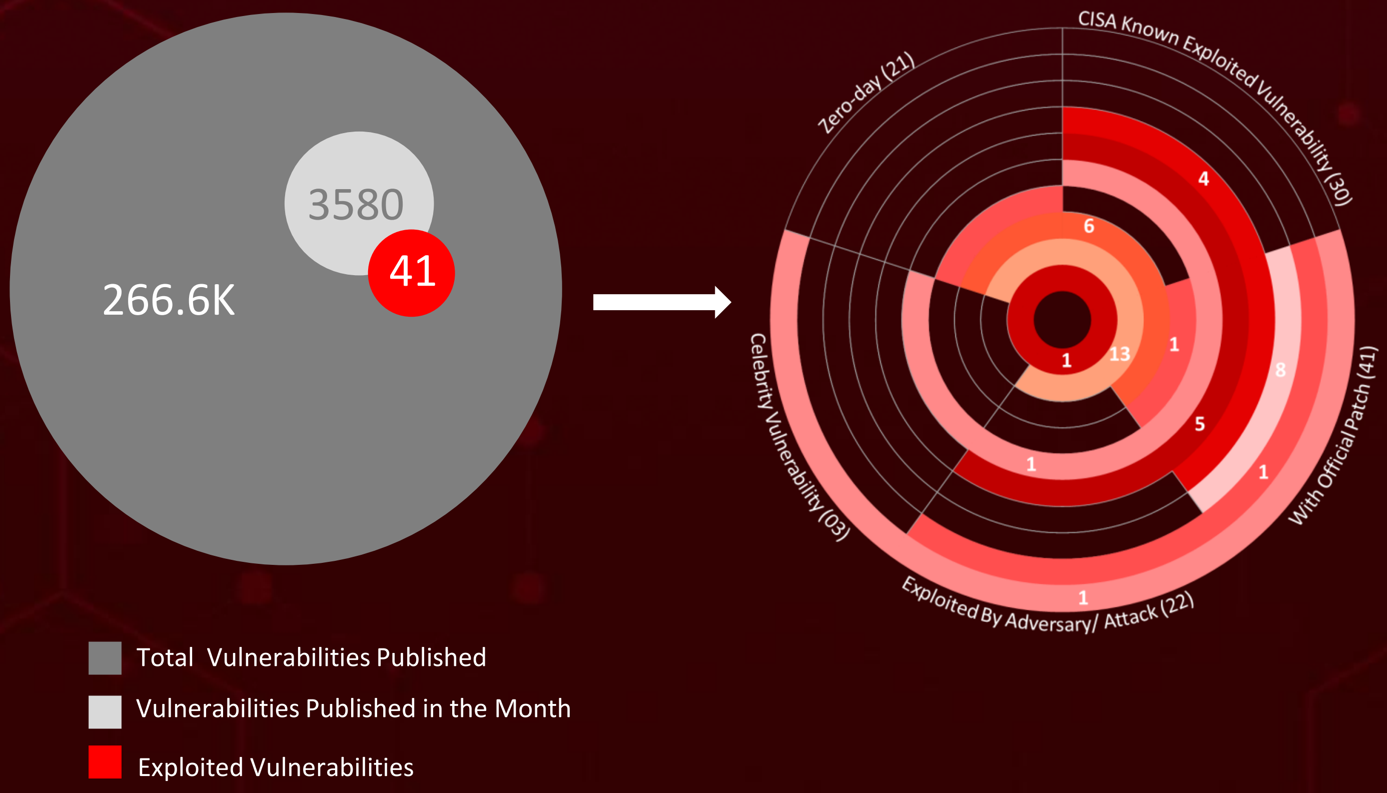
Summary

In **October**, the cybersecurity arena drew significant attention with the active exploitation of **twenty-one zero-day** vulnerabilities. Among them, **CVE-2024-47575** in FortiManager was exploited by **UNC5820** to compromise over 50 devices, enabling the theft of configurations, IP addresses, and credentials from FortiGate systems. Mozilla also fixed the critical zero-day flaw **CVE-2024-9680** in Firefox, which had been actively exploited to execute arbitrary code.

During this period, ransomware attacks surged, with variants such as **Akira, Fog, Cicada3301, LockBit 3.0, Babuk, and Embargo Ransomware** aggressively targeting victims. As ransomware tactics grow more sophisticated, organizations must bolster their defenses by implementing comprehensive backup and disaster recovery strategies. Additionally, training employees to detect and prevent phishing attacks remains essential.

Since August 2024, **Akira and Fog ransomware** strains have exploited vulnerabilities in SonicWall's SonicOS (**CVE-2024-40766**) and Veeam Backup & Replication (**CVE-2024-40711**), resulting in over 30 incidents involving unauthorized access and arbitrary code execution.

Concurrently, **Seventeen** threat actors have engaged in various campaigns. **GoldenJackal**, a skilled APT group, launched advanced cyberattacks on government and diplomatic targets in Europe, aiming to breach air-gapped systems and exfiltrate sensitive data. The Chinese APT group **Evasive Panda** employed a toolset called **CloudScout** to infiltrate organizations in Taiwan. As the cybersecurity landscape evolves, organizations must remain vigilant and proactively address emerging threats.



Insights

In October 2024, a geopolitical cybersecurity landscape unfolds, revealing **Russia, Thailand, Indonesia, Malaysia,** and **Philippines** as the top-targeted countries.

Highlighted in **October 2024** is a cyber battleground encompassing the **Government, Technology, Education, Healthcare** and **Retail** sectors, designating them as the top industries.

Awaken Likho, intensified its operations post-Russo-Ukrainian conflict by switching from UltraVNC to MeshAgent to target government and industrial networks.

Credential Theft Made Easy: New Windows Themes Vulnerability Exposes NTLM Credentials to Attackers

The ErrorFather campaign targeting Android users, delivering the variant of **Cerberus Banking Trojan**, stealing financial information

Lazarus exploited Chrome zero-day **CVE-2024-4947** via a fake DeFi game, targeting cryptocurrency users and deploying the **Manuscrypt** backdoor for persistent access.

HM Surf Unveiled: macOS Vulnerability Grants Hackers Access to Your Camera and Mic.

APT34 Exploiting CVE-2024-30088 in the Windows Kernel, to deploy a new backdoor called 'StealHook'.

Repellent Scorpius has distributed the Cicada3301 Ransomware-as-a-Service (RaaS), focusing on the United States and the United Kingdom in 24 confirmed attacks.

Ivanti, fixed three actively exploited zero-day vulnerabilities in its Cloud Services Appliance that could enable remote code execution and SQL command execution.

Threat Landscape

41 Vulnerabilities

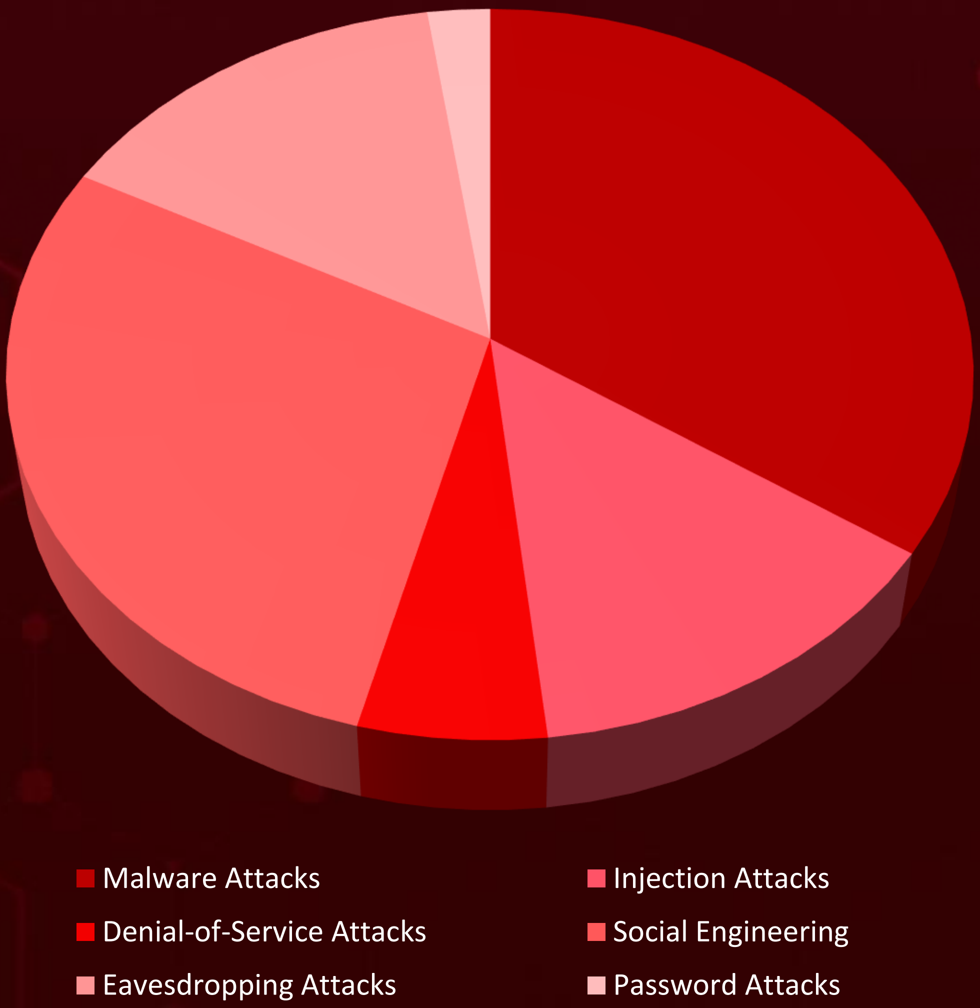
182 MITRE ATT&CK TTPs

32 Industries

17 Adversaries

195 Countries

53 Attacks



Celebrity Vulnerabilities

CVE ID	**ZERO-DAY**	**AFFECTED PRODUCTS**	**ASSOCIATED ACTOR**
CVE-2021-44228	✓	Apache Log4j2	Flax Typhoon
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-917	T1059: Command and Scripting Interpreter, T1190 : Exploit Public-Facing Application	https://logging.apache.org/security.html

CVE ID	**ZERO-DAY**	**AFFECTED PRODUCTS**	**ASSOCIATED ACTOR**
CVE-2020-1472	✗	Microsoft Netlogon	Iranian Threat Actors
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
ZeroLogon (Microsoft Netlogon Privilege Escalation Vulnerability)	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-330	T1068: Exploitation for Privilege Escalation; T1210: Exploitation of Remote Services	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-44133	⊗	macOS Sequoia versions before 15.0	-
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	Adload
HM Surf	⊗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINKS**
	CWE-284	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1203: Exploitation for Client Execution	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/108382

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2021-44228	Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)	Apache Log4j2	✓	✓	✓
CVE-2020-1472	ZeroLogon (Microsoft Netlogon Privilege Escalation Vulnerability)	Microsoft Netlogon	✗	✓	✓
CVE-2024-44133	HM Surf	macOS Sequoia	✗	✗	✓
CVE-2024-5217	ServiceNow Incomplete List of Disallowed Inputs Vulnerability	ServiceNow	✗	✓	✓
CVE-2024-4577	PHP-CGI OS Command Injection Vulnerability	PHP	✗	✓	✓
CVE-2024-29973	Zyxel Command Injection Vulnerability	Zyxel NAS326 V5.21, NAS542 V5.21 and earlier	✗	✓	✓
CVE-2024-21762	Fortinet FortiOS Out-of-Bound Write Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2023-38035	Ivanti Sentry Authentication Bypass Vulnerability	Ivanti Sentry	✓	✓	✓
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2023-35081	Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✓	✓	✓
CVE-2023-27997	Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS and FortiProxy SSL-VPN	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-22515	Atlassian Confluence Data Center and Server Broken Access Control Vulnerability	Atlassian Confluence Data Center and Server	✓	✓	✓
CVE-2022-42475	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2020-8515	Multiple DrayTek Vigor Routers Web Management Page Vulnerability	Multiple DrayTek Vigor	✓	✓	✓
CVE-2023-24229	DrayTek Command Injection Vulnerability	DrayTek Vigor	✓	✓	✓
CVE-2023-38831	RARLAB WinRAR Code Execution Vulnerability	RARLAB WinRAR	✓	✓	✓
CVE-2024-29824	Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability	Ivanti Endpoint Manager (EPM)	✗	✓	✓
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server and Data Center	✓	✓	✓
CVE-2024-40711	Veeam Backup & Replication Remote Code Execution Vulnerability	Veeam Backup & Replication	✗	✗	✓
CVE-2024-45519	Synacor Zimbra Collaboration Command Execution Vulnerability	Synacor Zimbra Collaboration	✗	✓	✓
CVE-2024-43573	Windows MSHTML Platform Spoofing Vulnerability	Windows MSHTML Platform	✓	✓	✓
CVE-2024-43572	Microsoft Management Console Remote Code Execution Vulnerability	Microsoft Management Console	✓	✓	✓
CVE-2024-6197	Open Source Curl Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-20659	Windows Hyper-V Security Feature Bypass Vulnerability	Microsoft Windows	✓	✗	✓
CVE-2024-43583	Winlogon Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-9680	Mozilla Firefox and Firefox ESR Use-After-Free Vulnerability	Mozilla Firefox	✓	✗	✓
CVE-2024-9379	Ivanti Cloud Services Appliance SQL Injection Vulnerability	Ivanti Cloud Services Appliance	✓	✓	✓
CVE-2024-9380	Ivanti Cloud Services Appliance OS Command Injection Vulnerability	Ivanti Cloud Services Appliance	✓	✓	✓
CVE-2024-9381	Ivanti Cloud Services Appliance Path Traversal Vulnerability	Ivanti Cloud Services Appliance	✓	✓	✓
CVE-2024-30088	Microsoft Windows Kernel TOCTOU Race Condition Vulnerability	Microsoft Windows Kernel	✗	✓	✓
CVE-2024-9486	Kubernetes Image Builder Hardcoded Credential Vulnerability	Kubernetes Image Builder	✗	✗	✓
CVE-2024-20412	Cisco FTC Static Credential Vulnerability	Cisco Firepower Threat Defense Software	✗	✗	✓
CVE-2024-9537	ScienceLogic SL1 Unspecified Vulnerability	ScienceLogic	✓	✓	✓
CVE-2024-37383	Roundcube Webmail Cross-site Scripting (XSS) Vulnerability	Roundcube Webmail	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-47575	Fortinet FortiManager Missing Authentication Vulnerability	Fortinet FortiManager	✓	✓	✓
CVE-2024-4947	Google Chromium V8 Type Confusion Vulnerability	Google Chromium	✓	✓	✓
CVE-2024-20481	Cisco ASA and FTD Denial-of-Service Vulnerability	Cisco Adaptive Security Appliance Cisco Firepower Threat Defense Software	✗	✓	✓
CVE-2024-50388	QNAP HBS 3 Hybrid Backup Sync OS Command Injection Vulnerability	QNAP HBS 3 Hybrid Backup Sync	✗	✗	✓
CVE-2024-38030	Microsoft Windows Themes Spoofing Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-21320	Microsoft Windows Themes Spoofing Vulnerabilit	Microsoft Windows	✗	✗	✓
CVE-2024-40766	SonicWall SonicOS Improper Access Control Vulnerability	SonicWall SonicOS	✗	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
XMRig	Cryptominer	-	Docker Swarm and Kubernetes	-	Exploiting container vulnerabilities
More_eggs	Backdoor	-	-	-	Spear-phishing
Nosedive	Botnet	CVE-2024-5217, CVE-2024-4577, CVE-2024-29973, CVE-2024-21762, CVE-2023-38035, CVE-2023-3519, CVE-2023-35081, CVE-2023-27997, CVE-2023-22515, CVE-2022-42475, CVE-2022-26134, CVE-2021-44228, CVE-2020-8515, CVE-2023-24229	RARLAB, Ivanti, ServiceNow, PHP-CGI, Zyxel, Fortinet, Citrix, Atlassian, Apache, DrayTek	✓	Deployed from Tier 2 Raptor Train Framework
Raptor Train	Framework	CVE-2024-5217, CVE-2024-4577, CVE-2024-29973, CVE-2024-21762, CVE-2023-38035, CVE-2023-3519, CVE-2023-35081, CVE-2023-27997, CVE-2023-22515, CVE-2022-42475, CVE-2022-26134, CVE-2021-44228, CVE-2020-8515, CVE-2023-24229	RARLAB, Ivanti, ServiceNow, PHP-CGI, Zyxel, Fortinet, Citrix, Atlassian, Apache, DrayTek	✓	Exploiting Vulnerabilities on SOHO networks and IoT devices
VeilShell	Backdoor	-	-	-	Phishing
GorillaBot	Botnet	-	-	-	Exploit vulnerabilities

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
JackalWorm	Worm	-	-	-	Infected USB Drives
GoldenDealer	Backdoor	-	-	-	Infected USB Drives
GoldenHowl	Backdoor	-	-	-	Infected USB Drives
GoldenRobo	Backdoor	-	-	-	Infected USB Drives
GoldenAce	Dropper	-	-	-	Infected USB Drives
GoldenUsbCopy	Stealer	-	-	-	Infected USB Drives
GoldenBlacklist	Stealer	-	-	-	Phishing
GoldenMailer	Stealer	-	-	-	Phishing
GoldenDrive	Stealer	-	-	-	-
Akira	Ransomware	CVE-2024-40711 CVE-2024-40766	Veeam Backup & Replication, SonicWall SonicOS	✓	Exploiting Vulnerabilities
Fog	Ransomware	CVE-2024-40711 CVE-2024-40766	Veeam Backup & Replication, SonicWall SonicOS	✓	Exploiting Vulnerabilities
StealHook	Backdoor	CVE-2024-30088	Windows Kernel	✓	Exploiting Vulnerabilities
DULLDROP	Trojan	CVE-2024-30088	Windows Kernel	✓	Dropped by malware
TONESHELL	Backdoor	-	-	-	-
WavyExfiller	Stealer	-	-	-	-
OneDoor	Backdoor	-	-	-	-

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
BingoShell	Backdoor	-	-	-	-
CoreWarrior	Trojan	-	Windows	-	-
Cerberus	Banking Trojan	-	Android	-	Social Engineering
DarkVision	RAT	-	-	-	-
PureCrypter	Loader	-	-	-	Social Engineering
Donut	Loader	-	-	-	-
Astaroth	Banking Trojan	-	-	-	Phishing
SingleCamper	Backdoor	-	-	-	Phishing
RustyClaw	Downloader	-	-	-	Phishing
MeltingClaw	Downloader	-	-	-	Phishing
DustyHammock	Backdoor	-	-	-	Phishing
ShadyHammock	Backdoor	-	-	-	Phishing
Cicada 3301	Ransomware	-	-	-	-
AdLoad	Loader	CVE-2024-44133	macOS Sequoia 15	✓	Exploiting Vulnerabilities
LockBit 3.0	Ransomware	-	-	-	Exploiting login credentials
Babuk	Ransomware	-	-	-	Exploiting login credentials
SRBMiner	Cryptominer	-	-	-	Docker remote API servers
Bumblebee	Loader	-	Windows	-	Phishing
Stealc	Information stealer	-	Windows and macOS	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Rhadamanthy s	Information stealer	-	Windows and macOS	-	Phishing
Atomic	Information stealer	-	Windows, macOS	-	Phishing
Manuscrypt	Backdoor	CVE-2024-4947	Google Chromium V8	✓	Exploiting Vulnerabilities
Sliver	HackTool	-	-	-	Exposed docker daemons
Tsunami	Backdoor	-	-	-	Exposed docker daemons
Embargo	Ransomware	-	Windows, Linux	-	Phishing
CloudScout	Information stealer	-	-	-	Leveraging stolen session cookies
MgBot	Framework	-	-	-	-
Nightdoor	Backdoor	-	-	-	-
Pronsis	Loader	-	-	-	Social Engineering
SUNSPINNER	Information stealer	-	-	-	Social Engineering
PURESTEALER	Information stealer	-	Windows	-	Social Engineering

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUC T
FIN6	Financial crime, Financial gain	-	-	More_eggs	-
Flax Typhoon	Information theft, Espionage	China	CVE-2024-5217, CVE-2024-4577, CVE-2024-29973, CVE-2024-21762, CVE-2023-38035, CVE-2023-3519, CVE-2023-35081, CVE-2023-27997, CVE-2023-22515, CVE-2022-42475, CVE-2022-26134, CVE-2021-44228, CVE-2020-8515, CVE-2023-24229	Nosedive, Raptor Train	RARLAB, Ivanti, ServiceNow, PHP-CGI, Zyxel, Fortinet, Citrix, Atlassian, Apache, DrayTek
SloppyLemming	Information theft and espionage	India	CVE-2023-38831	-	RARLAB WinRAR
APT37	Information theft and espionage	North Korea	-	VeilShell	-
GoldenJackal	Information theft and espionage	-	-	JackalWorm, GoldenDealer, GoldenHowl, GoldenRobo, GoldenAce, GoldenUsbCopy, GoldenBlacklist, GoldenMailer, GoldenDrive	-
Awaken Likho	Information theft and espionage	-	-	-	-
APT34	Information Theft & Financial Gainer	Iran	CVE-2024-30088	StealHook, DULLDROP	Windows Kernel

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
CeranaKeeper	Information theft and Espionage	China	-	TONESHELL, WavyExfiller, OneDoor, BingoShell	-
Water Makara	Information theft and espionage	-	-	Astaroth malware (aka Guildma)	-
UAT-5647	Information theft and espionage, Financial gain	Russia	-	SingleCamper (aka RomCom RAT, RomCom, SnipBot, RomCom 5.0), RustClaw, MeltingClaw, DustyHammoc k, ShadyHammo ck	-
Repellent Scorpius	Information theft and espionage, Financial gain	-	-	Cicada3301	-
Crypt Ghouls	Financial Gain, Information Theft, Espionage, Sabotage, Destruction	-	-	LockBit 3.0, Babuk	-
UNC5820	Information Theft	-	CVE-2024-47575	-	Fortinet FortiManager
Lazarus	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	CVE-2024-4947	Manuscrypt	Google Chrome
TeamTNT	Information Theft , Espionage, Sabotage, Destruction	-	-	Sliver, Tsunami	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Evasive Panda	Information theft and Espionage	China	-	CloudScout, MgBot, Nightdoor	Google Drive, Gmail, and Microsoft Outlook
UNC5812	Information theft and espionage	Russia	-	Pronsis Loader, SUNSPINNER, PURESTEALER	Windows and Android

Targeted Products

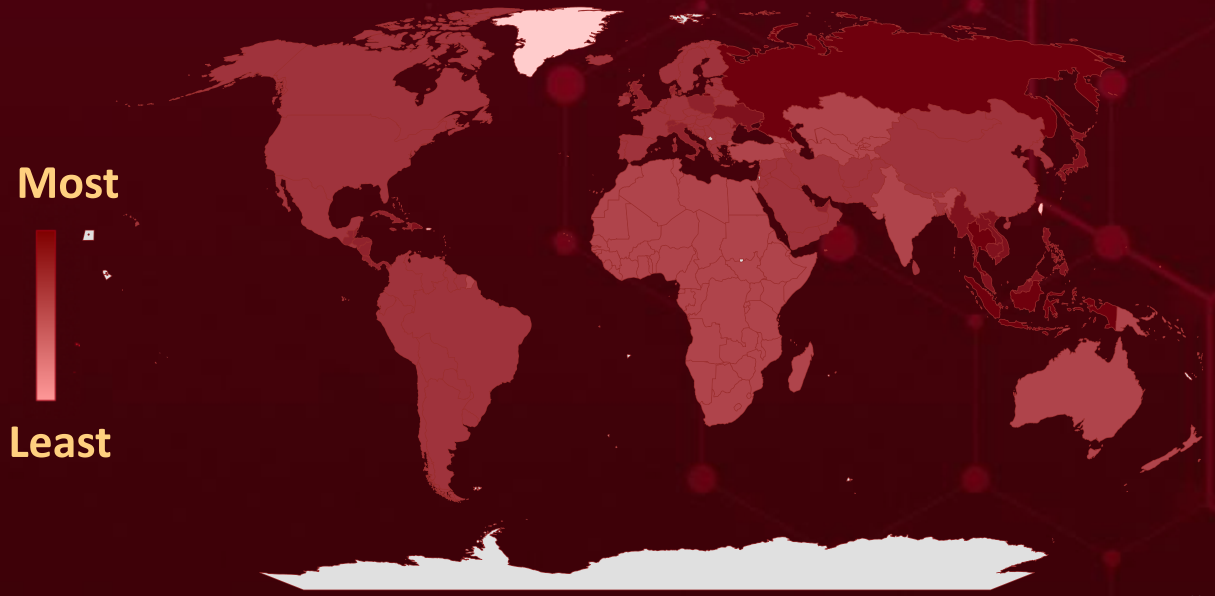
VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Operating system	macOS Sequoia versions before 15.0
THE APACHE SOFTWARE FOUNDATION	Framework	Apache Log4j2
Microsoft	Service	Microsoft Netlogon
	Server OS	Windows Server: 2008 – 2022 23H2
	Operating system	Windows: 10 - 11 23H2
	Software	ServiceNow Now Platform
php	Application	PHP version: 5 -8.3.7
ivanti	Application	Ivanti Sentry
	Cloud Appliance	Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior
	Mobile Endpoint Management	Ivanti Endpoint Manager Mobile (formerly MobileIron Core): before 11.10.0.3 Ivanti Endpoint Manager 2022 SU5 and prior versions

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
ZYXEL NETWORKS	Network Attached Storage	NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier
citrix	Application Delivery Controller (ADC)Gateway	Citrix NetScaler ADC and NetScaler Gateway
FORTINET	Network Management Appliance	FortiManager 7.6.0, FortiManager 7.4.0 through 7.4.4, FortiManager 7.2.0 through 7.2.7, FortiManager 7.0.0 through 7.0.12, FortiManager 6.4.0 through 6.4.14, FortiManager 6.2.0 through 6.2.12, FortiManager Cloud 7.4.1 through 7.4.4, FortiManager Cloud 7.2.1 through 7.2.7, FortiManager Cloud 7.0.1 through 7.0.12, FortiManager Cloud 6.4 (all versions)
	Web Proxy	Fortinet FortiProxy
	Operating system	Fortinet FortiOS versions: 7.4.0 through 7.4.2 7.2.0 through 7.2.6 7.0.0 through 7.0.13 6.4.0 through 6.4.14 6.2.0 through 6.2.15 6.0 all versions
ATLASSIAN	Enterprise Collaboration Software	Confluence Data Center and Confluence Server Versions- 8.0.x, 8.1.x, 8.2.x, 8.3.0, 8.3.1, 8.3.2, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.5.1
DrayTek	Router	DrayTek Vigor
	File Archiver	WinRAR version 6.22 and older versions

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
zimbra A SYNACOR PRODUCT	Email Server	Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1
	Browser	Firefox Version Prior to 131.0.2, Firefox ESR Version Prior to 128.3.1, and Firefox ESR Version Prior to 115.16.1
CISCO	Security Appliance	Cisco Adaptive Security Appliance Cisco Firepower Threat Defense Software
	Network Security Software	Cisco Firepower Threat Defense Software for Firepower 1000, 2100, 3100, and 4200 Series
	Container Builder	Kubernetes Image Builder
SL1	Monitoring Platform	ScienceLogic SL1 versions prior to 12.1.3 ScienceLogic SL1 versions prior to 12.2.3 ScienceLogic SL1 versions prior to 12.3 ScienceLogic SL1 versions prior to 10.1.x ScienceLogic SL1 versions prior to 10.2.x ScienceLogic SL1 versions prior to 11.1.x ScienceLogic SL1 versions prior to 11.2.x ScienceLogic SL1 versions prior to 11.3.x
roundcube open source webmail software	Webmail client	Roundcube Webmail versions before 1.5.7 and Roundcube Webmail versions before 1.6.7

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
QNAP	Backup Software	QNAP HBS 3 Hybrid Backup Sync 25.1.x
	Browser	Google Chrome prior to 125.0.6422.60
SONICWALL	Operating systems	SonicWall SonicOS SOHO (Gen 5) version 5.9.2.14-12o and older, Gen6, Firewalls Version 6.5.4.14-109n and older, Gen7 Firewalls SonicOS build version 7.0.1-5035 and older
veeam	Backup Software	Veeam Backup & Replication before 12.2.0.334 versions

Targeted Countries



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Color	Countries
🟥	Russia
🟥	Thailand
🟥	Indonesia
🟥	Malaysia
🟥	Philippines
🟥	Myanmar
🟥	Cambodia
🟥	Dominican Republic
🟥	Singapore
🟥	Japan
🟥	Ukraine
🟥	Vietnam
🟥	Laos
🟥	Poland
🟥	United Arab Emirates
🟥	Jamaica
🟥	Costa Rica
🟥	Panama
🟥	Cuba
🟥	Belize

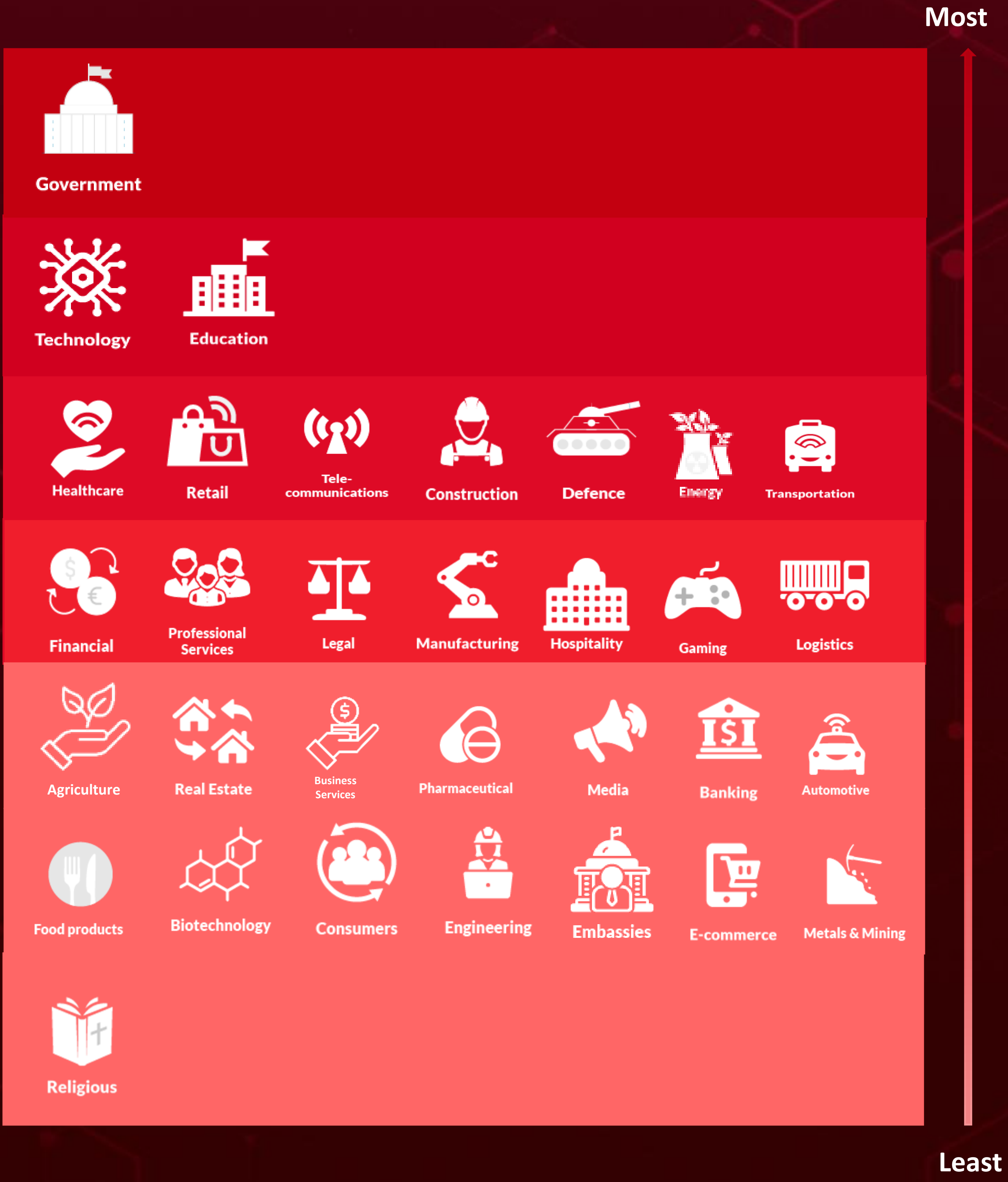
Color	Countries
🟥	Denmark
🟥	Bahamas
🟥	Grenada
🟥	Nicaragua
🟥	Guatemala
🟥	Barbados
🟥	Haiti
🟥	Switzerland
🟥	Honduras
🟥	Trinidad and Tobago
🟥	Italy
🟥	United Kingdom
🟥	Slovenia
🟥	Czech Republic
🟥	Nepal
🟥	Finland
🟥	Belarus
🟥	France
🟥	Ecuador
🟥	Germany

Color	Countries
🟥	Greece
🟥	Dominica
🟥	Bulgaria
🟥	Saudi Arabia
🟥	Albania
🟥	Suriname
🟥	Guyana
🟥	Montenegro
🟥	Canada
🟥	Brazil
🟥	Holy See
🟥	Oman
🟥	Chile
🟥	Peru
🟥	Hungary
🟥	Qatar
🟥	Iceland
🟥	Saint Lucia
🟥	Argentina
🟥	North Macedonia
🟥	Zimbabwe
🟥	Belgium
🟥	Iran

Color	Countries
🟥	Spain
🟥	Iraq
🟥	Andorra
🟥	Ireland
🟥	Bhutan
🟥	Israel
🟥	Bangladesh
🟥	China
🟥	Netherlands
🟥	Colombia
🟥	North Korea
🟥	Austria
🟥	Norway
🟥	Jordan
🟥	Pakistan
🟥	Kuwait
🟥	Paraguay
🟥	Bosnia and Herzegovina
🟥	Brunei
🟥	Latvia
🟥	Portugal
🟥	Lebanon
🟥	Romania

Color	Countries
🟥	Yemen
🟥	Saint Kitts & Nevis
🟥	Croatia
🟥	San Marino
🟥	United States
🟥	Serbia
🟥	Venezuela
🟥	Slovakia
🟥	Bahrain
🟥	South Korea
🟥	Maldives
🟥	Sri Lanka
🟥	Malta
🟥	Sweden
🟥	Mexico
🟥	Syria
🟥	Moldova
🟥	El Salvador
🟥	Monaco
🟥	Estonia
🟥	Mongolia
🟥	Liechtenstein
🟥	Uruguay

Targeted Industries



Most

Government

Technology, Education

Healthcare, Retail, Tele-communications, Construction, Defence, Energy, Transportation

Financial, Professional Services, Legal, Manufacturing, Hospitality, Gaming, Logistics

Agriculture, Real Estate, Business Services, Pharmaceutical, Media, Banking, Automotive

Food products, Biotechnology, Consumers, Engineering, Embassies, E-commerce, Metals & Mining

Religious

Least

TOP 25 MITRE ATT&CK TTPS

- T1059
  Command and Scripting Interpreter
- T1588
  Obtain Capabilities
- T1588.006
  Vulnerabilities
- T1190
  Exploit Public-Facing Application
- T1588.005
  Exploits
- T1068
  Exploitation for Privilege Escalation
- T1036
  Masquerading
- T1027
  Obfuscated Files or Information
- T1566
  Phishing
- T1041
  Exfiltration Over C2 Channel
- T1204
  User Execution
- T1083
  File and Directory Discovery
- T1059.001
  PowerShell
- T1203
  Exploitation for Client Execution
- T1574
  Hijack Execution Flow
- T1082
  System Information Discovery
- T1070
  Indicator Removal
- T1078
  Valid Accounts
- T1204.002
  Malicious File
- T1071
  Application Layer Protocol
- T1562
  Impair Defenses
- T1574.002
  DLL Side-Loading
- T1057
  Process Discovery
- T1105
  Ingress Tool Transfer
- T1566.002
  Spearphishing Link

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
More_eggs	SHA256	e1b4911959b6ca0db40873983e1f9d76e637818cb05d74e70b83701a5f4f4ef4, d207aebf701c7fb44fe06993f020ac3527680c7fa8492a0b5f6154ca
GorillaBot	MD5	276adc6a55f13a229a5ff482e49f3a0b, 63cbfc2c626da269c67506636bb1ea30, 7f134c477f307652bb884cafe98b0bf2, 3a3be84df2435623132efd1cd9467b17, 03a59780b4c5a3c990d0031c959bf7cc, 5b37be51ee3d41c07d02795a853b8577, 15f6a606ab74b66e1f7e4a01b4a6b2d7
	URL	hxxp[://]pen.gorillafirewall[.]su/
	SHA256	22a545fdb6ebbc5ba351c97d32cd008a1550a49891ae6112ddc8a6370376f053, 4cac6023b760e1fdae8c096a4db425eae3bbfe0d2554551efb76fc2f2d3a6b1b, e8320657b9ff24198170e6b30188304555b43281b654075052721717f66fb4df, 42845557a515bc05c290b3ab9d1ad291303691d472db9e09863bfc782b803ed2, d99d10559f1ad6bba1b59913604e261a613daa94af01ade8276effd692b5c03f, 826f9c8153c14a66ba730291e5f78d71d958c08cde45e2119afa227211ee5132, 6d10e4da8d8090e0e7e077ef4aead8b8720d1bd4f9b86d34ae66eac0e17e659c, b4a2a1900bab5b6e405cc78b72c5d1706c789b309bc1fa27ad746153ccb84004, 3905126f5f9f7430dee31c207706852e56292291449b563781bc6ee0b540343a, d4007f1ac2cb3a48db4bde7dbab7255421bf64f768a06492b81087f67a2e6c9c, e03580729f2f09dbd937d685fc9229959e84c9f329bee7eee16536bb8f9e60cf, 81c775f9540a66fded643fe4ec53dbbf35742bd3b069d95d689da313fc9b80a9

Attack Name	TYPE	VALUE
Akira Ransomware	SHA256	8a2d54e3230a4e7656ca760b512a879e0cacbe912a519a1be6916449bd6b5628, 87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d, 58e685695afc3a85d2632777a2b54967dc53d6a6fa1b7e2c110b2023b561bfe9, 1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218, 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c, ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d, c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddccd5bb37857e7bde6d2eb7, a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc, 2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422, 74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1
Fog Ransomware	SHA256	e67260804526323484f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3
Cerberus	SHA256	6c045a521d4d19bd52165ea992e91d338473a70962bcfded9213e592cea27359, 4c7f90d103b54ba78b85f92d967ef4cdcc0102d3756e1400383e774d2f27bb2e, 8f3e3a2a63110674ea63fb6abe4a1889fc516dd6851e8c47298c7987e67ff9b6, c570e075f9676e79a1c43e9879945f4fe0f54ef5c78a5289fe72ce3ef6232a14, a2c701fcea4ed167fdb3131d292124eb55389bc746fcef8ca2c8642ba925895c, 8faa93be87bb327e760420b2faa33f0f972899a47c80dc2bc07b260c18dfcb14, ee87b4c50e5573cba366efaa01b8719902b8bed8277f1903e764f9b4334778d0, 136d00629e8cd59a6be639b0eaef925fd8cd68cbcbdb71a3a407836c560b8579, 516282073b7d81c630d4c5955d396e1e47a2f476f03dea7308461fa62f465c11, 5bd21d0007d34f67faeb71081309e25903f15f237c1f7b094634584ca9dd873e, 6b8911dfdf1961de9dd2c3f9b141a6c5b1029311c66e9ded9bca4d21635c0c49, befe69191247abf80c5a725e1f1024f7195fa85a7af759db2546941711f6e6ae,

Attack Name	TYPE	VALUE
Cerberus	SHA256	9d966baefa96213861756fde502569d7bba9c755d13e586e7aaca3d0949cbdc3, 0c27ec44ad5333b4440fbe235428ee58f623a878baefe08f2dcdad62ad5ffce7, 880c9f65c5e2007bfed3a2179e64e36854266023a00e1a7066cbcf8ee6c93cbc
	SHA1	c7ebf2adfd6482e1eb2c3b05f79cdff5c733c47b
	MD5	f9d5b402acee67675f87d33d7d52b364
SingleCamper	SHA256	dee849e0170184d3773077a9e7ce63d2b767bb19e85441d9c55ee44d6f129df9, 2474a6c6b3df3f1ac4eadcb8b2c70db289c066ec4b284ac632354e9dbe488e4d
LockBit 3.0	MD5	8770189ed3ee558819fd6ddf677b0c28, 6e3e5d703ed9bed4b7327a73bc585c04
	SHA1	4dec26dfcd3fd938886c9586a8eb62d7a2495be4, 583f34dd59d30be4a10dc7021984df0225cef147
	SHA256	a54519b7530039b9fba9a4143bf549b67048f441bbebf9f8d5cff1e539752189, dec147d7628d4e3479bc0ff31413621fb4b1b64a618469a9402a42816650f92b, 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce, a56b41a6023f828cccaaef470874571d169fdb8f683a75edd430fbd31a2c3f6e, d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee, 5e006f895382525e762a33e5dd5e8416bef56ae859f5e96f820cfba5c4c11226, C9dd51d4295c33e1df0d275669a1de9e1de374a51eb88d7f7b1a1e65f49f7794
Bumblebee	URLs	hxxp[:]//193[.]242[.]145[.]138/mid/w1/Midjourney[.]msi, hxxp[:]//193[.]176[.]190[.]41/down1/nvinstall[.]msi
	IPv4	193[.]242[.]145[.]138, 193[.]176[.]190[.]41
	SHA256	2bca5abfac168454ce4e97a10ccf8ffc068e1428fa65528621000 6b298de42fb, 106c81f547cfe8332110520c968062004ca58bcfd2dbb0accd51616dd694721f, c26344bfd07b871dd9f6bd7c71275216e18be265e91e5d0800348e8aa06543f9, 0ab5b3e9790aa8ada1bbadd5d22908b5ba7b9f078e8f5b4e8fcc27cc0011cce7, d3f551d1fb2c307edfceb65793e527d94d76eba1cd8ab0a5d1f86db11c9474c3, d1cabe0d6a2f3cef5da04e35220e2431ef627470dd2801b4ed22a8ed9a918768, 7df703625ee06db2786650b48ffefb13fa1f0dae41e521b861a16772e800c115

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2024-5217](CVE-2024-5217)	✗	ServiceNow Now Platform	Flax Typhoon
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
ServiceNow Incomplete List of Disallowed Inputs Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-184	T1059: Command and Scripting Interpreter, T1588: Obtain Capabilities, T1190: Exploit Public-Facing Application	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4577	✗	PHP version: 5 -8.3.7	Flax Typhoon
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:php:php:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
PHP-CGI OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.php.net/downloads

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29973	✗	NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier	Flax Typhoon
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
Zyxel Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.zyxel.com/global/en/support/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21762	✗	Fortinet FortiOS versions: 7.4.0 through 7.4.2 7.2.0 through 7.2.6 7.0.0 through 7.0.13 6.4.0 through 6.4.14 6.2.0 through 6.2.15 6.0 all versions	Flax Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
Fortinet FortiOS Out-of-Bound Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1203: Exploitation for Client Execution, T1588.005: Exploits, T1059.007: JavaScript	https://fortiguard.fortinet.com/psirt/FG-IR-24-015

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38035	✗	Ivanti Sentry versions 9.18. 9.17, 9.16 and older versions	Flax Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:mobileiron_sentry:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
Ivanti Sentry Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3519	✗	Citrix NetScaler ADC and NetScaler Gateway	Flax Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:adc:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:gateway:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35081	✗	Ivanti Endpoint Manager Mobile (formerly MobileIron Core): before 11.10.0.3	Flax Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:mobileiron_core:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://forums.ivanti.com/s/article/KB-Arbitrary-File-Write-CVE-2023-35081

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27997	✗	Fortinet FortiOS and FortiProxy	Flax Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1574: Hijack Execution Flow, T1499: Endpoint Denial of Service, T1499.004:Application or System Exploitation, T1005:Data from Local System	https://www.fortiguard.com/psirt/FG-IR-23-097

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-22515	☒	Confluence Data Center and Confluence Server Versions- 8.0.x, 8.1.x, 8.2.x, 8.3.0, 8.3.1, 8.3.2, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.5.1	Flax Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_server_and_data_center:*:*:*:*:*:*:*	Nosedive, Raptor Train
Atlassian Confluence Data Center and Server Broken Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://www.atlassian.com/software/confluence/download-archives

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-42475	☒	Fortinet FortiOS	Flax Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1588.006: Vulnerabilities, T1059: Command and Scripting Interpréter, T1210: Exploitation of Remote Services	https://www.fortiguard.com/psirt/FG-IR-22-398

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-8515	✗	DrayTek Vigor	Flax Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:draytek:vigor2960:-:*:*:*:*:*:*:*	Nosedive, Raptor Train
Multiple DrayTek Vigor Routers Web Management Page Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-router-web-management-page-vulnerability-%28cve-2020-8515%29/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-24229	✗	DrayTek Vigor2960	Flax Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:draytek:vigor2960:-:*:*:*:*:*:*:*	Nosedive, Raptor Train
DrayTek Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAIL
	CWE-77 CWE-78	T1059: Command and Scripting Interpreter	End-of-life

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831	✗	WinRAR version 6.22 and older versions	SloppyLemming
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*:*	-
RARLAB WinRAR Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter, T1204.002: Malicious File	WinRAR version 6.23 or later

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29824	✗	Ivanti Endpoint Manager 2022 SU5 and prior versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting, T1562.010: Downgrade Attack	https://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-26134	✗	Atlassian Confluence Server and Data Center	Flax Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:	Nosedive, Raptor Train
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Exécution	https://jira.atlassian.com/browse/CONFSERVER-79016

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-40711	✗	Veeam Backup & Replication before 12.2.0.334 versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	Akira and Fog ransomware
Veeam Backup & Replication Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter; T1068 : Exploitation for Privilege Escalation	https://www.veeam.com/kb4600

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-45519	✗	Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zimbra:collaboration:*:*:*:*:*:*:*:*	-
	✓		
Synacor Zimbra Collaboration Command Execution Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK

	CWE-863
	CWE-284
		T1059: Command and Scripting Interpreter
		T1190: Exploit Public-Facing Application
			https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P46;
			https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P41;
			https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.9;
			https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43573	✗	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows MSHTML Platform Spoofing Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter, T1204 : User Execution, T1189 : Drive-by Compromise	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43572	✗	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:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Management Console Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-707	T1059: Command and Scripting Interpreter, T1204 : User Execution, T1204.002: Malicious File	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2024-6197](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6197)	☒	CBL Mariner Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	-
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:haxx:libcurl:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Open Source Curl Remote Code Execution Vulnerability	☒		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-590	T1204 : User Execution; T1203 : Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6197

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2024-20659](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20659)	☒	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	-
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Hyper-V Security Feature Bypass Vulnerability	☒		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1211 : Exploitation for Defense Evasion, T1554 : Compromise Host Software Binary	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20659

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43583	✗	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:*:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Winlogon Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-250	T1059: Command and Scripting Interpreter; T1068 : Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43583

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9680	✗	Firefox Version Prior to 131.0.2, Firefox ESR Version Prior to 128.3.1, and Firefox ESR Version Prior to 115.16.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:*:*	-
Mozilla Firefox and Firefox ESR Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1189 : Drive-by Compromise	https://www.mozilla.org/en-US/firefox/enterprise/#download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9379	✗	Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*	-
Ivanti Cloud Services Appliance SQL Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1078 : Valid Accounts, T1190 : Exploit Public-Facing Application	https://forums.ivanti.com/s/article/Ivanti-Cloud-Services-Application-5-0-2-Download-Release-Notes-Patch-History

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9380	✗	Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*	-
Ivanti Cloud Services Appliance OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1190 : Exploit Public-Facing Application, T1078 : Valid Accounts	https://forums.ivanti.com/s/article/Ivanti-Cloud-Services-Application-5-0-2-Download-Release-Notes-Patch-History

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9381	✗	Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*	-
Ivanti Cloud Services Appliance Path Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1078 : Valid Accounts, T1190 : Exploit Public-Facing Application	https://forums.ivanti.com/s/article/Ivanti-Cloud-Services-Application-5-0-2-Download-Release-Notes-Patch-History

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-30088	✗	Windows Kernel	APT34
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	StealHook, DULLDROP
Microsoft Windows Kernel TOCTOU Race Condition Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-367	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30088

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9486	⊗	Kubernetes Image Builder	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes-sigs:image-builder:*:*:*:*:*:*:*:*	-
Kubernetes Image Builder Hardcoded Credential Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-798	T1552: Unsecured Credentials	https://github.com/kubernetes-sigs/image-builder/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20412	⊗	Cisco Firepower Threat Defense Software for Firepower 1000, 2100, 3100, and 4200 Series	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*	-
Cisco FTC Static Credential Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-259	T1110.003: Password Spraying, T1078: Valid Accounts	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9537	✗	ScienceLogic SL1 versions prior to 12.1.3 ScienceLogic SL1 versions prior to 12.2.3 ScienceLogic SL1 versions prior to 12.3 ScienceLogic SL1 versions prior to 10.1.x ScienceLogic SL1 versions prior to 10.2.x ScienceLogic SL1 versions prior to 11.1.x ScienceLogic SL1 versions prior to 11.2.x ScienceLogic SL1 versions prior to 11.3.x	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:sciencelogic:sl1:*:*:*:*:*:*:*:*	-
ScienceLogic SL1 Unspecified Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-829	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://docs.sciencelogic.com/latest/Content/Web_Admin_and_Accounts/System_Administration/sys_admin_system_upgrade.htm

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-37383</td><td>✗</td><td rowspan="2">Roundcube Webmail versions before 1.5.7 and Roundcube Webmail versions before 1.6.7</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Roundcube Webmail Cross-site Scripting (XSS) Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-79</td><td>T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1204: User Execution, T1114.002: Remote Email Collection</td><td>Roundcube Webmail version: 1.5.7 and 1.6.7</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-2024-47575</td><td>✗</td><td rowspan="2">FortiManager 7.6.0, FortiManager 7.4.0 through 7.4.4, FortiManager 7.2.0 through 7.2.7, FortiManager 7.0.0 through 7.0.12, FortiManager 6.4.0 through 6.4.14, FortiManager 6.2.0 through 6.2.12, FortiManager Cloud 7.4.1 through 7.4.4, FortiManager Cloud 7.2.1 through 7.2.7, FortiManager Cloud 7.0.1 through 7.0.12, FortiManager Cloud 6.4 (all versions)</td><td rowspan="2">UNC5820</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:fortinet:fortimanager:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Fortinet FortiManager Missing Authentication Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-306</td><td>T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application</td><td>https://fortiguard.fortinet.com/psirt/FG-IR-24-423</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4947	✗	Google Chrome prior to 125.0.6422.60	Lazarus Group
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Manuscrypt
Google Chromium V8 Type Confusion Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1204: User Execution, T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1068: Exploitation for Privilege Escalation	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20481	✗	Cisco Adaptive Security Appliance Cisco Firepower Threat Defense Software	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:firepower_threat_defense_software:*:*:*:*:*:*:*:*	-
Cisco ASA and FTD Denial-of-Service Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-772	T1574: Hijack Execution Flow, T1499: Endpoint Denial of Service, T1499.004:Application or System Exploitation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-bf-dos-vDZhLqrW

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTOR
CVE-2024-50388	✗	QNAP HBS 3 Hybrid Backup Sync 25.1.x	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:qnap:hbs3_hybrid_backup_sync:*:*:*:*:*:*:*:*	-
QNAP HBS 3 Hybrid Backup Sync OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1588.005: Exploits	https://www.qnap.com/en-us/security-advisory/qsa-24-41

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38030	✗	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows Themes Spoofing Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1003: OS Credential Dumping, T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21320	✗	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows Themes Spoofing Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-200	T1003: OS Credential Dumping, T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-40766	✗	SonicWall SonicOS SOHO (Gen 5) version 5.9.2.14-12o and older, Gen6, Firewalls Version 6.5.4.14-109n and older, Gen7 Firewalls SonicOS build version 7.0.1-5035 and older	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:sonicwall:sonicos:*:*:*:*:*:*:*	Akira and Fog Ransomware
SonicWall SonicOS Improper Access Control Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-284	T1190: Exploit Public-Facing: Application, T1068: Exploitation for Privilege: Escalation, T1078: Valid Accounts, T1210: Exploitation of Remote Services	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XMRig	XMRig is an open-source cryptocurrency mining software primarily used to mine Monero (XMR), a privacy-focused cryptocurrency. It is frequently exploited in malicious campaigns, where attackers install it on compromised systems to secretly mine Monero, consuming system resources. This makes it a popular tool in cryptojacking attacks.	Exploiting container vulnerabilities	-
TYPE		IMPACT	AFFECTED PRODUCTS
Cryptominer		Information Theft, Compromise Infrastructure, Financial Gains	Docker Swarm and Kubernetes
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
More_eggs	More_eggs is a JavaScript backdoor, part of the Golden Chickens Malware-as-a-Service (MaaS) toolkit, widely adopted by financially motivated cybercriminal groups. It leverages legitimate Windows processes to bypass detection mechanisms, making it more elusive to traditional security tools.	Spear-phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Information Theft, Compromise Infrastructure, Deploys Payloads, Evades detection tools	-
ASSOCIATED ACTOR			PATCH LINK
FIN6			-

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	TOP TARGETED CVEs
Nosedive	Nosedive is a custom variant of the Mirai malware, and the primary implant found across most Raptor Train networks. It operates entirely in memory, allowing it to execute commands, transfer files, and conduct DDoS attacks on compromised devices. Nosedive is typically deployed using a unique URL encoding technique and a domain injection method.	Deployed from Tier 2 Raptor Train Framework	CVE-2024-5217, CVE-2024-4577, CVE-2024-29973, CVE-2024-21762, CVE-2023-38035, CVE-2023-3519, CVE-2023-35081, CVE-2023-27997, CVE-2023-22515, CVE-2022-42475, CVE-2022-26134, CVE-2021-44228, CVE-2020-8515, CVE-2023-24229
TYPE		IMPACT	TOP AFFECTED PRODUCTS
Botnet		Information Theft, Compromise Infrastructure, Exfiltration of data	RARLAB, Ivanti, ServiceNow, PHP-CGI, Zyxel, Fortinet, Citrix, Atlassian, Apache, DrayTek
ASSOCIATED ACTOR			PATCH LINKS
Flax Typhoon			https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313,https://www.php.net/downloads,https://www.zyxel.com/global/en/support/download,https://fortiguard.fortinet.com/psirt/FG-IR-24-015,https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035,https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467,https://forums.ivanti.com/s/article/KB-Arbitrary-File-Write-CVE-2023-35081,https://www.fortiguard.com/psirt/FG-IR-23-097,https://www.atlassian.com/software/confluence/download-archives,https://www.fortiguard.com/psirt/FG-IR-22-398,https://jira.atlassian.com/browse/CONFSERVER-79016,https://logging.apache.org/security.html,https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-router-web-management-page-vulnerability-%28cve-2020-8515%29/

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	TOP TARGETED CVEs
Raptor Train	The Raptor Train botnet framework, active since mid-2020, has evolved into a sophisticated multi-tiered network that primarily targets SOHO networks and IoT devices. It enables scalable bot exploitation, remote control of C2 infrastructure, file transfers, command execution, and large-scale IoT-based DDoS attacks.	Exploiting Vulnerabilities on SOHO networks and IoT devices	CVE-2024-5217, CVE-2024-4577, CVE-2024-29973, CVE-2024-21762, CVE-2023-38035, CVE-2023-3519, CVE-2023-35081, CVE-2023-27997, CVE-2023-22515, CVE-2022-42475, CVE-2022-26134, CVE-2021-44228, CVE-2020-8515, CVE-2023-24229
		IMPACT	TOP AFFECTED PRODUCTS
TYPE		Sensitive Information Theft, Financial Loss, Compromised Infrastructure, Exfiltration of data	RARLAB, Ivanti, ServiceNow, PHP-CGI, Zyxel, Fortinet, Citrix, Atlassian, Apache, DrayTek
Framework			PATCH LINKS
ASSOCIATED ACTOR			https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313,https://www.php.net/downloads,https://www.zyxel.com/global/en/support/download,https://fortiguard.fortinet.com/psirt/FG-IR-24-015,https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035,https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467,https://forums.ivanti.com/s/article/KB-Arbitrary-File-Write-CVE-2023-35081,https://www.fortiguard.com/psirt/FG-IR-23-097,https://www.atlassian.com/software/confluence/download-archives,https://www.fortiguard.com/psirt/FG-IR-22-398,https://jira.atlassian.com/browse/CONFSERVER-79016,https://logging.apache.org/security.html,https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-router-web-management-page-vulnerability-%28cve-2020-8515%29/
Flax Typhoon			

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
VeilShell	VeilShell is a stealthy PowerShell-based malware used by North Korea's APT37. It's designed to evade detection and maintain persistence on compromised systems. The malware is often used as a backdoor to allow attackers to remotely access and control infected systems.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Stealthy access and Data exfiltration	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
APT37			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GorillaBot	GorillaBot is a new and advanced botnet that has executed over 300,000 DDoS attacks between September 4 to 27, 2024, targeting over 113 countries, including China and the U.S. It uses a variety of attack vectors, including UDP and TCP ACK floods, and exploits vulnerabilities in devices and systems.	Exploit vulnerabilities	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Massive DDoS attacks	-
Botnet			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JackalWorm	JackalWorm is a sophisticated piece of malware utilized by the GoldenJackal APT group. It detects presence of USB devices and replicates through them. Its primary function is to facilitate the spread of other malicious tools, notably the JackalControl trojan, across both air-gapped and connected systems.	Infected USB Drives	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Exfiltration	-
Worm			
ASSOCIATED ACTOR			PATCH LINK
GoldenJackal			--

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
GoldenDealer	GoldenDealer is a malicious component developed by the GoldenJackal APT group, designed to infiltrate air-gapped systems via USB drives. It monitors for USB insertion on compromised internet-connected machines and automatically copies itself and additional payloads onto the drives.	Infected USB Drives	-
		IMPACT	AFFECTED PRODUCTS
		Install other malware and Data exfiltration	-
TYPE			
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
GoldenJackal			--

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GoldenHowl	GoldenHowl is a modular backdoor malware developed by the GoldenJackal APT group, written in Python and designed to maintain control over infected systems. It is distributed as a self-extracting archive that contains both legitimate Python binaries and malicious scripts, allowing it to operate on internet-connected machines.	Infected USB Drives	-
		IMPACT	AFFECTED PRODUCTS
		Data exfiltration	-
TYPE			
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
GoldenJackal			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GoldenRobo	GoldenRobo is a malware tool utilized by the GoldenJackal APT group for file collection and data exfiltration from compromised systems. Operating on internet-connected PCs, it extracts files from USB drives and transmits them to an attacker-controlled server. Written in Go, GoldenRobo employs the legitimate Windows utility robocopy to facilitate its file-copying functions.	Infected USB Drives	-
		IMPACT	AFFECTED PRODUCTS
		Data exfiltration	-
TYPE			
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
GoldenJackal			--

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">GoldenAce</td><td rowspan="7">GoldenAce is a malware component used by the GoldenJackal APT group to propagate malicious software through USB drives targeting air-gapped systems. It operates by hiding malware on USB devices and automatically installing it on connected systems, facilitating the spread of other malicious components. GoldenAce employs a lightweight worm variant known as JackalWorm to enhance its distribution capabilities.</td><td>Infected USB Drives</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td rowspan="5">Install other malware</td><td rowspan="3">-</td></tr>
<tr><td><b>TYPE</b></td></tr>
<tr><td>Dropper</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>GoldenJackal</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="3">GoldenUsbCopy</td><td rowspan="7">GoldenUsbCopy is a malware component developed by the GoldenJackal APT group, designed to monitor USB drives and facilitate the theft of sensitive files. It operates by exfiltrating recently modified files that meet specific criteria, such as size and content type, without relying on AES encryption.</td><td>Infected USB Drives</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>Stealer</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>GoldenJackal</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
GoldenBlacklist	GoldenBlacklist is a malware component utilized by the GoldenJackal APT group to filter and archive specific email messages from compromised systems. It processes emails of interest before preparing them for exfiltration, ensuring that only valuable data is captured.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GoldenMailer	GoldenMailer is a malware component used by the GoldenJackal APT group to exfiltrate stolen information via email. It automates the process of sending collected files as email attachments to accounts controlled by the attackers, thereby facilitating data theft from compromised systems.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			--

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GoldenDrive	GoldenDrive is a malware component used by the GoldenJackal APT group to exfiltrate sensitive data by uploading it to Google Drive. This tool automates the process of transferring stolen files from compromised systems, enabling attackers to bypass traditional data transfer methods that might trigger security alerts.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			-

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
Akira	Akira ransomware, first identified in March 2023, targets both Windows and Linux systems, employing a hybrid encryption method using ChaCha20 and RSA. This ransomware utilizes a double extortion tactic, encrypting files and exfiltrating sensitive data before demanding large ransoms, often in the millions.	Exploiting Vulnerabilities	CVE-2024-40711 CVE-2024-40766
		IMPACT	AFFECTED PRODUCTS
TYPE		Data encryption and exfiltration, Financial Loss	Veeam Backup & Replication, SonicWall SonicOS
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
-			https://www.veeam.com/kb4600; https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Fog ransomware (aka Lost in the Fog)	Fog ransomware utilizes techniques such as 'pass-the-hash' attacks to escalate privileges, enabling it to access administrator accounts. Encrypted files typically receive the extensions .FOG or .FLOCKED.	Exploiting Vulnerabilities	CVE-2024-40711 CVE-2024-40766
		IMPACT	AFFECTED PRODUCTS
TYPE		Data encryption and exfiltration	Veeam Backup & Replication SonicWall SonicOS
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
-			https://www.veeam.com/kb4600; https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

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
StealHook	StealHook is an advanced backdoor designed for stealthy infiltration and data exfiltration. Its primary function is to harvest domain credentials from compromised systems, allowing attackers to infiltrate Microsoft Exchange servers within targeted organizations. Once inside, StealHook uses the compromised email accounts to exfiltrate sensitive data, through legitimate-looking email attachments.	Exploiting Vulnerabilities	CVE-2024-30088
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Steal Sensitive Data	Windows Kernel
ASSOCIATED ACTOR			**PATCH LINK**
APT34			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30088

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DULLDROP	DULLDROP is a stealthy Trojan that typically infiltrates systems as a secondary payload, either dropped by other malware or downloaded unknowingly from malicious websites. It remains inactive until executed with a specific argument, parameter, or component, or when triggered within a particular environment. This unique execution requirement allows DULLDROP to evade detection and avoid premature activation on unintended systems.	Dropped by malware	CVE-2024-30088
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Theft	Windows Kernel
ASSOCIATED ACTOR			**PATCH LINK**
APT34			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30088

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
TONESHELL	The TONESHELL backdoor employs a sophisticated side-loading technique and uses a precise series of commands to extract files from an infiltrated network.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
CeranaKeeper			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
WavyExfiller	WavyExfiller is a Python-based tool specifically designed to extract data from connected devices such as USB drives and hard drives. The tool targets external storage media, collecting sensitive files and information for later exfiltration. What sets WavyExfiller apart is its use of cloud-based services like Dropbox and PixelDrain to transfer stolen data, allowing it to bypass conventional detection mechanisms that monitor network traffic.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
CeranaKeeper			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
OneDoor	OneDoor is a sophisticated C++ backdoor that targets the Microsoft OneDrive REST API, leveraging its vulnerabilities to execute commands and facilitate data exfiltration.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
CeranaKeeper			-

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
BingoShell	BingoShell is a covert Python backdoor that exploits the pull request and issue comment features of GitHub to create a reverse shell. By leveraging these legitimate platform functionalities, BingoShell allows attackers to gain remote access to compromised systems, enabling them to execute commands and maintain control undetected.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
CeranaKeeper			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CoreWarrior	CoreWarrior is a persistent trojan designed for rapid propagation by generating numerous copies of itself. It reaches out to multiple IP addresses, establishing several sockets for backdoor access. This malware also hooks into Windows UI elements, enabling it to monitor user activities and interactions.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Trojan		System Compromise	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cerberus	Cerberus is a sophisticated Android banking malware, originally to steal financial data through various malicious techniques, including keylogging, overlay attacks, and remote control via VNC. The malware's capabilities include capturing keystrokes, executing overlay attacks for phishing, and enabling remote access to infected devices through VNC functionality. It can steal login credentials for banking apps, credit card details and other personal information.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Banking Trojan		Data Theft	Android
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
DarkVision RAT	DarkVision RAT is a highly flexible remote access trojan (RAT) written in C/C++ and assembly. Its powerful capabilities include keylogging, screen capturing, file manipulation, process injection, remote code execution, and password theft, making it a versatile tool for cybercriminals. Initially sold on Hack Forums and its official website for $40, the price of DarkVision RAT has since increased to $60, reflecting its growing demand and enhanced malicious features.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PureCrypter	PureCrypter is a .NET-based malware loader obfuscated using SmartAssembly, employing compression, encryption, and obfuscation techniques to evade detection by antivirus software. Its key features include persistence, code injection, and defense mechanisms, which are configurable using Google's Protocol Buffer message format. PureCrypter has been observed distributing a range of malicious payloads, including RATs and information stealers, making it a versatile and dangerous tool in cybercriminal campaigns.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Deploy malware	-
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
Donut	Donut is an open-source in-memory injector and loader designed for executing VBScript, JScript, EXE, DLL files, and .NET assemblies. As a shellcode generation tool, Donut creates x86 or x64 shellcode payloads from .NET assemblies, which can then be injected into arbitrary Windows processes. This allows attackers to run the injected code directly in memory, bypassing disk-based detection mechanisms. Due to its ability to execute a variety of file formats and deliver payloads stealthily.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Deploy malware	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Astaroth malware (aka Guildma)	Astaroth is a widely used information-stealing banking trojan, primarily targeting financial institutions in Latin America. Developed in Delphi, it employs advanced execution and attack methods to evade detection. In addition to stealing banking credentials, Astaroth seeks to capture login information for email accounts, e-commerce platforms, and streaming services.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Banking Trojan		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
Water Makara			-

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
SingleCamper	SingleCamper, a new variant of the RomCom malware family, utilizes advanced infection and evasion techniques. Typically distributed through phishing emails disguised as PDF attachments, it downloads additional malicious payloads from remote command-and-control servers. SingleCamper is equipped with capabilities for remote command execution and data exfiltration, while employing anti-sandbox techniques to evade detection.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
UAT-5647			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RustClaw	RustyClaw is a malware downloader built in RUST, incorporating advanced anti-analysis measures. Before initiating its malicious actions, the malware verifies the system's keyboard layout against specific language codes. Additionally, it generates a hash of its file name and checks it against a hardcoded value to prevent execution in sandbox environments with randomized file names. Once these checks are successful, RustyClaw can optionally display a decoy PDF to the infected user while downloading the next-stage implant to proceed with the attack.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Downloader		Downloads additional payload	-
ASSOCIATED ACTOR			PATCH LINK
UAT-5647			-

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
MeltingClaw	MeltingClaw is a C++-based downloader, sharing behavioral similarities with RustyClaw but featuring different configurations, such as distinct file names and storage locations. Like its counterpart, MeltingClaw downloads additional malicious payloads, but instead of traditional file storage, it stores these payloads within the Windows registry.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Downloads additional payload	-
ASSOCIATED ACTOR			**PATCH LINK**
UAT-5647			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DustyHammock	DustyHammock is a RUST-based backdoor designed to act as the central malicious component in an infection, facilitating communication with its command and control (C2) server and executing harmful actions. It begins by running hardcoded reconnaissance commands on the infected system, collecting information such as MAC addresses, Windows version, and the computer/username using the "whoami" and "chcp" commands. This data is then sent to the C2 server, which responds with specific tasks for DustyHammock to execute, enabling it to adapt and perform targeted malicious activities.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
UAT-5647			-

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
ShadyHammock	ShadyHammock is a C++-based backdoor equipped with the ability to bind to the system and listen for incoming requests. Its main functions include loading and executing payloads stored in designated registry locations, which are typically placed by its parent malware, MeltingClaw, and binding to localhost to receive commands from another malicious component.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
UAT-5647			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cicada3301	Cicada 3301 is a Rust-based ransomware that infiltrates systems and encrypts files with 36 different extensions, demanding a ransom for the decryption key. Beyond just encrypting data, it allows attackers to retain access to the compromised system, execute remote commands, and potentially return for further attacks, including data exfiltration and theft.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt data, Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Repellent Scorpius			-

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 CVE
Adload	AdLoad malware continues to infect Mac systems years after its initial emergence in 2017. As a package bundler, AdLoad has been documented distributing various subsequent payloads, including adware, bundleware, PiTM, backdoors, and proxy applications. It further entrenches itself by installing as a Launch Agent.	Potentially exploiting CVE-2024-44133 vulnerability	CVE-2024-44133
TYPE		IMPACT	AFFECTED PRODUCT
Loader		Privacy Breaches, Performance Issues, Annoyance from Ads, Financial Risks	macOS Sequoia 15
ASSOCIATED ACTOR			PATCH LINKS
-			https://support.apple.com/en-us/121238, https://support.apple.com/en-us/108382

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LockBit 3.0	LockBit 3.0 ransomware, encrypts data and may exfiltrate it, threatening to leak sensitive information if a ransom is not paid. Renowned for its stealthy tactics, it primarily targets enterprises and functions as a ransomware-as-a-service (RaaS).	Exploiting login credentials	-
TYPE		IMPACT	AFFECTED PRODUCT
Ransomware		Data Theft, Financial Loss, Operational Downtime, Reputation Damage	-
ASSOCIATED ACTOR			PATCH LINK
Crypt Ghouls			-

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 CVE
Babuk	Babuk ransomware is a newly emerged threat identified in 2021. It is a sophisticated ransomware designed for multiple platforms, with the most commonly utilized versions being for Windows and ARM for Linux. Additionally, ESX and a 32-bit legacy PE executable have been noted. Babuk employs an Elliptic Curve Algorithm to generate its encryption keys.	Exploiting login credentials	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft, Financial Loss, Operational Downtime, Reputation Damage	-
Ransomware			**PATCH LINK**
ASSOCIATED ACTOR			-
Crypt Ghouls			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SRBMiner	SRBMiner is a cryptominer targeting Docker hosts, specifically for mining XRP, a cryptocurrency developed by Ripple Labs. The attacker downloads SRBMiner from GitHub, installs it in the /usr/sbin directory, and initiates mining operations. This process compromises the integrity and security of Docker-based environments.	Docker remote API servers	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Resource Drain, Financial Risk, System Instability	-
Cryptominer			**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 CVE
Bumblebee	Bumblebee is an advanced malware loader identified in March 2022, primarily utilized by ransomware groups to deploy malicious payloads. Developed in C++, it utilizes sophisticated evasion methods, including Windows shortcut (.LNK) files and PowerShell commands, to achieve stealth and persistence.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Malicious Payload Delivery, System Compromise, Data Theft	Windows
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Stealc	Stealc is an information stealer offered as Malware-as-a-Service. It operates as a non-resident stealer with customizable data collection options and is developed using features from other well-known stealers. Written in C, it utilizes WinAPI functions and primarily targets data from web browsers, extensions, and desktop applications of cryptocurrency wallets.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Operational Disruption, Data Theft, Financial Loss	Windows and macOS
Information 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 CVE
Rhadamanthys	Rhadamanthys is an information stealer featuring a versatile array of modules and a multi-layered architecture. Available on the black market and regularly updated, it poses a continual threat. Its sophisticated design enables it to evade detection while carrying out various malicious activities, including the theft and exfiltration of sensitive information.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Operational Disruption, Data Theft, Financial Loss	Windows and macOS
Information stealer			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AMOS Stealer	Atomic, also known as AMOS, is macOS information-stealing malware currently delivered to targets via a fraudulent web browser update scheme called ClearFake.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Operational Disruption, Data Theft, Financial Loss	Windows and macOS
Information 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
Manuscrypt	Manuscrypt malware, also known as NukeSped, is an advanced tool for espionage and data theft. Its key features include keylogging to capture passwords, screen capture for recording user activities, and audio recording via the microphone. It also monitors clipboard data, gathers system information, and provides remote access for executing commands and manipulating files. These capabilities allow attackers extensive control over infected devices for surveillance and data exfiltration.	Exploiting vulnerabilities	CVE-2024-4947
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		Data Theft, Unauthorized Surveillance, Loss of Privacy, System Compromise, Persistent Access, Operational Disruption	Google Chromium V8
ASSOCIATED ACTOR			PATCH LINK
Lazarus Group			https://www.google.com/intl/en/chrome/?standalone=1

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Sliver	Sliver malware is an open-source, cross-platform framework designed for adversary emulation and red team operations. Its implants facilitate Command and Control (C2) communications through various protocols, such as mTLS, WireGuard, HTTP(S), and DNS, and are dynamically compiled with unique asymmetric encryption keys for each binary. This framework allows for the execution of commands and the delivery of payloads, including in-memory execution capabilities.	Exposed docker daemons	-
TYPE		IMPACT	AFFECTED PRODUCT
HackTool		Network Compromise, Operational Disruption, Increased Attack Surface	-
ASSOCIATED ACTOR			PATCH LINK
TeamTNT			-

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 CVE
Tsunami	Tsunami malware is a backdoor used by attackers to exploit vulnerable services and applications. It enables the execution of shell commands, and the downloading of malicious binaries, and turns compromised machines into launch points for additional attacks.	Exposed docker daemons	-
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		Remote Command Execution, Data Theft, Malware Propagation	-
ASSOCIATED ACTOR			PATCH LINK
TeamTNT			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Embargo	Embargo ransomware is a sophisticated and emerging threat, first detected in June 2024. It is believed to function as a ransomware-as-a-service (RaaS) model, enabling affiliates to deploy the malware in return for a portion of the ransom payments. Developed in Rust, a favored language for ransomware, it targets both Windows and Linux systems.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Encryption, Financial Loss, Reputational Damage	Windows, Linux
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CloudScout	CloudScout is a modular post-compromise toolkit developed in C#, allowing the team to customize its features specifically for the target environment. This toolset can extract data from multiple cloud services by utilizing stolen web session cookies. Additionally, CloudScout integrates smoothly with MgBot, via a plugin.	Leveraging stolen session cookies	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft, Potential for Further Intrusions, Loss of Privacy	-
Information stealer			PATCH LINK
ASSOCIATED ACTOR			-
Evasive Panda			

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 CVE
MgBot	MgBot is the hallmark malware framework of Evasive Panda, developed in C++ to access and exfiltrate data from various cloud services. It employs the pass-the-cookie technique to hijack authenticated sessions from web browsers.	-	-
TYPE		IMPACT	AFFECTED PRODUCT
Framework		Data Theft, Account Hijacking, Increased Attack Surface	-
ASSOCIATED ACTOR			PATCH LINK
Evasive Panda			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Nightdoor	Nightdoor is a sophisticated backdoor that leverages public cloud services for command-and-control communications. First detected in 2020, it establishes a reverse shell and employs anonymous pipes for input and output management. Additionally, Nightdoor can access file attributes, relocate and delete files, and execute self-uninstallation.	-	-
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		Unauthorized Access, System Control, Persistent Presence, Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
Evasive Panda			-

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 CVE
Pronsis	Pronsis Loader, developed in PHP, is converted into Java Virtual Machine (JVM) bytecode through the open-source JPHP project. Upon execution, Pronsis Loader triggers a complex malware delivery sequence that ultimately deploys SUNSPINNER and PURESTEALER.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Malware Propagation, System Compromise	Windows
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
UNC5812			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SUNSPINNER	SUNSPINNER is a deceptive graphical user interface (GUI) application developed using the Flutter framework and compiled for both Windows and Android platforms. Upon execution, SUNSPINNER seeks to connect to a new "backend server" and subsequently requests map markers, which are displayed on the app's GUI.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data Theft, Network Infection, Operational Disruption	Windows, Android
Information stealer			**PATCH LINK**
ASSOCIATED ACTOR			-
UNC5812			

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 CVE
PURESTEALER	PURESTEALER is a heavily obfuscated commodity infostealer developed in .NET, specifically designed to extract browser data, including passwords and cookies, as well as information from cryptocurrency wallets and various applications like messaging and email clients. It is marketed by the "Pure Coder Team," with pricing options ranging from $150 for a monthly subscription to $699 for a lifetime license.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Operational Disruption, Data Theft	Windows
Information stealer			**PATCH LINK**
ASSOCIATED ACTOR			-
UNC5812			

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRY	TARGETED REGION
FIN6 (aka Skeleton Spider, Gold Franklin, White Giant, ITG08, ATK 88, TAG-CR2, TAAL, Camouflage Tempest)	Unknown	Recruitment	Worldwide
	MOTIVE		
	Financial crime, Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	More_eggs	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.001: Malicious Link; T1037: Boot or Logon Initialization Scripts; T1037.001: Logon Script (Windows); T1218: System Binary Proxy Execution; T1218.010: Regsvr32; T1016: System Network Configuration Discovery; T1497: Virtualization/Sandbox Evasion; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1082: System Information Discovery; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1105: Ingress Tool Transfer; T1027: Obfuscated Files or Information; T1036: Masquerading; T1047: Windows Management Instrumentation; T1057: Process Discovery; T1053: Scheduled Task/Job			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
Flax Typhoon (aka Ethereal Panda, RedJuliett)	China	Military, Government, Higher Education, Telecommunications, Defense, Information Technology	Worldwide
	MOTIVE		
	Information theft, Espionage		
	TOP TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**TOP AFFECTED PRODUCTS**
	CVE-2024-5217, CVE-2024-4577, CVE-2024-29973, CVE-2024-21762, CVE-2023-38035, CVE-2023-3519, CVE-2023-35081, CVE-2023-27997, CVE-2023-22515, CVE-2022-42475, CVE-2022-26134, CVE-2021-44228, CVE-2020-8515, CVE-2023-24229	Nosedive, Raptor Train	RARLAB, Ivanti, ServiceNow, PHP-CGI, Zyxel, Fortinet, Citrix, Atlassian, Apache, DrayTek
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; TA0042: Resource Development; T1210: Exploitation of Remote Services; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1068: Exploitation for Privilege Escalation; T1071: Application Layer Protocol; T1505: Server Software Component; T1005: Data from Local System; T1571: Non-Standard Port; T1190: Exploit Public-Facing Application; T1204.002: Malicious File; T1027: Obfuscated Files or Information; T1496: Resource Hijacking; T1202: Indirect Command Execution; T1016: System Network Configuration Discovery; T1046: Network Service Discovery; T1104: Multi-Stage Channels; T1203: Exploitation for Client Execution; T1584.005: Botnet; T1584: Compromise Infrastructure; T1498: Network Denial of Service; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1588.001: Malware; T1587: Develop Capabilities; T1587.001: Malware			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
SloppyLemming (aka Outrider Tiger, Fishing Elephant)	India	Construction, Defense, Education, Energy, Equipment operators, Foreign Affairs, Government, IT providers, Law enforcement, Legislative, Logistics, Technology, Telecommunications, Textile, Transportation	Afghanistan, Bangladesh, Bhutan, China, Hong Kong, Indonesia, Japan, Macau, Maldives, Mongolia, Nepal, North Korea, Pakistan, South Korea, Sri Lanka, Taiwan
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2023-38831	-	RARLAB WinRAR
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1204: User Execution; T1204.002: Malicious File; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1562: Impair Defenses; T1055: Process Injection; T1212: Exploitation for Credential Access; T1580: Cloud Infrastructure Discovery; T1526: Cloud Service Discovery; T1530: Data from Cloud Storage; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1059.003: Windows Command Shell; T1068: Exploitation for Privilege Escalation; T1499: Endpoint Denial of Service; T1071: Application Layer Protocol			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT37 (aka Reaper, TEMP.Reaper, Ricochet Chollima, ScarCruft, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet)	North Korea	Aerospace, Automotive, Chemical, Education, Financial, Government, Healthcare, High-Tech, Manufacturing, Media, Technology, Transportation	Southeast Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	VeilShell	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1560: Archive Collected Data; T1132: Data Encoding; T1003: OS Credential Dumping; T1555: Credentials from Password Stores; T1027: Obfuscated Files or Information; T1070: Indicator Removal; T1070.004: File Deletion; T1112: Modify Registry; T1574: Hijack Execution Flow; T1574.014: AppDomainManager; T1033: System Owner/User Discovery; T1057: Process Discovery; T1069: Permission Groups Discovery; T1082: System Information Discovery; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.007: JavaScript; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
GoldenJackal	-	Government, Diplomatic Entities, Embassy	Europe, the Middle East, and South Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	JackalWorm, GoldenDealer, GoldenHowl, GoldenRobo, GoldenAce, GoldenUsbCopy, GoldenBlacklist, GoldenMailer, GoldenDrive	-
TTPs			
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1583.004: Server; T1584: Compromise Infrastructure; T1584.006: Web Services; T1587: Develop Capabilities; T1587.001: Malware; T1585: Establish Accounts; T1585.003: Cloud Accounts; T1588: Obtain Capabilities; T1588.002: Tool; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command: Shell; T1059.006: Python; T1106: Native API; T1569: System Services; T1569.002: Service Execution; T1204: User Execution; T1204.002: Malicious File; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547.001: Registry Run Keys /Startup Folder; T1547: Boot or Logon: Autostart Execution; T1053.005: Scheduled Task; T1564.001: Hidden Files and Directories; T1070.004: File Deletion; T1036.005: Match Legitimate Name or Location; T1036.008: Masquerade File Type; T1112: Modify Registry; T1027.013: Encrypted/Encoded File; T1552.001: Credentials In Files; T1552.004: Private Keys; T1087.001: Local Account; T1083: File and Directory Discovery; T1046: Network Service Discovery; T1120: Peripheral Device Discovery; T1057: Process Discovery; T1018: Remote System Discovery; T1518: Software Discovery; T1082: System Information Discovery; T1016.001: Internet Connection Discovery; T1135: Network Share Discovery; T1210: Exploitation of Remote Services; T1091: Replication Through Removable Media; T1560.002: Archive via Library; T1119: Automated Collection; T1005: Data from Local System; T1025: Data from Removable: Media; T1074.001: Local Data Staging; T1114.001: Local Email Collection; T1071.001: Web Protocols; T1092: Communication Through Removable Media; T1132.001: Standard Encoding; T1572: Protocol Tunneling; T1090.001: Internal Proxy; T1041: Exfiltration Over C2 Channel; T1052.001: Exfiltration over USB; T1132: Data Encoding; T1567.002: Exfiltration to Cloud Storage; T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol; T1016: System Network Configuration Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Awaken Likho (aka Core Werewolf, PseudoGamaredon)	-	Enterprises, Government	Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs

TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; T1593: Search Open Websites/Domains; T1593.002: Search Engines; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1204: User Execution; T1204.002: Malicious File; T1543: Create or Modify System Process; T1055: Process Injection; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1036.007: Double File Extension; T1083: File and Directory Discovery; T1057: Process Discovery; T1005: Data from Local System; T1070: Indicator Removal; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1133: External Remote Services; T1564.003: Hidden Window; T1059.010: AutoHotKey & AutoIT

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT34 (aka Earth Simnavaz, Helix Kitten, Twisted Kitten, Crambus, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13, DEV-0861, EUROPIUM, Hazel Sandstorm, Scarred Manticore, Evasive Serpens, Yellow Maero, Storm-0861, OilRig)	Iran **MOTIVE** Information theft and espionage	Aviation, Chemical, Defense, Education, Energy, Financial, Government, High-Tech, IT, Hospitality, Oil and gas, Telecommunications, Critical Infrastructure	Albania, Azerbaijan, Bahrain, China, Egypt, Iraq, Israel, Jordan, Kuwait, Lebanon, Mauritius, Oman, Pakistan, Qatar, Saudi Arabia, Turkey, UAE, UK, USA
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2024-30088	StealHook, DULLDROP	Windows Kernel

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1572: Protocol Tunneling; T1102: Web Service; T1132: Data Encoding; T1132.001: Standard Encoding; T1041: Exfiltration Over C2 Channel; T1556: Modify Authentication Process; T1556.002: Password Filter DLL; T1068: Exploitation for Privilege Escalation; T1105: Ingress Tool Transfer; T1078: Valid Accounts; T1078.003: Local Accounts; T1505: Server Software Component; T1505.003: Web Shell; T1048: Exfiltration Over Alternative Protocol; T1053: Scheduled Task/Job; T1070: Indicator Removal; T1112: Modify Registry; T1074: Data Staged; T1047: Windows Management Instrumentation

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
CeranaKeeper	China	Government	Thailand, Myanmar, Philippines, Japan, Taiwan, Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Singapore, Vietnam
	MOTIVE		
	Information theft and Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	TONESHELL, WavyExfiller, OneDoor, BingoShell	-
TTPs			
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.003: Virtual Private Server; T1587: Develop Capabilities; T1587.001: Malware; T1585: Establish Accounts; T1585.003: Cloud Accounts; T1072: Software Deployment Tools; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1140: Deobfuscate/Decode Files or Information; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1005: Data from Local System; T1039: Data from Network Shared Drive; T1074: Data Staged; T1074.001: Local Data Staging; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1132: Data Encoding; T1132.002: Non-Standard Encoding; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1573.002: Asymmetric Cryptography; T1090: Proxy; T1090.001: Internal Proxy; T1102: Web Service; T1102.002: Bidirectional Communication; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1588.002: Tool; T1588: Obtain Capabilities; T1105: Ingress Tool Transfer			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Water Makara	-	Manufacturing, Retail, Government, Healthcare, Construction, Automotive, Agriculture, Biotechnology, Technology, Media, Consulting	Latin America
	MOTIVE		
	Information theft and Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Astaroth malware (aka Guildma)	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1036: Masquerading; T1036.008: Masquerade File Type; T1568: Dynamic Resolution; T1568.002: Domain Generation Algorithms; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1132: Data Encoding; T1132.001: Standard Encoding			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5">UAT-5647 (aka RomCom, Tropical Scorpius, Void Rabisu, DEV-0978, Storm-0978)</td><td>Russia</td><td rowspan="3">Construction, Education, Energy, Financial, Government, Healthcare, High-Tech, Manufacturing, Shipping and Logistics, Transportation</td><td rowspan="3">Ukraine and Poland</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Information theft and espionage, Financial gain</td></tr>
<tr><th>TARGETED CVEs</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>-</td><td>SingleCamper (aka RomCom RAT, RomCom, SnipBot, RomCom 5.0), RustClaw, MeltingClaw, DustyHammock, ShadyHammock</td><td>-</td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1572; Protocol Tunneling; T1016: System Network Configuration Discovery; T1135: Network Share Discovery; T1033: System Owner/User Discovery; T1614: System Location Discovery; T1614.001: System Language Discovery; T1082: System Information Discovery; T1482: Domain Trust Discovery; T1083: File and Directory Discovery; T1069: Permission Groups Discovery; T1069.001: Local Groups; T1012: Query Registry; T1560: Archive Collected Data; T1003: OS Credential Dumping; T1104: Multi-Stage Channels; T1070: Indicator Removal; T1059: Command and Scripting Interpreter; T1059.001: PowerShell</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Repellent Scorpius	-	Advertising, Construction, Consulting & Professional Services, Consumer, E-commerce, Education, Financial Services, Food & Beverage, Gaming, Government, Healthcare, Hospitality, IT, Legal, Manufacturing, Medicine, Military, Real Estate, Retail, Technology, Telecommunications, Transportation, Travel & Tourism	United States, United Kingdom, Denmark, United Arab Emirates, Switzerland, Japan, Italy, England, Thailand, Canada, Greenland, Mexico, Nicaragua, Honduras, Cuba, Guatemala, Panama, Costa Rica, Dominican Republic, Haiti, Belize, El Salvador, Bahamas, Jamaica, Puerto Rico, Trinidad and Tobago, Dominica, Antigua and Barbuda, Barbados, Grenada
	MOTIVE		
	Information theft and espionage, Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Cicada3301	-

TTPs
TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1041: Exfiltration Over C2 Channel; T1574: Hijack Execution Flow; T1543: Create or Modify System Process; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1070: Indicator Removal; T1070.004: File Deletion; T1046: Network Service Discovery; T1016: System Network Configuration Discovery; T1570: Lateral Tool Transfer; T1486: Data Encrypted for Impact; T1490: Inhibit System Recovery; T1489: Service Stop; T1562: Impair Defenses; T1562.002: Disable Windows Event Logging; T1562.001: Disable or Modify Tools; T1562.004: Disable or Modify System Firewall; T1070.001: Clear Windows Event Logs; T1497: Virtualization/Sandbox Evasion; T1030: Data Transfer Size Limits;

NAME	ORIGIN	TARGETED INDUSTRY	TARGETED REGION
Crypt Ghouls	-	Business, Government, Mining, Energy, Finance, Retail	Russia
	MOTIVE		
	Financial Gain, Information Theft, Espionage, Sabotage, Destruction		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	LockBit 3.0, Babuk	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1199: Trusted Relationship; T1543: Create or Modify System Process; T1070: Indicator Removal; T1070.004: File Deletion; T1055: Process Injection; T1083: File and Directory Discovery; T1040: Network Sniffing; T1057: Process Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1486: Data Encrypted for Impact; T1490: Inhibit System Recovery; T1053: Scheduled Task/Job; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
UNC5820	-	All	All
	MOTIVE		
	Information Theft		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-47575	-	Fortinet FortiManager
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1190: Exploit Public-Facing Application; T1036: Masquerading; T1016: System Network Configuration Discovery; T1587: Develop Capabilities; T1587.003: Digital Certificates; T1074: Data Staged; T1585: Establish Accounts; T1585.002: Email Accounts; T1059: Command and Scripting Interpreter; T1222: File and Directory Permissions Modification			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Lazarus (aka UNC2970, Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor, Citrine Sleet, Gleaming Pisces)	North Korea	Cryptocurrency	Russia
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2024-4947	Manuscrypt	Google Chrome

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1588.005: Exploits; T1608: Stage Capabilities; T1608.001: Upload Malware; T1190: Exploit Public-Facing Application; T1583: Acquire Infrastructure; T1583.001: Domains; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.001: Malicious Link; T1132: Data Encoding; T1132.001: Standard Encoding; T1068: Exploitation for Privilege Escalation; T1036: Masquerading

NAME	ORIGIN	TARGETED INDUSTRY	TARGETED REGION
TeamTNT (aka Adept Libra)	-	All	Worldwide
	MOTIVE		
	Information Theft , Espionage, Sabotage, Destruction		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	Sliver, Tsunami	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1578: Modify Cloud Compute Infrastructure; T1578.002: Create Cloud Instance; T1211: Exploitation for Defense Evasion; T1036: Masquerading; T1552: Unsecured: Credentials; T1552.001: Credentials In Files; T1552.007: Container API; T1586: Compromise Accounts; T1586.003: Cloud Accounts; T1014: Rootkit; T1018: Remote System Discovery; T1102: Web Service; T1102.001: Dead Drop Resolver; T1071: Application Layer Protocol; T1071.004: DNS; T1090: Proxy; T1496: Resource Hijacking; T1588: Obtain Capabilities; T1588.006: Vulnerabilities			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
Evasive Panda (aka Bronze Highland, Daggerfly, Storm Cloud, StormBamboo)	China	Government and Religious organizations	Taiwan
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	CloudScout, MgBot, Nightdoor	Google Drive, Gmail, and Microsoft Outlook
TTPs			
TA0010: Exfiltration; TA0042: Resource Development; TA0004: Privilege Escalation; TA0002: Execution; TA0007: Discovery; TA0006: Credential Access; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0005: Defense Evasion; T1543.003: Windows Service; T1082: System Information Discovery; T1114.002: Remote Email Collection; T1114: Email Collection; T1095: Non-Application Layer Protocol; T1041: Exfiltration Over C2 Channel; T1548: Abuse Elevation Control Mechanism; T1027: Obfuscated Files or Information; T1550.004: Web Session Cookie; T1550: Use Alternate Authentication Material; T1548.002: Bypass User Account Control; T1140: Deobfuscate/Decode Files or Information; T1036.005: Match Legitimate Name or Location; T1036: Masquerading; T1560.001: Archive via Utility; T1569.002: Service Execution; T1543: Create or Modify System Process; T1185: Browser Session Hijacking; T1539: Steal Web Session Cookie; T1560: Archive Collected Data; T1530: Data from Cloud Storage; T1583.004: Server; T1583: Acquire Infrastructure; T1587.001: Malware; T1587: Develop Capabilities; T1569: System Services; T1106: Native API			

NAME	ORIGIN	TARGETED INDUSTRY	TARGETED COUNTRY
UNC5812	Russia	Military	Ukraine
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	Pronsis Loader, SUNSPINNER, PURESTEALER	Windows and Android
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0042: Resource Development; T1071.001: Web Protocols; T1053: Scheduled Task/Job; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1083: File and Directory Discovery; T1119: Automated Collection; T1203: Exploitation for Client Execution; T1041: Exfiltration Over C2 Channel; T1036: Masquerading; T1105: Ingress Tool Transfer; T1083: File and Directory Discovery; T1204.002: Malicious File; T1587.001: Malware; T1071: Application Layer Protocol; T1588.001: Malware; T1587: Develop Capabilities; T1588: Obtain Capabilities			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1592: Gather Victim Host Information	
	T1590: Gather Victim Network Information	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1598: Phishing for Information	T1598.003: Spearphishing Link
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.003: Virtual Private Server
		T1583.006: Web Services
		T1583.008: Malvertising
	T1587: Develop Capabilities	T1587.004: Exploits
		T1587.001: Malware
	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.006: Vulnerabilities
		T1588.005: Exploits
		T1588.003: Code Signing Certificates
	T1608: Stage Capabilities	T1608.001: Upload Malware
	T1650: Acquire Access	
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1584: Compromise Infrastructure	T1584.001: Domains
		T1584.002: DNS Server
		T1584.003: Virtual Private Server
		T1584.004: Server
		T1584.005: Botnet
	T1585: Establish Accounts	T1585.001: Social Media Accounts
TA0001: Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.001: Spearphishing Attachment
	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
	T1659: Content Injection	
	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
	T1091: Replication Through Removable Media	
	T1189: Drive-by Compromise	
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.001: Default Accounts
		T1078.004: Cloud Accounts

Tactic	Technique	Sub-technique
TA0002: Execution	T1204: User Execution	T1204.002: Malicious File
		T1204.001: Malicious Link
	T1203: Exploitation for Client Execution	
	T1047: Windows Management Instrumentation	
	T1609: Container Administration Command	
	T1053: Scheduled Task/Job	T1053.006: Systemd Timers
		T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.002: AppleScript
		T1059.009: Cloud API
		T1059.003: Windows Command Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.004: Unix Shell
		T1059.007: JavaScript
		T1059.008: Network Device CLI
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
		T1071.002: File Transfer Protocols
	T1090: Proxy	
	T1572: Protocol Tunneling	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1571: Non-Standard Port	
	T1659: Content Injection	
	T1573: Encrypted Channel	
	T1219: Remote Access Software	
	T1001: Data Obfuscation	
TA0006: Credential Access	T1003: OS Credential Dumping	
	T1056: Input Capture	T1056.001: Keylogging
	T1212: Exploitation for Credential Access	
	T1110: Brute Force	T1110.003: Password Spraying
	T1556: Modify Authentication Process	
	T1040: Network Sniffing	
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	T1552.004: Private Keys
	T1555: Credentials from Password Stores	T1555.005:Password Managers
		T1555.003: Credentials from Web Browsers

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.003: NTDS
	T1557: Adversary-in-the-Middle	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
TA0009: Collection	T1560: Archive Collected Data	
	T1056: Input Capture	T1056.001: Keylogging
	T1115: Clipboard Data	
	T1123: Audio Capture	
	T1584: Compromise Infrastructure	
	T1005: Data from Local System	
	T1557: Adversary-in-the-Middle	
	T1113: Screen Capture	
	T1530: Data from Cloud Storage	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0008: Lateral Movement	T1021: Remote Services	T1021.004: SSH
		T1021.002: SMB/Windows Admin Shares
		T1021.001: Remote Desktop Protocol
	T1570: Lateral Tool Transfer	
	T1563: Remote Service Session Hijacking	T1563.001: SSH Hijacking
		T1563.002: RDP Hijacking
	T1210: Exploitation of Remote Services	
	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
		T1550.002: Pass the Hash
TA0010: Exfiltration	T1048: Exfiltration Over Alternative Protocol	T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
		T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
		T1567.001: Exfiltration to Code Repository
	T1041: Exfiltration Over C2 Channel	
	T1020: Automated Exfiltration	
	T1537: Transfer Data to Cloud Account	
TA0003: Persistence	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1556: Modify Authentication Process	

Tactic	Technique	Sub-technique
TA0003: Persistence	T1098: Account Manipulation	T1098.005: Device Registration
	T1176: Browser Extensions	
	T1133: External Remote Services	
	T1136.002: Create Account	T1136.001: Local Account
		T1136.002: Domain Account
	T1505: Server Software Component	T1505.003: Web Shell
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1137: Office Application Startup	T1137.001: Office Template Macros
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1543.001: Launch Agent
		T1543.004: Launch Daemon
TA0004: Privilege Escalation	T1098: Account Manipulation	T1098.005: Device Registration
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1543.001: Launch Agent
		T1543.004: Launch Daemon
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
	T1055: Process Injection	
	T1134: Access Token Manipulation	
	T1068: Exploitation for Privilege Escalation	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.002: DLL Side-Loading
		T1574.014: AppDomainManager
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
TA0040: Impact	T1498: Network Denial of Service	
	T1561: Disk Wipe	T1561.001: Disk Content Wipe
	T1499: Endpoint Denial of Service	
	T1565: Data Manipulation	
	T1657: Financial Theft	
	T1489: Service Stop	
	T1486: Data Encrypted for Impact	
	T1496: Resource Hijacking	
	T1485: Data Destruction	
	T1490: Inhibit System Recovery	
	T1491: Defacement	T1491.001: Internal Defacement

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1112: Modify Registry	
	T1218: System Binary Proxy Execution	T1218.007: Msiexec
		T1218.005: Mshta
	T1070: Indicator Removal	T1070.006: Timestomp
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1600: Weaken Encryption	
	T1564: Hide Artifacts	T1564.001:Hidden Files and Directories
	T1550: Use Alternate Authentication Material	
	T1014: Rootkit	
	T1578: Modify Cloud Compute Infrastructure	
	T1036: Masquerading	
	T1656: Impersonation	
	T1134: Access Token Manipulation	
	T1140: Deobfuscate/Decode Files or Information	
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.009: Embedded Payloads
		T1027.010: Command Obfuscation
	T1562: Impair Defenses	T1562.001:Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
TA0007: Discovery	T1087: Account Discovery	T1087.002: Domain Account
	T1033: System Owner/User Discovery	
	T1049: System Network Connections Discovery	
	T1057: Process Discovery	
	T1007: System Service Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1124: System Time Discovery	
	T1217: Browser Information Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1614: System Location Discovery	T1614.001: System Language Discovery
	T1622: Debugger Evasion	
	T1518: Software Discovery	
	T1580: Cloud Infrastructure Discovery	
	T1046: Network Service Discovery	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	T1069.001: Local Groups
	T1069: Permission Groups Discovery	T1069.001: Local Groups
	T1482: Domain Trust Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1040: Network Sniffing	
	T1497: Virtualization/Sandbox Evasion	

Top 5 Takeaways

#1

In **October**, there were twenty-one zero-day vulnerabilities with ‘Three Celebrity Vulnerabilities' taking center stage. These featured flaws such as **ZeroLogon**, **Log4shell**, and **HM Surf**.

#2

Throughout the month, ransomware strains including **Akira, Fog, Cicada3301, LockBit 3.0, Babuk,** and **Embargo Ransomware** actively targeted victims.

#3

A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These include the **Tsunami, Embargo, CloudScout, CoreWarrior, Cerberus, DarkVision RAT, SRBMiner, Bumblebee, Stealc, Rhadamanthys, VeilShell and GorillaBot.**

#4

Seventeen active adversaries were identified across multiple campaigns, targeting the following key industries: **Government, Technology, Education, Healthcare** and **Retail.**

#5

Multiple campaigns leveraging sophisticated, previously unseen malware and ransomware variants orchestrated a total of **53** attacks. These attacks top impacted **Russia, Thailand, Indonesia, Malaysia, and Philippines.**

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **41 significant vulnerabilities** and block the indicators related to the **17 active threat actors, 53 active malware,** and **182 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 **41 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 (October 2024)

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

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

🐞	Red Vulnerability Report	🗡	Amber Attack Report
🐛	Amber Vulnerability Report	👽	Red Actor Report
🦗	Green Vulnerability Report	👾	Amber Actor Report
⚔	Red Attack Report		

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

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

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

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

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

Glossary:

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

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
XMRig	SHA256	505237e566b9e8f4a83edbe45986bbe0e893c1ca4c5837c97c6c4700cfa0930a, 0af1b8cd042b6e2972c8ef43d98c0a0642047ec89493d315909629bcf185dffd, c5391314ce789ff28195858a126c8a10a4f9216e8bd1a8ef71d11c85c4f5175c
	URL	hxxps[:]//solscan[.]live/bin/64bit/xmrig, hxxps[:]//solscan[.]live/bin/xmrig, hxxps[:]//solscan[.]live/so/xmrig[.]so
More_eggs	SHA256	e1b4911959b6ca0db40873983e1f9d76e637818cb05d74e70b83701a5f4f4ef4, d207aebf701c7fb44fe06993f020ac3527680c7fa8492a0b5f6154ca
Raptor Train	IPv4	114[.]255[.]70[.]20, 5[.]188[.]33[.]135, 202[.]182[.]109[.]151, 5[.]188[.]33[.]228, 185[.]14[.]45[.]160, 185[.]207[.]154[.]253, 14[.]1[.]98[.]223, 223[.]98[.]159[.]112, 210[.]61[.]186[.]117, 104[.]244[.]89[.]157, 114[.]255[.]70[.]30, 140[.]82[.]14[.]222, 45[.]32[.]196[.]165, 66[.]42[.]118[.]156, 85[.]90[.]216[.]178, 85[.]90[.]216[.]184, 23[.]236[.]69[.]82, 23[.]236[.]68[.]161, 23[.]236[.]69[.]110, 23[.]236[.]68[.]229, 208[.]85[.]16[.]100, 222[.]186[.]48[.]201, 222[.]186[.]48[.]204, 37[.]9[.]35[.]91,

Attack Name	TYPE	VALUE
Raptor Train	IPv4	149[.]28[.]98[.]243, 66[.]42[.]83[.]4, 45[.]91[.]82[.]49, 45[.]91[.]82[.]78, 66[.]42[.]101[.]23, 92[.]223[.]30[.]61, 92[.]223[.]30[.]95, 216[.]128[.]183[.]154, 37[.]61[.]229[.]163, 37[.]61[.]229[.]171, 45[.]32[.]185[.]75, 45[.]65[.]9[.]216, 45[.]65[.]9[.]235, 45[.]65[.]9[.]28, 92[.]223[.]30[.]82, 216[.]128[.]128[.]245, 195[.]234[.]62[.]188, 195[.]234[.]62[.]192, 85[.]90[.]216[.]69, 195[.]234[.]62[.]184, 89[.]44[.]198[.]200, 207[.]148[.]68[.]131, 108[.]61[.]177[.]81, 45[.]80[.]215[.]149, 45[.]92[.]70[.]111, 45[.]13[.]199[.]140, 45[.]13[.]199[.]152, 45[.]13[.]199[.]207, 45[.]13[.]199[.]84, 45[.]13[.]199[.]96, 45[.]13[.]199[.]104, 45[.]13[.]199[.]45, 45[.]135[.]117[.]136, 45[.]10[.]58[.]133, 45[.]10[.]58[.]130, 85[.]90[.]216[.]111, 5[.]8[.]33[.]26, 45[.]10[.]58[.]128, 195[.]234[.]62[.]197, 45[.]92[.]70[.]68, 5[.]45[.]184[.]68, 195[.]234[.]62[.]198, 92[.]38[.]185[.]47, 92[.]38[.]185[.]43, 85[.]90[.]216[.]112, 45[.]10[.]58[.]129, 5[.]181[.]27[.]219, 92[.]38[.]185[.]44, 45[.]135[.]117[.]131, 85[.]90[.]216[.]110,

Attack Name	TYPE	VALUE
Raptor Train	IPv4	37[.]61[.]229[.]17, 37[.]9[.]35[.]89, 85[.]90[.]216[.]116, 37[.]61[.]229[.]15, 92[.]38[.]185[.]46, 45[.]80[.]215[.]186, 85[.]90[.]216[.]115, 45[.]10[.]58[.]132, 92[.]38[.]185[.]45, 45[.]92[.]70[.]71, 207[.]148[.]122[.]69, 91[.]216[.]190[.]154, 23[.]236[.]68[.]193, 91[.]216[.]190[.]247, 91[.]216[.]190[.]74, 45[.]80[.]215[.]47, 139[.]180[.]137[.]219, 149[.]248[.]51[.]22, 65[.]20[.]97[.]251, 45[.]77[.]231[.]209, 78[.]141[.]238[.]97, 155[.]138[.]133[.]56, 92[.]38[.]178[.]232, 92[.]223[.]30[.]233, 92[.]38[.]135[.]146, 92[.]223[.]30[.]232, 92[.]223[.]30[.]241, 155[.]138[.]151[.]225, 5[.]181[.]27[.]19, 5[.]181[.]27[.]6, 195[.]234[.]62[.]18, 45[.]80[.]215[.]153, 45[.]80[.]215[.]154, 45[.]80[.]215[.]156, 92[.]38[.]176[.]156, 45[.]80[.]215[.]151, 5[.]181[.]27[.]21, 45[.]92[.]70[.]113, 45[.]92[.]70[.]115, 195[.]234[.]62[.]19, 92[.]38[.]176[.]131, 45[.]92[.]70[.]112, 45[.]80[.]215[.]150, 45[.]80[.]215[.]155, 89[.]44[.]198[.]195, 45[.]80[.]215[.]152, 89[.]44[.]198[.]254, 91[.]216[.]190[.]2, 91[.]216[.]190[.]80, 23[.]236[.]68[.]213,

Attack Name	TYPE	VALUE
VeilShell	SHA256	BEAF36022CE0BD16CAAEE0EBFA2823DE4C46E32D7F35E793AF4E1538E705379F, 9D0807210B0615870545A18AB8EAE8CECF324E89AB8D3B39A461D45CAB9EF957, 106C513F44D10E6540E61AB98891AEE7CE1A9861F401EEE2389894D5A9CA96EF, 6B95BC32843A55DA1F8186AEC06C0D872CAC13D9DF6D87114C5F8B7277C72A4F, AF74D416B65217D0B15163E7B3FD5D0702D65F88B260C269C128739E7E7A4C4D, 7E9F91F0CFE3769DF30608A88091EE19BC4CF52E8136157E4E0A5B6530D510EC
GorillaBot	MD5	276adc6a55f13a229a5ff482e49f3a0b, 63cbfc2c626da269c67506636bb1ea30, 7f134c477f307652bb884cafe98b0bf2, 3a3be84df2435623132efd1cd9467b17, 03a59780b4c5a3c990d0031c959bf7cc, 5b37be51ee3d41c07d02795a853b8577, 15f6a606ab74b66e1f7e4a01b4a6b2d7
	URL	hxxp[://]pen.gorillafirewall[.]su/
	SHA256	22a545fdb6ebbc5ba351c97d32cd008a1550a49891ae6112ddc8a6370376f053, 4cac6023b760e1fdae8c096a4db425eae3bbfe0d2554551efb76fc2f2d3a6b1b, e8320657b9ff24198170e6b30188304555b43281b654075052721717f66fb4df, 42845557a515bc05c290b3ab9d1ad291303691d472db9e09863bfc782b803ed2, d99d10559f1ad6bba1b59913604e261a613daa94af01ade8276effd692b5c03f, 826f9c8153c14a66ba730291e5f78d71d958c08cde45e2119afa227211ee5132, 6d10e4da8d8090e0e7e077ef4aead8b8720d1bd4f9b86d34ae66eac0e17e659c, b4a2a1900bab5b6e405cc78b72c5d1706c789b309bc1fa27ad746153ccb84004, 3905126f5f9f7430dee31c207706852e56292291449b563781bc6ee0b540343a, d4007f1ac2cb3a48db4bde7dbab7255421bf64f768a06492b81087f67a2e6c9c, e03580729f2f09dbd937d685fc9229959e84c9f329bee7eee16536bb8f9e60cf, 81c775f9540a66fded643fe4ec53dbbf35742bd3b069d95d689da313fc9b80a9

Attack Name	TYPE	VALUE
JackalWorm	SHA1	a87ceb21ef88350707f278063d7701bde0f8b6b7
GoldenDealer	SHA1	da9562f5268fa61d19648dff9c6a57fb8ab7b0d7
GoldenHowl	SHA1	5f12ffd272aabc0d5d611d18812a196a6ea2faa9
GoldenRobo	SHA1	6de7894f1971fdc1df8c4e4c2edcc4f4489353b6
GoldenAce	SHA1	24fbcec23e8b4b40fea188132b0e4a90c65e3ffb
GoldenUsbCopy	SHA1	7cb7c3e98cab2226f48ba956d3be79c52ab62140
GoldenBlacklist	SHA1	9cbe8f7079da75d738302d7db7e97a92c4de5b71
GoldenMailer	SHA1	c830efd843a233c170285b4844c5960ba8381979
GoldenDrive	SHA1	f7192914e00dd0ce31df0911c073f522967c6a97
Akira Ransomware	SHA256	8a2d54e3230a4e7656ca760b512a879e0cacbe912a519a1be6916449bd6b5628, 87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d, 58e685695afc3a85d2632777a2b54967dc53d6a6fa1b7e2c110b2023b561bfe9, 1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218, 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c, ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d, c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddccd5bb37857e7bde6d2eb7, a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc, 2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422, 74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1
Fog Ransomware	SHA256	e67260804526323484f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3

Attack Name	TYPE	VALUE
StealHook	SHA256	a24303234e0cc6f403fca8943e7170c90b69976015b6a84d64a9667810023ed7
DULLDROP	SHA256	b3257f0c0ef298363f89c7a61ab27a706e9e308c22f1820dc4f02dfa0f68d897, 54e8fbae0aa7a279aaedb6d8eec0f95971397fea7fcee6c143772c8ee6e6b498
TONESHELL	SHA256	e6ab24b826c034a6d9e152673b91159201577a3a9d626776f95222f01b7c21db, 6655c5686b9b0292cf5121fc6346341bb888704b421a85a15011456a9a2c192a, b15ba83681c4d2c2716602615288b7e64a1d4a9f4805779cebdf5e6c2399afb5
	File Name	MsOcrRes.orp, avk.dll, TurboActivate.dll
WavyExfiller	SHA256	e7b6164b6ec7b7552c93713403507b531f625a8c64d36b60d660d66e82646696, 451ee465675e674cebe3c42ed41356ae2c972703e1dc7800a187426a6b34efdc
	File Name	SearchApp.exe
OneDoor	SHA256	3f81d1e70d9ee39c83b582ac3bcc1cdfe038f5da31331cdbcd4ff1a2d15bb7c8
	File Name	OneDrive.exe
BingoShell	SHA256	24e12b8b1255df4e6619ed1a6ae1c75b17341eef7418450e661b74b144570017
	File Name	Update.exe
CoreWarrior	SHA256	85A6E921E4D5107D13C1EB8647B130A1D54BA2B6409118BE7945FD71C6C8235F, 8C97329CF7E48BB1464AC5132B6A02488B5F0358752B71E3135D9D0E4501B48D
Cerberus	SHA256	6c045a521d4d19bd52165ea992e91d338473a70962bcfded9213e592cea27359, 4c7f90d103b54ba78b85f92d967ef4cdcc0102d3756e1400383e774d2f27bb2e, 8f3e3a2a63110674ea63fb6abe4a1889fc516dd6851e8c47298c7987e67ff9b6, c570e075f9676e79a1c43e9879945f4fe0f54ef5c78a5289fe72ce3ef6232a14, a2c701fcea4ed167fdb3131d292124eb55389bc746fcef8ca2c8642ba925895c, 8faa93be87bb327e760420b2faa33f0f972899a47c80dc2bc07b260c18dfcb14, ee87b4c50e5573cba366efaa01b8719902b8bed8277f1903e764f9b4334778d0

Attack Name	TYPE	VALUE
Cerberus	SHA256	136d00629e8cd59a6be639b0eaef925fd8cd68cbcbdb71a3a407836c560b8579, 516282073b7d81c630d4c5955d396e1e47a2f476f03dea7308461fa62f465c11, 5bd21d0007d34f67faeb71081309e25903f15f237c1f7b094634584ca9dd873e, 6b8911dfdf1961de9dd2c3f9b141a6c5b1029311c66e9ded9bca4d21635c0c49, befe69191247abf80c5a725e1f1024f7195fa85a7af759db2546941711f6e6ae, 9d966baefa96213861756fde502569d7bba9c755d13e586e7aaca3d0949cbdc3, 0c27ec44ad5333b4440fbe235428ee58f623a878baefe08f2dcdad62ad5ffce7, 880c9f65c5e2007bfed3a2179e64e36854266023a00e1a7066cbcf8ee6c93cbc,
	SHA1	c7ebf2adfd6482e1eb2c3b05f79cdff5c733c47b
	MD5	f9d5b402acee67675f87d33d7d52b364
DarkVision RAT	Domain	severdops[.]ddns[.]net[:]8120
	SHA256	7aa49795bbe025328e0aa5d76e46341a95255e13123306311671678fdeabb617, 0de5f042eb250092454d786b6303dee434202d45dc3fec9e6b39237f9e92514f, 0fa8acdb672f0e6c184fc5d04bb8af92c0bf5db73de096606f23f4c38ef3347b, 10667e9d67706397f7ff96e892d3c0f0ae05d81df5bc17caf85fb356d531c0b8, 1a230bb362cde9ead2d9f867af181ae51292c626a3c9d1d30f5f3751b84ffe85, 201f31c84755a5cd6081c3db30626cc3f17cf84804c2deb66e27866daad259a3, 3295199ba2b4e9cfc448a574cb9e89f3ef131fd19dcf366fe2abb7b3b79eb887, 40d48f5e965a250ac45f2f9c9426743c66fe899f07e16c42339149e30b1956e9, 44de5a248b6e9c24ad547e73c3ba3c8cc9693ba6eaa5190be9b377845844ffb6, 47070e4f6545f9f1308a5aec1e6943e6a29891bce9523db5596544a52f9b3bf4, 478cf5482905fa2ac2a2280a03ad6716f153c372c15cd957a23a67ff3260c867, 5174ef9f7d5420ab4890173792d8aafc50b8bb3191b4c24f6f58ae73bd7212c3,

Attack Name	TYPE	VALUE
DarkVision RAT		5cce814cadb4fac6631ff3c988516b4c6618f0c71c7de3588fc0d7038c220f31, 7f97ba9a8e6b70708a001cff8677992fc1e768a62f9f21ddd14fb1c6924281bc, 808680e6761782a7817fd8e3f90463738d17216b3bca51f3ca4e7375458cba1b, a3bd7d3e7006439d1d53cf8db1f403df2162c8f7e8172d6911be203ea58a2d8d, b75354d8ad3f4e0f675ec6a64c82226d75116535198ef4974b17984ccebab63e, bf1c8cf3ab6213c250d1abf8094180fdcf8e871674482fce1930abe9826e61b9, cb06287e314bf4c684323c7925922cce2932a9e9e9b6aac34634487ac7741afd, e91586b66e6d05e3b118991b72896d37c3e625e4f54ceb4ad6b04f047a31593b, eafa30bac261cc682556812c7c513827f09ef75fc33dbeb61e5d3ff46c9f3808, ee1b2b016b56950986db7b08f451220b91f1d91a70fec0624e289e96c648cb44, f36626f1a71c68c4647347b25eb0000c0e6c5d7700cf16047a3d9967321cf14b, F3b00f34857586056178a56517e4c07effe1182604b11665fb8efb71be78cec4
PureCrypter	SHA256	27ccb9f336282e591e44c65841f1b5bc7f495e8561349977680161e76857be5d, 0a06a5dbe4358d59077f92924cc1418dc0919e2c8f97b92cc5cf5d8bcc83d844
Donut	SHA256	6e3346d47044d6df85a07aeda745d88f9cd46b20d22028d231add555bf00bf41
Astaroth malware (aka Guildma)	URLs	annotmykim[.]gruposenhordobonfim[.]io/?2/, blogonbel84[.]gruposenhordobonfim[.]org/?1/, blogonben[.]gruposenhordobonfim[.]org/?1/, blogonben8[.]gruposenhordobonfim[.]org/?1/, bruconlincol587[.]luminisconsultoria[.]io/?3/, bruncolinc59[.]lumiscoconsupoltronsia[.]org/?3/, claronqual[.]gruposenhordobonfim[.]org/?2/, clindnor[.]cenithbonfim[.]net/?2/, crafer[.]grupobonfim[.]net/?5/, crecil[.]gruposenhordobonfim[.]org/?2/, crgricill[.]gruposenhordobonfim[.]net/?3/, crigonval[.]gruposenhordobonfim[.]org/?5/, crigoval[.]gruposenhordobonfim[.]org/?5/,

Attack Name	TYPE	VALUE
Astaroth malware (aka Guildma)	URLs	pcrigvalbon[.]gruposenhordobonfim[.]org/?2/, dragounzolonoff[.]ceritbonfim[.]com/?3/, dramainco54[.]groupomonflowsacodonbonsait[.]io/?2/, drapunzol[.]cemiteriobonfim[.]com/?1/, drapunzol[.]cemiteriobonfim[.]com/?5/, drocannanbel[.]veritasinvest[.]io/?1/, florvaz[.]cemisionfinanceinvest[.]com/?3/, flovaz138[.]cemiteriobonfim[.]com/?3/, frulinzol[.]grupobonfim[.]org/?5/, gaminqual[.]soluclaoled[.]world/?2/, gramdinlhar[.]grupobonfim[.]org/?5/, graminqual[.]solucaoled[.]world/?2/, grammidhal[.]gruposenhordobonfim[.]org/?1/, htruriz[.]grupobonfim[.]net/?3/, murankel.limpanzin[.]io/?2/, plaminel516[.]gruposenhordobonfim[.]com/?1/, planhal[.]grupobonfim[.]org/?1/, planhalconnalminsenior[.]io/?3/, plarandiz[.]gruposenhordobonfim[.]org/?3/, plikinvintez371[.]gruposenhordobonfim[.]com/?3/, plikkentin37h[.]gruposenhordobonfim[.]com/?3/, prawinvinbil2[.]clienteasciendig[.]world/?2/, prawinzinbil66[.]clienteasciendig[.]world/?2/, prawinzinbil66[.]clienteascindig[.]world/?2/, pregonfer[.]gruposenhordobonfim[.]com/?5/, rehenninlhar[.]gruposenhordobonfim[.]org/?2/, prenharbisonvirenanal3[.]plurianbonfim[.]net/?2/, prenherninal6v[.]gruposenhordobonfim[.]com/?2/, prepor854[.]grupobonfim[.]net/?1/, prerherningbron38[.]grupatibonfim[.]net/?2/, prisonfinfel[.]grupobonfim[.]org/?3/, pritonggopatrimoniosoberano[.]world/?5/, pritongongor[.]patrimoniosoberano[.]world/?5/, rawinzinbil66[.]clienteascindig[.]world/?2/, rigonval[.]gruposenhordobonfim[.]org/?5/, sasanal[.]gruposenhordobonfim[.]org/?2/, scropenpaz[.]subindometa[.]world/?1/, sp[.]runal[.]pad[.]rimonios[.]oberano[.]world/?5/, sprunal[.]patrimoniosoberano[.]world/?5/, spunalu[.]patrimoniosoberano[.]world/?5/, stragir[.]nexuspatrimonial[.]city/?3/, stragiran48xpatrimonianal[.]city/?3/, stredenpintal7[.]sistemapreparatorio[.]io/?5/,

Attack Name	TYPE	VALUE
Astaroth malware (aka Guildma)	URLs	strehen78zinal[.]islandofinvolomartyreasurgical[.]io/?5/, strehensinvel[.]jllldobrasil[.]world/?1/, stresanal[.]gruposenhordobonfim[.]com/?2/, tibilaniznale7[.]intyoberbonfim[.]net/?2/, titblansuperioniank3[.]cenithbonfim[.]net/?3/, tribenpantrimonianal[.]cfdauctions[.]org/?2/, tripanroncol68[.]aberturaazulvision[.]xyz/?5/, tritanpinvaz[.]nexuspatrimonial[.]city/?5/, tritum[.]gruposenhordobonfim[.]org/?5/, trubenpal[.]paineira[.]cfd/?2/, trugomen[.]copinasultanbolimansire[.]io/?2/, trugonmennil[.]luminisconsultoria[.]io/?3/, trujanel[.]gruposenhordobonfim[.]net/?5/, urnasinvest[.]yunusgroup[.]net/?2/, valcredonlin59[.]unicicomonsultanlonko[.]org/?1/, valentinvest37[.]patrickbonfim[.]net/?5/, vaval[.]gruposenhordobonfim[.]net/?5/, velvinet6[.]unovetsnahels[.]org/?3/, veritasinvestio[.]io/?1/, veritasinvestio[.]io/?3/, vinherena[.]sonyofbonfim[.]net/?3/
SingleCamper	SHA256	dee849e0170184d3773077a9e7ce63d2b767bb19e85441d9c55ee44d6f129df9, 2474a6c6b3df3f1ac4eadcb8b2c70db289c066ec4b284ac632354e9dbe488e4d
RustClaw	SHA256	12bf973b503296da400fd6f9e3a4c688f14d56ce82ffcfa9edddd7e4b6b93ba9, 260a6644ab63f392d090853ccd7c4d927aba3845ced473e13741152cdf274bbd, 9062d0f5f788bec4b487faf5f9b4bb450557e178ba114324ef7056a22b3fbe8b, 43a15c4ee10787997682b79a54ac49a90d26a126f5eeeb8569022850a2b96057, aa09e9dca4994404a5f654be2a051c46f8799b0e987bcefef2b52412ac402105, 585ed48d4c0289ce66db669393889482ec29236dc3d04827604cf778c79fda36, 62f59766e62c7bd519621ba74f4d0ad122cca82179d022596b38bd76c7a430c4, 9fd5dee828c69e190e46763b818b1a14f147d1469dc577a99b759403a9dadf04, b1fe8fbbb0b6de0f1dcd4146d674a71c511488a9eb4538689294bd782df040df,

Attack Name	TYPE	VALUE
RustClaw	SHA256	7602e2c1ae27e1b36ee4aed357e505f14496f63db29fb4fcdd0d8a9db067a5c4, f3fe04a7e8da68dc05acb7164b402ffc6675a478972cf624de84b3e2e4945b93, 10e1d453d4f9ca05ff6af3dcd7766a17ca1470ee89ba90feee5d52f8d2b18a4c, a265ae8fed205efb5bcc2fb59e60f743f45b7ad402cb827bc98dee397069830c, 8104fdf9ff6be096b7e5011e362400ee8dd89d829c608be21eb1de959404b4b9, b55f70467f13fbad6dde354d8653d1d6180788569496a50b06f2ece1f57a5e91, bd25618f382fc032016e8c9bc61f0bc24993a06baf925d987dcec4881108ea2a, 78eaaf3d831df27a5bc4377536e73606cd84a89ea2da725f5d381536d5d920d8, 88a4b39fb0466ef9af2dcd49139eaff18309b32231a762b57ff9f778cc3d2dd7, 01ebc558aa7028723bebd8301fd110d01cbd66d9a8b04685afd4f04f76e7b80c, 7c9775b0f44419207b02e531c357fe02f5856c17dbd88b3f32ec748047014df8, 54ce280ec0f086d89ee338029f12cef8e1297ee740af76dda245a08cb91bab4d, bf5f2bdc3d2acbfb218192710c8d27133bf51c1da1a778244617d3ba9c20e6f7, fdbc6648c6f922ffcd2b351791099e893e183680fc86f48bf18815d8ae98a4f7, ac9e3bf1cc87bc86318b258498572793d9fb082417e3f2ff17050cf6ec1d0bb5, 0a02901d364dc9d70b8fcdc8a2ec120b14f3c393186f99e2e4c5317db1edc889
MeltingClaw	SHA256	45adf6f32f9b3c398ee27f02427a55bb3df74687e378edcb7e23caf6a6f7bf2a, B9677c50b20a1ed951962edcb593cce5f1ed9c742bc7bff827a6fc420202b045, 45adf6f32f9b3c398ee27f02427a55bb3df74687e378edcb7e23caf6a6f7bf2a
DustyHammock	SHA256	951b89f25f7d8be0619b1dfdcc63939b0792b63fa34ebfa9010f0055d009a2d3, 951b8951b89f25f7d8be0619b1dfdcc63939b0792b63fa34ebfa9010f0055d009a2d3

Attack Name	TYPE	VALUE
ShadyHammock	SHA256	ce8b46370fd72d7684ad6ade16f868ac19f03b85e35317025511d6eeee288c64, 9f635fa106dbe7181b4162266379703b3fdf53408e5b8faa6aeee08f1965d3a2, 1fa96e7f3c26743295a6af7917837c98c1d6ac0da30a804fed820daace6f90b0
Cicada3301	TOR Address	cicadabv7vicyvgz5khl7v2x5yygcgow7ryy6yppwmxii4eoobdaztqd[.]onion
	SHA256	7b3022437b637c44f42741a92c7f7ed251845fd02dda642c0a47fde179bd984e, dd98133b825a1632879b689b864b15a66741208343bc8ba080354e0133181d69, 2d614f088f486f0870b3839ddb361e33efb73526a0a585f691874039f23171cc, 3969e1a88a063155a6f61b0ca1ac33114c1a39151f3c7dd019084abd30553eab
Adload	**SHA256**	d94f62ec4b6ffcec35d5e639d02a52ce226629a5eb3e2a7190174ea8d3b40b5b, 956aae546af632ea20123bfe659d57e0d5134e39cdb5489bd6f1ba5d8bbd0472, 6587e61a8a7edb312da5798ffccf4a5ef227d3834389993b4df3ef0b173443dc, 3d063efde737b7b2e393926358cbb32469b76395e1a05e8c127a12e47550f264, 2d595880cfb1691dd43de02d1a90273919f62311a7668ef078709eff2fd6bd87, 7cb10a70fd25645a708c81f44bb1de2b6de39d583ae3a71df0913917ad1dffc3, 4a7c9829590e1230a448dd7a4272b9fbfbafccf7043441967c2f68f6082dde32, 68b6beb70bd547b75f2d36d70ca49f8b18542874480d39e33b09ee69eb1048b3, 1904b705105db4550371d678f8161826b98b1a9fca139fa41628214ed816d2f5, 2fb1d8e6454f43522f42675dcf415569e5df5d731e1d1390f793c282cce4a7aa, ee9ebdb1d9a7424cd64905d39820b343c5f76e29c9cd60c0cdd3bfe069fb7d51, c7721ab85bad163576c166a0a71c0dbe4cc491dda68c5a5907fd1d8cac50780d, 17e1b83089814128bc243315894f412026503c10b710c9c59d4aaf67bc209cb8, 0adab4bfe1c8d85cbaaa983ca588218086f86dc5d2c69eab5ea0563de40beecb,

Attack Name	TYPE	VALUE
Adload	SHA256	4b90225402be51bbfc307e85c99f6411295da8acbac16ca2afb8eed918c69ebf, b1a7e41eb188da431bd829592a5ee740e912cd47d059942c14c3d492e45c9afd
	URLs	hxxp[:]//m[.]skilledobject[.]com/a/rep, hxxp[:]//m[.]browseractivity[.]com/a/rep, hxxp[:]//m[.]enchantedreign[.]com/a/rep, hxxp[:]//m[.]activitycache[.]com/a/rep, hxxp[:]//m[.]activityinput[.]com/a/rep, hxxp[:]//m[.]opticalupdater[.]com/a/rep, hxxp[:]//m[.]connectioncache[.]com/a/rep, hxxp[:]//m[.]analyzerstate[.]com/a/rep, hxxp[:]//m[.]essencecuration[.]com/a/rep, hxxp[:]//m[.]microrotator[.]com/a/rep, hxxp[:]//m[.]articlesagile[.]com/a/rep, hxxp[:]//m[.]progresshandler[.]com/a/rep, hxxp[:]//m[.]originalrotator[.]com/a/rep, hxxp[:]//m[.]productiveunit[.]com/a/rep, hxxp[:]//api[.]toolenviroment[.]com/l, hxxp[:]//api[.]inetfield[.]com/l, hxxp[:]//api[.]operativeeng[.]com/l, hxxp[:]//api[.]launchertasks[.]com/l, hxxp[:]//api[.]launchelemnt[.]com/l, hxxp[:]//api[.]validexplorer[.]com/l, hxxp[:]//api[.]majorsprint[.]com/l, hxxp[:]//api[.]essentialenumerator[.]com/l, hxxp[:]//api[.]transactioneng[.]com/l, hxxp[:]//api[.]macreationsapp[.]com/l, hxxp[:]//api[.]commondevice[.]com/l, hxxp[:]//api[.]compellingagent[.]com/l, hxxp[:]//api[.]lookupindex[.]com/l, hxxp[:]//api[.]practicalsync[.]com/l, hxxp[:]//api[.]accessiblelist[.]com/l, hxxp[:]//api[.]functionconfig[.]com/l, hxxps[:]//vpnservices[.]live, hxxps[:]//upgrader[.]live, hxxp[:]//bapp[.]pictureworld[.]co
LockBit 3.0	MD5	8770189ed3ee558819fd6ddf677b0c28, 6e3e5d703ed9bed4b7327a73bc585c04
	SHA1	4dec26dfcd3fd938886c9586a8eb62d7a2495be4, 583f34dd59d30be4a10dc7021984df0225cef147
	SHA256	a54519b7530039b9fba9a4143bf549b67048f441bbebf9f8d5cff1e539752189, dec147d7628d4e3479bc0ff31413621fb4b1b64a618469a9402a42816650f92b, 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce,

Attack Name	TYPE	VALUE
LockBit 3.0	SHA256	a56b41a6023f828cccaaef470874571d169fdb8f683a75edd430fbd31a2c3f6e, d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee, 5e006f895382525e762a33e5dd5e8416bef56ae859f5e96f820cfba5c4c11226, C9dd51d4295c33e1df0d275669a1de9e1de374a51eb88d7f7b1a1e65f49f7794
Babuk	MD5	87667327439292f5d2b2c68d4b88c0ad
	SHA1	8a1673d5821d306209b1f540741598bbc90ed1d3
	SHA256	56682344aa1dc0a0a5b0d26bd3a8dfe8ceb8772d6cd9e3f8cbd78ca78fe3c2ab
SRBMiner	SHA256	0d4eb69b551cb538a9a4c46f7b57906a47bcabb8ef8a5d245584fbba09fc5084
Bumblebee	URLs	hxxp[:]//193[.]242[.]145[.]138/mid/w1/Midjourney[.]msi, hxxp[:]//193[.]176[.]190[.]41/down1/nvinstall[.]msi
	IPv4	193[.]242[.]145[.]138, 193[.]176[.]190[.]41
	SHA256	2bca5abfac168454ce4e97a10ccf8ffc068e1428fa655286210006b298de42fb, 106c81f547cfe8332110520c968062004ca58bcfd2dbb0accd51616dd694721f, c26344bfd07b871dd9f6bd7c71275216e18be265e91e5d0800348e8aa06543f9, 0ab5b3e9790aa8ada1bbadd5d22908b5ba7b9f078e8f5b4e8fcc27cc0011cce7, d3f551d1fb2c307edfceb65793e527d94d76eba1cd8ab0a5d1f86db11c9474c3, d1cabe0d6a2f3cef5da04e35220e2431ef627470dd2801b4ed22a8ed9a918768, 7df703625ee06db2786650b48ffefb13fa1f0dae41e521b861a16772e800c115
Stealc	SHA256	a834be6d2bec10f39019606451b507742b7e87ac8d19dc0643ae58df183f773c
	URL	hxxp[:]//95[.]182[.]97[.]58/84b7b6f977dd1c65[.]php
	IPv4	95[.]182[.]97[.]58
Rhadamanthys	SHA256	2853a61188b4446be57543858adcc704e8534326d4d84ac44a60743b1a44cbfe
	IPv4	91[.]103[.]140[.]200
	URL	hxxp[:]//91[.]103[.]140[.]200[:]9078/3936a074a2f65761a5eb8/6fmfpmi7[.]fwf4p
AMOS Stealer	SHA256	94379fa0a97cc2ecd8d5514d0b46c65b0d46ff9bb8d5a4a29cf55a473da550d5

Attack Name	TYPE	VALUE
AMOS Stealer	URL	hxxp[:]//85[.]209[.]11[.]155/joinsystem
	IPv4	85[.]209[.]11[.]155
Manuscrypt	SHA256	2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59ecbd25753, 2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59ecbd25753, 0036ef9eca61e045fd34726758631c2cb26770471f91ec39daefd81bae1a3d2c, 73534b9670133468081305bd442f7691cf2f2c1136f09d9508400546c417833a, 59a37d7d2bf4cffe31407edd286a811d9600b68fe757829e30da4394ab65a4cc
Sliver	**MD5**	8b553728900ba2e45b784252a1ff6d17, 9dc2819c176c60e879f28529b1b08da1
	SHA1	953bd0859c86e0a3a3da52fe392a7d579a9f937b, 538cb25bfae6501d8c3c7053a293e8ca85a8dba4
	SHA256	e576938b137260200dd6a7e650b32adbf9cbe4b69199e98b06b1a0f4f3b8fff3, b0555d287f41b160d3b8a275df2c00b112e98a5db7dd83907411415e5428f7a9
Tsunami	IPv4	95[.]182[.]101[.]23
	SHA256	0f37a4b3eb939b1a1750a7a132d4798aa609f0cd862e47f641dd83c0763d8c8f
	SHA1	37cb34a044c70d1acea5a3a91580b7bfc2a8e687
	MD5	87c8423e0815d6467656093bff9aa193
Embargo	SHA1	8a85c1399a0e404c8285a723c4214942a45bbff9, 612ec1d41b2aa2518363b18381fd89c12315100f
	MD5	5d55fb708834d5ccde15d36554ea63e8
	SHA256	ebffc9ced2dba66db9aae02c7ccd2759a36c5167df5cd4adb151b20e7eab173c
CloudScout	SHA1	9b6a473820a72111c1a38735992b55c413d941ee, 621e2b50a979d77ba3f271fab94326cccbc009b4, c058f9fe91293040c8b0908d3dafc80f89d2e38b, 4a5bcdaac0bc315edd00bb1fccd1322737bcbeeb, 67028aeb095189fdf18b2d7b775b62366ef224a9,

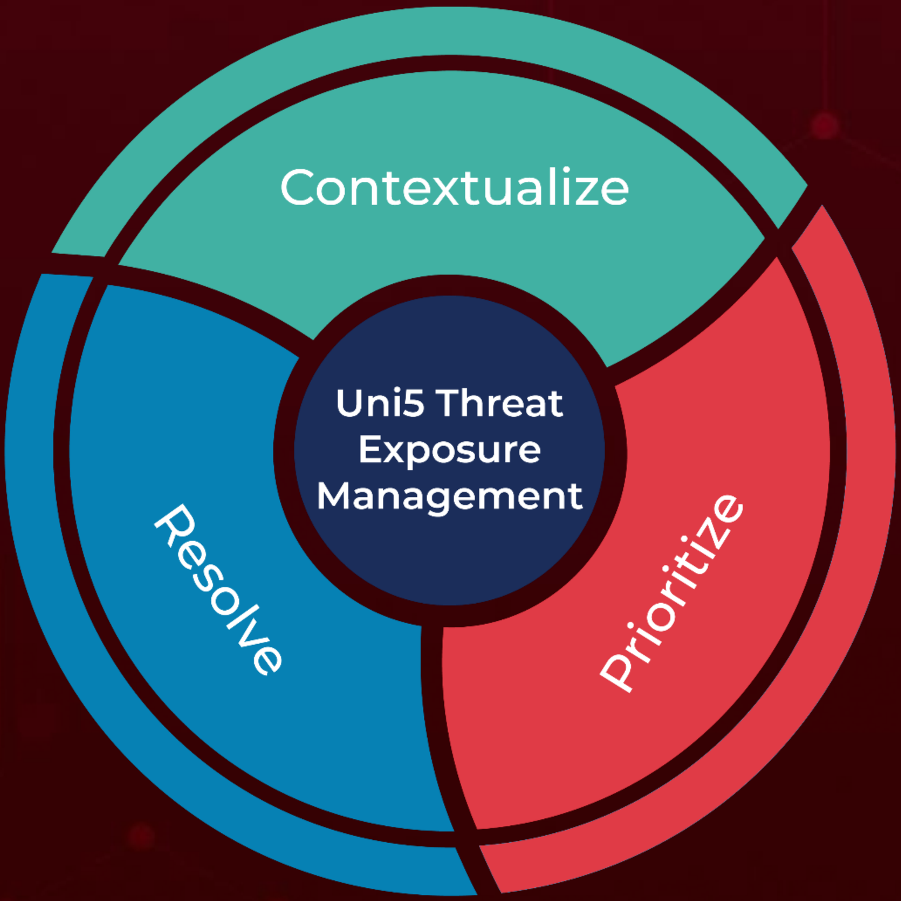
Attack Name	TYPE	VALUE
CloudScout	SHA1	b3556d1052bf5432d39a6068ccf00d8c318af146, 84f6b9f13cdcd8d9d15d5820536bc878cd89b3c8, 93c1c8ad2af64d0e4c132f067d369ecbebae00b7, 8eaa213ae4d482938c5a7ec523c83d2c2e1e8c0e, a1ca41fdb61f03659168050de3e208f0940f37d8
	File Name	CommonUtilities.dll, CGM.dll, CGD.dll, COL.dll
	SHA256	8ebce3ceaf166fe2edab157b88aa84349d2d848242ff305cdc7edb6a34e5b72f, d7468510a0123f4ecea9cb7c1636a024d3ab96cc856439a924349b00618b87ae, 1f34527a01bd3c05affe6c90aeaea926f57efa2fac06859f8427988865ccd310
MgBot	SHA1	c70c3750ac6b9d7b033addef838ef1cc28c262f3, 812124b84c5ea455f7147d94ec38d24bdf159f84, ad6c84859d413d627ac589aedf9891707e179d6c, 3dd958ca6eb7e8f0a0612d295453a3a10c08f5fe
Nightdoor	SHA1	547bd65eee05d744e075c5e12fb973a74d42438f, 348730018e0a5554f0f05e47bba43dc0f55795ac
Pronsis	MD5	d36d303d2954cb4309d34c613747ce58
	SHA1	e2de9ca2575dfe6114e688c44647a58a1ec325c2
	SHA256	f2058183f59cba1aed685d44e5c5b9d56995cfa54b38e18889c059b2bde36b3a
SUNSPINNER	SHA256	614e74654773e617475d519edd23380f531b60264fd7f8ed86aebf28efed4e39
	MD5	4ca65a7efe2e4502e2031548ae588cb8
	SHA1	eef25d4316a0c67ed00e3d40441fcab30ccd0a9d
PURESTEALER	MD5	b3cf993d918c2c61c7138b4b8a98b6bf
	SHA256	d66075b2c70c3de22c9e774ad9e5f88d3d85708d1a5b17ccd4e76049c86b49b5
	SHA1	a8cf0215610317b68a71d7a6fed7d9e07241d373

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

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

November 7, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com