Date of Publication
July 1, 2024

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

JUNE 2024

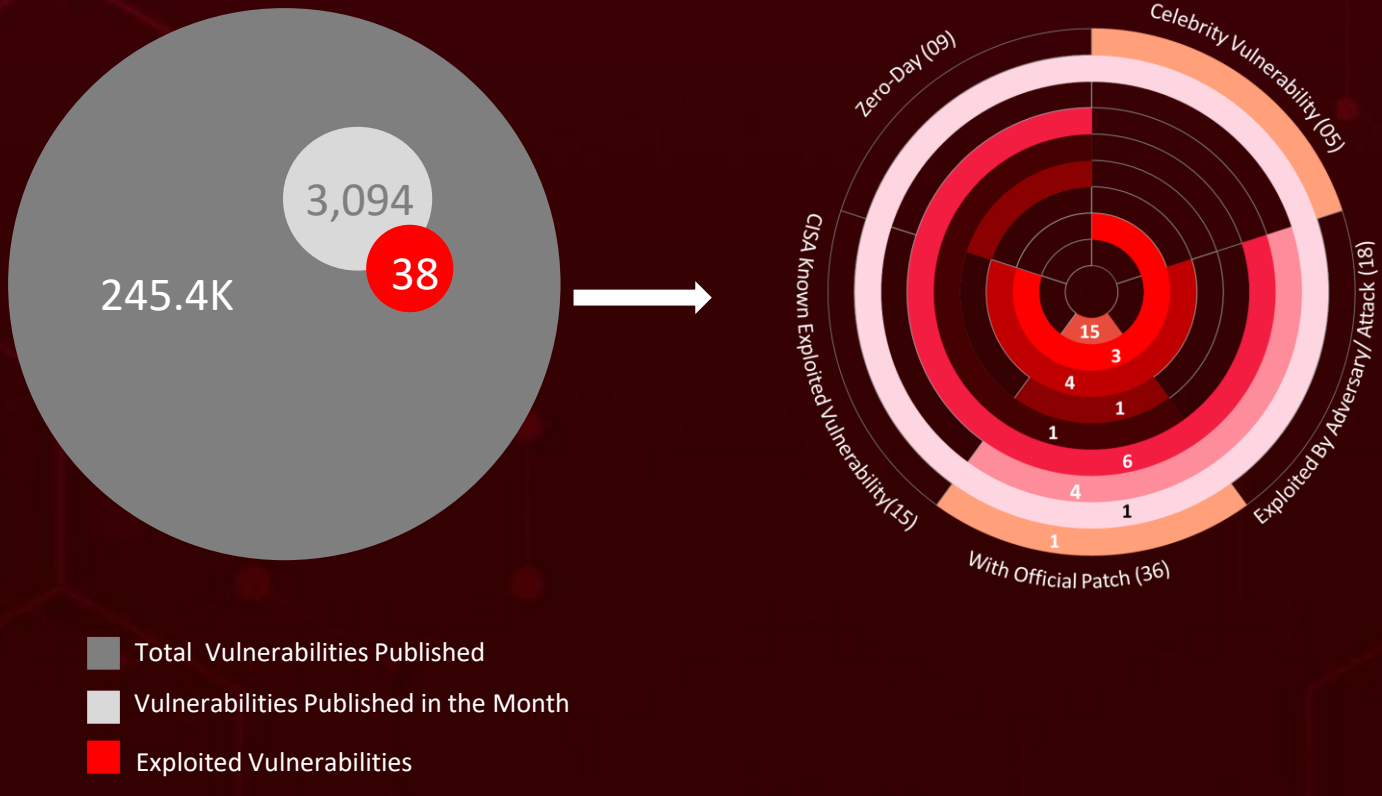
Table Of Contents

Summary

In June, the cybersecurity arena garnered significant attention following the identification of **nine zero-day** vulnerabilities. The Chief 'Five Celebrity Vulnerabilities,' which included critical flaws like **Zerologon, UEFIcanhazbufferoverflow, Baron Samedit, Pwnkit,** and **Log4shell,** all of which were leveraged to deploy ransomware and backdoors. Additionally, the **Arm Zero-Day** vulnerability **CVE-2024-4610**, has been actively exploited in the wild. While the threat actors are actively exploiting a critical path-traversal vulnerability, **CVE- 2024-28995**, in SolarWinds Serv-U.

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

Concurrently, **eleven** threat actors were engaged in various campaigns. **ExCobalt**, a cyber espionage-focused threat actor, has been targeting Russian organizations using an advanced Golang-based backdoor called **GoRed**. Additionally, the espionage organization **SneakyChef** has launched an effort using cutting-edge Remote Access Trojans (RATs) **SpiceRAT** and **SugarGh0st** to target government entities. This malware campaign has been active since at least August 2023.



Insights

In June 2024, a geopolitical cybersecurity landscape unfolds, revealing **South Korea, India, China** and **Japan** as the top-targeted countries

Highlighted in **June 2024** is a cyber battleground encompassing the **Technology, Government, Education, Energy** and **Telecommunications** sectors, designating them as the top industries

CVE-2024-4577 flaw in PHP impacts Windows, TellYouThePass ransomware gang is actively exploiting this vulnerability, leading to arbitrary code execution

Black Basta ransomware group, exploiting Windows Zero-day flaw CVE-2024-26169 to elevate their privileges

CVE-2024-4610

Zero-Day Flaw in Arm, has been actively exploited in the wild, Impacting the Bifrost and Valhall GPU kernel drivers

LilacSquid

targets IT organizations in the United States, energy sector across Europe and pharma in Asia to deploy Malwares

DISGOMOJI Malware

utilizing emojis to execute commands, targeting government agencies in India

ExCobalt

a cyber espionage-focused threat actor, has been targeting Russian organizations using an advanced Golang-based backdoor called GoRed

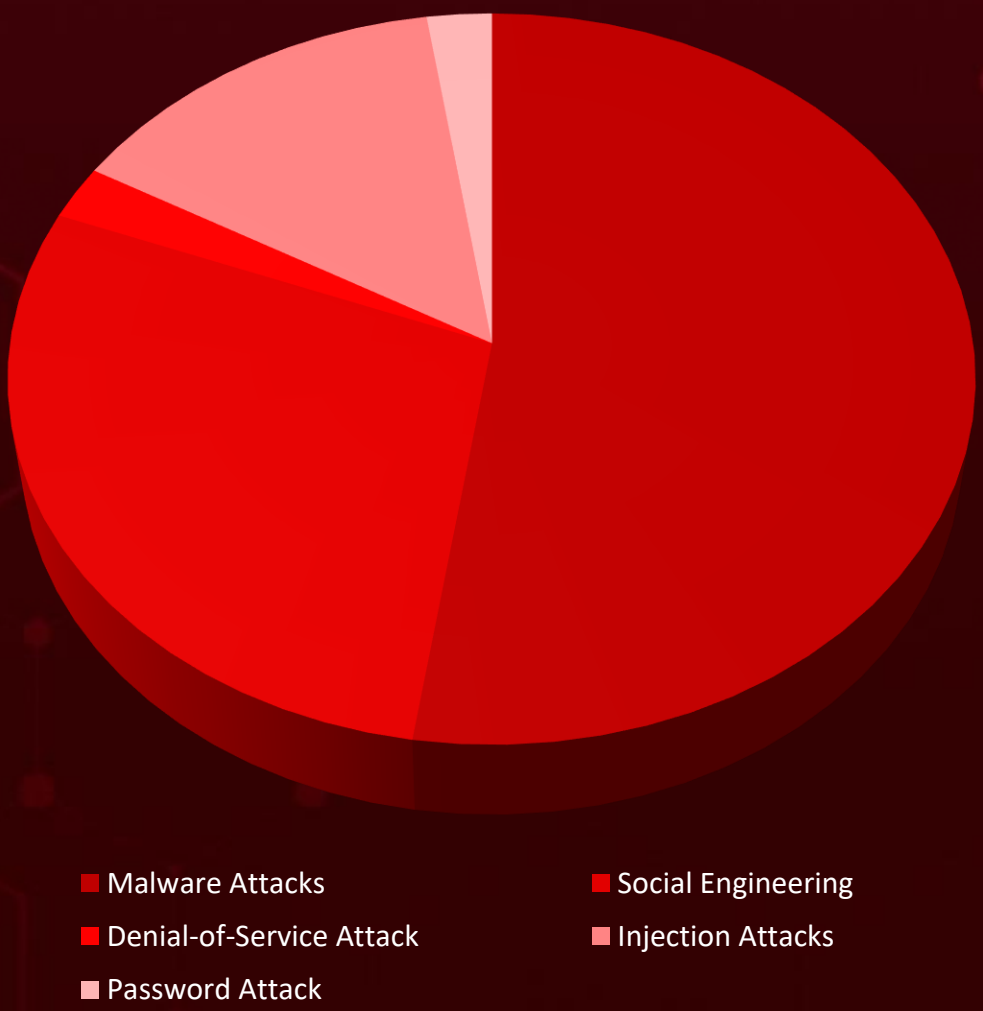
ChamelGang

a prominent cyberespionage Entity, deploys CatB ransomware, to achieve secondary financial gains alongside data theft

UNC3886

China-linked group, utilize rootkits maintain access and evade detection

Threat Landscape



Celebrity Vulnerabilities

<table>
<tr><th>CVE ID</th><th>ZERO-DAY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2020-1472</td><td>✗</td><td rowspan="2">Microsoft Netlogon</td><td rowspan="2">-</td></tr>
<tr><td>CISA KEV</td></tr>
<tr><td rowspan="2">✓</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*</td><td>RansomHub Ransomware</td></tr>
<tr><td rowspan="2">Zerologon (Microsoft Netlogon Privilege Escalation Vulnerability)</td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-330</td><td>T1068: Exploitation for Privilege Escalation</td><td>https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>ZERO-DAY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="8">CVE-2024-0762

NAME

UEFIcanhazbufferoverflow (Phoenix SecureCore UEFI firmware Buffer Overflow Vulnerability)</td><td>✗</td><td rowspan="2">Phoenix SecureCore for Intel Kaby Lake: from 4.0.1.1 before 4.0.1.998; Phoenix SecureCore for Intel Coffee Lake: from 4.1.0.1 before 4.1.0.562; Phoenix SecureCore for Intel Ice Lake: from 4.2.0.1 before 4.2.0.323; Phoenix SecureCore for Intel Comet Lake: from 4.2.1.1 before 4.2.1.287; Phoenix SecureCore for Intel Tiger Lake: from 4.3.0.1 before 4.3.0.236; Phoenix SecureCore for Intel Jasper Lake: from 4.3.1.1 before 4.3.1.184; Phoenix SecureCore for Intel Alder Lake: from 4.4.0.1 before 4.4.0.269; Phoenix SecureCore for Intel Raptor Lake: from 4.5.0.1 before 4.5.0.218; Phoenix SecureCore for Intel Meteor Lake: from 4.5.1.1 before 4.5.1.15</td><td rowspan="2">-</td></tr>
<tr><td>CISA KEV</td></tr>
<tr><td rowspan="3">✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>cpe:2.3:a:phoenix:securecore_for_intel_kaby_lake:*:*:*:*:*:*:*:*
cpe:2.3:a:phoenix:securecore_for_intel_coffee_lake:*:*:*:*:*:*:*:*
cpe:2.3:a:phoenix:securecore_for_intel_ice_lake:*:*:*:*:*:*:*:*
cpe:2.3:a:phoenix:securecore_for_intel_comet_lake:*:*:*:*:*:*:*:*
cpe:2.3:a:phoenix:securecore_for_intel_tiger_lake:*:*:*:*:*:*:*:*
cpe:2.3:a:phoenix:securecore_for_intel_jasper_lake:*:*:*:*:*:*:*:*
cpe:2.3:a:phoenix:securecore_for_intel_alder_lake:*:*:*:*:*:*:*:*
cpe:2.3:a:phoenix:securecore_for_intel_raptor_lake:*:*:*:*:*:*:*:*
cpe:2.3:a:phoenix:securecore_for_intel_alder_lake:*:*:*:*:*:*:*:*
cpe:2.3:a:phoenix:securecore_for_intel_meteor_lake:*:*:*:*:*:*:*:*</td><td>-</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-120</td><td>T1068: Exploitation for Privilege Escalation
T1542: Pre-OS Boot</td><td>https://www.phoenix.com/security-notifications/cve-2024-0762/</td></tr>
</table>

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-3156	✗	Sudo before 1.9.5p2	ExCobalt
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:sudo_project:sudo:*:*:*:*:*:*:*:*	GoRed Backdoor
Baron Samedit (Sudo Heap-Based Buffer Overflow Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-193	T1068: Exploitation for Privilege Escalation	https://www.sudo.ws/releases/stable/#1.9.5p2

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-4034	✗	Red Hat Polkit	ExCobalt
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:polkit_project:polkit:*:*:*:*:*:*:*:*	GoRed Backdoor
Pwnkit (Red Hat Polkit Out-of-Bounds Read and Write Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-125	T1068: Exploitation for Privilege Escalation T1059: Command and Scripting Interpreter	https://bugzilla.redhat.com/show_bug.cgi?id=2025869

<table>
<tr><th>CVE ID</th><th>ZERO-DAY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2021-44228</td><td>✓</td><td rowspan="2">Apache Log4j2</td><td rowspan="2">ExCobalt</td></tr>
<tr><td>CISA KEV</td></tr>
<tr><td rowspan="3">✓</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*</td><td>GoRed Backdoor</td></tr>
<tr><td rowspan="2">Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)</td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-917</td><td>T1059: Command and Scripting Interpreter</td><td>https://logging.apache.org/log4j/2.x/security.html</td></tr>
</table>

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-1800	Progress Telerik Report Server Insecure Deserialization Vulnerability	Progress Telerik Report Server	✗	✗	✓
CVE-2024-4358	Progress Telerik Report Server Authentication Bypass Vulnerability	Progress Telerik Report Server	✗	✗	✓
CVE-2024-29972	Zyxel NAS Command Injection Vulnerability	NAS326 and NAS542	✗	✗	✓
CVE-2024-29973	Zyxel NAS Command Injection Vulnerability	NAS326 and NAS542	✗	✗	✓
CVE-2024-29974	Zyxel NAS Remote Code Execution Vulnerability	NAS326 and NAS542	✗	✗	✓
CVE-2024-29975	Zyxel NAS Improper Privilege Management Vulnerability	NAS326 and NAS542	✗	✗	✗
CVE-2024-29976	Zyxel NAS Improper Privilege Management Vulnerability	NAS326 and NAS542	✗	✗	✗
CVE-2020-1472	Zerologon (Microsoft Netlogon Privilege Escalation Vulnerability)	Microsoft Netlogon	✗	✓	✓
CVE-2023-33246	Apache RocketMQ Command Execution Vulnerability	Apache RocketMQ	✗	✓	✓
CVE-2024-27348	Apache HugeGraph-Server Remote Command Execution Vulnerability	Apache HugeGraph-Server	✗	✗	✓
CVE-2024-29849	Veeam Backup Enterprise Manager Authentication Bypass Vulnerability	Veeam Backup Enterprise Manager	✗	✗	✓
CVE-2024-4577	PHP-CGI Argument Injection Vulnerability	PHP	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-50868	NSEC3 Closest Encloser Proof DoS Vulnerability	Windows Server	✓	✗	✓
CVE-2024-4610	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	Bifrost GPU Kernel Driver and Valhall GPU Kernel Driver	✓	✓	✓
CVE-2024-26169	Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability	Windows Server	✓	✓	✓
CVE-2024-29855	Veeam Recovery Orchestrator Authentication Bypass Vulnerability	Veeam Recovery Orchestrator	✗	✗	✓
CVE-2024-37079	VMware vCenter Server Heap-overflow Vulnerability	vCenter Server and Cloud Foundation	✗	✗	✓
CVE-2024-37080	VMware vCenter Server Heap-overflow Vulnerability	vCenter Server and Cloud Foundation	✗	✗	✓
CVE-2024-37081	VMware vCenter Server Multiple Local Privilege Escalation Vulnerabilities	vCenter Server and Cloud Foundation	✗	✗	✓
CVE-2024-28995	SolarWinds Serv-U Directory Transversal Vulnerability	SolarWinds Serv-U	✗	✗	✓
CVE-2023-34048	VMware vCenter Server Out-of-Bounds Write Vulnerability	VMware vCenter Server	✓	✓	✓
CVE-2022-41328	Fortinet FortiOS Path Traversal Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2022-22948	Vmware vCenter Server Information Disclosure Vulnerability	Vmware vCenter Server	✗	✗	✓
CVE-2023-20867	VMware Tools Authentication Bypass Vulnerability	VMware Tools	✓	✓	✓
CVE-2022-42475	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-0762	UEFIcanhazbufferoverflow (Phoenix SecureCore UEFI firmware Buffer Overflow Vulnerability)	Phoenix SecureCore UEFI firmware	✗	✗	✓
CVE-2022-2586	Linux Kernel nft_object Use-After-Free Privilege Escalation Vulnerability	Linux kernel	✗	✗	✓
CVE-2021-3156	Baron Samedit (Sudo Heap-Based Buffer Overflow Vulnerability)	Sudo before 1.9.5p2	✗	✓	✓
CVE-2021-4034	Pwnkit (Red Hat Polkit Out-of-Bounds Read and Write Vulnerability)	Red Hat Polkit	✗	✓	✓
CVE-2019-13272	Linux Kernel Improper Privilege Management Vulnerability	Linux kernel before 5.1.17	✗	✓	✓
CVE-2022-27228	Bitrix Arbitrary Code Execution Vulnerability	Bitrix before 21.0.100	✗	✗	✓
CVE-2021-44228	Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)	Apache Log4j2	✓	✓	✓
CVE-2021-40438	Apache HTTP Server-Side Request Forgery	Apache HTTP Server 2.4.48 and earlier	✗	✓	✓
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2019-12725	Zeroshell Remote Command Execution Vulnerability	Zeroshell 3.9.0	✗	✗	✓
CVE-2022-40691	Moxa Information Disclosure Vulnerability	Moxa SDS-3008: 2.1	✗	✗	✓
CVE-2024-5806	Progress MOVEit Transfer Improper Authentication Vulnerability	Progress MOVEit Transfer	✗	✗	✓
CVE-2024-5805	Progress MOVEit Gateway Improper Authentication Vulnerability	Progress MOVEit Gateway	✗	✗	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
PurpleInk	Trojan	-	-	-	Exploiting Vulnerable Application Servers
CarnavalHeist	Banking Trojan	-	Windows	-	Spam emails
TargetCompany	Ransomware	-	Windows, Linux, VMWare ESXi	-	Exploiting Public-Facing Application
RansomHub	Ransomware	CVE-2020-1472	Microsoft Netlogon	✓	Exploiting the Zerologon vulnerability
Knight ransomware	Ransomware	CVE-2020-1472	Microsoft Netlogon	✓	Exploiting the Zerologon vulnerability
Muhstik	Botnet	CVE-2023-33246	RocketMQ	✓	Exploiting a vulnerability in Apache RocketMQ
Fog Ransomware	Ransomware	-	-	-	Exploiting compromised VPN credentials
ValleyRAT	RAT	-	-	-	Phishing emails
WARMCOOKIE	Backdoor	-	-	-	Phishing emails
TellYouThePass	Ransomware	CVE-2024-4577	PHP	✓	Exploiting vulnerabilities
Black Basta	Ransomware	CVE-2024-26169	Microsoft Windows	✓	Exploiting vulnerabilities
DISGOMOJI	Backdoor	-	-	-	Phishing
PlugX	RAT	-	F5 BIG-IP	-	By Exploiting F5 BIG-IP appliances

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
BadSpace	Backdoor	-	Windows	-	Social Engineering
Noodle RAT	RAT	-	-	-	-
Fickle Stealer	Information Stealer	-	-	-	Phishing
VirtualPita	Backdoor	CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475	VMware vCenter Server, Fortinet FortiOS, VMware Tools	✓	Exploiting Vulnerabilities
VirtualPie	Backdoor	CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475	VMware vCenter Server, Fortinet FortiOS, VMware Tools	✓	Exploiting Vulnerabilities
VirtualGate	Backdoor	CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475	VMware vCenter Server, Fortinet FortiOS, VMware Tools	✓	Exploiting Vulnerabilities
MOPSLED	Backdoor	CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475	VMware vCenter Server, Fortinet FortiOS, VMware Tools	✓	Exploiting Vulnerabilities
RIFLESPINE	Backdoor	CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475	VMware vCenter Server, Fortinet FortiOS, VMware Tools	✓	Exploiting Vulnerabilities
SugarGh0st	RAT	-	-	-	Social Engineering
SpiceRAT	RAT	-	-	-	Social Engineering
DragonForce Ransomware	Ransomware	-	-	-	Phishing, Exploiting Vulnerabilities

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
GoRed Backdoor	Backdoor	CVE-2022-2586 CVE-2021-3156 CVE-2021-4034 CVE-2019-13272 CVE-2022-27228 CVE-2021-44228 CVE-2021-40438 CVE-2023-3519 CVE-2019-12725 CVE-2022-40691	Linux kernel, Sudo, Red Hat Polkit, Bitrix, Apache Log4j2, Apache HTTP Server, Citrix NetScaler ADC and NetScaler Gateway, Zeroshell, Moxa-SDS		Exploiting Vulnerabilities
XWorm RAT	RAT	-	-	-	Phishing
BMANAGER	Trojan	-	Windows	-	custom malware delivery platform
CatB Ransomware	Ransomware	-	-	-	-
InnoLoader	Loader	-	Windows	-	Social Engineering

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
LilacSquid	Information Theft, Espionage	-	-	PurpleInk	-
Operation Ghostwriter	Information Theft, Espionage, Sabotage, and destruction	Belarus	-	-	Microsoft Windows
Cardinal Threat Group	Information Theft, Espionage	-	CVE-2024-26169	Black Basta ransomware	-
UTA0137	Espionage	Pakistan	-	DISGOMOJI	-
Velvet Ant	Information Theft, Espionage	China	-	PlugX	-
UNC3886	Espionage	China	CVE-2023-34048 CVE-2022-41328 CVE-2022-22948 CVE-2023-20867 CVE-2022-42475	VirtualPita, VirtualPie, VirtualGate, MOPSLED and RIFLESPINE	VMware vCenter Server, Fortinet FortiOS, VMware Tools
SneakyChef	Espionage and Information theft	China	-	SugarGh0st, SpiceRAT	-
ExCobalt	Espionage	-	CVE-2022-2586 CVE-2021-3156 CVE-2021-4034 CVE-2019-13272 CVE-2022-27228 CVE-2021-44228 CVE-2021-40438 CVE-2023-3519 CVE-2019-12725 CVE-2022-40691	GoRed Backdoor	Linux kernel, Sudo, Red Hat Polkit, Bitrix, Apache Log4j2, Apache HTTP Server, Citrix NetScaler ADC and NetScaler Gateway, Zeroshell, Moxa-SDS

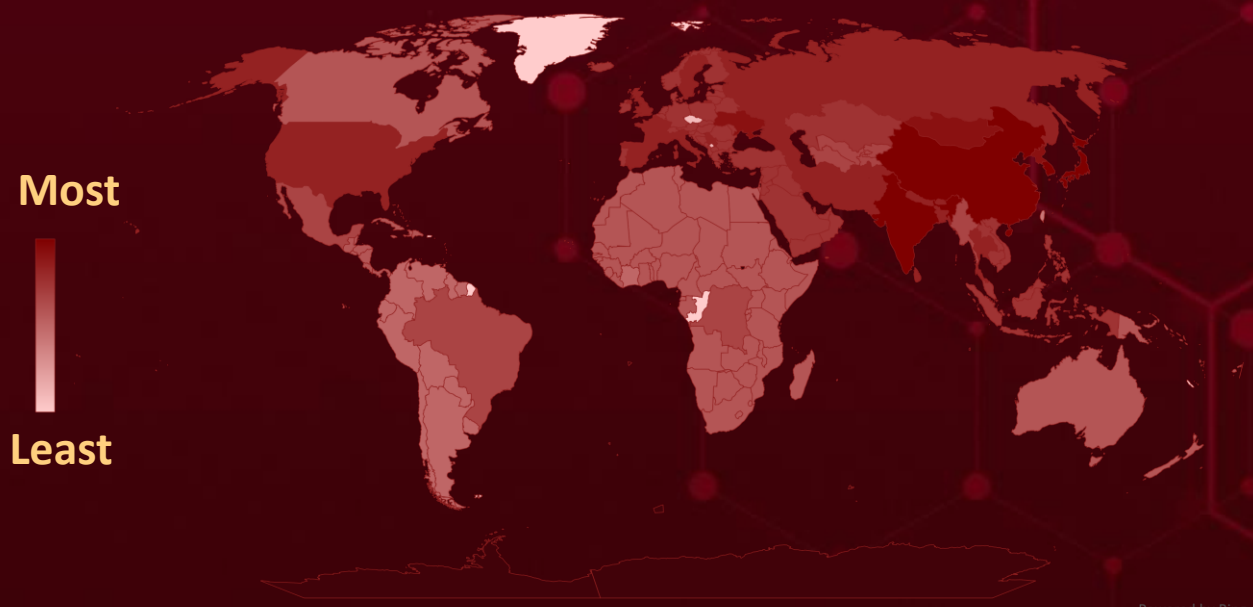
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UAC-0184	Espionage and Information theft	-	-	XWorm RAT	-
Boolka	Espionage and Information theft	-	-	BMANAGER	Windows
ChamelGang	Espionage and Information theft	-	-	CatB Ransomware	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
Progress	Software Company	Progress Telerik Report Server versions prior to 2024 Q1 (10.0.24.130)
		Progress MOVEit Transfer
		Progress MOVEit Gateway
ZYXEL	Communications equipment company	Zyxel NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier
Microsoft	Operating System	Microsoft Windows
THE APACHE SOFTWARE FOUNDATION	Software, Server	Apache RocketMQ 4.2.0 -5.1.0
		Apache HugeGraph-Server from version 1.0.0 to before 1.3.0 in Java8 & Java11
		Apache Log4j2
		Apache HTTP Server 2.4.48 and earlier
VEEAM	Software	Veeam Backup Enterprise Manager versions before prior to 12.1.2.172
		Veeam Recovery Orchestrator (VRO) version 7.0.0.337
php	Programming Language	PHP versions: 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8
	Server	Windows Server: 2012 – 2022 23H2
		Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
arm	Drivers	Bifrost GPU Kernel Driver: All versions from r34p0 to r40p0 Valhall GPU Kernel Driver: All versions from r34p0 to r40p0
vmware	Hypervisor	VMware vCenter Server: 7.0 U1 - 8.0.0c Cloud Foundation versions 4.x and 5.x.
		VMware vCenter Server
		VMware Tools
solarwinds	FTP Server	SolarWinds Serv-U 15.4.2 HF 1 and previous versions
FORTINET	Security Software	Fortinet FortiOS
	Operating System	Linux kernel
	Computer Program	Sudo before 1.9.5p2
	System Software	Red Hat Polkit
Bitrix24	CRM system	Bitrix before 21.0.100
citrix	Networking and Security Solution	Citrix NetScaler ADC and NetScaler Gateway
ZEROSHELL Net Services	System software	Zeroshell 3.9.0
MOXA	Smart Switch	Moxa SDS-3008: 2.1

Targeted Countries



Color	Countries
	South Korea
	India
	China
	Japan
	Mongolia
	North Korea
	Ukraine
	Azerbaijan
	Afghanistan
	Bhutan
	France
	Russia
	Georgia
	Cyprus
	Armenia
	Nepal
	Iran
	Pakistan
	Italy
	Serbia
	Sri Lanka
	Spain

Color	Countries
	Sweden
	Bangladesh
	Thailand
	United States
	Maldives
	United Kingdom
	Poland
	Syria
	Singapore
	Indonesia
	Norway
	Austria
	Estonia
	Iraq
	Belarus
	Ireland
	Belgium
	Bosnia and Herzegovina
	Denmark
	Brunei
	Qatar

Color	Countries
	Jordan
	Saudi Arabia
	Kazakhstan
	Slovenia
	Kuwait
	Greece
	Laos
	Turkey
	United Arab Emirates
	North Macedonia
	Bulgaria
	Oman
	Liechtenstein
	Philippines
	Lithuania
	Portugal
	Luxembourg
	Romania
	Malaysia
	San Marino
	Cambodia
	Finland
	Malta
	Slovakia
	Moldova

Color	Countries
	Albania
	Monaco
	Germany
	Andorra
	Switzerland
	Montenegro
	Hungary
	Croatia
	Iceland
	Netherlands
	Bahrain
	Latvia
	Vietnam
	Yemen
	Lebanon
	Timor-Leste
	Israel
	Congo
	Kyrgyzstan
	Tajikistan
	Mexico
	Turkmenistan

Color	Countries
	Myanmar
	Brazil
	Uzbekistan
	Zambia
	Seychelles
	Madagascar
	Malawi
	Angola
	Dominican Republic
	Tunisia
	Egypt
	Guinea-Bissau
	Mali
	Cabo Verde
	El Salvador
	State of Palestine
	Marshall Islands
	Bahamas
	Mauritania
	Uganda
	Mauritius
	Saint Lucia

Targeted Industries

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities	**T1082** System Information Discovery	**T1190** Exploit Public-Facing Application
T1068 Exploitation for Privilege Escalation	**T1105** Ingress Tool Transfer	**T1036** Masquerading	**T1566** Phishing	**T1027** Obfuscated Files or Information
T1041 Exfiltration Over C2 Channel	**T1486** Data Encrypted for Impact	**T1055** Process Injection	**T1204** User Execution	**T1071** Application Layer Protocol
T1083 File and Directory Discovery	**T1566.001** Spearphishing Attachment	**T1059.003** Windows Command Shell	**T1588.005** Exploits	**T1057** Process Discovery
T1562 Impair Defenses	**T1133** External Remote Services	**T1140** Deobfuscate/ Decode Files or Information	**T1056** Input Capture	**T1053** Scheduled Task/Job

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
TargetCompany	URLs	hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x.sh, hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x, hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/post.php
	SHA1	dffa99b9fe6e7d3e19afba38c9f7ec739581f656, 2b82b463dab61cd3d7765492d7b4a529b4618e57, 9779aa8eb4c6f9eb809ebf4646867b0ed38c97e1, 3642996044cd85381b19f28a9ab6763e2bab653c, 4cdee339e038f5fc32dde8432dc3630afd4df8a2, 0f6bea3ff11bb56c2daf4c5f5c5b2f1afd3d5098
RansomHub	SHA256	02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292, 34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087, 7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a, 8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7, ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00
Knight Ransomware	SHA256	104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2, 2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad, 36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e, 595cd80f8c84bc443eff619add01b86b8839097621cdd148f30e7e2214f2c8cb, 7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2, E654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23
Muhstik	SHA256	9e28f942262805b5fb59f46568fed53fd4b7dbf6faf666bedaf6ff22dd416572, 1f9cda58cea6c8dd07879df3e985499b18523747482e8f7acd6b4b3a82116957, 176c57e3fa7da2fb2afcd18242b79e5881c2244f5ab836897d4846885f1bd993, a7bf3c031ab66265ce724fc26c8f7565442a098b06b01ea8871f13179d168713,

Attack Name	TYPE	VALUE
Muhstik	SHA256	6730eb04edf45d590939d7ba36ca0d4f1d2f28a2692151e3c631e9f2d3612893, 86947b00a3d61b82b6f752876404953ff3c39952f2b261988baf63fbbbd6d6ae
Black Basta	SHA256	7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a, d9d2838327c081a6daf9528c77ff3a8ac88e8ff73521b97d34af0d3da5807e7c, a6fbdbf8efe0ea129636bb5b3d6d6faec298272a2afded7e7516f2491844abc7, e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757, df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415, d73f6e240766d,dd6c3c16eff8db50794ab8ab95c6a616d4ab2bc96780f13464d, b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9, 69192821f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944, 62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087, 462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7, 5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43, 58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd, 51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e, 05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431, 3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35, 350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd, 0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e, 892bb04889678134fbdde62d573eef1274c328b4e216ea7dc17ed0065fe8be37, 58edd2a0980b15f7fc6c892011751a30c134757142a54c2cedcbba4af2cbf855, 723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224, ca0273c55507c3aae95539812c2c5d9bbdc80deb8e714360fe4bcc65d257aeb0, 0c915ce6cd1676ecc99863f47ed28c6466a2532ce9df7bbd2ae810b7bbf026f7, 753a66f032d0d7a7c310a2e5f98c54e95e3d404400224d592657a02079c668d5,

Attack Name	TYPE	VALUE
Black Basta	SHA256	96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be, 82515c1c5675d68c0f1f7d7572d83819944cc951747879caf1653cf41ce792ba, 9f948af3a30f125dcd24d8a628b3a18c66b3d72baede8496ee735cbdfd9cf0c7, d943a4aabd76582218fd1a9a0a77b2f6a6715b198f9994f0feae6f249b40fdf9, ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e, 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-1800	✗	Progress Telerik Report Server versions prior to 2024 Q1 (10.0.24.130)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:progress:telerik_report_server:*:*:*:*:*:*:*:*	-
Progress Telerik Report Server Insecure Deserialization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://docs.telerik.com/report-server/implementer-guide/setup/upgrade

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4358	✗	Progress Telerik Report Server, version 2024 Q1 (10.0.24.305) or earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:progress:telerik_report_server:*:*:*:*:*:*:*:*	-
Progress Telerik Report Server Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-290	T1190: Exploit Public-Facing Application; T1040: Network Sniffing	https://docs.telerik.com/report-server/implementer-guide/setup/upgrade

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29972	✗	NAS326 V5.21(AAZF.16)C0 and earlier NAS542 V5.21(ABAG.13)C0 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	-
Zyxel NAS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/download

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	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	-
Zyxel NAS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29974		NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	-
Zyxel NAS Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29975		NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	-
Zyxel NAS Improper Privilege Management Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29976	✗	NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	-
Zyxel NAS Improper Privilege Management Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-1472	✓	Microsoft Netlogon	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	RansomHub Ransomware
Zerologon (Microsoft Netlogon Privilege Escalation Vulnerability)	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-330	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-33246	✗	Apache RocketMQ 4.2.0 - 5.1.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:rocketmq:*:*:*:*:*:*:*:*	Muhstik Botnet
Apache RocketMQ Command Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://rocketmq.apache.org/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-27348	✗	Apache HugeGraph-Server from version 1.0.0 to before 1.3.0 in Java8 & Java11	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:hugegraph-server:*:*:*:*:*:*:*:*	-
Apache HugeGraph-Server Remote Command Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1190 : Exploit Public-Facing Application	https://hugegraph.apache.org/docs/download/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29849	✗	Veeam Backup Enterprise Manager versions before prior to 12.1.2.172	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	-
Veeam Backup Enterprise Manager Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://www.veeam.com/kb4510

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4577	✗	PHP versions: 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:php:php:*:*:*:*:*:*:*:*	TellYouThePass ransomware
PHP-CGI Argument 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-2023-50868	✗	Windows Server: 2012 – 2022 23H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
NSEC3 Closest Encloser Proof DoS Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-400	T1498 : Network Denial of Service	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-50868

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4610	✗	Bifrost GPU Kernel Driver: All versions from r34p0 to r40p0 Valhall GPU Kernel Driver: All versions from r34p0 to r40p0	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:arm:bifrost_gpu_kernel_driver:*:*:*:*:*:*:*:* cpe:2.3:a:arm:valhall_gpu_kernel_driver:*:*:*:*:*:*:*:*	-
Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter	https://developer.arm.com/downloads/-/mali-drivers/bifrost-kernel; https://developer.arm.com/downloads/-/mali-drivers/valhall-kernel

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-26169	✗ ZERO-DAY	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	Cardinal Threat Group
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	Black Basta ransomware
Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-269	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26169

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29855	✗ ZERO-DAY	Veeam Recovery Orchestrator (VRO) version 7.0.0.337	-
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:veeam:recovery_orchestrator:*:*:*:*:*:*:*:*	-
Veeam Recovery Orchestrator Authentication Bypass Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-287	T1068: Exploitation for Privilege Escalation, T1591 : Gather Victim Org Information	https://www.veeam.com/kb4585

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-37079	✗	vCenter Server: 7.0 U1 - 8.0.0c Cloud Foundation versions 4.x and 5.x.	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:*	-
VMware vCenter Server Heap-overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter	https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u2d-release-notes/index.html , https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u1e-release-notes/index.html , https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u3r-release-notes/index.html , https://knowledge.broadcom.com/external/article?legacyId=88287

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-37080</td><td>✗</td><td rowspan="2">vCenter Server: 7.0 U1 - 8.0.0c
Cloud Foundation versions 4.x and 5.x.</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><th>NAME</th><th>CISA KEV</th><td rowspan="2">cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">VMware vCenter Server Heap-overflow Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-122</td><td>T1190: Exploit Public-Facing Application
T1059: Command and Scripting Interpreter</td><td>https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u2d-release-notes/index.html , https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u1e-release-notes/index.html , https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u3r-release-notes/index.html , https://knowledge.broadcom.com/external/article?legacyId=88287</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-37081	✗	vCenter Server: 7.0 U1 - 8.0.0c Cloud Foundation versions 4.x and 5.x.	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:*	-
VMware vCenter Server Multiple Local Privilege Escalation Vulnerabilities	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-264	T1190: Exploit Public-Facing Application T1548.003: Sudo and Sudo Caching T1068: Exploitation for Privilege Escalation	https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u2d-release-notes/index.html , https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u1e-release-notes/index.html , https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u3r-release-notes/index.html , https://knowledge.broadcom.com/external/article?legacyId=88287

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28995	✗	SolarWinds Serv-U 15.4.2 HF 1 and previous versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:solarwinds:serv-u:*:*:*:*:*:*:*:* cpe:2.3:a:solarwinds:serv-u:15.4.2:-:*:*:*:*:*:* cpe:2.3:a:solarwinds:serv-u:15.4.2:hotfix1:*:*:*:*:*:*	-
SolarWinds Serv-U Directory Transversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1005: Data from Local System T1006: Direct Volume Access	https://support.solarwinds.com/SuccessCenter/s/article/Serv-U-15-4-2-Hotfix-2-Release-Notes

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-34048	✗	VMware vCenter Server	UNC3886
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:*	VirtualPita, VirtualPie, VirtualGate, MOPSLED and RIFLESPINE
VMware vCenter Server Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23677

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-41328	✗	Fortinet FortiOS	UNC3886
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	VirtualPita, VirtualPie, VirtualGate, MOPSLED and RIFLESPINE
Fortinet FortiOS Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1588.006: Vulnerabilities T1059: Command and Scripting Interpreter	https://www.fortiguard.com/psirt/FG-IR-22-369

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-22948	✗	Vmware vCenter Server	UNC3886
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*	VirtualPita, VirtualPie, VirtualGate, MOPSLED and RIFLESPINE
Vmware vCenter Server Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-276	T1588.006: Vulnerabilities	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23623

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20867		VMware Tools	UNC3886
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:tools:*:*:*:*:*:*:*:*	VirtualPita, VirtualPie, VirtualGate, MOPSLED and RIFLESPINE
VMware Tools Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23675

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-42475		Fortinet FortiOS	UNC3886
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	VirtualPita, VirtualPie, VirtualGate, MOPSLED and RIFLESPINE
Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1588.006: Vulnerabilities T1059: Command and Scripting Interpreter	https://www.fortiguard.com/psirt/FG-IR-22-398

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-0762	✓	Phoenix SecureCore for Intel Kaby Lake: from 4.0.1.1 before 4.0.1.998; Phoenix SecureCore for Intel Coffee Lake: from 4.1.0.1 before 4.1.0.562; Phoenix SecureCore for Intel Ice Lake: from 4.2.0.1 before 4.2.0.323; Phoenix SecureCore for Intel Comet Lake: from 4.2.1.1 before 4.2.1.287; Phoenix SecureCore for Intel Tiger Lake: from 4.3.0.1 before 4.3.0.236; Phoenix SecureCore for Intel Jasper Lake: from 4.3.1.1 before 4.3.1.184; Phoenix SecureCore for Intel Alder Lake: from 4.4.0.1 before 4.4.0.269; Phoenix SecureCore for Intel Raptor Lake: from 4.5.0.1 before 4.5.0.218; Phoenix SecureCore for Intel Meteor Lake: from 4.5.1.1 before 4.5.1.15	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:phoenix:securecore_for_intel_kaby_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_coffee_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_ice_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_comet_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_tiger_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_jasper_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_alder_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_raptor_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_alder_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_meteor_lake:*:*:*:*:*:*:*:*	-
UEFIcanhazbufferoverflow (Phoenix SecureCore UEFI firmware Buffer Overflow Vulnerability)	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-120	T1068: Exploitation for Privilege Escalation	https://www.phoenix.com/security-notifications/cve-2024-0762/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-2586		Linux kernel	ExCobalt
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	GoRed Backdoor
Linux Kernel nft_object Use-After-Free Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation	https://lore.kernel.org/netfilter-devel/20220809170148.164591-1-cascardo@canonical.com/T/#t

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-3156		Sudo before 1.9.5p2	ExCobalt
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sudo_project:sudo:*:*:*:*:*:*:*:*	GoRed Backdoor
Baron Samedit (Sudo Heap-Based Buffer Overflow Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-193	T1068: Exploitation for Privilege Escalation	https://www.sudo.ws/releases/stable/#1.9.5p2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-4034		Red Hat Polkit	ExCobalt
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:polkit_project:polkit:*:*:*:*:*:*:*:*	GoRed Backdoor
Pwnkit (Red Hat Polkit Out-of-Bounds Read and Write Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1068: Exploitation for Privilege Escalation T1059: Command and Scripting Interpreter	https://bugzilla.redhat.com/show_bug.cgi?id=2025869

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-13272		Linux kernel before 5.1.17	ExCobalt
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	GoRed Backdoor
Linux Kernel Improper Privilege Management Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.1.17

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-27228	✗	Bitrix before 21.0.100	ExCobalt
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:bitrix24:bitrix24:*:*:*:*:*:*:*:*	GoRed Backdoor
Bitrix Arbitrary Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://helpdesk.bitrix24.com/open/15536776/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228	✓	Apache Log4j2	ExCobalt
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	GoRed Backdoor
Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1059: Command and Scripting Interpreter	https://logging.apache.org/log4j/2.x/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40438	✗	Apache HTTP Server 2.4.48 and earlier	ExCobalt
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*	GoRed Backdoor
Apache HTTP Server-Side Request Forgery	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1090: Proxy T1005: Data from Local System	https://httpd.apache.org/security/vulnerabilities_24.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3519	✗	Citrix NetScaler ADC and NetScaler Gateway	ExCobalt
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:*	GoRed Backdoor
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-12725	✗	Zeroshell 3.9.0	ExCobalt
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:zeroshell:zeroshell:3.9.0:*:*:*:*:*:*:*	GoRed Backdoor
Zeroshell Remote Command Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	Reached EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-40691	✗	Moxa SDS-3008: 2.1	ExCobalt
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:moxa:sds-3008_firmware:*:*:*:*:*:*:*:*	GoRed Backdoor
Moxa Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1588.006: Vulnerabilities	https://www.moxa.com/en/support/product-support/security-advisory/sds-3008-series-multiple-web-vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-5806	✗	Progress MOVEit Transfer: from 2023.0.0 before 2023.0.11, from 2023.1.0 before 2023.1.6, from 2024.0.0 before 2024.0.2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:progress:moveit_transfer:*:*:*:*:*:*:*:*	-
Progress MOVEit Transfer Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation	https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-5805	✗	MOVEit Gateway 2024.0.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:progress:moveit_gateway:*:*:*:*:*:*:*:*	-
Progress MOVEit Gateway Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation	https://community.progress.com/s/article/MOVEit-Gateway-Critical-Security-Alert-Bulletin-June-2024-CVE-2024-5805

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PurpleInk	A customized version of QuasarRAT, termed PurpleInk, is used as the primary implant after successfully breaching vulnerable internet-exposed application servers. PurpleInk is extensively obfuscated and highly versatile. It can execute new applications, perform file operations, gather system information, and enumerate directories and running processes.	Exploiting Vulnerable Application Servers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Compromised Infrastructure, Information Theft, Resource Hijacking	-
ASSOCIATED ACTOR			**PATCH LINK**
LilacSquid			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CarnavalHeist	CarnavalHeist is a new banking trojan malware that stands out for using a Python-based loader. It targets banking desktop applications, stealing credentials through overlay attacks and keylogging.	Spam emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Banking Trojan		Credential Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TargetCompany	The TargetCompany ransomware group has developed a new Linux variant using a custom shell script for payload delivery and execution. It targets VMWare ESXi environments to increase disruption and the chances of ransom payment.	Exploiting Public-Facing Application	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft, Espionage, Financial Loss	Windows, Linux, VMWare ESXi
Ransomware			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RansomHub	RansomHub, a newly emerged Ransomware-as-a-Service (RaaS) entity, has swiftly ascended to become one of the most prominent ransomware groups in operation. It is suspected to be an updated and rebranded iteration of the Knight ransomware. Both RansomHub's payload is written in Go, with most variants obfuscated using Gobfuscate.	Exploiting the Zerologon vulnerability	CVE-2020-1472
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft, Financial Gain, and Compromised infrastructure	Microsoft Netlogon
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472

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
Knight ransomware	Knight developed in Go, can initiate a reboot of an endpoint in safe mode before starting encryption. The source code for Knight, initially known as Cyclops, became available for purchase on underground online platforms in February 2024 after its creators decided to cease operations.	Exploiting the Zerologon vulnerability	CVE-2020-1472
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft, Financial Gain, and Compromised infrastructure	Microsoft Netlogon
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Muhstik	The Muhstik malware has been found targeting message queuing service applications, particularly the Apache RocketMQ platform. Muhstik, a notorious threat known for targeting IoT devices and Linux-based servers, for cryptocurrency mining and DDoS attacks.	Exploiting a vulnerability in Apache RocketMQ	CVE-2023-33246
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Denial Of Service, Espionage, Resource Hijacking	RocketMQ
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://rocketmq.apache.org/download/

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
Fog Ransomware	Fog ransomware has been targeting educational and recreational institutions in the United States. This ransomware attacks virtual environments within organizations, potentially causing significant disruption.	Exploiting compromised VPN credentials	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Data encryption, Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ValleyRAT	ValleyRAT, discovered in 2023 and linked to a China-based threat actor, is a Remote Access Trojan (RAT). This sophisticated malware employs a multi-stage infection process to execute various malicious activities.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Infiltrate and compromise systems	-
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
WARMCOOKIE	WARMCOOKIE functions as an initial backdoor tool, used to explore victim networks and deploy further malicious payloads. Each instance is compiled with a hard-coded C2 IP address and an RC4 key.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Steal information, install other malware,	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TellYouThePass	TellYouThePass is a ransomware threat that's been active since 2019. It encrypts files on a victim's computer and demands a ransom payment to restore them. It exploits vulnerabilities in software to gain access to systems. Recently, it's been seen targeting a new vulnerability (CVE-2024-4577) that impacts PHP.	Exploiting vulnerabilities	CVE-2024-4577
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Data encryption, Financial loss	PHP
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.php.net/downloads

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Black Basta	Black Basta is a ransomware-as-a-service (RaaS) group that emerged in early 2022. Cardinal Threat Group, known to be associated with Black Basta ransomware group, is believed to have exploited a Windows CVE-2024-26169 as zero-day.	Exploiting vulnerabilities	CVE-2024-26169
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft, Data encryption, Financial loss	Microsoft Windows
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
Cardinal Threat Group			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26169

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DISGOMOJI	DISGOMOJI, written in Golang and compiled for Linux systems, is a UPX-packed ELF2 binary that uses Discord for C2. DISGOMOJI maintains persistence on the system using cron jobs. The malware listens for new messages in the command channel on the Discord server, where C2 communication takes place through an emoji-based protocol.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		System Compromise	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
UTA0137			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PlugX (aka Korplug)	PlugX is a Remote Access Trojan (RAT) malware family that has been active since 2008. It serves as a backdoor, allowing attackers to gain full control over the victim's machine. Once the device is infected, the attacker can remotely execute a wide range of commands on the affected system.	By Exploiting F5 BIG-IP appliances	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Capture Screenshots, Execute commands	F5 BIG-IP
ASSOCIATED ACTOR			**PATCH LINK**
Velvet Ant			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BadSpace	BadSpace is a type of backdoor malware that provides unauthorized remote access to compromised systems, delivered via infected websites. BadSpace operate silently in the background, allowing attackers to maintain persistent access without the user's knowledge. BadSpace employs several techniques to detect and evade sandbox environments, making it difficult to analyze and detect.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Capture screenshots, Execute Commands	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Noodle RAT	Noodle RAT is available for both Windows and Linux. The Windows variant is an in-memory modular backdoor, while the Linux version can launch a reverse shell; both share identical command-and-control communication code.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Download malware, Execute commands	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Fickle Stealer	Fickle Stealer is an advanced information stealer written in Rust. This sophisticated malware employs a versatile targeting approach and utilizes four distinct distribution methods: a VBA dropper, a VBA downloader, a link downloader, and an executable downloader. Its primary objective is to harvest sensitive information from compromised systems.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Steal data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>VirtualPita</td><td rowspan="6">VIRTUALPITA is a 64-bit passive backdoor designed for VMware ESXi servers. It creates a listener on a hardcoded port number and often uses VMware service names and ports to disguise itself as a legitimate service. This backdoor supports arbitrary command execution, file upload and download, and the ability to start and stop the vmsyslogd service.</td><td>Exploiting Vulnerabilities</td><td>CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Backdoor</td><td rowspan="3">System Compromise</td><td>VMware vCenter Server, Fortinet FortiOS, VMware Tools</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>UNC3886</td><td>https://www.fortiguard.com/psirt/FG-IR-22-398 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23675 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23623 , https://www.fortiguard.com/psirt/FG-IR-22-369 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23677</td></tr>
</table>

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>VirtualPie</td><td rowspan="6">VIRTUALPIE is a lightweight backdoor written in Python that creates a daemonized IPv6 listener on a hardcoded port on a VMware ESXi server. It supports arbitrary command execution, file transfer capabilities, and reverse shell functionality. Communications are encrypted using RC4 and utilize a custom protocol.</td><td>Exploiting Vulnerabilities</td><td>CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Backdoor</td><td rowspan="3">System Compromise</td><td>VMware vCenter Server, Fortinet FortiOS, VMware Tools</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>UNC3886</td><td>https://www.fortiguard.com/psirt/FG-IR-22-398 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23675 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23623 , https://www.fortiguard.com/psirt/FG-IR-22-369 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23677</td></tr>
</table>

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>VirtualGate</td><td rowspan="6">VIRTUALGATE is a C utility program that consists of a dropper and a payload. The dropper decrypts a second-stage DLL payload, which uses VMware's VMCI sockets to execute commands on a guest virtual machine from a hypervisor host or between guest virtual machines on the same host.</td><td>Exploiting Vulnerabilities</td><td>CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Backdoor</td><td rowspan="3">Execute Commands</td><td>VMware vCenter Server, Fortinet FortiOS, VMware Tools</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>UNC3886</td><td>https://www.fortiguard.com/psirt/FG-IR-22-398 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23675 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23623 , https://www.fortiguard.com/psirt/FG-IR-22-369 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23677</td></tr>
</table>

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>MOPSLED</td><td rowspan="6">MOPSLED is a shellcode-based modular backdoor that communicates with its command-and-control (C2) server via HTTP or a custom binary protocol. Its core functionality involves retrieving plugins from the server and decrypting both embedded and external configuration files using a custom ChaCha20 encryption algorithm.</td><td>Exploiting Vulnerabilities</td><td>CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Backdoor</td><td rowspan="3">System Compromise</td><td>VMware vCenter Server, Fortinet FortiOS, VMware Tools</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>UNC3886</td><td>https://www.fortiguard.com/psirt/FG-IR-22-398 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23675 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23623 , https://www.fortiguard.com/psirt/FG-IR-22-369 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23677</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
RIFLESPINE	RIFLESPINE is a cross-platform backdoor that utilizes Google Drive for file transfer and command execution. It employs the CryptoPP library to implement the AES algorithm for data encryption and decryption.	Exploiting Vulnerabilities	CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	VMware vCenter Server, Fortinet FortiOS, VMware Tools
ASSOCIATED ACTOR			**PATCH LINK**
UNC3886			https://www.fortiguard.com/psirt/FG-IR-22-398 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23675 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23623 , https://www.fortiguard.com/psirt/FG-IR-22-369 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23677

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
SugarGh0st	SugarGh0st RAT is a remote access trojan and a customized variant of Gh0stRAT. It features customized commands to facilitate remote administration tasks as directed by the C2 server and a modified communication protocol, based on the similarity of the command structure and the strings used in the code.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Execute commands	-
ASSOCIATED ACTOR			**PATCH LINK**
SneakyChef			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SpiceRAT	SpiceRAT employs the DLL sideloading technique, exploiting a legitimate signed executable to load a malicious DLL loader binary. This advanced malware collects reconnaissance data from the victim's machine, including operating system details, hostname, username, and network information.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Steal Information	-
ASSOCIATED ACTOR			**PATCH LINK**
SneakyChef			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DragonForce Ransomware	DragonForce has been observed using a leaked ransomware builder from the LockBit ransomware group. DragonForce ransomware targets victims with the intent of extortion. The threat actor typically employs a double extortion tactic: first, they lock the victims out of their infected machines and exfiltrate data before encryption.	Phishing, Exploiting Vulnerabilities	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt data	-
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
GoRed Backdoor	GoRed Backdoor uses the RPC protocol to communicate with its command and control (C2) server. This malware can obtain credentials from compromised systems. Operators utilize DNS/ICMP tunneling, WSS, and QUIC to communicate with GoRed. It gathers various types of information from compromised systems, including details of active processes, host names, lists of network interfaces, and file system structures. GoRed serializes, encrypts, archives, and sends the collected data to a specialized server dedicated to storing compromised information.	Exploiting Vulnerabilities	CVE-2022-2586 CVE-2021-3156 CVE-2021-4034 CVE-2019-13272 CVE-2022-27228 CVE-2021-44228 CVE-2021-40438 CVE-2023-3519 CVE-2019-12725 CVE-2022-40691
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft, Encrypt Data	Linux kernel, Sudo, Red Hat Polkit, Bitrix, Apache Log4j2, Apache HTTP Server, Citrix NetScaler ADC and NetScaler Gateway, Zeroshell, Moxa-SDS
ASSOCIATED ACTOR			**PATCH LINK**
ExCobalt			https://lore.kernel.org/netfilter-devel/20220809170148.164591-1-cascardo@canonical.com/T/#t , https://www.sudo.ws/releases/stable/#1.9.5p2 , https://bugzilla.redhat.com/show_bug.cgi?id=2025869 , https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.1.17 , https://helpdesk.bitrix24.com/open/15536776/ , https://logging.apache.org/log4j/2.x/security.html , https://httpd.apache.org/security/vulnerabilities_24.html , https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467 , https://www.moxa.com/en/support/product-support/security-advisory/sds-3008-series-multiple-web-vulnerabilities

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
XWorm RAT	XWorm allows to gain unauthorized access to devices, facilitating the theft of sensitive information such as login credentials and passwords. Additionally, it includes features for clipboard monitoring, installing ransomware, and launching Distributed Denial of Service (DDoS) attacks.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
UAC-0184			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BMANAGER	The BMANAGER Trojan is a sophisticated malware providing remote access to attackers. It disguises itself as legitimate software, avoids detection, and can disable security features. Its primary functions include log keystrokes, data theft and system manipulation, posing significant cybersecurity threats.	custom malware delivery platform	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		System Compromise	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Boolka			-

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
CatB Ransomware	CatB is a ransomware that uses DLL hijacking to evade detection. It injects itself into the Microsoft Distributed Transaction Coordinator (MSDTC) service, a legitimate Windows process, and uses that process to encrypt the victim's files. This makes it harder for security scanners to identify the ransomware, as it is not running as a standalone process and may not show the typical behavior of ransomware.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			**PATCH LINK**
ChamelGang			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
InnoLoader	InnoLoader is a new unique malware that generates a distinct version with each download, complicating detection. It disguises itself as an installer, executing malicious actions and downloading additional payloads. The malware adapts its behavior based on C2 server instructions to evade detection.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Execute Commands	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
LilacSquid (aka UAT-4820)</td><td>-</td><td rowspan="3">Information Technology, Research, Industrial, Energy, Pharmaceutical, Oil and Gas</td><td rowspan="3">United States, Europe, Asia</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft, Espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>PurpleInk</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1584: Compromise Infrastructure; T1584.004: Server; T1587: Develop Capabilities; T1587.001: Malware; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1055: Process Injection; T1005: Data from Local System; T1001: Data Obfuscation; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
Operation Ghostwriter (aka UAC-0057, UNC1151, TA445, UAC-0051, PUSHCHA, DEV-0257, Storm-0257)</td><td>Belarus</td><td rowspan="2">Defense</td><td rowspan="2">Ukraine</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft, Espionage, Sabotage, and destruction</td></tr>
<tr><td></td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td></td><td>-</td><td>-</td><td>Microsoft Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1497: Virtualization/Sandbox Evasion; T1055: Process Injection; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1211: Exploitation for Defense Evasion; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1518: Software Discovery; T1518.001: Security Software Discovery; T1566: Phishing; T1480: Execution Guardrails; T1070: Indicator Removal; T1070.004: File Deletion; T1203: Exploitation for Client Execution; T1218: System Binary Proxy Execution; T1218.010: Regsvr32; T1218.011: Rundll32; T1140: Deobfuscate/Decode Files or Information; T1057: Process Discovery; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Cardinal Threat Group (aka Storm-1811, UNC4393)	-	-	Worldwide
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-26169	Black Basta ransomware (aka no_name_software)	-
TTPs			
TA0002: Execution, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0003: Persistence, TA0040: Impact, TA0042: Resource Development, 1588.006: Vulnerabilities, T1588.005: Exploits, T1588: Obtain Capabilities, T1068: Exploitation for Privilege Escalation, T1486: Data Encrypted for Impact, T1036: Masquerading, T1059: Command and Scripting Interpreter			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UTA0137	Pakistan	Government	India
	MOTIVE		
	Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	DISGOMOJI	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1053: Scheduled Task/Job; T1053.003: Cron; T1105: Ingress Tool Transfer; T1082: System Information Discovery; T1059: Command and Scripting Interpreter; T1071: Application Layer Protocol; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1547: Boot or Logon Autostart Execution; T1547.013: XDG Autostart Entries			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Velvet Ant	China	All	China, Hong Kong, Macau, Japan, Mongolia, North Korea, South Korea, Taiwan
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PlugX (aka Korplug)	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1133: External Remote Services; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1059.008: Network Device CLI; T1569: System Services; T1569.002: Service Execution; T1037.004: RC Scripts; T1133: External Remote Services; T1078.002: Domain Accounts; T1078.003: Local Accounts; T1574: Hijack Execution Flow; T1574.001: DLL Search Order Hijacking; T1562.004: Disable or Modify System Firewall; T1055: Process Injection; T1070.006: Timestomp; T1003.001: LSASS Memory; T1087.002: Domain Account; T1083: File and Directory Discovery; T1135: Network Share Discovery; T1018: Remote System Discovery; T1082: System Information Discovery; T1016: System Network Configuration Discovery; T1021.001: Remote Desktop Protocol; T1021.004: SSH; T1570: Lateral Tool Transfer; T1039: Data from Network Shared Drive; T1572: Protocol Tunneling; T1090.001: Internal Proxy; T1048: Exfiltration Over Alternative Protocol			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC3886	China	Government, Telecommunications, Technology, Aerospace, Defense, Energy and Utility	North America, Oceania, Europe, Africa, and Asia
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-34048 CVE-2022-41328 CVE-2022-22948 CVE-2023-20867 CVE-2022-42475	VirtualPita, VirtualPie, VirtualGate, MOPSLED and RIFLESPINE	VMware vCenter Server, Fortinet FortiOS, VMware Tools
TTPs			
TA0002:Execution; TA0004:Privilege Escalation; TA0042: Resource Development; TA0005: Defense Evasion; TA0006:Credential Access; TA0011: Command and Control; TA0003: Persistence; TA0008: Lateral Movement; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities; T1059: Command and Scripting Interpreter; T1014: Rootkit; T1021.004: SSH; T1021: Remote Services; T1078: Valid Accounts T1202: Indirect Command Execution; T1140: Deobfuscate/Decode Files or Information; T1095: Non-Application Layer Protocol; T1588.004: Digital Certificates; T1584: Compromise Infrastructure; T1071.001:Web Protocols; T1071: Application Layer Protocol; T1600: Weaken Encryption			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 SneakyChef	China	Government	Europe, Middle East, Africa and Asia
	MOTIVE		
	Espionage and Information theft		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	SugarGh0st, SpiceRAT	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003:Persistence; TA0004: Privilege Escalation; TA0005:Defense Evasion; TA0009:Collection; TA0006: Credential Access; T1053.005: Scheduled Task; T1566: Phishing; T1027: Obfuscated Files or Information; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1036: Masqueradin;g T1204: User Execution; T1204.002: Malicious File; T1059.005: Visual Basic; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1547.001: Registry Run Keys /Startup Folder; T1547: Boot or Logon Autostart Execution; T1056.001: Keylogging; T1056: Input Capture; T1218.010: Regsvr32; T1218: System Binary Proxy Execution

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 ExCobalt	-	Metallurgy, Telecommunications, Mining, Information Technology, Government, Software development	Russia
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-2586 CVE-2021-3156 CVE-2021-4034 CVE-2019-13272 CVE-2022-27228 CVE-2021-44228 CVE-2021-40438 CVE-2023-3519 CVE-2019-12725 CVE-2022-40691	GoRed Backdoor	Linux kernel, Sudo, Red Hat Polkit, Bitrix, Apache Log4j2, Apache HTTP Server, Citrix NetScaler ADC and NetScaler Gateway, Zeroshell, Moxa-SDS

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control;TA0040: Impact; TA0043: Reconnaissance; TA0042: Resource Development; T1595.002; Vulnerability Scanning; T1583.001: Domains; T1583.002: DNS Server; T1587.003: Digital Certificates; T1199: Trusted Relationship; T1195.001: Compromise Software Dependencies and Development Tools; T1059.003: Windows Command Shell; T1059.004: Unix Shell; T1059.006: Python; T1106: Native API; T1053.003: Cron; T1505.003: Web Shell; T1136.001: Local Account; T1068: Exploitation for Privilege Escalation; T1140: Deobfuscate/Decode Files or Information; T1027.002: Software Packing; T1027: Obfuscated Files or Information; T1601.001: Patch System Image; T1070.004: File Deletion; T1003.008: /etc/passwd and /etc/shadow; T1003.001: LSASS Memory; T1082: System Information Discovery; T1614.001: System Language Discovery; T1033: System Owner/User Discovery; T1087.001: Local Account; T1083: File and Directory Discovery; T1046: Network Service Discovery; T1057: Process Discovery; T1021.004: SSH; T1021.002: SMB/Windows Admin Shares; T1021.001: Remote Desktop Protocol; T1563.001: SSH Hijacking; T1560.001: Archive via Utility; T1560.002: Archive via Library; T1074: Data Staged; T1071.001: Web Protocols; T1132.001: Standard Encoding; T1071.004: DNS; T1572: Protocol Tunneling; T1132.002: Non-Standard Encoding; T1573.001: Symmetric Cryptography; T1090.001: Internal Proxy; T1095: Non-Application Layer Protocol; T1041: Exfiltration Over C2 Channel; T1048.001: Exfiltration Over Symmetric Encrypted Non-C2 Protocol; T1020: Automated Exfiltration; T1567: Exfiltration Over Web Service; T1485: Data Destruction; T1486: Data Encrypted for Impact

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UAC-0184	-	All	Ukraine, Finland
	MOTIVE		
	Espionage, Information theft		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	XWorm RAT	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1574: Hijack Execution Flow; T1547.001: Registry Run Keys / Startup Folder; T1574.002: DLL Side-Loading; T1055: Process Injection; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1057: Process Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1059.005: Visual Basic; T1566: Phishing; T1566.001: Spearphishing Attachment			

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

Boolka</td><td>-</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage, Information theft</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>BMANAGER</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0009: Collection; TA0006: Credential Access; TA0001: Initial Access; TA0010: Exfiltration; TA0040: Impact; TA0007: Discovery; T1059: Command and Scripting Interpreter; T1036: Masquerading; T1204:User Execution; T1204.002: Malicious File; T1583.004: Server; T1584.003: Virtual Private Server; T1584: Compromise Infrastructure; T1588.002: Tool; T1588: Obtain Capabilities; T1056.001: Keylogging; T1056:Input Capture; T1583.001: Domains; T1583: Acquire Infrastructure; T1189: Drive-by Compromise; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1203: Exploitation for Client Execution; T1569: System Services; T1569.002: Service Execution; T1543: Create or Modify System Process; T1543.003: Windows Service; T1001: Data Obfuscation; T1657:Financial Theft; T1082: System Information Discovery; T1083: File and Directory Discovery; T1210: Exploitation of Remote Services; T1005: Data from Local System; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1041: Exfiltration Over C2 Channel; T1565: Data Manipulation; T1565.002: Transmitted Data Manipulation; T1608: Stage Capabilities; T1608.001: Upload Malware</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
ChamelGang (aka CamoFei)</td><td>China</td><td rowspan="3">East Asia, South Asia, North America, South America, and Europe</td><td rowspan="3">Aviation, Business Services, Construction, Consulting, Critical Infrastructure, Education, Finance, Food, Gambling, Government, Healthcare, Legal, Manufacturing, Media, Non-Profit, Research, Retail, Software, Textiles</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>CatB Ransomware</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1003: OS Credential Dumping; T1016: System Network Configuration Discovery; T1068: Exploitation for Privilege Escalation; T1046: Network Service Discovery; T1057: Process Discovery; T1033: System Owner/User Discovery; T1027: Obfuscated Files or Information; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1082: System Information Discovery; T1482: Domain Trust Discovery; T1078: Valid Accounts; T1018: Remote System Discovery; T1069.002: Domain Groups; T1560.001: Archive via Utility; T1136.002: Domain Account; T1069.001: Local Groups; T1219: Remote Access Software; T1657: Financial Theft; T1490: Inhibit System Recovery; T1562.001: Disable or Modify Tools; T1486: Data Encrypted for Impact; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1598: Phishing for Information	T1598: Phishing for Information
	T1591: Gather Victim Org Information	T1591.004: Identify Roles
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
TA0042: Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits
		T1588.002: Tool
		T1588.006: Vulnerabilities
	T1584: Compromise Infrastructure	T1584.004: Server
		T1588.004: Digital Certificates
		T1584.003: Virtual Private Server
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.003: Digital Certificates
	T1608: Stage Capabilities	T1608.001: Upload Malware
	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.002: DNS Server
		T1583.004: Server
TA0001: Initial Access	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spearphishing Attachment
	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
	T1133: External Remote Services	
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1659: Content Injection	
	T1189: Drive-by Compromise	
	T1199: Trusted Relationship	
TA0002: Execution	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
		T1059.001: PowerShell
		T1059.005: Visual Basic
		T1059.004: Unix Shell
		T1059.006: Python
		T1059.007: JavaScript
		T1059.008: Network Device CLI
	T1204: User Execution	T1204.002: Malicious File
		T1204.001: Malicious Link
	T1053: Scheduled Task/Job	T1053.003: Cron
	T1569: System Services	T1569.002: Service Execution
		T1053.005: Scheduled Task
	T1203: Exploitation for Client Execution	
	T1106: Native API	
	T1047: Windows Management Instrumentation	

Tactic	Technique	Sub-technique
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1136: Create Account	T1136.001: Local Account
		T1136.002: Domain Account
	T1505: Server Software Component	T1505.003: Web Shell
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.009: Shortcut Modification
		T1547.013: XDG Autostart Entries
	T1037: Boot or Logon Initialization Scripts	T1037.005: Startup Items
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
		T1548.003: Sudo and Sudo Caching
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
	T1078.002: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1037: Boot or Logon Initialization Scripts	T1037.005: Startup Items
		T1037.004: RC Scripts
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.009: Shortcut Modification
		T1547.013: XDG Autostart Entries
TA0005: Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.008: Masquerade File Type
	T1027: Obfuscated Files or Information	T1027.009: Embedded Payloads
		T1027.010: Command Obfuscation
		T1027.012: LNK Icon Smuggling
		T1027.013: Encrypted/Encoded File
		T1027.002: Software Packing
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
		T1562.009: Safe Mode Boot
	T1140: Deobfuscate/Decode Files or Information	
	T1070: Indicator Removal	T1070.004: File Deletion
		T1070.006: Timestomp
		T1070.001: Clear Windows Event Logs
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.001: DLL Search Order Hijacking

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1218: System Binary Proxy Execution	T1218.011: Rundll32
		T1218.010: Regsvr32
		T1218.007: Msiexec
	T1497: Virtualization/Sandbox Evasion	
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
		T1548.003: Sudo and Sudo Caching
	T1480: Execution Guardrails	
	T1006: Direct Volume Access	
	T1601: Modify System Image	T1601.001: Patch System Image
	T1620: Reflective Code Loading	
	T1014: Rootkit	
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
	T1202: Indirect Command Execution	
	T1600: Weaken Encryption	
	T1211: Exploitation for Defense Evasion	
TA0006: Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1003: OS Credential Dumping	T1003.008: /etc/passwd and /etc/shadow
	T1110: Brute Force	T1110.004: Credential Stuffing
TA0007: Discovery	T1120: Peripheral Device Discovery	
	T1069: Permission Groups Discovery	T1069.001: Local Groups
	T1614: System Location Discovery	T1614.001: System Language Discovery
TA0008: Lateral Movement	T1550: Use Alternate Authentication Material	T1550.002: Use Alternate Authentication Material: Pass the Hash
	T1563: Remote Service Session Hijacking	T1563.001: SSH Hijacking
TA0009: Collection	T1039: Data from Network Shared Drive	
	T1560: Archive Collected Data	T1560.002: Archive via Library
TA0011: Command and Control	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
	T1132: Data Encoding	T1132.002: Non-Standard Encoding
	T1102: Web Service	
	T1571: Non-Standard Port	
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1573: Encrypted Channel	
	T1104: Multi-Stage Channels	
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1567: Exfiltration Over Web Service	
	T1048: Exfiltration Over Alternative Protocol	T1048.001: Exfiltration Over Symmetric Encrypted Non-C2 Protocol
	T1020: Automated Exfiltration	

Tactic	Technique	Sub-technique
TA0040: Impact	T1486: Data Encrypted for Impact	
	T1657: Financial Theft	
	T1490: Inhibit System Recovery	
	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	
	T1485: Data Destruction	
	T1489: Service Stop	
	T1496: Resource Hijacking	
	T1529: System Shutdown/Reboot	
	T1565: Data Manipulation	T1565.002: Transmitted Data Manipulation

Top 5 Takeaways

#1 In **June**, there were **nine zero-day** vulnerabilities, with the '**Five** Celebrity Vulnerabilities' taking center stage. These featured flaws such as **Zerologon, UEFIcanhazbufferoverflow, Baron Samedit , Pwnkit** and **Log4shell.**

#2 Over the course of the month, a variety of ransomware variants, including the well-known **Black Basta** strain, have been actively targeting victims on a global scale. **TargetCompany ransomware**, another malicious program, has focused its attacks on a more specific geographical range, primarily targeting victims in **Taiwan, India, Thailand,** and **South Korea**. Furthermore, **ExCobalt**, a cyber espionage-focused threat actor, has been targeting Russian organizations using an advanced Golang-based backdoor called **GoRed**.

#3 A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These include the **DISGOMOJI, PlugX, BadSpace, Noodle RAT, Fickle Stealer, VirtualPita, VirtualPie, VirtualGate, MOPSLED.**

#4 **Eleven** active adversaries were identified across multiple campaigns, targeting the following key industries: **Technology, Government, Education, Energy** and **Telecommunications**

#5 Multiple campaigns leveraging sophisticated, previously unseen malware and ransomware variants orchestrated a total of 29 attacks. These attacks top impacted **South Korea, India, China, and Japan.**

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **38 significant vulnerabilities** and block the indicators related to the **11 active threat actors, 29 active malware,** and **187 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 **38 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 (JUNE 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

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
PurpleInk	SHA256	2eb9c6722139e821c2fe8314b356880be70f3d19d8d2ba530adc9f466ffc67d8
CarnavalHeist	IPv4	104[.]41[.]51[.]80, 191[.]239[.]116[.]217, 191[.]239[.]123[.]241, 191[.]233[.]241[.]96, 191[.]234[.]212[.]140, 191[.]235[.]233[.]246, 4[.]203[.]105[.]118, 191[.]233[.]248[.]170
	SHA256	c300749ea44f886be1887b3e19b946efbdbbc3e1bf3e416c78cfbff8d23bf70a, 1b4f44a00f61b3e0c8cd6c3125f03b6d4897d6ab90c8a6dc899ed96acee80dd6, 8424e76c9a4ee7a6d7498c2f6826fcde390616dc65032bebf6b2a6f8fbf4a535, d9877dc1ba0f977d100e687da59c216454d27e3988532652ac8f6331debbd071, 0d94547a0b8f9795e97e2a4a58b0ece65b4ea4b6e6019cbc96e1c79f373b4587, f848c0f66afc7b5a10f060c1db129529a974ae0ad71a767f7c7793351bb7ca04, e50bde1e319e699f587d3b5403c487e46deed61cc3f078fe951e7cb9f6896259, f00cb0603c055c85c7cdf9963d919d527b13013c182dc115ba733d28da57b1d9, 2c53b4dc15882cf22772994d8ed0947e4a8b70aef3a12ab190017b3317c167ea, a6d995d015c16985b456bcc5cd44377c3e5e5cf72b17771eadc51e1d02a3c6ef, 21e22c4736e7567b198b505ed303c3ca933e0c2d931b886756f6db18a9884a75, 2c1251ae1ec9d417bbbdd1f6ac99baa3f16a7639d0c12cb2883ef8c22c73e58e, 46e754727efdc2c891319d25a67ee999a4d8a0b21b0113db08eead42cf51b780, cd9f5773bd7672a3e09f2d05ef26775e8c7241879d5f4d13c5c5bc1704c49fa1, f2db799d892f2a7ac82bfa15826e74d778abdfa153ccafb9db1fdf56a0248a40, 5782b9bc96ce5ad011c122496ff0ff0dc08d6444c6d2e98606ada82130d5f21a, 19c02c5724622be4eedff95633f3fbaa604449aa50cc0761693bb8adb1e8cf97, 3b450994add1e3a206c56a7f8fd28e4132cffb27f3df345e07e8908d7989751f,

Attack Name	TYPE	VALUE
CarnavalHeist	SHA256	1e8fd8531a0851bb4d8fb6d8dd4b1a9509c8a971b11b7d95871d7b39004650ad, 8c31dcbef5c00fd98e426a1ae84163b807a2c5d1476b2d306c8f7e9d01d8df23, 2bcd8cc83cf31a77a556d5462a7e75c5e2120891414684a6e21612d61d734673, 44df224b304a9d5d089be7d68d7e5cec4c76ec58fdc16c3f86b20a671b496cf4, b8b3963967232916cd721a22c80c11cd33057bd5629dcfa3f4b03d8a6dbf1403, 883c49b7c869019951eff94699480a7ecc97c9c45060a15797ecbd5fce060d26, e7aa64726783ec6f7249483e984ae20b31a091a488a3ed0f83c210702c506d20, b152346c2679392d7e15d1cc72a39a21d24e55360c4c1c845ef3524924e93fa9, 561e6a42e23d12abe6bba8c98f84c3ba7c45a5df840bfa6fd0dfea803c9b4b7e, 7e0051d9221c13a47245359a2cd2804b4d3d9302a321fc8085da1cf1a64bac91, 056b34444abe385addd08cc581a640b72d4f2cba05de2bfd0c897d5b273a7f28, ab3a284ae6e4e466a0715c162cfab85d75522bec48fa25947b16a0891ec2358a, 7232e3318fdc370e611b2bcbaaec3d58a0d687927714c24dc81fe60767d53a31, 3c89775ae7c35fe3d1ec7e75ac9d4a19959d082d31ab412af24312544 0ffea6c, aadbba21380dba5028a68b44c629988b0ca517f34c1adbd68f2edd604ea507fb, 278897ee9158f9843125bc2e26c14f96c4e79d5fc578b7e5973dc8dc919a3400, 049b7067ac87e44f464cb18e454d878ca6260b667a34f48ed0046c29b45bb149, 8573b7aa7ac688e2fb03845aa7903b5f58d880865e3b63c4884f8e29839a3754, f92af5e770018c9e1be5d934bb5699fcf4594d870988e7b18fb65501ef43f8f9, 3445066ae58aa68c09b2476e65f96f46d0a3ae0a09366d8f9e7e592ee3f2aa0c, d3a7f22886cd294549e5f93ec18ab04e085c397ef703f5543c3b967c1172bf41
	URLs	hxxps[://]is[.]gd/38qeon?0177551.5510, hxxps[://]is[.]gd/ROnj3W?0808482.5176, hxxps[://]notafiscaleletronica[.]nf-e[.]pro/danfe/?notafiscal=00510242.500611, hxxps[://]nota-fiscal[.]nfe-digital[.]top/nota-estadual/?notafiscal=00792011.977347, hxxps[://]nfe-

Attack Name	TYPE	VALUE
CarnavalHeist	URLs	visualizer[.]app[.]br/notas/?notafiscal=000851113082.35493424000, hxxp[://]adobe-acrobat-visualizer[.]brazilsouth[.]cloudapp[.]azure[.]com/Documentos, hxxps[://]104[.]41[.]51[.]80@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]239[.]116[.]217@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]239[.]123[.]241@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]233[.]241[.]96@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]234[.]212[.]140@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]235[.]233[.]246@80/Documentos/files/a3[.]cmd, hxxp:[//]191[.]235[.]87[.]229/Documentos/dc/c[.]cmd
TargetCompany	URLs	hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x.sh, hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x, hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/post.php
	SHA1	dffa99b9fe6e7d3e19afba38c9f7ec739581f656, 2b82b463dab61cd3d7765492d7b4a529b4618e57, 9779aa8eb4c6f9eb809ebf4646867b0ed38c97e1, 3642996044cd85381b19f28a9ab6763e2bab653c, 4cdee339e038f5fc32dde8432dc3630afd4df8a2, 0f6bea3ff11bb56c2daf4c5f5c5b2f1afd3d5098
RansomHub	SHA256	02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292, 34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087, 7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a, 8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7, ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00
Knight Ransomware	SHA256	104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2, 2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad, 36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e, 595cd80f8c84bc443eff619add01b86b8839097621cdd148f30e7e2214f2c8cb,

Attack Name	TYPE	VALUE
Knight Ransomware	SHA256	7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2, E654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23
Muhstik	SHA256	9e28f942262805b5fb59f46568fed53fd4b7dbf6faf666bedaf6ff22dd416572, 1f9cda58cea6c8dd07879df3e985499b18523747482e8f7acd6b4b3a82116957, 176c57e3fa7da2fb2afcd18242b79e5881c2244f5ab836897d4846885f1bd993, a7bf3c031ab66265ce724fc26c8f7565442a098b06b01ea8871f13179d168713, 6730eb04edf45d590939d7ba36ca0d4f1d2f28a2692151e3c631e9f2d3612893, 86947b00a3d61b82b6f752876404953ff3c39952f2b261988baf63fbbbd6d6ae
Fog Ransomware	SHA1	f7c8c60172f9ae4dab9f61c28ccae7084da90a06, 507b26054319ff31f275ba44ddc9d2b5037bd295, e1fb7d15408988df39a80b8939972f7843f0e785, 83f00af43df650fda2c5b4a04a7b31790a8ad4cf, 44a76b9546427627a8d88a650c1bed3f1cc0278c
ValleyRAT	SHA256	46ea0173f8f8ee07575c1ab440f7b06c9519cfc85c9094cde05497c0adeb73c5, a5c7dd4e3b2113a51c5c031a3e5f37a0783e41d983ccdc9dbfd6735018a39338, a5d96982f492aeaa3461f397c58f5ea90be6b6087550dd01a0b43c76dd675f2b, a245d1f716919f561df98c5df164652ee76e6201cc6d12287a07b98f821b5aef, d404c0f796c73159e5cd95b976cb79134b27e567917ce0026965074a8c79c154, 8c4de69e89dcc659d2fff52d695764f1efd7e64e0a80983ce6d0cb9eeddb806c, 9763543f309b96bd89953245dec616a0777399f389f128e5334cf58167bd12a9, 1ddd09c086a9626426885916af78201429528a20d1ef6bb133aec3b25223b519, 880a51fc964a355cf8b4bcc985f315ffb1d4ac0394e8043706e9c9d187784564, c70e8867fe9a63a147588a53e26c6e68753157326c5e759742333ad6d5c5dcc2, c017974a8b52d728763d8c4ed2112809c76271eb9e3c1d64d7ab7e8a60d29217, b8637cecec68d2275fa7ac89782467053d92621577e46c741a136a350a14fe99, b8ebcd9d2621972514d7499cf34ae0e27e825b322baba243d29139eff70c0ba2,

Attack Name	TYPE	VALUE
ValleyRAT	SHA256	b10c10aa20f008273e0491ec0e6b74e0cddafb15e8b70366e11258b960a93855, bb8158746f3a8ed8040ca7986c21e3de026e844142685c5c0b79922b527fe5d0, a4a6d4257ba42d31c48c812d75de7eeab54a986c31e666c448c74f44909a23c8, eac4ef2479304cbf26ca73886871af920f3a857b460352fbf1218fa0f6a4d469, c6f6c537aa9cce0cfacb002034691cad14aad7fbbd7aa3e56b48b83f502879d8, 86412961d59001ddb6aac7044790324737401d6cd858d03c9baa3620b26f7cd9, b4f1234da98edeb3876c3aaa01b867a54db91a24a4d90615ddf7a7b53f959840
	MD5	c563f62191ea363259939a6b3ce7f192
WARMCOOKIE	SHA256	ccde1ded028948f5cd3277d2d4af6b22fa33f53abde84ea2aa01f1872fad1d13
TellYouThePass	SHA256	d18453e564ca27514227478f225d85811fe15d08aa5fb1f613022c43155c5c54, 170d654b61810992fef6f18dbce5b4c7f5762cf36c9b41c36a14c9f6609f6e7d, f572898ab9f9a0fabac77d5d388680f84f85f9eb2c01b4e5de426430c6b5008f, 9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53, ea59d6a130a279dfde4df53640bd720419c7b5d9711a21a78af9453b1b3b5805, aa0ef20f9f8ca111b0d8a550daf6651f5b0557f0acb0a26545755c5a02263a9b
Black Basta	SHA256	7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a, d9d2838327c081a6daf9528c77ff3a8ac88e8ff73521b97d34af0d3da5807e7c, a6fbdbf8efe0ea129636bb5b3d6d6faec298272a2afded7e7516f2491844abc7, e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757, df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415, d73f6e240766d,dd6c3c16eff8db50794ab8ab95c6a616d4ab2bc96780f13464d, b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9, 69192821f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944,

Attack Name	TYPE	VALUE
Black Basta	SHA256	62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087, 462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7, 5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43, 58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd, 51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e, 05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431, 3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35, 350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd, 0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e, 892bb04889678134fbdde62d573eef1274c328b4e216ea7dc17ed0065fe8be37, 58edd2a0980b15f7fc6c892011751a30c134757142a54c2cedcbba4af2cbf855, 723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224, ca0273c55507c3aae95539812c2c5d9bbdc80deb8e714360fe4bcc65d257aeb0, 0c915ce6cd1676ecc99863f47ed28c6466a2532ce9df7bbd2ae810b7bbf026f7, 753a66f032d0d7a7c310a2e5f98c54e95e3d404400224d592657a02079c668d5, 96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be, 82515c1c5675d68c0f1f7d7572d83819944cc951747879caf1653cf41ce792ba, 9f948af3a30f125dcd24d8a628b3a18c66b3d72baede8496ee735cbdfd9cf0c7, d943a4aabd76582218fd1a9a0a77b2f6a6715b198f9994f0feae6f249b40fdf9, ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e, 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a
DISGOMOJI	MD5	0d4111ab5471c7f5b909bff336ba8cd66f9d8630, e5182d13d66c3efaa7676510581d622f98471895, 2dfe824d0298201e0efb30f16b3ce8a409ffe006

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	ffc66d40bcdcba5089d27121a2f1fac2a9f49c7aa214be98748f9624ae7d1bbf, ff9423ce5748687dc09be8093b67ca86a1f6a3dd19bd43b8a8669717a8876ea3, fa6d61a607162a8687b049b1844edae82afe911ff6684e8ff77297fbd9bffe63, f9e0ad7f6b3343a5d75a77f8032e7aa6b0363df030b47d4b83fb9414b90a17e8, f97970d5a629fc72647a6397ca9638fabf28f701656f058067f43038629e34b8, f96023de8014a90858746fe6fe788f907902e60dd05cf70328a6fe1e3e66cd34, f7d974093ff22f705d96750cd06a91f59b519cb8c50f7ffea627cddd68cf20d3, f78aab9b8ab7d116a4e0e9f6903a22c67ea2e01f6b99101b5be990aa9d73fff7, f75f29589e08aeda2e13954c5e20e446b670518008f8c3423fc03beed7a945d0, f758227b90f46a41203476df409e23cea56d4824a4fec0c0a210ae9fb838b70c, f61b8e667882e2735a7cc4b73affd651c172c9d4c4df02b8e96b4a234a30bd86, f60fcde71c1947be6b89b19c6d62a10de38599dbc82bdb7949eb0e0991102073, f5caef720f1e32e5539e81dc24d88a582b3d5c9b8146650f5df7b2b18522d858, f392d7794132e8754e3eed756c60abf31eac94d3c70c73e33cb97b77d0b68f32, f36bdf4c7fec3d8de696c6df386a437f37e3713e8e20b79e47172894315148a6, f346bb5b305e2e2db5372436eb07e2fefa707143d38186ca071f072d51a7b141, f30056753e5a088e5a0f161061a5a6b8327f8ec65f6d984759b9fe4cbadc8851, f1ef7c0f62154ec377d50960f39573b5c34ad2e0388fd59c2082a1d1bca22b2f, f1623a0411763ff5af44940ecd82c6acb824fcddc790622e1bd081ec1041781b, f0513c677361050e0c593f293ca2b7eeebbf6fd11511a8dcea68efdc5dd9ec75, efcad47ae25743c3b3126fcb4d12f6751de18b55a6eec0e388ec5ba29675a48e, ef24544e2f7ecbf45c2cc1f9eece9b26a61cf93b7d9362119f27bdb8f36a625b, eeedf0393e6b4884ed1c656eb1dd597297db44d680543b86cc0eb4b342e151fb,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	ee46bf00c0f7095c3f3e63f0e85dc2ec2f49d70a9aa3fda6046e1d42e89b5613, ee0703bede4979d42505f32e3b18f34d6da112682cffd62be5111fb2becbb598, edf4ccd0162ffa049fa728dfedde9041feb09496d7a8582df24eb283842a33ab, edd925fecf34153c5cfdc5b6e53bb0fc2105ca5d58b9fb20c81a481405e790d2, ecf291d795b71a85015c78cd45c023f7f9df40d78b36b603788a6f858fe45632, ec5da6e65f245f5f9c1f4061c035bf6064aac75fe9784f06930c976147349905, ec2a9812f5fcc681236e7d274cab1f4f205f79f699c7b8618d521f08dac6eb58, eb85cbf5f4113685ca6cc2c03b0b5b10279c4bb8024d1a495e42d2d241c3eea2, eb2bb071928213edfdc17cd0be46cb9663fcfa85f37cd7e9b013b618c5f6c86e, eaaa0aa016cb8cb46396a477c47ed5b55ac2492e6d45769edad65fb650ae17e5, e8899cf683a906bb0978752f5ce32755365d594a6bdfc7ba76e9b2375aca2285, e871818b00f1dfd2a8967cc75435fb5d1cd646308715eecc89a6bea3f89ad12b, e7b3f9aff12d5d08e52d85f574b677f3e840eedefb980e1591d42c17062d9ecd, e78773ee9aa7e4121bbd7118d93ac1842595034078917b2e488cea40aa171b1f, e73aaac7d49efb0c47ec76625f520791c1048211846f86ebc7345275586f3012, e5595db0c2b46f8baffd5586d40a1482fa5d72cadb2a47b93afb922a6a596a0e, e51bd357c4c1f806521bd46ca9567bb1aee40ab6e81aae39ae89360ed415d707, e4e9ad2de5826d53117c56f04a03cb0372cdd3b66aec9092c74d6eb8544bccb8, e3f2ae137a1a6f17c445643b21a74f102670cad115ae7491190e13beaa836c50, e3ba82f314465d1d8201d66218545f13d967db5341acda58900233655a8edfcc, e3af5d57eb873782d4d66a645131122568c0432581714754502b5eed3775edab, e34a2cfcb4afda6bc918393e6f151f757bd3abb4c7775b6ba18b0756a5786a40,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	e2e7e04eb8eff0359137c638cc8f0a9c0ffbc1fd714ff17540bf459cb1a5d7db, e26b98840286379cd63a2b85ecee23db4af54ba5e32579012cb7b1abb85baf69, e17b4328ab4dbcc281236aaa7cb9c1adc71ea4536e67737f85b1832302868f62, e137b0a42d08f51fe6bbf1dc320c4a252b6336df18d6a23272e38d49930d64da, dff4594e3076dd655db3c3ed4dc4363f614b724ab7da0786645b486c15762ca8, df9ec49b0e6c3c64cb411abc2aa8c798932a2891064ad4adfbba3bdf5a81a892, dd559945d8a3624f97c7512b14fc8c7280d1d5cf9be61baa5f9ce8c5c04c8bea, dcaf4d83af8ea96c3c377f90573dd49938fbd28e00dea7d9748a5440bf4a2766, dbe6c90018b0e779c509cff3d761bf2dc33f847bf07a6ccee4a92169eb3e1ee0, dad1b5790608300b8764dabe1b24008a7ed5e4aeb335bd5aeccc17e109306c95, da5034d5a8dad2e50cbe31b8ada9fc92ea3a6fd5a1d01334252ee1b9c2692832, d9e41e3a72fdbd630edc08af015e3bb2a664a1cc15b9f2b8e16d7097f9c96b77, d9c9bcfee1a579a5584698ee1c0d82ee9a8fc3054db1c3a65295483f4444f32a, d5bafe54f73dc17c3f5b8f2d09252c7f99e7e4c36cdc5bb55457c18cac079d3d, d5b37b2d69dab0a5d4b943abbe6b009bc9ed2f4ff2c05b57f3503b115bf240ed, d3a5007efc6a7540edad60d47058bd6b60a65c345885644546cffc3f2adc74f2, d35d5fcd188b0e403004c9756070530fd6fca18dfca76ce761bc3263017c38f8, d2f4c971cbb7e653d8054b8bf92a916ddd39ff3ba9c7c109215dac141fa1fd24, d2ebd9381ab0cd64b287e26463c180cc590a97e27428bece72df796dca33e896, d11391b6a1d254a9a477c4b48abd220145fdcb8453ae3f109185bd75a703d257, d0f02de7dbfa809c2f8c463a902817a9fdb6ae323f10d783b363565af60e7741, d05627c477d97d455fbbe832b4282a39e5ba8d2a957713c77378b788b0b4cddd, d00134b8ed2da80191cfe27ac3006a6864b96b6d86c667d56d6b4b36e7e9ca2b,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	cf83d9f9f55bd1cb5f571d9ea6900879029097f0e2aab4e4d50cda9de5b471fb, ce92aa8e8ee8854d47ac0c1adb8efb73fc2218c1e094855157e33018861b25e7, ce3452deb930a9972ba75df850af882617cb668286ab387e8718cd95d1052b1f, cc83a6144f3619a652a3c215ba566637aced184cbc5d8f6e528486725fd54f25, cbe9b54de250fe79624ae342d030fa13999e3aa019f1b12a2675fd3a9f2eb644, cb8e23bfa8a1178b7aaae57b1e76b216e4d93ff7bb9aa13b3c5ea7688d363878, cac18898d6185b349e3f5ae76fd0012098cf8aeafaf7f5aac3091f0555429966, c88191480451fe9ab7ff1b65243f5f14637a584646d5fb302646d50fdfaf5659, c81ef921513f3e39cffd9cb2a4d24aed816b52c44a1fed3ffad746f9061e3862, c4d494fcdd3e85b0c8507430b1b09e81185bc60de2922718b229aaac7de829d4, c42253745b945ed0ef3dba8a6fbf88abb80982d5c84cf18a8cef1778a0b01062, c3b6ad575ff07cac79151a7180671db8470d456f72e18b1b029592cc0975ec8d, c24e63117dc25d2ccf2efb4fdbf43b37ed82a238377062fb0d92417aaa103be7, c01048c9065eccae8c66fb8973f18ec6ce5aec8fbeacc6541d557c9d69147a36, bfedc08b3b5e819e9a4c43d7bcd80eb3c64ac0d6e6e272dd549931c9269d41b6, bfc2edab849faddf92c2b1f9d0b07f19224af9a5f4fdc598b5225bbdf8626c8a, bf347a490e4a725d5022d369f013ec3b092a09a23e69182cc9f4d6577cd054f7, bda2bb03d04dced72e990cb75046c8bca094b3493b8b401fb64c368c09378d19, bce6706d90bf6f28a25098f3da19ae834d1b987b22232573cd6e9cac2be1acc4, bb9ac991f7fe4d46c66a6aa99e9e9892dc9598cd77d124e57f4f8211f81442e1, bb10fe298daa4eaeb5c40e35aa32a599b9f03a21999c9748c94ff526f3f3d60e, ba451fbe6f75bfc7b159b4d6976f88d3710757ae31899196b64b721372f8a703, b9e85336b1241a4dc3229883baf954b46465b6888ce8565fec630148568d28dd,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	b9016e0424d69e035990a457b3ea6d1504c636686b261050ee192867e179e6ae, b83794d18978042fdf453aa0c0a87ed5648e384dc24ea053821bd2babc3f1f25, b792eaa20a51d86cb2b669e99c8ffb612fd1100869553fcf70af616cb2008605, b7693a98a1acb35d5aacf31f4ee1eedab48f03fc2ac5bd05ea7ba72b5e5465a3, b65d55b1b6ee5cc031bfcba21a1b434b5c6ebbe466e00f9a815aa67fec3210a8, b450a40cdf9cdb5675510871f34089e57a7d38da2982c8a7d3defc80902f84ce, b38b435374130c93e301dd8a5a14c35d2cd49761e47cc9f5b10876c47430d5c8, b24e71b4c2e370dad40b329a80cf9affbad4e0e4e8ce32bbb8eb02ac4d95637a, b0e8c24fe365b4798c870426f786843793ac24bc58f3fb9d1cf092ecf3685a0d, b053e614ef22d328ebeb2d5e2b521269d09dbe4cee7f75f7b77e282aaf30b3d9, b0343be14f4800c75585b1f862dcfb782db6bab6f87e9043baf77dd57159dee8, afd65701770caf5c3a573d56a59bf8818135a019f7af1f2aac97705f302a8626, afaf60c0ce17978c52bc471ba740beb3221ef1d64604a25ab9590399aaef61f5, af5c3c64fc7c023e3b8f5f4858fb74b8c6a81d594232f6e4d556b8fddafa8a15, af33428d578d1246c9a78624bdb2618834a562dade0b0b01d6caa1cab690bb8d, af2cd4e518ac90d6ef38d4ca2a7a7c7cc25e4a0343c4f2319e00190e98fee9ee, adf76f5e5c71ab96a18bb2d135f272954b1a1042442b98e6acbbd9917698c10e, adc48214b3829702f4e4dbe56a403c37ddd7c28607169c77120fec93b35ad3b0, ad8a87787fe3f2d4a1e6c6d31e73af1661737b88b24729b2baaa344203c7d26c, ab53aaa1756c973bd9e6e1496c40b1efba6314d8a3125e08378118f85fe3ca22, aa230c78cc89f34e9656ac04a91daa0e50c0969694e7d054efe68076ca6c542c, a917b3efe5aa4f4f34a6031765d0466d50e964092d095cb410521184e9c634fa, a8f49b1bbca938386582984e71d54c06f2c6ebecdabbe5ae9477b99fd314392d,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	a8bce520fe1da19bd4f0238a90807abd3ab2611dfe69840fce9fce92df1872b5, a81b937b7993e69094841fb01dfe3948efbe153c055e4291a89cf21ba44d901a, a767ca11d31388a0780ac60249f1065655876a1261c646c45c2368e6a381d800, a70583d710649ea5d21e8e437ffa632dd06935f58a34c57865106e0f79014847, a56362834603dc4de009eb959322427009004a15fed1229e980fb80681a5caa1, a5563cf63c7b735bdf4848a44f3ad866e001e9650a1ffb95ce859eb5c6b8b074, a470e931417cf65862ea1bdad5197df76abf68b4cf5f5822caf93c966efd5cec, a3bc410a91a7fc9f4bd3fb2437c70254c58fa65ca314ab6e3c3dbc67983adb0b, a39f72f901a79c81e4982005f061088957ad5103162f22a4d6ec9b347771aeaf, a29140c9ea0867110ac95b37883afe9f2b583f01d315349ca32df171b7c0d640, a203759e25498c084c8c77528060f0822297ef4c19bde1807af01890e085aea7, a17dc0336a1d9469765f7645cd8be005f6fb14753c098bb2376cceb832cf0beb, a144bedd15387bde8bb74f3122bf482c39c043d4745f1480fc2f492f4009ff70, a09ae44ed4a4cb622e8faecd36606d6b862e6c5d989779bfd5adbeaed8553e9c, a0319e90049271a8d48817f550811719b93f58402b4836a0a0254223ef1a457f, 9fa8bb5c922c66b4ccbac205d59823eda690f6f4968d407127861f4458c8cd5c, 9ed34049a73074015b2a401db2654184e252bc30619bef8d12e83e49657fa948, 9ddadbdbe00cb6f2e9d9e9c12f5b1829d7eafa18fb957c7bc75e5f3d0814c4f7, 9dd6aa069ef4447ab1c0fb7fb5f822d0129d12472a0e180e92cca92c5e8c360a, 9c5bcd146dd98ca118d1e4f072ede51039eab837d67c8890bb35fc005b53047d, 9c28d5f28d9795682d8124bfb8fa775fec6cab075badfcaf9d6b81af12d1335b, 9adb1171f314855689a7a38731de0f4f2fdc8be12ed6b814e45709ce9d28b2f1, 9a2bc2ac05066697ccb42fe2c33f85ba26bed0917d45125ec6deac41358ab1f0,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	96b0f5f46b12b6bec89349fd57d2e8525ffc5277657e0609c7f793da98af2d7e, 95e223b41143bd1e3321909c9c67176e1560895a910b5d0d2747d8b910d0b5a7, 95d9c2ba565a12b8c13c5ecb013bcd4d6fdda1262afa4df2cbf82952fa306987, 9386d192bedf26265143b8f99485c4bef25f043d82cf4d6660c766aa6db6026f, 931baece3c6039cc3a615956040cf1872fa7e0041b07e97f47e99ab4fade3b1a, 92f6335513ca65ec7a918a02ee9f2ca7bf0f0410997f0c39700d9b02c3b6049e, 9260c2e0cf723242e27c75c5345e5a0857e9ec003a4947680ca90f45317422f4, 920cac3f709f26566b6997e14b9401e7f812eeaad1baf986aa6c6dd7f6b5b15e, 8ee3cb99f6043e353b12e47ff65bc86028b113f7c5b89ea341c89e0ba5dfdc5e, 8ebdb02ac508735928625411f63ea7be1f252114298b9c6cf5932b3bdf8ba4d8, 8e76c6e2e7073d09356d3e8a90ce15b761a6b2c064faca06cf0988ea8b7fc802, 8e2c5f1516056acec5567b784c4a8b4ecb4456161588cd0e9c91fa5f5a1aaa25, 8d5cad3c0a5c909c9956392d06717ea7656e33479a6704a5d5b022db259871cb, 8cd478eaf5d21fc7ba88997a35e0a46a6773a7515c6a8aa5cd22b72fb9f9996d, 8cd3d44573a2b7e6a062de8df72441e35fab1f01a2de8e3b3695ec9358788e79, 8b0257e850a0674eed33440aef92e79d5b6e3d08e112708a4b4a2d4487daef40, 8940f27fcf2924f7d192ebad5710b502ce3a0c737bedbf1406f078026fb142c2, 877f80ea5733d99bcbb123327eee725fb88c931da7c9f73d7b7b331c5d7e5648, 859258cbcdd1209b0c96141bc3e4836d41d8312300798a5a4376f26de140b956, 84fb68f5a66cc56592de346757e33d4c6241b643d00689cdc0c63c27114df4b0, 83b43d77c3864b94163067ae5bacef6525f6265f8542cdf3d9d6b1ad5fd5d6db, 82d044378235074ffbbbb569de5238d09ef57c919b05982a2f596eb2215cf02f, 7f7b919dce87ec1e13e6210c5d0a8593e85fc24e099f8dab8fbf3090684b3f56,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	7f75430c44b964821e39c6761648eccc2da8a70889d82520d972467f4d352456, 7ef3c16df46c2826d7cfac5a84514c317884c349dd0a40c25305c465256a9196, 7bc4baa8314ba6649c4f44fdefc056d948fb3750b58a779581fbc387bdbe3a5a, 7aa9d03388045c0f31bea1dbecf8aad6de0702c33c0f192c4f5c28b160033b86, 79be03dee948545ce1733ca6c10390b7b84d8e9373a4a80149f07843b7ed0a35, 793945a2e27e1293e2cadb5e63b3e4c8f87dcb152699bad3c0c6fd9b41533ca8, 7906026b7ab2ba37f4735336f39b3c3bf7a67852331993c0d26cba5ce0d3042f, 780669cfc84e5271e4db6dd827e25aabe0b80cc705e99a101717e74c42627ce2, 7763452a185a0cca4101f140267c360409a24d80a64e599b2eed0dc3383c40af, 7697161fcc0c1bfe8ddb1911bf32b8adf6404fc96b8c30606473ebfe67c27aa5, 75345ab59320b45395eb28ecb987f1eff96badc4f4d28e9f1172e6ed9984f5ea, 74d31be042672b564c8f8a2c6d143ec2ae966e2f3457687f60ab0105cc1ef835, 74cfb6aa244e79ce9492b30b1f44f8bf78637c5f06be4c256768452395896db6, 74468aa16537c716b6e3cdd481b12004e18354a663876d16da431c3555589aee, 743a597c1bf22649896f72a5f94979071de235929085d527ee8271ed570e3eda, 7434e13d4642bdf24687d145f34c4c744570c5af19b71d97dd895c5be64e9be6, 742981da5d5c9934d1abae0d962794ccd7a396891e73d2d366d45b4ac5ebf881, 73be1517ce7b0b01ed6fcbad483b9842bf297aaf2988dd8e09c48cafb21354f2, 7391e33589f7531104fd3c7be5ce8e78ff32e59a41ee64c69c7515fe3358d18c, 6f61d01c6578eaf1d8c9aa0325f98a13d8e1bf291d9269c0c48cb00f0688cb9a, 6e27f6a40e94628ae1c64e2c8e674fbf1ee1441fff15002f6bd89d75d3b76e14, 6d5cd9cc6fe81f1995720e07ea8ae0a29320779b1788c865bfc229cbf263f963, 6d3122e14566370327c09cc3a64e8c5479eec26ceff372a3ae50a0cecb2385e8,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	6c1d2b965e1f6f8fe6c9e139664c5a61b56e7c57104450811d1100612d1bc23f, 6be415f3d774e76002c41275f15a334b6259e156244dcb673afff2a1c3155290, 6af8412ee3591045e97d8edc1ef8cb8e05a4bd026c9dedf08f508329d2cd275a, 68b4304c0bdaad8201515a7d1cf5eda2418344c0b67a3e4b258fc2d762ed5e09, 6878d216076606d3347fe1dbabca05b54fb6b61538c8e8f2ddb07f2c71a093a5, 678ea8ac8a616be02b7ecff7f28bcf77bd47dac9c51d2100f0d67debb49207eb, 66c424824ff9701fce476762098bb225224bb12f00f4faca822e2683e2817c2c, 6683ecc41e53221065513015a298bee810042b806cd39129a9384a1a243bed83, 667a7f942ffbb83be38766dd5390b7941e509b382d315b40ada50847aa51420a, 663aaedc2a446353b9d44e9acb47b1f77b864f1d303fd81a884ea13ba77bd2ec, 64f9efb81c175257251e257bd3ce866b3ca225eae74ed7a64ff20a5460a607d6, 610889a30d97c29d408dba053e392ea006cfe6e6a1c401933116346360df4e15, 6017379065c6d9b36dbf8cf2da01a2ca8340693b8f19b4c11d937a0179a63561, 5fe6778d75a76642cf54a009561ca23cdaa558255968ebe0880db8422245add1, 5ddbe11f7b67136af0fd62c2e9105cc07f3acc4854f35704d9e922d2de2ad384, 5be19d5dea37bf85e4b7a7110102ad39463d1586bac8fc815b4b0ab46eb68c6f, 5bca1ca46380106560414f794545f9e48348edd05cb8ac687cf27d764cffc6fc, 5bbbd83ea6a811e6ab65b45cf25edaff4e35aeb4a2992be9aff13bfe925c9cbc, 5ac78b09dd38e9fa32e2dca3217ea46450850464929075c98cbcf73b63bdd093, 590aa3d6c9b4cf88a8e606d6007c310190963c10fa03c12872e9d9108e921a87, 58eae06ab7e785f07373b0eb84b912347e969fc05ab78b00b6e49eac1e75eb43, 580f5ad561055be312a489ec1b25d4b8777e392187b0f2c67d1c2519e56cd51a, 57934ea7affdd9825c5b7ed21ec5a630e79cb00bdc34191e4aca4f6a3a00798a,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	55e0071730f48e0c4fa6f8d36dd55d6edb8231ea818a1ccf656015d93c940480, 55532e7529d225b688f29bbed13c8d8af5cd8115e82328c5213be40509c2a2a5, 54bee71bed4653cf36db9d2b74bdf21fc36924b1f676bec967b5a468341652af, 54a53069771efc780e1d7557f24c116f039588cc6ea54b8d7aec06f2456f407d, 5423c7ad6fabe5dc62a9250039a64f60711281f7b9776a675c43a50f62d21c02, 53306aced93b3789b5baf03a1e5d364b2777d2ad8849ee907d5344053a750f01, 530cbfdd0585f8a6e773a340dc8fc2761bc527d964b25fda5985ecc30b31172f, 5181039ff53f195a14b8193bc8879190512705c0de1fbeb26a0bbac23dc3bbc0, 514972453ef9dc059add5fd8fa4d2e5f293924ef1255918ef2253b67e229a1d2, 50d19553ce3092ee217451d0a3c174137b0a5c351cb3248973515b2cffbc2e2b, 4d8b94c894d473bc65e5afed24264e15cceecd81d8b07b8542ea5962af5a352c, 4d81c804d9dc7c1daed6626d98a81dea09892bd0f392fa1cae970d8e6aaba554, 4c226ca0d165545767131c30ac0aeb511d66019a0990d227dd7aa70c1f2c3324, 4bbab4461e3ffcdcd035c0bd13e3e53417221fdd22c47209a8d53eca104b13c4, 4b677aa4d48046bf539c985ce5e8d617d556059a3207bf3fe16f067535aafc48, 4a8189ab15f4fb4d8b507f483ae694aa1f866b4341bf9cc0c5d1eb09ea0dc5e2, 4a4598daf841035c7b729d4e4563d80d49a146db21cf8942ee279d1d68a82cbe, 49f56b8936b521c48d63d86a8275aac0cd411d4b48d867f4fe1d337f9ef4b1a6, 49725de88a7c45759581226304c1ebfa326c1bf92faca8e7bf46b29bd75f0da2, 4941977ec3177221cee1ea76995674695f116db9579f2435125159538072c7a7, 48f5f14263ddf276109dd65250d332ae6ad052854f4a72949144604880147f45, 47a25cec4ff0e19a643cce916a546a51ec57f76e8de8fe52661bb56894a84842, 46afd08ef4564bb7f4e2a61ff95003f485260a05733ee032b4dcc33d74ce926b,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	4673d0c47e9a73582ef27dc3b7d3b1b1ff6cba53ea245d2f69e7960502b89304, 45d44d4817a51b97aa24cee96f7dc287d1b66790243454e5ecec16ad297eadbc, 45091fce0cfbb124fdf1380876e5c15699df35a5d3d7804560500fbe7adc574f, 448a6529d7dd07aa8a6073897a39d7d96b2d69a9dbb8ef3d2729b7558c02bd3c, 4402195d27c944d4e85a1fe0abc140e359aeb072d7ab8e2c404d6773c4c2da32, 4339a0846be069f767685bd715a1d0e9d8237b85c23c544cdea153752b9d68d7, 42f91e85c5455738328206a3db07749715e3f32c099c7a0aafa8c2f3a6eeee38, 42113cfd76dc6ce3cbce371a01350f8cd108cfbe091374583fa26d7681f10a67, 41ceee9389e76a985617d8207f9079dd772b5837b6603a50c873978316969724, 41ca167bdbe6a0d9bf095e377a0f267c70d38220f9f1850238c6f62ec8dbb455, 3fec661b5d5db34fc55e41ec988511b84c7fb02248a419b56eec6652d3de1afd, 3eaf76e4c615088db086584ce37a42175623c4870789d36bb312d334b479e188, 3d98eea8be0266f0b7a061af4b02023d0b9e9c8c68fcf04b4c7c0143942b8330, 3cf561d7d28482aa706e0f09df3e0cae6e2f3b72d4aeeeff137780d1819ac5a1, 3bf0d59b9272ea9fdc0cd18f77bde8ca6efde2ab968c637841b4f59bde0b17f0, 3b94c2396fe7702db920b31eed93e6aa81a7c99ccee33f77bb78dedae320e72b, 3b94a080ebefba440f507cb2e6795aa451cd73570a6116a23de1b813b249296c, 380382cfc8f302294fdd806cba715149548026781db866539f2efcd72046f317, 3736d2dcdfd021fb5e6e1a4c527a7468b045e6cdb1f8fe5547b9e332426b80bb, 371222c41f87e6546ee10dbb34be7eab08f1a68a3de857bb1b5f28543e835d63, 351892dba00cd338ccb2b403442abc5fa89a61bb9c4e566137fd33a3f6570988, 342c80bbe3780c002a26ad0c56092e98dca0691f3d28fd4f568d3866997c9869, 31adc1bbf10b7d7c6295837cc9ccfb20cdd0ab5755d570b24e4b5ee078b704c9,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	317e73c447b5f3b4b0fdaff58122b35b0cb4433a9ccd89aee3eab8a1255b3c6e, 30d06e55c4cd9a877e567b7358f14e7fe9cf9e09bfdf6c1bde90320e31fb5bb9, 30a28b00785f89e379cb0b1eac98f18663af618b42485fa7740a3ea3acb3a9ae, 2f7b9edd8d10b438b6a807869fc16accfdc5043b1dbf0cc48a49df3c5dfee3ce, 2c74a1fc5d8c05d7751fa0d405ecb7f7a065e07bce35eb6906521decdbadace4, 2c1820576d8170eb2153300a6566e2ce61c5d9a8eec55d114f56bec49057386f, 2c027b0fadc8f6b42eecb49c37ef3ad45b35a7368e9560bc31bc0f6bc417eddc, 27e5615e928a07b2e35ad6d63795b5f8189af6f2130d5f69e9229b32059f1ee7, 27564b732c52a37b66af2609c2d1c943288f57683c64c82ff1bc066f88b34f34, 273866490a6ab7ae49601613caab7af9e53e62c880dd0a9cf2f0f31da9feca96, 2611a1c953e494b507e72371064c8a8a1a9f169c27043e8995f058f1c0d4f012, 25e87ce18542710125c3f158a762312e43404520e199e8fc47ba3aa1b40f71c9, 243cfd323e4d5f25b981841fd6c307fc02f405b68faa0b8e5d7395de01f3e856, 241541a1c8cb2ebf1b14e191ad1a13bd6ec85829d78e138fa11960334b746c2b, 20567b83523751ac0788fbed7cba1c694d4b52649beaff584b9f16afc764e875, 1f1e0c851dd748276586a628fb70fe33a23c09227696c3ee0e170c657f20c773, 1ed7b76e6fcc6deb6e34c3beb31e271924225b250a3f7aa6d5aa82f94dd4531e, 1e0956bcb231114e80eee9c52bd48ee9f3ea19229a82de1e1182bfb0ac613de6, 1c8920973cfa14fafcc7d97a3cb5a43d8e713a0f50faa2738be7c61af21a4832, 1b123cd6be4305682aa31e286a6614beeb3704a58af90983f336a87016a236d1, 1a814c66444f11b4872ac0c337a1f65204b294c3d14b27ae85fc351f23a8f397, 19f2d5f8d12fd40b1d76babf7cf7732f6edeb886774fec3feada4e931a01c80f, 18c838e58692a2a16c0a775d0c7a3f602974f1625c2fb6f4c549b943697cc06c,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	180005e1e6797c79fd6290bb11bc1f40b34c822a18654ca85e1ba74d96834059, 16fdf2e67d09240a26540d00658f7ca895d4bd899620f1e8f05da2bf2e35d614, 14e519558a6b06a283d670c3714aa54a01c8f35cdf47b2d567ccaff9cdb872a9, 14a1bae6bcd0ab3128a5b78b432fc855cced7df0205cd4d137ea80c8f61efcf8, 147a2f1250cf77932d2b2b099ae3680d79c1c659022200d536e8cdb13687a3d2, 13dc3cf913f40404eb0a6c89f6ed10559960924e1299fd2982da8c85dd43f6bb, 125a8c001a068036585c31885e362a751fddb8d9f570b3b01c8a4176351270ef, 11e3c5cc49b00d25641be96f837cb3a440be07a9030755903f0e4c0002bc8290, 0f7f3400b1b951e10acf5590d5ac9e1a85eda1e72fe2b4dd041a99c4b14d1c9b, 0f72daf30f593f4aff633453fbf7adf4eb6715578069f0bc126929a7f987f0d6, 0f51ac9d4f1a244b2fe68aa7a6205f20974d46fc075dd29d0c99ba4f84448e7f, 0e8697af2fe695e9cd8c2de149d37720a160703becb991e2b9c697ce4b7a0f0d, 0db594e6ab9a3712df9b739abf3c5b0f9107e72c95907af5870f15ec8501e7d4, 0c42ad1d178b241d497e2eefe7472c604af6a439971f358209cbd828116ee759, 0c18d65acaa18942b8d8f2a543afd3e6acc6326c600c699e0c699b2574cb9835, 0bb95a479871eb067b8dd782a2e2c099f8aec1070642fad21a728469a59a2c2b, 0b2d9d4edc773a8bbd4a4d908858383fc76b32a494894081d10c91d022b0957e, 09290d70fedb87a60828b05ff5c83c368bbd8eaba15153ee7952dabc2ef2bab7, 08851f21919f814520d4a2847783815657a7120bc6533fd5f702f84949a27522, 077c579784ea2965d5bf2c930f698d86a97e8c24a06889c5a418da3f4ef704af, 07320727c0bb45b54f4d50e128378f7eda3d9069936d2a2de5599b63d0bdf2c9, 01fdcaea7aeb248b39306c208e99591d6210f3c0a0735e9bbf007f1525e92ad1, 017222f47ad94cb527031f4ceb06ae77607b1ebd11dc0b83b6eb17da531a267d,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	00a710722e0b1aea3d2b8b0221567b39222ba1f810ee716eaf1036193552c19c, 009c73597f79472eba2715fc634bd78bd2bc9a21e05b7b4cfcb64a3beb5fe03a
BadSpace	IPv4	80[.]66[.]88[.]146, 185[.]49[.]69[.]41
	SHA256	6a195e6111c9a4b8c874d51937b53cd5b4b78efc32f7bb255012d05087586d8f, 2a5a12cc4ef2f0f527cc072243aa27d3e95e48402ef674e92c6709dc03a0836a, 2a4451ef47b1f4b971539fb6916f7954f80a6735cf75333fa9d19b169c31de2e, 9bc4c44b24f4ba71a1c7f5dd1c8135544218235ae58efa81898e55515938da6a, 475edfbb2b03182ef7c42c1bc2cc4179b3060d882827029a6e67c045a0c1149b, 676cbcaa74ee8e43abaf0a2767c7559a8f4a7c6720ecc5ae53101a16a3219b9a, 770cafb3fe795c2f13eb44f0a6073b8fe4fb3ee08240b3243c747444592d85ff, 84519a45da0535087202b576391d1952a4cc81213f0e470db65f1817b65ee9d7, a5f16fa960fe0461e2009bd748bc9057ef5cd31f05f48b12cfd7790fa741a24e, a725883bd1c39e48ab60b2c26b5692f7334a3e4544927057a9ffbdabfeedf432, ad2333e1403e3d8f5d9bd89d7178e85523fa7445e0a05b57fd9bc35547ec0d98, ba4c8be6a1eb92d79df396eea8658b778f4bc0f010da48e1d26e3fc55d83e9c7, b6ac7f6e3b03acd364123a07b2122d943c4111ac4786bb188d94eae0e5b22c02, bb74c6fc0323956dd140988372c412f8b32735fb0ed1ad416e367d29c06af9cc, c437e5caa4f644024014d40e62a5436c59046efc76c666ea3f83ab61df615314, ccde1ded028948f5cd3277d2d4af6b22fa33f53abde84ea2aa01f1872fad1d13
Noodle RAT	SHA256	c49371cd8dd33f725a780ea179e6281f5cb7f42e84a00836c8fe3350b7b9b2d0, a8db92a8f34caa5084a3fdb8a683a1854bff84612dfd25a965bc12a454a38556, 678edc2ea9473b02a13e9fc7557f6c7172f0f00f4237e2da91a6766c53db1d3d,

Attack Name	TYPE	VALUE
Noodle RAT	SHA256	275d63587f3ac511d7cca5ff85af2914e74d8b68edd5a7a8a1609426d5b7f6a9, 5cda94180b245de8421f226eb516d0aa1d3fd8167ebed4fa06070dd38344cec0, 61f34459815eb403ec841246a4277d825dcd25700baad867b61ec3166d034825, 67e60fca3d28dcae09b74ffd62f5efe462700b6d2b3334d519e4caac55820df0, 3bff2c5bfc24fc99d925126ec6beb95d395a85bc736a395aaf4719c301cbbfd4, 88b4904a582522d9a91fb4ad616adbd432c556b17427cfb177c8205f484792ba, bf5ea570bf4d18e60dd758a2461fbdf73a500dbd179e458aca81d65b5d9155e1, 7440a7b56d3670d4204a57974fa76ae76ca78168bb181640f565976d192cc159, 1e9add97a289de7f5679aceace7a3a39437a33254ac9c217d9a530e9369f60be, cac63e105d73d59c7f83779005ada0a4d3f7fb072cfc2c9590b64fe3896d2e3e, 5b4c421edb3571dbc7d581596a9ac952e453394b30132dec8e390ec561cd4abb, 3893f8a44a2d1fef45354984f3c6906ae8627c6f0c489f6f14e8da03197312ae, 0153c9e22428f08597fe87cb8bd6664f6481e05bbf4e3d4174f44d2524446bdb, c4fb9757ed6db6ab2bd4253cb8a1542a590443654260f2b947c288d5717487d6, 70b19172b743973a45f5d707d4eec4f8508d41aa684516f1fb8c75bec59d02bb, 96231be4cc6cf256eebd828af4338588272ea478c609a7f16a03bdf1a61dd431, bf553e82119e2483d36eff51cf152861938c584749ebc005d4d612876277b787, 7b07b722091d9658fe106448b6e1c6b7484d7b7d163ddeb19132174973b62759, b21f4039707eb4fc40ad1a7ed10be753ab3922c4a60bde819dcd74d44fef991d, 4c4d51b377faebf61f95663765e622eb652866ab9cc7e9964a5d02f4dc0b53d3, b24e160843d96c6d75452d6f4e379b73a417fc821b26ca85d740ca0a499615ab, e5fb5a3b8663fbb2686caf88fdb3362115dc0f0bf9cc5d32d1e42c00aa6660b4, d17d964cacb063a6fe685d6e5e7dbc02c597de51b46c994f0aadb56c3bf96f13,

Attack Name	TYPE	VALUE
Noodle RAT	SHA256	ba45dfa8e6b86140e526959c8568824ddd743d418231440d48740e76a33610ea, 1c2bbab6c496b66b108dc810649c19319655a2246f7fc6cf2a0911f5d73f2f3a, 14f9a20356fc0e1806524057e8366d994831e3568cf438694a5c4d5463c25010, 7e7bfe7e83867defa9280c8bce98cabcd0e6410cac7cc9a1baa88131b4a263b1, 45b3d192ed79541a9711c16c7d73bd4d0a74598ecb7b56416f8754fb5d6feb56, 53cebf50348e4507e92d23cfe3bbc87d6bf50e06962462d036542c37a50a23c1, a27d133f6a1bd72285f021403082dc8e47180fe56e88b274f474459088857603, 4198efb00840f440d96987518bd80dbc90cde3023bc8c2b0aae456af07875405, abdbbc10467421b93fe1df6da0de70a4d454adcced1bfc6c1cebf1207fba93db, bcac1d42c39932fb20f571655cd1bbe507c3fddda63d4f0ea8986a3dd5265f41, 68389b48c6f15b6da7f2d78c0864d6b9b9135f6ace3564d29b26f5dc9b5d6313, bf1b88385aebb37182421e967749f057fbefb4e4386bb47b5098abac7c70c476, 1a9ff06ac18f57a6382fdae54bf8735a6ad7d9c9f1f9aa0dfff0e3e828f1820b, 15f3536ac33588444cf6a632f17c74ee0ee8777d0d2166206222b4d5f66de715, ca2200ef6ce1abc37e5778b40e9b14031b81014560dae9c6a16fd7ba948c7656, bbcfc826f614433ff1b7c8031349cf5b411d868b07259eca9c19cd5af772b85e, 6933a01980378c2160740e5cecaba29530555e3d65bd89ef80db49419a419f8d, 5dac572374cb40561ea5dbc0dfc963d863f08862a0bd33fdac6ac8d0aa180ada, 24a827336a1f942925fd57e763109e3a83b1a5762c077c1e80bd057bb1b15bad
Fickle Stealer	SHA256	e9bc44cf548a70e7285499209973faf44b7374dece1413dfcdc03bf25a6c599c, a641d10798be5224c8c32dfaab0dd353cd7bb06a2d57d9630e13fb1975d03a53, 9ce52929765433ff8bf905764d7b83c4c3fcbefb4f12eabcf16ee3dddcd3759d, b7bdb0cc90b11c4738c2af218a1a53e4c65b6c91c6067c224164b8fcfc3eed8c,

Attack Name	TYPE	VALUE
Fickle Stealer	SHA256	f878a88b7dda1155fe939abe0500e32d5fba34569ca933bccb5603d9e0e96cc0, bfe2d817e20ecff45cc92b7b8f4e1cd0482b48a769940402eaa5b31c bfb9b908, 09b47fd0e1fcab827d1a723f9db7e402502ec91e57b7217ed85094abd98bc637, 978400108aa16e464b1fbc300bc270bc89193e3c3890d5e9373b3034b592b4da, e394f96ee040508063606343b1ad2158e266dcbd8beb3ba4a23936d1957e5ad6
VirtualPita	MD5	9ef5266a9fdd25474227c3e33b8e6d77, a7cd7b61d13256f5478feb28ab34be72, cd3e9e4df7e607f4fe83873b9d1142e3, 62bed88bd426f91ddbbbcfcd8508ed6a, 8e80b40b1298f022c7f3a96599806c43, c9f2476bf8db102fea7310abadeb9e01, 2c28ec2d541f555b2838099ca849f965, 2bade2a5ec166d3a226761f78711ce2f, 969d7f092ed05c72f27eef5f2c8158d6
VirtualPie	MD5	2716c60c28cf7f7568f55ac33313468b, 61ab3f6401d60ec36cd3ac980a8deb75, Bd6e38b6ff85ab02c1a4325e8af29ce4
VirtualGate	MD5	3c7316012cba3bbfa8a95d7277cda873
MOPSLED	MD5	89339821cdf6e9297000f3e6949f0404, c870ea6a598c12218e6ac36d791032b5
RIFLESPINE	MD5	fd3834d566a993c549a13a52d843a4e1, 4282de95cc54829d7ac275e436e33b78, c9c00c627015bd78fda22fa28fd11cd7, 047ac6aebe0fe80f9f09c5c548233407
SugarGh0st	Domains	account[.]drive-google-com[.]tk, account[.]gommask[.]online
	SHA256	8a563b3091b56eb0562f5442c90b4d28d4be2946a3dc4a225b4b96134f7e447b, d6bffa45aa2448b2fb584713395b742e02ef77c1d54f125cd501240e0dd91a13, 951a54d2c61c3257447c4ff5fd451ee581c76d3d4d88fa482b99f5410d7b7b6f, 8db5a7efe1a83e43cb4acdc596b0413b4beb54f9f8e13f978c07a6eeee6b8435, 31b7e97770ffe74dad914a37a78c8f9a7286c75b62b5fae1c4ec722837ad457e, e56537d09156bb77f4821d5ce005c7840ec41890de233d88a1152f68110098cf,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	06056f83e93849124dc435166c1b463bf34bbf99ea5671221ddaf6641e3db4f4, 81ded17e368abc280db4d9f83fb0aebe1ec58eb7e4103f98f0fb5269c8696551, 8190e8990bb7bc860691ce2d3ff6015d7f9a0339e77aa7c6e5e3ae5209bd6f4c, 727bcb28eb0282a389bd2c82e3fac57a9c348aedee23d18c8d136bbd8803b642, 0b6dcf9ba14096c631bd9a3f90180c5f6ad9177a828372414642 5b2f08b53e02, 653c3ea0ce07880ffe3a2acd735770cc2cbedb137cb5a29d4b059af5a569f98f, 2547f1a874c552da17abf6d5f88e626ed4bda71ca0bb39b2bc13b2d748a05409, 4b1f3cc69e905137263ec8c39bbdcbccd5e33c3abffe54d77de847a998fcf17a, 48cc1d2df6ea2a04201e74ce59983a0bf0964d59a0e5c5647068b653a0ec66d5, 05758a568e30b3f35092b8d43bf4f29a3e5e9b988dc541d51fc8233ebbec2874, a22e16fad2d88de1a625201408b2262d8335bef3d944f4f696ad825973af124d, 7684296728c10249f671cf80b58e04633031e1b74a88e8b4f7d31776fc643d10, 375e0b117c7e45266e9544c23e226dd791ac32d094e60b858ff823577be43acb, 944cd95eaf496ad6dd8859032c4577ad6917dec3a4c300eeca762e08a97243f5, 6b327a15877528e5e5b0891fd587cb2fc932d94404c756401af628195eb94831, 8cd0026ba4f0c8984bdb6daaddb6fa17088e3b9272859cc2c03195d36f47f334, 06ac9bcbc1d026fbe9a261afe62a1b5704dc64b89a28dae47441fa6ef6230eb9, 2432f192511fb377d69619fc7eb0612570e22e3ba88fc42e841552a66fe2dc8f, 53e7e7fce0d8fde3be0d6679193f924555df217b696f6dc201e1966e9f4efabd, ac5342050b0ec85a122846510e06f861960c45613ecc05e3951c57d7d02aa716, 21cf0efec4def4a95af75a7bfdef915bf103a9a6cd03593b4f665f49cdbe4a02, 58754bf9701a39bf13959157db5761d19a562264ac79a8ae47b82589d17a1a07, 5f40142782f5e13334caf25f3038be324b3f47a3ee465f6da4442ec6e7920d5b,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	862f6f60d6c145d99fb01476708c93e72f0b905ee54aba03904e92eaf3d8b2d9, 99ab797804684699925b70bdf2ecbbb878f4a86e7b971349036700c72ad15fb1, 653281c876250878eb503e4377c3f79bdfec31e94b27e5413a1b9f8f0f84a6a4, c8bfebff63e5f227aacb3a0aebcf40c973a4fbde6d37895c76498798e925cfb6, cac8c35fd03cc8698e53cafa64941be59870380ecedd2f4998e110787224241c, 18270dd537c3e2f02513b51c3a89814f4c34aa994aa8d823bc534fa39d95dde2, 4509575df3a0a791838f13405122def4eae7f5d2d8142f4830f6944ecd913f03, 823d23f1bcc76b08773e988be209b4a2f1cf99b094732cde395bc40f0729948e, 70359e4ce398ad356fd36f1f9306a570b36c552b83310332e5bf257f21cb1e9a, e2a8ffe20d91720516b242d0053ae58474be4205b9926993eab13e6662cb9a91, 267eec9cd5ff136364e0346d62df0cbb0294e0fb8f672685e785bf3ffddfb76e, 7ccb9b8964391360d6e122343d714301851c2332f0d50e037fe08591bd7c139d, 7caca38b67f9f629912f21bc0d76f8a5782fc62cccb93f53d2d07fd21fd30c33, 66f2712d989950e3b6c1f56a08b2e8689ea8a48bf84c7cee93583c7e78591f3c, b9a60ea9b1ac73e333b403f8471b5111a0ba67b60c9f0d7e44e2e290fccf6f42, 837164909df9b37bc31edcdb1207954337bad59a630b44f8ea06a594bcbe4035, 4cdc33e535d07e6519b1be0520349dedaefcc464734b24d1e656414100680efe, d31b5dd937655c14caff1cca6da88dc81f9cc523e119d43a9ac38dbb302eebbd, 21123d5bf92e763c4ef34fd4f9ddcb1b3a4a2c9ab0fd5657f4f30b0964979274, 75b39e923c69b488ae6981d314075f7e423ba2236150c20d41112db8f80a4827, 6071f84650b3226f60068f5f7a1dc7c7ec819ab7b6e8dcf34163638b966fda44b0, 510acd67d4c5fb45d6721283ed0eb4128347458ccb2b00feda9787f138c35278, 4f98dc3df220f41bce3c3a2714392279e68dd24a53c7c2f22a0a9850eb5d8476,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	2e2aef8948f5e2d93df7f4412fadc31500feb9035ceff18cce85393c6e230088, c0230704e1ee34666c40b2a3898666ba3929283ad0a86b63ab0fad6f4a0555ec, f7de8e94f280f9b943950a75ae78032c6501261a12650a6f757107bc8df6c3c2, bc73528b391f30acdd3c3a1674bc7973d3026c367142d72684facd68915851f6, e11908adf04627812cfa721189dfa06f884ceedff2dfa3b18578494995561716, 0fcc045db0d07ea4909a487273d313f796fa19ee8095a5272dfc5d6f3484f4ec, bdcc0bc3f5d022f99a1599c7cbed3aa2b6839e1e1d05ed2448dbd8b7ab34c784, 065f10e2a92b433a779c508e4add9c096b2891f5417fa183e58c8b8f7f9f8524, 87bda94d6b5ad0170c07abe540f530e797c6fec7410b30796e265cc21997d735, 401720fa24dc03cce8640b00d00c57676a8369ee49f456bd771a6ecbd81b82b6, 84572497f7022163bbb2e9885c942b1bcfa1793305c116ac898ee1b52ab6f898, 2f32e99c182f0f7cf6ff54d9d1a9d9f7e59823030d2a89e15890c2c8b1612caf, 57e3c92639027738e5a867d2f66d30a9509a96573d7a5eeee1c2a710faf9321c, 7528cf4daa8f0b4108ff220bc98f6046faf446653a3f98edc1d58350490d9fc8, b89ebfdfa9abb0ab618ebf2baf66b6cf27929d1e6599b3cb174c12e0a4c71d96, 6f8ccda88e0ff98c781ad6e027f4294eb54bff27a3ca1cd72aa83e4082013860, 162594cdb38526300af0db4acd13dd7a5a4ac07004bf32f887b6f1492361 60b7, f46b2a57ee2904ded87f6db77ed4373bfd71de12879bd939348ccb8fa8cc1403, a77789f32058b879d7e3831d2d20a885996b8f07694a954e1e717f0483660ccb, 984e8b3dda2c87bc8e3d21a05b07a8f52799c99aa45584aa2671efe62b5184c2, 3f23d9ffc16c5f455f7bd02bf57667efb3d0a645ffa13fa38e0a6f5022208dd4, 4e18b57c586b3bfb6bd825ecbee2bdfcce91c8414e40c0a7655edc327d62ac0f, f4ffced2a4c7f3e48f2a43e17e58f8feb0ad6cb2ad98fafc87d9a159230810fa,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	9483bccb2b0964d11b13ca01fba7ba6a21a531807d48eb3182ceaf7ed240ef2b, 26f92ea9f5eb220d9e544af757c57e5672971b9cd43b166e65c055b6978d6031, 2c8116dce38993762cdb687eab69786b9ccd1bd8c569dee8bef5a226579224bb, 4bcf097c19e18e3b3bfa4c45ebb4e67d565a0984211edf9e2fdc042b43141317, 67b648a7f0d24e5b56e83f73f9494be6a63f4d7372c960a2134054352c9c3490, 9ce558dc6af9c183d15012a5012a36184586e40f8a461a948192c3f055201766, b5953319cb28a0db7a70dff03949f1d98487456a273ac3cfb1f70f8cb3b07c18, e4b8fe0b0a87e5844deee4668d7638acd3ab9ea60a947eb1b32a4bd0691e5411, 7fffe1969dee2b4c72b4c5d0c75e493ecf6f3598a89d8538be3e7c53b898bbff, 6cb99d0073d2e6b7e15b22a74b98901dccb3c328d88f6e1c38b0af0379dd388c, 5a3811aee5156d928b2b634b512d382d89f8203cb883cab743a54cbc4f3f41f1, bfcfa5e291b0c9201344a73c8ef25c2912561e32c48af0ae0d30ad8199ffc8c4, c4a912f776579aa0126bbadd9261a4cd6efb3bcb5f5c7d64e96b11f3bdbc214b, f92c275dfd051481cb03557213195647dd7c68edf9f7beddcff0aadf298f371b, 1b14de17a12cdb92210b8543e3418c16f9fe00db3394fa74ab3a8f1c5904ecf0, c4e2301615cbab9abf2d94327bb7839df64d88fc5c508a2f33c3f0fc881be7c3, 066b3631682f63b4a44ecfa5b6dfb100d8052429a7e1c5b1ba8cab4832529f26, fb76bc19e177372d210bcfe9b1f35fb296b0b7cb64f0ad5075a64d06a3c85159, 2c4356614ddeb8085367167b301a8e437166142e738adb27bf26c09da3acae56, 4b1b7257fd376286501043eb27debc850300a674962068e044a34e697381d694, 0618b63352d0ae02d0f02ce8adf02d1c16fd56b18e903622bc95e520388743e0, 792ca7508ce158e20eff7b838fafb6120afc81b3677a84eb066810544ccf1577, 49fa747eee1bebed9bbb74b7b555f8018fb4e0e11f74349c2f7ac89a225d27f8,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	1b9604b50e8c0c6cf2496855a3c367d72fc447839fab708b20d649cf276f572a, 698c73f004e7f46bc371e0476193456071d9f7df9662cca7aa0e010b4fcedf57, 0986b26fcc87723d73e80c280f1bbc221fdb188ab8666f098caac6d896f1c4d1, 27ace9002f5bc7b3474ec3ec7ac72ed094fa2d29d9b2e8b5b1a787b50afd4f05, e498efd08ced0eccaebc4721cee807858d40fde428fd5ea61ce06272a25282a0, 26dfb13aea6f55e01f4dc54bb91ea7d9afd3bd73bd0c95b63345364ed149ff80, aa58e1b322877ff660961e18558488c49491a523a12373f95c41a1dfe60ad477, 43c40fe84b53b2573564331db15f5fea8cdf599d6c9c2f361dd154a9b78cd6aa, 3df795503a11b3c1a7ce3aeaf72f436ec9d7704c8189f9aa4abbc4f6db69d155, f0f587aa4eac787e4caf5f4b8795b7cc8a4c33fbb518ec2d616516076570f393, bae38315e5a6622d01b66db561efa206e698f3cb6157645dabd4f0267b8d2c91, 5779a2234b0531171625983798997847d56cdcd421cacf0a1860bbe4ba70b79, 35a9c2e8d911c8793a4b464633beaa2c6772601d6d58bf12c456e694a4adcf46, 220dd9d5ba1c6e087c8294eb01b7e0dfeb39b3a9c99567da102df44b2f04dbd7, dd4fc4760401b8dc37b0a823af19d0f7b5c2039704caf5327f8f8c6d00bd148c, d18cf366f549a8828dc02e6540a191b3625da36995806dab559d6b020fe74695, db6a8b9988ab1b83d8c1e6b5bd0a4bbf2baacf1ed84220026f9ae8a867e5eec2, e121a6c8cccecbe1a27c2003c255096f04c23f13b24a1f035775348f2aae53d0, daed820a32723e146e762343d0a32f041d21bd2e603b355b2f91d0bc7d98927c, 41bb112c6d4c609d53111ad1bb7cc687ec8ab848b6039c7a8eb64fee311b0822, 1c1499485254acb0d94ec6b4ffcb0c33d1dc154b5d95cc433a44c8bbb66c718f, f87c6b520253d9d6b14a443ea2096baeb8cf532e9cc8843f39e6168cd873669d, 4f02b04252b268bffdc6584ced29254209fcac4ba7388527efa43786cad17aaa,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	33dc74a86e72a353412da885e5e07fe64b65f1769fe7ef17aa79b6bd6b36d0dc, f7cbe4349d4f95bbf08e1d649490fffe85e345976467bd1e0a066acfd3c2bb35, 88c6525924bf306dc21aada7898084622bf6a224465123025a53b1c187ff8ae9, 3edc38bb3ad101f6e56d99e4c9f173c16346315ec7bb36e3d7f327dbcbdcd606, 502a08fa74475ad5affeaac4a0f9e491df59a20c97796ce88284e79821ac8483, e71d4f329b7353f95f5f13f3fd33c4727f9f06f96083e199c18ad3cf1a2351fa, 6af30df6ee33ee44e93e34aed5fbe80bef0e7d1832d96f60c61e3eace5df315e, 65d96b763572ad2a7a03ab964225414de9fc7f4b820a603ef3f94f9203fbe4b2, d3da04c58d81445754a4a837f3784e5fa7ec54ceeb8e595a836e9b87dc0c39cd, 44bab852fa3bbaec1a03c900a8dace3c3553bf3c8289e5ffe9457633af0ea74a, b02bc37b60170d53ff9d17ae0f75e6df5cde7287cede634bcb0042545585dd90, 948ce1b8169805870338a59415ef470029323fc824a84bed9a760b2d78affb44, adfdf33b7f14b4509d1d1ec5155bb57ae381b6a04ebc97281a58d3246d7abaa3, 1a11ba0de41e053025e98f64d4b6ac044f6afd0db00fb91f97c447a4e63a5e78, 17c6aaa3efc51678cf4c269ba99e62859967c5d2a6da0303e66d60c1e04b20b6, 638ef4333b1b2993e945dbbc57f8a2a2ee0ab84bf02ef11a6a343a07f673784a, 40bd419635471cf6c8df65142cb1cadfc1ed88bb6f9f921abbdaf5041503bc96, bf30f0045791417fa1e691b4974d5651ffd4310a536f30df325fe89365f1fd70, 15929ca0bf26f189592cc6f2ba7fae8d10b0d84d86ecce2f74f583f7ebf849ed, 832225013088d9619cca1bfc3192652fb434a2442ec33316342969c330b46825, 1cd45dac19c6d340f604546504393060d9b313d5b16a85f947e19daebc41dee5, 1073bf25ac3af08cf3f48c2cbaed489ef43671387211d6e63f96aa7fcf1ec0b3, 543a1c4db82edce36ae07e4836b4d4a7640355bdf728d5ed41370892bf97d8a8, e39a3ceb034e425f4554df867871bb7c5df43ba116dea05b173c4bd444789aea

Attack Name	TYPE	VALUE
SpiceRAT	IPv4	45[.]144[.]31[.]57, 94[.]198[.]40[.]4
	Domains	stock[.]adobe-service[.]net, app[.]turkmensk[.]org
	URL	http://94.198.40.4/homepage/index.aspx, http://stock.adobe-service.net/homepage/index.aspx, http://app.turkmensk.org/homepage/index.aspx
	SHA256	6ca2415aabb806a871889c2ab48ad05b1ba444b5867ceadbcea3ab7f23de72f4, b84ebbe57151844ac7ac9fc5d488e4696f37f98779d13dceafe6c5a7f2219a4c, 0374a9812c7e43db1bde605cc3decff3d77c8b041b959a5422e4da0b60e0f6dc, 48c65bb99ce954df0ee492b92e634d602d621295be2ff87e57fcb07c8b33db8b, bd3d9bad4d460da08a4a3ae655e7c49b8435efd39ea4faa19ed052c7f65423ab, 598c2b0b15b7b35b93f7435aecbd377de66ac3ccc4b7af8edce1ce3bc6d773cd, e2330f64c92a49927098f8a07de9da8fc54c87a89dc549f6ebdcf3bc78732db2, 9d4283c05417c0b49a00c6e5159eb5bcb52142036f94fcdfb9712b231d020955, 197f3be195767142f1a4da0ad9e108c23993361d1a180b62749a9b84ed0b1a45, 4d4d8f9941fa5e378f6019d1a4e20bb70bce31db23720724ec35a373eb7ecf75, 9f1cd725116114ab72c772c99a4809f5870dfceebb1f47f24c68025e34e714f9, 427b6dc489cbfad36413fce6f71e82e158a6632c9986c1dee1af7676a129f048, dde3e5dca9e0498db558dd8e83f27143ad86cd0fcca1a33964ee4f3100682db8
DragonForce Ransomware	MD5	d54bae930b038950c2947f5397c13f84
	SHA1	e164bbaf848fa5d46fa42f62402a1c55330ef562
	SHA256	1250ba6f25fd60077f698a2617c15f89d58c1867339bfd9ee8ab19ce9943304b
	Tor Address	Z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion n, 3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd[.]onion

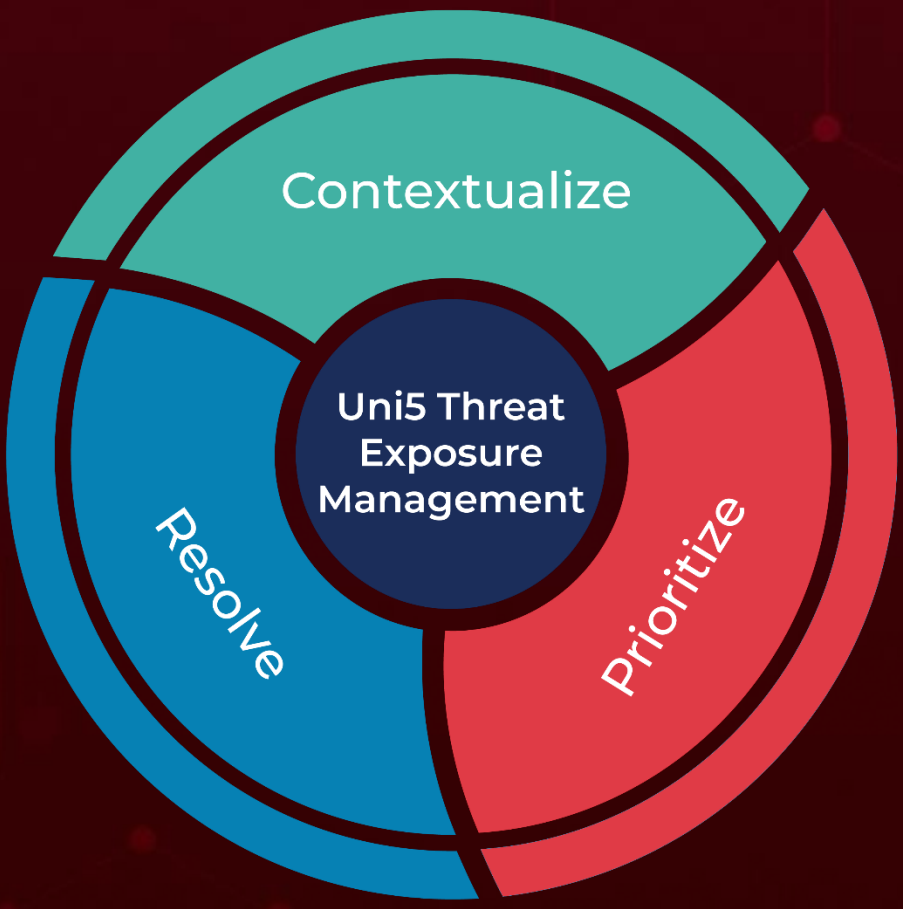
Attack Name	TYPE	VALUE
GoRed Backdoor	MD5	6ea3feb1888ce02e3d0d2857b5ef71c4, 64db61efc8acf370b91110b6f93d4dce, 63f6de3c86de55172b147b947f29c808, d3cd9d9bad6450e8fd4fd2e972639c69, cad5cb82baccd1f28e381e5c924f204a, 6f6e7fe49a8d5696f389e202d3b8c7e2, b5dc9a67f76fa18784b51fd3c5b9607c, caf68b393d56548074b9434564cb0625, b747c05888caf380edf6b2baab142272, 0385b0f83dbfc99c243ff066e3fe3cb2, 7dc1e49f1664af70d85d31af70f29071, fc3b7f47958f6c1c6a93a2f2f970734c, c02bee46d6a7a46f54e6abe003fec897, ad5c0363e7e28c69007f891fbc3dd030
	SHA1	c5540ec2ec79a21f07b0d793cc36b024a0db64cc, a81373d92d798418109552fb91d4c407d4c37a89, 5a504869350a4bdbcda22b09dbe7b05a7551a860, a190448a0c01a6e58610de27d022ccba0e755f79, 81861a853216f78219dd8cb0b4717d5d63260e7d 1d784e6c7d12fb7730895f21e4bfd3cde4b3900f, de243b57b087f5d1cde50db1949aa3744f1f6b5e, 680cb0a25e4a5148f5a1f7d3b75fad4fd345cdb0, ef50067027e27bea188023fa6a8ce9054c7d4ce9, 4f6164321d10c7a54a54398ccc7b11c1e7390e38, 1981f9a1d885c0ccb2d1f5910765a52d1989bc37, 8030f2430234426ab3bdc8cdd995be7c4805d7d2, 58d03630792f287184177660d9fd846fbde5416c, 3dd9bd38a8f8166b1af25cb523a9a6f25b1791df
	SHA256	67b7a8fad28dcc40c0889e5c4e40aef9348441c64bba74bd6d b885d88ce6d246, f43c99ef85166774ed47cad96c70b8273aa82c313e55bb08d9 c74e2b3f59b000, f91c9fd27bf0e3a7e82998721946ee70735ec46ee672ca80e3 062aa2d5195447, be246cdf932aa5b1c2ada0d74c8d1eca4028538b28fb61d7a8 d930b4266fd55c, ec36fcd64432843292d16f601a758ba4091ada906c5c4c4e54 0e326676911141, 41d35016c78f86eee8972808c7de8c200ff24625639adff5b9d 0ab8773fff6b4, aca34d7c3832879f6f7ebe8f7c59160896909574c94d1d12d7 c71b6f7918bc50, 8d055f3ad4d01f601df24a7c20ded981005adef7e6d2675041 5d1f95a471c2e3, 17e57c5e71b99a386b18728eac4a27e83415756071c9e8585 9940da41e94976b,

Attack Name	TYPE	VALUE
GoRed Backdoor	SHA256	32d76f2fe1188a131cb3219356639e83c60d47a703e40b8801a364d98e37128f, f3bb44d52e43477ce43c91eb8d9830e356fc105b96377edd6b190fcccda61e2f, ab801eaa9ad11199e1382a124d6024f9551a5a33ca1b9e5cafc0098621abb91f, e2b2ebe1b82d1c122dc2750f318f2484fe5361fcd964bfdcdcae631cf32f8d37, 4561a38ff34cc71cc73d54e2adfbd378f58d54596b012ff1841fdd7fc42063c3, f56b7fbc5dda7e46aff1b7753a1edb1f6fad5c8953dd3dbff30b3d8675b1dbd3
XWorm RAT	SHA256	0d16de10ce708b990d1b0ae26ac12792c91864426c88a8c73a475f7f33db014b, dd8377e9c3620d0732bededcd0d219f77f7bcffbc49470a9b7ff22db33fe4a185
BMANAGER	SHA256	7266f20123edcb2e0b92ac0b63225b8db2c5ff349818b339ef1553bff06719e4
	URL	hxxp[:]//updatebrower.com/download/bmanager[.]txt
	Domains	mainnode[.]beonlineboo[.]com, node[.]beonlineboo[.]com
CatB Ransomware	Bitcoin Address	bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz
	SHA256	35a273df61f4506cdb286ecc40415efaa5797379b16d44c240e3ca44714f945b, 512587a73cd03c6324ade468689510472c6b9e54074f3cf115aa54393b14f037, 9990388776daa57d2b06488f9e2209e35ef738fd0be1253be4c22a3ab7c3e1e2, 83129ed45151a706dff8f4e7a3b0736557f7284769016c2fb00018d0d3932cfa, 3661ff2a050ad47fdc451aed18b88444646bb3eb6387b07f4e47d0306aac6642, c8e0aa3b859ac505c2811eaa7e2004d6e3b351d004739e2a00a7a96f3d12430c
InnoLoader	Domains	valuescent[.]website, caretouch[.]hair, whipunit[.]hair, eyesnose[.]hair, nightauthority[.]xyz, cattlebusiness[.]icu, monkeyagreement[.]fun, laughvein[.]hair, brotherpopcorn[.]website, selectionword[.]xyz

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

July 1, 2024 . 7:15 AM

More at www.hivepro.com