Date of Publication
June 24, 2024

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

17 to 23 JUNE 2024

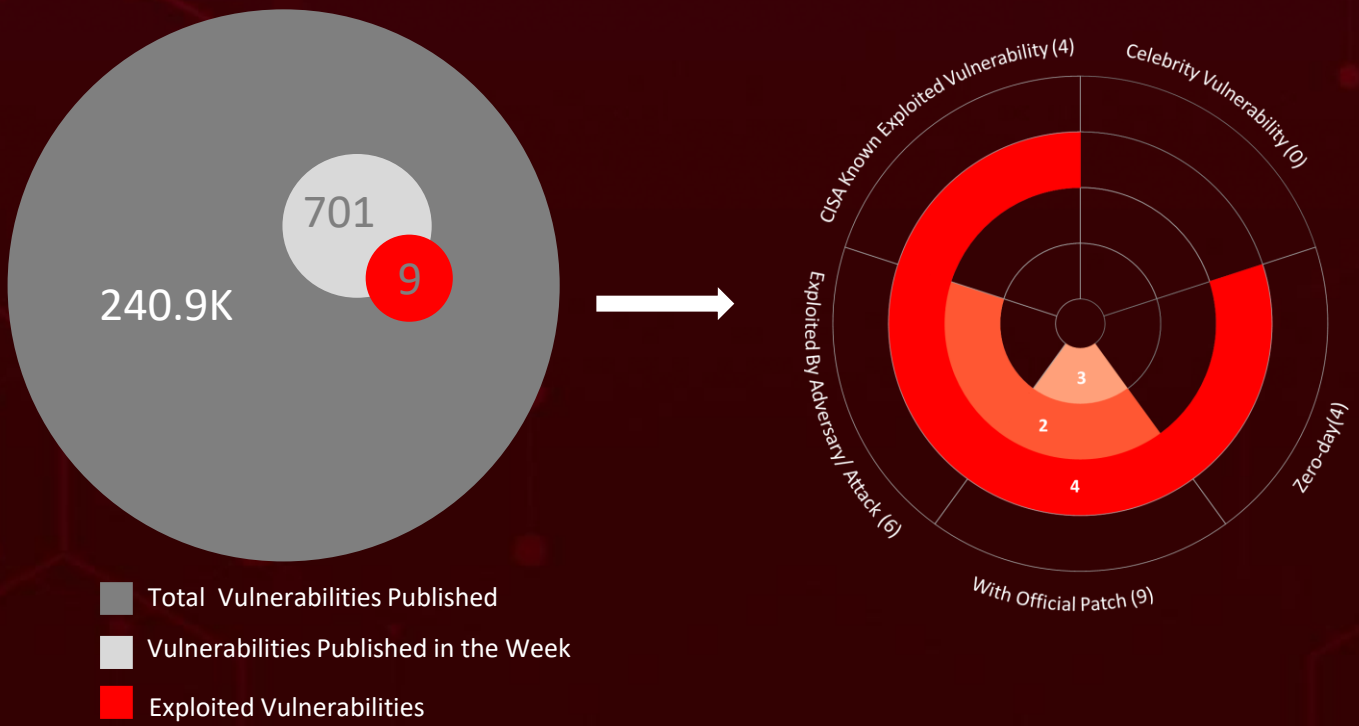
Table Of Contents

Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **ten** attacks were executed, **nine** vulnerabilities were uncovered, and **three** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs uncovered that the China-linked cyber espionage group **UNC3886** has been employing various techniques to evade detection and maintain access to compromised systems. Their attacks focus on entities in North America, Southeast Asia, Oceania, and other regions, including industries like government, telecommunications, technology, aerospace, defense, and energy.

Furthermore, threat actors are currently exploiting a critical path-traversal vulnerability, **CVE-2024-28995**, within SolarWinds Serv-U. Using publicly available proof-of-concept (PoC) exploits, attackers leverage this vulnerability to gain unauthorized access, allowing them to read sensitive files on the target server without requiring authentication. These rising attacks present a significant and immediate threat to users globally.



High Level Statistics

10
Attacks Executed

9
Vulnerabilities Exploited

3
Adversaries in Action

- DISGOMOJI
- PlugX
- BadSpace
- Noodle RAT
- Fickle Stealer
- VirtualPita
- VirtualPie
- VirtualGate
- MOPSLED
- RIFLESPINE
- CVE-2024-37079
- CVE-2024-37080
- CVE-2024-37081
- CVE-2024-28995
- CVE-2023-34048
- CVE-2022-41328
- CVE-2022-22948
- CVE-2023-20867
- CVE-2022-42475
- UTA0137
- Velvet Ant
- UNC3886

Insights

UNC3886
China-linked group, utilize rootkits maintain access and evade detection

Fickle Stealer
a Rust-based information stealer, employing four distinct distribution techniques: VBA dropper, VBA downloader, link downloader, and executable downloader, to harvest sensitive information

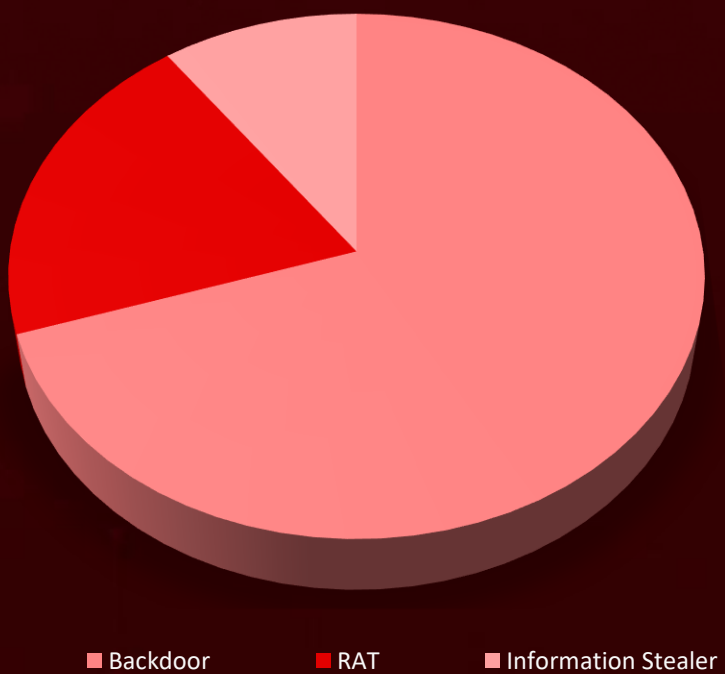
BadSpace
a new Windows backdoor, propagate itself under the guise of fake browser updates

Velvet Ant
A highly sophisticated, state-sponsored cyber threat group, exploited F5 BIG-IP appliances to establish a persistent connection to an internal network and exfiltrate data

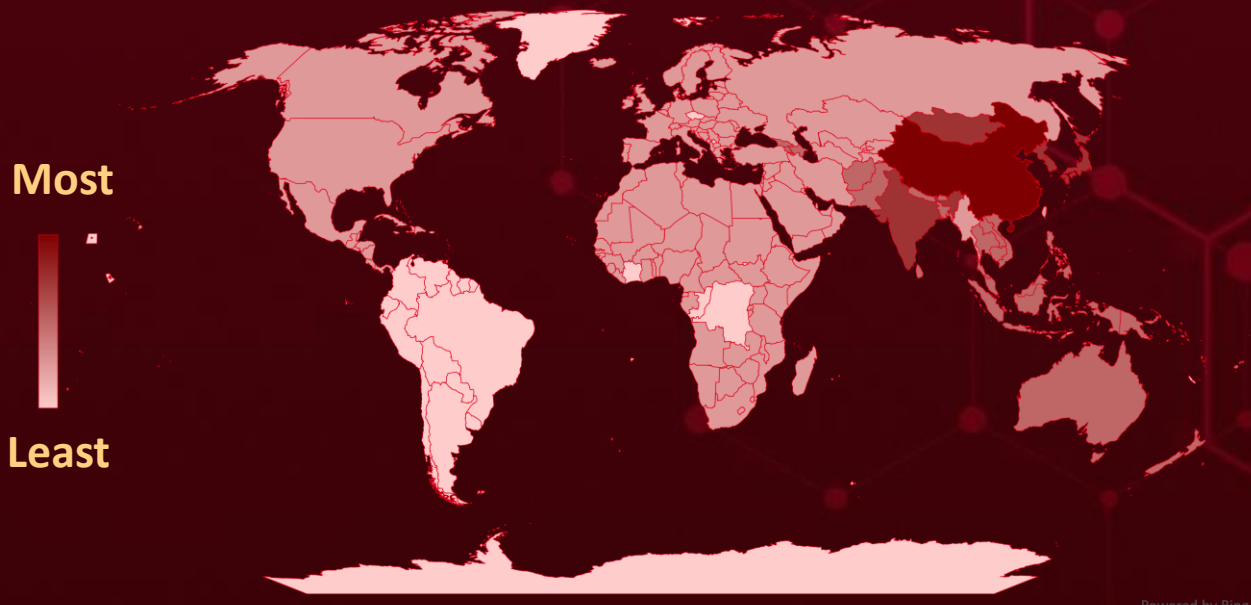
CVE-2024-28995
Threat actors are actively exploiting a critical path-traversal vulnerability, in SolarWinds Serv-U. By leveraging publicly available proof-of-concept (PoC) exploits

UTA0137
a Pakistan-based threat actor, utilizing emojis to execute commands on infected devices

Threat Distribution

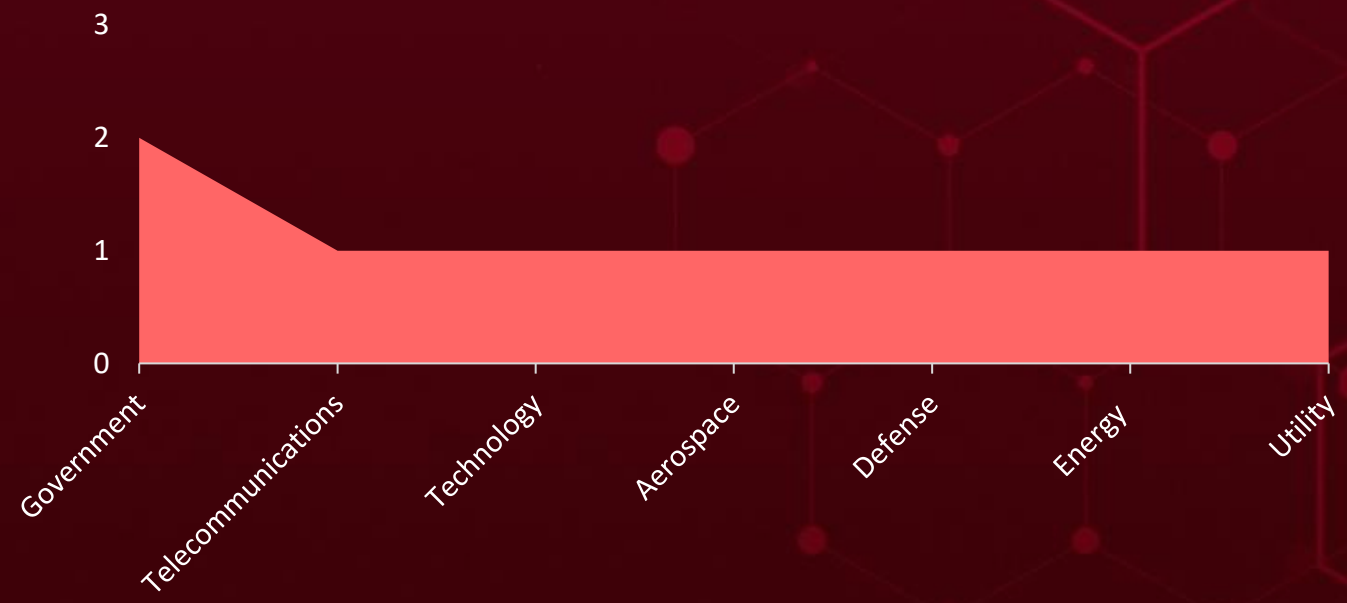


Targeted Countries



Countries	Countries	Countries	Countries
China	Papua New Guinea	Algeria	Germany
Mongolia	New Zealand	Equatorial Guinea	Mozambique
South Korea	Philippines	Romania	Ghana
North Korea	Pakistan	Eritrea	Cabo Verde
India	Singapore	South Africa	Greece
Japan	Brunei	Estonia	Niger
Marshall Islands	Azerbaijan	Trinidad and Tobago	Grenada
Palau	Samoa	Eswatini	Norway
Nepal	Kiribati	Namibia	Guatemala
Cambodia	Solomon Islands	Ethiopia	Panama
Tuvalu	Laos	Cameroon	Guinea
Armenia	Sri Lanka	Bahamas	Portugal
Bangladesh	Vietnam	Austria	Guinea-Bissau
Cyprus	Tonga	Finland	Rwanda
Bhutan	Afghanistan	Comoros	Haiti
Fiji	Malaysia	France	Saudi Arabia
Thailand	Vanuatu	Slovakia	Honduras
Georgia	United Kingdom	Gabon	Sierra Leone
Maldives	Serbia	Andorra	Hungary
Australia	Canada	Gambia	Croatia
Micronesia	Egypt	Denmark	Iceland
Indonesia	Syria	Bahrain	South Sudan
Nauru	El Salvador	Dominica	Angola
	Papua New Guinea		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter

T1566 Phishing

T1588 Obtain Capabilities

T1105 Ingress Tool Transfer

T1036 Masquerading

T1562 Impair Defenses

T1027 Obfuscated Files or Information

T1053 Scheduled Task/Job

T1082 System Information Discovery

T1588.006 Vulnerabilities

T1027.002 Software Packing

T1204.001 Malicious Link

T1190 Exploit Public-Facing Application

T1041 Exfiltration Over C2 Channel

T1548 Abuse Elevation Control Mechanism

T1059.001 PowerShell

T1133 External Remote Services

T1068 Exploitation for Privilege Escalation

T1204 User Execution

T1071 Application Layer Protocol

Attacks Executed

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	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
UTA0137			-
IOC TYPE	**VALUE**		
MD5	0d4111ab5471c7f5b909bff336ba8cd66f9d8630, e5182d13d66c3efaa7676510581d622f98471895, 2dfe824d0298201e0efb30f16b3ce8a409ffe006		

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			-
IOC TYPE	**VALUE**		
SHA256	ffc66d40bcdcba5089d27121a2f1fac2a9f49c7aa214be98748f9624ae7d1bbf, ff9423ce5748687dc09be8093b67ca86a1f6a3dd19bd43b8a8669717a8876ea3,		

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
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**
-			-
IOC TYPE	**VALUE**		
SHA256	6a195e6111c9a4b8c874d51937b53cd5b4b78efc32f7bb255012d05087586d8f, 2a5a12cc4ef2f0f527cc072243aa27d3e95e48402ef674e92c6709dc03a0836a		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Noodle RAT	Noodle RAT is available in both Windows and Linux versions. The Windows variant is an in-memory modular backdoor deployed through a loader. It can execute commands to download/upload files, run malware, act as a TCP proxy, and self-delete. The Linux version, an ELF variant, can launch a reverse shell, download/upload files, schedule tasks, and initiate SOCKS tunneling. Both versions utilize identical code for command-and-control communications.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Download malware, Execute commands	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	c49371cd8dd33f725a780ea179e6281f5cb7f42e84a00836c8fe3350b7b9b2d0, a8db92a8f34caa5084a3fdb8a683a1854bff84612dfd25a965bc12a454a38556		

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
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**
-			-
IOC TYPE	**VALUE**		
SHA256	e9bc44cf548a70e7285499209973faf44b7374dece1413dfcdc03bf25a6c599c, a641d10798be5224c8c32dfaab0dd353cd7bb06a2d57d9630e13fb1975d03a53		

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>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>MD5</td><td colspan="3">9ef5266a9fdd25474227c3e33b8e6d77, a7cd7b61d13256f5478feb28ab34be72</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>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>MD5</td><td colspan="3">2716c60c28cf7f7568f55ac33313468b, 61ab3f6401d60ec36cd3ac980a8deb75</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
VirtualGate	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.	Exploiting Vulnerabilities	CVE-2023-34048, CVE-2022-41328, CVE-2022-22948 CVE-2023-20867, CVE-2022-42475
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Execute Commands	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

IOC TYPE	VALUE
MD5	3c7316012cba3bbfa8a95d7277cda873

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>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>MD5</td><td colspan="3">89339821cdf6e9297000f3e6949f0404, c870ea6a598c12218e6ac36d791032b5</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>RIFLESPINE</td><td rowspan="6">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. The threat actor creates an encrypted file containing instructions for RIFLESPINE, which the malware executes on the target endpoint. The filename must include the target's MAC address. The outputs are then encrypted, stored in a temporary file, and re-uploaded to Google Drive.</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="4">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>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>MD5</td><td colspan="3">fd3834d566a993c549a13a52d843a4e1, 4282de95cc54829d7ac275e436e33b78</td></tr>
</table>

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

Vulnerabilities Exploited

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><td>NAME</td><td>CISA KEV</td><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>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-37081</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><td>NAME</td><td>CISA KEV</td><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 Multiple Local Privilege Escalation Vulnerabilities</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-264</td><td>T1190: Exploit Public-Facing Application
T1548.003: Sudo and Sudo Caching
T1068: Exploitation for Privilege Escalation</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-2024-28995	✗	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

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
UTA0137</td><td>Pakistan</td><td rowspan="3">Government</td><td rowspan="3">India</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>DISGOMOJI</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">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</td></tr>
</table>

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

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

UNC3886</td><td>China</td><td rowspan="3">Government, Telecommunications, Technology, Aerospace, Defense, Energy and Utility</td><td rowspan="3">North America, Oceania, Europe, Africa, and Asia</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2023-34048
CVE-2022-41328
CVE-2022-22948
CVE-2023-20867
CVE-2022-42475</td><td>VirtualPita, VirtualPie, VirtualGate, MOPSLED and RIFLESPINE</td><td>VMware vCenter Server, Fortinet FortiOS, VMware Tools</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">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</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actors **UTA0137, Velvet Ant, UNC3886** and malware **DISGOMOJI, PlugX, BadSpace, Noodle RAT, Fickle Stealer, VirtualPita, VirtualPie , VirtualGate, MOPSLED , RIFLESPINE.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **nine exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **UTA0137, Velvet Ant, UNC3886** and malware **DISGOMOJI, PlugX, BadSpace, Noodle RAT, Fickle Stealer, VirtualPita, VirtualPie , VirtualGate, MOPSLED , RIFLESPINE** in Breach and Attack Simulation(BAS).

Threat Advisories

DISGOMOJI: Linux Malware Leveraging Emojis for C2

F5 BIG-IP Exploited in Three-Year Espionage Campaign by Velvet Ant

BadSpace Backdoor Infiltrates via Fake Browser Updates

VMware Address Critical Heap-Overflow and Privilege Escalation Flaws

Surge in QR Code Phishing Attacks, Hits Chinese Citizens

Noodle RAT: Understanding the Full Scope of this Cross-Platform Malware

Active Exploitation of SolarWinds Serv-U Flaw for Accessing Private Data

Fickle Stealer's Dynamic Attack Strategies

UNC3886 Covert Operations Leveraging Rootkits and Backdoored Applications

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 threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
DISGOMOJI	MD5	0d4111ab5471c7f5b909bff336ba8cd66f9d8630, e5182d13d66c3efaa7676510581d622f98471895, 2dfe824d0298201e0efb30f16b3ce8a409ffe006
PlugX (aka Korplug)	SHA256	ffc66d40bcdcba5089d27121a2f1fac2a9f49c7aa214be98748f9624ae7d1bbf, ff9423ce5748687dc09be8093b67ca86a1f6a3dd19bd43b8a8669717a8876ea3, fa6d61a607162a8687b049b1844edae82afe911ff6684e8ff77297fbd9bffe63, f9e0ad7f6b3343a5d75a77f8032e7aa6b0363df030b47d4b83fb9414b90a17e8, f97970d5a629fc72647a6397ca9638fabf28f701656f058067f43038629e34b8, f96023de8014a90858746fe6fe788f907902e60dd05cf70328a6fe1e3e66cd34, f7d974093ff22f705d96750cd06a91f59b519cb8c50f7ffea627cddd68cf20d3, f78aab9b8ab7d116a4e0e9f6903a22c67ea2e01f6b99101b5be990aa9d73fff7, f75f29589e08aeda2e13954c5e20e446b670518008f8c3423fc03beed7a945d0, f758227b90f46a41203476df409e23cea56d4824a4fec0c0a210ae9fb838b70c, f61b8e667882e2735a7cc4b73affd651c172c9d4c4df02b8e96b4a234a30bd86, f60fcde71c1947be6b89b19c6d62a10de38599dbc82bdb7949eb0e0991102073,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	f5caef720f1e32e5539e81dc24d88a582b3d5c9b8146650f5df7b2b18522d858, f392d7794132e8754e3eed756c60abf31eac94d3c70c73e33cb97b77d0b68f32, f36bdf4c7fec3d8de696c6df386a437f37e3713e8e20b79e47172894315148a6, f346bb5b305e2e2db5372436eb07e2fefa707143d38186ca071f072d51a7b141, f30056753e5a088e5a0f161061a5a6b8327f8ec65f6d984759b9fe4cbadc8851, f1ef7c0f62154ec377d50960f39573b5c34ad2e0388fd59c2082a1d1bca22b2f, f1623a0411763ff5af44940ecd82c6acb824fcddc790622e1bd081ec1041781b, f0513c677361050e0c593f293ca2b7eeebbf6fd11511a8dcea68efdc5dd9ec75, efcad47ae25743c3b3126fcb4d12f6751de18b55a6eec0e388ec5ba29675a48e, ef24544e2f7ecbf45c2cc1f9eece9b26a61cf93b7d9362119f27bdb8f36a625b, eeedf0393e6b4884ed1c656eb1dd597297db44d680543b86cc0eb4b342e151fb, ee46bf00c0f7095c3f3e63f0e85dc2ec2f49d70a9aa3fda6046e1d42e89b5613, ee0703bede4979d42505f32e3b18f34d6da112682cffd62be5111fb2becbb598, edf4ccd0162ffa049fa728dfedde9041feb09496d7a8582df24eb283842a33ab, edd925fecf34153c5cfdc5b6e53bb0fc2105ca5d58b9fb20c81a481405e790d2, ecf291d795b71a85015c78cd45c023f7f9df40d78b36b603788a6f858fe45632, ec5da6e65f245f5f9c1f4061c035bf6064aac75fe9784f06930c976147349905, ec2a9812f5fcc681236e7d274cab1f4f205f79f699c7b8618d521f08dac6eb58, eb85cbf5f4113685ca6cc2c03b0b5b10279c4bb8024d1a495e42d2d241c3eea2, eb2bb071928213edfdc17cd0be46cb9663fcfa85f37cd7e9b013b618c5f6c86e, eaaa0aa016cb8cb46396a477c47ed5b55ac2492e6d45769edad65fb650ae17e5, e8899cf683a906bb0978752f5ce32755365d594a6bdfc7ba76e9b2375aca2285,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	e871818b00f1dfd2a8967cc75435fb5d1cd646308715eecc89a6bea3f89ad12b, e7b3f9aff12d5d08e52d85f574b677f3e840eedefb980e1591d42c17062d9ecd, e78773ee9aa7e4121bbd7118d93ac1842595034078917b2e488cea40aa171b1f, e73aaac7d49efb0c47ec76625f520791c1048211846f86ebc7345275586f3012, e5595db0c2b46f8baffd5586d40a1482fa5d72cadb2a47b93afb922a6a596a0e, e51bd357c4c1f806521bd46ca9567bb1aee40ab6e81aae39ae89360ed415d707, e4e9ad2de5826d53117c56f04a03cb0372cdd3b66aec9092c74d6eb8544bccb8, e3f2ae137a1a6f17c445643b21a74f102670cad115ae7491190e13beaa836c50, e3ba82f314465d1d8201d66218545f13d967db5341acda58900233655a8edfcc, e3af5d57eb873782d4d66a645131122568c0432581714754502b5eed3775edab, e34a2cfcb4afda6bc918393e6f151f757bd3abb4c7775b6ba18b0756a5786a40, e2e7e04eb8eff0359137c638cc8f0a9c0ffbc1fd714ff17540bf459cb1a5d7db, e26b98840286379cd63a2b85ecee23db4af54ba5e32579012cb7b1abb85baf69, e17b4328ab4dbcc281236aaa7cb9c1adc71ea4536e67737f85b1832302868f62, e137b0a42d08f51fe6bbf1dc320c4a252b6336df18d6a23272e38d49930d64da, dff4594e3076dd655db3c3ed4dc4363f614b724ab7da0786645b486c15762ca8, df9ec49b0e6c3c64cb411abc2aa8c798932a2891064ad4adfbba3bdf5a81a892, dd559945d8a3624f97c7512b14fc8c7280d1d5cf9be61baa5f9ce8c5c04c8bea, dcaf4d83af8ea96c3c377f90573dd49938fbd28e00dea7d9748a5440bf4a2766, dbe6c90018b0e779c509cff3d761bf2dc33f847bf07a6ccee4a92169eb3e1ee0, dad1b5790608300b8764dabe1b24008a7ed5e4aeb335bd5aeccc17e109306c95, da5034d5a8dad2e50cbe31b8ada9fc92ea3a6fd5a1d01334252ee1b9c2692832,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	d9e41e3a72fdbd630edc08af015e3bb2a664a1cc15b9f2b8e16d7097f9c96b77, d9c9bcfee1a579a5584698ee1c0d82ee9a8fc3054db1c3a65295483f4444f32a, d5bafe54f73dc17c3f5b8f2d09252c7f99e7e4c36cdc5bb55457c18cac079d3d, d5b37b2d69dab0a5d4b943abbe6b009bc9ed2f4ff2c05b57f3503b115bf240ed, d3a5007efc6a7540edad60d47058bd6b60a65c345885644546cffc3f2adc74f2, d35d5fcd188b0e403004c9756070530fd6fca18dfca76ce761bc3263017c38f8, d2f4c971cbb7e653d8054b8bf92a916ddd39ff3ba9c7c109215dac141fa1fd24, d2ebd9381ab0cd64b287e26463c180cc590a97e27428bece72df796dca33e896, d11391b6a1d254a9a477c4b48abd220145fdcb8453ae3f109185bd75a703d257, d0f02de7dbfa809c2f8c463a902817a9fdb6ae323f10d783b363565af60e7741, d05627c477d97d455fbbe832b4282a39e5ba8d2a957713c77378b788b0b4cddd, d00134b8ed2da80191cfe27ac3006a6864b96b6d86c667d56d6b4b36e7e9ca2b, cf83d9f9f55bd1cb5f571d9ea6900879029097f0e2aab4e4d50cda9de5b471fb, ce92aa8e8ee8854d47ac0c1adb8efb73fc2218c1e094855157e33018861b25e7, ce3452deb930a9972ba75df850af882617cb668286ab387e8718cd95d1052b1f, cc83a6144f3619a652a3c215ba566637aced184cbc5d8f6e528486725fd54f25, cbe9b54de250fe79624ae342d030fa13999e3aa019f1b12a2675fd3a9f2eb644, cb8e23bfa8a1178b7aaae57b1e76b216e4d93ff7bb9aa13b3c5ea7688d363878, cac18898d6185b349e3f5ae76fd0012098cf8aeafaf7f5aac3091f0555429966, c88191480451fe9ab7ff1b65243f5f14637a584646d5fb302646d50fdfaf5659, c81ef921513f3e39cffd9cb2a4d24aed816b52c44a1fed3ffad746f9061e3862, c4d494fcdd3e85b0c8507430b1b09e81185bc60de2922718b229aaac7de829d4, c42253745b945ed0ef3dba8a6fbf88abb80982d5c84cf18a8cef1778a0b01062,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	c3b6ad575ff07cac79151a7180671db8470d456f72e18b1b029592cc0975ec8d, c24e63117dc25d2ccf2efb4fdbf43b37ed82a238377062fb0d92417aaa103be7, c01048c9065eccae8c66fb8973f18ec6ce5aec8fbeacc6541d557c9d69147a36, bfedc08b3b5e819e9a4c43d7bcd80eb3c64ac0d6e6e272dd549931c9269d41b6, bfc2edab849faddf92c2b1f9d0b07f19224af9a5f4fdc598b5225bbdf8626c8a, bf347a490e4a725d5022d369f013ec3b092a09a23e69182cc9f4d6577cd054f7, bda2bb03d04dced72e990cb75046c8bca094b3493b8b401fb64c368c09378d19, bce6706d90bf6f28a25098f3da19ae834d1b987b22232573cd6e9cac2be1acc4, bb9ac991f7fe4d46c66a6aa99e9e9892dc9598cd77d124e57f4f8211f81442e1, bb10fe298daa4eaeb5c40e35aa32a599b9f03a21999c9748c94ff526f3f3d60e, ba451fbe6f75bfc7b159b4d6976f88d3710757ae31899196b64b721372f8a703, b9e85336b1241a4dc3229883baf954b46465b6888ce8565fec630148568d28dd, b9016e0424d69e035990a457b3ea6d1504c636686b261050ee192867e179e6ae, b83794d18978042fdf453aa0c0a87ed5648e384dc24ea053821bd2babc3f1f25, b792eaa20a51d86cb2b669e99c8ffb612fd1100869553fcf70af616cb2008605, b7693a98a1acb35d5aacf31f4ee1eedab48f03fc2ac5bd05ea7ba72b5e5465a3, b65d55b1b6ee5cc031bfcba21a1b434b5c6ebbe466e00f9a815aa67fec3210a8, b450a40cdf9cdb5675510871f34089e57a7d38da2982c8a7d3defc80902f84ce, b38b435374130c93e301dd8a5a14c35d2cd49761e47cc9f5b10876c47430d5c8, b24e71b4c2e370dad40b329a80cf9affbad4e0e4e8ce32bbb8eb02ac4d95637a, b0e8c24fe365b4798c870426f786843793ac24bc58f3fb9d1cf092ecf3685a0d, b053e614ef22d328ebeb2d5e2b521269d09dbe4cee7f75f7b77e282aaf30b3d9,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	b0343be14f4800c75585b1f862dcfb782db6bab6f87e9043baf77dd57159dee8, afd65701770caf5c3a573d56a59bf8818135a019f7af1f2aac97705f302a8626, afaf60c0ce17978c52bc471ba740beb3221ef1d64604a25ab9590399aaef61f5, af5c3c64fc7c023e3b8f5f4858fb74b8c6a81d594232f6e4d556b8fddafa8a15, af33428d578d1246c9a78624bdb2618834a562dade0b0b01d6caa1cab690bb8d, af2cd4e518ac90d6ef38d4ca2a7a7c7cc25e4a0343c4f2319e00190e98fee9ee, adf76f5e5c71ab96a18bb2d135f272954b1a1042442b98e6acbbd9917698c10e, adc48214b3829702f4e4dbe56a403c37ddd7c28607169c77120fec93b35ad3b0, ad8a87787fe3f2d4a1e6c6d31e73af1661737b88b24729b2baaa344203c7d26c, ab53aaa1756c973bd9e6e1496c40b1efba6314d8a3125e08378118f85fe3ca22, aa230c78cc89f34e9656ac04a91daa0e50c0969694e7d054efe68076ca6c542c, a917b3efe5aa4f4f34a6031765d0466d50e964092d095cb410521184e9c634fa, a8f49b1bbca938386582984e71d54c06f2c6ebecdabbe5ae9477b99fd314392d, a8bce520fe1da19bd4f0238a90807abd3ab2611dfe69840fce9fce92df1872b5, a81b937b7993e69094841fb01dfe3948efbe153c055e4291a89cf21ba44d901a, a767ca11d31388a0780ac60249f1065655876a1261c646c45c2368e6a381d800, a70583d710649ea5d21e8e437ffa632dd06935f58a34c57865106e0f79014847, a56362834603dc4de009eb959322427009004a15fed1229e980fb80681a5caa1, a5563cf63c7b735bdf4848a44f3ad866e001e9650a1ffb95ce859eb5c6b8b074, a470e931417cf65862ea1bdad5197df76abf68b4cf5f5822caf93c966efd5cec, a3bc410a91a7fc9f4bd3fb2437c70254c58fa65ca314ab6e3c3dbc67983adb0b, a39f72f901a79c81e4982005f061088957ad5103162f22a4d6ec9b347771aeaf,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	a29140c9ea0867110ac95b37883afe9f2b583f01d315349ca32df171b7c0d640, a203759e25498c084c8c77528060f0822297ef4c19bde1807af01890e085aea7, a17dc0336a1d9469765f7645cd8be005f6fb14753c098bb2376cceb832cf0beb, a144bedd15387bde8bb74f3122bf482c39c043d4745f1480fc2f492f4009ff70, a09ae44ed4a4cb622e8faecd36606d6b862e6c5d989779bfd5adbeaed8553e9c, a0319e90049271a8d48817f550811719b93f58402b4836a0a0254223ef1a457f, 9fa8bb5c922c66b4ccbac205d59823eda690f6f4968d407127861f4458c8cd5c, 9ed34049a73074015b2a401db2654184e252bc30619bef8d12e83e49657fa948, 9ddadbdbe00cb6f2e9d9e9c12f5b1829d7eafa18fb957c7bc75e5f3d0814c4f7, 9dd6aa069ef4447ab1c0fb7fb5f822d0129d12472a0e180e92cca92c5e8c360a, 9c5bcd146dd98ca118d1e4f072ede51039eab837d67c8890bb35fc005b53047d, 9c28d5f28d9795682d8124bfb8fa775fec6cab075badfcaf9d6b81af12d1335b, 9adb1171f314855689a7a38731de0f4f2fdc8be12ed6b814e45709ce9d28b2f1, 9a2bc2ac05066697ccb42fe2c33f85ba26bed0917d45125ec6deac41358ab1f0, 96b0f5f46b12b6bec89349fd57d2e8525ffc5277657e0609c7f793da98af2d7e, 95e223b41143bd1e3321909c9c67176e1560895a910b5d0d2747d8b910d0b5a7, 95d9c2ba565a12b8c13c5ecb013bcd4d6fdda1262afa4df2cbf82952fa306987, 9386d192bedf26265143b8f99485c4bef25f043d82cf4d6660c766aa6db6026f, 931baece3c6039cc3a615956040cf1872fa7e0041b07e97f47e99ab4fade3b1a, 92f6335513ca65ec7a918a02ee9f2ca7bf0f0410997f0c39700d9b02c3b6049e, 9260c2e0cf723242e27c75c5345e5a0857e9ec003a4947680ca90f45317422f4, 920cac3f709f26566b6997e14b9401e7f812eeaad1baf986aa6c6dd7f6b5b15e,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	8ee3cb99f6043e353b12e47ff65bc86028b113f7c5b89ea341c89e0ba5dfdc5e, 8ebdb02ac508735928625411f63ea7be1f252114298b9c6cf5932b3bdf8ba4d8, 8e76c6e2e7073d09356d3e8a90ce15b761a6b2c064faca06cf0988ea8b7fc802, 8e2c5f1516056acec5567b784c4a8b4ecb4456161588cd0e9c91fa5f5a1aaa25, 8d5cad3c0a5c909c9956392d06717ea7656e33479a6704a5d5b022db259871cb, 8cd478eaf5d21fc7ba88997a35e0a46a6773a7515c6a8aa5cd22b72fb9f9996d, 8cd3d44573a2b7e6a062de8df72441e35fab1f01a2de8e3b3695ec9358788e79, 8b0257e850a0674eed33440aef92e79d5b6e3d08e112708a4b4a2d4487daef40, 8940f27fcf2924f7d192ebad5710b502ce3a0c737bedbf1406f078026fb142c2, 877f80ea5733d99bcbb123327eee725fb88c931da7c9f73d7b7b331c5d7e5648, 859258cbcdd1209b0c96141bc3e4836d41d8312300798a5a4376f26de140b956, 84fb68f5a66cc56592de346757e33d4c6241b643d00689cdc0c63c27114df4b0, 83b43d77c3864b94163067ae5bacef6525f6265f8542cdf3d9d6b1ad5fd5d6db, 82d044378235074ffbbbb569de5238d09ef57c919b05982a2f596eb2215cf02f, 7f7b919dce87ec1e13e6210c5d0a8593e85fc24e099f8dab8fbf3090684b3f56, 7f75430c44b964821e39c6761648eccc2da8a70889d82520d972467f4d352456, 7ef3c16df46c2826d7cfac5a84514c317884c349dd0a40c25305c465256a9196, 7bc4baa8314ba6649c4f44fdefc056d948fb3750b58a779581fbc387bdbe3a5a, 7aa9d03388045c0f31bea1dbecf8aad6de0702c33c0f192c4f5c28b160033b86, 79be03dee948545ce1733ca6c10390b7b84d8e9373a4a80149f07843b7ed0a35, 793945a2e27e1293e2cadb5e63b3e4c8f87dcb152699bad3c0c6fd9b41533ca8, 7906026b7ab2ba37f4735336f39b3c3bf7a67852331993c0d26cba5ce0d3042f,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	780669cfc84e5271e4db6dd827e25aabe0b80cc705e99a101717e74c42627ce2, 7763452a185a0cca4101f140267c360409a24d80a64e599b2eed0dc3383c40af, 7697161fcc0c1bfe8ddb1911bf32b8adf6404fc96b8c30606473ebfe67c27aa5, 75345ab59320b45395eb28ecb987f1eff96badc4f4d28e9f1172e6ed9984f5ea, 74d31be042672b564c8f8a2c6d143ec2ae966e2f3457687f60ab0105cc1ef835, 74cfb6aa244e79ce9492b30b1f44f8bf78637c5f06be4c256768452395896db6, 74468aa16537c716b6e3cdd481b12004e18354a663876d16da431c3555589aee, 743a597c1bf22649896f72a5f94979071de235929085d527ee8271ed570e3eda, 7434e13d4642bdf24687d145f34c4c744570c5af19b71d97dd895c5be64e9be6, 742981da5d5c9934d1abae0d962794ccd7a396891e73d2d366d45b4ac5ebf881, 73be1517ce7b0b01ed6fcbad483b9842bf297aaf2988dd8e09c48cafb21354f2, 7391e33589f7531104fd3c7be5ce8e78ff32e59a41ee64c69c7515fe3358d18c, 6f61d01c6578eaf1d8c9aa0325f98a13d8e1bf291d9269c0c48cb00f0688cb9a, 6e27f6a40e94628ae1c64e2c8e674fbf1ee1441fff15002f6bd89d75d3b76e14, 6d5cd9cc6fe81f1995720e07ea8ae0a29320779b1788c865bfc229cbf263f963, 6d3122e14566370327c09cc3a64e8c5479eec26ceff372a3ae50a0cecb2385e8, 6c1d2b965e1f6f8fe6c9e139664c5a61b56e7c57104450811d1100612d1bc23f, 6be415f3d774e76002c41275f15a334b6259e156244dcb673afff2a1c3155290, 6af8412ee3591045e97d8edc1ef8cb8e05a4bd026c9dedf08f508329d2cd275a, 68b4304c0bdaad8201515a7d1cf5eda2418344c0b67a3e4b258fc2d762ed5e09, 6878d216076606d3347fe1dbabca05b54fb6b61538c8e8f2ddb07f2c71a093a5, 678ea8ac8a616be02b7ecff7f28bcf77bd47dac9c51d2100f0d67debb49207eb,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	66c424824ff9701fce476762098bb225224bb12f00f4faca822e2683e2817c2c, 6683ecc41e53221065513015a298bee810042b806cd39129a9384a1a243bed83, 667a7f942ffbb83be38766dd5390b7941e509b382d315b40ada50847aa51420a, 663aaedc2a446353b9d44e9acb47b1f77b864f1d303fd81a884ea13ba77bd2ec, 64f9efb81c175257251e257bd3ce866b3ca225eae74ed7a64ff20a5460a607d6, 610889a30d97c29d408dba053e392ea006cfe6e6a1c401933116346360df4e15, 6017379065c6d9b36dbf8cf2da01a2ca8340693b8f19b4c11d937a0179a63561, 5fe6778d75a76642cf54a009561ca23cdaa558255968ebe0880db8422245add1, 5ddbe11f7b67136af0fd62c2e9105cc07f3acc4854f35704d9e922d2de2ad384, 5be19d5dea37bf85e4b7a7110102ad39463d1586bac8fc815b4b0ab46eb68c6f, 5bca1ca46380106560414f794545f9e48348edd05cb8ac687cf27d764cffc6fc, 5bbbd83ea6a811e6ab65b45cf25edaff4e35aeb4a2992be9aff13bfe925c9cbc, 5ac78b09dd38e9fa32e2dca3217ea46450850464929075c98cbcf73b63bdd093, 590aa3d6c9b4cf88a8e606d6007c310190963c10fa03c12872e9d9108e921a87, 58eae06ab7e785f07373b0eb84b912347e969fc05ab78b00b6e49eac1e75eb43, 580f5ad561055be312a489ec1b25d4b8777e392187b0f2c67d1c2519e56cd51a, 57934ea7affdd9825c5b7ed21ec5a630e79cb00bdc34191e4aca4f6a3a00798a, 55e0071730f48e0c4fa6f8d36dd55d6edb8231ea818a1ccf656015d93c940480, 55532e7529d225b688f29bbed13c8d8af5cd8115e82328c5213be40509c2a2a5, 54bee71bed4653cf36db9d2b74bdf21fc36924b1f676bec967b5a468341652af, 54a53069771efc780e1d7557f24c116f039588cc6ea54b8d7aec06f2456f407d, 5423c7ad6fabe5dc62a9250039a64f60711281f7b9776a675c43a50f62d21c02, 53306aced93b3789b5baf03a1e5d364b2777d2ad8849ee907d5344053a750f01,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	530cbfdd0585f8a6e773a340dc8fc2761bc527d964b25fda5985ecc30b31172f, 5181039ff53f195a14b8193bc8879190512705c0de1fbeb26a0bbac23dc3bbc0, 514972453ef9dc059add5fd8fa4d2e5f293924ef1255918ef2253b67e229a1d2, 50d19553ce3092ee217451d0a3c174137b0a5c351cb3248973515b2cffbc2e2b, 4d8b94c894d473bc65e5afed24264e15cceecd81d8b07b8542ea5962af5a352c, 4d81c804d9dc7c1daed6626d98a81dea09892bd0f392fa1cae970d8e6aaba554, 4c226ca0d165545767131c30ac0aeb511d66019a0990d227dd7aa70c1f2c3324, 4bbab4461e3ffcdcd035c0bd13e3e53417221fdd22c47209a8d53eca104b13c4, 4b677aa4d48046bf539c985ce5e8d617d556059a3207bf3fe16f067535aafc48, 4a8189ab15f4fb4d8b507f483ae694aa1f866b4341bf9cc0c5d1eb09ea0dc5e2, 4a4598daf841035c7b729d4e4563d80d49a146db21cf8942ee279d1d68a82cbe, 49f56b8936b521c48d63d86a8275aac0cd411d4b48d867f4fe1d337f9ef4b1a6, 49725de88a7c45759581226304c1ebfa326c1bf92faca8e7bf46b29bd75f0da2, 4941977ec3177221cee1ea76995674695f116db9579f2435125159538072c7a7, 48f5f14263ddf276109dd65250d332ae6ad052854f4a729491446048801 47f45, 47a25cec4ff0e19a643cce916a546a51ec57f76e8de8fe52661bb56894a84842, 46afd08ef4564bb7f4e2a61ff95003f485260a05733ee032b4dcc33d74ce926b, 4673d0c47e9a73582ef27dc3b7d3b1b1ff6cba53ea245d2f69e7960502b89304, 45d44d4817a51b97aa24cee96f7dc287d1b66790243454e5ecec16ad297eadbc, 45091fce0cfbb124fdf1380876e5c15699df35a5d3d7804560500fbe7adc574f, 448a6529d7dd07aa8a6073897a39d7d96b2d69a9dbb8ef3d2729b7558c02bd3c, 4402195d27c944d4e85a1fe0abc140e359aeb072d7ab8e2c404d6773c4c2da32,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	4339a0846be069f767685bd715a1d0e9d8237b85c23c544cdea153752b9d68d7, 42f91e85c5455738328206a3db07749715e3f32c099c7a0aafa8c2f3a6eeee38, 42113cfd76dc6ce3cbce371a01350f8cd108cfbe091374583fa26d7681f10a67, 41ceee9389e76a985617d8207f9079dd772b5837b6603a50c873978316969724, 41ca167bdbe6a0d9bf095e377a0f267c70d38220f9f1850238c6f62ec8dbb455, 3fec661b5d5db34fc55e41ec988511b84c7fb02248a419b56eec6652d3de1afd, 3eaf76e4c615088db086584ce37a42175623c4870789d36bb312d334b479e188, 3d98eea8be0266f0b7a061af4b02023d0b9e9c8c68fcf04b4c7c0143942b8330, 3cf561d7d28482aa706e0f09df3e0cae6e2f3b72d4aeeeff137780d1819ac5a1, 3bf0d59b9272ea9fdc0cd18f77bde8ca6efde2ab968c637841b4f59bde0b17f0, 3b94c2396fe7702db920b31eed93e6aa81a7c99ccee33f77bb78dedae320e72b, 3b94a080ebefba440f507cb2e6795aa451cd73570a6116a23de1b813b249296c, 380382cfc8f302294fdd806cba715149548026781db866539f2efcd72046f317, 3736d2dcdfd021fb5e6e1a4c527a7468b045e6cdb1f8fe5547b9e332426b80bb, 371222c41f87e6546ee10dbb34be7eab08f1a68a3de857bb1b5f28543e835d63, 351892dba00cd338ccb2b403442abc5fa89a61bb9c4e566137fd33a3f6570988, 342c80bbe3780c002a26ad0c56092e98dca0691f3d28fd4f568d3866997c9869, 31adc1bbf10b7d7c6295837cc9ccfb20cdd0ab5755d570b24e4b5ee078b704c9, 317e73c447b5f3b4b0fdaff58122b35b0cb4433a9ccd89aee3eab8a1255b3c6e, 30d06e55c4cd9a877e567b7358f14e7fe9cf9e09bfdf6c1bde90320e31fb5bb9, 30a28b00785f89e379cb0b1eac98f18663af618b42485fa7740a3ea3acb3a9ae, 2f7b9edd8d10b438b6a807869fc16accfdc5043b1dbf0cc48a49df3c5dfee3ce,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	2c74a1fc5d8c05d7751fa0d405ecb7f7a065e07bce35eb6906521decdbadace4, 2c1820576d8170eb2153300a6566e2ce61c5d9a8eec55d114f56bec49057386f, 2c027b0fadc8f6b42eecb49c37ef3ad45b35a7368e9560bc31bc0f6bc417eddc, 27e5615e928a07b2e35ad6d63795b5f8189af6f2130d5f69e9229b32059f1ee7, 27564b732c52a37b66af2609c2d1c943288f57683c64c82ff1bc066f88b34f34, 273866490a6ab7ae49601613caab7af9e53e62c880dd0a9cf2f0f31da9feca96, 2611a1c953e494b507e72371064c8a8a1a9f169c27043e8995f058f1c0d4f012, 25e87ce18542710125c3f158a762312e43404520e199e8fc47ba3aa1b40f71c9, 243cfd323e4d5f25b981841fd6c307fc02f405b68faa0b8e5d7395de01f3e856, 241541a1c8cb2ebf1b14e191ad1a13bd6ec85829d78e138fa11960334b746c2b, 20567b83523751ac0788fbed7cba1c694d4b52649beaff584b9f16afc764e875, 1f1e0c851dd748276586a628fb70fe33a23c09227696c3ee0e170c657f20c773, 1ed7b76e6fcc6deb6e34c3beb31e271924225b250a3f7aa6d5aa82f94dd4531e, 1e0956bcb231114e80eee9c52bd48ee9f3ea19229a82de1e1182bfb0ac613de6, 1c8920973cfa14fafcc7d97a3cb5a43d8e713a0f50faa2738be7c61af21a4832, 1b123cd6be4305682aa31e286a6614beeb3704a58af90983f336a87016a236d1, 1a814c66444f11b4872ac0c337a1f65204b294c3d14b27ae85fc351f23a8f397, 19f2d5f8d12fd40b1d76babf7cf7732f6edeb886774fec3feada4e931a01c80f, 18c838e58692a2a16c0a775d0c7a3f602974f1625c2fb6f4c549b943697cc06c, 180005e1e6797c79fd6290bb11bc1f40b34c822a18654ca85e1ba74d96834059, 16fdf2e67d09240a26540d00658f7ca895d4bd899620f1e8f05da2bf2e35d614, 14e519558a6b06a283d670c3714aa54a01c8f35cdf47b2d567ccaff9cdb872a9, 14a1bae6bcd0ab3128a5b78b432fc855cced7df0205cd4d137ea80c8f61efcf8,

Attack Name	TYPE	VALUE
PlugX (aka Korplug)	SHA256	147a2f1250cf77932d2b2b099ae3680d79c1c659022200d536e8cdb13687a3d2, 13dc3cf913f40404eb0a6c89f6ed10559960924e1299fd2982da8c85dd43f6bb, 125a8c001a068036585c31885e362a751fddb8d9f570b3b01c8a4176351270ef, 11e3c5cc49b00d25641be96f837cb3a440be07a9030755903f0e4c0002bc8290, 0f7f3400b1b951e10acf5590d5ac9e1a85eda1e72fe2b4dd041a99c4b14d1c9b, 0f72daf30f593f4aff633453fbf7adf4eb6715578069f0bc126929a7f987f0d6, 0f51ac9d4f1a244b2fe68aa7a6205f20974d46fc075dd29d0c99ba4f84448e7f, 0e8697af2fe695e9cd8c2de149d37720a160703becb991e2b9c697ce4b7a0f0d, 0db594e6ab9a3712df9b739abf3c5b0f9107e72c95907af5870f15ec8501e7d4, 0c42ad1d178b241d497e2eefe7472c604af6a439971f358209cbd828116ee759, 0c18d65acaa18942b8d8f2a543afd3e6acc6326c600c699e0c699b2574cb9835, 0bb95a479871eb067b8dd782a2e2c099f8aec1070642fad21a728469a59a2c2b, 0b2d9d4edc773a8bbd4a4d908858383fc76b32a494894081d10c91d022b0957e, 09290d70fedb87a60828b05ff5c83c368bbd8eaba15153ee7952dabc2ef2bab7, 08851f21919f814520d4a2847783815657a7120bc6533fd5f702f84949a27522, 077c579784ea2965d5bf2c930f698d86a97e8c24a06889c5a418da3f4ef704af, 07320727c0bb45b54f4d50e128378f7eda3d9069936d2a2de5599b63d0bdf2c9, 01fdcaea7aeb248b39306c208e99591d6210f3c0a0735e9bbf007f1525e92ad1, 017222f47ad94cb527031f4ceb06ae77607b1ebd11dc0b83b6eb17da531a267d, 00a710722e0b1aea3d2b8b0221567b39222ba1f810ee716eaf1036193552c19c, 009c73597f79472eba2715fc634bd78bd2bc9a21e05b7b4cfcb64a3beb5fe03a

Attack Name	TYPE	VALUE
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, 275d63587f3ac511d7cca5ff85af2914e74d8b68edd5a7a8a1609426d5b7f6a9, 5cda94180b245de8421f226eb516d0aa1d3fd8167ebed4fa06070dd38344cec0,

Attack Name	TYPE	VALUE
Noodle RAT	SHA256	61f34459815eb403ec841246a4277d825dcd25700baad867b61ec3166d034825, 67e60fca3d28dcae09b74ffd62f5efe462700b6d2b3334d519e4caac55820df0, 3bff2c5bfc24fc99d925126ec6beb95d395a85bc736a395aaf4719c301cbbfd4, 88b4904a582522d9a91fb4ad616adbd432c556b17427cfb177c8205f484792ba, bf5ea570bf4d18e60dd758a2461fbdf73a500dbd179e458aca81d65b5d9155e1, 7440a7b56d3670d4204a57974fa76ae76ca78168bb181640f565976d192cc159, 1e9add97a289de7f5679aceace7a3a39437a33254ac9c217d9a530e9369f60be, cac63e105d73d59c7f83779005ada0a4d3f7fb072cfc2c9590b64fe3896d2e3e, 5b4c421edb3571dbc7d581596a9ac952e453394b30132dec8e390ec561cd4abb, 3893f8a44a2d1fef45354984f3c6906ae8627c6f0c489f6f14e8da03197312ae, 0153c9e22428f08597fe87cb8bd6664f6481e05bbf4e3d4174f44d2524446bdb, c4fb9757ed6db6ab2bd4253cb8a1542a590443654260f2b947c288d5717487d6, 70b19172b743973a45f5d707d4eec4f8508d41aa684516f1fb8c75bec59d02bb, 96231be4cc6cf256eebd828af4338588272ea478c609a7f16a03bdf1a61dd431, bf553e82119e2483d36eff51cf152861938c584749ebc005d4d612876277b787, 7b07b722091d9658fe106448b6e1c6b7484d7b7d163ddeb19132174973b62759, b21f4039707eb4fc40ad1a7ed10be753ab3922c4a60bde819dcd74d44fef991d, 4c4d51b377faebf61f95663765e622eb652866ab9cc7e9964a5d02f4dc0b53d3, b24e160843d96c6d75452d6f4e379b73a417fc821b26ca85d740ca0a499615ab, e5fb5a3b8663fbb2686caf88fdb3362115dc0f0bf9cc5d32d1e42c00aa6660b4, d17d964cacb063a6fe685d6e5e7dbc02c597de51b46c994f0aadb56c3bf96f13, ba45dfa8e6b86140e526959c8568824ddd743d418231440d48740e76a33610ea, 1c2bbab6c496b66b108dc810649c19319655a2246f7fc6cf2a0911f5d73f2f3a,

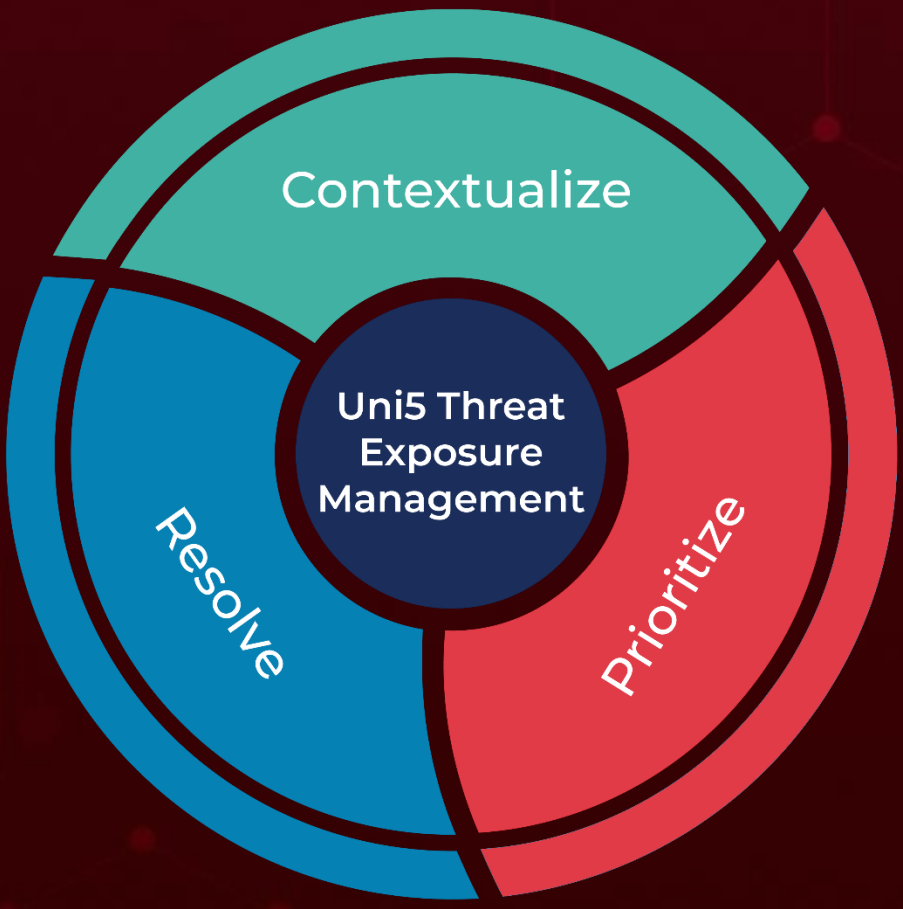
Attack Name	TYPE	VALUE
Noodle RAT	SHA256	14f9a20356fc0e1806524057e8366d994831e3568cf438694a5c4d5463c25010, 7e7bfe7e83867defa9280c8bce98cabcd0e6410cac7cc9a1baa88131b4a263b1, 45b3d192ed79541a9711c16c7d73bd4d0a74598ecb7b56416f8754fb5d6feb56, 53cebf50348e4507e92d23cfe3bbc87d6bf50e06962462d036542c37a50a23c1, a27d133f6a1bd72285f021403082dc8e47180fe56e88b274f474459088857603, 4198efb00840f440d96987518bd80dbc90cde3023bc8c2b0aae456af07875405, abdbbc10467421b93fe1df6da0de70a4d454adcced1bfc6c1cebf1207fba93db, bcac1d42c39932fb20f571655cd1bbe507c3fddda63d4f0ea8986a3dd5265f41, 68389b48c6f15b6da7f2d78c0864d6b9b9135f6ace3564d29b26f5dc9b5d6313, bf1b88385aebb37182421e967749f057fbefb4e4386bb47b5098abac7c70c476, 1a9ff06ac18f57a6382fdae54bf8735a6ad7d9c9f1f9aa0dfff0e3e828f1820b, 15f3536ac33588444cf6a632f17c74ee0ee8777d0d2166206222b4d5f66de715, ca2200ef6ce1abc37e5778b40e9b14031b81014560dae9c6a16fd7ba948c7656, bbcfc826f614433ff1b7c8031349cf5b411d868b07259eca9c19cd5af772b85e, 6933a01980378c2160740e5cecaba29530555e3d65bd89ef80db49419a419f8d, 5dac572374cb40561ea5dbc0dfc963d863f08862a0bd33fdac6ac8d0aa180ada, 24a827336a1f942925fd57e763109e3a83b1a5762c077c1e80bd057bb1b15bad
Fickle Stealer	SHA256	e9bc44cf548a70e7285499209973faf44b7374dece1413dfcdc03bf25a6c599c, a641d10798be5224c8c32dfaab0dd353cd7bb06a2d57d9630e13fb1975d03a53, 9ce52929765433ff8bf905764d7b83c4c3fcbefb4f12eabcf16ee3dddcd3759d, b7bdb0cc90b11c4738c2af218a1a53e4c65b6c91c6067c224164b8fcfc3eed8c, f878a88b7dda1155fe939abe0500e32d5fba34569ca933bccb5603d9e0e96cc0,

Attack Name	TYPE	VALUE
Fickle Stealer	SHA256	bfe2d817e20ecff45cc92b7b8f4e1cd0482b48a769940402eaa5b31cbfb9b908, 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

What Next?

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

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



REPORT GENERATED ON

June 24, 2024 • 6:45 AM

More at www.hivepro.com