Date of Publication
March 28, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

20 to 26 MARCH 2023

Table Of Contents

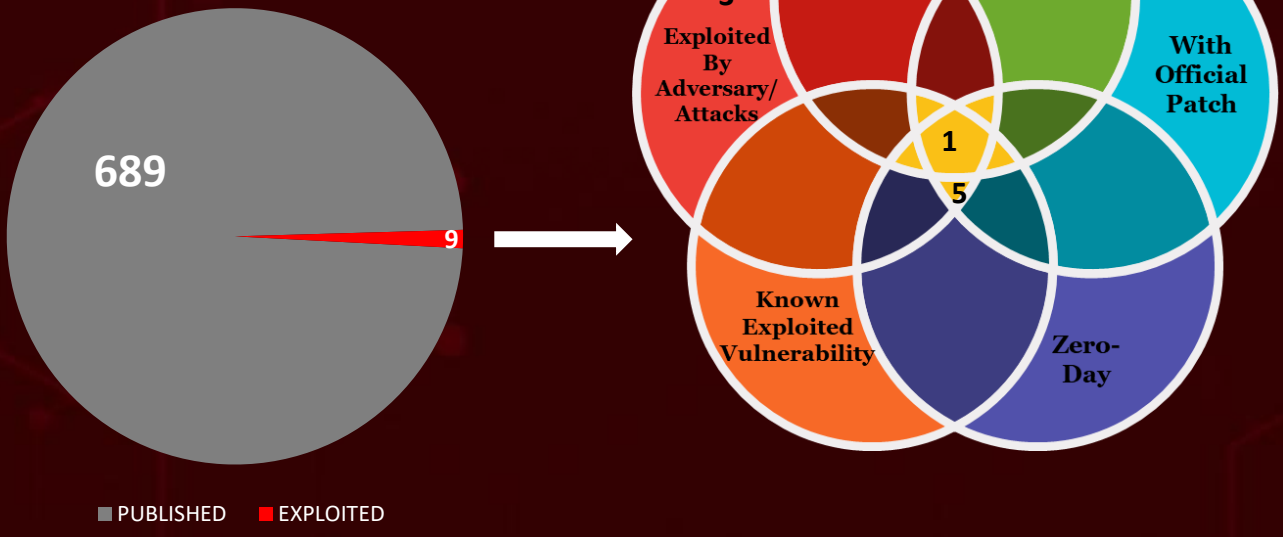
Summary

HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, they identified a total of **19 attacks** that were executed. These attacks were taking advantage of **nine** different **vulnerabilities** in various systems. Additionally, HiveForce Labs identified **five** different **adversaries** that were actively carrying out these attacks.

Interestingly, **two** of the vulnerabilities that were being exploited had not yet been **patched**. These two vulnerabilities were being targeted by the **Hinatabot** Go-based botnet.

Moreover, HiveForce Labs also found that **UNC961 (Prophet spider)** was exploiting a group of **six old vulnerabilities** to carry out attacks. Furthermore, they identified two new actors called **Bad Magic** and **Winter Vivern** that were involved in recent attacks.

Apart from these threats, there was also an increase in the number of **macOS malware** attacks over the past week. These attacks included **CloudMensis**, **DazzleSpy**, **EggShell**, **KeySteal**, **Poseidon**, **Pureland**, **Xloader**, and **Zuru**. All these attacks were observed to be on the rise, posing a significant threat to users of macOS systems.



High Level Statistics

19
Attacks Executed

9
Vulnerabilities Exploited

5
Adversaries in Action

- Chinotto
- HookSpoofer
- Gozi
- HinataBot
- PowerMagic
- ShellBot
- Mispadu
- ALC
- CloudMensis
- DazzleSpy
- EggShell
- KeySteal
- Poseidon
- Pureland
- Xloader
- Zuru
- BlackGuard
- Cinoshi
- APERETIF

- CVE-2017-17215
- CVE-2014-8361
- CVE-2022-41328
- CVE-2021-44228
- CVE-2021-26084
- CVE-2019-19781
- CVE-2021-22205
- CVE-2017-7504
- CVE-2020-14750

- Reaper
- UNC3886
- Bad Magic
- Winter Vivern
- UNC961

Insights

9 Years Old vulnerability got exploited

Multiple **macOS** Malware on the rise

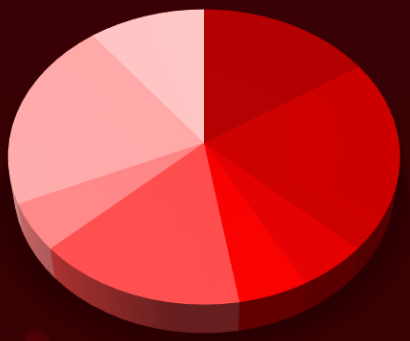
6 Zero Days exploited in the wild

FortiOS Vulnerability was exploited by UNC3886

Prophet Spider Exploits old vulnerabilities to target North America

3 Vulnerabilities has no patch available

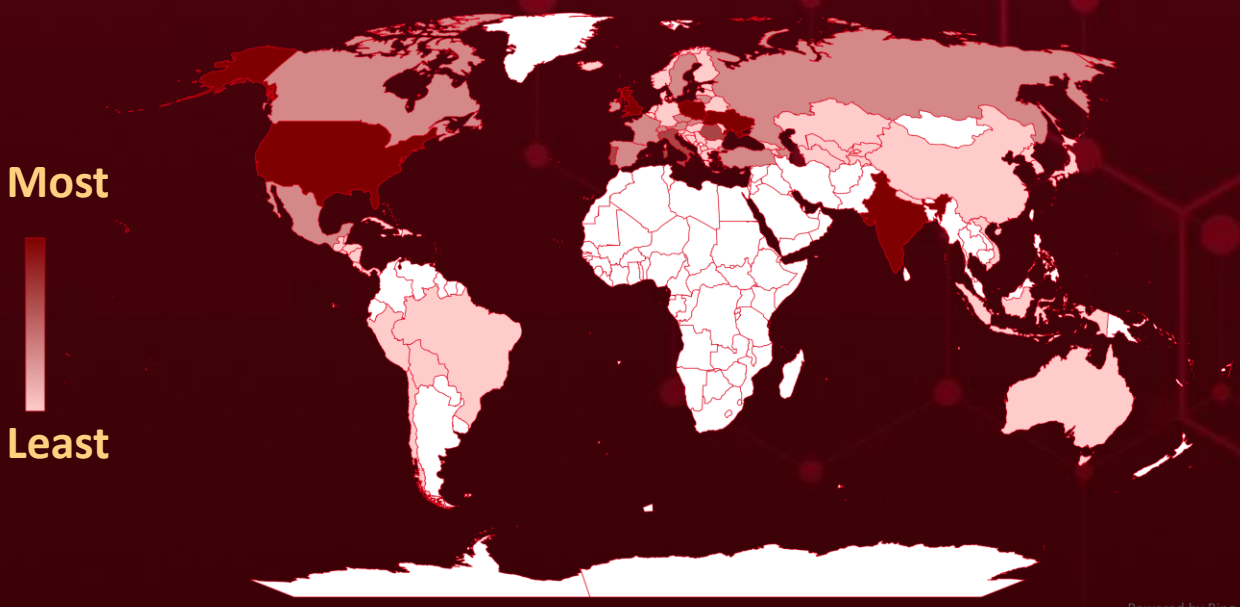
Threat Distribution



- Backdoor
- Botnet
- Trojan
- RAT
- Point-of-sale
- Information Stealer
- Loader
- Scareware
- Malware-as-a-service

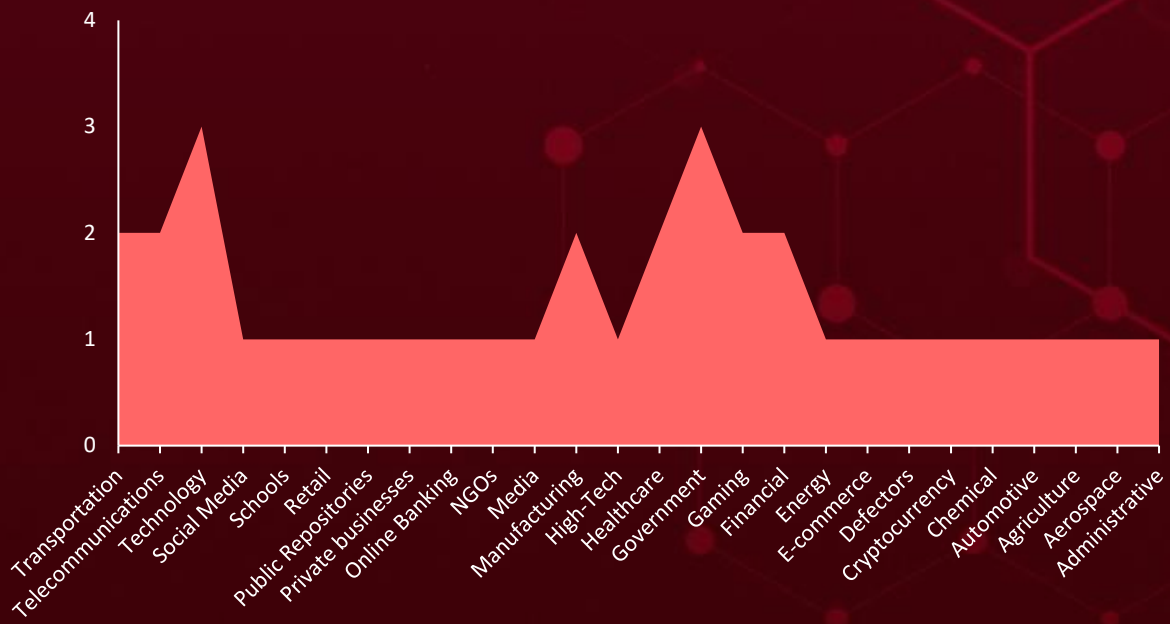
6 Vulnerabilities are tagged as KEV by CISA

Targeted Countries



Countries	Countries	Countries	Countries	Countries
Poland	Czech Republic	Bulgaria	Cayman Islands	Panamá
Ukraine	China	Denmark	Île de Clipperton	Puerto Rico
India	Finland	Luxembourg	Costa Rica	Saba
United Kingdom	Monaco	Estonia	Cuba	San Andrés
United States	Bolivia	Malta	Kòrsou	Saint-Barthélemy
Romania	Norway	Uzbekistan	Dominica	Saint Kitts and Nevis
Italy	Georgia	Vietnam	República Dominicana	Sainte-Lucie
Portugal	Belgium	Kazakhstan	El Salvador	Saint-Martin
Spain	Germany	North Korea	Dependencias Federales de Venezuela	Saint-Pierre-et-Miquelon
Russia	Gernamy	Vatican	Kalaallit Nunaat/Grønland	Saint Vincent and the Grenadines
Cyprus	Nepal	Kuwait	Gwinàd	Sint Eustatius
Switzerland	Greece	Albania	Gwadloup	Sint Maarten
France	North Macedonia	Kyrgyzstan	Guatemala	Trinidad and Tobago
Azerbaijan	Holy See	Anguilla	Ayiti/Haïti	Turks and Caicos Islands
Ireland	Hong Kong	Antigua and Barbuda	Honduras	US Virgin Islands
Slovakia	San Marino	Aruba	Jumieka	
Turkey	Hungary	Bahamas	Martinique/Matinik	
Sweden	South Korea	Barbados	Montserrat	
Lithuania	Iceland	Belize	Nicaragua	
Austria	Tajikistan	Bermuda	Nueva Esparta	
Mexico	Andorra	Boneiru		
Canada	Moldova	British Virgin Islands		

Targeted Industries



TOP MITRE ATT&CK TTPS

T1071
Application Layer Protocol

T1059
Command and Scripting Interpreter

T1082
System Information Discovery

T1036
Masquerading

T1560
Archive Collected Data

T1027
Obfuscated Files or Information

T1573
Encrypted Channel

T1547.001
Registry Run Keys / Startup Folder

T1518
Software Discovery

T1204
User Execution

T1056
Input Capture

T1547
Boot or Logon Autostart Execution

T1057
Process Discovery

T1140
Deobfuscate/Decode Files or Information

T1113
Screen Capture

T1552
Unsecured Credentials

T1497
Virtualization/ Sandbox Evasion

T1566
Phishing

T1021
Remote Services

T1059.001
PowerShell

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Chinotto	Chinotto is a malware with variants for Windows, Android, and Powershell, and can communicate with its command-and-control server using HTTP commands.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Control and Exfiltrate Sensitive Information	-
ASSOCIATED ACTOR			PATCH LINK
Reaper			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
HookSpoofer	HookSpoofer is a novel Infostealer with keylogging and clipper capabilities that is spreading through bundlers. It is an enhanced version of Stormkitty, written in C#, and includes anti-analysis strategies to avoid detection by VirtualBox, Sandbox, Debugger, VirusTotal, and Any.Run	Bundlers	-
TYPE		IMPACT	AFFECTED PRODUCTS
Information Stealer		Exfiltrate Sensitive Information	-
ASSOCIATED ACTOR			PATCH LINK
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Gozi	Gozi is a binary that bypasses Italy's geofencing and creates a loader process on the victim's computer.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Financial losses and compromised personal information in Italian individuals	-
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
HinataBot	HinataBot is a large Go-based malware recently discovered in HTTP and SSH honeypots. It is named after a character from the anime series Naruto and utilizes various communication methods, including dialing out and listening for incoming connections, and has been observed with distributed denial-of-service (DDoS) flooding attacks using protocols such as HTTP, UDP, TCP, and ICMP.	old vulnerabilities and weak credentials	CVE-2017-17215 CVE-2014-8361
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		distributed denial-of-service (DDoS)	Huawei HG532 routers; Realtek SDK
ASSOCIATED ACTOR			**PATCH LINK**
			No patch available

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PowerMagic	PowerMagic, a PowerShell backdoor, is used as a loader for the CommonMagic framework, which consists of several executable modules and communicates via named pipes. The backdoor communicates with the C&C server, downloads and executes commands, and uploads results in response.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Exfiltrate Sensitive Information	-
ASSOCIATED ACTOR			**PATCH LINK**
Bad Magic			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ShellBot	ShellBot, also referred to as PerlBot, is a DDoS Bot malware that uses the IRC protocol to communicate with its C&C server. Developed in Perl, it has been in use for a long time and continues to be utilized to launch attacks against Linux systems.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		denial-of-service (DDoS) attacks	-
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
Mispadu	Mispadu is a malware-as-a-service and has been linked to various spam campaigns, and it is capable of stealing both monetary and credential information while acting as a backdoor through keystroke and screenshot capture.	Malvertising and Spamming campaigns	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Cause Financial and Credential Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ALC	ALC is a scareware posing as ransomware, as it does not encrypt files on the victim's device. ALC merely disables the task manager and displays a ransom notice on the locked screen.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Scareware		Disables the Task Manager, Locks 5he Screen, and Displays a Ransom Note	-
ASSOCIATED ACTOR			**PATCH LINK**
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CloudMensis	CloudMensis (BadRAT) is distributed as a malicious Microsoft Word document, which executes a macro when opened, allowing the attacker to gain remote access and control of the victim's computer.	malicious Microsoft Word document	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Remote Access Trojan (RAT)		Exfiltrate documents, keystrokes, and screen captures	-
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
DazzleSpy	DazzleSpy is a highly sophisticated piece of malware that evades detection and maintains a foothold on infected machines. It installs a LaunchAgent that masquerades as an Apple launch service and targets an executable called "softwareupdate" to maintain persistence, while containing code for searching and writing files, exfiltrating data, and running shell commands.	unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Remote Access Trojan (RAT)		Data Theft, Compromise of Sensitive Information, and Potential Financial Losses	-
ASSOCIATED ACTOR			**PATCH LINK**
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
EggShell RAT	EggShell RAT is a free and open-source RAT that allows attackers to gain remote access and control of a victim's computer, making it a popular tool among cybercriminals.	via social engineering tactics	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Remote Access Trojan (RAT)		Gain unauthorized access to sensitive information	-
ASSOCIATED ACTOR			**PATCH LINK**
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
KeySteal	Keysteal is a malicious app designed to extract user passwords and other credentials stored in macOS Keychain without administrator privileges.	Via malicious app	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Remote Access Trojan (RAT)		Compromise sensitive business 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
Poseidon	Poseidon is a malware that uses spear-phishing attacks to gain access to targeted organizations, installs malware on their networks, and steals sensitive information, particularly intellectual property and trade secrets.	via spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Point-of-sale		theft of valuable commercial information and intellectual property	-
ASSOCIATED ACTOR			**PATCH LINK**
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Pureland	Pureland InfoStealer is designed to steal sensitive information, such as login credentials and personal information, from victims. It is often distributed via phishing emails and is capable of evading detection by antivirus software.	via spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft, Compromise of Sensitive Information, and Potential Financial Losses	-
ASSOCIATED ACTOR			**PATCH LINK**
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XLoader	XLoader is a macOS malware that targets organizations using Java applications, such as online banking. Its keylogger and info-stealing capabilities make it attractive to criminals, but its implementation on macOS is clumsy and likely to raise suspicions.	via spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		Compromise sensitive information on infected devices, potentially leading to financial losses, reputational damage, and legal consequence	-
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
Zuru	Zuru is a macOS malware that spreads through trojanized versions of various backend tools used for SSH and remote connections. It surveils the local environment, connects to a command-and-control server, and executes remote commands via a backdoor.	trojanized versions of iTerm2	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		data theft, financial loss, and damage	-
ASSOCIATED ACTOR			**PATCH LINK**
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlackGuard	The BlackGuard stealer malware spreads via removable media and takes over cryptocurrency wallets, while also being able to pilfer sensitive data from multiple applications and support the theft of popular cryptocurrencies.	removable media and hijacks crypto wallets	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		data theft, financial loss, and damage	-
ASSOCIATED ACTOR			**PATCH LINK**
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cinoshi	Cinoshi is a novel Malware-as-a-Service (MaaS) platform. Cinoshi's toolkit includes a stealer, botnet, clipper, and cryptominer. This MaaS platform is promoting stealer and web panel for free, which is unusual.	unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Malware-as-a-service		data theft, financial loss, and damage	-
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
APERETIF	The APERETIF trojan automates the collection of victim information, maintains access, and communicates with the actor-controlled domain marakanas[.]com through beaconing. It uses whomami within PowerShell for its initial activity.	compromised WordPress websites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		data theft, financial loss, and damage	-
ASSOCIATED ACTOR			**PATCH LINK**
Winter Vivern			-

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-2017-17215	ZERO-DAY	Huawei HG532: All versions	-
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:huawei:huawei_hg532:*:*:*:*:*:*:*:*	HinataBot
Remote Code Execution Vulnerability in Huawei HG532 routers			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	No Patch Available

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2014-8361	ZERO-DAY	Realtek SDK: All versions	-
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:realtek:realtek_sdk:*:*:*:*:*:*:*:*	HinataBot
Remote Code Execution Vulnerability in Realtek SDK			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	No Patch Available

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-41328		FortiOS: 6.4.0 - 6.4.11, 6.2.0 - 6.2.13, 6.0.0 - 6.0.16, 7.0.0 - 7.0.9, 7.2.0 - 7.2.3	UNC3886
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:6.4.0:*:*:*:*:*:*:*	-
Privilege escalation in FortiOS			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1068: Exploitation for Privilege Escalation	http://fortiguard.com/psirt/FG-IR-22-369

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228		Apache Log4j: 2.0 - 2.14.1	UNC961(Prophet Spider)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	-
Apache Remote Code Execution Vulnerability (**LOG4J**)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917 CWE-20 CWE-502 CWE-400	T1027: Obfuscated Files or Information; T1562: Impair Defenses	https://logging.apache.org/log4j/2.x/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26084	✗ ZERO-DAY	Atlassian Confluence Server: 6.0.1 - 7.12.4	UNC961(Prophet Spider)
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:atlassian_confluence_server:*:*:*:*:*:*:*:*	-
Atlassian Confluence Server Arbitrary Code Execution	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	https://jira.atlassian.com/browse/CONFSERVER-67940

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-19781	✗ ZERO-DAY	Citrix NetScaler Application Delivery Controller: 10.5 - 13.0	UNC961(Prophet Spider)
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:citrix_netscaler_application_delivery_controller:*:*:*:*:*:*:*:*	-
Citrix Application Delivery Controller and Citrix Gateway Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1562: Impair Defenses	https://support.citrix.com/article/CTX267027

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22205		Gitlab Community Edition: 11.9.0 - 13.10.2 GitLab Enterprise Edition: 11.9.0 - 13.10.2	UNC961(Prophet Spider)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gitlab:gitlab_community_edition:13.10.2:*:*:*:*:*:*:*	-
GitLab Community and Enterprise Editions From 11.9 Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1027: Obfuscated Files or Information; T1562: Impair Defenses	http://about.gitlab.com/releases/2021/04/14/security-release-gitlab-13-10-3-released/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-7504		JBoss Application Server: 4	UNC961(Prophet Spider)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:red_hat:jboss_application_server:4:*:*:*:*:*:*:*	-
JbossMQ HTTP Invocation Layer deserialization vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502		No Patch Available

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-14750	✗ ZERO-DAY	Oracle WebLogic Server: 10.3.6.0.0 - 14.1.1.0.0	UNC961(Prophet Spider)
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:oracle_weblogic_server:*:*:*:*:*:*:*:*	-
Oracle WebLogic Server Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1014: Rootkit; T1037: Boot or Logon Initialization Scripts; T1080: Taint Shared Content; T1542: Pre-OS Boot; T1543: Create or Modify System Process; T1546: Event Triggered Execution; T1547: Boot or Logon Autostart Execution; T1553: Subvert Trust Controls; T1562: Impair Defenses; T1569: System Services; T1574: Hijack Execution Flow	https://www.oracle.com/security-alerts/alert-cve-2020-14750.html

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Reaper (APT 37, Ricochet Chollima, ScarCruft, Thallium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10)</td><td>North Korea</td><td rowspan="2">Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, Transportation, Defectors, NGOs</td><td rowspan="2">China, Czech, Hong Kong, India, Japan, Kuwait, Nepal, Poland, North Korea, Romania, Russia, South Korea, UK, USA, Vietnam</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Chinotto</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1212: Exploitation for Credential Access; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1056: Input Capture; T1056.001: Keylogging; T1113: Screen Capture; T1584: Compromise Infrastructure; T1584.006: Web Services; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys/Startup Folder; T1140: Deobfuscate/Decode Files or Information; T1033: System Owner/User Discovery; T1082: System Information Discovery; T1560: Archive Collected Data; T1560.002: Archive via Library; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC3886	China	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-41328	Chinotto	Firewalls, IoT devices, hypervisors, and VPN
TTPs			
T1565: Data Manipulation; T1565.001: Stored Data Manipulation; T1027: Obfuscated Files or Information; T1070: Indicator Removal; T1070.003: Clear Command History; T1070.004: File Deletion; T1078: Valid Accounts; T1140: Deobfuscate/Decode Files or Information; T1202: Indirect Command Execution; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1222: File and Directory Permissions Modification; T1497: Virtualization/Sandbox Evasion; T1497.001: System Checks; T1620: Reflective Code Loading; T1552: Unsecured Credentials; T1555: Credentials from Password Stores; T1555.005: Password Managers; T1016: System Network Configuration Discovery; T1033: System Owner/User Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1087: Account Discovery; T1518: Software Discovery; T1074: Data Staged; T1074.001: Local Data Staging; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1059.004: Unix Shell; T1059.006: Python; T1129: Shared Modules; T1095: Non-Application Layer Protocol; T1102: Web Service; T1102.001: Dead Drop Resolver; T1105: Ingress Tool Transfer; T1571: Non-Standard Port; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1021: Remote Services; T1021.004: SSH			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED CITIES
	Unknown	Administrative, Agriculture, and Transportation	Donetsk, Lugansk, and Crimea (Cities in Ukraine)
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
Bad magic	-	-	-
TTPs			
T1070.004: File Deletion; T1027: Obfuscated Files or Information; T1566.001: Spearphishing Attachment; T1204: User Execution; T1560: Archive Collected Data; T1560.002: Archive via Library; T1112: Modify Registry; T1012: Query Registry; T1083: File and Directory Discovery; T1204.001: Malicious Link; T1036: Masquerading; T1036.007: Double File Extension; T1218: System Binary Proxy Execution; T1218.007: Msiexec; T1546: Event Triggered Execution; T1546.016: Installer Packages; T1027.009: Embedded Payloads; T1070: Indicator Removal; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1113: Screen Capture; T1140: Deobfuscate/Decode Files or Information			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	Unknown	Government, Telecommunications, and Private businesses.	Azerbaijan, Cyprus, Poland, Lithuania, India, Vatican, Ukraine, Italy, and Slovakia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
Winter Vivern (UAC-0114)	-	APERETIF	-
TTPs			
T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1137: Office Application Startup; T1055: Process Injection; T1055.011: Extra Window Memory Injection; T1036: Masquerading; T1497: Virtualization/Sandbox Evasion; T1202: Indirect Command Execution; T1010: Application Window Discovery; T1018: Remote System Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1071: Application Layer Protocol; T1095: Non-Application Layer Protocol; T1573: Encrypted Channel; T1071.001: Web Protocols; T1497.003: Time Based Evasion; T1564: Hide Artifacts			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED CITIES</th></tr>
<tr><td rowspan="3"> 
UNC961(Prophet Spider)</td><td>Unknown</td><td rowspan="2">Energy, Financial Services, Healthcare, Manufacturing, Media, Retail, Technology, Telecommunications</td><td rowspan="2">North America, India, United Kingdom, United States</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage; Financial Gain</td></tr>
<tr><td></td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td></td><td>CVE-2021-44228
CVE-2021-26084
CVE-2019-19781
CVE-2020-14750
CVE-2021-22205
CVE-2017-7504</td><td>-</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1505: Server Software Component; T1505.003: Web Shell; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1069: Permission Groups Discovery; T1069.001: Local Groups; T1069.002: Domain Groups; T1016: System Network Configuration Discovery; T1033: System Owner/User Discovery; T1049: System Network Connections Discovery; T1140: Deobfuscate/Decode Files or Information; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1059.004: Unix Shell; T1543: Create or Modify System Process; T1543.003: Windows Service; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1105: Ingress Tool Transfer; T1197: BITS Jobs; T1112: Modify Registry; T1070: Indicator Removal; T1070.007: Clear Network Connection History and Configurations; T1047: Windows Management Instrumentation; T1569: System Services; T1569.002: Service Execution; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1048: Exfiltration Over Alternative Protocol; T1071: Application Layer Protocol; T1071.002: File Transfer Protocols; T1021: Remote Services; T1021.004: SSH; T1572: Protocol Tunneling; T1135: Network Share Discovery; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1003.003: NTDS; T1482: Domain Trust Discovery; T1087: Account Discovery; T1087.002: Domain Account</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **9 exploited vulnerabilities** and block the indicators related to the threat actor **Reaper, UNC3886, Bad Magic, Winter Vivern, UNC961** and malware **Chinotto, HockSpoofer, Gozi, HinataBot, PowerMagic, ShellBot, Mispadu, ALC, CloudMensis, DazzleSpy, EggShell, KeySteal, Poseidon, Pureland, Xloader , Zuru, BlackGuard, Cinoshi,** and **APERETIF.**

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 **9 exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Reaper, UNC3886, Bad Magic, Winter Vivern, UNC961** and malware **Chinotto, HockSpoofer, Gozi, HinataBot, PowerMagic, ShellBot, Mispadu, ALC, CloudMensis, DazzleSpy, EggShell, KeySteal, Poseidon, Pureland, Xloader , Zuru, BlackGuard, Cinoshi,** and **APERETIF** in Breach and Attack Simulation(BAS).

Threat Advisories

Reaper, North Korean hacking group, targets defectors

HookSpoofer A Novel Infostealer with Advanced Capabilities

New HinataBot Go-Based Botnet with DDoS Capabilities and Mirai Connection

Gozi Malware Spreads through Fake Italian Revenue Agency Email Campaign

Winter Vivern with Pro-Russian Objectives Targets Government

UNC3886 targets technologies with custom malware and exploits zero-day vulnerabilities

Bad Magic APT employs new CommonMagic Framework and PowerMagic Backdoor

ShellBot Malware Targets Mismanaged Linux Servers

Mispadu Targets Latin America with MalSpamming

A Deserialization Vulnerability Found in Apache Dubbo

ALC: Is It a Scareware or a Ransomware?

Rising Trend of macOS Malware

New Variant of BlackGuard Stealer Malware Steals Sensitive Information and Crypto Wallets

A Financially Motivated Threat Group UNC961 Targeting North American Organizations

Cinoshi A Novel Malware-as-a-Service Platform

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 been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Chinotto	URLs	hxxp[:]//141.105.65[.]165/data/ hxxp[:]//141.105.65[.]165/files/ hxxp[:]//141.105.65[.]165/main/ hxxp[:]//141.105.65[.]165/support/ hxxp[:]//attiferstudio[.]com/install.bak/sony/ hxxp[:]//ri-guard[.]com/download/temp/cn-var/ hxxp[:]//koaagj.co[.]kr/files/2014/12/fix/ hxxp[:]//jdwanxiang[.]com/win/shenti/ hxxps[:]//clovery-shapes.000webhostapp[.]com/defcon/ hxxp[:]//hk-law.co[.]kr/data/file/joomla/ hxxp[:]//172.93.193[.]158/data/
	SHA256	e96a18b5837c7a7d83215d70ca10b84ee8c7b6e8dbd4d215586ec062d328ce86 1304fbeca197e4e67959c0b89b619cc109e4825d0da26ac41277eb34d2a19bc6 1409c4d0bd9a22a1e5adf016fffb83bbf3bd9f72ae0773780a409b980ed97763 6c1f0deadbfe5aede933592a9692b18879232a29bfdda5a666b91475b4746612 c9ea7afef5ac790297bdd0fb78c06186516957542e5da326075a0e2d230c27c1 a320ef003f43b28960043f95076c2066891e3a6a785476a2615a1f7b50a11c78 a88dc9a152cc7758a1df5aa33cf7b31cdb14e593a8744f2059602a49b8b04e0f 1fcf8bfcd70b97c6d3c9ac93602db4ee41a5d09f0a4b92fa67b76668fb33811d

Attack Name	TYPE	VALUE
Chinotto	SHA256	309cb38fbcd0132552fc739dd37d32c24b91ba712bebb9886d4638bceb2d8bf3 001e8e66fa4afc58cab23f5ee490f3080ef985c83d3b2a4555fc9c39cfe56bd8 3f0f0060bebd891008eaf8a647d91803107fc52294ceaab8b59b89958db4a0de 58cdb73495c2d6120f81f3752828f532b6a70ce7617b725e6989cf2d9cdb6aa4 5e67b5aed329e6545a36eff46bb6db8bdaa17841a4ec77228955d81872fed549 ccb6b0e02f7a9d7a541d0ed352706de943c178650a675eff667cb848ec0dc977 c0a36e340cc38c9abd07029e3d621395575c9a4a64459334ef84b623d1058865 40341da349e684593bbd01b244f94c28aa024ee49c3b3ebc89960e53e40750ae 9c30265e5b8f7b6017141815001a0678a99d05dc8302b50517c47d5f282b3c36 575631e9548b0f91addf3ce68bc5b4b9e86a17c069a221815062e1aa93d2978e cd2028bf873293aa330eb21ab96f8e71fa91e2d212852e81f292e769c0fba2d7 2a22da882f05dc159b055b01de7331e22fb6b5ce858308015a912b49487c56f0 b4a8d58b5d5e49d9d65b8b9faba344923cbac87473f2a32c646e359799ed655e 3d6c99e137bf5653134049caf9010d4c6d82360bf569ecca05fe15440d7fd0b0 ff5fc46c9598a5fbc9b54fbbd05ee0bb86549ecbba715093413326b58a1b9d2b b364bac52981edd74fbc45cca4216e66da5df9918000cc4617156ab42c914e7e b73ee977154402f8eecc5a446baf0dba456a37d1ca9348858540a8d048f3fd37 2fa36a4eb676f3afb1774224bc59041944ddfa4a3417630d01659ba3f0ced834 ead97a3920ff557299bcd4ccde1770c759263b93b70414258ec9030bbd0cb750 bdb33062bddd53043bab508e8e96b7c8353549d8eaa4b9004e7b3303e8a4e91b 0b6202a043f8dcf0690660c5c8f7a75f07336ca5576164295da34a569129548f 8078fc582b8f5eb81ef5d8da2b11fb4ce63f52fdeb1c2ceb3ac7a01113f9f3ee 60804ebbb655ea68b9e0bce63d5edbd03e0f75837f44539fec28dc12d44b5ba5

Attack Name	TYPE	VALUE
Chinotto	SHA256	e6d9c5a401a733ceb80b004deb347092affe572eda4e1ca6aa6c77bb0c6ea7e8
HookSpoofer	MD5	bd4345c3a7cc6f6e261986e1f5f1e8bc de90466d983da595e863339c34ee4b6b 7fce055a581c0b116a9679291bf89b7d 474e0cd6bc1f0fb71bbffa1ae7dd8e66
HinataBot	IPV4	77[.]73[.]131[.]247 156[.]236[.]16[.]237 185[.]112[.]83[.]254
	SHA256	01422e34b2114c68cdb6ce685cd2e5673bbe5652259a0c4b862d5de2824a9375 1b958fd718f1419700c53fed10807e873e8399c354877b0a3dfceac7a8581456 8a84dc2a9a06b1fae0dd16765509f88f6f54559c36d4353fd040d02d4563f703 4aba67fdd694219ff0dff07ebd444ed154edacc00c3a61f9b661eabe811a0446 71154ad6bd1a8a79fc674c793bb82b8e7d1371eca0f909c6e4a98ef8e7f5d1da c6a7e25290677cc7b9331343166b140f2c320764a815b241747e6913b1a386d9 92adfbe6aae06d7c99469aeb6551db8eee964b589f2b8774e29d987cfbd0e0d6 8eda08ce362c09b5f45772467f94d5370068c1798f78c5316f15647ac898c621 ff7638c0c893c021c3a059a21a71600249881afd84dc0d751d99db1c8edd3cac a3fac6fea9201c3c3eaae47bd95e0be93e91298e48df75540958834f9e75ac4d 9875bb9dd6d159a3b327de80e151ef7f3831c0d6833ae781490d68e426b73680 6ec35ef48ffdf9a92aa8845c336b327c280e1f20d7130ba0856540aed3233bbc C0aa34dd8dbf654d5230d4ef1db61f9befc89a0ea16cb7757edbf8a8090c9146 5643bf01e113de246575a9ec39ea12a85f9babb6ac069132ad8d1a7bfa56ed1b 845134ee7335f07b23e081f024cad5cbfc9ef453d6e2adc7970d6543292e5bcc 995681f388f5e0a405c282ae9ce22dc41f2249f0f5208254e1eec6e302d7ad7d 07326cce5325eabbe1caa2b3f8a4ab78e7913b65703c0afc3bab808441c30688 61181b4b7b7040ce4ab9c489a2b857f5a7fe8407c422327fff798f3b55e0cbe3

Attack Name	TYPE	VALUE
HinataBot	SHA256	75c050580725279a6592eecc2b02b6fa78f5469c2f08fb1d0e2fe616beb8bf0d E3427838132b6161f10e77d0beca1beac90c63a8ccc4aabd523041aec25aab67
Gozi	SHA256	a3cec099b936e9f486de3b1492a81e55b17d5c2b06223f4256d49afc7bd212bc c99f4de75e3c6fe98d6fbbcd0a7dbf45e8c7539ec8dc77ce86cea2cfaf822b6a 9d1e71b94eab825c928377e93377feb62e02a85b7d750b883919207119a56e0d ebea18a2f0840080d033fb9eb3c54a91eb73f0138893e6c29eb7882bf74c1c30 df4f432719d32be6cc61598e9ca9a982dc0b6f093f8314c8557457729df3b37f 061c271c0617e56aeb196c834fcab2d24755afa50cd95cc6a299d76be496a858 876860a923754e2d2f6b1514d98f4914271e8cf60d3f95cf1f983e91baffa32b
	IPV4	62[.]173[.]141[.]252 31[.]41[.]44[.]33 109[.]248[.]11[.]112
PowerMagic	SHA1	b63d4c3618b93e362c8fdbda3bf5ab8d65386b5c
	Domains	webservice-srv[.]online webservice-srv1[.]online
	SHA256	22bb73e97b01be2e11d741f3f4852380b3dae91d9ac511f33de8877a9e7c0534
	MD5	fee3db5db8817e82b1af4cedafd2f346 ecb7af5771f4fe36a3065dc4d5516d84 ebaf3c6818bfc619ca2876abd6979f6d ce8d77af445e3a7c7e56a6ea53af8c0d bec44b3194c78f6e858b1768c071c5db 9e19fe5c3cf3e81f347dd78cf3c2e0c2 8c2f5e7432f1e6ad22002991772d589b 7c0e5627fd25c40374bc22035d3fadd8 765f45198cb8039079a28289eab761c5 1fe3a2502e330432f3cf37ca7acbffac 1de44e8da621cdeb62825d367693c75e 1032986517836a8b1f87db954722a33f 0a95a985e6be0918fdb4bfabf0847b5a

Attack Name	TYPE	VALUE
ShellBot	MD5	bef1a9a49e201095da0bb26642f65a78 3eef28005943fee77f48ac6ba633740d 55e5bfa75d72e9b579e59c00eaeb6922 6d2c754760ccd6e078de931f472c0f72 7ca3f23f54e8c027a7e8b517995ae433 2cf90bf5b61d605c116ce4715551b7a3 7bc4c22b0f34ef28b69d83a23a6c88c5 176ebfc431daa903ef83e69934759212
	URLs	x-x-x[.]online/ak 193.233.202[.]219/mperl 193.233.202[.]219/niko1 hxxp://34.225.57[.]146/futai/perl 80.94.92[.]241/bash hxxp://185.161.208[.]234/test.jpg hxxp://39.165.53[.]17:8088/iposzz/dred hxxp://80.68.196[.]6/ff
	IPV4:PORT	164.90.240[.]68:6667 206.189.139[.]152:6667 176.123.2[.]3:6667 164.132.224[.]207:80 51.195.42[.]59:8080 192.3.141[.]163:6667 49.212.234[.]206:3303
Mispadu	MD5	E903B37B1E42D0B8BF0514CB13A46233 E5967A8274D40E0573C28B664670857E 0ADB9B817F1DF7807576C2D7068DD931 2858CDF0B9FB6DDD18709909DF612063 3FB45296ABDC78792FB609C187B4A89D AB80D005BCC4641D5D1AE75FBB2723B9 0D8D82E1810F549F8645535C836D7AFD 293B9621798EE17005D1EFFE463A8989 618A60899AAE66EA55E5DC8374C7B828 B41E2B88FFF36FF4937DC19F2677EE84 72E83B133A9E4CECD21FDB47334672F6 A96125294AFA1C3F92AB7BE615DC1CBE
	Domains	germogenborya[.]top germogenborya[.]at grintour[.]newdestuner[.]xyz russk22[.]icu
	IPV4:PORT	104[.]238[.]182[.]44:4000 104[.]238[.]182[.]44:4001 140[.]82[.]47[.]181:4000 140[.]82[.]47[.]181:4001

Attack Name	TYPE	VALUE
Mispadu	URLs	hxxps[:]//www.zairtaz[.]com/wp-content/plugins/license/inc/hydra/do/it.php?f=9&w=Windows%2010, hxxps[:]//imberform[.]com/img/?dew98fy348erf7i, hxxp[:]//vasuk[i].in/wp-content/img/do/it.php?f=9&w=Windows%207, hxxp[:]//luzca[.]com/img/do/it.php?f=2&w=Windows%207, hxxp[:]//nbviajesacapulco[.]com/pruc/it.php?f=9&w=Windows%207, hxxp[:]//nbviajesacapulco[.]com/pixel/it.php?f=2&w=Windows%207, hxxp[:]//www.castleblack[.]online/cfr/it.php?f=2&w=Windows%207, hxxps[:]//dicktres.com[.]br/pontecom/wp-content/img/do/it.php, hxxps[:]//bdadvisors[.]ma/img/do/it[.]php?f=2&w=Windows%2010, hxxp[:]//blog.traveldealsbd[.]com/images/arrow/do/it.php?b1=1&v1=1033&v2=1033&v3=Windows%207&v4=User&v5=X64, hxxp[:]//tripsapata[.]com/assets/images/swan/do/it.php, hxxps[:]//blablamap[.]net/images/arrow/do/it.php, hxxp[:]//facturacion.sat[.]gob.educationalwriters.com/do/it.php?f=2&w=Windows%207, hxxp[:]//aguiasoft.com[.]br/blog/hydra/do/it.php?b1=1&v1=3082&v2=2058&v3=windows%207&v4=admin&v5=x64, hxxp[:]//explanada2023[.]com/wp-includes/stylish/it.php?f=2&w=Windows%207, hxxp[:]//vaadiandkoh[.]com/ue/app/do/it.php?f=9&w=Windows%207, hxxp[:]//websylvania[.]com/psj/do/it.php?b1=1&v1=3082&v2=1034&v3=windows%207&v4=admin&v5=x64, hxxp[:]//publicpressmagazine[.]com/images/swan/do/it.php?b1=1&v1=1033&v2=1033&v3=Windows%207&v4=User&v5=X86, hxxps[:]//factura61[.]click/2/?CQ9OCKlYIQOSZqMxY43B80jdDceyL69GLzh6HNkZ, hxxps[:]//sxconstructions[.]com[.]au/wp-content/img/do/it.php?b1&v1=1033&v2=1033&v3=&v4=Windows%207&v5=User&v6=X%2086&v7=, hxxps[:]//kh7jv[.]store/?JDCE8IFt3QZJ2Ms4FQv8bp5q9KM6bFvMKUeE7QOLg7z4Kl9Oa48sMGRJDCE8IFt3QZJ2Ms4FQv8bp5q9KM6bFvMKUeE7QOLg7z4Kl9Oa48sMGR, hxxps[:]//sxconstructions[.]com.au/wp-content/img/do/it.php?f=2&w=Windows%210, hxxps[:]//sxconstructions[.]com.au/wp-content/img/do/it.php?info2=DATOS,

Attack Name	TYPE	VALUE
Mispadu	URLs	hxxp[:]//highlineadsl[.]com/ddd/it.php?f=3&w=Windows%207, hxxp[:]//germogenborya[.]top/rest/?h=CODE, hxxp[:]//vaadiandkoh[.]com/ue/app/do/it.php?f=9&w=Windows%207, hxxp[:]//grintour[.]newdestuner[.]xyz/g1, hxxp[:]//grintour.newdestuner[.]xyz/dhyhsh3a.php, hxxps[:]//facturaciones[.]click/?7kqhhbEE9Y1FiEBZ0Uc7izRLyJ2TWdZFK0qnXvXU, hxxp[:]//russk22[.]icu/brbr.txt, hxxps[:]//bola.com[.]au/images/hh/cfdi/do/it.php?f=2&w=Windows%2010, hxxps[:]//splendidgifts.com[.]my/hiway/ap2/do/it.php?b1&v1=1033&v2=1033&v3=&v4=Windows%2010&v5=User&v6=X64, hxxps[:]//tequilamisorpresa[.]com/ytweshdg.php?id=, hxxp[:]//formas-mexico[.]com/formas.xls, hxxps[:]//retiro10[.]click/, hxxps[:]//facturaciones[.]click, hxxps[:]//facturasnet[.]store, hxxps[:]//facturaciones3[.]click/, hxxps[:]//retiro10[.]store/, hxxp[:]//grintour[.]newdestuner[.]xyz/g1, hxxp[:]//grintour.newdestuner[.]xyz/dhyhsh3a.php, hxxps[:]//facturaciones[.]click/?7kqhhbEE9Y1FiEBZ0Uc7izRLyJ2TWdZFK0qnXvXU, hxxp[:]//russk22[.]icu/brbr.txt, hxxps[:]//bola.com[.]au/images/hh/cfdi/do/it.php?f=2&w=Windows%2010, hxxps[:]//splendidgifts.com[.]my/hiway/ap2/do/it.php?b1&v1=1033&v2=1033&v3=&v4=Windows%2010&v5=User&v6=X64, hxxps[:]//tequilamisorpresa[.]com/ytweshdg.php?id=, hxxp[:]//formas-mexico[.]com/formas.xls, hxxps[:]//retiro10[.]click/, hxxps[:]//facturaciones[.]click, hxxps[:]//facturasnet[.]store, hxxps[:]//facturaciones3[.]click/, hxxps[:]//retiro10[.]store/
	Registry	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run:WinDriver

Attack Name	TYPE	VALUE
Mispadu	Filenames	%AppData%\Roaming\herman\a3x\herndon\Factura_Deuda_423534.cmd %AppData%\Roaming\herman\exe\vayala\jordan.exe %AppData%\Roaming\herman\a3x\Factura_Deuda_423534.a3x %AppData%\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\DriverAudio.lnk %USER%\Downloads\sastreria.xls.exe %PUBLIC%\gnVzjGd.vbs
ALC	MD5	3E6D52E151154065EB9DA3DA48DC7A7D B6F780C70F6DD53A28286CF2D23F2359 79058D9B0FDFDADA59C18DF8AC026224 7384C4FCCF3818EF77C6188D7104A0B5 8D1C52CB4E6A5EA02275637D26F90F60 2B410375146A9BB550EDCA0BAE42A1CB 9A5E23DCC123B4B7526CE1D61DAB6CA4
	SHA256	2943a567bc05bc66ca6201dbc5f00bec3f774a47b1b94289a2ae8e79834c21a5 bbc6a34b48a4c71a4d9c2ae2d8c975f3b6caf2e17b86057ccbcb6686d1d5a642 bff07ae5ccea66b658783fcf940eaf6baa453b534af2ebe9b70f14923871d82f dc50ac15414b7274533cde5e1b28bfaa85353de38d4b21a8cb996412c0f6e432 0abe1ab9c75395a4ca829028d9c8c6530bd3bfda49e4b856b6f3539b9aa36ea5 1c5377db817c03f3c2711d351e380611291b5935ba0e2b0de763e4ef470e5bab 456961cba9a8dfce1b66081c6a73c2f1ec676fcdedac24c678f890a3425e7260 48b074b48bde3f15ca28983f26e855bafd6f19e8240d938b14f31417b39d9fd2 7efa5acd25e6276d122b2e2b8055a64dc4c757fc6067d3307973327154a507ff 84d4ca11c23a20bb220c15dbe3a363fb774081b6106c351fc9d8eab4f3b5b62c
	Email	Alc@cock[.]li
CloudMensis	SHA1	d7bf702f56ca53140f4f03b590e9afcbc83809db 0aa94d8df1840d734f25426926e529588502bc08 c3e48c2a2d43c752121e55b909fc705fe4fdaef6
DazzleSpy	SHA1	ee0678e58868ebd6603cc2e06a134680d2012c1b
EggShell RAT	SHA1	556a2174398890e3d628aec0163a42a7b7fb8ffd

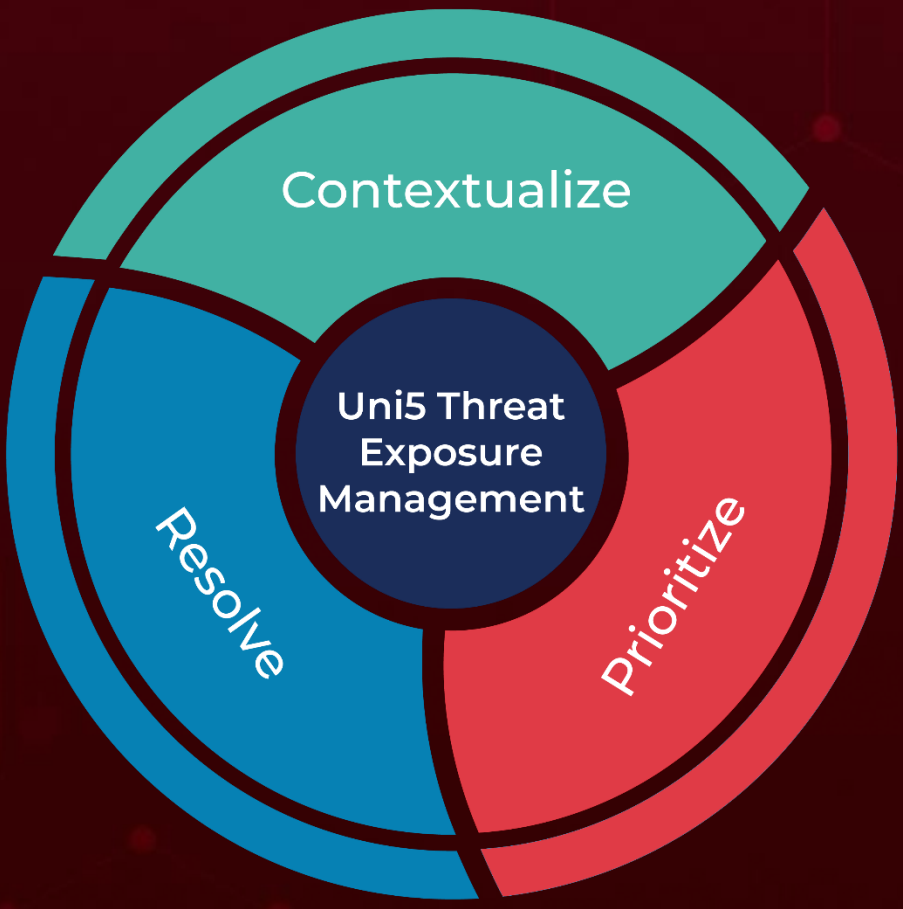
Attack Name	TYPE	VALUE
KeySteal	SHA1	26622e050d5ce4d68445b0cdc2cb23f9e27318ba 3951a7bd03e827caf7a0be90fdfc245e6b1e9f8a 5a8a7e665fdd7a422798d5c055c290fa8b7356d9 749ee9eaa0157de200f3316d912b9b8d8bb3a553 79c222b00b91801bb255376c9454d5bc8079c4a9 7f537a0a77fc8d629b335d52ffef40ea376bd673 8446f80f073db57466459bcbfcaefda3c367cd52 b81bf1b65b8ec0a11105d96cc9f95bb25214add5 ca985f4395e47f1bf9274013b36a0901343fc5a5 d2314f1534ecc1ab97f03cdacf9ed05349f5c574 d4e30bce71e025594339dacf4004075fa22962ea d85b6531843d5c29cc3bbb86e59d47249db89b9a d8cd78c16ca865d69f2eb72212b71754f72b4479
Poseidon	SHA1	cb8be6d2cefe46f3173cb6b9600fb40edb5c5248 c91b0b85a4e1d3409f7bc5195634b88883367cad
Pureland	SHA1	0b5153510529e21df075c75ad3dbfe7340ef1f70 1eec28e16be609b5c678c8bb2d4b09b39aa35c05 2480d3f438693cf713ce627b8e67ab39f8ae6bea 308cb5cbc11e0de60953a16a9b8ad8458b5eda67 397d5edae7086bb804f9384396a03c52c2b38daa 398de17ae751f7b4171d6d88c8d29ee42af9efb5 406c7c1f81c3170771afc328ca0d3882ee790e98 411482a5cebe1fc89661cc0527047fa4596ed2d6 49d7c260e89dd5bc288111cbe2bf521e95bbe199 68be8c909a809487d2a3ae418d7ec5adf9d770cb 8baf7c147d3d54b8e2a2e6e26d852028d03ee64b 8e698a7f186b7eda34a56477d5e86e0ad778b53d aa033e9f102bc8d98360e6079da3c8b4d7e2d3c8 acc1139ecfa0a628edf89b70a3e01a1424a00d5b f462fa129de484b0cf09a9b4d975b168e5c69370
XLoader	SHA1	7edead477048b47d2ac3abdc4baef12579c3c348 958147ab54ee433ac57809b0e8fd94f811d523ba fb83d869f476e390277aab16b05aa7f3adc0e841
Zuru	SHA1	20acde856a043194595ed88ef7ae0b79191394f9
BlackGuard	IPV4	23.83.114[.]131
	SHA256	88e9780ce5cac572013aebdd99d154fa0b61db12faffeff6f29f9 d2800c915b3
	SHA1	88e9780ce5cac572013aebdd99d154fa0b61db12
	MD5	3235ebcead914e4a210dc9dbe5c36c2f

Attack Name	TYPE	VALUE
Cinoshi	MD5	1798e35f14a67741f3425ba67373667d 40a85e9ac222d66a0f5cf526868ef2a9 29f3e408da86aafe535e179767fb2345
	SHA1	b929ed50142b9b43fb85c5b1ddb87ec00ca09f24 b4553412217971d814650995ce9d98c78660fdab 783303902cafad79efc585fd25705853b4150338
	SHA256	e3aafd9f478b82cbb53ec020cdc2e00e0c4de60a7f66a1166e54ab75b6a9e8c3 cf1705c39dc3dbf65856ac6f5462027d9a290ab2d38da08f76aabd684b8a9944 9b7d799895932d8359d7eb5da378b67a481331fa1a912075339d972496d122d6
	URLs	hxxps[:]//tryno.ru/robots hxxps[:]//anaida[.]evisyn[.]lol
APERETIF	SHA1	0fe3fe479885dc4d9322b06667054f233f343e20 83f00ee38950436527499769db5c7ecb74a9ea41 a19d46251636fb46a013c7b52361b7340126ab27 a574c5d692b86c6c3ee710af69fccbb908fe1bb8 c7fa6727fe029c3eaa6d9d8bd860291d7e6e3dd0 f39b260a9209013d9559173f12fbc2bd5332c52a
	URLs	hxxps[:]//applesaltbeauty[.]com/wordpress/wp-includes/widgets/classwp/521734i hxxps[:]//marakanas[.]com/Kkdn7862Jj6h2oDASGmpqU4Qq4q4.php hxxps[:]//natply[.]com/wordpress/wp-includes/fonts/ch/097214o hxxps[:]//ocs-romastassec[.]com/goog_comredira3cf7ed34f8.php
	IPV4	176.97.66[.]57 179.43.187[.]175 179.43.187[.]207 195.54.170[.]26 80.79.124[.]135
	Domains	bugiplaysec[.]com marakanas[.]com mfa_it_sec@outlook[.]com ocs-romastassec[.]com ocspdep[.]com security-ocsp[.]com troadsecow[.]com

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

March 28, 2023 . 6:00 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com