

Date of Publication

March 1, 2023



Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Actors, and Attacks

FEBRUARY 2023

Top 5 Takeaways

#1

In February, there were **nine zero-day** vulnerabilities. **Four** of them were exploited by **threat actors** in the past month, while the remaining **five** were addressed by vendors such as Microsoft, Apple, and Forta.

#2

Throughout the month, various ransomware strains including **Nevada, ESXiArgs, ClOp, Trigona, MortalKombat, GlobeImposter, DarkBit, and HardBit** were active.

#3

The **Democratic People's Republic of Korea (DPRK)** used vulnerabilities **CVE-2021-44228, CVE-2021-20038, and CVE-2022-24990** to carry out a ransomware attack against the healthcare systems of **South Korea and the United States.**

#4

Numerous new malware families have been observed targeting victims worldwide. These include **TrickGate, HeadCrab, VectorStealer, MalVirt, Graphiron, and SoulSearcher.**



#5

ProxyShellMiner exploits Windows Exchange servers' vulnerabilities to install **cryptocurrency** miners.



Significant Vulnerabilities of the Month	Active Threat Actors of the Month	Active Malware of the Month	Top Targeted Countries	Top Targeted Industries	Potential MITRE ATT&CK TTPs
					
73	18	35	France Norway USA South Korea	Government Healthcare Energy Financial Manufacturing	244

Detailed Report

🔧 Vulnerabilities of the Month

VENDOR	CVE	PATCH DETAILS
	<u>CVE-2021-34527*</u> <u>CVE-2017-11882</u> <u>CVE-2018-0802*</u> <u>CVE-2018-0798</u> <u>CVE-2023-21823*</u> <u>CVE-2023-21715*</u> <u>CVE-2023-23376*</u> <u>CVE-2023-21808</u> <u>CVE-2023-21716</u> <u>CVE-2023-21718</u> <u>CVE-2023-21815</u> <u>CVE-2023-21803</u> <u>CVE-2023-21717</u> <u>CVE-2023-21777</u> <u>CVE-2023-21806</u> <u>CVE-2023-21804</u> <u>CVE-2023-21819</u> <u>CVE-2023-21689</u> <u>CVE-2023-21688</u> <u>CVE-2023-23381</u> <u>CVE-2023-21690</u> <u>CVE-2021-34473</u> <u>CVE-2021-34523</u> <u>CVE-2021-31207</u>	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34527 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-11882 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-0802 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-0798 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21823 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21715 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23376 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21808 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21716 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21718 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21815 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21803 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21717 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21777 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21806 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21804 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21819 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21689 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21688 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23381 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21690 https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-may-11-2021-kb5003435-028bd051-b2f1-4310-8f35-c41c9ce5a2f1 https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-april-13-2021-kb5001779-8e08f3b3-fc7b-466c-bbb7-5d5aa16ef064
	<u>CVE-2017-8291*</u>	https://www.openwall.com/lists/oss-security/2017/04/28/2

* zero-day vulnerability

VENDOR	CVE	PATCH DETAILS
	CVE-2023-20076	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL
	CVE-2021-21974 CVE-2021-21973 CVE-2021-21972 CVE-2023-20858	https://www.vmware.com/security/advisories/VMSA-2021-0002.html https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-ac-announcements/GUID-7464A525-BCF4-4329-9228-B040C9C16D22.html https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-ac-announcements/GUID-35DA49E4-41F3-485B-88E5-AE69B354F2FB.html
	CVE-2023-0696 CVE-2023-0697 CVE-2023-0698 CVE-2023-0699 CVE-2023-0700 CVE-2023-0701 CVE-2023-0702 CVE-2023-0703 CVE-2023-0704 CVE-2023-0705	https://www.google.com/intl/en/chrome/?standalone=1
	CVE-2023-22501	https://confluence.atlassian.com/jira/jira-service-management-server-and-data-center-advisory-cve-2023-22501-1188786458.html
	CVE-2023-0286 CVE-2022-4304 CVE-2022-4203 CVE-2023-0215 CVE-2022-4450 CVE-2023-0216 CVE-2023-0217 CVE-2023-0401	https://www.openssl.org/news/vulnerabilities.html
	CVE-2023-0669*	https://my.goanywhere.com/webclient/DownloadProductFiles.xhtml
	CVE-2023-23529* CVE-2023-23514 CVE-2023-23522 CVE-2023-23520 CVE-2023-23530 CVE-2023-23531	https://support.apple.com/en-us/HT213633 https://support.apple.com/en-us/HT213635 https://support.apple.com/en-us/HT213638 https://support.apple.com/en-gb/HT201222 Update to version macOS Ventura 13.2



* zero-day vulnerability

VENDOR	CVE	PATCH DETAILS
	CVE-2023-24483 CVE-2023-24484 CVE-2023-24485 CVE-2023-24486	https://support.citrix.com/article/CTX477616/citrix-virtual-apps-and-desktops-security-bulletin-for-cve202324483 https://support.citrix.com/article/CTX477617/citrix-workspace-app-for-windows-security-bulletin-for-cve202324484-cve202324485 https://support.citrix.com/article/CTX477618/citrix-workspace-app-for-linux-security-bulletin-for-cve202324486
	CVE-2022-27925 CVE-2022-37042	https://wiki.zimbra.com/wiki/Security_Center
	CVE-2021-4034	https://oss.oracle.com/pipermail/el-errata/2022-January/012089.html https://www.debian.org/security/2022/dsa-5059 https://oss.oracle.com/pipermail/el-errata/2022-January/012084.html http://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.434679 https://oss.oracle.com/pipermail/el-errata/2022-January/012086.html https://gitlab.freedesktop.org/polkit/polkit/-/commit/a2bf5c9c83b6ae46cbd5c779d3055bff81ded683 https://www.debian.org/its/security/2022/dla-2899
	CVE-2022-39952 CVE-2021-42756 CVE-2022-27482 CVE-2022-27489 CVE-2022-38375 CVE-2023-23780	https://www.fortiguard.com/psirt/FG-IR-22-300 https://www.fortiguard.com/psirt/FG-IR-21-186 https://www.fortiguard.com/psirt/FG-IR-22-046 https://www.fortiguard.com/psirt/FG-IR-22-048 https://www.fortiguard.com/psirt/FG-IR-22-329 https://www.fortiguard.com/psirt/FG-IR-22-118
	CVE-2021-44228*	https://logging.apache.org/log4j/2.x/security.html
	CVE-2021-20038	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026
	CVE-2022-24990	https://forum.terra-master.com/en/viewtopic.php?t=3030



* zero-day vulnerability

Threat Actors of the Month


NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p><u>BlueBravo (APT 29, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook , ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa)</u></p> 	Russia	Aerospace, Defense, Education, Energy, Financial, Government, Healthcare, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks and Imagery	Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chechnya, Chile, China, Cyprus, Czech, Denmark, France, Georgia, Germany, Hungary, India, Ireland, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Latvia, Lebanon, Lithuania, Luxembourg, Mexico, Montenegro, Netherlands, New Zealand, Poland, Portugal, Romania, Russia, Singapore, Slovakia, Slovenia, Spain, South Korea, Switzerland, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO
	MOTIVE		
	Information theft and espionage		
	CVEs		



NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p><u>OilRig (APT 34, Helix Kitten, Twisted Kitten, Crambus, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13)</u></p> 	Iran	Chemicals, Education, Energy, Financial, Government, Legal, Oil and Gas, Telecommunications, Aviation, High-Tech, Hospitality.	Oman, Azerbaijan, Bahrain, Iraq, Israel, Jordan, Kuwait, Lebanon, Mauritius, Qatar, Saudi Arabia, South Africa, Turkey, United Arab Emirates, Middle East, North Africa, Pakistan, Turkey, UK, USA.
	MOTIVE		
	Information theft and espionage		
	CVEs		



NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p>LABYRINTH <u>CHOLLIMA(Lazarus Group, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace , Gods Apostles ,Gods Disciples)</u></p> 	North Korea	Aerospace, Defense, Energy, Engineering, Financial, Government, Healthcare, Research, Manufacturing, Media, Shipping and Logistics, Technology and BitCoin	Australia, Bangladesh, Belgium, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Netherlands, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	CVEs		
	CVE-2022-27925 CVE-2022-37042 CVE-2021-4034 CVE-2021-34527		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p>Mustang Panda <u>APT(Bronze President ,TEMP.Hex ,HoneyMyte,Red Lich,Earth Preta)</u></p> 	China	Government and Public sectors	Asia and Europe
	MOTIVE		
	Information theft and espionage		
	CVEs		



NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p>NewsPenguin</p> 	Unknown	Defense, Government, Maritime and Shipbuilding.	Pakistan
	MOTIVE		
	Information theft and espionage		
	CVE		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p>TA505(Graceful Spider, Gold Evergreen , Gold Tahoe, TEMP.Warlock, ATK 103, SectorJ04, Hive0065, Chimborazo)</p> 	Russia	Agriculture, Automotive, Chemicals, Consulting, Education, Energy, Engineering, FMCG, Financial, Food and Beverage, Government, Healthcare, Hospitality, Insurance, Logistics, Manufacturing, Maritime, Media, NGO, Oil and Gas, Online, Pharmaceuticals, Real Estate, Retail, Technology, Telecommunications, Transportation	Argentina, Australia, Belgium, Brazil, Canada, Chile, Colombia, Congo, Europe, France, Germany, Ghana, Hungary, India, Indonesia, Italy, Japan, Latvia, Malaysia, Mexico, Algeria, Bahrain, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Libya, Morocco, Syria, Tunisia, Yemen, Myanmar, Netherlands, Oman, Poland, Portugal, Qatar, Russia, Saudi Arabia, South Africa, State, Brunei, Cambodia, East Timor, Laos, Philippines, Singapore, Thailand, South Korea, Spain, Taiwan, United Arab Emirates, United Kingdom, United States, Vietnam, Austria, Switzerland
	MOTIVE		
	Financial crime, Financial gain		
	CVEs		
	CVE-2023-0669		



NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p>Nodaria (UAC-0056)</p> 	Russia	Government	Ukraine
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
 <p>KillNet</p> 	Russia	Government, Healthcare	NATO countries
	MOTIVE		
	Sabotage and destruction		
	CVEs		

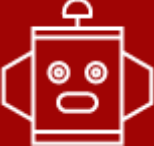

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p>Tonto Team (HeartBeat, Karma Panda, CactusPete, Bronze Huntley, LoneRanger, Earth Akhlut) </p>	China	Government, Defense, IT, Energy, Financial, Educational, Healthcare, Media, and Technology	India, Japan, Mongolia, Russia, South Korea, Taiwan, USA, and Eastern Europe
	MOTIVE		
	Information theft and espionage		
	CVEs		
	CVE-2017-11882 CVE-2018-0802 CVE-2018-0798		



NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p>DEV-0147 </p>	China	Diplomatic Entities, government agencies and think tanks	South America, Asia and Europe
	MOTIVE		
	Data Exfiltration		
	CVEs		



NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p>Red Eyes (Reaper, APT 37, Ricochet Chollima, ScarCruft, Thallium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10) </p>	North Korea	Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, Transportation	China, Czech, Hong Kong, India, Japan, Kuwait, Nepal, Poland, Romania, Russia, South Korea, UK, USA, Vietnam
	MOTIVE		
	Information theft and espionage		
	CVEs		
	CVE-2017-8291		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p><u>Dalbit</u> (m00nlight)</p> 	Unknown	Technology, Industrial, Chemical, Construction, Automobile, Semiconductor, Education, Wholesale, Media, Food, Shipping, Hospitality, Energy, Shipbuilding, Consulting	Korea
	MOTIVE		
	Information theft		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
 <p><u>Earth Kitsune APT</u></p> 	North Korea	Research, Think Tanks	North Korea, China, Brazil, and Japan.
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p><u>WIP26</u></p> 	Unknown	Telecommunications	Middle East
	MOTIVE		
	Information theft and Espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 <p><u>Hydrochasma</u></p> 	Unknown	Healthcare, Transportation	Asia
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
 Clasiopa 	Unknown	Materials research	Asia
	MOTIVE		
	Espionage		
	CVE		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
 SteelClover 	Unknown	Unknown	Japan
	MOTIVE		
	Financial gain		
	CVE		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
 TA866 	Unknown	All	United States and Germany
	MOTIVE		
	Financial gain		
	CVE		



Malware of the Month

NAME	OVERVIEW	TYPE	DELIVERY METHOD
<u>GraphicalNeutrino and BEATDROP</u> 	GraphicalNeutrino and BEATDROP are malicious software used by the Russian-linked threat group BlueBravo in targeted cyber attacks, using legitimate Western services for command-and-control communications to evade detection.	Malware Family	Malicious Zip files
<u>TrickGate</u> 	TrickGate is a notorious Packer-as-a-Service that has evaded detection from cyber security measures for over six years. Despite its elusive nature is being used to spread a wide range of malicious tools such as ransomware, RATs, information stealers, bankers, and miners.	Packer-as-a-Service	Phishing Emails
<u>HeadCrab malware</u> 	A newly discovered HeadCrab malware, designed to target vulnerable Redis servers online, has been able to infect over a thousand servers since September 2021 and has created a botnet that mines Monero cryptocurrency.	Botnet	Unknown
<u>VectorStealer</u> 	VectorStealer is a malware that steals .rdp files through phishing emails, can be generated for USD 63 in Bitcoin, exfiltrates stolen information through SMTP, Discord, or Telegram, and uses the KGB Crypter to evade antivirus detection.	Information Stealer	Phishing Emails
<u>Ice Breaker</u> 	Online gaming and gambling companies have been targeted by as Ice Breaker. The attacks are grouped together and referred to as Ice Breaker. The intrusions make use of smart social engineering strategies to install a JavaScript backdoor.	Backdoor	Social Engineering

NAME	OVERVIEW	TYPE	DELIVERY METHOD
MalVirt 	MalVirt is a cluster of virtualized .NET malware loaders that use obfuscated virtualization and the Windows Process Explorer driver to evade anti-analysis and terminate processes.	Loaders	Malvertising
Nevada Ransomware 	The Nevada Ransomware is a Rust-based locker with an affiliate platform first announced on the RAMP underground community. The ransomware has been upgraded and improved functionality for Windows and Linux/ESXi systems. Updated builds have been made available to affiliates.	Ransomware	Ransomware-as-a-service
Medusa Botnet 	The Mirai botnet has recently been seen downloading and spreading a new botnet called the Medusa Botnet is written in Python and can perform various malicious activities like DDoS attacks, Ransomware attacks, and brute force attacks.	Botnet	Unknown
PlugX malware 	Mustang Panda APT group employs PlugX malware in a four-stage infection chain that leverages malicious shortcut (LNK) files and DLL search-order-hijacking to load the PlugX malware into the memory of legitimate software.	Remote Access Trojan	Phishing Emails
ESXiArgs Ransomware 	The ESXiArgs ransomware attack exploits the CVE-2021-21974 vulnerability to allow remote code execution and has impacted servers in several countries, primarily developed nations. The attackers demand a ransom in bitcoins.	Ransomware	Unknown
Cl0p Ransomware 	A new variant of the Cl0p ransomware for Linux has been discovered. The executable file in ELF format has a flawed encryption algorithm, which allows for the decryption of the locked files without requiring a ransom payment.	Ransomware	Unknown

NAME	OVERVIEW	TYPE	DELIVERY METHOD
<u>Trigona Ransomware</u> 	Trigona has gained momentum lately due to its utilization of the double-extortion technique of encrypting crucial assets within an organization and demanding payment of ransom, or else the stolen data from these systems will be publicly released on the internet.	Ransomware	Emails, Remote Desktop Protocol (RDP) and exploiting vulnerabilities.
<u>Redline Stealer</u> 	SteelClover is an attack group that has been operating for several years and is now using Google Ads to spread malicious files that infect systems with Ursnif and Redline Stealer malware.	Information Stealer	Malvertising
<u>Graphiron</u> 	Nodaria an espionage group has been spotted deploying a newly created malware named Graphiron in attacks aimed at Ukraine. The malware is coded in Go and can gather a significant amount of data from compromised computers.	Information Stealer	Unknown
<u>Bisonal.DoubleT backdoor</u> 	Tonto Team APT used the Bisonal.DoubleT is a unique tool. This malware lets an attacker get remote access to an infected computer and run various instructions on it in order to gather information about the compromised host.	Backdoor	Malicious emails
<u>MortalKombat Ransomware</u> 	An unidentified actor using the MortalKombat ransomware to steal cryptocurrency from victims. The ransomware encrypts various files on the victim machine's file system, leaving the machine inoperable without deleting the volume shadow copies.	Ransomware	Phishing Emails
<u>Laplas Clipper</u> 	The theft of cryptocurrency was carried out via a GO variant of the Laplas Clipper malware. Clipper targets by employing regular expressions to monitor the victim's clipboard for their cryptocurrency wallet address.	Clipper	Phishing Emails

NAME	OVERVIEW	TYPE	DELIVERY METHOD
QuasarLoader 	DEV-0147 an espionage group uses tools like ShadowPad and QuasarLoader for persistent access, deploying other malware and post-exploitation activities to abuse identity infrastructure for its data exfiltration operations.	Webpack Loader	Phishing and unpatched applications
Globelmposter 	Globelmposter malware family, can delete volume shadow copies, and its delivery methods and functionalities are consistent with those of the new variant TZW.	Ransomware	Phishing Emails
ProxyShellMiner 	ProxyShellMiner exploits Windows Exchange servers' vulnerabilities, which are used to gain unauthorized access and compromise an organization, leading to the installation of cryptocurrency miners.	Miner	Unknown
DarkBit Ransomware 	The DarkBit is a newly emerged threat a GO-based Binary that targets windows OS. The ransomware encrypts files utilizing multithreading and Advanced Encryption Standard 256-bits.	Ransomware	Unknown
WhiskerSpy 	Earth Kitsune APT distributed a trojanized codec installer, with a new backdoor WhiskerSpy, and abused Google Chrome's native messaging host and OneDrive side-loading vulnerabilities for persistence.	Backdoor	Social Engineering
SoulSearcher 	SoulSearcher is a type of second-stage loader used by the Soul malware framework, responsible for executing the Soul module payload and parsing its configuration, with multiple variants found in the wild since 2017.	Malware Family	Unknown

NAME	OVERVIEW	TYPE	DELIVERY METHOD
<u>Stealc</u> 	Stealc is designed to steal sensitive data from various sources including cryptocurrency wallets and browser extensions for cryptocurrency wallets.	Information Stealer	Unknown
<u>Mylobot</u> 	Mylobot malware can turn an infected computer into a proxy by taking full control of it, and it is designed to evade detection and remain persistent on infected machines.	Botnet	Unknown
<u>DarkCloud Stealer</u> 	DarkCloud Stealer functions through a multi-stage process, and the final payload, written in Visual Basic, is loaded into the device's memory.	Information Stealer	Phishing Emails
<u>HardBit Ransomware</u> 	HardBit is a strain that focuses on extorting cryptocurrency payments from organizations in exchange for data decryption.	Ransomware	Unknown
<u>Icarus Stealer</u> 	The Icarus Stealer malware is equipped with a Hidden Virtual network computing (hVNC) feature, which enables the attacker to generate a concealed desktop and traverse the compromised system without any contact with the primary desktop.	Information Stealer	Unknown
<u>Atharvan</u> 	Atharvan is designed to run on Windows OS and has several features that allow attackers to take control of the infected system and monitor activity.	Remote Access Trojan	Unknown
<u>Malicious ChatGPT</u> 	The attackers have typosquatted domains that mimic the official ChatGPT website, which can easily mislead users. Encouraging users to download malicious files that can infect and steal sensitive data.	Information Stealer	Social Engineering and Phishing
<u>WinorDLL64</u> 	WinorDLL64 seems to be associated with the malware downloader Wslink.	Backdoor	Unknown

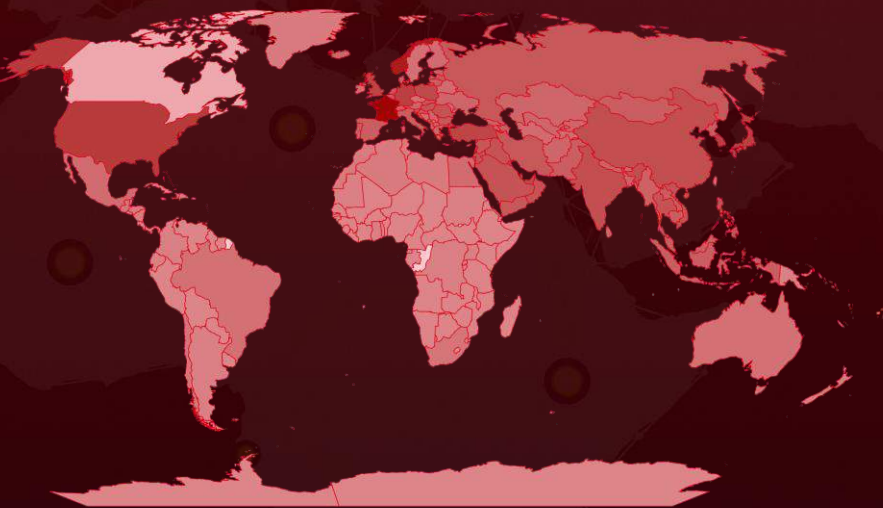
NAME	OVERVIEW	TYPE	DELIVERY METHOD
PureCrypter 🔗	PureCrypter has been used to distribute various strains of ransomware and information stealers. The malware leverages a compromised non-profit organization's domain as C2 to deliver a secondary payload.	Malware Downloader	Phishing Emails
EXFILTRATOR-22 🔗	Exfiltrator-22 is a new post-exploitation framework for spreading ransomware. It is believed to be created by former LockBit 3.0 affiliates and is offered for a subscription fee ranging from \$1,000 per month to \$5,000 for lifetime access.	Post-Exploitation Framework	Unknown
AgentTesla 🔗	GuLoader is delivered in new campaigns by the attackers via AgentTesla. It is a .NET-based Trojan that steals through keylogging and password stealing.	Trojan	Phishing Emails
WasabiSeed 🔗	The TA866 attack chain involves a multi-step process of downloading and running an MSI package containing WasabiSeed and Screenshotter. Further loads additional payloads such as AHK Bot and Rhadamanthys Stealer.	Malware Downloader	Malicious Emails

🌐 Targeted Countries

Most



Least



Powered by Bing

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

Targeted Industries

Most



Government



Healthcare



Energy



Financial



Manufacturing



Media



Education



Technology



Defence



Transportation



Chemical



Tele-communications



Engineering



Aerospace



Food products



Hotels



Pharmaceutical



Retail



Logistics



Insurance



Automotive



Electrical



Construction



Utilities



Real Estate



Legal



Oil & Gas



Consumers



Professional Services



Research Organizations



Think-Tanks



NGOs



Cryptocurrency



Marine



Gaming



Aviation



Religious



Metals & Mining



Cryptocurrency



Entertainment



Jewelry

Least

⚙️ Potential MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1589:Gather Victim Identity Information	T1583:Acquire Infrastructure	T1078:Valid Accounts	T1047:Windows Management Instrumentation	T1037:Boot or Logon Initialization Scripts	T1037:Boot or Logon Initialization Scripts	T1027:Obfuscated Files or Information
T1592:Gather Victim Host Information	T1583.003:Acquire Infrastructure: Virtual Private Server	T1078.003:Valid Accounts: Local Accounts	T1053:Scheduled Task/Job	T1037.005:Boot or Logon Initialization Scripts: Startup Items	T1037.005:Boot or Logon Initialization Scripts: Startup Items	T1027.002:Obfuscated Files or Information: Software Packing
T1595:Active Scanning	T1584:Compromise Infrastructure	T1133:External Remote Services	T1053.005:Scheduled Task/Job: Scheduled Task	T1053:Scheduled Task/Job	T1053:Scheduled Task/Job	T1027.005:Obfuscated Files or Information: Indicator Removal from Tools
	T1586:Compromise Accounts	T1189:Drive-by Compromise	T1059:Command and Scripting Interpreter	T1053.005:Scheduled Task/Job: Scheduled Task	T1053.005:Scheduled Task/Job: Scheduled Task	T1027.006:Obfuscated Files or Information: HTML Smuggling
	T1587:Develop Capabilities	T1190:Exploit Public-Facing Application	T1059.001:Command and Scripting Interpreter: PowerShell	T1078:Valid Accounts	T1055:Process Injection	T1027.007:Obfuscated Files or Information: Dynamic API Resolution
	T1587.001:Develop Capabilities: Malware	T1195:Supply Chain Compromise	T1059.003:Command and Scripting Interpreter: Windows Command Shell	T1078.003:Valid Accounts: Local Accounts	T1055.002:Process Injection: Portable Executable Injection	T1036:Masquerading
	T1587.002:Develop Capabilities: Code Signing, Certificates	T1199:Trusted Relationship	T1059.004:Command and Scripting Interpreter: Unix Shell	T1098:Account Manipulation	T1055.003:Process Injection: Thread Execution Hijacking	T1036.002:Masquerading: Right-to-Left Override
	T1588:Obtain Capabilities	T1566:Phishing	T1059.005:Command and Scripting Interpreter: Visual Basic	T1133:External Remote Services	T1055.012:Process Injection: Process Hollowing	T1036.004:Masquerading: Masquerade Task or Service
	T1588.002:Obtain Capabilities: Tool	T1566.001:Phishing: Spearphishing Attachment	T1059.007:Command and Scripting Interpreter: JavaScript	T1136:Create Account	T1068:Exploitation for Privilege Escalation	T1036.005:Masquerading: Match Legitimate Name or Location
	T1588.005:Obtain Capabilities: Exploits	T1566.002:Phishing: Spearphishing Link	T1106:Native API	T1137:Office Application Startup	T1078:Valid Accounts	T1036.007:Masquerading: Double File Extension
	T1588.006:Obtain Capabilities: Vulnerabilities	T1566.003:Phishing: Spearphishing via Service	T1129:Shared Modules	T1197:BITS Jobs	T1078.003:Valid Accounts: Local Accounts	T1055:Process Injection
	T1608:Stage Capabilities		T1203:Exploitation for Client Execution	T1505:Server Software Component	T1134:Access Token Manipulation	T1055.002:Process Injection: Portable Executable Injection
	T1608.001:Stage Capabilities: Upload Malware		T1204:User Execution	T1505.003:Server Software Component: Web Shell	T1134.002:Access Token Manipulation: Create Process with Token	T1055.003:Process Injection: Thread Execution Hijacking
	T1608.005:Stage Capabilities: Link Target		T1204.001:User Execution: Malicious Link	T1543:Create or Modify System Process	T1134.003:Access Token Manipulation: Make and Impersonate Token	T1055.012:Process Injection: Process Hollowing
			T1204.002:User Execution: Malicious File	T1543.002:Create or Modify System Process: Systemd Service	T1543:Create or Modify System Process	T1070:Indicator Removal
			T1559:Inter-Process Communication	T1546:Event Triggered Execution	T1543.002:Create or Modify System Process: Systemd Service	T1070.004:Indicator Removal: File Deletion
			T1559.001:Inter-Process Communication: Component Object Model	T1546.010:Event Triggered Execution: Applnit DLLs	T1546:Event Triggered Execution	T1070.006:Indicator Removal: Timestamp
			T1569:System Services	T1546.015:Event Triggered Execution: Component Object Model Hijacking	T1546.010:Event Triggered Execution: Applnit DLLs	T1070.007:Indicator Removal: Clear Network Connection History and Configurations
			T1569.002:System Services: Service Execution	T1546.016:Event Triggered Execution: Installer Packages	T1546.015:Event Triggered Execution: Component Object Model Hijacking	T1078:Valid Accounts
				T1547:Boot or Logon Autostart Execution	T1546.016:Event Triggered Execution: Installer Packages	T1078.003:Valid Accounts: Local Accounts
				T1547.001:Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547:Boot or Logon Autostart Execution	T1112:Modify Registry
				T1556:Modify Authentication Process	T1547.001:Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1134:Access Token Manipulation
				T1574:Hijack Execution Flow	T1548:Abuse Elevation Control Mechanism	T1134.002:Access Token Manipulation: Create Process with Token
				T1574.001:Hijack Execution Flow: DLL Search Order Hijacking	T1548.002:Abuse Elevation Control Mechanism: Bypass User Account Control	T1134.003:Access Token Manipulation: Make and Impersonate Token
				T1574.002:Hijack Execution Flow: DLL Side-Loading	T1574:Hijack Execution Flow	T1140:Deobfuscate/Decode Files or Information
					T1574.001:Hijack Execution Flow: DLL Search Order Hijacking	T1197:BITS Jobs
					T1574.002:Hijack Execution Flow: DLL Side-Loading	T1202:Indirect Command Execution
						T1218:System Binary Proxy Execution
						T1218.007:System Binary Proxy Execution: MsExec
						T1218.011:System Binary Proxy Execution: Rundll32
						T1221:Template Injection
						T1480:Execution Guardrails
						T1497:Virtualization/Sandbox Evasion
						T1497.001:Virtualization/Sandbox Evasion: System Checks
						T1497.002:Virtualization/Sandbox Evasion: User Activity Based Checks
						T1497.003:Virtualization/Sandbox Evasion: Time Based Evasion
						T1548:Abuse Elevation Control Mechanism
						T1548.002:Abuse Elevation Control Mechanism: Bypass User Account Control
						T1553:Subvert Trust Controls
						T1553.002:Subvert Trust Controls: Code Signing
						T1556:Modify Authentication Process
						T1562:Impair Defenses
						T1562.001:Impair Defenses: Disable or Modify Tools
						T1562.003:Impair Defenses: Impair Command History Logging
						T1564:Hide Artifacts
						T1564.003:Hide Artifacts: Hidden Window
						T1574:Hijack Execution Flow
						T1574.001:Hijack Execution Flow: DLL Search Order Hijacking
						T1574.002:Hijack Execution Flow: DLL Side-Loading
						T1620:Reflective Code Loading
						T1622:Debugger Evasion

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact	
T1003:OS Credential Dumping	T1007:System Service Discovery	T1021:Remote Services	T1005:Data from Local System	T1001:Data Obfuscation	T1011:Exfiltration Over Other Network Medium	T1486:Data Encrypted for Impact	
T1056:Input Capture	T1010:Application Window Discovery	T1021.001:Remote Services: Remote Desktop Protocol	T1056:Input Capture	T1071:Application Layer Protocol	T1020:Automated Exfiltration	T1489:Service Stop	
T1056.001:Input Capture: Keylogging	T1012:Query Registry	T1021.005:Remote Services: VNC	T1056.001:Input Capture: Keylogging	T1071.001:Application Layer Protocol: Web Protocols	T1029:Scheduled Transfer	T1490:Inhibit System Recovery	
T1110:Brute Force	T1016:System Network Configuration Discovery	T1210:Exploitation of Remote Services	T1074:Data Staged	T1090:Proxy	T1030:Data Transfer Size Limits	T1491:Defacement	
T1528:Steal Application Access Token	T1018:Remote System Discovery	T1570:Lateral Tool Transfer	T1113:Screen Capture	T1090.001:Proxy: Internal Proxy	T1041:Exfiltration Over C2 Channel	T1496:Resource Hijacking	
T1539:Steal Web Session Cookie	T1033:System Owner/User Discovery		T1114:Email Collection	T1090.002:Proxy: External Proxy	T1048:Exfiltration Over Alternative Protocol	T1498:Network Denial of Service	
T1552:Unsecured Credentials	T1046:Network Service Discovery		T1114.002:Email Collection: Remote Email Collection	T1090.004:Proxy: Domain Fronting	T1048.003:Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	T1499:Endpoint Denial of Service	
T1552.001:Unsecured Credentials: Credentials In Files	T1049:System Network Connections Discovery		T1115:Clipboard Data	T1095:Non-Application Layer Protocol	T1567:Exfiltration Over Web Service	T1529:System Shutdown/Reboot	
T1555:Credentials from Password Stores	T1057:Process Discovery		T1119:Automated Collection	T1102:Web Service		T1531:Account Access Removal	
T1555.003:Credentials from Password Stores: Credentials from Web Browsers	T1082:System Information Discovery		T1213:Data from Information Repositories	T1102.002:Web Service: Bidirectional Communication		T1561:Disk Wipe	
T1556:Modify Authentication Process	T1083:File and Directory Discovery		T1560:Archive Collected Data	T1104:Multi-Stage Channels			
T1558:Steal or Forge Kerberos Tickets	T1087:Account Discovery		T1560.001:Archive Collected Data: Archive via Utility	T1105:Ingress Tool Transfer			
	T1087.001:Account Discovery: Local Account		T1560.002:Archive Collected Data: Archive via Library	T1132:Data Encoding			
	T1087.002:Account Discovery: Domain Account			T1132.001:Data Encoding: Standard Encoding			
	T1120:Peripheral Device Discovery		T1219:Remote Access Software				
	T1124:System Time Discovery		T1571:Non-Standard Port				
	T1135:Network Share Discovery		T1572:Protocol Tunneling				
	T1497:Virtualization/Sandbox Evasion		T1573:Encrypted Channel				
	T1497.001:Virtualization/Sandbox Evasion: System Checks		T1573.001:Encrypted Channel: Symmetric Cryptography				
	T1497.002:Virtualization/Sandbox Evasion: User Activity Based Checks		T1573.002:Encrypted Channel: Asymmetric Cryptography				
	T1497.003:Virtualization/Sandbox Evasion: Time Based Evasion						
T1518:Software Discovery							
T1518.001:Software Discovery: Security Software Discovery							
T1614:System Location Discovery							
T1614.001:System Location Discovery: System Language Discovery							
T1622:Debugger Evasion							

Recommendations

Security Teams
















































This digest can be used as a guide to help security teams prioritize the **73 significant vulnerabilities** and block the indicators related to the **18 active threat actors**, **35 active malware**, and **244 potential MITRE TTPs**.

Uni5 Users








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

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

Hive Pro Threat Advisories (December 2022)

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

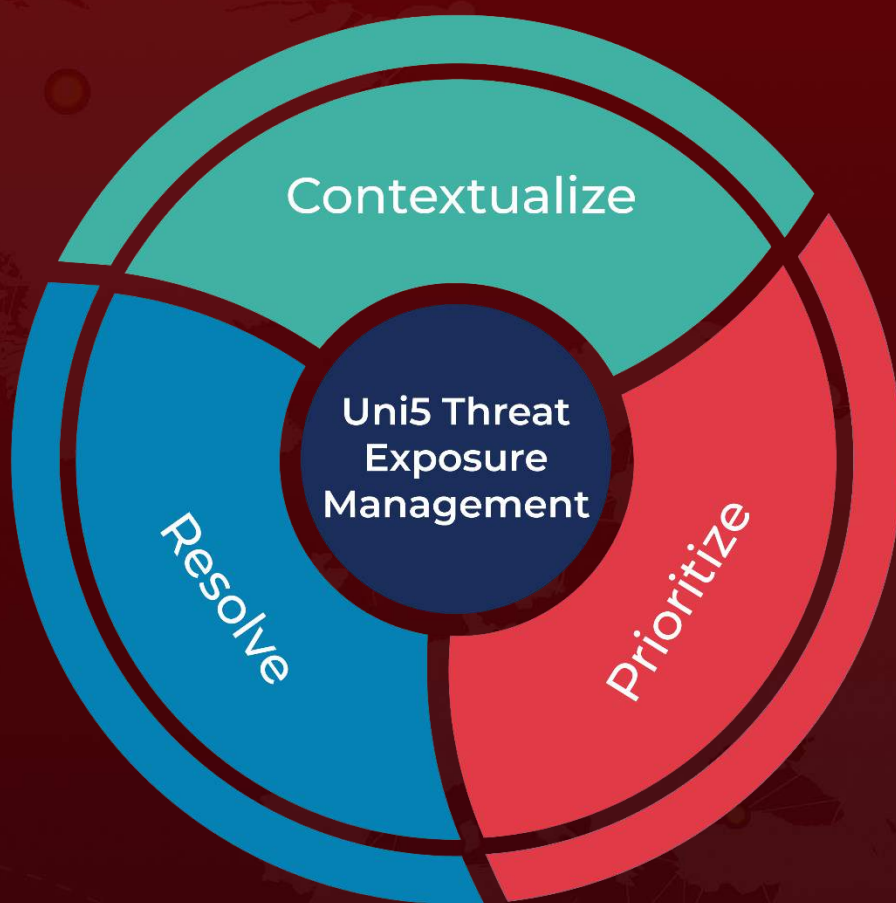
Click on any of the icons to get directed to the advisory

	Red Vulnerability Report
	Amber Vulnerability Report
	Green Vulnerability Report
	Red Attack Report
	Amber Attack Report
	Red Actor Report
	Amber Actor Report

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 1, 2023 • 4:30 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com