Date of Publication
April 3, 2023

Hive Pro

HiveForce Labs

MONTHLY
THREAT DIGEST

Vulnerabilities, Actors, and Attacks

MARCH 2023

Top 5 Takeaways

#1 In March, four zero-day vulnerabilities were addressed, while four others had no patch and were being exploited.

#2 Throughout the month, multiple active strains of ransomware were observed, including IceFire, BianLian, Dark Power, BlackSnake, and Royal.

#3 Unknown actors from Russia were focusing on exploiting an elevation of privilege vulnerability (CVE-2023-23397) present in Microsoft Outlook.

#4 Lazarus carried out the SmoothOperator campaign by exploiting a vulnerability (CVE-2023-29059) in 3CXDesktopApp, which allowed them to target organizations across the globe.

#5 Several Remote Access Trojans, such as KeySteal, EggShell RAT, DazzleSpy, CloudMensis, Remcos RAT, AsyncRAT, HiatusRAT, Snip3, and ParallaxRAT, were active during March.

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
65	24	50	France Norway Turkey Cyprus India	Government Technology Manufacturing Telecommunications Financial	248

Detailed Report

Vulnerabilities of the Month

VENDOR	CVE	PATCH DETAILS
TRUSTED COMPUTING GROUP	CVE-2023-1017 CVE-2023-1018	https://trustedcomputinggroup.org/resource/errata-for-tpm-library-specification-2-0/
cisco	CVE-2023-20078 CVE-2023-20079 CVE-2022-20968*	CVE-2023-20078: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP CVE-2023-20079; CVE-2022-20968: No patch available
FORTINET	CVE-2022-41329 CVE-2022-42476 CVE-2023-25610 CVE-2022-41328 CVE-2022-45861 CVE-2022-29056 CVE-2023-25605 CVE-2022-39951 CVE-2022-41333 CVE-2023-23776 CVE-2022-22297 CVE-2022-40676 CVE-2022-39953 CVE-2022-27490 CVE-2023-25611	https://www.fortiguard.com/psirt/FG-IR-22-477 https://www.fortiguard.com/psirt/FG-IR-22-401 https://www.fortiguard.com/psirt/FG-IR-20-078 https://www.fortiguard.com/psirt/FG-IR-22-364 https://www.fortiguard.com/psirt/FG-IR-23-001 https://www.fortiguard.com/psirt/FG-IR-23-050 https://www.fortiguard.com/psirt/FG-IR-22-488 https://www.fortiguard.com/psirt/FG-IR-22-254 https://www.fortiguard.com/psirt/FG-IR-22-388 https://www.fortiguard.com/psirt/FG-IR-22-447 https://www.fortiguard.com/psirt/FG-IR-21-218 https://www.fortiguard.com/psirt/FG-IR-22-369 https://www.fortiguard.com/psirt/FG-IR-22-281 https://www.fortiguard.com/psirt/FG-IR-22-309 https://www.fortiguard.com/psirt/FG-IR-18-232 https://www.fortiguard.com/psirt/FG-IR-21-218
Microsoft	CVE-2022-21894 CVE-2023-23415 CVE-2023-23397* CVE-2023-23404 CVE-2023-23411 CVE-2023-23416 CVE-2023-23392 CVE-2023-21708 CVE-2023-1017 CVE-2023-1018 CVE-2023-24880*	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21894 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23415 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23397 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23404 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23411 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23416 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23392 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21708 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-1017 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-1018 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24880
3CX	CVE-2023-29059	No Patch Available

* zero-day vulnerability

VENDOR	CVE	PATCH DETAILS
	CVE-2023-1213 CVE-2023-1214 CVE-2023-1215 CVE-2023-1216 CVE-2023-1217 CVE-2023-1218 CVE-2023-1219 CVE-2023-1220 CVE-2023-1221 CVE-2023-1222 CVE-2023-1223 CVE-2023-1224 CVE-2023-1225 CVE-2023-1227 CVE-2023-1229 CVE-2023-1230 CVE-2023-1231 CVE-2023-1232 CVE-2023-1234 CVE-2023-1235	Update Google Chrome to version 111.0.5563.64 for Mac/Linux and 111.0.5563.64/.65 for Windows. Patch Link https://www.google.com/intl/en/chrome/?standalone=1
IBM Aspera	CVE-2022-47986	https://www.ibm.com/support/pages/node/6952319
Cf	CVE-2023-26359 CVE-2023-26360* CVE-2023-26361	ColdFusion 2018 update 15 and earlier versions to update 16 ColdFusion 2021 update 5 and earlier versions to update 6 https://coldfusion.adobe.com/2023/03/released-coldfusion-2021-and-2018-march-2023-security-updates/
HUAWEI	CVE-2017-17215	No Patch Available
REALTEK	CVE-2014-8361	No Patch Available
APACHE	CVE-2021-44228 CVE-2023-23638	https://logging.apache.org/log4j/2.x/security.html https://github.com/apache/dubbo/releases
Jira	CVE-2021-26084	https://jira.atlassian.com/browse/CONFSERVER-67940
citrix	CVE-2019-19781	https://support.citrix.com/article/CTX267027
GitLab	CVE-2021-22205	http://about.gitlab.com/releases/2021/04/14/security-release-gitlab-13-10-3-released/
JBoss	CVE-2017-7504	No Patch Available
ORACLE	CVE-2020-14750	https://www.oracle.com/security-alerts/alert-cve-2020-14750.html

* zero-day vulnerability

Threat Actors of the Month

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Blackfly (APT41, Wicked Panda, Winnti Group)	China	Materials, composites semiconductor, telecoms, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food.	Asia
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Iron Tiger (APT 27,Emissary Panda,LuckyMouse,Bronze Union,TG-3390,TEMP.Hippo,Budworm,Group 35,ATK 15,Earth Smilodon,Red Phoenix,ZipToken)	China	Aerospace, Aviation, Defense, Education, Embassies, Government, Manufacturing, Technology, Telecommunications, and Think Tanks.	Australia, Canada, China, Germany, Hong Kong, India, Iran, Israel, Japan, Mongolia, Philippines, Russia, Spain, South Korea, Taiwan, Thailand, Tibet, Turkey, UK, USA and Middle East.
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
APT-C-61 (Tengyun Snake)	Unknown	National Institutions, Military, Government, Chimical, Diplomats and Scientific Research	South Asia, Iran, Turkey
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Mustang Panda APT (Bronze President, TEMP.Hex , HoneyMyte, Red Lich, Earth Preta)	China	Political, Aviation, Education, Government, NGOs, Think Tanks, Telecommunications	Australia, Bangladesh, Belgium, China, Cyprus, Ethiopia, Germany, Greece, Hong Kong, India, Indonesia, Japan, Mongolia, Myanmar, Nepal, Pakistan, Philippines, Russia, Singapore, South Africa, South Korea, South Sudan, Taiwan, UK, USA, Vietnam and UN, Europe, and Asia
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
DEV-0569	Unknown	Industrial, Engineering, Transportation, Education, Retail, Government, Aerospace, Defense, Gas Utilities, Food Products, Consumer, Pharmaceuticals, Automotive, Legal, Renewable Electricity, Insurance, Airlines, Media, Financial, Technology, Storage & Peripherals, HealthCare, Hotels, Real estate, Telecommunications, Building Materials, Electrical Equipment, Banks, Manufacturing	France, Spain, United States, Brazil, Mexico, India, Germany, Italy, Canada, Australia, Portugal, United Kingdom, Netherlands, China, Trinidad and Tobago, Belgium, Puerto Rico, Finland, Cote d'Ivoire, Malaysia
	MOTIVE		
	Financial gain		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
TA499(Vovan; Lexus)	Russia **MOTIVE** Sabotage and Espionage **CVEs**	Government	North America and Europe

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Sharp Panda	China **MOTIVE** Information theft and espionage **CVEs**	Government	Southeast Asia

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
8220 gang	China **MOTIVE** Financial gain **CVEs**	Technology, Cloud service vendors	USA, Sweden, Spain, Mali, Norway, China, Australia

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Dark Pink APT (Saaiwc Group, APT-LY-005)	Unknown	Government	ASEAN countries
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Tick(BRONZE BUTLER, CTG-2006, REDBALDKNIGHT, Stalker Panda)	China	Cybersecurity, Government, Defense	East Asia
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
YoroTrooper	Unknown	Energy and Government	Europe and CIS countries
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
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, BlueBravo)	China **MOTIVE** Information theft and espionage **CVEs**	Defense, Energy, Government, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks, and Imagery.	Australia, Azerbaijan, Belarus, Belgium Brazil, Bulgaria, Canada, Chechnya, China, Cyprus, Czech, France, Georgia, Germany, Hungary, India, Ireland, Israel, Japan, Kazakhstan, Kyrgyzstan, Latvia, Lebanon, Lithuania, Luxembourg, Mexico, Montenegro, Netherlands, New Zealand, Poland, Portugal, Romania, Russia, Slovakia, Slovenia, Spain, South Korea, Turkey, Uganda, UK, Ukraine, USA, Uzbekistan

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

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
UNC3886	China		Worldwide
	MOTIVE		
	Information theft and espionage		
	CVEs		
	CVE-2022-41328		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED CITIES
Bad magic	Unknown	Administrative, Agriculture, and Transportation	Donetsk, Lugansk, and Crimea (Cities in Ukraine)
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Winter Vivern (UAC-0114)	Unknown	Government, Telecommunications, and Private businesses.	Azerbaijan, Cyprus, Poland, Lithuania, India, Vatican, Ukraine, Italy, and Slovakia
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED CITIES
UNC961(Prophet Spider)	Unknown	Energy, Financial Services, Healthcare, Manufacturing, Media, Retail, Technology, Telecommunications	North America, India, United Kingdom, United States
	MOTIVE		
	Information theft and espionage; Financial Gain		
	CVEs		
	CVE-2021-44228 CVE-2021-26084 CVE-2019-19781 CVE-2020-14750 CVE-2021-22205 CVE-2017-7504		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Dark Power ransomware	Unknown	All industries	Worldwide
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
ChinaZ	China		Worldwide
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Bitter APT	South Asia	Energy, Engineering, Government	Bangladesh, China, India, Pakistan, and Saudi Arabia
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Gallium(aka Phantom Panda)	China	Telecommunications	Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, UAE, Yemen.
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT 41	China	Telecommunications	Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, UAE, Yemen.
	MOTIVE		
	Financial crime, Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Donot group (APT-Q-38)	South Asia	Government agencies, Defense military	Afghanistan, China, Bangladesh, Bhutan, India, Iran, Maldives, Nepal, Pakistan, and Sri Lanka.
	MOTIVE		
	Espionage and Information theft		
	CVEs		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
LABYRINTH CHOLLIMA (aka HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Lazarus Group)	North Korea	Automotive, Food & Beverage, Hospitality, Managed Information Technology Service Provider (MSP), Manufacturing	Worldwide
	MOTIVE		
	Financial gain and Information Theft		
	CVEs		
	CVE-2023-29059		

Malware of the Month

NAME	OVERVIEW	TYPE	DELIVERY METHOD
SCARLETEEL	The SCARLETEEL operation was a sophisticated cloud operation that involved stealing sensitive data by exploiting a misconfigured Kubernetes container, gaining access to one AWS account and attempting to pivot to additional associated AWS accounts.	Malware Family	exploiting a public-facing service in a self-managed Kubernetes cluster
ParallaxRAT	ParallaxRAT carries out numerous malicious activities, including keylogging and remote control of affected machines. Specifically, it gains unauthorized access to files, captures keystrokes, and takes control of the remote desktop.	Remote Access Trojan	via phishing emails
SysUpdate	SysUpdate was designed to target Linux platforms and evade detection by utilizing a sophisticated loading mechanism. Additionally, it employed a unique method of command-and-control communication through DNS TXT queries, which allowed for precise targeting of a vulnerability in a program signed by Wazuh.	Trojan	Unknown
Snip3	Snip3 crypter, a multi-stage remote access trojan (RAT) loader, was recently identified distributing RAT families such as QuasarRAT and DcRAT to target victims across numerous industry verticals, and the crypter has been updated with advanced approaches that allow it to deploy the final Remote Access Trojan (RAT) payload while remaining undetected.	Remote Access Trojan	via phishing emails

NAME	OVERVIEW	TYPE	DELIVERY METHOD
MQsTTang	MQsTTang is a custom backdoor attributed to the Mustang Panda APT group. It uses the MQTT protocol for C&C communication and is distributed via spearphishing through RAR archives with names related to diplomacy and passports.	Backdoor	via phishing emails
Royal Ransomware	Royal ransomware is distinct in that it uses a custom-made file encryption tool as well as double extortion tactics. The latter entails threatening to publicly expose encrypted data if the victim does not pay a ransom in Bitcoin. The demanded amount typically spans from $1 million to $11 million.	Ransomware	Via phishing emails or RDP compromise
LokiBot	LokiBot is a constantly evolving information-stealing malware that creates a backdoor on infected machines to collect sensitive data, and it uses ISO files and API hashing techniques to bypass detection and inject malicious code.	Infostealer	Via phishing emails
HiatusRAT	The Hiatus hacking campaign targets DrayTek Vigor routers to steal data and create a covert proxy network. The campaign uses a malicious script, HiatusRAT malware, and tcpdump to capture network traffic and pass command and control server traffic through a SOCKS5 proxy.	Remote Access Trojan	Via business-grade routers, specifically, DrayTek Vigor models 2960 and 3900 running an i386 architecture.
RedLine	RedLine Stealer collects a wide range of data and sent it to the command-and-control server.	Infostealer	Via phishing emails

NAME	OVERVIEW	TYPE	DELIVERY METHOD
ImBetter	ImBetter Stealer malware has been discovered to be capable of stealing sensitive data and cryptocurrency wallets from its victims through phishing websites. These fake sites imitate popular crypto-wallets and online file converters, tricking users into downloading the malware and putting their confidential information at risk.	Stealer	Via phishing websites
SYS01	The SYS01 stealer has been targeting critical government infrastructure employees, manufacturing companies, and other industries, and using various delivery techniques, including DLL side-loading, to steal and exfiltrate information from victims	Stealer	Via Google ads
AsyncRAT	AsyncRAT is a .NET-based open-source RAT that allows remote access and control of computers with keylogging and defense evasion features, making it popular among cybercriminals. Its configuration is encrypted with AES-256 in CBC mode and has been publicly available since 2019	Remote Access Trojan	Via OneNote attachments
FormBook	FormBook is an infostealer malware that extracts different kinds of data from compromised systems, such as keystrokes, screenshots, and credentials saved in web browsers.	Infostealer	Via OneNote attachments
BlackSnake	BlackSnake ransomware has been discovered with clipper functionality that intercepts and replaces the cryptocurrency wallet addresses of victims with those of attackers.	Ransomware	Unknown

NAME	OVERVIEW	TYPE	DELIVERY METHOD
ScrubCrypt	ScrubCrypt is a crypter used by the 8220 gang that utilizes a distinctive BAT packing mechanism to secure applications. After undergoing Base64 decoding, AES decryption, and unzipping, the regular .NET Reflective Injection code is visible.	Crypter	Via phishing websites
GoBruteforcer	GoBruteforcer malware targets web servers and uses Golang programming language. It employs CIDR block scanning to access servers through brute force and deploy an IRC bot with the attacker's URL.	Trojan	Via brute force
KamiKakaBot	KamiKakaBot malware is designed to steal data from web browsers such as Chrome, Edge, and Firefox, including saved credentials, browsing history, and cookies. It can also allow the attackers to execute remote code on infected devices.	Infostealer	via phishing emails
BlackLotus	BlackLotus is a dangerous UEFI bootkit that can take full control of the operating system boot process, allowing it to disable security measures and deploy its own payloads; it exploits a known vulnerability in UEFI Secure Boot and is capable of running on up-to-date Windows 11 systems, and is advertised and sold on underground forums for $5,000 to unknown threat actors.	Bootkit	Via CVE-2022-21894
IceFire ransomware	The IceFire ransomware strain, previously identified on Windows systems, has now expanded its scope to target Linux enterprise networks of several media and entertainment industry organizations.	Ransomware	Via CVE-2022-47986

NAME	OVERVIEW	TYPE	DELIVERY METHOD
Prometei	The Prometei v3 botnet, an upgraded version of the Prometei botnet malware, has compromised over 10,000 systems mining the Monero cryptocurrency.	Botnet	Via phishing websites
BianLian ransomware	BianLian ransomware group is ramping up data-leak extortion to extract payments, using similar tactics & a custom backdoor, and bringing 30 new C2 servers online monthly.	Ransomware	Unknown
DotRunpeX	DotRunpeX malware attack vectors have been linked to dozens of campaigns. The DotRunpeX is a second-stage infection used to deploy a variety of malware families, most notably stealers, RATs, loaders, and downloaders.	Injector	Unknown
Chinotto	Chinotto is a malware with variants for Windows, Android, and Powershell, and can communicate with its command-and-control server using HTTP commands.	BackDoor	via phishing emails
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	Infostealer	Via Bundlers
Gozi	Gozi is a binary that bypasses Italy's geofencing and creates a loader process on the victim's computer.	Loader	via phishing emails

NAME	OVERVIEW	TYPE	DELIVERY METHOD
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.	Botnet	Via old vulnerabilities and weak credentials
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.	Backdoor	Unknown
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.	Backdoor	Unknown
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.	Trojan	via Malvertising and Spamming campaigns

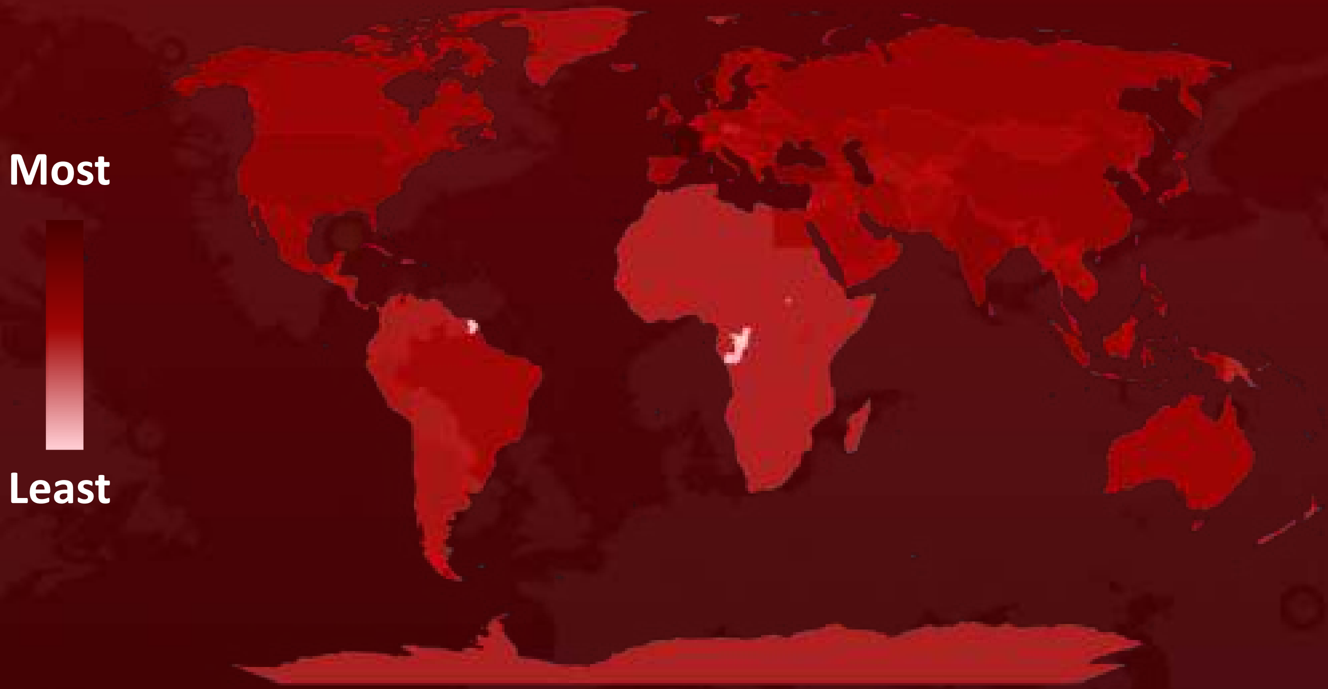
NAME	OVERVIEW	TYPE	DELIVERY METHOD
ALC	ALC is a scareware posing as ransomware, as it does not encrypt files on the victim's device. ALC merely disables the task manager and displays a ransom notice on the locked screen.	Infostealer	Via Bundlers
CloudMensis	CloudMensis (BadRAT) is distributed as a malicious Microsoft Word document, which executes a macro when opened, allowing the attacker to gain remote access and control of the victim's computer.	Remote Access Trojan	Via malicious Microsoft Word document
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.	Remote Access Trojan	Unknown
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.	Remote Access Trojan	Via social engineering tactics
KeySteal	Keysteal is a malicious app designed to extract user passwords and other credentials stored in macOS Keychain without administrator privileges	Remote Access Trojan	Via malicious app

NAME	OVERVIEW	TYPE	DELIVERY METHOD
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.	Point-of-sale	Via phishing emails
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.	Infostealer	Via phishing emails
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.	Infostealer	Via phishing emails
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.	Trojan	Via trojanized versions of iTerm2
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	Infostealer	removable media and hijacks crypto wallets

NAME	OVERVIEW	TYPE	DELIVERY METHOD
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	Malware-as-a-service	Unknown
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.	Trojan	Via compromised WordPress websites
Dark Power Ransomware	Dark Power ransomware uses Nim programming language to create malware that encrypts specific services and processes, excludes crucial system files, clears logs, and generates a ransom note in every folder	Ransomware	Unknown
ChinaZ DDoSClient (or ChinaZ)	ChinaZ DDoSClient is an infamous DDoS botnet used by a Chinese threat group to target Windows and Linux systems, likely by using stolen account credentials from scanners and SSH Brute Force malware.	DDoS botnets	Unknown
mim221	A Chinese cyber espionage group attributed to the Operation Soft Cell campaign has been observed infiltrating Microsoft Exchange servers to deploy web shells for command execution.	Stealer	Unknown
DBatLoader (aka ModiLoader and NatsoLoader)	DBatLoader is used to deliver the payload, the attackers use multilayer obfuscation techniques and various file formats, such as PDF, HTML, ZIP, and OneNote.	Loader	Via phishing emails

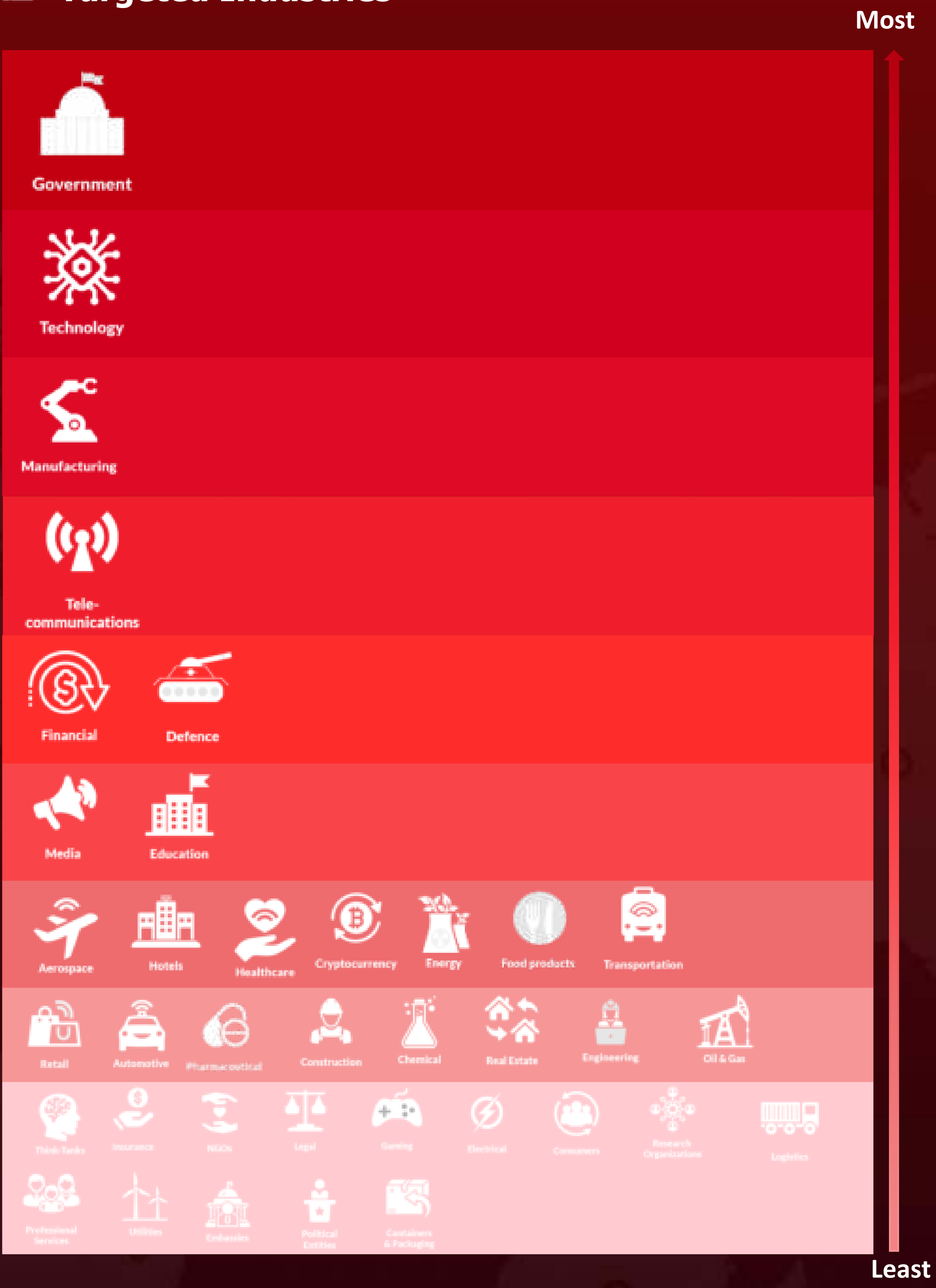
NAME	OVERVIEW	TYPE	DELIVERY METHOD
Formbook	The FormBook stealer can search for, viewing, interact with files, and take screenshots. The malware has advanced stealing and evasion functions including the ability to pull stored and recorded victim input.	Information stealer	Via DBatLoader
Remcos RAT	Remcos is a RAT that attackers use to perform actions on infected machines remotely and control PCs with any Windows OS, including XP and newer. The RAT captures screenshots, record keystrokes, and send the collected information.	Remote Access Trojan	Via DBatLoader
Creal Stealer	The Creal stealer binary is compiled with PyInstaller, indicating that it was written in Python. There are 50 samples in the wild, demonstrating that threat actors were actively using the open-source code to infect unwitting victims.	DDoS botnets	Via Phishing site impersonating a cryptocurrency mining platform
ICONIC Stealer (aka SUDDENICON)	The SmoothOperator campaign conducted a supply chain attack targeting downstream customers via rigged installers. The ICO file containing URLs hosting the final-stage payload ICONIC Stealer is capable of harvesting system information and sensitive data stored in web browsers.	Stealer	Via Compromised 3CX DesktopApp vulnerability (CVE-2023-29059)
Donot	Donot samples use different malicious code implantation methods and change the code details of attack components. Donot executes shellcode to download subsequent DLL components by carrying macros in documents.	Downloader	Using macro documents, self-extracting RAR archives, and EXE components

Targeted Countries



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

Targeted Industries



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	T1053: Scheduled Task/Job	T1037: Boot or Logon Initialization Scripts	T1205: Traffic Signaling
T1589.002: Email Addresses	T1583.001: Domains	T1078.002: Domain Accounts	T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1053: Scheduled Task/Job	T1006: Direct Volume Access
T1590: Gather Victim Network Information	T1583.003: Virtual Private Server	T1091: Replication Through Removable Media	T1053.005: Scheduled Task	T1078: Valid Accounts	T1053.005: Scheduled Task	T1014: Rootkit
T1590.002: DNS	T1583.004: Server	T1133: External Remote Services	T1059: Command and Scripting Interpreter	T1078.002: Domain Accounts	T1055: Process Injection	T1027: Obfuscated Files or Information
T1593: Search Open Websites/Domains	T1584: Compromise Infrastructure	T1189: Drive-by Compromise	T1059.001: PowerShell	T1133: External Remote Services	T1055.002: Portable Executable Injection	T1027.001: Binary Padding
T1593.002: Search Engines	T1584.005: Botnet	T1190: Exploit Public-Facing Application	T1059.003: Windows Command Shell	T1197: BITS Jobs	T1055.003: Thread Execution Hijacking	T1027.002: Software Packing
T1595: Active Scanning	T1584.006: Web Services	T1195: Supply Chain Compromise	T1059.004: Unix Shell	T1205: Traffic Signaling	T1055.011: Extra Window Memory Injection	T1027.005: Indicator Removal from Tools
	T1586: Compromise Accounts	T1195.002: Compromise Software Supply Chain	T1059.005: Visual Basic	T1542: Pre-OS Boot	T1055.012: Process Hollowing	T1027.006: HTML Smuggling
	T1587: Develop Capabilities	T1199: Trusted Relationship	T1059.006: Python	T1542.003: Bootkit	T1078: Valid Accounts	T1027.007: Dynamic API Resolution
	T1587.001: Malware	T1566: Phishing	T1106: Native API	T1574: Hijack Execution Flow	T1078.002: Domain Accounts	T1027.009: Embedded Payloads
	T1587.002: Code Signing Certificates	T1566.001: Spearphishing Attachment	T1129: Shared Modules	T1574.002: DLL Side-Loading	T1134: Access Token Manipulation	T1036: Masquerading
	T1588: Obtain Capabilities	T1566.002: Spearphishing Link	T1203: Exploitation for Client Execution	T1037: Boot or Logon Initialization Scripts	T1134.002: Create Process with Token	T1036.004: Masquerade Task or Service
	T1588.002: Tool		T1204: User Execution	T1098: Account Manipulation	T1484: Domain Policy Modification	T1036.005: Match Legitimate Name or Location
	T1588.005: Exploits		T1204.001: Malicious Link	T1137: Office Application Startup	T1484.001: Group Policy Modification	T1036.006: Space after Filename
	T1588.006: Vulnerabilities		T1204.002: Malicious File	T1176: Browser Extensions	T1543: Create or Modify System Process	T1036.007: Double File Extension
	T1608: Stage Capabilities		T1559: Inter-Process Communication	T1505: Server Software Component	T1543.001: Launch Agent	T1055: Process Injection
	T1608.001: Upload Malware		T1559.002: Dynamic Data Exchange	T1505.003: Web Shell	T1543.002: Systemd Service	T1055.002: Portable Executable Injection
	T1608.002: Upload Tool		T1569: System Services	T1543: Create or Modify System Process	T1543.003: Windows Service	T1055.003: Thread Execution Hijacking
			T1569.002: Service Execution	T1543.001: Launch Agent	T1543.004: Launch Daemon	T1055.011: Extra Window Memory Injection
				T1543.002: Systemd Service	T1546: Event Triggered Execution	T1055.012: Process Hollowing
				T1543.003: Windows Service	T1546.004: Unix Shell Configuration Modification	T1070: Indicator Removal
				T1543.004: Launch Daemon	T1546.008: Accessibility Features	T1070.001: Clear Windows Event Logs
				T1546: Event Triggered Execution	T1546.016: Installer Packages	T1070.003: Clear Command History
				T1546.004: Unix Shell Configuration Modification	T1547: Boot or Logon Autostart Execution	T1070.004: File Deletion
				T1546.008: Accessibility Features	T1547.001: Registry Run Keys / Startup Folder	T1070.006: Timestomp
				T1546.016: Installer Packages	T1547.004: Winlogon Helper DLL	T1070.007: Clear Network Connection History and Configurations
				T1547: Boot or Logon Autostart Execution	T1547.006: Kernel Modules and Extensions	T1070.009: Clear Persistence
				T1547.001: Registry Run Keys / Startup Folder	T1547.010: Port Monitors	T1078: Valid Accounts
				T1547.004: Winlogon Helper DLL	T1548: Abuse Elevation Control Mechanism	T1078.002: Domain Accounts
				T1547.006: Kernel Modules and Extensions	T1548.002: Bypass User Account Control	T1112: Modify Registry
				T1547.010: Port Monitors	T1574: Hijack Execution Flow	T1134: Access Token Manipulation
					T1574.002: DLL Side-Loading	T1134.002: Create Process with Token
					T1068: Exploitation for Privilege Escalation	T1140: Deobfuscate/Decode Files or Information
						T1197: BITS Jobs
						T1202: Indirect Command Execution
						T1218: System Binary Proxy Execution
						T1218.001: Compiled HTML File
						T1218.005: Mshta
						T1218.007: Msiexec
						T1218.011: Rundll32
						T1222: File and Directory Permissions Modification
						T1222.002: Linux and Mac File and Directory Permissions Modification
						T1480: Execution Guardrails
						T1484: Domain Policy Modification
						T1484.001: Group Policy Modification
						T1497: Virtualization/Sandbox Evasion
						T1497.001: System Checks
						T1497.003: Time Based Evasion
						T1542: Pre-OS Boot
						T1542.003: Bootkit
						T1548: Abuse Elevation Control Mechanism
						T1548.002: Bypass User Account Control
						T1550: Use Alternate Authentication Material
						T1550.002: Pass the Hash
						T1553: Subvert Trust Controls
						T1553.001: Gatekeeper Bypass
						T1553.002: Code Signing
						T1562: Impair Defenses
						T1562.001: Disable or Modify Tools
						T1564: Hide Artifacts
						T1564.001: Hidden Files and Directories
						T1574: Hijack Execution Flow
						T1574.002: 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
T1056: Input Capture	T1040: Network Sniffing	T1091: Replication Through Removable Media	T1005: Data from Local System	T1001: Data Obfuscation	T1020: Automated Exfiltration	T1485: Data Destruction
T1056.001: Keylogging	T1497: Virtualization/Sandbox Evasion	T1550: Use Alternate Authentication Material	T1025: Data from Removable Media	T1071: Application Layer Protocol	T1041: Exfiltration Over C2 Channel	T1486: Data Encrypted for Impact
T1056.002: GUI Input Capture	T1497.001: System Checks	T1550.002: Pass the Hash	T1039: Data from Network Shared Drive	T1071.001: Web Protocols	T1048: Exfiltration Over Alternative Protocol	T1489: Service Stop
T1003: OS Credential Dumping	T1497.003: Time Based Evasion	T1021: Remote Services	T1056: Input Capture	T1071.002: File Transfer Protocols	T1537: Transfer Data to Cloud Account	T1490: Inhibit System Recovery
T1003.001: LSASS Memory	T1622: Debugger Evasion	T1021.001: Remote Desktop Protocol	T1056.001: Keylogging	T1090: Proxy	T1567: Exfiltration Over Web Service	T1496: Resource Hijacking
T1003.003: NTDS	T1007: System Service Discovery	T1021.002: SMB/Windows Admin Shares	T1056.002: GUI Input Capture	T1090.003: Multi-hop Proxy	T1567.002: Exfiltration to Cloud Storage	T1498: Network Denial of Service
T1040: Network Sniffing	T1010: Application Window Discovery	T1021.004: SSH	T1074: Data Staged	T1095: Non-Application Layer Protocol		T1499: Endpoint Denial of Service
T1110: Brute Force	T1012: Query Registry	T1080: Taint Shared Content	T1074.001: Local Data Staging	T1102: Web Service		T1529: System Shutdown/Reboot
T1212: Exploitation for Credential Access	T1016: System Network Configuration Discovery	T1210: Exploitation of Remote Services	T1113: Screen Capture	T1102.001: Dead Drop Resolver		T1565: Data Manipulation
T1528: Steal Application Access Token	T1016.001: Internet Connection Discovery	T1570: Lateral Tool Transfer	T1114: Email Collection	T1102.002: Bidirectional Communication		T1565.001: Stored Data Manipulation
T1539: Steal Web Session Cookie	T1018: Remote System Discovery		T1114.001: Local Email Collection	T1104: Multi-Stage Channels		
T1552: Unsecured Credentials	T1033: System Owner/User Discovery		T1115: Clipboard Data	T1105: Ingress Tool Transfer		
T1552.001: Credentials In Files	T1046: Network Service Discovery		T1119: Automated Collection	T1132: Data Encoding		
T1552.002: Credentials in Registry	T1049: System Network Connections Discovery		T1125: Video Capture	T1132.001: Standard Encoding		
T1552.002: Credentials in Registry	T1057: Process Discovery		T1185: Browser Session Hijacking	T1132.002: Non-Standard Encoding		
T1552.004: Private Keys	T1069: Permission Groups Discovery		T1213: Data from Information Repositories	T1205: Traffic Signaling		
T1552.005: Cloud Instance Metadata API	T1069.001: Local Groups		T1560: Archive Collected Data	T1219: Remote Access Software		
T1555: Credentials from Password Stores	T1069.002: Domain Groups		T1560.001: Archive via Utility	T1571: Non-Standard Port		
T1555.001: Keychain	T1082: System Information Discovery		T1560.002: Archive via Library	T1572: Protocol Tunneling		
T1555.003: Credentials from Web Browsers	T1083: File and Directory Discovery			T1573: Encrypted Channel		
T1555.005: Password Managers	T1087: Account Discovery			T1573.001: Symmetric Cryptography		
T1558: Steal or Forge Kerberos Tickets	T1087.002: Domain Account			T1573.002: Asymmetric Cryptography		
	T1120: Peripheral Device Discovery					
	T1124: System Time Discovery					
	T1135: Network Share Discovery					
	T1482: Domain Trust Discovery					
	T1518: Software Discovery					
	T1518.001: Security Software Discovery					
	T1526: Cloud Service Discovery					
	T1614: System Location Discovery					

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **65 significant vulnerabilities** and block the indicators related to the **35 active threat actors, 50 active malware,** and **248 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 (March 2023)

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

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

🔴🐞	Red Vulnerability Report
🟡🐞	Amber 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.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

April 3, 2023 • 6:10 AM

More at www.hivepro.com