Date of Publication
January 2, 2023

Hive Pro

HiveForce Labs

MONTHLY
THREAT DIGEST

Vulnerabilities, Actors, and Attacks

DECEMBER 2022

Top 5 Takeaways

#1 In December, there were **15 zero-day** vulnerabilities, most of which were addressed by Microsoft

#2 Ransomware strains like **Blackhunt, NYX, Redeemer, Vohuk, Amelia, Putin Team, Meow, BlueSky, ScareCrow, Mallox, Agenda, Nokoyawa 2.0**, and **PloyVice** were active throughout the month.

#3 Several new malware families, such as **Miscloak, Darkdew, Bluehaze, DuckLogs, AppleJeus**, and **RisePro**, have been observed targeting victims all over the world.

#4 A new Chinese-speaking APT group called **MirrorFace** has been targeting **Japanese** political entities, while the **Lazarus** campaign has once again targeted **cryptocurrency** users and organizations by deploying a fake website.

#5 New botnets called **GoTrim**, **Truebot**, and **Zerobot** were also identified in December.

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
103	16	34	USA India Germany Vietnam Indonesia	Government Defense Financial Telecommunications Technology	177

Detailed Report

Significant Vulnerabilities of the Month

VENDOR	CVE	PATCH DETAILS
Microsoft	CVE-2022-41080 CVE-2022-41082* CVE-2022-41040* CVE-2022-41123 CVE-2022-37958 CVE-2017-0144* CVE-2021-1675 CVE-2021-34527* CVE-2017-11882 CVE-2018-0802* CVE-2022-44698* CVE-2022-44710* CVE-2022-44690 CVE-2022-44693 CVE-2022-41089 CVE-2022-41076 CVE-2022-44678 CVE-2022-44681 CVE-2022-44713 CVE-2022-41127 CVE-2022-44670 CVE-2022-44683 CVE-2020-1380* CVE-2019-0708 CVE-2021-26855* CVE-2022-41128*	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41080 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41123 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37958 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0144 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2018-0802 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44698 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44710 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44690 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44693 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41089 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41076 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44678 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44681 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44713 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41127 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44670 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44683 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1380 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128
citrix	CVE-2022-27518*	https://www.citrix.com/downloads/citrix-adc/ https://www.citrix.com/downloads/citrix-gateway/

VENDOR	CVE	PATCH DETAILS
vmware	CVE-2022-31702 CVE-2022-31703 CVE-2022-31700 CVE-2022-31701 CVE-2022-31705 CVE-2022-31707 CVE-2022-31708 CVE-2022-22965*	https://www.vmware.com/security/advisories/VMSA-2022-0031.html https://www.vmware.com/security/advisories/VMSA-2022-0032.html https://www.vmware.com/security/advisories/VMSA-2022-0033.html https://www.vmware.com/security/advisories/VMSA-2022-0034.html https://tanzu.vmware.com/security/cve-2022-22965
samba	CVE-2022-38023 CVE-2022-37966 CVE-2022-37967 CVE-2022-45141	https://www.samba.org/samba/history/security.html
cisco	CVE-2017-12240 CVE-2018-0125 CVE-2018-0147 CVE-2018-0171 CVE-2021-1497	https://sec.cloudapps.cisco.com/security/center/publicationListing.x
	CVE-2022-42854 CVE-2022-42821 CVE-2022-32942 CVE-2022-42861 CVE-2022-42864 CVE-2022-46689 CVE-2022-42845 CVE-2022-42842 CVE-2022-40303 CVE-2022-40304 CVE-2022-42840 CVE-2022-42855 CVE-2022-42841	https://support.apple.com/en-ae/HT213533
WordPress	CVE-2022-45359	https://www.wordfence.com/blog/2022/12/psa-yith-woocommerce-gift-cards-premium-plugin-exploited-in-the-wild/
ForgeRock	CVE-2021-35464	https://backstage.forgerock.com/knowledge/kb/article/a47894244

VENDOR	CVE	PATCH DETAILS
	CVE-2022-4174 CVE-2022-4175 CVE-2022-4176 CVE-2022-4177 CVE-2022-4178 CVE-2022-4181 CVE-2022-4182 CVE-2022-4186 CVE-2022-4189 CVE-2022-4190 CVE-2022-4262*	https://www.google.com/intl/en/chrome/?standalone=1
FreeBSD	CVE-2022-23093	https://www.freebsd.org/security/advisories/FreeBSD-SA-22:15.ping.asc
ubuntu	CVE-2022-41974	https://ubuntu.com/security/CVE-2022-3328
debian	CVE-2022-41973 CVE-2022-3328	https://github.com/opensvc/multipath-tools/releases/tag/0.9.2
DW DIGITAL WATCHDOG Everything's Digital	CVE-2022-34538	No patch available
FLIR	CVE-2022-37061	https://gist.github.com/Nwqda/9e16852ab7827dc62b8e44d6180a6899
phpMyAdmin	CVE-2018-12613	No patch available
Tenda	CVE-2020-10987	No patch available
D-Link	CVE-2020-25506 CVE-2014-8361	No patch available
netwrix	CVE-2022-31199	https://bishopfox.com/blog/netwrix-auditor-advisory

VENDOR	CVE	PATCH DETAILS
FORTINET	CVE-2022-35843 CVE-2022-33876 CVE-2022-33875 CVE-2022-40680 CVE-2022-38379 CVE-2022-30305 CVE-2022-42475*	https://www.fortiguard.com/psirt/FG-IR-22-253 https://www.fortiguard.com/psirt/FG-IR-22-252 https://www.fortiguard.com/psirt/FG-IR-22-255 https://www.fortiguard.com/psirt/FG-IR-21-248 https://www.fortiguard.com/psirt/FG-IR-22-220 https://www.fortiguard.com/psirt/FG-IR-21-170 https://www.fortiguard.com/psirt/FG-IR-22-398
ZIVIF	CVE-2017-17106	No patch available
HUAWEI	CVE-2017-17215*	http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en
REALTEK	CVE-2021-35395	https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en
HIKVISION	CVE-2021-36260	No patch available
telesquare	CVE-2021-46422	No patch available
f5	CVE-2022-01388	No patch available
TOTO LINK The Smartest Network Device	CVE-2022-25075 CVE-2022-26186 CVE-2022-26210	https://github.com/EPhaha/IOT_vuln/blob/main/TOTOLink/A3000RU/README.md
ZYXEL	CVE-2022-30525	No patch available
	CVE-2022-47939 CVE-2022-47941 CVE-2022-47942 CVE-2022-47938 CVE-2022-47940	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.18.18 https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.2 https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.15.61

* zero-day vulnerability

Active Threat Actors of the Month

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
MirrorFace	China	Political entities, Media, Defense, Think tanks, Academic institutions, and diplomatic organizations	Japan
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
ScarCruft (Reaper, TEMP.Reaper, APT 37, Ricochet Chollima, Thallium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10)	North Korea	Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, and Transportation.	China, Czech, Hong Kong, India, Japan, Kuwait, Nepal, Poland, Romania, Russia, South Korea, UK, USA, and Vietnam.
	MOTIVE		
	Information theft and espionage		
	CVEs		
	CVE-2020-1380 CVE-2022-41128		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Scattered Spider		Telecommunications and Business process outsourcing	Worldwide
	MOTIVE		
	Financial crime		
	CVE		
	CVE-2021-35464		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
UNC4191	China	Public and Private sector	Southeast Asia, the U.S., and Europe.
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Lazarus Group (Labyrinth Chollima, 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)	North Korea	Aerospace, Defense, Energy, Engineering, Financial, Government, Media, Shipping and Logistics, Technology and BitCoin exchanges.	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		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
BackdoorDiplomacy	China	Government, Telecommunications.	Albania, Bhutan, Croatia, Georgia, Germany, Ghana, India, Libya, Namibia, Nigeria, Poland, Saudi Arabia, South Africa, Sri Lanka, UAE, Uzbekistan.
	MOTIVE		
	Information theft and espionage		
	CVEs		
	CVE-2021-26855		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Vice Society	Unknown **MOTIVE** Financial crime **CVE** CVE-2021-1675 CVE-2021-34527	Education, Food Products, Hotels, Financial Services, Professional Services, Insurance, HealthCare, Automotive, Transportation, Media, Pharmaceuticals, Retail, Manufacturing	Antigua and Barbuda, Argentina, Australia, Austria, Brazil, Canada, Colombia, France, Germany, Greece, India, Indonesia, Ireland, Italy, Lebanon, Malaysia, Netherlands, New Zealand, Saudi Arabia, Singapore, Spain, Sweden, Thailand, United Kingdom, United States

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Calisto (Cold River, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53)	Russia **MOTIVE** Information theft and espionage **CVEs**	Defense, NGOs, Think Tanks, communication technologies, Cybersecurity.	Canada, India, Lebanon, UAE, Ukraine, USA, Switzerland.

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Agrius (DEV-0227)	Iran **MOTIVE** Information theft and espionage, Sabotage and destruction **CVEs**	Jewelry, HR and IT consulting firms.	U.S.A, UK, Australia, Canada, France, Germany, Turkey, Japan, India, UAE, Israel.

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
TA505 (Graceful Spider,Gold Evergreen,Gold Tahoe,TEMP.Warlock,ATK 103,SectorJ04,Hive0065,Chimborazo)	Russia	Education	USA, Mexico, Pakistan, and Brazil
	MOTIVE		
	Financial crime, Financial gain		
	CVEs		
	CVE-2022-31199		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
SilenceGroup(Contract Crew,Whisper Spider,TEMP.TruthTeller,ATK 86,TAG-CR8)	NA	Education	USA, Mexico, Pakistan, and Brazil
	MOTIVE		
	Financial crime		
	CVEs		
	CVE-2022-31199		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
MuddyWater (Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17)	Iran	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation, Aerospace	Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Malta Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Pakistan, Russia, Saudi Arabia, Tajikistan, Thailand, Tunisia, Turkmenistan Turkey, UAE, Ukraine, USA
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Gamaredon Group (Winterflounder, Primitive Bear, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Shuckworm, Actinium, Trident Ursa, DEV-0157, UAC-0010)	Russia	Defense, Government, Law enforcement, NGO.	Albania, Austria, Australia, Bangladesh, Brazil, Canada, Chile, China, Colombia, Croatia, Denmark, Georgia, Germany, Guatemala, Honduras, India, Indonesia, Iran, Israel, Italy, Japan, Kazakhstan, Latvia, Malaysia, Netherlands, Nigeria, Norway, Pakistan, Papua New Guinea, Poland, Portugal, Romania, Russia, South Africa, South Korea, Spain, Sweden, Turkey, UK, Ukraine, USA, Vietnam.
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
Cloud Atlas (Inception Framework, Oxygen, ATK 116 , The Rocra)	Russia	Aerospace, Defense, Embassies, Energy, Engineering, Financial, Government, Oilandgas, Research	Afghanistan, Armenia, Austria, Azerbaijan, Belarus, Belgium, Brazil, Congo, Cyprus, France, Georgia, Germany, Greece, India, Indonesia, Iran, Italy, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Lebanon, Lithuania, Malaysia, Moldova, Morocco, Mozambique, Oman, Pakistan, Paraguay, Portugal, Qatar, Romania, Russia, SaudiArabia, Slovenia, SouthAfrica, Suriname, Switzerland, Tajikistan, Tanzania, Turkey, Turkmenistan, Uganda, Ukraine, UAE, USA, Uzbekistan, Venezuela, Vietnam
	MOTIVE		
	Information theft and espionage		
	CVEs		
	CVE-2017-11882 CVE-2018-0802		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
SideCopy	Pakistan	Defense, Embassies, Government	India
	MOTIVE		
	Financial crime		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
BlueNoroff (APT 38, Stardust Chollima , CTG-6459, Nickel Gladstone, T-APT-15, ATK 117)	North Korea	Cryptocurrencies, smart contracts, DeFi, blockchains, and FinTech industry	Russia, Poland, Slovenia, Ukraine, China, India, US, Hong Kong, Singapore, the UAE, Indonesia, the UK, Sweden, Germany, Bulgaria, Estonia, Malta, Czechia, Japan
	MOTIVE		
	Financial crime		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
APT5 (aka Bronze Fleetwood, Keyhole Panda, Manganese, UNC2630)	China	Defense, High-Tech, Industrial, Technology, Telecommunications	Burma, Brunei, East Timor, Vietnam, Indonesia, Cambodia, Laos, Malaysia, Singapore, Thailand, Philippines
	MOTIVE		
	Information theft and espionage		
	CVE		
	CVE-2022-27518		

Active Malware of the Month

NAME	OVERVIEW	TYPE	DELIVERY METHOD
BLUELIGHT	Bluelight is a type of malware that allows an attacker to gain unauthorized access to a computer or network. It can allow the attacker to remotely control the system and access sensitive data.	Backdoor	Phishing emails
MISTCLOAK	MISTCLOAK is a launcher written in C++ that executes an encrypted executable payload stored in a file on disk. It is usually introduced inside networks via an infected USB device.	Malware Family	Unknown
BLUEHAZE	BLUEHAZE is a type of malware that is designed to launch NCAT and create a reverse shell to a predetermined command and control (C2) server. It is written in C/C++ and is used by attackers to gain remote access to a target system.	Malware Family	Unknown
DARKDEW	DARKDEW is a malware that is written in C++ and specifically targets removable drives, such as USB sticks or external hard drives. It is designed to install other malware onto a system when the infected drive is connected to it.	Malware Family	Unknown
NCAT	NCAT is a tool that can be used for a range of networking tasks, including security and administration. It is a command-line utility that was developed as part of the Nmap Project.	Malware Family	Unknown
DuckLogs	DuckLogs is a new info-stealing malware variant, it captures and exfiltrates data from infected PCs such as credentials, cookies, crypto wallets, browser data, and others.	Info Stealer	Malware-as-a-Service

NAME	OVERVIEW	TYPE	DELIVERY METHOD
Redeemer	Redeemer is written in C/C++ binary that targets Windows. The executable encrypts the victim's system and drops a ransom note named “Read Me.TXT”	Ransomware	Unknown
NYX	NYX is written in C/C++ ransomware developed in 2022. The group claims to exfiltrate the victim's data before encryption and may use a Double Extortion scheme.	Ransomware	Unknown
Vohuk	Vohuk Ransomware is a type of malware that encrypts a victim's files and demands a ransom from the victim to restore access to the files.	Ransomware	Phishing emails and Malicious adds
BlackHunt	Blackhunt is a new ransomware that targets RDP ports.	Ransomware	Malicious email attachments
AppleJeus	AppleJeus is a type of malware that specifically targets the Mac operating system. It was first discovered in 2018 and is thought to be the work of the Lazarus Group	Malware	Phishing emails and malicious software updates
Irafau	The Irafau is a backdoor trojan is a type of malware that enables a remote user to have unauthorized access to the infected computer.	backdoor	Unknown
Quarian	The Quarian is a backdoor trojan is a type of malware that enables a remote user to have unauthorized access to the infected computer.	backdoor	Unknown
BlackMagic	BlackMagic ransomware gang targets its victims using a double extortion approach in which it initially exfiltrates the victim's data, followed by encryption, and has primarily targeted several firms in Israel's transportation and logistics niche.	Ransomware	Phishing emails

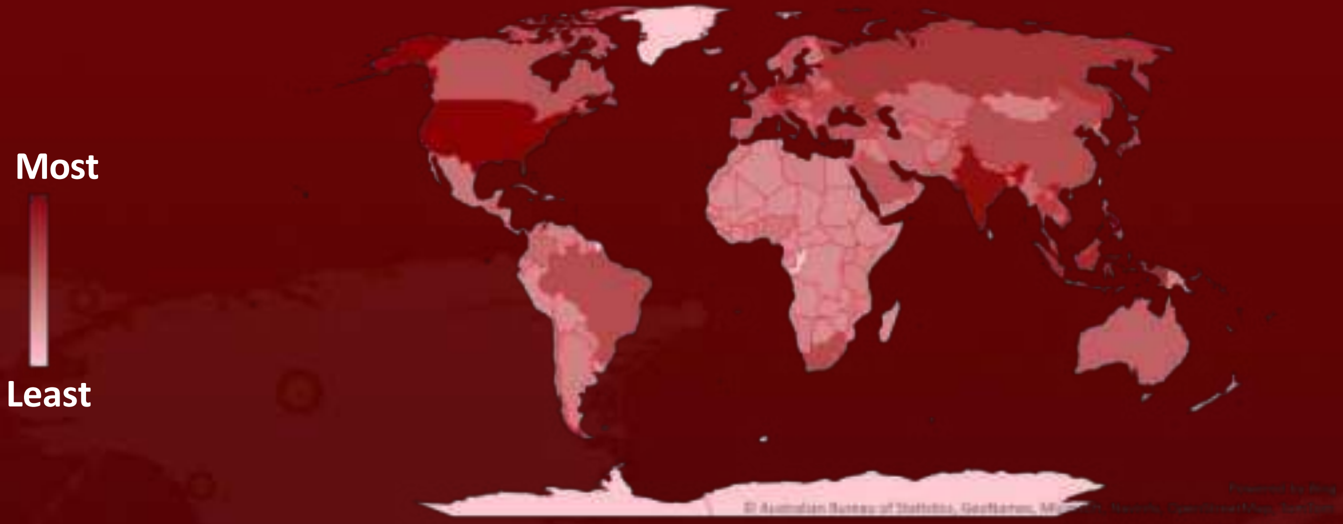
NAME	OVERVIEW	TYPE	DELIVERY METHOD
Zerobot	Zerobot’has two variants, both are written in Go programming language, and is more sophisticated has a number of advanced features, which include self propagation, self-replication and attacks for different protocols.	Botnet	Unknown
Dolphin	Dolphin, written in C++, is a backdoor that collects information and executes commands automatically or as issued by its operators.	Backdoor	Unknown
Rokrat	Rokrat is a backdoor commonly distributed as an encoded. binary file downloaded and decrypted by shellcode following the. exploitation of weaponized documents.	Backdoor	Phishing emails
Fantasy	'Fantasy' is an evolution of the 'Apostle' wiper, which the threat actor used in previous campaigns. Code similarities between Fantasy and Apostle (ESET) Wipers are a category of malware aiming to delete data on breached computers, causing digital destruction and business interruption.	Wiper	Unknown
Truebot	Truebot malware is a downloader malware that spreads through infected systems, collects information on targets, and deploys malicious payloads. The attacker's command and control (C2) receives the collected data.	Malware	Phishing emails
RisePro	RisePro is a type of malware that has been designed to steal sensitive information from infected computers and send it back to the attacker.	Information stealer	Malware-as-a-service

NAME	OVERVIEW	TYPE	DELIVERY METHOD
SiestaGraph	SiestaGraph tends to make use of a .NET API package that can be used conversely of Microsoft Graph API. Following the initial access, the threat actor gathers domain user and group information before exporting and archiving victim mailboxes as PST files.	Backdoor	Microsoft Exchange RCE exploit
aioconsol	A zero-day supply chain attack called "aioconsol" was discovered on December 9, 2022, in a Python package published on the Python Package Index (PyPI) on December 6, 2022. All three versions of the package were published on the same day and contain malicious code that writes a binary file called "test.exe“ and executes it as part of the installation process.	supply chain attack	Unknown
Nokoyawa 2.0	Nokoyawa is a 64-bit Windows-based ransomware family that first appeared in early February 2022. The threat group behind Nokoyawa conducts double-extortion ransomware attacks, first stealing data from companies, then encrypting files, and demanding a ransom payment. The 2.0 version of the Rust-based Nokoyama ransomware was revised in late September 2022.	Ransomware	Unknown
Ekipa RAT	Ekipa is a remote access trojan (RAT) that is used for targeted attacks and can be purchased on underground forums for a high price of $3,900. It primarily spreads and operates using Microsoft Office and Visual Basic for Applications. The trojan also comes with a control panel and tools for creating malicious macros in MS Word, Excel add-ins, and MS Publisher.	Remote Access Trojan	Phishing

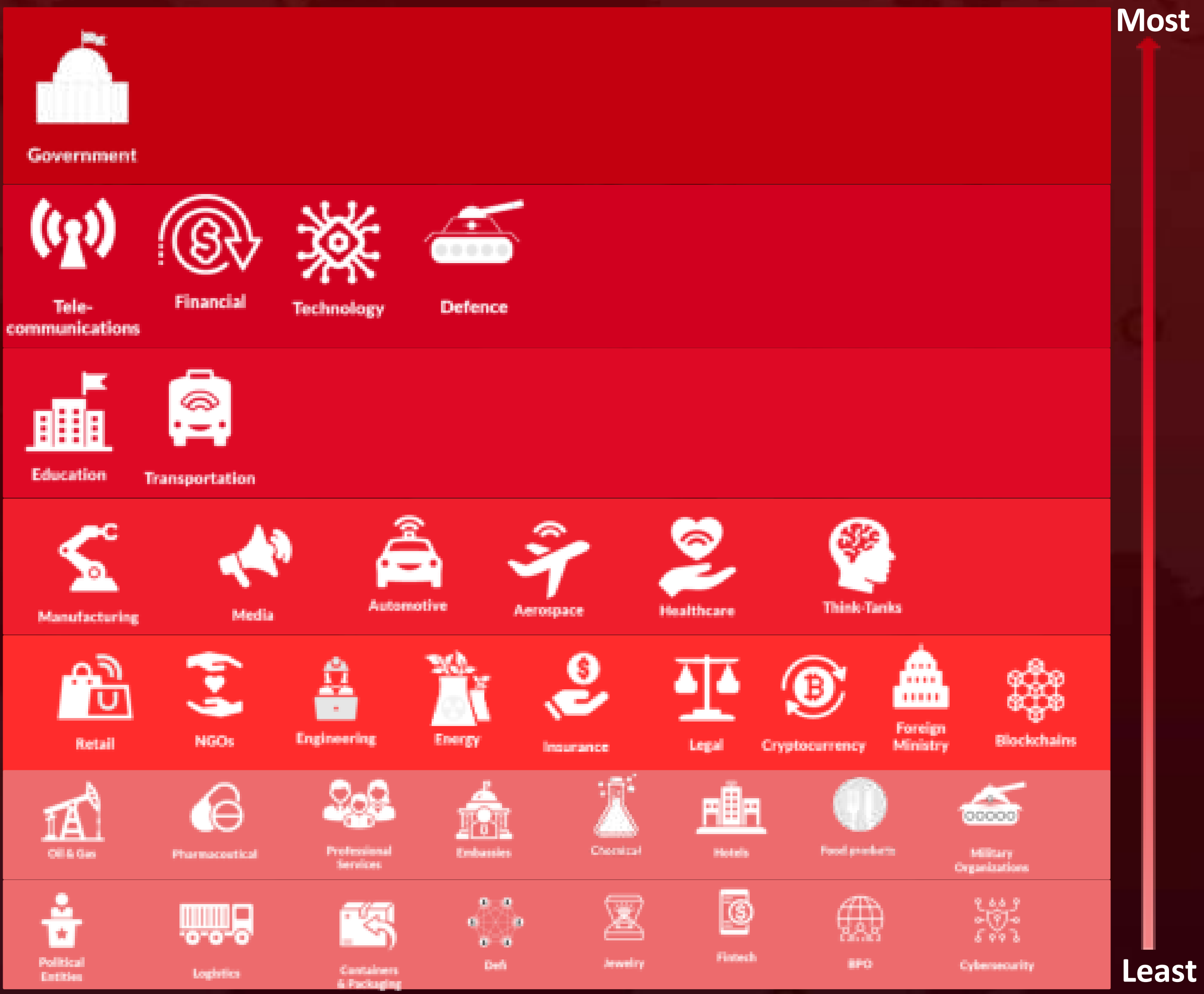
NAME	OVERVIEW	TYPE	DELIVERY METHOD
PolyVice	The PolyVice ransomware is a 64-bit Windows binary compiled with MinGW that uses a hybrid encryption approach to securely encrypt files by combining asymmetric and symmetric encryption methods. To speed up the file encryption process, the PolyVice locker uses a multi-threading technique	Ransomware	Exploiting PrintNightmare (CVE-2021-1675 & CVE-2021-34527)
GuLoader	GuLoader is an advanced malware downloader that uses polymorphic shellcode to bypass traditional security solutions.. A new shellcode anti-analysis method scans the entire process memory for virtual machine (VM)-related strings to prevent researchers from analyzing the shellcode. A significant number of anti-analysis techniques are employed by GuLoader, making detection and protection difficult.	Loader	Phishing
ArkeiStealer	Threat actors are currently disseminating ArkeiStealer via Windows Installer binaries disguised as trading applications. The trading application has been backdoored with the SmokeLoader downloader, which also includes an information stealer.	Stealer	Unknown
GoTrim	GoTrim botnet is written in Go Programming language and uses “::trim::” to split data to send and receive from the command-and-control server.	Botnet	Brute-Force on CMS
Mallox	Mallox ransomware strains have been spotted in the wild, indicating that the ransomware is operational, propagating rapidly, and infecting entities. A loader then downloads and encrypts data on the victim's device with Mallox ransomware from a remote source.	Ransomware	An unknown .NET-based loader

NAME	OVERVIEW	TYPE	DELIVERY METHOD
Unknown	A number of campaigns have been launched that spread InfoStealer malware written in the .NET programming language using phishing emails and Windows Shortcut (LNK) files and Batch Scripts (BAT). Based on the TTPs and evidence extracted, it appears the attacks were conducted by the same adversary (internally called AUI001).	Infostealer	phishing emails
ScareCrow	ScareCrow is a new ransomware strain based on Conti. As soon as the executable is executed, the files are encrypted and the extension .CROW is appended to them. It drops a ransom note named "readme.txt" that contains three Telegram handles for contacting the Threat Actor (TA).	Ransomware	Unknown
BlueSky	The BlueSky ransomware first surfaced in the second half of 2022. Ransomware like this resembles Conti and Babuk ransomware. When BlueSky Ransomware is executed, files are encrypted and a .BLUESKY extension is added to them.	Ransomware	Unknown
Meow	Meow Ransomware is a newly discovered form of malware that encrypts a victim's files and adds the .MEOW extension. It is based on the Conti ransomware. When it infects a device, it leaves behind a ransom note called "readme.txt" that provides victims with four email addresses and two Telegram handles they can use to contact the attackers and potentially negotiate for the decryption of their files.	Ransomware	Unknown
Putin Team	Putin Team, a group that claims to be of Russian origin but lacks any concrete evidence to support this, modified the leaked source code of Conti ransomware to create the Meow Ransomware. Putin Team uses a Telegram channel to share information about its victims.	Ransomware	Unknown

Targeted Countries


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

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	T1584: Compromise Infrastructure	T1078: Valid Accounts	T1047: Windows Management Instrumentation	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1027: Obfuscated Files or Information
T1590: Gather Victim Network Information	T1584.002: DNS Server	T1078.002: Domain Accounts	T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1053.005: Scheduled Task	T1027.002: Software Packing
T1591: Gather Victim Org Information	T1584.005: Botnet	T1091: Replication Through Removable Media	T1053.005: Scheduled Task	T1078: Valid Accounts	T1055: Process Injection	T1036: Masquerading
T1591.004: Identify Roles	T1586: Compromise Accounts	T1189: Drive-by Compromise	T1059: Command and Scripting Interpreter	T1078.002: Domain Accounts	T1055.002: Portable Executable Injection	T1036.004: Masquerade Task or Service
T1592: Gather Victim Host Information	T1587: Develop Capabilities	T1190: Exploit Public-Facing Application	T1059.001: PowerShell	T1098: Account Manipulation	T1068: Exploitation for Privilege Escalation	T1055: Process Injection
T1595: Active Scanning	T1588: Obtain Capabilities	T1566: Phishing	T1059.003: Windows Command Shell	T1136: Create Account	T1078: Valid Accounts	T1055.002: Portable Executable Injection
T1598: Phishing for Information	T1588.001: Malware	T1566.001: Spearphishing Attachment	T1059.005: Visual Basic	T1136.001: Local Account	T1078.002: Domain Accounts	T1070: Indicator Removal
	T1588.002: Tool	T1566.002: Spearphishing Link	T1059.006: Python	T1505: Server Software Component	T1134: Access Token Manipulation	T1070.001: Clear Windows Event Logs
	T1588.006: Vulnerabilities	T1078.003: Local Accounts	T1059.007: JavaScript	T1505.003: Web Shell	T1484: Domain Policy Modification	T1070.004: File Deletion
	T1608: Stage Capabilities	T1200: Hardware Additions	T1106: Native API	T1505.004: IIS Components	T1543: Create or Modify System Process	T1078: Valid Accounts
	T1583: Acquire Infrastructure		T1129: Shared Modules	T1543: Create or Modify System Process	T1543.003: Windows Service	T1078.002: Domain Accounts
	T1587.001: Malware		T1203: Exploitation for Client Execution	T1543.003: Windows Service	T1546: Event Triggered Execution	T1112: Modify Registry
	T1583.006: Web Services		T1204: User Execution	T1546: Event Triggered Execution	T1546.016: Installer Packages	T1134: Access Token Manipulation
			T1204.001: Malicious Link	T1546.016: Installer Packages	T1547: Boot or Logon Autostart Execution	T1140: Deobfuscate/Decode Files or Information
			T1204.002: Malicious File	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder	T1218: System Binary Proxy Execution
			T1559: Inter-Process Communication	T1547.001: Registry Run Keys / Startup Folder	T1547.008: LSASS Driver	T1218.005: Mshta
			T1559.001: Component Object Model	T1547.008: LSASS Driver	T1548: Abuse Elevation Control Mechanism	T1218.007: Msiexec
				T1556: Modify Authentication Process	T1574: Hijack Execution Flow	T1218.011: Rundll32
				T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking	T1221: Template Injection
				T1574.001: DLL Search Order Hijacking	T1574.002: DLL Side-Loading	T1484: Domain Policy Modification
				T1574.002: DLL Side-Loading	T1574.005: Executable Installer File Permissions Weakness	T1497: Virtualization/Sandbox Evasion
				T1574.005: Executable Installer File Permissions Weakness	T1078.003: Local Accounts	T1497.001: System Checks
				T1078.003: Local Accounts	T1484.001: Group Policy Modification	T1497.003: Time Based Evasion
						T1548: Abuse Elevation Control Mechanism
						T1553: Subvert Trust Controls
						T1553.001: Gatekeeper Bypass
						T1553.005: Mark-of-the-Web Bypass
						T1556: Modify Authentication Process
						T1562: Impair Defenses
						T1564: Hide Artifacts
						T1564.001: Hidden Files and Directories
						T1574: Hijack Execution Flow
						T1574.001: DLL Search Order Hijacking
						T1574.002: DLL Side-Loading
						T1574.005: Executable Installer File Permissions Weakness
						T1078.003: Local Accounts
						T1484.001: Group Policy Modification
						T1070.006: Timestomp
						T1562.002: Disable Windows Event Logging
						T1562.009: Safe Mode Boot

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	T1020: Automated Exfiltration	T1485: Data Destruction
T1003.002: Security Account Manager	T1010: Application Window Discovery	T1021.001: Remote Desktop Protocol	T1025: Data from Removable Media	T1001.001: Junk Data	T1041: Exfiltration Over C2 Channel	T1486: Data Encrypted for Impact
T1003.003: NTDS	T1012: Query Registry	T1021.002: SMB/Windows Admin Shares	T1056.001: Keylogging	T1071: Application Layer Protocol		T1489: Service Stop
T1003.006: DCSync	T1016: System Network Configuration Discovery	T1080: Taint Shared Content	T1074: Data Staged	T1071.001: Web Protocols		T1490: Inhibit System Recovery
T1056.001: Keylogging	T1018: Remote System Discovery	T1091: Replication Through Removable Media	T1074.001: Local Data Staging	T1071.002: File Transfer Protocols		T1491: Defacement
T1110: Brute Force	T1033: System Owner/User Discovery	T1210: Exploitation of Remote Services	T1113: Screen Capture	T1071.004: DNS		T1495: Firmware Corruption
T1539: Steal Web Session Cookie	T1046: Network Service Discovery	T1570: Lateral Tool Transfer	T1114: Email Collection	T1090: Proxy		T1496: Resource Hijacking
T1552: Unsecured Credentials	T1049: System Network Connections Discovery		T1114.001: Local Email Collection	T1095: Non-Application Layer Protocol		T1499: Endpoint Denial of Service
T1552.001: Credentials In Files	T1057: Process Discovery		T1119: Automated Collection	T1102: Web Service		T1529: System Shutdown/Reboot
T1555: Credentials from Password Stores	T1082: System Information Discovery		T1213: Data from Information Repositories	T1104: Multi-Stage Channels		T1531: Account Access Removal
T1555.003: Credentials from Web Browsers	T1083: File and Directory Discovery		T1557: Adversary-in-the-Middle	T1105: Ingress Tool Transfer		T1565: Data Manipulation
T1556: Modify Authentication Process	T1124: System Time Discovery		T1560: Archive Collected Data	T1132.001: Standard Encoding		T1561: Disk Wipe
T1557: Adversary-in-the-Middle	T1135: Network Share Discovery		T1560.001: Archive via Utility	T1571: Non-Standard Port		T1561.002: Disk Structure Wipe
	T1497: Virtualization/Sandbox Evasion		T1560.002: Archive via Library	T1573: Encrypted Channel		T1561.001: Disk Content Wipe
	T1497.001: System Checks			T1573.001: Symmetric Cryptography		
	T1497.003: Time Based Evasion			T1219: Remote Access Software		
	T1518: Software Discovery					
	T1518.001: Security Software Discovery					
	T1614.001: System Language Discovery					

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **103 significant vulnerabilities** and block the indicators related to the **16 active threat actors, 34 active malware,** and **177 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).

Note: The term "Zerobot" in this advisory refers to a specific type of malware and is not related with the organization zerobot.ai

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 🟨🐛 🟥⚔ 🟨⚔	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.

REPORT GENERATED ON

January 2, 2023 • 1:30 AM

More at www.hivepro.com