Date of Publication
February 01, 2023

Hive Pro

HiveForce Labs

MONTHLY THREAT DIGEST

Vulnerabilities, Actors, and Attacks

JANUARY 2023

Top 5 Takeaways

#1 In January, there were 2 zero-day vulnerabilities from Microsoft were addressed.

#2 Active strains of ransomware like CatB, MacOS, CrySIS, Mimic and RATs like Pupy, Quasar, BADNEWS, Powe, NetSupport, NjRAT, Warzone, Loda, Orcus, Remcos, SparkRAT were seen throughout the month.

#3 Malware families like IcedID, Unidentified, SHC-compiled Linux, GuLoader, KopiLuwak, Emotet, NeedleDropper, Gootkit loader, BOLDMOVE, and CryptBot were observed targeting victims globally.

#4 The Blind Eagle group recently launched a campaign targeting entities in Ecuador, while the Kasablanka group, a cybercriminal organization, targeted Russia from Sept to Dec 2022.

#5 Information stealers, including Titan, Album, Vidar, Rhadamanthys, and LummaC2, were also discovered in January.

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
59	16	34	USA China UK Saudi Arabia	Government Financial IT Energy Media Manufacturing	241

Detailed Report

⚙ Vulnerabilities of the Month

VENDOR	CVE	PATCH DETAILS
Microsoft	CVE-2017-0199* CVE-2023-21674* CVE-2023-21743 CVE-2023-21763 CVE-2023-21764 CVE-2023-21730 CVE-2023-21561 CVE-2023-21551 CVE-2023-21679 CVE-2023-21546 CVE-2023-21555 CVE-2023-21556 CVE-2023-21543 CVE-2023-21535 CVE-2023-21548 CVE-2017-11882 CVE-2022-26923 CVE-2022-34689	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0199 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21674 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21743 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21763 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21764 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21730 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21561 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21551 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21679 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21546 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21555 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21556 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21543 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21535 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21548 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-11882 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26923 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-34689
Synology	CVE-2022-43931	https://www.synology.com/en-global/security/advisory/Synology_SA_22_26
FORTINET	CVE-2022-39947 CVE-2022-45857 CVE-2022-41336 CVE-2022-35845 CVE-2022-42475	https://www.fortiguard.com/psirt/FG-IR-22-061 https://www.fortiguard.com/psirt/FG-IR-22-371 https://www.fortiguard.com/psirt/FG-IR-22-313 https://www.fortiguard.com/psirt/FG-IR-22-274 https://www.fortiguard.com/psirt/FG-IR-22-250 https://www.fortiguard.com/psirt/FG-IR-22-398

VENDOR	CVE	PATCH DETAILS
ZOHO	CVE-2022-47523 CVE-2022-28219 CVE-2022-47966	https://www.manageengine.com/privileged-session-management/advisory/cve-2022-47523.html https://www.manageengine.com/products/active-directory-audit/cve-2022-28219.html https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html
JWT	CVE-2022-23529	https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3
Cacti	CVE-2022-46169	https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf https://github.com/Cacti/cacti/commit/b43f13ae7f1e6bfe4e8e56a80a7cd867cf2db52b https://github.com/Cacti/cacti/commit/a8d59e8fa5f0054aa9c6981b1cbe30ef0e2a0ec9 https://github.com/Cacti/cacti/commit/7f0e16312dd5ce20f93744ef8b9c3b0f1ece2216
CISCO	CVE-2023-20025 CVE-2023-20026	No Patch Available
vmware	CVE-2022-22972 CVE-2022-31706 CVE-2022-31704 CVE-2022-31710 CVE-2022-31711	https://www.vmware.com/security/advisories/VMSA-2022-0014.html https://www.vmware.com/security/advisories/VMSA-2023-0001.html
f5	CVE-2022-1388	https://support.f5.com/csp/article/K23605346
GitLab	CVE-2022-41903 CVE-2022-23521	https://about.gitlab.com/update/
CentOS	CVE-2022-44877	CWP users should upgrade their versions to 0.9.8.1147 or later

VENDOR	CVE	PATCH DETAILS
	CVE-2023-0128 CVE-2023-0130 CVE-2023-0131 CVE-2023-0132 CVE-2023-0133 CVE-2023-0134 CVE-2023-0135 CVE-2023-0136 CVE-2023-0137 CVE-2023-0138 CVE-2023-0139 CVE-2023-0140 CVE-2023-0141 CVE-2022-3656 CVE-2023-0471 CVE-2023-0472 CVE-2023-0473 CVE-2023-0474	https://www.google.com/intl/en/chrome/?standalone=1
QNAP	CVE-2022-27596	https://www.qnap.com/en/security-advisory/qsa-23-01

Threat Actors of the Month

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Blind Eagle	Colombia	Energy, Financial, Government, Healthcare, Manufacturing	Colombia, Ecuador, Panama, Spain
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Turla (Waterbug,Venomous Bear,Group 88,SIG2,SIG15,SIG23,Iron Hunter,CTG-8875,Pacifier APT,ATK 13,ITG12,Makersmark,Krypton,Belugasturgeon,Popeye,Wraith,TAG-0530)	Russia	Aerospace, Defense, Education, Embassies, Energy, Government, High-Tech, IT, Media, NGOs, Pharmaceutical, Research, Retail	Afghanistan, Algeria, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bolivia, Botswana, Brazil, China, Chile, Denmark, Ecuador, Estonia, Finland, France, Georgia, Germany, Hong Kong, Hungary, India, Indonesia, Iran, Iraq, Italy, Jamaica, Jordan, Kazakhstan, Kyrgyzstan, Kuwait, Latvia, Mexico, Netherlands, Pakistan, Paraguay, Poland, Qatar, Romania, Russia, Serbia, Spain, Saudi Arabia, South Africa, Sweden, Switzerland, Syria, Tajikistan, Thailand, Tunisia, Turkmenistan, UK, Ukraine, Uruguay, USA, Uzbekistan, Venezuela, Vietnam, Yemen.
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Saaiwc Group (APT-LY-1005, Dark Pink)	China, North Korea, Iran, and Pakistan	Military, Government, Development, Religious, and Non-profit	Vietnam, Malaysia, Indonesia, Cambodia, Philippines, Bosnia and Herzegovina
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Patchwork (Dropping Elephant, Chinastrats, APT-C-09, Monsoon, Quilted Tiger, TG-4410, Zinc Emerson, ATK 11, Confucius, EHDevel, Manul, Viceroy Tiger, Mahabusa)	India	Aviation, Defense, Energy, Financial, Government, IT, Media, NGOs, Pharmaceutical, and Think Tanks.	Bangladesh, China, Japan, Pakistan, South Korea, Sri Lanka, UK, USA, Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, UAE, Yemen, Brunei, Myanmar, Cambodia, Timor-Leste, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, Vietnam.
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
NoName057(16)[NoName05716, 05716nnm , Nnm05716]	Russia	Foreign Affairs, Shipping, Government, Critical Infrastructure, Financial	Ukraine and NATO countries
	MOTIVE		
	Hacktivist & Destruction		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Vice Society	Unknown	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
	MOTIVE		
	Financial crime		
	CVE		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Earth Bogle	Unknown	-	Middle East and North Africa.
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Kasablanka	Morocco	Government	Russia
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
APT15 (Playful Taurus, BackdoorDiplomacy, Vixen Panda, KeChang, and NICKEL)	China	Aerospace, Aviation, Chemical, Defense, Embassies, Energy, Government, High-Tech, Industrial, Manufacturing, Mining, Oil and gas, Utilities and Uyghur communities.	North and South America, Africa, and the Middle East.
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
APT40(Leviathan, Kryptonite Panda,TEMP.Periscope,TEMP.Jumper,Bronze Mohawk,Mudcarp,Gadolinium,ATK 29,ITG09,TA423,Red Ladon)	China	Defense, Engineering, Government, Manufacturing, Research, Shipping and Logistics, Transportation and other Maritime-related targets across multiple verticals.	Belgium, Cambodia, Germany, Hong Kong, Indonesia, Laos, Malaysia, Myanmar, Norway, Philippines, Saudi Arabia, Switzerland, Thailand, UK, USA, Vietnam and Asia Pacific Economic Cooperation (APEC)
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
TICK (Bronze Butler,CTG-2006,TEMP.Tick,RedBaldNight,Stalker Panda)	China	Critical infrastructure, Defense, Engineering, Government, High-Tech, Industrial, Manufacturing, Media, Technology and International relations.	China, Hong Kong, Japan, Russia, Singapore, South Korea, Taiwan, USA.
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Cobalt Sapling (Moses Staff, DEV-0500, Abraham's Ax)	Iran	Chile, Germany, India, Israel, Italy, Turkey, UAE, USA, Saudi Arabia	Energy, Financial, Government, Manufacturing, Transportation, Utilities, Defense, Engineering, Legal, Media, Satellite Imagery, Technology.
	MOTIVE		
	Sabotage and destruction		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
Bluebottle	Unknown	Financial	Benin, Burkina Faso, Burundi, Cameroon, Comoros, The Republic of Congo, The Democratic Republic of Congo, The Ivory Coast, The Republic of Djibouti, Gabon, Guinea, Equatorial Guinea, Madagascar, Mali, Niger, The Central African Republic, Rwanda, Senegal, Seychelles, Tchad, Togo, Argentina, Paraguay, Bangladesh
	MOTIVE		
	Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Vice Society	Unknown	Brazil, Argentina, Switzerland, and Israel	Energy, Financial, Government, Manufacturing, Transportation, Utilities, Defense, Engineering, Legal, Media, Satellite Imagery, Technology.
	MOTIVE		
	Financial Crime		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Sandworm Team (Sandworm,Iron Viking, CTG-7263,Voodoo Bear,Quedagh, TEMP.Noble,ATK 14,BE2,UAC-0082,UAC-0113)	Russia **MOTIVE** Sabotage and destruction **CVEs**	Education, Energy, Government, Telecommunications.	Azerbaijan, Belarus, France, Georgia, Iran, Israel, Kazakhstan, Kyrgyzstan, Lithuania, Poland, Russia, Ukraine.

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
UNC2565	Unknown **MOTIVE** Financial Crime **CVE**	Government, Retail, Banking/Financial/Wealth Management, Healthcare, Outsourcing & Hosting, Technology/IT, Transportation & Shipping, Insurance, Automotive, Discrete Manufacturing, Wholesale	North America, Europe,Asia, Middle East, Africa, Central America and Caribbean, South America, Oceania, Middle East, Southeast Asia

Malware of the Month

NAME	OVERVIEW	TYPE	DELIVERY METHOD
IcedID	The IcedID botnet has been distributing itself through malvertising attacks using Google pay-per-click ads since December 2022. The new IcedID botnet loader is delivered through an MSI file, which drops several files and invokes a malicious loader routine through rundll32.exe.	Malware Family	Malicious files
Unidentified Malware	An unidentified strain of Linux malware is exploiting vulnerabilities in WordPress plugins to compromise sites by injecting malicious JavaScript. These JavaScripts are run sequentially until one of them succeeds in compromising the site.	Malware Family	Unknown
CatB Ransomware	CatB is ransomware that uses DLL hijacking to evade detection. It injects itself into the Microsoft Distributed Transaction Coordinator (MSDTC) service, a legitimate Windows process, and uses that process to encrypt the victim's files.	Ransomware	Unknown
SHC-compiled Linux malware	New Linux malware discovered that installs CoinMiner via dictionary attacks on insecure Linux SSH servers. The malware consists of Shc downloader, XMRig CoinMiner and Perl-based DDoS IRC Bot. Spread through poorly secured Linux SSH servers.	Malware Family	Unknown
Pupy RAT	Pupy RAT malware using DLL side-loading to avoid detection by disguising as legitimate WerFault.exe process. Delivered through ISO image containing malicious DLL, shortcut and Excel files. Shortcut opens WerFault.exe process and DLL side-loading executes malicious DLL.	Remote Access Trojan	Malicious files

NAME	OVERVIEW	TYPE	DELIVERY METHOD
MacOS Ransomware	MacOS ransomware contains four ransomware. KeRanger (2016) distributed through compromised BitTorrent client Transmission. FileCoder (2018) spread through malicious ads on websites. MacRansom (2019) spread through email attachments. EvilQuest (2020) spread through malicious internet downloads.	Ransomware	Phishing emails and Malicious adds
QuasarRAT	QuasarRAT is a RAT that enables remote control and access of victim's computer. Can steal information and perform malicious activities. Spread through email attachments, infected software installers and compromised websites. Capabilities: keystroke recording, screenshot taking and executing arbitrary code.	Remote Access Trojan	Phishing emails and malicious software updates
GuLoader	GuLoader is a highly advanced malware downloader first detected in 2019. Uses polymorphic shellcode to bypass security and includes anti-analysis measures. Multi-stage deployment with VBS dropper, registry-stored payload, and PowerShell script. Maps DJB2	Malware	Phishing emails and Malicious adds
LummaC2 Information stealer	LummaC2 Stealer is an information stealer that focuses on Chromium and Mozilla-based browsers. Its purpose is to steal sensitive information, such as cryptocurrency wallets and two-factor authentication (2FA) extensions, from a victim's device.	Information stealer	Unknown
KopiLuwak	KopiLuwak is designed for cyber espionage. Latest infection process uses techniques to avoid detection, such as mimicry of ordinary LAN addresses in C&C infrastructure and use of almost "fileless" encrypted Trojan for remote administration embedded in the computer's registry.	Malware	Unknown

NAME	OVERVIEW	TYPE	DELIVERY METHOD
QUIETCANARY	QUIETCANARY is a .NET-based backdoor that collects and leaks data from compromised users. Lightweight, executed only on the second connection to the host. Publicly known as "Tunnus".	Backdoor	Unknown
ANDROMEDA	ANDROMEDA is a malware that targets Windows systems to create an infected network. This botnet is used to distribute other associated malware familie	Backdoor	Unknown
PowerDism	PowerDism malware is used by the Saaiwc Group as a PowerShell backdoor to steal information and execute commands on targeted systems. They use custom tools, publicly available exploits.	Backdoor	Unknown
BADNEWS RAT	BADNEWS RAT is spread through malicious RTF files. It has the ability to run commands, collect directory lists, and download additional payloads, with the BADNEWS Trojan as the final payload. The Trojan is embedded within the RTF document and uses a stolen digital signature for increased effectiveness.	Remote Access Trojan	Unknown
Emotet	Emotet is a modular malware that acts as a downloader for other malware variants and uses EtterSilent malware document builder. It employs a new social engineering technique through an Excel attachment that instructs how to avoid Microsoft's "Mark-of-the-Web" detection.	Malware	Phishing emails
NeedleDropper	NeedleDropper is a new dropper strain used by attackers to conceal malicious payloads. It is delivered via spam email attachments and uses the vulnerabilities in an Excel sheet to initiate the vbc.exe script, which releases the payload into a temporary folder.	Malware	Malicious files

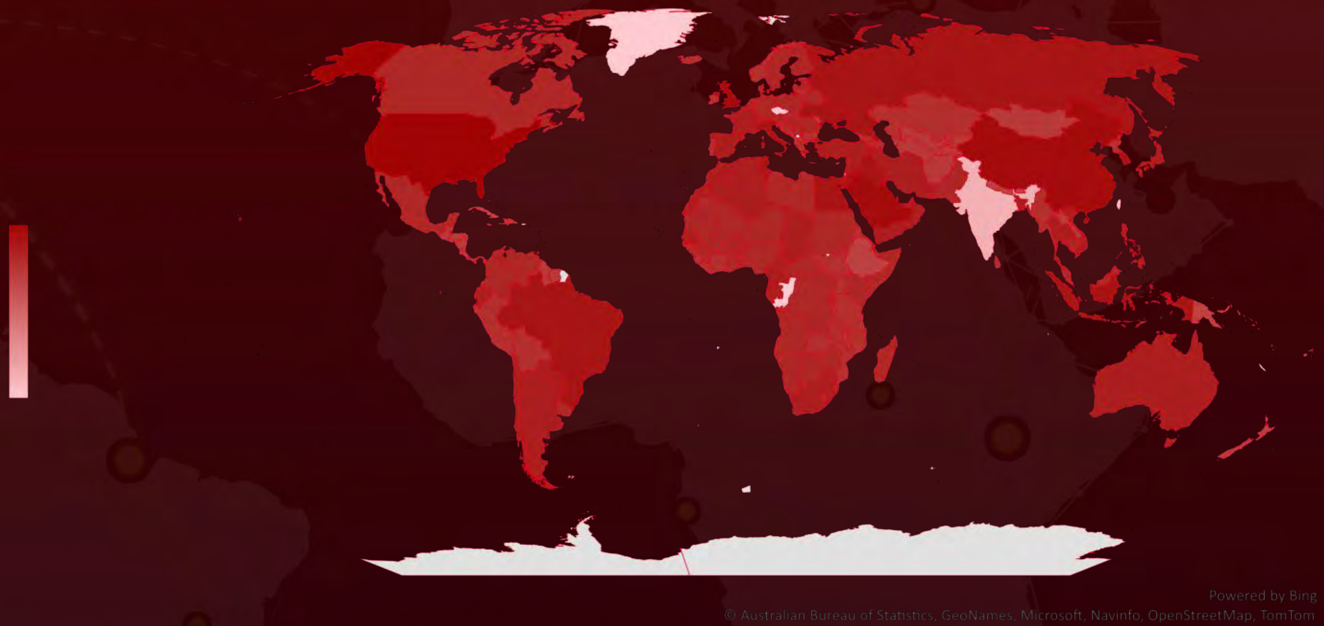
NAME	OVERVIEW	TYPE	DELIVERY METHOD
Gootkit loader ↗	Gootkit is a type of malware spread through SEO poisoning, often used in APT operations. It installs malicious DLLs by exploiting the legitimate program VLC Media Player.	malware	SEO poisoning
PoweRAT ↗	PoweRAT is a newly discovered malware that combines a stealer and RAT. It's spread via the Python Package Index (PyPI) and found in several packages, including pyrologin, easytimestamp, discorder, discord-dev, style.py, and pythonstyles, starting with the setup.py file	Remote Access Trojan	PyPI
Rhadamanthys Stealer ↗	Rhadamanthys Stealer is a new and active malware strain marketed as MaaS. It spreads through Google Ads and phishing websites mimicking popular software, as well as through malicious attachments in spam emails.	Information stealer	Phishing emails
NetSupport RAT ↗	NetSupport Manager is a genuine remote support tool, but has been misused by cyber criminals as NetSupport Manager RAT in harmful campaigns. The original purpose was to provide remote technical support or computer assistance.	Remote Access Trojan	Phishing
NjRAT ↗	NjRAT (aka Bladabindi) is a RAT malware discovered in 2013 that allows unauthorized access and control of victim devices. It enables attackers to carry out intrusive operations on a compromised device.	Remote Access Trojan	Phishing emails
Warzone RAT ↗	Warzone RAT is a remote access trojan (RAT) malware that allows attackers to gain unauthorized access and control over victim devices. Warzone RAT enables attackers to perform various intrusive operations on compromised devices, such as keylogging, screen capture, file transfer, and executing arbitrary code.	Remote Access Trojan	Phishing emails

NAME	OVERVIEW	TYPE	DELIVERY METHOD
Loda RAT	Loda RAT is a remote access trojan (RAT) malware that enables attackers to gain unauthorized access and control over victim devices. It allows attackers to perform various intrusive operations on compromised devices, such as keylogging, screen capture, file transfer, and executing arbitrary code.	Remote Access Trojan	Phishing emails
Turian Backdoor	Turian Backdoor is a type of malware that allows an attacker to gain unauthorized access and control over a victim's device. It functions as a backdoor, allowing the attacker to execute arbitrary code, steal sensitive information, and carry out other malicious activities on the compromised device.	Backdoor	Phishing emails
BOLDMOVE	BOLDMOVE is a type of malware used by cyber criminals to carry out malicious activities on infected devices. It is a remote access trojan (RAT) that enables attackers to gain unauthorized access and control over a victim's device. BOLDMOVE can perform various intrusive operations, such as keylogging, screen capture, file transfer, and executing arbitrary code.	Malware	Phishing emails
Orcus RAT	Orcus RAT is a dangerous RAT malware that enables attackers to remotely control infected systems. A recent variant of Orcus RAT has been found disguised as a cracked version of Hangul Word Processor 2022, distributed through file-sharing sites. It can steal sensitive information and perform other malicious actions.	Remote Access Trojan	Unknown

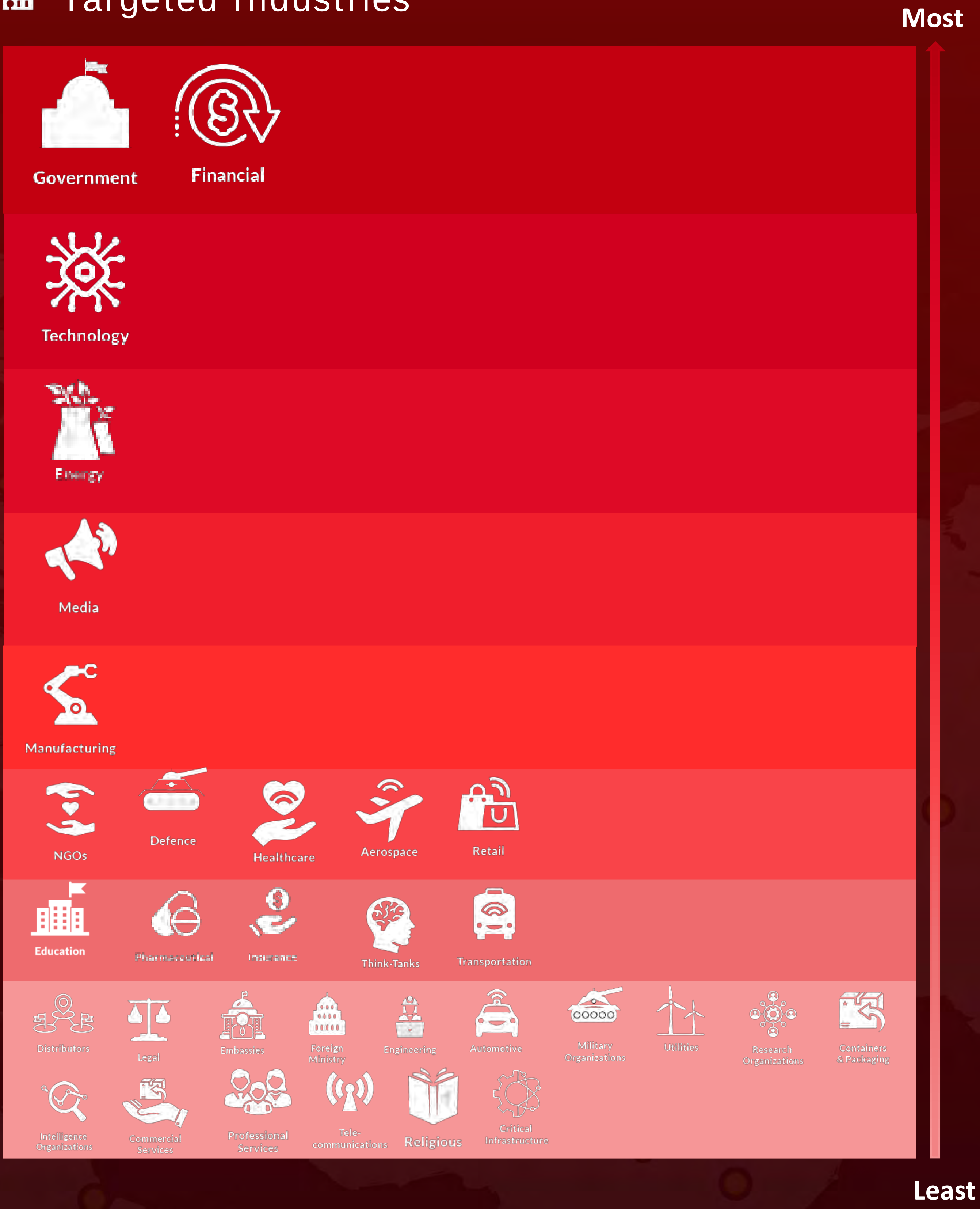
NAME	OVERVIEW	TYPE	DELIVERY METHOD
CrySIS Ransomware	CrySIS (also known as Dharma) is a ransomware-as-a-service (RaaS) that penetrates systems using vulnerable RDP servers, then encrypts data with AES-256 and RSA-1024 encryption. Its source code was made public, enabling its purchase and repurposing.	Ransomware	Phishing emails
Vidar Info-stealer	Vidar is an effective information-stealing malware that evades detection by using Russian VPNs, moving to the Tor network, and expanding its infrastructure. It operates on a conventional business model where subscribers pay $130-$750 for a customizable subscription targeting specific information types.	Information stealer	Phishing emails
Album Stealer	Album Stealer can evade detection through multiple phases using vulnerable apps via DLL side loading. It conceals critical data and strings with the ConcurrentDictionary class and sends information gathered from an infected system to a C&C server.	Information stealer	Unknown
Remcos RAT	Remcos RAT is a type of malware that allows a remote attacker to take control of an infected computer. The attacker can then perform a variety of actions on the infected machine, such as stealing sensitive information, monitoring the user's activities, and executing arbitrary code.	Remote Access Trojan	Phishing emails
SparkRAT	SparkRAT is a Golang-based RAT that supports Windows, Linux, and macOS. It can self-update through its C&C server and communicates using the WebSocket protocol. It has over 20 commands that allow it to execute tasks, control infected machines, manipulate processes/files, and steal information.	Remote Access Trojan	Unknown

NAME	OVERVIEW	TYPE	DELIVERY METHOD
Titan Stealer	Titan Stealer is a cross-platform information-stealing malware spread through a Telegram channel. It captures data from infected Windows devices, allowing the attacker to access login activity and data, including browser credentials and cryptocurrency wallets.	Information stealer	Unknown
CryptBot	CryptBot is a data stealer targeting Windows computers. It collects system configuration data by scanning the 'Uninstall' registry tree for specific registry keys	malware	Unknown
Mimic ransomware	Mimic ransomware discovered in June 2022 encrypts files using Everything APIs. It has features like removing shadow copies, terminating apps/services, and deactivating Windows Defender. Multiple threads for fast encryption and to complicate analysis for security researchers.	Ransomware	Unknown

Targeted Countries


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

Targeted Industries



Most

Government Financial

Technology

Energy

Media

Manufacturing

NGOs Defence Healthcare Aerospace Retail

Education Pharmaceutical Insurance Think-Tanks Transportation

Distributors Legal Embassies Foreign Ministry Engineering Automotive Military Organizations Utilities Research Organizations Containers & Packaging

Intelligence Organizations Commercial Services Professional Services Tele-communications Religious Critical Infrastructure

Least

Potential MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1598.002: Phishing for Information: Spearphishing Attachment	T1608.006: Stage Capabilities: SEO Poisoning	T1566.001: Phishing: Spearphishing Attachment	T1569.002: System Services: Service Execution	T1574.002: Hijack Execution Flow: DLL Side-Loading	T1574.002: Hijack Execution Flow: DLL Side-Loading	T1622: Debugger Evasion
T1598: Phishing for Information	T1608.003: Stage Capabilities: Install Digital Certificate	T1566: Phishing	T1569.001: System Services: Launchctl	T1574.001: Hijack Execution Flow: DLL Search Order Hijacking	T1574.001: Hijack Execution Flow: DLL Search Order Hijacking	T1620: Reflective Code Loading
T1592: Gather Victim Host Information	T1608: Stage Capabilities	T1195: Supply Chain Compromise	T1569: System Services	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1574.002: Hijack Execution Flow: DLL Side-Loading
T1590: Gather Victim Network Information	T1588.006: Obtain Capabilities: Vulnerabilities	T1190: Exploit Public-Facing Application	T1559.002: Inter-Process Communication: Dynamic Data Exchange	T1556: Modify Authentication Process	T1548.003: Abuse Elevation Control Mechanism: Sudo and Sudo Caching	T1574.001: Hijack Execution Flow: DLL Search Order Hijacking
	T1588.005: Obtain Capabilities: Exploits	T1189: Drive-by Compromise	T1559.001: Inter-Process Communication: Component Object Model	T1554: Compromise Client Software Binary	T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control	T1574: Hijack Execution Flow
	T1588.002: Obtain Capabilities: Tool	T1078: Valid Accounts	T1559: Inter-Process Communication	T1547.009: Boot or Logon Autostart Execution: Shortcut Modification	T1548: Abuse Elevation Control Mechanism	T1564.003: Hide Artifacts: Hidden Window
	T1588.001: Obtain Capabilities: Malware		T1204.002: User Execution: Malicious File	T1547.008: Boot or Logon Autostart Execution: LSASS Driver	T1547.009: Boot or Logon Autostart Execution: Shortcut Modification	T1564.001: Hide Artifacts: Hidden Files and Directories
	T1588: Obtain Capabilities		T1204.001: User Execution: Malicious Link	T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.008: Boot or Logon Autostart Execution: LSASS Driver	T1564: Hide Artifacts
	T1587.002: Develop Capabilities: Code Signing Certificates		T1204: User Execution	T1547: Boot or Logon Autostart Execution	T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1562.004: Impair Defenses: Disable or Modify System Firewall
	T1587.001: Develop Capabilities: Malware		T1203: Exploitation for Client Execution	T1546.001: Event Triggered Execution: Change Default File Association	T1547: Boot or Logon Autostart Execution	T1562.001: Impair Defenses: Disable or Modify Tools
	T1587: Develop Capabilities		T1129: Shared Modules	T1546: Event Triggered Execution	T1546.001: Event Triggered Execution: Change Default File Association	T1562: Impair Defenses
	T1584: Compromise Infrastructure		T1106: Native API	T1543.004: Create or Modify System Process: Launch Daemon	T1546: Event Triggered Execution	T1556: Modify Authentication Process
			T1059.007: Command and Scripting Interpreter: JavaScript	T1543.003: Create or Modify System Process: Windows Service	T1543.004: Create or Modify System Process: Launch Daemon	T1553.005: Subvert Trust Controls: Mark-of-the-Web Bypass
			T1059.006: Command and Scripting Interpreter: Python	T1543.001: Create or Modify System Process: Launch Agent	T1543.003: Create or Modify System Process: Windows Service	T1553.002: Subvert Trust Controls: Code Signing
			T1059.005: Command and Scripting Interpreter: Visual Basic	T1543: Create or Modify System Process	T1543.001: Create or Modify System Process: Launch Agent	T1553: Subvert Trust Controls
			T1059.003: Command and Scripting Interpreter: Windows Command Shell	T1505.003: Server Software Component: Web Shell	T1543: Create or Modify System Process	T1548.003: Abuse Elevation Control Mechanism: Sudo and Sudo Caching
			T1059.002: Command and Scripting Interpreter: AppleScript	T1505: Server Software Component	T1134: Access Token Manipulation	T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control
			T1059.001: Command and Scripting Interpreter: PowerShell	T1197: BITS Jobs	T1078: Valid Accounts	T1548: Abuse Elevation Control Mechanism
			T1059: Command and Scripting Interpreter	T1176: Browser Extensions	T1068: Exploitation for Privilege Escalation	T1497.001: Virtualization/Sandbox Evasion: System Checks
			T1053.005: Scheduled Task/Job: Scheduled Task	T1137: Office Application Startup	T1055.012: Process Injection: Process Hollowing	T1497: Virtualization/Sandbox Evasion
			T1053: Scheduled Task/Job	T1136: Create Account	T1055: Process Injection	T1222.002: File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification
			T1047: Windows Management Instrumentation	T1098: Account Manipulation	T1053.005: Scheduled Task/Job: Scheduled Task	T1222: File and Directory Permissions Modification
				T1078: Valid Accounts	T1053: Scheduled Task/Job	T1221: Template Injection
				T1053.005: Scheduled Task/Job: Scheduled Task		T1218.011: System Binary Proxy Execution: Rundll32
				T1053: Scheduled Task/Job		T1218.010: System Binary Proxy Execution: Regsvr32
						T1218.007: System Binary Proxy Execution: Msiexec
						T1218: System Binary Proxy Execution
						T1216: System Script Proxy Execution
						T1202: Indirect Command Execution
						T1197: BITS Jobs
						T1140: Deobfuscate/Decode Files or Information
						T1134: Access Token Manipulation
						T1127: Trusted Developer Utilities Proxy Execution
						T1112: Modify Registry
						T1078: Valid Accounts
						T1070.006: Indicator Removal: Timestomp
						T1070.004: Indicator Removal: File Deletion
						T1070.001: Indicator Removal: Clear Windows Event Logs
						T1070: Indicator Removal
						T1055.012: Process Injection: Process Hollowing
						T1055: Process Injection
						T1036.005: Masquerading: Match Legitimate Name or Location
						T1036.004: Masquerading: Masquerade Task or Service
						T1036: Masquerading
						T1027.009: Obfuscated Files or Information: Embedded Payloads
						T1027.007: Obfuscated Files or Information: Dynamic API Resolution
						T1027.005: Obfuscated Files or Information: Indicator Removal from Tools
						T1027.002: Obfuscated Files or Information: Software Packing
						T1027: Obfuscated Files or Information

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1606.001: Forge Web Credentials: Web Cookies	T1622: Debugger Evasion	T1210: Exploitation of Remote Services	T1602: Data from Configuration Repository	T1573.002: Encrypted Channel: Asymmetric Cryptography	T1041: Exfiltration Over C2 Channel	T1565.001: Data Manipulation: Stored Data Manipulation
T1606: Forge Web Credentials	T1614.001: System Location Discovery: System Language Discovery	T1021.002: Remote Services: SMB/Windows Admin Shares	T1560.002: Archive Collected Data: Archive via Library	T1573: Encrypted Channel	T1020: Automated Exfiltration	T1565: Data Manipulation
T1557.002: Adversary-in-the-Middle: ARP Cache Poisoning	T1614: System Location Discovery	T1021: Remote Services	T1560.001: Archive Collected Data: Archive via Utility	T1571: Non-Standard Port		T1529: System Shutdown/Reboot
T1557: Adversary-in-the-Middle	T1518.001: Software Discovery: Security Software Discovery		T1560: Archive Collected Data	T1219: Remote Access Software		T1499: Endpoint Denial of Service
T1556: Modify Authentication Process	T1518: Software Discovery		T1557.002: Adversary-in-the-Middle: ARP Cache Poisoning	T1132.002: Data Encoding: Non-Standard Encoding		T1498: Network Denial of Service
T1555.004: Credentials from Password Stores: Windows Credential Manager	T1497.001: Virtualization/Sandbox Evasion: System Checks		T1557: Adversary-in-the-Middle	T1132.001: Data Encoding: Standard Encoding		T1496: Resource Hijacking
T1555.003: Credentials from Password Stores: Credentials from Web Browsers	T1497: Virtualization/Sandbox Evasion		T1530: Data from Cloud Storage	T1132: Data Encoding		T1490: Inhibit System Recovery
T1555: Credentials from Password Stores	T1482: Domain Trust Discovery		T1213: Data from Information Repositories	T1105: Ingress Tool Transfer		T1489: Service Stop
T1552.004: Unsecured Credentials: Private Keys	T1135: Network Share Discovery		T1123: Audio Capture	T1104: Multi-Stage Channels		T1486: Data Encrypted for Impact
T1552.002: Unsecured Credentials: Credentials in Registry	T1124: System Time Discovery		T1119: Automated Collection	T1102: Web Service		
T1552: Unsecured Credentials	T1087.001: Account Discovery: Local Account		T1115: Clipboard Data	T1095: Non-Application Layer Protocol		
T1539: Steal Web Session Cookie	T1087: Account Discovery		T1114: Email Collection	T1071.001: Application Layer Protocol: Web Protocols		
T1110: Brute Force	T1083: File and Directory Discovery		T1113: Screen Capture	T1071: Application Layer Protocol		
T1056.001: Input Capture: Keylogging	T1082: System Information Discovery		T1074.001: Data Staged: Local Data Staging	T1001: Data Obfuscation		
T1056: Input Capture	T1057: Process Discovery		T1074: Data Staged			
T1040: Network Sniffing	T1049: System Network Connections Discovery		T1056.001: Input Capture: Keylogging			
T1003: OS Credential Dumping	T1040: Network Sniffing		T1056: Input Capture			
	T1033: System Owner/User Discovery		T1005: Data from Local System			
	T1018: Remote System Discovery					
	T1016: System Network Configuration Discovery					
	T1012: Query Registry					
	T1010: Application Window Discovery					
	T1007: System Service Discovery					

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **59 significant vulnerabilities** and block the indicators related to the **16 active threat actors, 34 active malware,** and **241 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 (January 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 🟨🐞 🟥⚔ 🟥⚔					

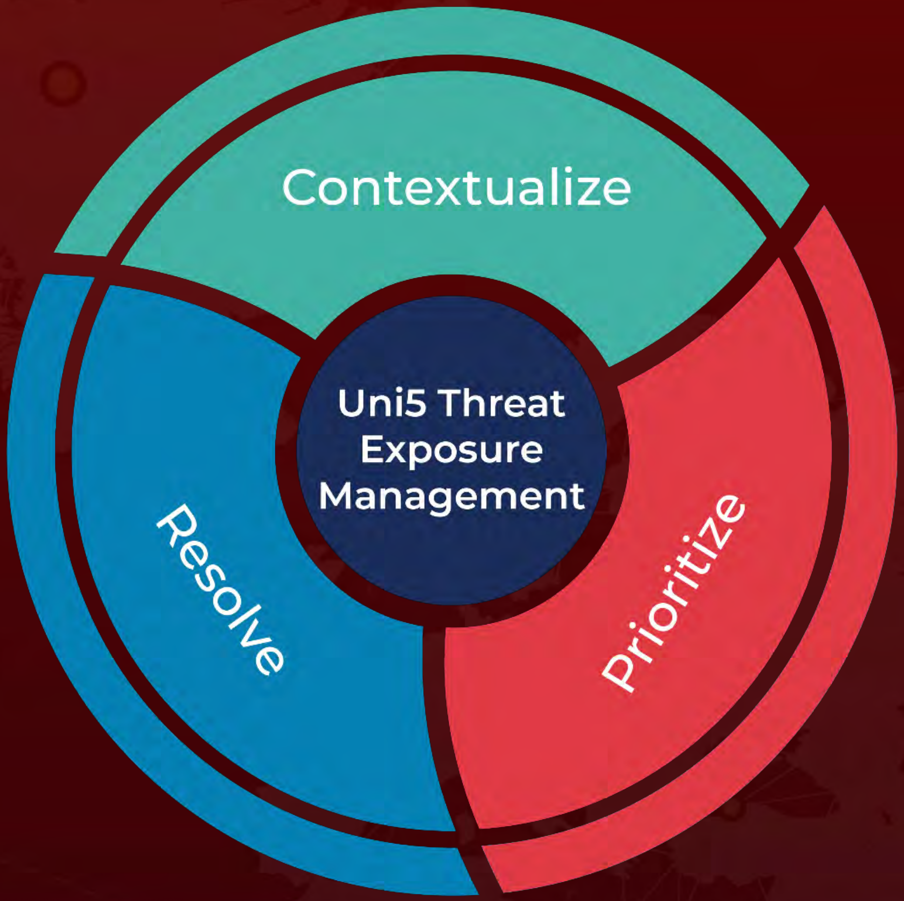
Click on any of the icons to get directed to the advisory

🟥🐞	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.



REPORT GENERATED ON

February 1, 2023 • 5:30 AM

More at www.hivepro.com