Date of Publication
December 1, 2022

Hive Pro

MONTHLY

THREAT DIGEST

Vulnerabilities & Threats that Matter

NOVEMBER 2022

Top 5 Takeaways

#1 In November, two popular **zero-day** vulnerabilities (**CVE-2022–41040** and **CVE-2022–41082**) i.e **ProxyNotShell** from Microsoft were finally addressed.

#2 New ransomware strains like **Royal, Venus, Azov, Punisher**, and **RansomExx** have been observed targeting victims all over the world.

#3 November also had **seven new zero-day** vulnerabilities, six from **Microsoft** and one of them from **Google Chrome**.

#4 **FIN7** espionage gang was seen exploiting a two-month-old **Microsoft** vulnerability and **Fox Kitten** was also seen exploiting the year-old **log4j** vulnerability.

#5 The pre-announced **Critical OpenSSL** vulnerabilities were addressed.

Vulnerabilities of the Month	Threat Actors of the Month	Malware of the Month	Top Targeted Countries	Top Targeted Industries	Common MITRE ATT&CK TTPs
43	14	16	Germany USA UAE Turkey India Japan	Government Telecommunications Financial	188

Detailed Report

Vulnerabilities of the Month

VENDOR	CVE	PATCH DETAILS
msi	CVE-2019-16098	No Patch Available
vmware	CVE-2022-31685 CVE-2022-31686 CVE-2022-31687 CVE-2022-31690	For CVE-2022-31685, CVE-2022-31686, CVE-2022-31687 Upgrade VMware Workspace ONE Assist to 22.10 Links: https://resources.workspaceone.com/view/kk9llj32v29bty77s536/en https://resources.workspaceone.com/view/96kl35y9pjmyhfbdxpp3/en https://resources.workspaceone.com/view/r6wdzxhmtd6zksdmswbp/en For CVE-2022-31690: Upgrade VMware Spring Security to 5.7.5 and 5.6.9 Links: https://github.com/spring-projects/spring-security/releases/tag/5.7.5 https://github.com/spring-projects/spring-security/releases/tag/5.6.9
	CVE-2022-4135* CVE-2022-3885 CVE-2022-3886 CVE-2022-3887 CVE-2022-3888 CVE-2022-3889 CVE-2022-3890	Upgrade Google Chrome to 107.0.5304.87 for Mac and Linux and 107.0.5304.87/.88 for Windows https://www.google.com/intl/en/chrome/?standalone=1
OpenSSL Cryptography and SSL/TLS Toolkit	CVE-2022-3602 CVE-2022-3786	Upgrade to OpenSSL version 3.0.7
citrix	CVE-2022-27510 CVE-2022-27513 CVE-2022-27516	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516
f5	CVE-2022-41800 CVE-2022-41622	https://support.f5.com/csp/article/K94221585 https://support.f5.com/csp/article/K13325942
HEIMDAL SECURITY	CVE-2021-3671 CVE-2019-14870 CVE-2022-3437 CVE-2022-41916 CVE-2022-42898 CVE-2022-44640 CVE-2021-44758	Upgrade to Heimdal version 7.7.1
ATLASSIAN	CVE-2022-43782 CVE-2022-43781	https://jira.atlassian.com/browse/CWD-5888 https://jira.atlassian.com/browse/BSERV-13522
THE APACHE SOFTWARE FOUNDATION	CVE-2021-44228*	https://logging.apache.org/log4j/2.x/security.html

VENDOR	CVE	PATCH DETAILS
Microsoft	CVE-2022-30190 CVE-2020-1472 CVE-2021-42287 CVE-2021-42278 CVE-2021-34527 CVE-2022-41128* CVE-2022-41040* CVE-2022-41082* CVE-2022-41091* CVE-2022-41073* CVE-2022-41125* CVE-2022-34721	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42287 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42278 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41091 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41073 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41125 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34721
	CVE-2022-40303 CVE-2022-40304	Upgrade macOS Ventura to 13.0.1 Links: https://support.apple.com/en-gb/HT213504

*zero-day vulnerability

Threat Actors of the Month

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
APT 10(Stone Panda, menuPass Team, menuPass,Red Apollo,CVNX, Potassium, Hogfish, Happyyongzi, Cicada, Bronze Riverside, CTG-5938,ATK 41,TA429,ITG01)	China **MOTIVE** Information theft and espionage **CVEs**	Aerospace, Defense, Energy, Financial, Government, Healthcare, High-Tech, IT, Media, NGOs, Pharmaceutical, Telecommunications, Think- Tanks, Biomedical, Consulting , Manufacturing, Oil and Gas	Australia, Belgium, Brazil, Canada, China, Finland, France, Germany, Hong Kong, India, Israel, Italy, Japan, Montenegro, Netherlands, Norway, Philippines, Singapore, South Africa, South Korea, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 Black Basta ransomware gang	N/A **MOTIVE** Financial Gain **CVEs** CVE-2022-30190 CVE-2021-42287 CVE-2021-42278 CVE-2021-34527 CVE-2020-1472	Automotive,Construction, Cosmetics,Energy, Healthcare,Heating, Manufacturing,Pharmaceuticals,Plumbing,Telecommunication,Transportation, Textile	Australia, Canada, Germany, India, Japan, New Zealand, Singapore, UAE, UK, USA

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 APT 36(Transparent Tribe, ProjectM, Mythic Leopard, TEMP.Lapis, Copper Fieldstone,Earth Karkaddan, C-Major)	Pakistan **MOTIVE** Information theft and espionage **CVEs**	Defense, Education, Government, Embassies and Research Organizations	Afghanistan, Australia, Austria, Azerbaijan, Belgium, Botswana, Bulgaria, Canada, China, Czech, Germany, India, Iran, Japan, Kazakhstan, Kenya, Malaysia, Mongolia, Nepal, Netherlands, Oman, Pakistan, Romania, Saudi Arabia, Spain, Sweden, Thailand, Turkey, UAE, UK, USA.

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 FRwL	Russia **MOTIVE** Financial crime **CVE**		Ukraine

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 Earth Longzhi (APT41)	China **MOTIVE** Financial crime, Information theft and espionage **CVEs** CVE-2019-16098	Defense, Aviation, Insurance,Government, Healthcare,Academic, Infrastructureindustries and UrbanDevelopment	East and Southeast Asia

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 Gold Dupont (Sprite Spider)	N/A **MOTIVE** Financial crime **CVEs**	Manufacturing, Education, Banking, Technology, Media, Finance, Healthcare, Government	USA, France, Brazil, Taiwan, Germany, Turkey, Slovenia, Israel, Ireland

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 FIN7 (Gold Niagara,Calcium, Navigator,ATK 32,APT-C-11,ITG14,TAG-CR1)	Russia **MOTIVE** Financial crime **CVEs** CVE-2022-34721	Retail, Government, Financial Services, IT, E-Commerce	U.S.A, UK, Australia, Canada, France, Germany, Turkey, Japan, India, UAE, Israel

NAME	ORIGIN	TARGET INDUSTRIES	TARGET REGIONS
Billbug (Lotus Blossom, Spring Dragon, Dragonfish, Thrip, Bronze Elgin, CTG-8171, ATK 1, ATK 78)	China **MOTIVE** Information theft and espionage **CVEs**	Government, Defense and Certificate Authority	Asia

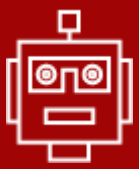
NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
LazarusGroup(Labyrinth Chollima,Group 77, Hastati Group,Whois HackingTeam,New RomanicCyberArmyTeam,Zinc,Hidden Cobra ,Appleworm ,APT-C-26 ,ATK3,SectorA01, ITG0)	North Korea **MOTIVE** Information theft and espionage, Sabotage And destruction, Financial crime **CVEs**	Education, chemical manufacturing, governmental research centers, IT service providers, utility providers, and telecommunications.	Germany, Brazil, India, Italy, Mexico, Switzerland, Saudi Arabia, Turkey, and the United States.

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 Fox Kitten	Iran **MOTIVE** Information theft and espionage **CVE** CVE-2021-44228	Aviation, Chemical, Energy, Defense, Engineering, Financial, Government, Healthcare, IT, Media, Manufacturing, Oil and gas,Retail, Telecommunications.	Australia, Austria, Finland, France, Germany, Hungary, Israel, Italy, Kuwait, Lebanon, Malaysia, Poland, Saudi Arabia, UAE, USA.

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 Earth Preta (Mustang Panda, Bronze President, TEMP.Hex, HoneyMyte, Red Lich)	China **MOTIVE** Information theft and espionage **CVEs**	Aviation, Education, Government, NGOs, Think Tanks, Telecommunications	United States, Canada, Mexico,Guatemala, Belize, El Salvador, Costa Rica,Panama, Colombia, Ecuador, Brazil,Argentina, Chile, Falkland Islands, Guinea,Ghana, Zambia, Botswana, South Africa, Egypt, Saudi Arabia, Yemen, Kuwait,Qatar, Bahrain,Iran,Afghanistan, Armenia,Azerbaijan,Georgia, Turkey,Cyprus, Greece, India, Sri Lanka, Australia,Indonesia, Malaysia, Thailand, Myanmar,Bangladesh, Bhutan, Nepal, China, Vietnam, Philippines, South Korea, Japan, Russia, Mongolia, Portugal, Italy, United Kingdom, Ireland, Finland, Estonia, Latvia, Lithuania, Poland, Belarus, Ukraine, Romania, Hungary, Bulgaria, North Macedonia, Albania, Croatia, Germany, Austria, Czechia, Belgium, Denmark, Malta

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 Cheshire	N/A **MOTIVE** Financial crime **CVEs**		Worldwide

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 OilRig (APT 34, Helix Kitten, Twisted Kitten , Crambus, Chrysene , Cobalt Gypsy , TA452 , IRN2, ATK 40, ITG13)	Iran **MOTIVE** Information theft and espionage **CVEs**	Aviation, Chemical, Education, Energy, Financial, Government, High-Tech, Hospitality, Oil, and gas, Telecommunications	Middle-East

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
 DEV-0569	N/A **MOTIVE** Financial crime **CVEs**	Electrical, Insurance, Renewable Electricity, Professional Services, Banks, Consumer, Telecommunications, Household Durables, Internet Software & Services, Retail, Diversified Consumer Services	USA, Canada, Germany, Malaysia, Italy, Ivory Coast, Puerto Rico, Finland, UK

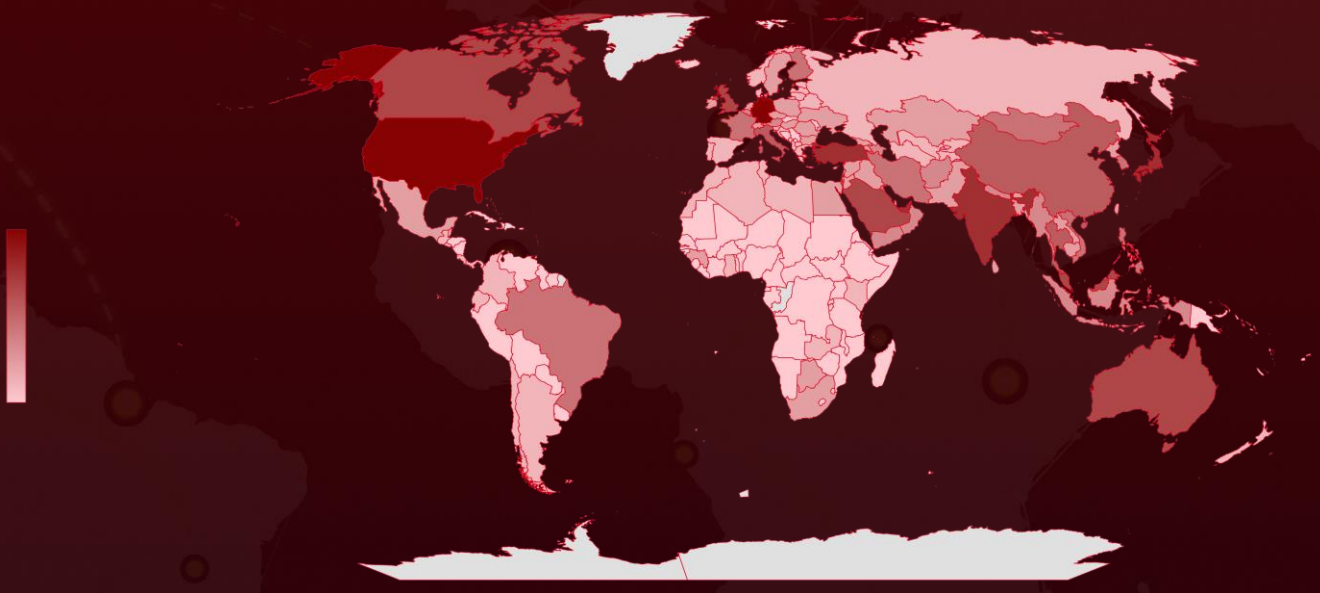
Malware of the Month

NAME	OVERVIEW	TYPE	DELIVERY METHOD
LODEINFO	LODEINFO is a sophisticated fileless malware that employs a RAR self-extracting archive (SFX) file. The loader sends target machine data to the C2.	Loader	Spear-phishing email
BlueFox	BlueFox Stealer has been marked malware-as-a-service since December 2021. A subscription to the customizable malware costs $350 per month on underground forums. A typical information stealer focused on cryptocurrency wallets.	Information stealer	Malware-as-a-service
Black Basta	Black Basta ransomware payload was delivered by exploiting Microsoft weaknesses Follina (CVE-2022-30190) and FIN7's Endpoint Detection and Response (EDR) security evasion tool.	Ransomware	Exploiting Microsoft flaws Follina (CVE-2022-30190)
Azov	The Azov ransomware executable is dropped and executed as a random file, scanning the compromised machine's directories, encrypting all files, and appending the. azov extension to the names of encrypted files.	Ransomware	cracks and pirated software
KmsdBot	KmsdBot is Golang-based malware that leverages the Secure Shell (SSH) cryptographic protocol to obtain access to targeted systems to mine cryptocurrencies and carry out distributed denial-of-service (DDoS) attacks.	Cryptominer	Unknown
BATLOADER	The "BatLoader" dropper is used to dispense a range of malware tools on victim devices, including a banking Trojan, an information stealer, and the Cobalt Strike post-exploit toolkit.	Loader	Unknown

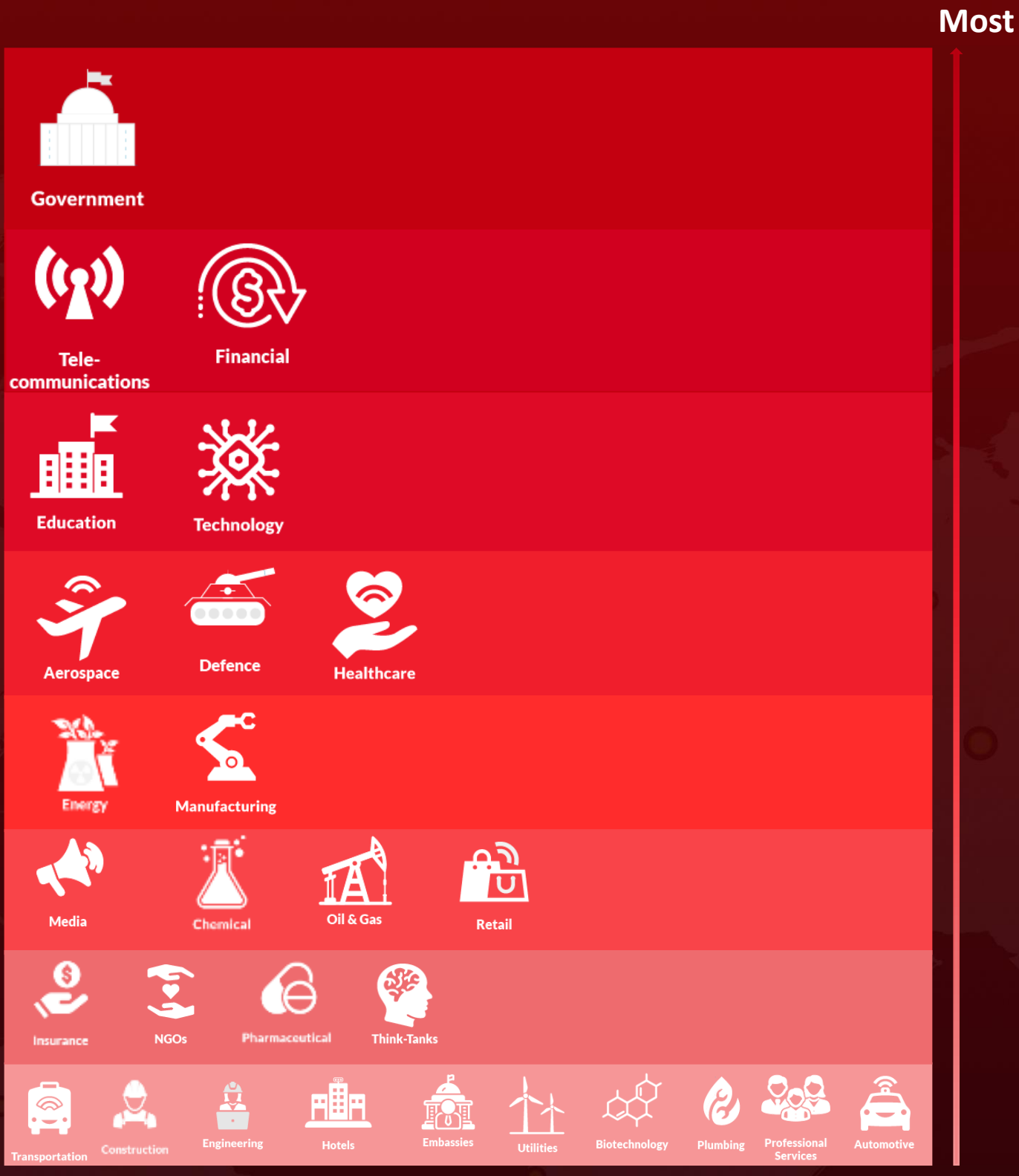
NAME	OVERVIEW	TYPE	DELIVERY METHOD
Bumblebee	The Bumblebee loader usually comes in the form of a DLL-like binary packed with a custom packer. Using BumbleBee, the threat actors loaded a meterpreter and cobalt strike beacons.	Loader	Unknown
DTrack	DTrack, is a flexible backdoor that unloads malware in stages The backdoor is currently installed by infiltrating networks with stolen credentials or abusing Internet-exposed servers.	Backdoor	Unknown
Typhon	Typhon stealer is a Malware-as-a-service that became widely known in early August 2022 offering capabilities to steal crypto-wallets, monitor keystrokes, and evade antivirus programs.	Stealer	Unknown
XMRig	XMRig crypto-mining malware employed on unpatched VMware Horizon server. To install XMRig crypto mining, the intruder exploited Log4Shell (CVE-2021-44228).	Crypto-mining malware	Exploited Log4Shell (CVE-2021-44228)
Venus	Venus ransomware aka Goodgame has been a source of concern since August 2022. It is an example of the legacy ransomware model: a standalone package sold on underground markets	Ransomware	Unknown
RapperBot	The new RapperBot malware version creates a botnet capable of launching DDoS attacks. It can launch Telnet brute-force strikes, and DoS attacks using the Generic Routing Encapsulation (GRE) tunneling protocol	Botnet	Unknown
Aurora botnet	Aurora botnet a Malware-as-a-Service (MaaS) since August 2022 has been transformed into a stealer. Exfiltrate data directly from disks and load additional payloads	Information stealer	Unknown

NAME	OVERVIEW	TYPE	DELIVERY METHOD
Qakbot	Qakbot An information stealer and banking Trojan with backdoor capabilities. It inserts malicious replies into the middle of existing email conversations, using the compromised accounts of other infection victims	Information Stealer	Spear-Phishing
Royal	Royal Ransomware is a newly used service in early 2022, with the objective of gaining access to a victim's environment, encrypting all their files and extorting a ransom in order to regain access.	Ransomware	Phishing mails
RansomExx	RansomExx is a ransomware variant that operates on a ransomware-as-a-service(RaaS) model and has been active since it first appeared in 2018 as Defray777. The latest version, dubbed RansomExx2,is primarily intended to work on Linux.	Ransomware	Unknown
Punisher	A new variant of the Punisher ransomware is spreading disguised as a COVID tracking application. Punisher Encryptor is a.NET binary that runs on Windows operating systems.	Ransomware	Phisihing

Targeted Countries



Targeted Industries



Common MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1589: Gather Victim Identity Information	T1583: Acquire Infrastructure	T1078: Valid Accounts	T1047: Windows Management Instrumentation	T1037: Boot or Logon Initialization Scripts	T1037: Boot or Logon Initialization Scripts	T1027: Obfuscated Files or Information
T1589.002: Email Addresses	T1583.001: Domains	T1078.001: Default Accounts	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1027.002: Software Packing
T1590: Gather Victim Network Information	T1583.004: Server	T1133: External Remote Services	T1053.005: Scheduled Task	T1053.005: Scheduled Task	T1053.005: Scheduled Task	T1027.005: Indicator Removal from Tools
T1592: Gather Victim Host Information	T1584: Compromise Infrastructure	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1078: Valid Accounts	T1055: Process Injection	T1027.006: HTML Smuggling
T1593: Search Open Websites/Domains	T1584.005: Botnet	T1195: Supply Chain Compromise	T1059.001: PowerShell	T1078.001: Default Accounts	T1055.012: Process Hollowing	T1036: Masquerading
T1593.002: Search Engines	T1585: Establish Accounts	T1566: Phishing	T1059.003: Windows Command Shell	T1098: Account Manipulation	T1068: Exploitation for Privilege Escalation	T1036.005: Match Legitimate Name or Location
T1595: Active Scanning	T1585.002: Email Accounts	T1566.001: Spearphishing Attachment	T1059.004: Unix Shell	T1133: External Remote Services	T1078: Valid Accounts	T1036.007: Double File Extension
T1598: Phishing for Information	T1586: Compromise Accounts	T1566.002: Spearphishing Link	T1059.005: Visual Basic	T1136: Create Account	T1078.001: Default Accounts	T1055: Process Injection
T1598.002: Spearphishing Attachment	T1587: Develop Capabilities		T1059.007: JavaScript	T1136.001: Local Account	T1134: Access Token Manipulation	T1055.012: Process Hollowing
	T1587.001: Malware		T1106: Native API	T1136.002: Domain Account	T1543: Create or Modify System Process	T1070: Indicator Removal
	T1587.003: Digital Certificates		T1129: Shared Modules	T1505: Server Software Component	T1543.003: Windows Service	T1070.004: File Deletion
	T1588: Obtain Capabilities		T1203: Exploitation for Client Execution	T1543: Create or Modify System Process	T1546: Event Triggered Execution	T1070.006: Timestomp
	T1588.001: Malware		T1204: User Execution	T1543.003: Windows Service	T1547: Boot or Logon Autostart Execution	T1078: Valid Accounts
	T1588.002: Tool		T1204.001: Malicious Link	T1546: Event Triggered Execution	T1547.001: Registry Run Keys / Startup Folder	T1078.001: Default Accounts
	T1588.006: Vulnerabilities		T1204.002: Malicious File	T1547: Boot or Logon Autostart Execution	T1547.012: Print Processors	T1112: Modify Registry
	T1608: Stage Capabilities		T1569: System Services	T1547.001: Registry Run Keys / Startup Folder	T1548: Abuse Elevation Control Mechanism	T1134: Access Token Manipulation
	T1608.001: Upload Malware		T1569.002: Service Execution	T1547.012: Print Processors	T1548.002: Bypass User Account Control	T1140: Deobfuscate/Decode Files or Information
	T1608.006: SEO Poisoning			T1554: Compromise Client Software Binary	T1574: Hijack Execution Flow	T1202: Indirect Command Execution
				T1556: Modify Authentication Process	T1574.001: DLL Search Order Hijacking	T1211: Exploitation for Defense Evasion
				T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading	T1218: System Binary Proxy Execution
				T1574.001: DLL Search Order Hijacking		**T1218.005: Mshta**
				T1574.002: DLL Side-Loading		**T1218.007: Msiexec**
						T1218.010: Regsvr32
						T1218.011: Rundll32
						T1497: Virtualization/Sandbox Evasion
						T1497.001: System Checks
						T1497.003: Time Based Evasion
						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
						T1553.004: Install Root Certificate
						T1553.005: Mark-of-the-Web Bypass
						T1556: Modify Authentication Process
						T1562: Impair Defenses
						T1562.001:Disable or Modify Tools
						T1562.004: Disable or Modify System Firewall
						T1562.009: Safe Mode Boot
						T1564: Hide Artifacts
						T1564.003: Hide Artifacts: Hidden Window
						T1574: Hijack Execution Flow
						T1574.001: DLL Search Order Hijacking
						T1574.002: DLL Side-Loading
						T1622: Debugger Evasion

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1003: OS Credential Dumping	T1007: System Service Discovery	T1021: Remote Services	T1005: Data from Local System	T1001: Data Obfuscation	T1020: Automated Exfiltration	T1485: Data Destruction
T1003.001: LSASS Memory	T1010: Application Window Discovery	T1021.001: Remote Desktop Protocol	T1056: Input Capture	T1071: Application Layer Protocol	T1041: Exfiltration Over C2 Channel	T1486: Data Encrypted for Impact
T1003.002: Security Account Manager	T1012: Query Registry	T1021.002: SMB/Windows Admin Shares	T1056.001: Keylogging	T1071.001: Web Protocols	T1567: Exfiltration Over Web Service	T1489: Service Stop
T1003.006: DCSync	T1016: System Network Configuration Discovery	T1080: Taint Shared Content	T1113: Screen Capture	T1090: Proxy		T1490: Inhibit System Recovery
T1040: Network Sniffing	T1016.001: Internet Connection Discovery	T1210: Exploitation of Remote Services	T1114: Email Collection	T1090.001: Internal Proxy		T1491: Defacement
T1056: Input Capture	T1018: Remote System Discovery	T1550: Use Alternate Authentication Material	T1119: Automated Collection	T1090.002: External Proxy		T1491.001: Internal Defacement
T1056.001: Keylogging	T1033: System Owner/User Discovery	T1550.002: Pass the Hash	T1560: Archive Collected Data	T1090.004: Domain Fronting		T1496: Resource Hijacking
T1110: Brute Force	T1040: Network Sniffing	T1570: Lateral Tool Transfer		T1095: Non-Application Layer Protocol		T1499: Endpoint Denial of Service
T1187: Forced Authentication	T1046: Network Service Discovery			T1102: Web Service		T1565: Data Manipulation
T1528: Steal Application Access Token	T1049: System Network Connections Discovery			T1104: Multi-Stage Channels		
T1539: Steal Web Session Cookie	T1057: Process Discovery			T1105: Ingress Tool Transfer		
T1552: Unsecured Credentials	T1069: Permission Groups Discovery			T1219: Remote Access Software		
T1555: Credentials from Password Stores	T1069.001: Local Groups			T1571: Non-Standard Port		
T1555.003: Credentials from Web Browsers	T1069.002: Domain Groups			T1573: Encrypted Channel		
T1555.004: Windows Credential Manager	T1082: System Information Discovery			T1573.001: Symmetric Cryptography		
T1556: Modify Authentication Process	T1083: File and Directory Discovery			T1573.002: Asymmetric Cryptography		
T1558: Steal or Forge Kerberos Tickets	T1087: Account Discovery					
	T1087.002: Domain Account					
	T1120: Peripheral Device Discovery					
	T1124: System Time Discovery					
	T1135: Network Share Discovery					
	T1482: Domain Trust Discovery					
	T1497: Virtualization/Sandbox Evasion					
	T1497.001: System Checks					
	T1497.003: Time Based Evasion					
	T1518: Software Discovery					
	T1518.001: Security Software Discovery					
	T1614: System Location Discovery					
	T1622: Debugger Evasion					

Threat Advisories (November 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				

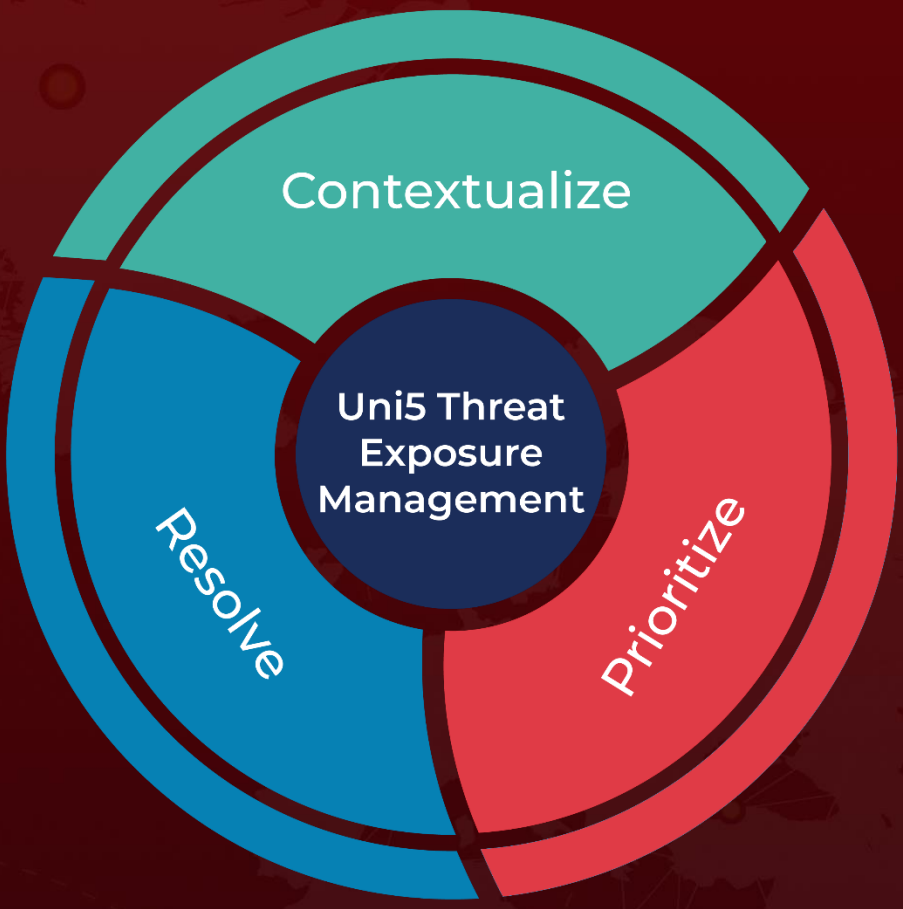
Click on any of the icons to get directed to the advisory

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

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

December 1, 2022 . 11:30 AM

More at www.hivepro.com