Hive Pro

THREAT DIGEST

Vulnerabilities & Threats that Matter
October 2022

Top 5 Takeaways

#1 In October, one vulnerability remained unpatched in VMware although the flaw had been known about for a year. Another 22-year-old vulnerability (CVE-2022-35737), in the SQLite library API, has now been addressed.

#2 A new vulnerability (CVE-2022-42889) in Apache Commons Text text2shell is like the infamous Log4Shell.

#3 The Bring Your Own Vulnerable Driver (BYOVD) attack is utilized by the Lazarus group and BlackByte Ransomware to infiltrate victims' vulnerable infrastructures.

#4 A new tailgate campaign instigated by threat actors **Hafnium** and **OilRig** intends to exploit the **Fortinet** Authentication Bypass vulnerability.

#5 The Budworm espionage gang leveraged Log4j vulnerabilities to compromise the Apache Tomcat service and exfiltrate sensitive data.

Vulnerabilities of the Month	Threat Actors of the Month	Malware of the Month	Top Targeted Countries	Top Targeted Industries	Common MITRE ATT&CK TTPs
51	11	6	UAE Saudi Arabia Turkey Japan Qatar	Technology Telecommunications Government	134

Detailed Report

⚙ Vulnerabilities of the Month

VENDOR	CVE	PATCH DETAILS
msi	CVE-2019-16098	No Patch Available
FORTINET	CVE-2022-40684	Upgrade to FortiOS version 7.07 or 7.2.2 or above Upgrade to FortiProxy version 7.07 or 7.2.1 or above Upgrade to FortiSwitchManager version 7.2.1 or above
zimbra	CVE-2022-41352*	https://blog.zimbra.com/2022/10/new-zimbra-patches-9-0-0-patch-27-8-8-15-patch-34/
vmware	CVE-2021-22048 CVE-2021-39144 CVE-2022-31678	For CVE-2021-22048: No Patch Available For CVE-2021-39144 & CVE-2022-31678: https://kb.vmware.com/s/article/89809
	CVE-2022-3445 CVE-2022-3446 CVE-2022-3447 CVE-2022-3448 CVE-2022-3449 CVE-2022-3450 CVE-2022-3723*	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
Adobe	CVE-2022-35710 CVE-2022-35711 CVE-2022-35712 CVE-2022-35690 CVE-2022-38418 CVE-2022-38424 CVE-2022-38450 CVE-2022-42339 CVE-2022-35698 CVE-2022-38440 CVE-2022-38441 CVE-2022-38442 CVE-2022-38444 CVE-2022-38445 CVE-2022-38446 CVE-2022-38447 CVE-2022-38448	https://helpx.adobe.com/security/products/coldfusion/apsb22-44.html https://helpx.adobe.com/security/products/acrobat/apsb22-46.html https://helpx.adobe.com/security/products/magento/apsb22-48.html https://helpx.adobe.com/security/products/dimension/apsb22-57.html
THE APACHE SOFTWARE FOUNDATION	CVE-2021-44228* CVE-2021-45105	https://logging.apache.org/log4j/2.x/security.html
	CVE-2022-42889	Upgrade to Apache Commons Text 1.10.0. https://lists.apache.org/thread/n2bd4vdsgkqh2tm14l1wyc3jyol7s1om

VENDOR	CVE	PATCH DETAILS
Microsoft	CVE-2022-22035 CVE-2022-37968 CVE-2022-37976 CVE-2022-37979 CVE-2022-37988 CVE-2022-38000 CVE-2022-38048 CVE-2022-38053 CVE-2022-41033* CVE-2022-41036 CVE-2022-41038 CVE-2022-41043* CVE-2022-41081 CVE-2021-31207 CVE-2021-34473 CVE-2021-34523	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22035 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37968 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37976 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37979 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37988 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38000 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38048 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38053 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41033 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41036 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41038 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41043 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41081 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31207 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523
SQLite	CVE-2022-35737	https://www.sqlite.org/cves.html
DREAM SECURITY Digital Trust	CVE-2021-26606	Update MagicLine 4.0 to version 1.0.0.18 or later

***zero-day vulnerability**

Threat Actors of the Month

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Polonium	Lebanon **MOTIVE** Information theft and espionage **CVEs**	Engineering, Information Technology, Law, Communications, Marketing, Media, Insurance, Social Services, Defense, IT, Manufacturing	Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Earth Aughisky	China	Government, Telecommunications, Technology, Manufacturing, Transportation, Healthcare	Taiwan, Japan
	MOTIVE		
	Sabotage and Destruction		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
APT41(Winnti, Group 72, BARIUM, LEAD, GREF, WICKED PANDA, Double Dragon, TG-2633, Bronze Atlas, Red Kelpie, Blackfly, Earth Baku, SparklingGoblin, Grayfly)	China	Construction, Defense, Education, Energy, Financial, Government, Healthcare, High-Tech, Hospitality, Manufacturing, Media, Oil and gas, Petrochemical, Pharmaceutical, Retail, Telecommunications, Transportation, gaming.	Australia, Bahrain, Brazil, Canada, Chile, Denmark, Finland, France, Georgia, Hong Kong, India, Indonesia, Italy, Japan, Malaysia, Mexico, Myanmar, Netherlands, Pakistan, Philippines, Poland, Qatar, Saudi Arabia, Singapore, South Korea, South Africa, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.
	MOTIVE		
	Financial crime, Information theft and espionage		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
OilRig (Helminth, Clayslide, APT34, IRN2, COBALT GYPSY, ITG13, CHRYSENE, HEXANE, LYCEUM, HELIX KITTEN)	Iran	Chemicals, Education, Energy, Financial (Finance), Government, Legal, Oil and Gas, Telecommunications	Oman, Azerbaijan, Bahrain, Iraq, Israel, Jordan, Kuwait, Lebanon, Mauritius, Qatar, Saudi Arabia, South Africa, Turkey, UAE, MENA region
	MOTIVE		
	Information theft and espionage, Financial gain		
	CVE		
	CVE-2022-40684		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Budworm (Emissary Panda, APT27, LuckyMouse, Bronze Union, TG-3390, TEMP.Hippo, Group35, ATK 15, IronTiger, EarthSmilodon, RedPhoenix, ZipToken)	China **MOTIVE** Information theft and espionage **CVEs** CVE-2021-44228 CVE-2021-45105	Aerospace, Aviation, Defense, Education, Embassies, Government, Manufacturing, Technology, Think Tanks, Telecommunications	Australia, Canada, China, Germany, Hong Kong, India, Iran, Iraq, Israel, Japan, Jordan, Kuwait, Lebanon, Mongolia, Oman, Palestine, Philippines, Qatar, Russia, Saudi Arabia, South Korea, Spain, Syria, Taiwan, Thailand, Tibet, Turkey, UK, United Arab Emirates, USA, Yemen

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
WIP19	China **MOTIVE** Espionage **CVEs**	Telecommunications and IT service providers	Middle East and Asia

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
DEV-0960	Unkown **MOTIVE** Financial gain **CVEs**	Transportation	Ukraine and Poland

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Hafnium (UNC2639, UNC2640, UNC2643, Ant)	China	Healthcare, Legal, NGO, Education	USA, UK, Russia, Bangladesh, Belgium, Iran, Turkey, Norway, New Zealand, Germany, Canada, Australia, South Korea, Japan, Italy, France, UAE
	MOTIVE		
	Information theft and espionage, Financial gain		
	CVE		
	CVE-2022-40684		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Daixin Team	Unknown	Energy, Media and Healthcare	USA
	MOTIVE		
	Financial gain		
	CVEs		

NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
SideWinder (Rattlesnake, T-APT-04, APT-C-17, Razor Tiger, Baby Elephant, Operation Origami)	India	Defense, Government, Hospitality, Legal, Transportation	Afghanistan, Bangladesh, China, Hungary, Myanmar, Nepal, Pakistan, Qatar, Saudi Arabia , Sri Lanka
	MOTIVE		
	Information theft and espionage		
	CVEs		

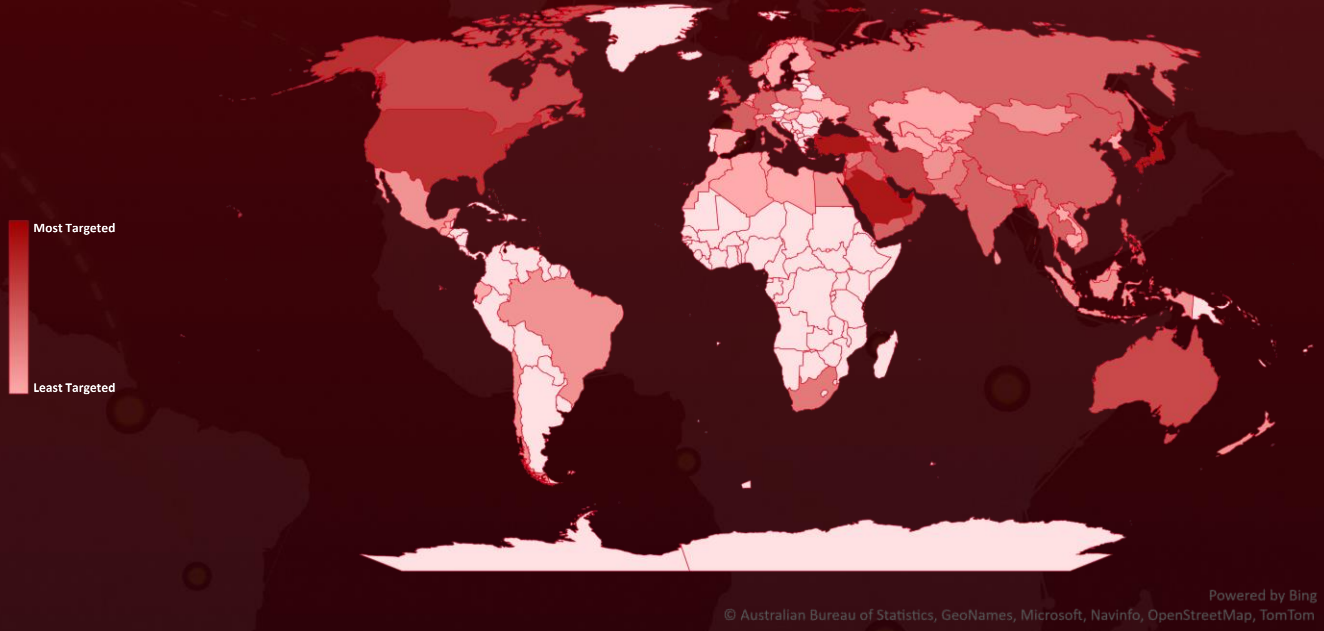
NAME	ORIGIN	TARGET INDUSTRIES	TARGET COUNTRIES
Lazarus Group (Labyrinth Chollima, Group77, Hastati Group, Whois Hacking Team, NewRomanicCyber ArmyTeam, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK3, SectorA01, ITG03)	North Korea	Aerospace, Defense, Engineering, Financial, Government, Media, Shipping and Logistics, Technology and Cryptocurrencies	Australia, Bangladesh, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	CVEs		

Malware of the Month

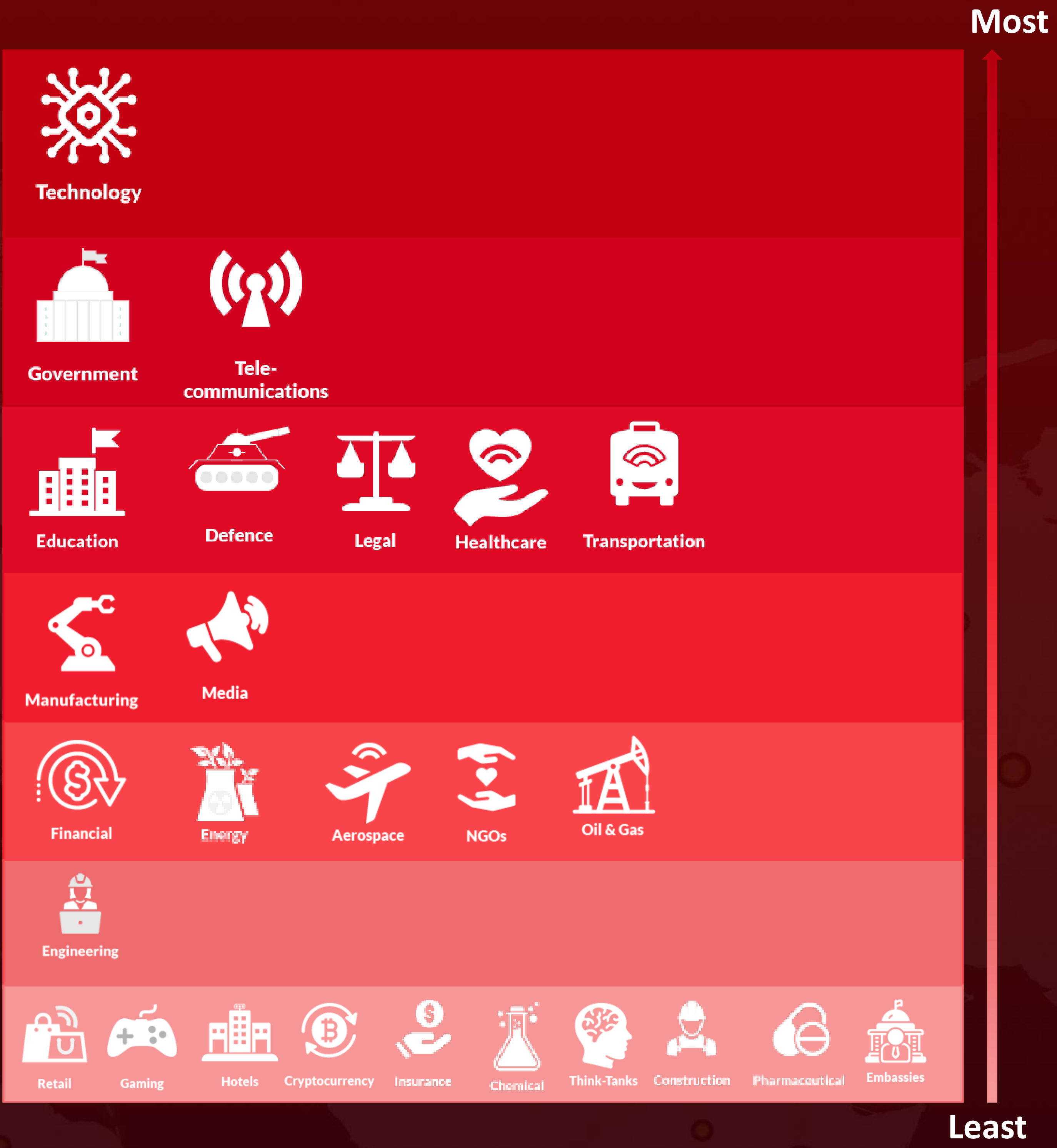
NAME	OVERVIEW	TYPE	DELIVERY METHOD
BlackByte	BlackByte is the latest to embrace BYOVD to achieve its objectives. Recent attacks mounted by the group have taken advantage of a vulnerability (CVE-2019-16098) in the Micro-Star MSI Afterburner RTCore64.sys driver to disable security products.	Ransomware	Known vulnerability(CVE-2019-16098) in the legitimate vulnerable driver RTCore64.sys
LilithBot	LilithBot malware variant inspects for the presence of several DLLs and Win32 PortConnector to validate that the LilithBot is running on a host machine rather than a virtual machine.	malware-as-a-service	Unknown
Prestige	Prestige uses the CryptoPP C++ library to encrypt each eligible file using AES as part of its encryption procedure	Ransomware	Unknown

NAME	OVERVIEW	TYPE	DELIVERY METHOD
Spyder Loader	Spyder Loader is packaged as a 64-bit Portable Executable (PE) DLL in the recent intrusion. During the initial infection stage, Spyder Loader loads AES-encrypted blobs that create the next-stage payload, "wlbsctrl.dll."	Loader	Unknown
URSNIF	URSNIF (also known as Gozi or Gozi/ISFB) is one of the oldest banker malware families, with reported attacks dating back to 2007. On the infected computer, the LDR4 variation appears as a DLL module that is executed via the DllRegisterServer function, although there are frequently other arbitrarily named decoy functions exported to mislead sandboxes.	Backdoor	Phishing via a recruitment-related lure
LV	LV starts its attack chain with the exploitation of Exchange servers in the intended network when a web shell file is dropped in the public access directories leveraging ProxyShell. To aid lateral movement, they employed Mimikatz to leak credentials.	Ransomware	Exploiting ProxyShell (CVE-2021-31207, CVE-2021-34473 & CVE-2021-34523)

Targeted Countries


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

Targeted Industries



Most

Technology

Government
Tele-communications

Education
Defence
Legal
Healthcare
Transportation

Manufacturing
Media

Financial
Energy
Aerospace
NGOs
Oil & Gas

Engineering

Retail
Gaming
Hotels
Cryptocurrency
Insurance
Chemical
Think-Tanks
Construction
Pharmaceutical
Embassies

Least

Common MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1591: Gather Victim Org Information	T1583: Acquire Infrastructure	T1078: Valid Accounts	T1047: Windows Management Instrumentation	T1037: Boot or Logon Initialization Scripts	T1037: Boot or Logon Initialization Scripts	T1014: Rootkit
T1592: Gather Victim Host Information	T1583.003: Virtual Private Server	T1189: Drive-by Compromise	T1053: Scheduled Task/Job	T1037.005: Startup Items	T1037.005: Startup Items	T1027: Obfuscated Files or Information
T1598: Phishing for Information	T1584: Compromise Infrastructure	T1190: Exploit Public-Facing Application	T1053.002: At	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1036: Masquerading
T1598.002: Spearphishing Attachment	T1584.006: Web Services	T1566: Phishing	T1053.005: Scheduled Task	T1053.002: At	T1053.002: At	T1036.005: Match Legitimate Name or Location
	T1586: Compromise Accounts	T1566.001: Spearphishing Attachment	T1059: Command and Scripting Interpreter	T1053.005: Scheduled Task	T1053.005: Scheduled Task	T1055: Process Injection
	T1587: Develop Capabilities		T1059.001: PowerShell	T1078: Valid Accounts	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
	T1587.001: Malware		T1059.003: Windows Command Shell	T1098: Account Manipulation	T1055.001: Dynamic-link Library Injection	T1055.012: Process Hollowing
	T1587.002: Code Signing Certificates		T1059.007: JavaScript	T1205: Traffic Signaling	T1055.012: Process Hollowing	T1070: Indicator Removal
	T1588: Obtain Capabilities		T1072: Software Deployment Tools	T1543: Create or Modify System Process	T1068: Exploitation for Privilege Escalation	T1070.004: File Deletion
	T1588.001: Malware		T1106: Native API	T1546: Event Triggered Execution	T1078: Valid Accounts	T1078: Valid Accounts
	T1588.006: Vulnerabilities		T1129: Shared Modules	T1547: Boot or Logon Autostart Execution	T1543: Create or Modify System Process	T1112: Modify Registry
	T1608: Stage Capabilities		T1203: Exploitation for Client Execution	T1547.001: Registry Run Keys / Startup Folder	T1546: Event Triggered Execution	T1140: Deobfuscate/Decode Files or Information
	T1608.004: Drive-by Target		T1204: User Execution	T1547.006: Kernel Modules and Extensions	T1547: Boot or Logon Autostart Execution	T1205: Traffic Signaling
			T1204.002: Malicious File	T1547.009: Shortcut Modification	T1547.001: Registry Run Keys / Startup Folder	T1211: Exploitation for Defense Evasion
			T1569: System Services	T1574: Hijack Execution Flow	T1547.006: Kernel Modules and Extensions	T1218: System Binary Proxy Execution
			T1569.002: Service Execution	T1574.002: DLL Side-Loading	T1547.009: Shortcut Modification	T1218.004: InstallUtil
					T1548: Abuse Elevation Control Mechanism	T1222: File and Directory Permissions Modification
					T1548.002: Bypass User Account Control	T1480: Execution Guardrails
					T1574: Hijack Execution Flow	T1548: Abuse Elevation Control Mechanism
					T1574.002: DLL Side-Loading	T1548.002: Bypass User Account Control
						T1550: Use Alternate Authentication Material
						T1550.002: Pass the Hash
						T1562: Impair Defenses
						T1564: Hide Artifacts
						T1574: Hijack Execution Flow
						T1574.002: DLL Side-Loading
						T1620: Reflective Code Loading

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	T1041: Exfiltration Over C2 Channel	T1486: Data Encrypted for Impact
T1003.001: LSASS Memory	T1012: Query Registry	T1021.001: Remote Desktop Protocol	T1056: Input Capture	T1008: Fallback Channels	T1567: Exfiltration Over Web Service	T1489: Service Stop
T1056: Input Capture	T1016: System Network Configuration Discovery	T1021.004: SSH	T1056.001: Keylogging	T1071: Application Layer Protocol	T1567.002: Exfiltration to Cloud Storage	T1490: Inhibit System Recovery
T1056.001: Keylogging	T1018: Remote System Discovery	T1072: Software Deployment Tools	T1113: Screen Capture	T1071.001: Web Protocols		T1496: Resource Hijacking
T1110: Brute Force	T1033: System Owner/User Discovery	T1210: Exploitation of Remote Services	T1114: Email Collection	T1090: Proxy		T1565: Data Manipulation
T1552: Unsecured Credentials	T1049: System Network Connections Discovery	T1550: Use Alternate Authentication Material	T1114.002: Remote Email Collection	T1095: Non-Application Layer Protocol		
T1552.002: Credentials in Registry	T1057: Process Discovery	T1550.002: Pass the Hash	T1115: Clipboard Data	T1102: Web Service		
T1555: Credentials from Password Stores	T1082: System Information Discovery	T1563: Remote Service Session Hijacking	T1125: Video Capture	T1102.002: Bidirectional Communication		
	T1083: File and Directory Discovery	T1563.001: SSH Hijacking	T1213: Data from Information Repositories	T1105: Ingress Tool Transfer		
	T1087: Account Discovery	T1563.002: RDP Hijacking	T1560: Archive Collected Data	T1132: Data Encoding		
	T1135: Network Share Discovery	T1570: Lateral Tool Transfer	T1560.002: Archive via Library	T1205: Traffic Signaling		
	T1201: Password Policy Discovery			T1571: Non-Standard Port		
	T1614: System Location Discovery			T1572: Protocol Tunneling		
				T1573: Encrypted Channel		
				T1573.001: Symmetric Cryptography		

Threat Advisories (October 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 🔴🐞						

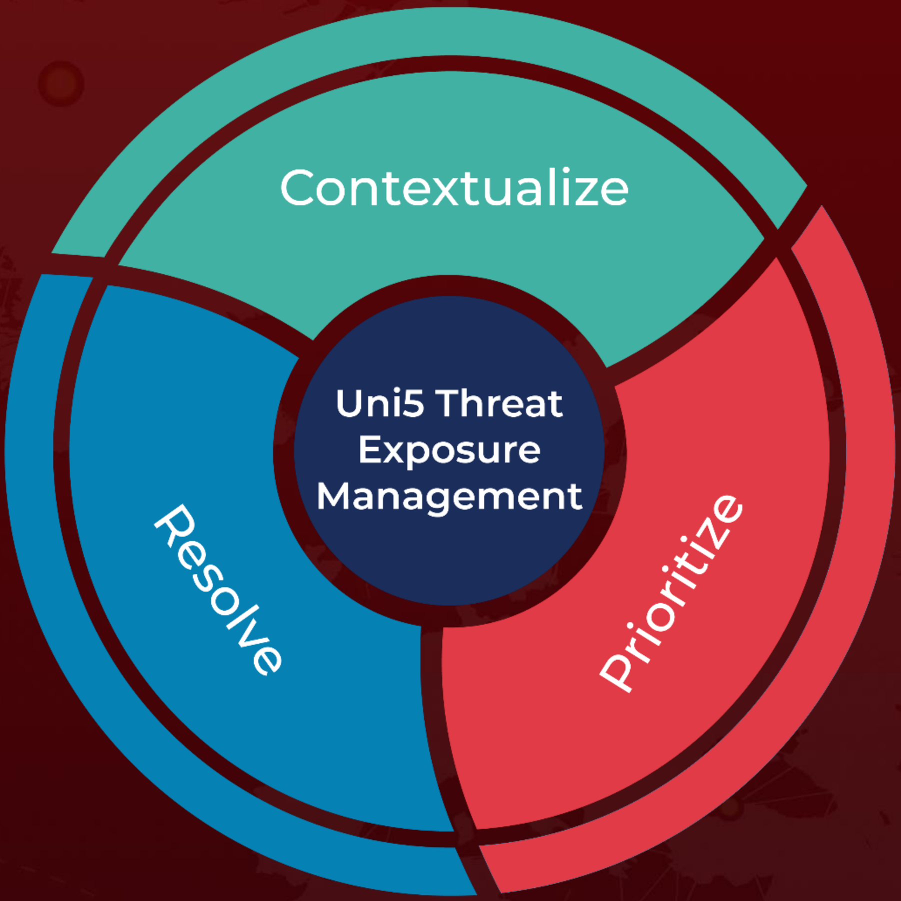
Click on any of the icons to get directed to the advisory

🔴🐞	Red Vulnerability Report
🟡🐞	Amber Vulnerability Report
🟢🐞	Green Vulnerability Report
🔴⚔	Red Attack Report
🟡⚔	Amber Attack Report
🔴👽	Red Actor Report

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 2, 2022 • 5:30 AM

More at www.hivepro.com