Hive Pro
THREAT DIGEST

Fix What Matters to Your Business

Summary of Vulnerabilities & Threats

10–16 October 2022

The second week of October 2022 witnessed the discovery of 639 vulnerabilities out of which 41 gained the attention of Threat Actors and security researchers worldwide. Among these 41, there was four zero-day. Hive Pro Threat Research Team has curated a list of 41 CVEs that require immediate action.

This week also witnessed a spike in cryptojacking campaigns, with intruders exploiting DLL Side-Loading flaws in Microsoft OneDrive.

Further, we also observed 4 Threat Actor groups being highly active in the last week. First was the POLONIUM, a Lebanon threat actor, popular for Information theft and espionage that leveraged cloud services to employ backdoors. The second was the Earth Aughisky, a Chinese threat actor, popular for Sabotage and Destruction that conducted a spear-phishing campaign. The third was the WIP19, a Chinese threat actor, popular for Espionage targeted telcos with malware. The fourth was the Budworm, a Chinese threat actor, popular for Information theft and espionage that exploited Log4j vulnerabilities. Common TTPs which could potentially be exploited by these threat actors or CVEs can be found in the detailed section.

Published Vulnerabilities	Interesting Vulnerabilities	Active Threat Groups	Targeted Countries	Targeted Industries	ATT&CK TTPs
639	41	4	60	16	89

Detailed Report

Interesting Vulnerabilities

VENDOR	CVE	PATCH DETAILS
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
zimbra	CVE-2022-41352*	Patch is unavailable Recommendations: https://blog.zimbra.com/2022/09/security-update-make-sure-to-install-pax-spax/
Microsoft	CVE-2022-41033* CVE-2022-41043* CVE-2022-37968 CVE-2022-41038 CVE-2022-38053 CVE-2022-41036 CVE-2022-37976 CVE-2022-37979 CVE-2022-22035 CVE-2022-38000 CVE-2022-41081 CVE-2022-38048 CVE-2022-37988	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41033 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41043 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-37968 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41038 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-38053 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41036 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-37976 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-37979 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22035 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-38000 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41081 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-38048 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-37988
vmware	CVE-2021-22048	Patch is unavailable

* zero-day vulnerability

VENDOR	CVE	PATCH DETAILS
LOG4J	CVE-2021-44228* CVE-2021-45105	https://logging.apache.org/log4j/2.x/security.html
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
	CVE-2022-3445 CVE-2022-3446 CVE-2022-3447 CVE-2022-3448 CVE-2022-3449 CVE-2022-3450	Update Google Chrome to version 106.0.5249.119 Patch Link https://www.google.com/intl/en/chrome/?standalone=1

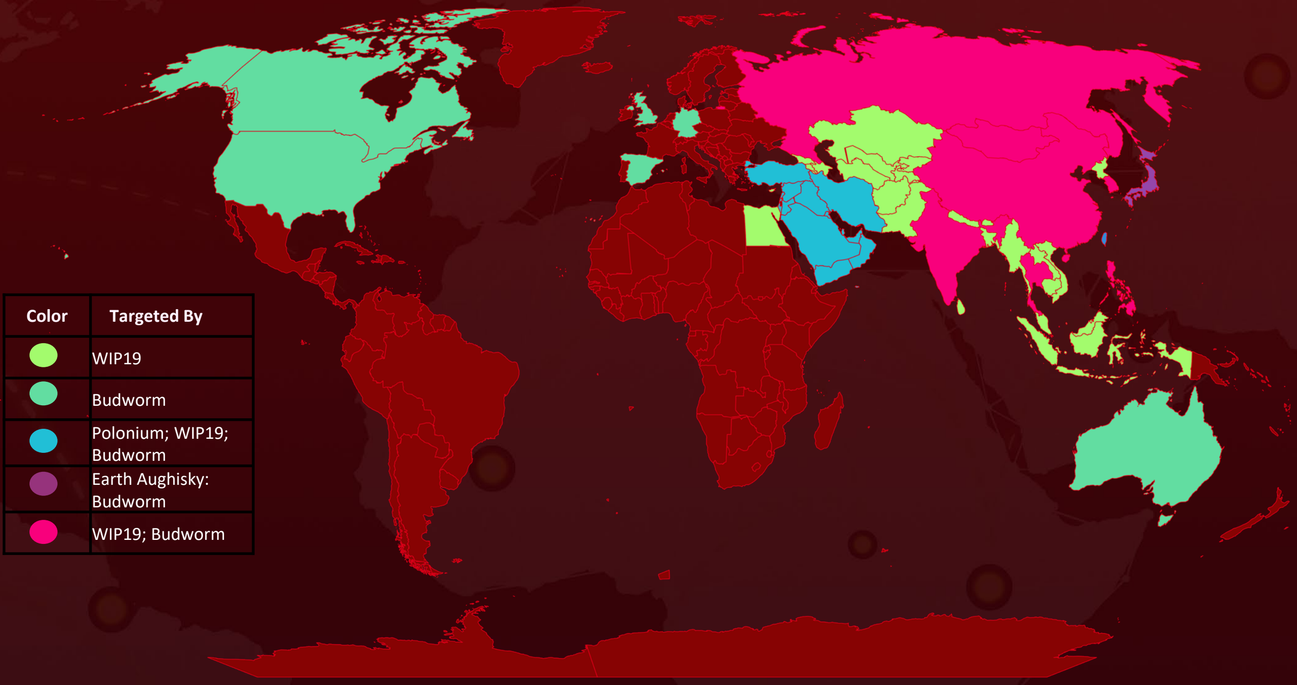
* zero-day vulnerability

Active Actors

ICON	NAME	ORIGIN	MOTIVE
	Polonium	Lebanon	Information theft and espionage
	Earth Aughisky	China	Sabotage and Destruction

ICON	NAME	ORIGIN	MOTIVE
	WIP19	China	Espionage
	Budworm(Emissary Panda, APT27, Lucky Mouse, Bronze Union, TG-3390, TEMP.Hippo ,Group35,ATK 15, Iron Tiger, Earth Smilodon, Red Phoenix , ZipToken)	China	Information theft and espionage

Targeted Locations



Color	Targeted By
●	WIP19
●	Budworm
●	Polonium; WIP19; Budworm
●	Earth Aughisky: Budworm
●	WIP19; Budworm

Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Targeted Industries

Aerospace

Legal

Insurance

Transportation

Media

Defence

Technology

Engineering

Telecommunications

Government

Manufacturing

Aviation

Think-Tanks

Healthcare

Education

Embassies

Common MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1592: Gather Victim Host Information	T1583: Acquire Infrastructure	T1078: Valid Accounts	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1027: Obfuscated Files or Information
T1598: Phishing for Information	T1583.003: Virtual Private Server	T1190: Exploit Public-Facing Application	T1053.002: At	T1053.002: At	T1053.002: At	T1036: Masquerading
	T1584: Compromise Infrastructure	T1199: Trusted Relationship	T1053.005: Scheduled Task	T1053.005: Scheduled Task	T1053.005: Scheduled Task	T1036.005: Match Legitimate Name or Location
	T1586: Compromise Accounts	T1566: Phishing	T1059: Command and Scripting Interpreter	T1078: Valid Accounts	T1055: Process Injection	T1055: Process Injection
	T1587: Develop Capabilities		T1059.001: PowerShell	T1205: Traffic Signaling	T1055.012: Process Injection: Process Hollowing	T1055.012: Process Hollowing
	T1587.001: Malware		T1059.003: Windows Command Shell	T1543: Create or Modify System Process	T1068: Exploitation for Privilege Escalation	T1070: Indicator Removal on Host
	T1588: Obtain Capabilities		T1072: Software Deployment Tools	T1546: Event Triggered Execution	T1078: Valid Accounts	T1070.004: File Deletion
	T1588.001: Malware		T1106: Native API	T1547: Boot or Logon Autostart Execution	T1543: Create or Modify System Process	T1078: Valid Accounts
	T1608: Stage Capabilities		T1129: Shared Modules	T1547.001: Registry Run Keys / Startup Folder	T1546: Event Triggered Execution	T1112: Modify Registry
			T1203: Exploitation for Client Execution	T1547.009: Shortcut Modification	T1547: Boot or Logon Autostart Execution	T1140: Deobfuscate/Decode Files or Information
			T1204: User Execution	T1574: Hijack Execution Flow	T1547.001: Registry Run Keys / Startup Folder	T1205: Traffic Signaling
			T1204.002: Malicious File	T1574.002: DLL Side-Loading	T1547.009: Shortcut Modification	T1211: Exploitation for Defense Evasion
					T1548: Abuse Elevation Control Mechanism	T1218: System Binary Proxy Execution
					T1548.002: Bypass User Account Control	T1218.004: InstallUtil
					T1574: Hijack Execution Flow	T1480: Execution Guardrails
					T1574.002: DLL Side-Loading	T1548: Abuse Elevation Control Mechanism
						T1548.002: Bypass User Account Control
						T1553: Subvert Trust Controls
						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	T1072: Software Deployment Tools	T1005: Data from Local System	T1001: Data Obfuscation	T1041: Exfiltration Over C2 Channel	T1490: Inhibit System Recovery
T1056: Input Capture	T1016: System Network Configuration Discovery	T1210: Exploitation of Remote Services	T1056: Input Capture	T1008: Fallback Channels	T1567: Exfiltration Over Web Service	T1496: Resource Hijacking
T1056.001: Keylogging	T1033: System Owner/User Discovery	T1570: Lateral Tool Transfer	T1056.001: Keylogging	T1071: Application Layer Protocol	T1567.002: Exfiltration to Cloud Storage	T1565: Data Manipulation
T1110: Brute Force	T1049: System Network Connections Discovery		T1113: Screen Capture	T1071.001: Web Protocols		
T1555: Credentials from Password Stores	T1057: Process Discovery		T1114: Email Collection	T1090: Proxy		
	T1082: System Information Discovery		T1115: Clipboard Data	T1095: Non-Application Layer Protocol		
	T1083: File and Directory Discovery		T1125: Video Capture	T1102: Web Service		
	T1087: Account Discovery		T1560: Archive Collected Data	T1102.002: Bidirectional Communication		
	T1135: Network Share Discovery		T1560.002: Archive via Library	T1105: Ingress Tool Transfer		
	T1201: Password Policy Discovery			T1132: Data Encoding		
	T1614: System Location Discovery			T1205: Traffic Signaling		
				T1571: Non-Standard Port		
				T1572: Protocol Tunneling		
				T1573: Encrypted Channel		
				T1573.001: Symmetric Cryptography		

Threat Advisories

https://www.hivepro.com/vulnerability-in-fortinet-allows-authentication-bypass/

https://www.hivepro.com/zero-day-remote-code-execution-vulnerability-in-zimbra-collaboration-suite/

https://www.hivepro.com/polonium-employs-backdoors-to-target-israel/

https://www.hivepro.com/the-surge-of-cryptojacking-campaigns/

https://www.hivepro.com/did-patch-tuesday-address-the-zero-day-flaw-in-microsoft-exchange/

https://www.hivepro.com/earth-aughisky-uses-a-new-set-of-malware/

https://www.hivepro.com/vmware-could-not-fix-a-vulnerability-that-has-been-disclosed-for-eleven-months/

https://www.hivepro.com/google-releases-chrome-106-to-address-vulnerabilities/

https://www.hivepro.com/security-flaws-in-multiple-adobe-products/

https://www.hivepro.com/budworm-attackers-return-with-new-espionage-strikes-against-the-united-states/

https://www.hivepro.com/wip19-targets-it-service-providers-and-telcos-with-custom-malware/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

October 17, 2022 • 3:46 AM

More at www.hivepro.com