Hive Pro

THREAT DIGEST

Fix What Matters to Your Business

Summary of Vulnerabilities & Threats

29 August – 04 September 2022

The last week of August 2022 witnessed the discovery of 390 vulnerabilities out of which 13 gained the attention of Threat Actors and security researchers worldwide. Among these 13, there was one vulnerability that is awaiting reanalysis on the National Vulnerability Database (NVD). Hive Pro Threat Research Team has curated a list of 13 CVEs that require immediate action.

This week also witnessed highly targeted Moisha ransomware outbreaks employing double-extortion techniques. In addition, the RedAlert ransomware dubbed N13V targeted the Chile government's Microsoft and VMware ESXi servers.

Further, we also observed 2 Threat Actor groups being highly active in the last week. First was MuddyWater, an Iranian threat actor group popular for Information theft and espionage, was observed exploiting two Log4j vulnerabilities in SysAid applications to target Israeli organizations. Second was APT 40, a Chinese threat actor group, popular for Information theft and espionage, was spotted deploying phishing campaigns with ScanBox malware against the Australian government. 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
390	13	2	41	18	52

Detailed Report

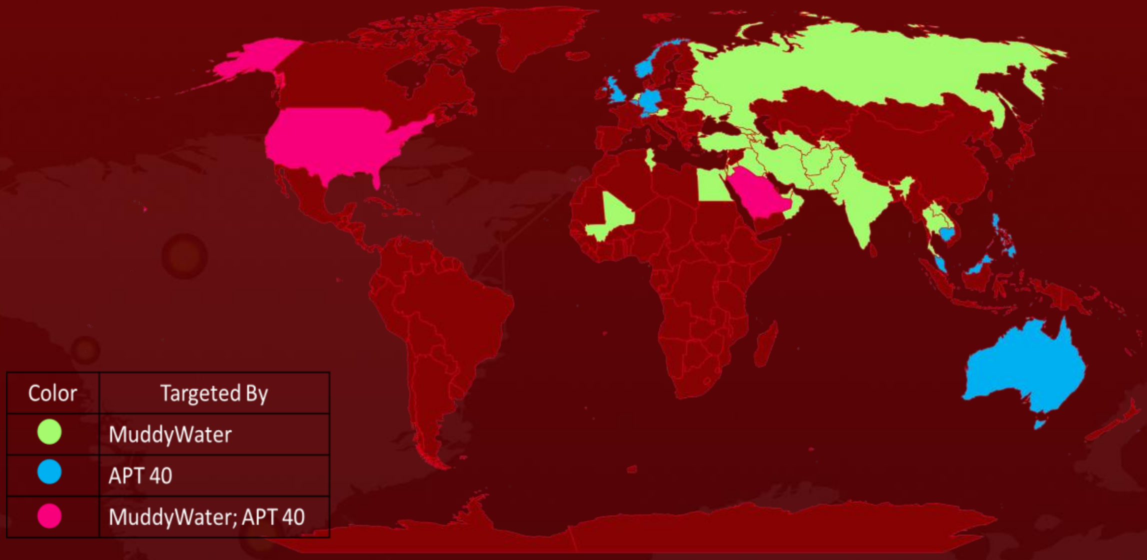
Interesting Vulnerabilities

VENDOR	CVE	PATCH DETAILS
SysAid	CVE-2021-44228 CVE-2021-45046	https://www.sysaid.com/security-compliance/important-update-regarding-apache-log4j https://www.sysaid.com/product/on-premises/latest-release
ATLASSIAN	CVE-2022-36804	https://confluence.atlassian.com/bitbucketserver/bitbucket-server-and-data-center-advisory-2022-08-24-1155489835.html
	CVE-2022-3038 CVE-2022-3039 CVE-2022-3040 CVE-2022-3041 CVE-2022-3042 CVE-2022-3043 CVE-2022-3044 CVE-2022-3045 CVE-2022-3046 CVE-2022-3071	Update Google Chrome to version 105.0.5195.52 Patch Link: https://www.google.com/intl/en/chrome/?standalone=1

Active Actors

ICON	NAME	ORIGIN	MOTIVE
	MuddyWater(Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17)	Iran	Information theft and espionage
	APT 40 (Temp.Periscope, Leviathan, KRYPTONITE PANDA, TEMP.Jumper,BronzeMohawk,Mudcarp ,Gadolinium,ATK29,ITG09)	China	Information theft and espionage

Targeted Locations



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

Targeted Industries

Aerospace

Education

Energy

Financial

Government

Healthcare

Media

NGOs

Technology

Oil & Gas

Transportation

Defence

Manufacturing

Legal

Tele-communications

Research Organizations

Engineering

Food products

Common MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation
T1589: Gather Victim Identity Information	T1588: Obtain Capabilities	T1133: External Remote Services	T1059: Command and Scripting Interpreter	T1133: External Remote Services	T1547: Boot or Logon Autostart Execution
T1598: Phishing for Information	T1588.006: Vulnerabilities	T1190: Exploit Public-Facing Application	T1059.001: PowerShell	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
T1598.003: Spearphishing Link		T1566: Phishing	T1059.003: Windows Command Shell	T1547.001: Registry Run Keys / Startup Folder	T1068: Exploitation for Privilege Escalation
		T1195: Supply Chain Compromise	T1053: Scheduled Task/Job	T1136: Create Account	T1053: Scheduled Task/Job
		T1189: Drive-by Compromise	T1106: Native API	T1136.001: Local Account	T1055: Process Injection
			T1204: User Execution	T1053: Scheduled Task/Job	T1574: Hijack Execution Flow
				T1505: Server Software Component	
				T1574: Hijack Execution Flow	

TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0009: Collection	TA0011: Command and Control	TA0040: Impact
T1027: Obfuscated Files or Information	T1003: OS Credential Dumping	T1083: File and Directory Discovery	T1056: Input Capture	T1071: Application Layer Protocol	T148: Data Encrypted for Impact
T1070: Indicator Removal on Host	T1003.001: LSASS Memory	T1082: System Information Discovery		T1071.001: Web Protocols	T1489: Service Stop
T1574: Hijack Execution Flow	T1056: Input Capture	T1016: System Network Configuration Discovery		T1102: Web Service	T1490: Inhibit System Recovery
T1140: Deobfuscate/DecodeFiles or Information	T1552: Unsecured Credentials	T1049: System Network Connections Discovery		T1095: Non-Application Layer Protocol	
T1027: Obfuscated Files or Information	T1552.001: Credentials In Files	T1518: Software Discovery			
T1036: Masquerading		T1057: Process Discovery			
T1112: Modify Registry		T1046: Network Service Discovery			
		T1012: Query Registry			
		T1120: Peripheral Device Discovery			

Threat Advisories

https://www.hivepro.com/muddywater-targets-israeli-organizations-by-exploiting-unpatched-log4j-vulnerabilities/

https://www.hivepro.com/rce-flaw-resides-in-the-atlassian-bitbucket-server-and-data-center/

https://www.hivepro.com/moisha-ransomware-spotted-launching-highly-targeted-attacks/

https://www.hivepro.com/apt40-deployed-scanbox-malware-to-target-the-australian-government/

https://www.hivepro.com/multiple-vulnerabilities-addressed-by-google-with-chrome-105/

https://www.hivepro.com/chile-governments-windows-and-linux-servers-hit-by-redalert-ransomware/

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

September 5, 2022 • 12:51 AM

More at www.hivepro.com