

Vulnerabilities & Threats that Matter
1-7 August 2022

Summary



The first week of August 2022 witnessed the discovery of 461 vulnerabilities out of which 12 gained the attention of Threat Actors and security researchers worldwide. Among these 12, there was 1 zero-day, and 10 vulnerabilities that is awaiting analysis on the National Vulnerability Database (NVD). Hive Pro Threat Research Team has curated a list of 12 CVEs that require immediate action.

Further, we also observed 1 Threat Actor groups being highly active in the last week. LockBit Gang, an unknown threat actor group popular for financial crime and gain, was observed exploiting vulnerabilities of Windows to perform targeted attacks. 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
461	12	1	60	30	26


Detailed Report

🔧 Interesting Vulnerabilities

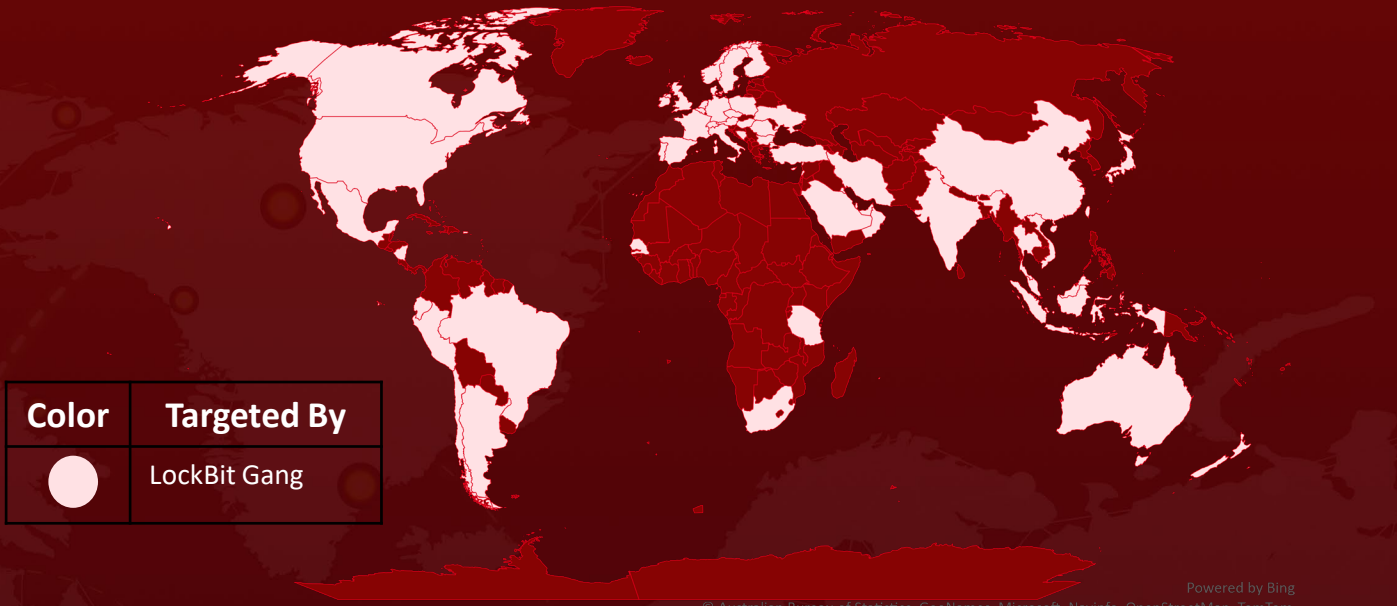
VENDOR	CVE	PATCH LINK
	CVE-2021-44228 CVE-2022-31656 CVE-2022-31658 CVE-2022-31659 CVE-2022-31660 CVE-2022-31661 CVE-2022-31664 CVE-2022-31665 CVE-2022-31657 CVE-2022-31662 CVE-2022-31663	https://www.vmware.com/security/advisories/VMMSA-2021-0028.html https://kb.vmware.com/s/article/89096
	CVE-2022-30190*	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

* zero-day vulnerability

👤 Active Actors

ICON	NAME	ORIGIN	MOTIVE
	LockBit Gang	Unknown	Financial Gain

Targeted Locations



Targeted Industries



Insurance



Engineering



Energy



Family Services



Distributors



Defence



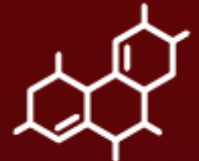
Education



Food products



Real Estate



Biotechnology



Professional Services



Hotels



Media



Manufacturing



Transportation



Marine



Construction



Pharmaceutical



Chemical



Healthcare



Automotive



Retail



Technology



Electrical



Consumers



Metals & Mining



Telecommunications



Aviation



Oil & Gas

Common MITRE ATT&CK TTPs

TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defence Evasion
T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1140: Deobfuscate/Decode Files or Information
T1566: Phishing	T1059.001 : PowerShell	T1574.002: DLL Side-Loading	T1574.002: DLL Side-Loading	T1574: Hijack Execution Flow
	T1106: Native API	T1556: Modify Authentication Process	T1055: Process Injection	T1574.002: DLL Side-Loading
			T1055.012: Process Hollowing	T1553: Subvert Trust Controls
			T1068: Exploitation for Privilege Escalation	T1553.002: Code Signing
				T1556: Modify Authentication Process
				T1055: Process Injection
				T1055.012: Process Hollowing

TA0006: Credential Access	TA0007: Discovery	TA0009: Collection	TA0011: Command and Control
T1056: Input Capture	T1082: System Information Discovery	T1056: Input Capture	T1102: Web Service
T1556: Modify Authentication Process	T1049: System Network Connections Discovery	T1560: Archive Collected Data	T1003: OS Credential Dumping
T1555: Credentials from Password Stores	T1083: File and Directory Discovery		T1105: Ingress Tool Transfer
T1555.003: Credentials from Web Browsers	T1057: Process Discovery		T1573: Encrypted Channel

Threat Advisories

<https://www.hivepro.com/woody-rat-leverages-follina-to-target-russia/>

<https://www.hivepro.com/manjusaka-cybercriminals-new-attack-framework-weapon/>

<https://www.hivepro.com/vmware-products-impacted-by-an-authentication-bypass-vulnerability-and-other-flaws/>

<https://www.hivepro.com/lockbit-3-0-makes-a-comeback-by-exploiting-log4j/>

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a 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

August 8, 2022 • 2:36 AM

© 2022 All Rights are Reserved by HivePro



More at www.hivepro.com