Hive Pro

THREAT DIGEST

Weekly Threat Digest: 16-22 May 2022

Date of Publication

25 May 2022

Summary

The third week of May 2022 witnessed the discovery of 466 vulnerabilities out of which 6 gained the attention of Threat Actors and security researchers worldwide. Among these 6, there were 2 zero-day and 2 vulnerabilities about which the National vulnerability Database (NVD) is awaiting analysis while one of them was not present in the NVD at all. Hive Pro Threat Research Team has curated a list of 6 CVEs that require immediate action.

Further, we also observed two Threat Actor groups being highly active in the last week. Lazarus, a North Korean threat actor group popular for Information theft and espionage, was observed targeting Korea with NukeSped backdoor. Additionally, a new ransomware family Axxes, was observed targeting the H Hotel, Dubai. 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
466	6	2	26	10	27

Detailed Report

Interesting Vulnerabilities

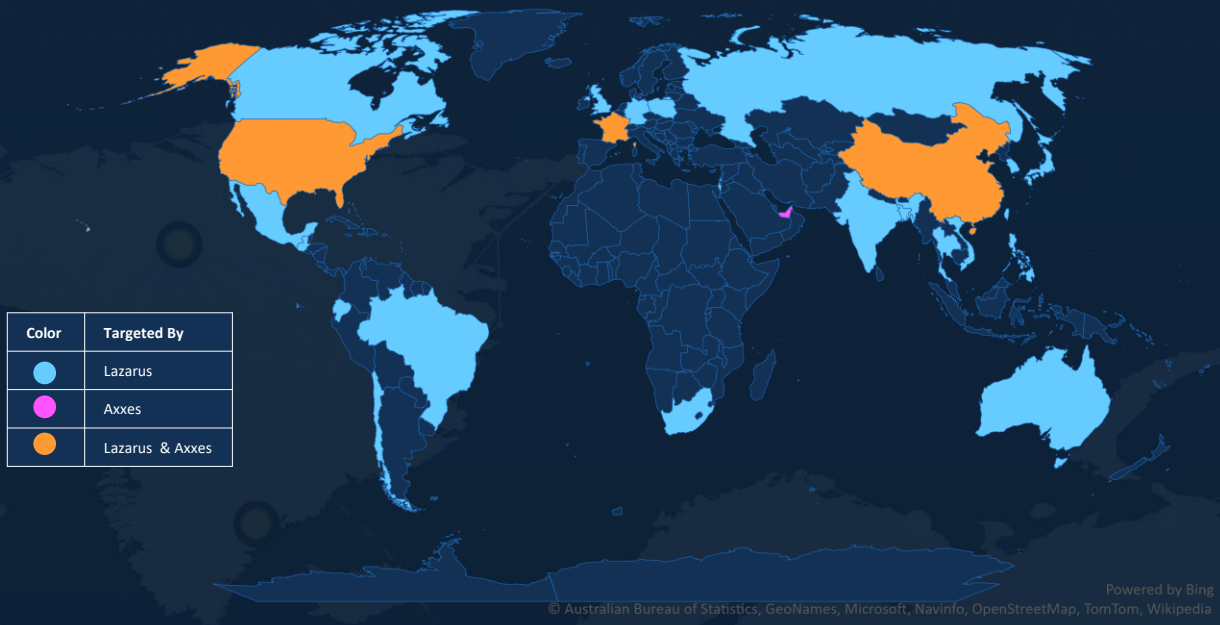
VENDOR	CVE	PATCH LINK
vmware	CVE-2021-44228* CVE-2022-22954 CVE-2022-22960 CVE-2022-22972 CVE-2022-22973	https://www.vmware.com/security/advisories/VMSA-2021-0028.html https://www.vmware.com/security/advisories/VMSA-2022-0011.html https://www.vmware.com/security/advisories/VMSA-2022-0014.html
	CVE-2022-1096*	https://www.google.com/intl/en/chrome/?standalone=1

* zero-day vulnerability

Active Actors

ICON	NAME	ORIGIN	MOTIVE
	Axxes Ransomware Group	Unknown	Financial Gain
	Lazarus Group (Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03)	North Korea	Information theft and espionage, Sabotage and destruction, Financial crime

Targeted Locations



Targeted Industries

Common MITRE ATT&CK TTPs

TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1587: Develop Capabilities	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1548: Abuse Elevation Control Mechanism	T1548: Abuse Elevation Control Mechanism
T1587.003: Digital Certificates	T1566: Phishing	T1059.001: PowerShell	T1547.001: Registry Run Keys / Startup Folder	T1547: Boot or Logon Autostart Execution	T1140: Deobfuscate/ Decode Files or Information
T1587.001: Malware	T1566.001: Spearphishing Attachment	T1203: Exploitation for Client Execution	T1543: Create or Modify System Process	T1547.001: Registry Run Keys / Startup Folder	T1036: Masquerading
T1588: Obtain Capabilities		T1204: User Execution	T1543.003: Windows Service	T1543: Create or Modify System Process	T1036.005: Match Legitimate Name or Location
T1588.005: Exploits		T1204.002: Malicious File		T1543.003: Windows Service	T1112: Modify Registry
T1588.006: Vulnerabilities					T1027: Obfuscated Files or Information
					T1221: Template Injection

TA0006: Credential Access	TA0007: Discovery	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1056: Input Capture	T1083: File and Directory Discovery	T1560: Archive Collected Data	T1573: Encrypted Channel	T1048: Exfiltration Over Alternative Protocol	T1486: Data Encrypted for Impact
T1056.001: Keylogging		T1005: Data from Local System	T1573.001: Symmetric Cryptography		
		T1056: Input Capture	T1105: Ingress Tool Transfer		
		T1056.001: Keylogging			
		T1113: Screen Capture			

Threat Advisories

https://www.hivepro.com/vulnerabilities-in-vmware-when-chained-together-grants-full-system-control/

https://www.hivepro.com/google-chromes-second-zero-day-in-2022/

https://www.hivepro.com/new-ransomware-group-axxes-is-on-the-rise/

https://www.hivepro.com/lazarus-distributes-nukesped-to-vmware-horizon-servers-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

25 May 2022 • 5:00 PM

More at www.hivepro.com