Hive Pro

THREAT DIGEST

Vulnerabilities & Threats that Matter
25 - 31 July 2022

Summary

The Last week of July 2022 witnessed the discovery of 462 vulnerabilities out of which 7 gained the attention of Threat Actors and security researchers worldwide. Among these 7, 2 of them were zero-days, there was 1 vulnerability that is awaiting analysis on the National Vulnerability Database (NVD). Hive Pro Threat Research Team has curated a list of 7 CVEs that require immediate action.

Further, we also observed 4 Threat Actor groups being highly active in the last week. APT29, a Russian threat actor group popular for Information theft and espionage was seen launching phishing campaigns to launch malware via cloud storage services, EvilNum an unknown threat actor group popular for Information theft and espionage was seen targeting Decentralized Finance (DeFi) sector, APT37 a North Korean threat actor group popular for Information theft and espionage was seen launching attack campaigns using Konni RAT and KNOTWEED an Austrian threat actor group popular for financial crime and gain, was observed exploiting 0-day vulnerabilities of Windows and Adobe to perform targeted attacks against European and Central American customers. 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
462	7	4	52	22	64

Detailed Report

Interesting Vulnerabilities

VENDOR	CVE	PATCH DETAILS
APACHE	CVE-2022-33891	https://spark.apache.org/downloads.html
	CVE-2022-2294*	https://www.google.com/intl/en/chrome/?standalone=1 Update to Google Chrome version 103.0.5060.114 for Windows, MacOS, and Linux.
Microsoft	CVE-2022-22047* CVE-2021-31199 CVE-2021-31201 CVE-2021-36948	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22047 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31201 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31199 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36948
Adobe	CVE-2021-28550	https://helpx.adobe.com/security/products/acrobat/apsb21-29.html

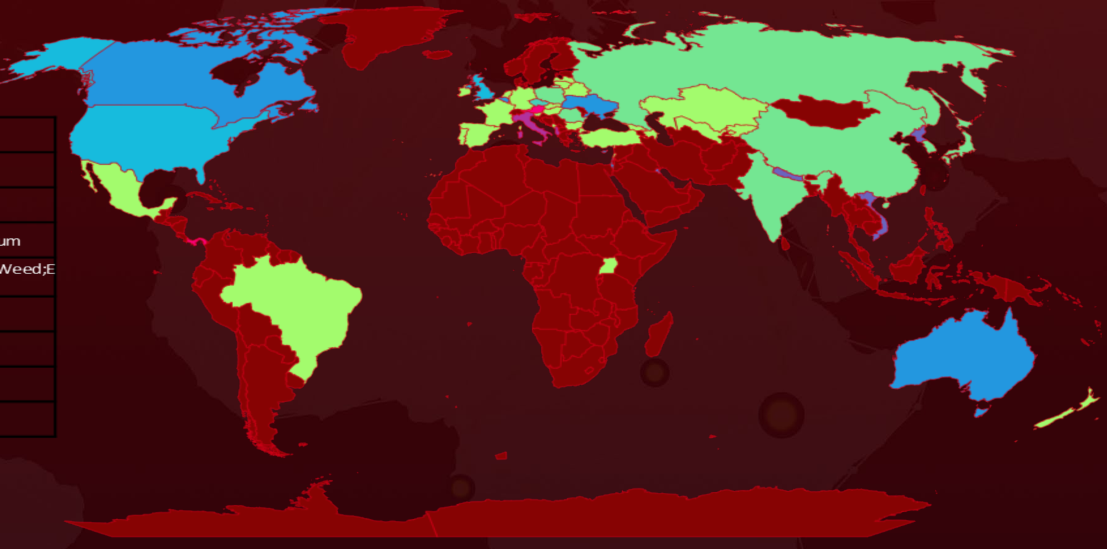
* zero-day vulnerability

Active Actors

ICON	NAME	ORIGIN	MOTIVE
	APT 29(CozyBear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, Nobelium, Iron Ritual , Cloaked Ursa)	Russia	Information theft and espionage
	Evilnum(Jointworm, Knockout Spider, TA4563, DeathStalker)	Unknown	Information theft and espionage
	APT 37(Reaper, TEMP.Reaper, Ricochet Chollima, ScarCruft, Thallium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10)	North Korea	Information theft and espionage
	KNOTWEED	Austria	Financial Gain

Targeted Locations

Color	Targeted By
●	APT29
●	APT29;APT37
●	APT29;APT37;Evilnum
●	APT29;APT37;KnotWeed;Evilnum
●	APT29;Evilnum
●	APT37
●	Evilnum
●	KnotWeed



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

Targeted Industries

Defence

Government

Legal

Media

NGOs

Pharmaceutical

Tele-communications

Think-Tanks

Transportation

Financial

Automotive

Chemical

Healthcare

Education

Manufacturing

Technology

Energy

Aerospace

Strategic Consultancies

Retail

Engineering

Common MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0004: Privilege Escalation	TA0005: Defence Evasion
T1589: Gather Victim Identity Information	T1588: Obtain Capabilities	T1566: Phishing	T1059: Command and Scripting Interpreter	T1547: Boot or Logon AutostartExecution	T1547: Boot or Logon AutostartExecution	T1548: Abuse Elevation Control Mechanism	T1574: Hijack Execution Flow
T1592: Gather Victim Host Information	T1588.002: Tool	T1566.001: SpearphishingAttachment	T1059.001: PowerShell	T1547.001: Registry Run Keys / Startup Folder	T1547.001: Registry Run Keys / Startup Folder	T1548.002: Bypass User Account Control	T1574.002: DLL Side-Loading
		T1190: Exploit Public-Facing Application	T1059.003: Windows Command Shell	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1068: Exploitation for Privilege Escalation	T1140: Deobfuscate/DecodeFiles or Information
			T1059.005: Visual Basic	T1574.002: DLL Side-Loading	T1574.002: DLL Side-Loading	T1546: Event Triggered Execution	T1553: Subvert Trust Controls
			T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1055: Process Injection		T1553.005: Mark-of-the-Web Bypass
			T1053.005: Scheduled Task	T1053.005: Scheduled Task	T1053: Scheduled Task/Job		T1027: Obfuscated Files or Information
			T1569: System Services	T1543: Create or Modify System Process	T1053.005: Scheduled Task		T1027.005: Indicator Removal from Tools
			T1569.002: Service Execution	T1543.003: Windows Service	T1543: Create or Modify System Process		T1564.001: Hidden Files and Directories
			T1204: User Execution	T1068: Exploitation for Privilege Escalation	T1543.003: Windows Service		T1070: Indicator Removal on Host
			T1204.002: Malicious File	T1546: Event Triggered Execution	T1134: Access Token Manipulation		T1070.004: File Deletion
			T1203: Exploitation for Client Execution		T1134.001: Token Impersonation/Theft		T1055: Process Injection

TA0005: Defence Evasion	TA0006: Credential Access	TA0007: Discovery	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1014: Rootkit	T1555: Credentials from Password Stores	T1082: System Information Discovery	T1560: Archive Collected Data	T1071: Application Layer Protocol	T1567:Exfiltration Over Web Service	T1486: Data Encrypted for Impact
T1134: Access Token Manipulation	T1555.003: Credentials from Web Browsers	T1016: System Network Configuration Discovery		T1102: Web Service	T1567.002: Exfiltration to Cloud Storage	T1489: Service Stop
T1134.001: Token Impersonation/Theft	T1606: Forge Web Credentials	T1057: Process Discovery		T1105: Ingress Tool Transfer		T1490: Inhibit System Recovery
T1202: Indirect Command Execution	T1606.001: Web Cookies	T1012: Query Registry				
T1564: Hide Artifacts	T1539: Steal Web Session Cookie	T1083: File and Directory Discovery				
T1548: Abuse Elevation Control Mechanism		T1007: System Service Discovery				
T1548.002: Bypass User Account Control		T1033: System Owner/User Discovery				
T1550:Use Alternate Authentication Material		T1518: Software Discovery				

Threat Advisories

https://www.hivepro.com/knotweed-exploits-zero-days-to-target-us-and-europe/

https://www.hivepro.com/apt37-employs-konni-malware-to-target-high-level-organizations/

https://www.hivepro.com/evilnum-strikes-commodities-and-cryptocurrency-forum/

https://www.hivepro.com/spyware-group-candiru-exploits-chrome-zero-day-to-target-middle-east/

https://www.hivepro.com/shell-command-injection-vulnerability-found-in-apache-spark/

https://www.hivepro.com/revamped-version-of-redeemer-ransomware-has-been-uncovered-on-dark-web-forums/

https://www.hivepro.com/apt29-utilizes-cloud-storage-service-to-deliver-malicious-payloads/

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 1, 2022 • 2:29 AM

More at www.hivepro.com