

Fix What Matters to Your Business

Summary of Vulnerabilities & Threats

22-28 August 2022

The fourth week of August 2022 witnessed the discovery of 604 vulnerabilities out of which one gained the attention of Threat Actors and security researchers worldwide. Among these two, there was one vulnerability that is awaiting analysis on the National Vulnerability Database (NVD). The Hive Pro Threat Research Team has curated a list of two CVEs that require immediate action.



This week also saw an upsurge in the use of the BianLian ransomware, which targeted the manufacturing, education, healthcare, and finance industries. In addition to this, there was a spike in the employment of the Grandoreiro banking trojan, which conducted phishing operations, and the DarkTortilla crypter, which distributes remote access trojans (RATs).

Further, we also observed 3 Threat Actor groups being highly active in the last week. First was CHARMING KITTEN, an Iranian threat actor group popular for Information theft and espionage, was observed employing a new data extraction tool HYPERSCAP. Second was Karakurt, an unknown threat actor group, popular for financial crime and witnessed increased attacks with an impact on the public health sectors. Third was Kimsuky, a North Korean threat actor group, popular for information theft and espionage and it was observed running phishing campaigns. 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
604	2	3	68	18	54

Detailed Report

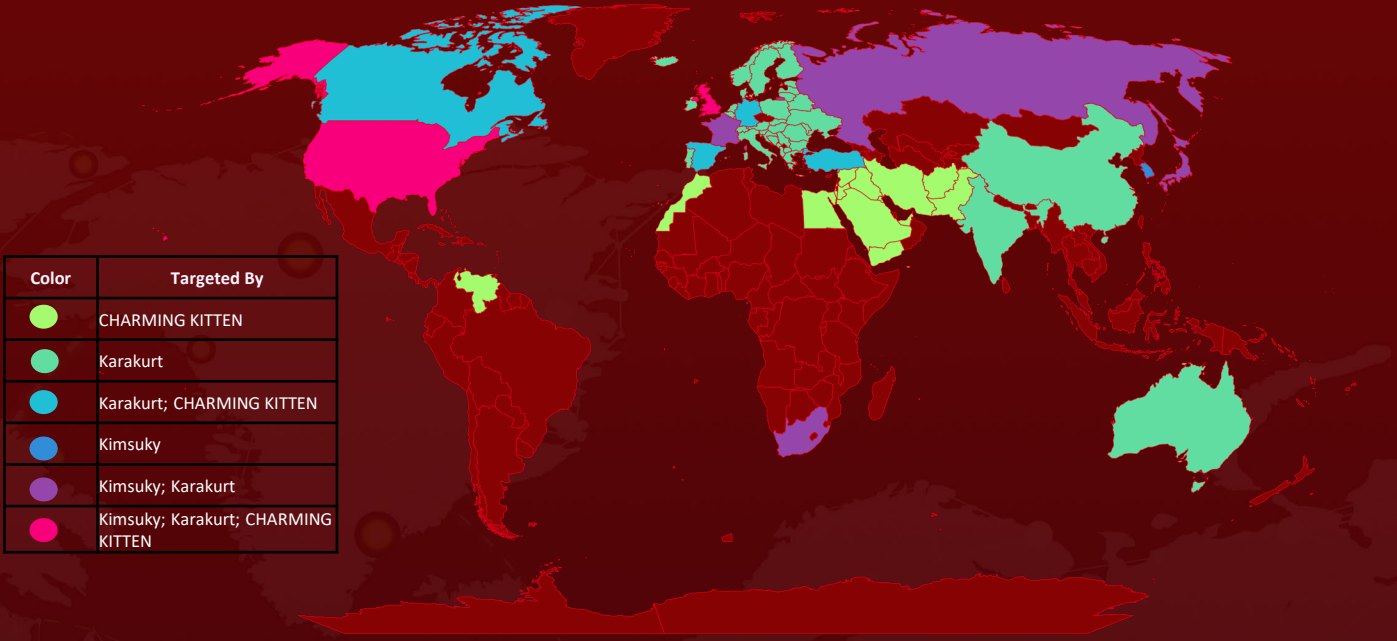
🔧 Interesting Vulnerabilities

VENDOR	CVE	PATCH DETAILS
 paloalto NETWORKS	CVE-2022-0028	Upgrade to Palo Alto PAN-OS versions above 10.2.2-h2, 10.1.6-h6, 10.0.11-h1, 9.1.14-h4, 9.0.16-h3, 8.1.23-h1
 GitLab	CVE-2022-2884	Update GitLab Community Edition and Enterprise Edition versions 15.3.1, 15.2.3, and 15.1.5 to address the issue

👤 Active Actors

ICON	NAME	ORIGIN	MOTIVE
	CHARMING KITTEN(Newscaster, Parastoo, APT35, Phosphorus, Magic Hound, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, TarhAndishan,TA453, TunnelVision,UNC788)	Iran	Information theft and espionage
	Karakurt	Unknown	Financial gain
	Kimsuky(Velvet Chollima, Thallium, Cerium, Black Banshee, ITG16, TA406)	North Korea	Information theft and espionage

Targeted Locations



Color	Targeted By
Light Green	CHARMING KITTEN
Green	Karakurt
Cyan	Karakurt; CHARMING KITTEN
Blue	Kimsuky
Purple	Kimsuky; Karakurt
Pink	Kimsuky; Karakurt; CHARMING KITTEN

Targeted Industries

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

 Aerospace	 Education	 Energy	 Financial	 Government	 Healthcare
 Media	 NGOs	 Technology	 Oil & Gas	 Pharmaceutical	 Defence
 Manufacturing	 Retail	 Tele-communications	 Insurance	 Entertainment	 Cryptocurrency

Common MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1589: Gather Victim Identity Information	T1588: Obtain Capabilities	T1091: Replication Through Removable Media	T1204: User Execution	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1127: Trusted Developer Utilities Proxy Execution
T1589.001: Credentials	T1586: Compromise Accounts	T1566 : Phishing	T1204.002: Malicious File	T1078: Valid Accounts	T1055: Process Injection	T1078: Valid Accounts
T1589.002: Email Addresses	T1586.002: Email Accounts	T1566.001: Spearphishing Attachment	T1059: Command and Scripting Interpreter	T1574: Hijack Execution Flow	T1078: Valid Accounts	T1055: Process Injection
		T1190: Exploit Public-Facing Application	T1059.005: Visual Basic	T1133: External Remote Services	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow
		T1078: Valid Accounts	T1569: System Services			T1070: Indicator Removal on Host
		T1133: External Remote Services				T1218: System Binary Proxy Execution
						T1497: Virtualization/Sandbox Evasion
						T1027: Obfuscated Files or Information
						T1027.002: Software Packing
						T1036: Masquerading
						T1140: Deobfuscate/Decode Files or Information
						T1562: Impair Defenses
						T1553 : Subvert Trust Controls

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0010: Exfiltration	TA0011: Command and Control	TA0040: Impact
T1056: Input Capture	T1497: Virtualization/Sandbox Evasion	T1091: Replication Through Removable Media	T1113: Screen Capture	T1020: Automated Exfiltration	T1105: Ingress Tool Transfer	T1486: Data Encrypted for Impact
	T1082: System Information Discovery	T1210: Exploitation of Remote Services	T1560: Archive Collected Data	T1048: Exfiltration Over Alternative Protocol	T1102: Web Service	T1498: Network Denial of Service
	T1083: File and Directory Discovery		T1560.001: Archive via Utility	T1567: Exfiltration Over Web Service	T1219: Remote Access Software	T1498.002: Reflection Amplification
	T1518: Software Discovery		T1114: Email Collection	T1567.002: Exfiltration to Cloud Storage	T1104: Multi-Stage Channels	
	T1518.001: Security Software Discovery		T1115: Clipboard Data			
	T1120: Peripheral Device Discovery		T1056: Input Capture			
	T1057: Process Discovery					

Threat Advisories

<https://www.hivepro.com/multiple-industries-targeted-by-uptick-of-bianlian-ransomware/>

<https://www.hivepro.com/denial-of-service-vulnerability-in-pan-os-exploited-in-the-wild/>

<https://www.hivepro.com/grandoreiro-banking-trojan-attacks-industries-in-spanish-speaking-countries/>

<https://www.hivepro.com/input-validation-flaw-in-gitlabs-community-and-enterprise-software/>

<https://www.hivepro.com/iranian-aps-new-data-extraction-tool-hyperscrape/>

<https://www.hivepro.com/darktortilla-crypter-is-set-to-become-a-formidable-threat/>

<https://www.hivepro.com/healthcare-industry-tore-down-by-karakurt-ransomware-group/>

<https://www.hivepro.com/kimsuky-targets-south-korean-entities-with-phishing-campaign/>

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

August 29 2022 • 12:43 AM

© 2022 All Rights are Reserved by HivePro



More at www.hivepro.com