Hive Pro

THREAT DIGEST

Vulnerabilities & Threats that Matter
11-17 July 2022

Summary

The second week of July 2022 witnessed the discovery of 580 vulnerabilities out of which 37 gained the attention of Threat Actors and security researchers worldwide. Among these 37, there was 1 zero-day, and 2 vulnerabilities that were awaiting analysis on the National Vulnerability Database (NVD). Hive Pro Threat Research Team has curated a list of 37 CVEs that require immediate action.

Further, we also observed 2 Threat Actor groups being highly active in the last week. BlackCat alias ALPHV, an unknown threat actor group popular for financial crime and gain, was observed targeting organizations all around the world using quadruple extortion techniques and Transparent Tribe, an APT group popular for Information theft and espionage was seen launching phishing campaigns to target education sector. 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
580	37	2	World-wide	11	61

Detailed Report

Interesting Vulnerabilities

VENDOR	CVE	PATCH LINK
node JS	CVE-2022-32213 CVE-2022-32214 CVE-2022-32215 CVE-2022-32212 CVE-2022-32223 CVE-2022-32222 CVE-2022-2097	https://nodejs.org/en/blog/release/v14.20.0/ https://nodejs.org/en/blog/release/v16.16.0/ https://nodejs.org/en/blog/release/v18.5.0/
Microsoft	CVE-2022-22047* CVE-2022-22026 CVE-2022-22049 CVE-2022-30216 CVE-2022-22038 CVE-2022-30221 CVE-2022-30222 CVE-2022-22022 CVE-2022-22041 CVE-2022-30206 CVE-2022-30226 CVE-2022-22029 CVE-2022-33678 CVE-2022-33676 CVE-2022-33677	https://support.microsoft.com/en-us/topic/installation-updates-2f9c1819-310d-48a7-ac12-25191269903c#WindowsVersion=Windows_11
	CVE-2022-26706	https://support.apple.com/en-us/HT213256 https://support.apple.com/en-us/HT213257

* zero-day vulnerability

Detailed Report

Interesting Vulnerabilities

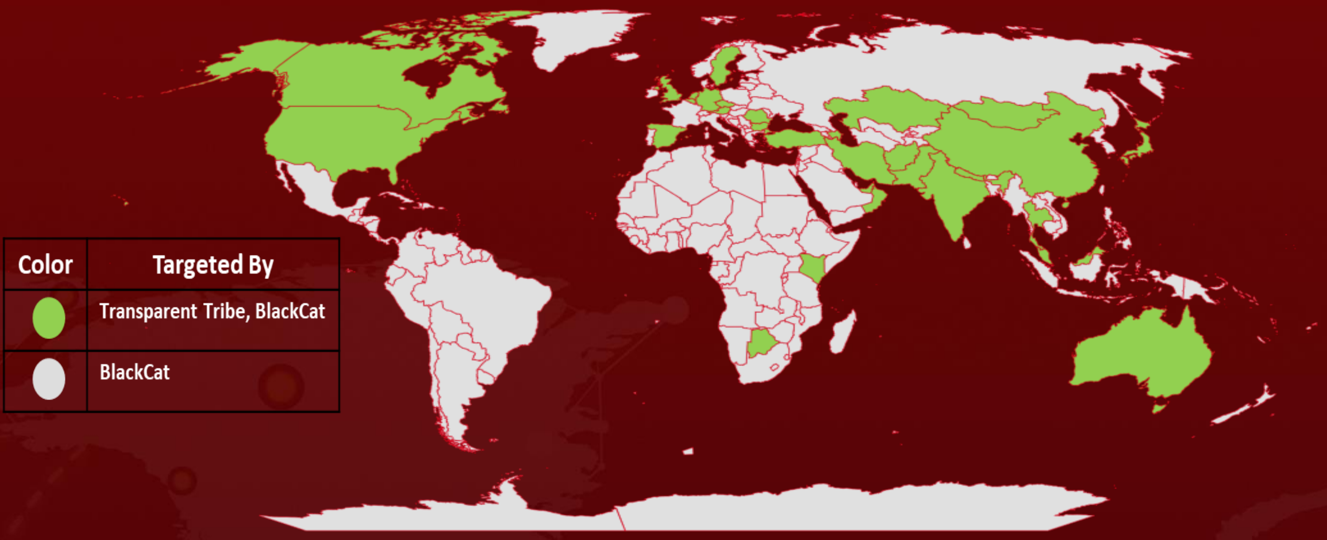
VENDOR	CVE	PATCH LINK
Adobe	CVE-2022-34230 CVE-2022-34229 CVE-2022-34228 CVE-2022-34227 CVE-2022-34226 CVE-2022-34224 CVE-2022-34223 CVE-2022-34222 CVE-2022-34221 CVE-2022-34220 CVE-2022-34219 CVE-2022-34217 CVE-2022-34216 CVE-2022-34215	https://get.adobe.com/reader

* zero-day vulnerability

Active Actors

ICON	NAME	ORIGIN	MOTIVE
🤖	BlackCat aka ALPHV	Unknown	Financial Gain
🤖	Transparent Tribe(APT36, Mythic Leopard)	Pakistan	Information theft and espionage

Targeted Locations



Color	Targeted By
🟢	Transparent Tribe, BlackCat
⚪	BlackCat

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

Targeted Industries

Insurance

Research Organizations

Tele-communications

Government

Education

Embassies

Defence

Manufacturing

Engineering

Construction

Transportation

Common MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation
T1592: Gather Victim Host Information	T1586: Compromise Accounts	T1133: External Remote Services	T1053: Scheduled Task/Job	T1098: Account Manipulation	T1484: Domain Policy Modification
T1590: Gather Victim Network Information	T1583.002: Acquire Infrastructure: DNS Server	T1190: Exploit Public-Facing Application	T1072: Software Deployment Tools	T1574.001: Hijack Execution Flow: DLL Search Order Hijacking	T1574.001: Hijack Execution Flow: DLL Search Order Hijacking
	T1583.001: Acquire Infrastructure: Domains	T1091: Replication Through Removable Media	T1059.003: Command and Scripting Interpreter: Windows Command Shell	T1574.002: Hijack Execution Flow: DLL Side-Loading	T1574.002: Hijack Execution Flow: DLL Side-Loading
	T1584.001: Compromise Infrastructure: Domains	T1189: Drive-by Compromise	T1059: Command and Scripting Interpreter	T1543: Create or Modify System Process	T1574: Hijack Execution Flow
	T1608.004: Stage Capabilities: Drive-by Target	T1566.001: Phishing: Spearphishing Attachment	T1203: Exploitation for Client Execution	T1133: External Remote Services	T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control
		T1566.002: Phishing: Spearphishing Link	T1204: User Execution	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job
		T1133: External Remote Services	T1059.005: Command and Scripting Interpreter: Visual Basic	T1574: Hijack Execution Flow	T1543: Create or Modify System Process
		T1078: Valid Accounts	T1203: Exploitation for Client Execution	T1078: Valid Accounts	T1078: Valid Accounts
			T1204.001: User Execution: Malicious Link		T1055: Process Injection
			T1204.002: User Execution: Malicious File		

TA0005: Defense Evasion	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0011: Command and Control
T1078: Valid Accounts	T1027: Obfuscated Files or Information	T1003: OS Credential Dumping	T1040: Network Sniffing	T1091: Replication Through Removable Media	T1071.001: Application Layer Protocol: Web Protocols
T1222: File and Directory Permissions Modification	T1574.001: Hijack Execution Flow: DLL Search Order Hijacking	T1528: Steal Application Access Token	T1482: Domain Trust Discovery	T1072: Software Deployment Tools	T1568: Dynamic Resolution
T1036: Masquerading	T1574.002: Hijack Execution Flow: DLL Side-Loading	T1558: Steal or Forge Kerberos Tickets	T1083: File and Directory Discovery		
T1027: Obfuscated Files or Information	T1484: Domain Policy Modification	T1212: Exploitation for Credential Access	T1615: Group Policy Discovery		
T1497: Virtualization/Sandbox Evasion	T1574: Hijack Execution Flow	T1555: Credentials from Password Stores	T1518: Software Discovery		
T1218.008: System Binary Proxy Execution: Odbcconf	T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control	T1040: Network Sniffing	T1497: Virtualization/Sandbox Evasion		
T1218.011: System Binary Proxy Execution: Rundll32	T1112: Modify Registry				
T1218.007: System Binary Proxy Execution: Msiexec	T1564.001: Hide Artifacts: Hidden Files and Directories				
T1055: Process Injection	T1036.005: Masquerading: Match Legitimate Name or Location				

TA0010: Exfiltration	TA0040: Impact
T1020: Automated Exfiltration	T1490: Inhibit System Recovery
T1048: Exfiltration Over Alternative Protocol	T1486: Data Encrypted for Impact
T1537: Transfer Data to Cloud Account	
T1041: Exfiltration Over C2 Channel	

Threat Advisories

https://www.hivepro.com/transparent-tribes-latest-campaign-targets-the-education-sector/

https://www.hivepro.com/microsoft-uncovers-a-macos-app-sandbox-escape-vulnerability/

https://www.hivepro.com/raspberry-robin-worm-infects-multiple-windows-network-devices/

https://www.hivepro.com/adobe-addresses- new-vulnerabilities-in-adobe-acrobat-and-reader/

https://www.hivepro.com/havanacrypt-ransomware-spreads-through-fake-google-updates/

https://www.hivepro.com/microsoft-releases-updates-for-exploited-zero-day-and-other-vulnerabilities-resulting-in-rce/

https://www.hivepro.com/havanacrypt-ransomware-spreads-through-fake-google-updates/

https://www.hivepro.com/several-bugs-in-node-js-lead-to-remote-code-execution/

https://www.hivepro.com/blackcat-ransomware-group-implements-quadruple-extortion/

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

July 19, 2022 • 2:47 AM

More at www.hivepro.com