Hive Pro

Weekly Threat Digest: 21-27 February 2022

Overview:

The last week of February 2022 witnessed 2 highly exploited vulnerabilities which were published by National Vulnerability Database (NVD) on 13th January 2022. These vulnerabilities came into highlight after Cybersecurity and Infrastructure Security Agency (CISA) added them to the known exploited vulnerabilities catalog.

The Hive Pro Threat Research team has also spotted two Threat Actor groups that have been extremely active in the last week. APT10, a well-known Chinese threat actor group famously known for information theft and espionage, has been detected targeting 28 different countries with the latest attack on Taiwanese financial institutions. Furthermore, a highly complex and innovative ransomware group known as UNC2596 targeted 50+ companies in 11 different countries. 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
350	2	2	17	18	79

Detailed Report:

Interesting Vulnerabilities:

Vendor	CVEs	Patch Link
ZABBIX	CVE-2022-23131 CVE-2022-23134	https://support.zabbix.com/browse/ZBX-20384 https://support.zabbix.com/browse/ZBX-20350

Active Actor:

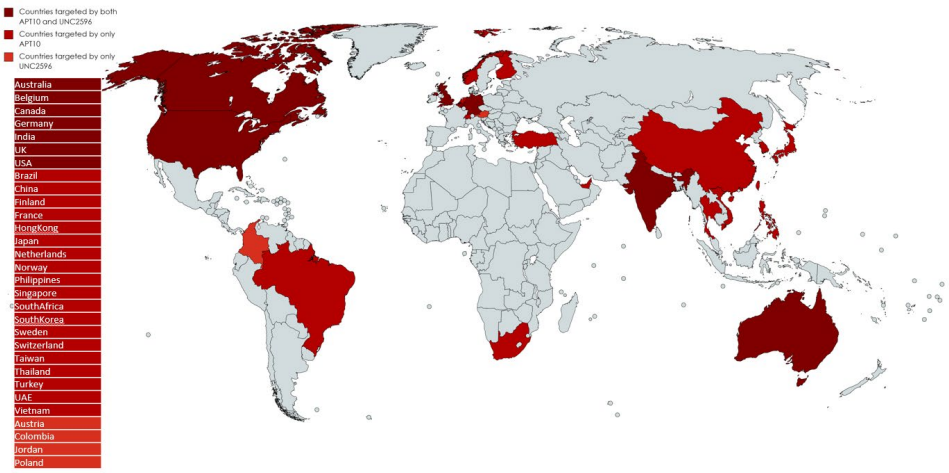
Icon	Name	Origin	Motive
	APT10 (Stone Panda, APT 10, menuPass, Red Apollo, CVNX, Potassium, Hogfish, Happyyongzi, Cicada, Bronze Riverside, CTG-5938, ATK 41, TA429, ITG01)	China	Information theft and espionage
	UNC2596	Unknown	ecrime

* Zero-day vulnerability

Hive Pro

Weekly Threat Digest: 21-27 February 2022

Targeted Locations:



Targeted Sectors:

Common TTPs:

TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1583: Acquire Infrastructure	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1140: Deobfuscate/Decode Files or Information
T1583.001: Domains	T1566: Phishing	T1059.001: PowerShell	T1574.001: DLL Search Order Hijacking	T1574.001: DLL Search Order Hijacking	T1574: Hijack Execution Flow
T1583.003: Virtual Private Server	T1566.001: Spearphishing Attachment	T1059.003: Windows Command Shell	T1574.002: DLL Side-Loading	T1574.002: DLL Side-Loading	T1574.001: DLL Search Order Hijacking
T1588: Obtain Capabilities	T1199: Trusted Relationship	T1106: Native API	T1574.011: Services Registry Permissions Weakness	T1574.011: Services Registry Permissions Weakness	T1574.002: DLL Side-Loading
T1588.002: Tool	T1078: Valid Accounts	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1055: Process Injection	T1574.011: Services Registry Permissions Weakness
T1588.003: Code Signing Certificates		T1053.005: Scheduled Task	T1053.005: Scheduled Task	T1055.003: Thread Execution Hijacking	T1070: Indicator Removal on Host
T1608: Stage Capabilities		T1204: User Execution	T1078: Valid Accounts	T1055.012: Process Hollowing	T1070.003: Clear Command History
T1608.001: Upload Malware		T1204.002: Malicious File	T1098: Account Manipulation	T1053: Scheduled Task/Job	T1070.004: File Deletion
T1608.002: Upload Tool		T1047: Windows Management Instrumentation	T1136: Create Account	T1053.005: Scheduled Task	T1036: Masquerading
T1608.003: Install Digital Certificate		T1129: Shared Modules	T1136.001: Local Account	T1078: Valid Accounts	T1036.005: Match Legitimate Name or Location
T1608.005: Link Target		T1569: System Services	T1543: Create or Modify System Process	T1068: Exploitation for Privilege Escalation	T1036.003: Rename System Utilities
T1587: Develop Capabilities		T1569.002: Service Execution	T1543.003: Windows Service	T1134: Access Token Manipulation	T1027: Obfuscated Files or Information
T1587.003: Digital Certificates			T1505: Server Software Component	T1134.001: Token Impersonation/Theft	T1055: Process Injection
			T1505.003: Web Shell		T1055.003: Thread Execution Hijacking
					T1055.012: Process Hollowing
					T1218: Signed Binary Proxy Execution
					T1218.004: InstallUtil
					T1553: Subvert Trust Controls
					T1553.002: Code Signing
					T1078: Valid Accounts
					T1112: Modify Registry
					T1134: Access Token Manipulation
					T1134.001: Token Impersonation/Theft
					T1497: Virtualization/Sandbox Evasion
					T1497.001: System Checks
					T1564: Hide Artifacts
					T1564.003: Hidden Window
					T1620: Reflective Code Loading
					T1480: Execution Guardrails
					T1562: Impair Defenses
					T1562.001: Disable or Modify Tools

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0040: Impact
T1056: Input Capture	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1560: Archive Collected Data	T1568: Dynamic Resolution	T1486: Data Encrypted for Impact
T1056.001: Keylogging	T1087.002: Domain Account	T1021: Remote Services	T1560.001: Archive via Utility	T1568.001: Fast Flux DNS	T1489: Service Stop
T1003: OS Credential Dumping	T1083: File and Directory Discovery	T1021.001: Remote Desktop Protocol	T1119: Automated Collection	T1105: Ingress Tool Transfer	
T1003.004: LSA Secrets	T1046: Network Service Scanning	T1021.004: SSH	T1005: Data from Local System	T1090: Proxy	
T1003.003: NTDS	T1018: Remote System Discovery		T1039: Data from Network Shared Drive	T1090.002: External Proxy	
T1003.002: Security Account Manager	T1016: System Network Configuration Discovery		T1074: Data Staged	T1071: Application Layer Protocol	
T1555: Credentials from Password Stores	T1049: System Network Connections Discovery		T1074.001: Local Data Staging	T1071.001: Web Protocols	
T1555.003: Credentials from Web Browsers	T1010: Application Window Discovery		T1074.002: Remote Data Staging	T1071.004: DNS	
	T1012: Query Registry		T1056: Input Capture	T1095: Non-Application Layer Protocol	
	T1033: System Owner/User Discovery		T1056.001: Keylogging	T1573: Encrypted Channel	
	T1057: Process Discovery			T1573.002: Asymmetric Cryptography	
	T1082: System Information Discovery				
	T1497: Virtualization/Sandbox Evasion				
	T1497.001: System Checks				
	T1518: Software Discovery				
	T1518.001: Security Software Discovery				

Weekly Threat Digest: 21-27 February 2022

Threat Advisories:

https://www.hivepro.com/chinese-apt-group-targets-financial-institutions-in-the-campaign-operation-cache-panda/

https://www.hivepro.com/zabbix-affected-by-two-actively-exploited-vulnerabilities/