Hive Pro

Weekly Threat Digest: 28 March - 3 April 2022

Overview:

The fourth week of March 2022 witnessed the discovery of 500 vulnerabilities out of which 7 gained the attention of Threat Actors and security researchers worldwide. Among these 10, there were 3 awaiting analysis and 2 were not present in the NVD at all. Hive Pro Threat Research Team has curated a list of 7 CVEs that require immediate action.

Furthermore, we also observed three threat actor groups being highly active in the last week. A financially motivated threat actor called TA551 primarily targeted English, German, Italian, and Japanese speakers through IcedID an email-based malware. A new variant of the famous PlugX malware called Talisman has been discovered to be used by Chinese state-sponsored threat actor RedFoxtrot. These attacks were staged on telecommunication and defense sectors in South Asian countries to protect the Belt and Road initiative. Deep Panda aka APT 19, a Chinese APT group, exploited the infamous Log4Shell vulnerability in VMware Horizon servers to stage attack on various sectors across the globe. Common TTPs which could potentially be exploited by these threat actors or CVEs can be found in the detailed section below.

Published Vulnerabilities	Interesting Vulnerabilities	Active Threat Groups	Targeted Countries	Targeted Industries	ATT&CK TTPs
500	7	3	27	16	46

Detailed Report:

Interesting Vulnerabilities:

Vendor	CVEs	Patch Link
SONICWALL	CVE-2022-22274	https://www.hivepro.com/dos-vulnerability-discovered-in-sonicwall-next-generation-firewall/
SOPHOS	CVE-2022-1040	https://www.hivepro.com/sophos-firewall-rce-vulnerability-actively-exploited/
spring	CVE-2022-22965*	https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement https://tanzu.vmware.com/security/cve-2022-22965
	CVE-2022-22674* CVE-2022-22675*	https://support.apple.com/en-us/HT213220

Hive Pro

Weekly Threat Digest: 28 March - 3 April 2022

Vendor	CVEs	Patch Link
TREND MICRO	CVE-2022-26871*	https://files.trendmicro.com/jp/ucmodule/apexcentral/win/2019/apexcentral_2019_gm_win_ja_3945_r3.exe https://appweb.trendmicro.com/supportNews/NewsDetail.aspx?id=4395
ZYXEL NETWORKS	CVE-2022-0342	https://support.zyxel.eu/hc/en-us/articles/4672704562578-USG-FLEX-ATP-Series-Firmware-Update-5-21-Patch-1-Installation-Notes

*Zero-day Vulnerability

Active Actors:

Icon	Name	Origin	Motive
	TA551 (Gold Cabin, Shathak)	Unknown	Financial gain
	RedFoxtrot (Nomad Panda)	China	Information theft and espionage
	APT 19 (Deep Panda, Codoso, Sunshop Group, TG-3551, Bronze Firestone, Pupa)	China	Information theft and espionage

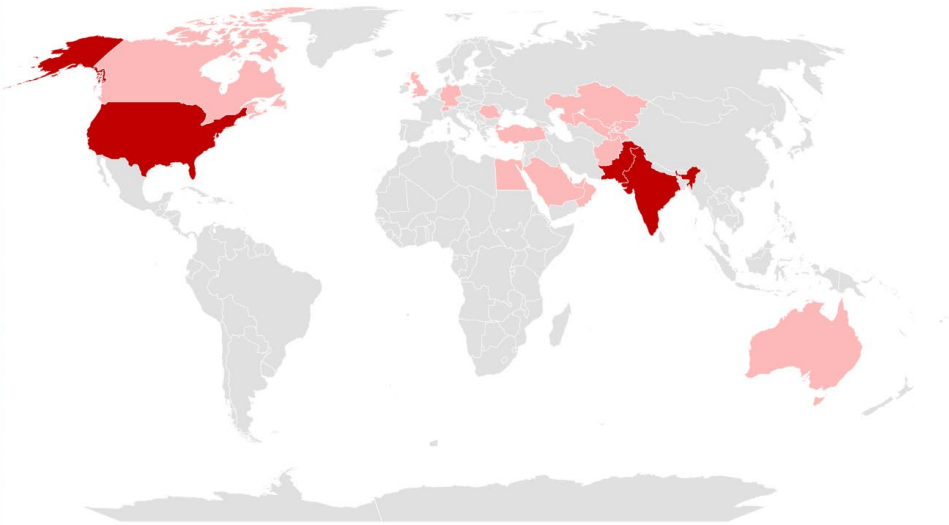
Targeted Sectors:

Hive Pro

Weekly Threat Digest: 28 March - 3 April 2022

Targeted Locations:

Countries	Count
India	2
Pakistan	2
United States of America	2
Afghanistan	1
Australia	1
Bahrain	1
Canada	1
Egypt	1
Germany	1
Jordon	1
Kazakhstan	1
Kuwait	1
Kyrgyzstan	1
Lebanon	1
Oman	1
Qatar	1
Romania	1
Saudi Arabia	1
Switzerland	1
Tajikistan	1
Turkey	1
United Arab Emirates	1
United Kingdom	1
Uzbekistan	1



Common TTPs:

TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access
T1583: Acquire Infrastructure	T1189: Drive-by Compromise	T1059: Command and Scripting Interpreter	T1098: Account Manipulation	T1548: Abuse Elevation Control Mechanism	T1548: Abuse Elevation Control Mechanism	T1110: Brute Force
T1583.001: Domains	T1190: Exploit Public-Facing Application	T1059.001: PowerShell	T1547: Boot or Logon Autostart Execution	T1134: Access Token Manipulation	T1134: Access Token Manipulation	T1110.003: Password Spraying
T1583.006: Web Services	T1133: External Remote Services	T1059.005: Visual Basic	T1547.006: Kernel Modules and Extensions	T1134.002: Create Process with Token	T1134.002: Create Process with Token	T1056: Input Capture
T1587: Develop Capabilities	T1566: Phishing	T1059.004: Unix Shell	T1547.001: Registry Run Keys / Startup Folder	T1547: Boot or Logon Autostart Execution	T1564: Hide Artifacts	T1056.004: Credential API Hooking
T1587.001: Malware	T1566.001: Spearphishing Attachment	T1059.003: Windows Command Shell	T1547.009: Shortcut Modification	T1547.006: Kernel Modules and Extensions	T1564.001: Hidden Files and Directories	T1056.001: Keylogging
T1588: Obtain Capabilities	T1199: Trusted Relationship	T1203: Exploitation for Client Execution	T1543: Create or Modify System Process	T1547.001: Registry Run Keys / Startup Folder	T1562: Impair Defenses	T1003: OS Credential Dumping
T1588.004: Digital Certificates	T1078: Valid Accounts	T1106: Native API	T1543.003: Windows Service	T1547.009: Shortcut Modification	T1562.004: Disable or Modify System Firewall	T1111: Two-Factor Authentication Interception
T1588.006: Vulnerabilities		T1053: Scheduled Task/Job	T1133: External Remote Services	T1543: Create or Modify System Process	T1562.001: Disable or Modify Tools	T1552: Unsecured Credentials
		T1204: User Execution	T1137: Office Application Startup	T1543.003: Windows Service	T1070: Indicator Removal on Host	
		T1204.002: Malicious File	T1542: Pre-OS Boot	T1068: Exploitation for Privilege Escalation	T1070.004: File Deletion	
		T1047: Windows Management Instrumentation	T1542.003: Bootkit	T1055: Process Injection	T1070.006: Timestomp	
			T1053: Scheduled Task/Job	T1055.001: Dynamic-link Library Injection	T1036: Masquerading	
			T1505: Server Software Component	T1053: Scheduled Task/Job	T1036.005: Match Legitimate Name or Location	
			T1505.003: Web Shell	T1078: Valid Accounts	T1027: Obfuscated Files or Information	
			T1078: Valid Accounts		T1027.006: HTML Smuggling	
					T1027.002: Software Packing	
					T1542: Pre-OS Boot	
					T1542.003: Bootkit	
					T1055: Process Injection	
					T1055.001: Dynamic-link Library Injection	
					T1218: Signed Binary Proxy Execution	
					T1218.001: Compiled HTML File	
					T1078: Valid Accounts	
					T1497: Virtualization/Sandbox Evasion	

TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1010: Application Window Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1071: Application Layer Protocol	T1048: Exfiltration Over Alternative Protocol	T1485: Data Destruction
T1083: File and Directory Discovery	T1021.001: Remote Desktop Protocol	T1560.003: Archive via Custom Method	T1071.001: Web Protocols	T1048.003: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	T1486: Data Encrypted for Impact
T1120: Peripheral Device Discovery	T1021.002: SMB/Windows Admin Shares	T1560.002: Archive via Library	T1132: Data Encoding	T1041: Exfiltration Over C2 Channel	T1491: Defacement
T1057: Process Discovery	T1021.004: SSH	T1213: Data from Information Repositories	T1132.001: Standard Encoding	T1537: Transfer Data to Cloud Account	T1491.001: Internal Defacement
T1012: Query Registry		T1005: Data from Local System	T1001: Data Obfuscation		T1561: Disk Wipe
T1082: System Information Discovery		T1074: Data Staged	T1001.003: Protocol Impersonation		T1561.001: Disk Content Wipe
T1016: System Network Configuration Discovery		T1074.001: Local Data Staging	T1573: Encrypted Channel		T1561.002: Disk Structure Wipe
T1033: System Owner/User Discovery		T1056: Input Capture	T1573.001: Symmetric Cryptography		T1490: Inhibit System Recovery
T1124: System Time Discovery		T1056.004: Credential API Hooking	T1008: Fallback Channels		T1489: Service Stop
T1497: Virtualization/Sandbox Evasion		T1056.001: Keylogging	T1105: Ingress Tool Transfer		T1529: System Shutdown/Reboot
			T1571: Non-Standard Port		
			T1090: Proxy		
			T1090.002: External Proxy		

Weekly Threat Digest: 28 March - 3 April 2022

Threat Advisories:

Sophos Firewall RCE vulnerability actively exploited

DOS Vulnerability discovered in SonicWall Next-Generation Firewall

Prolific threat actor TA551 using new malware IcedID

New PlugX variant “Talisman” used by famous Chinese APT

RCE Spring Framework Zero-Day vulnerability “Spring4Shell”

Two Vulnerabilities affecting Apple macOS exploited-in-the-wild

Actively exploited vulnerability affects Trend Micro Apex Central

Authentication Bypass Vulnerability in Zyxel Firmware