# Hive Pro

# Weekly Threat Digest: 7 - 13 March 2022

## Overview:

The second week of March 2022 witnessed the discovery of 538 vulnerabilities out of which 16 gained the attention of Threat Actors and security researchers worldwide. Among these 16, there were 3 zero-days and 5 other vulnerabilities about which the National vulnerability Database (NVD) is awaiting analysis, while 6 of them are undergoing analysis, and 3 were not present in the NVD at all. Hive Pro Threat Research Team has curated a list of 16 CVEs that require immediate action.

Further, we also observed 3 Threat Actor groups being highly active in the last week. APT41, a well-known Chinese threat actor group popular for espionage and financial gain, was observed targeting US state government networks using the famous Log4j vulnerability (CVE-2021-44228) and the USAHerds program (CVE-2021- 44207). Additionally, a famous Initial Access Broker (IAB) was also prominent targeting organizations from the US, UK, and India. Another threat actor from China, Mustang Panda, was observed targeting European diplomats using a revised version of the PlugX backdoor. 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 |
|---|---|---|---|---|---|
| 538 | 16 | 3 | 42 | 19 | 89 |

## Detailed Report:

### Interesting Vulnerabilities:

| Vendor | CVEs | Patch Link |
|---|---|---|
|  | CVE-2022-23187<br>CVE-2022-24094<br>CVE-2022-24095<br>CVE-2022-24096<br>CVE-2022-24097 | https://helpx.adobe.com/security/products/illustrator/apsb22-15.html<br>https://helpx.adobe.com/security/products/after_effects/apsb22-17.html |
|  | CVE-2022-26384<br>CVE-2022-26383<br>CVE-2022-26387<br>CVE-2022-26381 | https://cdn.stubdownloader.services.mozilla.com/builds/firefox-stub/en-US/win/bb09da6defac4081f06e02ac17730b9b6f1e13db4315d371a03b167a2f4b3155/Firefox%20Installer.exe |

# Hive Pro

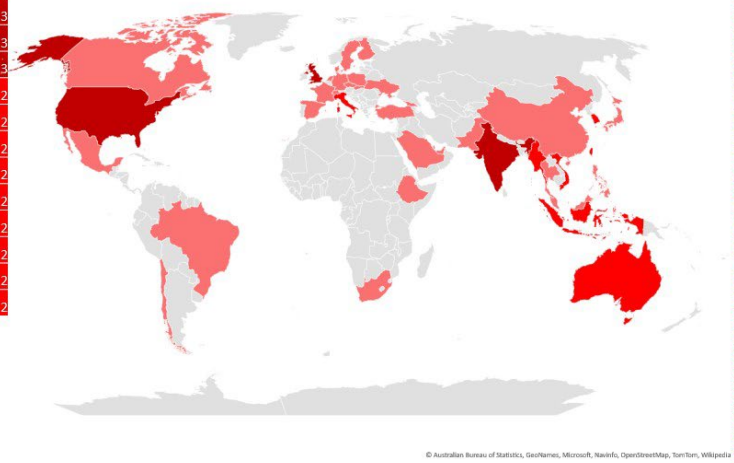
# Weekly Threat Digest: 7 - 13 March 2022

| Vendor | CVEs | Patch Link |
|---|---|---|
| Microsoft | CVE-2022-24512*<br>CVE-2022-21990*<br>CVE-2022-24459*<br>CVE-2022-23277<br>CVE-2022-22006<br>CVE-2022-24501 | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24512<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21990<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24459<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23277<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22006<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24501 |
|  | CVE-2022-0847 | https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/snapshot/linux9d2231c5d74e13b2a0546fee6737ee4446017903.tar.gz |

*Zero-day Vulnerability

## Targeted Locations:

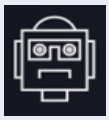
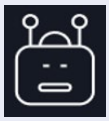
| Country | Count |
|---|---|
| India | 3 |
| UK | 3 |
| USA | 3 |
| Australia | 2 |
| Hong Kong | 2 |
| Indonesia | 2 |
| Italy | 2 |
| Myanmar | 2 |
| Singapore | 2 |
| South Korea | 2 |
| Taiwan | 2 |
| Vietnam | 2 |




| Country | Count |
|---|---|
| Bahrain | 1 |
| Brazil | 1 |
| Canada | 1 |
| Chile | 1 |
| China | 1 |
| Czech | 1 |
| Denmark | 1 |
| Ethiopia | 1 |
| Finland | 1 |
| France | 1 |
| Georgia | 1 |
| Germany | 1 |
| Japan | 1 |
| Malaysia | 1 |
| Mexico | 1 |
| Netherlands | 1 |
| Pakistan | 1 |
| Philippines | 1 |
| Poland | 1 |
| Qatar | 1 |
| Saudi Arabia | 1 |
| Slovakia | 1 |
| South Africa | 1 |
| Spain | 1 |
| Sweden | 1 |
| Switzerland | 1 |
| Thailand | 1 |
| Turkey | 1 |
| UAE | 1 |
| Ukraine | 1 |

# Weekly Threat Digest: 7 - 13 March 2022

## Active Actors:

| Icon | Name | Origin | Motive |
|---|---|---|---|
|  | APT41 (Double Dragon, TG-2633, Bronze Atlas, Red Kelpie, Blackfly, Earth Baku, SparklingGoblin, Grayfly) | China | Espionage and financial gain |
|  | Prophet Spider | Unknown | Crypto mining, ransomware, and extortion. |
|  | Mustang Panda (Bronze President, TEMP.Hex, HoneyMyte, Red Lich, RedDelta, TA416) | China | Information theft and espionage |

## 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 | T1197: BITS Jobs | T1547: Boot or Logon Autostart Execution | T1197: BITS Jobs |
| T1583.001: Domains | T1133: External Remote Services | T1059.001: PowerShell | T1547: Boot or Logon Autostart Execution | T1547.001: Registry Run Keys / Startup Folder | T1480: Execution Guardrails |
| T1588: Obtain Capabilities | T1566: Phishing | T1059.004: Unix Shell | T1547.001: Registry Run Keys / Startup Folder | T1543: Create or Modify System Process | T1480.001: Environmental Keying |
| T1588.002: Tool | T1566.001: Spearphishing Attachment | T1059.005: Visual Basic | T1136: Create Account | T1543.003: Windows Service | T1564: Hide Artifacts |
| | T1566.002: Spearphishing Link | T1059.003: Windows Command Shell | T1136.001: Local Account | T1546: Event Triggered Execution | T1564.001: Hidden Files and Directories |
| | T1091: Replication Through Removable Media | T1203: Exploitation for Client Execution | T1543: Create or Modify System Process | T1546.003: Windows Management Instrumentation Event Subscription | T1564.006: Run Virtual Instance |
| | T1195: Supply Chain Compromise | T1053: Scheduled Task/Job | T1543.003: Windows Service | T1546.008: Accessibility Features | T1574: Hijack Execution Flow |
| | T1195.002: Compromise Software Supply Chain | T1053.005: Scheduled Task | T1546: Event Triggered Execution | T1068: Exploitation for Privilege Escalation | T1574.001: DLL Search Order Hijacking |
| | T1078: Valid Accounts | T1569: System Services | T1546.008: Accessibility Features | T1574: Hijack Execution Flow | T1574.002: DLL Side-Loading |
| | | T1204: User Execution | T1546.003: Windows Management Instrumentation Event Subscription | T1574.001: DLL Search Order Hijacking | T1574.006: Dynamic Linker Hijacking |
| | | T1204.002: Malicious File | T1133: External Remote Services | T1574.002: DLL Side-Loading | T1562: Impair Defenses |
| | | T1204.001: Malicious Link | T1574: Hijack Execution Flow | T1574.006: Dynamic Linker Hijacking | T1562.001: Disable or Modify Tools |
| | | T1047: Windows Management Instrumentation | T1574.001: DLL Search Order Hijacking | T1055: Process Injection | T1070: Indicator Removal on Host |
| | | | T1574.002: DLL Side-Loading | T1053: Scheduled Task/Job | T1070.003: Clear Command History |
| | | | T1574.006: Dynamic Linker Hijacking | T1053.005: Scheduled Task | T1070.001: Clear Windows Event Logs |
| | | | T1542: Pre-OS Boot | | T1070.004: File Deletion |
| | | | T1542.003: Bootkit | | T1036: Masquerading |
| | | | T1053: Scheduled Task/Job | | T1036.007: Double File Extension |
| | | | T1053.005: Scheduled Task | | T1036.004: Masquerade Task or Service |
| | | | T1505: Server Software Component | | T1036.005: Match Legitimate Name or Location |
| | | | T1505.003: Web Shell | | T1112: Modify Registry |
| | | | | | T1027: Obfuscated Files or Information |
| | | | | | T1027.001: Binary Padding |
| | | | | | T1542: Pre-OS Boot |
| | | | | | T1542.003: Bootkit |
| | | | | | T1014: Rootkit |
| | | | | | T1218: Signed Binary Proxy Execution |
| | | | | | T1218.001: Compiled HTML File |
| | | | | | T1218.004: InstallUtil |
| | | | | | T1218.005: Mshta |
| | | | | | T1218.007: Msiexec |
| | | | | | T1218.010: Regsvr32 |
| | | | | | T1218.011: Rundll32 |
| | | | | | T1553: Subvert Trust Controls |
| | | | | | T1553.002: Code Signing |

| TA0006: Credential Access | TA0007: Discovery | TA0008: Lateral Movement | TA0009: Collection | TA0011: Command and Control | TA0010: Exfiltration | TA0040: Impact |
|---|---|---|---|---|---|---|
| T1110: Brute Force | T1083: File and Directory Discovery | T1021: Remote Services | T1560: Archive Collected Data | T1071: Application Layer Protocol | T1052: Exfiltration Over Physical Medium | T1486: Data Encrypted for Impact |
| T1110.002: Password Cracking | T1046: Network Service Scanning | T1021.001: Remote Desktop Protocol | T1560.003: Archive via Custom Method | T1071.004: DNS | T1052.001: Exfiltration over USB | T1490: Inhibit System Recovery |
| T1056: Input Capture | T1135: Network Share Discovery | T1021.002: SMB/Windows Admin Shares | T1560.001: Archive via Utility | T1071.002: File Transfer Protocols | | T1496: Resource Hijacking |
| T1056.001: Keylogging | T1120: Peripheral Device Discovery | T1091: Replication Through Removable Media | T1119: Automated Collection | T1071.001: Web Protocols | | T1489: Service Stop |
| T1003: OS Credential Dumping | T1057: Process Discovery | | T1005: Data from Local System | T1568: Dynamic Resolution | | |
| T1003.001: LSASS Memory | T1518: Software Discovery | | T1074: Data Staged | T1568.002: Domain Generation Algorithms | | |
| T1003.003: NTDS | T1082: System Information Discovery | | T1074.001: Local Data Staging | T1573: Encrypted Channel | | |
| | T1614: System Location Discovery | | T1056: Input Capture | T1573.001: Symmetric Cryptography | | |
| | T1614.001: System Language Discovery | | T1056.001: Keylogging | T1105: Ingress Tool Transfer | | |
| | T1016: System Network Configuration Discovery | | | T1104: Multi-Stage Channels | | |
| | T1016.001: Internet Connection Discovery | | | T1090: Proxy | | |
| | T1049: System Network Connections Discovery | | | T1219: Remote Access Software | | |
| | T1033: System Owner/User Discovery | | | T1102: Web Service | | |
| | | | | T1102.001: Dead Drop Resolver | | |

# Weekly Threat Digest: 7 - 13 March 2022

## Threat Advisories:

Dirty Pipe: A privilege escalation vulnerability in Linux Kernel
Microsoft addressed three zero-day vulnerabilities March 2022 Patch Tuesday Update
Mozilla release Security Advisories for multiple vulnerabilities affecting Firefox and Firefox ESR
Multiple security vulnerabilities in Adobe After Effects and Illustrator
Chinese state-sponsored threat group APT41 targets U.S. critical organizations using two Zero-Days
RangnarLocker Ransomware hits Critical Infrastructure Compromising 50+ Organizations
Prophet Spider exploits Log4j and Citrix vulnerabilities to deploy webshells
Mustang Panda targets European diplomats using enhanced PlugX backdoor