Hive Pro

Weekly Threat Digest: 14 - 20 March 2022

Overview:

The third week of March 2022 witnessed the discovery of 567 vulnerabilities out of which 22 gained the attention of Threat Actors and security researchers worldwide. Among these 22, there were 2 vulnerabilities about which the National vulnerability Database (NVD) is awaiting analysis, while 2 more of them are undergoing reanalysis, and 14 were not present in the NVD at all. Hive Pro Threat Research Team has curated a list of 22 CVEs that require immediate action.

Furthermore, we also observed five threat actor groups being highly active in the last week. The Sandworm Team, a well-known Russian threat actor group popular for sabotage and destruction, was observed using a new malware known as Cyclops Blink. Additionally, a new threat actor, Exotic Lily, was acting as Initial Access Broker (IAB) for Conti and Diavol ransomware groups exploiting the zero-day vulnerability in Microsoft MSHTML (CVE-2021-40444). Another threat actor from Russia, UAC-0056, was observed targeting Western European and North American ministries as well as private sectors. Two ransomware gangs, Pandora and Lockbit, were active across different organizations around 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
567	22	5	36	15	60

Detailed Report:

Interesting Vulnerabilities:

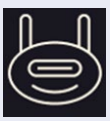
Vendor	CVEs	Patch Link
	CVE-2021-20083	https://wordpress.org/news/2022/03/wordpress-5-9-2-security-maintenance-release/
	CVE-2022-24728 CVE-2022-24729	https://www.drupal.org/project/drupal/releases/9.2.15 https://www.drupal.org/project/drupal/releases/9.3.8
	CVE-2022-0337	https://download3.operacdn.com/pub/opera/desktop/84.0.4316.42/win/Opera_84.0.4316.42_Setup_x64.exe
	CVE-2022-0337	https://files02.tchspt.com/temp/MicrosoftEdgeSetup.exe

Hive Pro

Weekly Threat Digest: 14 - 20 March 2022

Vendor	CVEs	Patch Link
	CVE-2022-0971 CVE-2022-0972 CVE-2022-0973 CVE-2022-0974 CVE-2022-0975 CVE-2022-0976 CVE-2022-0977 CVE-2022-0978 CVE-2022-0979 CVE-2022-0980 CVE-2022-0337	https://www.google.com/intl/en/chrome/?standalone=1
	CVE-2022-0778	https://github.com/openssl/openssl/commit/a466912611aa6cbdf550cd10601390e587451246 https://github.com/openssl/openssl/commit/3118eb64934499d93db3230748a452351d1d9a65
	CVE-2022- 25636	https://git.kernel.org/pub/scm/linux/kernel/git/netfilter/nf.git/snapshot/nf-b1a5983f56e371046dcf164f90bfaf704d2b89f6.tar.gz
	CVE-2021-22986	https://support.f5.com/csp/article/K03009991
	CVE-2018-13379	https://www.fortiguard.com/psirt/FG-IR-18-384
	CVE-2021-25220 CVE-2022-0396 CVE-2022-0635 CVE-2022-0667	https://www.isc.org/bind/

Active Actors:

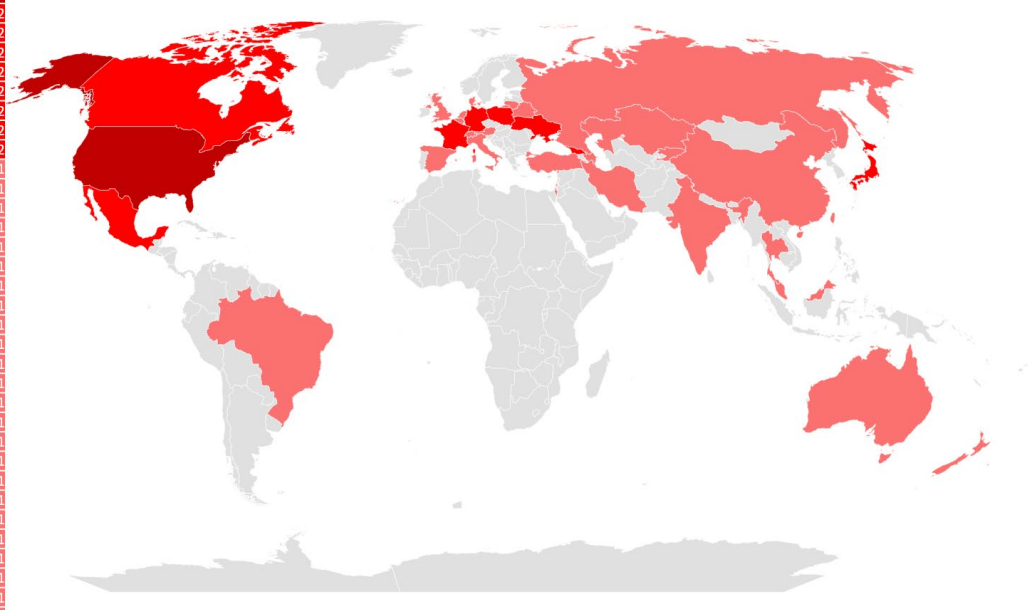
Icon	Name	Origin	Motive
	Sandworm Team (ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, VOODOO BEAR)	Russia	Sabotage and destruction

Weekly Threat Digest: 14 - 20 March 2022

Icon	Name	Origin	Motive
	Exotic Lily	Unknown	Ecrime
	UAC-0056 (SaintBear, UNC2589, TA471)	Russia	Information theft
	Pandora Ransomware Gang	Unknown	Ecrime, Information theft, and Financial gain
	Lockbit 2.0	Unknown	Financial gain

Targeted Locations:

Countries	Count
USA	3
France	2
Georgia	2
Germany	2
Japan	2
Poland	2
Ukraine	2
Canada	2
Mexico	2
Australia	1
Austria	1
Azerbaijan	1
Belarus	1
Belgium	1
Brazil	1
China	1
Denmark	1
Hong Kong	1
India	1
Iran	1
Israel	1
Italy	1
Kazakhstan	1
Kyrgyzstan	1
Lithuania	1
Malaysia	1
Netherlands	1
New Zealand	1
Russia	1
Singapore	1
Spain	1
Switzerland	1
Taiwan	1
Thailand	1
Turkey	1
United Kingdom	1



Weekly Threat Digest: 14 - 20 March 2022

Targeted Sectors:

Common TTPs:

TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access
T1587: Develop Capabilities	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1562: Impair Defenses	T1557: Adversary-in-the-Middle
T1587.001: Malware	T1133: External Remote Services	T1059.007: JavaScript	T1547.001: Registry Run Keys / Startup Folder	T1547.001: Registry Run Keys / Startup Folder	T1562.004: Disable or Modify System Firewall	T1110: Brute Force
T1588: Obtain Capabilities	T1566: Phishing	T1059.004: Unix Shell	T1037: Boot or Logon Initialization Scripts	T1037: Boot or Logon Initialization Scripts	T1070: Indicator Removal on Host	T1110.001: Password Guessing
T1588.006: Vulnerabilities	T1566.001: Spearphishing Attachment	T1059.003: Windows Command Shell	T1037.004: RC Scripts	T1037.004: RC Scripts	T1070.004: File Deletion	T1056: Input Capture
	T1078: Valid Accounts	T1203: Exploitation for Client Execution	T1133: External Remote Services	T1068: Exploitation for Privilege Escalation	T1036: Masquerading	T1056.004: Credential API Hooking
		T1204: User Execution	T1556: Modify Authentication Process	T1055: Process Injection	T1036.005: Match Legitimate Name or Location	T1556: Modify Authentication Process
		T1204.002: Malicious File	T1137: Office Application Startup	T1078: Valid Accounts	T1556: Modify Authentication Process	T1003: OS Credential Dumping
		T1047: Windows Management Instrumentation	T1542: Pre-OS Boot		T1112: Modify Registry	T1003.003: NTDS
			T1542.001: System Firmware		T1027: Obfuscated Files or Information	
			T1137: Office Application Startup		T1027.006: HTML Smuggling	
			T1137.001: Office Template Macros		T1027.002: Software Packing	
			T1078: Valid Accounts		T1542: Pre-OS Boot	
					T1542.001: System Firmware	
					T1055: Process Injection	
					T1078: Valid Accounts	
					T1497: Virtualization/Sandbox Evasion	

TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1087: Account Discovery	T1021: Remote Services	T1557: Adversary-in-the-Middle	T1071: Application Layer Protocol	T1041: Exfiltration Over C2 Channel	T1485: Data Destruction
T1083: File and Directory Discovery	T1021.001: Remote Desktop Protocol	T1560: Archive Collected Data	T1071.001: Web Protocols	T1567: Exfiltration Over Web Service	T1486: Data Encrypted for Impact
T1057: Process Discovery	T1021.002: SMB/Windows Admin Shares	T1560.001: Archive via Utility	T1132: Data Encoding	T1567.002: Exfiltration to Cloud Storage	T1565: Data Manipulation
T1012: Query Registry		T1056: Input Capture	T1132.002: Non-Standard Encoding		T1499: Endpoint Denial of Service
T1018: Remote System Discovery		T1056.004: Credential API Hooking	T1573: Encrypted Channel		T1499.004: Application or System Exploitation
T1518: Software Discovery			T1573.002: Asymmetric Cryptography		T1490: Inhibit System Recovery
T1082: System Information Discovery			T1008: Fallback Channels		T1498: Network Denial of Service
T1497: Virtualization/Sandbox Evasion			T1105: Ingress Tool Transfer		T1498.001: Direct Network Flood
			T1571: Non-Standard Port		
			T1090: Proxy		
			T1090.003: Multi-hop Proxy		

Weekly Threat Digest: 14 - 20 March 2022

Threat Advisories:

Pandora Ransomware Targets Multiple Plants around the Globe

LockBit 2.0 Ransomware affiliates targeting Renowned Organizations

Sandworm Team using a new modular malware Cyclops Blink

Environment Variables Leak affect Multiple browsers

Major Content Management Systems affected by Multiple vulnerabilities

New Threat Actor Exotic Lily acting as Initial Access Broker for Conti and Diavol ransomware group

Russian threat actors leveraging misconfigured multifactor authentication to exploit PrintNightmare vulnerability

Russian threat actor UAC-0056 targets European countries

Multiple Google Chrome Vulnerabilities affects all Platforms

Attackers could gain root access using vulnerability in Linux Kernel Netfilter Firewall

OpenSSL exposed to Denial-of-service vulnerability causing Infinite Loop

Attackers Escape Kubernetes Containers using “cr8escape” Vulnerability in CRI-O

Russia under Attack from New RURansom Wiper