Hive Pro

Weekly Threat Digest: 4 - 10 April 2022

Overview:

The second week of April 2022 witnessed the discovery of 438 vulnerabilities out of which 3 gained the attention of Threat Actors and security researchers worldwide. All these 3 were zero-day and require immediate action.

Further, we also observed 3 Threat Actor groups being highly active in the last week. Armageddon, a well-known Russian threat actor group popular for information theft and espionage, was observed targeting European government agencies Additionally, 2 Threat Actor groups originating from China were observed targeting organizations all around the world. Common TTPs which could potentially be exploited by these threat actors or CVEs can be found in the detailed section.

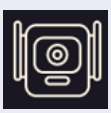
Published Vulnerabilities	Interesting Vulnerabilities	Active Threat Groups	Targeted Countries	Targeted Industries	ATT&CK TTPs
438	3	3	53	16	54

Detailed Report:

Interesting Vulnerabilities:

Vendor	CVEs	Patch Link
WatchGuard	CVE-2022-23176*	https://www.watchguard.com/support/release-notes/fireware/12/en-US/EN_ReleaseNotes_Fireware_12_7/index.html
Apache LOG4J	CVE-2021-44228*	https://logging.apache.org/log4j/2.x/manual/migration.html https://kb.vmware.com/s/article/87073
spring	CVE-2022-22965*	https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement https://tanzu.vmware.com/security/cve-2022-22965

Active Actors:

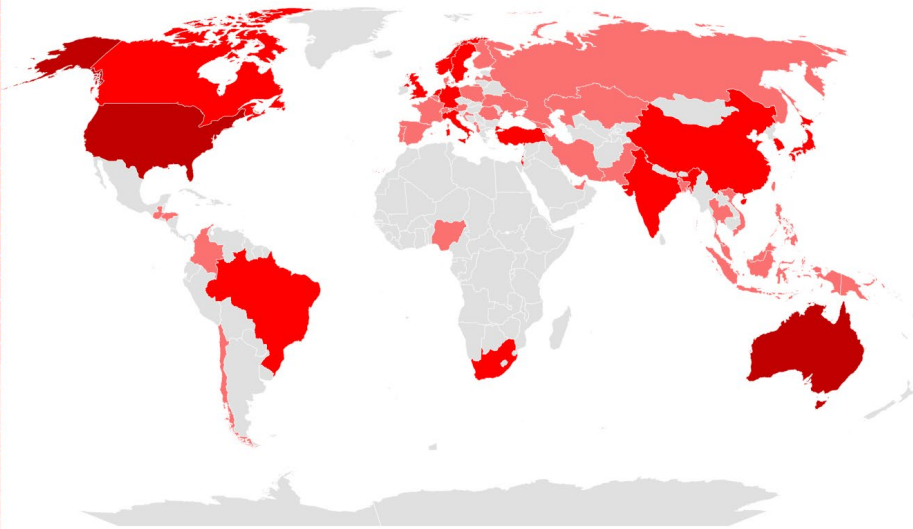
Icon	Name	Origin	Motive
	APT 10 (Stone Panda, menuPass, Red Apollo, CVNX, Potassium, Hogfish, Happyyongzi, Cicada, Bronze Riverside, CTG-5938, ATK 41, TA429, ITG01)	China	Information theft and espionage
	APT 19(Deep Panda, Codoso, Sunshop, TG-3551, Bronze Firestone, Pupa)	China	Information theft and espionage
	Armageddon(Gamaredon Group, Winterflounder, Primitive Bear, BlueAlpha, Blue Otso, Iron Tilden, SectorC08, Callisto, Shuckworm, Actinium, DEV-0157, UAC-0010)	Russia	Information theft and espionage

Hive Pro

Weekly Threat Digest: 4 - 10 April 2022

Targeted Locations:

Countries	Count
USA	3
Australia	3
Turkey	2
Norway	2
South Korea	2
Brazil	2
Italy	2
Canada	2
Netherlands	2
China	2
South Africa	2
Germany	2
Sweden	2
India	2
UK	2
Israel	2
Japan	2
UAE	1
Finland	1
Portugal	1
Hong Kong	1
Switzerland	1
Bangladesh	1
Philippines	1
Indonesia	1
Russia	1
Thailand	1
Belgium	1



Countries	Count
Honduras	1
Ukraine	1
Poland	1
Colombia	1
Romania	1
Albania	1
Singapore	1
Malaysia	1
France	1
Montenegro	1
Georgia	1
Croatia	1
Taiwan	1
Nigeria	1
Austria	1
Denmark	1
Guatemala	1
Pakistan	1
Papua New Guinea	1
Vietnam	1
Kazakhstan	1
Iran	1
Spain	1
Chile	1
Latvia	1

Targeted Sectors:

Media	Construction	Defence	IT
Think Tanks	Healthcare	Aerospace	NGOs
High-Tech	Law Enforcements	Energy	Tele-communications
Government	Financial	Education	Pharmaceutical

Common TTPs:

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1592: Gather Victim Host Information	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	T1564: Hide Artifacts
	T1588: Obtain Capabilities	T1566.001: Spearphishing Attachment	T1059.003: Windows Command Shell	T1574.002: DLL Side-Loading	T1574.002: DLL Side-Loading	T1574: Hijack Execution Flow
	T1588.003: Code Signing Certificates	T1199: Trusted Relationship	T1106: Native API	T1053: Scheduled Task/Job	T1055: Process Injection	T1574.001: DLL Search Order Hijacking
	T1588.002: Tool	T1078: Valid Accounts	T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1055.012: Process Hollowing	T1574.002: DLL Side-Loading
			T1053.005: Scheduled Task	T1078: Valid Accounts	T1053: Scheduled Task/Job	T1070: Indicator Removal on Host
			T1569: System Services		T1053.005: Scheduled Task	T1070.003: Clear Command History
			T1569.002: Service Execution		T1078: Valid Accounts	T1070.004: File Deletion
			T1204: User Execution			T1036: Masquerading
			T1204.002: Malicious File			T1036.005: Match Legitimate Name or Location
			T1047: Windows Management Instrumentation			T1036.003: Rename System Utilities
						T1027: Obfuscated Files or Information
						T1027.002: Software Packing
						T1055: Process Injection
						T1055.012: Process Hollowing
						T1620: Reflective Code Loading
						T1014: Rootkit
						T1218: Signed Binary Proxy Execution
						T1218.004: InstallUtil
						T1553: Subvert Trust Controls
						T1553.002: Code Signing
						T1078: Valid Accounts

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration
T1056: Input Capture	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1560: Archive Collected Data	T1568: Dynamic Resolution	T1041: Exfiltration Over C2 Channel
T1056.001: Keylogging	T1087.002: Domain Account	T1021: Remote Services	T1560.001: Archive via Utility	T1568.001: Fast Flux DNS	
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		
T1003.003: NTDS	T1018: Remote System Discovery		T1039: Data from Network Shared Drive		
T1003.002: Security Account Manager	T1082: System Information Discovery		T1074: Local Data Staged		
	T1016: System Network Configuration Discovery		T1074.001: Local Data Staging		
	T1049: System Network Connections Discovery		T1074.002: Remote Data Staging		
			T1056: Input Capture		
			T1056.001: Keylogging		
			T1113: Screen Capture		

Hive Pro

Weekly Threat Digest: 4 - 10 April 2022

Threat Advisories:

Deep Panda deploys new rootkit “Fire Chili” by exploiting Log4shell in VMware horizon
Sandworm Team using a new modular malware Cyclops Blink
APT 10, a state-sponsored Chinese threat group, conducting a global cyber espionage operation
RCE Spring Framework Zero-Day vulnerability “Spring4Shell”
Attacks on European Union and Ukrainian government entities carried out by the Armageddon group