Hive Pro

Weekly Threat Digest: 14-20 February 2022

Overview:

The third week of February 2022 witnessed the discovery of 551 vulnerabilities out of which 17 gained the attention of Threat Actors and security researchers worldwide. Among these 17, there were 2 zero-day and 7 other vulnerabilities about which the National vulnerability Database (NVD) is awaiting analysis while 9 were not present in the NVD at all. Hive Pro Threat Research Team has curated a list of 17 CVEs that require immediate action.

Further, we also observed 2 Threat Actor groups being highly active in the last week. APT28, a well-known Russian threat actor group popular for information theft and espionage, was observed targeting US-based defense contractors (CDCs). Additionally, a highly sophisticated and innovative ransomware family BlackCat, first observed in November 2021 was also prominent targeting 30+ organizations in 17 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
551	17	2	17	18	31

Detailed Report:

Interesting Vulnerabilities:

Vendor	CVEs	Patch Link
	CVE-2022-24086* CVE-2022-24087	https://helpx.adobe.com/security/products/magento/apsb22-12.html
	CVE-2022-0609* CVE-2022-0603 CVE-2022-0604 CVE-2022-0605 CVE-2022-0606 CVE-2022-0607 CVE-2022-0608 CVE-2022-0610	https://www.google.com/intl/en/chrome/?standalone=1
vmware	CVE-2021-22040 CVE-2021-22041 CVE-2021-22042 CVE-2021-22043 CVE-2021-22050	https://www.vmware.com/security/advisories/VMSA-2022-0004.html
	CVE-2021-44731	https://ubuntu.com/security/notices/USN-5292-1
	CVE-2022-0633	https://downloads.wordpress.org/plugin/updraftplus.1.22.4.zip https://updraftplus.com/wp-content/uploads/updraftplus.zip

* Zero-day vulnerability

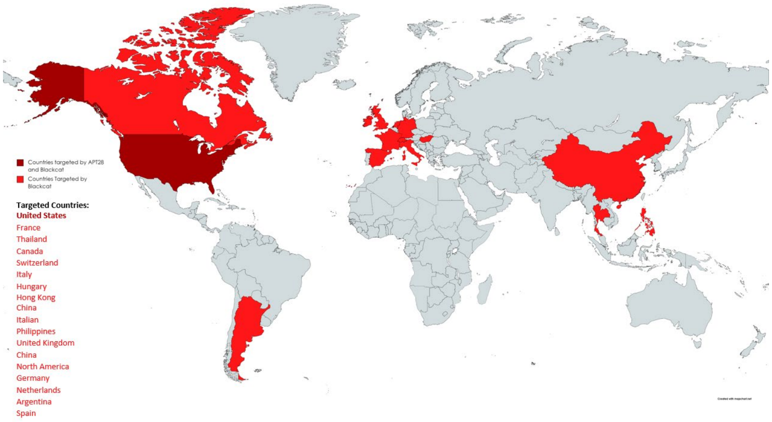
Hive Pro

Weekly Threat Digest: 14-20 February 2022

Active Actor:

Icon	Name	Origin	Motive
	APT28 (FANCY BEAR, STRONTIUM, Sofacy, Zebrocy, Sednit, Pawn Storm, TG-4127, Tsar-Team, Iron Twilight, Swallowtail, SNAKEMACKEREL, Frozen Lake)	Russia	Information theft and espionage
	Blackcat (ALPHV)	Unknown	Financial gain

Targeted Locations:


Countries targeted by APT28 and Blackcat
Countries Targeted by Blackcat

Targeted Countries:
United States
France
Thailand
Canada
Switzerland
Italy
Hungary
Hong Kong
China
Italian
Philippines
United Kingdom
China
North America
Germany
Netherlands
Argentina
Spain

Targeted Sectors:

Airline	Defense	Insurance	Financial	Government	High-Tech
Education	Engineering	Healthcare	Industrial	Chemical	Think Tanks
Media	Oil and gas	Telecommunications	Retail	Automotive	Construction

Common TTPs:

TA0043: Reconnaissance	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1589: Gather Victim Identity Information	T1189: Drive-by Compromise	T1059: Command and Scripting Interpreter	T1543: Create or Modify System Process	T1543: Create or Modify System Process	T1140: Deobfuscate/Decode Files or Information
T1589.001: Credentials	T1190: Exploit Public-Facing Application	T1203: Exploitation for Client Execution	T1543.003: Windows Service	T1543.003: Windows Service	T1202: Indirect Command Execution
	T1133: External Remote Services		T1133: External Remote Services	T1068: Exploitation for Privilege Escalation	T1027: Obfuscated Files or Information
	T1566: Phishing		T1078: Valid Accounts	T1078: Valid Accounts	T1027.002: Software Packing
	T1566.002: Spearphishing Link		T1078.004: Cloud Accounts	T1078.004: Cloud Accounts	T1550: Use Alternate Authentication Material
	T1195: Supply Chain Compromise		T1078.002: Domain Accounts	T1078.002: Domain Accounts	T1550.002: Pass the Hash
	T1078: Valid Accounts				T1078: Valid Accounts
	T1078.004: Cloud Accounts				T1078.004: Cloud Accounts
	T1078.002: Domain Accounts				T1078.002: Domain Accounts
					T1497: Virtualization/Sandbox Evasion

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0040: Impact
T1110: Brute Force	T1482: Domain Trust Discovery	T1550: Use Alternate Authentication Material	T1213: Data from Information Repositories	T1090: Proxy	T1485: Data Destruction
T1110.003: Password Spraying	T1083: File and Directory Discovery	T1550.002: Pass the Hash	T1213.002: Sharepoint	T1090.003: Multi-hop Proxy	T1486: Data Encrypted for Impact
T1003: OS Credential Dumping	T1082: System Information Discovery				T1499: Endpoint Denial of Service
T1003.003: NTDS	T1007: System Service Discovery				T1499.004: Application or System Exploitation
	T1497: Virtualization/Sandbox Evasion				T1499.001: OS Exhaustion Flood
					T1490: Inhibit System Recovery

Weekly Threat Digest: 14-20 February 2022

Threat Advisories:

https://www.hivepro.com/critical-magento-zero-day-vulnerability-actively-exploiting-multiple-e-commerce-websites/

https://www.hivepro.com/blackcat-ransomware-group-attacks-on-the-rise/

https://www.hivepro.com/vmware-addresses-security-flaws-discovered-during-tianfu-cup-pwn-contest/

https://www.hivepro.com/first-zero-day-vulnerability-of-google-chrome-this-year-actively-exploited-in-wild/

https://www.hivepro.com/privilege-escalation-vulnerability-in-snap-package-manager-puts-linux-users-at-risk/

https://www.hivepro.com/russian-state-sponsored-cyber-actors-targeting-u-s-critical-infrastructure/

https://www.hivepro.com/millions-of-wordpress-site-backups-at-risk-due-to-a-vulnerability-in-updraftplus-plugin