Hive Pro

Weekly Threat Digest: 9-15 May 2022

Overview:

The second week of May 2022 witnessed the discovery of 650 vulnerabilities out of which 3 gained the attention of Threat Actors and security researchers worldwide. All 3 of them are zero-days . Hive Pro Threat Research Team has curated a list of 3 CVEs that require immediate action.

Further, we also observed a Threat Actor groups being highly active in the last week. Oilrig, an Iranian threat actor group popular for Information theft and espionage, was observed targeting Jordan with phishing emails. 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
650	3	1	14	10	13

Detailed Report:

Interesting Vulnerabilities:

Vendor	CVEs	Patch Link
Microsoft	CVE-2022-26925* CVE-2022-22713* CVE-2022-29972*	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26925 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22713 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-29972

*zero-day vulnerability

Active Actors:

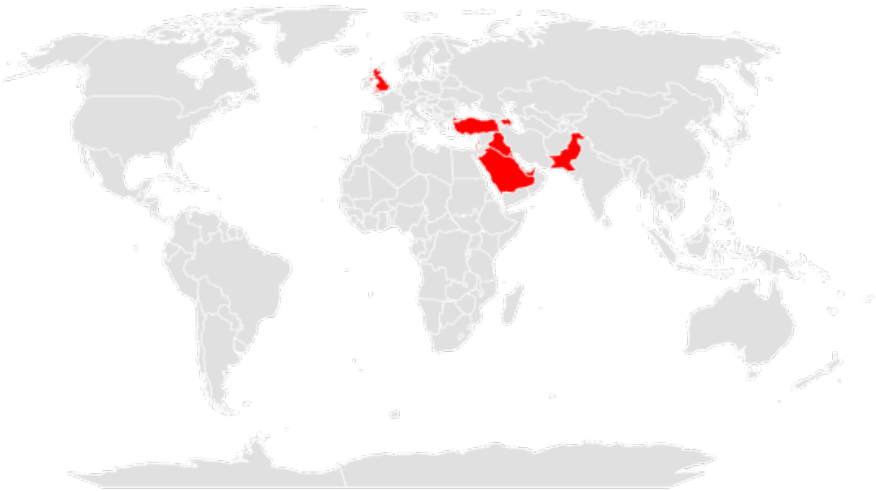
Icon	Name	Origin	Motive
	OilRig (APT 34, Helix Kitten, Twisted Kitten, Crambus , Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13)	Iran	Information theft and espionage

Hive Pro

Weekly Threat Digest: 9-15 May 2022

Targeted Locations:

- Azerbaijan
- Iraq
- Israel
- Kuwait
- Lebanon
- Mauritius
- Pakistan
- Qatar
- Saudi Arabia
- Turkey
- UAE
- UK
- USA
- Jordan



Targeted Sectors:

Common TTPs:

TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0005: Defense Evasion
T1588: Obtain Capabilities T1588.006: Vulnerabilities	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter T1059.001: PowerShell T1059.003: Windows Command Shell	T1480: Execution Guardrails
		T1053: Scheduled Task/Job T1053.005: Scheduled Task	
		T1204: User Execution T1204.002: Malicious File	
		T1047: Windows Management Instrumentation	

TA0007: Discovery	TA0011: Command and Control	TA0010: Exfiltration	TA0006: Credential Access
T1087: Account Discovery T1087.001: Local Account	T1071: Application Layer Protocol T1071.004: DNS	T1041: Exfiltration Over C2 Channel	T1557: Adversary-in-the-Middle
T1083: File and Directory Discovery	T1132: Data Encoding T1132.002: Non-Standard Encoding		
T1049: System Network Connections Discovery			
	T1568: Dynamic Resolution T1568.002: Domain Generation Algorithms		

Weekly Threat Digest: 9-15 May 2022

Threat Advisories:

Three zero-days addressed in Microsoft's May 2022 Patch Tuesday

OilRig is back with another Phishing Email attack, delivering the Saitama Backdoor