Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

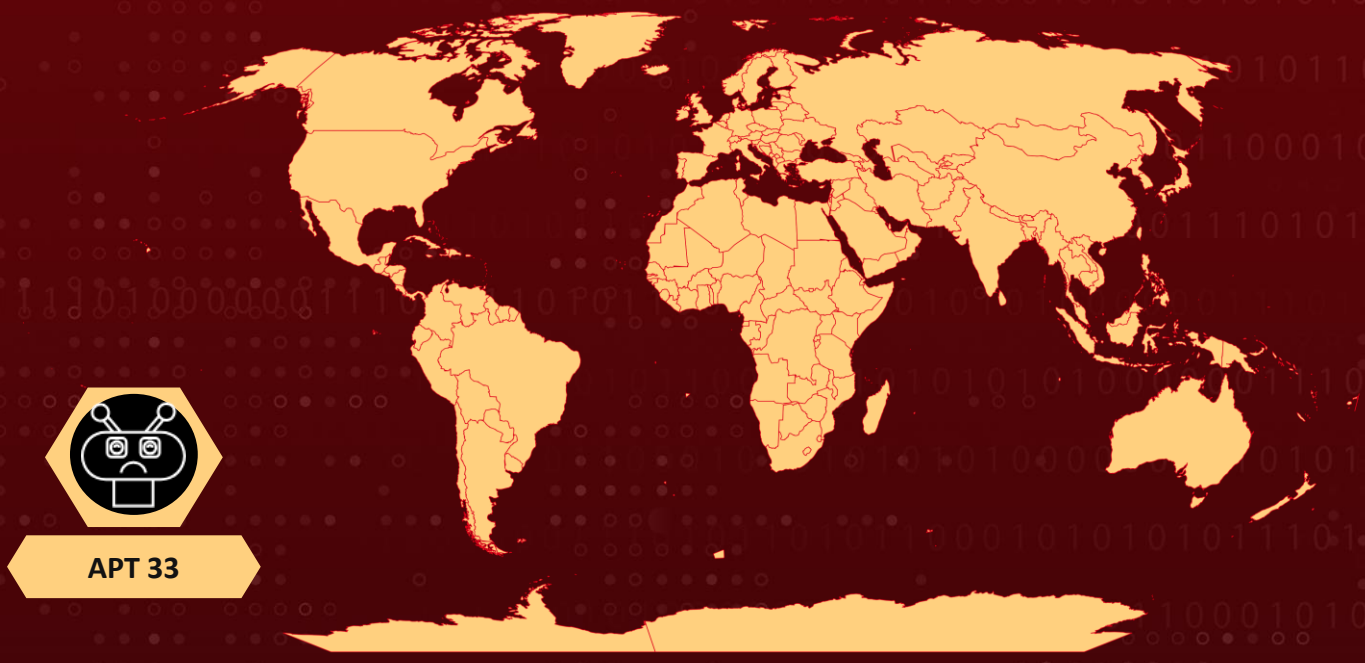
APT 33 Uses Password Spray Campaigns to Infiltrate Organizations

Date of Publication	Admiralty code	TA Number
September 18, 2023	A1	TA2023375

Summary

Attack Began: February 2023
Actor Name: APT 33 (aka Peach Sandstorm, Elfin, Magnallium, Holmium, ATK 35, Refined Kitten, TA451, Cobalt Trinity)
Target Industries: Aviation, construction, defense, education, energy, financial services, healthcare, government, satellite, pharmaceutical sector, and telecommunications sectors.
Target Region: Worldwide

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	Zoho ManageEngine products	✗	✓	✓
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server	✓	✓	✓

Actor Details

#1 APT 33 (aka Peach Sandstorm) is an Iranian nation-state threat actor that was initially identified in 2013. This group is notorious for conducting cyber espionage campaigns and has been associated with various cyberattacks. During the initial phase of this campaign, APT 33 executed password spray attacks against numerous organizations across various sectors and geographic regions.

#2 Since February 2023, there has been a noticeable shift in APT 33's tactics. They are now using a mix of publicly available and custom tools for tasks like reconnaissance, maintaining access, and moving laterally within targeted networks and systems. APT 33 appears to be utilizing two distinct sets of techniques in the initial stages of their intrusion operations in 2023.

#3 The first techniques includes password spray attacks to infiltrate different environments. They attempted to access accounts by trying different passwords, often using easily guessable ones. Just one compromised account could serve as a gateway for reconnaissance, lateral movement within the network, or accessing sensitive resources. They later employed AzureHound and Roadtools to gather data from victims' Azure Active Directory and cloud environments.

#4 The second technique involves exploitation of vulnerabilities in Zoho ManageEngine and Confluence using public proof-of concepts (POCs). They targeted CVE-2022-47966, a remote code execution vulnerability in certain on-premises Zoho ManageEngine products, and CVE-2022-26134, another remote code execution vulnerability in Confluence Server and Data Center. These vulnerabilities gave them opportunities to breach their target environments.

#5 They used compromised Azure credentials, established new Azure subscriptions within victims' tenants, and exploited Azure Arc for persistence, gaining control over on-premises devices in the victims' network. In their attack, they used multiple techniques, including Golden SAML for lateral movement, established persistence with AnyDesk, loaded custom malicious DLLs for harmful payloads, and utilized EagleRelay to tunnel malicious traffic to their C2 infrastructure. To mask their actions, APT 33 operated from TOR (The Onion Router) IPs and utilized a "go-http-client" user agent to avoid detection by defenders.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGETED INDUSTRIES
APT 33 (aka Peach Sandstorm, Elfin, Magnallium, Holmium, ATK 35, Refined Kitten, TA451, Cobalt Trinity)	Iran **MOTIVE** Information theft and espionage, Sabotage and destruction	Worldwide	Aviation, construction, defense, education, energy, financial services, healthcare, government, satellite, pharmaceutical sector, and telecommunications sectors.

Recommendations

Apply Patch: Install the security patch provided to address the CVE-2022-47966 and CVE-2022-26134 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

Reset Passwords: Reset all administrators and user password for any accounts targeted during a password spray attack is a prudent step to enhance security. Ensure that the new passwords are strong and adhere to your organization's password policy.

Behavioral Anomaly Detection: Deploy advanced behavioral anomaly detection systems that can identify deviations from normal user and system behavior, flagging activities such as password spraying, unusual execution of commands or tools.

Multi-Factor Authentication (MFA): Implement multi-factor authentication across all user accounts to strengthen access controls. This additional layer of security reduces the risk of unauthorized access, even if passwords are compromised.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0003** Persistence	**TA0008** Lateral Movement	**TA0011** Command and Control
TA0043 Reconnaissance	**TA0002** Execution	**TA0006** Credential Access	**TA0004** Privilege Escalation
TA0042 Resource Development	**T1589** Gather Victim Identity Information	**T1589.001** Credentials	**T1078** Valid Accounts
T1572 Protocol Tunneling	**T1651** Cloud Administration Command	**T1098** Account Manipulation	**T1203** Exploitation for Client Execution
T1021 Remote Services	**T1110** Brute Force	**T1110.003** Password Spraying	**T1574** Hijack Execution Flow
T1574.002 DLL Side-Loading	**T1072** Software Deployment Tools	**T1574.001** DLL Search Order Hijacking	**T1105** Ingress Tool Transfer
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1588.005** Exploits	

Indicator of Compromise (IOCs)

TYPE	VALUE
IPv4	192.52.166[.]76, 108.62.118[.]240, 102.129.215[.]40, 76.8.60[.]64

Patch Link

https://www.atlassian.com/software/confluence/download-archives

https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

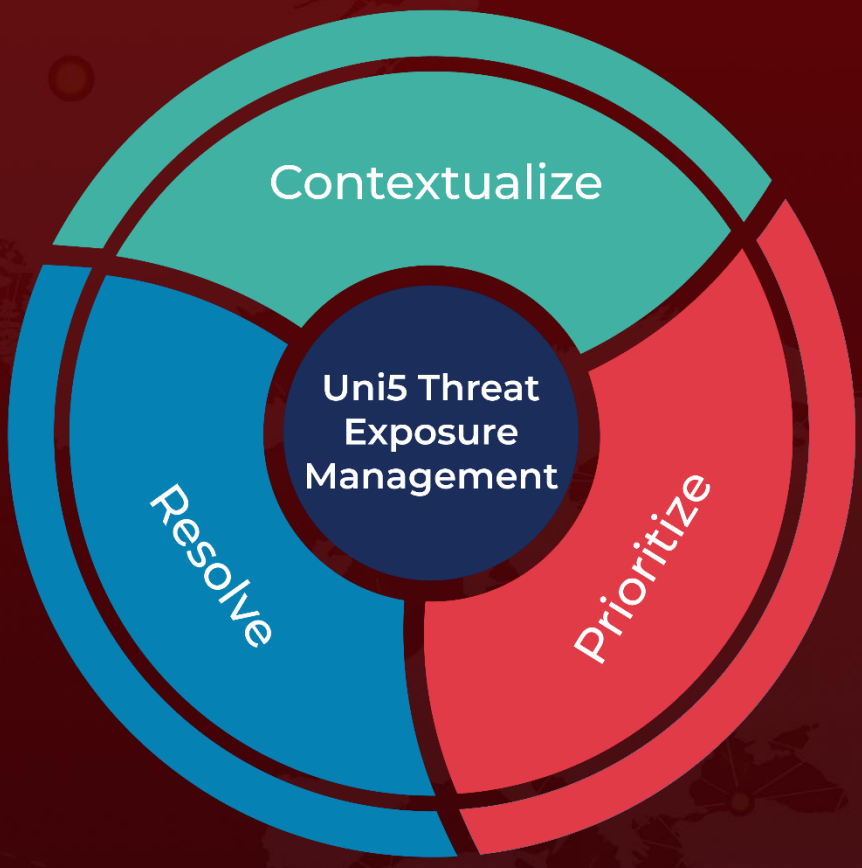
References

https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 18, 2023 . 8:10 AM

More at www.hivepro.com