



An Iranian APT Behind Recent Password Spray Attacks

CRITICALITY



19/09/2023

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

An Iranian nation-state Advanced Persistent Threat (APT33) has been observed conducting password spray attacks on multiple organizations globally.



Threat Details

Iran-linked APT33 (aka Peach Sandstorm) has mounted password spray attacks on a global scale since February 2023. The group has shown particular interest in organizations in the satellite, defense, and pharmaceutical sectors, the main purpose of the campaign is believed to be intelligence collection in support of Iranian state interests.

The group uses a variety of tactics, including password spray attacks, exploits targeting unpatched appliances, and the use of open-source security frameworks for reconnaissance and data harvesting.

In this attack scenario, threat actors use a single password across multiple accounts in an application to avoid account lockouts. Once they gain access to an account, they use publicly available tools such as AnyDesk, Azure Arc, AzureHound, or Roadtools, and custom tools such as the EagleRelay tunneling tool. These tools are used to search for specific information, maintain their presence, and move laterally within the system. The AzureHound was used to gather data from Microsoft Entra ID (formerly Azure Active Directory) and Azure Resource Manager using Microsoft Graph and Azure REST APIs, while the Roadtools provided access to Microsoft Entra ID.

The threat actor also employs multiple persistence mechanisms, such as creating new Azure subscriptions or leveraging compromised Azure resources. They installed the Azure Arc client on a compromised device and connected it to an Azure subscription controlled by Peach Sandstorm. This allowed them to control devices in the target's on-premises environment from their cloud.

The observed activity took place mostly during regular working hours in Iran, between 9:00 AM and 5:00 PM Iran Standard Time (IRST). The APT group behind the attacks used TOR IPs and a user agent called "go-http-client" during the password spray campaign.

Additionally, the Peach Sandstorm APT group attempted to exploit security vulnerabilities in Zoho ManageEngine (CVE-2022-47966) and Atlassian Confluence (CVE-2022-26134) to gain access to their targets' environments.



Recommendations



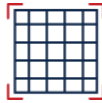
Prevention

- **Appendix A** contains the recommendations to prevent such attacks.



Detection

- **Appendix B** contains a sample of Indicators of compromise of this threat the full list is in the attached file.



MITRE ATT&CK

- **Appendix C** contains the Mitre ATT&CK details.

References

Intelligence, M. T. (n.d.). *Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets*. Retrieved from Microsoft: <https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/>

Paganini, P. (n.d.). *Iran-linked Peach Sandstorm APT is behind password spray attacks against thousands of organizations globally between February and July 2023*. Retrieved from Security Affairs: https://securityaffairs.com/150868/intelligence/iranian-peach-sandstorm-password-spray.html?utm_source=dlvr.it&utm_medium=twitter



Contact Us

Bahrain National CERT - National Cyber Security Center "NCSC"

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Center recommends the entities to follow the below steps:

- Check and monitor your Office 365 Security and Compliance Center for any suspicious events.
- Enforce password reset for all users. Please enforce a strong password policy as well.
- Ensure that your entity is using MFA for all logins. MFA using number matching is recommended to improve the sign-in security.
- DisableLegacy Authentication for all users on your environment, this type of authentication could allow attackers to bypass MFA authentication.
- Remove any inactive/old accounts from your Active Directory.



Appendix B – Indicators of Compromise

Type	Value
Peach Sandstorm Adversary IP	▪ 192[.]52[.]166[.]76 ▪ 108[.]62[.]118[.]240 ▪ 102[.]129[.]215[.]40 ▪ 76[.]8[.]60[.]64 ▪ 102[.]141[.]49[.]6

**Appendix C – MITRE ATT&CK**

Tactic	Technique
Initial Access	T1190: Exploit Public-Facing Application T1606.002: Forge Web Credentials - SAML Tokens
Persistence	T1574.001: Hijack Execution Flow - DLL Search Order Hijacking
Credential Access	T1110.003: Brute Force - Password Spraying
Lateral Movement	T1021.001: Remote Services - Remote Desktop Protocol



Appendix D – Best Practices

Bahrain National CERT team recommends organizations to implement the following best security practices.

- Backup daily important new/changed data, software and configuration settings, store disconnected data retained for at least three months. Test restoration initially, annually, and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts to read emails or to browse the web.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
[http://www.asd.gov.au/publications/protect/Microsoft Office Macro Security.pdf](http://www.asd.gov.au/publications/protect/Microsoft%20Office%20Macro%20Security.pdf)
- Whitelist applications of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- Harden user application. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Activate multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls while prioritizing the implementation of the top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement strategies to mitigate cyber security incidents. (<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Use network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Use The host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Use endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free Symon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



-
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
 - Detect and response to incidents continuously with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
 - Refer to MITRE Corporation which provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix E – TLP Definitions

RED

For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

AMBER

Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that **TLP:AMBER+STRICT** restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.

GREEN

Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.

CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction