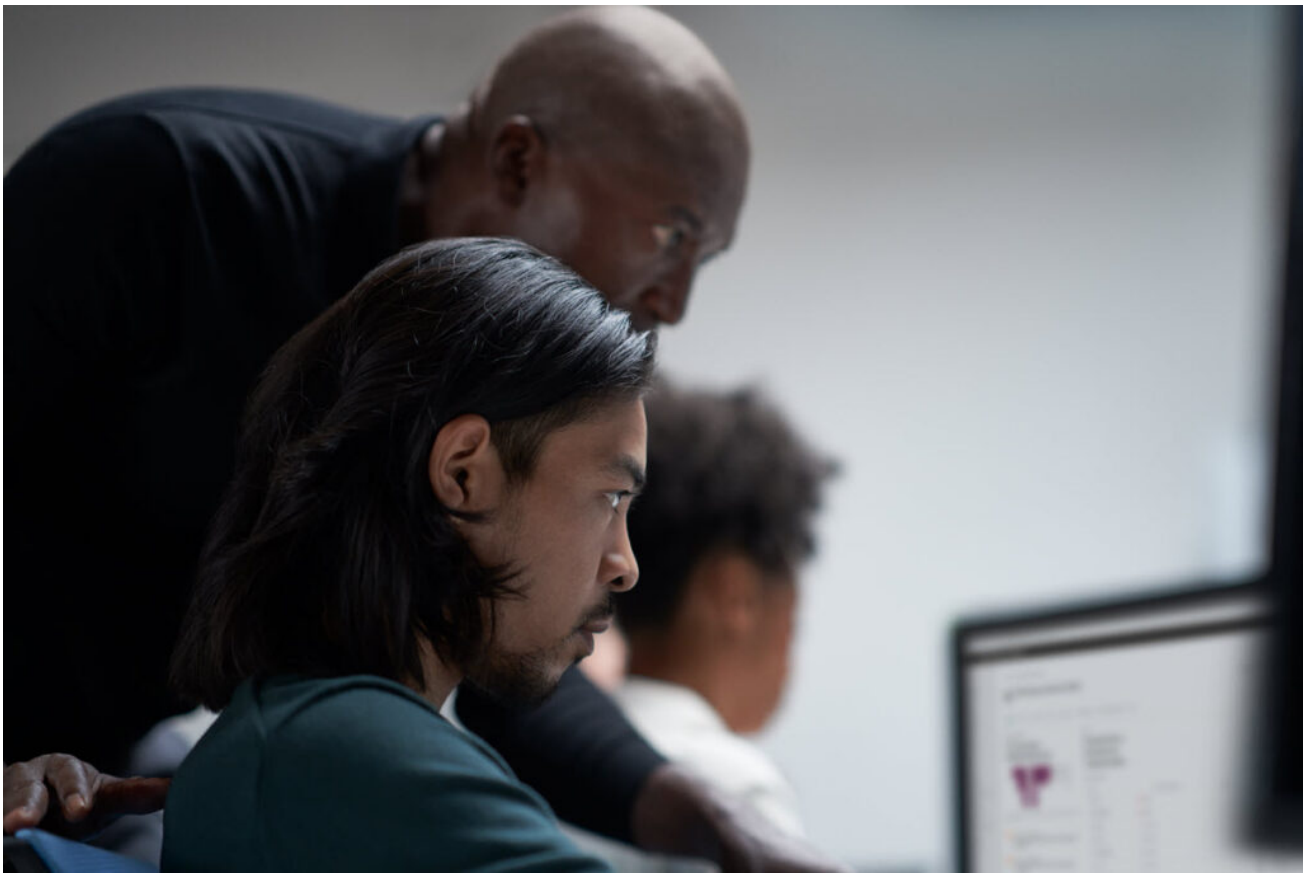
Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets

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

September 14, 2023

Skip to main content



By

Since February 2023, Microsoft has observed password spray activity against thousands of organizations carried out by an actor we track as Peach Sandstorm (HOLMIUM). Peach Sandstorm is an Iranian nation-state threat actor who has recently pursued organizations in the satellite, defense, and pharmaceutical sectors around the globe. Based upon the profile of victim organizations targeted and the observed follow-on intrusion activity, Microsoft assesses that this initial access campaign is likely used to facilitate intelligence collection in support of Iranian state interests.

In cases where Peach Sandstorm successfully authenticated to an account, Microsoft observed the group using a combination of publicly available and custom tools for discovery, persistence, and lateral movement. In a small number of intrusions, Peach Sandstorm was observed exfiltrating data from the compromised environment.

Given the volume of activity, ongoing attempts to access targets of interest, and risks associated with post-compromise activity, Microsoft is reporting on this campaign to raise awareness of recent Peach Sandstorm tradecraft and empower organizations to harden their attack surfaces and defend against this activity. As with any observed nation state actor activity, Microsoft directly notifies customers that have been targeted or compromised by Peach Sandstorm and provides them with the information they need to secure their accounts.

Who is Peach Sandstorm?

Peach Sandstorm is an Iranian nation-state group known to target organizations in multiple countries. In past attacks, Peach Sandstorm has pursued targets in the aviation, construction, defense, education, energy, financial services, healthcare, government, satellite, and telecommunications sectors. Activity that Microsoft attributes to Peach Sandstorm overlaps with public reporting on groups known as APT33, Elfin, and Refined Kitten.

Throughout 2023, Peach Sandstorm has consistently demonstrated interest in organizations in the satellite, defense, and to a lesser extent, pharmaceutical sectors. In the initial phase of this campaign, Peach Sandstorm conducted password spray campaigns against thousands of organizations across several sectors and geographies. While Microsoft observed several organizations previously targeted by Peach Sandstorm, the volume of activity and range of organizations suggests that at least a subset of the initial activity is opportunistic.

In past operations, Peach Sandstorm relied heavily, but not exclusively, on password spray attacks as a means of gaining access to targets of interest. In some cases, Peach Sandstorm has used this tradecraft to compromise an intermediate target and enable access to downstream environments. As one example, Peach Sandstorm carried out a wave of attacks in 2019 that coincided with a rise in tensions between the United States and the Islamic Republic of Iran.

Unlike password spray operations which are noisy by definition, a subset of Peach Sandstorm's 2023 post-compromise activity has been stealthy and sophisticated. Many of the cloud-based tactics, techniques, and procedures (TTPs) seen in these most recent campaigns are materially more sophisticated than capabilities used by Peach Sandstorm in the past.

Intrusion chain

Microsoft observed Peach Sandstorm using two distinct sets of TTPs in the early stages of the intrusion lifecycle in 2023 attacks. In later stages of known compromises, the threat actor used different combinations from a set of known TTPs to drop additional tools, move laterally, and ultimately exfiltrate data from a target.

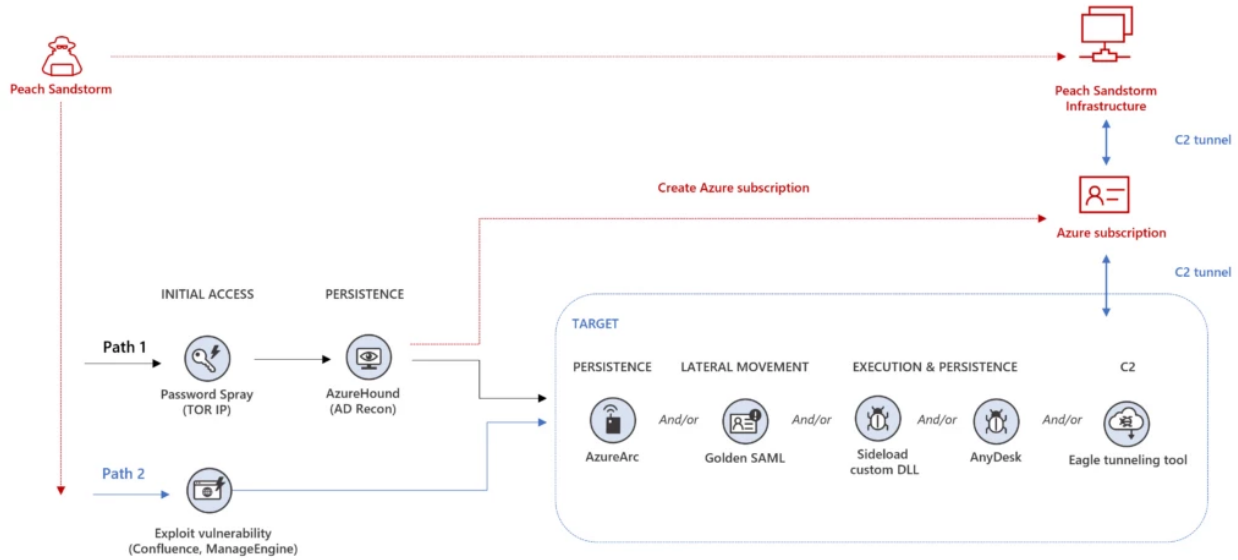


Figure 1. Peach Sandstorm 2023 tradecraft

Path 1: Password spray activity, internal reconnaissance with AzureHound or Roadtools, and multiple persistence mechanisms

Password spray activity

Between February and July 2023, Peach Sandstorm carried out a wave of password spray attacks attempting to authenticate to thousands of environments. Password spraying is a technique where threat actors attempt to authenticate to many different accounts using a single password or a list of commonly-used passwords. Unlike brute force attacks that target a single account using many passwords, password spray attacks help adversaries maximize their chances for success and minimize the likelihood of automatic account lockouts.

Even a single compromised account could allow an adversary to conduct reconnaissance, move laterally, or access sensitive resources, often without attracting attention from defenders.

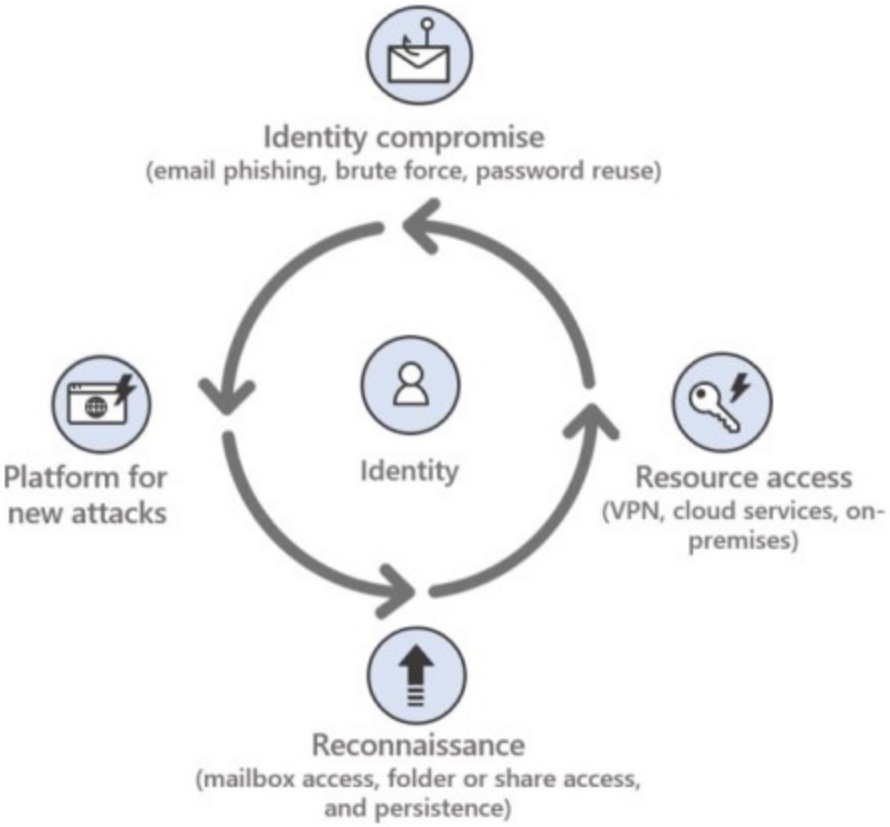


Figure 2. Identity attack lifecycle

Long-running password spray campaigns offer insight into adversaries' pattern of life. Activity observed in this campaign aligned with an Iranian pattern of life, particularly in late May and June, where activity occurred almost exclusively between 9:00 AM and 5:00 PM Iran Standard Time (IRST). While Peach Sandstorm has carried out high-volume password spray campaigns in the past, elements of the most recent campaign were unique. Specifically, Peach Sandstorm consistently conducted the password sprays from *TOR IPs* and used a *"go-http-client"* user agent.

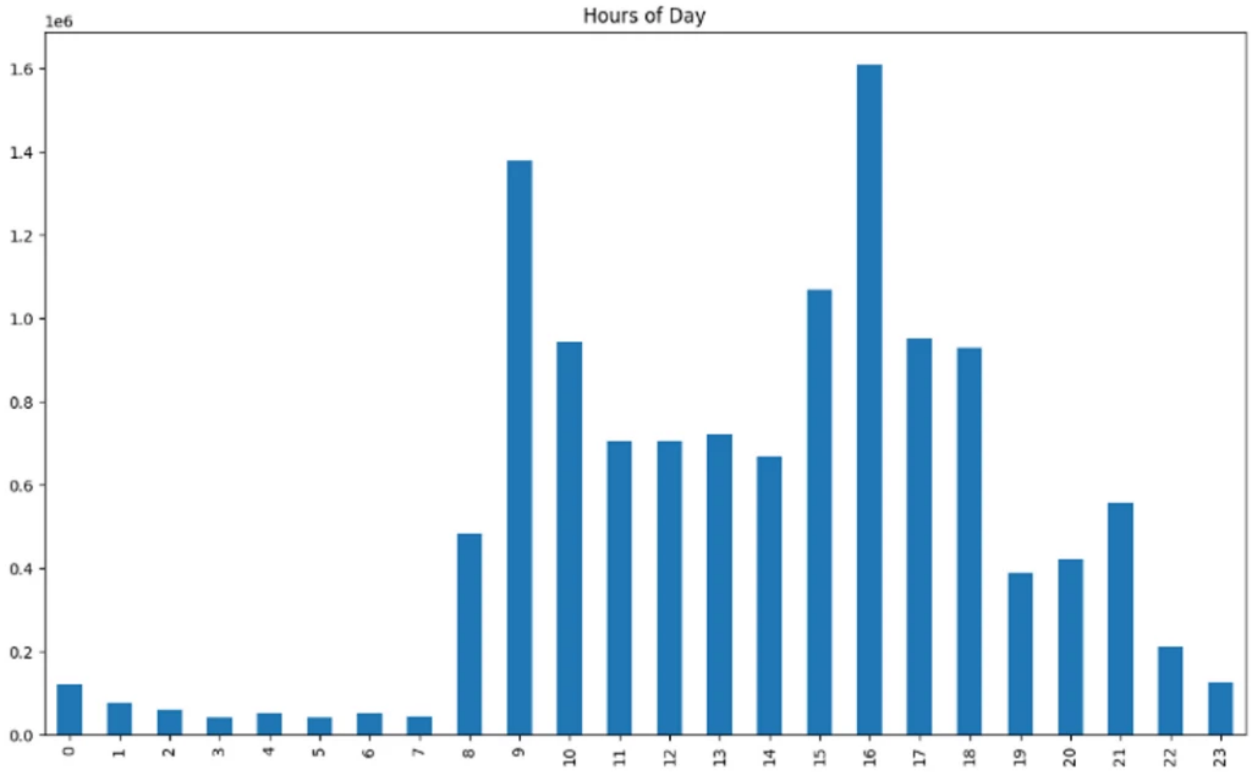


Figure 3. Peach Sandstorm authentication attempts by hour (April-July 2023)

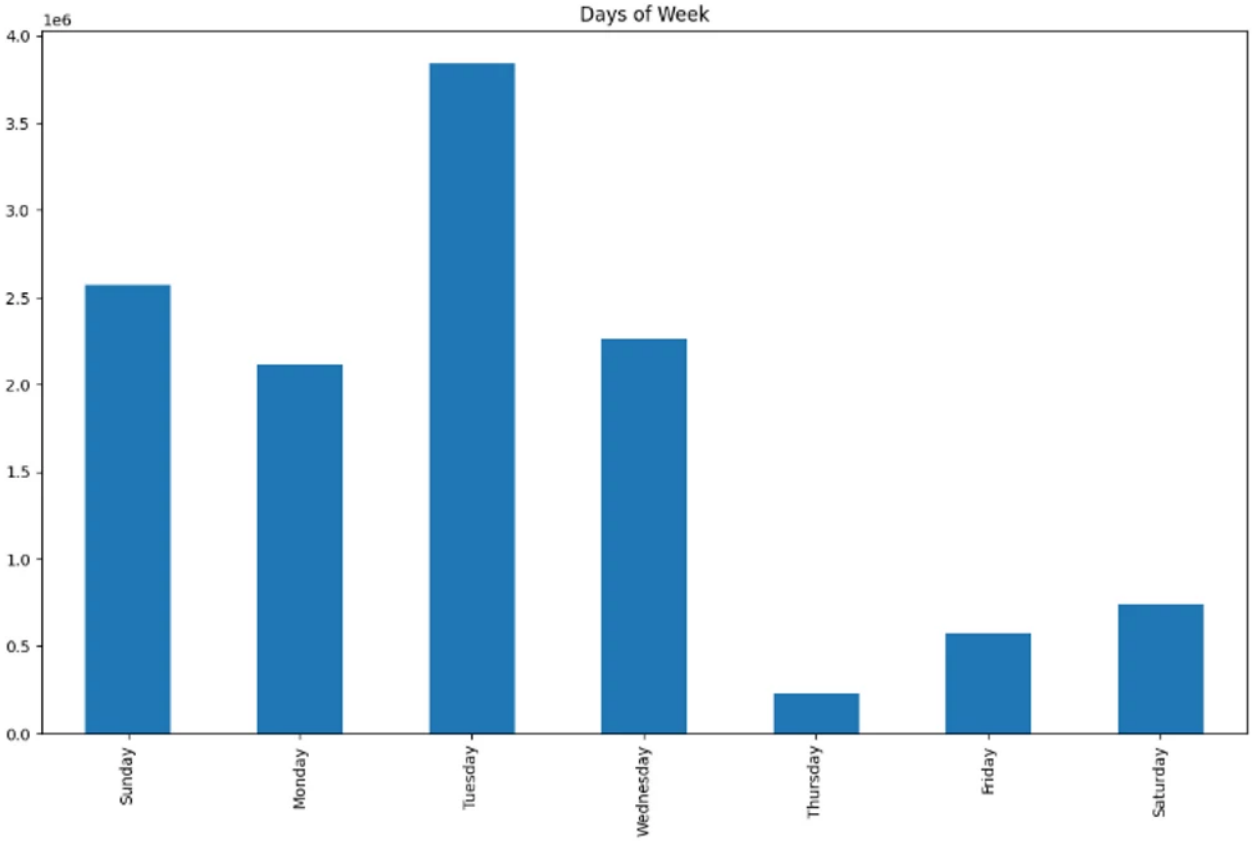


Figure 4. Peach Sandstorm authentication attempts by day of the week (April-July 2023)

Internal reconnaissance with AzureHound or Roadtools

In a small subset of instances where Peach Sandstorm successfully authenticated to an account in a targeted environment, Microsoft observed the threat actor using AzureHound or Roadtools to conduct reconnaissance in Microsoft Entra ID (formerly Azure Active Directory). In this campaign, Peach Sandstorm used AzureHound, a Go binary that collects data from Microsoft Entra ID and Azure Resource Manager through the Microsoft Graph and Azure REST APIs, as a means of gathering information on a system of interest. Similarly, Roadtools, a framework to access Microsoft Entra ID, allowed Peach Sandstorm to access data in a target's cloud environment and conveniently dump data of interest to a single database.

AzureHound and Roadtools have functionality that is used by defenders, red teams, and adversaries. The same features that make these tools useful to legitimate users, like pre-built capabilities to explore and seamlessly dump data in a single database, also make these tools attractive options for adversaries seeking information about or from a target's environment.

Multiple persistence mechanisms

In cases where Microsoft observed this particular intrusion chain, the threat actor used one or more persistence mechanisms. In some cases, Peach Sandstorm created a new Azure subscription on a target's tenant and/or leveraged previously compromised Azure resources. These subscriptions were subsequently used to facilitate communication with Peach Sandstorm's infrastructure.

Peach Sandstorm also abused Azure Arc, a capability that allows users to secure, develop, and operate infrastructure, applications, and Azure services anywhere, to persist in compromised environments. In this campaign, Peach Sandstorm installed the Azure Arc client on a device in the compromised environment and connected it to an Azure subscription controlled by Peach Sandstorm. This effectively allowed Peach Sandstorm to control devices in a target's on-premises environment from Peach Sandstorm's cloud.

Path 2: Remote exploitation of vulnerable internet-facing applications

Initial access using remote exploitation

In this wave of activity, Peach Sandstorm also attempted to exploit vulnerabilities with a public proof-of-concept (POC) in Zoho ManageEngine or Confluence, to access targets' environments.

- CVE-2022-47966 is a remote code execution vulnerability affecting a subset of on-premises Zoho ManageEngine products. Microsoft recommends organizations using vulnerable applications patch this vulnerability as multiple groups have been observed exploiting this vulnerability.

- CVE-2022-26134 is a remote code execution vulnerability in Confluence Server and Data Center. Recommendations that help organizations protect against exploitation of multiple vulnerabilities, including CVE-2022-26134, can be found in the recommendations section of this report.

Post-compromise activity

The following post-compromise activity affected organizations in the defense, satellite, and pharmaceutical sectors:

In a subset of intrusions in this campaign, Peach Sandstorm deployed AnyDesk, a commercial remote monitoring and management tool (RMM) to maintain access to a target. AnyDesk has a range of capabilities that allow users to remotely access a network, persist in a compromised environment, and enable command and control (C2). The convenience and utility of a tool like AnyDesk is amplified by the fact that it might be permitted by application controls in environments where it is used legitimately by IT support personnel or system administrators.

In a March 2023 intrusion, Peach Sandstorm conducted a Golden SAML attack to access a target's cloud resources. In a Golden SAML attack, an adversary steals private keys from a target's on-premises Active Directory Federated Services (AD FS) server and use the stolen keys to mint a SAML token trusted by a target's Microsoft 365 environment. If successful, a threat actor could bypass AD FS authentication and access federated services as any user.

In at least one intrusion, Microsoft observed Peach Sandstorm using a legitimate VMWare executable to carry out a search order hijack. DLL search order hijacking allows adversaries to introduce malicious code into an environment in a way that blends in with normal activity.

In a handful of environments, Microsoft observed Peach Sandstorm using EagleRelay to tunnel traffic back to their infrastructure. In these instances, Peach Sandstorm created a new virtual machine in a compromised Azure subscription. These virtual machines were used to run EagleRelay, a custom tool, to tunnel traffic between actor-controlled systems and targets' systems. In at least one case, Microsoft also saw Peach Sandstorm attempting to move laterally in a compromised environment using remote desktop protocol (RDP).

Additional context

The capabilities observed in this campaign are concerning as Microsoft saw Peach Sandstorm use legitimate credentials (gleaned from password spray attacks) to authenticate to targets' systems, persist in targets' environments, and deploy a range of tools to carry out

additional activity. Peach Sandstorm also created new Azure subscriptions and leveraged the access these subscriptions provided to conduct additional attacks in other organizations' environments. While the specific effects in this campaign vary based on the threat actor's decisions, even initial access could adversely impact the confidentiality of a given environment. Microsoft continues to work across its platforms to identify abuse, take down malicious activity, and implement new proactive protections to discourage malicious actors from using our services. We encourage customers and the industry to report abuse.

As Peach Sandstorm increasingly develops and uses new capabilities, organizations must develop corresponding defenses to harden their attack surfaces and raise costs for these attacks. Microsoft will continue to monitor Peach Sandstorm activity and implement robust protections for our customers.

Mitigations

To harden an attack surface against Peach Sandstorm activity, defenders can implement the following:

- Reset account passwords for any accounts targeted during a password spray attack. If a targeted account had system-level permissions, further investigation may be warranted.
- Revoke session cookies in addition to resetting passwords
  Revoke any multifactor authentication (MFA) setting changes made by the attacker on any compromised users' accounts
  Require re-challenging MFA for MFA updates as the default
- Implement the Azure Security Benchmark and general best practices for securing identity infrastructure, including:
  - Create conditional access policies to allow or disallow access to the environment based on defined criteria.
  - Block legacy authentication with Microsoft Entra ID by using Conditional Access. Legacy authentication protocols don't have the ability to enforce MFA, so blocking such authentication methods will prevent password spray attackers from taking advantage of the lack of MFA on those protocols.
  - Enable AD FS web application proxy extranet lockout to protect users from potential password brute force compromise.

- Secure accounts with credential hygiene:
    - Practice the principle of least privilege and audit privileged account activity in your Microsoft Entra ID environments to slow and stop attackers.
    - Deploy Microsoft Entra ID Connect Health for Active Directory Federation Services (AD FS). This captures failed attempts as well as IP addresses recorded in AD FS logs for bad requests in the *Risky IP report*.
    - Use Microsoft Entra ID password protection to detect and block known weak passwords and their variants.
    - Turn on identity protection in Microsoft Entra ID to monitor for identity-based risks and create policies for risky sign ins.
- Use MFA to mitigate successful password spray attacks. Keep MFA always-on for privileged accounts and apply risk-based MFA for normal accounts.
- Consider transitioning to a passwordless primary authentication method, such as Azure MFA, certificates, or Windows Hello for Business.
- Secure RDP or Windows Virtual Desktop endpoints with MFA to harden against password spray or brute force attacks.

Securing critical assets like AD FS servers is a high-value measure to protect against golden SAML attacks. The guidance provided below is applicable beyond just Peach Sandstorm activity and can help organizations harden their attack surfaces against a range of threats.

- It's critical to treat your AD FS servers as a Tier 0 asset, protecting them with the same protections you would apply to a domain controller or other critical security infrastructure. AD FS servers provide authentication to configured relying parties, so an attacker who gains administrative access to an AD FS server can achieve total control of authentication to configured relying parties (include Microsoft Entra ID tenants configured to use the AD FS server).
- Practicing credential hygiene, notably the recommendations provided above, is critical for protecting and preventing the exposure of highly privileged administrator accounts. This especially applies on more easily compromised systems like workstations with controls like logon restrictions and preventing lateral movement to these systems with controls like the Windows Firewall.
- Migration to Microsoft Entra ID (formerly Azure Active Directory) authentication is recommended to reduce the risk of on-premises compromises moving laterally to your authentication servers. Customers can use the following references on migration:
    Use the activity report to move AD FS apps to Microsoft Entra ID
    Move application authentication to Microsoft Entra ID

Indicators of compromise

Indicator	Type	Description
192.52.166[.]76	IP address	Peach Sandstorm adversary IP
108.62.118[.]240	IP address	Peach Sandstorm adversary IP
102.129.215[.]40	IP address	Peach Sandstorm adversary IP
76.8.60[.]64	IP address	Peach Sandstorm adversary IP

Detection details

Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate Peach Sandstorm activity on your network:

> Peach Sandstorm actor activity detected

Microsoft Defender for Identity

The following alerts might indicate activity associated with password spray campaigns.

- Password Spray
- Atypical travel
- Unfamiliar Sign-in properties

Microsoft Defender for Cloud Apps

The following alerts might indicate activity associated with password spray campaigns.

- Activity from a Tor IP address
- Suspicious Administrative Activity
- Impossible travel activity
- Multiple failed login attempts
- Activity from a password-spray associated IP address

Organizations with Defender for Cloud Apps can turn on app governance, a set of security and policy management capabilities designed for OAuth-enabled apps registered on Azure Active Directory, Google, and Salesforce. The following detections in App governance might indicate activity associated with password spray campaigns.

- Numerous Azure AD enumeration calls using PowerShell
- Suspicious enumeration activities performed using AAD PowerShell

Hunting queries

Microsoft Sentinel

Microsoft customers can use a range of Microsoft Sentinel content to help detect Peach Sandstorm activity described in this blog. The Azure Active Directory solution contains several analytics rules and hunting queries for Microsoft Entra ID data that can help uncover initial access activity including password sprays. Specific analytics rules of value include:

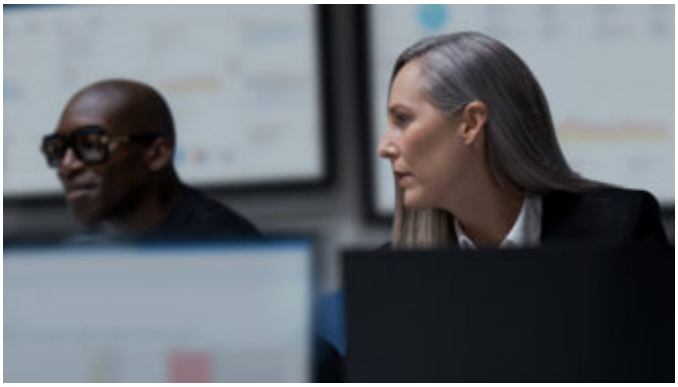
References

Further reading

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

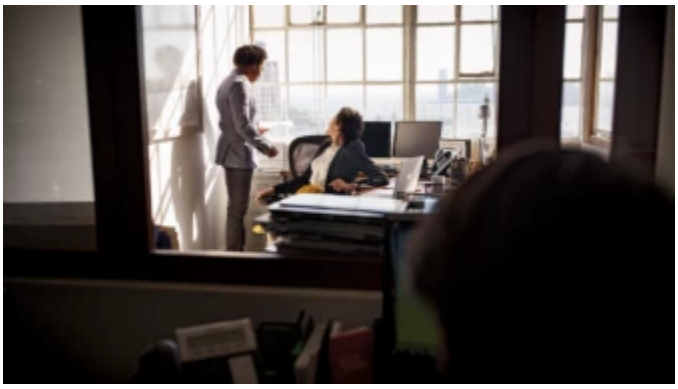
To get notified about new publications and to join discussions on social media, follow us on Twitter at https://twitter.com/MsftSecIntel.

Related Posts



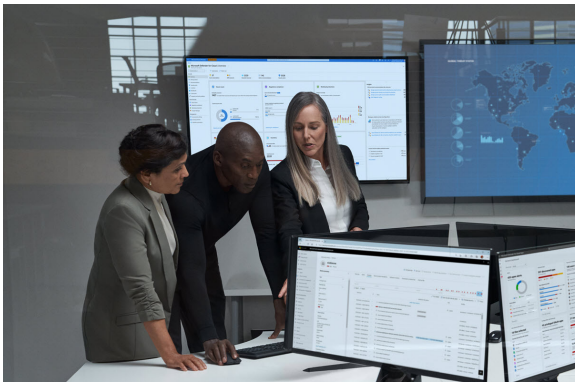
Flax Typhoon using legitimate software to quietly access Taiwanese organizations

China-based actor Flax Typhoon is exploiting known vulnerabilities for public-facing servers, legitimate VPN software, and open-source malware to gain access to Taiwanese organizations, but not taking further action.



Midnight Blizzard conducts targeted social engineering over Microsoft Teams

Microsoft Threat Intelligence has identified highly targeted social engineering attacks using credential theft phishing lures sent as Microsoft Teams chats by the threat actor that Microsoft tracks as Midnight Blizzard (previously tracked as NOBELIUM).



Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets

Today, Microsoft is reporting on a distinct subset of Mint Sandstorm (formerly known as PHOSPHORUS), an Iranian threat actor that specializes in hacking into and stealing sensitive information from high-value targets. This subset is technically and operationally mature, capable of developing bespoke tooling and quickly weaponizing recently disclosed vulnerabilities.