Research Incident response Microsoft Entra Cloud threats
28 min read

Microsoft Incident Response lessons on preventing cloud identity compromise

By Microsoft Incident Response

December 5, 2023

Threat intelligence

Microsoft Entra ID

Microsoft Incident Response

Microsoft Security Experts

Token theft

Microsoft observed a surge in cyberattacks targeting identities in 2023, with attempted password-based attacks increasing by more than tenfold in the first quarter of 2023 compared to the same period in 2022. Threat actors leverage compromised identities to achieve a significant level of access to target networks. The compromise of an identity, under certain circumstances, could enable threat actors to compromise the identity platform instance and could lead to additional malicious attacks, or even tenant destruction. Microsoft Incident Response (IR) is often engaged in cases where organizations have lost control of their Microsoft Entra ID (previously Azure Active Directory) tenant, due to a combination of misconfiguration, administrative oversight, exclusions to security policies, or insufficient protection for identities.

The team has observed common misconfigurations for both Microsoft Entra ID and on-premises Active Directory across various industry verticals. While Microsoft Entra ID differs from on-premises Active Directory in how it functions and how it is architected, similar high-level incident response and hardening principles can be applied to both. Concepts such as administrative least privilege, regularly reviewing access and application permissions and reviewing activity are important to secure both Active Directory and Microsoft Entra ID.

Microsoft IR engages with hundreds of customers each year, including many of the largest organizations worldwide. These organizations can have hundreds of thousands to millions of active users of Microsoft Entra ID and incredibly complex identity systems. In this blog, we present details on the common misconfigurations observed in these engagements and provide guidance on how to properly configure Microsoft Entra ID to remove risks and harden environments against cyberattacks. This blog is designed to be a Microsoft Entra ID companion piece to a previously published Microsoft IR blog on lessons learned on securing on-premises Active Directory.

- Excessive privilege granted to users
- Excessive privilege granted to workload identities
- Poor device access control
- Poor application access control
- Misconfigured delegated administrative privileges (DAP) permissions
- Misconfigured Conditional Access policy
- OAuth and consent phishing
- Self-service password reset & MFA social engineering
- Recommended focus areas to prevent identity compromise

To understand a compromise incident and aid in investigations, Microsoft IR retrieves the configuration of Microsoft Entra ID by reading tenant metadata from the Microsoft Graph API. This data is used to both investigate threat actor activity and to aid in providing recommendations for securing Microsoft Entra ID. In addition to configuration metadata, we also leverage native cloud forensic log sources such as Microsoft Entra ID sign-in and audit data – these data sources are available to any organization using Microsoft Entra ID. Open-source tools such as the Microsoft Entra ID Response PowerShell module, developed in conjunction with the Microsoft Entra ID product group, or the untitled goose tool from CISA can retrieve this same data.

Additionally, Microsoft IR uses Microsoft 365 Defender advanced hunting data such as log data from Microsoft Defender for Cloud Apps, and any other relevant log sources a customer may have. In cases of hybrid identity, logs from systems such as Active Directory Federation Services (AD FS) or third-party multifactor authentication (MFA) providers are also relevant. Depending on the nature of the investigation, traditional endpoint forensic sources may also need to be examined.

Misconfigured hybrid identity setups

In the following sub-sections, we present details on the different scenarios involving misconfigured hybrid identity setups that could lead to compromise of Microsoft Entra ID.

Compromised Active Directory Federation Services or equivalent federated identity systems

Each organization's hybrid identity configuration is unique, and many organizations use a federated identity provider when users authenticate to cloud apps, such as Microsoft 365. These federated identity providers enable user authentication. While a significant percentage of organizations have now moved to cloud-native authentication in Microsoft Entra ID, these federated identity providers, such as AD FS and other third-party identity providers, are still in use.

Microsoft IR finds that federated identity providers present an administrative blind spot within organizations. Hybrid identity can be architecturally complicated with many moving pieces, which often lends itself to operational oversight. Securing these hybrid identity systems is complex, especially legacy solutions, and a single misconfiguration can lead to a significant compromise of an organization's entire identity plane.

Federated identity providers are a favored target of some nation-state actors: these threat actors understand that if they can compromise the Tier 0 identity plane, then they can persist undetected within an environment for extended periods of time and take control of all identities. Microsoft has published blogs covering the sophisticated cyberattacks seen against AD FS, such as MagicWeb. A deep dive into this tactic was also covered in the Microsoft IR Cyberattack series.

Microsoft IR has also been engaged in multiple incidents where the Token Signing Certificate (TSC) was stolen from on-premises federation servers. Using this stolen certificate, attackers could forge their own SAML tokens and authenticate successfully to Microsoft Entra ID. With this certificate, a threat actor can successfully authenticate as any user in the tenant with any claims without requiring the user's credentials.

Recommendations

- Microsoft IR strongly recommends moving to native Microsoft Entra ID authentication and decommissioning AD FS (or other federated identity providers) where possible. This reduces the overall complexity of the organization's identity plane and makes it easier to secure identities.
- If you must use federated identity providers, it's important to secure and monitor them appropriately.
    - For organizations using AD FS, ensure that the Microsoft Entra Connect Health client is installed. This client correlates multiple Event IDs from AD FS and enriches Microsoft Entra ID sign-in data with that information. This can both help with creating detection and threat hunting rules and serve as a valuable source of forensic data in the event of a

compromise.Ensure that appropriate logging is enabled for AD FS and those logs are sent to a SIEM such as Microsoft Sentinel, where detection rules can be created, for both user and system-level compromise, including certificate theft. If an attacker can steal the token signing certificate from AD FS, they can forge their own tokens to authenticate to Entra ID. In these cases, Entra ID will alert on anomalies with the token issuer. Additionally, sign ins using forged tokens may trigger other risk events such as unfamiliar features.If your current MFA solution is integrated to AD FS, consider using native integrated MFA, especially phishing-resistant, options available in Entra ID

    - For organizations with Microsoft Defender for Identity and Microsoft Defender for Endpoint, ensure the agents are deployed to AD FS. Both products have specific capabilities to detect cyberattacks against AD FS.
- For other federated identity providers, ensure those services are configured in line with best practices and that both user logon telemetry and system-level audit events are sent to a central SIEM. Threat actors can dwell in environments, especially identity systems, for months or years before being detected, so it is important that key logs are kept for a long period of time. This helps responder teams understand how initial access was gained and ensure complete threat actor eviction from the environment.

Complex identity systems

Modern identity systems are complex and have changed significantly as ways of working have evolved. Organizations can have multiple identity providers, third-party MFA providers, custom systems designed for user onboarding and offboarding, and other interconnected systems. All these systems form an end-to-end trust chain that is an attractive target for threat actors. The more complex these systems are, the more difficult it is to adequately secure them. Organizations may have network appliances that complete 802.1x authentication, custom identity governance systems that manage user lifecycle, certificate authorities and HSM devices. Each system requires patching and vulnerability management, sufficient monitoring and maintenance and human expertise to ensure secure configuration. Additionally, certificate and credential management across these systems add further complexity.

For example, AD FS is trusted to issue tokens for users. Other systems, such as Microsoft Entra ID, accept those tokens and then authorize the users they represent. If AD FS is compromised, then the legitimacy of those tokens is in question. Each system needs to be adequately secured and monitored to ensure complete trust, as a compromise of a single system could lead to compromise of them all.

Figure 1. Example of a modern hybrid identity plane

If a user signs into Microsoft 365 and the authentication is via a non-Microsoft identity provider, and then MFA is provided by yet another provider, significant complexity is added to the authentication flow. For instance, different systems may be responsible for validating passwords, checking certificates, performing MFA, and issuing tokens – these may be on-premises systems, non-Windows platforms, or third-party cloud solutions. In these situations, each system that forms part of this authentication flow trusts the others.

For example, Microsoft IR was recently engaged with an organization that suffered tenant-level compromise of Microsoft Entra ID. Once the investigation was complete, it was determined that an internet-facing on-premises server, which lacked MFA or proper access controls, had been compromised. That server ran a custom piece of software designed to sync users between multiple business systems. Once the threat actor gained access to the server, they uncovered the credentials for a Global Administrator-level service account. Servers that host key identity applications and integration services are often not held to the same security standard as Domain Controllers, decreasing the security posture of the entire identity plane significantly.

Misconfiguration or administrative oversight on any one of these interconnected systems leads to a decrease in overall security controls. If Microsoft Entra ID is configured to offload MFA to a third-party MFA provider and that MFA is misconfigured, Microsoft Entra ID will still trust the telemetry and configuration of that service.

Recommendations

- It's crucial to understand all the systems that form your identity plane and how authentication and authorization flow between them. Understand which systems are responsible for which workloads within your identity trust chain.
- Treat the entire authentication system as tier 0, as compromise of a single link within it can lead to complete compromise.
- Ensure that all systems are configured in line with best practices and that the collective configuration is enforcing implemented policies as expected.
- For all systems forming your identity plane, ensure that sufficient logging is available, and that data is kept for a long period

of time, preferably 2 years or more. Logging should include user logon events, administrative activity, and configuration changes. Having sufficient logging not only helps detect potential cyberattacks, but it can also alert on changes to any individual system that can reduce overall security posture, and, in the event of an incident, serve as a source of forensic information.
- Where possible, simplify the authentication and authorization mechanisms in your environment. This helps to reduce the attack surface of identity compromise. With each additional system, you increase the overhead of securing those systems and increase the chance of misconfiguration or compromise of one of them.

Compromised synced service accounts

In the hybrid identity world, most users and groups are synced from on-premises Active Directory to Microsoft Entra ID. This is required to allow users to access cloud resources via the same set of credentials used on premises. However, in engagements seen by Microsoft IR, accounts used to manage Microsoft Entra ID, such as Global Administrators, have also been synced to Microsoft Entra ID from on-premises. Staff then often use the same credentials to manage both environments.

If Active Directory is compromised and the credentials for these accounts are found by a threat actor, this allows them to easily pivot into Microsoft Entra ID, expanding the scope of the compromise. Synced service accounts are particularly vulnerable to exploitation. Microsoft IR commonly sees service accounts used to manage both on-premises Active Directory and Microsoft Entra ID targeted by threat actors. These accounts generally hold a high level of privilege in Microsoft Entra ID (often Global Administrator) but aren't subject to the same controls such as MFA or Microsoft Entra Privileged Identity Management (PIM).

Microsoft IR has been involved in numerous investigations where on-premises Active Directory compromise led to Microsoft Entra tenant compromise. Threat actors sometimes uncover account credentials in clear text due to poor handling of credentials in an on-premises environment. If the threat actor already has a foothold in the on-premises environment, controls such as MFA are often not enforced as these networks are seen as 'trusted'.

Recommendations

- Microsoft IR strongly recommends that accounts used to administer Microsoft Entra ID are native to Microsoft Entra ID using managed authentication and are not synced from on-premises Active Directory. This reduces the scope of compromise if Active Directory gets compromised by preventing a threat actor from leveraging the same credentials to compromise Microsoft Entra ID. Specific guidance to protect Microsoft 365 from on-premises cyberattacks can be found at https://aka.ms/protectm365 and https://aka.ms/securitysteps.
- Any account that holds privilege in on-premises Active Directory, such as Domain Administrators and the respective groups such as Domain Admins, should be completely excluded from being synced to Microsoft Entra ID.
- The credentials for service accounts that interact with Microsoft Entra ID and Active Directory should be stored securely, and not in clear text where they are easily recoverable by a threat actor.
- Privileged accounts should not be excluded from Microsoft Entra Conditional Access policies, regardless of network location. These accounts should always be held to the highest standards of security, specifically the use of Privileged Identity Management and phishing-resistant credentials such as FIDO2, including for break glass accounts.
- Service accounts that require both privileges to on-premises Active Directory and Microsoft Entra ID should have specific technical controls applied to them. This can include Conditional Access blocking access from non-approved locations or IP addresses, specific detection rules, and monitoring to alert on anomalous activity with these accounts.

Token theft of highly privileged accounts

Token theft is an increasingly common tactic used by threat actors. This technique can allow threat actors to access even MFA-protected resources. Token theft utilizes either credential stealing malware, to steal tokens from end user devices, or adversary-in-the-middle (AiTM) infrastructure to steal tokens during authentication.

AiTM attacks are targeted at users through phishing campaigns. Users are tricked to not only enter their user credentials to a malicious site, but the malicious site also steals the tokens associated with the sign in. These tokens have already satisfied MFA and can be reused by the adversary. This token is then imported to a threat actor-controlled device and access to MFA protected resources granted. Microsoft IR has previously written on the increase of token theft attacks.

Figure 2. Overview of adversary-in-the-middle token theft

Microsoft IR has seen cases where Global Administrator accounts were directly targeted by AiTM phishing. As result, a Global Administrator tier token was stolen, leading to tenant-level compromise.

In addition to AiTM phishing, tokens can also be stolen from endpoint devices themselves via credential-stealing malware. Microsoft IR has been engaged with organizations where credential-stealing malware was installed on an administrator's endpoint device via an initial phishing email. While the admin used separate accounts for their day-to-day and administrative work, the Global Administrator had signed into both accounts from the same device. The malware had the capability to extract all the credentials and tokens on the device, eventually leading to tenant-level compromise.

Tokens on endpoints are typically stored as cookies, and theft can occur in several ways. Commodity malware such as Emotet, Redline, IcedID, and others have the capability to steal both credentials and tokens. Pirated or cracked software often has token and cookie stealing malware embedded within it as well.

Figure 3. Example of token theft via installed malware

Recommendations

- To increase the security of these accounts, phishing-resistant MFA methods such as FIDO2 keys and certificate-based authentication should be used. Authentication strengths can be used to enforce these MFA methods for the highest privileged accounts. Authentication strengths can prevent admins using weaker MFA methods, such as SMS or phone calls.
- To remove the attack vector of direct phishing attempts, users that hold privilege in Microsoft Entra ID should not have a mailbox assigned.
- When accessing Microsoft Entra ID to complete administrative tasks, access should be granted via a native Microsoft Entra account, not one synced from on-premises Active Directory.
- Access to the Microsoft Entra ID Portal and other similar management interfaces should also be restricted to only hardened workstations known as privileged access workstations. These workstations are designed to only administer Microsoft Entra ID and restricted from accessing other sites to reduce the attack surface of endpoint compromise.
- Microsoft has published a specific incident response playbook for cloud token theft. It is worth familiarizing yourself with to understand how to respond quickly.
- To prevent token theft more broadly, token protection (also known as token binding more generally) is currently in preview in Microsoft Entra Conditional Access. As a preview feature, it has certain limitations; however, it is still a valuable control. Token protection seeks to prevent replay of primary refresh token theft by binding an issued token to a specific device.

Excessive privilege granted to users

Much like on-premises Active Directory, Microsoft IR often sees accounts granted privilege that they do not require. While organizations often have mature technical controls over their Global Administrator accounts, these controls do not cover other privileged roles in Microsoft Entra ID. Global Administrator lives atop the privilege hierarchy, but there are also other roles that can lead to compromise. These include, but are not limited to:

- Privileged Role Administrator – can add users to Global Administrator and other privileged roles
- Privileged Authentication Administrator – can reset the password of or register MFA for a Global Administrator
- Security Administrator – can read and manage security related settings across Microsoft Entra ID and Microsoft 365 Defender
- Application Administrator – can generate a credential on any Microsoft Entra ID application
- Domain Name Administrator – can add a federated domain
- Conditional Access Administrator – can degrade access conditions
- Intune Administrator – can manage all aspects of Intune, including deploying software and remote wiping devices

These roles, along with others, are now flagged as privileged in the Microsoft Learn documentation, allowing organizations to focus on securing users that hold those roles. In many of our engagements, Global Administrators are not directly compromised. A user holding another privileged role is often initially targeted, and from there, the threat actor could escalate up to Global Administrator. In one instance, a service desk staff member who held the Privileged Authentication Administrator role was socially engineered into updating the MFA details for a Global Administrator. Once this had occurred, the threat actor completed self-service password reset for the Global Administrator account and then took control of the tenant.

Recommendations

- Microsoft IR recommends that organizations audit current role assignments to ensure privileged users are granted only the access required– enforcing least privilege to organizational resources. Roles that Microsoft considers privileged are now highlighted in the documentation, and in the Microsoft Entra portal itself – highlighting the importance of managing users in these roles.
- Ensure that all roles that could lead to tenant-level compromise are protected, not just Global Administrator. Changes to these roles should generate a high-priority alert to be investigated to confirm the activities are not malicious.
- AzureHound, the cloud sibling of BloodHound, can be used to visually map attack paths through Microsoft Entra ID. It is recommended that sanctioned audits using this tool are run and attack paths are removed or mitigated.
- Microsoft Entra PIM can provide further protection to these roles by ensuring users have just-in-time access to their roles and requesting that access is governed by additional workflows.

Excessive privilege granted to workload identities

A workload identity is a non-human identity created and assigned to a workload (such as a script, application, or other services) to allow them to authenticate and access other resources. For example, you may create a workload identity to provide custom integration between Microsoft Teams and Exchange Online. In Microsoft Entra ID, these are known as applications and service principals. Like users, these applications and service principals can be assigned to roles, such as Global Administrator, or provided specific access to API endpoints. Credentials like secrets or certificates are generated for the workload identity, and then used to authenticate.

Like service accounts in on-premises Active Directory, these workload identities are often granted much higher privileges than required, for example:

- Directory.ReadWrite.All – Allows the app to read and write data in your organization's directory, such as users, and groups
- User.ReadWrite.All – Allows the app to read and write the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user
- Mail.ReadWrite – Allows the app to create, read, update, and delete mail in all mailboxes without a signed-in user

Even though the applications ask for and are subsequently granted access to these broad privileges, usually the applications require much less access to function correctly. For instance, they may need access to a specific mailbox, not all mailboxes. Microsoft has published specific guidance to understand appropriate permission scoping in Microsoft Entra ID.

These service principals and applications are often not secured to the same level as standard user accounts. Part of that is the nature of how they work: it is not possible to configure MFA for these applications, as they are non-human identities. Additionally, where a user may notice strange behavior on their account and provide feedback to security teams, there is no equivalent feedback for applications. Often, malicious activity from workload identities goes unnoticed because detection logic is focused on user identities.

Recommendations

- Applications and service principals should be granted access using the least-privilege principle. Often internal development teams or external third-party vendors request privileges over and above what are required because they make it easier for the service to work. However, this presents a significant risk and should be avoided.
- Microsoft recommends the use of strong credentials, such as certificates, for applications, instead of client secrets. Microsoft IR often finds client secrets held in clear text in emails or saved in easy to find locations. If the application is interacting with Microsoft Azure or other Microsoft services, then the use of Entra ID Managed Identities is recommended. Managed Identities eliminate the need for organizations to manage the credentials for these workloads.
- If providing access to the Microsoft Graph, exceptionally granular permissions are available for the various endpoints. Security teams should challenge requests for high privileges across Microsoft Graph. The permissions reference page lists the name of the permission and what access is provided if that permission is granted.
- For security teams and administrators that are familiar with Active Directory and less so with Microsoft Entra ID, it's worth understanding how the permissions structure in Microsoft Entra ID and Microsoft Graph works. That way you are better informed to challenge requests for excessive privilege.
- Conditional Access for workload identities is available as a feature in Microsoft Entra Workload ID. As previously mentioned, due to the nature of these identities, MFA and similar controls cannot be enforced. With Conditional Access, however, you can allow access from specific IP locations or block access based on elevated risk patterns detected by Microsoft.
- Alerts should be configured to detect new credentials, additional privileges being added to existing applications, and

anomalous sign-in activity. Much like users, service principals generate log in data and detections for new IP addresses or locations should be created. Threat actors have been known to compromise accounts with access to generate new credentials on pre-existing applications with high privilege, thereby allowing tenant takeover.

Poor device access control

In many engagements, Microsoft IR has detected threat actors registering their own devices to the Microsoft Entra tenant, giving them a platform to escalate the cyberattack. While simply joining a device to a Microsoft Entra tenant may present limited immediate risk, it could allow a threat actor to establish a foothold in the environment. Conditional Access or Microsoft Intune policy misconfiguration may allow this threat actor-controlled device to be marked as compliant. The threat actor could then access additional and potentially sensitive company resources. From there, they might be able to locate additional credentials or compromise further users to escalate privilege within the environment.

Microsoft IR was recently engaged with an organization that allowed users to join their own devices to Microsoft Entra ID. Threat actors compromised a regular user account via phishing and then used the compromised credentials to join their own device to the tenant. The actors then leveraged a misconfiguration in Intune to allow that device to be marked as compliant. From there, the threat actor was able to satisfy Conditional Access and access Microsoft 365, where they located the credentials of a privileged account sent via email.

Recommendations

- If you allow end users to register or join their own devices to your Microsoft Entra tenant, then Microsoft IR recommends you control the ability to complete those actions via Conditional Access.
- Using Conditional Access, you can add additional security to your tenant by creating policies to require MFA when joining or registering a device. Depending on the requirements of your business, you could enforce the MFA requirement to particular users, or locations such as untrusted locations. Microsoft IR recommends, however, requiring MFA for all device join events where possible.

Figure 4. Microsoft Entra Conditional Access policies for device join actions.

- Auditing and alerting should be configured for device joining events to detect anomalous behavior such as users registering multiple devices, suspicious device names, or unusual times. Users themselves can be sent notifications via Intune each time a device is enrolled via their account; if they didn't initiate the action, they can report it as suspicious.
- Hold members of the Intune Administrator role to the same security standard as more well known privileged roles, such as Global Administrator

Poor application access control

When analyzing customer tenants, Microsoft IR often finds that their lines of business applications do not have sufficient access controls applied to them. Applications such as IT service management and ticketing systems, code repos, HR systems, and more are available to any user, including guest accounts. Microsoft IR was recently engaged with an organization where the threat actor compromised a user by phishing. Once the actor had control over the account, they accessed the MyApps portal and began systematically accessing all the applications listed there. Eventually, they signed into the IT system used for onboarding and offboarding accounts and requested a new privileged account, despite having no reason to have access to that system. A new account was provisioned, giving the actor a privileged account under their control.

Microsoft IR often detects threat actors browsing the https://myapps.microsoft.com portal and trying to access all the applications visible there. Often the compromised user account has no business justification to access these applications, but access is granted to groups containing all user accounts or have no access control at all. These applications may have confidential data, contain unsecured credentials, or could allow threat actors to gain insights into business processes to facilitate social engineering.

Recommendations

Access to all business applications should be restricted to only those that require it. Microsoft Entra ID provides the capability to both restrict access to applications, and to hide the visibility of applications in the MyApps portal. Access to applications should always be governed by a security group, so that users are granted only the access required to work. To ensure that users can still access applications they require, self-service capability for requesting access is available in Microsoft Entra ID. Requests for access can be delegated to application owners, so that IT teams don't need to fulfill every request.

Access reviews and entitlement management capabilities in Entra ID can help organizations management the on going governance of access and entitlement lifecycle at scale. These tools work together to allow users to gain access to the applications and data they need easily and give security teams the tools to ensure access is granted on as needed basis.

Misconfigured delegated administrative privileges (DAP) permissions

The DAP permissions model was created to allow Cloud Solution Providers (CSP) to provide services and licensing support to customers. A CSP could send an invitation to a customer to request a partner relationship. Prior to an update to the permissions model, upon accepting one of these invitations, the CSP would gain Global Administrator rights in the customer tenant.

In addition, customers themselves could not manage which users held privilege in their tenant. Membership in 'AdminAgents' group in the CSP tenant would provide downstream privilege to any customer tenants configured. These permissions are often a relic of previous partners or historical licensing agreements and the CSP may no longer be actively engaged with the customer.

CSP tenants have become an attractive threat actor target, as compromise of a single tenant can provide administrative access to any number of downstream tenants. Microsoft IR has been engaged in several incidents with organizations that have lost control of their tenant via a delegated administrative privilege configuration they were unaware existed. The threat actor compromised an account located in the AdminAgents group in the partner tenant via phishing. They then used the downstream privilege to create a Global Administrator account in our customer's tenant and take control. Both the partner and the customer were unaware this relationship existed.

Recommendations

- Review the list of delegated administrative privileges in your tenant to understand if any such partnerships exist. If any are configured, assess if your business still requires your partner to retain privilege in your tenant.
- If they do require privilege, Microsoft recommends migrating to granular delegated admin privileges (GDAP). This updated permission model better aligns with Zero Trust principle of least privilege access and hands more control back into the hands of the customers themselves.
- Depending on the nature of the partner relationship, it may be possible to remove the delegated partner configuration entirely, and instead on-board accounts native to your tenant and securely provide the credentials to any resource that requires access to your tenant.

Misconfigured Conditional Access policy

It is common for Microsoft IR to find gaps in Conditional Access policies, particularly policies covering the most privileged accounts. It's important to understand that threat actors can enumerate Conditional Access policies using a regular user account. By enumerating Conditional Access policies, threat actors can find those gaps and attempt to move laterally through them. For example, if MFA is excluded for users in a particular group or from specific locations, then a threat actor will attempt to add themselves to that group or compromise an account already excluded.

Furthermore, corporate networks are often excluded from MFA entirely and considered 'trusted' locations. This configuration and mindset are representative of the way of work from years ago, where being on the corporate network granted users and devices implicit trust. If a threat actor can find a way onto that network by compromising a device already connected to the network or gaining access via VPN, then at that point, they are considered 'trusted' and are unlikely to be further prompted for strong authentication.

Additionally, Microsoft IR regularly sees organizations that have configured their Conditional Access policies in a way that is overly complicated. While these policies are often created with the right intentions, as the policies add up, it becomes hard to tell which are enforced. The combination of these policies can give users a poor experience. This can make them susceptible to cyberattacks like MFA fatigue/spam. If users are being prompted dozens of times a day for MFA or being signed out of their session every few hours, they are going to pay less attention to a prompt for their credentials or an MFA prompt on their phone. As a result, when a threat actor-generated MFA prompt is sent to them, they might be less likely to consider it suspicious and report it as fraudulent.

Recommendations

- There are often legitimate business reasons why exclusions to Conditional Access need to apply; however, it is key that your privileged and Tier 0 accounts continue to be secured correctly.
- Alerts should be configured for any changes, additions, or deletions to Conditional Access. This will help detect both

accidental and malicious changes to your policies.

- Any groups that are configured as exclusion groups for policies should be monitored for changes. Privileged users can be excluded from key policies by being placed into a group that then excludes them from policies. Microsoft Entra ID Access Reviews can be used to ensure continued governance of the members of these groups.
- Microsoft IR recommends enforcing strong authentication for users regardless of location, even if connecting via a corporate network, starting with your most privileged accounts. This is a key component of Zero Trust security principles, where we verify users and devices explicitly, regardless of location.
- It is worth periodically reviewing Conditional Access policies to ensure they are enforcing the expected controls. To help with this, you can simulate sign-in events with the 'What If' tool. Often multiple policies can be rolled into one. This provides better and more consistent user experience, and even just simplifying policy design can lead to improved security. There is also built in insights and reporting into Conditional Access, to help both identity and address gaps in policy.

It's important to note that Zero Trust does not mean users should be prompted for MFA each time they access a resource. Modern strong authentication methods such as Windows Hello for Business provide the best combination of security and useability.

OAuth and consent phishing

Consent phishing expands on traditional phishing by tricking users into installing malicious OAuth applications rather than tricking them into providing their credentials. With consent phishing, users are tricked into providing threat actors with direct access to their personal or organizational data. The user may be presented with a link in an email that when clicked requests that the user consent to an application. The consent page will show the permissions requested by the application, and if the user has the right to consent, the application, and in turn the threat actor, is granted access to the data. These applications may be named in a way that appears that they are legitimate to users.

Figure 5.Example application consent prompt

These kinds of cyberattacks are of particular concern if administrative accounts are targeted. If a privileged user is targeted by consent phishing, they may have the ability to consent to organization-wide permissions, granting the threat actor broad access into your tenant.

When standard users are targeted by consent phishing, the permissions requested can be considered low impact, but this type of cyberattack can provide a means for a threat actor to harvest information and data that can lead to higher impact. For example, if a user clicks and consents to a malicious application that provides access to only their email and OneDrive, that may be considered a minor incident. With that access though, the threat actor could enumerate all the corporate data that the user can access. That user may have access to sensitive credentials, personally identifiable information, or market sensitive information, which the threat actor can locate.

Microsoft, often with the help of security researchers and the security community, disables known malicious OAuth applications. At the same time, it's important to protect yourself from these kinds of cyberattacks.

Recommendations

- Microsoft Entra ID provides strong and granular controls to protect your organization from consent phishing and other malicious application consent. These settings are configured in the Microsoft Entra portal. Microsoft IR recommends that the first or second option be selected. If your organization has the capability to respond effectively to all requests for application consent, then the first option, 'Do not allow user consent', is the most secure.

Figure 6. User consent options in Microsoft Entra ID

- Many organizations do not have the resources available to manage every request; in these cases, the second option provides the best mix of security and user experience. Staff can consent to applications that are from verified publishers or those considered to have a low impact in terms of permissions requested.
- Microsoft Defender for Cloud Apps can be utilized to investigate and remediate risky OAuth apps.
- As previously mentioned, privileged users should not have mailboxes assigned to them. This reduces the attack vector of traditional and consent phishing being targeted towards them.

Self-service password reset & MFA social engineering

Microsoft IR has seen cases of threat actors leveraging social engineering techniques to have service desk or similar staff update the self-service password reset (SSPR) and MFA details for users.

Microsoft IR commonly sees service desk staff being targeted via social engineering tactics. Often, a threat actor impersonates a user by creating an outlook.com or gmail.com mailbox with the same name as the legitimate user. They then send an email to the service desk and say that they have a new email address or phone number and ask the service desk to update their MFA details. Once this is completed, the threat actor could initiate self-service password reset and take over control of the account. With this initial foothold to the environment, they could pivot into Microsoft 365 and attempt to escalate privilege. Microsoft IR has seen these attempts target Global Administrator accounts directly as well as regular users.

Certain threat actors may even call the service desk and impersonate the user, taking information from sites such as LinkedIn, other information acquired from open-source intelligence (OSINT), or personal data lost in other breaches to successfully pass any identity validation required. The service desk then resets the password on the user account, or updates an MFA method, granting access to the attacker.

On top of being an initial access vector, this can also be a persistence mechanism deployed by threat actors to regain control over an already compromised account. If a user is detected as compromised and their credentials reset, the threat actor can again complete the SSPR workflow to regain access to that account.

Recommendations

- While SSPR is the preferred method of credential reset and is more secure than other methods, such as emailing credentials in clear text, it could still be susceptible to social engineering. Business processes should attempt to reduce the risk of these attempts succeeding. Importantly, empower your service desk staff to say no, or require additional validation, when something seems suspicious.
- Requests for updates to SSPR and MFA details should be validated to confirm they are legitimate, such as by challenging the user via the phone or having them confirm other details a threat actor would not have (e.g., employee ID numbers). Additionally, visual confirmation, via video calling, that the user is who they say they are can be a strong control.
- MFA registration can be further secured through the use of Temporary Access Passes (TAP). A TAP is a time-limited passcode that can be generated for users. More mature organizations have begun using these to protect the MFA registration process. A user will call the helpdesk and verify their identity. They are then granted a TAP which allows them access to the MFA registration portal for a short period of time, allowing them to then register their own MFA device.
- Ensure that IT admin staff that have the privilege to update passwords or MFA details for other privileged users are held to high security standards, such as phishing resistant MFA.
- Detections should be created for potential social engineering attempts for SSPR and MFA. These could include detections such as an update to SSPR details followed by risky sign-ins. A threat actor that takes control over an account will likely then attempt to sign into it, and if it is from a different location or has other unfamiliar features, it may trigger additional risk.

Recommended focus areas to prevent identity compromise

In real-world engagements, Microsoft IR sees combinations of the above issues and misconfigurations that could lead to total Microsoft Entra ID compromise. Depending on the motivation of the threat actor, this could further lead to additional malicious attacks, or even tenant destruction.

Figure 7. Example cyberattack chain where misconfiguration leads to tenant compromise.

In the above cyberattack chain, a regular user was compromised through phishing. Through additional weak controls, poor credential hygiene, and lack of additional security over Tier 0, the entire tenant was compromised.

Compared to Active Directory, cyberattacks on Microsoft Entra ID are relatively new, and additional new attacks are constantly emerging. Microsoft IR recommends focusing on controls that will prevent your most privileged accounts being compromised. Focusing on protecting and hardening identities with the highest privilege makes the biggest impact in preventing identity compromise.

- Reduce privilege – All user and non-human identities should be assigned access according to the principle of least privilege.

This will help prevent single user compromise leading to tenant-level compromise.

- Protect Tier 0 – All Global Administrator accounts, equivalent service principals, and accounts with additional paths to Tier 0 should be held to stricter security controls, including phishing-resistant MFA.
- Use cloud-only administrative accounts – All accounts that have privilege in Microsoft Entra ID should be cloud-native and not synced from Active Directory.
- Protect hybrid identity – In instances of complex hybrid identity, ensure that all interconnected systems such as AD FS or third-party MFA are configured and monitored properly.
- Accelerate your passwordless journey to reduce the risk of credential theft by phishing and other password-based attacks.

Much like on-premises Active Directory, protecting Microsoft Entra ID requires continued governance and monitoring. By reducing risk and controlling our most privileged accounts, you have the best chance of preventing or detecting attempts at tenant-wide compromise.

Matthew Zorich (@reprise_99 on X), *Microsoft Incident Response*

Listen to Matt discuss the importance of knowledge sharing and practical experimentation in incident response in the Microsoft Threat Intelligence Podcast episode, Incident Response with Empathy.

Learn more

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 X (formerly Twitter) at https://twitter.com/MsftSecIntel.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: https://thecyberwire.com/podcasts/microsoft-threat-intelligence.

Related Posts

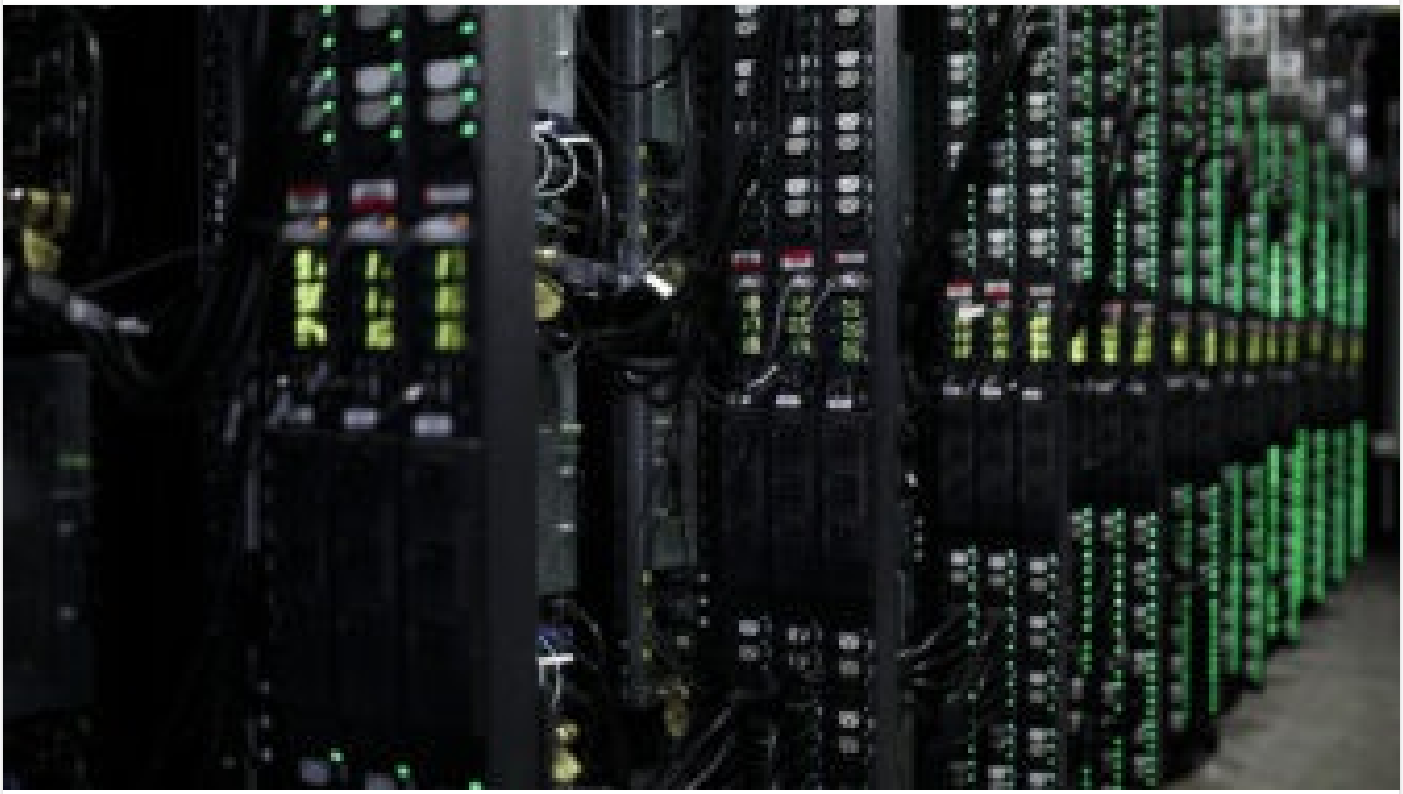
Research
Threat intelligence

Microsoft Incident Response
Threat actors

Oct 25
17 min read

Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction

Microsoft has been tracking activity related to the financially motivated threat actor Octo Tempest, whose evolving campaigns represent a growing concern for many organizations across multiple industries.

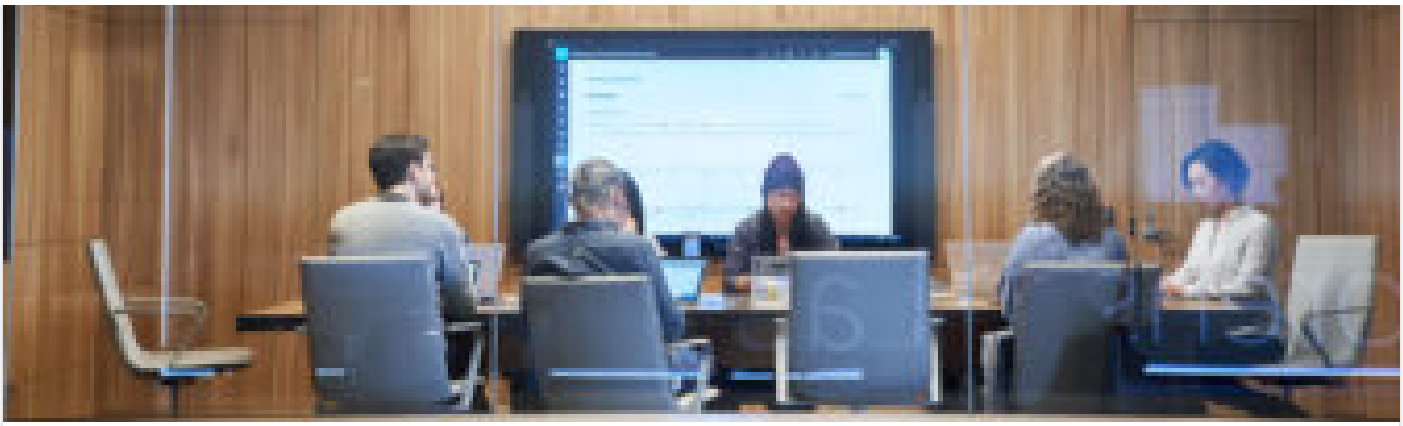


Research
Threat intelligence
Microsoft Defender
Cloud threats

Oct 3
9 min read

Defending new vectors: Threat actors attempt SQL Server to cloud lateral movement

Microsoft security researchers recently identified an attack where attackers attempted to move laterally to a cloud environment through a SQL Server instance. The attackers initially exploited a SQL injection vulnerability in an application within the target's environment to gain access and elevated permissions to a Microsoft SQL Server instance deployed in an Azure Virtual Machine (VM). The attackers then used the acquired elevated permission to attempt to move laterally to additional cloud resources by abusing the server's cloud identity.

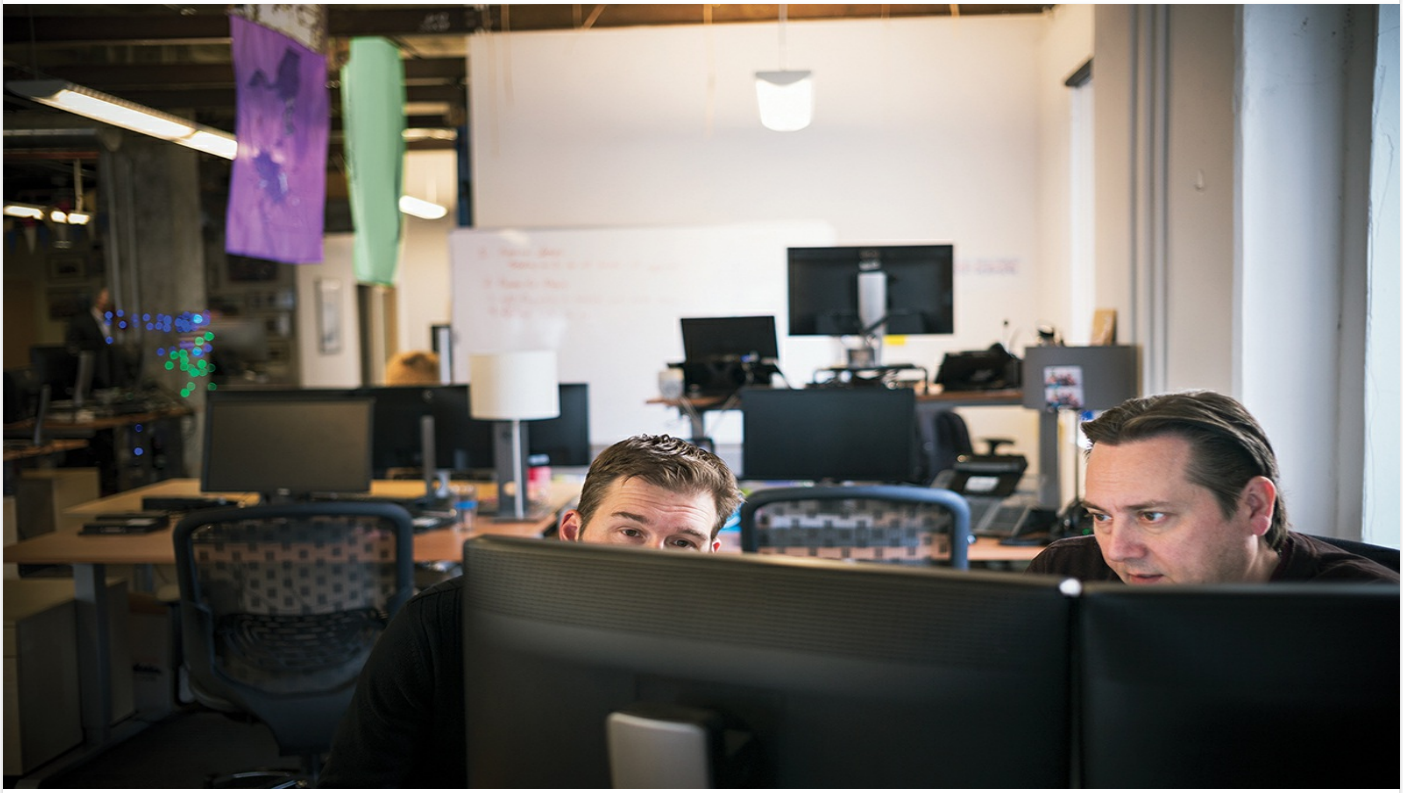


Research
Incident response
Microsoft Incident Response
Ransomware

Jul 6
18 min read

The five-day job: A BlackByte ransomware intrusion case study

In a recent investigation by Microsoft Incident Response of a BlackByte 2.0 ransomware attack, we found that the threat actor progressed through the full attack chain, from initial access to impact, in less than five days, causing significant business disruption for the victim organization.



Research
Incident response
Threat actors

Apr 11
8 min read

Guidance for investigating attacks using CVE-2022-21894: The BlackLotus campaign

This guide provides steps that organizations can take to assess whether users have been targeted or compromised by

threat actors exploiting CVE-2022-21894 via a Unified Extensible Firmware Interface (UEFI) bootkit called BlackLotus.

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy