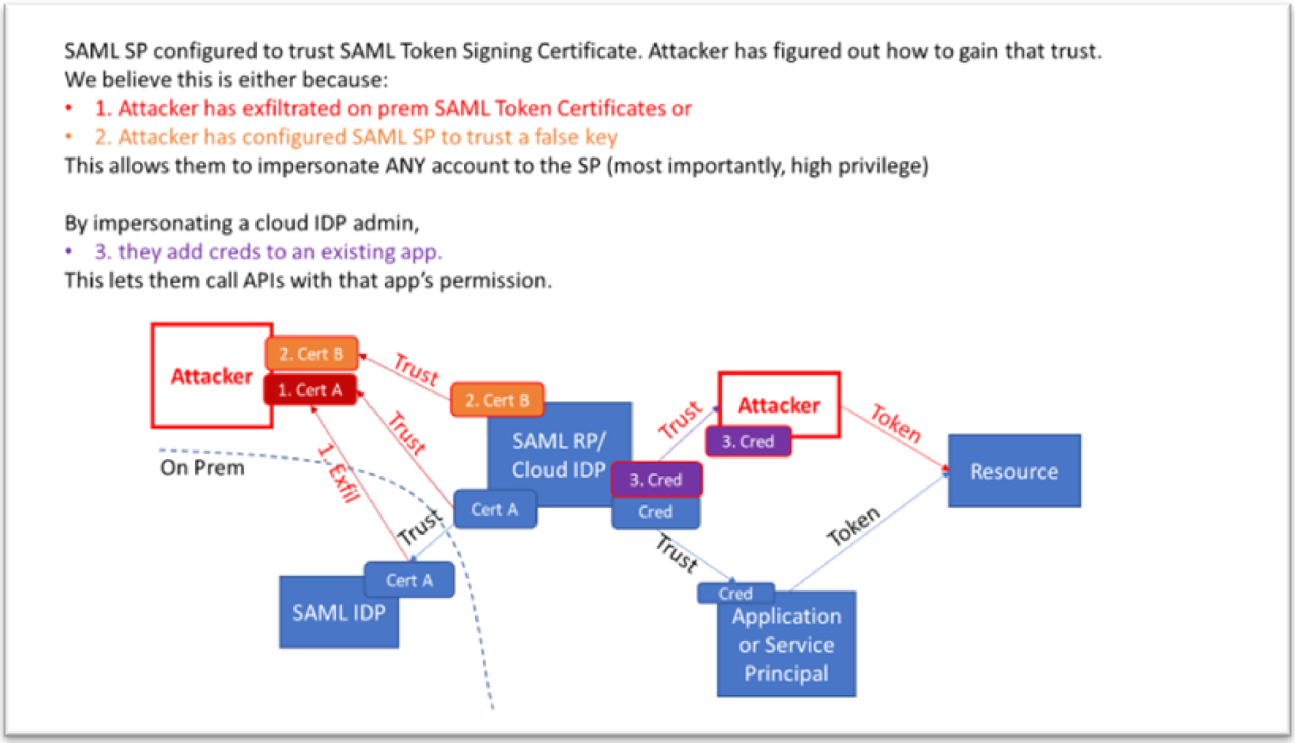
Solorigate AzureAd IOCs

techcommunity.microsoft.com/t5/azure-active-directory-identity/understanding-quot-solorigate-quot-s-identity-iocs-for-identity/ba-p/2007610

December 21, 2020



SAML SP configured to trust SAML Token Signing Certificate. Attacker has figured out how to gain that trust.
We believe this is either because:

- 1. Attacker has exfiltrated on prem SAML Token Certificates or
- 2. Attacker has configured SAML SP to trust a false key

This allows them to impersonate ANY account to the SP (most importantly, high privilege)

By impersonating a cloud IDP admin,

- 3. they add creds to an existing app.

This lets them call APIs with that app's permission.

Understanding "Solorigate"'s Identity IOCs - for Identity Vendors and their customers.

Dec 21 2020 11:46 AM

Microsoft recently disclosed a set of complex techniques used by an advanced actor to execute attacks against several key customers. While we detected anomalies by analyzing requests from customer environments to the Microsoft 365 cloud, the attacks generalize to any Identity Provider or Service provider. For this reason, we want to detail what we know about these attacks from an Identity specific lens, so Identity vendors, IAAS, PAAS, and SAAS vendors (and organizations who use these products) can detect them, remediate them, and most importantly, prevent them. This document is broadly intended to support the security teams who are focused on protection, hunting, and remediation in Identity vendors in the interest of protecting our mutual customers. It generally assumes an advanced understanding of identity infrastructure and related components.

As part of our ongoing security processes, we leverage threat intelligence and monitor for new indicators that could signal attacker activity. There are two anomalies pertinent to this report, and discussed at https://aka.ms/solorigate:

1. Anomalies in SAML tokens being presented for access. In some impacted tenants, we detected anomalous SAML tokens - signed with customer certificates - being presented for access to the Microsoft Cloud. The anomalies indicate that the customer SAML token signing certificates may have been compromised, and that an attacker could be forging SAML tokens to access any resources that trust those certificates. Because compromise of a SAML token signing certificate typically requires administrative access, there is a high probability the presence of forged tokens implies customer on premises infrastructure may be compromised. Because the signing certificate is the root of trust for the federated trust relationship, it is unlikely Service Providers would detect the forgeries.
2. Anomalies in Microsoft 365 API access patterns in a tenant. We have detected such anomalies in some impacted tenants which originate from an existing applications and service principals. This pattern indicates that an attacker with administrative credentials – possibly related to the SAML issues above - has added their own credentials to existing applications and service principals. The Microsoft 365 application program interfaces (APIs) can be used to access email, documents, chats, and configuration settings, such as email forwarding. Because highly privileged Azure AD administrative accounts are required to add credentials to service principals, these changes imply that one or more such privileged accounts have been compromised and may have made other significant changes within the impacted tenant.

Built-in security and monitoring capabilities provided by the Microsoft Cloud detected these anomalies, but such anomalies could present at any Identity Provider or Resource Provider, regardless of vendor. Any resource which trusts a customer's compromised SAML token signing certificate should be considered at risk. The SAML attack is not specific to any particular identity system or identity vendor you use. It impacts any vendor's on-premises or cloud identity system, and any resources that depend on industry-standard SAML identity federation. Likewise, while the specific mechanism for impersonating applications may vary from vendor to vendor, the pattern is vendor independent. We are not aware of any Microsoft software or cloud service vulnerability that has led to the exposure of customer SAML token signing certificates, the change in API usage, addition of credentials to service principals, or exposure of administrative credentials on premises or in the cloud. The traffic detected did not impact our production cloud environment

Elements of the activity we have detected and discuss in this blog suggest it was orchestrated by a sophisticated attacker. We believe over time this activity may be determined to be state-sponsored, but we do not have sufficient evidence to support that conclusion at this time.

It is important to emphasize – these attacks were criminal in nature, and so sophisticated that even top security companies fell victim to them. The fault lies with the criminal actor, not the victims. Further, these attacks leveraged broadly used patterns that impact many levels of the IT industry – focusing on any one technology type or vendor limits our ability to see systemic problems. By studying them and learning from these broad issues together, we can improve security throughout the industry.

We are sharing this information to help vendors who provide Identity Providers and Service Provider software and services, as well as their customers, hunt for activity and better defend against similar attacks. We will update this information as our investigations evolve.

First things first – understanding typical environments

Identity experts may skip this section, but it may help level set terminology and understanding of key components of the attack.

The following describes a typical environment. However, several caveats are worth mentioning:

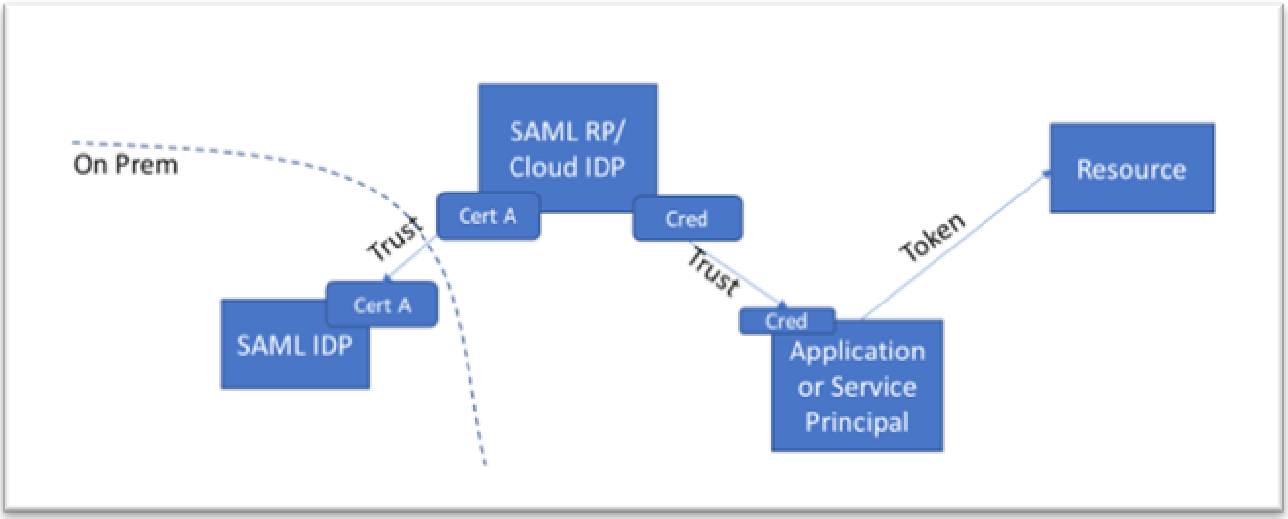
1. Most customers run on premises identity infrastructure. Microsoft offers popular versions of all such infrastructure, but several other vendors offer similar infrastructure.
2. Not all components of this infrastructure are present in all environments.
3. The sophisticated actor adapted their attack to specific environments.

For these reasons, it is important that you consider how elements of the attack pattern can impact your organization, even if your organization varies from the typical elements described below.

Components pertinent to this attack typically include:

- A SAML Identity Provider (IDP), which brokers authentication requests from applications to that directory. Applications and other identity providers – called Service Providers, or SPs – refer clients to federation servers to acquire access tokens which are signed by the SAML token signing certificate.
- SAML Service Providers (SP), also called Relying Parties, which are applications told to trust the tokens coming from a federation server, and which accept claims made in SAML tokens because they are signed by the trusted federation server’s SAML token signing certificate.
- Cloud Identity Providers (Cloud IDPs), which would typically act as a Service Provider to the SAML Identity Provider but acts as an identity provider to applications which have been told to use it. (This is called Identity Provider chaining – where one Identity provider delegates authentication to another if so configured). Azure AD is an example of a Cloud IDP.

- Cloud Service Providers (Cloud SPs), which rely on the tokens issued by a cloud IDP to validate requests.
- Applications and Service Principals in Azure AD are two types of code that authenticate to Azure AD using certificates, keys, or passwords and to other applications or APIs using OAuth 2.0 access tokens granted Azure AD in order to talk to other applications, including Microsoft 365 Graph APIs.



Typical Components

If this is new to you, you can think of tokens as a ticket to a show, the SP as the ticket taker, and the IDP as the box office, and the signature as the little holograph on the ticket. If someone wants to go to the show, they go to the IDP, get a token, then present it to the SP who validates the holograph then lets them into the show.

In terms of a typical email interaction with Microsoft 365 with federated auth, think in terms of a user going to their on premises federation server to get a signed token, then presenting that token to Microsoft 365 (via Azure AD as a chained IDP) to get access after the signature is validated. If an application is trying to access that data, it will be pre-configured to know the IDP location, so it will always come to Azure AD first to get the token, but otherwise the OAUTH flows are similar.

For SAML federation relationships where Azure AD has been configured to trust a tenant-configured SAML token signing certificate from a customer-configured federation server, the federation server is the Identity Provider (IDP)and Azure AD is the Service Provider (SP).

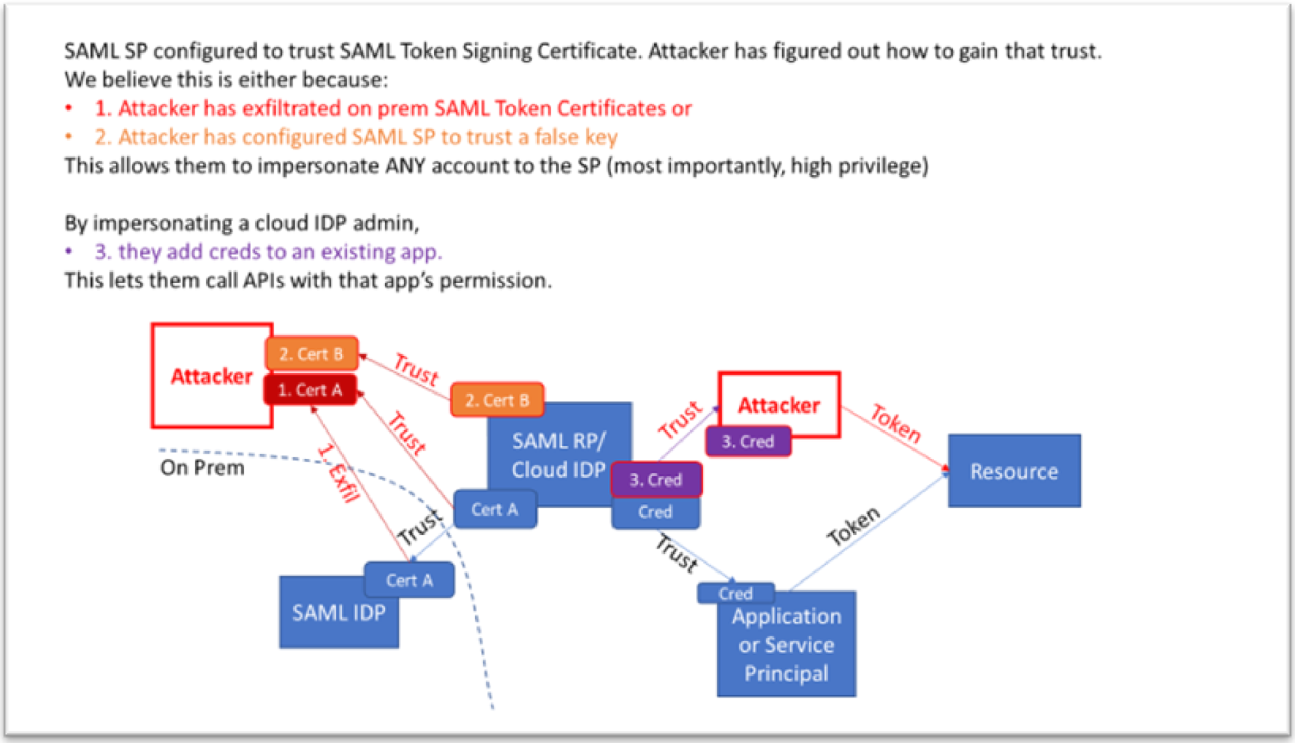
Applications and Service Principals in Azure AD don't use SAML or delegate trust to on premises federation servers; credentials must be managed directly in Azure AD.

Attacker Patterns

OK, let's lay all of this out in terms of the typical attack patterns, and how you might go about looking for them. The actions were targeted in nature and varied from target to target. Not all indicators of compromise or methodologies are present in all cases.

A rough overview of an indicative attack is as follows (see also https://aka.ms/solorigate). Each attack varied in details, but this pattern emerged repeatedly:

- The attacker compromises network management vendor software which is typically deployed with high privileges in on premises networks.
- The attacker uses the on premises administrative access to extract SAML Token Signing certificate.
- The attacker uses the stolen SAML Token Signing certificate to forge SAML tokens representing privileged cloud users.
- The attacker uses the forged token to sign in impersonating the privileged user and add credentials to an existing application or service principal.
- The attacker uses the added credentials to impersonate the existing application or service principal, and call Microsoft 365 APIs to extract mail.



SAML SP configured to trust SAML Token Signing Certificate. Attacker has figured out how to gain that trust.
We believe this is either because:

- 1. Attacker has exfiltrated on prem SAML Token Certificates or
- 2. Attacker has configured SAML SP to trust a false key

This allows them to impersonate ANY account to the SP (most importantly, high privilege)

By impersonating a cloud IDP admin,

- 3. they add creds to an existing app.

This lets them call APIs with that app's permission.

Attacker Patterns

The details of each phase of the attack are described below.

Pattern 1: Forged SAML tokens using Stolen SAML Token Signing Material

The first significant pattern we have seen is evidence of forged SAML tokens. It is worth noting that we don’t retain logs for very long. We do this in accordance with our data retention and privacy policies. It varies by agreement, but is generally is 30 days, and we never log complete tokens, so we can’t see every aspect of a SAML token. Customers who want longer retention are encouraged to configure storage in Azure Monitor or other systems. What token anomalies we did detect were tokens which were anomalous in lifetime, usage location, or claims (particularly MFA claims). The anomalies were sufficient to convince us that the tokens were forged. We did not find this pattern in all cases.

What we found

- Tokens with expiration instant exactly 3600 seconds or 144000 seconds (no milliseconds value) – note 144000 (40 hours) is exceptionally long
- Tokens which were received at the same time as the issuance time– no latency between creation and usage
- Tokens which were received BEFORE the issuance time – falsified issuance time after token received
- Tokens used from outside normal user locations
- Tokens which contained claims which were not previously seen from the tenant’s federation server
- Tokens indicating MFA used when token claimed auth from within corporate boundary where MFA not required

What it implies

- SAML token signing certificate was exfiltrated from the customer environment and used to forge tokens by the actor.
- Administrative access to SAML Token Signing Certificate storage compromised, either via service administrative access or by direct device storage or memory inspection.
- Deep penetration of the customer environment, with administrative access to identity infrastructure or the hardware environment on which it executes.

What to look for

- SAML Tokens received by the SP with configurations which deviate from the IDP’s configured behavior.
- SAML Tokens received by the SP without corresponding issuing logs at the IDP.
- SAML Tokens received by the SP with MFA claims but without corresponding MFA activity logs at the IDP.
- SAML Tokens which are received from IP addresses, agents, times, or for services which are anomalous for the requesting identity represented in the token.
- Evidence of unauthorized administrative activity.

What to do

- Determine mechanism of certificate exfiltration and remediate (see below)
- Roll all SAML token signing certificates
- Consider reducing your reliance on prem SAML trust where possible
- Consider using an HSM to manage your SAML Token Signing Certificates

Pattern 2: Illegitimate registrations of SAML Trust Relationships

In some cases, the SAML token forgeries described above correspond to configuration changes in the Service Provider. By impersonating a user with valid administrative credentials, the actor can change the configuration of the SAML Service Provider (in our case, Azure AD). In this case, the actor tells Azure AD to trust their certificate by, in effect, saying to the SP "There's another SAML IDP you should trust, validate it with this public key."

What we found

- Addition of federation trust relationships at the SP done which later resulted in SAML authentications of users with administrative privileges. The attacker took care to follow naming conventions of or impersonate existing federation server names (e.g. FED_SERVER01 exists, and they add FED_SERVERO1). The impersonated users later took actions consistent with attacker patterns described below.
- Token forgeries consistent with pattern 1, above.
- These calls came from different IP addresses for each call and user, but generally tracked back to anonymizing VPN servers.

What it implies

- Administrative access to the Azure AD was gained.
- Attacker may have been unable to gain a toe-hold on premises, or was experimenting with other persistence mechanisms.
- Attacker may have been unable to exfiltrate tokens, possibly due to use of HSM.

What to look for

Anomalous administrative session associated with modification of federation trust relationships.

What to do

- Review all federation trust relationships, ensure all are valid.
- Determine mechanism of administrative account impersonation (see below).
- Roll administrative account credentials.

Pattern 3: Adding credentials to existing applications

Once the attacker was able to impersonate a privileged Azure AD admin account, they added credentials to existing applications or service principals, usually with the permissions they wanted already associated and high traffic patterns (e.g. mail archival applications). There are some cases in which we see the attacker add permissions to existing applications or service principals. We also see cases in which a new application or service principal was set up for a short while and used to add the permissions to the existing applications or service principals, possibly to add a layer of indirection (e.g. using it to add a credential to another service principal, then deleting it).

What we found

- Addition of federation trust relationships at the SP done which later resulted in SAML authentications of users with administrative privileges. The impersonated users later took actions consistent with attacker patterns described below.
- Service Principals added into well known administrative roles such as Tenant Admin or Cloud Application Admin.
- Reconnaissance to identify existing applications with application roles that have permissions to call Microsoft Graph.
- The applications or service principals impersonated were different from customer to customer – the actor did not have a “go to” target.
- The applications or service principals included both customer developer and vendor developed software.
- No Microsoft 365 applications or service principals were used impersonated (customer credentials cannot be added to these applications and service principals).
- Token forgeries consistent with pattern 1, above.

What it implies

- Administrative access to the Azure AD was gained.
- Attacker did extensive recon to find unique applications which could be used to obfuscate their activity.

What to look for

- Anomalous administrative session associated with modification of federation trust relationships.
- Unexpected service principals added to privileged roles in cloud environments.

What to do

- Review all applications and service principals for credential modification activity.
- Review all applications and service principals for excess permissions.
- Remove all inactive service principals from your environment.
- Regularly roll creds for all applications and service principals.

Pattern 4: Queries impersonating existing applications

With credentials added to an existing application or service principal, the actor proceeded to acquire an OAUTH access token for the application using the forged credentials, and call APIs with the permissions which had been assigned to that applications. Most of the API calls we detected were focused on email and document extraction, but in some cases API calls added users, or added permissions to other applications or service principals. Calls were generally very targeted, synchronizing then monitoring email for specific users.

What we found

- Application calls attempting to authenticated to Microsoft Graph resource with applicationID: "00000003-0000-0000-c000-000000000000"
- Impersonated calls to the Microsoft Graph Mail.Read and Mail.ReadWrite endpoints.
- Impersonating calls came from anomalous endpoints. These endpoints were not repeated from customer to customer. The endpoints were usually Virtual Private Server (VPS) vendors.

What it implies

- Attacker was primarily interested in persistence and reconnaissance.
- Attacker was attempting to obfuscate their activity.

What to look for

- Anomalous requests to your resources from trusted applications or service principals.
- Requests from service principals that added or modified groups, users, applications, service principals, or trust relationships.

What to do

- Review all federation trust relationships, ensure all are valid.
- Determine mechanism of administrative account impersonation (see below).
- Roll administrative account credentials.

Other Observations

This section relates other observations of attacker behavior.

Attacker access to on premises resources

Our optics into on premises behavior are limited, but here are the indicators we have as to how on premises access was gained. We recommend using on premises tools like Microsoft Defender for Identity (formerly Azure ATP) to detect other anomalies:

- Compromised network management software used as command and control to place malicious binaries which exfiltrated SAML token signing certificate.
- Compromised vendor credentials with existing administrative access (vendor network compromised).
- Compromised service account credentials associated with compromised vendor software.
- Use of non-MFA service account.

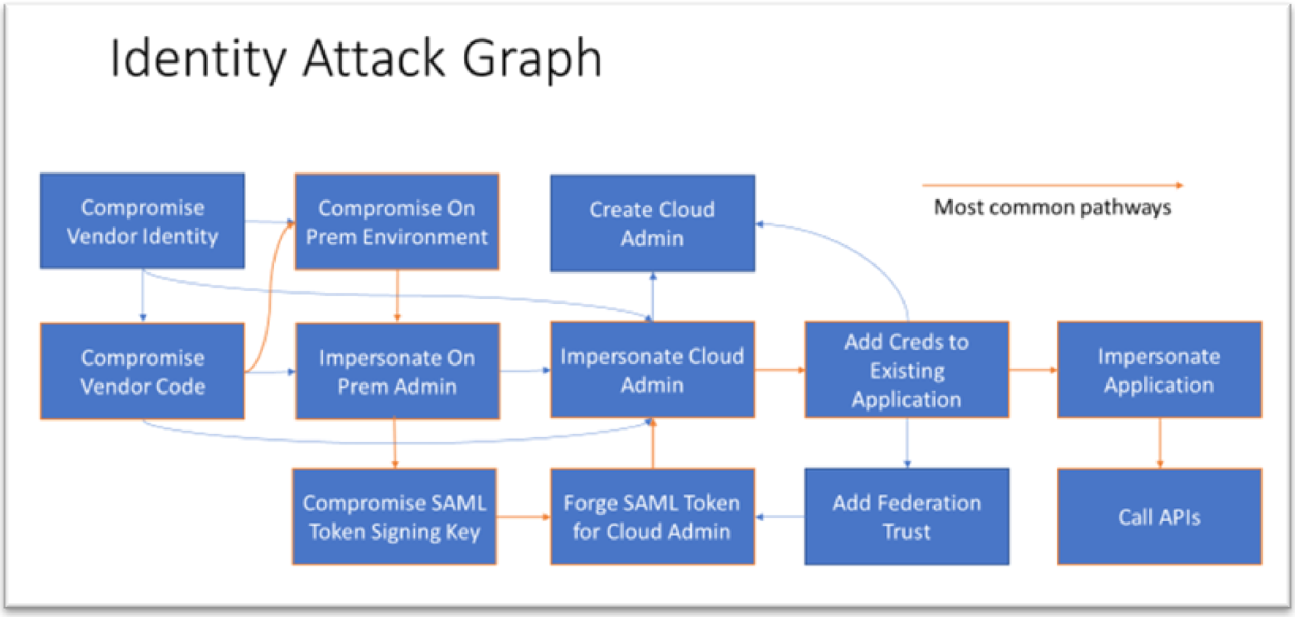
Attacker access to cloud resources

For administrative access to the Microsoft 365 cloud, we observed:

- Forged SAML tokens impersonating accounts with cloud administrative privileges.
- Accounts without MFA required – these are easily compromised (see https://aka.ms/yourpassworddoesntmatter)
- Access from trusted vendor accounts where the attacker had compromised the vendor environment.

Identity Attack Graph

This graph summarizes the vectors and combinations tracked in this document.


Identity Attack Graph

Most common pathways

Compromise Vendor Identity
Compromise On Prem Environment
Create Cloud Admin
Compromise Vendor Code
Impersonate On Prem Admin
Impersonate Cloud Admin
Add Creds to Existing Application
Impersonate Application
Compromise SAML Token Signing Key
Forge SAML Token for Cloud Admin
Add Federation Trust
Call APIs

Other Guidance

The following guidance may assist customers in protecting their environments.

- We published an Azure AD Workbook to help you hunt for the behaviors described in this document.

- To protect Microsoft 365 resources from a compromise of on-premises environments: https://aka.ms/protectm365
- If your organization has been compromised, review recovery guidance from DART at https://aka.ms/dartrecoveryguide
- To configure for Zero Trust to increase explicit request verification, least privileged access, and assumed breach protection: https://aka.ms/ztguide

Stay up to date

The Solarwinds attack is an ongoing investigation, and our teams continue to act as first responders to these attacks. As new information becomes available, we will make updates through our Microsoft Security Response Center (MSRC) blog at https://aka.ms/solorigate.