



WHITEPAPER

# When Trust is Broken: Lessons from the SolarWinds Cyber Attack

# Table of Contents

Executive Summary .....	3
Contributors .....	6
Audience .....	6
Attack Overview .....	6
Series of Events .....	7
Planning and Trespassing .....	7
Supply Chain Compromised .....	21
Stolen SAML Signing Key .....	27
Creating and Impersonating New Trusted Identities and Credentials .....	32
Addition of Federation Trusts to IdP Server .....	41
Email Accounts Compromised .....	45
Conclusion .....	49
References .....	51
About Easy Dynamics .....	51

# Executive Summary

Trust, whether in the public or private sector, is only possible when service providers protect access to their sensitive data and safeguard the identities of those who rely on the service. Protection against unauthorized access has historically been achieved through perimeter defenses made up of firewalls, remote proxies, and virtual private networks (VPN). These protections often rely on rigorous access criteria of remote workers but lack robust defenses once access to the network is gained. This results in limited protection against service discovery, lateral movement, and privilege escalation within the network. On December 13, 2020, The Cybersecurity & Infrastructure Security Agency (CISA) issued Emergency Directive 21-01 in response to a known compromise involving SolarWinds Orion products. The directive highlighted a significant and ongoing Cybersecurity threat by (nation-state) actors successfully breaching perimeter defenses of our US Government and private sector organizations. The attack exposed Credentials as a significant attack vector and made clear that reliance on perimeter defenses is rapidly becoming less effective in an environment where distributed cloud services have become the norm. Organizations are recognizing there is a growing and critical role Identity has in protecting information services as “Identity is Everything”<sup>1</sup> in addressing modern cybersecurity attacks.

Identity, Credential, and Access Management (ICAM) is not a new topic. The National Institute of Standards and Technology’s (NIST) Special Publication (SP) 800-63 Digital Identity Guidelines has seen three revisions since its inception and is currently drafting revision 4. ICAM is a broad topic with hundreds of vendors that enable the techniques and capabilities needed to support a growing and complex set of use cases. While the SolarWinds attack targeted multiple vendors and products, this paper addresses the techniques and threats discovered concerning the digital identity aspects of the attack. Accordingly, Easy Dynamics presents our assessment of the SolarWinds attack by delineating the events, deployed techniques, and mitigations. Our specific focus on the digital identity aspects of the attacks allows organizations to evaluate the threats and reevaluate their identity security posture in light of these new threats.

The following summary table lays out key digital identity elements of the attack, deployed attack techniques, attack summary, and our predominant recommendations.

---

1 Heckman, J. (2021). [CISA: ‘Identity is everything’ for cyber defense post-SolarWinds](#). Federal News Network.

## Attack Elements

### Planning & Trespassing

Deployed Techniques	Summary
Brute Force: Password Guessing & Spraying	Unauthorized access gained via unsophisticated password-based attacks.
Unsecured Administrator Credentials & Exposed Services	Inappropriately secured administrative credentials accessible via external remote access services (e.g. VPN).
Spear Phishing	Passwords/credentials obtained through targeted email attacks, ostensibly from a trusted sender.

### Supply Chain Compromised

Deployed Techniques	Summary
Sidecar Process Malware Injection	Attackers inserted their SUNSPOT malware into SolarWinds' software development supply chain.

### Stolen SAML Signing Key

Deployed Techniques	Summary
Gained Admin Privileges on SAML Federation Server	Admin privileges allowed the attacker to steal SAML signing keys, enabling creation of new SAML tokens with any custom privilege, which continued to appear being from a trusted source.

### Creating and Impersonating New Trusted Identities and Credentials

Deployed Techniques	Summary
Addition of Credentials	Attacker able to forge SAML tokens with any desired claims and lifetime, allowing for the impersonation of any privileged account.
Impersonation and Movement via Custom Crafted SAML Tokens	Allows to attacker to illegitimately call APIs, move laterally within the target organization and exfiltrate data.
Generation of SAML Tokens Using Stolen Signing Key	"Golden SAML attack" allows for surveillance and data theft.

### Addition of Federation Trusts to IdP Server

Deployed Techniques	Summary
Authentication of External Bad Actors through Federation Trusts	Attacker gains sufficient admin privileges within the cloud tenant to add a malicious certificate trust relationship for forging SAML tokens, enabling for provision of new malicious user accounts.

### Email Accounts Compromised

Deployed Techniques	Summary
Compromised Email Authentication Through Signed SAML Tokens	Access to private email addresses of leadership at major government agencies and private sector organizations.

Organizations responsible for designing, developing, and securing their digital identities should take advantage of the insights gained from the SolarWinds attack. Acting as a central resource for access control, organizations must support the advancement of policies, governance, and practices along with the implementation of tools and techniques to protect against a growing set of identity attack vectors. This paper aims to review these insights and provide recommendations from real-world experiences to mitigating, detecting, and hunting against these threats.

This paper provides specific vendor resources with techniques to address portions of a particular attack vector. While hundreds of vendors exist with solutions that address these challenges broadly or specifically, our paper aims to limit recommendations to the three largest public cloud services providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Computing Services (GCP).

## Contributors

Thank you to the following individuals for their time and contributions to this paper: Sheridan Crossley, Jamie Danker, Courtney Farnsworth, James L. Fisher, Dari FitzGerald, Garrett Folks, Ray Gauss, JJ Harkema, Pirooz Javan, Pranav Kothare, Kyle Laker, Hector Portillo, James Stevens, Brian Walsh, David Ylizarde, and Dmitriy Zaslavskiy.

## Audience

IT Decision Makers, System Owners, Security Officers, Security Professionals, Engineers, and Testers that support or federate with a Credential Service Provider (CSP). This includes public sector and private sector organizations that maintain a CSP, as well as integrators that are supporting these organizations in designing, securing, and building the systems that issue, maintain, and authenticate credentials.

## Attack Overview

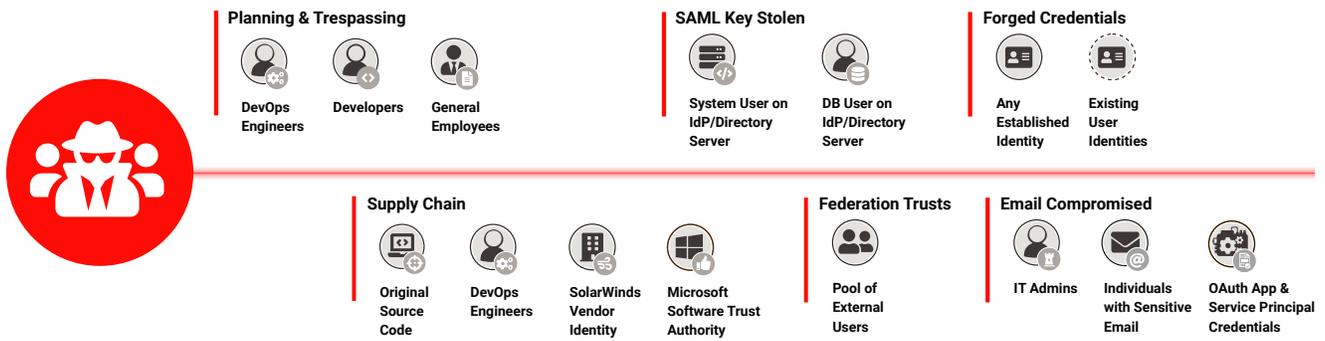
In December 2020 as FireEye was investigating a cybersecurity breach, it discovered and subsequently informed SolarWinds that their Orion Platform had suffered a cyberattack. The attack was perpetrated via software updates made available to SolarWinds' clients between March and June of 2020.

While new aspects of the attack are still being discovered, researched, and reported, this whitepaper focuses on the digital identity aspects of the attack learned to date based on publicly available information reported by government authorities and private sector organizations. Easy Dynamics assembled this information to support our clients in assessing their potential exposure to, and the impact of, the SolarWinds attack.

As we looked through the various digital identity related attack vectors, we captured the identities involved, relevant standards, and reviewed the mitigation guidance to include our assessment and recommendations.

An illustration of the entire incident, known to date, is depicted below and encapsulates the digital identities targeted with each event and the approximate timing in relation to the other events.

# Series of Events



**i** Each event below is described with mitigations as well as detection and hunting techniques that organizations can consider when developing corresponding defenses. Some mitigation topics sourced from the MITRE ATT&CK knowledge base.

## EVENT

# Planning and Trespassing

## Targeted Identities By Access Risk



**DevOps Engineers**  
 High Risk  
 Access to source code, build servers, potentially customer data



**Developers**  
 Medium Risk  
 Access to source code



**General Employees**  
 Medium Risk  
 General system access, varying privileges, and data sensitivity access

## Event Description

Prior to the injection of SUNSPOT malware into the Orion platform, the threat actor performed extensive reconnaissance activities to gather the information needed to trespass and compromise the systems involved. This reconnaissance occurred through a variety of avenues, including humans, automation, and robotic process automation (RPA). The supply chain infiltration was accomplished through a compromised password due to dictionary and brute force password attacks and/or due to unsecured administrator credentials. There is further evidence that the attackers compromised Exchange Mail Servers to facilitate very

targeted spear phishing of SolarWinds developers.<sup>2</sup>

## ATTACK TECHNIQUE

# Brute Force: Password Guessing & Spraying

[CISA's December Alert \(AA20-352A\)](#) explains that in some cases, initial unauthorized access was gained via password-based attacks. Password-based attacks in this category are both unsophisticated and shockingly effective. Adversaries can guess or brute force common passwords to a single account or may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials.

**MITRE ATT&CK IDs:** [T1101.001](#), [T1101.003](#)

## BRUTE FORCE: PASSWORD GUESSING & SPRAYING

# Mitigation

### Multifactor Authentication (MFA)

#### Mitigation

MFA can be especially effective against brute force attacks by creating an additional out-of-bound channel that both slows down an attacker and adds a proof-of-possession barrier. MFA adds significant complexity to any attempts for successful account takeover.

All targeted identities should have access to systems that have policies enforcing MFA using the requisite combination of approved authenticators outlined in NIST 800-63-3B.

---

#### Standards

NIST recommends a risk-based approach to determining authentication assurance levels and developing a corresponding authentication profile.

When selecting MFA methods, several permitted authenticator types should be considered, such as Out-of-Band Devices, MFA OTP Device, and MFA Cryptographic Software.<sup>3</sup>

---

<sup>2</sup> Virsec Systems. [SolarWinds Attack End-to-End Demo](#). (2021). YouTube.

<sup>3</sup> [NIST Special Publication 800-63B Digital Identity Guidelines](#). (2017).

**Easy Dynamics Guidance**

Consider the usage of MFA across all authentications that occur in the organization, including desktop, remote access, and public services. The movement to eliminate the use of passwords continues to gain momentum. Including a second, biometric or pin-based cryptographic factor provides significantly can reduce the risk of account take over.

We strongly favor the use of Cryptographic Software and Devices which enforce standards such as FIDO2 Universal Authentication Framework (UAF), Universal Second Factor (U2F) and Client to Authentication Protocol (CTAP). Avoid using second factors that can be intercepted such as SMS and email.

When operating in a cloud environment, ensure to properly configure MFA:

- ✓ [Azure AD MFA](#)
- ✓ [Adding Multi-Factor Authentication \(MFA\) to a User Pool - Amazon Cognito](#)
- ✓ [AWS Cognito Custom Auth Challenges](#)
- ✓ [Adding multi-factor authentication to your web app \(google.com\)](#)

---

## Protect against Failed Authentications

**Mitigation**

Organizations should set policies and access management solutions that protect against repeat failed login attempts.

---

**Standards**

NIST SP 800-53 has recommended controls for various system account types and establishing organizational policies and enforcement recommendations available in [AC-2 Account Management](#) and [AC-7 Unsuccessful Logon Attempts](#).

If employing a Memorized Secret, Verifiers SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.<sup>4</sup> When required by authenticator type, "verifier SHALL implement controls to protect against online guessing attacks."<sup>5</sup>

---

---

4 [NIST Rate Limiting \(Throttling\), NIST 800-53 R5: Unsuccessful Login Attempts & Session Termination](#). (2017).

5 [NIST SP 800-63B - 5.2.2 Rate Limiting \(Throttling\)](#). (2017).

**Easy Dynamics Guidance**

We strongly encourage organizations to move away from memorized secrets. Most modern browsers now support WebAuthN, allowing relying parties to easily integrate modern strong authentication, such as security keys or built-in platform authenticators such as biometric readers. If memorized secrets must be used for some reason, ensure that repeated failed login attempts lead to increasingly more difficult subsequent authentication attempts to mitigate against automated attacks.

Prevent Credential Stuffing and Password spraying by implementing defenses such as CAPTCHA, IP Block-listing, and device fingerprinting. For a simple-to-follow guide reference:

- [Credential Stuffing Prevention - OWASP Cheat Sheet Series](#).

The vulnerability of Memorized Secrets cannot be overstated. Organizations should consider the feasibility of additional protections:

- ✓ [Azure AD Smart Lockout](#)
- ✓ [AWS Cognito OotB Auth Flow](#)
- ✓ [AWS Cognito Custom Pre-Auth Triggers](#)
- ✓ [Fine-Grained Password Policies concepts \(google.com\)](#)

---

**Password Policies****Mitigation**

Password complexity has varied through the years but updated guidance now includes user experience as a key element of tackling the problem.

---

**Standards**

NIST SP 800-63B has recommendations about password policies including length, truncation, hints, rate limiting, encryption, storage, and comparing secrets against a database of stolen passwords from known breaches.

Verifiers SHOULD permit claimants to use “paste” functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and, in many cases, increase the likelihood that users will choose stronger memorized secrets.<sup>6</sup>

---

**Easy Dynamics Guidance**

If using memorized secrets, compare secrets against commonly used sources, such as those that we have curated:

- [Havelbeenpwned](#)
- [Google \(Preview\)](#)
- [Azure](#)

Some of these recommendations can be enforced through cloud provider services' password policies:

- [AWS User Pool Password Policies](#)
- [Azure AD Password Policies](#)
- [Enforce and monitor password requirements for users - Cloud Identity Help \(google.com\)](#)

Additional advanced security:

- [AWS Advanced Security to User Pool](#)

---

6 [NIST Special Publication 800-63B - 5.1.1.2 Memorized Secret Verifiers](#). (2017).

---

## Audit

**Mitigation** Ensure logging is turned on and collected for all access control decisions. Make sure to evaluate what options are available for logging additional metadata per authentication context to capture all available session data.

---

**Standards** NIST 800-53 has detailed recommendations for auditing, including policies for retention, review and analysis in the [Audit Family of Controls](#).

---

**Easy Dynamics Guidance** Ensure logging is turned on with sufficient granularity to detect the addition of new principals and/or credentials, and audit regularly.

Use machine learning anomaly detection algorithms to identify adding credentials and extra privileges.

---

## BRUTE FORCE: PASSWORD GUESSING & SPRAYING

# Detection & Hunting 🔍

## AWS

**Recommendations** If your enterprise is using Amazon Cognito to manage users, then consider turning on advanced security features for a given user pool, enabling detailed event logging in CloudWatch to then leverage CloudWatch Alarms to notify administrators about risky events.

- 
- References**
- [Enable Multi-factor Authentication](#)
  - [AWS Advanced Security to User Pool](#)
  - [User Adaptive Authentication](#)
  - [View Advanced Security Metrics](#)

## Microsoft Azure

### Recommendations

If your enterprise has an **Azure AD P1** license or higher, you can connect Azure AD to Azure Sentinel and subsequently analyze the sign-in logs to determine further course of action. The objective here is to look for events that have repeated sign-in failures from either multiple locations or multiple attempts for a single account.

A good starting point with hunting for this type of threat is under **Azure Sentinel > Hunting**. Tweaking and running the following queries will give you a good basis for discovering any potential issues:

- Azure Active Directory sign-ins from new locations
- Permutations on logon attempts by UserPrincipalNames indicating potential brute force
- Potential IIS brute force
- Brute force attack against Azure Portal
- Anomalous Failed Logon

If you have an **Azure AD P2** license, detection becomes even more robust. Administrators are given full access to Identity Protection Sign-in risk and you can use the provided reports in the Azure Portal regarding Risky users and Risky sign-ins to detect these issues without any further configuration.

---

### References

- [Enable Multi-factor Authentication](#)
- [Advanced multistage attack detection in Azure Sentinel](#)
- [Identity Protection Sign-in risk](#)
- [Azure provided Reports](#)

---

## Google Cloud

### Recommendations

If your organization is using Google Identity to manage users, enable companywide MFA and ensure your login events are properly logged. Review events and, at a minimum, enable:

- ✓ [Access Transparency logs](#)
- ✓ [Login audit log](#)
- ✓ [OAuth Token audit log](#)
- ✓ [Rules audit log](#)
- ✓ [SAML audit log](#)
- ✓ [Secure LDAP audit log](#)

---

### References

- [Enforce uniform MFA to company-owned resources | Cloud Identity \(google.com\)](#)
- [Available audit logs - Google Workspace Admin Help](#)

ATTACK TECHNIQUE

# Unsecured Administrator Credentials & Exposed Services

[CISA's December Alert](#) explains that in some cases, initial unauthorized access was gained via “inappropriately secured administrative credentials accessible via external remote access services.” Typically, these attacks are a result of insufficient operational security by organizations that provide remote access to their networks via VPN or other remote services and allow adversaries to leverage valid accounts that were not properly secured.

**MITRE ATT&CK IDs:** [T1078](#), [T1133](#)

UNSECURED ADMINISTRATOR CREDENTIALS & EXPOSED SERVICES

## Mitigation

### Application Developer Guidance

**Mitigation**

Commercial, open-source, and custom applications are often seeded with default credentials and at times, insecurely, and can be easily overlooked by an organization and guessed by an adversary. Be sure to change default passwords of applications and systems and ensure that credentials are not stored in plaintext or hardcoded.

**Standards**

NIST guidance for Verifiers can be applied in similar guidance to applications persisting passwords on disk or memory. Memorized secrets shall be salted and hashed using a suitable one-way key derivation function. Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash.<sup>7</sup>

In a draft proposal, IETF has more recent guidance in [draft-ietf-kitten-password-storage-06 - Best practices for password hashing and storage](#).

**Easy Dynamics Guidance**

When storing passwords, use OWASP [Password Storage Cheat Sheet](#) for specific guidance on Salting and hashing.

Enumerate all applications for default credentials. Take advantage of OWASP [Testing for default credentials](#).

7 [NIST Special Publication 800-63B - 5.1.1.2 Memorized Secret Verifiers](#). (2017).

## Password Policies

<b>Mitigation</b>	Password complexity has varied through the years but updated guidance now includes user experience as a key element of tackling the problem.
<b>Standards</b>	<p>NIST SP 800-63B has recommendations about password policies including length, truncation, hints, rate limiting, encryption, storage, and comparing secrets against a database of stolen passwords from known breaches.</p> <p>Verifiers SHOULD permit claimants to use “paste” functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and, in many cases, increase the likelihood that users will choose stronger memorized secrets.<sup>8</sup></p>
<b>Easy Dynamics Guidance</b>	<p>If using memorized secrets, compare secrets against commonly used sources, such as those that we have curated:</p> <ul style="list-style-type: none"><li>• <a href="#">Havelbeenpwned</a></li><li>• <a href="#">Google (Preview)</a></li><li>• <a href="#">Azure</a></li></ul> <p>Some of these recommendations can be enforced through cloud provider services’ password policies:</p> <ul style="list-style-type: none"><li>• <a href="#">AWS User Pool Password Policies</a></li><li>• <a href="#">Azure AD Password Policies</a></li><li>• <a href="#">Enforce and monitor password requirements for users - Cloud Identity Help (google.com)</a></li></ul> <p>Additional advanced security:</p> <ul style="list-style-type: none"><li>• <a href="#">AWS Advanced Security to User Pool</a></li></ul>

---

## Disable/Remove Services

<b>Mitigation</b>	Remove/Disable remotely accessible services that are not necessary on all endpoints.
<b>Standards</b>	NIST SP 800-53 has recommended controls for remote connection configuration settings such as functions, ports, protocols and services in <a href="#">CM-6 Configuration Management</a> .
<b>Easy Dynamics Guidance</b>	<p>Organizations looking to move their services to infrastructure with lower attack surfaces as shifting a large portion of the responsibility from organization to service provider, often a cloud service.</p> <p>These services should be combined with Zero Trust Architecture (ZTA) and strong, modern authentication with behavioral analytics. Ensure no implicit trusts are in place for access to remote services.</p>

---

8 [NIST Special Publication 800-63B - 5.1.1.2 Memorized Secret Verifiers](#). (2017).

## Limit Access to Resource Over Network

**Mitigation** Organizations should limit and/or eliminate any implicit trusts on all IT assets on the network.

---

**Standards** NIST SP 800-53 restricts or prohibits access to interfaces through [SC-7 Boundary protection](#).

---

**Easy Dynamics Guidance** While a ZTA ensures that there are not implicit trusts based on network location, that does not necessarily mean that all ports of all devices should be publicly accessible. Software can still have vulnerabilities and there are still reasonable limitations on what ports should be exposed. Further, not only is limiting ingress traffic important but egress as well. In a ZTA, this access should be limited to being through the configured access gateway and still require proper authentication.

Create firewall, access control, or network security group rules to limit Internet ingress and egress traffic. Design systems such that their need to consume services from the public Internet is limited (for example, using a local/internal software update mirror). Ensure all exposed ports provide access only to properly authenticated identities.

---

## Multifactor Authentication (MFA)

**Mitigation** MFA can be especially effective against brute force attacks by creating an additional out-of-bound channel that both slows down an attacker and adds a proof-of-possession barrier. MFA adds significant complexity to any attempts for successful account takeover.

All targeted identities should have access to systems that have policies enforcing MFA using the requisite combination of approved authenticators outlined in NIST 800-63-3B.

---

**Standards** NIST recommends a risk-based approach to determining authentication assurance levels and developing a corresponding authentication profile.

When selecting MFA methods, several permitted authenticator types should be considered, such as Out-of-Band Devices, MFA OTP Device, and MFA Cryptographic Software.<sup>9</sup>

---

---

9 [NIST 800-63B Authenticator and Verifier Requirements](#). (2017).

### Easy Dynamics Guidance

Consider the usage of MFA across all authentications that occur in the organization, including desktop, remote access, and public services.

The movement to eliminate the use of passwords continues to gain momentum. Including a second, biometric or pin-based cryptographic factor provides significantly can reduce the risk of account take over.

We strongly favor the use of Cryptographic Software and Devices which enforce standards such as FIDO2 Universal Authentication Framework (UAF), Universal Second Factor (U2F) and Client to Authentication Protocol (CTAP). Avoid using second factors that can be intercepted such as SMS and email.

When operating in a cloud environment, ensure to properly configure MFA:

- ✓ [Azure AD MFA](#)
- ✓ [Adding Multi-Factor Authentication \(MFA\) to a User Pool - Amazon Cognito](#)
- ✓ [AWS Cognito Custom Auth Challenges](#)
- ✓ [Adding multi-factor authentication to your web app \(google.com\)](#)

## Network Segmentation

### Mitigation

As a method of limiting access, create logical segmentation of IT assets is not only necessary for network traffic performance but still effective against various methods of lateral movement.

### Standards

NIST SP 800-53 recommends restricting or prohibiting access to interfaces in [SC-7 Boundary protection](#).

### Easy Dynamics Guidance

Network segmentation is all about limiting access to resources based on predefined rules to reduce or slow down lateral movement. Devices should be organized into small subnets or network security groups with properly designed firewall and access control rules to limit improper network traffic between devices and to limit device discoverability.

We strongly encourage combining network segmentation with ZTA to ensure all communication is secured regardless of network location.

---

## Anomaly Detection of Authentications

### Mitigation

Analyze all authentications to develop a normal usage profile to detect any anomalies in authentication and access.

### Standards

To our knowledge, no standard exists on methodologies for detecting anomalous user behavior. However, one recent publication through IEEE provides some perspective on designing user profiles for anomaly detection:

- [Designing Security User Profiles via Anomaly Detection for User Authentication | IEEE Conference Publication | IEEE Xplore](#)

#### Easy Dynamics Guidance

We strongly encourage every organization to develop a risk-based profile for authentication sessions based on a risk assessment i.e., [FIPS199](#) and develop corresponding AuthN Risk profiles that identify factors to include as potential sensors (time, location of subject, subject's device, OS and security posture, etc.) and how to monitor.

---

## UNSECURED ADMINISTRATOR CREDENTIALS & EXPOSED SERVICES

# Detection & Hunting 🔍

### AWS

#### Recommendations

If your enterprise is using AWS, make sure to reference available benchmarks and leading practices for securing your VPC and IAM accounts. If you are processing login events, collect and analyze adequate data to develop normal behavior patterns. Use IP insights as an unsupervised learning algorithm for detecting anomalous behavior.

#### References

- [Detect suspicious IP addresses with the Amazon SageMaker IP Insights algorithm | AWS Machine Learning Blog](#)
  - [CloudWatch Anomaly Detection](#)
  - [AWS Security Hub](#)
  - [Center for Internet Security \(CIS\) AWS Foundations Benchmark](#)
  - [AWS Foundational Security Best Practices standard](#)
- 

### Microsoft Azure

#### Recommendations

If your enterprise has an **Azure AD P1** license or higher, you can connect [Azure AD to Azure Sentinel](#) and subsequently analyze the sign-in logs to determine further course of action. The objective here is to look for events that have repeated sign-in failures from either multiple locations or detect these issues without any further configuration.

#### References

- [Anomaly Detector - Anomaly Detection System | Microsoft Azure](#)
  - [Identity Protection Sign-in risk](#)
- 

### Google Cloud

#### Recommendations

If your organization is using Google Identity and Security, consider reviewing best practices and mapping mitigation techniques combined with rigorous monitoring.

---

References

- [3 steps to detect and remediate security anomalies with Cloud Anomaly Detection | Google Cloud Blog](#)
- [Anomaly detection using streaming analytics & AI | Google Cloud Blog](#)

---

ATTACH TECHNIQUE

## Spear Phishing

Another method by which the threat actor could have attained passwords and/or credentials is via spear phishing. Increasingly sophisticated, spear phishing attacks on U.S. organizations had a 65% success rate in 2019, and “when it comes to targeted attacks, 65% of active groups relied on spear phishing as the primary infection vector.”<sup>10</sup>

**MITRE ATT&CK IDs:** [T1598.001](#), [T1598.002](#), [T1598.003](#)

SPEAR PHISHING

## Mitigation

### User Training

**Mitigation**

Phishing attacks are common, occur daily, and are a highly effective means for achieving account takeover but can be avoided when common signs can be detected.

---

**Standards**

While no official standards exist for user training, NIST has introduced the [Phish Scale](#) to give IT administrators a better understanding on how to address training.

---

**Easy Dynamics Guidance**

Training content is difficult to create and keep current. Choose a vendor that demonstrates and proves a commitment to keeping content current through frequency of updates. When selecting a vendor, evaluate what live and passive exercises are supported and make sure to enable phishing exercises often.

We recommend evaluating cybersecurity training vendors or leveraging available studies by trusted organizations [Gartner Magic Quadrant for Security Awareness Computer-Based Training](#).

---

### Use Phishing Resistant Modern Authentication Protocols

**Mitigation**

Modern authentication protocols, specifically Universal Second Factor (U2F) from the Fast Identity Online Alliance, provides protections against phishing attacks.

---

10 Rosenthal, M. (2021). [Must-Know Phishing Statistics: Updated 2021](#). Tessian.

---

**Standards**

- Fast Identity Online (FIDO2) - [Download FIDO Authentication Specifications - FIDO Alliance](#)
- WebAuthN - [Web Authentication: An API for accessing Public Key Credentials - Level 3 \(w3c.github.io\)](#)

---

**Easy Dynamics Guidance**

With passwordless authentication, attackers do not have the opportunity to obtain credentials. A U2F dongle is simple to use and provides a pre-baked cryptographic private key that can be registered as a second factor. These [FIPS 140-2](#) validated hardware security keys or embedded (or bound) authenticators (biometrics or pins) are strongly resistant to phishing attacks. When implemented over WebAuthN, CTAP2, services can leverage external authenticators for authentication over FIDO2 enabled browsers and Operating Systems over USB, NFC, or BLE for passwordless, second factor MFA.

---

### Make downgrading authentication a friction-driven process

**Mitigation**

Organizations adopting phishing-resilient authenticators should consider how that can be bypassed with alternative authentication methods.

---

**Standards**

No available standards

---

**Easy Dynamics Guidance**

A common theme is to support multiple authentications, critical to allowing users to transition to more secure authenticators. However, when doing so, adversaries can leverage an alternative, less secure authentication to gain access to the system. Easy Dynamics recommends that organizations consider:

1. Removing weaker authentication options
2. Increasing friction of reducing to a non-MFA Cryptographic authenticator
3. Limit entitlements and ensure authentication context is passed to relying parties and communicated for risk evaluation by the application

---

## SPEAR PHISHING

# Detection & Hunting 🔍

### AWS

**Recommendations**

Amazon Fraud Detector can be used to build a machine learning-driven solution modeled on phishing attack registries, known phishing attributes like those from the NIST Phish Scale, and custom data sets to alert administrators and users to potential phishing attacks.

Several third-party phishing detection solutions are available in the AWS Marketplace.

---

**References**

- [Amazon Fraud Detector](#)
- [AWS Marketplace: Phishing](#)

---

**Microsoft Azure**

**Recommendations**

Office 365's Threat Explorer can help detect phishing threats with confidence levels and top targeted users.

Azure Sentinel can leverage Fusion-based machine learning techniques to detect certain types of phishing attacks.

---

**References**

- [Office 365 Threat Explorer](#)
- [Advanced Multi-Stage Attack Detection in Azure Sentinel](#)

EVENT

# Supply Chain Compromised

## Targeted Identities by Access Risk



**Original Source Code**  
High Risk  
Legitimate code replaced by malicious code



**DevOps Engineers**  
Medium Risk  
Access to source code



**SolarWinds Vendor Identity**  
Medium Risk  
Trusted source of product updates



**Microsoft Software Trust Authority**  
High Risk  
Validates trusted source of product updates

## Event Description

Adversaries were able to compromise the build process of the SolarWinds Orion IT management product with SUNSPOT, a piece of malware specifically designed to inject SUNBURST code, the actual SolarWinds backdoor and customer threat, into the software build. By avoiding detection, the attackers were able to insert their malware into SolarWinds' supply chain. When SolarWinds' customers updated their software, the attackers' backdoor was distributed into thousands of networks across the globe, enabling the attackers to target networks of interest with secondary attack stages.<sup>11</sup>

<sup>11</sup> [Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.](#) (2020). FireEye.

## ATTACK TECHNIQUE

# Sidecar Process Malware Injection

The SUNSPOT malware used a sophisticated approach to intercept the compilation stage of the build environment in two pernicious ways:

-  Awaiting a build process, “it will spawn a new thread to determine if the Orion software is being built and, if so, hijack the build operation to inject SUNBURST. The monitoring loop executes every second, allowing SUNSPOT to modify the target source code on disk before it has been read by the compiler.”<sup>12</sup>
-  Once the build process is complete, SUNSPOT will restore “the original source code and [delete] the temporary [backdoor]” file.<sup>13</sup>

**MITRE ATT&CK IDs:** [T1053.005](#), [T1140](#), [T1036](#), [T1027](#), [T1480](#), [T1057](#), [T1565.001](#)

## SIDECAR PROCESS MALWARE INJECTION

# Mitigation

### Verify Build Environment

#### Mitigation

By using a trusted, and **verifiable** build environment, organizations can ensure that the environment used to compile software has not been tampered with.

#### Standards

NIST recommends adopting a [Secure Software Development Framework](#) (SSDF) that defines how organizations should approach building a supporting toolchain for software and defining security checks as part of that process.

#### Easy Dynamics Guidance

Containers have made the process of replicating well-known configurations easier than ever before. Hashes of container images verify that the same image is being used every time and address the issue of tampering quite well.

We recommend using a containerized build system to provide the well-known, verifiable build environments for organizations. Build containers can be customized to limit user permissions within the container to specific actions needed to execute the software build process.

Container-based builds can be used locally or as part of popular services such as GitHub Actions, CircleCI, Jenkins, etc.

<sup>12</sup> [SUNSPOT: An Implant in the Build Process](#). (2021). SUNSPOT.

<sup>13</sup> Ibid.

## Signature Verification

### Mitigation

Code signing can be an effective mechanism to verify the authenticity of code both before and after the compilation process. Digital signatures can and should be widely used to prevent tampering of both the build process and resulting artifacts.

---

### Standards

NIST's SSDF section on "Protect Software" includes recommendations to publicly provide hashes for release files using code signing with established certificate authorities.

---

### Easy Dynamics Guidance

All authors of software should be using git commit signatures to verify their source contributions. Instructions for GPG signing are available for both [GitHub](#) and [BitBucket](#). Each developer should have one key available for signing code to be submitted to a given project. Only commits signed with keys from trusted identities should be allowed into the git history and to kick off any build processes.

Additionally, the resulting artifacts of the build process need to be verified. This process relies heavily on having an untampered build environment and varies depending on how software is being distributed. A good first start is to publicly provide checksums for any downloadable portions of the software and follow best practices for the relevant distribution mechanism.

<https://reproducible-builds.org/> is a not-for-profit organization dedicated solely to this topic. Their site goes in-depth on how and why reproducible builds are so important. For those pursuing this effort, the site is well worth visiting.

---

## Approved Software

### Mitigation

By building and maintaining an approved list of software, it becomes less likely that malicious software will be introduced into an environment.

---

### Standards

- [NIST SP 800-53B CM-11](#)
- [NIST SP 800-53B CM-8](#)

---

### Easy Dynamics Guidance

Develop organizational guidance and policies on how and when software can be installed including pre-approved lists of software and how to properly install it.

---

## Principle of Least Privilege

### Mitigation

Follow best practices for creating service principals, avoiding administrative access if possible, and only granting access that is absolutely necessary to perform duties or access to system files and resources on the server.

**Standards** NIST SP 800-53 has recommendations for organizational policies and practices for implementing least privilege in [AC-6 Least Privilege](#).

Related controls:

- [AC-3 Access Enforcement](#)
- [AC-4 Information Flow Management](#)

[NIST 800-171 Rev2](#)

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts

---

**Easy Dynamics Guidance** There should be no remote access to the build process to prevent outside code or actors from manipulating or accessing the build environment.

The build process should read files directly from the source repository to ensure a single source of all changes to the code.

Access to the directories where source code is being read from during the compilation process should be restricted to the build tools.

---

## Password Policies

**Mitigation** Password complexity has varied through the years but updated guidance now includes user experience as a key element of tackling the problem.

---

**Standards** NIST SP 800-63B has recommendations about password policies including length, truncation, hints, rate limiting, encryption, storage, and comparing secrets against a database of stolen passwords from known breaches.

Verifiers SHOULD permit claimants to use “paste” functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and, in many cases, increase the likelihood that users will choose stronger memorized secrets.<sup>14</sup>

---

14 [NIST Special Publication 800-63B - 5.1.1.2 Memorized Secret Verifiers](#). (2017).

#### Easy Dynamics Guidance

If using memorized secrets, compare secrets against commonly used sources, such as those that we have curated:

- [Havelbeenpwned](#)
- [Google \(Preview\)](#)
- [Azure](#)

Some of these recommendations can be enforced through cloud provider services' password policies:

- [AWS User Pool Password Policies](#)
- [Azure AD Password Policies](#)
- [Enforce and monitor password requirements for users - Cloud Identity Help \(google.com\)](#)

Additional advanced security:

- [AWS Advanced Security to User Pool](#)

---

## SIDECAR PROCESS MALWARE INJECTION

# Detection & Hunting 🔍

### General/Any

#### Recommendation

Running scans on the produced/consumed binaries can aid in detecting a compromised supply chain. Should the supply chain become compromised as was the case during the SolarWinds attack, code signing will do little if anything to prevent a compromise. To help detect and prevent the supply chain compromise from affecting additional systems, binary scans of the provided software should be run to detect abnormal behavior and signs of malware.

Files that are critical to the build process need to be inspected for compromise. Checking the hash of files can ensure they have not been modified outside of the approved process for doing so. Checking file locations can also help to ensure files are not being supplied from outside or untrusted systems.

---

#### References

- [Defending Against Software Supply Chain Attacks \(cisa.gov\)](#)
- [Data Manipulation: Stored Data Manipulation, Sub-technique T1565.001 - Enterprise | MITRE ATT&CK®](#)
- [Hashing Source Code Files with Visual Studio to Assure File Integrity](#)

## GitHub/Bitbucket

### Recommendation

**Watch for unsigned or improperly signed commits.**

When accepting contributions to source code, ensure that the commits are signed with trusted keys known to belong only to the author of the trusted contributor.

---

### References

- [Signing commits - GitHub Docs](#)
  - [Signing commits - Bitbucket Docs](#)
  - [Requiring signed commits - GitHub](#)
-

## EVENT

## Stolen SAML Signing Key

### Targeted Identities by Access Risk

**System User on IdP/Directory Server**

High Risk

Often has elevated/super admin privileges

**DB User on IdP/Directory Server**

Medium Risk

Access to sensitive information

### Event Description

Another phase of this devastating cyberattack provided a means for the adversary to steal administrative credentials at either the identity provider system or database levels. The theft granted the attacker the ability to affect significant damage by obtaining the SAML token-signing keypair. This allowed the attacker to bypass any authentication and access control checks to create any SAML token, containing any desired privilege, and yet appear to have been issued from a trusted source.

## ATTACK TECHNIQUE

## Gained Admin Privileges on SAML Federation Server

Once perimeter defenses were breached, the threat actor was able to leverage existing trusts to acquire additional administrative permissions within the on-premises environment to laterally move using multiple different credentials. The credentials used for lateral movement were always different from those used for remote access. Once the APT actor gained local administrator privileges, they can use several techniques to gain lateral movement. Details on the method of acquiring those admin credentials, outside of those required by SolarWinds agents, have not been made public, but there are several techniques the adversary could have used:

1. Credential theft from service account - Harvest encrypted service credentials from the Local Security Authority (LSA) registry hive and inject them into any malicious service to achieve lateral movement.
2. Domain credential theft - From local Domain Credentials Cache (msvcachedv2), which contains hashes of domain user's credentials who have authenticated to the local

machine.

3. SAM hash harvesting – Credentials saved as NTLM hashes in SAM.

The adversary exploited existing privileges of the SolarWinds software and used them to escalate permissions and gain access to high value assets, including the IdP’s SAML token-signing certificate, enabling them to bypass authentication via the “Golden SAML” attack, first identified and reported by CyberArk in 2017.

**MITRE ATT&CK ID:** [T1078](#)

## GAINED ADMIN PRIVILEGES ON SAML FEDERATION SERVER

# Mitigation

### Principle of Least Privilege

<b>Mitigation</b>	Follow best practices for creating of service principals, avoiding administrative access if possible and only granting access that is absolutely necessary to perform duties or access to system files and resources on the server.
<hr style="border-top: 1px dashed #ccc;"/>	
<b>Standards</b>	<p>NIST SP 800-53 has recommendations for organizational policies and practices for implementing least privilege in <a href="#">AC-6 Least Privilege</a>.</p> <p>Related controls:</p> <ul style="list-style-type: none"> <li>• <a href="#">AC-3 Access Enforcement</a></li> <li>• <a href="#">AC-4 Information Flow Management</a></li> </ul> <p><a href="#">NIST 800-171 Rev2</a> 3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts</p>
<hr style="border-top: 1px dashed #ccc;"/>	
<b>Easy Dynamics Guidance</b>	<p>Perform a full audit to identify all privileged and service account access on-premise, in the cloud, including local, domain and accounts. Evaluate permissions and document justification for persistent permission assignment.</p> <p>Unassign unnecessary local administrative privileges. When vendor applications require local administrative privileges, work with them to identify the necessary access and grant only those privileges required for the application to function properly.</p>

## Privileged Account Management

**Mitigation** Privileged access, often with broad network access, can have a significant potential impact and should be protected at all costs. Recent architectures are emerging for fine-grained access in cloud environments.

**Standards** NIST SP 800-53 has recommended controls for limiting remote access in [AC-17 Remote Access](#).  
NIST SP 800-207 [Zero Trust Architecture](#) provides a definition for ZTA and gives general deployment models with use cases for organizations to begin their ZT journeys.

**Easy Dynamics Guidance** We find that the guidance in NIST 800-53 AC-17 is outdated as it heavily emphasizes the use of virtual private networks (VPNs) for remote access.  
Easy Dynamics recommends that organizations move towards a Zero Trust Architecture (ZTA) for highly dynamic, cloud-based environments. Avoid using VPN or bastion hosts and use an access gateway or controller that leverages a non-repudiable identity and issues short-lived ephemeral tokens and certificates.

- [Zero Trust Deployment Center | Microsoft Docs](#)
- [Zero Trust architectures: An AWS perspective | AWS Security Blog \(amazon.com\)](#)
- [Google BeyondCorp for Zero Trust Models](#)

Additional guidance on a reference architecture for cloud-based ZTA remote access:  
[A Reference Architecture for Fine-Grained Access Management on the Cloud \(infoq.com\)](#)

---

## Ephemeral Credentials through Just-in-Time (JIT) / Just Enough Admin (JEA) Access

**Mitigation** Elevation of human and non-human access in real-time for a set period of time with granular permissions to perform privileged access by minimizing standing access.

**Standards** NIST 800-53 has recommendations for account management and access enforcement in

- [AC-2 Account Management](#)
- [AC-3 Access Enforcement](#)

**Easy Dynamics Guidance** Evaluate Privileged Access Management (PAM) solution to validate existing configurations, leverages an MFA Access manager, supports ephemeral credentials, record sessions, and supports behavioral analytics to detect anomalies.

---

## Restrict Tier0 Access

**Mitigation** Limit access to assets that provide direct control of security and identity infrastructure from a hardened control point.

**Standards** NIST 800-53 does not have direct guidance on Tier0 but does provide guidance on access enforcement.

- [AC-2 Account Management](#)
- [AC-3 Access Enforcement](#)
- [CP-10 System Recovery and Reconstitution](#)

---

**Easy Dynamics Guidance** Enable access to Tier0 assets through a governed Privileged Access Workstation, that acts as a hardened control point. If using virtual desktop interface (VDI), rebuild images on a periodic frequency that meets your organization's risk posture.

---

## Usage of High Entropy Secrets

**Mitigation** For service accounts and service principals with administrative rights, use high entropy secrets, like certificates, stored securely.

---

**Standards** [NIST SP 800-63B](#) – Sec. 5 Authenticator and Verifier Requirements and 8.2 Threat Mitigation Strategies.

---

**Easy Dynamics Guidance** Include monitoring of changes to secrets for service accounts and service principals within security monitoring program.

---

## Protect Private Keys

**Mitigation** Store private keys on persistent storage that is highly governed and in a non-exportable manner.

---

**Standards** [NIST 800-57 Part 2](#), Recommendation for Key Management.

[FIPS 140-3](#), Security Requirements for Cryptographic Modules.

---

**Easy Dynamics Guidance** If the SAML token signing server supports Hardware Security Modules (HSM), the SAML token-signing keys should be generated and stored in FIPS-201 compliant HSM. This would prevent the theft of private cryptographic keys. The focus would then shift to restricting access to processes that can programmatically call the HSM API to create digital signatures.

If installing certificates on a local machine, ensure private keys cannot be exported.

Ensure that management events related to private keys (and other high-value assets) are logged and auditable. This includes general read operations as well as failed operations.

---

## Revoke signing certificates

**Mitigation** Ensure compromised certificates are revoked. Issue new certificates on the AD FS server(s) and synchronize them to Azure AD (and any other cloud applications that use AD FS for authentication).

**Standards** [NIST SP 800-63B](#) – Sec. 5 Authenticator and Verifier Requirements and 8.2 Threat Mitigation Strategies.

**Easy Dynamics Guidance** Rotate the token-signing AD FS certificate in rapid succession twice to ensure the compromised certificate is no longer cached.<sup>15</sup>

## GAINED ADMIN PRIVILEGES ON SAML FEDERATION SERVER

# Detection & Hunting 🔍

### Windows/Microsoft Domain Environment

**Environment** Windows/Microsoft Domain Environment

**Recommendations** Search logs for high-volume of LDAP queries in short time filtering for non-DC devices. This is a sign of APT reconnaissance and an attempt to find highly privileged accounts for lateral movement.

Search logs for Enumeration of high-value DC assets followed by logon attempts. This validates the fact that credentials were stolen and subsequently used. This will help identify privileged access accounts that were compromised along with the timestamp to figure out a point in time when additional hunting for exfiltration or compromise should begin.

**References** [Using Microsoft 365 Defender to protect against Solorigate - Microsoft Security](#)

### Windows Server Operating Systems

**Environment** Windows Server Operating Systems

**Recommendations** Identifying certificate export events in ADFS: Search event logs for certificate export events in ADFS.<sup>16</sup>

**References** [Sygnia Advisory for Detection of Golden SAML attacks](#)

<sup>15</sup> [Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452](#). (2020). MANDIANT/FireEye.

<sup>16</sup> Search for 1) event id 1007 (enabled by default) in the 'Microsoft-Windows-CertificateServicesClient-Lifecycle-System' Windows Event Log; 2) PowerShell script block logs: search for event ids ,Export-PfxCertificate' or ,certutil -exportPFX' in event ids 4103 and 4104; 3) Command line audit tools to find event id 4688 'certutil -exportPFX'; 4) Look for Sysmon Event id 18 – certificate extraction with ADFSdump

EVENT

# Creating and Impersonating New Trusted Identities and Credentials

## Targeted Identities by Access Risk



**Existing User Identities**

Varied Risk

Addition of identities to an application's permitted users reveals new attack surfaces



**Any Established Identity, Whether Person or Privileged Service Account**

High Risk

Attackers can select highly privileged accounts with access to sensitive systems and data

## Event Description

Once the SAML token-signing certificate was acquired, the intruder could forge SAML tokens with any desired entitlements and lifetime they chose. Since the token is signed with an actual SAML token-signing private key, the actor can access, for an identity profile with the required entitlements, any resource configured to trust the SAML token-signing certificate. This allows the actor to impersonate the most highly privileged accounts within the network, including super administrators.

Forged credentials, using the SAML tokens created by the compromised token signing certificate, could then be granted the entitlements to further gain additional access to any resources or cloud environment (regardless of vendor) configured to trust the certificate. For instance, the actor could use their administrator privileges to grant additional permissions to the target Application or Service Principal.<sup>17</sup> Given that SAML tokens are signed with their own trusted certificate, the behavior is highly likely to go unnoticed without advanced behavioral monitoring by the organization.

Additional authentication credentials were added to existing Microsoft Azure service principals (The service principal object defines an application's authorized actions within a cloud tenant instance, the individuals that can access the application, and the resources an application can access.).

<sup>17</sup> [Customer Guidance on Recent Nation-State Cyber Attacks](#). (2020). MSRC.

## ATTACK TECHNIQUE

# Addition of Backdoor Credentials for Robust Persistence

To achieve a more reliable persistence mechanism as network defenders are attempting to purge the intruder, the intruder was able to create additional credentials to leverage as a backdoor if they need to get back into the compromised systems later. They achieved this by utilizing the forged SAML token certificates, to compromise at least one web platform:

1. “CISA has observed the threat actor adding authentication credentials, in the form of assigning tokens and certificates, to existing Azure/Microsoft 365 (M365) application service principals. These additional credentials provide persistence and escalation mechanisms and a programmatic method of interacting with the Microsoft Cloud tenants (often with Microsoft Graph Application Programming Interface [API]) to access hosted resources without significant evidence or telemetry being generated.”<sup>18</sup>
2. “The actor has been observed adding credentials (X.509 keys or password credentials) to one or more legitimate OAuth Applications or Service Principals.”<sup>19</sup>

**MITRE ATT&CK ID:** [T1098.001](#), [T1484](#), [T1606.002](#)

## ADDITION OF BACKDOOR CREDENTIALS FOR ROBUST PERSISTENCE

# Mitigation

### Privileged Account Management

#### Mitigation

Privileged access, often with broad network access, can have a significant potential impact and should be protected at all costs. Recent architectures are emerging for fine-grained access in cloud environments.

#### Standards

NIST SP 800-53 has recommended controls for limiting remote access in [AC-17 Remote Access](#).

NIST SP 800-207 [Zero Trust Architecture](#) provides a definition for ZTA and gives general deployment models with use cases for organizations to begin their ZT journeys.

<sup>18</sup> [Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations](#). (2020). CISA Alert (AA20-352A).

<sup>19</sup> [Customer Guidance on Recent Nation-State Cyber Attacks](#). (2020). MSRC.

**Easy Dynamics Guidance**

We find that the guidance in NIST 800-53 AC-17 is outdated as it heavily emphasizes the use of virtual private networks (VPNs) for remote access.

Easy Dynamics recommends that organizations move towards a Zero Trust Architecture (ZTA) for highly dynamic, cloud-based environments. Avoid using VPN or bastion hosts and use an access gateway or controller that leverages a non-repudiable identity and issues short-lived ephemeral tokens and certificates.

- [Zero Trust Deployment Center | Microsoft Docs](#)
- [Zero Trust architectures: An AWS perspective | AWS Security Blog \(amazon.com\)](#)
- [Google BeyondCorp for Zero Trust Models](#)

Additional guidance on a reference architecture for cloud-based ZTA remote access:  
[A Reference Architecture for Fine-Grained Access Management on the Cloud \(infoq.com\)](#)

**User Account Management**

**Mitigation**

User Account Management

**Standards**

NIST 800-53, Section 3.1

**Easy Dynamics Guidance**

Ensure that user accounts with administrative rights follow best practices, including use of privileged access workstations, Just in Time/Just Enough Administration (JIT/JEA), and strong authentication. Reduce the number of users that are members of highly privileged Directory Roles. To reduce the attack surface of the organizations system employ the principle of least privilege.<sup>20</sup>

**Approved Software**

**Mitigation**

Reduce surface area by removing/disabling unused or unnecessary applications and service principals. Reduce permissions on active applications and service principals, especially application (AppOnly) permissions. [Customer Guidance on Recent Nation-State Cyber Attacks – Microsoft Security Response Center.](#)

**Standards**

- [NIST SP 800-53B CM-11](#)
- [NIST SP 800-53B CM-8](#)

<sup>20</sup> [Customer Guidance on Recent Nation State Cyberattacks.](#) (2020). MSRC.

**Easy Dynamics Guidance**

As a global administrator validate enterprise applications and application registrations in Azure AD. If these applications and service principals are not in use, then remove them so that the attack surface area is reduced and the potential for breach is limited.

Keep an inventory of all applications and registrations. Periodically audit and validate them continuously to maintain and improve your security posture.

---

**ADDITION OF BACKDOOR CREDENTIALS FOR ROBUST PERSISTENCE**

## Detection & Hunting 🔍

### Windows Server

**Recommendations**

If you have not done so already, enable audit policies for employee devices as well as servers. This will help the collection of information that is relevant to any advanced persistent threats.

After configuring them, forward events to Azure Sentinel and look for the following:

- Account logon events that are not expected.
- Creation or modification of users, security groups, distribution groups.

---

**References**

- [Audit Policy Recommendations | Microsoft Docs](#)
- [Connect Windows security event data to Azure Sentinel | Microsoft Docs](#)
- [User Account Added to Privileged Group](#)
- [Group added to Privileged Group](#)

---

### AWS

**Recommendations**

Connect AWS Cloud Trail events to Azure Sentinel and look for any changes to IAM policies. While some of them may be warranted, change to policies is indicative of threat actors trying to evade detection.

---

**References**

- [AWS IAM Policy Change](#)

## ATTACK TECHNIQUE

## Lateral Movement and Privilege Escalation Using Stolen SAML Signing Key

The theft of the SAML token signing key is disastrous to an organization's cybersecurity because that signing key is the root of trust for the entire enterprise. It can be used to forge any request as any user (including administrator) to any network service that trusts that signing key to sign SAML session tokens. Essentially, the adversary now has full access and full control of the network.

Specifically, with the ability to alter crucial aspects of the SAML token signing process, the threat actor:

-  Can "add illegitimate credentials to existing application service principals, enabling the attacker to call APIs with the permission assigned to that application."
-  Has the freedom to both move laterally within the victim's organization, and to exfiltrate data.

With keys in hand, the attacker has the capability to create new SAML tokens based on trusted sources, including those with elevated privileges. These were used to sign SAML tokens that could be verified against the identity provider's legitimate public key.<sup>21</sup>

The specific technique used, known as the Golden SAML attack, was published by CyberArk in 2017; however, this was the first known incident in the wild.<sup>22</sup> The authorization flow for a forged token is approximately as follows:

-  The attacker (via a browser) tries to access a protected resource within the application (service provider) while impersonating a legitimate user.
-  The application determines the correct identity provider and redirects the attacker's browser to login via an identity provider along with instructions on where to send the browser back when the login has been accepted.
-  The attacker intercepts the authentication request, forges a SAML token representing assertions of the impersonated user, adds desired privileges, and redirects the browser back to the application.
-  The application verifies the assertions against the identity provider's public key assuming the user is legitimate and redirects the attacker's browser to protected resources they are authorized to access.

21 [Advice for incident responders on recovery from systemic identity compromises](#). (2020). MSRC.

22 LaFerrera, M. (2021). [A Golden SAML Journey: SolarWinds Continued](#). Splunk.

Based on observed, post-compromise activity, the attacker used the forged SAML tokens to move laterally for surveillance and data theft.<sup>23</sup>

It is important to note the following characteristics of the SAML-based attack:

1. There is no defect in the SAML protocol involved in this attack. The attacker was able to forge properly signed SAML tokens because the token-signing private keys were stolen.
2. This type of attack is theoretically possible to cross every enterprise service that relies on SAML 2.0 for Single Sign-On. It is not specific to organizations using SolarWinds products or Microsoft Active Directory Federation Services (AD FS).
3. The Microsoft Detection and Response Team (DART) has noted: “Anomalous logins using the SAML tokens signed with a compromised token-signing certificate, which can be used against any on-premises resources (regardless of identity system or vendor) as well as against any cloud environment (regardless of vendor) because they have been configured to trust the certificate. An organization may miss the use of illegitimate SAML tokens because they are signed with a legitimate certificate” (DART, 2020).
4. Using the stolen private key, the attackers can systematically generate SAML tokens that would have been legitimately generated after federated login, thereby effectively “bypass[ing] the Duo multi-factor authentication (MFA) protecting access to Outlook Web App (OWA)” (CISA Alert AA20-352A, 2020).

**MITRE ATT&CK ID:** [T1558, T1606.002](#)

---

<sup>23</sup> [Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor](#). (2021). FireEye.

## LATERAL MOVEMENT AND PRIVILEGE ESCALATION USING STOLEN SAML SIGNING KEY

# Mitigation

### Password Policies

#### Mitigation

Password complexity has varied through the years but updated guidance now includes user experience as a key element of tackling the problem.

---

#### Standards

NIST SP 800-63B has recommendations about password policies including length, truncation, hints, rate limiting, encryption, storage, and comparing secrets against a database of stolen passwords from known breaches.

Verifiers SHOULD permit claimants to use “paste” functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and, in many cases, increase the likelihood that users will choose stronger memorized secrets.<sup>24</sup>

---

#### Easy Dynamics Guidance

If using memorized secrets, compare secrets against commonly used sources, such as those that we have curated:

- [Havelbeenpwned](#)
- [Google \(Preview\)](#)
- [Azure](#)

Some of these recommendations can be enforced through cloud provider services' password policies:

- [AWS User Pool Password Policies](#)
- [Azure AD Password Policies](#)
- [Enforce and monitor password requirements for users - Cloud Identity Help \(google.com\)](#)

Additional advanced security:

- [AWS Advanced Security to User Pool](#)

---

### Privileged Account Management

#### Mitigation

Privileged access, often with broad network access, can have a significant potential impact and should be protected at all costs. Recent architectures are emerging for fine-grained access in cloud environments.

---

#### Standards

NIST SP 800-53 has recommended controls for limiting remote access in [AC-17 Remote Access](#).

NIST SP 800-207 [Zero Trust Architecture](#) provides a definition for ZTA and gives general deployment models with use cases for organizations to begin their ZT journeys.

---

<sup>24</sup> [Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations](#). (2020). CISA Alert (AA20-352A).

#### Easy Dynamics Guidance

We find that the guidance in NIST 800-53 AC-17 is outdated as it heavily emphasizes the use of virtual private networks (VPNs) for remote access.

Easy Dynamics recommends that organizations move towards a Zero Trust Architecture (ZTA) for highly dynamic, cloud-based environments. Avoid using VPN or bastion hosts and use an access gateway or controller that leverages a non-repudiable identity and issues short-lived ephemeral tokens and certificates.

- [Zero Trust Deployment Center | Microsoft Docs](#)
- [Zero Trust architectures: An AWS perspective | AWS Security Blog \(amazon.com\)](#)
- [Google BeyondCorp for Zero Trust Models](#)

Additional guidance on a reference architecture for cloud-based ZTA remote access:  
[A Reference Architecture for Fine-Grained Access Management on the Cloud \(infoq.com\)](#)

---

### Key Rotation

#### Mitigation

Rotating token signing key is important to prevent key exhaustion, leakage, and exposure. The longer the key is used, the higher the probability of a breach.

---

#### Standards

[NIST SP 800-57](#)

---

#### Easy Dynamics Guidance

If your ADFS server has been compromised then rotate the token-signing AD FS certificate in rapid succession twice to ensure the compromised certificate is no longer cached.

For the long term establish a process (automated or human) to rotate the token-signing keys periodically.

---

### Restrict Tier0 Access

#### Mitigation

Limit access to assets like AD FS farms and domain controllers.

---

#### Standards

[NIST 800-53](#) - AC-2 Account Management, AC-3 Access Enforcement, and CP-10 System Recovery and Reconstitution.

---

#### Easy Dynamics Guidance

Enable access to Tier0 assets through a governed Privileged Access Workstation, that acts as a hardened control point. If using virtual desktop interface (VDI), rebuild images on a periodic frequency that meets your organization's risk posture.

## LATERAL MOVEMENT AND PRIVILEGE ESCALATION USING STOLEN SAML SIGNING KEY

# Detection & Hunting 🔍

### Microsoft Azure - Windows Server

#### Recommendations

Forward Windows events to Azure Sentinel and look for the following:

Look for user accounts, especially privileged and service accounts, behaving abnormally.

Correlate service provider login events with corresponding authentication events in ADFS and Domain Controllers may help yield suspicious logins. Search for logins to service providers using SAML SSO which do not have corresponding 4769 (Kerberos service ticket was requested), 1200 (Federation Service issued a valid token), and 1202 (Federation Service validated a new credential).

Also, hunt for the following events to search privilege escalation:

4672(S): Special privileges assigned to new logon, 4674(S, F): An operation was attempted on a privileged object.

---

#### References

- [Sygnia Advisory for Detection of Golden SAML attacks](#)
- [4674\(S, F\) An operation was attempted on a privileged object. \(Windows 10\) - Windows security | Microsoft Docs](#)
- [4672\(S\) Special privileges assigned to new logon. \(Windows 10\) - Windows security | Microsoft Docs](#)

## EVENT

# Addition of Federation Trusts to IdP Server

## Targeted Identities by Access Risk

**Pool of External Users**

Medium Risk

External and now trusted users would likely have the default application access specified by the organization

## Event Description

Additional federation trusts were added to the existing IdPs, including on-premises environments, which could allow for the actual authentication of an entire pool of users to take place using the attacker's specified infrastructure, outside of an organization.

## ATTACK TECHNIQUE

# Authentication of External Bad Actors through Federation Trusts

Propelling the attack to another level, "...if the malicious cyber actors [were] unable to obtain an on-premises signing key, they would attempt to gain sufficient administrative privileges within the cloud tenant to add a malicious certificate trust relationship for forging SAML tokens."<sup>25</sup> This enabled:

- The addition of new federation trusts allows the advanced persistent threat (APT) actors to provision and authenticate new user accounts that present SAML signing-tokens that will be trusted by any application leveraging the IdP for authentication.<sup>26</sup>
- "Authentication [to] occur outside of an organization's known infrastructure and may not be visible to the legitimate system owner."<sup>27</sup>

25 [Detecting Abuse of Authentication Mechanisms](#). (2020). NSA.

26 [Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations](#). (2020). CISA Alert (AA20-352A).

[Customer Guidance on Recent Nation-State Cyber Attacks](#). (2020). MSRC.

27 [Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations](#). (2020). CISA Alert (AA20-352A).

**MITRE ATT&CK ID:** [T1484.002](#)

## AUTHENTICATION OF EXTERNAL BAD ACTORS THROUGH FEDERATION TRUSTS

# Mitigation

### Approval for Domain Trust Modifications

<b>Mitigation</b>	Requiring a second approval for modifications to domain trust policies mitigates risk by requiring an attacker to have access to multiple accounts with the ability to add federated trust.
<b>Standards</b>	NIST controls recommend requests to create accounts, which is analogous to adding federated trusts, require approval by organization-defined personnel or roles. <sup>28</sup>
<b>Easy Dynamics Guidance</b>	Purchase, integrate, and develop ICAM products that require second party approval when adding federated trust partners. This concept is like principles implemented in missile launch systems that require two physical keys and the concurrence of two operators to approve a launch.

### Principle of Least Privilege

<b>Mitigation</b>	Follow best practices for creating service principals, avoiding administrative access if possible, and only granting access that is absolutely necessary to perform duties or access to system files and resources on the server.
<b>Standards</b>	<p>NIST SP 800-53 has recommendations for organizational policies and practices for implementing least privilege in <a href="#">AC-6 Least Privilege</a>.</p> <p>Related controls:</p> <ul style="list-style-type: none"><li>• <a href="#">AC-3 Access Enforcement</a></li><li>• <a href="#">AC-4 Information Flow Management</a></li></ul> <p><a href="#">NIST 800-171 Rev2</a> 3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts</p>
<b>Easy Dynamics Guidance</b>	Use Role-Based Access Control and ensure that roles for users and user groups are updated, as necessary. The default setting should be limited, with no access to federated trust settings. Only assign roles with more access as the need arises. This reduces risk by making it less likely a compromised account can add federation trusts to the IdP.

28 [Security and Privacy Controls for Information Systems and Organizations](#). (2020). NIST.

## Just-in-Time Access

### Mitigation

Similar to the principle of least privilege, restrict the ability to modify domain trust to only the time that it is necessary. Meaning, grant privileges to modify federated trusts to accounts as necessary, for a set period of time. The typical user will not need 24/7 access to federation settings.

### Standards

NIST 800-53 has recommendations for account management and access enforcement in

- [AC-2 Account Management](#)
- [AC-3 Access Enforcement](#)

### Easy Dynamics Guidance

Deploy a Privileged Access Management (PAM) solution to validate existing PAM configurations, support JIT access provisioning, record sessions and supports behavioral analytics to detect anomalies. Modern PAM solutions lease credentials and any credential requested with the ability to create a new trust should be tightly governed and monitored. Meaning, make it hard to get a credential that can actually create a new federation trust.

- [Xton Access Manager](#)
- <https://www.boundaryproject.io>
- <https://goteleport.com>

## AUTHENTICATION OF EXTERNAL BAD ACTORS THROUGH FEDERATION TRUSTS

# Detection & Hunting 🔍

### General

#### Recommendations

Utilize a logging solution with alerts for any creation, updates, or deletions of federated trusts. Identify the event type/signature of modifications to domain trust and monitor events of that type.

Look for indications of the attackers:

- Making configuration changes in the Identity Provider.
- Using an access token associated with an existing application or service principal and using that access token to call APIs with the permissions assigned to that application or principal.

#### References

[Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments](#)

### Microsoft Azure

#### Recommendations

Perform Azure Sentinel queries to track domain federation trust settings modifications. This will return notifications when new federations are added, or when existing federation privileges are upgraded. When this occurs, double-check to ensure that the changes to federation were made by the organization. If you are using Okta or Azure AD in conjunction with Azure, you can link their output to Azure Sentinel to make it easier to monitor.

---

**References**

- [SolarWinds Post-Compromise Hunting with Azure Sentinel](#)
- [Azure Sentinel Query for Detecting ADFS Domain Trust Modifications](#)
- [Connecting Okta SSO Data to Azure Sentinel](#)
- [Connecting Azure AD Data to Azure Sentinel](#)

---

**AWS Cognito****Recommendations**

If you are using AWS Cognito as an ICAM solution, consider logging Cognito events in CloudTrail. This will allow you to query for modifications to the User Pools and detect any suspicious activity.

---

**References**

- [Logging Amazon Cognito API Calls with AWS CloudTrail](#)
- [Amazon Cognito User/Identity Pool Actions](#)

---

**Sygnia****Recommendations**

Detecting malicious ADFS trust modification. Search for event id 307 (The Federation Service configuration was changed). Event id 510 with the same Instance ID – could be more than one event per single 307 event. These events should be reviewed, specifically searching for “Configuration: Type: IssuanceAuthority” where “Property Value” references an unfamiliar Domain.

---

**References**

[Sygnia Advisory for Detection of Golden SAML attacks](#)

---

**Okta****Recommendations**

Search for Events in the [Okta System Log API](#) that correspond to modifications of domain trusts. A good place to start would be to confirm that all events of type “system.idp.lifecycle.create” are expected and valid.

---

**References**

- [Okta Event Types](#)
- [Okta Log Formats and Examples](#)

EVENT

# Email Accounts Compromised

## Targeted Identities by Access Risk



### IT Administrators

High Risk

Often has access to escalate privileges and reset credentials to other accounts



### Individuals with Sensitive Email

High Risk

While in some cases it might be difficult to target which users might have sensitive data in emails, if the right individual is compromised the consequences could be disastrous



### OAuth Application & Service Principal Credentials

High Risk

Rogue or compromised principals created in Azure AD with consent to user information across the entire platform of applications

## Event Description

CISA has observed SAML tokens to target email accounts belonging to key personnel, including IT and incident response personnel.<sup>29</sup> The same technique can be used to impersonate those key personnel for other system access.

Since the SAML authentication token is generated after a user is challenged for multi-factor authentication (MFA), this SAML attack bypasses MFA. Similarly, changing an account password will not negate an already issued forged SAML token.

The actor has been observed adding credentials (X.509 keys or password credentials) to one or more legitimate OAuth Applications or Service Principals, usually with existing *Mail.Read* or *Mail.ReadWrite* permissions, which grants the ability to read mail content from Exchange Online via Microsoft Graph or Outlook REST. Examples include mail archiving applications. Permissions are usually, but not always, AppOnly.<sup>30</sup>

<sup>29</sup> [Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations](#). (2020). CISA Alert (AA20-352A).

<sup>30</sup> [Customer Guidance on Recent Nation-State Cyber Attacks](#). (2020). MSRC.

ATTACK TECHNIQUE

# Compromised Email Authentication Through Signed SAML Tokens

Data access has relied on leveraging minted SAML tokens to access user files/email or impersonating the Applications or Service Principals by authenticating and obtaining Access Tokens using credentials. The actor periodically connects from a server at a hosting provider to access specific users' emails using the permissions granted to the impersonated Application or Service Principal. In many cases, the targeted users are key IT and security personnel. By impersonating existing applications that use permissions like Mail.Read to call the same APIs leveraged by the actor, the access is hidden amongst normal traffic. For this reason, if you suspect you are impacted you should assume your communications are accessible to the actor.<sup>31</sup>

**MITRE ATT&CK ID:** [T1098.002](#), [T1114](#), [T1071.003](#), [T1567](#)

COMPROMISED EMAIL AUTHENTICATION THROUGH SIGNED SAML TOKENS

## Mitigation

### Avoid the use email for sensitive information

**Mitigation**

SMTP is a dated protocol and should be avoided for sensitive transfer of information.

**Standards**

[August 2020 ITL Bulletin - Security Considerations for Exchanging Files Over the Internet \(nist.gov\)](#)

NIST SP 800-53 includes controls regarding Access Control and Enforcement.  
[AC-4 Information Flow Management.](#)

[NIST SP 800-45 Version2](#), Section 3 Signing and Encrypting Email Messages.

31 [Customer Guidance on Recent Nation-State Cyber Attacks](#). (2020). MSRC.

**Easy Dynamics Guidance**

Email was designed without consideration for encryption and thus encryption systems are bolted on after the fact. Sensitive information can travel with no chain of custody or ability to identify the original source of material because it can easily be scrubbed, making unattributed data exfiltration a simple task. Adding encryption protects the message at transport and gives a false sense of trust in the sender without assurances for how the user accessed the email system.

If sensitive information is to be transmitted via email encrypt the email and provide another layer of security as it requires both the encryption key and the private certificate to decrypt the email. This is supported by Outlook clients. [S/MIME for encryption in Exchange Online - Office 365 | Microsoft Docs](#).

Evaluate controls enforced by the credential service provider for email systems to force a minimum of [Authenticator Assurance Level 2](#).

Ultimately, when transmitting sensitive information, it is best to use a system designed from the ground up for the secure transmission of data.

---

## Encrypt Sensitive Information

**Mitigation**

Sensitive information persisted to block storage should be evaluated for encryption.

**Standards**

NIST SP 800-53 includes controls regarding protecting sensitive information in: [SC-28 Protection of Information at Rest](#). NIST SP800-175B Rev1, [Guideline for Using Cryptographic Standards in Federal Government: Cryptographic Mechanisms](#).

**Easy Dynamics Guidance**

Increasing access rigor through front door attacks of email systems does not protect if local, administrative access has been gained by an adversary. Encryption of data at rest provides additional defenses. Use proven, standard algorithms and store private keys in an acceptable key vault.

---

## Network Intrusion Prevention

**Mitigation**

System monitoring includes an ability to detect and notify based on malicious.

**Standards**

[NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems \(IDPS\)](#), Section 4, Network Based IDPS.

NIST SP 800-53 includes controls for [SI-4 System Monitoring](#).

**Easy Dynamics Guidance**

Increasing access rigor through front door attacks of email systems does not protect if local, administrative access has been gained by an adversary. Encryption of data at rest provides additional defenses. Use proven, standard algorithms and store private keys in an acceptable key vault.

## Data Loss Prevention

### Mitigation

Once an adversary has gained control of a system, additional DLP features can restrict handling of the data.

### Standards

[FIPS 199, Standards for Security Categorization of Federal Information and Information Systems \(nist.gov\)](#)

NIST SP 800-53 includes controls for data loss:

[SC-7 Boundary Protection](#)

[SC-7 \(10\) Data Exfiltration](#)

### Easy Dynamics Guidance

Establish policies to classify information and ensure your organization has systems to support data loss prevention. Create policies that support email data classification that supports SMTP messages and attachments. DLP packages can prevent exfiltration of information it does make it harder for attackers to extract sensitive information. DLP policies should be juxtaposed with the categorization of information within your organization.

---

## COMPROMISED EMAIL AUTHENTICATION THROUGH SIGNED SAML TOKENS

# Detection & Hunting 🔍

### General

#### Recommendations

If you are using Azure Sentinel, then check the audit logs for applications that have been granted read permissions to mailboxes followed by consent to use the application. Going through this exercise will help validate the legitimacy of access.

Another way to detect the compromise of email accounts is to check for signs of exfiltration. The access of mail items using Microsoft's Graph API can be audited and anomalies in the volume of queries made against the API can be detected and validated using Azure Sentinel.

Finally, if you have a Microsoft 365 E5 subscription you can also detect the compromise of email accounts by analyzing the Azure Sentinel logs for Exchange Online events related to exfiltration. This is slightly different from the previous query where the mail items are accessible via the Graph API. In this case, a high volume of accessing mail items directly from a client application is indicative of exfiltration.

## References

[Using Microsoft 365 Defender to protect against Solorigate - Microsoft Security](#)

See [Anomalous use of MailItemAccess by GraphAPI](#) for more details.

For more information see [MailItemsAccessed throttling](#).

---

# Conclusion

Even after you have taken every possible step to remove the threat actor, there is no guarantee the bad guys have been purged and no longer have access to your organization's data. Since the SolarWinds attack has been described by Microsoft's CEO as "the largest and most sophisticated attack the world has ever seen," many organizations have had to reprioritize strategic initiatives to respond to this incident and protect themselves from potential future ones. Hackers infiltrated government systems, including Treasury, Justice, and Homeland Security, as well as major private sector organizations, reaching all the way to critical and sensitive source code at Microsoft. There has never been a more important time to evaluate how crucial Cybersecurity will be for protecting our economic livelihood and expected standard of living. Attack vectors targeting Digital Identities have been and will continue to grow as a successful means for our adversaries to gain access to and take control of our information systems.

Easy Dynamics has been an enabler of Digital Identity centric services for organizations across public and private sectors since 2010. We will continue to help in the education of leading practices and support our nation's initiatives in bringing attention, improving how we evaluate risk, management privacy, and learning from events such as this to improve how we address threats in the future.



For questions or media inquiries,  
please send us a message at:

[whitepapers@easydynamics.com](mailto:whitepapers@easydynamics.com)

# References

Bienstock, D., & Baker, A. (2019, March 21). Print media Academy. Retrieved May 2021 ,04, from <https://troopers.de/troopers19/agenda/fpxwmn/>

Channele2e. (2021). SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details. Retrieved from <https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/>

Cimpanu, Catalin. (2020, December 31). SolarWinds hackers accessed Microsoft source code. ZDNet. <https://www.zdnet.com/article/solarwinds-hackers-accessed-microsoft-source-code/>

Cimpanu, Catalin. (2021, January 12). Third malware strain discovered in SolarWinds supply chain attack. ZDNet. <https://www.zdnet.com/article/third-malware-strain-discovered-in-solarwinds-supply-chain-attack/>

Conikee, Chetan. (2021, January 3). #Solorigate : SUPERNOVA forensics using Code Property Graph. Security Boulevard. <https://securityboulevard.com/01/2021/solorigate-supernova-forensics-using-code-property-graph/>

CrowdStrike Intelligence Team. (2021, January 11). SUNSPOT: An Implant in the Build Process. CrowdStrike. <https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/>

Detection and Response Team (DART). (2020, December 21). Advice for incident responders on recovery from systemic identity compromises. Microsoft. <https://www.microsoft.com/security/blog/21/12/2020/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/>

ExtraHop. (2021, January 19). Threat Intel: Analyzing the SolarWinds Attack. CSO Online. <https://www.csoonline.com/article/3603586/threat-intel-analyzing-the-solarwinds-attack.html>

FireEye. (2020, December 13). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. Threat Research. <https://www.fireeye.com/blog/threat-research/12/2020/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>

FireEye/Mandiant. (2021, April 9). Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452. Retrieved from <https://www.fireeye.com/content/dam/collateral/en/wp-m-unc2452.pdf>

GitHub. (2021). Shadow0ps/solorigate\_sample\_source. [https://github.com/Shadow0ps/solorigate\\_sample\\_source](https://github.com/Shadow0ps/solorigate_sample_source)

Heckman, Jory. (2021, March 10). CISA: 'Identity is everything' for cyber defense post-SolarWinds. Federal News Network. <https://federalnewsnetwork.com/cybersecurity/03/2021/cisa-identity-is-everything-for-cyber-defense-post-solarwinds/>

Hinchliffe, Alex. (2019, March 15). DNS Tunneling: How DNS can be (ab)used by malicious actors. UNIT 42, Palo Alto Networks. <https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors/>

LaFerrera, Marcus. (2021, January 8). A Golden SAML Journey: SolarWinds Continued. [https://www.splunk.com/en\\_us/blog/security/a-golden-saml-journey-solarwinds-continued.html](https://www.splunk.com/en_us/blog/security/a-golden-saml-journey-solarwinds-continued.html)

Microsoft Security Response Center (MSRC). (2020, December 13). Customer Guidance on Recent Nation-State

Cyber Attacks. <https://msrc-blog.microsoft.com/13/12/2020/customer-guidance-on-recent-nation-state-cyber-attacks/>

Microsoft Security Response Center (MSRC). (2020, December 31). Microsoft Internal Solorigate Investigation Update. <https://msrc-blog.microsoft.com/31/12/2020/microsoft-internal-solorigate-investigation-update/>

National Security Agency (NSA). (2020, December). Detecting Abuse of Authentication Mechanisms. [https://media.defense.gov/2020/Dec/01/1-1-2002554125/17/AUTHENTICATION\\_MECHANISMS\\_CSA\\_U\\_OO\\_20\\_198854.PDF](https://media.defense.gov/2020/Dec/01/1-1-2002554125/17/AUTHENTICATION_MECHANISMS_CSA_U_OO_20_198854.PDF)

NIST Special Publication 63–800B Digital Identity Guidelines. (2017). <https://pages.nist.gov/3-63-800/sp-800-63b.html-5#authenticator-and-verifier-requirements>

Onelogin. (2015). SAML Response Examples - SAML Assertion Example. [SAMLTool.com. https://www.samltool.com/generic\\_sso\\_res.php](https://www.samltool.com/generic_sso_res.php)

Reiner, Shaked. (2017, November 21). Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps. CyberArk Labs. <https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps>

Reiner, Shaked. (2020, December 29). Golden SAML Revisited: The Solorigate Connection. CyberArk. <https://www.cyberark.com/resources/threat-research-blog/golden-saml-revisited-the-solorigate-connection>

Rosenthal, Maddie. (2021, February 10). Must-know Phishing Statistics: Updated 2021. Human Layer Security. <https://www.tessian.com/blog/phishing-statistics2020/>

SolarWinds. (2021). Orion Platform. Retrieved from <https://www.solarwinds.com/orion-platform>

Sygnia. (2020, December). Detection and Hunting of Golden SAML Attack. <https://www.sygnia.co/golden-saml-advisory>

U.S. Cybersecurity and Infrastructure Security Agency (CISA). (2020, December). What Every Leader Needs to Know About the Ongoing APT Cyber Activity. CISA Insights. [https://www.cisa.gov/sites/default/files/publications/CISA20%Insights20%-20%What20%Every20%Leader20%Needs20%to20%Know20%About20%the20%Ongoing20%APT20%Cyber20%Activity20%-20%FINAL\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/CISA20%Insights20%-20%What20%Every20%Leader20%Needs20%to20%Know20%About20%the20%Ongoing20%APT20%Cyber20%Activity20%-20%FINAL_508.pdf)

U.S. Cybersecurity and Infrastructure Security Agency (CISA). (2021, January 7). Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. CISA Alert AA-20 352A. <https://us-cert.cisa.gov/ncas/alerts/aa352-20a>

Virsec Systems. (2021, January 27). SolarWinds Attack End-to-End Demo [Video]. YouTube. [https://www.youtube.com/watch?v=Njr\\_cHWijXM&t=41s](https://www.youtube.com/watch?v=Njr_cHWijXM&t=41s)

# About Easy Dynamics

Easy Dynamics Corporation is a leading 8(a) and Woman-Owned Small Business (WOSB) technology services provider with a core focus in Cybersecurity, Cloud Computing, and Information Sharing. We are builders, problem solvers, and trusted advisors who bring well-architected solutions and management consulting to our clients to align them with the best practices their missions demand. As industry leaders, we are committed to delivering unparalleled quality and service in all aspects of our organization and providing our customers with outstanding technical excellence and the business acumen to advise them on both tactical and strategic initiatives.

## Contact Information



2000 Corporate Ridge, Suite 240, McLean, VA 22102



[whitepapers@easydynamics.com](mailto:whitepapers@easydynamics.com)



[www.easydynamics.com](http://www.easydynamics.com)



Office: (202) 558-7275