THREAT BULLETINS

Microsoft Cloud Environment Post-Compromise Threat Activity Detection

TLP:WHITE

Jan 08, 2021

On January 8, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) distributed an alert (AA21-008A) as a companion alert to (AA20-352A). The predated alert focuses on an advanced persistent threat (APT) actor’s compromise of SolarWinds Orion products as an initial access vector into networks of entities including US government, critical infrastructure, and private network organizations.

This alert addresses activity irrespective of the initial access vectors leveraged that CISA attributes to an APT threat actor. Specifically, this alert serves to address threat actor exploitation via the compromise of applications in a victim's Microsoft 365 (M365)/Azure environment in addition to the utilization of additional credentials and API access to cloud resources of private and public sector organizations.

These tactics, techniques, and procedures (TTPs) feature three key components:

- Compromising or bypassing federated identity solutions.
- Using forged authentication tokens to move laterally to Microsoft cloud environments.
- Using privileged access to a victim's cloud environment to establish difficult-to-detect persistence mechanisms for Application Programming Interface (API)-based access.

This Alert describes these TTPs and offers an overview of, and guidance on, available open-source tools including the CISA-developed tool, **Sparrow**, which was created for network defenders to analyze their Microsoft Azure Active Directory (AD), Office 365 (O365), and M365 environments to detect potentially malicious activity.

Frequently, CISA has observed the APT actor gaining Initial Access [TA0001] to victims' enterprise networks via compromised SolarWinds Orion products (e.g., Solorigate, Supernova). However, CISA is investigating instances in which the threat actor may have obtained initial access by Password Guessing [T1110.001], Password Spraying [T1110.003], and/or exploiting inappropriately secured administrative or service credentials (Unsecured Credentials [T1552]) instead of utilizing the compromised SolarWinds Orion products.

CISA observed this threat actor moving from user context to administrator rights for Privilege Escalation [TA0004] within a compromised network and using native Windows tools and techniques, such as Windows Management Instrumentation (WMI), to enumerate the Microsoft Active Directory Federated Services

(ADFS) certificate-signing capability. This enumeration allows threat actors to forge authentication tokens (OAuth) to issue claims to service providers—without having those claims checked against the identity provider—and then to move laterally to Microsoft Cloud environments (Lateral Movement [TA0008]).

The threat actor has also used on-premises access to manipulate and bypass identity controls and multi-factor authentication. This activity demonstrates how sophisticated adversaries can use credentials from one portion of an organization to move laterally (Lateral Movement [TA0008]) through trust boundaries, evade defenses and detection (Defense Evasion [TA0005]), and steal sensitive data (Collection [TA0009]).

This level of compromise is challenging to remediate and requires a rigorous multi-disciplinary effort to regain administrative control before recovering.

Mitigations:

Detection

Guidance on identifying affected SolarWinds software is well documented. However, once an organization identifies a compromise via SolarWinds Orion products or other threat actor TTPs—identifying follow-on activity for on-premises networks requires fine-tuned network and host-based forensics.

The nature of cloud forensics is unique due to the growing and rapidly evolving technology footprints of major vendors. Microsoft's O365 and M365 environments have built-in capabilities for detecting unusual activity. Microsoft also provides premium services (Advanced Threat Protection [ATP] and Azure Sentinel), which enable network defenders to investigate TTPs specific to the Solorigate activity.

Detection Tools

There are a number of open-source tools available to investigate adversary activity in Microsoft cloud environments and to detect unusual activity, service principals, and application activity. Publicly available PowerShell tools that network defenders can use to investigate M365 and Microsoft Azure include:

- CISA's Sparrow
- Open-source utility Hawk, and
- CrowdStrike's Azure Reporting Tool (CRT).

Additionally, Microsoft's Office 365 Management API and Graph API provide an open interface for ingesting telemetry and evaluating service configurations for signs of anomalous activity and intrusion.

Note: These open-source tools are highlighted and explained to assist with on-site investigation and remediation in cloud environments but are not all-encompassing. Open-source tools can be complemented by services such as Azure Sentinel, a Microsoft premium service that provides comprehensive analysis tools, including custom detections for the activity indicated.

General Guidance on Using Detection Tools

1. Audit the creation and use of service principal credentials. Look for unusual application usage, such as use of dormant applications.

2. Audit the assignment of credentials to applications that allow non-interactive sign-in by the application. Look for unexpected trust relationships added to the Azure Active Directory.

3. Download the interactive sign-ins from the Azure admin portal or use the Microsoft Sentinel product. Review new token validation time periods with high values and investigate whether it was a legitimate change or an attempt to gain persistence by a threat actor.

For additional Mitigation details, including Sparrow and
Hawk Tool insights, please review the (AA21-008A) CISA alert.

Reference(s)	cisa, cisa, Health Industry Cybersecurity Practices
Report Source(s)	Government Agency

Sources

- Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
- Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Publication

Alert ID 911cbfec

View Alert

Tags Microsoft 365, SolarWinds, Azure

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the New Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, new notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org