Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services

us-cert.cisa.gov/ncas/analysis-reports/ar21-013a

Summary

This Analysis Report uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor tactics and techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of several recent successful cyberattacks against various organizations' cloud services. Threat actors are using phishing and other vectors to exploit poor cyber hygiene practices within a victims' cloud services configuration. The information in this report is derived exclusively from several CISA incident response engagements and provides the tactics, techniques, and procedures; indicators of compromise (IOCs) that CISA observed as part of these engagements; and recommended mitigations for organization to strengthen their cloud environment configuration to protect against, detect, and respond to potential attacks.

For a downloadable copy of IOCs, see AR21-013A.stix.

Note: the activity and information in this Analysis Report is not explicitly tied to any one threat actor or known to be specifically associated with the advanced persistent threat actor attributed with the compromise of SolarWinds Orion Platform software and other recent activity.

Description

Background

These types of attacks frequently occurred when victim organizations' employees worked remotely and used a mixture of corporate laptops and personal devices to access their respective cloud services. Despite the use of security tools, affected organizations typically had weak cyber hygiene practices that allowed threat actors to conduct successful attacks.

Technical Details

The cyber threat actors involved in these attacks used a variety of tactics and techniques—including phishing, brute force login attempts, and possibly a "pass-the-cookie" attack—to attempt to exploit weaknesses in the victim organizations' cloud security practices.

Phishing

CISA observed cyber threat actors using phishing emails with malicious links to harvest credentials for users' cloud service accounts (*Phishing: Spearphishing Link* [T1598.003]). The cyber actors designed emails that included a link to what appeared to be a secure message and also emails that looked like a legitimate file hosting service account login. After a targeted recipient provided their credentials, the threat actors then used the stolen credentials to gain *Initial Access* [TA0001] to the user's cloud service account (*Valid Accounts* [T1078]). CISA observed the actors' logins originating from foreign locations (although the actors could have been using a proxy or The Onion Router (Tor) to obfuscate their location). The actors then sent emails from the user's account to phish other accounts within the organization. In some cases, these emails included links to documents within what appeared to be the organization's file hosting service.

In one case, an organization did not require a virtual private network (VPN) for accessing the corporate network. Although their terminal server was located within their firewall, due to remote work posture, the terminal server was configured with port 80 open to allow remote employees to access it—leaving the organization's network vulnerable. The threat actor attempted to exploit this by launching brute force login attempts (*Brute Force* [T1110]).

Forwarding Rules

In several engagements, CISA observed threat actors collecting sensitive information by taking advantage of email forwarding rules, which users had set up to forward work emails to their personal email accounts (*Email Collection: Email Forwarding Rule* [T1114.003]).

Modified Forwarding

In one case, CISA determined that the threat actors modified an existing email rule on a user's account—originally set by the user to forward emails sent from a certain sender to a personal account—to redirect the emails to an account controlled by the actors. The threat actors updated the rule to forward all email to the threat actors' accounts.

Keyword Search Rule

Threat actors also modified existing rules to search users' email messages (subject and body) for several finance-related keywords (which contained spelling mistakes) and forward the emails to the threat actors' account.

New Rule Creation and Forwarding

In addition to modifying existing user email rules, the threat actors created new mailbox rules that forwarded certain messages received by the users (specifically, messages with certain phishing-related keywords) to the legitimate users' Really Simple Syndication (RSS) Feeds or RSS Subscriptions folder in an effort to prevent warnings from being seen by the legitimate users.

Authentication

CISA verified that the threat actors successfully signed into one user's account with proper multi-factor authentication (MFA). In this case, CISA believes the threat actors may have used browser cookies to defeat MFA with a "pass-the-cookie" attack (*Use Alternate Authentication Material: Web Session Cookie* [T1550.004]).

The threat actors attempted brute force logins (*Brute Force* [T1110]) on some accounts. However, this activity was not successful. This thwarted attempt was due, in part, to the threat actors not guessing a correct username/password combination, as well as the organization's use of MFA to access their cloud environment.

Solution

CISA recommends the following steps for organizations to strengthen their cloud security practices.

- Implement conditional access (CA) policies based upon your organization's needs.
- Establish a baseline for normal network activity within your environment.
- Routinely review both Active Directory sign-in logs and unified audit logs for anomalous activity.
- Enforce MFA.
- Routinely review user-created email forwarding rules and alerts, or restrict forwarding.
- Have a mitigation plan or procedures in place; understand when, how, and why to reset passwords and to revoke session tokens.
- Follow recommend guidance on securing privileged access.
- Consider a policy that does not allow employees to use personal devices for work. At a minimum, use a trusted mobile device management solution.
- Resolve client site requests internal to your network.
- Consider restricting users from forwarding emails to accounts outside of your domain.
- Allow users to consent only to app integrations that have been pre-approved by an administrator.
- Audit email rules with enforceable alerts via the Security and Compliance Center or other tools that use the Graph API to warn administrators to abnormal activity.
- Implement MFA for all users, without exception.
- Conditional access should be understood and implemented with a zero-trust mindset.
- Ensure user access logging is enabled. Forward logs to a security information and event management appliance for aggregation and monitoring so as to not lose visibility on logs outside of logging periods.
- Use a CA policy to block legacy authentication protocols.
- Verify that all cloud-based virtual machine instances with a public IP do not have open Remote Desktop Protocol (RDP) ports. Place any system with an open RDP port behind a firewall and require users to use a VPN to access it through the firewall.

- Focus on awareness and training. Make employees aware of the threats—such as phishing scams—and how they are delivered. Additionally, provide users training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities.
- Establish blame-free employee reporting and ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently.
- Ensure existing built-in filtering and detection products (e.g., those for spam, phishing, malware, and safe attachments and links are enabled.
- Organizations using M365 should also consider the following steps.
    - Assign a few (one to three) trusted users as electronic discovery (or eDiscovery) managers to conduct forensic content searches across the entire M365 environment (Mailboxes, Teams, SharePoint, and OneDrive) for evidence of malicious activity.
    - Disable PowerShell remoting to Exchange Online for regular M365 users. Disabling for non-administrative users will lower the likelihood of a compromised user account being used to programmatically access tenant configurations for reconnaissance.
    - Do not allow an unlimited amount of unsuccessful login attempts. To configure these settings, see password smart lockout configuration and sign-in activity reports.
    - Consider using a tool such as Sparrow or Hawk—open-source PowerShell-based tools used to gather information related to M365—to investigate and audit intrusions and potential breaches.[1][2]

Resources

- See CISA's Alert on Technical Approaches to Uncovering and Remediating Malicious Activity for guidance on identifying and handling cyber incidents.
- Review CISA's General Telework Guidance geared toward system administrators.
- See CISA's Analysis Report: Microsoft Office 365 Security Observations (May 2019) for additional guidance.
- CISA also released an Alert: Microsoft Office 365 Security Recommendations with guidance on securing M365 environments.

References

Revisions

January 13, 2021: Initial Version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.