JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA23-193A

July 12, 2023

Enhanced Monitoring to Detect APT Activity Targeting Outlook Online

SUMMARY

In June 2023, a Federal Civilian Executive Branch (FCEB) agency identified suspicious activity in their Microsoft 365 (M365) cloud environment. The agency reported the activity to Microsoft and the Cybersecurity and Infrastructure Security Agency (CISA), and Microsoft determined that advanced persistent threat (APT) actors accessed and exfiltrated unclassified Exchange Online Outlook data.

CISA and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory to provide guidance to critical infrastructure organizations on enhancing monitoring of Microsoft Exchange Online environments. Organizations can enhance their cyber posture and position themselves to detect similar malicious activity by implementing logging recommendations in this advisory. Organizations that identify suspicious, anomalous activity should contact Microsoft for proceeding with mitigation actions due to the cloud-based infrastructure affected, as well as report to CISA and the FBI.

TECHNICAL DETAILS

In Mid-June 2023, an FCEB agency observed `MailItemsAccessed` events with an unexpected `ClientAppID` and `AppID` in M365 Audit Logs. The `MailItemsAccessed` event is generated when licensed users access items in Exchange Online mailboxes using any connectivity protocol from any client. The FCEB agency deemed this activity suspicious because the observed `AppId` did not normally access mailbox items in their environment. The agency reported the activity to Microsoft and CISA.

Microsoft determined that APT actors accessed and exfiltrated unclassified Exchange Online Outlook data from a small number of accounts. The APT actors used a Microsoft account (MSA) consumer key to forge tokens to impersonate consumer and enterprise users. Microsoft remediated the issue by first blocking tokens issued with the acquired key and then replacing the key to prevent continued misuse.[1]

The affected FCEB agency identified suspicious activity by leveraging enhanced logging—specifically of `MailItemsAccessed` events—and an established baseline of normal Outlook activity (e.g., expected `AppID`). The `MailItemsAccessed` event enables detection of otherwise difficult to detect adversarial activity.

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

CISA and FBI are not aware of other audit logs or events that would have detected this activity. Critical infrastructure organizations are strongly urged to implement the logging recommendations in this advisory to enhance their cybersecurity posture and position themselves to detect similar malicious activity.

LOGGING

CISA and the FBI strongly encourage critical infrastructure organizations to ensure audit logging is enabled. **Note:** Per CISA's Microsoft Exchange Online Microsoft 365 Minimum Viable Secure Configuration Baselines, FCEB agencies shall enable audit logging. These minimum viable secure configuration baselines are part of CISA's Secure Cloud Business Applications (SCuBA) Project, which provides guidance for FCEB agencies securing their cloud business application environments and protecting federal information created, accessed, shared, and stored in those environments. Although tailored to FCEB agencies, the project provides security guidance applicable to all organizations with cloud environments. The Office of Management and Budget (OMB) M-21-31 requires Microsoft audit logs be retained for at least twelve months in active storage and an additional eighteen months in cold storage. This can be accomplished either by offloading the logs out of the cloud environment or natively through Microsoft by creating an audit log retention policy.

In addition to enabling audit logging, CISA and FBI strongly encourage organizations to:

- **Enable Purview Audit (Premium) logging.** This logging requires licensing at the G5/E5 level. See Microsoft's guidance on Assigning Microsoft 365 Licenses to Users for additional information.
- **Ensure logs are searchable by operators.** The relevant logs need to be accessible to operational teams in a platform (e.g., security operations center [SOC] tooling) that enables hunting for this activity and distinguishing it from expected behavior within the environment.
- **Enable Microsoft 365 Unified Audit Logging (UAL).** UAL should be enabled by default, but organizations are encouraged to validate these settings.
- **Understand your organization's cloud baseline.** Organizations are encouraged to look for outliers and become familiar with baseline patterns to better understand abnormal versus normal traffic.

GENERAL CLOUD MITIGATIONS

All mitigation actions for this activity are the responsibility of Microsoft due to the cloud-based infrastructure affected; however, CISA and the FBI recommend that critical infrastructure organizations implement the following to harden their cloud environments. Although, these mitigations will not prevent this or related activity where actors leverage compromised consumer keys, they will reduce the impact of less sophisticated malicious activity targeting cloud environments. **Note:** These mitigations align with CISA's SCuBA Technical Reference Architecture (TRA), which describes essential components of security services and capabilities to secure and harden cloud business applications, including the platforms hosting the applications.

- **Apply CISA's recommended baseline security configurations** for Microsoft Defender for Office 365, Azure Active Directory, Exchange Online, OneDrive for Business, Power BI, Power Platform, SharePoint Online, and Teams [SCuBA TRA Section 6.6].
- **Separate administrator accounts from user accounts** according to the National Institute of Standards and Technology's (NIST's) guidance, AC-5: Separation of Duties. Only allow designated administrator accounts to be used for administration purposes. If an individual user requires administrative rights over their workstation, use a separate account without administrative access to other hosts.
- **Collect and store access and security logs** for secure cloud access (SCA) solutions, endpoint solutions, cloud applications/platforms and security services, such as firewalls, data loss prevention systems, and intrusion detection systems [SCuBA TRA Section 6.8.1].
- **Use a telemetry hosting solution** (e.g., SIEM solution) that aggregates logs and telemetry data to facilitate internal organization monitoring, auditing, alerting, and threat detection activities [SCuBA TRA Section 6.8.1].
- **Review contractual relationships with all Cloud Service Providers (CSPs)** and ensure contracts include:
  - Security controls the customer deems appropriate.
  - Appropriate monitoring and logging of provider-managed customer systems.
  - Appropriate monitoring of the service provider's presence, activities, and connections to the customer network.
  - Notification of confirmed or suspected activity.

REPORTING SUSPICIOUS ACTIVITY

Organizations are encouraged to report suspicious activity to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870). The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or IC3.gov.

RESOURCES

- CISA: Microsoft Exchange Online Microsoft 365 Minimum Viable Secure Configuration Baselines
- CISA: SCuBA Project
- Microsoft: Assigning Microsoft 365 Licenses to Users
- CISA: SCuBA TRA
- CISA: Recommended Baseline Security Configurations (Microsoft)
  - Defender for Office 365
  - Azure Active Directory
  - Exchange Online
  - OneDrive for Business
  - Power BI
  - Power Platform
  - SharePoint Online
  - Teams

- NIST: AC-5: Separation of Duties

REFERENCES

[1] Microsoft Security Response Center (MSRC) blog: Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email

ACKNOWLEDGEMENTS

Microsoft contributed to this CSA.

DISCLAIMER