



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

Enhanced Monitoring to Detect APT Activity Targeting Outlook Online

Release Date: July 12, 2023

Alert Code: AA23-193A

RELATED TOPICS: SECURING NETWORKS <[/topics/cyber-threats-and-advisories/securing-networks](#)>, CYBER THREATS AND ADVISORIES <[/topics/cyber-threats-and-advisories](#)>



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

Give Feedback

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.

Download the PDF version of this report:

 AA23-193A Enhanced Monitoring to Detect APT Activity Targeting Outlook Online <sites/default/files/2023-07/aa23-193a_joint_csa_enhanced_monitoring_to_detect_apt_activity_targeting_outlook_online_2.pdf>
(PDF, 410.82 KB)

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.

(Updated July 14, 2023) 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. Microsoft determined that this activity was part of a campaign targeting multiple organizations (all of which have been notified by Microsoft). [1
<<https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/>>]

Give Feedback

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.

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.

Give Feedback

- **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 \(TRA\)](https://www.cisa.gov/sites/default/files/2022-12/scuba_tra_rfc_eg_508c.pdf) <https://www.cisa.gov/sites/default/files/2022-12/scuba_tra_rfc_eg_508c.pdf>, which describes essential components of security services and capabilities to secure and harden cloud business applications, including the platforms hosting the applications.

Give Feedback

- **Apply CISA's recommended baseline security configurations** for Microsoft Defender for Office 365 <[sites/default/files/publications/microsoft 365 defender m365 minimum viable scb draft v0.1.pdf](#)>, Azure Active Directory <[sites/default/files/publications/microsoft azure active directory m365 minimum viable scb draft v0.1.pdf](#)>, Exchange Online <[sites/default/files/publications/microsoft exchange online m365 minimum viable scb draft v0.1.pdf](#)>, OneDrive for Business <[sites/default/files/publications/microsoft onedrive for business m365 minimum viable scb draft v0.1.pdf](#)>, Power BI <[sites/default/files/publications/microsoft%20power%20bi%20m365%20minimum%20viable%20scb%20v0.1.pdf](#)>, Power Platform <[sites/default/files/publications/microsoft%20power%20platform%20m365%20minimum%20viable%20scb%20draft%20v0.1.pdf](#)>, SharePoint Online <[sites/default/files/publications/microsoft sharepoint online m365 minimum viable scb draft v0.1.pdf](#)>, and Teams <[sites/default/files/publications/microsoft teams m365 minimum viable scb draft v0.1.pdf](#)> [SCuBA TRA Section 6.6 <[sites/default/files/2022-12/scuba_tra_rfc_eg_508c.pdf](#)>].
- **Separate administrator accounts from user accounts** according to the National Institute of Standards and Technology's (NIST's) guidance, AC-5: Separation of Duties <<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r5.pdf>>. 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 <http://www.cisa.gov/sites/default/files/2022-12/scuba_tra_rfc_eg_508c.pdf>].
- **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 <[sites/default/files/2022-12/scuba_tra_rfc_eg_508c.pdf](#)>].

Give Feedback

- **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 1-844-Say-CISA). The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their [local FBI field office](#) <<http://www.fbi.gov/contact-us/field-offices>> or [IC3.gov](#) <<https://www.ic3.gov/>>.

RESOURCES

- CISA: Microsoft Exchange Online Microsoft 365 Minimum Viable Secure Configuration Baselines <sites/default/files/publications/microsoft_exchange_online_m365_minimum_viable_scb_draft_v0.1.pdf>
- CISA: SCuBA Project <resources-tools/services/secure-cloud-business-applications-scuba-project>
- Microsoft: Assigning Microsoft 365 Licenses to Users
- CISA: SCuBA TRA <sites/default/files/publications/scuba_tra_rfc_eg_508c.pdf>

Give Feedback

- CISA: Recommended Baseline Security Configurations (Microsoft)
 - [Defender for Office 365](#) </sites/default/files/publications/microsoft 365 defender m365 minimum viable scb draft v0.1.pdf>
 - [Azure Active Directory](#) </sites/default/files/publications/microsoft azure active directory m365 minimum viable scb draft v0.1.pdf>
 - [Exchange Online](#) </sites/default/files/publications/microsoft exchange online m365 minimum viable scb draft v0.1.pdf>
 - [OneDrive for Business](#) </sites/default/files/publications/microsoft onedrive for business m365 minimum viable scb draft v0.1.pdf>
 - [Power BI](#) </sites/default/files/publications/microsoft power bi m365 minimum viable scb v0.1.pdf>
 - [Power Platform](#) </sites/default/files/publications/microsoft power platform m365 minimum viable scb draft v0.1.pdf>
 - [SharePoint Online](#) </sites/default/files/publications/microsoft sharepoint online m365 minimum viable scb draft v0.1.pdf>
 - [Teams](#) </sites/default/files/publications/microsoft teams m365 minimum viable scb draft v0.1.pdf>
- NIST: AC-5: Separation of Duties <<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r5.pdf>>

Update July 14, 2023:

- Microsoft: Microsoft Mitigates China-based Threat Actor Storm-0558 Targeting of Customer Email <<https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/>>
- Microsoft: Mitigation for China-Based Threat Actor Activity <<https://blogs.microsoft.com/on-the-issues/2023/07/11/mitigation-china-based-threat-actor/>>
- Microsoft: Analysis of Storm-0558 Techniques for Unauthorized Email Access <<https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/>>

End Update

Give Feedback

REFERENCES

[1] Microsoft Security Response Center (MSRC) blog: Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email <<https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/>>

ACKNOWLEDGEMENTS

Microsoft contributed to this CSA.

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. The FBI, and CISA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI and CISA.

This product is provided subject to this [Notification](#) </notification> and this [Privacy & Use](#) </privacy-policy> policy.

Give Feedback

Tags

Audience: Industry

Co-Sealers and Partners: Federal Bureau of Investigation

Topics: Cyber Threats and Advisories </topics/cyber-threats-and-advisories>, Securing Networks </topics/cyber-threats-and-advisories/securing-networks>



Please share your thoughts

We recently updated our anonymous [product survey](#); we welcome your feedback.

Related Advisories

[Give Feedback](#)

JUL 31, 2025 ■ CYBERSECURITY ADVISORY |
AA25-212A

CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization

[</news-events/cybersecurity-advisories/aa25-212a>](#)

JUL 22, 2025 ■ CYBERSECURITY ADVISORY |
AA25-203A

#StopRansomware: Interlock

[</news-events/cybersecurity-advisories/aa25-203a>](#)

MAY 21, 2025 ■ CYBERSECURITY ADVISORY |
AA25-141B

Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations

[</news-
events/cybersecurity-advisories/aa25-141b>](#)

MAR 12, 2025 ■ CYBERSECURITY ADVISORY |
AA25-071A

#StopRansomware: Medusa

[Ransomware](#) [</news-events/cybersecurity-
advisories/aa25-071a>](#)

[Return to top](#)

Give Feedback

Topics [</topics>](#)

Spotlight [</spotlight>](#)

Resources & Tools [</resources-tools>](#)

News & Events [</news-events>](#)

Careers [</careers>](#)

About [</about>](#)



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY



CISA Central

1-844-Say-CISA contact@cisa.dhs.gov



CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA](#) </about>

[Budget and Performance](#)

[DHS.gov](#) <<https://www.dhs.gov>>

[<https://www.dhs.gov/performance-financial-reports>](#)

[FOIA Requests](#)

<<https://www.dhs.gov/foia>>

[No FEAR Act](#) </no-fear-act>

[Office of Inspector General](#)

<<https://www.oig.dhs.gov/>>

[Privacy Policy](#) </privacy-policy>

[Subscribe](#)

[The White House](#)

<<https://www.whitehouse.gov/>>

[USA.gov](#) <<https://www.usa.gov>>

[Website Feedback](#) </forms/feedback>

Give Feedback