GRADIENT

Reviewing the 2023 Microsoft Exchange Online Intrusion

WHITE PAPER

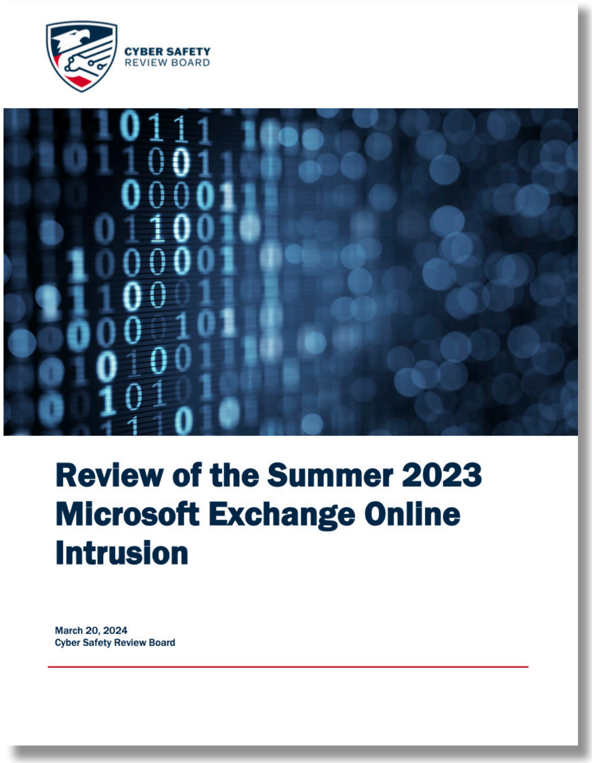
In the summer of 2023, a threat actor conducted an extensive cyber intrusion targeting Microsoft Exchange Online mailboxes and compromising 22 organizations and over 500 individuals worldwide. This large-scale attack, exploiting a legacy Microsoft key dating back to 2016, underscores the severe risks of stolen credentials and highlights the urgent need for robust credential management and authentication practices.

Executive Summary

In the summer of 2023, a threat actor conducted an extensive cyber intrusion targeting Microsoft Exchange Online mailboxes and compromising 22 organizations and over 500 individuals worldwide. This large-scale attack, exploiting a legacy Microsoft key dating back to 2016, underscores the severe risks of stolen credentials and highlights the urgent need for robust credential management and authentication practices.

CISA's Cyber Safety Review Board recently issued a comprehensive report, Review of the Summer 2023 Microsoft Exchange Online Intrusion, which analyzes this attack, its root causes, responses, lessons, and recommendations. Based on this review, the 2023 Microsoft Exchange Online breach highlights the significant consequences of lapses in credential management. An overly long-lived key intended for consumer systems became a backdoor for attackers, known as Storm-0558, to access sensitive enterprise accounts. This breach exposed the email communications of high-profile individuals and organizations globally.

The incident reveals critical vulnerabilities: long-lived keys, inadequate key rotation procedures, overly broad key privileges, and a lack of segregation between consumer and enterprise key systems. The Cyber Safety Review Board underscores a path forward by emphasizing the importance of short-lived keys, key rotation automation, secure key handling, token constraints, and standardized authentication protocols to mitigate the escalating threat of credential-based attacks.



CYBER SAFETY REVIEW BOARD

Review of the Summer 2023 Microsoft Exchange Online Intrusion

March 20, 2024
Cyber Safety Review Board

The Microsoft Exchange Online Breach and its Implications

The Microsoft Exchange Online breach was a long-term cyber campaign carried out by a Chinese espionage group known as Storm-0558. The attack targeted Microsoft Exchange Online, the cloud-based email service used by millions of businesses and organizations worldwide. After potentially months of reconnaissance within Microsoft's network, the attackers compromised a critical Microsoft Services Account (MSA) key. This key allowed them to forge authentication tokens and impersonate legitimate users, infiltrating Microsoft Exchange Online accounts undetected in 2023.

2016 Microsoft creates the Microsoft Services Account (MSA) key at issue

The breach accessed accounts belonging to U.S. government agencies, foreign governments, senior government officials, private sector organizations, and private individuals globally. As devastating as the attack was, the impact could have been much worse. The compromised key could theoretically have granted access to a broader range of Microsoft cloud applications and third-party applications that were luckily spared.

Intrusion impacted accounts belonging to 22 U.S. government agencies, foreign governments, senior government officials, private sector organizations, and over 500 individuals globally

Recipe for a Breach: the Key Ingredients

- **2016: Microsoft creates the Microsoft Services Account (MSA) key at issue.** This key was intended for signing authentication tokens within its consumer account system.
- **2021: Microsoft stopped manual rotation of signing keys**, after a major cloud outage that was linked to their manual rotation process.
- **Mid-2021: A threat actor breaches Microsoft's corporate network, through token theft from a compromised engineer's laptop from a recently acquired company.** During integration with the company, Microsoft issued corporate credentials to the engineer, whose laptop had been compromised prior to acquisition.
- **Mid-2021 to Late 2022: The attackers likely spent a significant amount of time within Microsoft's network conducting reconnaissance.** Their goal was to identify and gain access to authentication and identity data, which presumably included the legacy Microsoft Services Account (MSA) key, though this has not been confirmed.
- **May-June 2023: Armed with the compromised MSA key, the attack entered its active phase.** Attackers forged authentication tokens to impersonate legitimate users and infiltrate Microsoft Exchange Online accounts undetected.
- **June 2023: After investigating customer identified anomalies, Microsoft revoked the MSA key's ability to sign tokens**, closed a vulnerability enabling consumer-based keys to access enterprise services, and implemented myriad other mitigations

Key Root Cause Findings

The Cyber Safety Review Board's investigation identified several critical shortcomings in Microsoft's credential management practices that enabled the threat actor to successfully attack. At its core was a long-lived Microsoft Services Account key, created in 2016 for consumer systems but never properly decommissioned. Microsoft's reliance on manual key rotation processes further exacerbated the issue, as delays in key retirement left gaps in security. The company had plans to retire the key but faced complications stemming from concerns about potential disruptions caused by manual rotation. This delay meant the vulnerable key remained active for an extended period.

Furthermore, this legacy MSA key inadvertently became a gateway to enterprise accounts. There was a lack of adequate segregation between the enterprise and consumer key systems. The OIDC (OpenID Connect) endpoint service failed to differentiate between keys signed for the different identity systems. This allowed the attackers to exploit a consumer-grade key to infiltrate sensitive enterprise email accounts. Finally, the compromised key had overly broad access privileges.

Highlights from the Board's Recommendations: Identity & Credential Management Best Practices

Based on its analysis of the breach, the Board emphasized the following best practices to strengthen credential management and prevent similar attacks:

Automated, Frequent Key Rotation: Implementing automated, frequent (e.g., monthly) key rotation limits the blast radius and duration of a potential compromise.

Bound Tokens: Microsoft's authentication system used easily transferable "bearer tokens" without proof-of-possession requirements. Linking tokens to specific operations or user sessions further tightens security.

Secure Key Storage: Storing keys in isolated systems and using technologies such as dedicated Hardware Security Modules (HSMs) can reduce the risk of key compromise.

Limited Key Scope: Limiting key functionality and access reduces the potential damage if a key is compromised. They suggested tying encryption keys to customer tenants.

Common Authentication Libraries: Having all services use the same libraries will help ensure more consistent token validation behavior and authorization policy.

Stateful Tokens: Recording tokens in a database and verifying issuance at access time could help identify tokens generated by malicious third parties.

Proprietary Data in Tokens: While an adversary could detect and reproduce this, integrating proprietary-specific data into token generation could potentially help identify tokens generated by malicious third parties.

Gradient's Solution: Anchored, Short-Lived Credentials and Much More

Affordable and quick to implement in your environment, Gradient delivers frictionless, passwordless enterprise authentication secured with a multi-layered approach that directly addresses the vulnerabilities exposed in the Microsoft Exchange Online intrusion and aligns perfectly with the key recommendations outlined by the Cyber Safety Review Board, enhancing your organization's overall security posture. Here's how GCM can safeguard your organization:

Anchored Credentials are Bound Tokens on Steroids: For devices with supporting hardware, such as today's laptops and mobile phones, Gradient can leverage anchored credentials for authentication, for users, devices, endpoints, and sessions, securing these credentials so they can only be used from – and are anchored to – the user's device. These credentials store private keys within a Trusted Platform Module (TPM, as found on Windows devices) or Secure Enclave (as found on Apple products) on the device. These are hardware components specifically designed for secure key storage. All operations on the private key occur within this secure environment, rendering them inaccessible to malware or unauthorized processes running on the main processor. Since the keys never leave the TPM or Secure Enclave, this prevents attackers from stealing or misusing credentials on unauthorized systems.

Short-Lived Credentials with 10-Minute Durations, Much Shorter than the Board's Suggestion of a Month: if a month is good at limiting the blast radius, how about minutes? Gradient operates with extremely short-lived credentials. These credentials, along with their associated keys, are only valid for minutes. The limited lifespan significantly reduces the window of opportunity for attackers to exploit them to the point of impracticality.

Automated Key Rotation Seamless to the User: Automated high-frequency key rotation is a core feature of GCM, eliminating the risks of legacy keys. This ensures proactive security. Credential issuance is done continually and seamlessly to the user.

Secure Key Storage with No Peer: In addition to the security provided by anchored credentials on endpoints, keys within the GCM infrastructure are stored in highly secure, isolated hardware Secure Enclaves, a purpose-built backend design that successfully withstood over 13,000 man-hours of DoD red-teaming with no side channel vulnerabilities. This keeps them protected from attackers even if other system defenses are compromised.

Fine-Grained Scope Limitations: GCM starts with unique keys per customer tenant – but goes well beyond. GCM keys are restricted by customer, user, device, and even individual operation or session. This minimizes the blast radius in the event of a key compromise.

Conclusion

The Microsoft Exchange Online breach underscores the severe consequences of inadequate credential management. It also tragically proves that even the most sophisticated organizations can fall prey to targeted cyberattacks. By adopting the robust practices outlined by the Cyber Safety Review Board and leveraging innovative solutions like Gradient Cybersecurity Mesh (GCM), organizations can significantly fortify their security posture.

GCM offers a groundbreaking approach to enterprise authentication. Its anchored, short-lived credentials, coupled with automated key rotation and secure storage, eliminate stolen credentials, responsible for more than 85% of cyber attacks.[1] With GCM, you can move beyond passwords while simultaneously securing your organization against identity compromise.

If you're ready to prioritize proactive cybersecurity, eliminate the risk of stolen credentials, and explore the transformative benefits of GCM, contact us today to schedule a demo.

[1] **Google Cloud's 2023 Threat Horizons Report**

What is Gradient

Gradient offers the only cybersecurity solution that continually protects and communicates, via patented secure hardware attestation, the complete security posture of every platform, all the way from the legitimacy of the hardware to the firmware (UEFI), kernel, kernel packages, and more, to establish a dynamic "fingerprint."

Gradient enhances the conventional authentication and conditional access flow for users, devices, and APIs to include the continual validation of both identity and the complete platform fingerprint. As a result, Gradient ensures that only legitimate users on valid, legitimate machines running correct, uncompromised software are allowed, where each of these attributes is re-evaluated at regular intervals to ensure they reflect the most up-to-date information on the state of every device on your network. This is dynamic attribute-based access control (ABAC) for everything, everywhere.