CYBER SAFETY
REVIEW BOARD

# Review of the Summer 2023 Microsoft Exchange Online Intrusion

March 20, 2024
Cyber Safety Review Board

## TABLE OF CONTENTS

## MESSAGE FROM THE CHAIR AND DEPUTY CHAIR

It is not an exaggeration to say that cloud computing has become an indispensable resource to this nation, and indeed, much of the world. Numerous companies, government agencies, and even some entire countries rely on this infrastructure to run their critical operations, such as providing essential services to customers and citizens. Driven by productivity, efficiency, and cost benefits, adoption of these services has skyrocketed over the past decade, and, in some cases, they have become as indispensable as electricity. As a result, cloud service providers (CSPs) have become custodians of nearly unimaginable amounts of data. Everything from Americans' personal information to communications of U.S. diplomats and other senior government officials, as well as commercial trade secrets and intellectual property, now resides in the geographically-distributed data centers that comprise what the world now calls the "cloud."

The cloud creates enormous efficiencies and benefits but, precisely because of its ubiquity, it is now a high-value target for a broad range of adversaries, including nation-state threat actors. An attacker that can compromise a CSP can quickly position itself to compromise the data or networks of that CSP's customers. In effect, the CSPs have become one of our most important critical infrastructure industries. As a result, these companies must invest in and prioritize security consistent with this "new normal," for the protection of their customers and our most critical economic and security interests.

When a hacking group associated with the government of the People's Republic of China, known as Storm-0558, compromised Microsoft's cloud environment last year, it struck the espionage equivalent of gold. The threat actors accessed the official email accounts of many of the most senior U.S. government officials managing our country's relationship with the People's Republic of China.

As is its mandate, the Cyber Safety Review Board (CSRB, or the Board) conducted deep fact-finding around this incident. The Board concludes that this intrusion should never have happened. Storm-0558 was able to succeed because of a cascade of security failures at Microsoft, as outlined in this report. Today, the Board issues recommendations to Microsoft to ensure this critical company, which sits at the center of the technology ecosystem, is prioritizing security for the benefit of its more than one billion customers. In the course of its review, the Board spoke with a range of large CSPs to assess the state of their security practices, and—as is also its mandate—the Board today issues recommendations to all CSPs for establishing specific security controls for identity and authentication in the cloud. All technology companies must prioritize security in the design and development of their products. The entire industry must come together to dramatically improve the identity and access infrastructure that safeguards the information CSPs are entrusted to maintain. Global security relies upon it.

We, and all the members of CSRB, are grateful for Microsoft's full cooperation in this review. The company provided extensive oral and written submissions since November 2023, and we believe answered all of our questions to the best of its ability. We also received full cooperation from U.S. intelligence, law enforcement, and cyber defense agencies.

As we complete our third review since the Board's establishment in 2022, we are gratified more broadly to observe the track record of cooperation that CSRB has developed with industry, security researchers, the academic community, and foreign government agencies. We are more confident than ever in the Board's role as a truly public-private institution that conducts authoritative fact-finding and issues actionable recommendations in the wake of major cyber incidents.

We are grateful to Alejandro Mayorkas, Secretary of Homeland Security, and to Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency, for their continued belief in and support of this Board, including by charging us with consequential mandates like this review of the Microsoft Exchange Online incident.

We offer our thanks to the 20 organizations and individual experts who offered their experience and expertise to allow us to conduct this comprehensive review. Finally, we express deep appreciation to our colleagues on the Board for their continued commitment to our charge, and to the determined and gifted staff who helped the Board discharge its task and bring this important review to conclusion.

**Robert Silvers**
Chair

**Dmitri Alperovitch**
Deputy Chair

## EXECUTIVE SUMMARY

In May and June 2023, a threat actor compromised the Microsoft Exchange Online mailboxes of 22 organizations and over 500 individuals around the world. The actor—known as Storm-0558 and assessed to be affiliated with the People's Republic of China in pursuit of espionage objectives—accessed the accounts using authentication tokens that were signed by a key Microsoft had created in 2016. This intrusion compromised senior United States government representatives working on national security matters, including the email accounts of Commerce Secretary Gina Raimondo, United States Ambassador to the People's Republic of China R. Nicholas Burns, and Congressman Don Bacon.

Signing keys, used for secure authentication into remote systems, are the cryptographic equivalent of crown jewels for any cloud service provider. As occurred in the course of this incident, an adversary in possession of a valid signing key can grant itself permission to access any information or systems within that key's domain. A single key's reach can be enormous, and in this case the stolen key had extraordinary power. In fact, when combined with another flaw in Microsoft's authentication system, the key permitted Storm-0558 to gain full access to essentially any Exchange Online account anywhere in the world. As of the date of this report, Microsoft does not know how or when Storm-0558 obtained the signing key.

This was not the first intrusion perpetrated by Storm-0558, nor is it the first time Storm-0558 displayed interest in compromising cloud providers or stealing authentication keys. Industry links Storm-0558 to the 2009 Operation Aurora campaign that targeted over two dozen companies, including Google, and the 2011 RSA SecurID incident, in which the actor stole secret keys used to generate authentication codes for SecurID tokens, which were used by tens of millions of users at that time. Indeed, security researchers have tracked Storm-0558's activities for over 20 years.

On August 11, 2023, Secretary of Homeland Security Alejandro Mayorkas announced that the Cyber Safety Review Board (CSRB, or the Board) would "assess the recent Microsoft Exchange Online intrusion . . . and conduct a broader review of issues relating to cloud-based identity and authentication infrastructure affecting applicable cloud service providers and their customers."

The Board conducted extensive fact-finding into the Microsoft intrusion, interviewing 20 organizations to gather relevant information (see Appendix A). Microsoft fully cooperated with the Board and provided extensive in-person and virtual briefings, as well as written submissions. The Board also interviewed an array of leading cloud service providers to gain insight into prevailing industry practices for security controls and governance around authentication and identity in the cloud.

The Board finds that this intrusion was preventable and should never have occurred. The Board also concludes that Microsoft's security culture was inadequate and requires an overhaul, particularly in light of the company's centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations. The Board reaches this conclusion based on:

1. the cascade of Microsoft's avoidable errors that allowed this intrusion to succeed;
2. Microsoft's failure to detect the compromise of its cryptographic crown jewels on its own, relying instead on a customer to reach out to identify anomalies the customer had observed;
3. the Board's assessment of security practices at other cloud service providers, which maintained security controls that Microsoft did not;
4. Microsoft's failure to detect a compromise of an employee's laptop from a recently acquired company prior to allowing it to connect to Microsoft's corporate network in 2021;
5. Microsoft's decision not to correct, in a timely manner, its inaccurate public statements about this incident, including a corporate statement that Microsoft believed it had determined the likely root cause of the intrusion when in fact, it still has not; even though Microsoft acknowledged to the Board in November 2023 that its September 6, 2023 blog post about the root cause was inaccurate, it did not update that post until March 12, 2024, as the Board was concluding its review and only after the Board's repeated questioning about Microsoft's plans to issue a correction;
6. the Board's observation of a separate incident, disclosed by Microsoft in January 2024, the investigation of which was not in the purview of the Board's review, which revealed a compromise that allowed a different

nation-state actor to access highly-sensitive Microsoft corporate email accounts, source code repositories, and internal systems; and

7. how Microsoft's ubiquitous and critical products, which underpin essential services that support national security, the foundations of our economy, and public health and safety, require the company to demonstrate the highest standards of security, accountability, and transparency.

Throughout this review, the Board identified a series of Microsoft operational and strategic decisions that collectively point to a corporate culture that deprioritized both enterprise security investments and rigorous risk management.

To drive the rapid cultural change that is needed within Microsoft, the Board believes that Microsoft's customers would benefit from its CEO and Board of Directors directly focusing on the company's security culture and developing and sharing publicly a plan with specific timelines to make fundamental, security-focused reforms across the company and its full suite of products. The Board recommends that Microsoft's CEO hold senior officers accountable for delivery against this plan. In the meantime, Microsoft leadership should consider directing internal Microsoft teams to deprioritize feature developments across the company's cloud infrastructure and product suite until substantial security improvements have been made in order to preclude competition for resources. In all instances, security risks should be fully and appropriately assessed and addressed before new features are deployed.

Based on the lessons learned from its review and its fact-finding into prevailing security practices across the cloud services industry, the Board, in addition to the recommendations it makes to the President of the United States and Secretary of Homeland Security, also developed a series of broader recommendations for the community focused on improving the security of cloud identity and authentication across the government agencies responsible for driving better cybersecurity, cloud service providers, and their customers.

- **Cloud Service Provider Cybersecurity Practices:** Cloud service providers should implement modern control mechanisms and baseline practices, informed by a rigorous threat model, across their digital identity and credential systems to substantially reduce the risk of system-level compromise.
- **Audit Logging Norms:** Cloud service providers should adopt a minimum standard for default audit logging in cloud services to enable the detection, prevention, and investigation of intrusions as a baseline and routine service offering without additional charge.
- **Digital Identity Standards and Guidance:** Cloud service providers should implement emerging digital identity standards to secure cloud services against prevailing threat vectors. Relevant standards bodies should refine, update, and incorporate these standards to address digital identity risks commonly exploited in the modern threat landscape.
- **Cloud Service Provider Transparency:** Cloud service providers should adopt incident and vulnerability disclosure practices to maximize transparency across and between their customers, stakeholders, and the United States government, even in the absence of a regulatory obligation to report.
- **Victim Notification Processes:** Cloud service providers should develop more effective victim notification and support mechanisms to drive information-sharing efforts and amplify pertinent information for investigating, remediating, and recovering from cybersecurity incidents.
- **Security Standards and Compliance Frameworks:** The United States government should update the Federal Risk Authorization Management Program and supporting frameworks and establish a process for conducting discretionary special reviews of the program's authorized Cloud Service Offerings following especially high-impact situations. The National Institute of Standards and Technology should also incorporate feedback about observed threats and incidents related to cloud provider security.

# 1 FACTS

## 1.1 OVERVIEW

In May 2023, a threat actor known as Storm-0558[1] compromised the Microsoft Exchange Online mailboxes of a broad range of victims in the United States (U.S.), the United Kingdom (U.K.), and elsewhere. Storm-0558, assessed by multiple sources to pursue espionage objectives and maintain ties with the People's Republic of China (PRC),[2, 3] accessed email accounts in the U.S. Department of State (State Department, or State), U.S. Department of Commerce (Commerce Department, or Commerce), and U.S. House of Representatives.[4] This included the official and personal mailboxes of U.S. Commerce Secretary Gina Raimondo; Congressman Don Bacon; U.S. Ambassador to the PRC, R. Nicholas Burns; Assistant Secretary of State for East Asian and Pacific Affairs, Daniel Kritenbrink;[5] and additional individuals across 22 organizations.[6] These senior officials have substantial responsibilities for many aspects of the U.S. government's bilateral relationship with the PRC. Storm-0558 had access to some of these cloud-based mailboxes for at least six weeks,[7, 8] and during this time, the threat actor downloaded approximately 60,000 emails from State Department alone.[9]

State Department was the first victim to discover the intrusion when, on June 15, 2023, State's security operations center (SOC) detected anomalies in access to its mail systems.[10] The next day, State observed multiple security alerts from a custom rule it had created, known internally as "Big Yellow Taxi,"[11] that analyzes data from a log known as MailItemsAccessed, which tracks access to Microsoft Exchange Online mailboxes. State was able to access the MailItemsAccessed log to set up these particular Big Yellow Taxi alerts because it had purchased Microsoft's government agency-focused G5 license that includes enhanced logging capabilities through a product called Microsoft Purview Audit (Premium).[12] The MailItemsAccessed log was not accessible without that "premium" service.[13]

Though the alerts showed activity that could have been considered normal—and, indeed, State had seen false positive Big Yellow Taxi detections in the past—State investigated these incidents and ultimately determined that the alert indicated malicious activity. State triaged the alert as a moderate-level event and, on Friday, June 16, 2023, its security team contacted Microsoft.[14, 15] Microsoft opened and conducted an investigation of its own, and over the next 10 days, ultimately confirmed that Storm-0558 had gained entry to certain user emails through State's Outlook Web Access (OWA). Concurrently, Microsoft expanded its investigation to identify the 21 additional impacted organizations and 503 related users impacted by the attack and worked to identify and notify impacted U.S. government agencies.[16]

Microsoft initially assumed that Storm-0558 had gained access to State Department accounts through traditional threat vectors, such as compromised devices or stolen credentials. However, on June 26, 2023, Microsoft discovered that the threat actor had used OWA to access emails directly using tokens that authenticated Storm-0558 as valid

[1] Microsoft uses its internal naming taxonomy to label threat actors based on several characteristics including country of origin, infrastructure, and objectives. *Source: Lambert, John; Microsoft, "Microsoft shifts to a new threat actor naming taxonomy," April 18, 2023, https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/*
[2] Anonymized.
[3] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[4] Anonymized.
[5] Schappert, Stefanie; CyberNews, "*Another US Congressman reveals emails hacked by China*," November 15, 2023, https://cybernews.com/news/us-congressman-emails-hacked-china-microsoft/
[6] Anonymized.
[7] Anonymized.
[8] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[9] State Department, "*Department Press Briefing – September 28, 2023*," September 28, 2023, https://www.state.gov/briefings/department-press-briefing-september-28-2023/
[10] Anonymized.
[11] Sakellariadis, John and Miller, Maggie; Politico, "*All thanks to 'Big Yellow Taxi': How State discovered Chinese hackers reading its emails*," September 15, 2023, https://www.politico.com/news/2023/09/15/digital-tripwire-helped-state-uncover-chinese-hack-00115973
[12] State Department, Board Meeting.
[13] Microsoft, "*Compare Office 365 Government Plans: Microsoft 365*," https://www.microsoft.com/en-us/microsoft-365/enterprise/government-plans-and-pricing
[14] Anonymized.
[15] State Department, Board Meeting.
[16] Microsoft, Board Meeting.

users. Such tokens should only come from Microsoft's identity system, yet these had not. Moreover, tokens used by the threat actor had been digitally signed with a Microsoft Services Account (MSA)[17] cryptographic key that Microsoft had issued in 2016. This particular MSA key should only have been able to sign tokens that worked in consumer OWA, not Enterprise Exchange Online. Finally, this 2016 MSA key was originally intended to be retired in March 2021, but its removal was delayed due to unforeseen challenges associated with hardening the consumer key systems.[18] This was the moment that Microsoft realized it had major, overlapping problems: first, someone was using a Microsoft signing key to issue their own tokens; second, the 2016 MSA key in question was no longer supposed to be signing new tokens; and third, someone was using these consumer key-signed tokens to gain access to enterprise email accounts.

According to Microsoft, this discovery triggered an all-hands-on-deck investigation by Microsoft that ran overnight from June 26 into June 27, 2023, focusing on the 2016 MSA key that had issued the token as well as the access token itself. By the end of the day, Microsoft had high confidence that the threat actor had forged a token using a stolen consumer signing key. Microsoft then escalated this intrusion internally, assigning it the highest urgency level and coordinating its investigation across multiple company teams. As a result, Microsoft developed 46 hypotheses to investigate, including some scenarios as wide-ranging as the adversary possessing a theoretical quantum computing capability to break public-key cryptography or an insider who stole the key during its creation. Microsoft then assigned teams for each hypothesis to try to: prove how the theft occurred; prove it could no longer occur in the same way now; and to prove Microsoft would detect it if it happened today. Nine months after the discovery of the intrusion, Microsoft says that its investigation into these hypotheses remains ongoing.[19]

Microsoft began notifying potentially impacted organizations and individuals on or about June 19 and July 4, 2023, respectively.[20, 21] As detailed below, this effort had varying degrees of success. Ultimately, Microsoft determined that Storm-0558 used an acquired MSA consumer token signing key to forge tokens to access Microsoft Exchange Online accounts for 22 enterprise organizations, as well as 503 related personal[22] accounts, worldwide.[23] Of the 503 personal accounts reported by Microsoft, at least 391 were in the U.S. and included those of former government officials,[24] while others were linked to Western European, Asia-Pacific (APAC), Latin American, and Middle Eastern countries and associated victim organizations.[25, 26, 27]

Microsoft found no sign of an intrusion into its identity system and, as of the conclusion of this review, has not been able to determine how Storm-0558 had obtained the 2016 MSA key; it did find a flaw in the token validation logic used by Exchange Online that could allow a consumer key to access enterprise Exchange accounts if those Exchange accounts were not coded to reject a consumer key. By June 27, 2023, Microsoft believed it had identified the technique used to access victim accounts and rapidly cleared related caching data in various downstream Microsoft systems to invalidate all credentials derived from the stolen key. Microsoft believed that this mitigation was effective, as it almost immediately observed Storm-0558 begin to use phishing to try to gain access to the email boxes it had previously compromised.[28] However, by the conclusion of this review, Microsoft was still unable to demonstrate to the Board that it knew how Storm-0558 had obtained the 2016 MSA key.

[17] Consumer accounts are validated by MSA consumer signing keys, and Azure AD accounts are validated through Azure AD enterprise signing keys. As these keys are from separate providers, and managed in separate systems, they should not be able to validate for the other system. *Source: SecureTeam, "Microsoft Key Used for Unauthorised Email Access," July 27, 2023, https://secureteam.co.uk/2023/07/27/microsoft-key-used-for-unauthorised-email-access/*
[18] Microsoft, Board Meeting.
[19] Microsoft, Board Meeting.
[20] Anonymized.
[21] Anonymized.
[22] The term "personal" in this context means an individual account. "A Microsoft [personal] account is the name given to the identity service that provides authentication and authorization to Microsoft's consumer services. You use a personal Microsoft account to connect to Microsoft apps, services, and devices." *Source: Microsoft, "What's the difference between a Microsoft account and a Microsoft 365 work or school account?" October 10, 2023, https://support.microsoft.com/en-au/office/what-s-the-difference-between-a-microsoft-account-and-a-microsoft-365-work-or-school-account-72f10e1e-cab8-4950-a8da-7c45339575b0*
[23] Microsoft, Board Meeting.
[24] Anonymized.
[25] Microsoft, Board Meeting.
[26] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[27] Microsoft, Response to Board Request for Information.
[28] Microsoft, Board Meeting.

## 1.2 INTRUSION DETAILS

### 1.2.1 TIMELINE

The Board finds that the intrusion began in May 2023 and known adversaries' techniques were remediated by the end of June 2023. A high-level timeline follows, and a more complete chronology is included in Appendix B.

**May-June 15, 2023: Initial Intrusion, Before Discovery**

Storm-0558 compromised Microsoft Exchange Online mailboxes of certain victims in the U.S., the U.K., and elsewhere between May and the first half of June.[29, 30] However, the Board heard that Microsoft's window of compromise may have started earlier than May 15, as it had published, based on standard 30-day log retention practices.[31]

**June 15-19, 2023: Department of State Detects the Intrusion**

State first detected anomalous activity on June 15, notified Microsoft on June 16, and, with support from Microsoft, investigated and analyzed the data over the course of the holiday weekend. By June 19, State determined that a threat actor had accessed six State email accounts, including those of personnel supporting the Secretary of State's upcoming trip to Beijing. State discovered that the threat actor accessed six other accounts between June 21 and June 24, and later discovered the compromise of one other account through the analysis of a seized virtual private server (VPS).[32]

**June 16-26, 2023: The Investigation Broadens; Department of Commerce is Identified as a Victim**

State reached out to Microsoft, the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI).[33, 34] CISA already had personnel at State conducting proactive threat hunting who began collecting data for analysis;[35] FBI shared details about the threat actor, its targets and exploitation vectors, and other indicators of compromise.[36, 37] After outreach from State, on June 16, Microsoft conducted an initial investigation, which assumed that Storm-0558 had gained entry to user emails through State's OWA.[38]

On June 19, Microsoft notified an organization in the U.K. that it was a victim; Microsoft later identified other victim organizations in the U.K.[39] On June 23, Microsoft notified Commerce Department that it, too, was a victim.[40] On or about June 26, Microsoft determined that Storm-0558 was using the stolen 2016 MSA key to issue tokens that allowed it to access both consumer and enterprise accounts.[41]

**June 24, 2023: Closing the Attack Vector**

On June 24, Microsoft invalidated the stolen key the threat actor was using.[42, 43] Microsoft believed that this action ended Storm-0558's access to the email accounts, as it almost immediately observed Storm-0558 attempt phishing and other methods to regain access to the email boxes it had previously compromised.[44]

**July 4, 2023 and Beyond: Continue Victim Notification and Remediation**

Microsoft began victim notification during its initial investigation, and this continued for weeks. Because of the nature of the intrusion, only Microsoft was able to identify most of the victims. It worked with the U.S. government to provide

[29] Anonymized.
[30] Anonymized.
[31] Anonymized.
[32] State Department, Board Meeting.
[33] FBI, Response to Board Request for Information.
[34] State Department, Board Meeting.
[35] Anonymized.
[36] State Department, Board Meeting.
[37] FBI, Board Meeting.
[38] Microsoft, Board Meeting.
[39] Anonymized.
[40] Commerce Department, Board Meeting.
[41] Microsoft, Board Meeting.
[42] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[43] Anonymized.
[44] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

victim information, and federal agencies undertook separate efforts to notify impacted individuals.[45, 46] These different efforts had varying degrees of success. Microsoft also took additional steps to ensure that the 2016 MSA key was replaced and that previously issued tokens would not work on any impacted individual customers' environments.[47]

### 1.2.2 THREAT ACTOR PROFILE

Storm-0558 has been active since approximately the year 2000.[48] Microsoft described Storm-0558 as "a China-based threat actor with activities and methods consistent with espionage objectives. While we have discovered some minimal overlaps with other Chinese groups such as Violet Typhoon (ZIRCONIUM, APT31), we maintain high confidence that Storm-0558 operates as its own distinct group." Microsoft historically observed the group primarily targeting U.S. and European diplomatic, economic, and legislative governing bodies; media companies, think tanks, and telecommunications and equipment services providers; and individuals connected to Taiwan and Uyghur geopolitical interests.[49] Microsoft assesses that the Microsoft Exchange Online intrusion was a targeted information-collection operation aimed at fulfilling the PRC's intelligence needs.[50]

Microsoft has developed insights into Storm-0558's activity clusters, ways in which its operational network overlaps with Microsoft's environment, and its affiliates and partnerships.[51] FBI and CISA assess that this latest campaign by Storm-0558 was also consistent with that of a nation-state threat actor with a high level of sophistication,[52] particularly with its knowledge of identity and access management (IAM) systems.[53]

Following disclosure of the Storm-0558 breach, Google's Threat Analysis Group was able to link at least one entity tied to this threat actor to the group responsible for the 2009 compromise of Google and dozens of other private companies in a campaign known as Operation Aurora,[54, 55] as well as the RSA SecurID incident.[56, 57] The threat group believed to have been behind the Operation Aurora campaign has been known to compromise cloud identity systems, steal source code, and engage in token-forging activities to gain access to targeted individuals' email accounts.[58, 59] Particularly, this threat group sought to understand the location of account login source code and the specific engineers involved in its development, ways in which organizations deploy account login systems to their production environment, and where and how organizations manage their cryptographic keys for account login cookies. In the wake of these attacks, investigators assessed that this threat group's tooling and reconnaissance activities suggest that it is well resourced, technically adept, and deeply knowledgeable of many authentication techniques and applications.[60]

[45] Anonymized.
[46] Anonymized.
[47] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[48] Anonymized.
[49] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[50] Microsoft, Board Meeting.
[51] Microsoft, Board Meeting.
[52] FBI, Board Meeting.
[53] CISA, Board Meeting.
[54] Google, Board Meeting.
[55] Operation Aurora was a series of cyberattacks from China that targeted U.S. private sector companies in 2010, compromising the networks of Yahoo, Adobe, Dow Chemical, Morgan Stanley, Google, and more than two dozen other companies to steal their trade secrets. Google was the only company that confirmed it was a victim and publicly attributed the incident to China. The incident is viewed as a milestone in the recent history of cyber operations because it raised the profile of cyber operations as a tool for industrial espionage. *Source: Council on Foreign Relations, "Operation Aurora," January 2010, https://www.cfr.org/cyber-operations/operation-aurora*
[56] The 2011 RSA SecureID intrusion resulted in the compromise of sensitive information relating to its two-factor SecurID authentication system. *Source: Schwartz, Mathew; Dark Reading, "RSA Pins SecurID Attacks On Nation State," October 12, 2011, https://www.darkreading.com/cyberattacks-data-breaches/rsa-pins-securid-attacks-on-nation-state*
[57] Anonymized.
[58] O'Gorman, Gavin and McDonald, Geoff; Symantec, "*The Elderwood Project*," September 6, 2012, https://www.cs.cornell.edu/courses/cs6410/2012fa/slides/Symantec_ElderwoodProject_2012.pdf
[59] Google specifically described the attack as a highly sophisticated and targeted attack on their corporate infrastructure that resulted in theft of intellectual property and access to targeted Gmail accounts. *Source: Google Official Blog, "A new approach to China," January 12, 2010, https://googleblog.blogspot.com/2010/01/new-approach-to-china.html*
[60] Google, Board Meeting.

### 1.2.3 2023 COMPROMISE OF MICROSOFT EXCHANGE ONLINE

#### 1.2.3.1 Storm-0558's Possession of the 2016 MSA Key

Microsoft learned that, in 2021, Storm-0558 had accessed a variety of documents stored in SharePoint and assessed that the threat actor was specifically looking for information on Azure service management and identity-related information.[61] Despite Microsoft's pursuit of the 46 key-theft hypotheses,[62] the Board assesses that Microsoft does not know how Storm-0558 obtained the 2016 MSA key. Microsoft stated in a September 6, 2023 blog post that the most probable way Storm-0558 had obtained the key was from a crash dump[63] to which it had access during the 2021 compromise of Microsoft's systems. However, Microsoft had only theorized that such a scenario was technically feasible in the 2016 timeframe. While Microsoft updated this blog on March 12, 2024 to correct its assessment of these theories,[64] it has not determined that this is how Storm-0558 obtained the key.[65]

The Board further determines that Microsoft has no evidence or logs showing the stolen key's presence in or exfiltration from a crash dump. During the Board's interview with Microsoft in November 2023, Microsoft said that soon after publication, it realized that the statements in the September 6 blog were inaccurate: Microsoft had found no evidence of a crash dump containing the 2016 MSA key material.[66] While Microsoft's latest update about this incident acknowledges that it did not find a crash dump containing the impacted 2016 MSA key material,[67] the possibility that the threat actor had accessed other keys and sensitive data, in addition to the 2016 MSA key, also remains unresolved,[68] adding to the Board's concern about the full consequences of the incident and remaining uncertainty.

In its November 2023 interview, Microsoft also told the Board that it was debating when to issue a new or updated blog based on the progress of its investigation but had not made any decisions.[69] In a written response to the Board on March 5, 2024, Microsoft maintained that it "intends to publish an update to the blog in the near future."[70] Over six months after its publication of the September 6 blog, and four months after acknowledging to the Board that the blog was inaccurate, Microsoft publicly corrected its mistaken assertions in an addendum, based on its "latest knowledge."[71]

#### 1.2.3.2 How Storm-0558 Used the 2016 MSA Key

Storm-0558 established its first identified component of external hosting infrastructure to execute the Exchange Online intrusion and gained access to email accounts on May 15, 2023.[72] After State notified Microsoft about the intrusion on June 16, 2023, Microsoft reviewed logs pertaining to the event, from the month of May, and identified that the first instance of malicious activity took place days after Storm-0558 had established its infrastructure. Microsoft also said that Storm-0558 had, in the past, used more sophisticated covert networks, but Microsoft believes that a previous disruption of the threat actor's infrastructure forced it to use a less sophisticated infrastructure for this intrusion that was more readily identifiable once discovered.[73] In this instance, Storm-0558 occasionally used infrastructure located geographically near its targets, likely to try to blend in with legitimate activity.[74, 75]

[61] Microsoft, Response to Board Request for Information.
[62] Microsoft, Board Meeting.
[63] A system crash (also known as a "bug check" or a "Stop error") occurs when Windows cannot run correctly. The dump file that is produced from this event is called a system crash dump. *Source: Microsoft Learn, "Generate a kernel or complete crash dump," September 2, 2022, https://learn.microsoft.com/en-us/troubleshoot/windows-client/performance/generate-a-kernel-or-complete-crash-dump*
[64] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023 (updated March 12, 2024), https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
[65] Microsoft, Board Meeting.
[66] Microsoft, Board Meeting.
[67] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023 (updated March 12, 2024), https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
[68] Anonymized.
[69] Microsoft, Board Meeting.
[70] Microsoft, Response to Board Request for Information.
[71] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023 (updated March 12, 2024), https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
[72] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[73] Microsoft, Board Meeting.
[74] Anonymized.
[75] Microsoft, Board Meeting.

Microsoft designed its consumer MSA identity infrastructure more than 20 years ago. Later, it introduced an enterprise Entra infrastructure, previously known as Azure Active Directory (AD). Initially, the consumer MSA system had no process for automated signing key rotation or deactivation and utilized a manual process instead. Over time, Microsoft automated the key rotation process in the enterprise system with the intent for the consumer MSA system to follow and use the same technology, but it had not done so in the consumer MSA system before the intrusion. Microsoft continued to rotate consumer MSA keys infrequently and manually until it stopped the rotation entirely in 2021 following a major cloud outage linked to the manual rotation process. While Microsoft had paused manual key rotation, it neither had, nor created, an automated alerting system to notify the appropriate Microsoft teams about the age of active signing keys in the consumer MSA service.[76]

Thus, possession of the 2016 MSA key—dated though it was—enabled the threat actor to forge authentication tokens that allowed it to access email systems. This access should have been limited to consumer email systems,[77] but due to a previously unknown flaw that allowed tokens to access enterprise email accounts, Storm-0558 was able to get into systems such as those at State and Commerce. The flaw was caused by Microsoft's efforts to address customer requests for a common OpenID Connect (OIDC) endpoint service that listed active signing keys for both enterprise and consumer identity systems.[78] However, Microsoft had not adequately updated the software development kits (SDKs), which Microsoft and its partners both used, to differentiate between the consumer MSA and the enterprise signing keys within the common endpoint. As a result, this allowed successful authentication to the Entra system for certain applications, such as mail, regardless of which key was used.[79]

Thus, as illustrated in Figure 1, the stolen 2016 MSA key in combination with the flaw in the token validation system permitted the threat actor to gain full access to essentially any Exchange Online account.[80, 81]

### Cloud Service Vulnerabilities

Cloud service providers (CSPs) do not always register and publicly disclose common vulnerabilities and exposures (CVEs) in their cloud infrastructure when mitigating those vulnerabilities does not require customer action.[82] This lack of disclosure, which is counter to accepted norms for cybersecurity more generally, makes it difficult for CSP customers to understand the risks posed by their reliance on potentially vulnerable cloud infrastructure.[83]

Microsoft does not know when Storm-0558 discovered that consumer signing keys (including the one it had stolen) could forge tokens that worked on both OWA consumer and enterprise Exchange Online. Microsoft speculates that the threat actor could have discovered this capability through trial and error. It assessed that during this incident, the actor was researching Microsoft technologies and used this knowledge to pivot and circumvent Microsoft's security measures within test cloud tenants.[84]

[76] Microsoft, Board Meeting.
[77] Microsoft, Board Meeting.
[78] OpenID providers like the Microsoft identity platform provide an OpenID Provider Configuration Document at a publicly accessible endpoint containing the provider's OIDC endpoints, supported claims, and other metadata. Client applications can use the metadata to discover the URLs to use for authentication and the authentication service's public signing keys. *Source: Microsoft; "OpenID Connect on the Microsoft identity platform," October 23, 2023, https://learn.microsoft.com/en-us/entra/identity-platform/v2-protocols-oidc*
[79] Microsoft, Board Meeting.
[80] Anonymized.
[81] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[82] Anonymized.
[83] Anonymized.
[84] Microsoft, Board Meeting.

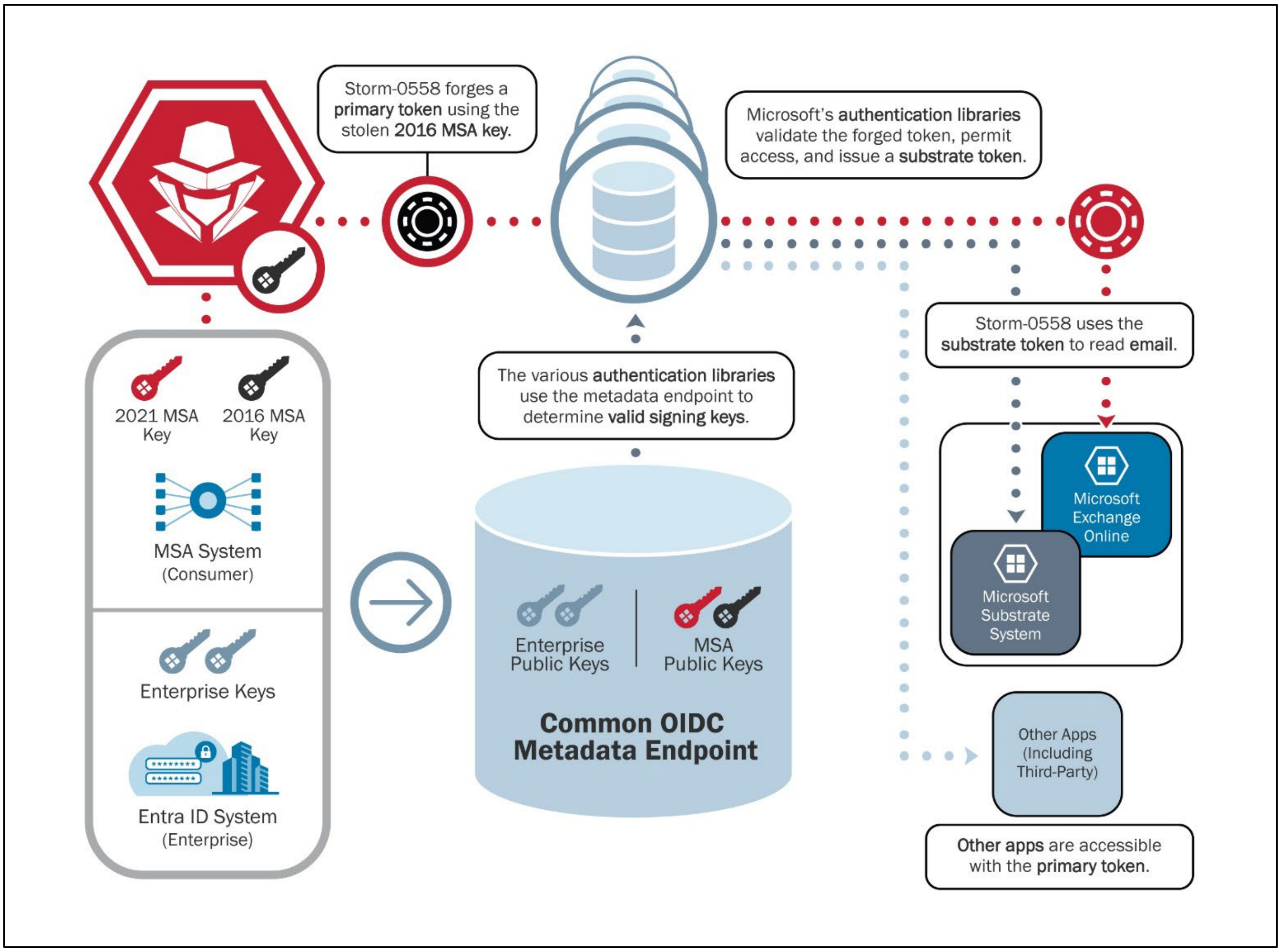

Storm-0558 forges a primary token using the stolen 2016 MSA key.
Microsoft's authentication libraries validate the forged token, permit access, and issue a substrate token.
2021 MSA Key
2016 MSA Key
MSA System (Consumer)
Enterprise Keys
Entra ID System (Enterprise)
The various authentication libraries use the metadata endpoint to determine valid signing keys.
Enterprise Public Keys
MSA Public Keys
Common OIDC Metadata Endpoint
Storm-0558 uses the substrate token to read email.
Microsoft Exchange Online
Microsoft Substrate System
Other Apps (Including Third-Party)
Other apps are accessible with the primary token.

*Figure 1: Storm-0558 Token Abuse with Stolen 2016 MSA Key*

### 1.2.4 2021 COMPROMISE OF MICROSOFT CORPORATE NETWORK BY STORM-0558

Microsoft told the Board that Storm-0558 had compromised Microsoft's corporate network via an engineer's account, which occurred between April and August 2021. Microsoft believes, although it has produced no specific evidence to such effect, that this 2021 intrusion was likely connected to the 2023 Exchange Online compromise because it is the only other known Storm-0558 intrusion of Microsoft's network in recorded memory. During this 2021 incident, Microsoft believes that Storm-0558 gained access to sensitive authentication and identity data.[85]

As announced on March 26, 2020 and completed on April 23, 2020, Microsoft acquired a company called Affirmed Networks[86] that worked in 5G technology and advanced networking. Microsoft believes that prior to the acquisition, Storm-0558 targeted an engineer and compromised their device due to their experience in 5G technology and advanced networking. After the acquisition, Microsoft supplied corporate credentials to the acquired engineer that allowed access to Microsoft's corporate environment with the compromised device. Leveraging this access, Storm-0558 captured an authentication token, then replayed the token to authenticate as the Microsoft employee on Microsoft's corporate network.[87, 88]

[85] Microsoft, Board Meeting.
[86] Khalidi, Yousef; Microsoft, "*Microsoft announces agreement to acquire Affirmed Networks to deliver new opportunities for a global 5G ecosystem*," March 26, 2020, https://blogs.microsoft.com/blog/2020/03/26/microsoft-announces-agreement-to-acquire-affirmed-networks-to-deliver-new-opportunities-for-a-global-5g-ecosystem/
[87] Microsoft, Board Meeting.
[88] Anonymized.

While Storm-0558 exhibited an advanced understanding of Microsoft's network and demonstrated a particular interest in information associated with identity and engineering, Microsoft does not have direct evidence linking the two incidents. Microsoft's insider threat investigation also did not find evidence to indicate that a malicious insider was a part of the 2023 intrusion. Through its ongoing investigations, Microsoft said it believes that alternative initial access vectors, such as an insider threat, remain unlikely.[89]

Still, the 2021 compromise of Microsoft's corporate network highlights gaps within the company's mergers and acquisitions (M&A) security compromise assessment and remediation process. Microsoft told the Board that, where applicable and based on the risk profile associated with the acquisition and the terms of the agreement, Microsoft deploys telemetry and threat intelligence tools to assess whether an acquisition has been compromised, and remediation can occur pre- or post-closing. Microsoft and the acquisition target formalize a security incident response process to coordinate security incidents until close. Following the acquisition, Microsoft's internal audit team may conduct security audits of an acquisition leveraging findings from due diligence security assessments to inform the scope of these assessments.[90]

### 1.2.5 INCIDENT IMPACT

The Microsoft Exchange Online intrusion was significant: Storm-0558's combined possession of the 2016 MSA key and its ability to access enterprise Exchange accounts allowed the threat actor to access any Microsoft Exchange Online account. Although Microsoft expressed confidence resulting both from extensive log analysis and direct actor tracking that this intrusion only impacted Microsoft Exchange Online, the stolen key also could have been used by the threat actor to access other Microsoft cloud applications had it chosen to do so. These include both Microsoft and third-party applications reliant on Microsoft's identity provider (IDP) that were either intentionally (due to supporting consumer accounts) or unintentionally (due to using client libraries or bespoke code that failed to properly validate authentication tokens) trusting tokens signed by the stolen key.[91, 92, 93] Microsoft believes that Storm-0558 itself limited the scope of this intrusion, as it appeared to be selective in its targeting, balancing its information-gathering objectives with probabilities of detection.[94] The Board believes that the actor also prioritized high-value and time-sensitive collection missions.

Yet while the number of victims was relatively low given the breadth of the access available to the actor, they were widespread: Storm-0558 accessed the email accounts of 22 enterprise organizations,[95] including government agencies and three think tanks.[96] This intrusion also impacted the personal accounts of individuals likely associated with these organizations.[97] The non-U.S. victims included four foreign government entities, three private sector organizations, and four educational entities.[98]

**Impacted U.K. Accounts**

Storm-0558 compromised several U.K. organizations' email accounts and exfiltrated an unknown number of emails. Initially, Microsoft reported three affected accounts to the National Cyber Security Centre (NCSC),[99] but further investigation by Microsoft revealed additional victims. This discovery underscores both the evolving nature of this incident's impact assessment and the delayed victim identification.[100] The Board has not learned why these U.K. individuals were chosen over others.

[89] Microsoft, Board Meeting.
[90] Microsoft, Response to Board Request for Information.
[91] Anonymized.
[92] Microsoft, Board Meeting.
[93] Anonymized.
[94] Microsoft, Board Meeting.
[95] Microsoft, Board Meeting.
[96] Anonymized.
[97] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[98] Anonymized.
[99] NCSC, the U.K.'s version of FBI Cyber Division, supports the most critical organizations in the U.K., the wider public sector, industry, subject matter experts, and the general public. *Source: NCSC, "What we do," https://www.ncsc.gov.uk/section/about-ncsc/what-we-do*
[100] NCSC, Board Meeting.

Microsoft knew the identity of all of the individuals whom Storm-0558 targeted, many of whom were linked to entities associated with Western European, APAC, Latin American, and Middle Eastern countries.[101, 102] Of these accounts, the intrusion impacted at least 391 personal email accounts in the U.S,[103] including some Hotmail accounts belonging to current and former employees of an affected government organization.[104]

The threat actor compromised the official and personal mailboxes of many senior U.S. government officials, some of which likely contained information about the U.S.'s diplomatic and economic policies toward the PRC. The timing of the intrusion, just before Secretary Blinken's trip to Beijing in 2023, combined with the seniority of the officials targeted, highlights a potential partial rationale for such intrusions.[105]

## 1.3 INCIDENT MANAGEMENT

### 1.3.1 HOW STATE DEPARTMENT DISCOVERED THE INTRUSION

State Department was the first entity to detect the intrusion when on June 16, 2023, a State SOC analyst observed multiple alerts from the "Big Yellow Taxi" custom alert rule. Detecting an intrusion like this is difficult; State Department found Storm-0558 because it had purchased enhanced logging through the G5 licenses,[106] which few, if any, victims had similarly acquired.[107] As standard practice, State's SOC uses that enhanced logging to build custom alerts like "Big Yellow Taxi" in response to an evolving threat environment.[108] Just purchasing the additional logging alone would not have been enough; in fact, the Board heard that few organizations analyzed the voluminous MailItemsAccessed log in detail, and such in-depth analysis would be difficult for smaller organizations.

State, however, used the data to build custom detection rules to enable it to identify anomalous access to mailboxes such as the activity undertaken in this intrusion. State Department's SOC designed custom alerting capabilities based on three years of experience dealing with anomalous access to mailboxes. In particular, State curated log events like the MailItemsAccessed data to enumerate all applications accessing mailboxes within its infrastructure, and to trigger alerts for any anomalous events.[109] It also designed a rule to detect deviations in mailbox activity by comparing baseline interactions of applications with Exchange Online.[110] These rules provided detailed information about application IDs touching mailboxes, specific application details, and context about particular mailboxes involved, thereby enhancing State's ability to pinpoint potential issues quickly.[111]

### 1.3.2 INVESTIGATION AND ANALYSIS

#### 1.3.2.1 Microsoft's Investigation

After receiving State Department's report on June 16, 2023, Microsoft began an initial investigation using its normal processes, which involved Microsoft's Detection and Response Team (DART). Microsoft attributed the intrusion to Storm-0558 after identifying infrastructure associated with the threat actor. This investigation continued until June 26, 2023. At the time, Microsoft determined the impact was larger in scope and may have involved the compromise of Microsoft's systems. Specifically, Microsoft discovered the threat actor was able to access emails directly using forged tokens signed with a consumer token signing key that was supposed to have been inactive. Once it identified and revoked the stolen 2016 MSA key, Microsoft was able to use the key to inform its hunting efforts: since the key was inactive at this point, the Microsoft identity system was not using it to sign any tokens. Thus, all signing instances using this key constituted nefarious activity. This insight helped Microsoft determine that its identity system had not issued the invalid tokens and identify threat actor activities with high confidence,[112] meaning the threat actors had an MSA

[101] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[102] Microsoft, Response to Board Request for Information.
[103] Anonymized.
[104] Anonymized.
[105] Anonymized.
[106] State Department, Board Meeting.
[107] Anonymized.
[108] State Department, Board Meeting.
[109] State Department, Board Meeting.
[110] Anonymized.
[111] State Department, Board Meeting.
[112] Microsoft, Board Meeting.

key that could be used to issue working—though fraudulently issued—tokens that could grant application access to mailboxes within the enterprise environment.[113]

In response, on June 26, 2023, Microsoft launched an overnight investigation focusing on the key and token and assessed with high confidence that the threat actor had forged a token using a consumer MSA key that should have been inactive. Upon confirming that Storm-0558 had forged the token, Microsoft began converging individual processes into its Software and Services Incident Response Plan (SSIRP), which has different urgency levels based on multiple criteria, including the number of impacted customers. On June 27, 2023, Microsoft assigned this intrusion a SEV-0 rating, the highest urgency level. This meant that the incident required robust communication, visibility, and coordination across Microsoft and up to its most senior leadership, including its Board of Directors.[114]

Microsoft's incident response plan leverages several specialty teams that coordinate response for large and small incidents. While some incidents are local, like a good faith researcher reporting a vulnerability that can be repaired without needing cross-team coordination, in this case Microsoft leveraged its standardized global security response processes, allowing it to coordinate across multiple teams and establish separate workstreams for containment, customer impact, incident notifications, and investigating the key's exfiltration. For the last workstream, it assembled team members from DART, the Microsoft Threat Intelligence Center (MSTIC), and various security teams to hypothesize potential egress points for the key. This collaborative effort generated the three sub-workstreams dedicated to investigating Microsoft's 46 hypotheses.[115]

After reexamining the 2021 compromise of the engineer and analyzing what Storm-0558 could have accessed using the stolen credentials at that time, Microsoft determined that it needed to expand its investigation to scan for the presence of the 2016 MSA key across its network. Microsoft told the Board that it continues to engage in this work. Additionally, after Microsoft put protections in place to prevent future token generation by invalidating the key, it saw the actor experiment and unsuccessfully attempt to generate new tokens.[116, 117] Storm-0558's use of the invalid key to sign authentication requests allowed Microsoft's teams to determine the scope of the threat actor's access.[118] Microsoft found no evidence of a breach in the perimeter of the signing system. During the investigation, Microsoft examined the threat actor's targeting methods, and looked for evidence of a compromise or the introduction of an external device into the corporate network as possible attack vectors. The investigation uncovered what Microsoft believes is the precise number of targeted individuals, and enabled Microsoft's acquisition of the malware that Storm-0558 used to sign tokens for accessing OWA. This discovery was pivotal in focusing the search across Microsoft's logs for any additional threat activity. Microsoft has not yet determined how Storm-0558 obtained the 2016 MSA key and says that it is continuing to investigate.[119]

#### 1.3.2.2 Investigations by Victim Organizations

Victims found it difficult to investigate these intrusions after initial detection because Microsoft could not, or in some cases did not, provide victim organizations with holistic visibility into all necessary data. Although Microsoft activated enhanced logging for identified victims who did not have the appropriate license, Microsoft could not give historical logs to customers unless they already had the premium licenses at the time of the intrusion. Thus, customers could capture data from the time that Microsoft enabled additional logging capabilities but were unable to view past intrusion activity.

State's SOC had limited visibility into the activity but, based on the particular email accounts that the threat actor accessed, quickly determined that the targeted individuals were supporting the Secretary's upcoming trip to Beijing. This approach significantly aided State in refining its analysis of the activity. Later joined in its response by the National Security Agency (NSA), CISA, and Microsoft, State confirmed the intrusion into the mailboxes on June 19, 2023. It then began a comprehensive investigation to understand what was happening and what the actor had exfiltrated. On June 21, 2023, after issuing a legal process to the U.S.-based VPS provider that hosted the attacker's infrastructure, the government obtained a disk image from the provider that contained valuable insights into the threat actor's intrusion

[113] Anonymized.
[114] Microsoft, Board Meeting.
[115] Microsoft, Board Meeting.
[116] Microsoft, Board Meeting.
[117] Anonymized.
[118] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[119] Microsoft, Board Meeting.

attempts and follow-on activity. That same day, the FBI was notified of the intrusion and received this information. In parallel with CISA, FBI conducted an independent analysis on the disk image and made its findings available to the broader group.[120]

Microsoft first notified Commerce's Office of the Chief Information Officer (OCIO) about the intrusion into the Commerce Department's systems on June 23, 2023, one week after State Department's discovery. According to Microsoft's initial reports, Storm-0558 accessed and exfiltrated data from Commerce on June 21, 2023.[121, 122] However, later audit logs provided by Microsoft showed Storm-0558 had initially accessed Commerce data on June 6, 2023.[123]

Commerce Department's Enterprise SOC (ESOC) team immediately contacted CISA for assistance, marking the beginning of the entity's efforts to understand the intrusion.[124] It then asked Microsoft to share relevant logs, and Microsoft provided some data and activated G5 logging. However, Commerce could not view past activity as these logs only captured data from the time that Microsoft enabled the advanced logging. Microsoft told Commerce that it had derived some of its information about the incident from additional logging capabilities available to internal Microsoft teams for monitoring threat actor behavior.[125, 126] Commerce Department asked Microsoft to share these logs so that it could do its own assessment of the incident, including any potential impact to other subordinate bureaus' systems. Microsoft shared certain portions of Commerce's impacted unified audit logs and provided Internet Protocol (IP) addresses that the organization could use to search across its network. This incomplete dataset impacted Commerce Department's ability to do a complete assessment of the incident.[127]

Commerce Department collected all affected user devices, temporarily suspended impacted mailbox usage, and deployed signatures at its ESOC to monitor for and detect related activity. Commerce also shared all signatures with subordinate Bureaus to deploy. To monitor for follow-on threat activity and identify impact beyond initial reporting, Commerce activated G5 logging, but as discussed, it could not analyze historical telemetry for malicious activity because Microsoft could only provide these logs and data going forward—it had not collected and did not possess the data for earlier activity because Commerce did not have the G5 licenses then.[128]

#### 1.3.2.3 Investigations by Government Incident Responders

On June 21, 2023, State Department notified the FBI Washington Field Office's Cyber Task Force that a threat actor had accessed official State mailboxes between June 13 and June 20, 2023. FBI told the Board that Microsoft was critically important to its ability to understand the nature of the compromise, who the targets were, and how the threat actor had exploited the vulnerability. Microsoft also helped FBI in continuing to develop proof of high-level attribution to Storm-0558 and voluntarily provided indicators of compromise (IoCs) for further investigation.[129]

CISA was a central point for information sharing related to detection, mitigation, and remediation across and between federal agencies, and with private sector partners and victims. It also shared guidance to agencies for how to detect this intrusion, specifically to examine their logs, to the extent that they had access to the G5 service level, for unexpected MailItemsAccessed events with irregular application IDs.[130] At the time of the intrusion, CISA was already providing State Department with proactive threat hunting services as part of a routine, by-request engagement. CISA shifted to incident response following State's detection of Storm-0558 activity and analyzed the pattern of threat activity. CISA also collected data and surveyed observations from other stakeholder organizations to search for compromises beyond State.[131]

CISA tried to recreate Storm-0558's activity but could not replicate the forged token as it did not possess the necessary stolen MSA key. Without the 2016 MSA key, CISA could only emulate the incident in a limited way and had to rely on its knowledge of Exchange Online and logs from State Department to conduct its investigation. Leveraging tokens it

[120] State Department, Board Meeting.
[121] Anonymized.
[122] Commerce Department, Board Meeting.
[123] Commerce Department, Board Meeting.
[124] Commerce Department, Response to Board Request for Information.
[125] Commerce Department, Board Meeting.
[126] Anonymized.
[127] Commerce Department, Board Meeting.
[128] Commerce Department, Board Meeting.
[129] FBI, Board Meeting.
[130] Anonymized.
[131] CISA, Board Meeting.

generated in OWA, similar to those used by Storm-0558, CISA conducted a test to emulate the application programming interface (API) used by the threat actor to exfiltrate email. Subsequent forensics on the threat actor's tooling validated that CISA's emulation accurately reflected Storm-0558's activities other than the initial token forgery. As a result of this emulation work, CISA assessed that the threat actor could not avoid generating the MailItemsAccessed log data during the intrusion, which meant that it could detect similar future activity if it had the relevant logs.[132]

CISA also worked with international partners; the NCSC engaged CISA during the first week of its investigation after realizing the breadth of the intrusion. The NCSC told the Board that the conversations were useful as the NCSC and CISA shared information on intrusion impacts and each organization's respective engagement with Microsoft.[133]

While Microsoft has longstanding relationships with CISA, in this instance, Microsoft delayed reaching out to CISA until it could confirm additional details of the intrusion. Microsoft did not know the root cause of the intrusion for some time and was reluctant to share data with CISA and others until it had more certainty. CISA reached out to Microsoft to share its investigative efforts, at which point Microsoft confirmed that it had observed CISA's replication of the intrusion using a test commercial tenant. As a result of this outreach, Microsoft further engaged with CISA and provided detailed briefings, disclosing how it had uncovered Storm-0558's presence within its network and providing details on the nature and methodology of the threat actor. During these discussions, Microsoft provided some of the intrusion's technical details and gave CISA limited access to its forensics about the threat actor's infrastructure.[134]

**International Partners: NCSC**

The U.K. victims did not have enhanced logging capabilities, which inhibited the NCSC's ability to verify Microsoft's claims of earlier threat activity. During its response, the NCSC had to balance disabling the compromised environment with leaving it operational so it could further analyze the intrusion and ensure that Storm-0558 could not regain access if the NCSC's mitigations failed to close the underlying vulnerability.[135]

Based on Microsoft's initial advice, the NCSC suspected the threat actor was likely stealing tokens from endpoints, particularly iOS devices. This led the NCSC to gather as many devices as possible from victims over the first two days of its investigation. However, this theory proved fruitless, highlighting the difficulty that organizations faced in determining the intrusion's attack vector. By the second week of the NCSC's investigation, Microsoft had revoked the key and the NCSC's focus shifted from stopping malicious activity to identifying exfiltrated data. Finally, by mid-July, the NCSC turned its attention to examining potentially compromised corporate accounts.[136]

### 1.3.3 VICTIM COORDINATION AND NOTIFICATION

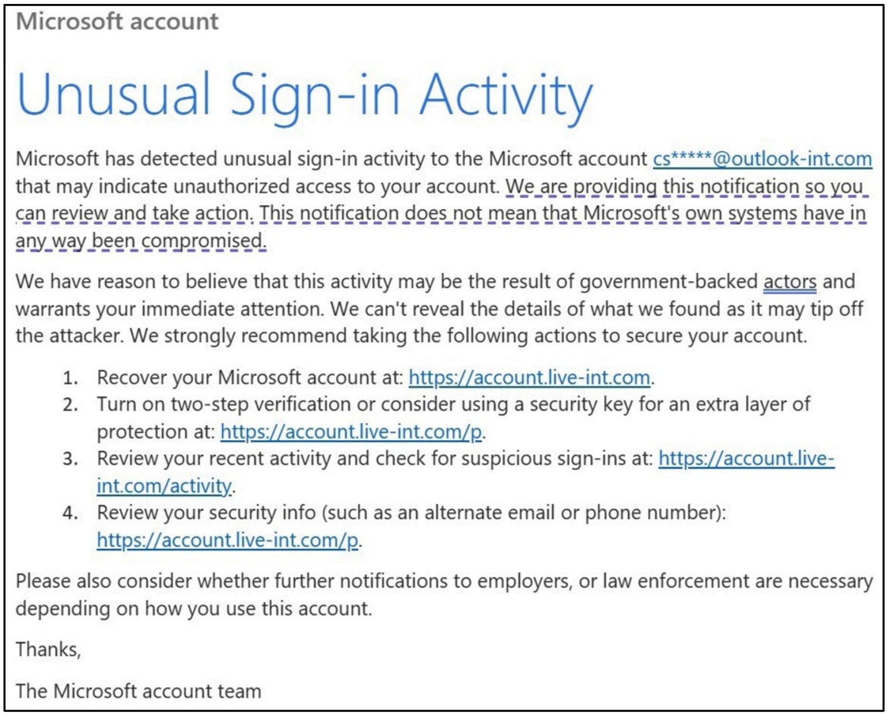
Victim coordination was complicated for this incident as it involved multiple U.S. government agencies, foreign governments, senior government officials, private sector organizations, and private individuals. While both Microsoft and government agencies undertook separate efforts to notify victims, Microsoft had legal and contractual limitations on what victim information it could share with the government, absent victim consent.[137]

FBI worked with Microsoft to obtain the U.S. victim information, and on July 10, 2023, Microsoft lawfully provided FBI with a list of affected email accounts and related subscriber information for those accounts. FBI engaged directly with almost every victim with an affected personal account. For compromised enterprise accounts, FBI worked with system owners, who in turn informed individuals whose accounts were part of the intrusion.[138]

By July 25, 2023, FBI had identified the owners of nearly all affected accounts and had begun issuing leads to notify government officials deemed to have the most sensitive information, in line with FBI Cyber Division policy on victim notification requirements. FBI learned that some victims were unaware that a threat actor had accessed their emails. Microsoft informed FBI that it had notified customers through several methods, including short message service (SMS)

[132] CISA, Board Meeting.
[133] NCSC, Board Meeting.
[134] CISA, Board Meeting.
[135] NCSC, Board Meeting.
[136] NCSC, Board Meeting.
[137] Microsoft, Board Meeting.
[138] FBI, Board Meeting.

text messages, nation-state notifications (NSNs),[139] emails sent to recovery accounts (see Figure 2), and pop-up messages via an authenticator application, but some victims told FBI that they viewed these notifications as possible spam and disregarded them. As a result, FBI changed its stance and notified every identified account owner through coordination with FBI field offices, Department of Justice (DoJ), CISA, State, and Commerce. FBI provided each victim with a joint Cybersecurity Advisory previously published by FBI and CISA on July 12, 2023, as well as a copy of Microsoft's blog outlining analysis of Storm-0558 activity and cyber hygiene best practices.[140]



Microsoft account

Unusual Sign-in Activity

Microsoft has detected unusual sign-in activity to the Microsoft account cs*****@outlook-int.com that may indicate unauthorized access to your account. We are providing this notification so you can review and take action. This notification does not mean that Microsoft's own systems have in any way been compromised.

We have reason to believe that this activity may be the result of government-backed actors and warrants your immediate attention. We can't reveal the details of what we found as it may tip off the attacker. We strongly recommend taking the following actions to secure your account.

1. Recover your Microsoft account at: https://account.live-int.com.
2. Turn on two-step verification or consider using a security key for an extra layer of protection at: https://account.live-int.com/p.
3. Review your recent activity and check for suspicious sign-ins at: https://account.live-int.com/activity.
4. Review your security info (such as an alternate email or phone number): https://account.live-int.com/p.

Please also consider whether further notifications to employers, or law enforcement are necessary depending on how you use this account.

Thanks,

The Microsoft account team

*Figure 2: Microsoft Victim Notification Email*

### Case Study: Congressman Don Bacon

Congressman Don Bacon is a Member of the House of Representatives and currently serves on the House Armed Services Committee, including its Strategic Forces and Tactical Air and Land Forces subcommittees. Congressman Bacon is also a member of the House Taiwan Caucus.[141] As a prominent congressional voice on national security matters, Congressman Bacon is a high-value target for adversarial intelligence-gathering objectives. Microsoft's first noticed outreach to Congressman Bacon about the intrusion was an email prompting him to change his password, sent a month before FBI contacted him. Congressman Bacon thought the password change email looked strange and was potentially fraudulent, so he changed his password directly rather than using the link provided in the notification instructions. He later learned from FBI that his personal email had been compromised. FBI assured him that his devices were secure and that he had done nothing wrong; rather, the intrusion originated from a compromise affecting Microsoft. Microsoft did not advise Congressman Bacon to take any action to protect his account beyond the one email recommending a password change. At some point after the initial password change email, Microsoft sent another that provided details about the intrusion, including that Microsoft believed it had been synchronized with Secretary of State Antony Blinken's visit, June 16 to June 21, 2023, and Commerce Secretary Gina Raimondo's visit, August 27 to August 30, 2023, to China.[142]

[139] Whenever an organization or individual account holder is targeted or compromised by observed nation-state activities, Microsoft delivers an NSN directly to that customer to give them the information they need to investigate the activity. *Source: Lambert, John; Microsoft, "Microsoft Digital Defense Report shares new insights on nation-state attacks," October 25, 2021, https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/*

[140] FBI, Board Meeting.

[141] United States Congress, "*Committees and Caucuses,*" https://bacon.house.gov/about/committees-and-caucuses.htm

[142] Rep. Don Bacon, Board Meeting.

From July 4 to July 14, 2023, Microsoft issued notifications to 63 high-profile individuals in the U.K.[143] who were identified as having been directly targeted or compromised by observed nation-state activities. However, the NCSC was concerned that some victims may not pay attention to these notifications even though the notifications may point to a widely reported incident. All Enterprise NSNs explicitly identified Storm-0558 as the PRC-affiliated threat actor, and a dedicated team issued an individualized NSN to each affected person. This process is unique to NSNs and is distinct from the notifications sent to other personal victims via email or other automated methods.[144] The NCSC provided the most sensitive impacted individuals with tailored and dedicated briefings summarizing the intrusion and asked victims what data may have been exfiltrated from their emails. The NCSC explored all available avenues and obtained the victim identities through a difficult, time-consuming process.[145]

### 1.3.4 REMEDIATION AND RECOVERY

Between June 24 and July 3, 2023, to remediate Storm-0558's activity, Microsoft:

1) revoked the key's ability to sign tokens and cleared related caching data stored in downstream systems;[146]
2) accelerated an update to change the way that Exchange Online accepted tokens, blocking any requests using the same method as Storm-0558 had used to exploit the vulnerability;[147, 148]
3) fixed the flaw that allowed unauthorized access to enterprise data with consumer keys by updating various software packages within its applications and rapidly deploying these updates across its systems;[149]
4) rotated other signing keys for enterprise and consumer tokens, issuing the new keys from enterprise infrastructure that it deemed safer;
5) enhanced how it monitors and alerts for suspicious activities within its identity systems, a process Microsoft was continuing to refine at the time of its discussion with the Board;[150] and
6) developed and tailored contextual guides that detailed the intrusion and provided them to organizations and individual customers.[151]

**Microsoft's Engagement with the PRC Government**

Given the culpability of a PRC-affiliated threat actor in this compromise, the Board was pleased to be told that Microsoft first contacted the PRC government only after it had remediated the incident, having its first communication with the PRC government on August 17, 2023. Typically, Microsoft directly engages with the PRC government at a high level after incidents such as this. In this case, Microsoft published a blog in July 2023, and its legal teams engaged in follow-on discussions with the PRC government.[152]

## 1.4 PUBLIC REPORTING

On July 11, 2023, Microsoft published its first blog about the Exchange Online intrusion, disclosing that Storm-0558 had used an MSA consumer signing key that enabled it to forge authentication tokens and access Exchange Online and

[143] Anonymized.
[144] Anonymized.
[145] NCSC, Board Meeting.
[146] Microsoft, Board Meeting.
[147] Microsoft identified the design flaw within the GetAccessTokensForResources API. Source: Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[148] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[149] Anonymized.
[150] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[151] Microsoft, Board Meeting.
[152] Microsoft, Board Meeting.

Outlook accounts.[153] Microsoft stated that it had notified all impacted customers and launched an investigation,[154, 155] and publicly named Commerce as an affected entity; however, the Board learned that Microsoft did not provide Commerce forewarning that the blog post would publicly name Commerce as an affected entity.[156]

Microsoft published a second blog on July 14, 2023, filling some gaps in the first blog post, including indicators and technical details. This second post also provided insights into detecting the attacker infrastructure. Microsoft also provided details on the scale of the intrusion, characteristics of Storm-0558's infrastructure, and portions of the malware the threat actor had used to conduct the intrusion.[157] Researchers in the security community scrutinized the timing and content of Microsoft's second blog, and identified gaps and inconsistencies in Microsoft's public accounts of the intrusion, including tactics, techniques, and procedures (TTPs), IoCs, and indicators of attack (IoA).[158]

In response to Microsoft's blogs, Wiz, a cloud security company, launched a limited independent review of the incident. Wiz concluded that the compromised 2016 MSA key could sign access tokens for many types of applications, far beyond Microsoft's initial reporting. For Wiz, this revelation underscored the need for a broader awareness and proactive measures across all affected stakeholders.[159] CISA also conducted an in-depth review of Microsoft's public statements. CISA's findings pointed to the need for greater clarity and transparency from Microsoft about the initial compromise's blast radius, token scope, and impact. Specifically, CISA noted information gaps in what additional capabilities the stolen key granted the threat actor, Microsoft's incident response measures, and the potential for threat actors to access internal servers or additional key material.[160]

On September 6, 2023, Microsoft published a third blog, entitled "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*." This blog stated that, "Our investigation found that a consumer signing system crash in April of 2021 resulted in a snapshot of the crashed process ('crash dump')." The blog went on to say that "a race condition allowed the key to be present in the crash dump" and that the crash dump "was subsequently moved from the isolated production network into our debugging environment on the internet connected corporate network." Finally, Microsoft said that the engineer's account that Storm-0558 had compromised in 2021 "had access to the debugging environment containing the crash dump which incorrectly contained the key" and while it had no logs showing the actual exfiltration, "this was the most probable mechanism by which the actor acquired the key."[161]

As Microsoft continued to investigate, it determined that elements of the September 6 blog related to how the actor acquired the impacted customer token signing key were likely inaccurate. Microsoft told the Board that although the blog stated its "technical investigation has concluded," it continued to investigate the threat actor and subsequently determined that while a crash dump could have included key material and that such a dump could have been moved out of the secure token signing environment, Microsoft had not found any dump containing this key material, as it had mistakenly asserted in the September 6 blog.[162]

During the Board's interview with Microsoft in November 2023, Microsoft told the Board that it was considering issuing a new or updated blog on its ongoing investigative findings, but that it had not yet made any decisions in that regard. In this meeting, Microsoft confirmed that although its investigation into how the threat actor obtained the key material had been ongoing, it had no change in the number of customers impacted, depth of impact, or time of impact. At that time, Microsoft intended to publish an update to the blog in the near future.[163] In a written response to follow-up questions on this topic from the Board, Microsoft responded, "We believe that describing how the company is

[153] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

[154] Tamari, Shir; Wiz, "*Compromised Microsoft Key: More Impactful Than We Thought*," July 21, 2023, https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr

[155] Anonymized.

[156] Commerce Department, Board Meeting.

[157] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

[158] Anonymized.

[159] Tamari, Shir; Wiz, "*Compromised Microsoft Key: More Impactful Than We Thought*," July 21, 2023, https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr

[160] CISA, Board Meeting.

[161] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023, https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

[162] Microsoft, Board Meeting.

[163] Microsoft, Board Meeting.

considering updating its public statements would entail disclosure of attorney-client privileged information. However, we will continue to assess the September 6, 2023 blog, including whether to update it, upon completion of the investigation." [164]

On March 12, 2024, Microsoft published an addendum to its September 6 blog that provided further information as it related to Microsoft's ongoing investigation. In its update, Microsoft clarified that, in the past, its standard debugging process did not prohibit the ability to move crash dump material out of the secure signing environment, indicating that such a scenario was once possible. Microsoft's statement also confirmed that the race condition discussed above could allow the crash dump to move from the secure token signing environment, but would not impact whether the 2016 MSA key could be present in the crash dump. [165]

Ultimately, this March 12 addendum maintained that Microsoft's "leading hypothesis remains that operational errors resulted in key material leaving the secure token signing environment that was subsequently accessed in a debugging environment via a compromised engineering account." Still, Microsoft did not recant its initial crash dump theory as a likely root cause, as it initially implied in its September 6 blog. [166] At the conclusion of the Board's review, even in the context of Microsoft's March 12 update, Microsoft has not identified a crash dump that contains the 2016 MSA key, or any other evidence of the key having been moved inappropriately.

[164] Microsoft, Response to Board Request for Information.

[165] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023 (updated March 12, 2024), https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

[166] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023 (updated March 12, 2024), https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

# 2 FINDINGS AND RECOMMENDATIONS

## 2.1 CLOUD SERVICE PROVIDERS

### 2.1.1 MICROSOFT CORPORATE SECURITY CULTURE

The Board concludes that Microsoft's security culture was inadequate. The Board reaches this conclusion based on:

1. the cascade of Microsoft's avoidable errors that allowed this intrusion to succeed;
2. Microsoft's failure to detect the compromise of its cryptographic crown jewels on its own, relying instead on a customer to reach out to identify anomalies the customer had observed;
3. the Board's assessment of security practices at other CSPs, which maintained security controls that Microsoft did not;
4. Microsoft's failure to detect a compromise of an employee's laptop from a recently acquired company prior to allowing it to connect to Microsoft's corporate network in 2021;
5. Microsoft's decision not to correct, in a timely manner, its inaccurate public statements about this incident, including a corporate statement that Microsoft believed it had determined the likely root cause of the intrusion when in fact, it still has not; even though Microsoft acknowledged to the Board in November 2023 that its September 6, 2023 blog post about the root cause was inaccurate, it did not update that post until March 12, 2024, as the Board was concluding its review and only after the Board's repeated questioning about Microsoft's plans to issue a correction;
6. the Board's observation of a separate incident, disclosed by Microsoft in January 2024, the investigation of which was not in the purview of the Board's review, which revealed a compromise that allowed a different nation-state actor to access highly-sensitive Microsoft corporate email accounts, source code repositories, and internal systems; and
7. how Microsoft's ubiquitous and critical products, which underpin essential services that support national security, the foundations of our economy, and public health and safety, require the company to demonstrate the highest standards of security, accountability, and transparency.

If Microsoft had not paused manual rotation of keys; if it had completed the migration of its MSA environment to rotate keys automatically; if it had put in place a technical or other control to generate alerts for aging keys, the 2016 MSA key would not have been valid in 2023. Further, if Microsoft had not made the error that allowed consumer keys to authenticate to enterprise customer data (or, alternatively, if it had detected and addressed this flaw), the scope of the intrusion would have been far narrower and would not have impacted the State Department, Commerce Department, or any other enterprise customers. If Microsoft had deployed alerting or prevention to detect forged tokens that do not conform to Microsoft's own token generation algorithms, this incident likely could also have been stopped or detected by Microsoft all on its own. Even after all this, if Microsoft had other security controls in place for its digital identity system—as the Board finds other CSPs had in place at the time—this intrusion vector could have been blocked or detected. Finally, once State Department alerted Microsoft to the intrusion, Microsoft did not have the logs or other forensic data to determine how or when Storm-0558 had stolen the key.

The decision to completely stop manual rotation of signing keys in 2021 after a large cloud outage, along with failing to prioritize the development of an automated key rotation solution, are troubling examples of decision-making processes within the company that did not prioritize security risk management at a level commensurate with the threat and with Microsoft technology's vital importance to more than one billion of its customers worldwide. Taken together with the inadequate controls in the authentication system to detect and mitigate key theft after multiple attempts by the threat actor to compromise identity and authentication systems, including in Operation Aurora in 2009 and RSA SecureID in 2011—something that all other major CSPs have worked to address in their systems' architectures—the Board finds that Microsoft had not sufficiently prioritized rearchitecting its legacy infrastructure to address the current threat landscape. In addition, the failure to detect the compromise of an employee's laptop in an acquired company in 2021, prior to allowing it to connect to Microsoft's corporate network, raises questions about the robustness of Microsoft's M&A compromise assessment program.

The Board is also concerned with Microsoft's public communications after the incident. In its September 6, 2023 blog post entitled "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," Microsoft explained that Storm-0558 likely stole the 2016 MSA key in the "crash dump" scenario described above. However, soon after publishing that blog, Microsoft determined it did not have any evidence showing that the crash dump contained the 2016 MSA key. This led Microsoft to assess that the crash dump theory was no longer any more probable than other theories as the mechanism by which the actor had acquired the key, which Microsoft chose to leave uncorrected for more than six months after publishing its September 6 blog.

The Board is troubled that Microsoft neglected to publicly correct this known error for many months. Customers (private sector and government) relied on these public representations in Microsoft's blogs. The loss of a signing key is a serious problem, but the loss of a signing key through unknown means is far more significant because it means that the victim company does not know how its systems were infiltrated and whether the relevant vulnerabilities have been closed off. Left with the mistaken impression that Microsoft has conclusively identified the root cause of this incident, Microsoft's customers did not have essential facts needed to make their own risk assessments about the security of Microsoft cloud environments in the wake of this intrusion. Microsoft told the Board early in this review that it believed that the errors in the blog were "not material." The Board disagrees. After several written follow up questions from the Board regarding the blog, Microsoft informed the Board on March 5, 2024, that it would be updating the blog in the "near future." One week following this communication, and more than six months after its publication of the September 6 blog, Microsoft corrected its mistaken assertions through an addendum to the blog's existing webpage.

The Board also takes note of a separate incident that Microsoft disclosed in January 2024. This disclosure revealed a compromise that allowed a different nation-state actor, which Microsoft calls Midnight Blizzard and the U.S. government has previously attributed to the Russian Foreign Intelligence Service (SVR),[167] to access highly-sensitive Microsoft corporate email accounts.[168] Nearly two months later, Microsoft published a new blog post stating that Midnight Blizzard had also gained unauthorized access to some of Microsoft's source code repositories and internal systems.[169] While this second intrusion was outside of the scope of the Board's current review, the Board is troubled that this new incident occurred months after the Exchange Online compromise covered in this review. This additional intrusion highlights the Board's concern that Microsoft has not yet implemented the necessary governance or prioritization of security to address the apparent security weaknesses and control failures within its environment and to prevent similar incidents in the future.

Individually, any one of the failings described above might be understandable. Taken together, they point to a failure of Microsoft's organizational controls and governance, and of its corporate culture around security.

Microsoft's products and services are ubiquitous. It is one of the most important technology companies in the world, if not the most important. This position brings with it utmost and global responsibilities. It requires a security-focused corporate culture of accountability, which starts with the CEO, to ensure that financial or other go-to-market factors do not undermine cybersecurity and the protection of Microsoft's customers.

Unfortunately, throughout this review, the Board identified a series of operational and strategic decisions that collectively point to a corporate culture in Microsoft that deprioritized both enterprise security investments and rigorous risk management. These decisions resulted in significant costs and harm for Microsoft customers around the world. The Board is convinced that Microsoft should address its security culture.

In 2002, Microsoft's founder and then-CEO, Bill Gates, wrote an email to the entire Microsoft workforce on the importance of prioritizing security in product development. He wrote:

> So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve. A good example of this is the changes we made in Outlook to avoid e-mail-borne viruses. If we discover a risk that a feature could compromise someone's

[167] CISA, "*SVR Cyber Actors Adapt Tactics for Initial Cloud Access*," February 26, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

[168] MSRC; Microsoft, "*Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*," January 19, 2024, https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

[169] MSRC; Microsoft, "*Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*," March 8, 2024, https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

> privacy, that problem gets solved first. If there is any way we can better protect important data and minimize downtime, we should focus on this. These principles should apply at every stage of the development cycle of every kind of software we create, from operating systems and desktop applications to global Web services.[170]

The Board concludes that Microsoft has drifted away from this ethos and needs to restore it immediately as a top corporate priority. The Board is aware of Microsoft's recent changes to its security leadership and the "Secure Future Initiative" that it announced in November 2023.[171] The Board believes that these and other security-related efforts should be overseen directly and closely by Microsoft's CEO and its Board of Directors, and that all senior leaders should be held accountable for implementing all necessary changes with utmost urgency. The Board recommends the following:

- **RECOMMENDATION 1:** Microsoft's customers would benefit from its CEO and Board of Directors directly focusing on the company's security culture. The CEO and Board should develop, and share publicly, a plan with specific timelines to make fundamental, security-focused reforms across the company and its full suite of products, and then hold leaders at all levels of the company accountable for its implementation. Given the company's critical importance to its more than one billion customers and the national security of this nation and, indeed, the entire world, progress in this area should be rapid and substantial.
- **RECOMMENDATION 2:** Microsoft leadership should consider directing internal Microsoft teams to deprioritize feature developments across the company's cloud infrastructure and product suite until substantial security improvements have been made. In all instances, security risks should be fully and appropriately assessed and addressed before new features are deployed.
- **RECOMMENDATION 3:** As noted in the National Cybersecurity Strategy, "The most capable and best-positioned actors in cyberspace must be better stewards of the digital ecosystem. Today, end users bear too great a burden for mitigating cyber risks."[172] Microsoft and all CSPs should heed this call and take accountability for the security outcomes of their customers, ensuring that senior leaders make security a business priority, creating internal incentives and fostering an across-the-board culture to make security a design requirement.
- **RECOMMENDATION 4:** The Board notes that some CSPs, including Microsoft until recently, offer granular logging, which can be invaluable in security incident detection, investigation, and response—as a part of a paid package offering to their core services. This course of business should stop. Security-related logging should be a core element of cloud offerings and CSPs should provide customers the foundational tools that provide them with the information necessary to detect, prevent, or quantify an intrusion, recognizing that many customers will still require additional or third-party analytic capabilities to build a fully mature security program.

### 2.1.2 CSP CYBERSECURITY PRACTICES

During this review, the Board identified best practices drawn from all CSPs that would materially improve the security of cloud systems. These include automated regular key rotation; storage of keys in segmented and isolated key systems (e.g., hardware security modules [HSMs] or similar); use of stateful token validation; limiting scope of keys (e.g., to individual customers in some cases); use of proprietary data in token generation algorithms that could allow for detection of adversary-forged tokens that may not include such data; and the use of tokens bound to particular operations or sessions rather than broad bearer tokens.

As a result of threat actors targeting authentication and identity systems in the 2009 Operation Aurora intrusions,[173,][174] the Board found that other CSPs recognized the importance of addressing this threat model by implementing different approaches to secure their identity systems. This is unsurprising and appropriate, as each CSP is different and

[170] Wired, "*Bill Gates: Trustworthy Computing*," January 17, 2002, https://www.wired.com/2002/01/bill-gates-trustworthy-computing/
[171] Smith, Brad; Microsoft, "*A new world of security: Microsoft's Secure Future Initiative*," November 2, 2023, https://blogs.microsoft.com/on-the-issues/2023/11/02/secure-future-initiative-sfi-cybersecurity-cyberattacks/
[172] The White House, "*National Cybersecurity Strategy*," March 1, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[173] Anonymized.
[174] Google, Board Meeting.

should choose a security architecture best suited to its technological infrastructure and customer use cases, such as those demonstrated in the following examples.

- Google re-worked its identity system to rely as much as possible on stateful tokens, in which every credential is assigned a unique identifier at issuance and recorded in a database as irreversible proof that the credential Google receives is one that it had issued. Google also implemented fully automatic key rotation where possible and tightened the validation period for stateless tokens, reducing the window of time for threat actors to locate and obtain active keys. Google also undertook a comprehensive overhaul of its infrastructure security including implementing Zero Trust networks and hardware-backed, Fast IDentity Online (FIDO)-compliant two-factor authentication (2FA) to protect these identity systems.[175]
- Similarly, the Amazon Web Services (AWS) IAM Signature Version 4 (SigV4) protocol provides each customer with unique authentication keys for each of their users or roles, but these keys are not bearer tokens nor are they used directly for signing. Having no tokens, these credentials are not susceptible to token replay. Instead, highly compartmentalized signing keys are cryptography-derived, and each request is signed in a way that can only authorize the same specific action, which can be safely retried.[176]
- Oracle Cloud Infrastructure also enables and requires each customer tenancy to have its own public-private key pair that signs each request sent on an encrypted Transport Layer Security (TLS) connection, in a token spoofing-resistant manner.[177]

CSPs should implement security architectures with a level of security commensurate with their critical role in the ecosystem by making decisions through sound engineering practices that are based on an informed threat model. This is especially true for core digital identity systems. CSPs should also collect forensics in their production and corporate environments so that they can determine the true cause of any intrusion (which was not the case with the stolen 2016 MSA key).

The Board therefore recommends that CSPs adopt the following security practices, or their equivalents, as needed to achieve the high level of security they require.

- **RECOMMENDATION 5:** Given Microsoft's inability to determine how and when the adversary was able to steal its signing key, all CSPs should review and revise as appropriate their logging and overall forensics capabilities around their identity systems and other systems that enable environment-level compromise, such as root key material. CSPs should maintain sufficient forensics to detect exfiltration of those data, including logging all access to those systems and any private keys stored within them. These logs should be analyzed continuously for any unauthorized insider or external threat actor activity. Retention should include all time the key was in active use and extend at least two years beyond the expiration of that key. Longer retention periods of at least 10 years may be appropriate for some high-value log types.
- **RECOMMENDATION 6:** CSPs should engineer their digital identity and credential systems in such a way that substantially reduces the risk of complete system-level compromise. This should be an overriding, top-priority, design goal in the engineering process and be informed by a rigorous threat model developed by the CSP in response to its understanding of the threat landscape. The Board spoke with all major U.S.-based CSPs to gain an understanding of their existing practices and develop a set of recommended baseline best practices. While the specific practices implemented may vary for different use cases and situations, the Board believes technical mechanisms exist today across the industry that can, if broadly implemented, significantly reduce the likelihood of complete system-level compromise. Each of these practices is implemented by at least one major CSP, demonstrating their technical feasibility. Some of these practices, while compatible with accepted industry standards, would also benefit from additional standards development, which is discussed in another recommendation. These mechanisms include the following.[178]

[175] Google, Board Meeting.
[176] AWS, Board Meeting.
[177] Oracle, Board Meeting.
[178] Each of these mechanisms would have, if in place at the time of the incident, aided in the prevention, impact reduction, or detection of the reviewed incident. For some mechanisms, as outlined in the Facts section and in the Recommendations, partial implementation aided in the response to this incident. Broad implementation across CSPs would enhance the resilience of critical digital identity systems.

  - **Stateful tokens**: Microsoft's authentication system accepted a token that it had not issued. By storing records in a database when tokens are issued and validating against that database at access time, CSPs may enforce that only tokens issued by the CSP can access customer data. Note: this approach is not possible for use with third-party services reliant on an IDP maintained by a cloud provider.
  - **Automated frequent key rotation**: Microsoft paused manual key rotations for its MSA system in 2021 but did not remove the 2016 MSA key. By rotating encryption keys frequently (e.g., monthly) and in an automated manner with monitoring of rotation systems, CSPs can ensure that the blast radius of a compromised key is limited in duration.
  - **Per customer keys (key scope)**: Microsoft had a single key that signed tokens for all consumer, and due to the validation flaw, enterprise customers. Tying encryption keys to customer tenancy would limit the scope of key compromise.
  - **Bound tokens**: Microsoft's identity system used bearer tokens that did not require any proof of possession, thus making the tokens more vulnerable to replay attacks. By digitally binding tokens to specific requests or network sessions, token theft and token replay attacks can be eliminated. While this incident demonstrates the risks of key compromise, some victims and responders spent significant time investigating bearer token replay attacks to which not all CSPs are vulnerable.
  - **Common authentication libraries**: Microsoft used a variety of different client libraries to verify tokens across different systems. This diversity complicated implementing uniform, and correct, validation behavior, as well as made the remediation efforts much more complex and time sensitive. By ensuring that all CSP services use the same authentication libraries, CSPs can more effectively enforce consistent token validation behavior and authorization policy.
  - **Secure key storage**: While Microsoft separated the organization and production environments, this incident illustrated that Microsoft insufficiently protected MSA system key material. By storing key material in isolated systems and leveraging, where feasible, technologies such as dedicated HSMs, the risk of key compromise can be reduced. The Board recognizes that in some situations and levels of scale, traditional HSM technology may not be viable but believes that the core idea of isolated key storage with minimal key release is appropriate.
  - **Linkable tokens**: The relationship between the tokens used in this incident was not exposed in logs made available to customers, making them difficult to track. By linking all tokens derived from a single root authentication event together and exposing this linking to their customers in logs, CSPs and customers can better track and discover identity-related attacks and respond, including in an automated way.
  - **Proprietary data use in token generation algorithm:** Some CSPs inject proprietary data into their generated authentication tokens, which they can use to differentiate between tokens that their own systems generated and those generated by malicious third parties. While one cannot rely on the fact that the adversary would not detect and reproduce such behavior, it can nevertheless prove potentially helpful as a "canary in the coal mine" alert that the CSP is observing tokens that had not been generated by its own code.

- **RECOMMENDATION 7:** CISA should validate annually with major CSPs that provide services to the U.S. government which of these and other applicable security practices they are implementing. CISA should publish the results of its validation review (including stating that a company refused to provide requested information if that is the case).

- **RECOMMENDATION 8:** The National Institute of Standards and Technology (NIST) and the Risk Management Framework (RMF) Joint Task Force (JTF) should update Special Publication (SP) 800-53's control catalog to better account for risks to cloud-based digital identity systems, including incorporating the technical recommendations of the Board from this incident, as appropriate.

- **RECOMMENDATION 9:** Large enterprises need robust compromise assessment and remediation processes for entities they acquire or with whom they merge. These processes should recognize that smaller, acquiree companies may have less robust security procedures and that adversaries may view them as an entry point onto a parent company's corporate network. This can include targeting them after announcement of an acquisition but before closing.

### 2.1.3 AUDIT LOGGING NORMS

Logging is essential to detection, investigation, and remediation of potential intrusions. In this case, the logs State Department used to detect this incident (MailItemsAccessed) are of critical value and have enabled detection of other nation-state compromises involving Exchange Online. Despite this obvious utility, these logs, and similar logs at other CSPs, are not available for all types of critical business data stored by CSPs. The Board recommends the following.

- **RECOMMENDATION 10:** CSPs, as part of a CISA-led task force, should define and adopt a minimum standard for default audit logging in cloud services. This standard should, at a minimum, ensure that all access (including access by the CSP itself) to customer business data in the cloud produces logs that are available to the customer without additional charges, with a minimum default retention of six months by the CSP.

### 2.1.4 DIGITAL IDENTITY STANDARDS AND GUIDANCE

The Board finds that the current ecosystem of Digital Identity standards does not provide the security necessary to counter modern threat actors, and that some CSPs have not sufficiently prioritized implementing emerging standards that improve the security of digital identity systems. This is both a current problem (the need to implement emerging standards) and a long-term need (upleveling the security bar of digital identity standards). The Board recommends the following.

- **RECOMMENDATION 11:** CSPs should implement emerging standards such as Open Authorization (OAuth) 2 Demonstrating Proof-of-Possession (DPoP) (bound tokens) and OpenID Shared Signals and Events (SSE) (sharing session risk) that better secure cloud services against credential related attacks.
- **RECOMMENDATION 12:** Relevant standards bodies should refine and update these standards to account for a threat model of advanced nation-state attackers targeting core CSP identity systems.
- **RECOMMENDATION 13:** CSPs and relevant standards bodies, such as OpenID Foundation (OIDF), Organization for the Advancement of Structured Information Standards (OASIS), and The Internet Engineering Task Force (IETF), should develop or update profiles for core digital identity standards such as OIDC and Security Assertion Markup Language (SAML) to include requirements and/or security considerations around key rotation, stateful credentials, credential linking, and key scope.

### 2.1.5 CSP TRANSPARENCY

Customers rely on CSPs for more than their cloud services—they rely on CSPs to be transparent about security incidents and vulnerabilities, as these disclosures will influence decisions the customers make about their own risk tolerance and investment decisions, along with necessary transparency to their own customers, clients, and regulators. Moreover, these customers reasonably expect that CSPs will update them, in a timely manner, about security incidents as investigations evolve, including correcting any information that later proves to be wrong. Finally, the U.S. government relies on CSPs to share information about incidents with a potential national security nexus, including suspected nation-state intrusions. During its review, the Board finds that Microsoft fell short, as, for many months, it chose to not update the September 6 blog that incorrectly implied that the 2016 MSA key had been stolen from a crash dump and that it had identified and corrected the issues that led to the adversary stealing the key.

The Board recommends that all CSPs adopt transparency and disclosure practices commensurate with their customers' needs and expectations, including the following.

- **RECOMMENDATION 14:** U.S.-based CSPs should report all incidents suspected to have been perpetrated by an actor affiliated with a nation-state targeting their infrastructure and corporate systems to the U.S. government, even in the absence of a regulatory obligation to report. Separately, CISA and the Office of Management and Budget (OMB) should consider appropriate contractual provisions with CSPs to require such reporting. [179]

[179] CISA, "*Cyber Incident Reporting for Critical Infrastructure Act of 2022*," March 9, 2022, https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-o-f2022_508.pdf

- **RECOMMENDATION 15:** CSPs should be transparent to U.S. government agencies, customers, and other stakeholders on what they know as well as what they do not know when initially investigating a cyber incident.
- **RECOMMENDATION 16:** CSPs should promptly correct significant factual inaccuracies as they discover them in their public or customer statements.
- **RECOMMENDATION 17:** CSPs should commit to disclosing through the CVE process all vulnerabilities, including flaws such as the one in Microsoft's token validation logic and those that do not require customer action to patch. CSPs should work with the CVE program to develop necessary updates to Common Weakness Enumeration (CWE) to account for the particulars of cloud environments. CSPs should collaborate with the CVE Program to develop these norms and commit to timely and comprehensive disclosure of these vulnerabilities, enabling organizations to make thoughtful risk decisions about all their vendors' security programs, including cloud services. The Board believes that incorporating all known vulnerabilities across the entire technology stack in CVE's comprehensive repository would be a public benefit for industry and government customers, as well as security researchers.

### 2.1.6 VICTIM NOTIFICATION PROCESSES

Victim notification in cyber incidents is never simple and can be even more complicated when attackers compromise cloud-based services. In this intrusion, the Board found that some victims ignored or did not see the notifications, and some who saw them believed them to be spam or phishing. In some cases, Storm-0558 compromised the personal accounts of some government employees, but Microsoft was initially unable to share the employee's names with their employer due to legal restrictions and recommended the U.S. government issue a warrant for the information so it could provide those details. This impacted and delayed the agencies' ability to aid their employees in responding to that aspect of the intrusion.

The Board recommends that CSPs and the U.S. government improve processes for notifying individuals of intrusions, including ensuring receipt of such notifications, to include the following.

- **RECOMMENDATION 18:** CSPs and the U.S. government, in conjunction with major mobile device platform vendors, should develop a targeted, quickly recognizable "amber alert" style victim notification mechanism for high-impact situations. The alert should be more readily distinguishable from notification emails, which are frequently mistaken by victims for phishing, building on some existing mechanisms for NSNs within platform providers' ecosystems where the mobile device operating system can send a native system alert about the compromise of an end user's CSP account, such as a push notification.
- **RECOMMENDATION 19:** CSPs should develop a process to identify and categorize high-impact incidents involving compromised accounts that present higher risks to national security, such as those of government officials. CSPs should verify whether the victim is in receipt of the notifications; provide guidance to the victim on how they can further protect their information; and detail next steps based on the severity or type of incident, particularly when the victim is targeted by a nation-state actor.
- **RECOMMENDATION 20:** CSPs and the U.S. government should develop mechanisms to incentivize and enable CSPs to connect victims with the appropriate U.S. government resources, international partners, and different sets of victims. These mechanisms should enable collaborative investigation and sharing of best practices to break down silos and barriers that create independent and duplicative investigative workstreams, even within U.S. government and allied partner agencies.

## 2.2 U.S. GOVERNMENT

### 2.2.1 SECURITY STANDARDS AND COMPLIANCE FRAMEWORKS

A large, vibrant, and diverse ecosystem of secure cloud services is important for the economic competitiveness of the U.S. and the execution of the U.S. government's varied missions.

Cloud services are a critical component of the cybersecurity ecosystem, especially when they protect the most sensitive government data. However, the Board finds that existing compliance requirements for government cybersecurity do not consistently require sound practices around key management or token issuance. To address this, the Federal Risk

Authorization Management Program (FedRAMP) can play a key role in ensuring stronger cybersecurity practices, including in cloud-based digital identity, across the cloud service ecosystem.

| FedRAMP |
|---|
| FedRAMP was established by OMB in December 2011 to promote the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies.<br>The General Services Administration (GSA) operates the FedRAMP Program Management Office (PMO) and is governed by the FedRAMP Board. FedRAMP leverages many controls that are published in NIST SP 800-53 “Security and Privacy Controls for Information Systems and Organizations.” |

The Board concludes that a more flexible tailoring of security controls for cloud-based digital identity systems provides a path to balance the importance of securing these systems with the other important goal of supporting such an ecosystem. To that end, the Board recommends updating both the FedRAMP program itself as well as the supporting frameworks that implement the Federal Information Security Modernization Act (FISMA) such as the NIST RMF. Specifically, the Board recommends the following.

- **RECOMMENDATION 21:** FedRAMP, in coordination with OMB and CISA, should establish a minimum threshold for periodically re-evaluating legacy FedRAMP authorization packages. For example, some FedRAMP authorized packages are for services that have become especially widely used across the government while others may be considered High Value Assets (HVA) that may merit more regular review. FedRAMP should consult with CISA and NIST to identify additional relevant security requirements for critical components (such as digital identity access) of these higher-risk FedRAMP authorized providers, and how to effectively tailor security baselines to focus cloud provider effort on addressing these requirements. This threshold should drive the priority in which FedRAMP PMO re-reviews FedRAMP authorized security packages for continuous data monitoring.

- **RECOMMENDATION 22:** FedRAMP should work with OMB to establish a Technical Advisory Group (TAG). The TAG should be available to FedRAMP for consultation for technical, strategic, and operational direction. The TAG should regularly provide recommendations on security best practices and ways to iteratively improve FedRAMP continuous monitoring requirements and guidance.

- **RECOMMENDATION 23:** FedRAMP should establish a process for conducting discretionary special reviews of FedRAMP authorized Cloud Service Offerings (CSOs) that convene security experts within the federal government to make recommendations for security improvements for the CSO. Recommendations from these reviews should inform the issuance (or continuation) of a FedRAMP authorization. FedRAMP should establish criteria for these reviews that limit their scope to especially high-impact situations.

- **RECOMMENDATION 24:** FedRAMP should strengthen the minimum audit logging standards (e.g., FedRAMP Assignment of AU-2) to align with the goal of logging access to sensitive business data (including by the CSP itself). FedRAMP should further require that these logs be made available to customers (not just the CSP itself) at no additional cost.

- **RECOMMENDATION 25:** NIST is encouraged to continue releasing point updates to add and remove controls from its security and privacy control baselines to maintain focus on contemporary threats, and to consult with the FedRAMP program to incorporate feedback about observed threats and incidents related to cloud provider security.

## APPENDIX A: REVIEW PARTICIPANTS – EXTERNAL PARTIES

The Board's review involved organizations and individuals representing a variety of viewpoints, including targeted organizations, law enforcement, CSPs, cloud security, incident response, regulators, cybersecurity and industry experts, and others. The Board requested information in the form of briefings and written materials.

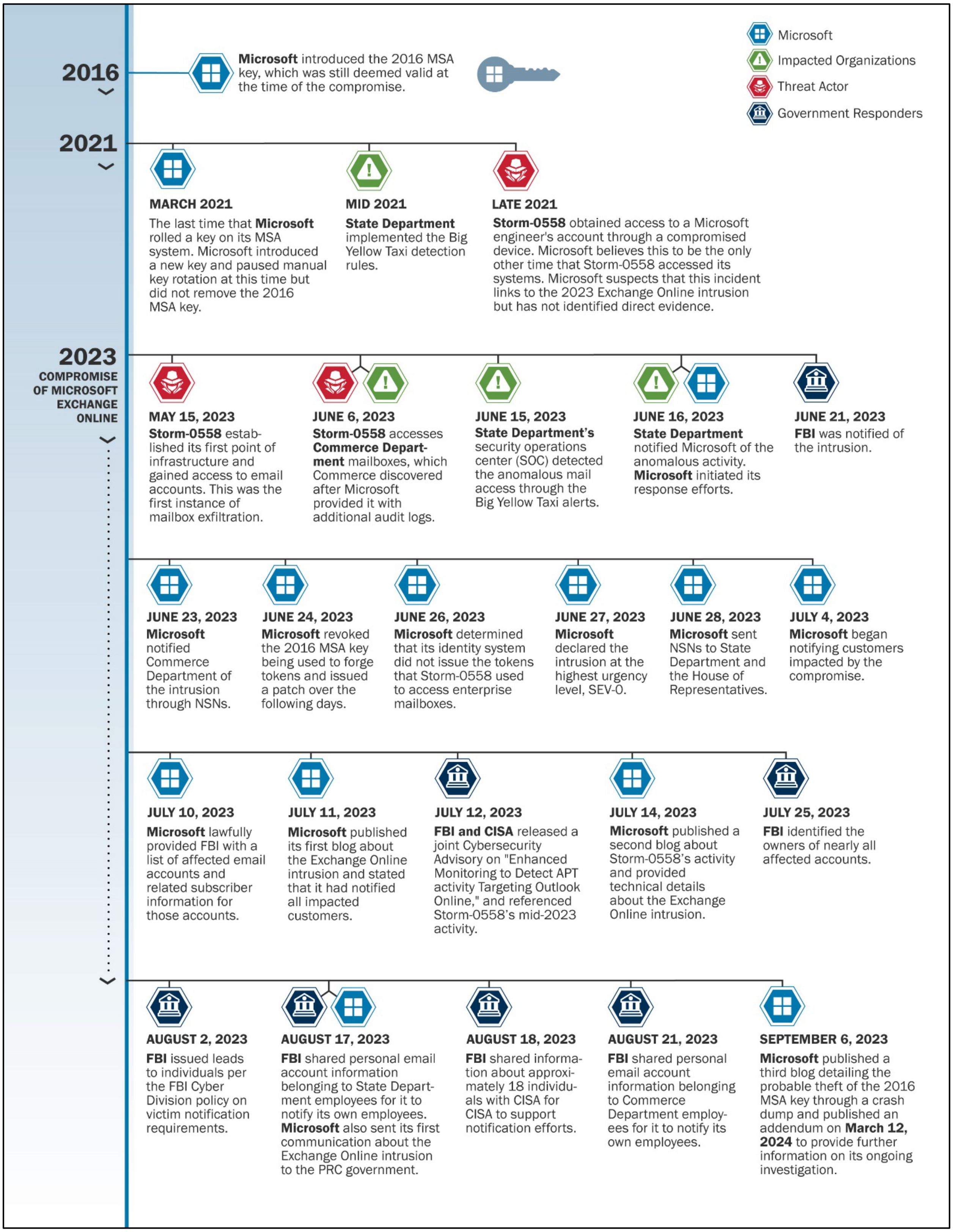
The Board is grateful for the voluntary participation of those parties that provided timely responses. Their efforts helped the Board collect the observable timeline of events, corroborate facts, and understand the complex and nuanced dimensions of the Microsoft Exchange Online intrusion and related cloud identity topics.

### RELATED BRIEFINGS

The Board engaged with 20 organizations with expertise in cloud security, cloud identity, and/or the Microsoft Exchange Online intrusion. Those organizations are identified below.

- Amazon Web Services, Inc.
- Broadcom Inc.
- Canadian Centre for Cyber Security
- CrowdStrike Holdings, Inc.
- Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Bureau of Investigation (FBI)
- Federal Risk and Authorization Management Program (FedRAMP)
- Google LLC
- International Business Machines Corporation (IBM)
- Lacework, Inc.
- Mandiant, Inc.
- Microsoft Corporation
- National Security Agency (NSA)
- Office of the Director of National Intelligence (ODNI)
- Office of Representative Don Bacon
- Oracle Corporation
- U.K. National Cyber Security Centre (NCSC)
- U.S. Department of Commerce
- U.S. Department of State
- Wiz Inc.

# APPENDIX B: MICROSOFT EXCHANGE ONLINE INTRUSION TIMELINE



Microsoft

Impacted Organizations

Threat Actor

Government Responders

**2016**

**Microsoft** introduced the 2016 MSA key, which was still deemed valid at the time of the compromise.

**2021**

**MARCH 2021**
The last time that **Microsoft** rolled a key on its MSA system. Microsoft introduced a new key and paused manual key rotation at this time but did not remove the 2016 MSA key.

**MID 2021**
**State Department** implemented the Big Yellow Taxi detection rules.

**LATE 2021**
**Storm-0558** obtained access to a Microsoft engineer's account through a compromised device. Microsoft believes this to be the only other time that Storm-0558 accessed its systems. Microsoft suspects that this incident links to the 2023 Exchange Online intrusion but has not identified direct evidence.

**2023**
**COMPROMISE OF MICROSOFT EXCHANGE ONLINE**

**MAY 15, 2023**
**Storm-0558** established its first point of infrastructure and gained access to email accounts. This was the first instance of mailbox exfiltration.

**JUNE 6, 2023**
**Storm-0558** accesses **Commerce Department** mailboxes, which Commerce discovered after Microsoft provided it with additional audit logs.

**JUNE 15, 2023**
**State Department's** security operations center (SOC) detected the anomalous mail access through the Big Yellow Taxi alerts.

**JUNE 16, 2023**
**State Department** notified Microsoft of the anomalous activity. **Microsoft** initiated its response efforts.

**JUNE 21, 2023**
**FBI** was notified of the intrusion.

**JUNE 23, 2023**
**Microsoft** notified Commerce Department of the intrusion through NSNs.

**JUNE 24, 2023**
**Microsoft** revoked the 2016 MSA key being used to forge tokens and issued a patch over the following days.

**JUNE 26, 2023**
**Microsoft** determined that its identity system did not issue the tokens that Storm-0558 used to access enterprise mailboxes.

**JUNE 27, 2023**
**Microsoft** declared the intrusion at the highest urgency level, SEV-0.

**JUNE 28, 2023**
**Microsoft** sent NSNs to State Department and the House of Representatives.

**JULY 4, 2023**
**Microsoft** began notifying customers impacted by the compromise.

**JULY 10, 2023**
**Microsoft** lawfully provided FBI with a list of affected email accounts and related subscriber information for those accounts.

**JULY 11, 2023**
**Microsoft** published its first blog about the Exchange Online intrusion and stated that it had notified all impacted customers.

**JULY 12, 2023**
**FBI and CISA** released a joint Cybersecurity Advisory on "Enhanced Monitoring to Detect APT activity Targeting Outlook Online," and referenced Storm-0558's mid-2023 activity.

**JULY 14, 2023**
**Microsoft** published a second blog about Storm-0558's activity and provided technical details about the Exchange Online intrusion.

**JULY 25, 2023**
**FBI** identified the owners of nearly all affected accounts.

**AUGUST 2, 2023**
**FBI** issued leads to individuals per the FBI Cyber Division policy on victim notification requirements.

**AUGUST 17, 2023**
**FBI** shared personal email account information belonging to State Department employees for it to notify its own employees. **Microsoft** also sent its first communication about the Exchange Online intrusion to the PRC government.

**AUGUST 18, 2023**
**FBI** shared information about approximately 18 individuals with CISA for CISA to support notification efforts.

**AUGUST 21, 2023**
**FBI** shared personal email account information belonging to Commerce Department employees for it to notify its own employees.

**SEPTEMBER 6, 2023**
**Microsoft** published a third blog detailing the probable theft of the 2016 MSA key through a crash dump and published an addendum on **March 12, 2024** to provide further information on its ongoing investigation.

*Figure 3: Microsoft Exchange Online Intrusion Timeline*

## APPENDIX C: REVIEW PARTICIPANTS – CSRB MEMBERS

The Cyber Safety Review Board members listed below participated in the review of the Summer 2023 Microsoft Exchange Online intrusion in the following roles and capacity.

Federal members serve in their official capacity and act on behalf of their agency or department. Private sector members have been appointed as Special Government Employees (SGEs) for the purposes of serving on the Cyber Safety Review Board. SGEs serve in their individual capacity, though current affiliations are included in the list below.

**Robert Silvers**, (*Chair*), Under Secretary for Policy, representing the Department of Homeland Security

**Dmitri Alperovitch**, (*Deputy Chair*), Co-Founder and Chairman, Silverado Policy Accelerator

**Jake Braun**, Acting Principal Deputy National Cyber Director, representing the Office of the National Cyber Director

**Jerry Davis**, Senior Vice President, Cyber Operations and Technology, Truist Bank

**Chris DeRusha**, Federal Chief Information Security Officer, representing the Office of Management and Budget

**Eric Goldstein**, Executive Assistant Director for Cybersecurity, representing the Cybersecurity and Infrastructure Security Agency

**Rob Joyce**, Director of Cybersecurity, representing the National Security Agency

**Cynthia Kaiser**, Deputy Assistant Director, representing the Federal Bureau of Investigation

**Marshall Miller**, Principal Associate Deputy Attorney General, representing the Department of Justice

**Chris Novak**, Co-Founder and Managing Director, Verizon Threat Research Advisory Center

**Tony Sager**, Senior Vice President and Chief Evangelist, Center for Internet Security

**John Sherman**, Chief Information Officer, representing the Department of Defense

## APPENDIX D: ACRONYMS

| | |
|---|---|
| 2FA | two-factor authentication |
| AD | Active Directory |
| APAC | Asia-Pacific |
| API | application programming interface |
| AWS | Amazon Web Services |
| CEO | Chief Executive Officer |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CSO | Cloud Service Offering |
| CSP | cloud service provider |
| CSRB | Cyber Safety Review Board, or the Board |
| CVE | common vulnerability and exposure |
| CWE | Common Weakness Enumeration |
| DART | Detection and Response Team |
| DoJ | Department of Justice |
| DPoP | Demonstrating Proof-of-Possession |
| ESOC | Enterprise Security Operations Center |
| FBI | Federal Bureau of Investigation |
| FedRAMP | Federal Risk Authorization Management Program |
| FIDO | Fast IDentity Online |
| FISMA | Federal Information Security Modernization Act |
| GSA | General Services Administration |
| HSM | hardware security module |
| HVA | High Value Asset |
| IAM | identity and access management |
| IDP | identity provider |
| IETF | The Internet Engineering Task Force |
| IoA | indicator of attack |
| IoC | indicator of compromise |
| IP | Internet Protocol |
| JTF | Joint Task Force |

| | |
|---|---|
| M&A | mergers and acquisitions |
| MSA | Microsoft Services Account |
| MSTIC | Microsoft Threat Intelligence Center |
| NCSC | National Cyber Security Centre |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NSN | nation-state notification |
| OASIS | Organization for the Advancement of Structured Information Standards |
| OCIO | Office of the Chief Information Officer |
| OIDC | OpenID Connect |
| OIDF | OpenID Foundation |
| OMB | Office of Management and Budget |
| OWA | Outlook Web Access |
| PMO | Project Management Office |
| PRC | People's Republic of China |
| RMF | Risk Management Framework |
| SAML | Security Assertion Markup Language |
| SDK | software development kit |
| Sigv4 | Signature Version 4 |
| SMS | short message service |
| SOC | security operations center |
| SSIRP | Software and Services Incident Response Plan |
| SVR | Russian Foreign Intelligence Service |
| TAG | Technical Advisory Group |
| TLS | Transport Layer Security |
| TTPs | tactics, techniques, and procedures |
| U.K. | United Kingdom |
| U.S. | United States |
| VPS | virtual private server |