Incident Report

mimecast.com/incident-report/

Published: March 16, 2021

Executive Summary

In January, we became aware of a security incident later determined to be conducted by the same sophisticated threat actor responsible for the SolarWinds supply chain attack. During our investigation, we learned that the threat actor used the SolarWinds supply-chain compromise to gain access to part of our production grid environment. Using this entry point, the threat actor accessed certain Mimecast-issued certificates and related customer server connection information. The threat actor also accessed a subset of email addresses and other contact information, as well as encrypted and/or hashed and salted credentials. In addition, the threat actor accessed and downloaded a limited number of our source code repositories, but we found no evidence of any modifications to our source code nor do we believe there was any impact on our products. **We have no evidence that the threat actor accessed email or archive content held by us on behalf of our customers**.

When we became aware of the security incident, we immediately launched an internal investigation. Our investigation was supported by leading third-party forensics and cyber incident response experts at Mandiant, a division of FireEye, and in coordination with law enforcement to aid their investigation into this threat actor. As the investigation progressed, we issued a series of advisories to affected customers, including recommended precautionary steps to mitigate risk.

We have now completed our forensic investigation with Mandiant and have eliminated the threat actor’s access to our environment. We have already taken a number of actions to prevent future access to our environment as described below and we will continue to monitor for threats and take precautionary steps as needed.

Incident Details and Remediation Actions

The following provides a more detailed summary of our investigation, as well as an overview of the steps taken to address this attack and further enhance our environment.

Phase 1

In January, Microsoft notified us that a certificate we provide to customers to authenticate Mimecast Sync and Recover, Continuity Monitor, and IEP products to Microsoft 365 Exchange Web Services had been compromised by a threat actor they were actively investigating. Microsoft informed us that the threat actor used the certificate to connect to a low single-digit number of our mutual customers’ M365 tenants from non-Mimecast IP address ranges.

While the evidence showed that this certificate was used to target only the small number of customers, we quickly formulated a plan to mitigate potential risk for all customers who used the certificate. We made a new certificate connection available and advised these customers and relevant supporting partners, via email, in-app notifications, and outbound calls, to take the precautionary step of switching to the new connection. Our public blog post provided visibility surrounding this stage of the incident.

We coordinated with Microsoft to confirm that there was no further unauthorized use of the compromised Mimecast certificate and worked with our customers and partners to migrate to the new certificate connection. Once a majority of our customers had implemented the new certificate connection, Microsoft disabled the compromised certificate at our request.

Phase 2

Supported by Mandiant, we confirmed that the incident was related to the SolarWinds Orion software compromise and was perpetrated by the same sophisticated threat actor. Our investigation determined that the initial intrusion resulted from SUNBURST malware, the backdoor present in the compromised version of SolarWinds Orion software we had previously used in our environment.

Our investigation revealed suspicious activity within a segment of our production grid environment containing a small number of Windows servers. The lateral movement from the initial access point to these servers is consistent with the mechanism described by Microsoft and other organizations that have documented the attack pattern of this threat actor. We determined that the threat actor leveraged our Windows environment to query, and potentially extract, certain encrypted service account credentials created by customers hosted in the United States and the United Kingdom. These credentials establish connections from Mimecast tenants to on-premise and cloud services, which include LDAP, Azure Active Directory, Exchange Web Services, POP3 journaling, and SMTP-authenticated delivery routes. **We have no evidence that the threat actor accessed email or archive content held by us on behalf of our customers.**

Although we were not aware that any of the encrypted credentials were decrypted or misused, we issued a specific advisory to customers hosted in the United States and United Kingdom to take precautionary steps to reset their credentials. At this time, we published an additional public blog post.

Phase 3

As the investigation progressed, we determined that the threat actor had established additional access methods to the same segment of our production grid environment. We removed and blocked the threat actor’s means of access. All compromised systems were Windows-based and peripheral to the core of our production customer infrastructure. We completely replaced all compromised servers to eliminate the threat.

At this point, we were able to determine the specific scope of data access and confirm exfiltration by the threat actor. **We have no evidence that the threat actor accessed email or archive content held by us on behalf of our customers.** The threat actor did access a subset of email addresses and other contact information and hashed and salted credentials. Some of this information required us to notify the affected customers and partners under certain regulations, which we have done. We are resetting the affected hashed and salted credentials as a precautionary step.

The investigation revealed that the threat actor accessed and downloaded a limited number of our source code repositories, as the threat actor is reported to have done with other victims of the SolarWinds Orion supply chain attack. We believe that the source code downloaded by the threat actor was incomplete and would be insufficient to build and run any aspect of the Mimecast service. We found no evidence that the threat actor made any modifications to our source code nor do we believe that there was any impact on our products. We will continue to analyze and monitor our source code to protect against potential misuse.

In March, we completed our forensic investigation with Mandiant.

Customer Impact

- We have no evidence that email or archive content was accessed by the threat actor.
- Beyond the low single-digit number of customers targeted by the threat actor, which we contacted as described in our first blog post, we are not aware that any other customers were actively targeted.
- As described in our second blog post, we recommended that customers hosted in the United States and United Kingdom reset as a precautionary measure any server connection credentials in use on the Mimecast platform.
- We are resetting the affected hashed and salted credentials as a precautionary step.
- We do not believe that the threat actor made any modifications to our source code.
- Forensic analysis of all customer-deployed Mimecast software has confirmed that the build process of the Mimecast-distributed executables was not tampered with.
- The threat actor accessed some information that required us to notify the affected customers and partners under certain regulations, which we have done.

Additional Mimecast Remediation Steps

- We have completed the following actions:
    - Rotated all impacted certificates and encryption keys.
    - Upgraded encryption algorithm strength for all stored credentials.
    - Implemented enhanced monitoring of all stored certificates and encryption keys.
    - Deployed additional host security monitoring functionality across all of our infrastructure.
    - Decommissioned SolarWinds Orion and replaced it with an alternative NetFlow monitoring system.
    - Rotated all Mimecast employee, system, and administrative credentials, and expanded hardware-based two-factor authentication for employee access to production systems.
    - Completely replaced all compromised servers.
    - Inspected and verified our build and automation systems to confirm that Mimecast-distributed executables were not tampered with.
    - Implemented additional static and security analysis across the source code tree.
- We are in the process of implementing a new OAuth-based authentication and connection mechanism between Mimecast and Microsoft technologies, which will provide enhanced security to Mimecast Server Connections. We will work with customers to migrate them to this new architecture as soon as it is available.

Forward-Looking Statements

This communication contains “forward-looking” statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995 and other federal securities laws, that are based on currently available information and our current beliefs, expectations and understanding. These forward-looking statements include statements regarding Mimecast’s current understanding of the identity and likely targets of the sophisticated threat actor, the scope and impact of the attack, the potential decryption and/or misuse of the encrypted credentials, the number and location of impacted customers, the level of impact on our source code and the build process of the Mimecast-distributed executables, the active targeting of any of our customers, our ability to limit access and eliminate the threat, the effectiveness of any current or future isolation and remediation efforts, the effectiveness of monitoring and prevention efforts on any future access going forward, the likelihood that other companies will be affected by the threat actor, and the information provided to us by third parties during the course of our ongoing investigation. Mimecast intends that all such forward-looking statements be covered by the safe harbor provisions for forward-looking statements contained in Section 21E of the Securities Exchange Act of 1934, as amended, and the Private Securities Litigation Reform Act of 1995. These statements are subject to future events, risks and uncertainties – many of which are beyond our control or are currently unknown to Mimecast. These risks and uncertainties include, but are not limited to, risks and uncertainties related to the uncovering of new information in the course of our investigation related to the nature, cause and scope of the issue, the reputational, financial, legal and other risks related to potential adverse impacts to our customers and partners, and the other risks, uncertainties and factors detailed in Mimecast’s filings with the Securities and Exchange Commission. Mimecast is providing the information in this communication as of this date and assumes no obligations to update the information included in this communication or revise any forward-looking statements, whether as a result of new information, future events or otherwise.