Important Security Update

mimecast.com/blog/important-security-update/

At Mimecast, we prioritize the security of our customers, and our commitment to being transparent with them, above all else. These two principles have guided our rapid response to the recent security incident, as well as this update and the customer and partner guidance we are providing today via directed actions in the Administration Console and the Mimecast Community.

As we previously shared, when Microsoft informed us about the compromise of a Mimecast-issued certificate used to authenticate a subset of Mimecast's products, we advised affected customers to break and re-establish their connections with newly issued keys. The vast majority of these customers have taken this action, and Microsoft has now disabled use of the former connection keys for all affected Mimecast customers.

We also launched an internal investigation, supported by leading third-party forensics experts, and we are coordinating our activities with law enforcement. Our investigation has now confirmed that this incident is related to the SolarWinds Orion software compromise and was perpetrated by the same sophisticated threat actor.

Our investigation also showed that the threat actor accessed, and potentially exfiltrated, 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.

Although we are not aware that any of the encrypted credentials have been decrypted or misused, we are advising customers hosted in the United States and United Kingdom to take precautionary steps to reset their credentials.

We have taken actions to isolate and remediate the identified threat, which we believe to be effective. We continue to examine and closely monitor our environment. We will continue to communicate updates directly to our customers if warranted, and, where appropriate, these will be disclosed here on the Mimecast Blog. While we are committed to transparency and sharing insights with our customers, there may be limits to the details we can provide at this time while elements of the investigation into this threat actor remain ongoing.

Recent threat intelligence reports have described the campaign of attacks waged by this threat actor. It is clear that this incident is part of a highly sophisticated large-scale attack and is focused on specific types of information and organizations.

Now more than ever, transparency and cooperation within the security community are essential to an effective response. We expect that additional organizations will learn or share that they were affected by the threat actor behind the SolarWinds Orion software compromise. We have benefited from the expertise shared by others facing this threat, and we are committed to doing the same, based on our own experience, to create a more secure and resilient community.

Protecting our customers will always be our company's top priority.

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 effectiveness of any current or future isolation and remediation efforts, 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 to 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.

Up Next

Email Security | Feb 02, 2021

Detecting and Preventing a TA551 Email Spam Strike