Mimecast links security breach to SolarWinds hackers

bleepingcomputer.com/news/security/mimecast-links-security-breach-to-solarwinds-hackers/

Sergiu Gatlan

By
Sergiu Gatlan

- January 26, 2021
- 10:01 AM
- 0

Email security company Mimecast has confirmed today that the threat actor behind the SolarWinds supply-chain attack is behind the security breach it disclosed earlier this month.

"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," Mimecast said.

"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."

The company added that there is no evidence that any of the encrypted credentials accessed during the breach were decrypted or misused.

However, United States and United Kingdom Mimecast customers are advised to reset credentials to prevent potential attacks from abusing them.

The threat actor that coordinated the SolarWinds supply-chain attacks is tracked as StellarParticle (CrowdStrike), UNC2452 (FireEye), SolarStorm (Palo Alto Unit 42), and Dark Halo (Volexity).

While its identity remains unknown, a joint statement issued by the FBI, CISA, ODNI, and the NSA says that it is likely a Russian-backed Advanced Persistent Threat (APT) group.

Kaspersky also made a connection between the Russian Turla hacking group and the SolarWinds hackers after finding feature overlaps between the Sunburst backdoor and the Kazuar backdoor linked to Turla in the past.

Attack discovered following a Microsoft notification

The company was alerted by Microsoft that some of its self-issued certificates customers use to authenticate to a subset of Mimecast's products were compromised.

While the exact number of affected customers using the stolen certificates to secure the connection to the Microsoft 365 cloud was not disclosed, Mimecast said that roughly 10 percent of their customers "use this connection."

Mimecast's products are currently used by more than 36,000 customers, with 10% of them amounting to roughly 3,600 impacted customers.

The company found evidence that "a low single-digit number of our customers' M365 tenants were targeted" by the SolarWinds hackers.

Mimecast reached out to these customers to remediate and address this issue and, according to today's update, "[t]he 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."

One week ago, cybersecurity firm Malwarebytes also confirmed that the SolarWinds hackers were able to gain access to some internal company emails.

Related Articles:

T-Mobile confirms Lapsus$ hackers breached internal systems

GitHub: Attackers stole login details of 100K npm user accounts

GitHub: How stolen OAuth tokens helped breach dozens of orgs

Okta: Lapsus$ breach lasted only 25 minutes, hit 2 customers

GitHub notifies owners of private repos stolen using OAuth tokens

- Breach
- Hack
- Security Breach
- SolarWinds

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: