UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00093

MIMECAST CERTIFICATE HACKED

DATE ISSUED: 18th January 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A sophisticated threat actor has managed to compromise Mimecast-issued security certificate that is used to verify and authenticate connections to Mimecast's Sync and Recover servers, Continuity Monitor and Internet Email Protect. This could enable them to access Microsoft 365 Exchange Web Servers without alerting authorities.

BREAKDOWN

This particular compromise could mean that an attacker could seize control of the connection whereby inbound and outbound mail passes across the network as well as potentially intercept, eavesdrop, or seize and exfiltrate critical information and communications. The stolen Mimecast has not had a specific associated use case identified at this stage. The suspected attacks would require an attacker to have access to a compromised device between any Mimecast's customer users and servers and be on the same local network in order to execute the man-in-the-middle style attack. Should the attacker manage to compromise the system, there is the possibility that Microsoft 365 security measures, such as threat protection and alerting, may be disabled by the attacker. Mimecast has issued a statement to say that there is the potential for this threat to affect 10% of their customer base and that their investigation remains ongoing. Any additional information as it comes to light will be shared publicly via their blog listed in the references below. Those customers known to have been affected have been notified by Mimecast and assisted with remediation efforts.

REMEDIATION STEPS

- Deploy defense-in-depth security strategy and measures to provide layers of protection.
- Use network monitoring to detect and isolate any abnormal or malicious behaviours on the network.
- Contact your Mimecast account manager should you have any concerns about your network.

REFERENCES & RESOURCES

Mimecast https://www.mimecast.com/blog/important-update-from-mimecast/
Threatpost https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/