FINISHED INTELLIGENCE REPORTS

HC3 Sector Alert: Phishing Campaigns Leveraging Legitimate Email Marketing Platforms

TLP:WHITE

Apr 08, 2022

On April 7, 2022, the Health Sector Cybersecurity Coordination Center (HC3) distributed a report regarding a breach affecting a legitimate email marketing platform to send phishing emails. According to the report, this campaign targets users in the cryptocurrency and financial sectors, however, threat actors can pivot and use the unauthorized access to target users in the Healthcare and Public Health (HPH) sector.

Out of an abundance of caution, Health-ISAC is sharing this report as organizations should be aware of this threat and adhere to the provided mitigations.

On April 4, 2022, the email marketing platform company, Mailchimp, confirmed a breach impacting one of the company's internal tools used by its customer support and account administration teams. Although Mailchimp deactivated the compromised employee accounts after learning of the breach, the threat actors were able to

view around 300 Mailchimp user accounts and obtain audience data from 102 of them, according to the company's CISO. The threat actors were also able to access API keys for an undisclosed number of customers which would allow them to create custom email campaigns such as phishing campaigns and send them to mailing lists without accessing the MailChimp customer portal.

While HC3 is currently only aware of a phishing campaign abusing this unauthorized access to send a fake data breach notification emails to users in the cryptocurrency and finance sectors (which was reportedly executed with exceptional sophistication and planning), the Healthcare and Public Health (HPH) sector should remain cautious of suspicious emails originating from legitimate email marketing platforms such as MailChimp. It is important to note that APT groups have previously leveraged legitimate mass-mailing services in malicious email campaigns to target a wide variety of organizations and industry verticals.

Reference(s)	HHS.gov
Report Source(s)	HC3

Recommendations
User awareness training (M1017) remains one of the most important defenses against phishing attacks, which is a form of social engineering, especially in this campaign where emails originated from a legitimate sender. Additional mitigations include implementing Antivirus (M1049) and network intrusion prevention systems (M1031) as well as restricting web-based content (M1021) that may not be necessary for business operations. Anti-spoofing and email authentication mechanisms (M1054) can also be implemented to filter messages based on validity checks of the sender domain (using SPF) and the integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross-domain) to perform similar message filtering and validation.

Release Date
Apr 08, 2022

Sources

Phishing Campaigns Leveraging Legitimate Email Marketing Platforms

Alert ID 259e5b26

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags Mailchimp, HC3, Phishing

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**