HC3: Sector Alert

April 7, 2022 TLP: WHITE Report: 202204071500

Phishing Campaigns Leveraging Legitimate Email Marketing Platforms

Executive Summary

HC3 is aware of a breach affecting a legitimate email marketing platform to send phishing emails. While this campaign targeted users in the cryptocurrency and financial sectors, it is possible the unauthorized access may be leveraged to target users in the Healthcare and Public Health (HPH) sector. These organizations should be aware of this threat and take the corresponding mitigations.

Report

PSA: Watch out for phishing emails from genuine mailing lists, following Mailchimp hack (April 5, 2022)
https://9to5mac.com/2022/04/05/mailchimp-hack-phishing-alert/

Analysis

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.

Patches, Mitigations, and Workarounds

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 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. Additional HC3 resources related to the malicious use of email marketing services and phishing campaigns can be found below:

- HC3. "Malicious Use of Email Marketing Services," February 11, 2021.
  https://www.hhs.gov/sites/default/files/threat-posed-by-bulk-email-services.pdf
- HC3. "Phishing Campaigns Demonstrate Importance of User Training and Awareness," September 2, 2021.
  https://www.hhs.gov/sites/default/files/phishing-analyst-note-tlpwhite.pdf

HC3: Sector Alert

April 7, 2022 TLP: WHITE Report: 202204071500

References

CISA. "Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks," August 25, 2020. https://www.cisa.gov/uscert/ncas/tips/ST04-014

Mitre. "Techniques, Enterprise, Phishing, ID: T1566," October 18, 2021. https://attack.mitre.org/techniques/T1566/

Abrams, Lawrenece. "Hackers breach MailChimp's internal tools to target crypto customers," April 4, 2022. https://www.bleepingcomputer.com/news/security/hackers-breach-mailchimps-internal-tools-to-target-crypto-customers/

Microsoft, "New sophisticated email-based attack from NOBELIUM," May 27, 2021. https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback