LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Malicious Use of Email Marketing Services

02/11/2021

TLP: WHITE, ID# ***202102111030***

Agenda

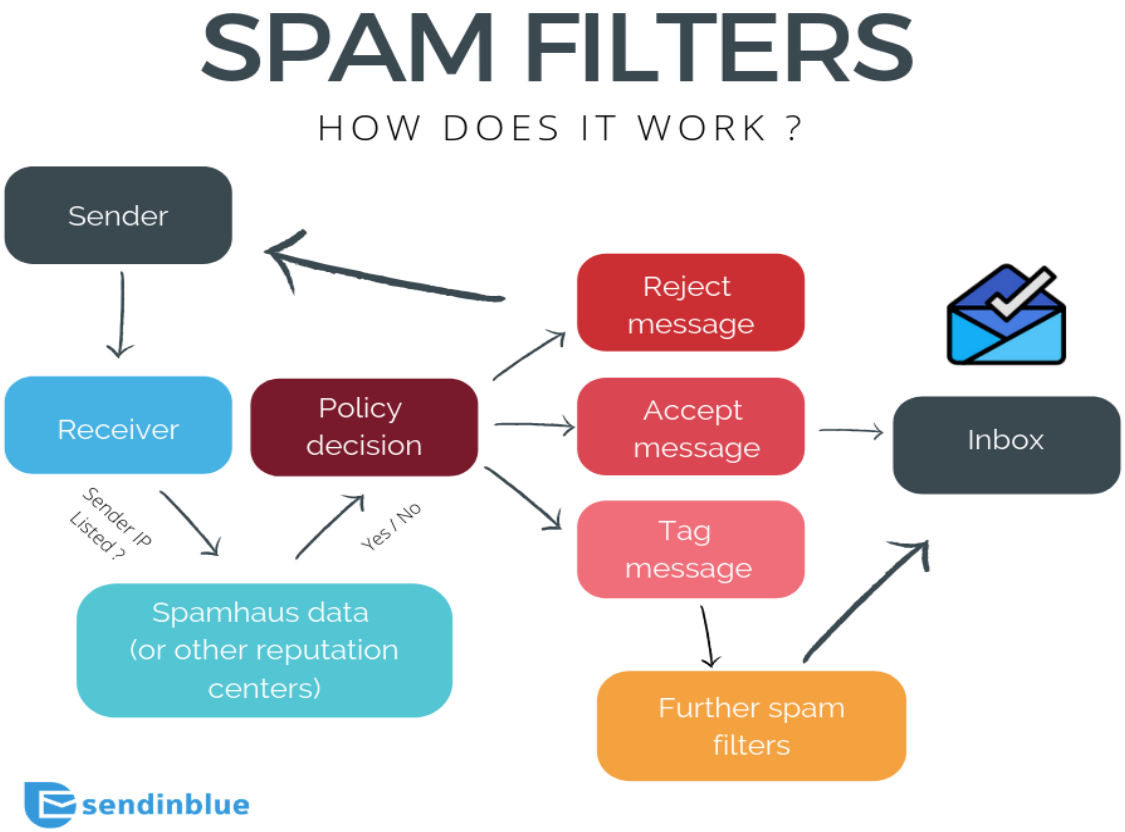
- What are Email Marketing Services?
- Who are Common Email Marketing Service Providers?
- Overview of Threat Actors' Use of Email Marketing Service Providers
- Recent Credential Harvesting Campaign
- Dark Web Activity
- Mitigations & Best Practices

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

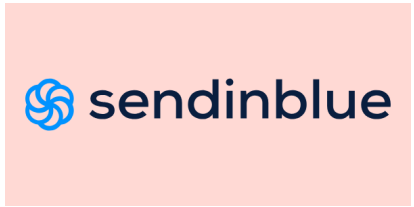
Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

"Email marketing is a highly effective way to nurture and convert leads. However, it's not a game of chance, as to whether your message winds up in spam filters. Instead, email marketing is an automated process that targets specific prospects and customers with the goal of influencing their purchasing decisions. **Email marketing success is measured by open rates and click-through rates**." - Vicki Woschnick of the Weidert Group



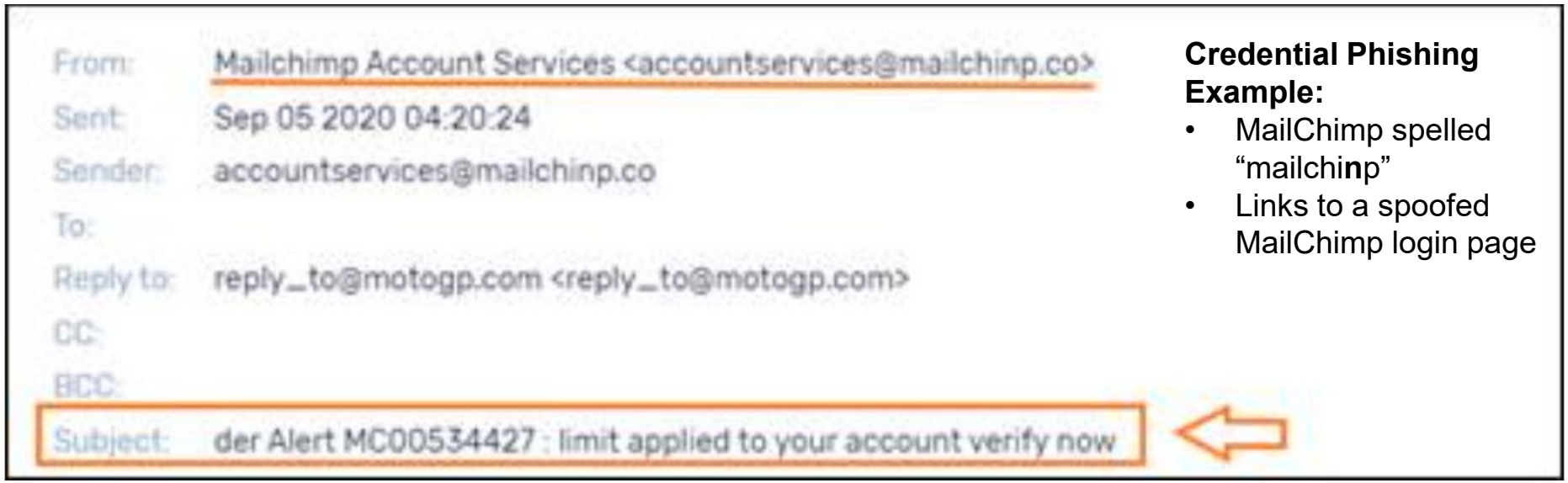
Who are Common Email Marketing Service Providers?

- ActiveCampaign
- Aweber
- Campaign Monitor
- Campayn
- GetResponse
- Klaviyo
- MailChimp
- MailerLite
- Sender
- SendGrid
- Sendinblue
- SendPulse



Compromised Email Marketing Customer Accounts

- Spoofing login pages
- Purchase credentials
- Cracked passwords



Credential Phishing Example:

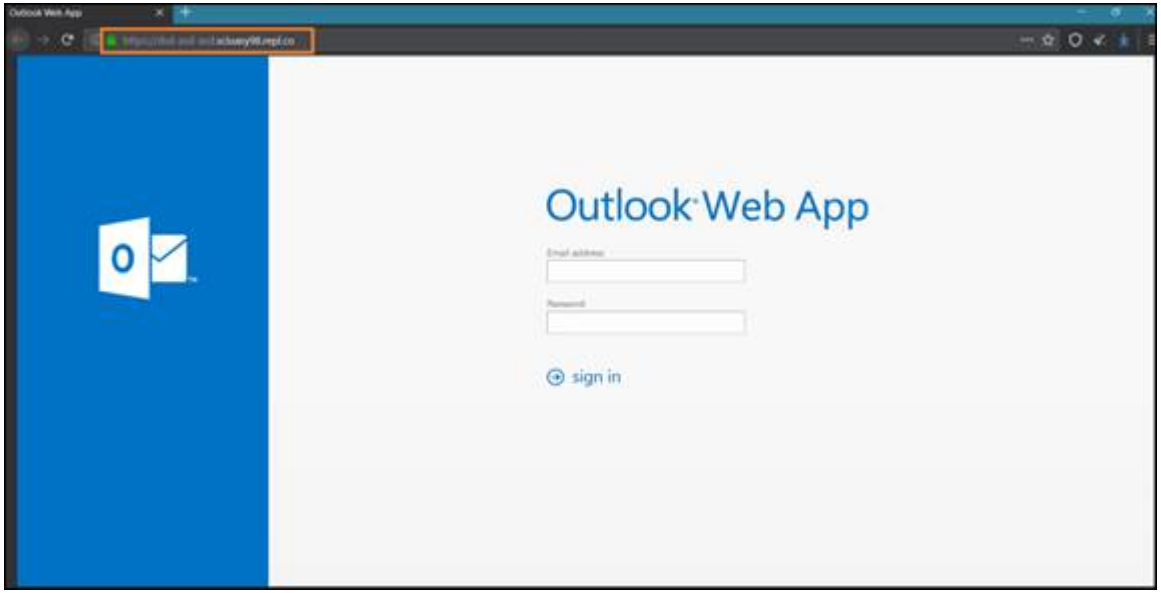
- MailChimp spelled "mailchi**n**p"
- Links to a spoofed MailChimp login page

How the Malicious Emails Get Through Filters

- Trusted domains and obfuscated links

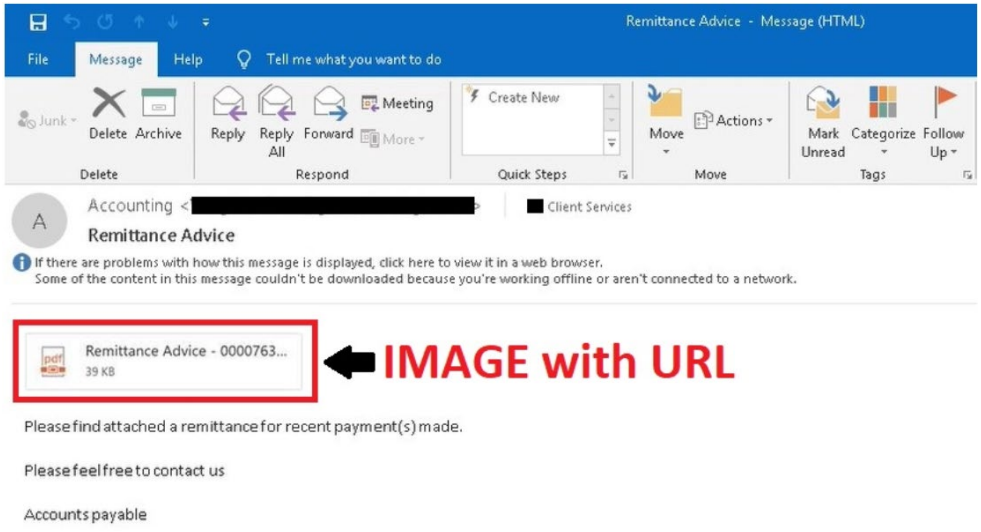
Trusted Domain Example: URL in the email body: 'hxxps://u14869500.ct.[trusted email service provider's domain][.]net/ls/click?upn='

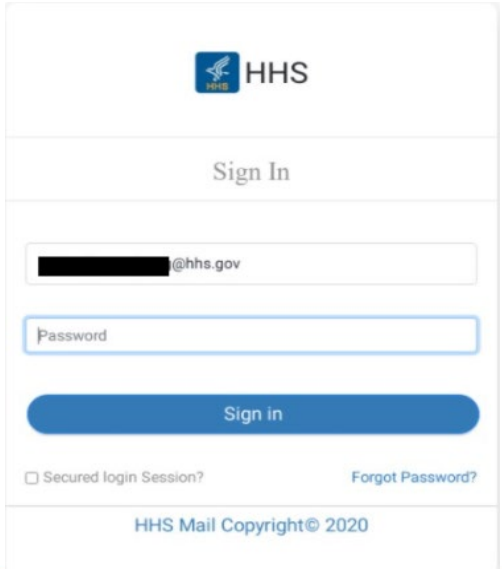
The query opens a fake Outlook Web App login page: 'hxxps://dsd-asd-asd.sciuasy98.repl[.]co/'



Recent Credential Harvesting Campaign

- Between October 2020 and at least January 2021, researchers at Cyjax identified a global phishing campaign.
- The campaign targeted commercial and government entities in various sectors, including healthcare, defense, banking, chemical, energy, and transportation.
- A reputable email marketing company was used to send the phishing emails.
- The email contains an image with an embedded URL, disguised as a file attachment.
- If the attachment is clicked on, potential victims are directed to an email login page pre-loaded with the victim's email address.
- The login pages are themed with the intended victim's organization name or logo.





Cost of Email Marketing Service Provider Accounts

Number of emails per month (Price to purchase USD)

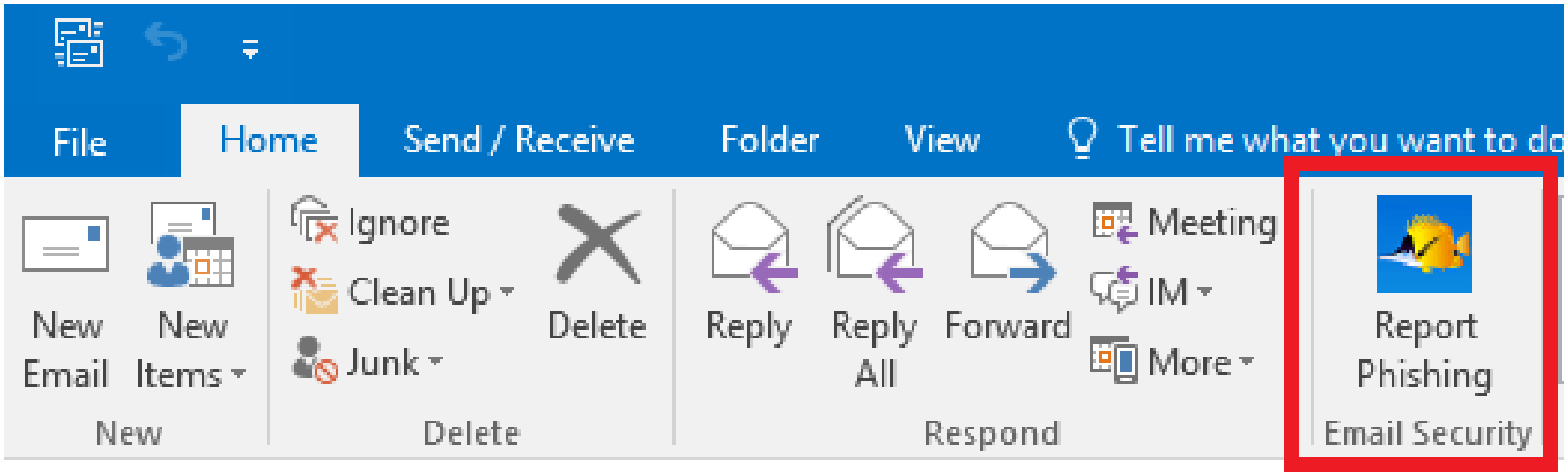
August 2020	November 2020	Email Provider
40k ($15)	40k ($80)	SendGrid
10 million ($400)	2.5 million ($300)	SendGrid
	50k ($60)	sendinblue
	SMS Sending ($200)	sendinblue

Prevent Email Marketing Account Takeovers

- Identify if email marketing is used at your organization
- Identify the account holders
- Monitor email addresses associated with email marketing accounts
- Use Multi-Factor Authentication (MFA) if available
- Have a password reset policy and password managers
- Use strong passwords

Prevent Receiving Malicious Marketing Emails

- Implementation of reporting mechanism for malicious emails
- Create a block list to target compromised accounts that repeatedly send malicious/junk email
- Never open links from unknown or untrustworthy sources → Extra Phishing Training
- Decide as an organization if it is necessary to have marketing emails; if so, can they be filtered better?



Reference Materials

References

- Woschnick,Vicki. "Top 10 Most Effective Marketing Strategies." Weidert Group. June 25, 2020. https://www.weidert.com/blog/top-10-most-effective-marketing-strategies.
- Finser,Ewen. "11 Best SendGrid Alternatives [2021]: SendGrid Competitors." TheDigital merchant. January 27, 2021. https://thedigitalmerchant.com/crm/email-marketing/10-best-sendgrid-alternatives/.
- Aleksandrova, Daria. "How Scammers Leverage Email Delivery Services like SendGrid and MailChimp in Phishing Attacks." CYREN. September 20, 2020. https://www.cyren.com/blog/articles/how-scammers-leverage-email-delivery-services-like-sendgrid-and-mailchimp-in-phishing-attacks.
- Krebs, Brian. "Sendgrid Under Siege from Hacked Accounts." Krebs on Security. August 28, 2020. https://krebsonsecurity.com/2020/08/sendgrid-under-siege-from-hacked-accounts/.
- Chavez, Art. "Phishing: How to Protect Against Email Attacks Sent from Compromised SendGrid Accounts." AGARI. September 28, 2020. https://www.agari.com/email-security-blog/phishing-bec-sendgrid-accounts/.
- Thomas, William. “Credential harvesting campaign targets government, military, and private sector organisations.” Cyjax. January 13, 2021. https://www.cyjax.com/2021/01/13/credential-harvesting-campaign-targets-government-military-and-private-sector-organisations/.

Questions

Upcoming Briefs

- A Retrospective Look at Healthcare Cybersecurity in 2020 (2/18)
- Securing SSL/TLS in Healthcare (2/25)

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV