HC3: Sector Alert

August 10, 2022 TLP: White Report: 202208101700

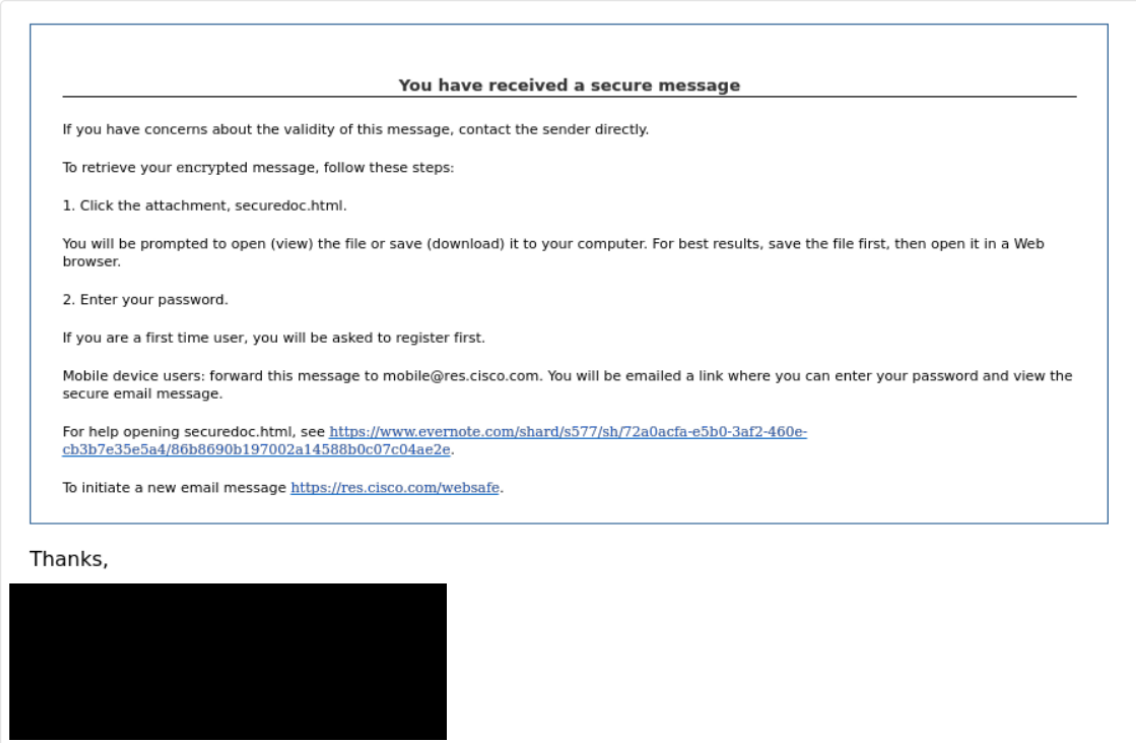
Secure Message/Evernote Themed Phishing Campaign

Executive Summary

HC3 has been made aware of a malspam campaign that is currently targeting various healthcare providers. The campaign has a subject of "(Victim Organization) (Date) Business Review" and utlizes a Secure Message theme. Inside of the email is a malicious link which lures the recipient to a *Victim Organization* themed Evernote site. On the site is an HTML download which has been identified as a malicious phishing Trojan. The file contains JavaScript which renders an Adobe and Microsoft themed page that attempts to harvest Outlook, IONOS, AOL, or other credentials. This campaign may have leveraged business email compromises (BECs) of HPH-related and possibly non-HPH entities.

Report

The campaign has a subject of "(Victim Organization) (Date) Business Review" and utlizes a Secure Message theme.



You have received a secure message

If you have concerns about the validity of this message, contact the sender directly.

To retrieve your encrypted message, follow these steps:

1. Click the attachment, securedoc.html.

You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser.

2. Enter your password.

If you are a first time user, you will be asked to register first.

Mobile device users: forward this message to mobile@res.cisco.com. You will be emailed a link where you can enter your password and view the secure email message.

For help opening securedoc.html, see https://www.evernote.com/shard/s577/sh/72a0acfa-e5b0-3af2-460e-cb3b7e35e5a4/86b8690b197002a14588b0c07c04ae2e.

To initiate a new email message https://res.cisco.com/websafe.

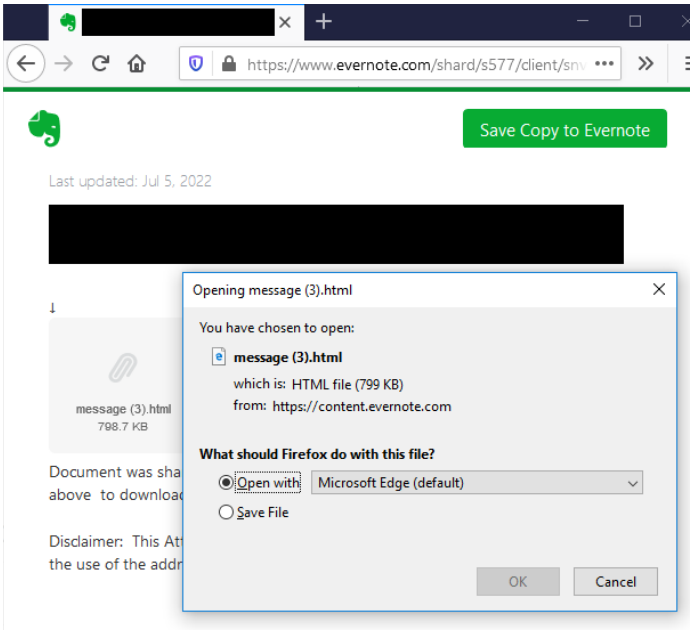
Thanks,

[redacted]

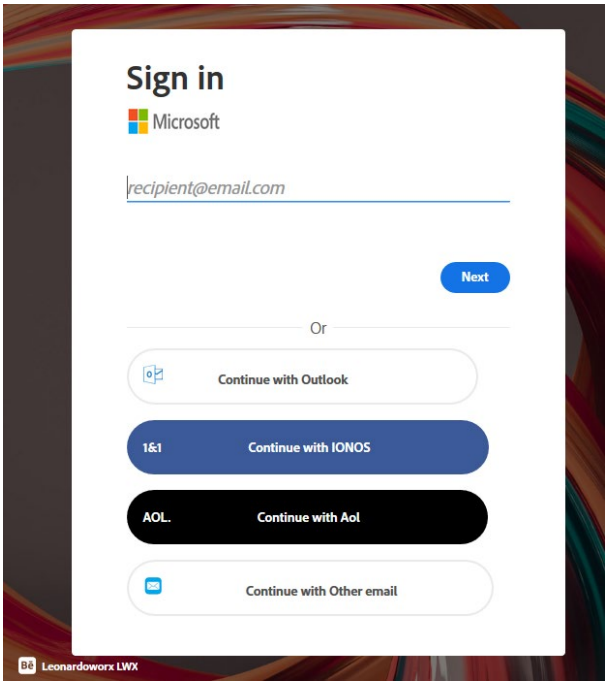
HC3: Sector Alert

August 10, 2022 TLP: White Report: 202208101700

Inside of the email is a malicious link which lures the recipient to a Victim Organization themed Evernote site.



On the site is an HTML download which has been identified as a malicious phishing Trojan. The file contains JavaScript which renders an Adobe and Microsoft themed page that attempts to harvest Outlook, IONOS, AOL, or other credentials.



HC3: Sector Alert

August 10, 2022 TLP: White Report: 202208101700

Observed IOCs:

Subject Format:

(Victim Organization) (Date) Business Review

Post Request Domains:

- hxxps://aan0[.]com/css/j28202[.]php
- hxxps://aax0[.]live/js/xml[.]php
- hxxps://en-00[.]com/js/xml[.]php

Malicious File Attachments Names:

- message (3).html
- message.html

MD5 Hashes of the Malious File Attachments:

- be563f4728de661b13be11d45a1eec69
- e0beab4bf8304f46a9e8440821f457b4

Malicious URLs:

- hxxps://www[.]evernote[.]com/shard/s577/sh/318807e5-6704-63af-90c4-d660cc278a92/3e3e26bd78e84f397366ca87e848e4b0
- hxxps://www[.]evernote[.]com/shard/s577/sh/72a0acfa-e5b0-3af2-460e-cb3b7e35e5a4/86b8690b197002a14588b0c07c04ae2e

Analysis

This malspam campaign utilizes a Trojan which is a type of malicious code or software that acts like a legitimate application or file to trick you into loading and executing it on your device. Once installed, a Trojan can perform the action it was designed for—damaging, disrupting, stealing, or inflicting harm on your data or network.

Patches, Mitigations, and Workarounds

The following actions should be taken to help protect your organization:

- Update your operating system and software applications. Cybercriminals tend to exploit security holes in outdated software programs.
- Protect each account with complex, unique passwords. Use a passphrase and/or a complex combination of letters, numbers, and symbols.
- Back up your files regularly. Should a Trojan infect your computer, this will help you restore your data.
- In general, avoid opening unsolicited emails from senders you do not know.
- Do not open a link or an attachment in an email unless you're confident it comes from a legitimate source.
- Do not download or install programs if you do not have complete trust in the publisher.
- Do not visit unsafe websites and do not click on pop-up windows that promise free programs that perform useful tasks.

HC3: Sector Alert

August 10, 2022 TLP: White Report: 202208101700

References

Johansen, Alison Grace. “What is a Trojan? Is it a virus or is it malware?,” Norton. 24 July 2020. https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html#

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback