HC3: Sector Alert

September 19, 2022 TLP: White Report: 202209191500

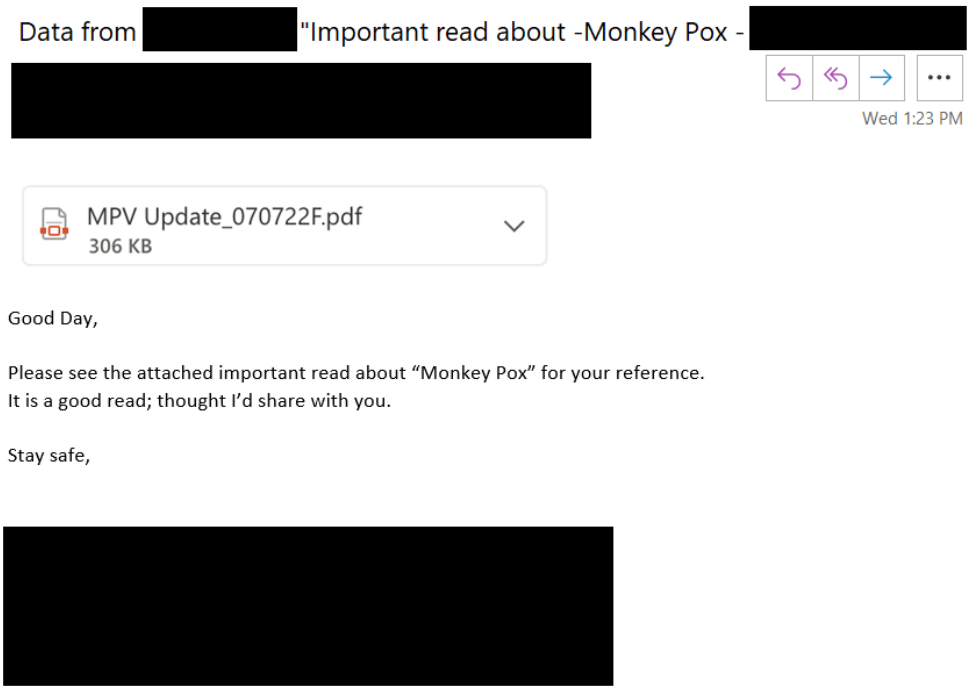
Monkey Pox-Themed Phishing Campaign

Executive Summary

HC3 has been made aware of a monkepox-themed malspam campaign that is currently targeting healthcare providers. The campaign has a subject of “Data from (Victim Organization Abbreviation): "Important read about -Monkey Pox– (Victim Organization) (Reference Number)” and utilizes an “Important read about Monkey Pox” theme. Inside of the email is a PDF with a malicious link which lures the recipient to a Lark Docs site. The site is Adobe Doc cloud-themed and offers a secure fax MonkeyPox PDF download. Clicking the download attempts to harvest Outlook, 0365, or Other Mail credentials. This campaign may have leveraged business email compromises (BECs) of HPH-related and possibly non-HPH entities.

Report

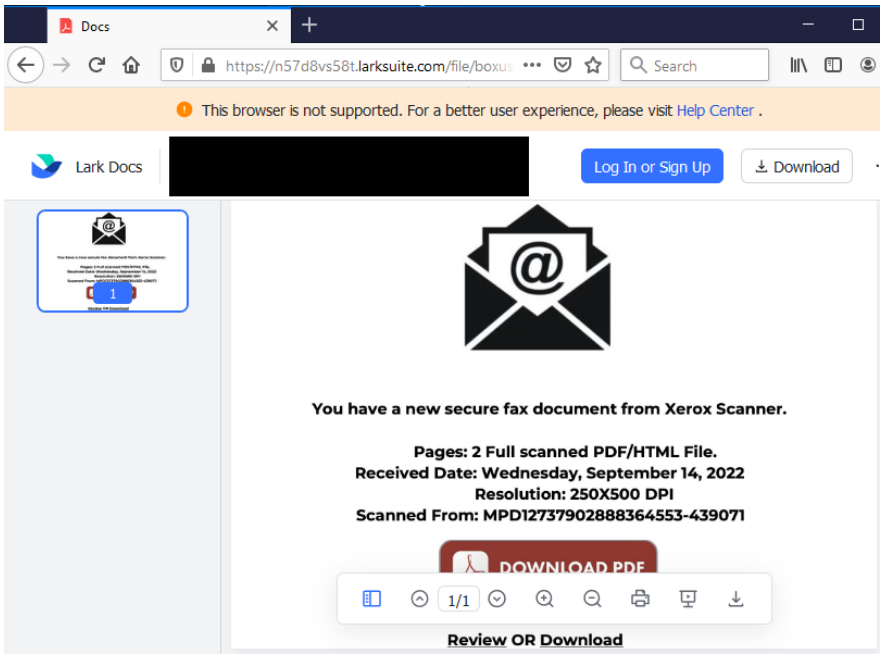
The campaign has a subject of “Data from (Victim Organization Abbreviation): "Important read about - Monkey Pox – (Victim Organization) (Reference Number) and utilizes an “Important read about Monkey Pox” theme.



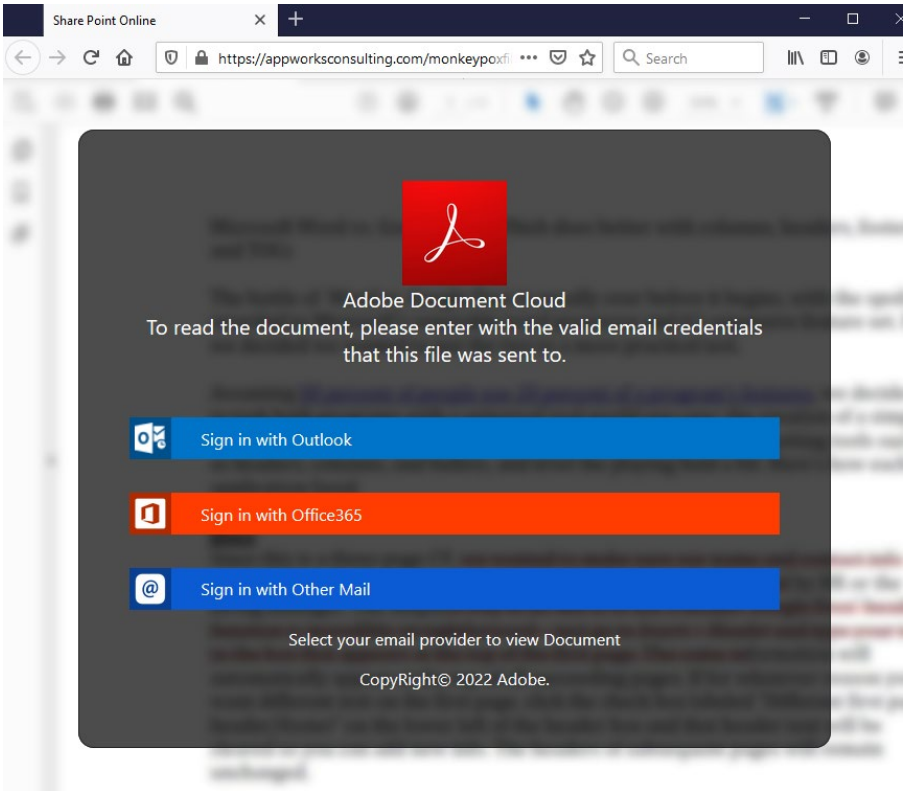
Inside of the email is a PDF with a malicious link which lures the recipient to a Lark Docs site. The site is Adobe Doc cloud themed and offers a secure fax Monkey Pox PDF download.

HC3: Sector Alert

September 19, 2022 TLP: White Report: 202209191500



Clicking the download attempts to harvest Outlook, O365, or Other Mail credentials.



HC3: Sector Alert

September 19, 2022 TLP: White Report: 202209191500

HC3 Observed IOCs:

Subject Format:

Data from (Victim Organization Abbreviation): "Important read about -Monkey Pox – (Victim Organization) (Reference Number)

Site:

hxxps://is.gd/sB5WaT

Redirects to:

hxxps://n57d8vs58t.larksuite.com/file/boxuscyFa0hnj2mpYGSSEBFhshf

Lures to:

hxxps://security.feishu.cn/link/safety?target=https%3A%2F%2Fis.gd%2FTnzqDX&scene=ccm&logParams=%7B%22location%22%3A%22ccm_drive%22%7D&lang=en-US

Redirects to:

hxxps://appworksconsulting.com/monkeypoxfile/NewFolder/

Post:

hxxps://appworksconsulting.com/monkeypoxfile/NewFolder/next.php

Malicious File Attachments Names:

MPV Update_070722F.pdf

Patches, Mitigations, and Workarounds

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

- Protect each account with complex, unique passwords. Use a passphrase and/or a complex combination of letters, numbers, and symbols.
- 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.

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