Donation Scam Lure Exploits Israel-Palestine Conflict

Lures impersonating charity organization asks for donations via Bitcoin

About the Threat

Proofpoint Threat Intelligence Services (PTIS) has identified ongoing, timely charity donation scams leveraging the Israel-Palestine conflict.

The lures impersonate international aid organizations, outlining the humanitarian implications of the conflict while asking for donations via a provided Bitcoin address.

These attacks exploit the attention the crisis is currently receiving to exploit recipient good will, solicit donations, and steal funds.

Attackers commonly exploit high-profile international crises and conflicts to carry out malicious activities, such as distributing malicious software (malware) or stealing funds.

Recommended Training

- Use our "Charity Scams" Attack Spotlight to educate users about charity-related scams and how best to avoid them.
- Use our February 2023 Threat Alert, "Phishing Campaigns Use Earthquake-Themed Lures," to inform users about a similar charity scam.
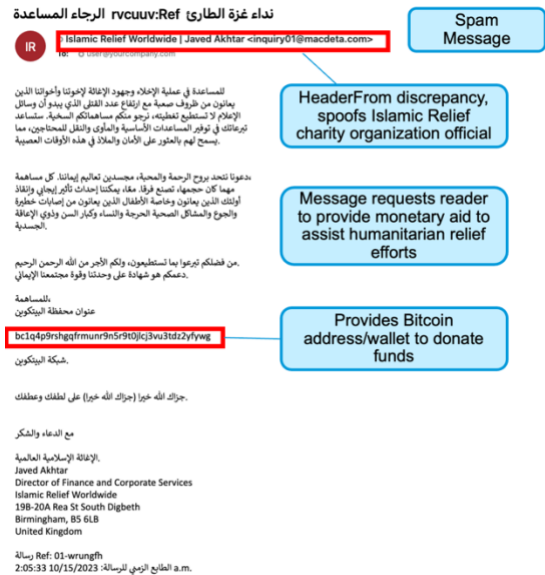
Example of a charity lure seen by Proofpoint researchers.

Email communication to users on next page

Threat Alert: Israel-Palestine Humanitarian Crisis Donation Scam (Oct 2023)

Communication to Users

[Greeting]

We are writing to alert you about a trending threat that we have become aware of. Please review the following information and reach out to [insert organizational contact] if you have any questions or concerns.

Thank you,

Threat Alert: Israel-Palestine Humanitarian Crisis Donation Scam

- Cybercriminals have launched charity donation scams attempting to take advantage of the ongoing Israel-Palestine crisis.
- These scams imitate international aid organizations, outline the humanitarian implications of the crisis, and then ask for donations in Bitcoin.

Key Actions (at Work and at Home)

- **Remember that cybercriminals commonly leverage current events in phishing attacks.** High-profile events like the Israel-Palestine conflict spark a lot of interest and conversation. Attackers know people will be tempted to engage with emails that mention these kinds of topics.
- **Always vet organizations prior to donating.** It can be tempting to immediately donate to a charity following a high-profile crisis. Be cautious of any requests for donation following a crisis, and instead directly navigate to a trusted charity instead of following emailed links. Additionally, be cautious of any requests for cryptocurrency-based donations, as these are often fraudulent.
- **Report ANY suspicious emails** using the "Report Phish" button **<update section to include your organization's reporting process>**. Remember: Our organization occasionally sends phishing simulations.

Accidentally clicked? Contact <update section to include your organization's contact>. Phishing emails can be tricky. If you think you've interacted with a malicious message, contact our IT security team right away. We're here to help.