Eventbrite-Themed Event Management Lures Distribute Malware

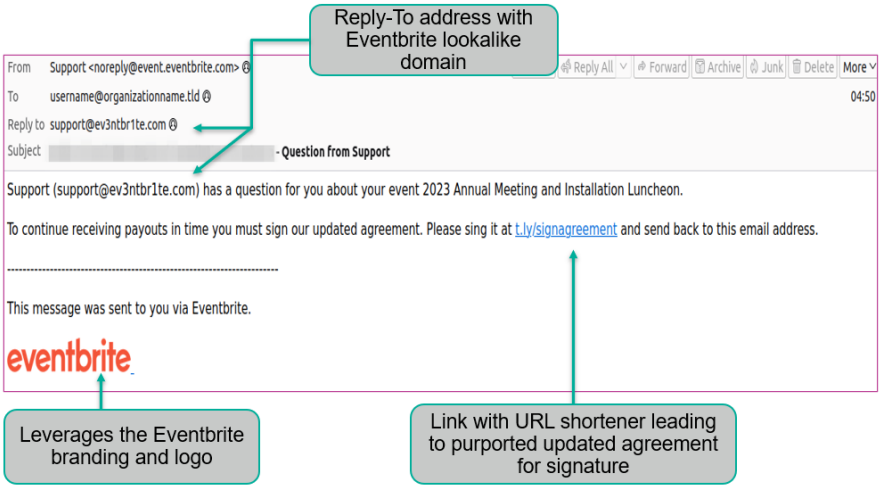
Lures include a link leading to purported updated agreement requiring a signature

About the Threat

Proofpoint Threat Intelligence Services (PTIS) has identified a phishing campaign focused on malware delivery.

Messages abuse the Eventbrite brand, which is an event management and ticketing platform. The lures include a shortened link purportedly leading to an updated agreement requiring a signature.

Following the link leads to the installation of stealer malicious software (malware), which when installed steals saved information from a user's web browser. Targeted information can include saved login credentials and credit card information.



Example of an Eventbrite lure seen by Proofpoint researchers

Recommended Training

- To test users' response to a similar lure, search for the "Eventbrite Agreement" drive-by simulated phishing template in the Security Education Platform.
- Use our "Email Attack Methods: Malicious Links" and "60 Seconds to Better Security: What is a Shortened URL" microlearning modules to teach users how to spot and avoid potentially dangerous links in emails.
- Use our November 2023 Threat Alert, "Phishing Attacks Abuse Booking[.]com Branding," to inform users about another series of attacks that also abused an organization's branding.

Email communication to users on next page

Threat Alert: Eventbrite-Themed Lures Distribute Malware (Dec 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: Eventbrite-Themed Lures Distribute Malware

- Cybercriminals have launched a series of phishing attacks attacks abusing Eventbrite branding.
- The lures are intended to look like they come from Eventbrite; however, the reply-to email address is support[@]ev3ntbr1te[.]com. Note the substitution of numbers for letters, which is a common cybercriminal method for creating a lookalike email address.
- The lures encourage recipients to follow a shortened link to sign a purportedly updated user agreement in order to continue receiving payouts.
- Following the link leads to the installation of malicious software (malware) on the recipient's device.

Key Actions (at Work and at Home)

- **Go beyond surface clues.** Familiar logos, branding, and names are not automatic indicators that an email or website is safe. Cybercriminals often imitate well-known organizations.
- **Remain alert to phishing indicators.** Mismatches between sending addresses and an organization's name are always warning signs, as are apparent substitutions of characters in an email address or web page URL.
- **Remember cybercriminals take advantage of strong emotions.** An email warning of issues related to receiving payments can be extremely stressful. Keep in mind cybercriminals seek to capitalize on moments of anxiety and the difficulty in thinking clearly in such situations.
- **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.