

Online Leader Invites You to This Webex Phish

cofense.com/online-leader-invites-you-to-this-webex-phish/

Cofense

October 29, 2020



Phish Found in Environments Protected by SEGs

Cisco Ironport

By Ashley Tran, *Cofense Phishing Defense Center*

The Cofense Phishing Defense Center (PDC) team has identified a phishing campaign that attempts to harvest Webex credentials. This is not the first time we have seen an active Webex campaign, however, as we have noted before. It is actually an attack method that became increasingly common as non-essential workers were pushed into remote working conditions due to the pandemic. The previous Webex phish utilized

implications of vulnerabilities and SSL certificate fixes for Webex, but this one takes a more subtle approach: acting as a Webex event invite.

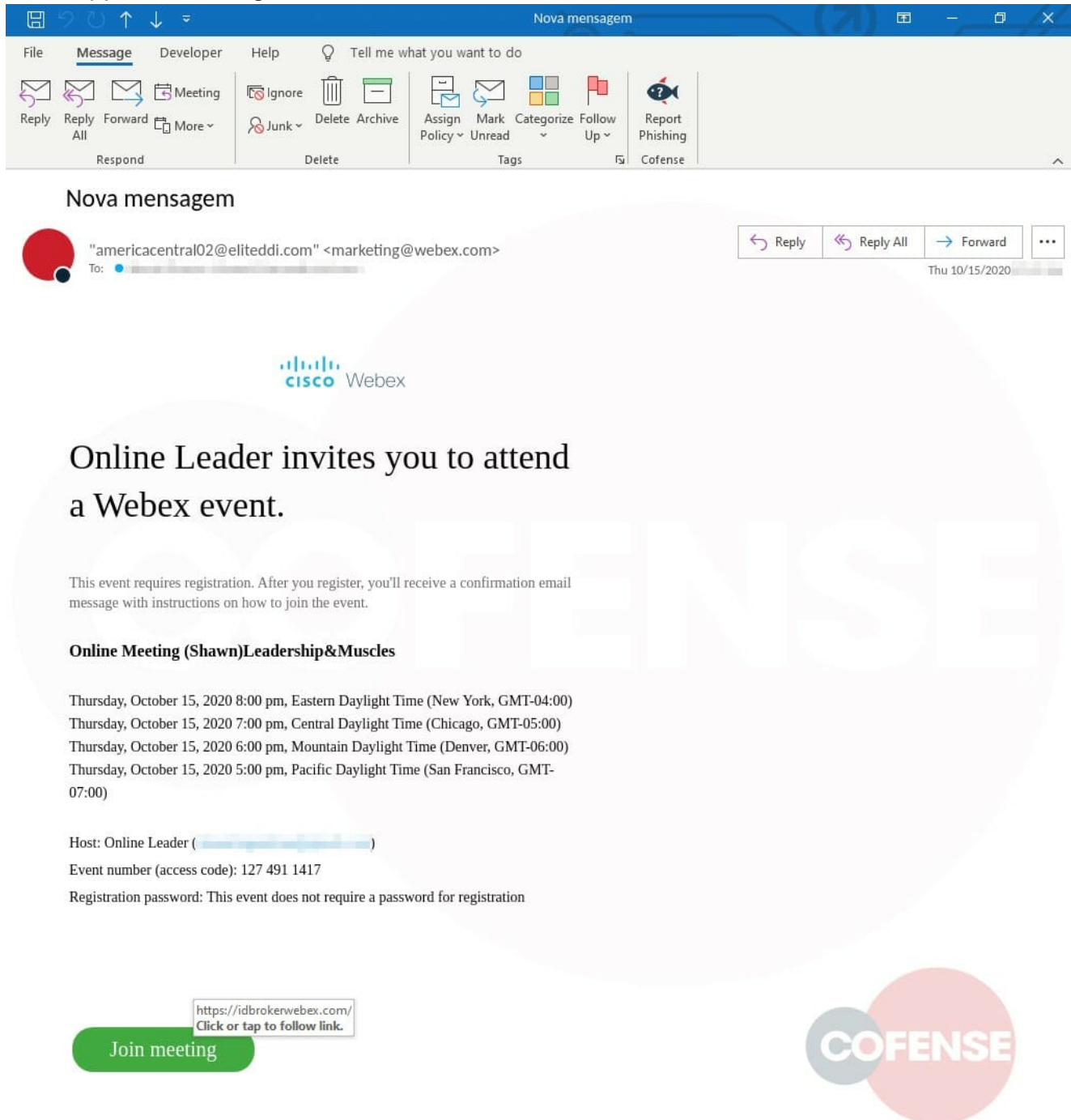


Figure 1: Email Body

The email shown in Figure 1 looks like a relatively normal Webex event invite at a glance. This email is a simple Webex invite that anyone who uses Webex may be accustomed to. This invite says that the user has been invited to the event “Leadership&Muscles,” the host is “Online Leader” and, although it is vague, the mentions of “Leadership” and “Online Leader”

may have most users determine this has to do with work and – without typical phishing language urging them to join – many may not feel so threatened; they may opt to join the meeting out of curiosity.

And should a user think to hover-check the button to “join a meeting,” the URL that will show as a preview will be: `hxxp://idbrokerwebex[.]com`

Despite the threat actor’s attempts to make this email seem legitimate, however, the subject of the email already appears off compared to what is seen in the body – a Portuguese subject paired with an English body? If that does not reveal the true nature of this email then the threat actor’s carelessness with the From and Sender fields will. Although it is obvious there was an attempt to make the email appear as though it is coming from Webex with the inclusion of “,” the real sender email is next to it: `americacentral02[@]eliteddi[.]com`.

Looking into the domain `eliteddi.com`, we can see that it was recently registered, as seen in Figure 2.

The screenshot shows a DomainIQ report for the domain `eliteddi.com`. The report includes the following information:

- Overview:** `eliteddi.com` was registered on April 29, 2020 and is associated with [Yuri Luiz Martin Lima](#), [testeddi03@gmail.com](#). It is registered at [Publicdomainregistry](#). The registrant's email address is associated with 2 domains, and the registrant name is associated with 1 domain. Combined, a total of 2 related domains were identified. The domain is hosted on [192.185.214.103](#), located in US – TX – Houston, which is the host for 30 domains. We have 2 historical whois records for this domain going back to April 30, 2020.
- Domain Details:**

Status:	Registered	Website Pages:	1
Appraised Value:	Unknown	Search Results:	Unknown
Alexa Rank:	Unknown/None	External Links:	Unknown
Flags:	None	Backlinks:	Unknown
- Whois Record Information:**

Registrar:	PUBLICDOMAINREGISTRY
Creation Date:	April 29, 2020
Expires:	April 29, 2021
Nameservers:	NS88.HOSTGATOR.COM.BR NS89.HOSTGATOR.COM.BR
- DNS Record Information:**

IP Addresses:	192.185.214.103 US – TX – Houston 30 domains
---------------	--

Figure 2: Domain Registration Information for `eliteddi.com`

This was perhaps done in a bid to give themselves a domain to use for sending emails. When utilizing their own registered domains, this gives the threat actor a legitimate DKIM, SPF and DMARC to bypass resources. This domain was presumably also used as practice in setting up this attack because, as noted in Figure 3, the domain is also the host to the

same Webex phish. Because the domain eliteddi[.]com is not part of the actual email itself, and isn't actually a part that a user would typically interact with, it can be assumed that this domain was part of the threat actor's practice attempt before launching this attack.

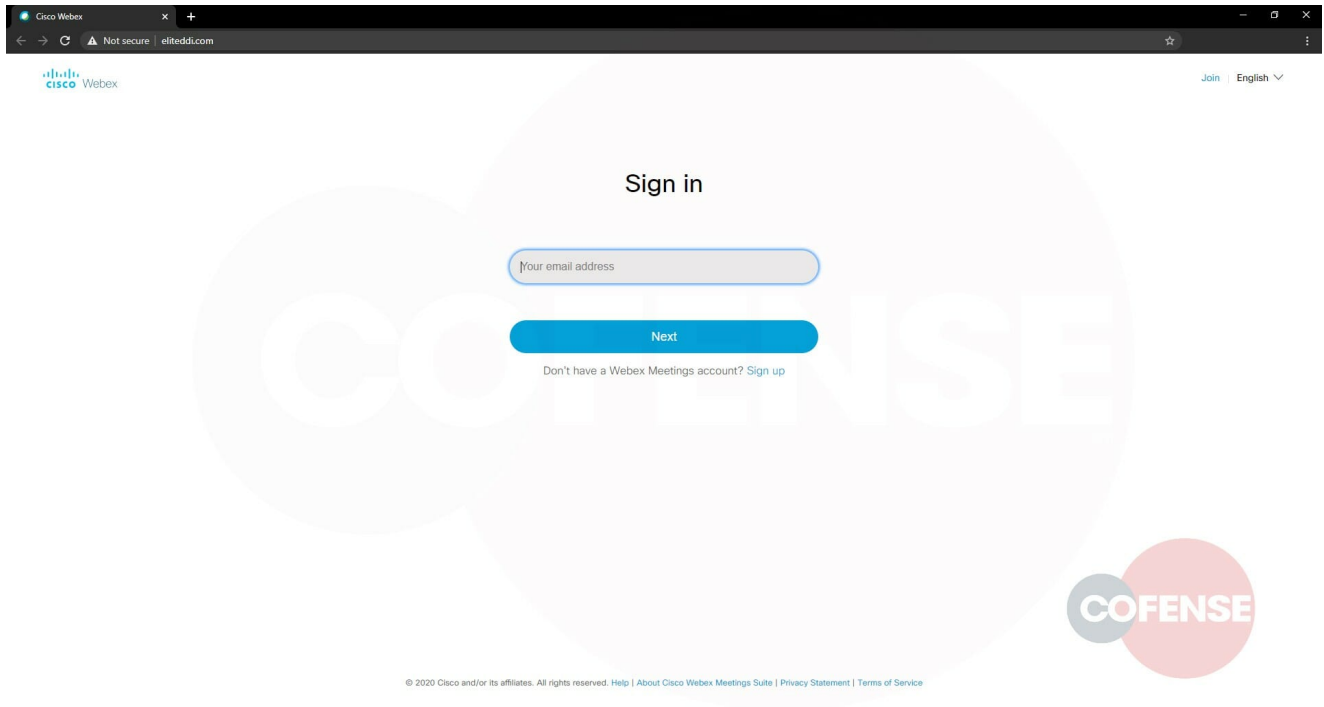


Figure 3: Webex phish found on the sender domain eliteddi[.]com

Taking a look at the URL found embedded into the email itself we can see that this URL looks much more legitimate than the one seen in the threat actor's practice attempts. This fraudulent domain was also recently registered according to information found on its corresponding Whois record, as seen in Figure 4.

Report for **idbrokerwebex.com** – contact@privacyprotect.org

Overview

idbrokerwebex.com was registered 5 days ago and is associated with contact@privacyprotect.org. It is registered at [PublicDomainRegistry](#).

No related domain names available.

The domain is hosted on [216.172.161.34](#), located in US – TX – Houston, which is the host for 48 domains.


We have **1** historical whois record for this domain going back to October 11, 2020.

[Contact Owner](#)
[Ownership Record](#)
[Tools](#)
[Help](#)

Domain Details

<u>Status:</u> Registered	<u>Website Pages:</u> Unknown
<u>Appraised Value:</u> Unknown	<u>Search Results:</u> Unknown
<u>Alexa Rank:</u> Unknown/None	<u>External Links:</u> Unknown

Website Snapshot



Whois Record Information [View](#)

Registrar: [PDR LTD. D/B/A PUBLICDOMAINREGI...](#)

Creation Date: October 10, 2020

Expires: October 10, 2021

Nameservers: [NS430.HOSTGATOR.COM.BR](#)
[NS431.HOSTGATOR.COM.BR](#)

DNS Record Information

IP Address(es): [216.172.161.34](#)

Figure 4: Domain information for idbrokerwebex[.]com

One thing to note for this fraudulent domain is that the threat actor has tried to mimic a real Webex URL, one that is typically just a quick redirect when logging into Webex Teams, but would still be a familiar site to users. The small difference between the legitimate and the phishing URLs, though, is a simple “.” separating idbroker from webex – a small mistaken mistype of a user trying to get to this domain can lead to a huge mistake in this case.

The phish itself can be noted in Figure 2.

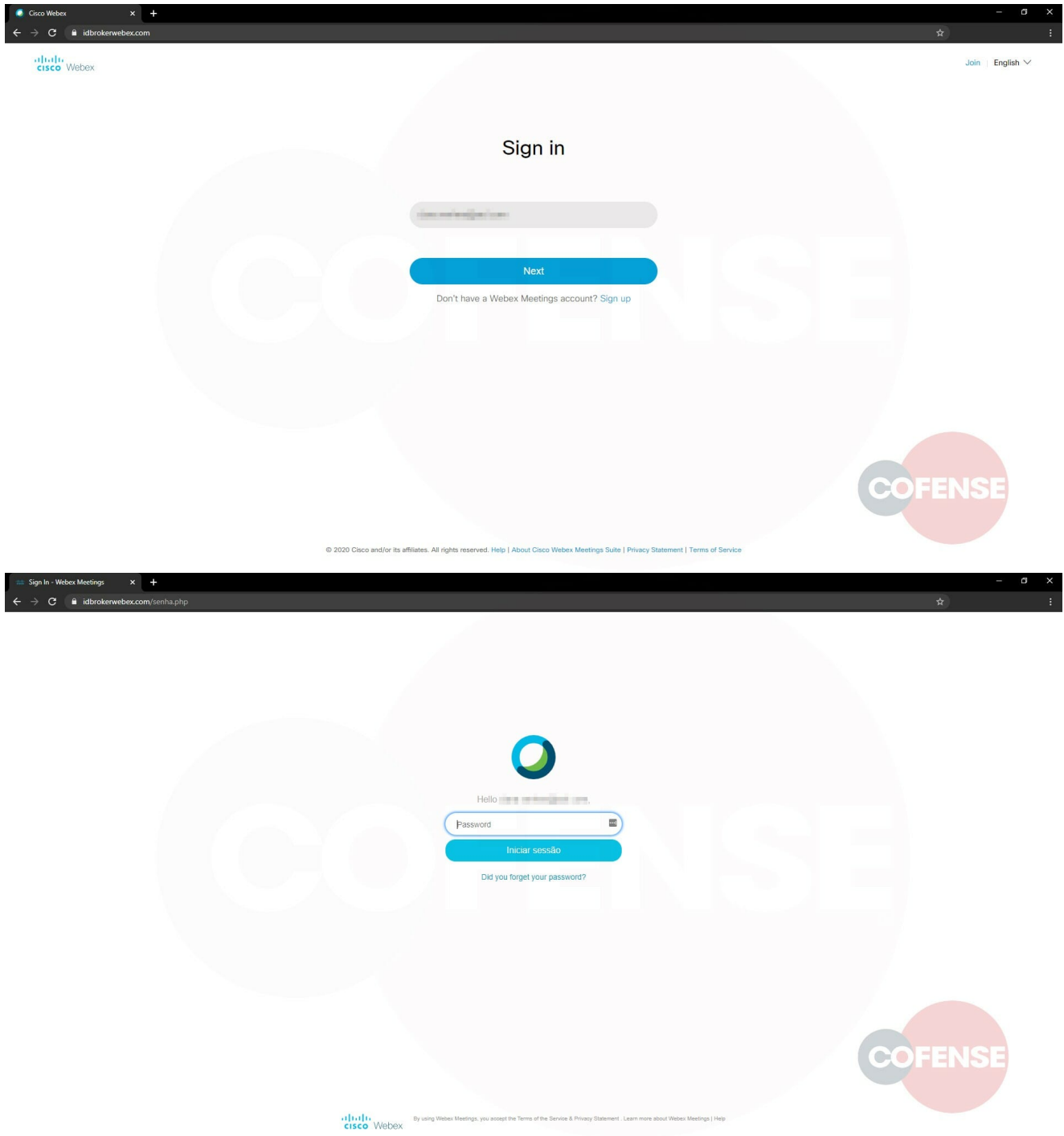
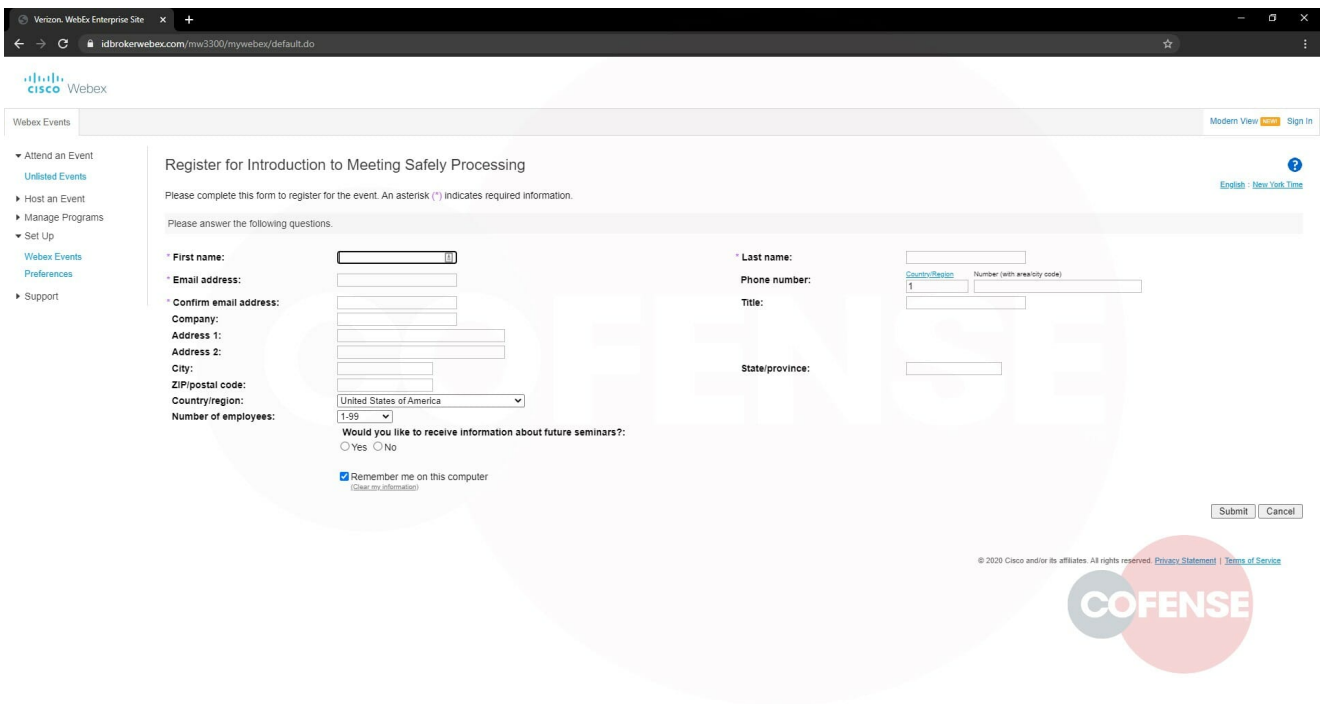


Figure 5-6: Phishing Page

The Webex phish similar to this has utilized the same template when phishing for credentials, essentially a perfect copy of Webex’s login page. This page does not have any noticeable flaws in grammar anywhere or weird formatting. In fact, even the URL in the address bar does not give anything away immediately should a user glance at it for any sort of validation.

Compared to the phishing page seen hosted on the threat actor’s “practice” domain noted above, this one actually has a certificate for the site that, in turn, adds a lock in the address bar which, to most, indicates that a site is “secure.” This is a relatively common addition, especially with the use of website builders that give creators a certificate to work with. However, as noted numerous times in other blogs, threat actors are using that perception to trick users into trusting their phishing attacks.

The second step of this attack can be noted in Figures 7-8. This step acts more as a distraction mechanism, as the page looks like any other Webex event registration page. Here the user would input any amount of information as long as the fields are required, then move on to the final confirmation page. While this page is more than likely just an attempt to put any suspicions the user had initially to rest, this page also has the potential to garner more information about the user.



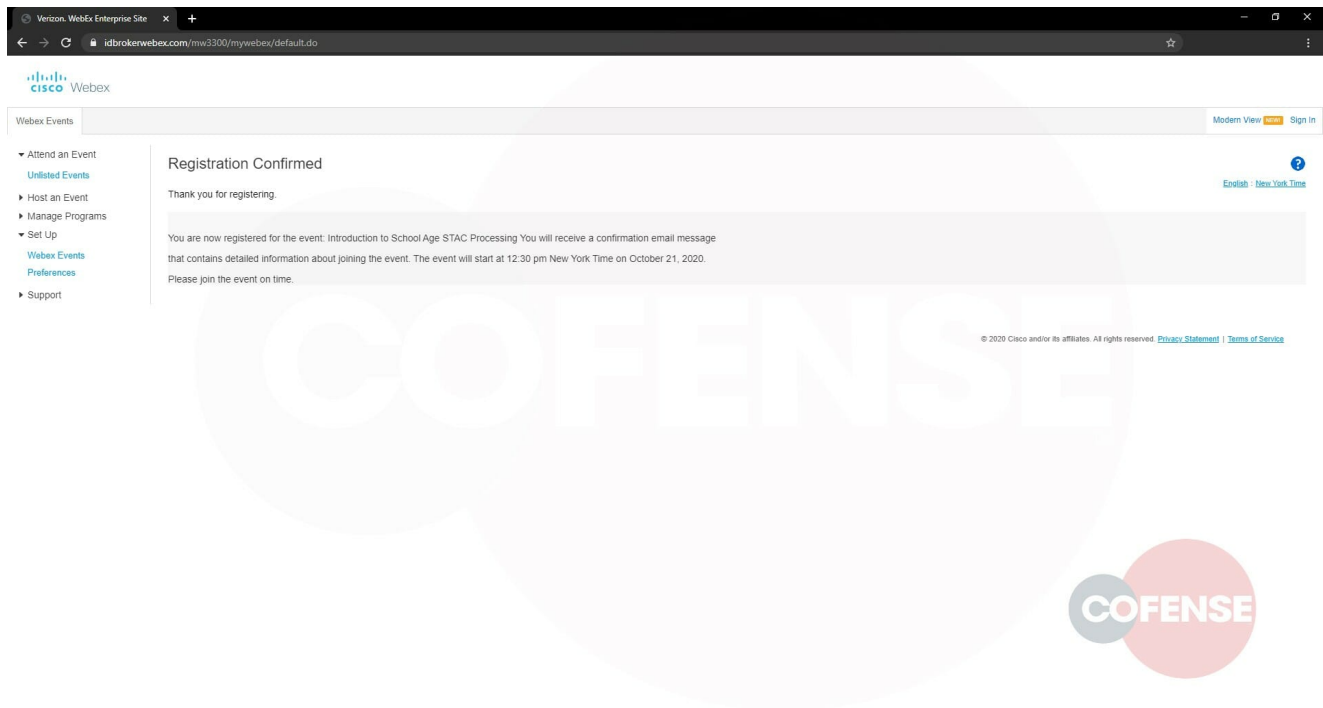


Figure 7-8: “Event” Registration

Indicators of Compromise

Network IOC	IP
hxxp://eliteddi[.]com	192.185.214.103
hxxp://idbrokerwebex[.]com	216.172.161.34

All third-party trademarks referenced by Cofense whether in logo form, name form or product form, or otherwise, remain the property of their respective holders, and use of these trademarks in no way indicates any relationship between Cofense and the holders of the trademarks. Any observations contained in this blog regarding circumvention of end point protections are based on observations at a point in time based on a specific set of system configurations. Subsequent updates or different configurations may be effective at stopping these or similar threats.

The Cofense® and PhishMe® names and logos, as well as any other Cofense product or service names or logos displayed on this blog are registered trademarks or trademarks of Cofense Inc.

Don't miss out on any of our phishing updates! Subscribe to our blog.