TA4903: Actor Spoofs U.S. Government, Small Businesses in Phishing, BEC Bids

proofpoint.com/us/blog/threat-insight/ta4903-actor-spoofs-us-government-small-businesses-phishing-bec-bids

February 21, 2024

Share with your network!

March 06, 2024 Selena Larson, Jake G. and Dusty Miller

Key takeaways

- TA4903 is a unique threat actor that demonstrates at least two distinct objectives: (1) credential phishing and (2) business email compromise (BEC).
- TA4903 routinely conducts campaigns spoofing various U.S. government entities to steal corporate credentials.
- The actor also spoofs organizations in various sectors including construction, finance, healthcare, food and beverage, and others.
- The campaign volumes range from hundreds of messages to tens of thousands of messages per campaign.
- The messages typically target entities in the U.S., although additional global targeting has been observed.
- TA4903 has been observed using the EvilProxy MFA bypass tool.
- In late 2023, TA4903 began adopting QR codes in credential phishing campaigns.

Overview

TA4903 is a financially motivated cybercriminal threat actor that spoofs both U.S. government entities and private businesses across many industries. The actor mostly targets organizations located in the United States, but occasionally those located globally, with high-volume email campaigns. Proofpoint assesses with high confidence the objectives of the campaigns are to steal corporate credentials, infiltrate mailboxes, and conduct follow-on business email compromise (BEC) activity.

Proofpoint began observing a series of campaigns spoofing federal U.S. government entities in December 2021. The campaigns, which were subsequently attributed to TA4903, first masqueraded as the U.S. Department of Labor. In 2022 campaigns, the threat actors purported to be the U.S. Departments of Housing and Urban Development, Transportation, and Commerce. During 2023, the actor began to spoof the U.S. Department of Agriculture.

In mid-2023 through 2024, Proofpoint observed an increase in credential phishing and fraud campaigns using different themes from TA4903. The actor began spoofing various small and medium-sized businesses (SMBs) across various industries including construction, manufacturing, energy, finance, food and beverage, and others. Proofpoint observed an increase in the tempo of BEC themes as well, including using themes such as “cyberattacks” to prompt victims to provide payment and banking details.

Most credential phishing messages associated with this actor contain URLs or attachments leading to credential phishing websites. In some cases, including the government-themed campaigns, messages contain PDF attachments that contain embedded links or QR codes leading to websites that appear to be direct clones of the spoofed government agency.

Based on Proofpoint's research and tactics, techniques, and procedures (TTPs) observed in open-source intelligence, activity related to TA4903's impersonation of U.S. government entities goes back to at least mid-2021. TTPs associated with the actor's broader credential phishing and BEC activities are observable as long ago as 2019.

Campaign details

Government bid spoofing

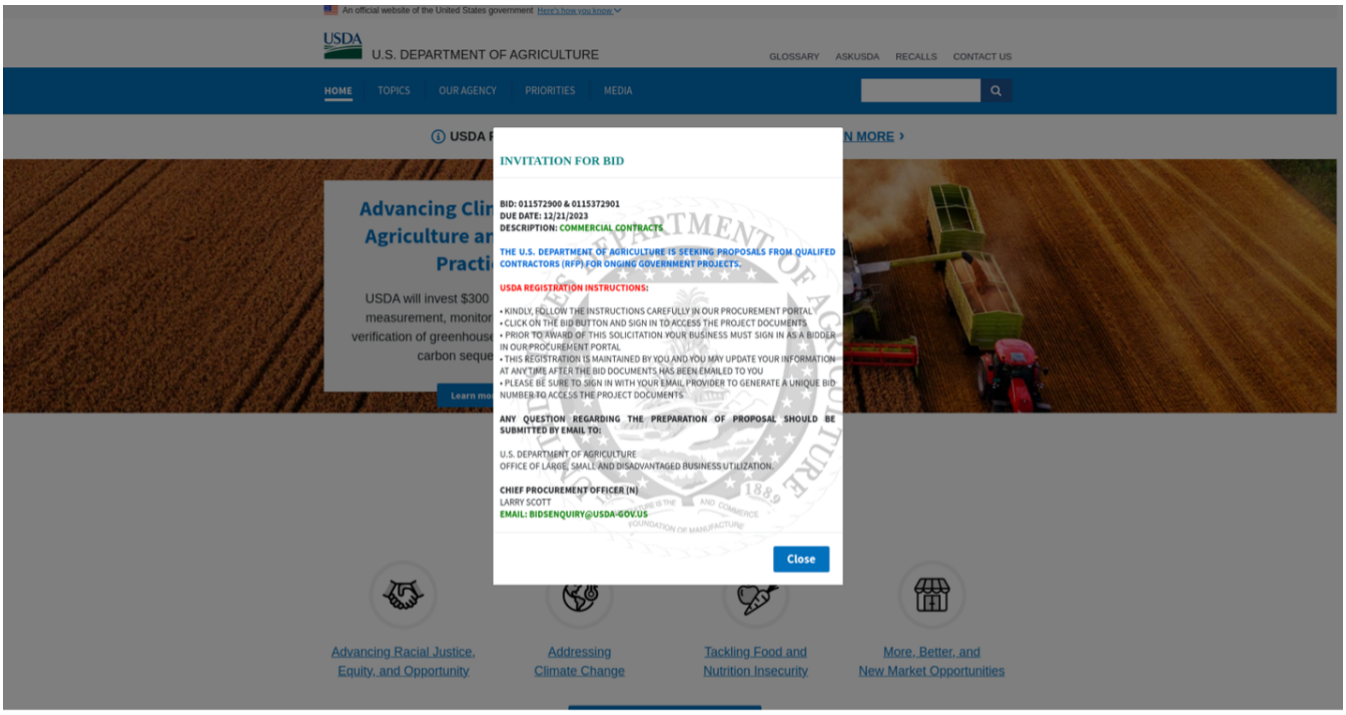
Historically, Proofpoint mostly observed TA4903 conducting credential theft campaigns using PDF attachments leading to portals spoofing U.S. government entities, typically using bid proposal lures. In late 2023, TA4903 began spoofing the USDA and began incorporating QR codes into their PDFs, a technique previously unobserved by this actor.

Messages may purport to be, for example:

> From: U.S. Department of Agriculture <entry@ams-usda[.]com>
>
> Subject: Invitation To Bid
>
> Attachment: usda2784748973bid.pdf

Example of one page of a multi-page PDF spoofing the USDA. The "Bid Now" button is hyperlinked to the same URL as the QR code.

In these campaigns, the PDF attachments are typically multiple pages long and have both embedded URLs and QR codes that lead to government-branded phishing websites.



Example credential phishing website operated by TA4903, designed to capture O365 and other email account credentials.

In 2023, Proofpoint observed TA4903 spoof the U.S. Department of Transportation, the U.S. Small Business Administration (SBA), and the USDA using similar themes.

O365 credential theft

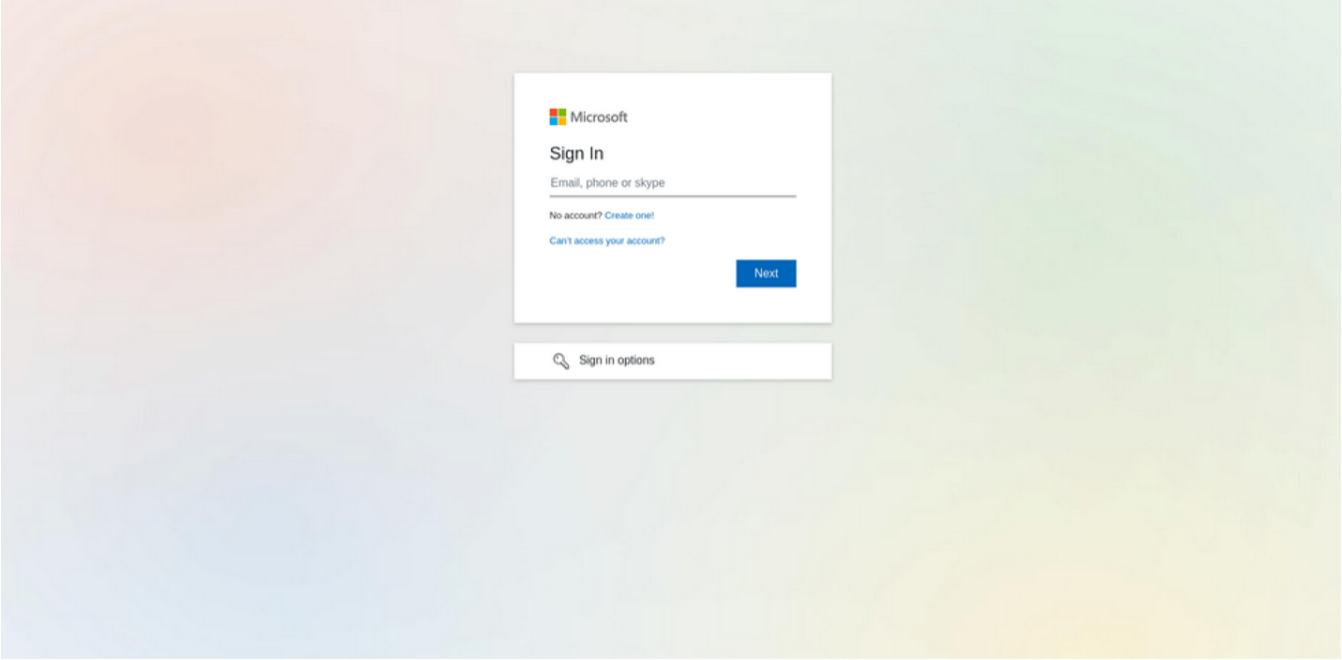
In 2023, Proofpoint observed new tactics, techniques, and procedures from this actor including using lure themes referencing confidential documents, ACH payments, and secure message lures, and use either URLs, HTML attachments, or zipped HTML attachments, which is a significant expansion in activity observed before 2023.

Typically, the actor uses actor-owned and operated domain infrastructure that spoofs various North American companies to deliver email. Occasionally the actor will use freemail addresses, however, that is unusual. It is possible Proofpoint did not previously observe this activity either because the actor was not using these themes with regularity, or the activity may have been occurring outside of Proofpoint visibility.

For example, in late November 2023, Proofpoint observed the following messages:

> From: Finance Dept. via Orga-Portal <donotreply@secureserver5[.]com>
>
> Subject: New Receipt from Finance Department
>
> Attachment: 11-30Receipt.zip

These ZIP attachments contained HTML documents that contained URLs that redirected to a website spoofing a Microsoft O365 login page. This site was designed to steal username and password credentials.



Spoofed Microsoft O365 landing portal.

TA4903 was observed using EvilProxy, a reverse proxy multifactor authentication bypass toolkit, throughout 2023, but its use dropped off later in the year and it has not been observed yet in 2024.

Imposter / direct BEC cyberattack theme

Beginning in mid-2023, Proofpoint began observing campaigns departing from its typical email lures but which aligned with the BEC objective demonstrated by TA4903. The actor used themes such as “cyberattack” or “payment” themes and used actor-owned lookalike domains spoofing likely suppliers of organizations to send the BEC messages. The messages are "benign" in that they do not contain malicious URLs or attachments but feature sender and reply-to email addresses owned by the threat actor spoofing a legitimate entity. These campaigns differed from previously observed BEC activity as it was broadly distributed to many victims, not targeted follow-on activity.

For example, on 17 May 2023, TA4903 sent emails spoofing produce and manufacturing companies. Emails purported to alert the recipient that the sender organization had suffered a cyberattack and requested updated banking information. This was the first time Proofpoint had observed TA4903 conducting a BEC supplier domain spoof attack using a cyberattack theme, and it has been used multiple times since.

Hello Everyone,

I regret to inform you that our company has recently been the victim of a cyber attack, which has resulted in the compromise of our banking information. As a result, we urgently need to update our banking information to prevent any further unauthorized access and potential loss of funds.

We take the security and privacy of our clients very seriously, and have already taken appropriate measures to contain the situation and mitigate the impact. However, in order to ensure the safety of our financial transactions, we need to update our banking information immediately.

Could you kindly provide me with information on who is responsible for updating banking information within your organization?

If you have any questions or concerns regarding this matter, please do not hesitate to contact us. We appreciate your understanding and cooperation in this matter, and look forward to continuing our valued partnership.

Thank you for your prompt attention to this urgent matter.

Best regards,

Example cyberattack themed BEC email body copy.

So far in 2024, Proofpoint has observed multiple TA4903 campaigns conducting BEC activity using invoicing or remittance themes.

Links to follow-on BEC activity

Proofpoint researchers previously seeded researcher-owned credentials to one of the spoofed government bid portals in an attempt to view follow-on activity through an internal honeypot. This honeypot was designed to observe the behavior of phishing threat actors once they have obtained access to a compromised account using stolen credentials.

Proofpoint researchers seeded credentials to one of the Department of Transportation-themed credential capture portals. Within six days, the credentials were used to login to the Proofpoint-owned email account. The threat actor searched email history for keywords including “bank information,” “payment,” and “merchant.” Proofpoint assesses with high confidence the actor was attempting to look for existing threads to conduct BEC activities such as invoice fraud or payroll redirect using thread hijacking techniques.

Proofpoint has observed several instances of targeted BEC campaigns attempting to perform invoice fraud. These campaigns usually utilize lookalike domains and reply-to manipulation to deceive the recipients. Researchers believe with high confidence that the themes and targets for these campaigns are created with the information gathered from accounts compromised during prior credential phishing campaigns, typically targeting the original victim’s business partners and financial institutions.

It is likely that TA4903's credential phishing campaigns are precursors to follow-on BEC activity, using information stolen from compromised accounts to identify possible targets, create likely personas, and craft email lures.

Actor attribution

TA4903 is a financially motivated cybercriminal actor with an initial objective of stealing corporate credentials and likely follow-on objectives of conducting BEC. Proofpoint clustered this threat activity based on the following characteristics:

- The government-related domain and sender emails are similar in construction, typically using “bids” and the government agency acronyms in the domain names.
- Additional spoofed domains typically include entities from verticals including construction, energy, manufacturing, finance, and others. These domains typically include spelling errors, for example being one letter off of the legitimate domain or include extraneous letters like “llc”.
- The threat actor uses consistent email lure and PDF content, and while the specific department changes between government-themed campaigns, the lure themes and PDFs are consistent in their design.
- PDF documents often have consistent metadata traits, such as the author name, Edward Ambakederemo.
- The credential capture webpages use a consistent phishing kit with minimal modifications.
- The actor uses the same hosting providers and for most of the activity Proofpoint has observed.
- Information used in domain registration has identifiable traits or is otherwise directly linked to infrastructure previously known to be associated with TA4903.

Conclusion

TA4903 is a persistent, financially motivated threat actor that generally targets organizations in the U.S. with high-volume email campaigns. Proofpoint assesses with high confidence that TA4903 activity leads to BEC objectives following their initial credential harvesting activity. The actor frequently registers new domains relating to both government entities and private organizations in a variety of sectors, which it then uses for its credential phishing activity. Once access to a compromised mailbox is achieved, the actor will search for information relevant to payments, invoices, etc., and likely conduct follow-on activities such as sending additional emails related to payment fraud from the compromised inbox.

The actor’s recent BEC campaigns that move away from government spoofing and instead purport to be from small and medium-sized businesses have become more frequent. These campaigns are observed at a higher operational tempo than previously observed government spoofing or other credential theft campaigns. It is possible the actor’s techniques have shifted as a result of the efficacy of such campaigns, or it is just a temporary change in the overall TTPs.

Analyst note: After publication of this report, researchers identified TA4903 return to using government-themed credential phishing campaigns. The high-volume campaign spoofed the Department of Labor and contained PDFs with links to a credential phishing website.

Emerging Threats signatures

TA4903 domains are added weekly to the Emerging Threats PRO ruleset.

Rule Name: ETPRO PHISHING TA4903 Domain in DNS Lookup

Example indicators of compromise

Indicator	Description	First Seen
d398eef8cf3a69553985c4fd592a4500b791392cf86d7593dbdbd46f8842a18d	SHA256 usda278474897849493bid.pdf	November 2023
hxxps://auth01-usda[.]com	Credential Phishing Landing Page	November 2023
hxxp://tracking[.]tender-usdabids[.]com	Credential Phishing Landing Page	December 2023
ed4134de34fbc67c6a14c4a4d521e69b3cd2cb5e657b885bd2e8be0e45ad2bda	ams-usdabid48428492894.pdf	December 2023
Shortsync[.]net	Credential Phishing Domain	December 2023
15b9ae1ab5763985af2e6fe0b22526d045666609ad31829b8926466599eeb284	SHA256 11-30Receipt.zip	November 2023
orga-portal[.]com	Credential Phishing Domain	December 2023
6f776331d7c49ab6e403f84409c062db0b2027429e47e3533e8c6098c5f12156	SHA256 Bid Instruction.pdf	March 2024
index-dol[.]com	Credential Phishing Landing Page	March 2024
hxxps://index-dolbid2024[.]com	Credential Phishing Landing Page	March 2024

Subscribe to the Proofpoint Blog