Advanced Office365 Phishing Attack on U.S. Government Contractors

AMJAD ALQAHTANI **(WKH221)**

DERYA YAVUZ **(HVX258)**

Introduction

- This is a very deliberate and carefully-constructed organized phishing attack targeting the Department of Labor contractors.
- Over 10 different phishing campaigns launched simultaneously over the course of months with official-resembling ruses
- Main goal: **harvesting Office365 / MS Online credentials for official DoL contractors.**

Why this case?

- Relevance of this threat to any major corporation of today
- Demonstrate how **educated** and **deliberate** attacks have become and how much of an impact they could have – in this case, a potential national security threat
- Highlight the importance of cybersecurity awareness training

Attack Vector

- **Malicious Email** - Email with insignia and seals from senior officer, PDF attachment with a project bid link. Sender impersonated **“Chief Procurement Officer”** persona.
- Victim clicks BID button on the PDF, leading them to **Landing page** that replicated the exact HTML and CSS in the form of the actual DoL website.
- User sees and clicks a pop-up to **"initiate a bid”,** leading them to a **Credential harvesting page** with a fake login that asks for O365 email and password.
- **To reduce mistyped credentials count, the attackers threw a fake error and asked for the credentials again.**
- **In either case, redirects were included to the original DOL website to lessen suspicion.**

Limitations

Making spoofed domains look legitimate:

- DOL-related domains with variations of punctuation, sender email addresses spoofed to originate from **no-reply@dol[.]gov**

Evading the MX filters and email spam filtering tools (SPF, DKIM, and DMARC) by:

- emails passed through abused servers owned by non-profit organizations
- newly registered and unreported domains that were not denylisted or blocked
- domains not on anti-phishing lists

Ruse & Vector

U.S DEPARTMENT OF LABOR
INVITATION FOR BID
To:

U.S DEPARTMENT Of LABOR

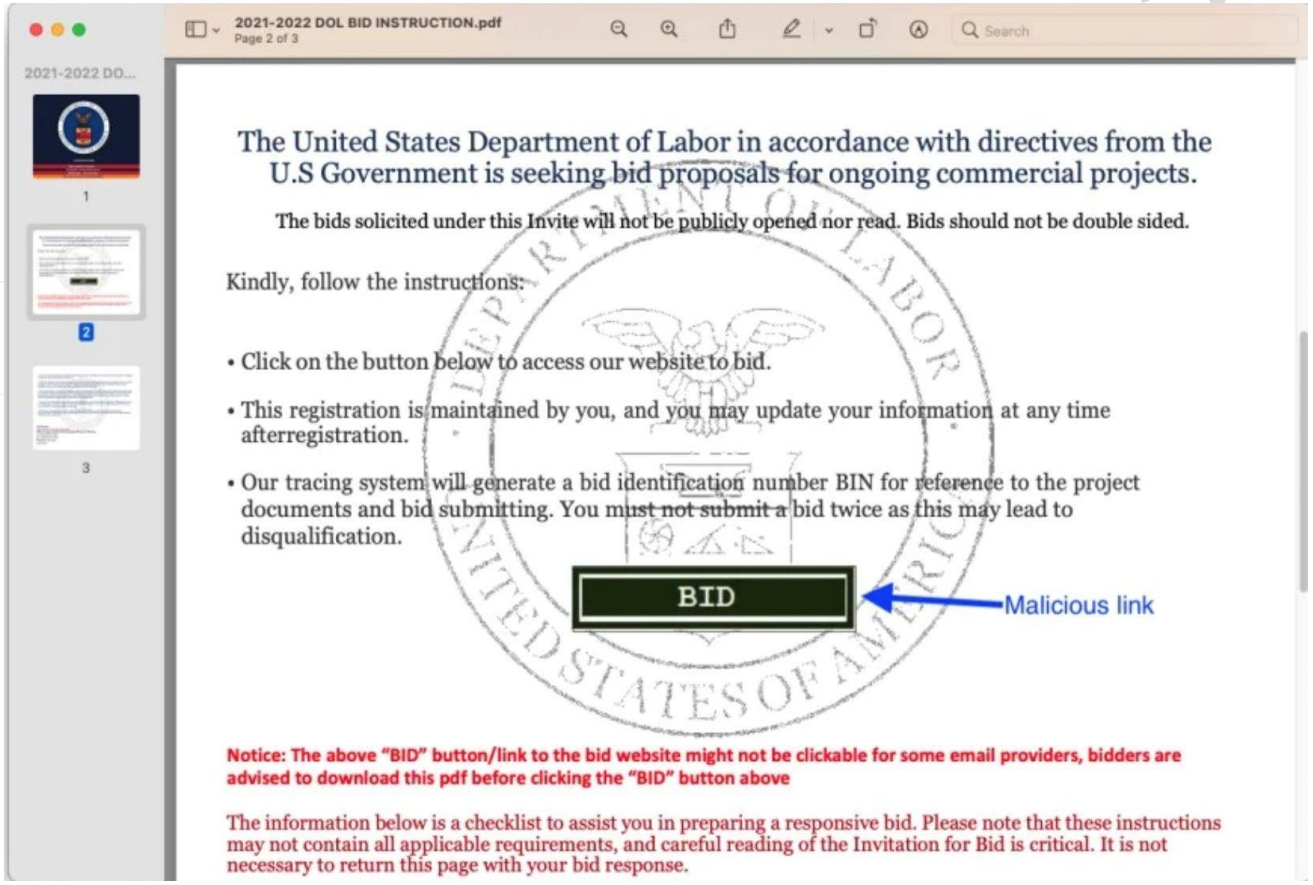
(For Immediate Release)

Attn:

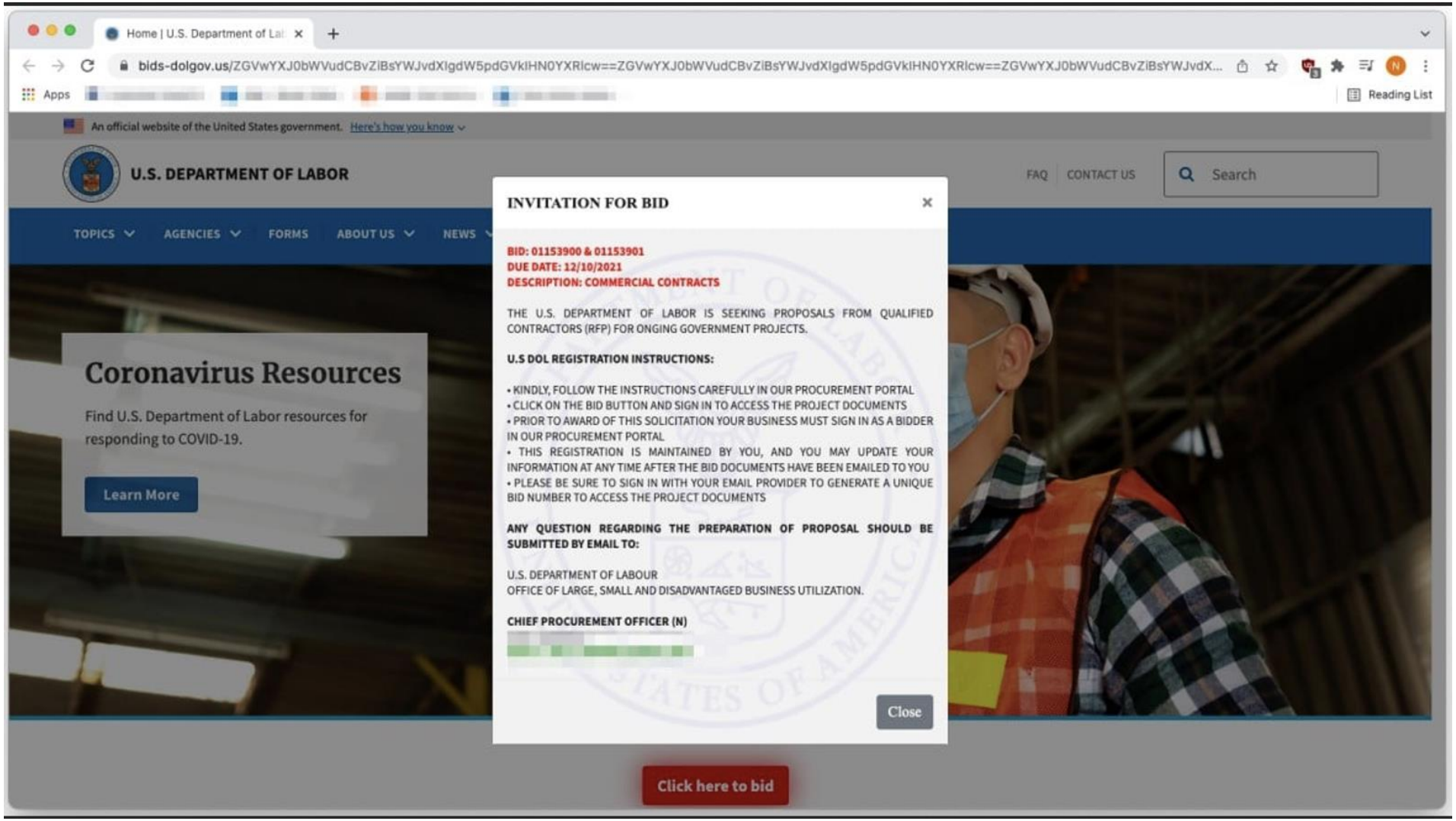
INVITATION FOR BID
BID: 01153900 & 01153901
Due Date: 12/10/2021
Description: Commercial Contracts

The U.S. Department of Labor is seeking proposals from qualifed contractors (RFP) for ongoing government projects.
U.S DOL Registration Instructions:
. Kindly download the attached bid document and follow the instructions carefully to access our Procurement portal
. Click on the "BID" button on the bid document and sign in to access the project documents
. Prior to award of this solicitation your business must sign in as a bidder in our Procurement portal
. This registration is maintained by you and you may update your information at any time after the bid documents has been emailed to you
. Please be sure to sign in with your email provider to generate a unique bid number to access the project documents
. Attached Bid File should be downloaded (Office 365 users might not be able to click the bid button if file is not downloaded)
Any Question regarding the preparation of proposal should be submitted by email to:

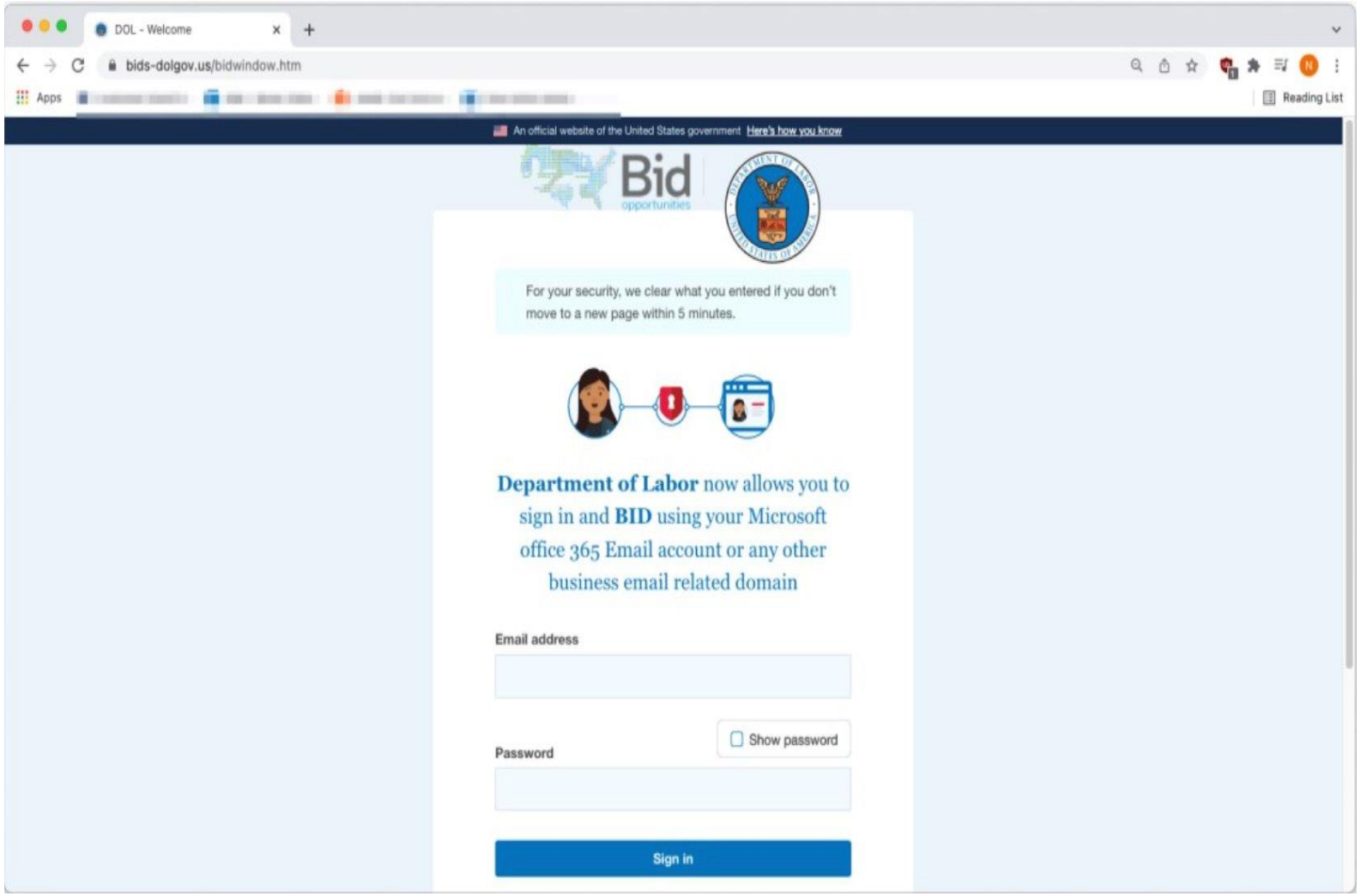
U.S. Department of Labour
Office of Large, Small and Disadvantaged Business Utilization.
Chief Procurement Officer (N)



Attached malicious PDF with accurate branding elements.



Landing page with pop-up notification to increase credibility.



Credential harvesting page utilized by attackers.

Recommendations

- Robust **email spam filtering (SPF, DMARC, DKIM),** employing a zero external trust policy, extensive denylists
- Learning on a tight cadence and **phishing training courses** including modern ruses that have been used in the pasts, teaching the **common indicators of spam** to high-risk employees – tailored for **employee privileges and types**
- Secure SMTP (Mail) server configuration – deny emails from non-local IP addresses to non-local mailboxes from unauthorized users **[addressed in Questions section]**
- Ensure **MFA** is implemented as an additional defense even if credentials are compromised.
- Follow **NIST CSF** and **CISA** guidelines to keep organizational security posture up-to-date.

Conclusion

- Phishing training in government organizations is especially important due to the nature of **sensitive federal information** stored – anyone can be a target as phishing attacks have been getting increasingly complex and intricate.
- Organizations should **take robust technical security measures** to secure their email configuration and **block incoming phishing attempts.**
- Official U.S. government domains usually end in **.gov** or **.mil** rather than .com or another suffix. The U.S. government does not typically send out cold emails to solicit bids for projects. These are especially important to highlight in **specialized training sessions.**

Questions?

1. What is the relevance of SMTP filtering?
    1. **While most phishing attempts are external and our main recommendations that we would like to highlight are phishing awareness training, robust email spam filtering (SPF, DKIM, DMARC) and enforcing Multi-Factor Authentication – SMTP filtering could also prevent against potentially maliciously-influenced internal actors, as well as proxying inbound email traffic to evade phishing attempts.**
    2. **As mentioned in this article, an inbound SMTP proxy server can be utilized to verify and authenticate incoming traffic – if any flagged email from a denylisted domain is received in incoming traffic, then the inbound SMTP proxy server can block before they are received at the actual SMTP server (if the company employs one).**

References

1. Toulas, B. (2022, January 19). Office 365 phishing attack impersonates the US Department of Labor. BleepingComputer. https://www.bleepingcomputer.com/news/security/office-365-phishing-attack-impersonates-the-us-department-of-labor/
2. Blanchard, D. (2022, February 2). Phishing scam targets U.S. Department of Labor with fake job offers. Tech.co. Retrieved from https://tech.co/news/phishing-scam-dol
3. Kay, R. (2021, October 21). Fresh Phish: Phishers lure victims with fake invites to bid on nonexistent federal projects. INKY. Retrieved from https://www.inky.com/en/blog/fresh-phish-phishers-lure-victims-with-fake-invites-to-bid-on-nonexistent-federal-projects
4. What Is Anti-Phishing? Techniques to Prevent Phishing. (2024, September 25). Perception Point. https://perception-point.io/guides/phishing/how-to-prevent-phishing-attacks/
5. Leveraging Outbound SMTP Proxy Server Can Protect Your Organization From Blacklisting. Link