Advanced Office365 Phishing Attack on U.S. Government Contractors

Derya Yavuz (hvx258) and Amjad Alqahtani (wkh221)

Group Contribution

- Amjad – Editing the report, researching the topic in detail
- Derya – Writing out the report in detail, creation and editing of slides

Introduction

Cyber threats against government contractors have escalated with attackers using sophisticated phishing schemes. This case study examines a phishing campaign targeting U.S. government contractors that employs convincing lures and crafted fake documents. In 2022, a well-planned phishing campaign impersonating the U.S. Department of Labor successfully targeted Office 365 users. The campaign not only threatens sensitive project information but also exposes gaps in cybersecurity awareness among contractors.

Technically, attackers sent emails that mimicked official government domains and impersonated Department of Labor personnel, inviting recipients to bid on non-existent government projects. These emails were very carefully crafted with near-official graphics, language and attachments – directing victimized users to a realistic phishing site, tricking them into entering their Office 365 credentials, therefore gaining unauthorized access into their O365 environment and internal resources. The attackers' techniques for creating a convincing appearance and stealing login details while avoiding detection are especially noteworthy. Given the implications of compromised government contracts on national security and contractor privacy, analyzing this case is essential for understanding emerging phishing tactics and developing stronger defenses against them.

Motivation

We chose this topic due to the relevance of this attack to any real-life organization, since phishing attacks have been on the rise with many different ruses and intricate attack patterns. The techniques used by attackers to create a convincing appearance and steal login details of real users while avoiding detection are extremely interesting and showcase just how important cybersecurity awareness and training could be to avoid compromise. This case also emphasized just how easily a national security threat could be formed by untrained users clicking malign links – and thus, just how important it has become to create and enforce a robust cybersecurity awareness training program across all employees of an organization, to have a line of defense in the human factor.

Attack Vector

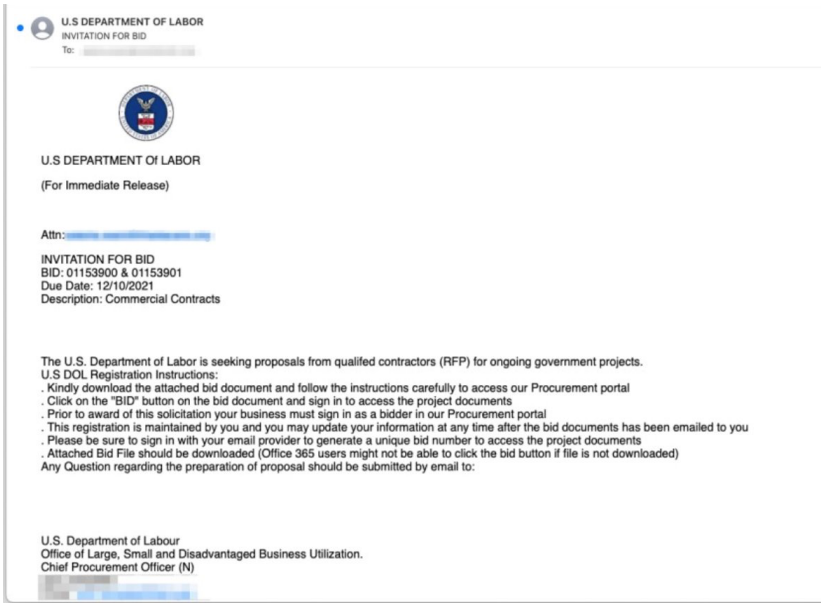
This attack overall consisted of over 10 different phishing campaigns all launched simultaneously against varying targets. The main attack vector is the spoofed Department of Labor email sender emails designed to look similar to **no-reply@dol[.]gov** and accompanying domains that appeared to be originating from the Department of Labor. Attackers carefully selected and targeted DoL's Google Workspace and Microsoft 365 (Office 365) users as victims for their campaigns.

While the use of this vector is clever to achieve impersonation for a more successful phishing campaign, a potential problem that could damage the credibility was evading MX filters and other various email spam filtering tools. However, the crafted emails passed through abused servers owned by non-profit organizations, that used newly registered or unreported domains that were not blocked from email servers or were included in anti-phishing lists.

The main ruse employed by the attacker was to pretend as a Senior Department of Labor employee, namely under “Chief Procurement Officer”, sending emails complete with the Department of Labor letterhead, design and font choices that contained a malicious PDF attachment asking the recipient to click the link in order to begin bidding on a new project.

The attack flow progressed when the victim clicked the “BID” button on the malicious PDF, ending on the **landing page** that was a direct replica of the exact HTML/CSS content of the official Department of Labor website, complete with a pop-up notification to “initiate a bid”. The victim then would click this pop-up notification and get redirected to the credential harvesting page designed to look similar to Office365 login. The attackers also covered all their error bases – to reduce the mistyped credentials count, they threw a fake error message upon the first receipt of credentials into the harvesting page, prompting the user to re-enter credentials. Then, upon successful harvesting, this page would then be redirected to the official Department of Labor site, to make the user less suspicious.

The phishing emails exploited a critical vulnerability in security awareness - the assumption of legitimacy when interacting with familiar government branding. By emulating trusted federal sites, attackers bypassed basic security checks, capturing sensitive login information and data from contractors who believed they were on authentic agency portals.



U.S DEPARTMENT OF LABOR
INVITATION FOR BID
To:

U.S DEPARTMENT Of LABOR

(For Immediate Release)

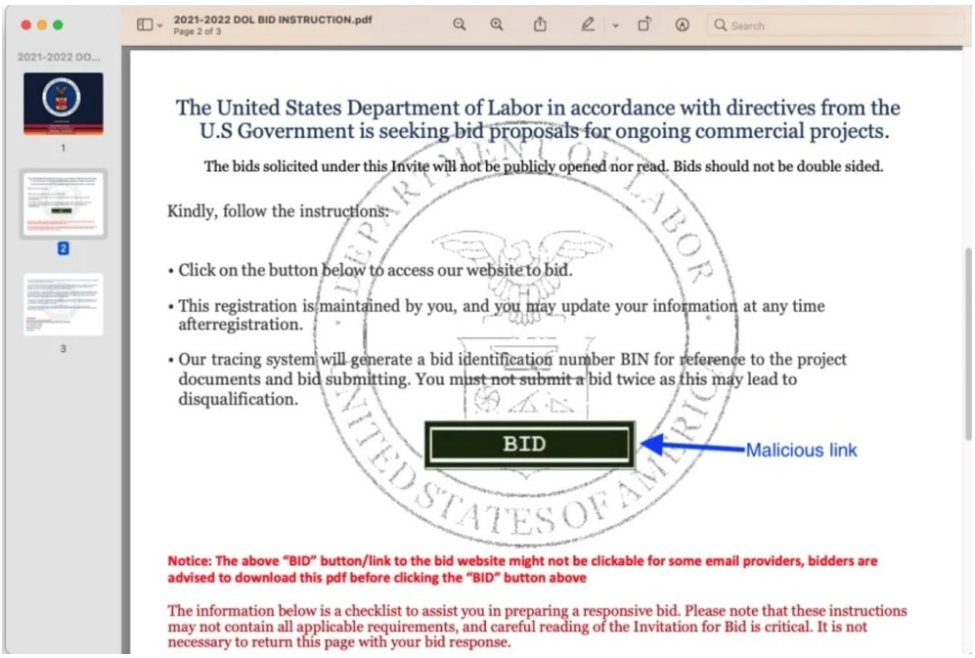
Attn:

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

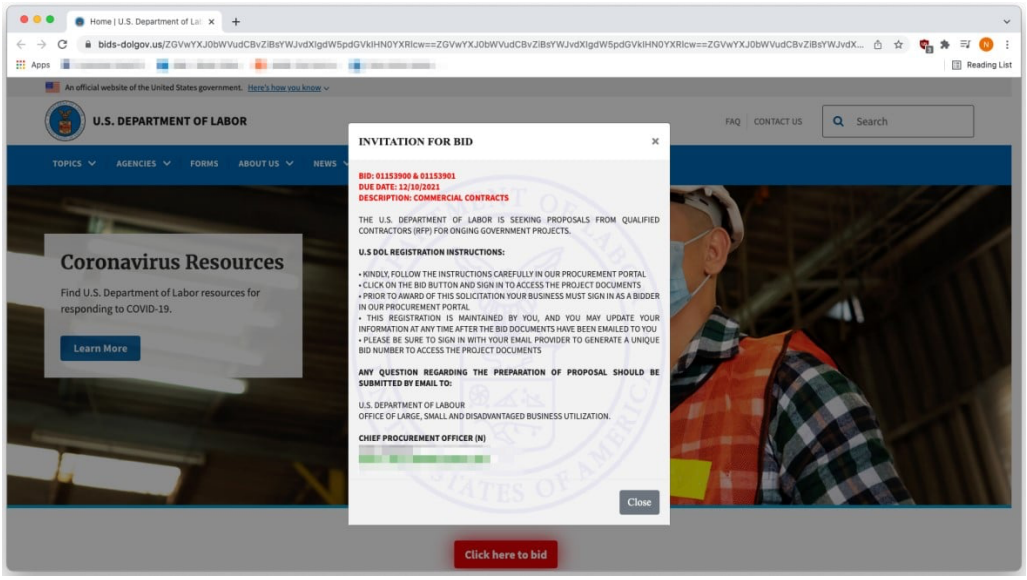
The U.S. Department of Labor is seeking proposals from qualifed contractors (RFP) for ongoing government projects.
U.S DOL Registration Instructions:
. Kindly download the attached bid document and follow the instructions carefully to access our Procurement portal
. Click on the "BID" button on the bid 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)

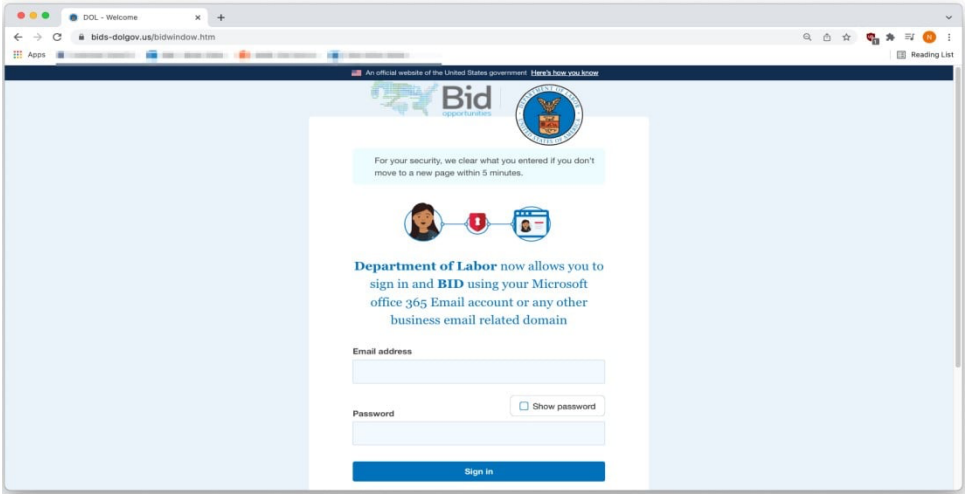
Email template utilized by the attackers.



Malicious PDF with the BID button leading the attack flow included in the email.



Landing page with pop-up notification for the BID invitation to increase credibility.



Malicious replica of the official DoL login as the credential harvesting page.

Recommendations

Phishing involving ruses with government agencies due to their credibility and believability still remains a strong threat against the community. At an organizational level, there are certain measures to be taken and implemented at a regular cadence through people, processes and procedures. Since humane mistakes such as clicking a seemingly reliable link is at the heart of phishing ruses, enterprise administrators and security professionals within the organization must lean on a tight cadence of phishing training courses including modern, specialized ruses that could have been used in the past as well to better articulate lessons learned. These training courses need to be tailored towards different positions, i.e. executives and regular employees should have differing difficulties in training. The training should also aim to teach that official US government domains usually only end in **.gov** and **.mil** rather than **.com**, and federal organizations will usually not send cold emails to solicit bids or other projects.

For technical precautions, employing an organization-wide antivirus software with regular and wide-cast scanning will help identify indicators of compromise. An organization-wide zero-trust policy should be prioritized, which emphasizes the principle of applying thorough identity verification no matter what user, device or resource needs to access organization internals.

Additionally, robust email spam filtering should be employed. SMTP servers should also not be configured to accept and forward emails from non-local IP addresses to non-local mailboxes by unauthenticated and unauthorized users, and mailbox administrators should pay careful attention to this. **[3]** 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.

As mentioned in the referenced article **[5],** 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). **[5]**

To further protect users, URL analysis tools can be implemented to evaluate the safety of links within emails and other communications in real-time. These tools can block or flag suspicious links, reducing the likelihood that employees will click on harmful URLs embedded in phishing emails. By combining these technical defenses such as robust email filtering, and URL analysis tools with regular training, organizations can create a resilient, multi-layered defense against phishing attacks.

Conclusion

This particularly constructed phishing attack that targeted the Department of Labor, underscored the growing sophistication of phishing schemes, especially those leveraging government official impersonation tactics and seemingly official attachments to gain credibility. As a result of these successful campaigns, attackers compromised numerous Office 365 credentials in an undetected fashion until it was too late to prevent. As cybercriminals keep on refining their tactics and evolving with the nature of the environment, organizations and employees should remain vigilant and trained, investing in regular cybersecurity awareness and best practices training. Implementing a zero-tolerance policy and social engineering training within all members of the organization will prove to be crucial in protecting data and sensitive information disclosures. Organizations should take robust technical security measures to secure their email configuration and block incoming phishing attempts.

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