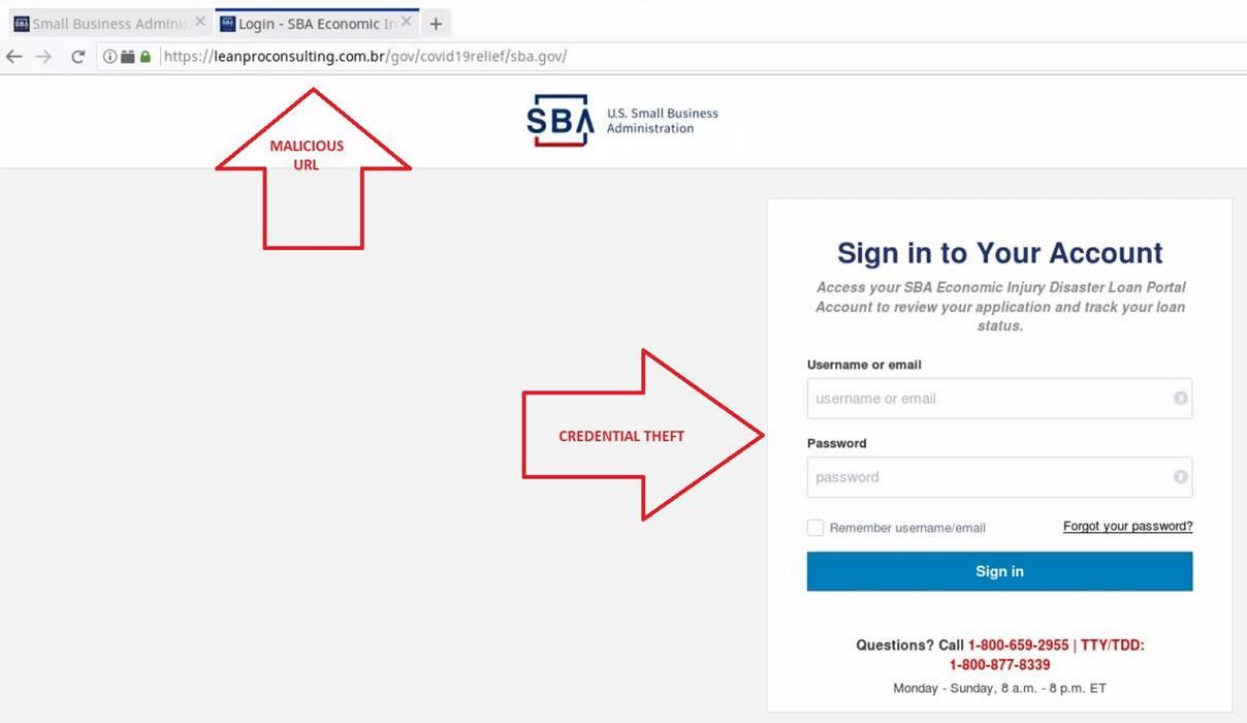
Threat Actors Spoofing COVID-19 Loan Relief Webpages



Summary

In an alert (AA20-225A), the Cybersecurity and Infrastructure Security Agency (CISA) warns of an unknown malicious threat actor spoofing a COVID-19 loan relief webpage.

Threat Type

- Phishing

Overview

CISA has issued an alert (AA20-225A) warning of an unknown threat actor spoofing the Small Business Administration's COVID-19 loan relief webpage. Using phishing emails, the actor includes a link to the spoofed webpage which is actually used for credential theft and malicious redirects. Analysts have stated the emails target Federal Civilian Executive Branch and state, local, tribal, and territorial government recipients. Upon clicking the link, victims are prompted to enter their SBA Economic Injury Disaster Loan Portal Account information to review application and check on loan status. Further information can be found in the alert located within the Reference section below.

Indicators of Compromise

- A complete list of IoCs can be found in the Reports section to the right.

Recommendations

- Ensure anti-virus software and associated files are up to date.
- Search for existing signs of the indicated IoCs in your environment.
- Consider blocking and or setting up detection for all URL and IP based IoCs.
- Keep applications and operating systems running at the current released patch level.
- Exercise caution with attachments and links in emails.

Mitigations

CISA recommends using the following best practices to strengthen the security posture of an organization's systems. System owners and administrators should review any configuration change prior to implementation to avoid unwanted impacts.

- Include warning banners for all email’s external to the organization.
- Maintain up-to-date antivirus signatures and engines. See Protecting Against Malicious Code.
- Ensure systems have the latest security updates. See Understanding Patches and Software Updates.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' permissions to install and run unwanted software applications. Do not add users to the local administrators’ group unless required.
- Enforce a strong password policy. See Choosing and Protecting Passwords.
- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known. See Using Caution with Email Attachments.
- Enable a personal firewall on agency workstations that is configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs). Sign up to receive CISA’s alerts on security topics and threats.

- Sign up for CISA's free vulnerability scanning and testing services to help organizations secure internet-facing systems from weak configuration and known vulnerabilities. Email vulnerability_info@cisa.dhs.gov

- to sign up. See https://www.cisa.gov/cyber-resource-hub for more information about vulnerability scanning and other CISA cybersecurity assessment services.

References:

- https://us-cert.cisa.gov/ncas/alerts/aa20-225a
- https://www.cyber.nj.gov/alerts-advisories/malicious-cyber-actor-spoofing-covid-19-loan-relief-webpage