TLP:WHITE

Alert (AA20-225A)

More Alerts

Malicious Cyber Actor Spoofing COVID-19 Loan Relief Webpage via Phishing Emails

Original release date: August 12, 2020

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is currently tracking an unknown malicious cyber actor who is spoofing the Small Business Administration (SBA) COVID-19 loan relief webpage via phishing emails. These emails include a malicious link to the spoofed SBA website that the cyber actor is using for malicious re-directs and credential stealing.

For a downloadable copy of IOCs, see STIX file.

Technical Details

CISA analysts observed an unknown malicious cyber actor sending a phishing email to various Federal Civilian Executive Branch and state, local, tribal, and territorial government recipients. The phishing email contains:

- A subject line, **SBA Application – Review and Proceed**
- A sender, marked as **disastercustomerservice@sba[.]gov**
- Text in the email body urging the recipient to click on a hyperlink to address: `hxxps://leanproconsulting[.]com.br/gov/covid19relief/sba.gov`
- The domain resolves to IP address: `162.214.104[.]246`

Figure 1 is a screenshot of the webpage arrived at by clicking on the hyperlink.

TLP:WHITE

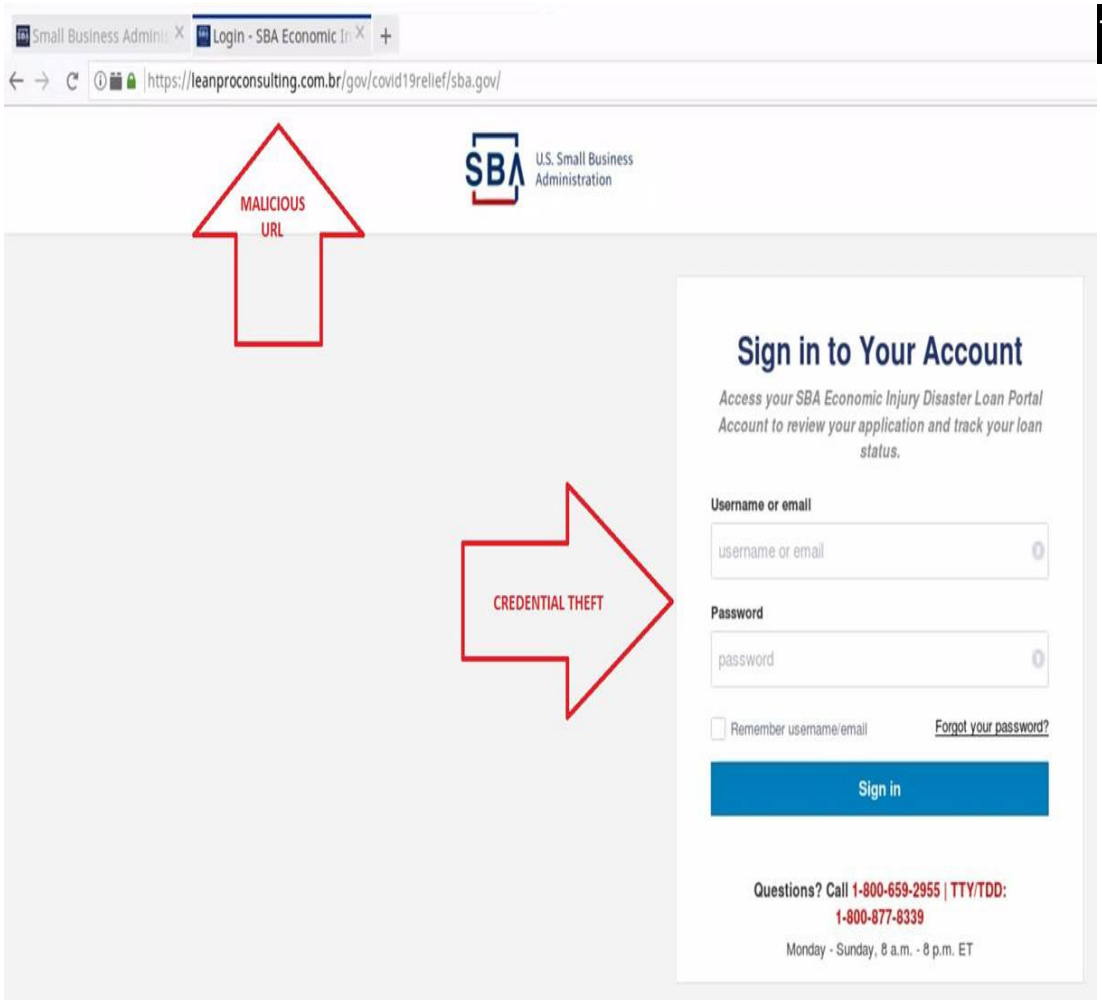

Figure 1: Webpage arrived at via malicious hyperlink.

Indicators of Compromise

CISA observed the following additional indicators of compromise.

162[.]214[.]104[.]246
152[.]199[.]21[.]175
13[.]86[.]113[.]170
13[.]69[.]66[.]140
52[.]129[.]92[.]13
185[.]60[.]217[.]28
23.63.253[.]11
192.64.119[.]222
142[.]11[.]196[.]128
admin@columbiadb[.]com
disastercustomerservice@sba-gov-us[.]xyz
leanproconsulting[.]com[.]br
ci-mpsnare[.]iovation[.]com

TLP:WHITE

www[.]leanproconsulting[.]com[.]br
dc[.]services[.]visualstudio[.]com
scontent-ber1-1[.]xx[.]fbcdn[.]net
isrg.trustid.ocsp[.]identrust[.]com
www.sba-gov-us[.]xyz
hxxp://www[.]leanproconsulting[.]com[.]br/wp-content/uploads/2018/08/Lean-Pro-Consulting_2018v3[.]png
hxxp://www[.]leanproconsulting[.]com[.]br/wp-content/uploads/2018/08/Consultorias_lean[.]gif
hxxp://www[.]leanproconsulting[.]com[.]br/wp-content/uploads/2018/08/Treinamentos_Lean[.]gif
hxxp://www[.]leanproconsulting[.]com[.]br/wp-content/uploads/2018/08/Auditorias_lean[.]gif
1d38c3dcc5f78b571df164d28689029380dec30c
e9ea1de80c556afcb17f3597018901965b0a0d4d5bed9bf8c44ab5831276d624
3fa4912eb43fc304652d7b01f118589259861e2d628fa7c86193e54d5f987670
8abc7daa81c8a20bfd88b6a60ecc9ed1292fbb6cedbd6f872f36512d9a194bba
20082887a470f83d94ff7ff32311f574

For a downloadable copy of IOCs, see STIX file.

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 emails 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.

TLP:WHITE

- 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.

Resources

- CISA Binding Operational Directive 18-01
- CISA Insights: Enhance Email and Web Security
- CISA Tip: Using Caution with Email Attachments
- CISA Alert (AA20-099A): COVID-19 Exploited by Malicious Cyber Actors
- CISA Tip: Avoiding Social Engineering and Phishing Attacks
- VirusTotal

Revisions

August 12, 2020: Initial Version