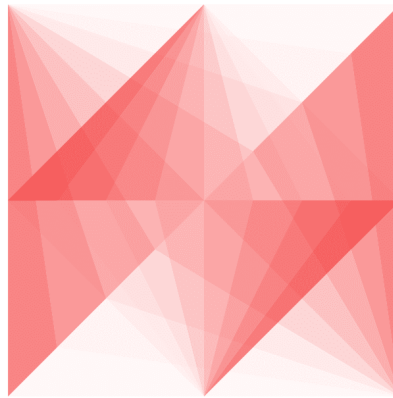


What Service NSW has to do with Russia?

 osint.fans/service-nsw-russia-association

Gabor Szathmari

September 22, 2020



OSINT Fans

22 Sep 2020 • Posted by Gabor Szathmari

3 min read

One interesting offshoot of researching [.gov.au websites running outside Australia](#) was an odd service running from Russia. How the Service NSW – a website offering government services online – ended up associating with a Russian datacentre?

[According to this Shodan query](#), the domain name `mta.comms.service.nsw.gov.au` (an email server belonging to Service NSW) appear to be hosted on the IP address

`82.202.226.62` .


Shodan Developers Monitor View All... Show API Key Try out the new beta website!

SHODAN hostname:gov.au -country:AU country:"RU" Q Home Explore Downloads Reports Pricing Enterprise Access

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
6

TOP COUNTRIES



Russian Federation 6

TOP SERVICES

| | |
|-------------|---|
| FTP | 1 |
| DNS | 1 |
| HTTP | 1 |
| MySQL | 1 |
| HTTP (8080) | 1 |

TOP ORGANIZATIONS

| | |
|-----------------------------|---|
| OOO Network of data-cent... | 6 |
|-----------------------------|---|

TOP PRODUCTS

| | |
|--------------|---|
| Apache httpd | 2 |
| MySQL | 1 |
| nginx | 1 |

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

82.202.226.62
mta.comms.service.nsw.gov.au
OOO Network of data-centers Selectel
Added on 2020-08-22 20:57:45 GMT
Russia

```

220 (vsFTPd 3.0.3)
530 Login incorrect.
530 Please login with USER and PASS.
211-Features:
EPRT
EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
211 End

```

82.202.226.62 [🔗](#)
mta.comms.service.nsw.gov.au
OOO Network of data-centers Selectel
Added on 2020-09-10 04:42:04 GMT
Russia

```

HTTP/1.1 301 Moved Permanently
Date: Thu, 10 Sep 2020 04:42:02 GMT
Server: Apache/2.4.25 (Debian) mod_fcgid/2.3.9 OpenSSL/1.0.2u
X-Redirect-By: WordPress
Location: http://xn--e1afaigh5dwd.xn--p1ai/
Content-Length: 3
Connection: close
Content-Type: text/html; charset=UTF-8

```

82.202.226.62 [🔗](#)
mta.comms.service.nsw.gov.au
OOO Network of data-centers Selectel
Added on 2020-09-10 04:42:04 GMT
Russia

```

HTTP/1.1 301 Moved Permanently

```

Six Australian Government-related services appear to be running from ... Russia?
The GeolIP database shows that this IP (82.202.226.62) belongs to Selectel, an IT company with six data centres in Moscow and St. Petersburg.

What is going on here?

Before anyone gets excited, **there is no direct association between Service NSW and Russia**. The reality is more boring, but with a clever twist.

Links to banking malware

According to [Hybrid Analysis](#) report from earlier, the IP address **82.202.226.62** was associated with a phishing campaign.

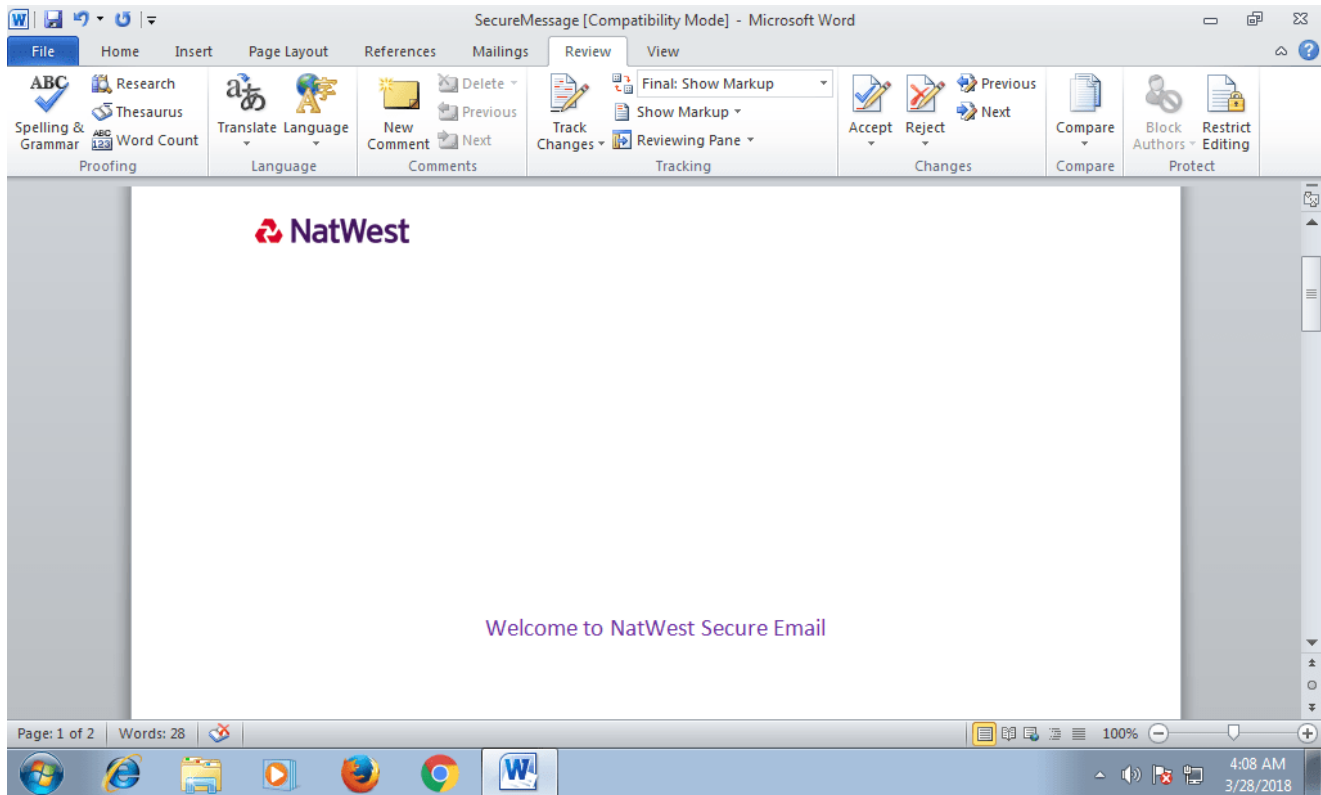
The screenshot shows the Hybrid Analysis web interface. At the top, there is a search bar with the text "IP, Domain, Hash...". Below the search bar, there is a table titled "Login to Download Contacted Hosts (CSV)". The table has four columns: "IP Address", "Port/Protocol", "Associated Process", and "Details".

| IP Address | Port/Protocol | Associated Process | Details |
|-------------------------|---------------|-----------------------------|--------------------|
| 202.218.252.73 OSINT | 80 TCP | powershell.exe PID: 3688 | Japan |
| 216.239.34.21 | 80 TCP | dkgw.exe PID: 3644 | United States |
| 82.214.141.134 | 449 TCP | dkgw.exe PID: 3644 | Poland |
| 82.202.226.62 | 447 TCP | dkgw.exe PID: 3644 | Russian Federation |
| 31.134.60.181 | 449 TCP | dkgw.exe PID: 3644 | Poland |

Below the table, there is a section titled "Contacted Countries" with a world map. The map shows several countries highlighted in blue, including the United States, Japan, Poland, and the Russian Federation. Blue lines connect these countries, indicating network connections between them.

On the right side of the interface, there is a sidebar with various navigation options: Incident Response, Indicators, File Details, Screenshots (8), Hybrid Analysis (8), Network Analysis (4), DNS Requests (4), Contacted Hosts (5), Contacted Countries, HTTP Traffic (2), Suricata Alerts (5), Extracted Strings, Extracted Files (14), Notifications, Community (1), and Back to top.

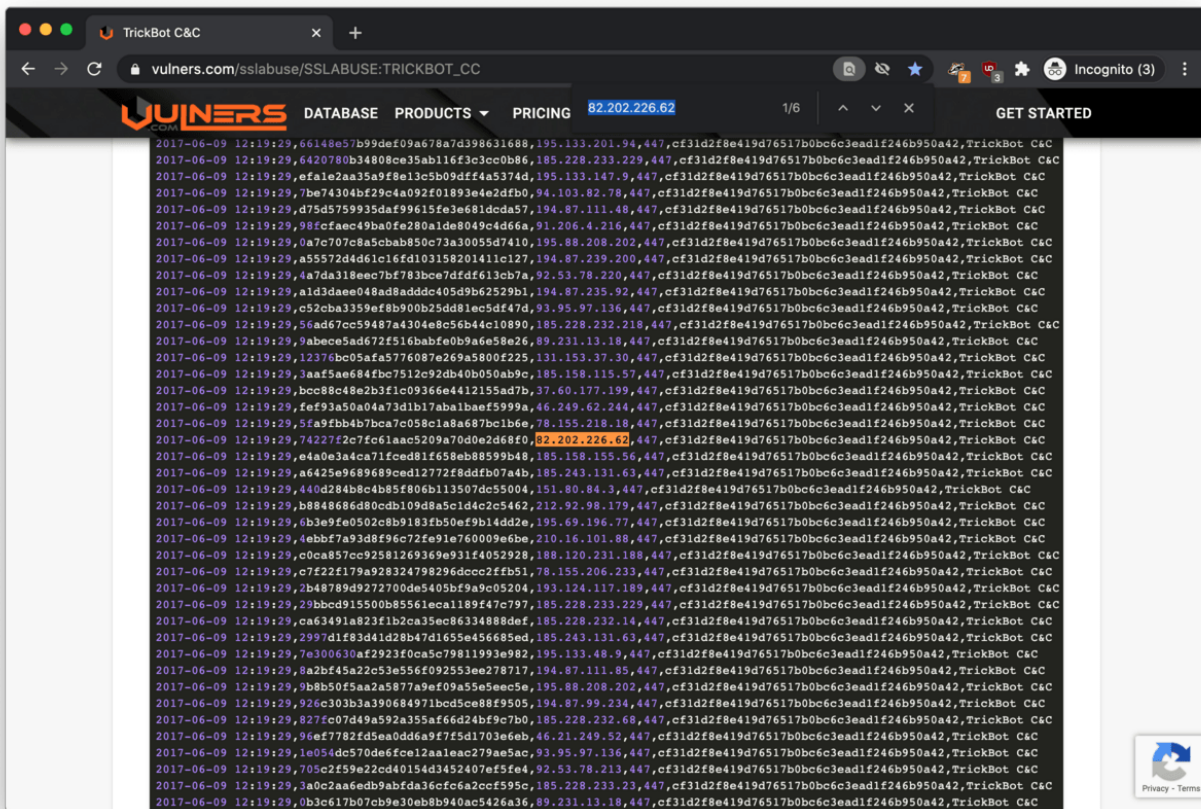
A malware analysis of a phishing campaign shows the IP is associated with malware. The phishing campaign featured a Word document with a malicious payload trying to download a banking trojan on the victims' computer. The screenshots of this Word document with the malicious payload indicate that the campaign was targeting NatWest (UK bank) customers.



The phishing campaign was targeting NatWest Bank customers in the UK.

An additional search reveals that the Russian IP address is (was) associated with a banking trojan called Trickbot. This piece of malicious software was developed in 2016 with the sole purpose of stealing from bank accounts, Bitcoin wallets and downloading other harmful code to the victims' PC.

According to Vulners, the IP (82.202.226.62) appears to be a 'Command and Control' (C2) server, which is an important network infrastructure element to control and operate the botnet.



Vulners.com confirms that the Russian IP address was associated with the Trickbot baking trojan.

How Trickbot is related to Service NSW?

The last remaining question is, what Trickbot has to do with the NSW Government? If we do a reverse DNS lookup on [82.202.226.62](https://www.vulners.com/sslabuse/SSLABUSE:TRICKBOT_CC), it resolves to

[mta.comms.service.nsw.gov.au](https://www.vulners.com/sslabuse/SSLABUSE:TRICKBOT_CC).

Network Tools: DNS,IP,Email x +

mxtoolbox.com/SuperTool.aspx?action=ptr:82.202.226.62&newAppVersion=1

MX TOOLBOX® Pricing Tools Delivery Center Monitoring Products Support Login

SuperTool MX Lookup Blacklists DMARC Diagnostics Domain Health DNS Lookup Analyze Headers All Tools

SuperTool Beta7

82.202.226.62 Reverse Lookup

ptr:82.202.226.62 Find Problems ptr

| Type | IP Address | Domain Name | TTL |
|------|--|------------------------------|--------|
| PTR | 82.202.226.62 OOO "Network of data-centers "Selectel" (AS50340) | mta.comms.service.nsw.gov.au | 21 hrs |

| Test | Result |
|------------------------|------------------|
| ✔ DNS Record Published | DNS Record found |

smtp diag blacklist subnet tool dns propagation

Reported by rs2.vscale.io on 9/21/2020 at 8:14:49 PM (UTC -5), just for you. Transcript

ABOUT THE SUPERTOOL!

All of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool. Input a domain name or IP Address or Host Name. Links in the results will guide you to other relevant tools and information. And you'll have a chronological history of your results.

Feedback Contact Terms & Conditions Site Map API Privacy

Your IP is: 103.217.166.56
Phone: (866)-MXTOOLBOX / (866)-698-6652 | feedback@mxtoolbox.com
© Copyright 2004-2020, MXToolBox, Inc. All rights reserved.

Free MxToolBox Account
Get 1 Free Monitor*, Email Notifications and Troubleshooting Info

Delivery Center
Real-time insight into the Email Deliverability of you or your 3rd party senders

Blacklist Monitoring
100+ Blacklist Monitored + Delisting Support

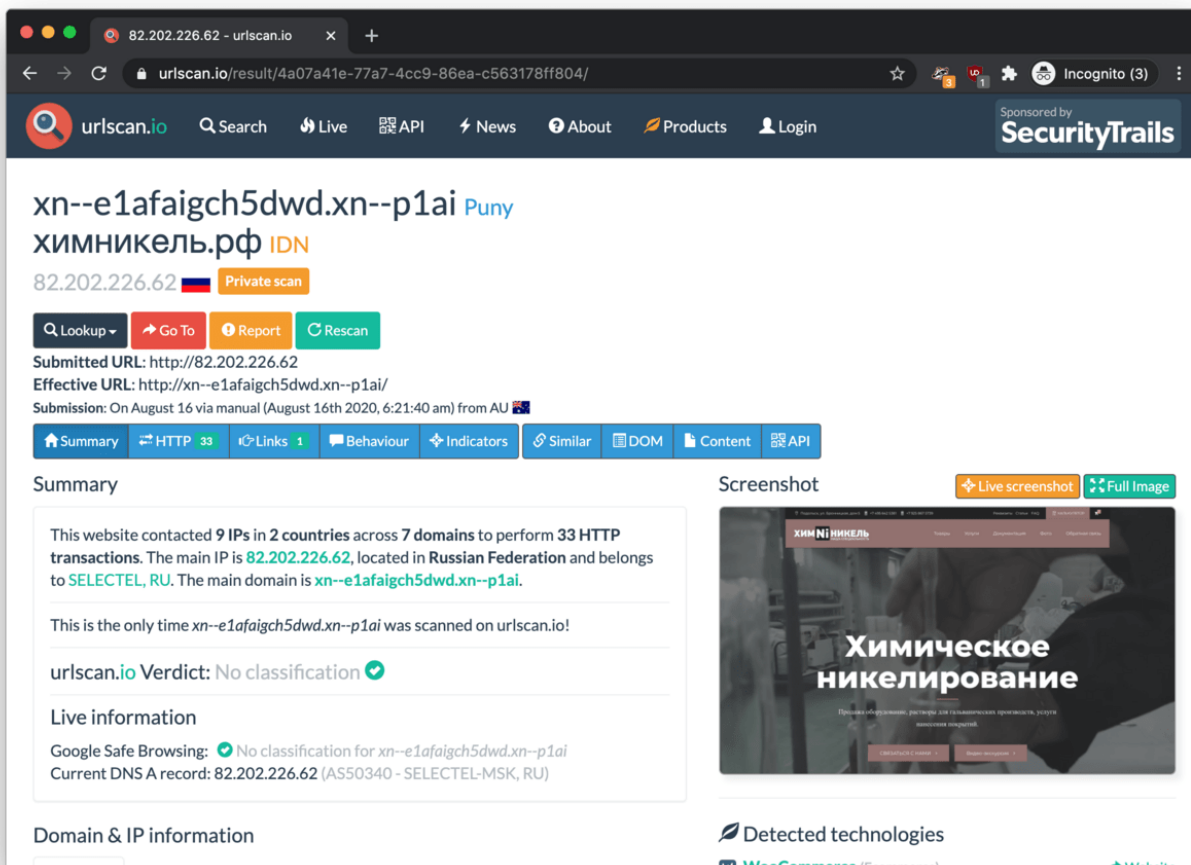
MailFlow Monitoring
Round-trip email server monitoring for latency and email deliverability issues

Bulk Lookup
Run Bulk lists of IPs and Domains Blacklist, MX/NS/A Record, GeolIP, & more data

A reverse DNS lookup shows that the Russian IP resolves to a Service NSW domain name. The answer is that it is a clever attempt to disguise any communication between the infected PCs and the Trickbot C2 server (82.202.226.62) on corporate networks.

Big companies usually monitor and log network traffic originating from their internal network. If a security analyst drills into the network logs to identify covert communication channels between the corporate network and C2 servers on the Internet, a reverse DNS lookup on **82.202.226.62** will result in the innocuous-looking domain name **mta.comms.service.nsw.gov.au** seemingly belonging to a government-run website.

As DNS records for reverse DNS lookups are managed by the hosting provider (Selectel in this case), the malware operator may choose any arbitrary hostname to deceive security analysts.



The website on the Russian IP address was likely to be hacked and turned into a C2 server. This is confirmed when we visit <http://82.202.226.62>. The website on this IP address seems to belong to a chemical company based in Russia. The website is hosted on WordPress, which was likely to be hacked and turned into a Command and Control server for the banking malware.

Conclusion

Security analysis should not always trust reverse DNS lookups when hunting for malware. As this example shows, the operators of Trickbot were actively trying to evade detection by disguising the Command and Control IP address as a legitimate NSW Government service.

What Service NSW can do in this situation is contacting either Selectel or [RU-CERT](#) to have the deceptive reverse DNS record removed.

Related Posts

[Gumtree and Australia Post Credit Card Scam](#)

[fvpn – A self-hosted VPN for OSINT investigations](#)

[Full Address Search with the Unclaimed Money Portal](#)

[Bulletproftlink - A phishing service from Malaysia \(Part 3\)](#)

[BulletProftLink - A phishing service from Malaysia \(Part 2\)](#)