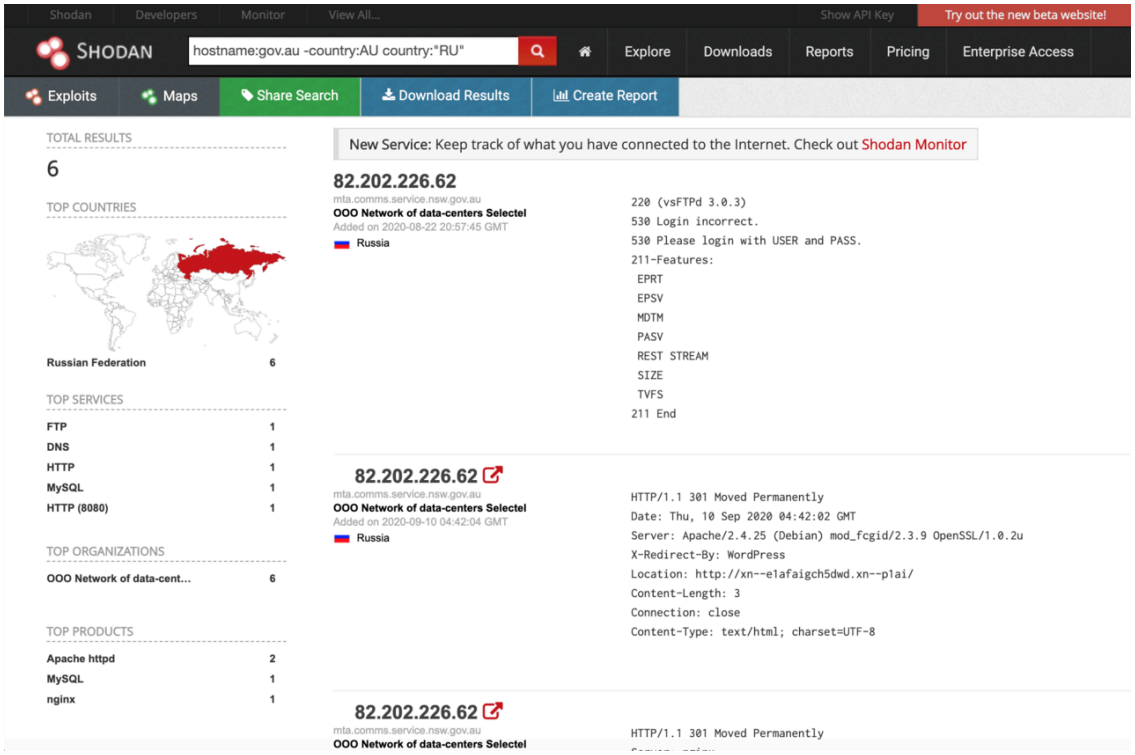
What Service NSW has to do with Russia?

By Hunter22

Published: 2020-09-22 · Archived: 2026-04-05 22:00:44 UTC

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`.



Six Australian Government-related services appear to be running from ... Russia?

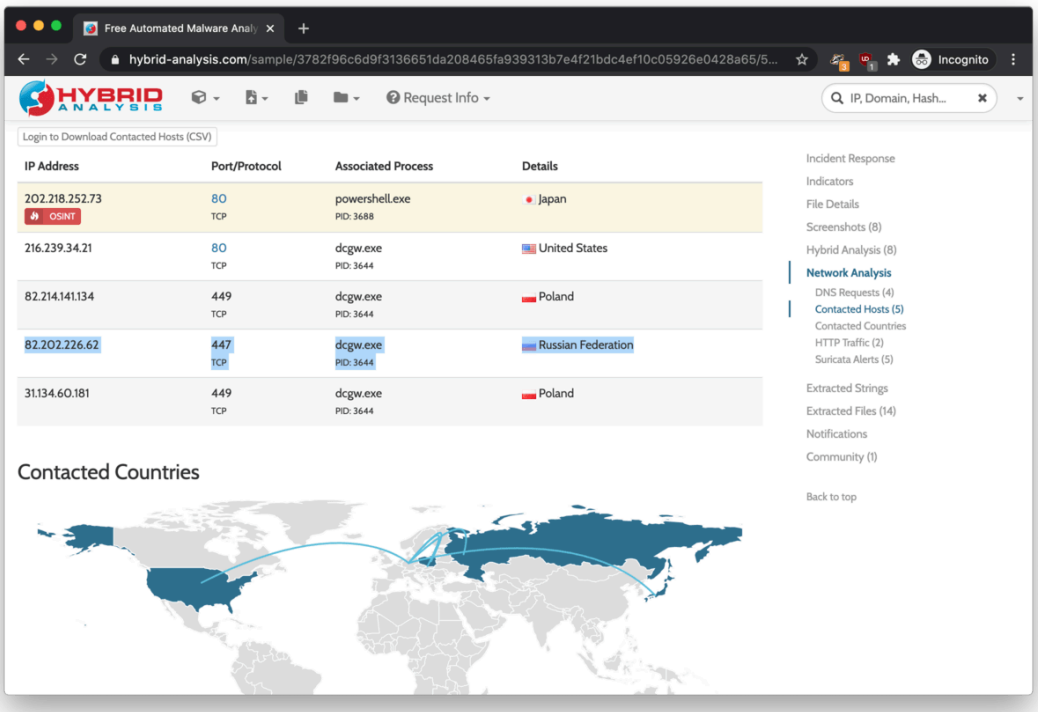
The GeoIP database shows that this IP (82.202.226.62) belongs to Selectel, an IT company with six data centres in Moscow and St. Petersburg.

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.

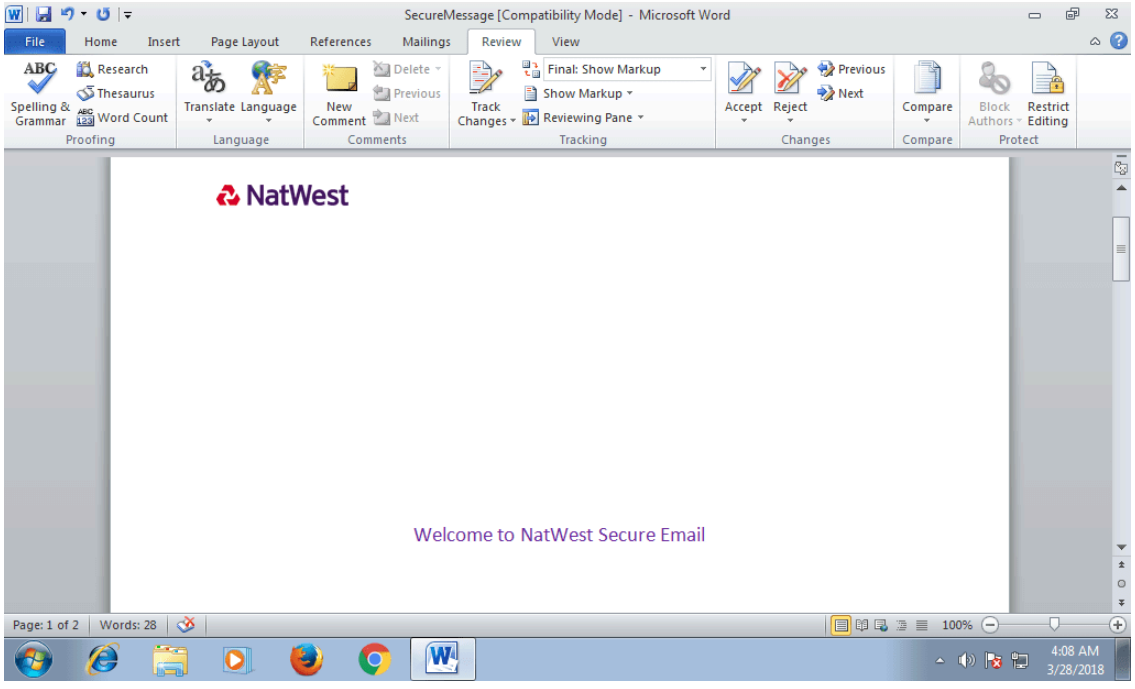
Links to banking malware

According to Hybrid Analysis report from earlier, the IP address `82.202.226.62` was associated with a phishing campaign.



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.

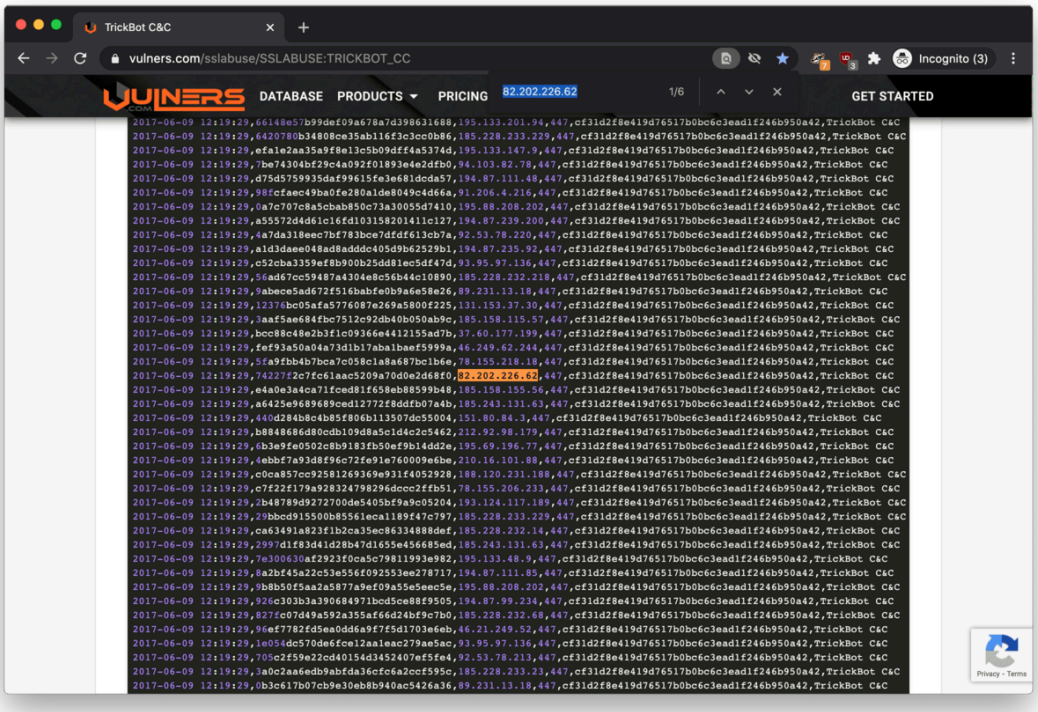


The phishing campaign was targeting NatWest Bank customers in the UK.

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,

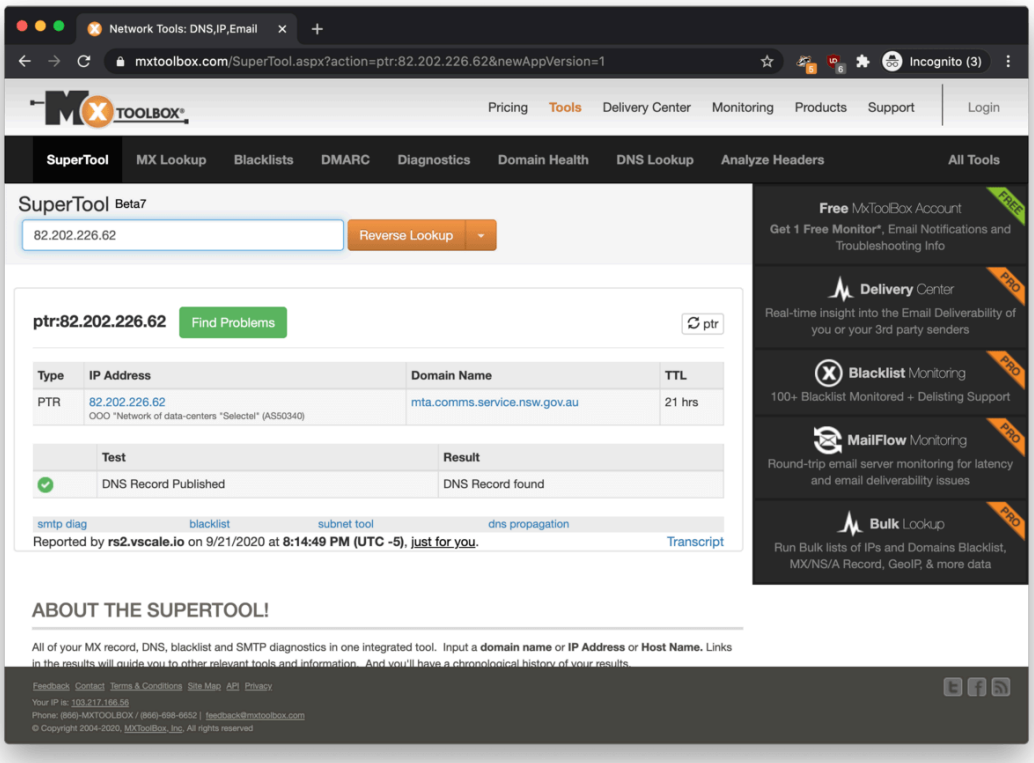
Bitcoin wallets and downloading other harmful code to the victims' PC.

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.

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`, it resolves to `mta.comms.service.nsw.gov.au`.

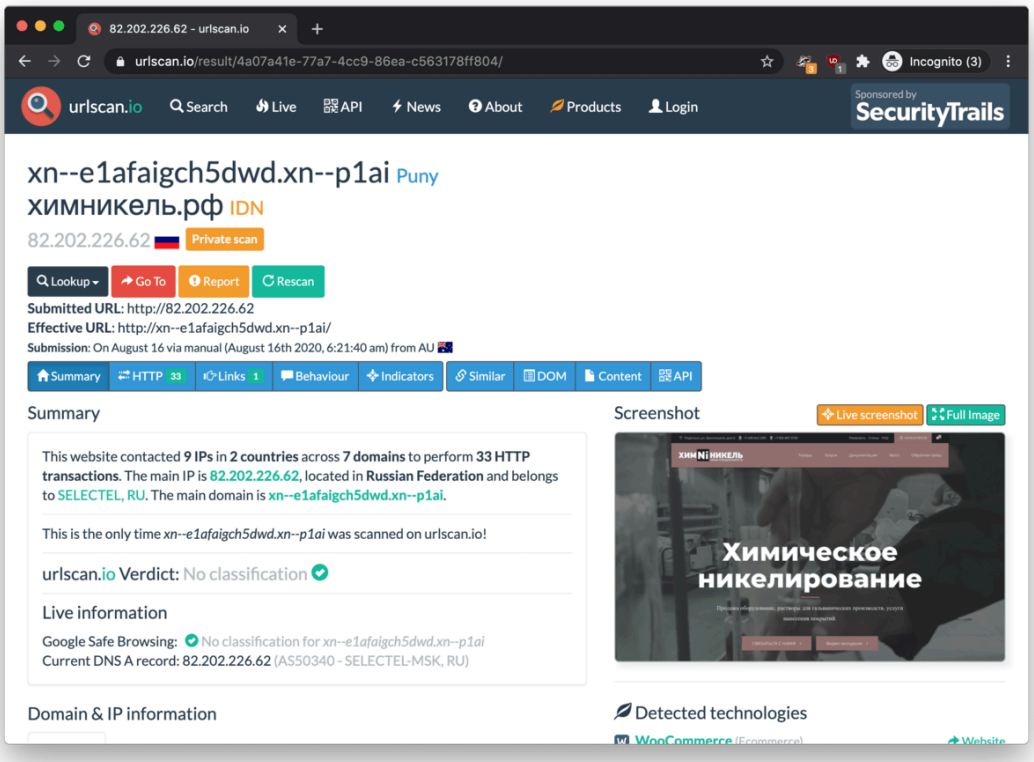


A reverse DNS lookup shows that the Russian IP resolves to a Service NSW domain name.

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.

Source: https://osint.fans/service-nsw-russia-association