proofpoint.

LUMEN iT

Threat Briefing: Australia and New Zealand (October 2019)

Segment title
Threats of Interest to Australia and New Zealand Proofpoint customers

Title
Threat Briefing: Australia and New Zealand (October 2019)

Key findings

- Over 50 malicious email campaigns specifically geo-targeted Australia and New Zealand since May of 2019 while over 100 impacted Australia and New Zealand as well as other targets worldwide.
- Emotet, the global malware campaign leader, returned from a third quarter break in September of 2019, and fully resumed campaigns on a global and regional basis within the Australia and New Zealand geography.
- The second-highest volume malware strains appearing in Australia and New Zealand via email were the Ursnif banking Trojan, followed by Danabot, which was first in the region (https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0).
- Australia and New Zealand threats also include the types of impostor attacks (including business email compromise or BEC) and phishing attacks that affect organizations worldwide.

What's new:

- Emotet is by far the global volume leader. No longer merely a banking Trojan, Emotet is a full-featured botnet, frequently downloading secondary payloads (most often banking Trojans, but potentially any malware), sending spam, potentially conducting DDoS attacks, and much more.
- This is part of a larger trend towards the widespread installation of robust malware like RATs and botnets, creating concerns about the future ways in which threat actors will leverage these large installations. Emotet is interesting because it is usually delivered in high volume campaigns that target geographies with regionally specific lures.
- Similarly, Ursnif and Danabot are robust bankers with global footprints that also appear in regionally targeted campaigns

Implications
Although many campaigns that affect Australia and New Zealand resemble trends in the global threat landscape, high proportions of both Ursnif and Danabot (originally discovered by Proofpoint in Australia) set the region apart somewhat from North America and Europe where threats tend to be a bit more varied. Geo-targeted Emotet campaigns affecting the region specifically were common before the apparent summer hiatus and then resumed in September.

Similarly, differences in email fraud attacks between Australia /New Zealand and the rest of the world suggest that threat actors are tailoring geo targeting strategies to increase success rates in the region, focusing on harder-to-implement (and detect) techniques. The low rates of .co.au and .co.nz New Zealand accounts used for email fraud attacks suggest that threat actors see no need to fraudulently register country-specific domains in a region with strong international ties.

Overview

In the five-month period between May 1, 2019, to October 28, 2019, threat actors conducted hundreds of malicious email campaigns, dozens of which affected organizations in Australia and New Zealand. Over 50 campaigns distributed millions of messages that specifically geo-targeted Australia and New Zealand.

In these campaigns, Proofpoint researchers observed the stolen branding of several notable organizations including major shipping providers, government agencies, professional services companies, and more.

Many threats do target Australia and New Zealand specifically, but the region is also frequently included in global or multinational campaigns. These campaigns are typically sent by financially motivated cybercriminals. Overall, the majority of malware being distributed to Australia and New Zealand affects banking and financial services most directly.

Below is a brief overview of high-risk malware payloads that target Australia and New Zealand organizations.

Emotet

Emotet is a robust global botnet that loads third-party malware and its own modules used for spamming, credential stealing, network spreading, and email harvesting.

Between February 1, 2019, and May 31, 2019, an actor known as “TA542” launched over 40 high-volume campaigns impacting Australia and New Zealand (among other countries) that collectively distributed tens of millions of messages targeting all industries. Australia and New Zealand comprise one of the core regions consistently targeted by Emotet (along with Germany, the United States, and Canada).

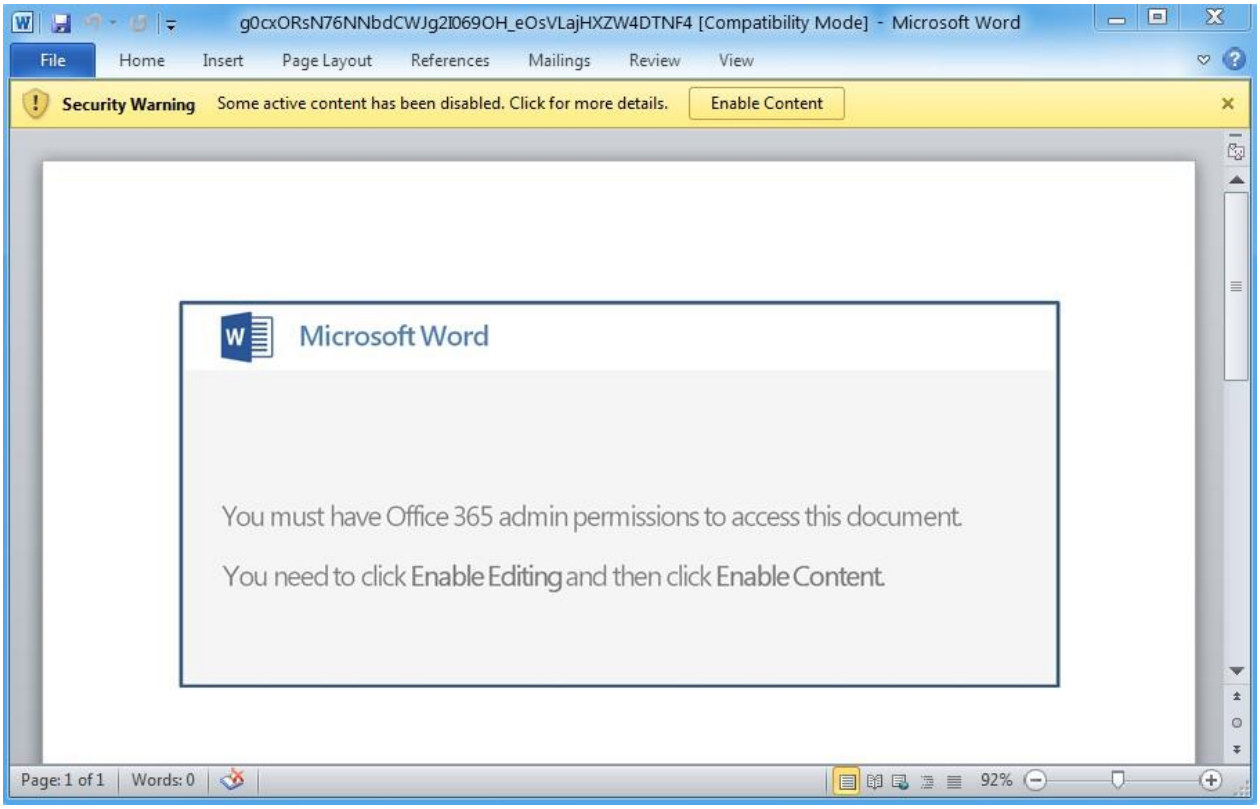

Figure 1: Example Microsoft Word document with macros that, once enabled, install Emotet

The messages most often contained malicious Microsoft Word documents and/or URLs that linked to malicious documents. However, we also observed PDFs with links to Microsoft Word documents with macros, PDFs with links to Zip archives with JScript files inside, password-protected Zip archives with JScript files inside, and URLs linking to Zipped JavaScript. The Word documents contained macros that, when enabled, installed an instance of Emotet. Similarly, the scripts, if executed, downloaded and installed Emotet.

- Also Read: Threat Actor Profile, TA542 from Banker to Malware Distribution Service

During the period of May 31 through the end of August of 2019 no new Emotet campaigns were launched, and the malware was considered to be on hiatus throughout the entire third quarter of 2019. However, the Command and Control (C&C) infrastructure which runs the botnet itself re-awakened at the end of August.

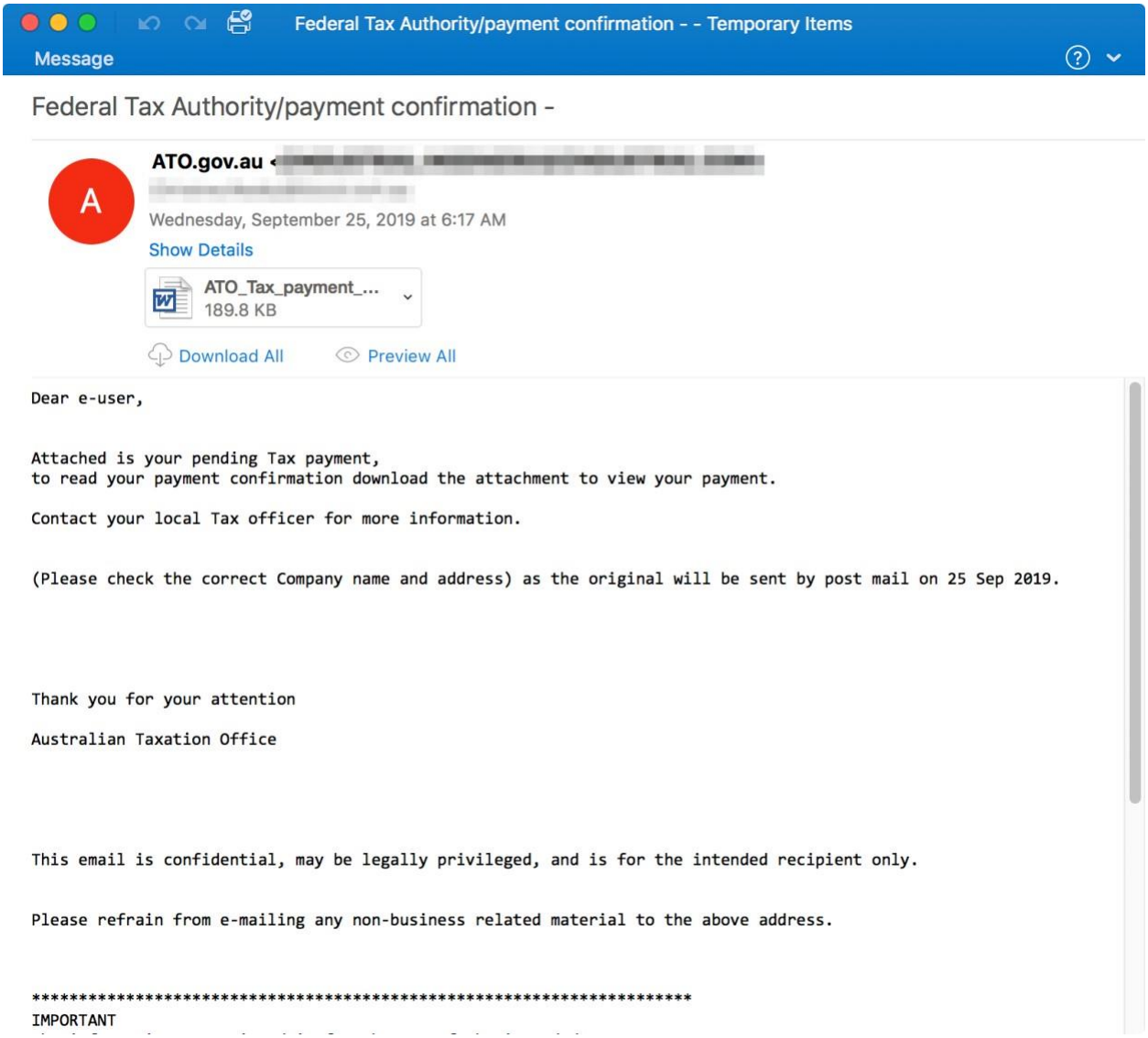

Figure 2: A sample malicious email sent by TA542 using a lure which attempts to impersonate the Australian Taxation Office. The attached Microsoft Word Document that contains macros that, when enabled, download Emotet, which often leads to other secondary payloads.

On September 19, TA542 resumed its attacks in full on a global as well as a regional basis in Australia and New Zealand. As of October 28, over two dozen attacks have been launched that specifically targeted Australia and New Zealand since the Emotet botnet resumed operations.

As with previous campaigns, the attacks consisted of malicious emails containing Microsoft Word and Adobe Acrobat PDF documents as well as URLs which, when opened or clicked on, installs Emotet and other types of malware as secondary payloads, which include “The Trick”, as well as Ursnif (which is less common as a secondary payload but is also frequently deployed as a primary payload in other malicious email campaigns also affecting the region), banking Trojans that are described below.

The Trick

The Trick is a modular banking Trojan that is frequently deployed by Emotet as a secondary payload. The main threat from The Trick is its ability to intercept and log traffic to banking sites. The main bot is responsible for persistence, downloading of additional modules, loading affiliate payloads, and loading updates for the malware.

The Trick initially will attempt to stop any Antivirus-related services using PowerShell. The Trick may load the following modules (32-bit or 64-bit depending on the infected machine & capability; and a domain controller can receive more modules than a regular infection):

- systeminfo: Used to collect system information
- injectDLL: Responsible for injecting browsers and performs the web injection
- bcClientDLL: The backconnect module
- mailsearcher: Module to search the victims email
- NewBCtestnDll64: Known to appear only on Domain Controllers
- bcClientDllTestTest64: Cnown to appear only on Domain Controllers
- pwgrab64: Password grabber, replaced in 2019 with tpwgrabu64
- domainDLL: Collect credentials from Domain Controller
- outlookDLL: Collect Outlook credentials
- importDLL: Collect sensitive browser data
- tabdll: Propagates Trick using EternalRomance exploit
- ShareDLL: Propagates Trick via SMB
- wormDLL: Propagates Trick via SMB
- networkDLL: Collect network and system information

Ursnif

Ursnif is a Trojan that can be used to steal data from users of online banking websites, with the help of web injects, proxies, and VNC (remote access software) connections. It can steal data such as stored passwords as well as download updates, modules, or other malware on the remote client system. Ursnif affects organizations worldwide, but is frequently seen in Australia, Japan, and several European countries.

There are now multiple variants of Ursnif in the wild, following the release of an earlier version’s source code (version 2.13.241). Variants include Dreambot, Gozi ISFB, and Papras.

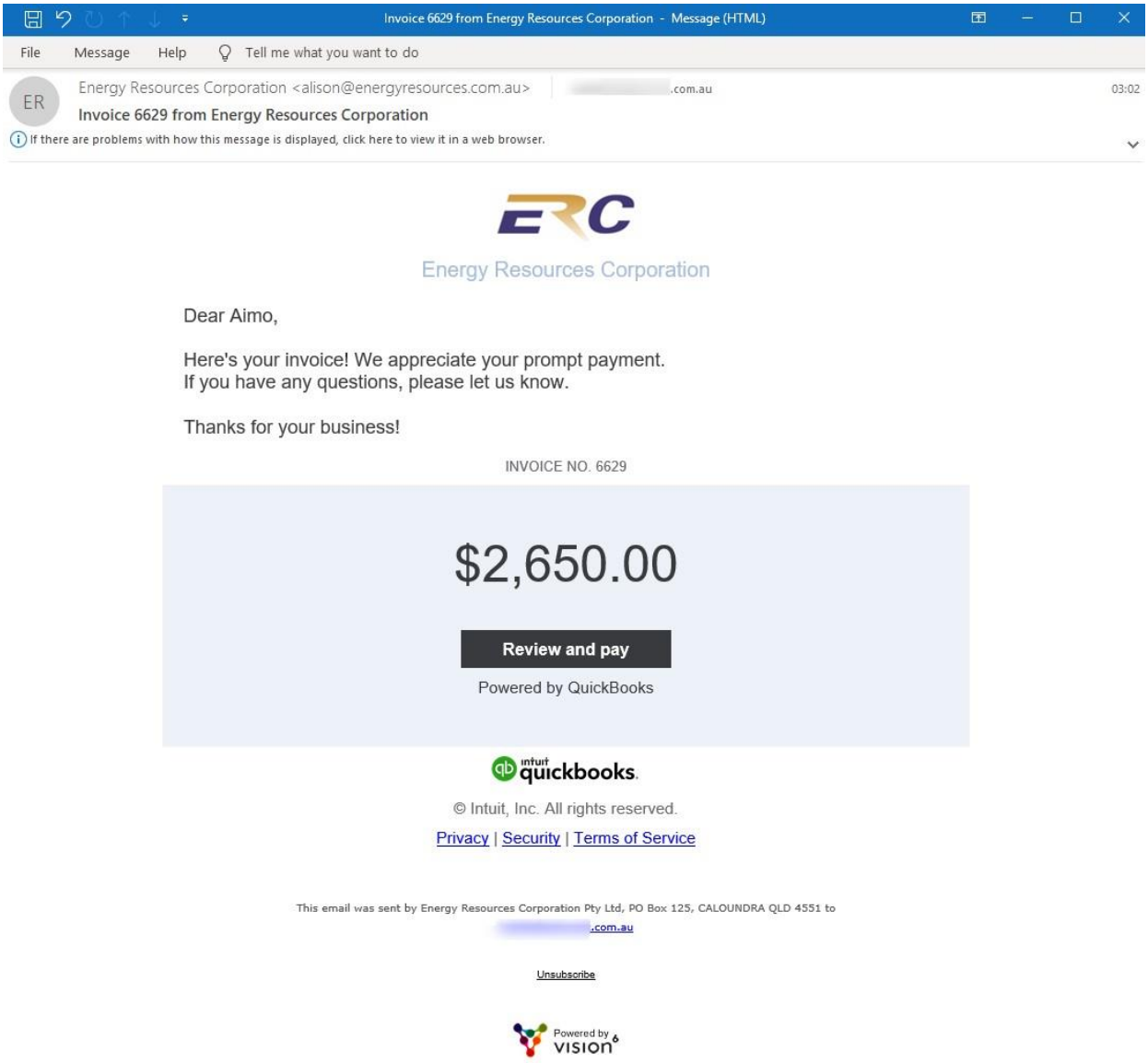

Figure 3: Example email targeting an Australian recipient for a threat actor distributing Ursnif, abusing the branding of a local utility company

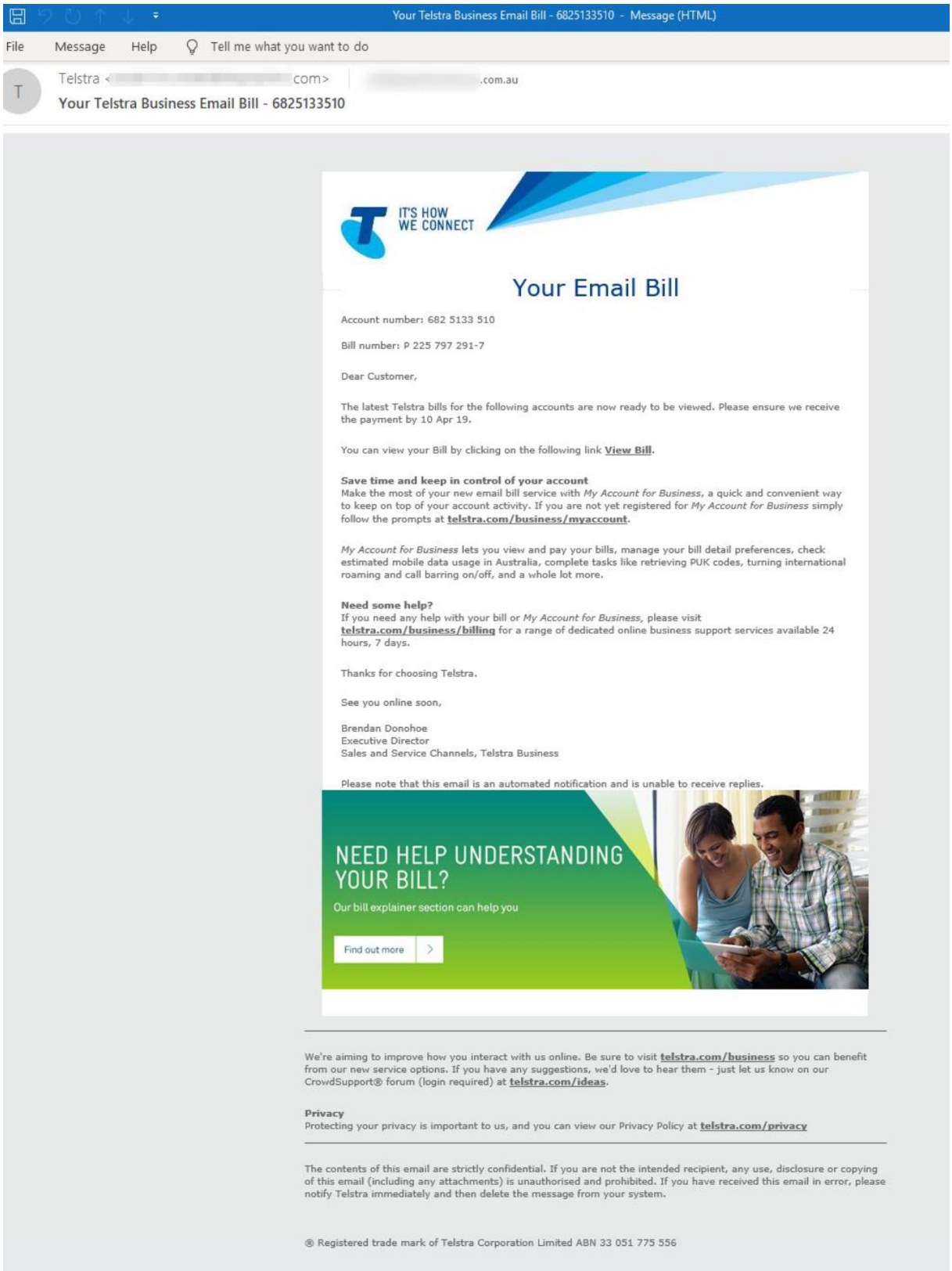

Figure 4: Example email targeting an Australia and New Zealand recipient for a threat actor distributing Ursnif, abusing the branding of regional telecommunications provider, Telstra.

Danabot

Last year saw a marked shift away from high-volume, immediately destructive ransomware campaigns to the distribution of banking Trojans, information stealers, and downloaders. In Q2 2019, banking Trojans made up about a quarter of malicious payloads we observed in email. Danabot, originally discovered in Australian campaigns, adds to the growing diversity of this segment specifically and malicious email campaigns in general.

Danabot generally targets users in Australia via emails containing malicious URLs. Written in Delphi, the malware is still under active development. Danabot now has multiple affiliate IDs, with “Affid 5” primarily associated with attacks targeting Australia. We also found additional samples in malware repositories other than those we observed in the wild, potentially suggesting distribution by other actors.

DanaBot consists of a Downloader component, distributed via URLs embedded in malicious emails, which downloads an encrypted file containing the main DLL.

The DLL, in turn, connects using raw TCP connections to port 443 and downloads additional modules including:

- VNCDLL.dll - "VNC"
- StealerDLL.dll - "Stealer"
- ProxyDLL.dll - "Sniffer"

Together with configuration files including:

- A list of whitelisted sites for the Sniffer module
- Banking web injects
- Lists of CryptoCurrency processes and files to monitor

It also uploads files including:

- Detailed system information
- Screenshot of the user's desktop
- A list of files on the user's hard disk

Figure 5: Example email targeting an Australia and New Zealand recipient for a threat actor distributing Danabot, attempting to mimic communications from local law enforcement.

- Also Read: [DanaBot - A new banking Trojan surfaces own Under]

Vidar

Vidar is a forked version of Arkei Stealer, a credential stealer that is capable of collecting passwords, cookies, auto-filling data from forms, exfiltrating crypto currency wallets, personal files, diagnostics data about the client machine, and inventorying installed software. While it is distributed through multiple vectors, we observed at least one campaign specifically targeting Australia via email.

The malware is written in C++ and appears to have started activities at the beginning of October 2018. Its known features include:

- Searching for specific documents
- Stealing ID from cookie browsers
- Stealing browser histories (also from tor browser)
- Stealing wallets
- Stealing data from 2FA software
- Grabbing message from messenger software
- Screenshot
- Loader settings
- Telegram notifications (on server-side)
- Machine inventory of installed software

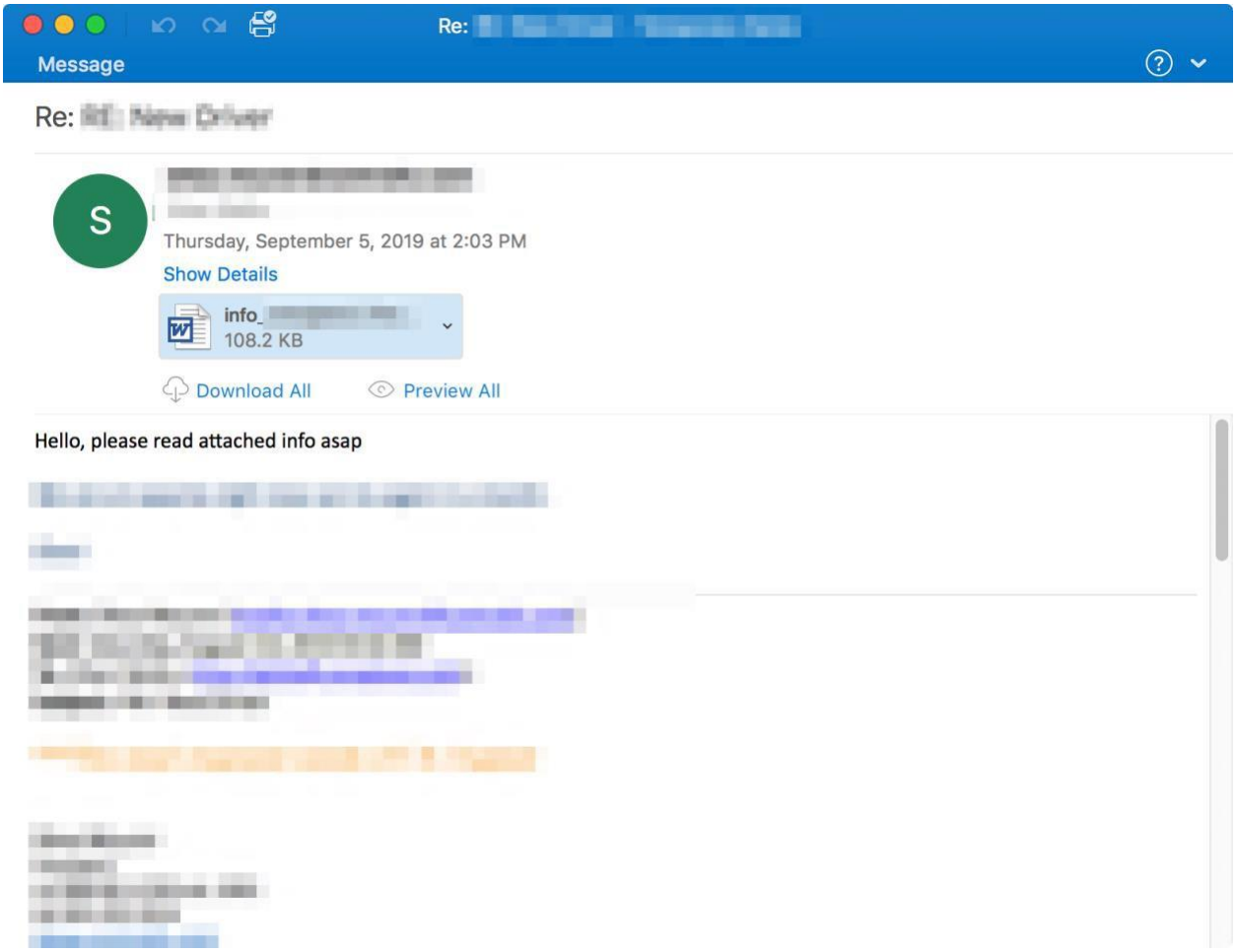

Figure 6: Example email including an attachment with macros that if executed, download and install Vidar.

Human-Centric Threats

While this advisory is focused specifically on malware threats, ubiquitous phishing attacks, business email compromise (BEC), and other forms of imposter attacks remain ongoing threats, both in Australia and New Zealand and internationally. Proofpoint advises vigilance against a range of attacks including:

- Credential Phishing is the most common type of phishing observed by Proofpoint researchers. These emails target a victim's login credentials such as usernames and passwords for a range of sites and services. These campaigns are usually high-volume emails with linked or embedded spoofs of login pages for reputable entities including banks, universities, electronic signature services, and social media and file sharing platforms. Figure 6 shows an example phishing landing page targeting government contractors in Australia, attempting to steal a variety of personal data.

- Malicious emails with the intent of attempting to impersonate a person, commercial entity, or respected brand, such as a bank or an internet service provider. This type of imposter activity could be used for financial fraud, including business email compromise (BEC), in conjunction with other social engineering mechanisms to achieve their desired result, whether delivery of malware, credential phishing, or further network compromise.

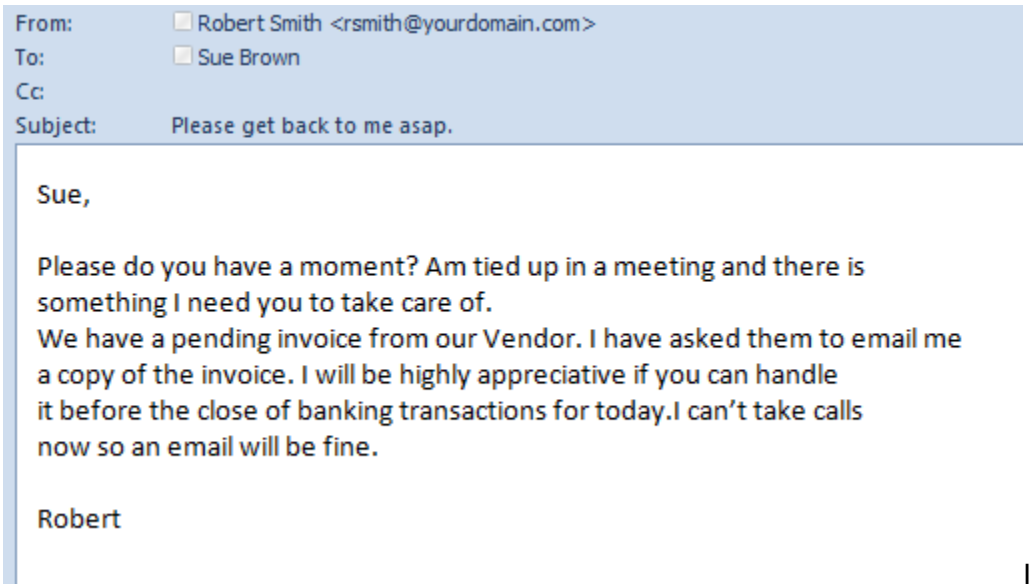

Figure 7: An example of a threat actor engaging in business email compromise (BEC), which is a type of known imposter activity relying on social engineering without any links or attachments leading to malware or phishing kits.

Conclusion

In 2019, threats specific to Australia and New Zealand interests, whether abusing Australia and New Zealand brands or affecting Australia and New Zealand organizations through specific geo-targeting, mean that defenders at companies operating in the region must be cognizant of highly targeted attacks as well as broad-based international attacks. Campaigns delivering banking Trojans and the Emotet botnet (at least until its summer hiatus) lead the pack in Australia and New Zealand, creating risks for organizations and individuals with compelling lures and carefully crafted social engineering. While Australia and New Zealand-targeted threats are not new, Emotet in particular, with its frequent region-specific email campaigns, was bringing new attention to geo-targeting in Australia and New Zealand and beyond through May 2019. Danabot and Ursnif also appeared in high proportions in the region, again creating challenges for defenders looking to prevent the relatively quiet infections from spreading or exfiltrating data.

Similarly, differences in email fraud attacks between Australia and New Zealand and the rest of the world suggest that threat actors are tailoring tactics to increase success rates in the region, focusing on harder-to-implement (and detect) techniques. The low rates of co.au and co.nz accounts used for email fraud attacks suggest that threat actors see no need to fraudulently register country-specific domains in a region with strong international ties.