Beyond “North America” - Threat actors target Canada specifically | Proofpoint US

By May 23, 2019 Proofpoint Threat Insight Team

Published: 2019-05-23 · Archived: 2026-04-05 18:10:39 UTC

Overview

Between January 1, 2019, to May 1, 2019, threat actors conducted thousands of malicious email campaigns, hundreds of which were sent to Canadian organizations. While discussions of threats in this region often focus on “North America” generally or just the United States, nearly 100 campaigns during this period were either specifically targeted at Canadian organizations or were customized for Canadian audiences. Much of this is due to Emotet. TA542, the primary actor behind Emotet, is known for the development of lures and malicious mail specific to given regions. However, we also saw customization ranging from French-language lures to brand abuse from a number of actors geo-targeting Canada.

In these campaigns, Proofpoint researchers observed stolen branding from several notable Canadian companies and agencies including major shipping and logistics organizations, national banks, and large government agencies. Top affected industries in Canada include financial services, energy/utilities, manufacturing, healthcare, and technology.

In addition to campaigns that are specifically geo-targeted at Canada, we frequently observe Canadian organizations being affected by global or multinational campaigns. These campaigns are typically sent by financially motivated cybercriminals, but can also be orchestrated/sent by national, state-sponsored threat actors known as Advanced Persistent Threats (APT). Overall, the majority of malware being distributed to Canadian customers affects banking and financial services most directly.

Below is a brief of high-risk malware payloads that frequently impact Canadian interests.

Emotet

Emotet is a type of general-purpose malware that evolved from a well-known banking Trojan, “Cridex”, which was first discovered in 2014. Originally targeting Western European banks, it has since been developed into a robust global botnet that is comprised of several modules, each of which equips Emotet with different spamming, email logging, information stealing, bank fraud, downloading, and DDoS, among others.

Emotet activity in 2019 included several high-volume campaigns that collectively distributed tens of millions of messages primarily targeting the manufacturing and healthcare industries. Beginning in mid-January 2019, TA542 distributed millions of Emotet-laden emails in both English and German.

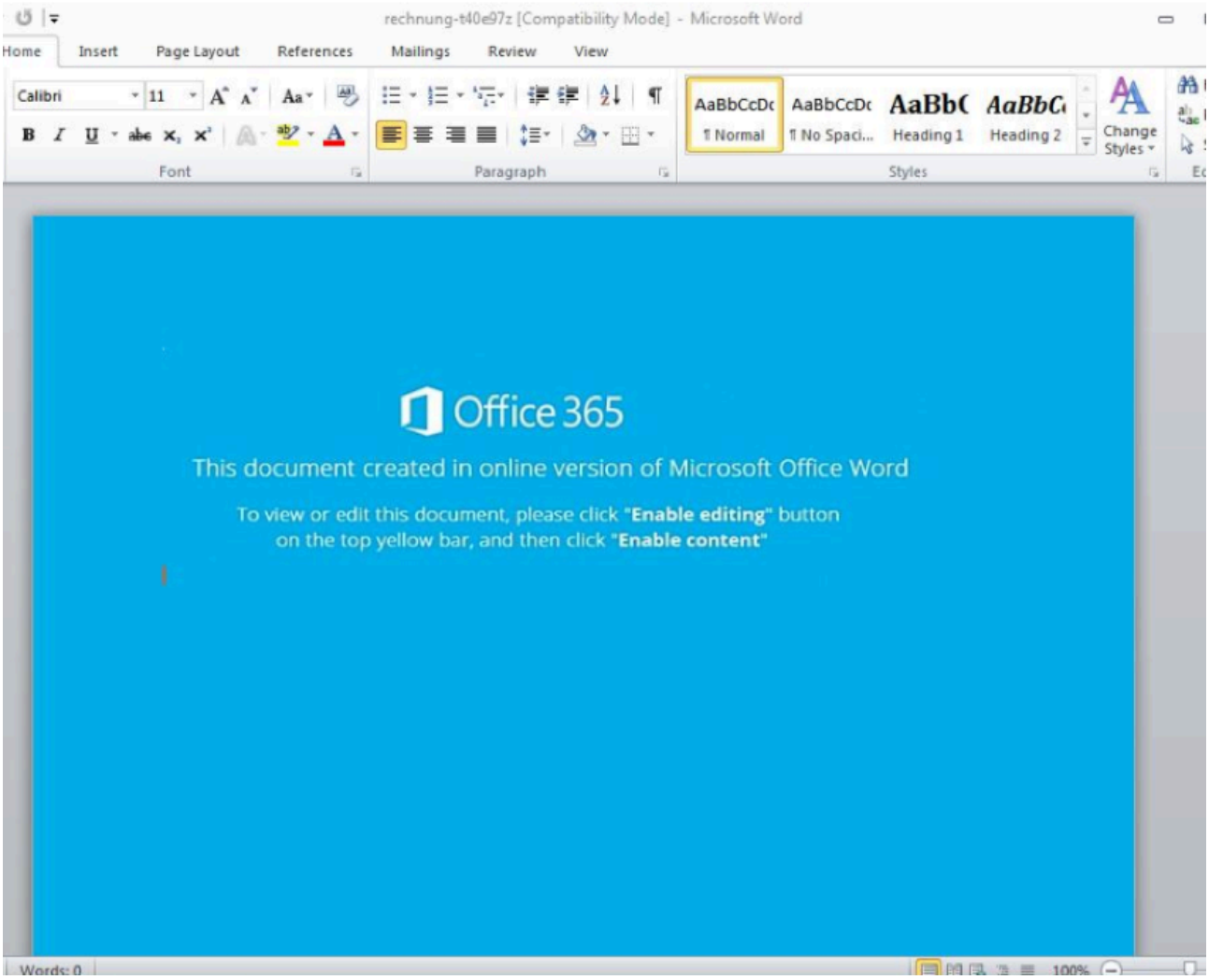


Figure 1: Word Document with macros, that once enabled, install Emotet

The messages were sent with attached malicious Microsoft Word documents and/or URLs that linked to malicious documents. The Word documents contained macros that, when enabled, installed an instance of Emotet. In this particular campaign, TA542 also spoofed Amazon invoices, which included links to malicious Word documents.

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 victim PCs.

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.

Others

While Emotet and Ursnif are the most common threats that geotarget North American countries including Canada, Proofpoint researchers are tracking several other malware strains with significantly smaller footprints that remain noteworthy threats for Canadian organizations. These include:

IcedID

IcedID is a banking Trojan that Proofpoint researchers originally observed being distributed by Emotet in April of 2017. Since then, it has also been distributed by other unaffiliated actors. IcedID is international in scope and affects countries including the US, Canada, Italy, and others.

Between January 1 to May 1, 2019, several IcedID affiliates appeared to target Canadian organizations at higher rates than other geographies.

The Trick

The Trick is a modular banking Trojan. The main bot enables persistent infections, downloading of additional modules, loading affiliate payloads, and loading updates for the malware. The Trick initially will attempt to disable any antivirus-related services by abusing PowerShell.

GandCrab

GandCrab is a type of ransomware that encrypts users' files, typically appending a ".gdcb" extension and leaving a ransom note "GDCB-DECRYPT.txt" in each directory of the client machine's hard disk.

This malware appears to be shared among threat actors using an affiliate business model and is deployed via malicious advertising and malicious email attachments. While ransomware is now relatively rare in email, GandCrab has consistently appeared in email campaigns this year.

GandCrab displays a ransom note instructing the user to visit a payment portal that is located on a TOR ("dark web") site in order to pay the ransom

```
---= GANDCRAB =---
Attention!
All your files documents, photos, databases and other important files are encrypted and have the extension: .GDCB
The only method of recovering files is to purchase a private key. It is on our server and only we can recover your fi
les.
The server with your key is in a closed network TOR. You can get there by the following ways:
1. Download Tor browser - https://www.torproject.org/
2. Install Tor browser
3. Open Tor Browser
4. Open link in tor browser: http://gdcbghvjyqy7jclk.onion/[id]
5. Follow the instructions on this page

If Tor/Tor browser is locked in your country or you can not install it, open one of the following links in your regul
ar browser:
1. http://gdcbghvjyqy7jclk.onion.top/[id]
2. http://gdcbghvjyqy7jclk.onion.casa/[id]
3. http://gdcbghvjyqy7jclk.onion.guide/[id]
4. http://gdcbghvjyqy7jclk.onion.rip/[id]
5. http://gdcbghvjyqy7jclk.onion.plus/[id]

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

DANGEROUS!
Do not try to modify files or use your own private key - this will result in the loss of your data forever!
```

Figure 2: GandCrab Ransom note deposited as a TXT file on the client hard disks.

Danabot

DanaBot is a Trojan that includes banking site web injections and stealer functions. Proofpoint researchers observed one DanaBot affiliate (Affid 11) specifically targeting Canada with “Canada Post” themed lures between January 1 and May 1, 2019.

Formbook

FormBook is a browser form stealer/keylogger that is under active development. This malware is notable in its use of "decoy domains" in its command and control (C&C) communications; typically it will connect to 15 randomly selected domains, one of which is replaced by the correct C&C.

Dridex

Dridex is a banking Trojan that steals personal banking information and credentials for other sites, such as social media platforms and webmail. First spotted in November 2014, Dridex is considered to be a successor of Cridex, a similar banking Trojan.

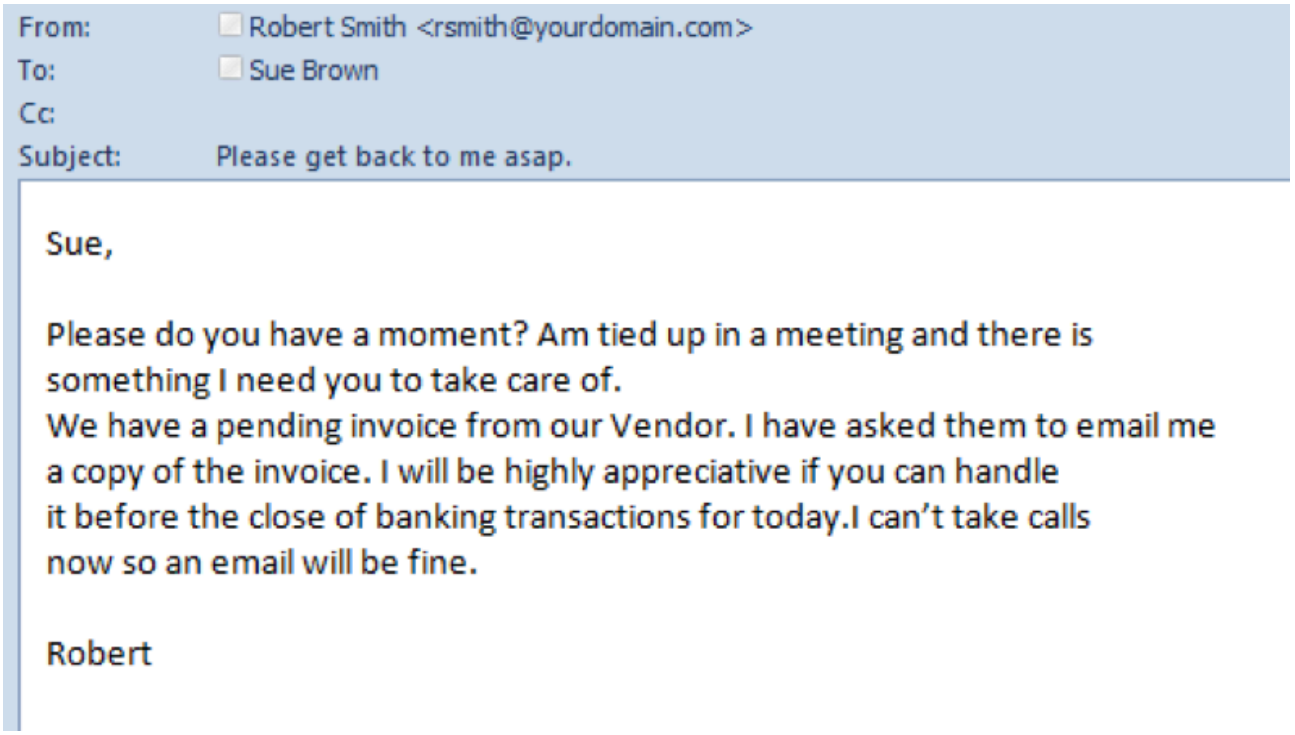
The malware appears to be under the control of one group and is sold as a service to others. Each Dridex affiliate distributes the malware in a different manner. The distribution varies in sophistication and frequency. Observed delivery mechanisms include:

- Microsoft Word documents arriving as an email attachment that utilizes social engineering and macros to infect users
- MIME-formatted Microsoft Word or Excel email attachments utilizing malicious macros
- Spammed URLs leading to zipped executables. The URLs may utilize a public redirector service such as google.com with the final payload hosted on another site such as dropbox.com or copy.com
- Exploit Kits

Conclusion

While this blog is focused specifically on malware threats affecting Canada, often among other regions, ubiquitous phishing attacks, Business Email Compromise (BEC), and other forms of imposter attacks remain ongoing threats, both internationally and in Canada. Organizations in Canada and elsewhere should remain vigilant of the following:

- Credential Phishing, which the most common threat observed by Proofpoint researchers, is a type of phishing that specifically targets a victim’s login credentials such as usernames and passwords. 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.
- 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.



I

Figure 3: An example of a threat actor engaging in business email compromise (BEC), which is a type of known imposter activity.

Conclusion

In 2019, threats specific to Canadian interests, whether abusing Canadian brands, or affecting Canadian organizations through specific geo-targeting mean that defenders at Canadian companies must be cognizant of threats far more targeted than "North America." Banking Trojan and the Emotet botnet lead the pack, creating risks for organizations and individuals with compelling lures and carefully crafted social engineering. While Canada-targeted threats are not new, Emotet in particular, with its frequent region-specific email campaigns, is bringing new attention to geo-targeting in Canada and beyond.
