What About Canada, Eh? – The Canadian Threat Landscape

- Posted on:January 5, 2016 at 3:23 pm
- Posted in:Deep Web
- Author:
  Natasha Hellberg (Senior Threat Researcher)

As a Canadian Threat Analyst, one challenge that I and others like me face is that there are very few threat reports that focus on or cover Canada. There are a few, but we generally have to rely on reports from the US (like Trend Micro's report examining the North American Underground), and then extrapolate these into the Canadian context. After all, US and Canadian threats are the same, right?

Actually that's not the case. Our culture, motivations, behaviors, and political climate are all unique to Canada. These influence how threat actors here behave. As a result, American statistics are not always an accurate reflection of threats to Canada, and Canadians. This is a factor that should be considered when looking at statistics relating to threats here in Canada.

Let's look at the threat metrics for Canada in recent months and weeks to give a bit of a glimpse into the Canadian threat landscape as it pertains to malware.

What are the volumes and trends in Canadian malware infections as seen by Trend Micro?

Currently, the most prominent threat in Canada is the OpenCandy adware toolbar. Users are tricked into installing this onto their machine, which is then used to also download malware onto it. Adware, infostealers and banking Trojans make up the balance of the commonly seen threats in Canada for the month of November 2015. Notably, there is one conspicuous absence: ransomware. Although ransomware currently a leading threat in the US, we did not see it as a particularly common threat in Canada in November 2015.

Adware		Malware	
Family	**Count**	**Family**	**Count**
OPENCANDY	4,425	DRIDEX	1,250
INSTALLCORE	731	DLOADR	525
MYPCBACKUP	450	BARTALEX	217
FakeGooG	377	FAREIT	191
PRICEGONG	362	UPATRE	164
ESMAYLBAKS	279	PASSVIEW	96
DEALPLY	246	RAMNIT	86
RegCleanPro	222	ZBOT	67
TOMOS	171	ADLOAD	65
SPIGOT	147	DYER	62

Figure 1. Top adware and malware families in November 2015

What are the patterns of malicious IPs and domains in Canada?

Canada is not a significant hoster of malicious sites, with only 0.2% of global traffic to malicious sites headed to sites hosted in Canada. However, there is one key factor that differentiates malicious web sites in Canada from those in other countries.

Unlike other countries, the ratio of malicious IP addresses and malicious domains hosted is almost 1:1. This indicates that malicious domains in Canada tend to be hosted on only one IP address and don’ t move around or use multiple ones at the same time, as they do elsewhere.

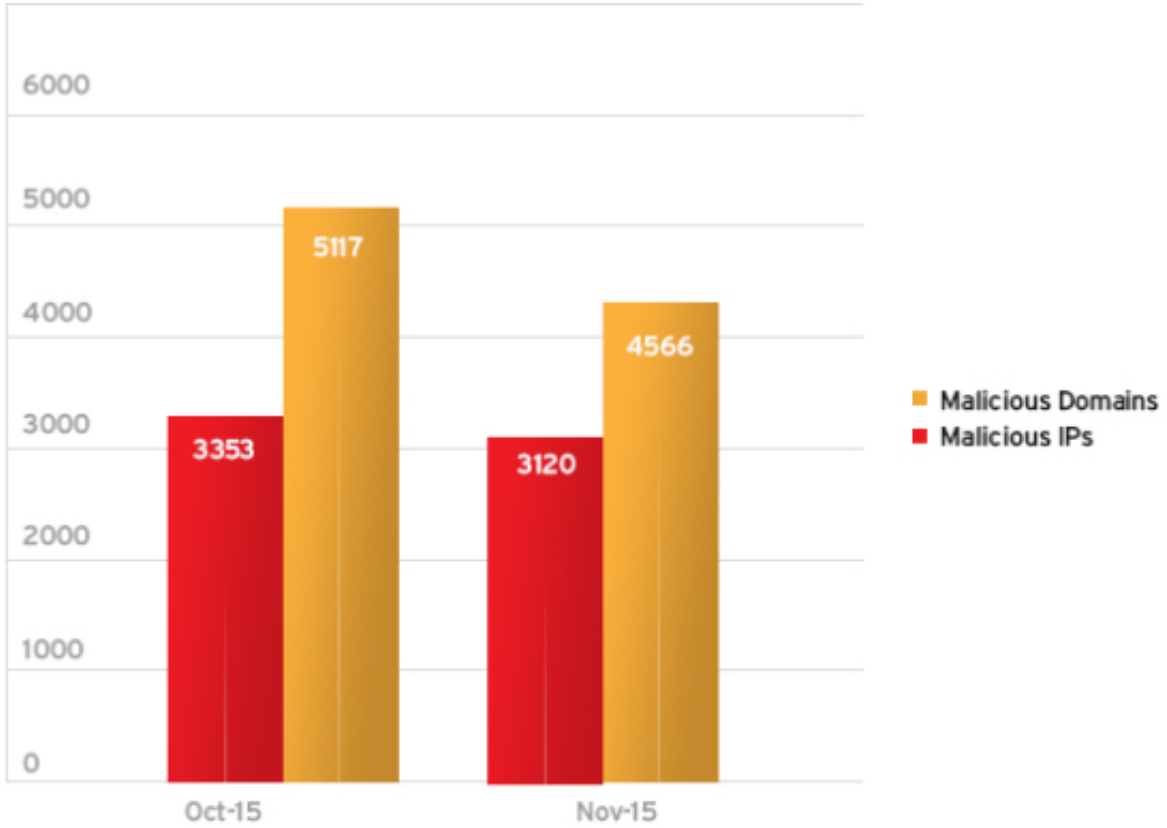


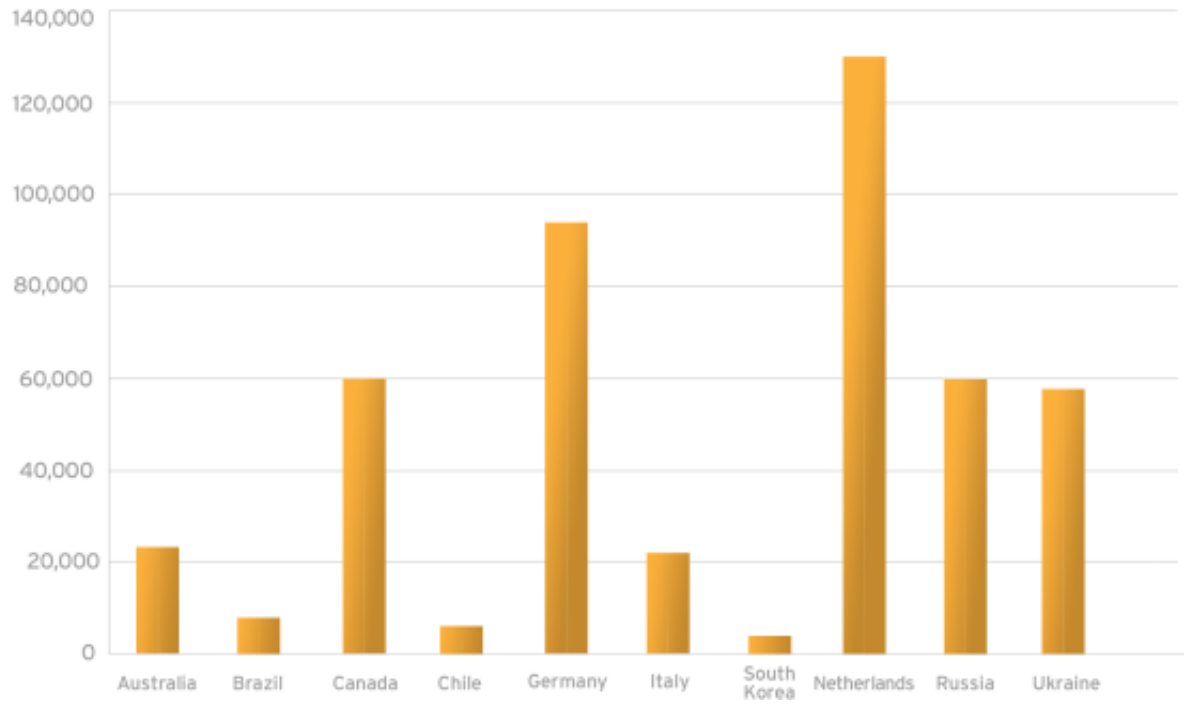
Figure 2. Malicious IP addresses and domains hosted in Canada

As such, it appears that peer-to-peer and fast-flux systems are not commonly used for hosting malicious websites and domains in Canada. This highlights how the infrastructure for malicious hosting in Canada is not as sophisticated as it is in other countries that are more well-known cybercrime hotspots. Instead, it seems that legitimate websites that have been injected with malicious content are more commonly used.

Which country "attacks" Canada the most?

To determine which country most frequently "attacks" Canada, we examined where websites visited by Canadian users and blocked by our products were hosted. Looking at the November data, one thing is clear: the malicious site(s) that Canadians visit are predominantly hosted in the United States. The number of "hits" to malicious sites in the US is higher by one order of magnitude than any other country.

Country	Hits
Australia	26,564
Brazil	11,137
Canada	59,791
Chile	8,204
Germany	92,205
Italy	21,803
South Korea	5,244
Netherlands	127,379
Russia	59,446
Ukraine	57,077
US	1,456,355



Figures 3 and 4. Countries visited by Canadian users that contain malicious sites, excluding the United States

What's more interesting is the *other* countries that are significant sources of malicious website traffic. Australia's numbers is due to a lot of peer-to-peer nodes of ZeuS (and its successors); the activity from the Netherlands, Germany, Russia, and Ukraine is due to the presence of bulletproof hosting companies in these countries. These bulletproof hosters are used to host the command-and-control (C&C) infrastructure of various botnets, and it seems by the statistics that that like other countries, Canadians are also victims of these sites.

Is there such a thing as a Canadian Underground?

Yes, there is.

While it is not as large or well-developed as other underground communities, there is a viable Canadian underground community as well. Unlike the US underground, it is primarily focused on the sale of fake/stolen documents and credentials. This includes both faked identification, such as driver's licenses and passports, as well as stolen credit card and other banking information. It also includes credit "fullz" (complete dumps of an individual's personal information), which include an individual's credit reports and even their Apple ID credentials.

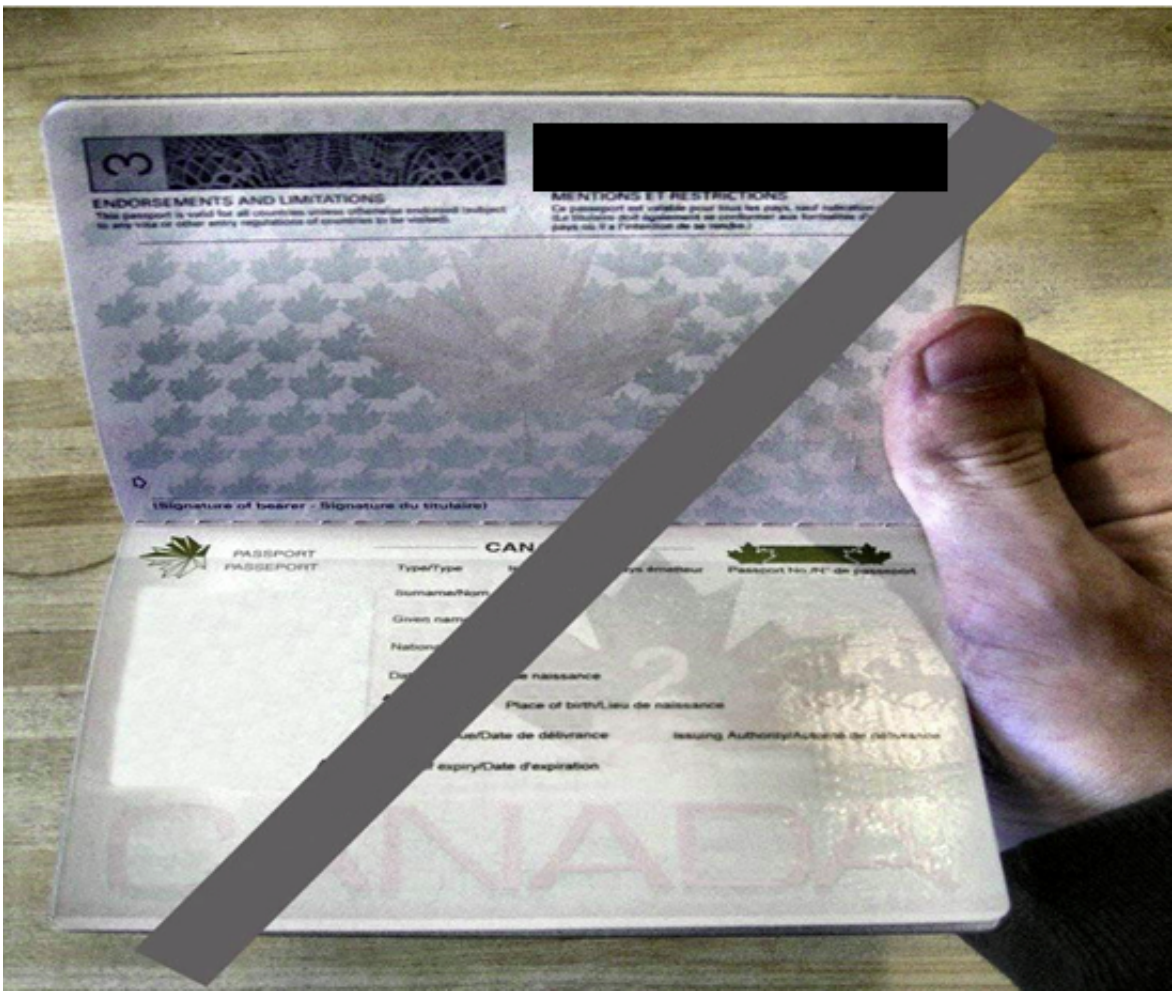


Figure 5. Sample of fake Canadian passport for sale

The most interesting thing to note in the Canadian underground is the absence of underground toolkits and infrastructure services that could be attributed to being hosted in Canada. Despite extensive searches, VPN services, botnet toolkits, DDoS services and the like could not be found. This is particularly notable given that some of the higher profile skid/gaming gang members reside in Canada; so the lack of these services is surprising.

Finally, it was comforting to note that in addition to the lack of underground service/infrastructure offerings, there also appears to be a no market for violent crime-related services. We could not find weapons for sale or murder-for-hire offers, nor "all services" trafficking-type underground services hosted in Canada, or serving a primarily Canadian market. We can only assume that Canadian's reputation for being nice and law abiding appears also extends to its underground.

What kind of stolen and faked credentials can be found on the Canadian Underground?

Almost any kind of documentation and credentials were found during our research. This included driver's licenses from every province, Canadian Passports, and Social

Insurance Number (SIN) cards. It also included VISA, Master Card, and American Express cards, and banking cards from every major financial institution.

Pricing for these products tends to be somewhat lower than for American information, as one can see in our North American Underground paper.

Country & Fake Document Type	Cost
USA Passport Scan	$30.00 per passport scan
Canada Passport Scan	$17.00-24.00 per passport scan
UK Passport Scan	$28.00 per passport scan
USA Counterfeit Passport	$780.00 per counterfeit passport
Canada Passport Scan	$670.00 per counterfeit passport
UK Passport Counterfeit	$730.00 per counterfeit passport
USA Drivers License Scan	$145.00 per license scan
USA Counterfeit Drivers License	$727.00 per counterfeit drivers license
Canada Counterfeit Drivers License	$630.00 per counterfeit drivers license
UK Counterfeit Drivers License	$700.00 per counterfeit drivers license
Counterfeit CVS Prescription Label	$100.00 per 3 labels
Counterfeit Walgreens Prescription Label	$100.00 per 3 labels
Counterfeit Roland Prescription Label	$100.00 per 3 labels
Counterfeit US Auto Insurance Card	$38.00 per forged card

Figure 6. Cost comparison of fake document types by country, etc.

Not only can one acquire fake documentation, the sale of credit and debit card information is thriving. In this case, the costs tend to be higher than US equivalents. One could infer this is not only because of the smaller supply, but that unlike in the US, Canadian cards include Chip and Pin technology making them harder to make use of.

Service	Cost
Canada Credit Card Classic Numbers	$47.00-$50.00 USD per 40 card numbers
Canada Credit Card Gold/Platinum/Business Numbers	$50.00-$65.00 USD per 35 card numbers
US Credit Card (Physical)	$210.00 - $874.00 USD per card
US Credit Card Classic Numbers	$19.00- $22.00 USD per 100 card numbers
US Credit Card Gold/Platinum/Business Numbers	$36.00-$42.00 USD per 50 card numbers

Figure 7. Canada versus US cost comparison of bulk credit card numbers

Banking information is also available for sale. During the time of our research one could find sites selling many different Canadian Financial Institution (CFI) account information. Pursuing it further, the seller was even willing to provide screen shots of recent accounts and amounts to prove the authenticity of the goods he was selling.

Figures 8 and 9. CFI banking credentials for sale

Using malware configs, we assessed which Canadian brand was most often targetted by malware in 2015. Based on our analysis, the most predominately attempted brand of credential attempted to be captured was Toronto Dominion (TD) Bank, by more than twice more than the next most targeted brand.

BRAND	UNIQUE SHA1S
TORONTO DOMINION BANK	359
BANK OF MONTREAL	156
CIBC	71
SCOTIABANK	65
ROYAL BANK OF CANADA (RBC)	64
VANCITY	62
BANQUE NATIONALE	34
SERVUS CREDIT UNION	31
CONEXUS	31
MEMBERDIRECT ONLINE BANKING	31
HARRIS BANK	31
HSBC	31
DESJARDINS	11
MBNA (TD BANK)	7
KOODO MOBILE	5
ROGERS	3
TELUS	2
CHASE CANADA	2
FIDO	2
ING DIRECT (SCOTIA BANK)	2
BANQUE LAURENTIENNE	1

Figure 10. Canadian brands targeted by malware in 2015

While investigating we found that various telecommunications company brands (Telus, Rogers, Fido) were also targeted.

What about drugs – both illegal and pharmaceutical? Can these be found?

Another focus of the Canadian underground understandably is drug trade – both illegal drugs sold to Canadians and US markets, as well as prescription drug sales sold to primarily US and international customers.

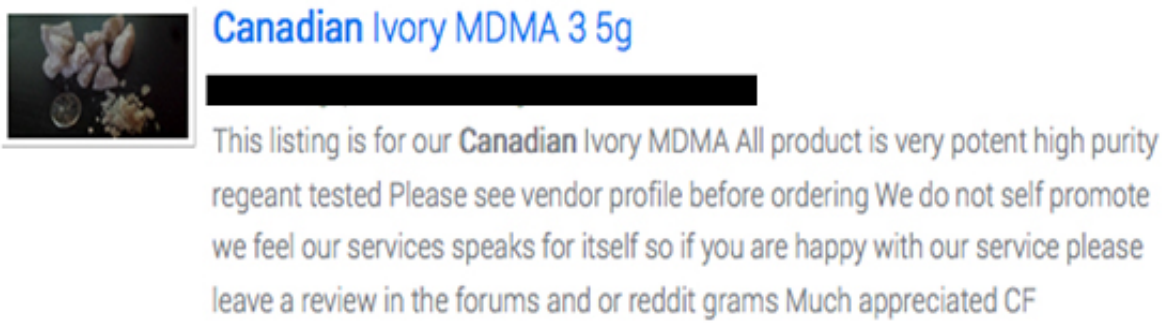


Figure 11. Advertisement for illegal drugs

During our research we were able find Canadian based sellers for many different varieties of drugs. As an example, the above seller appears to do a fairly active trade, and was even given high sellers scores by his customers for quality and timeliness of delivery.

Summary

As a long time threat researcher here in Canada, it was particularly interesting seeing statistics that directly pertain to directly to Canada. It was also interesting to see how similar (and different) the Canadian underground community can be.

It would be interesting to compare these against other countries and other global statistics just to see how we compare directly using the same methodology and metrics. Maybe that's what I'll do next year – so keep an eye here for new updates!

Related Posts:

- Attack of the Solo Cybercriminals – Frapstar in Canada
- Magnitude Exploit Kit Uses Newly Patched Adobe Vulnerability; US, Canada, and UK are Most At Risk
- Recent Crypto-Ransomware Attacks: A Global Threat
- Macro Threats and Ransomware Make Their Mark: A Midyear Look at the Email Landscape

Tags: Canadian underground

Featured Stories

- 2016 Predictions: The Fine Line Between Business and Personal
- Pawn Storm Targets MH17 Investigation Team
- FBI, Security Vendors Partner for DRIDEX Takedown
- Japanese Cybercriminals New Addition To Underground Arena
- Follow the Data: Dissecting Data Breaches and Debunking the Myths

Recent Posts

- Let's Encrypt Now Being Abused By Malvertisers
- What About Canada, Eh? – The Canadian Threat Landscape
- Operation Black Atlas, Part 2: Tools and Malware Used and How to Detect Them
- New Targeted Attack Group Buys BIFROSE Code, Works in Teams
- Adobe Flash Player Fixes 79 Bugs; Microsoft Issues 12 Patches in December Patch Tuesday

2016 Security Predictions

- From new extortion schemes and IoT threats to improved cybercrime legislation,

Trend Micro predicts how the security landscape is going to look like in 2016. Read more

Popular Posts

Blog of News Site "The Independent" Hacked, Leads to TeslaCrypt Ransomware
The German Underground: Buying and Selling Goods via Droppers
Hacking Team Flash Zero-Day Integrated Into Exploit Kits
Cybercriminals Improve Android Malware Stealth Routines with OBAD
New Targeted Attack Group Buys BIFROSE Code, Works in Teams

Latest Tweets

- Senior Threat Researcher Kyle Wilhoit (@lowcalspam) shares insight on BlackEnergy: bit.ly/1TEhaxv
  about 26 mins ago
- Parting is such sweet sorrow-- #Microsoft officially dumps #InternetExplorer 8, 9 & 10: bit.ly/1UxIqhd
  about 3 hours ago
- From Dark Reading: How Technologies Incubated A Decade Ago Shape The World Today ubm.io/1UxHidx
  about 4 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe