January 06, 2016

Canadian cyberthreats differ from those in the U.S.: Report

While the U.S. and Canada both see their fair shares of malware such as Dridex and other banking trojans, but there was one conspicuous absence from the list of common threats shared between the two nations. Ransomware

While prominent in the U.S., Trend Micro researchers said in the research firm's Canada threat landscape report that ransomware was not a common threat in the Great White North

"For whatever reasons the market forces just aren't driving them in that direction," Christopher Budd, Global Threat Communications Manager at Trend Micro told SCMagazine.com.

hers examined Canada's threat pe including malware and its dark web

The exact reason for this absence is unclear an ated by Budd nor the report, but he hinted cybercriminals could be doing so to benefit while deciding it's not worth using ransomware attacks against Canadians because they are not culturally attuned to fall victim to such an attack.

Budd pointed out that ransomware attacks have worked their way around the globe, initially rising to prominence in New Zealand and the UK, before cybercriminals used it to target Americans. So, it is possible that Canadians may be targeted more in the future, he said.

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

The most prominent threats in Canada right now are the OpenCandy (*see chart at left)* adware toolbar and Dridex malware.

One area where there is some crossover is hosting. Canadians tend to be victimized by sites hosted south of the border.

Cybercriminals in the U.S. help influence the Canadian threat landscape by providing infrastructure for hosting malicious content. According to the report, the majority of malicious sites that Canadians visit are predominantly hosted in the U.S. as malicious hosting in Canada isn't as sophisticated as it is in other countries.

Researchers also noted an absence of underground toolkits and infrastructure services such as VPN services, botnet toolkits, DDoS services, and there is little market for violent crimes for hire in Canada's dark web. Budd said it's likely that cybercriminals look to the U.S. for the toolkits and infrastructure services.

"If you have a mature market place where you can buy what you need there's no need to build a new one," Budd said.

The the portions of the dark web hosted in Canada are primarily focused on the sale of fake and stolen documents and credentials such as driver's licenses, passports and dumps of personal information.

- twitter
- linkedin
- google
- 0 Comments
- Email
- Print

You must be a registered member of SC Magazine to post a comment.
Click here to login | Click here to register

Sponsored Links