The Representation of Victim Nations in Stolen Data Markets

Dr. Olga Smirnova, Associate Professor, Eastern Carolina University
smirnovao@ecu.edu

ABSTRACT: The cybercriminals sell stolen data on various online platforms such as Open Web and Dark Web forums. To this date, there is limited research on the types of products sold on the "Dark Web". This brief reports geographic distribution of victim nations differences between Open and Dark web forums. The criminals tend to advertise in line with their perceptions of detection. The forums where advertisements occur have larger impact on prices and types of exchanges than the geographical locations where the data comes from.

Cybercriminals, like regular criminals, engage in illegal acts by calculating their rewards relative to their perceived risk of detection. Various situational characteristics and prior experiences with illegal acts affect offenders' behavior. There is now a robust market for personal information acquired through phishing, hacking, and data breaches which can be sold to others for use in identity theft and fraud.

To that end, the demand and supply of stolen data may be driven by the potential risk of detection and extradition relative to any potential profits from the transactions. Vendors will likely target different countries based on their perceptions of detection and ease of getting rewards. Examining the distribution of products sold enables researchers to better understand the scope of harm caused to countries by data thieves. Examining the prices also allows us to understand the potential perception of risk and availability of information.

One of the key factors affecting offenders' risk calculations may be the online platform where they operate. For instance, the "open web" or unencrypted World Wide Web stolen data markets can be easily found through any search engine.

There are also "dark web" platforms operating on TOR (The Onion Router) that can only be located via specialized encryption and software (e.g. special plugins). The contents of the websites and resources on the dark web cannot be indexed or accessed by traditional open web search engines. As a result, actors operating on this platform may feel a greater degree of anonymity.

This study examined the distribution of products sold in a sample of 2,443 threads from 18 web forums and shops on both the open and dark web where criminals and hackers buy, sell, and trade stolen financial and personal information. The analysis focused on CVV/dumps products, that contain all information on a credit/debit card needed to make a purchase.

European nations were the number one target, followed by the US. Tor shops included geographic identifiers in all ads, though they varied in specificity from generic language (World/International) to specific countries (E.g. US, Germany, EU). The use of generic language may be a deliberate strategy of risk avoidance by offenders as a means to minimize prosecution and reduce their likelihood of identification.

While the majority of data sold within this sample of markets had some geographic identifier, ads without geographic identifiers had higher prices listed. In addition, ads with geographic identifiers had more exchanges (positive and negative comments made by potential buyers), suggesting a greater likelihood that sellers were turning a profit through the sale of data. Figure 1 shows average prices and average positive, negative, and neutral comments for ads with and without geographic identifiers. Figure 2 shows the geographic distribution of ads on different forums.

At the same time, the forums where the ads were placed had a greater influence on pricing. We interpret this as a relationship between the reliability and trustworthy reputation of a forum and the price for data.

Targeting specific forums for police action is essential to help disrupt the overall dark market operations. Comparing open and dark web market venues for stolen data may help our understanding of those markets. The US and EU remain the largest targets of cybercriminals, who employ various strategies (e.g. using Tor shops) to avoid detection.

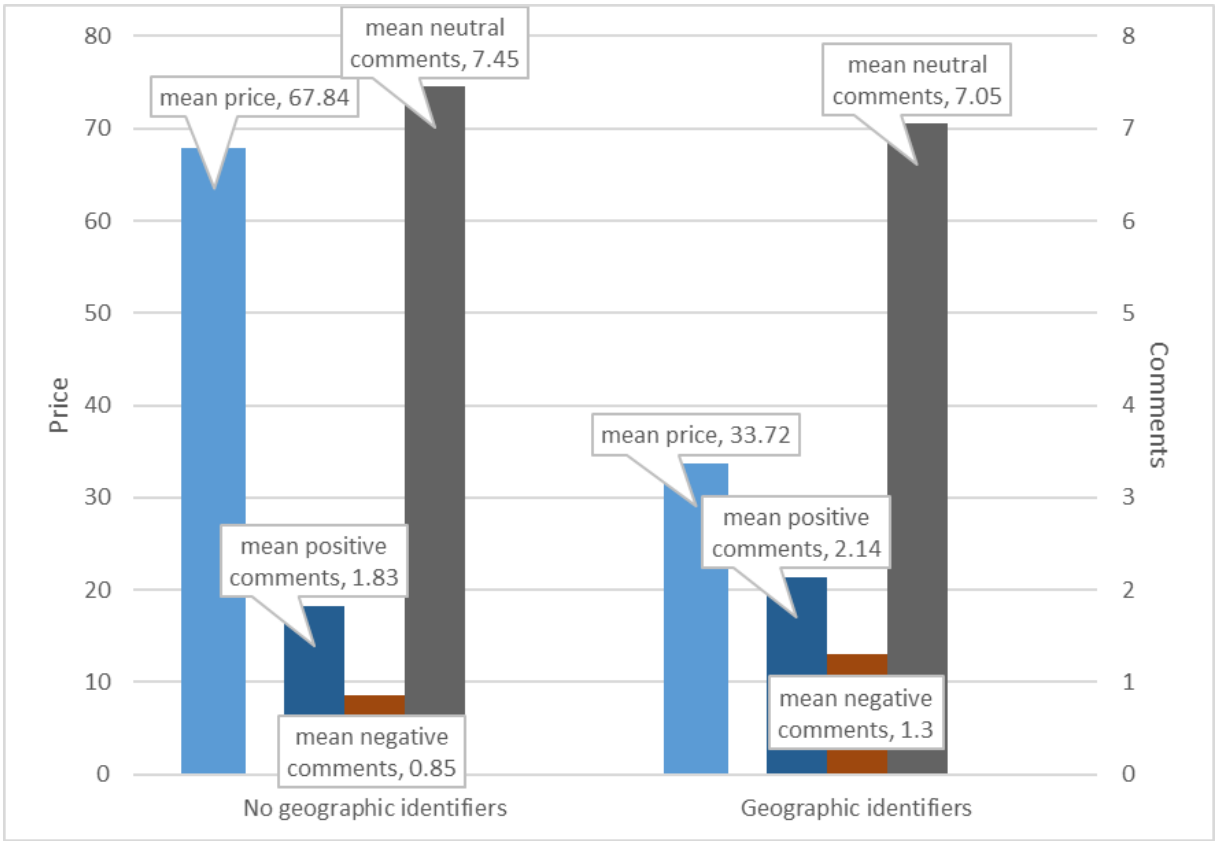

Figure 1. Average price and average positive, negative, and neutral comments with and without geographic identifiers.

Note: Ads with geographic identifiers have, on average, lower prices, but more discussion (higher averages of positive, negative, and neutral comments).

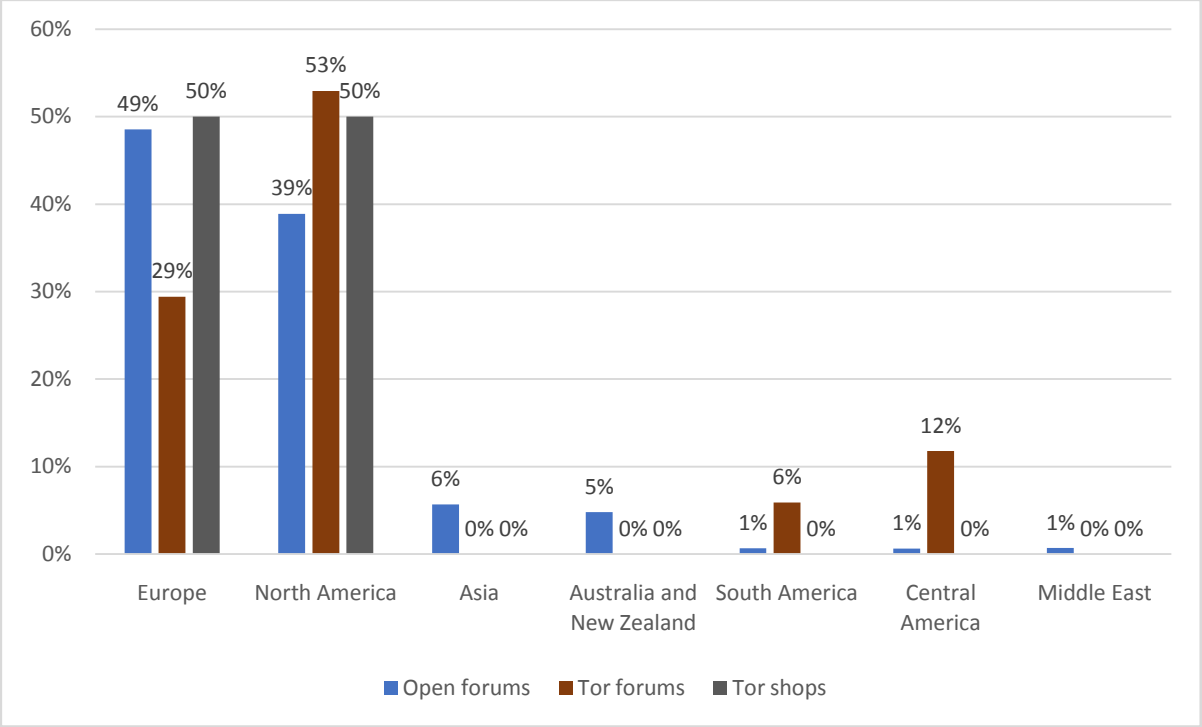

Figure 2: Regional representation on different dark markets.
Note: U.S. represents about 71% of North American stolen data.

References: Based on Smirnova, Olga and Tom Holt. 2017. "Examining the Geographic Distribution of Victim Nations in Stolen Data Markets," American Behavioral Scientist, Vol. 61(11), 1403-1426