A Pilot Study investigating a relationship between the price of Stolen Credit Card Data and Credit Card Data Breaches

Michael Davies – Cyber Security Centre for Doctoral Training – University of Oxford – michael.davies@cs.ox.ac.uk

There is growing anecdotal and research evidence that cyber criminals are employing business methods to facilitate their activities. This study exploits economic theory to investigate a relationship between the market price of stolen credentials and significant card data breach. Such a relationship could underpin the development of a model that could act as an indicator / warning of such breaches in the future.

1. Introduction and Background

Anecdotal evidence of increasing use of business methods by cyber criminals. This project employs economic theory using supply and demand to identify a relationship between price of credentials and data breach. Data breaches often unreported or worse undetected for significant periods. Analysing the price of stolen credentials during 2014 and significant data breach over the same period attempt, to identify a relationship that could underpin the development of a model that warns of significant data breach.

2. Methodology

Credit card credential data from Black Market Archive, a significant resource of research data recently added to the Internet Archive. GRAMS/Cloud9 data for single vendor Hackyboy provided time series data of price credentials. Time series of data breach information from Forbes/Krebs. A number of assumptions employed that underpin analytical process.

3. Analysis

Data derived from GRAMS Dark Net search engine is predominantly narcotics related but includes the Cloud9 carding site with Hackyboy vendor information, in CSV format and conducive to analysis. Data comprised daily price listings of stolen credit cards. Analysis focussed on single credit cards (ignoring bulk card sales) and assumed homogeneity of daily card data inputs to enable average price calculation. Visual analysis of data revealed price reduction points at A, B, and C, that could be evidence of possible price suppression. Fragmented data after Jan 15 therefore this period was not considered for analysis. Assumed that time from initial breach to arrival of stolen credentials could be achieved in 7 days.

4. Results

The data derived from the GRAMS search engine is shown below with price reduction points circled.

With this data superimposed on to the incidence of significant data breach, the temporal proximity of price reduction point A and the inferred date of breach at Jimmy John’s and Albertsons is shown below.

5. Conclusions

Demonstrating that the fluctuations in price levels advertised on the Hackyboy vendor site were linked to the incidence of credit breach were hampered by two key factors. It is apparent from a visual inspection of the timeline above that the sheer number of data breaches witnessed over the analysis period made it difficult to attribute any single data breach to a subsequent price fluctuation. This was compounded by lack of information around when actual breaches occurred. Nevertheless, the pilot study does identify potential avenues of research and the importance of the Black Market Archive, with its 1.6 terabytes of data, as an invaluable research resource.

References:
- Branden, G; Christians, N; Decary-Hetu, D; et al, Dark Net Market Archives, 2015 from www.gwern.net/Black-Market-archives
- Forbes (2014) www.forbes.com/sites/moneybuilder/2015/01/1
- Herley, C; & Flor, D; (2010), Nobody Sells Gold for the Price of Silver; Economics of Information, Security and Privacy (pp 33-53)