McAfee Labs Report Reveals Prices of Stolen Data on Dark Web
Thursday, October 15, 2015 04:01:00 AM (GMT)

Hidden Data Economy Report Exposes Price Points for Stolen Data Bought and Sold In Cybercriminal Marketplaces

News Highlights:

- Average estimated price for stolen credit and debit cards: $5 to $30 in the United States; $20 to $35 in the United Kingdom; $20 to $40 in Canada; $21 to $40 in Australia; and $25 to $45 in the European Union
- Bank login credentials for a $2,200 balance bank account selling for $190
- Bank login credentials plus stealth funds transfers to U.S. banks priced from $500 for a $6,000 account balance, to $1,200 for a $20,000 account balance
- Bank login credentials and stealth funds transfers to U.K. banks range from $700 for a $10,000 account balance, to $900 for a $16,000 account balance
- Online payment service login credentials priced between $20 and $50 for account balances from $400 to $1,000; between $200 and $300 for balances from $5,000 to $8,000

Intel® Security today released ***The Hidden Data Economy*** report, which provides examples of how different types of stolen data are being packaged and offering prices for each type of data. Intel Security Group’s McAfee Labs organization examined pricing for stolen credit and debit card data, bank account login credentials, stealth bank transfer services, online payment service login credentials, premium content service login credentials, enterprise network login credentials, hospitality loyalty account login credentials, and online auction account login credentials.

“Like any unregulated, efficient economy, the cybercrime ecosystem has quickly evolved to deliver many tools and services to anyone aspiring to criminal behavior,” said Raj Samani, chief technology officer for Intel Security EMEA. “This ‘cybercrime-as-a-service’ marketplace has been a primary driver for the explosion in the size, frequency and severity of cyber attacks. The same can be said for the proliferation of business models established to sell stolen data and make cybercrime pay.”

Over the years, the McAfee Labs team has worked with IT security vendors, law enforcement and others to identify and evaluate numerous websites, chat rooms, and other online platforms, communities, and marketplaces where stolen data is bought and sold. Drawing on this experience, its researchers can now provide an overall assessment of the “state of the cybercrime economy” along with illustrations of key types and prices of data.

Payment cards

Payment card data is perhaps the most well-known data type stolen and sold. McAfee Labs researchers found a value hierarchy in how this stolen data is packaged, priced and sold in the dark market. A basic offering includes a software-generated, valid number that combines a primary account number (PAN), an expiration date and a CVV2 number. Sellers refer to a valid number combination as a “Random.” Valid credit card number generators can be purchased or found for free online.

Prices rise when the offering includes additional information that allows criminals to accomplish more things with the core data. This includes data such as the bank account ID number, the victim’s date of birth, and information categorized as “Fullzinfo,” including the victim’s billing address, PIN number, social security number, date of birth, the mother’s maiden name, and even the username and password used to access, manage and alter the cardholder’s account online.

The following table illustrates the average prices for credit and debit card account information across regions based on the combination of data elements available:

Package	U.S.	U.K.	Canada	Australia	EU

Basic or “Random”	$5-$8	$20-$25	$20-$25	$21-$25	$25-$30
With Bank ID#	$15	$25	$25	$25	$30
With Date of Birth	$15	$30	$30	$30	$35
With Fullzinfo	$30	$35	$40	$40	$45

“A criminal in possession of the digital equivalent of the physical card can make purchases or withdrawals until the victim contacts the card issuer and challenge the charges,” continued Samani. “Provide that criminal with extensive personal information which can be used to ‘verify’ the identity of a card holder, or worse yet allow the thief to access the account and change the information, and the potential for extensive financial harm goes up dramatically for the individual.”

Payment service accounts

The prices for compromised online payment service accounts appear to be dictated solely by account balance. This is likely due to their limited uses and scenarios for exploit. Account login credentials for accounts containing from $400 to $1,000 have been estimated to cost between $20 and $50, while login credentials for accounts containing from $5,000 to $8,000 range from $200 to $300.

Bank login credentials

Cybercriminals can purchase banking login credentials and services allowing them to stealthily transfer stolen funds across international borders. McAfee Labs found login credentials for a $2,200 balance account selling for $190. Bank login credentials coupled with the ability to stealthily transfer funds to U.S. banks ranged from $500 for a $6,000 account balance, to $1,200 for a $20,000 account balance. United Kingdom transfers ranged from $700 for a $10,000 account balance, to $900 for a $16,000 account balance.

Online premium content services

The report also assesses dark market prices for account login credentials to online content services such as online video streaming($0.55 to $1), premium cable channel streaming services ($7.50), premium comic book services ($0.55), and professional sports streaming ($15). These relatively low price points suggest that cybercriminals have ramped up automated theft operations to make their cybercrime business models profitable.

Loyalty, community accounts

Some online services, such as login credentials to hotel loyalty programs and online auction accounts, would appear to be low value targets, but researchers found that these credentials are also offered for sale on the dark market. Apparently, these allow buyers to conduct online purchases under the guise of their victims. McAfee Labs researchers found a major hotel brand loyalty account with 100,000 points for sale for $20, and an online auction community account with high reputation marks priced at $1,400.

For more information, please read the full report: ***The Hidden Data Economy***.

For guidance on how consumers can better protect themselves from the consequences of data breaches and the fraud and theft that often follow, please visit: ***Consumer Blog***.

About McAfee Labs

McAfee Labs is the threat research division of Intel Security and one of the world’s leading sources for threat research, threat intelligence, and cybersecurity thought leadership. The McAfee Labs team of more than 400 researchers collects threat data from millions of sensors across key threat vectors—file, web, message, and network. It then performs cross-vector threat correlation analysis and delivers real-time threat intelligence to tightly integrated McAfee endpoint, content, and network security products through its cloud-based McAfee Global Threat Intelligence service. McAfee Labs also develops core threat detection technologies—such as application profiling, and graylist management—that are incorporated into the broadest security product portfolio in the industry.

About Intel Security

McAfee Labs is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique McAfee Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. The mission of Intel Security is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com.

No computer system can be absolutely secure.

Note: Intel, Intel Security, the Intel logo, McAfee and the McAfee logo are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

View source version on businesswire.com: http://www.businesswire.com/news/home/20151014006624/en/

--30-- CM/SF

Contact:

Intel Security
Chris Palm, 408-346-3089
chris.palm@intel.com
or
Zeno Group
Janelle Dickerson, 650-801-0936
Janelle.Dickerson@zenogroup.com

1.2

Industries: Technology, Data Management, Hardware, Internet, Software, Security
Languages: English
Primary Identifiers: INTC-US
Related Identifiers: INTC-US, US458140100
Source: Intel Security
Subjects: Survey, Product/Service