the Availability Digest

www.availabilitydigest.com
@availabilitydig

Going Prices for Personal Information

January 2014

Hacking financial data-processing systems to steal credit-card, debit-card, and personal information has become big business. Not only are hundreds of millions of people put at financial risk each year, but the hackers make big profits without ever using this data. Rather, they simply sell it in a hackers' black market to resellers..

Hackers are Successful

Recent indictments against a Russian team[1] demonstrate how effective knowledgeable hackers can be. This group of five individuals operated a prolific hacking operation that was responsible for several of the largest known data breaches. The team included two who specialized in penetrating corporate computer networks. A third individual specialized in harvesting data from the penetrated networks. A forth individual provided anonymous web-hosting services that were used for the hacking activities. A fifth individual sold the information obtained from the hacking activities to willing buyers around the world.

During a five-year period, this team was able to steal almost 200 million credit card numbers and related personal information:

- Two million credit-card numbers were stolen from Carrefour, a French multinational retailer.
- Over 4 million credit-card numbers were stolen from Hannaford, a regional U.S. supermarket chain.
- Heartland Payment Systems, one of the world's largest credit-card and debit-card payments processors, had 130 million card numbers stolen and suffered losses of USD $200 million.
- Thirty-million card numbers was stolen from the computer networks of Commidea, a provider of electronic payment processing.
- Dexia Bank Belgium suffered a large card-number loss that resulted in almost USD $2 million dollars in losses.
- Dow Jones, a publisher of news, business, and financial information, suffered the loss of 10,000 login credentials.

[1] Grand Jury Indictment, United States District Court, District of New Jersey, Criminal No. 09-626 (JBS) S-2.
http://krebsonsecurity.com/wp-content/uploads/2013/07/DVKRK-Indictment.pdf
Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce Charges Against Russian National for Hacking NASDAQ Servers, *FBI New York Field Office*; July 25, 2013.

- Euronet, a global provider of financial transaction services, lost two-million card numbers.

- 800,000 card numbers were stolen from a Visa licensee.

- 950,000 card numbers at a loss of over USD $90 million were stolen from Global Payments Systems, a global financial transaction processing company.

- Over 500,000 Diners Club credit cards were exposed at a loss of over USD $300 million.

- Ingenicard, a provider of international electronic cash cards, suffered the loss of card numbers, which later were used to withdraw USD $9 million in a 24-hour period.

And then there was the recent Target breach in which 110 million credit cards and debit cards were compromised.

Going Prices for Personal Information

What do these malicious people do with all of these cards? Do they withdraw large sums from ATMs and make thousands of purchases? No, that is too much work. Rather, they simply sell the stolen information to others in underground cyber marketplaces.

Did you know that your birthdate is worth somewhere between USD $11 and USD $25? According to an investigation by Dell SecureWorks (http://www.secureworks.com), the following are going prices for different classes of personal information (all dollar amounts that follow are USD):[2]

Information	Price
Visa and Master Card:	
- US	$4
- UK, Australia, Canada	$8
- EU and Asia	$15
American Express Card:	
- US	$7
- UK, Australia, Canada	$13
- EU, Asia	$18
Discover Card:	
- US	$8
- UK, Australia, Canada	$12
- EU, Asia	$18
Credit card with mag stripe data:	
- US	$12
- UK, Australia, Canada	$20
- EU, Asia	$28
Individual Dossier (Fultz* – see below):	
- US	$25
- UK, Australia, Canada	$30
- EU, Asia	$40
VBV (Verified by Visa):	
- US	$10
- UK, Australia, Canada	$17
- EU, Asia	$25

[2] The Underground Hacking Economy is Alive and Well, *Dell SecureWorks blog*; November 18, 2013.
Stolen CREDIT CARD details? Nah… crooks desire your PRIVATES, *The Register*; November 22, 2013.

Information	Price
Date of Birth:	
- US	$11
- UK, Australia, Canada	$15
- EU, Asia	$25
Bank account – account number, user name, password – over $70,000 balance	$300

*An individual dossier, or “Fultz” in hacker terms, includes an individual’s name, address, phone numbers, email addresses with passwords, date of birth, social security number, employer identification number, bank account information (account numbers, routing numbers, account types), online banking credentials, and credit-card and debit-card information (magnetic stripe information and PINs).

Hackers have come to realize that merely having the card number and CVV is not always enough to meet the security requirements of some retailers. Having the date of birth, the social security number, and the VBV number of a victim allows the answering of additional security questions.

Credit card and debit card information is sold to “cashers,” who use the information to write the magnetic stripes of fake credit cards and debit cards. The fake cards are then used to withdraw cash from ATMs and to make illegal purchases.

Credit card, debit card, and personal information of non-U.S. citizens sell for more than that of U.S. citizens. This may be because U.S. systems are better protected than others around the world. Therefore the personal information of U.S. citizens is harder to use and consequently less valuable.

In addition to personal information, other services advertised on the web include:

- Access to groups of computers at costs ranging from $20 for 1,000 computers to $250 for 15,000 computers.
- Remote Access Trojan (RAT) for $50 to $300.
- Hacking a website and stealing data for $100 to $300 per website.

A group of computers to which access has been purchased may be harvested for personal information or infected with ransomware to extort a fee to free the computer. If used as a botnet, the group can be used to send malicious spam on behalf of other spammers or to launch DDoS attacks. Botnets in Asia tend to sell for less than those in the U.S. It is thought that this is because the U.S. provides a faster and more reliable Internet connection.

DDoS attacks are probably becoming the major availability threat to companies’ online services. Hackers will gladly do this for you for a small price:

- $3 to $5 per hour
- $90 to $100 per day
- $400 to $600 per week

All DDoS providers guarantee that the attacked website would remain offline.

Doxing is another service provided by hackers, Doxing involves getting all of the information possible about a victim. Doxing methods include searching public information sites and social media sites and manipulating the victim via social engineering, infecting them with an information-stealing Trojan. Doxing fees range from $25 to $100 per victim.

For the future, there is no shortage of hackers willing to do almost anything computer-related for money. They are continually finding ways to monetize personal and business data.

Protecting Yourself

The means to protect your sensitive data are well known but not always followed. Organizations should employ firewalls, intrusion protection systems for networks and hosts, and malware protection software. They should scan for vulnerabilities and monitor their logs on a 24x7 basis. Sensitive data and emails should be encrypted in-place and in-flight. Organizations should educate their employees to never click on email links or attachments without checking with the sender first. Email and web surfing are the two major infection vectors.

Individuals should avoid clicking on email links or attachments from untrusted sources. They should ensure that their antivirus software is maintained up-to-date, as should all updates to other applications they use. Free software or trial software should not be installed. Banking statements and card statements should be reconciled on a periodic basis to make sure that there has been no unauthorized activity. An interesting suggestion is to use a separate computer dedicated to online banking and bill paying. This computer should not be used for email or web surfing.

Summary

Hackers are clever and resourceful. Whatever protections we put in place, it does not seem long before they have worked out ways to circumvent them. And they have good reason to do so. A theft of even a modest amount of personal information can mean big payments to them. Imagine stealing the data for one million credit cards and selling this data at $4 per card - $4 million dollars over and over as the data is sold to more and more resellers.

The protections we have against this malicious activity are well-known but not always followed. It is important that organizations and individuals incorporate protective actions in their everyday life. Perhaps the key actions are for organizations to encrypt sensitive data in-place and in-flight and for individuals to avoid clicking on email links and attachments from unknown sources.

Acknowledgement

We would like to thank Stacie Neall for pointing us to this information.