the Availability Digest

www.availabilitydigest.com
@availabilitydig

The Darknet

September 2014

Where have all the credit cards gone?
Long time passing.
Where have all the credit cards gone?
Long time ago.
Where have all the credit cards gone?
Gone to Darknet, every one.
Oh, when will we ever learn?
Oh, when will we ever learn?
- Pete Seeger (paraphrased)

Over the 2013 Christmas holidays, Target[1] was hit with a massive theft of credit-card information. More recently, it appears that Home Depot has suffered a similar fate.

But what use is this stolen information? Do the hackers use forged credit cards to make a lot of purchases? No, they sell the information on the Darknet, often for millions of dollars.

Recent Hacks

The Target hack occurred over a three-week period prior to the 2013 holiday season. POS (point-of-sale) terminals in its U.S. stores were infected with malicious software that captured the magnetic-stripe data from cards that were being swiped in its terminals. The data was then sent to the attacker. Personal information from 110 million cards was stolen.

The recent suspected Home Depot hack may even surpass the Target hack. As with the Target hack, it also appears that magnetic-stripe data was compromised in the POS terminals by malicious software and sent to the attacker. In the case of Home Depot, the attack may have been going on for up to four months before it was detected.

How Were the Breaches Detected?

In neither case was the breach discovered by the victim company. In the case of Target, credit-card companies were faced with a suddenly large number of fraudulent purchases. Upon investigation, they found that batches of stolen cards had shown up on an underground web site that deals in stolen personal information. The card companies purchased some batches and analyzed recent activity of the cards. In all cases, the common denominator was Target Stores. From the card samples, it was determined that the Target breach occurred over a three-week period prior to Christmas, 2013.

[1] Target Compromises Millions of Payment Cards, *The Availability Digest*. January 2014. http://www.availabilitydigest.com/public_articles/0901/target.pdf

In the case of Home Depot, the scenario was somewhat different. On Tuesday, September 2nd, it was noted that new batches of stolen card information had suddenly appeared on the same web site. Analysis of these cards led to Home Depot as being the common source. Evidently, the Home Depot hack had been going on since April or May, perhaps for four months or so. By delaying the sale of the stolen data, the hackers were able to accumulate much more before being detected.

Interestingly, in the Home Depot case, batches of cards from U.S. banks were labeled "American Sanctions." Card batches issued by European banks were labeled "European Sanctions." Was the Home Depot attack in retribution for sanctions imposed against Russia for its Ukraine activities? Who knows?

Infecting POS Terminals

The U.S. Secret Service has been investigating a POS terminal malware infection called "Backoff" since October, 2013. It is not known if this is the malware that infected the Target and Home Depot terminals, but that is a possibility.

Unfortunately, this malware was not recognized by antivirus software until August, 2014. Seven POS system vendors have confirmed that multiple of their clients have been affected by Backoff. The Secret Service estimates that perhaps 1,000 U.S. businesses have been infected.

The Darknet

Where does this stolen information go? To the Darknet, where it is put up for sale.

The Darknet is a private network where connections are made only between trusted peers. It is structured to maintain the anonymity of its users. A person can only access a Darknet web site if he has been approved by the other members of the web site. For instance, if you want to get onto a hacker's web site, you have to prove to the current members that you are a legitimate hacker.

The Darknet actually originated quite legally under the auspices of ARPANET, the predecessor to the Internet. Launched in 2002, a project called Tor was set up by the U.S. Naval Research Laboratory with the purpose of protecting U.S. intelligence communications. It allowed groups of people using the Internet to maintain complete anonymity.

Tor is an acronym for The Onion Ring project because of its many layers of protection. Tor directs Internet traffic through a worldwide, volunteer network of more than 5,000 relays to conceal a user's location and usage from anyone conducting network surveillance. Tor is currently supported by the non-profit Tor Project (www.torproject.com) and is heavily used legitimately by groups of people who need to keep their communications absolutely private.[2]

Unfortunately, this is also what purveyors of illegal products such as stolen information need to advertise their wares. Any illegal use of the Tor network is now known as the Darknet. Most of the use of the Darknet can be traced to sources in Russia and Eastern Europe (see http://carder.su/).

Hackers dealing in stolen payment card information on the Darknet are known as "carders." Carders even have their own blogging web site that can be found at www.cardersforum.se. Included on this web site is a Bitcoin exchange. Bitcoins are typically used for transactions in the Darknet because, like the Darknet, they are completely anonymous.[3]

Typical offers on the Darknet include U.S. stolen identities for $25 each, European stolen identities for $40 each, and credentials for bank accounts with balances between $70,000 and $150,000 for $300.

[2] In June 2013, whistleblower Edward Snowden used Tor to send information to the *Washington Post* and *The Guardian*.
[3] Mt. Gox, Largest Bitcoin Exchange, Goes Belly Up, *Availability Digest*; March 2014. http://www.availabilitydigest.com/public_articles/0903/bitcoins.pdf

How Carders Make Money?

How do carders make money from stolen credit cards? The process takes many steps. The first step is that the attackers sell their stolen information to brokers who buy in bulk. The brokers then break the stolen information into smaller batches and sell the batches to carders. The carders have several ways to make money off of the stolen payment card information.

One technique is to use a credit card to purchase pre-paid cards. These cards are then used to buy gift cards issued by stores such as Amazon. The gift cards are used to purchase high value items such as computers, smart phones, and game consoles.

The carder has the purchased items sent to a "mule." A mule is in innocent and unsuspecting person who has been recruited through legitimate channels such as Angie's list with the promise of "easy work-at-home jobs." The mule reships the items for a fee to a location specified by the carder, who then assembles them into packages for resale overseas or on auction sites at significant discounts. By frequently changing shipping addresses used by the mules (often to unoccupied houses or offices), the carder can escape discovery.

The carders have discovered another way to make money. They scam spammers. A carder will sign up as an affiliate of a spam campaign – for instance, an online pharmacy. However, instead of sending out junk email, it uses the stolen credit cards to purchase items being promoted by the spammer. The carder earns a cut of 40% to 50% for everything it "sells." It is not until a card company detects that a sale is fraudulent that the spammer gets a chargeback and often higher merchant fees because of the large number of fraudulent sales. The spammer loses the money on its sale but has already paid the carder, who is no longer anywhere to be found.

What to Do?

Law enforcement agencies around the world are attempting to track criminal rings who deal in stolen information. Fifty-six members of a card fraud ring centered in Russia and who stole information from Visa, MasterCard, Discover, and American Express have been sentenced.

Of course, law enforcement is after the fact. The key solution to fraudulent card transactions is to prevent card-information theft in the first place. This can best be accomplished by encrypting information from the payment card as it is being read by the POS terminal and then using only the encrypted information to authorize the payment. Smart cards, prevalent in Europe, do just this. Using a computer chip embedded into the card, a smart card sends its card number to the issuing bank in encrypted form. The POS terminal never sees the card number in plain text, so no malware can intercept it.

Summary

The United States is a mecca for carders because it is one of the last countries (and the largest source of payment card transactions) to adopt smart-card technology.

However, this is about to change. The U.S. payment-card industry has mandated that all merchants be smart-card compatible by October, 2015, (except for gas stations, which have until 2017) or face a "liability shift." If a merchant does not process at least 75% of its transactions through an smart-card-enabled terminal (whether via chip-cards or magnetic-stripe cards) and accepts a disputed or fraudulent card payment, the merchant will be liable for the transaction rather than the issuer.

Similar attacks to those launched against Target and Home Depot are likely to continue until magnetic stripes have been completely phased out. For the time being, smart cards continue to be adorned with magnetic stripes so that they can be used in magnetic-stripe POS terminals. However, once all payment cards have been converted to smart cards and all POS terminals have been replaced with those that will read smart cards, magnetic stripes will disappear. This may take a while, but its time is coming.

Acknowledgements

Information for this article was taken from the following sources:

Carders Scamming Spammers, *Darknet.org*; May 25, 2006.
Stolen Target Credit Cards and the Black Market: How the Digital Underground Works, *Tripwire*; Dec. 21, 2013.
Stolen Identities are cheap on the Darknet, *Robert Siciliano blog*; January 27, 2014.
US card thief faces lengthy jail term, *BBC*; April 10, 2014.
Backoff Malware: Infection Assessment, *United States Secret Service*; August 2014.
Home Depot's credit cards may have been hacked, *USA Today*; September 3, 2014.
Home Depot probes possible hack, *USA Today*; September 3, 2014.
Darknet, *Wikipedia*.
Darknets!, *Krypt3ia*.