Know Your Enemy - A Profile

Profile: Automated Credit Card Fraud

Assessment Date: 6 June, 2003

EXECUTIVE SUMMARY

Automation of Credit Card Fraud

For several years the Honeynet Project and Alliance members have been monitoring individuals using the Internet to trade or deal in stolen credit card information. In the past, these individuals (commonly called "carders") typically acted on their own without significant organization or automation. Recently, the Project has identified an organized exchange for stolen credit card information linking hundreds of carders worldwide through specialized IRC channels and related web sites. This network provides far greater automation of a number of illicit activities contributing to credit card fraud and identity theft, including: compromising merchant sites, validating and verifying stolen credit card information, and the sale or exchange of stolen information. As with the automation and dissemination of exploit code in the vulnerability cycle, this implies a significant capacity for increased criminal activity.

WHAT IS HAPPENING

Stolen credit cards and related identity information (name, address, phone, etc.) have long been a popular form of illicit "currency" among cyber-criminals and within the blackhat community. However, the skill sets required to successfully steal credit card information online, and to successfully sell or exchange such information, have historically been limited to a relatively small number of online criminals possessing the full range of such skills.

Recently, an international network of IRC channels and related Web sites has arisen to facilitate credit card fraud and other forms of identity theft and payments fraud. Between 2 April 2003 and 13 May 2003, affiliated researchers observed over a dozen such IRC channels as traffic for these channels passed through an IRC proxy on a compromised host. The use of IRC channels and semi-covert Web sites for illicit activity is nothing new; this case, however, has several distinctive features:

***Automation of carding activities**:* IRC bots were run on many of the intercepted channels to enable and facilitate elements of the attack and exploitation process, including: target (merchant site) identification, target exploitation, card validation, card verification, and accessing open proxies used to conceal online identity during commission of crimes. Users need master only a series of custom IRC commands to carry out many key activities of credit card / identity theft.

***Distribution of carding information**:* Many of the above bot functions leverage extensive databases of application-level attacks, merchant sites to target for credit card fraud (a vulnerable site is said to be *cardable*), and credit card data, including card numbers, expiry dates, card validation values (known as CVVs) and associated personal identity information. One or more bot functions appear to draw data from third-party sources in real time, determining the validity and available credit of cards.

***Active participation of channel moderators**:* In addition to their officially sanctioned duties in assisting new users and policy channel activity, several channel moderators were observed actively facilitating and participating in illicit behavior.

The end result is that for worldwide participants on these IRC channels, many of the technical and logistical barriers to large-scale online identity theft and subsequent credit card fraud have been removed.

TOOLS AND TACTICS

The IRC channels utilized by carders provide a sophisticated set of automated response generators or "bots" to facilitate the compromise of merchant sites, the validation or verification of card info from merchant records, and access to open proxies used to conceal online identity during commission of crimes. The executable for one common bot was downloaded from its author's public web site. This bot is implemented in a monolithic script, with several associated flat-file databases that include a list of exploit URI (universal resource identifier) strings that can be executed through a Web browser to compromise a merchant website, a list of stolen identities, and a set of lists of targets (mostly Internet merchant sites) known to be vulnerable to credit card fraud, differentiated by industry (e.g. clothing, books, electronics). These tools are used in combination with an IRC client, so that text messages exchanged on an IRC channel can be monitored by the tool, which recognizes standard commands and sends responses to the channel. Such a combination of tool and IRC client functions as a bot. For example, active carders may remotely access the bot's databases, using the ***!cardable*** command to identify target merchants, and the ***!exploit*** command to obtain exploit URI strings that they may use to compromise merchant sites. Carders focus on targets of opportunity, with some vulnerable merchant sites apparently being compromised repeatedly. The ***!cc*** command, the command most often used, returns a random merchant record from a flat file of stolen credit card and identity information.

Channel participants do little to hide their activities. They transmit almost all their traffic clear text across public IRC networks, typically leveraging IRC proxies on compromised hosts to obfuscate their entry points into the network. The ***!proxy*** command requests a bot to provide the host name of an open proxy from its database and the ***!proxychk*** command conveniently verifies the availability and correct operation of a proxy.

Typically, a prospective seller of stolen identities posts a sample of stolen information to a channel, including personal identity and payment instruments, e.g. credit card numbers, expiry dates, and, in some cases, PIN numbers and CVV2 numbers. This advertising/negotiation activity is the principal online activity, with actual deals being concluded via IRC private messages or other out-of-band means not readily susceptible to monitoring via honeypots. Carders and buyers alike use a variety of commands to verify that stolen credit card data is valid; for example, ***!chk*** is used to verify the correctness of credit card numbers, while ***!bank*** decodes the identity of the issuing bank. Of particular interest are the ***!cvv2*** command, which verifies the card verification value associated with a given card, and the ***!cclimit*** command, which obtains the available credit limit associated with a given card. The existence of these commands implies significant knowledge and/or compromise of credit card networks.

WHO'S INVOLVED

Principal IRC channels used for this activity include:

#cc
#ccards
#ccinfo
#ccpower
#ccs
#masterccs
#thacc
#thecc
#virgincc

Principal associated websites include:

www.ccpower.info
www. ccpowerforms.org
www.ccpowerforums.net
www.ccsquad.org
www.ccworldz.net
www.forum-gs.net

Migration between channels and websites is frequent, complicating efforts to monitor illegal activities.

Preliminary analysis indicates international involvement in CC fraud, with the bulk of activity concentrated in South Asia and the Pacific Rim. There appear to be several distinct user groups: *lurkers*, apparently the vast majority of users, who join channels for varying periods but don't publicly participate; *active participants*, who message the channel for help using tools or to offer stolen identities or other contraband for sale or trade; and *moderators*, who monitor the IRC channels and offer support to users. Of special note is the apparent active involvement of moderators in the use of the channels for illicit activity. In addition to their sanctioned role as gatekeepers and enforcers of channel rules, the moderators facilitate illicit activity by assisting newcomers in using the bots, verifying/vouching for principal actors, and facilitating offline dealmaking. They may also have a commercial interest in the channel, accepting payments or items in trade in return for access. Finally, the existence of numerous bots and databases indicates a small, skilled base of "*power users*" driving tool development. It appears that this power-user base of moderators and toolmakers is small, probably numbering less than ten individuals. The monolithic nature of bot implementation implies a sole author, but several functionally similar but nevertheless distinct bots have been observed on various channels, implying the existence of multiple authors.

While the IRC channels are ostensibly established for carding, in practice they are also open forums for exchange of all sorts of stolen information and illicit activity, including the fencing of identities stolen offline (e.g. copied from a hotel ledger by a corrupt clerk) and stolen computer equipment. While online merchant customer records are the most common contraband, participants also offer other forms of goods and even services.

The chief motive for most participants appears to be financial gain. Typically, a prospective seller posts a generalized description of stolen identity/card information to a channel, usually including a sample in the form of a compromised merchant record. Prospective buyers may also post requests for specific goods to the channel. Many sellers are looking for someone to help them convert their contraband to cash, soliciting access to Paypal or other online payments system that originate payments from credit cards online in return for a percentage cut (typically 50-60% of the take). Others are looking to trade contraband relevant to one instrument or channel (e.g. stolen ATM PINs and account numbers) for one more familiar to them (e.g. credit card numbers with CVVs) or for non-financial goods or services (e.g. root shell accounts on compromised systems). In almost all observed cases, deals were concluded out of band, presumably via private IRC messages, or e-mail or other simple means.

There is also a significant cultural component to these channels and websites. Lurkers and newbies are frequently recruited by active users and moderators to use the tools to commit what may be their first financial crimes. Supporting material found in related Web sites promotes “carding’ as an alternative lifestyle choice rather than criminal activity.

CONCLUSIONS

By implementing and widely deploying automated aids to website attack and compromise, credit card and personal identity acquisition, concealment of identity during criminal activity, and exchange of stolen goods and services, power users within the carding community have decreased barriers of entry to the community and facilitated the commission of crimes by members of the community. The dollar volume of related crime is significant and appears to be on the increase, despite efforts by responsible IRC network operators to curtail illicit and illegal activity on their networks. By presenting their activities as a lifestyle choice rather than criminal fraud, members of the carding community entice others to join them. They pose a growing threat to the financial community, online merchants, and individual cardholders.

IRC COMMANDS IN REFERENCE TO CREDIT CARD EXCHANGE

!cardable *classification*	Returns URLs of sites known to be vulnerable to credit card fraud from a database forwarded through the IRC channel. The *classification* argument returns sites of a particular type, e.g. *electronics* returns the URL of an electronics vendor.
!cc	Obtains a credit card number from a database forwarded through the IRC channel.
!cclimit *card_number*	Determines the available credit for a specified credit card.
!chk *card_number*	Checks a credit card for validity.
!cvv2 *card_number expiry_date*	Returns a valid CVV2 number for a given card.
!exploit	Returns an exploit URI string from a database of known application-level Web server attacks.
!order.log	Provides transaction detail of compromised website.
!proxychk	Verifies that an IRC proxy is working.

INTERNET RELAY CHATS, DEMONSTRATING TACTICS & MOTIVES

A non-online source of credit card information:

```
#masterccs 02:13:38 Pedro: Hi all, i work in the LaTourista hotel here inPeru and i have access to all ccs with full info, im looking for paypal, anyone interested ??? msg me !!! i verify first!
```

Carders advertise their trading capacity:

```
#MasterCcs 12:01:41 BigDealer: ACTION have a drop thrue WU if u guys want to cash out cc  on any name u send I'll cash it out 50/50 msg me I can cash out up to 20 K a week
#MasterCcs 08:43:33 BiggerDealer: ACTION has a drop in a bank if u want to cash out stuff up to 100 000K a week msg me
```

Trading CCs for exploits and tools:

```
#MasterCcs 12:40:28 Spiner: ACTION wants 0day exploits or Redhat 7.2,7.3 rootkit. msg me for trade … i have root
```

Solicitation for channel advertisers:

```
#masterccs 08:00:34 Card-InFo: ACTION Good news For Shell Holder: If u have Shell/hosting and wanna Advertise then msg
Op1 and Op2 and Op3 We will adv urs shell/hosting wid Auto msg
```

Channel ops discuss a difficult newbie:

```
#masterccs 14:18:40 TheOp: yeah i know AsstOp^- :P
#masterccs 14:19:07 AsstOp^-: hehehe
#masterccs 14:19:27 AsstOp^-: that bastard is killing me i tried to help him but he wont tell me whats happening on the command i told him
#masterccs 14:19:29 AsstOp^-: how can i help him them stupid as
#masterccs 14:19:31 AsstOp^-: ass
```

Solicitation for a bot author or owner:

```
#MasterCcs 06:58:06 BoogieMan: I need a Chk BOT ! i'll give to the Owner Sop access to the channel
```

Carder asks operator to banish a ripper, who cheated the carder:

```
#aimtech 18:23:22 ^Alky^: Vietkey ripped me cc akick him now
#aimtech 18:23:32 ^Alky^: ACTION thank TheOp
```

A newbie receives instruction and gets his first CC:

```
#MasterCcs 10:00:49 newbie: what i have to type to get cc info ?
#MasterCcs 10:01:15 helper: type !cc
#MasterCcs 10:04:04 newbie: !cc
#MasterCcs 10:05:33 Ccs`: newbie!cc Name: Yukio XXXXXXXX |Address: X-X-X-XXX |City: Koduru-shi |State: Tokyo |Zip: XXX-XXXX |Phone: N\A
 |Country: Japan |CardType: American Express |Card Number: XXXXXXXXXXXXXXX XXXX
```

A newbie expresses anxiety:

```
#Masterccs 17:32:23 newbie: wont i get caught if i use these???
#masterccs 17:32:38 helper: mabe
#masterccs 17:32:40 helper: mabey
#masterccs 17:32:48 helper: if your smart you wont get caught
#Masterccs 17:32:59 newbie: how can i not get caught baby
#masterccs 17:33:00 helper: i boaught at least 20,000$ worth of stuff
#masterccs 17:33:10 helper: i donno figure it out :P
#Masterccs 17:33:18 newbie: awww :-(
```

Another non-online source of CCs:

```
#MasterCcs 10:43:23 traderx: i work at a credit card collection agancy and we get there banking information i need someone to drop money in and send me half we split 50/50 pls don't ripping ... loosers , i know when someone 's a ripper so don't waste my ... time
```

A non-online use of CCs:

```
#CaRd-WorLD 12:24:45 QBar: ACTION looks for someone that can create fake plastic cards with the name & card serial I provide (I have pin code for XX cards!!!)
```

A newbie expresses anxiety:

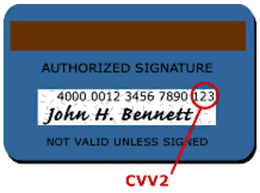
```
#card-world 21:17:27 newbie1: what is this site about
#CaRd-wOrLd 21:17:47 newbie2: why does all this look like BS to me?
#card-world 21:18:13 Helper: !chk XXXXXXXXXXXXXXXX XXXX
#card-world 21:18:20 CcVeR:  Helper [X XXXXXXXXXXXXXXXX XXXXXX ] This transaction has been Declined.
#card-world 21:18:27 newbie1: i dunno
#card-world 21:18:30 newbie1: looks the same to me
#card-world 21:18:34 newbie1: or illegal
#card-world 21:18:46 Helper: it is ILLEGAL
#card-world 21:18:49 Helper: so what if its illegal?
#card-world 21:19:00 newbie1: then what do i do with it
#card-world 21:19:07 newbie1: i like illegal
#card-world 21:19:13 Helper: lol
#card-world 21:19:23 Helper: search a valid cc
#card-world 21:19:25 Helper: and use it
#card-world 21:19:25 Helper: lol
#card-world 21:19:29 Helper: :|
#card-world 21:19:32 newbie1: no way
#CaRd-wOrLd 21:20:00 newbie2: how the hell do you confirm these cc's?
#CaRd-wOrLd 21:20:05 newbie2: especially the cvv2?
#card-world 21:20:15 newbie1: anyone know where i can get up to date direct tv files
#CaRd-wOrLd 21:20:19 newbie2: these bots have merchant accounts or what?
#card-world 21:20:22 newbie1: i cant find ... except pay sites
#card-world 21:21:53 newbie1: anyone know of a channel or server that has a lot of good direct tv hu card files and info
```

A bot owner solicits a channel op:

```
#card-world 05:09:19 RelaxedCC: ACTION Need a CC bot in your channel? /msg RelaxedCC and i will be in your channel!
```

CARD VERIFICATION VALUE (CVV)

A card verification value, or CVV, is a three- or four-digit number printed on a credit card (and encoded on the mag strip) for fraud protection. It provides a cryptographic check of the information embossed on the credit card. The use of the CVV in an online transaction is intended to signify the physical presence of the card at the transaction's origin, e.g. in the hands of an online customer, thus reducing the occurrence of credit card fraud in card-not-present transactions. Unfortunately, as CVVs have been captured and stored in merchant databases that are subsequently compromised, the anti-fraud value of the CVV has recently diminished. (See http://usa.visa.com/business/merchants/fraud_basics_cvv2 for more information.)


AUTHORIZED SIGNATURE
4000 0012 3456 7890 123
John H. Bennett
NOT VALID UNLESS SIGNED
CVV2