RC23741 (W0510-039) October 10, 2005
Computer Science

IBM Research Report

Electronic Identification as Economic Commodities in the Black Market

Alan Boulanger
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598

Research Division
Almaden - Austin - Beijing - Haifa - India - T. J. Watson - Tokyo - Zurich

Alan Boulanger
Global Security Analysis Lab
TJ Watson Research Center
IBM
boulange@watson.ibm.com

July 22, 2005

Electronic Identification as Economic Commodities in the Black Market.

Abstract:

The business world has transformed from small localized physical markets into a massive global virtual marketplace. As this electronic marketplace continues to grow and expand there is increased dependence upon the reliability of electronic identities. These virtual identities are the basic foundation of this electronic economy and their use facilitates everything from simple telephone calls to the purchase of on-line goods and services. All transactions in this marketplace rely on an electronic identifier in some form and thus ensuring the security and authenticity of this information is of the up most importance. The current gaps in security has provided criminals an opportunity to profit from the acquisition, trafficking, and use of these electronic identities. Every acquired identity can provide a criminal with anonymous access to high valued goods and services with a very low risk of prosecution. The U.S. Government Accounting Office reported in 2002 that the prevalence and cost of identity theft is growing at a rate of 40 to 50 percent per year(1). The federal trade commission reported that identity theft cost consumers and businesses over $50 billion in 2003 alone and is growing at an alarming rate(2).

As with any valuable commodity, these electronic identities themselves have an intrinsic value and are actively exchanged in underground virtual marketplaces around the world. The subject of this article addresses the trafficking of stolen electronic identities and how various elements of that market impact the street-value of the commodity. The data for this article was obtained through interviewing investigators from federal law enforcement agencies and the financial service sectors, who are actively investigating electronic identity theft, as well as former 'informants' who have at one time participated in this shadow economy.

Definition of Electronic Identification:

There has been some definition drift of the popular term "identity theft". For the purposes of this article, identify theft will be limited in scope to theft, or impersonation, of an electronic identifier by an unauthorized user. An electronic identity will be defined here as any data that is used to identify and, in part, authenticate, a particular individual, or device, accessible through an electronic network. Law enforcement would consider this data to be an "access control device".

Examples of electronic identities include:

- Cell phone credentials.
- Credit card numbers and PIN's.
- Financial account information and PIN's.

Cellular Phone Electronic Identity Theft:

An mature example of widespread electronic identity theft occurred in the cellular telephone industry. The first wireless telephone network to be widely deployed was the Advanced Mobile Telephone System, or AMPS, developed by AT&T in 1983. In AMPS network, every handset had an 32 bit immutable electronic serial number, or ESN, installed during the manufacturing process. This code was used to uniquely identify the device. When the handset was activated, the dealer would then program the handset Numeric Address Module, NAM, with the subscriber's 10 digit Mobile Identification Number (MIN). Once a handset had the valid ESN/MIN pair, it would be allowed access to the cellular network and be able to make and receive calls. Airtime usage was recorded and billed to the subscriber associated with the MIN of the handset.

One of the serious problems with the AMPS network was the lack of security and confidentiality of the system. The system utilized a simple analog radio signal making the system vulnerable to eavesdropping. Anyone with an inexpensive radio frequency scanner was able to scan for and listen in on cellular telephone conversations.

Another problem was the electronic identifiers (ESN/MIN) for that phone were transmitted unencrypted on these open channels. Using a scanner and a simple decoding circuit, these electronic identities were easily intercepted and decoded. Once the electronic identity of a phone is acquired, it is then possible to transfer the identification to another handset and create a clone of the legitimate subscriber's phone. All calls usage made with the cloned phone will be billed to the subscriber's account and thus created a opportunity for fraud.

From 1983 to 1989 there were few incidents of cellular phone fraud through cloning. Then in 1990, the technology to acquire and reprogram phones began to emerge. At the time, cellular phone usage was much more expensive and thus provided enough motivation to discover ways to obtain free cellular service.

Emergence of phone cloning

In the early 1990's, there was estimate 5 million cellular telephone subscribers paying an average of approximately $100 per month in usage fees. During this time the capability to clone the phones of these subscribers became widely available (figure 1). Cell phone enthusiasts were the first group to start cloning phones for personal use. These enthusiasts, or "phreakers", communicated with each other and began exchanging information on how to program and clone cell phones. At this time, much of the communication was conducted in voice bridges and electronic bulletin board systems (BBS) and the emerging Internet Relay Chat rooms (IRC). Soon these individuals began exchanging electronic identifications (ESN/MIN) pairs.

Criminals soon recognized the utility of this new cloning technology. With a cloned phone a criminal can make free phone calls with very little risk of detection and prosecution. For a criminal group, a cloned phone is an ideal communication device. Since the electronic identity is associated with a legitimate subscriber, there is less of a chance of the phone being tapped by law enforcement. At the time, the wiretaps laws were limited in scope to that of the old land-line PSTN model. Only a specific phone number could be subjected to a wiretap. A cloned phone could also be used in a criminal enterprise such as a "call-sell" operation. A call-sell operation is where illegal long distance phone service is sold to individuals for a small fee. The operator would fraudulently obtain long distance service and then rent the phone to someone who could then make expensive overseas long distance phone calls.

As criminal interest in cell phone cloning rose, so did the demand for electronic identifiers. What was once the domain for hobbyists and phreakers, was becoming a full criminal enterprise costing the service providers millions of dollars a month in losses. This is turn transformed the electronic identifier of cell phones into a marketable commodity.

In the early 1990s the underground price for a working ESN/MIN pair was approximately $50-$100. Phreakers at the time had some difficulty in obtaining the ESN/MIN pairs as the technology was immature and not capable obtaining the information in bulk so the supplies of working pairs was limited. The price was also influenced by the lack of billing controls by the service providers who, at the time, were less able to detect fraudulent usage. As a result, each ESN/MIN pair was likely to generate a high yield of usage before being detected and shut off by the service provider.

As the cloning technology matured, so did the demand for electronic identities. In 1993-1994, the cellular phone industry began seeing a sharp increase in fraudulent usage. The information on how to capture and clone cell phones was widely available. The criminal community generated huge demand for cloned phones and thus began the wholesale acquisition and distribution electronic identities. Devices that automated the capture of ESN/MIN pairs were manufactured and distributed in the black market (figure 2). Hacker's began attacking the service providers directly to obtain subscription information. This data was stolen and actively traded on BBS's, IRC chat rooms and the emerging World Wide Web. The underground market became flooded with ESN/MIN pairs and the cost of acquiring an electronic identity dropped dramatically from $50-$100/pair retail, down to $10-$15/pair retail, and $2-$5/pair, wholesale for large blocks of numbers. Also influencing the price of a electronic identity was the net yield of service per identity began to fall. The service providers deployed anti-faud measures and were better able to detect and quickly react to cellular phone fraud. This countermeasure in part reduced the intrinsic value that was obtained from each electronic identity. Criminals seeking convert communications with a cloned cell phone would find their phones were shut off more quickly. Call-sell operators were forced to purchase more identities as their phones were getting shut off sooner or were denied long distance service.

In an attempt to curb cloning, some service providers began requiring PIN's to be used when roaming. If a subscriber traveled outside their home area, the network would require the customer

to enter a code to be able to resume service. If the code was not entered correctly then service was suspended until the subscriber returned to their home area.

This simple countermeasure had a profound impact on the price of older ESN/MIN pairs. The street price for an identity without PIN fell from $10-$15/pair retail, and $2-$5/pair wholesale, down $1-$5/pair retail and $.10-.$50/pair wholesale. The underground market was being flooded with non-working and limited use electronic identities. This situation caused an sharp drop in demand for the older identities and increased the demand for complete sets of ENS/MIN/PIN based identities. In 1997-2000, an identity with PIN would retail for about $20/pair and wholesale for $2-4$/pair with PIN in the underground market.

In late 1990's the service providers were suffering large losses. The Cellular Telephone Industry Association reported at that time that cellular phone fraud could exceed $1b in 1996 and then in 1999, the US Secret Service statistics reported that an average fraud loss per cloned phone was $1,606. The service providers responded to these mounting losses by introducing improved digitally authenticated technologies such as CDMA/TDMA and GSM. These technologies utilize spread-spectrum radio frequencies to provide greater capacity as well as thwart electronic eavesdropping. In addition to ensuring the privacy of the cellular subscriber, these technologies greatly benefited the service provider by reducing the ability to clone digital phones.

As digital cellular technology because more widely adopted, the intrinsic value of stolen cellular electronic identity plummeted. The cellular service providers had implemented a technology that rendered all of the devices used to eavesdrop and capture electronic credentials obsolete. The addition of stronger authentication to in-call connection setup made cloned phones easier to detect and lock out of the system. The phones themselves became so difficult to clone that it became impractical and unprofitable for criminals to continue their use. The underground trafficking of stolen ESN/MIN pairs dried up and today, in 2005, there are only isolated incidents of cell phone cloning activity.

The technological barriers were effective in reducing the demand for ESN/MIN pairs. However, it had little impact on the demand by criminal groups for a means of untraceable, anonymous communication. As the service providers clamped down on the technology of cellular phone cloning, they saw a corresponding increase in another type of criminal activity. Subscription fraud.

Subscription fraud occurs when service is acquired using fraudulent or stolen financial information, usually in the form of credit card numbers. Criminals will use stolen financial identities to either subscribe to cellular phone service or purchase prepaid cellular, or disposable, phones. Using stolen credits cards work well in that it is likely that the phone will be viable for at least one credit card billing cycle before being detected and having it's service terminated. As with cloning phones, criminals know they are able to acquire anonymous cellular service with very little risk of prosecution and that it is far easier to obtain stolen financial identification than it is to overcome the technical barriers associated with cloning digital phones.

Financial Identity Theft:

Credit card fraud if the most common form of electronic identity theft today. Individuals and organized criminal groups acquire credit card credentials and use them to purchase goods and services. A recent report estimated that credit card fraud will cost on-line business as much as $50 billion in 2005 and cost US retailers $1.5 billion a year annually(3). These figures represent about 2 per cent of all on-line, card not present, or CNP, transactions.

Credit card fraud increased dramatically on the heels of the emerging Internet and World Wide Web. The World Wide Web shifted the focus of the Internet from academia and research to that a an electronic virtual marketplace where goods and services can be obtained on-line with an electronic payment - usually by credit card.

In the 1980's credit card fraud became more common. Individuals, know as "carders" would use stolen credit card information to make purchases such as computer equipment or airline tickets. These purchases were often made over the telephone and the items were delivered to a drop site specified by the carder. In the early 1990's the emerging Internet streamlined this process. More goods and services were available on-line and the preferred method of payment for the new e-merchants was the credit card. This provided an opportunity for criminals to safely make purchases with stolen credit card information with a few simple mouse clicks. The technology at that time was so new that there were few investigative techniques in place to detect and trace this illegal activity.

This new marketplace caused an immediate increase in demand for credit card information. As with the cellular phone credentials, credit card credentials soon became a marketable commodity that was actively exchanged in the underground market. As with cellular phone fraud, at first these electronic identities were simply exchange amongst small groups of people. These individuals would then make as many transactions as possible until the fraud was detected and the credit card denied.

As more people participated in this activity the demand for valid, working credit cards grew and people began selling credit card information on BBS's and the Internet in web servers and IRC chat rooms. In the early days of e-commerce, on-line merchants would require a name, address, valid credit card number, expiration date, and delivery information, to complete a transaction. The information required to make an on-line purchase was easily obtained. Individuals would steal mail, and forage through trash (dumpster diving) of individual and businesses to obtain copies of credit card transactions. This information was then either used to commit fraud or sold to other criminal groups. In the late 1980's and early 1990's a valid credit card number could be purchased for approximately $50-$75 retail each and $1-$5 each wholesale in blocks. This price was influence by the high probability that the card would be viable and have a high yield before being denied.

On-line merchants and payment processing centers would store the customer information their servers thus making them an attractive target. Hackers would then attack a vulnerable systems and download the customer database and acquire thousands of valid credit cards numbers. Soon the underground market became saturated with card information and the cost of acquiring a valid

credit card began to drop. Also during this period, antifraud technology was developed and deployed to address the rising rate of on-line fraud. This technology was able to detect suspicious account activity and deny authorization until the charges could be verified. As a result of these countermeasures, stolen cards were less likely to work and combined with the large supply of stolen card credentials, the price of obtaining a stolen credit card fell from $50 in the late 1980's, down to $10 retail in the mid-late 1990's.

In 2001 online merchants plagued by losses resulting from charge-backs were required by the major credit card companies, to include a security code, such as CVV/CVC/CID, to complete the transaction. The CVV/CVC/CID is a code that is printed on the back of an issued credit card. The introduction of the CVV/CVC/CID code was an attempt to thwart the use of credit card information that was stolen from the either receipts or "skimmed". Skimming a credit card involves recording and decoding the data residing on the magnetic strip (figure 3). In 2001, the major credit card companies, mandated that the CVV/CVC/CID code be used in the authorization and processing of all card-not-present transactions. After the transaction has been authorized, then the CVV/CVC/CID code is to be discarded and not stored in any way.

This simple requirement had the same immediate effect on the street-price of stolen credit cards as the PIN requirement for roaming had on the price of ESN/MIN pairs. The existing inventory of stolen credit card numbers in circulation became practically worthless.

This countermeasure did not dampen the demand for stolen electronic credentials.
It sparked the demand for more complete credit card information. To obtain this information criminal groups sought other points of vulnerability in the system. Since the security code requirement mandating that the security code never be stored, compromising an e-merchant would not likely be profitable. So instead criminal groups began attacking softer targets; financial institutions, credit card processing organizations and consumers directly. The focus of attack had also shifted. Once content with acquiring credit card information, these new attacks sought electronic banking information, as well as the personal information of individuals.

During this time there was reported a large increase in what is know as "phishing" attacks. In a phishing attack, a criminal sends unsolicited e-mail to a large number of Internet users. This e-mail will appear to have originated from a financial institution, e-commerce web site, or on-line payment system. The contents of the e-mail will attempt to solicit account information, or direct the victim to click on a link, in order to carry out some transaction. The link will bring the victim to a web page masquerading as the legitimate counterpart where they are prompted to enter their credentials and personal information. This information is recorded and routed back to the criminal. Once obtained, this information can be used to impersonate the victim's identity and commit fraud or takeover the victims account.

Phishing is generally not efficient method for the bulk collection of identities as the percentage of the number of e-mail lures sent to the number of replies received is very small. However, the massive volume of phishing attempts can collectively generate a sufficient number of complete valid electronic credentials to be worth the effort.

Several years after the credit card companies mandated the inclusion of the security code, criminals developed the ability to generate these security codes themselves. Once again access control information became as easy to obtain and exploit as before. Criminals seeking electronic credentials once again targeted on-line merchants and financial institutions. Identities of individuals where physically stolen from mailboxes and harvested from trash containers. Phishing was widely employed and lures in the form of unsolicited e-mail was sent to millions of Internet users. Complete personal information (name, address, SSN) profiles were made available to on-line subscribers. The market for electronic identities again flourished.

Today‘s market.

Today there is an active marketplace for financial identities. Millions of access devices and personal information records are exchanged monthly in covert chat rooms and underground Internet portals around the world. These marketplace are often run by criminal organizations seeking electronic credentials for the purpose of committing financial fraud.

Hackers who have acquired an inventory of stolen credentials will often want to get rid the evidence of their crimes quickly. They will then seek to wholesale these identities to an black-market broker. The broker is often part of an organized criminal enterprise that resells that access devices to the retail black-market as well as use the devices for their own financial gain.

Black-market brokers often begin by setting up shop on IRC channels. They will run an automated ‘bot’ that is used to mediate the exchange of electronic financial identities, or “dumps”. For low-grade electronic identities, the transaction can take place directly on the IRC channel. A person interested in purchasing a block of access devices will advertise the number of devices as well as the payment terms. Payment requirements involve an immediate cash transfer or payment though a on-line payment system to a specified account. Often a seller will resell the same block of stolen identities to multiple buyers and, as a result, a larger percentage of the identities will generate little or no yield. This is why carders consider electronic identities purchased directly on IRC to be poor quality.

Once a block of identities is acquired, the buyer can then begin to verify the quality of the product using what is known as a “dump check”. A dump check verifies the validity of a credit card by posting a small, usually $1.00, charge to the account. If the card is valid, then the account is credited with the same amount. Because the amount is small, and there is no net loss to the consumer, most consumers will not notice the charge, or, if they do, assume is was a mistake that was corrected and will not report the activity as suspicious.

More sophisticated marketplaces will start in IRC but buyers will then will be directed to temporary web sites (figure 4 & 5). The web sites are anonymous as they have been established on a computer that has been compromised by hackers. Brokers usually have access to a large collection of hacked systems in which to set up shop. The average life span of a particular server is usually only a few weeks. Transactions in these systems are usually among a group of trusted individuals and entry into this market is by referral only.

Most of these brokers and markets are located overseas and in countries that are less likely to cooperate with US law enforcement. Therefore, the risk of getting arrested by the local police and extradited to the US is very low. It is from these countries that the brokers will utilize the newly purchased access devices to commit financial fraud. The first requirement is securing access to an anonymous method for retrieving their funds. Getting cash advances and draining bank accounts is of little use unless they can cash out safely and anonymously. One way to accomplish this is to post advertisements on the Internet, and in publications, seeking someone to act as a financial proxy, or "mule". The advertisement will often be pitched as a work-from-home job or business opportunity. The job of the mule would be to open an bank account and accept funds. Whenever funds are deposited into the account, the mule will retain a percentage of the deposit and send a money order of the remainder to the broker at their overseas drop site address. This arrangement is ideal for the broker. It is very safe in that there is nothing directly linking the mule to the broker. Any investigation of fraud will terminate at the mules' account. The only information the mule can provide to investigators is the address to the overseas drop-site. Since the funds are exported as cashier's checks the broker has immediate, anonymous, access to their money. This type of low-risk high-yield criminal activity is directly responsible for a large percentage of identity theft

Today, in the "St Petersburg market", electronic identification (name/account information) can be purchased wholesale for several dollars each. The actual access devices sold per transaction are usually in blocks of 1000 identities. Of every block sold, only a certain percentage of the identities will be viable. Depending on the volume of the purchase and the timeliness (length of time in circulation in the black market) of the access devices, the prices range from $.50 per to $3 US on IRC, ICQ, temporary web sites.

The current retail street price for one valid access device (credit card) with basic personal information (DOB, SSN) appears to have stabilized in the $7 - $10 US range wholesale. This pricing structure is based on receiving a substantial block of 50 or more electronic identities. Usually blocks if electronic identities will not be broken down into smaller blocks unless the purchaser is a close or preferred associate of seller.

As a personal profile becomes more developed, with the addition of credit agency-type information with more complete and active banking information, the price increases to $50 - $75 US. This price range is similar to that of a simple credit card profile in the 1990's . Some extraordinary profiles can demand retail prices in the $150 - $200 US range. Another tactic for determining street-price works on a percentage basis where the cost of a profile can average 1% to 1.5% of victim's credit limit. Identities of wealthy targets, those with higher credit limits and regular international travel that will not invalidate after a foreign purchase, have been known to may push the percentage scale up a half-point or more. A small premium is can also be given for corporate cards as these have a longer shelf life than personal identities.

Debit/ATM cards with a PIN are naturally the "holy grail" for card makers due to potential street appeal. "Theft Potential", duplicity issues, and economics dictate the price of these identities and there is no average set price associated with these cards. Oftentimes the price is determined by the balance and history of the account. If the account has a low average balance, then transferring

the funds to a mule or drop site may not be worth the acquisition costs. However, accounts with large average balances and low levels of activity are the most lucrative.

Conclusion:

Electronic identities have a black market street value directly related to the benefits they can generate for a criminal enterprise. The value of these transferable commodities is influenced by the same economic forces that shape any marketplace: supply and demand. In the communication industry, the demand for ESN/MIN pairs was fueled by the benefits derived from cloning cell phones. The supply at the time was limited by the ability to acquire pairs and as a result the price stabilized in the $50-$100 US range. Several years later, the capability to acquire ESN/MIN pairs in bulk was optimized and the resulting increase in supply drove the street price down to $10-$5 per pair. The introduction of PIN's dropped the demand for older pairs and increased the demand for the new triads. Finally during the mid to late 1990's the switch from an open analog system to the new authenticated digital system introduced an insurmountable obstacle to phone cloning. As a result, the demand for stolen ESN/MIN information dried up and effectively ended phone cloning. However, this disruptive technology did not reduce the demand for illicit communication, but rather pushed the criminals to find the next weakest link. In the case of the communications industry, as the rate of fraud dropped due to the inability to clone cell phones, there was an corresponding increase in subscription fraud. Criminals found the next weakest link in that it was far easier to use stolen financial identification to obtain service than it was to use stolen cellular phone credentials to clone a phone.

The underground market for stolen financial identities appears to be following the same trends as with the trade of ESN/MIN information in the early-1990's. If the financial industry were able to deploy a similar disruptive technology, such as a perfect fraud detection system, there would be a abrupt drop in the demand for stolen financial identities and the black market for such commodities would be shut down. However this hypothetical technological barrier would not diminish demand for illegal access to financial services. It would simply motivate the criminal elements to seek the next weakest link in the system. As with the communications sector, any solution that reduces fraud with stolen financial credentials will likely contribute to a corresponding increase in application fraud. Application fraud is fueled by the availability of personal information than can be easily acquired. Protecting personal information is a challenging technical problem and any proposed solution should carefully research the potential weakest link in the new environment with the same vigor as the people seeking to exploit it.

Figure 1.


CE EVIDENCE
EVIDENCE
CellPhone
ESN
Reader
ESNR-5900C
CURTIS
ELECTRO
DEVICES
50859007

Figure 2

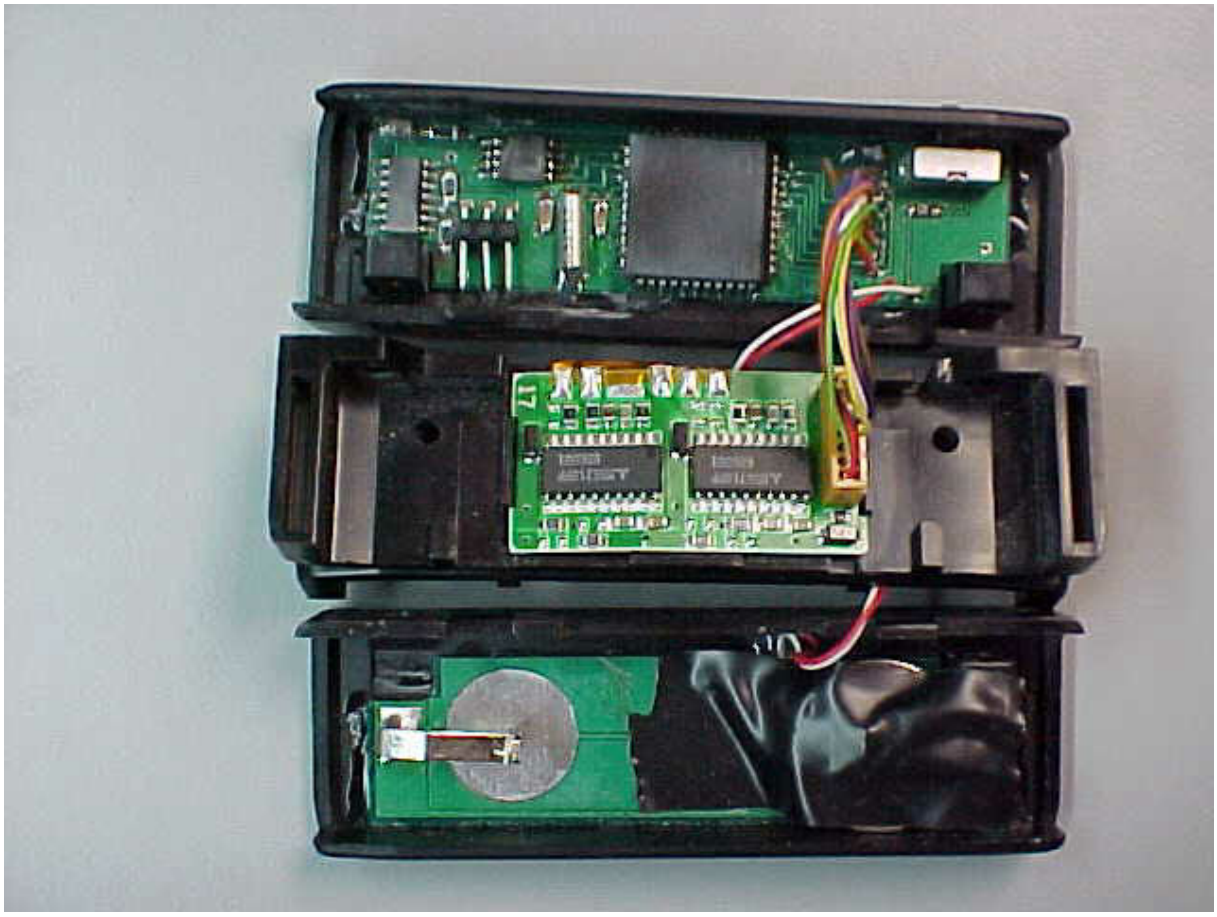

Figure 3.

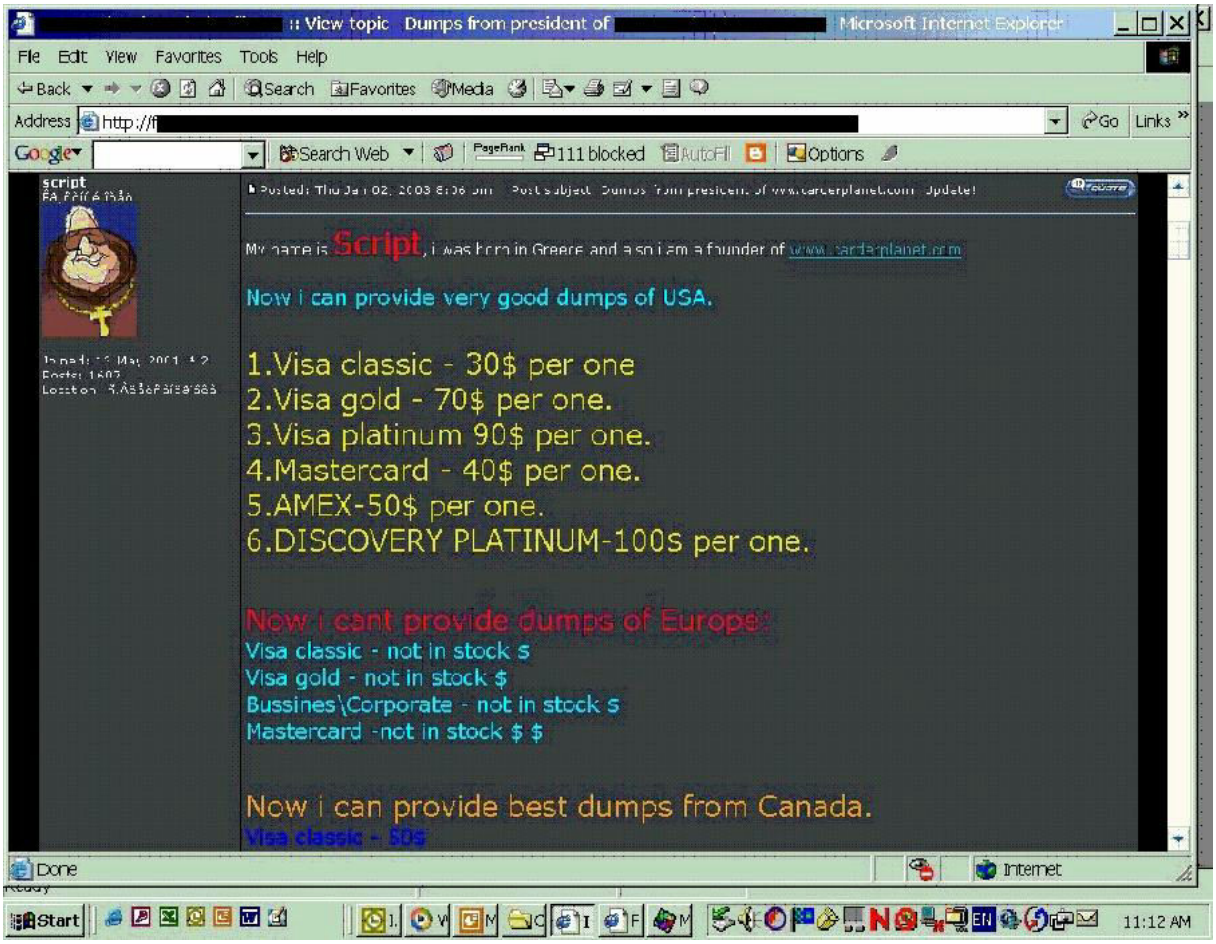
:: View topic Dumps from president of
Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://
Go Links
Google Search Web 111 blocked AutoFill Options
script
My name is Script, i was born in Greece and also i am a founder of www.cardersplanet.com
Now i can provide very good dumps of USA.
1.Visa classic - 30$ per one
2.Visa gold - 70$ per one.
3.Visa platinum 90$ per one.
4.Mastercard - 40$ per one.
5.AMEX-50$ per one.
6.DISCOVERY PLATINUM-100S per one.
Now i cant provide dumps of Europe:
Visa classic - not in stock s
Visa gold - not in stock $
Bussines\Corporate - not in stock s
Mastercard -not in stock $ $
Now i can provide best dumps from Canada.
Visa classic - 50s
Done
Internet
Start
11:12 AM

Figure 4

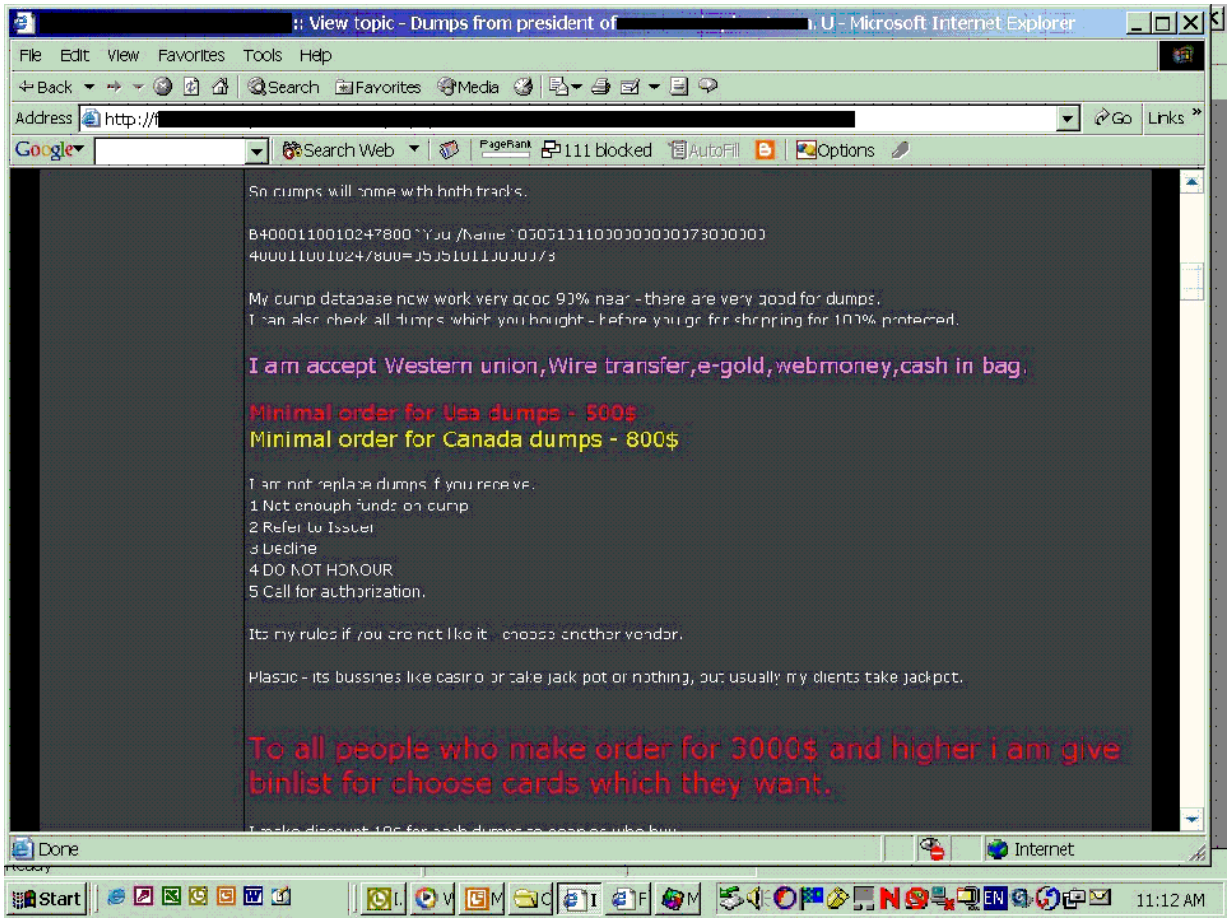

Figure 5

References:

1. Government Accounting Office : GAO Report - 02-766 : June 2002
2. Federal Trade Commission report, http://www.ftc.gov/opa/2003/09/idtheft.htm
3. Epay News.Fraud statistics summary, http://www.epaynews.com/statistics/fraud.html