Project date: 02/17/2009 3:28 AM

info@ultrascan-agi.com

unedited version

Five Levels Ultrascan

Third level Ultrascan

Subject: Ultrascan-AGI Cyber Crime Market Research for ATM Skimming Devices

Amsterdam: 17 February, 2009

1 Skimming losses: a low estimation

In 2007, total worldwide skimming related losses were over US $ 1.2 billion a year.

Based on Wincor Nixdorf's ATM market share, we estimate Wincor Nixdorf ATM related losses were (minimum) US $240 million.

In 2008 and 2009, we see an increase in the number of criminals active with skimming, indicating an increase in total skimming losses.

While researching the stolen card trade on the ten most important (underground) markets, where tens of millions of cards are traded, we saw an increase in offered cards of 900% (!) in the second half of 2008.

2 Wincor Nixdorf and skimming

Wincor ATM's have been a skimming target since the beginning of 2002.

2.1 Recent history of skimming

Skimmers have been sold by public criminal "verified vendors". The first skimming models that entered the Dutch market were mainly manufactured for the older ATM models, but they also fitted the new ATM's.

In the past six years we have seen a number of different criminal vendors becoming successful. The two most notorious names were "**Dron**" and "**Cha0**".

We will focus on these two vendors because both cases can be verified.

2.1.1 Dron

Nicholas Joehle, a.k.a Dron, was caught early 2007 – please see the FBI press release http://www.scribd.com/doc/1275910/US-Treasury-GPA0707-investigations.
Dron was the number one vendor because he had been active in the internet underground for many years. He was not a government employee and his identity has never been cloned by the FBI or USSS. His products were sought after because of their high quality and the steady supply.

Each year Dron released updates for his skimming products. If a skimmer passed the concept phase, the vendor manufactured it in bulk, making sure he would have at least 200 to 400 skim sets in stock to meet demand.

The **bezels**, that are manufactured tailor-made, are crucial and can only be ordered in BULK in Asia (*Hong Kong, China*).
A vendor typically supplies 200 to 400 first line buyers or independent distributors, who are organized in so-called Open Source Criminal Networks (OSCN). They pass the skimming sets on to the actual skimmers, operating in cells that travel around the world and always have enough skimming sets available to offset possible losses.

2.1.2 Cha0

The Turkish ATM hacker and skim set developer Cha0 has been arrested recently, according to "official sources". However, according to our own technical and human intelligence, Cha0 is still a free man and his organization thrives.

Cha0's goal in life is to build an OSCN that defines cyber crime and influences society, based on an anonymous cell structure and equipped with in-house developed technical equipment.

Starting early 2004, Cha0 mainly sold re-engineered POS terminals in small numbers for about euro 5.000 including mini camera. Only by the end of 2004 did he start selling ATM skimmers.
Cha0 has carefully built his business empire by convincing small selective groups of customers of his trustworthiness. At the same time he has managed to get thousands of followers through his cyber crime discussion fora. At this moment he has a following of at least ten thousand elite cyber criminals.
He is using his in-house developed open source card reader software as a marketing tool to attract new members and to build his reputation, giving it away for free.

An advertorial for Wincor Nixdorf and NCR skim products:

we sell the equipment. But we do not sell to anyone and anytime. To buy the GSM skimmers you should have recommendations, only in that case we can talk about the deal. We sell the equipment from stock anytime because we do have the assembled equipment. Sometime we assemble special suites and sell them, but we do not always have assembled suites in stock. That's why when we offer you're the equipment here and now, you'd better buy it immediately because, say, in a week we wouldn't have them in stock.

The product line
(ProCash 2050) – the most popular model in Europe. Reliable, easy to install model with anti-vandals shell
http://********www.wincor-nixdorf.co...050/index.html
(ProCash 2150) - Reliable, easy to install model with anti-vandals shell. Comparing to the 2050 is not so widespread in Europe.
********www.tusson.com/content.php?code=29
(NCR 5684) – the most popular model in the central and southern Europe. Reliable, easy to install model with anti-vandals shell. Most generally used in southern European countries, USA, Africa states, and Australia. The model is very easy to install into, it has the best disguising (masking) shell of 2008
********www.criso.com/atms/5684.html
(NCR 56845 is not so widespread as 5684 is. Most generally used in southern European countries, USA, Africa states, and Australia. The model is very easy to install into, it has the best disguising (masking) shell of 2008
http://********www.moneyhandlingmach.../ncr_5685.html

We can also provide you with two-model set.
(suitable with ProCash 2050 and ProCash 2150)
(suitable with NCR 5684 and NCR 5684)
The two-model set simplifies the task of finding ATM by twice. Thus, you can find more profitable and ease places for

installing the equipment.
* Don't mix up ProCash 2050 and ProCash 2150 with ProCash 2050XE and ProCash 2150XE. The latter have the port for earphones of blind people, the shell can not be installed on these models.

Prices
All models have the same price.
1 set = ? 8.500 + shipment costs
2 sets = ? 16.000 + free shipment
3 sets = ? 24.000 + free shipment
4 sets = ? 32.000 + free shipment
5 sets = ? 40.000 + free shipment
The price for two-model set is ? 9,800

We always quickly ship orders
We ship orders worldwide. I don't like unresolved questions that's why it pays to deliver the order ASAP as we receive the money. The faster we send the better we sleep. That's why we talk about selling only assembled and ready-to-go devices. In other words, you wouldn't wait ages while your equipment is being assembled, tested etc. We sell only tested equipment.

How we do tests?
1. Every devices are tested for bugs during 24 hours marginally.
2. Every shell is tested on the native model to ensure ideal installation
3. Every shell is thoroughly checked for painting defects etc, the client receives defects free equipment
Shipment methods, terms and details are defined individually. We conduct shipment of every order using different methods, from different cities and countries for the security purpose.

Clients support
After the purchase the client can receive any advise on configuring software, equipment tuning, security matters and others. We give you recommendations based on a solid experience.
The client is never left face to face with his problems. You get the answers instantly, so we will help you to understand how it works, how to install the equipment and will give you advice on the real work.

Cha0 is the first one to develop a bespoke skimmer for the Wincor Nixdorf ATM models. Currently, this skimmer does not fit the Dutch ATM's, because they have been fitted with anti-skim sets.
However, our researchers believe that in 2009 countries such as Venezuela and Morocco, where law enforcement and banks have little knowledge about skimming, will show a major increase in skimming activities.
In these countries ATM's are often positioned at insecure places, there are few security protocols in place and bank employees are willing to co-operate in skimming deals to add their low wages.

For example, the village of Tarquist in Morocco.
Here you will find an ATM at a station, where after 21:00 hours only junks roam about. The only law enforcement available is a young soldier observing by passers, and who is usually smoking a joint from locally produced hashish. Police is not available in such villages, only soldiers, who visit the village on occasion to prevent local fights.
There is no law and order.

2.2 Accessories

2.2.1 Pin pad

The pin pads that are currently offered in the market are ideal for every Wincor Nixdorf ATM. The old 3mm pad has been made even thinner (photos 1 and 2) to counter the new design changes that have or will be implemented by Wincor. The keys now have the exact size and they have solved the spongy effect.
These pinpads have a built-in GPRS module that communicates directly with a mobile telephone. After each second 'track + pin code' an SMS is sent with the information. These new pinpads use Sony Ericsson 850i mobile phones to send the data by SMS. The batteries of the 2008 generation pinpads usually are from Nokia or Motorola, because of their endurance and compatibility (2-3 days in a warm climate).
The non-GPRS skimmers use a Flash MB card and a ROM chip connected to the strip reader. All other bonus details, like stickers, are normally only used for skimming operations in third world countries such as Morocco (http://www.swipeusa.com/product_pages/accessories.html).

2.2.2 Camera's

For cameras mini cameras can be bought in spy shops. Currently, an exact time stamp in the format 00:00:00 is added to the pictures.
The first skimmers by Dron and Cha0 also had mini cameras. But, especially, the media attention prevented further use of cameras by most skimmers. They rather take the risk of losing the skim set, flash card and stolen data.
Some skimmers use 'multilayer printed-circuit boards', like the ones in a pc, laptop or mobile, to store the pictures.

2.2.3 Bezels

The bezel is the piece of plastic that actually fits in the card reader mouth. These are manufactured bespoke in size and ATM colours in Asia and produced in bulk. Manufacturing and production is flexible and can be quickly tailored to the customer's wishes or to adaptations by ATM manufacturers.

2.2.4 Data processing

The software for data processing is developed by the same persons that develop the skim sets. The software manages the whole skimming process and encrypts the data before it is sent by the GPRS module.
With the same software, the encrypted data can be copied directly on to a clone card, preventing the skimmer from manually processing the data, eliminating an extra step. This also makes prosecution more difficult.

2 2009 Expectations

2.3 Vendors

Ultrascan-AGI expects the top ten vendors to develop their distribution channels and increase the number of associated elite cyber criminals.

The total number of vendors will likely increase because their cross border operations and the differing national laws will make it hard to prosecute them.

Retired skimmers will become the new vendors. Their motto: hand out ten skim sets for free and you will be a multi millionaire within a month.

There are more crime cells and older skimsets will be used in countries where ATM's do not yet have anti skim devices.

2.4 ATM Skim sets integrated in the Anti skimmer

Recently, Russian crime labs developed mini skim sets (see picture) that will be integrated in the anti skimmer . The anti skimmer will be replaced by an exact replica, placing a very small reading strip on the mouth of the ATM anti skimmer.
The goal of the developers was to develop the smallest possible skim set that would deal with the anti skim set.

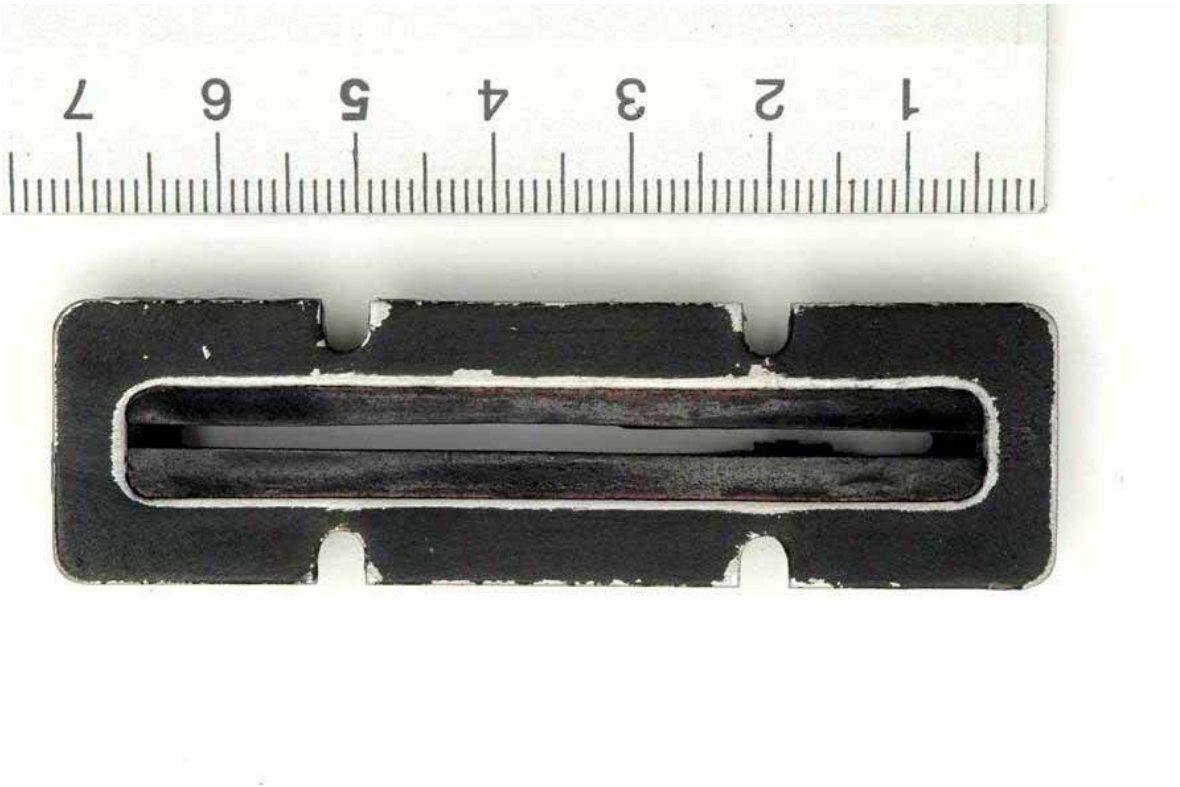

Photo 1. Smallest skimmer after test runs

Starting November 2008 competing OSCN's are planning to develop even smaller skim sets that leave out the plastic parts and only use the bare minimum: a strip with a plastic piece and a small disk would be enough.
New skim sets for the smaller ATM's have been taken into production, also because these smaller ATM's have become more common in the rest of the world.

Photo 2. The new very thin key pad, side view

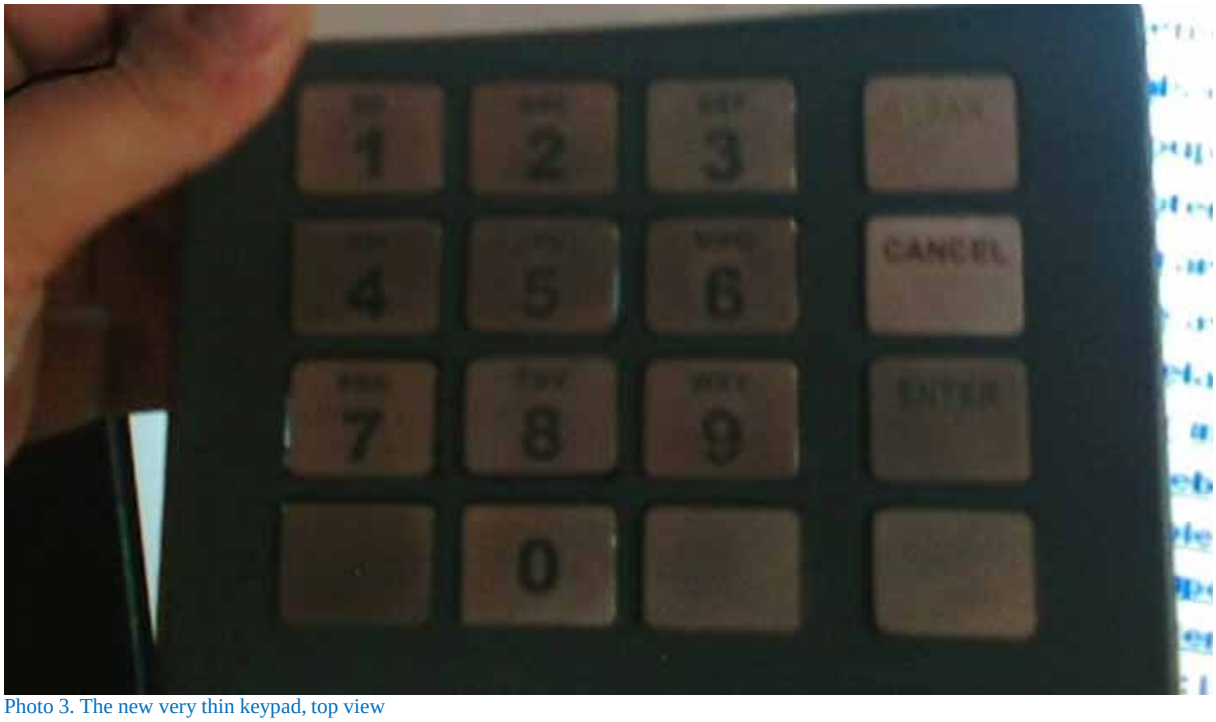

Photo 3. The new very thin keypad, top view

Photo 4. Back side plastic bezel.

Photo 5. Front side plastic bezel

2.5 Information leap of criminal networks

The criminal vendors and groups of elite cyber criminals have knowledge about all product improvements that are being developed and implemented in the banking industry. This knowledge is available because of low compliance demands, insecurity, infiltration and corruption at banking organizations, supervising (government) regulators and suppliers.

In 2009 several countries will implement new security protocols to prevent skimming with non-embossed cards. Non-embossed cards will not be accepted or swallowed by ATM's. However, Ultrascan-AGI believes the effect will be limited because the OSCN have taken up the distribution of card embossing machines, enabling criminals to print any card.

Dynamic control on card transactions will increase, thereby limiting the use of skimmed data. This will limit the damage, but will not decrease the number of criminals or incidents.

2.6 Anti skim enhancements

In 2009 anti skim enhancements will force skimmers using old(er) skim sets to relocate to countries that have not (yet) implemented anti skimming measures, and where banks and government are unprepared for skimming.

The Netherlands has anti skimming alerts on NCR models: 5684/5685
France has anti skimming alerts on NCR 5884/5885 and Wincor 2050/2150

Green anti skimmer within the EU: NCR 5886

Most anti skimming sets that do not send alerts because they are not electronically connected. This applies to a significant number of Wincor models: 2050/2150.

2.7 Chip and PIN

Knowledge about 'Chip and Pin' has been publicly available since 1992. 'Chip and Pin' encryption and reading techniques are known to OSCN's since 2006 and will be distributed in accordance with the implementation of 'Chip and Pin'.

2.8 Information sharing via criminal information data bases

Information sharing between anonymous cells of skimming gangs takes place via criminal information data bases.
Via these data bases gangs have access to complete ATM skimming manuals, and share and add information about suitable skimming spots.
The following authentic information is gathered per country and city and published in these data bases:

Country with german bias of life. On my opinion, people are goner, but not stingy, lasy, though friendly. Not suspicious.
High standart of life.
Salary: 3.000 - 4.000 euro

Many ATMs .
Models (by shares):
Toothed (NCR 5886) _____ 3
Citroen (WN) _____ 5
Citroen wide (WN) _____ 2
Sofa narrow (NCR 5684) _____ 1
Sofa wide (NCR 5685) _____ 1
Who is tourists? __ From the whole world
Availability of additional cams_____ yes. In atm-kiosks
Availability of antiskimmer_____ 50/50
In the store pin required? _____ Yes
Tourist's seasons: _____ All year (in winter: skiing)
Much police? _____ At nightfall - yes.
Methods police's control. _____ Standart.
A lot of chip cards? _____ no, but have. percent not ascertain.
City wake up / fall asleep: _____ 6-00…23-00 (the bigger city, the later) shopes closing early.
ATM at branches? _____ 90%
Good cellphone operator _____ Vodafone.
SMS cost_____ ---
Is country convenient and comfortable for working with skimmer? _____ If know all details over every city about cams, etc., yes.
Is country convenient for cashing? _____ No.
To work in this country - you must know way of life, feel places, I mean, come here and choose succesful places momentally - It's not about this country. For example, good places in evening, in the afternoon may seem bad for you, and easy place in afternoon, at night may seem worse another one. You must see and you must feel places on your time and your situation.
Not recommend to set up skimmer in the morning.
Not recommend work in small cities (<15k)
Everywhere cams. Before work you must planing all details.

Hungary

Setting up actual only in big cities (more 15k population)
Usually models:
Toothed (NCR 5886)
Sofa narrow (NCR 5684)
Sofa wide (NCR 5685)

All over country two languages: Hungarian and German. They think they are second part of Germany.

All who go there for working, see there 2 ATMs, which are placed beside, where 40-50 people in a hour. One give out euros, second local currency. Don't set up skimmers on this ATM, there around 6 cams.

A lot of evening places, at which u must set up about 6pm and take off about 11pm.

Not recommend to set up skimmers in the morning - more probability, that skimmer will be picked up by police, etc.

Approximate statistic:
9 days working - 1 picked up skimmer. In touristic places.

A lot of germans, especially at the weekends. They are going there for vacation. Because of that a lot of german dumps.

Statistic by dumps :

20% german golds.
30% german visa and mc classic .
5% local gold cards.
30% local visa and mc classic.
5 % local visa electron.
10% other.

Tourists the whole year.
Police respect expensive cars, and cars with foreign numbers.

Italy

Standart of life (avg salary) _____ 2000-3000 euro
Many ATMs? _____ not so much

Models:
Toothed (NCR 5886) _____ 3
Citroen (WN) _____ 1
Citroen wide (WN) _____ 3
Sofa narrow (NCR 5684) _____ 1
Sofa wide (NCR 5685) _____ 1

Who is tourists? __ From the whole world
Availability of additional cams _____ No
Availability of antiskimmer _____ 50/50
Entering PIN in shops ? _____ Yes
Touristic season: _____ Whole year
Much police? _____ after nightfall - yes
Method of police control_____ Standart
A lot of chip cards? _____ small amount.

City wake up - fall asleep: _____ 6-00…23-00 ATMs in branches? _____ 90% Good cellphone operator _____ Vodafone, Wind SMS cost _____ --- Is country convenient and comfortable for working with skimmer? _____ Yes. Is country convenient for cashing? _____ Yes.

3 Netherlands

At the end of November 2008, an inter-regional law enforcement (LE) co-operation that includes Europol has been set. We expect to see the first effects at the beginning of February 2009, when the police will start apprehending groups of skimmers every day.
The goals are to improve co-operation between LE departments, to disrupt and to deter Romanian skimming gangs. The police mainly focus on Romanian cells that are equipped with skim sets for Diebold ATM's and the railway ticket machines (Ascom).
There are Diebold ATM's that have been skimmed more than 8 times in the second half of 2008.
In the coming months the new ABN-AMRO 5 seconds Klikklak skim sets for Wincor ATM's with anti skimming equipment will enter the market.
For the second half of 2009 we expect skimsets for the smaller ATM machines to enter the market.

4 What can the Ultrascan-AGI offer?

Ultrascan-AGI employs a network of over 3200 experts in 69 countries. These people are the base of our knowledge. This human intelligence network has been set up in 1996..
Our network not only incorporates (ex) law enforcement people, but also (ex) military and intelligence people, academics, physicians and specialists in many different fields.
Over 90% percent are locals who speak the local language and have their own local network of people.

4.1 Human Intelligence

Through our human intelligence Ultrascan-AGI has knowledge about the 15 thousand plus elite members of the OSCN's, who are divided in groups of which some are only accessible to Russian or Chinese criminals.
These networks are engaged in all kinds of financial fraud from data breaches to committing internet banking fraud through DNS hijacking.

4.2 Product knowledge

Ultrascan-AGI has the ability to identify the latest skimming equipment.
Through our human intelligence we are the first ones that know about new designs, production and vendors of skim sets.
Ultrascan-AGI can inform you directly about hardware and software updates that will be distributed by criminal networks or disrupt, through our own programs, existing channels and criminal networks.

4.3 Product development / improvement

Based on our information lead Ultrascan-AGI can be part of ATM product improvement cycles.

4.4 Education

Ultrascan-AGI can train, possibly in co-operation with Interpol, LE departments, banks and/or ATM manufacturers and owners on managing this type of criminal activities.
We can assist local banks and/or ATM franchisers in introducing or improving security protocols.
This service could be extremely suitable for countries such as Morocco or Venezuela, because in these countries banks and LE's are unprepared. In these countries the risks are extremely high.

4.5 Research & Disruption

Ultrascan-AGI offers its own programs and people to disrupt existing criminal distribution channels and networks.
In comparable situations where criminals have conspired against certain companies Ultrascan-AGI's R&D efforts have led to a substantial decrease in criminal activities against our client(s) compared the companies that were not using our services.

Because in certain countries, part of the problem is corruption at banks and government and limited law and order, an independently operating anti skim hit & run team can have more effect than training bank and government employees. Such a team can also identify locally involved banking employees and report about country or location specific risks.

4.6 Prevention

As a security partner of an ATM manfacturer, Ultrascan-AGI can report monthly about the security situation in countries of interest to the manufacturer or can actively limit those security risks.
This service can cover one or all of the ATM manufacturer's products and can give the manufacturer a (profitable) market lead.

Appendix 1: Photos

Photo 1 Plastic bezel with invisible skimmer

Photo 2 Plastic bezel with invisible skimmer

Photo 3. software and hardware skimming instruction package

Photo 4 software and hardware skimming instruction package

Photo 5 Wincor ATM skimmer inserted

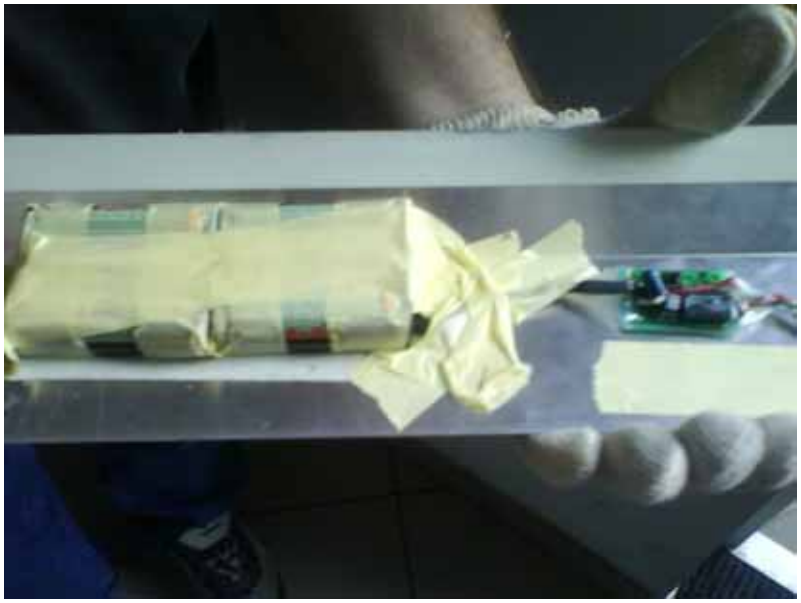

Photo 6 Battery attached to GPRS Phone

Photo 7 Battery connected to GPRS phone

Photo 8 Complete skimset placed on wincor ATM

Photo 9 Backside of skimmer

Photo 10 Sony phone

Photo 11 Skimmer for wincor ATM

Photo 12 Battery attached to GPRS phone

Photo 13 Skimmer hardware inside

Photo 14 Skimmer plastic front