

FEBRUARY 2011

INFORMATION UPDATE:

The following information reflects information received from Nov. 2010 to Feb. 2011.

Dräger

Number of lists:21
Records:2597
Hits:945

Tracker

Number of lists:34
Records:845
Hits:337

SAP13

Number of lists:85
Records:2827
Hits:709

Enquiries

Enquiries:155
Replies:492

INSIDE THIS ISSUE...

SAICB UPDATE 1

FRAUDLINE 1

ARTICLE: SBD— VEHICLE THEFT 2

ARTICLE: MCAFFEE— 6

CYBERCRIME

CONTACT 11

SAICB UPDATE

SAICB UPDATE

The SAICB had its 2011 Strategy meeting on 2 February 2011 to review our priority areas and determine the focus areas for the medium and long term for the SAICB. The draft strategy document is currently being prepared for review by the Board.

CASES UPDATE

Since November 2010, the SAICB has successfully prosecuted 3 cases through the courts , and has another 5 cases to be finalized in the next two months. The value of the current cases is approximately R10 million.

CLONED VEHICLE PROJECT

The SAICB cloned vehicle project , in conjunction with the South African Police (SAP), has been in operation since October 2010. Updates will be forthcoming in future editions. The following is a brief idea of what the project entails and the challenges the SAICB and the industry are facing.

Definition of a cloned vehicle: Cloning is the crime in which stolen vehicles assume the identity of not stolen, legally owned vehicles.

The cloning of vehicles takes place when criminals legalize stolen and/or hijacked vehicles by reproducing the stamped VIN number, the printed VIN sticker and the stamped engine number of legally owned vehicles onto a stolen or hijacked vehicle of the same make, model and colour.

There are various ways used by criminal syndicates to obtain the identity (VIN and engine number) of vehicles to be used to clone the vehicle identity.

In the past syndicates purchased wrecked vehicles and then transferred the particulars of the wrecked vehicle onto a stolen or hijacked vehicle. This method of cloning is still used today but not as frequently as in the past.

FRAUDLINE

From November 2010 to end January 2011, **429** reports were received of which **33** reports were for the short term insurance industry, **2** reports were received for Brokers and **12** reports for the life industry.

Since 2002, **27630** reports have been received of which **936** reports were for the short term industry **138** reports for the brokers and **378** reports were for the life industry.

For further information on the statistics, please contact Melanie Pillay on melaniep@saicb.co.za



0860 002526
insurance@fraudline.co.za

MEMBERS

SANTAM
MUTUAL & FEDERAL
HOLLARD
LION OF AFRICA
REGENT
TELESURE
ABSA INSURANCE
STANDARD BANK
INSURANCE
OUTSURANCE
MOMENTUM
MIWAY

PARTNERS

SOUTH AFRICAN
INSURANCE
ASSOCIATION (SAIA)
TRANSUNION
FRAUDLINE
MEMEX
SAFPS
UNICODE
BACSA
NEWORDER
DATADOT
CGC
SAVRALA

SAICB UPDATE—*CONT...*

By using this method criminal syndicates had unnecessary expenses because they had to purchase the wrecked vehicle and this also left a trail through receipts that could be traced back to the purchaser of the wrecked vehicle.

The modus operandi of the criminal syndicates changed and they have started utilizing dormant records on the eNatis system. These dormant records are records of vehicles that have been exported out of the country after the vehicle was manufactured or the vehicle was exported by the then registered owner.

This method of cloning is very efficient as the vehicle identity that is used for the cloning is no longer in the country and nobody is likely to complain that his vehicle's identity is being used. These records are obtained through corruption from within the Department of Transport. Through thorough investigation by the SAP this method of cloning has been virtually stopped.

The criminal syndicates then moved their focus and have now gone back to wrecked vehicles. The only difference now is that they use only the record of the wrecked vehicles. These records are obtained through negligence and corruption in the Department of Transport, the banking sector and the insurance industry.

This modus operandi has left the insurance industry with wrecked vehicles that they cannot dispose of. This has resulted in the accumulation of storage fees of the insurance salvage.

The criminal syndicates have also started to abuse the records of vehicles that are still under finance, and as previously mentioned is due to corruption in the various structures that handle the vehicle finance. This modus operandi has caused innocent consumers to sit with a vehicle in their possession that is no longer registered in their name.

The ongoing project will deal with all forms of cloning and monthly successes and statistics will be included in upcoming issues.

ARTICLE— HOW ARE THIEVES STEALING MODERN VEHICLES?

HOW ARE THIEVES STEALING MODERN VEHICLES?

Introduction

Developments in vehicle security over recent years have made it increasingly difficult for thieves to steal vehicles by conventional means and this has led to thieves using burglary and fraud, as well as more advanced methods of theft.

This white paper has been prepared exclusively by SBD in order to alert the automotive industry to the increasing security threat posed by the use of electronic theft tools.

The current situation

Statistics show that on a global scale the number of vehicle thefts has been steadily declining over the past 10 years but in developed markets the latest data shows that reductions are beginning to slow and in some instances theft numbers are starting to rise again.

ARTICLE— HOW ARE THIEVES STEALING MODERN VEHICLES? *CONT...*

There are huge new vehicle markets emerging in Brazil, Russia, India, and China (the BRIC group), and it is likely that the demand from these markets will be partially met using stolen vehicles. Thieves in these markets are learning from the knowledge and experience of criminals from overseas who have been stealing cars for many years.

Advances in technology have made it difficult for thieves to steal modern cars through the use of low tech methods and equipment. As such, it is becoming increasingly popular for Organised Crime Groups (OCG) to utilise electronic theft tools to acquire vehicles.

Electronic theft tools are designed to bypass on-board security systems either by imitating the coded signals sent from key transponders and radio frequency (RF) devices or by utilising OE key learning protocols to program keys. Despite the complexity of modern vehicles and the security systems built into their electronic architecture, there are still weaknesses that attack tool designers have been able to exploit. There is a common misconception, especially amongst insurers, that new cars cannot be stolen without the use of the original key. The reality is that although immobilisers have been responsible for the significant theft reduction in the markets where they are fitted, the availability of technical information and the expertise with which to identify system weaknesses means that a range of tools and methods are now widely available.

Achieving advanced vehicle security does not necessarily mean expensive changes are necessary. Improvements can be made to existing systems. SBD believe that vehicle manufacturers and suppliers need to take steps to understand the current vulnerabilities that are being exploited in order to design more robust security systems to tackle the problems being faced by the increasing popularity and availability of electronic theft tools.

Types of Tools

The tools that thieves are using to conduct electronic attacks can be divided into two main groups:

Theft Tools

These are tools that have been designed specifically to target and exploit the weaknesses in the vehicle's security systems in order to steal cars. They are often produced by the thieves themselves either by adapting replacement parts of the vehicle electronics to allow them to perform the functions that they require, or as an independent stand-alone system.

Legitimate Tools

These are tools that are designed for automotive locksmiths and security professionals to be used for diagnostic and maintenance applications. They are produced as an OEM tool by the vehicle manufacturer themselves, or as an aftermarket tool produced by a legitimate supplier.

Despite some measures being taken to try to prevent the unauthorised use of these legitimate tools, it is apparent that thieves are still able to obtain and use them for criminal gain. Further precautions need to be taken to ensure that their use is limited to the professionals that require them during service operations. This can be achieved by making the tools more difficult to use, or by creating a more diverse and adaptable system that would reduce the number of vehicles that the tools were compatible with.

The electronic theft tools being used by thieves host a variety of different functions. SBD have identified the main functions that can be harnessed by criminals during the process of stealing a vehicle:

Key Programming

This gives the user the ability to programme new Transponder, RF controls or Smart Keys to the vehicle immobiliser, locking and alarm systems. Connection to the vehicle can be achieved either through the OBD port or directly through the CAN-BUS or K-Line harness. Methods have been publicised for accessing CAN harness connections from outside the vehicle. This

ARTICLE— HOW ARE THIEVES STEALING MODERN VEHICLES? *CONT...*

enables manipulation of the locking and alarm systems meaning that thieves do not have to force entry to the vehicle's interior before starting their procedure.

Transponder Cloning

Transponder cloning devices allow the user to identify, prepare, read, copy and write a range of transponders. The transponder holds the unique identity which is communicated with the immobiliser unit in the vehicle. It confirms that the correct key has been inserted into the ignition and allows the vehicle to be operated. Cloning of this device would allow a thief to replicate this communication with an alternative key and in the absence of the original key.

Immobiliser Programming

Software protection for immobiliser systems can be relatively low. Tools are available which allow for direct manipulation of the software to disable the immobiliser function or to allow replacement of an ECU with a pre-matched or 'virgin' ECU and transponder set.

EEPROM programming

Some manufacturer's systems are vulnerable to reading or re-writing of the EEPROM and some stored data. Using this method, PIN-code security protocols used for verification prior to programming can be overcome. The devices that perform these functions are connected either through the CAN-BUS or directly to the ECU, or to the memory IC itself and allow a thief to bypass the security checks needed by some maintenance devices.

Relay Attack

Relay attack tools have been designed to target the increasing number of vehicles that use Smart Key technology. A pair of devices are used to capture the signals emitted by the vehicle and Smart Key, and extend their range so that the key and vehicle believe that they are within the authorised operation range. In doing so, a thief is able to enter the vehicle and start the engine without having the original key and without alerting the owner of the vehicle. Relay attacks can typically operate over a range of 100 to 1,000 metres, depending on environmental conditions and the equipment used.

For more information on relay attack, please refer to SBD report 2266: Relay Attacks – A Real Threat to Smart Key Security?

RF Code Grabbing

Code grabbing tools also target the signal sent from the key fob to the vehicle. They enable the thief to record the signals sent from an RF key fob when the owner wishes to lock and unlock their vehicle. In doing so, these signals can be re-transmitted at a later time in order to gain access to the vehicle, without the need for the original key. This is a covert method which allows the thief to gain access to the vehicle without arousing any suspicion. The effectiveness of this tool is not limited to fixed code systems. Some rolling code and crypto code systems can also be compromised by grabbing tools.

RF Blocking

RF blocking is the deliberate interference of the communication between the RF key fob and the vehicle usually without the driver being aware that the vehicle has not responded in the normal way. This can be achieved by using equipment that generates an RF signal, such as an electronic doorbell or garage door opener, or a specially designed tool that emits a continuous transmission to target a signal of a specific frequency. This is a highly effective method of preventing a driver from locking their vehicle and setting the alarm and is used all over the world. Legal restrictions exist which identify the frequency that a vehicle key fob must operate under and so thieves can target this frequency and ensure that the signal is blocked.

For more information on RF code grabbing and RF blocking, please refer to SBD report 2263: RF Interference and the Future for Vehicle Entry.

ARTICLE— HOW ARE THIEVES STEALING MODERN VEHICLES? *CONT...*

Despite the equipment described in this section being fairly advanced in its functionality, it would be a mistake to assume that the operation of these devices requires a high level of skill or expertise. Most of these devices require very little input from the user, with some requiring only to be connected to initiate the attack. They are simple to use and are highly effective, which makes them attractive to thieves.

Availability

The consumer market of the modern world is no longer constrained by the boundaries dividing countries. The internet has provided a complete catalogue of products that are available for purchase from almost any corner of the globe. Electronic tools developed in one country are readily available to any internet user via auction sites, specialist retailers, or discussion forums.

SBD have found reports of electronic theft tools being used frequently throughout Europe (especially in Russia and Poland); throughout Asia (in China, Japan and Malaysia); and also in the USA. Many thieves operating in these areas are targeting high specification luxury vehicles to be sold for a large profit, as well as more common vehicles that are stolen to meet market demand.

The origin of the design and manufacture of these tools is also widespread. There are numerous suppliers operating in Asia, Europe and the Middle East, each offering devices able to perform a multitude of functions.

The sale of tools is not illegal, even those that clearly have no legitimate purpose. Although they may be illegal to use, there is no restriction on supply and a number of companies have been formed specifically to design and distribute electronic devices aimed at overcoming vehicle security systems.

Cost

The cost of the tools typically range between €1,000 to €6,000, with the most expensive of the tools being used by thieves reaching up to €30,000. This price tag will not be considered an issue by most of the thieves operating today, and represents a good investment for repeated theft of luxury models. Spending €6,000 on a tool that will enable the thief to steal a car worth €50,000 will give the potential for a very quick profit and at a comparatively low risk.

It is unlikely that the purchase price of these tools will deter thieves because most will be operating within an organised crime group (OCG) and it is reasonable to assume that the purchase will be funded through other illegal operations. Once acquired, the tool can be distributed through their operating markets in order to gain a substantial return.

How has this happened and what needs to be done?

The basic principles on which the design of vehicle security is based have remained relatively unchanged over recent years and this does not reflect the advances in technology that the automotive industry is experiencing in other sectors. As such, thieves are developing sophisticated methods of theft that surpass the level of technology evident in vehicle security systems.

The majority of vehicle security systems appear to be designed to prevent authorised users from tampering with the vehicle in any intrusive way. Security protocols have been integrated to prohibit the programming of systems in the vehicle without permission from the vehicle manufacturer. Despite this, thieves are able to overcome these protocols and gain access to the vehicle's internal network via pre-programmed 'back doors'. These back doors are often inserted by suppliers during development to allow for simple maintenance of the system, but can be easily manipulated by thieves once the system weakness has been identified.

ARTICLE— HOW ARE THIEVES STEALING MODERN VEHICLES? *CONT...*

The capability of vehicle security systems has been compromised in recent years due to the advanced theft techniques being used by criminals and through the lack of awareness by some vehicle manufacturers in understanding the risks that are currently affecting their vehicle range.

Traditional theft methods required door locks to be broken, alarm sirens to be silenced, and ignition locks to be physically removed taking time and causing noise. Without physical damage needing to be inflicted there are less immediate warning signs that there is a theft in progress. This lowers the risk of a thief being discovered attacking a vehicle and increases the opportunities available to them.

SBD believe that more robust security systems need to be put in place in order to tackle the growing problems found in the use of electronic theft tools. Vehicle manufacturers and suppliers need to focus on improving a vehicle's susceptibility to attack by electronic means, especially considering the emerging markets where there is little legislation for security, but already a large amount of information and theft tools readily available to thieves.

For more information regarding the theft methods being utilised by criminals in the modern world, please refer to SBD report 2196: Vehicle crime in the 21st century and the impact of electronic theft methods.

Should you have further questions regarding the issues raised in this white paper, please feel free to contact SBD directly. Our in-house team of experts are well equipped to assist with your enquiries and can offer consultancy opportunities to allow us to work with you in the development of new solutions.

SBD (Secured by Design Ltd) - SBD is an independent, technical consultancy specialising in the design and development of vehicle security, low speed crash, telematics and ITS systems. From technical trends reports to conducting end user surveys, SBD has over 15 years of experience of providing strategic advice, insight and expertise to the automotive and associated industries.

THANK YOU TO JUANITA APPLEBY, MARKETING ANALYST FROM SBD FOR PERMISSION TO USE THESE ARTICLES. FOR FURTHER INFORMATION - www.sbd.co.uk

ARTICLE—A GOOD DECADE FOR CYBERCRIME

A GOOD DECADE FOR CYBERCRIME

Introduction

Despite a global recession, improved security and international crackdown efforts, cybercrime has thrived over the last decade, growing by double digits year after year.

To put the growth into perspective, the FBI-backed Internet Crime Complaint Center reported that cybercrime losses to consumers in the U.S. alone doubled from 2008 to 2009 to \$560 million¹ while consumer complaints grew by more than 22 percent. It is no wonder complaints have grown given that the amounts of malicious software computer users have to face when they get online, from *viruses* and *worms* to phony security software. In fact, in 2010 McAfee detected an average of 60,000 new pieces of *malware* each day. And many of these new threats were aimed at places where we want to let down our guard and connect with friends and family—on social networks. But sadly, cyber crooks have dug their claws in here too. McAfee² recently reported that malware directed at social media are some of the fastest growing threats today.

ARTICLE— A GOOD DECADE FOR CYBERCRIME CONT...

If that wasn't enough, recent events have further indicated that cybercrime has reached a new level of maturity and pervasiveness. We've seen targeted attacks against governments and organizations as cyber criminals have used their skills not just for profit, but for protest. For example, hackers have recently turned their skills to online activism, or "hacktivism," in the case of WikiLeaks, the media group that publishes news leaks on the Internet. The "hacktivists" have been busy launching attacks to take down the websites of organizations they deem unsupportive of the controversial news source.

So, how did we get here, to a world where protests are conducted through cyberwarfare, and millions³ of Internet users have fallen victim to an online scam, virus or other attack? Where did cybercrime start and where is it heading? We answer these questions in "A Good Decade for Cybercrime."

A Good Decade for Cybercrime

In the late 1990s Dunbar armoured car employee Allen Pace masterminded a plan that led to what is still considered the largest cash robbery in U.S. history. Pace, a Dunbar safety inspector, used his inside access to photograph and research the company's armoured car depot. He then recruited five childhood friends to help him sneak into Dunbar's Los Angeles facility. They ambushed the guards and ransacked a vault making off with \$18.9 million. Unfortunately for Pace, some of the looted money was traced back to the crime. He was caught and sentenced to 24 years in prison.

Fast forward to today when some of the most successful criminals don't have to leave the comfort of their own homes to pull off crimes 10 times bigger than the Dunbar robbery. All they need is an Internet connection, a little tech savvy and a lot of bad will.

Take the example of Albert Gonzalez, who, with a team of hackers called Shadowcrew, broke into the databases of well-known retail giants including TJ Maxx, Barnes and Noble and BJ's Wholesale Club, to gain access to more than 180 million payment card accounts between 2005 and 2007. He and his crew were estimated to cost the companies they compromised more than \$400 million in re-imbursments, forensics and legal fees.

Or, just take a look at the recently busted "scareware" ring that sold \$180 million worth of phony security software to computer users by tricking them into believing their computers were at risk. Read more about McAfee's report on scareware [here](#).

What these examples tell us is that there is no doubt that we are in a new era of crime—an era that can make successful crooks *hundreds of millions* of dollars, with less risk than traditional crimes. This is the era of cybercrime.

What happened over the last decade to change the face of crime so dramatically? First, after a steady start in the '90s when cybercrime began to take root, Internet use exploded over the last decade, growing five-fold from the 361 million users in 2000 to nearly 2 billion users in 2010⁴. Also, the Internet grew in sophistication and revenue opportunities. With its rich landscape of e-commerce sites, paid services and online banking, the Internet became a treasure trove of money and information that proved irresistible to cyber crooks. Suddenly, the banking and credit card information of billions of people were potentially accessible to those employing the right exploit or scam. The arrival of social media sites later in the decade added another incredible opportunity for thieves to target personal and identity information.

While the lures to cybercrime were growing exponentially, so were the cyber crooks' skills. Technical advances have allowed crooks to spread their malware more easily, and better hide their own identities.

For Internet users, it has been a decade of exciting online advances that allow us to communicate, express ourselves, and

ARTICLE— A GOOD DECADE FOR CYBERCRIME CONT...

do business in ways that were never possible before. It has also been a decade of escalating online threats, putting our money and identities at risk.

To better understand this cybercrime landscape and how it has developed, let's take a look back at the *Decade of Cybercrime*.

A Decade Of Cybercrime

2000–2003—Notoriety and Personal Challenge

Following the world's anticlimactic scramble against Y2K, cyber crooks looked for ways to turn attention toward real computer threats—themselves. They showed off their skills by temporarily taking down popular websites, such as CNN, Yahoo and E-Bay by flooding them with traffic, known as a *Distributed Denial of Service (DDoS) attack*. They also launched widespread attacks aimed at crippling users' computers.

One popular method was sending spam emails that invited recipients to click on a link or attachment, causing them to accidentally install malware. This is what happened in 2000 with the infamous "I love you" worm, which travelled as a spam email with "I love you" in the subject line and an attachment that purported to be a "love letter for you." This proved enticing enough that tens of millions of Windows users fell for it.

Scammers also learned how to write "*macro viruses*" that could be built into common documents such as Microsoft Word DOC files, so when the computer user simply opened the infectious file, the virus would run automatically.

These attacks gave the cyber crooks the attention they sought—headlines screamed with news of website attacks and the latest fast-moving virus—but they didn't bring the payday that scammers came to crave in coming years. Meanwhile...

Wi-fi hotspots starting gaining traction and digital music became all the rage, with the introduction of the iPod and music services such as Napster. These advances would later offer cyber crooks opportunities to steal information from users on unsecured wireless networks. They also tricked users into downloading dangerous files on music sharing services by labelling them as in-demand songs.

By 2009, McAfee would see a 40 percent increase in websites that either delivered infected MP3 files or were built solely to spread infection to those looking for MP3s online.

2004–2005—Lure of Money and Professionalism

By this time cyber scammers had proved their skills and it was time to move beyond doing damage and make real money.

A clever turn came with the advent of *adware*, or advertising supported software, which automatically displays pop-ups or downloads ads to the user's computer to get the user to buy products or services.

For example, a shopper searching online for car insurance might encounter an adware pop-up displaying an ad for a car insurance company, as an attempt to lure them into buying their insurance. Adware vendors grew their businesses by getting their software installed on as many systems as they could. One method they used was the pay-per-install affiliate model. Attackers jumped at the opportunity to install different adware packages on millions of systems while collecting handsome checks along the way.

Spyware, which tracks which websites we visit, or records what we type, was another prevalent threat during this time. With

ARTICLE— A GOOD DECADE FOR CYBERCRIME CONT...

both adware and spyware, cybercriminals showed they were serious about making money, and eroding our privacy.

Another important cybercrime advance of this era was the development of software that could gain privileged access to a computer while at the same time hiding its presence. Cyber crooks used this software, called *rootkits*, to hide malware and even prevent security checks from finding it. Using this trick, cyber crooks could stealthily steal passwords and credit card information as well as spread viruses.

Other advances had a broader effect on overall Internet security. Cyber crooks could now infect hundreds or even thousands of machines at the same time, controlling them remotely, without computer users' knowledge. By enabling an army of so-called *zombie computers* that blindly followed their commands, cyber criminals gained enormous computing power, which they could use to launch attacks on other computers or websites or distribute spam. In either case, the goal was to make money, either by blackmail (threatening companies that they would attack their computers and websites if they didn't pay up), or by sales generated by spam.

In fact, *botnets* are still prevalent—McAfee Labs™ reported in 2010 that it sees an average of six million new botnet infections each month, and Spanish police recently shut down what is believed to be the world's largest botnet, consisting of millions of infected computers. The so-called Mariposa botnet was linked to 13 million unique Internet Protocol (IP) addresses, which were used for stealing banking information and launching DDoS attacks.

Meanwhile ...

Customer data breaches became more common as cybercriminals tapped into large company databases to gain huge amounts of consumer information. At the same time, ID theft started to grow.

Within five years, it would be a major problem affecting 11.1 million Americans. Facebook also launched during this period. Like other social networking sites, it would later prove to be a fertile place for cyber crooks to perpetuate their scams.

2006–2008—Gangs and Discretion

With a growing amount of money at stake, cybercriminals began organizing into gangs. Some even had a Mafia-like structure, with malicious hackers, programmers and data sellers reporting to managers, who in turn reported to a boss who was in charge of distributing cybercrime kits.

To protect their growing business empires, attackers also became more discrete in their methods, while still showing off their tech savvy. For example, cyber crooks would use their skills to find unknown vulnerabilities in applications and then try to exploit the vulnerabilities before they could be patched.

They could spread malware or even take complete control over users' computers just by taking advantage of a hole that the software maker had not closed.

Attackers were also looking for ways to manipulate software features for their own purposes. For instance, a feature in Microsoft Windows software called Autorun was designed to automatically launch programs from external devices. By taking advantage of this feature, cyber crooks could get Microsoft's flagship operating system to automatically launch malicious code.

By exploiting both software vulnerabilities and features, cybercriminals were discreetly gaining access to user's systems while at the same time thumbing their noses at software makers.

Meanwhile ...

ARTICLE— A GOOD DECADE FOR CYBERCRIME *CONT...*

Unique services such as Skype and Twitter launched, offering computer users new ways to keep connected and share information. Along with Facebook, Twitter would soon become an irresistible platform for crooks to interact with users, and try to trick them out of money and information.

This was also the period when the iPhone came to market, leading to more and more mobile applications and criminal opportunities.

2009–2010—Social Networking and Engineering

As social networking sites such as Facebook and Twitter started to takeoff in the later part of the decade, cybercrooks realized they could get their hands on a wealth of personal information if they played the game right.

With users posting everything from where they lived and worked to their current location, all cyber crooks had to do was virtually interact with users to gain access to their information.

They still do this by employing *social engineering*, meaning they find out which topics interest Internet users and then design attacks using popular subjects as a lure. For instance, a cyber cook can track hot topics on Twitter and then post a message mentioning the topic, with a link to a dangerous website that aims to steal credit card and other personal information.

In one recent social engineering scam cyber crooks took advantage of Facebook users' curiosity over who was viewing their profiles to get them to download a phony application that was supposed to let them see who was looking at their page.

Instead of the desired app, victims download a malicious program that accessed their Facebook message centre to send spam, including messages advertising the very scam they fell for.

Another ongoing Facebook scam involves cyber crooks gaining access to users' accounts and then sending messages from the account holder to their friends saying that they have been robbed while abroad and need the friend to wire money to them to get them home. This "I've been robbed!" scam is another good example of social engineering that has cost many unwitting, warm hearted friends hundreds to thousands of dollars.

Cyber crooks also began distributing scareware. It still remains one of the most common Internet threats today, representing a significant evolution in cybercrime because it demonstrates just how successful attackers can be when they know how to manipulate the psychology of their victims. By playing to Internet users' fears that computers and information can be at risk, cyber crooks have been able to gain unprecedented access to machines while making hundreds of millions of dollars.

Finally, as attacks targeted consumers, they also honed in on corporations, governments and organizations, serving as a form of social protest and rebellion. The case of the WikiLeaks "hacktivists," who launched DDoS attacks against websites such as MasterCard and Visa after they distanced themselves from the news leak site, is one example. The Stuxnet worm, which was aimed at utility companies and control systems, and even nuclear facilities, is another. Gradually, cybercrime has turned from an act of personal challenge and notoriety, to a targeted and lucrative enterprise, as well as a political tool.

Given how far crime has come in the last 10 years, we can't help but wonder what's ahead.

Cybercrime: What's Next?

Social Scammers and App Spoilers

Looking ahead to future cybercrime trends, McAfee Labs predicts the continuation of social networking scams and tricks,

ARTICLE— A GOOD DECADE FOR CYBERCRIME CONT...

such as malicious links, phony friend requests and *phishing* attempts. For example, you may receive a message that appears to be from a friend, asking for money or information.

Scams are likely to get more sophisticated and personalized, especially if users continue to share a great deal of information. McAfee Labs also foresees more Twitter abuse where cyber crooks post tweets on hot topics with dangerous links to bait user clickthroughs.

Location-based services, such as Foursquare, Google Places and Gowalla present other concerns. With more and more users posting where they are in the physical world, crooks have ample opportunities to figure out users' patterns, current location and when they're away from home. Put together with other available online information, such as their address, this online data can lead to serious real world crimes, like robbery.

Finally, the proliferation of mobile devices and applications presents another opportunity for cyber crooks. They've already turned their attention in this direction—McAfee Labs⁵ reported that mobile threats grew and became more targeted in the third-quarter of 2010 and predicts that 2011 will be a turning point for threats to mobile devices. By targeting applications, crooks can potentially steal enormous amounts of personal and banking information from users.

Users' desire for ubiquitous applications that will work across their multiple devices means that by targeting just one app cybercriminals can do damage across various platforms, whether it be the iPhone, Android or Windows-based phones.

While many of the types of attacks will stay the same (i.e. phishing, dangerous websites and downloads, and spam) cyber crooks' methods will become more targeted and clever. The days of destruction for bragging rights is over—now it's all about money and discretion.

1. <http://scamfraudalert.wordpress.com/2010/03/13/fbi-2009-cybercrime-statistics/>
2. <http://www.mcafee.com/us/about/news/2010/q3/20100810-02.aspx>
3. Javelin Strategy's 2010 Identity Theft Survey
4. <http://www.internetworldstats.com/stats.htm>
5. McAfee Q3 2010 Threat Report

About McAfee

McAfee, headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse and shop the Web more securely. Backed by its unrivalled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee secures your digital world.

www.mcafee.com

For questions contact: Francie Coulter at francie_coulter@mcafee.com or (408) 346-3436 or Kim Eichorn at kim_eichorn@mcafee.com or (408) 346-3606

CONTACT

For further information or if you wish to reproduce any of the articles in this Newsletter, please contact : Hugo van Zyl on hugovz@saicb.co.za or Melanie Pillay on melaniep@saicb.co.za