Report

A Good Decade for Cybercrime

McAfee's Look Back at Ten Years of Cybercrime

Table of Contents

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 million[1] 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, cybercrooks have dug their claws in here too. McAfee[2] recently reported that malware directed at social media are some of the fastest growing threats today.

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 cybercriminals 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 millions[3] 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 armored 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 armored 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 reimbursements, 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.

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

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 2010[4]. 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 cybercrooks. 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 cybercrooks' 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 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, cybercrooks 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 cybercrooks 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 cybercrooks opportunities to steal information from users on unsecured wireless networks. They also tricked users into downloading dangerous files on music sharing services by labeling 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.

4. http://www.internetworldstats.com/stats.htm

2004–2005—Lure of Money and Professionalism

By this time cyberscammers 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 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. Cybercrooks used this software, called *rootkits*, to hide malware and even prevent security checks from finding it. Using this trick, cybercrooks could stealthily steal passwords and credit card information as well as spread viruses

Other advances had a broader effect on overall Internet security. Cybercrooks 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, cybercriminals 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 cybercrooks 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, cybercrooks 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, cybercrooks 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 …

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 cybercrooks 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 cybercook 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 cybercrooks 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 center to send spam, including messages advertising the very scam they fell for.

Story of a Cybergang

In 2006, a credit card thief using the online name John Dillinger emerged as a key suspect in the FBI's Operation CardKeeper—an initiative to discover who was behind the theft of tens of thousands of credit card numbers from corporate databases. Dillinger and several other Americans were accused of receiving stolen credit card numbers from accomplices abroad and then using the numbers to buy goods that they later resold.

As it turns out, Dillinger was part of an international cybergang that stretched from the United States to Poland and Romania. Dillinger and the other Americans purchased information that was electronically copied from the magnetic strip on the back of stolen credit or debit cards and then placed the information on counterfeit cards so they could use them to make purchases and cash withdrawals. Meanwhile, other members of the gang sold personal information such as Social Security numbers, through online forums. The personal information was later used to obtain credit cards with the victims' names on them.

The head of the cybergang was thought to be from Poland and nicknamed "Blindroot." Blindroot and his accomplices would hack into third-party Web servers and then rent space on the servers to other cybercriminals for illicit activities, such as hosting phishing sites for credit card fraud.

Dillinger and 16 other hackers and information traders in both the U.S. and Poland were eventually arrested in the operation. Although the true extent of their network was never discovered, authorities said that more than 100,000 credit card numbers were compromised in Virginia alone, and several thousand identities were being trafficked over the Internet.

Another ongoing Facebook scam involves cybercrooks 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, warmhearted friends hundreds to thousands of dollars.

Cybercrooks 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, cybercrooks 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, 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.

Identity Theft In-Depth

In 2000, the Federal Commission on Identity Theft announced the identity theft program, offering a toll-free number and consumer education website to combat what it saw as a growing problem affecting 600,000 to 700,000 Americans a year. Much of the threat occurred at home—through stolen mail, *dumpster diving* and theft by people known to the victim, even friends and relatives.

Ten years later, identity theft has become so common that 11.1 million American adults were estimated to be victims of identity theft in 2009 while the annual fraud amount increased to $59 billion. Even Federal Reserve Board Chairman, Ben Bernanke, and his wife were victimized as part of a sophisticated identity-fraud ring dubbed "Big Head." A crook stole his wife's purse, which contained her checkbook to a joint account.

While identity theft is still often perpetrated using old school methods such as pick pocketing, a growing amount of theft is now done online, through phishing, phony websites and corporate data breaches.

The truth is there are myriad more ways for thieves to obtain our personal information today than there was before the Internet boom. But while identity theft methods have changed, what haven't changed are the repercussions. Identity theft victims cannot only lose money, but also their credit and reputations. In this era of cybercrime, identity theft is one of the most common and serious threats.

McAfee Labs also foresees more Twitter abuse where cybercrooks 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 cybercrooks. They've already turned their attention in this direction—McAfee Labs[5] 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) cybercrooks' methods will become more targeted and clever. The days of destruction for bragging rights is over—now it's all about money and discretion.

Cybercrime Growth: Are Computer Users Partially To Blame?

When it comes to cybercrime, it's easy to point a finger at the bad guys. But how much of their success is due to our own actions, or inactions? Consider this—Despite widespread education on the prevalence and danger of Internet threats, a recent survey found that just 58 percent of consumers said they had a complete security suite. What's more, when the survey takers actually scanned their computers for the software they discovered that only 37 percent were fully protected. This means that nearly two-thirds of users were leaving themselves exposed and making it easier for the cybercrooks. Given these facts, it's not surprising that 545,000 households had to replace their PCs during a six month period in 2009 after they were infected with malware.

The reason surveyors checked for complete security suites is because threats are constantly changing and becoming more sophisticated. These days basic protection simply isn't enough. Despite this, 25 percent of consumers use free security software, which doesn't typically protect against emerging threats and is often used to upsell the customer to a more comprehensive, paid version.

In addition to not being as diligent as we should when protecting our computers, it appears that we also need to become better at safeguarding our information.

In the last two years alone, seven million U.S. consumers—or one in 13 households—admitted to giving out their personal information to phishers—scammers who tricked them into revealing information by pretending to be legitimate companies or organizations. And now scammers are aiming attacks at social networks, where younger people in particular like to let their guard down and express themselves. Unfortunately, it's working. Another study shows that social networking users aged 18-24 have experienced a spike in fraud and data exposures compared to other groups.

Clearly we have to get better at protecting both our computers and our personal information if we want to slow cybercrooks' success. Technology can only take us so far, and the rest is education and vigilance on the part of computer users.

Sources: 2010 NCSA study; Consumer Reports State of the Net report in 2010; *Javelin Strategy & Research*, 2010.

5. McAfee Q3 2010 Threat Report

Top 5 Exploits—Representing different periods of cybercrime eras

1. MyDoom's Mass Infection: Estimated damage $38 billion

This fast-moving worm first struck in 2004 and tops our list in terms of monetary damage. The worm was designed to infect computers and send spam emails. Due to the volume of spam sent, it slowed down global Internet access by 10 percent and reduced access to some websites by 50 percent, causing billions of dollars in lost productivity and online sales.

2. "I LOVE YOU" Worm's False Affection: Estimated damage $15 Billion

The "I love you" worm (named after the subject line of the email it came in) proved irresistible in 2000 as millions of users opened the spam message and downloaded the attached "love letter" file. Unfortunately, instead of sweet nothings, they got a bitter virus. This infamous worm cost companies and government agencies $15 billion to shut down their computers and remove the infection.

3. Conficker's Stealthy Destruction: Estimated damage $9.1 Billion

This 2007 worm infected millions of computers and then took its infections further than the first two worms on our list as cybercrooks moved from notoriety to professionalism. Conficker was designed to download and install malware from sites controlled by the virus writers. The malware included a *keystroke logger* and other PC-control software that gave cybercrooks users' personal information as well as access to their machines.

4. Stuxnet Worm—Targeted and Dangerous: Damage unknown

This recent worm targets critical infrastructure, such as utility companies and control systems, by taking advantage of several vulnerabilities in Windows.

Stuxnet has reportedly damaged government facilities in India, the U.S. and Indonesia, as well as nuclear facilities in Iran. The creators of the worm are still unknown, but the world is aware of their presence and the threat of targeted attacks.

5. Zeus Botnet—Versatile Information Stealer: Damage unknown

Cybercrooks named this botnet after a Greek god, and while it's not all-powerful, it has been a thorn in computer users' sides since 2007.

One of its main talents is stealing personal information by infecting computers and capturing data entered into Internet banking sites including passwords. It can also control infected computers and capture identity information. And recently, Zeus has shown its sophistication with 700 variants detected per day, including new mobile capabilities.

Top 5 Scams—The most common scams, snaring the most victims

1. *Scareware*—Selling fake antivirus software is one of the most insidious and successful scams of recent years. Cybercrooks play on users' fear that their computer and information is at-risk by displaying misleading pop-ups. Crooks then prompt victims to purchase antivirus software to fix the problem. When the victim agrees to purchase, they hand their money and credit card information over to the very attackers behind the scam.
2. *Phishing Scams*—Phishing, or trying to trick users into giving up personal information, is one of the most common and persistent online threats. In fact, over 49,000[6] phishing sites were detected at the end of 2009. Phishing attempts can come in a variety of ways, such as through spam emails, spam instant messages, fake friend requests and social networking posts. Usually cybercrooks pretend to be a legitimate business or organization and asked for your information.
3. *Phony Websites*—In recent years cybercrooks have become more and more adept at creating fake websites that look like the real deal. From phony banking sites, to auction sites and e-commerce pages, crooks are constantly laying online traps hoping you will be fooled into entering your credit card or personal information. Often these phony websites are used as part of a phishing attempt, where a cybercrook sends out a message with a link to the fraudulent website.

6. Anti-Phishing Working Group Q4/2009 report (Jan. 2010)

And, given that a recent study indicated that the number of websites—many of them phony—infected with malicious software or ads have reached 1.2 million[7], users should beware.

4. *Online Dating Scams*—Like the "I Love You" virus, online dating scams tug on victims' heartstrings to get what they want. The typical online dating scam starts with the scammer posting an attractive picture on an online dating site. The scammer then sends out messages to other members of the site expressing interest. The next step is to strike up a one-on-one conversation with victims, usually via email or instant messages, where they tell a sob story. The crook creates a personal relationship in order to ask for cash, merchandise or other favors.

5. *Nigerian Scam*—This scam, also known the "advance fee fraud," usually consists of a spam message from a foreigner who needs help moving millions of dollars out of their homeland and offers the recipient a percentage of his or her fortune to assist in the transfer. Unfortunately, despite the fact that this scam is too good to be true, many recipients have fallen for it and some have lost thousands of dollars in the process since the scammer asks for a variety of fees upfront to facilitate the deal.

Lexicon

Adware—Software that generates revenue by displaying advertisements targeted at the user. Adware earns revenue from either the vendor or the vendor's partners. Certain types of adware have the capability to capture or transmit personal information.

Botnet—A collection of zombie PCs. Botnet is short for robot network. A botnet can consist of tens or even hundreds of thousands of zombie computers. A single PC in a botnet can automatically send thousands of spam messages per day. The most common spam messages come from zombie computers.

DDoS attacks—DDoS, or denial-of-service attacks, target a computer server, or network by flooding it with traffic. A denial-of-service attack overwhelms its target with false connection requests so the target ignores legitimate requests.

Dumpster diving—The practice of sifting through trash in the hopes of finding valuable material, including sensitive information.

Keystroke logger—A program that covertly records what you type on a keyboard, including passwords and other sensitive information.

Macro viruses—A program or code segment written in the application's internal macro language. Some macro viruses replicate or spread; others simply modify documents or other files on the user's machine without spreading.

Malware—Malware, short for malicious software, aims to infect computer systems without the owner's consent.

Phishing—A method of fraudulently obtaining personal information, such as passwords, Social Security numbers, and credit card details by sending spoofed emails that appear to be sent from trusted sources, such as banks or legitimate companies. Typically, phishing emails request that recipients click on a link in an email to verify or update contact details or credit card information.

Rootkits—A set of software tools that can alter files or processes in an infected computer while concealing its presence.

Scareware—A type of malware designed to trick users into purchasing or downloading useless or potentially dangerous software, usually phony anti-virus software. It's called scareware because users are scared into thinking something is wrong with their machine to get them to download the software.

Social engineering—The act of manipulating a computer user into performing certain actions or divulging personal information, rather than simply using technical means to get what the cybercrook wants.

7. Malware is Everywhere, Report Says (PCMag, November 2010)

Virus—A computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission.

Worm—A virus that spreads by creating duplicates of itself on other drives, systems or networks. A mass-mailing worm is one that requires a user's intervention to spread, (e.g., opening an attachment or executing a downloaded file). Most of today's email viruses are worms.

Zombie computer—A computer that has been compromised and can be controlled remotely by a cybercrook.

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 unrivaled 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

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

rpt_cybercrime_1210_fnl_ETMG