White Paper

The Cybercrime Arms Race

By Eugene Kaspersky
Founder and CEO of Kaspersky Lab

www.kaspersky.com

Contents

Cybercrime Is Here to Stay

Our society has evolved to the point where many if not most of us spend a significant portion of our lives online. In many ways, this online virtual world mirrors our real world. Criminals, who are an unfortunate but integral part of our social structure, quite naturally have also appeared in the virtual world. The presence of cybercriminals has become more pervasive today because the freely growing online exchange of money and data has created an increasingly tempting target. Today the cybercrime ecosystem is close to maturity – well-defined relationships and business models are already in place. A new class of cybercriminals freely and openly buys and sells malicious code. These cybercriminals range from petty fraudsters who steal small sums in large quantities to individuals who attempt to steal large sums of money at one time.

Today the cybercrime ecosystem is close to maturity, with well-defined relationships and business models in place.

Criminal activity has always mirrored legitimate business – the image of a Mafia accountant may be the first to come to mind. However, it is worth noting that cybercrime is not currently organized into one or more worldwide Mafia-like organizations with a “Dr. No” figure at the helm. Rather, it’s an interdependent world based on groups who have complementary functionality. For example, the individual or group owning a botnet capable of launching DDoS attacks or distributing spam needs email addresses. Someone else, whom the botnet owner need not know or have other contact with, fills this need by stealing and selling the needed addresses. This business model in many ways mirrors the business model of legitimate businesses. Just as a motor production company’s presence in an area spawns spin-off industries, such as carburetor manufacturers or nuts and bolts suppliers, cybercriminals need not be connected organizationally, but only for mutual economic benefit.

Cybercrime As a Business

Contemporary cybercrime is like any other business. It behaves according to traditional business principles such as profitability, ease of use, risk management, and emerging markets.

Cybercrime Is Profitable

The most important criterion for any business is profitability, and cybercrime is no exception. As a matter of fact, cybercrime is extremely profitable. Large sums have been stolen successfully in one-shot deals, as well as by acquiring small sums in large quantities. For example, in 2007 alone there was an average of one cybercrime reported per month.

The most important criterion for any business is profitability, and cybercrime is no exception.

- **January 2007** – Russian hackers, with the aid of Swedish middle-men, steal 800,000 euros from Swedish bank Nordea.
- **February 2007** – Brazilian police arrest 41 hackers for using a Trojan to steal bank account details used to make 4.74 million dollars.
- **February 2007** – Seventeen members of Internet fraud gang arrested in Turkey for stealing up to 500,000 dollars.
- **February 2007** – Li Jun arrested for the "Panda burning Incense" virus used to steal gaming and instant messaging (IM) account names; believed to have made around 13,000 dollars by selling the malware.
- **March 2007** – Five eastern Europeans imprisoned in the UK for credit card fraud; they stole an estimated 1.7 million pounds.
- **June 2007** – 150 cybercriminals arrested in Italy; alleged to have bombarded Italian users with fake emails to generate around 1.25 million euros in ill-gotten gains.
- **July 2007** – Russian cyber thieves allegedly used a Trojan to steal 500,000 dollars from Turkish banks.
- **August 2007** – Ukrainian Maxim Yastremsky [aka "Maksik"] detained in Turkey for allegedly making tens of millions of dollars from ID theft.
- **September 2007** – Gregory Kopiloff charged in the U.S. for allegedly using P2P file-sharing software Limewire and Soulseek to gather information used in ID fraud; allegedly made thousands of dollars in purchases using stolen data.

- **October 2007** – Greg King arrested in the U.S. for participationin the February 2007 DDoS attack on Castle Cops; faces a maximum sentence of 10 years in prison and 250,000 dollars in fines.
- **November 2007** – The FBI arrests eight individuals in the second phase of its anti-botnet initiative dubbed "Operation Bot Roast", which has allegedly so far uncovered more than 20 million dollars in economic losses and more than one million victim computers.
- **December 2007** – Cybercriminals broke into computers at the U.S. Department of Energy's Oak Ridge National Laboratory (ORNL); reportedly also targeted Los Alamos National Laboratory and Lawrence Livermore National Laboratory. Over 12,000 Social Security numbers and birth dates of ORNL visitors between 1999 and 2004 were stolen. This breach is a national security issue and leaves the individual victims vulnerable to identity theft and financial fraud.

These examples are merely the tip of the iceberg. The victims and/or law enforcement agencies cleared these examples for public discussion. Most cybercrimes are either investigated in-house by the affected organizations or by law enforcement agencies conducting undercover investigations. The results are almost never made public. Figure 1, from a recent report by the Computer Security Institute, shows the reasons that organizations choose not to report such incidents.

Most cybercrimes are either investigated in-house by the affected organizations or by law enforcement agencies conducting undercover investigations. The results are almost never made public.

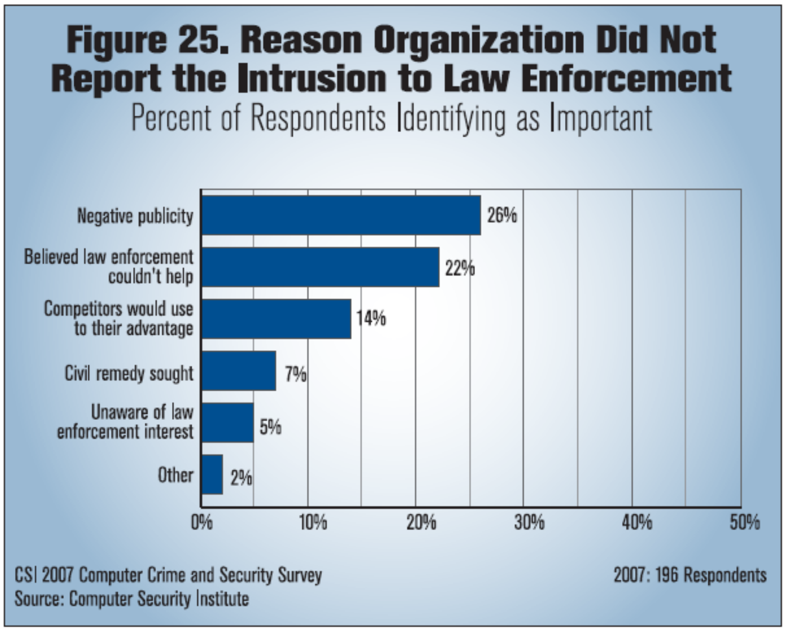
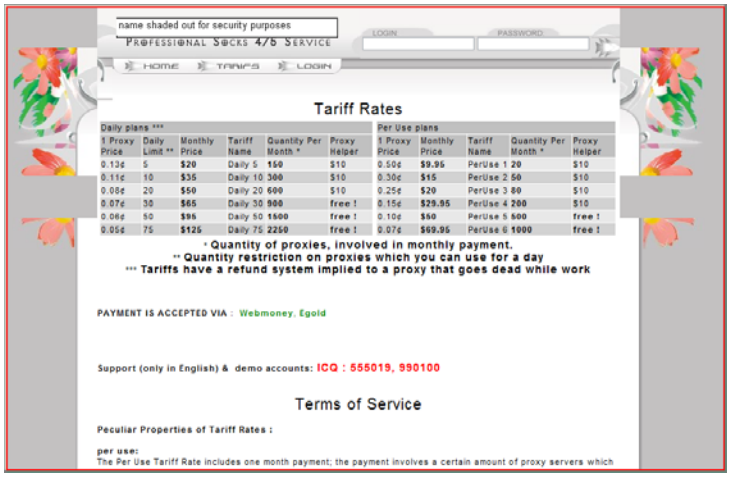


Figure 1 – Reasons Organizations Do Not Report Intrusion Incidents

Cybercrime Is Low-Risk and Easy

The second key factor in the rise of cybercrime as a business is that success comes with a minimum of risk. The psychological aspect of crime provides some measure of deterrence in the real world. In the virtual world, criminals never see their individual victims or the corporations they choose to attack. It is much easier to rob the rich or to rob someone you can't see, touch or feel.

Coupled with the cloak of anonymity is the plethora of online resources available, hawking everything from vulnerabilities, to Trojans for building botnets, to complete rent-a-botnet solutions. (See Figures 2 and 3.) The level of technical expertise required to run a cybercrime business continues to decrease in similar proportion to the increase in the number of Internet-savvy people.


name shaded out for security purposes
PROFESSIONAL SOCKS 4/5 SERVICE
LOGIN
PASSWORD
HOME
TARIFS
LOGIN

Tariff Rates

Daily plans ***						Per Use plans				
1 Proxy Price	Daily Limit **	Monthly Price	Tariff Name	Quantity Per Month *	Proxy Helper	1 Proxy Price	Monthly Price	Tariff Name	Quantity Per Month *	Proxy Helper
0.13¢	5	$20	Daily 5	150	$10	0.50¢	$9.95	PerUse 1	20	$10
0.11¢	10	$35	Daily 10	300	$10	0.30¢	$15	PerUse 2	50	$10
0.08¢	20	$50	Daily 20	600	$10	0.25¢	$20	PerUse 3	80	$10
0.07¢	30	$65	Daily 30	900	free !	0.15¢	$29.95	PerUse 4	200	$10
0.06¢	50	$95	Daily 50	1500	free !	0.10¢	$50	PerUse 5	500	free !
0.05¢	75	$125	Daily 75	2250	free !	0.07¢	$69.95	PerUse 6	1000	free !

* Quantity of proxies, involved in monthly payment.
** Quantity restriction on proxies which you can use for a day
*** Tariffs have a refund system implied to a proxy that goes dead while work

PAYMENT IS ACCEPTED VIA : Webmoney, Egold

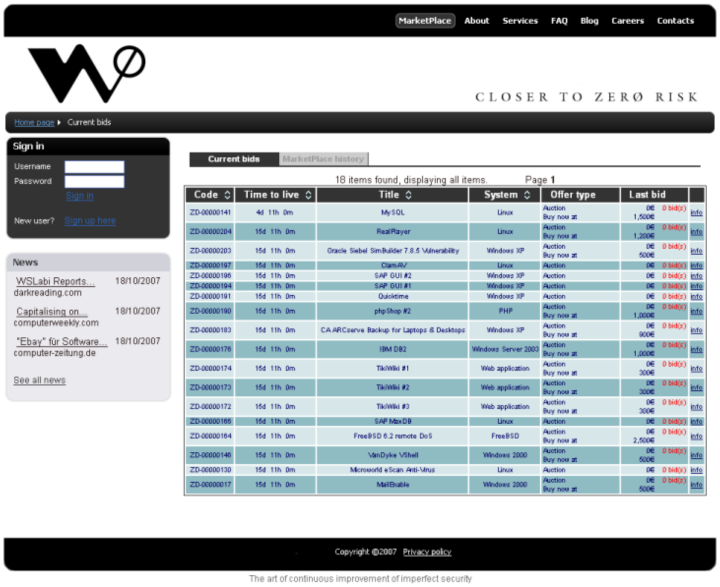
Support (only in English) & demo accounts: ICQ : 555019, 990100

Terms of Service

Peculiar Properties of Tariff Rates :

per use:
The Per Use Tariff Rate includes one month payment; the payment involves a certain amount of proxy servers which

Figure 2 – Screenshot of a Website That Sells Botnets



WSLabi Reports... 18/10/2007
darkreading.com

Capitalising on... 18/10/2007
computerweekly.com

"Ebay" für Software... 18/10/2007
computer-zeitung.de

See all news

18 items found, displaying all items. Page 1

Code	Time to live	Title	System	Offer type	Last bid	
ZD-00000141	4d 11h 0m	MySQL	Linux	Auction Buy now at	0€ 0 bid(s) 1,500€	info
ZD-00000204	15d 11h 0m	RealPlayer	Linux	Auction Buy now at	0€ 0 bid(s) 1,200€	info
ZD-00000203	15d 11h 0m	Oracle Siebel SimBuilder 7.8.5 Vulnerability	Windows XP	Auction Buy now at	0€ 0 bid(s) 500€	info
ZD-00000197	15d 11h 0m	ClamAV	Linux	Auction	0€ 0 bid(s)	info
ZD-00000196	15d 11h 0m	SAP GUI #2	Windows XP	Auction	0€ 0 bid(s)	info
ZD-00000194	15d 11h 0m	SAP GUI #1	Windows XP	Auction	0€ 0 bid(s)	info
ZD-00000191	15d 11h 0m	Quicktime	Windows XP	Auction	0€ 0 bid(s)	info
ZD-00000190	15d 11h 0m	phpShop #2	PHP	Auction Buy now at	0€ 0 bid(s) 1,000€	info
ZD-00000183	15d 11h 0m	CA ARCserve Backup for Laptops & Desktops	Windows XP	Auction Buy now at	0€ 0 bid(s) 900€	info
ZD-00000176	15d 11h 0m	IBM DB2	Windows Server 2003	Auction Buy now at	0€ 0 bid(s) 1,000€	info
ZD-00000174	15d 11h 0m	TikiWiki #1	Web application	Auction Buy now at	0€ 0 bid(s) 300€	info
ZD-00000173	15d 11h 0m	TikiWiki #2	Web application	Auction Buy now at	0€ 0 bid(s) 300€	info
ZD-00000172	15d 11h 0m	TikiWiki #3	Web application	Auction Buy now at	0€ 0 bid(s) 300€	info
ZD-00000166	15d 11h 0m	SAP MaxDB	Linux	Auction	0€ 0 bid(s)	info
ZD-00000164	15d 11h 0m	FreeBSD 6.2 remote DoS	FreeBSD	Auction Buy now at	0€ 0 bid(s) 2,500€	info
ZD-00000146	15d 11h 0m	VanDyke VShell	Windows 2000	Auction Buy now at	0€ 0 bid(s) 500€	info
ZD-00000130	15d 11h 0m	Microworld eScan Anti-Virus	Linux	Auction	0€ 0 bid(s)	info
ZD-00000017	15d 11h 0m	MailEnable	Windows 2000	Auction Buy now at	0€ 0 bid(s) 500€	info

Copyright @2007 Privacy policy

The art of continuous improvement of imperfect security

Figure 3 – Screenshot of a Website That Sells New Vulnerabilities

Cybercrime Exploits Web 2.0 Opportunities

The avalanche of new services that are available via the Internet, along with a world population that now more readily adopts these new services, also contributes to the success of cybercrime. Areas that are especially vulnerable to attack include:

- **Internet-money and online banking** – Ecommerce and banks working diligently to enable online financial transactions fuel the ongoing struggle to balance speed and convenience with appropriate security.
- **Data storage facilities and applications "in the clouds"** – With data and applications increasingly being located on remote external servers, criminals can hijack the traffic to gain access to financial, confidential, and proprietary information.
- **Online games** – Crimes include password theft and theft of virtual property for resale at significant profit.
- **Online stock-exchange agencies** – This convenient and fast way to respond to stock market fluctuations creates a very tempting target for criminals because stock market data is a very liquid asset.
- **Web 2.0** – Online social networking, blogs, forums, wikis, MySpace, YouTube, Twitter – all rely on the easy downloading, publishing, and other information-sharing techniques that make every participant vulnerable to malware infections.

How Attacks Work

Every generation of criminals chooses its own tools. Today's cybercriminals use Trojans as their weapons of choice – to build botnets, to steal passwords and confidential data, to conduct DoS attacks, and to encrypt data in order to blackmail the victims. One disturbing characteristic of today's attacks is the newer goal of maintaining a presence on the infected machine. Cybercriminals are using a number of techniques to achieve this goal.

Today, some cybercriminals opt to conduct discrete attacks that target specific organizations. Writing unique malware for a single target is both time-consuming and difficult to deploy. However, once launched, these targeted attacks almost always succeed. These attacks usually provide significant return on investment for cybercriminals, making targeted attacks a small but important form of cybercrime.

Today's Botnets

Currently, botnets are made up of easy-to-manage quantities of infected machines that make it easier to control the bots and to process the harvested data. Profits depend both on numbers of victims and the frequency with which new malware is required. The greater the longevity of the malware on the machines, the more money the controllers earn. Other popular and effective methods that today's cybercriminals use to increase profit margins include competing against other controllers and the sabotage of security solutions.

Other popular and effective methods that today's cybercriminals use to increase profit margins include competing against other controllers and the sabotage of security solutions.

Cybercrime Techniques

Generally speaking, today's cybercriminals have to consider two different techniques to achieve the desired end result – delivery and deployment.

Delivery

The first step in any cybercrime is delivering and installing the malware. Cybercriminals use a number of techniques to accomplish this goal. Today's leading malware transmission techniques (also called "infection vectors") are spam mailings and infected websites. The ideal setup for criminals is a vulnerable victim machine that allows malware to be installed immediately, whether it is delivered by spam or by a "drive-by" scenario, where malware is downloaded from a website that the victim visited while surfing.

Deployment

Once the malware is delivered, the criminals strive for it to remain undetected for as long as possible. Malware writers use a number of technical strategies to maximize the lifespan of each piece of malware.

As a primary strategy, the malware writers depend on stealth not only for delivery, but also for survival. The less visible their malware is to antivirus early-warning radar systems and law enforcement agencies, the longer the malware can be used to provide access to infected machines and to harvest data. Common stealth techniques include rootkit technologies, suppression of system error messages, concealed increases in file size, many and varied packers, and suppression of antivirus warning messages.

Malware authors are also relying heavily on obfuscation techniques to avoid detection. Polymorphism is an obfuscation technique that was popular in the 1990's and then virtually disappeared. Today, malware writers have returned to polymorphism, but rarely do they attempt to morph code on victim machines. Instead, there is a distinct trend of server-side polymorphism – the re-compiling of code on web servers with "do-nothing instructions" that vary over time, making it significantly more difficult to detect the new malware residing on the server. In fact, today, there are websites where bots re-compile malware as often as every five minutes.

Attacking Security Solutions

Another common technique used in malware is the sabotage of security programs, to prevent detection and extend shelf-life. Malware sabotage often occurs through the termination of security processes, deletion of code, or modification of the Windows hosts file to prevent antivirus program updates. In addition, malware often removes malicious code that is already installed, not for the user's benefit, but to ensure "ownership" and control of the victim machine exclusively for its own benefit. This active competition between malicious programs highlights the rich opportunities that are available to malware writers and the criminals that sponsor them.

Malware often removes other malware that is already installed to ensure "ownership" and control of the victim machine exclusively for its own benefit.

The Human Factor

Ultimately, any security system is only as effective as the weakest link. In the case of online security, the weakest link is always the human factor. As a result, social engineering techniques are a key element in malware dissemination processes used today. Techniques are often as simple as sending links purportedly from a friend via email or instant messaging (IM). These links are crafted to look as if they lead to interesting online resources, but in reality, these links lead to infected web resources. Today, email messages can contain scripts that connect to infected websites without any user interaction at all. Even the educated, highly cautious person who never clicks on unsolicited links is in danger of infection by a "drive-by" download. The inclusion of current events in such campaigns occurs today with alarming speed, yielding astonishingly effective results. Phishing continues to be a major source of infection despite efforts by banks and other organizations that conduct online financial transactions to implement countermeasures. Too many innocent victims can still be convinced to explore interesting links and to accept official-looking communications as legitimate.

Final Thoughts from the Author

In order to manage cybercrime, we need to develop and implement a number of protection strategies. Naturally, anti-malware software and risk management strategies are vital at all levels.

However, I have stated this before and continue to believe that in addition to appropriate protection strategies, a successful anti-cybercrime strategy requires a community effort. There must be a functional Internet-Interpol and ongoing consumer education, much like that conducted to encourage seat belt usage. There should be legal measures requiring people to behave in a secure and legal fashion online, as well as legal consequences to support enforcement efforts. Just as with seat belts, unrelenting long-term education is needed to gain widespread acceptance for these measures.

While I don't believe we will ever abolish cybercrime any more than we have abolished crime in the physical world, I do believe that we can make the Internet a safer place. It will take more than the measures listed above, more than a single company, and more than a single government. We need a united community of individuals that each do their little bit for online security … a community like this can and will succeed in winning against cybercrime most of the time. And most of the time is a goal worth striving for.

I don't believe we will ever abolish cybercrime any more than we have abolished crime in the physical world … We need a united community that can and will succeed in winning against cybercrime most of the time.

Kaspersky Lab, Inc. • 500 Unicorn Park • Woburn, MA 01801
phone: (781) 503-1800 • fax: (781) 503-1818
www.kaspersky.com

About Us

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for large enterprises, SMBs, home users and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of more than 100 of the industry's leading IT security solution providers.

For the latest on antivirus, anti-spyware, anti-spam and other IT security issues and trends, visit www.viruslist.com.

Learn more at www.kaspersky.com