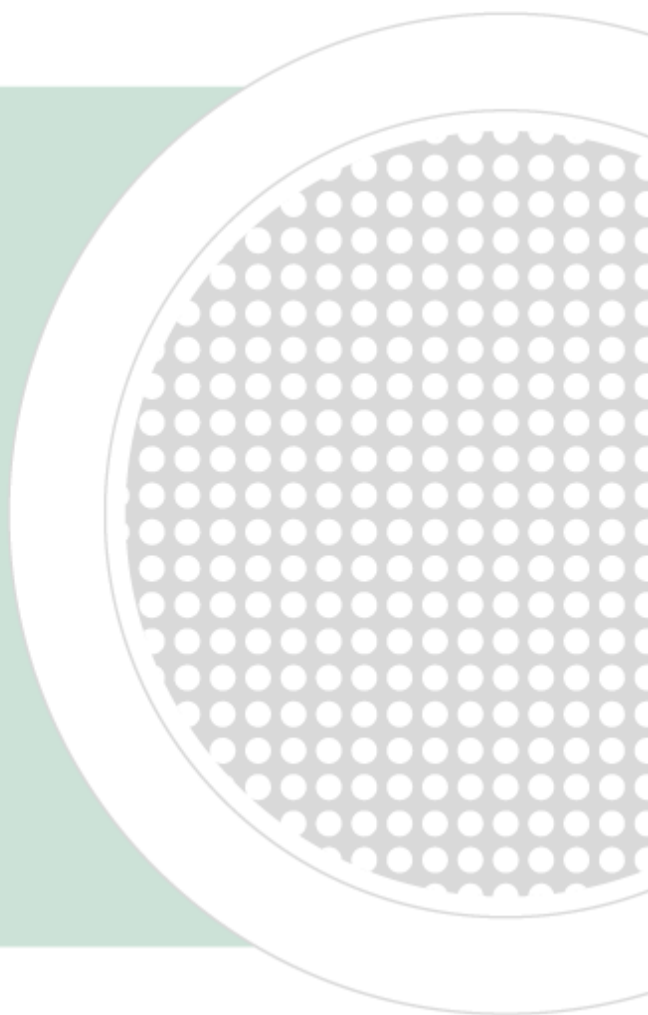


White Paper

# Computer Networks and Theft

by Yury Mashevsky  
Kaspersky Lab Virus Analyst



## Preface

Computers have become an integral part of our lives. Every day organizations and users rely on them more and more to store data and intellectual property, as well as valuable personal information. Although most people and organizations are careful about protecting their physical property, they are often less careful where virtual property is concerned. Many users remain oblivious to the fact that someone somewhere is interested in what they are doing, and conclude that they are not vulnerable to malware.

Many people may have varying degrees of awareness of how much cybercrime has evolved in recent years through the creation and application of new technologies. Most cybercrime is no longer committed by individual amateurs. Today's cybercrime is, instead, a very lucrative business run by highly organized groups. Various estimates of 2005 activity range from tens to hundreds of billions of dollars, a sum that far exceeds the revenue of the entire anti-virus industry. Of course, not all this money was "earned" by attacking users and organizations, but such attacks account for a significant proportion of cybercriminals' income.

The first part of this paper will examine attacks on individual users, including an analysis of what kind of virtual property is attractive to cybercriminals and the methods they use to obtain user data. The second part will focus on attacks on organizations, exploring both attacks on the organization's resources as well as attacks that target the organization's clients. Throughout the paper, we provide statistics that will help you understand the magnitude of the cybercrime problem. To heighten both your awareness and understanding of the risks, we will explore the vulnerabilities from the other side – from the cybercriminals' point of view.

# Table of Contents



Preface .....	i
Theft from Users.....	1
What is Stolen .....	1
How It Is Stolen.....	1
Dealing in Stolen Goods .....	5
Scams .....	6
Extortion .....	8
How Users Can Avoid Cybercrime.....	9
Attacks Targeting an Organization’s Clients.....	10
Attacks on Organizations.....	13
Theft of Internal Databases.....	13
Organizational Blackmail, Scams, and Ransom .....	14
The Unquantifiable Loss.....	15
Conclusion .....	16

## Theft from Users

No one likes to live in fear, but the fact of the matter is that users need to be exercising more caution than ever before as cybercrime rates rise. Neither Internet Service Providers (ISPs) nor sophisticated corporate firewalls can ensure that users won't become victims of cybercrime. Understanding more about the nature of online theft is key to the heightened awareness that can help prevent it.

### What is Stolen

What kind of virtual property is of interest to a cyberthief? A study of malicious programs conducted by Kaspersky Lab virus analysts shows that four types of virtual property are most often stolen, although no one should assume that cyberscammers limit themselves to stealing these four primary types of information –

- Data needed to access a range of financial services (online banking, card services, e-money) and online auction sites such as eBay
- Instant messaging (IM) and website passwords
- Passwords to mailboxes linked to ICQ accounts, as well as all email addresses found on the computer
- Passwords to online games, the most popular of which are Legend of Mir, Gamania, Lineage, and World of Warcraft

If you store any of the information above on your machine, then your data is of interest to cybercriminals. We'll take a look at why such data is stolen and what happens to it after we explore how the information is stolen.

### How It Is Stolen

In most cases, cybercriminals use dedicated malicious programs or social engineering methods to steal data. At times, they use a combination of the two methods to increase effectiveness.

Consider the malicious programs that are designed to spy on users' actions by recording their keystrokes or by searching for certain data in user files or the system registry. The data collected by these malicious programs is eventually sent to the author or user of the program, who has plans to either sell or use the information. Kaspersky Lab classifies such programs as Trojan-Spy or Trojan-PSW. Figure 1 shows the increase in the number of programs and variants that fall into this category.

---

Understanding more about the nature of online theft is key to the heightened awareness that can help prevent it.

---

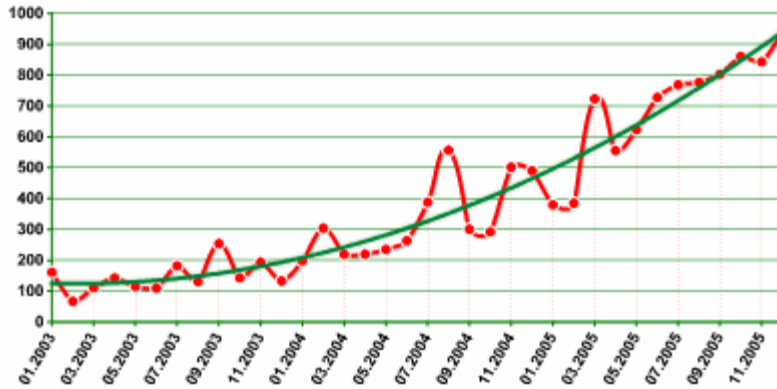


Figure 1 – Growth in the number of malicious programs designed to steal data

These spy programs arrive on victim machines in a number of ways –

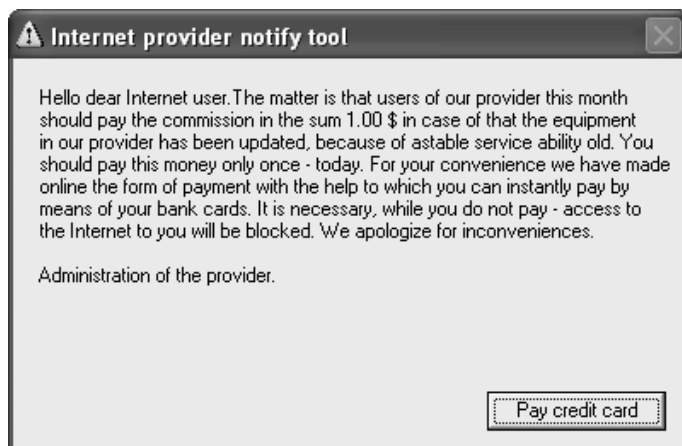
- During a visit to a malicious website
- Via email
- Via online chat
- Via message boards
- Via instant messaging programs

Using social engineering techniques in conjunction with these malicious programs can encourage users to behave the way cybercriminals want them to behave. One example, a variant of Trojan-PSW.Win32.LdPinch, is a common Trojan that steals passwords to instant messaging applications, mailboxes, FTP resources, and other information. After making its way onto the computer, the malicious program sends messages such as –

"Take a look at this  
<link to malicious program>  
Great stuff :-)

Most recipients click on the link and launch the Trojan because most people trust messages sent by ICQ, and don't doubt that the link was sent by a friend. After infecting your friend's computer, the Trojan spreads by sending itself on to all addresses in your friend's contact list, while at the same time delivering stolen data to the author or criminal using the Trojan.

Unfortunately, even inexperienced virus writers can now write such programs and use them in combination with social engineering techniques. By way of example, Trojan-Spy.Win32.Agent.ih is a program written by someone who is not very proficient in English. When launched, this Trojan causes the dialogue window shown in Figure 2 to be displayed.



*Figure 2 – Dialog window displayed by Trojan-Spy.Win32.Agent.ih*

The user is asked to pay only \$1 for Internet services, a classic case of social engineering in which –

- The user is given no time to consider the matter; payment must be made the day the user sees the message.
- The user is asked to pay a very small sum of money, a practice that significantly increases the number of people who will pay. Few people will make the effort to get additional information if they are only being asked for one dollar.
- Deception is used to motivate the user to pay. In this case, the user is told that Internet access will be cut off unless payment is made.
- The message appears to come from the ISP's administrators to reduce suspicion. The user is led to believe that the administrators have written a program to help them make payment more quickly and easily. It is also logical that the ISP would know the user's email address.

Notice that this Trojan leaves the user with no choice but to enter the requested credit card data. Because no other option is available, an obedient user will click on "Pay credit card", causing the dialog box shown in Figure 3 to be displayed.

Figure 3 – Credit card information dialog displayed by Trojan-Spy.Win32.Agent.ih

Of course, when the user fills in all the fields and clicks on “Pay 1\$”, no credit card transaction for \$1 will be processed. Instead, the credit card information is sent via email to the cybercriminals.

Social engineering methods are also often used independently of malicious programs, especially in phishing attacks that target customers of banks offering online banking services. Users receive emails, supposedly sent by the bank, stating that the customer's account has been blocked and asking the customer to follow the link in the message and enter his or her account details in order to unblock the account. While the link looks exactly like the Internet address of the bank's website, it actually links to a cybercriminal's website. If account details are entered, the cybercriminal can then gain access to the account. Figure 4 shows an example of a phishing email.

Dear Citi Cardmembers,

We recently reviewed your account and suspect that your CitiBank Account may have been accessed by an unauthorized third party. Protecting the security of your account and of the CitiBank Network is our primary concern. Therefore, as a preventative measure we have temporarily limited access to sensitive CitiBank Account Features.

**Click The link below in order to regain access to your Citi Cardmembers Account, simply:**  
[Update Your Account Online](#)

Please fill in the required informations.  
 This is required for us to continue to offer you a safe and risk free environment.

NOTE : Please ignore this message if you're not Debit Citi Cardmember.

Figure 4 – A phishing message targeting Citibank customers

Phishing attacks are also sent under the pretense of coming from a variety of other organizations, such as support services and social services.

Cybercriminals often help themselves to more than credit card information. They are also interested in the email addresses found on the victim machines. How do they steal these addresses? Special malicious programs, classified as SpamTools by Kaspersky Lab, play a crucial role. These programs scan victim machines for email addresses, and can even instantly filter the harvested addresses according to predefined criteria. For example, the program can be configured to ignore addresses which clearly belong to anti-virus companies. The harvested addresses are then sent to the author or user of the malicious program.

There are other ways of planting Trojans on user computers, and some of them are extremely brazen. Cybercriminals sometimes offer to pay website owners for loading malicious programs onto the machines of users who visit their websites. For example, the iframeDOLLARS.biz website offered webmasters a “partner program” that involved putting exploits on their websites so that malicious programs would be downloaded to the machines of those who viewed the sites. Of course, this was done without the users’ knowledge. These “partners” were offered \$61 per 1,000 infections.

---

**Cybercriminals sometimes offer to pay website owners for loading malicious programs onto the machines of users who visit their websites.**

---

## Dealing in Stolen Goods

Unquestionably, the main motivation for stealing data is to make money. The actual data theft is only the first step. But who needs credit card data and email addresses? Cybercriminals either use the information directly to withdraw money from the account, or sell the information to someone else for use. If an attack yields details used to access an online banking system or an e-payment system, the money can be obtained in a variety of ways –

- Via a chain of electronic exchange offices that exchange one e-currency for another
- Using similar services offered by other cybercriminals
- Buying goods in online stores

Often, legalizing or laundering the stolen money is the most dangerous stage of the process for cybercriminals. At this stage, they must provide some sort of identifying information, such as a delivery address for goods or a bank account number. To avoid detection, cybercriminals routinely use individuals who are called “money mules”, or “drops.” The drops themselves are often unaware of their role in the crime; they are often hired by supposedly international companies via job-search websites. A drop may even have a signed, stamped contract that appears perfectly legal. When detained and questioned by law-enforcement agencies, the drop is usually unable to provide any meaningful information about the employer. The contracts and bank details always turn out to be fake, as do the corporate websites with the postal addresses and telephone numbers used to contact the drops.

With the maturity of the cybercrime business today, cybercriminals no longer have to recruit drops themselves. They are supplied by people known as “drop handlers” in cybercrime jargon. Of course, each link in the chain takes a certain percentage for services rendered. However, cybercriminals believe that the additional security is worth the cost, especially given that they haven’t had to earn any of the money themselves.

As for stolen email addresses, they can be sold for substantial amounts of money to spammers, who will then use them for future mass mailings. More intriguing perhaps is what happens with online game accounts. Players often buy virtual weapons, charms, protection and other things for e-money. In some cases, cybercriminals have sold these resources for thousands of very real dollars. Cybercriminals can access these riches without having to pay for them, and don’t mind selling them at significantly reduced prices, since they have invested little or nothing. This explains the growing popularity of malicious programs that steal virtual gaming property. By the end of July 2006, the number of known modifications of malicious programs that steal passwords for the well-known game Legend of Mir exceeded 1,300. And unfortunately, Kaspersky Lab analysts have begun to see malicious programs that attack not just one game but several simultaneously.

## Scams

Scams are designed to get users to willingly part with their money. In most cases, scams take advantage of people’s love of getting something for nothing. Business is continually expanding into new areas. With more and more goods and services being made available online, new offers appear every day.

Criminals have been quick to follow legitimate business into the online world and have now implemented online versions of real-world scams. Such schemes typically attract buyers or customers by offering goods at prices that are much lower than those offered by legitimate vendors. Figure 5 shows a fragment of the web page of one such Russian e-store.

	<p><b>Toshiba Satellite A45-5120</b></p> <p>Celeron-2.6GHz, 256MB, 40Gb, 15TFT(1024x768), DVD-CDRW, FM56k, Eth 10/100, WI-FI, 361x274x43, 3kg, Win XP</p> <p>Цена - 160 \$ <a href="#">Купить...</a></p>
	<p><b>Toshiba Satellite M35-5320</b></p> <p>Centrino P-M 1.5GHz, 512MB, 60Gb, 15.4TFT(1280x800), Video 32MB NVIDIA FX Go5200, DVD/CD-RW, FM56, Eth10/100, WI-FI, 355x267x353, 2.8kg, Win XP-H</p> <p>Цена - 250 \$ <a href="#">Купить...</a></p>
	<p><b>Toshiba Satellite A65-51762</b></p> <p>Pentium 4-3,2GHz, 512MB, 60Gb, 15TFT(1024 x 768), ATI Mobility Radeon 7000 IGP 64MB, DVD-RW/CD-RW, FM56k, Eth 10/100, WI-FI, 343x282x45, 3.5kg, Win XP</p> <p>Цена - 250 \$ <a href="#">Купить...</a></p>

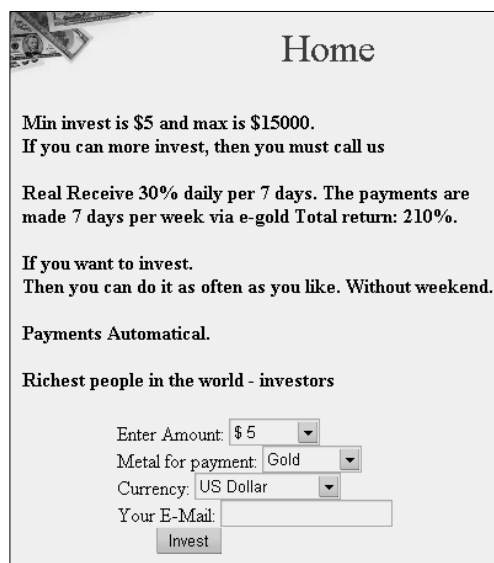
Figure 5 – Low-priced laptops on a scam website

Notice that the prices in Figure 5 are impossibly low. Such low prices should arouse user suspicion, making them think twice about buying things from such a website. However, cybercriminals can get around the problem by offering any of the following justifications –

- This is a sale of confiscated items
- These goods were purchased with stolen credit cards;
- These goods were purchased on credit using fake names

While such explanations remain extremely questionable, many people choose to believe them. They think it's alright to sell goods cheaply if the vendor didn't have to pay for them. When ordering, customers are asked to make a down payment or sometimes even prepay the full price. Naturally, once payment has been made, there will be no response from the cybercriminals' phone numbers or email addresses. And of course, the purchasers can't get their money back. These schemes are cleverly adapted for different locations. For example, because Russian vendors typically deliver goods purchased online by courier, cybercriminals may require an advance payment to cover cost of delivery. They explain that couriers are often sent to addresses where no goods have been ordered, yet the e-store owners still have to pay the courier. The cybercriminals then receive the delivery charge, while the customer receives nothing.

Bogus online stores are only one trap for users. Nearly all criminal schemes from the real world are mirrored by an identical scam in the cyberworld. Investment scams are another example. A “project” offers users an opportunity to invest their money at a very attractive rate – so attractive that it is hard to resist. Figure 6 shows part of one of such scam investment website.



The screenshot shows a web page titled "Home" with a background image of money. The text on the page is as follows:

**Home**

**Min invest is \$5 and max is \$15000.**  
**If you can more invest, then you must call us**

**Real Receive 30% daily per 7 days. The payments are made 7 days per week via e-gold Total return: 210%.**

**If you want to invest.**  
**Then you can do it as often as you like. Without weekend.**

**Payments Automatical.**

**Richest people in the world - investors**

Enter Amount: \$ 5  
Metal for payment: Gold  
Currency: US Dollar  
Your E-Mail:

Figure 6 – A scam investment website

Of course, the interest rate offered is absurd. However, in spite of the ludicrous nature of such schemes, some people will trust such “projects”, invest, and lose their money.

New bogus e-money exchange websites, new online financial pyramids, spam that describes special secret electronic wallets that double or triple the amounts received – the list is endless with new schemes continually emerging. All these scams are designed to play on people’s desire to get something for nothing.

## Extortion

In 2006 a dangerous trend in cybercrime became apparent in Russia and other Commonwealth of Independent States (CIS) countries. In January 2006, a new program, Trojan.Win32.Krotten, appeared. This Trojan modified the system registry of the victim computer, making it impossible for anyone to use the computer. After the affected computer was rebooted, Krotten displayed a message demanding that 25 hrivnia (about \$5) be transferred to the author’s bank account in exchange for returning the computer to normal.

Knowledgeable computer users could eliminate this malicious program either by finding and removing the malicious modifications on their own, or by re-installing the operating system. However, many other families of extortion programs are not so easy to eliminate. With the cost and time associated with getting assistance, the question of whether to pay was more often than not answered in the affirmative.

Krotten was distributed via online chat and on message boards under the guise of being a sensational program that provides free services, such as Voice over Internet Protocol (VoIP), Internet access, or cellular network access. On the heels of Krotten came the first modification of Virus.Win32.GpCode. This malicious program was mass mailed. It encrypted data files stored on the hard drive in such a way that the user could not decrypt them. Consequently, the user was asked to pay for the data to be decrypted. Folders with encrypted data contained a readme.txt file with the following content –

Some files are coded by RSA method.  
To buy decoder mail: xxxxxx@yandex.ru  
with subject: RSA 5 68251593176899861

In spite of the information that encryption was performed using an RSA algorithm, the author of the initial program had actually used standard symmetrical encryption. This made restoring data easier. In the course of just six months, GpCode evolved considerably, using different, more complex encryption algorithms. Different variants of the program demanded different

sums for decrypting data. The price varied from \$30 to \$70. These programs were only the beginning.

The number of families of extortion programs (Daideneg, Schoolboys, Cryzip, MayArchive, and others) increased throughout 2006. Unfortunately, these programs also expanded their geographical reach. By the middle of 2006, such malicious programs had been detected in Great Britain, Germany, and other countries. In addition, other methods of extortion continued to be used as extensively as before. For example, there was an attack on Alex Tew, 21, a British student who created a website where he sold advertising space in the form of squares a few pixels across. Tew managed to make \$1 million in four months with this unusual idea. Cybercriminals demanded that the successful student pay them a large amount of money, and threatened to organize a distributed denial-of-service (DDoS) attack on his website if payment was not made. Three days after receiving the threat the student's website underwent a DDoS attack. To Tew's credit, he refused to pay.

Why is extortion and blackmail so popular among cybercriminals? The answer is simple – the victims are easy prey and ready to yield to any demands just to have their lost or damaged data restored.

## How Users Can Avoid Cybercrime

This white paper is not intended to scare users into concluding that only an anti-virus program can save their data. In actual fact, there is no anti-virus solution that will help Internet users who don't exercise some basic precautions. These recommendations can help users avoid being easy prey for cybercriminals –

- Before making any payment or entering any personal data, find out what other users think of the website. Never rely on comments left on that site, itself as they could easily have been written by a cybercriminal. It's best to get the opinions of people you know personally.
- Avoid giving any details of your bank cards over the Internet. If you need to make a payment over the Internet, get a separate card or e-money account and transfer the necessary amount to the card or account just before making a purchase.
- If an online store, investment fund or other organization has a website on a third-level domain, especially one provided by a free hosting service, this should arouse suspicion. A self-respecting organization will always find the small sum needed to register a second-level domain.
- Check where and when the domain used by the online shop was registered, where the shop itself is located, and whether the addresses and telephone numbers provided are genuine. A simple telephone call can resolve several

---

The number of families of extortion programs increased throughout 2006. Unfortunately, these programs also expanded their geographical reach.

---

problems at once by confirming or dispelling doubts. If the domain name was registered a month ago and you are told that the company has been in the market for several years, the website warrants more detailed investigation.

- Do not pay money up front, even for courier delivery. Pay for all services only when you have received the goods. If told that you must pay delivery fees up front because people often order goods for delivery to bogus addresses, don't be persuaded. Err on the side of caution and choose a different store, rather than risking being swindled.
- Never reply to mailings from banks, investment funds, and other financial organizations. Such organizations never use mass mailings. If in doubt, phone the organization to find out if the email really did come from the alleged sender. Never use the telephone number given in the message, because that number will also belong to the cybercriminals.

---

Do not pay money up front, even for courier delivery. Pay for all services only when you have received the goods.

---

Now that we've examined cybercrime from the Internet user's perspective, it's time to turn our attention to cybercrime that specifically targets businesses and other organizations.

## Attacks Targeting an Organization's Clients

When cybercriminals manage to attack the clients of any organization, an immediate loss of credibility and trust is inevitable. Not surprisingly, clients expect a reliable online system to support their interaction with any reliable organization, not a system that will cause headaches and potentially place their data at risk.

For quite a long time, cybercriminals have primarily been targeting client data when they attack organizations. In previous sections of this paper, we explored exactly how such attacks are carried out, which malicious programs are used, and how users can be infected. To summarize, mass mailings, phishing, and programs that simply forward the needed data are common ways used to get at data that should be confidential between the client and the organization. Having obtained the needed personal account details, cybercriminals will access the account and steal the property that they set their sights on, whether it is money or something else.

In the overwhelming majority of cases, the target will be an account which is related to finance. Figure 7 shows the increase in the number of financial organizations whose clients were targeted between 2003 and 2006.

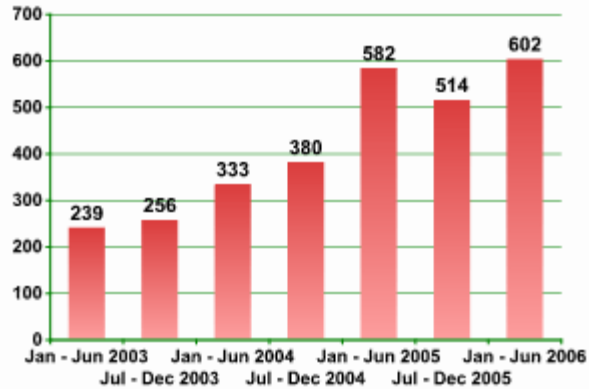


Figure 7– Growth in the number of financial institutions whose clients were targeted by malware designed to steal data  
Source: Kaspersky Lab

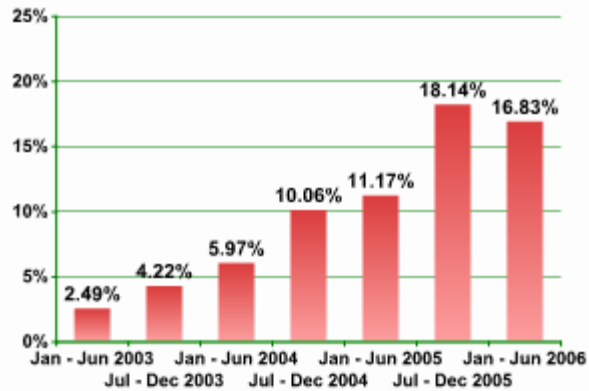
As the graph shows, the number of victims is increasing every year. In addition, the number of attacks will increase in correlation to the increasing popularity of a particular bank, electronic currency exchange, e-payment or other online financial system.

Many organizations and institutions (banks most of all) were so concerned about the unrelenting attacks on their clients that in the middle of 2005, they started taking measures to prevent data from being used once it had been stolen. One such measure was the two-part authentication that is commonly used today. Some companies even went so far as to place restrictions on the size and number of transactions which could be conducted within a specific time period. The home page of many banks and other financial institutions also often display warnings about cybercriminals, such as the one shown in Figure 8.



Figure 8 – Warning on the site of a financial institution

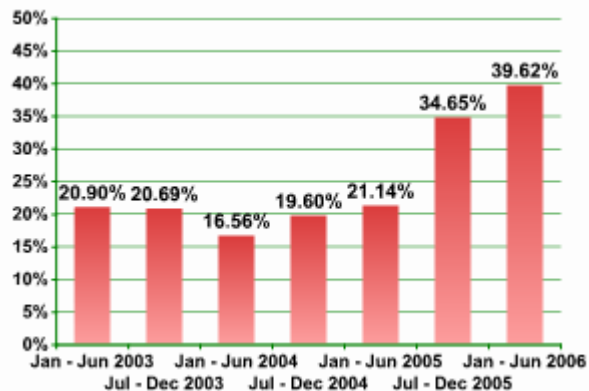
It remains to be seen how long such measures will continue to prove effective in protecting users. However, they do seem to have had a positive effect during the first half of 2006, when the overall percentage of malicious programs used for financial gain decreased for the first time in three years, as shown in Figure 9.



*Figure 9 – Decrease in percentage of malicious programs used to steal financial data (percentage of overall malicious traffic)*

Source: Kaspersky Lab

Cybercriminals constantly search for new ways to surmount the obstacles placed in their way. In spite of this drop in the percentage of malicious programs targeting online financial data, their total number continues to increase, as does the overall number of malicious programs. Also of great concern is the recent rise in the number of malicious programs capable of attacking the users of several payment systems at the same time has risen, as shown in Figure 10. An example is Trojan-Spy.Win32.Banker.asq, which targets almost 50 financial systems and institutions at the same time, including PayPal, CaixaBank, Postbank (Germany), and many other institutions around the world.



*Figure 10 – Increase in percentage of malicious programs that attack several financial institutions/payment systems at once (percentage of malicious programs targeting financial data)*

Source: Kaspersky Lab

This tactic of targeting several payment systems and institutions at once increases the likelihood of successfully finding victims. We have chosen to focus this paper primarily on attacks on clients of financial institutions and online financial services because these attacks are more common than attacks on the users of any other type of organization. However, cybercriminals cast their nets widely. Companies and institutions that are not connected to

finance per se, but which accept online payment for their services, are also of great interest to cybercriminals. Kaspersky Lab virus analysts have detected malicious programs that target the clients of tour firms and transport companies, pawn shops and e-commerce sites, as well as a range of other companies.

Unfortunately, there's no reason to think that the number of malicious programs used to commit such crimes is going to decrease. The same practices recommended for users earlier in this paper are applicable to and advisable for the clients and users of online banks, payment systems, and other companies and organizations. Do not pay money up front, even for courier delivery. Pay for all services only when you have received the goods

---

The most common type of cybercrime that organizations fall victim to is the theft of confidential data from internal databases.

---

## Attacks on Organizations

Scams, blackmail and ransom demands imposed by cybercriminals on institutions take place relatively frequently. However, the most common type of cybercrime that organizations fall victim to is the theft of confidential data from internal databases.

### Theft of Internal Databases

Scammers have recently shown more and more interest in users' personal data – email addresses, social security numbers, accounts for online games, and even PIN codes which a great number of institutions have chosen to store in internal databases. It's quite easy to profit from stolen databases, a fact that only fuels the crime. Both the seller of the database and the malicious users of the data being purchased can reap large profits.

Russia provides one such example of how widespread data theft is, even from organizations that are known for tight data security, such as the tax and customs services. Credit histories, databases containing customs declarations, car registration details, mobile phone numbers with associated addresses, and databases containing passport data are all freely available on the Russian black market. In some cases, the volume of data being sold is so large that it must be sold on hard disk, rather than removable storage media. The cost varies from tens of dollars to several thousand dollars, with the price varying according to the data's value and freshness.

Russia is not alone. Statistics from 2006 show many countries being hit with scandals over stolen credit card numbers and social security numbers. In the U.K., malicious users managed to steal Mastercard details from 2,000 clients of an e-commerce site. Criminals around the world are anxious to obtain and use such data.

Employees who are less than conscientious play an important role in data theft. Kaspersky Lab analysts are more frequently encountering spy programs written with the aid of insider information. For instance, there have been malicious programs created which not only permit malicious users to use internal logins and passwords from the organization under attack, but also demonstrate knowledge of the organization's internal database structure.

Withstanding an attack conducted using insider knowledge is extremely difficult, but it is possible. It is possible to protect users to some extent by implementing a few simple measures to reduce the risk of data theft. Organizations must take a holistic approach to protection – utilizing anti-virus software, firewalls, spam filters, and monitoring and auditing the network infrastructure using appropriate tools.

The number of users infected via the Internet is rising. Unfortunately, it's very simple for a remote malicious user to hack a web site, and installs a malicious program. That program is then downloaded onto the machines of users visiting the site, without their knowledge. Given this practice, organizations and companies should install an anti-virus solution which contains a web component, or use a separate product to monitor web content for the presence of malicious code.

## **Organizational Blackmail, Scams, and Ransom**

Whereas scammers primarily target rank and file users, blackmailers usually prefer to attack organizations. The most common attack method used by cyberblackmailers is a DDoS attack. Specific demands are made in conjunction with the threat that an attack is imminent. The blackmailers usually demand a specific sum, indicating that failure to pay by the specified date will result in access to network resources being blocked. Conducting such an attack via the Internet makes it relatively easy for remote malicious users to maintain anonymity.

E-commerce and bookmarking sites are popular targets for blackmailers, along with any other organizations which would suffer significant losses if their access to resources is blocked. The increase in the number of such attacks is partly due to the fact that victims often agree to pay up. Surely, reasons the victim, it makes more sense to fulfill the conditions imposed by the malicious user. However, as research from IBM shows, those who pay are more often attacked than those who refuse to do so.

DDoS attacks, however, aren't the only method used by cyberblackmailers. Earlier in this paper, we looked at malicious programs which encrypt data on the victim machine. Authors of such programs demand a specific sum for restoring the data which is being held hostage. Organizations, like individuals, can also fall victim to such attacks. And while the majority of users wait for

---

**Withstanding an attack conducted using insider knowledge is extremely difficult, but it is possible.**

---

anti-virus companies to provide a solution, organizations whose key business data has been encrypted may be less inclined to wait because of the magnitude of their potential losses. However, a decision to fulfill the criminal's demands typically leads to a vicious cycle of additional attacks, and the creation of new modifications of malicious programs.

## The Unquantifiable Loss

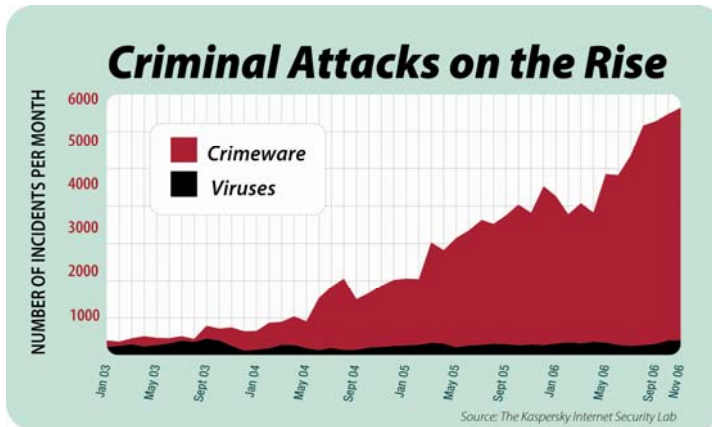
Much of our discussion has been about the loss of data, primarily financial data. However, organizations naturally have other valued assets, which may not be physically quantifiable. For instance, how much does a damaged reputation cost the organization?

There have been cases where malicious users first hack a site, and then install dedicated malicious programs that will mass mail spam. Spam is sent using the name of the victim, who is totally unaware of this, and it results in a loss of trust of both users and clients. The company's reputation suffers a blow, from which it may never fully recover.

Over the past couple of years, the number of portals being hacked, allowing malicious programs to be downloaded by innocent victims, has increased dramatically. We're not talking about small companies who truly might be unaware of the risks. Major commercial and governmental structures are at risk. Malicious code has been injected into Microsoft sites as well as security, defense, and law enforcement sites. This shows that although organizations may be well acquainted with the risks, they do not necessarily take sufficient action to address those risks.

## Conclusion

Data clearly shows that the number of attacks and the range of malicious code utilized by cybercriminals are increasing. Unfortunately, many users and organizations are more vulnerable than they like to admit.



Cybercriminals are constantly honing their methods and recruiting highly qualified people to join their ranks, including corporate insiders. Cybercrime operations are growing continually more sophisticated, with specific roles in the criminal process being clearly defined and appealing profits for all.

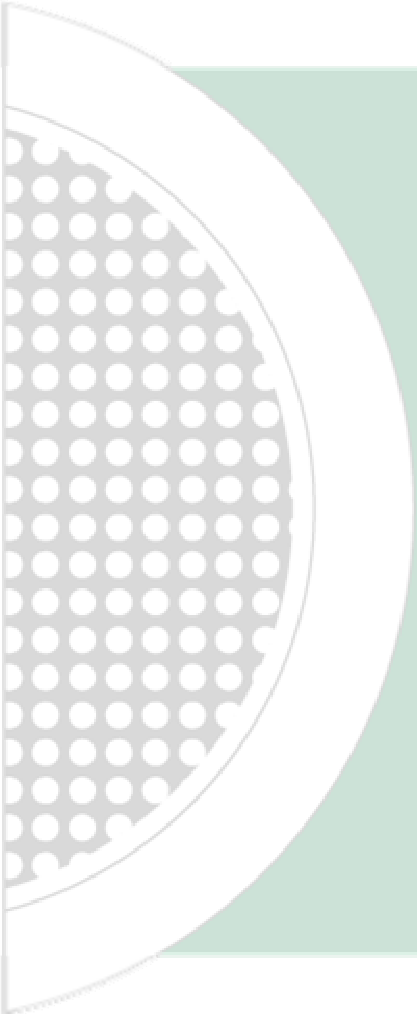
The number of attacks and victims is increasing year by year, with financial institutions being some of the primary victims of such attacks. The consequences are not only financial – an organization's reputation can be severely damaged, as can its IT infrastructure.

A holistic and highly focused approach is needed when approaching the issue of information security. Anti-virus solutions, spam filters, firewalls, network monitoring and auditing tools all have a role. Both users and organizations bear responsibility in protecting themselves. Only with such a concerted approach can we effectively withstand the growing rise of cybercrime.



Kaspersky Lab, Inc. • 300 Unicorn Park • Woburn, MA 01801  
phone: (781) 503-1800 • fax: (781) 503-1818  
[www.kaspersky.com](http://www.kaspersky.com)

## About Us

A decorative graphic on the left side of the page, consisting of a semi-circular shape with a white border and a grey interior filled with a pattern of small white dots.

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 home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of the industry's leading IT security solution providers.

Founded in 1997, Kaspersky Lab is an international information security software vendor. Kaspersky Lab is headquartered in Moscow, Russia and has regional offices in the UK, France, Germany, the Netherlands, Poland, Japan, China, and the United States. Further expanding the company's reach is its large partner network comprising over 500 companies globally.

[Learn more at www.kaspersky.com](http://www.kaspersky.com)