
# HI-TECH CRIME TRENDS 2016

GROUP-IB.COM

# KEY FINDINGS

## TARGETED ATTACKS ON BANKS

*Banks became the most attractive target for cybercriminals*

**Targeted attacks on banks, which are just beginning to spread throughout the world, have become common in Russia since 2013.** Russian criminal groups are experienced in successful hacking of almost all types of banking systems, including payment gateways, ATMs (Anunak), card processing, and trading terminals (Corkow).

**Over the reporting period, the losses of Russian banks from targeted attacks have soared by almost 300%** (more than 2/3 of thefts were committed by the Buhtrap group). All the groups dependent on them previously used to steal from legal bodies.

**Most professional groups, which used to attack companies, have now switched to attacking banks**, and the groups which have gained experience of targeted attacks in Russia are now entering foreign markets.

**Attacks on banks in Western and Eastern Europe, the CIS countries, the Asia-Pacific region, and the Middle East were carried out using a similar scheme.** The software tools used for penetrating systems, gaining additional user privileges, taking over domain control and even removing traces of attacks were identical or very similar. Some of these tools are perfectly legal and freely available on the Web.

**This scheme allows gaining access to critical systems and hacking them easily;** no expensive software development is necessary. Some groups have already ceased using privately developed trojans, and the continuous development of web services and software tools needed for targeted attacks sustains this trend.

$44mln

*The losses resulting from targeted attacks on banks in Russia*

**+292%**

*The same scheme was used by the Black Energy group in its attacks on the Kiev Borispol Airport and the Ukrainian power grid.*

## THEFTS FROM INDIVIDUALS AND COMPANIES

*Infections and thefts are becoming automated*

**In Russia, the amount of money stolen from companies by means of trojans for PC is decreasing from year to year.** Most professional groups that used to be responsible for most of these attacks have switched to attacking financial organizations; others, after gaining experience, began looking for potential victims outside Russia.

$16,7mln

*The amount of money stolen from russian companies by means of PC-based trojans*

**-50%**

Russian-speaking hackers have been boosting the supply of trojans for PC. These trojans are now used for attacks all over the world. The Russian hackers have been actively participating in developing new banking trojans, such as Panda Banker, Shifu, MidasBot, GozNym, Sphinx, and Corebot.

*16 out of the 19 trojans most actively used for theft worldwide can be linked to Russian-speaking cybercriminals.*

**Hackers rely on the automation of thefts:**

- All the new trojans designed to help steal money from companies that have appeared in Russia within the reporting period support the method of web-inject, which allows auto-upload. New Android trojans also tend to support this method.
- Using a completely legal service of card-to-card transfer, hackers have managed to completely automate phishing and vishing attacks on individuals. Such an attack may be completed in several minutes and is fully automated, i. e. it does not require any active participation from the hacker.

**Android trojans are being actively developed, with their functionality and availability growing.** This adds to the explosive growth of the number of successful attacks. Every day in Russia, 350 Android users fall victim to this scheme, and the amount of money stolen this way has increased by more than 450%. At the same time, the number of thefts from individuals by means of trojans for PC has significantly dropped, as only one criminal group still practices this scheme.

**$112K**

*The amount of money stolen from individuals with the help of PC-based trojans in Russia*

**-83%**

*The method of theft called auto-upload allows to change someone's banking details and payment amounts automatically, smoothly, and invisibly for the user.*

*A passive auto-upload is carried out while a user is forming a fraudulent payment, and an active auto-upload can be carried out even without victim's participation.*

**The amount of money stolen by means of such schemes around the world will be growing exponentially**, as the infection becomes invisible, and thefts become more and more automated:

- Android-based trojans started to spread through exploits, which allow installing malware during a user's visit to a compromised website and without the user's knowledge.
- New function: web injects for mobile browsers. This functionality is available through the newest version of Marcher, a very popular Android-based trojan, actively used for theft worldwide. The ability to manipulate the display of data on the screen by using malicious injections into the browser allows hackers to attack users of any online banking systems and to implement all the schemes that had previously been available on computers only, including auto-upload and concealing fraudulent transactions from the history of payments.
- Criminals begin protecting network communication between the C&C-server and the device, making it difficult to detect the trojan, and perform the infection in several stages. The main module is only

*Vishing is a kind of phishing, where the collection of data needed for stealing (such as usernames, passwords, or card details) is done on the phone.*

installed on devices with suitable parameters; for example, those with access to the mobile banking system of interest to the hackers.

**The number of dangerous mobile applications is growing.** Not only does such malware imitate the applications that are traditionally popular in a particular region, but it also responds to situational spikes of popularity: for example, such malware was disguised as the Pokemon Go app.

**Hackers are actively using common internet marketing tools to promote those malicious mobile apps**: keyword-targeted ads, false reviews and numbers of installations in GooglePlay, SEO-optimization of the websites from where the programs may be downloaded.

$6mln

*The amount of money stolen from individuals with the help of Android trojans in Russia*

+471%

## ESPIONAGE

*Tools for tapping conversations and intercepting traffic have become more readily available than ever before*

**More and more legitimate companies begin to offer such services as tracking the location or wiretapping of mobile phones** by using the attacks on SS7 channel. There is also a growing black market: such offers are increasingly seen on hacker forums.

**The method of intercepting traffic with BGP Hijacking, which is a perfect tool for espionage, attracts increasing attention from attackers.**

**Android trojans combine tools for both espionage and theft.** Thus, virtually all mobile trojans for theft, which are active in Russia, can be used to intercept text messages. This provides access to systems with two-factor authentication, such as cloud storages, e-mail, corporate systems, and through them, to all kinds of personal and confidential information.

*Active use of cyber-espionage for stovepiping intelligence has dramatically increased the level of threats for government officials, entrepreneurs, and journalists.*

## ATTACKS ON INDUSTRIAL COMPANIES AND CRITICAL INFRASTRUCTURE

*All factors contributing to the growth of the number of attacks are now in place*

**The media's growing interest in hacker attacks attracts new customers to this market.** Technological accidents, leakages of user data, disruptions in business processes are becoming attractive tools for the struggle for markets and buyers. The emergence of an effective scheme of targeted attack, which allows access to critical infrastructure without developing

costly malware, makes an attack easier for the contractor and reduces its cost for the customer.

**The owners of botnets for thefts have started selling access to the computers that are not of interest to themselves.** For example, we have seen negotiations for the sale of access to workstations communicating with SWIFT, and package deals for subsequent attacks with the use of encryption software. Likewise, attackers can gain access to the computers within the internal network of large industrial companies or energy suppliers.

*Sometimes, ransomware programs install remote management tools automatically.*

**New attack schemes continue to appear.** For example, an attack can be disguised as an encryption, and criminals can ask to provide remote access to an infected system in order to decrypt files manually.

**The recruitment potential of terrorist groups is growing.** The European migrant crisis, the deterioration of the socio-economic situation, the aggravation of ethnic and religious conflicts in many regions of the world — all these factors pave the way for terrorist and extremist groups which are openly recruiting more followers, including hackers, in the informal segment of the Internet.

## EXTORTION

*The number of attacks is growing and they are becoming more effective*

**The botnets used for DDoS-attacks are becoming popular again**, only now, they are no longer developed on Windows PCs, like it used to be earlier, but on Linux servers and simple IoT devices (IoT stands for Internet of Things).

**Available around the clock, not protected by any antivirus, IoT-devices have boosted the popularity of botnets for DDoS-attacks. The number of DDoS-extortionists without their own botnets is growing.** Some of them just send out threatening letters, while others commission short-term attacks to intimidate their victim.

**Attacks with the use of encryption software are becoming more efficient.** To increase the likelihood of receiving a ransom, hackers pay botnet owners to buy access to computers, which in turn have access to mission-critical systems. In addition, hackers have started to check the servers for which they already have passwords in order to find some mission-critical information which they can encrypt and thus increase the likelihood of receiving a ransom.

**New services simplifying the attacks have emerged.** There are new affiliate programs that distribute ransomware, which allows anyone to generate an executable file for extortion and provides the environment suitable for correspondence with a victim, for a share from a future ransom.

**An increasing number of attacks on mobile users.** Not only Android users are under threat. Criminals cannot infect an iOS-device with encryption malware, however, they can block it by intercepting its access to iCloud.

## BRAND ABUSE

*The range of threats for brands is expanding*

**Criminals are increasingly using online marketing tools for the promotion of websites and applications impersonating well-known brands.** Not only does this damage these brands' reputation, but it also results in loss of customers. Fake search advertising deprives official websites of their targeted traffic, and search engine optimisation methods used by the criminals leads to a drop in search rankings of official websites.

**The use of fake SSL-certificates increases the effectiveness of phishing attacks.** All malware that redirects users to fake websites uses SSL-certificates issued in the names of legitimate companies.

**The credibility of well-known brands allows for successful attacks not only on individuals, but also on companies.** For example, we have witnessed the creation and promotion of websites, which were full-blown copies of the Russian industrial and engineering companies, oil and gas companies, fertilizer manufacturers. This was done so as tomake fraudulent contracts on their behalf. An average proven damage from such attack has amounted to RUR 1,5 million (USD 23 thousand).

# FORECASTS

**Targeted attacks on banks will continue their victorious march throughout the world.**

- Professional criminal groups involved in attacks on legal entities will switch to attacking banks.
- The number of incidents involving Russian-speaking hackers will be growing worldwide, as Russian hackers have gained experience in the attacks on the Russian and Ukrainian banks, and now will foray into other regions as well.
- The teams engaged in logical attacks on ATMs will attempt SWIFT attacks. New tools and services for targeted attacks will appear.
- Hackers will increasingly search for insiders who could provide them with the right information and ensure the primary infection.
- The average damage resulting from a successful attack will increase.

**The amount of money stolen with the help of trojans for PCs will remain high, but gradually, other tools will prevail.**

- Attackers will use Android trojans with increasing frequency.
- As targeted attacks are gaining popularity, the hackers' methods will also be increasingly used for attacks on large companies' processing centers.
- Some botnets will be commercialized through the sale of access to companies' internal networks, and later these botnets will be sold to less experienced hackers.

**The number and volume of successful thefts by means of Android trojans will continue to grow.**

- Exploits for distributing Android trojans will be included in the standard exploit kits available on hacker markets.
- Web injects for mobile browsers will become more readily available, which will lead to further automation of theft attempts and to a growing number of theft victims.
- Additional products and services for improving the efficiency of the Android trojan attacks will emerge. Such services may include, for example, developing web fakes and web injects.
- As remote banking systems for corporate clients will become increasingly mobile-based, Android trojans will be used more and more often to steal money from legal entities.

**Phishing and vishing attacks on individuals will be increasingly automated** The appearance of new phishing kits with an automated billing system and payment confirmation will significantly increase the effectiveness of these attacks in various countries.

**The number of DDoS-attacks with the purpose of extortion will be growing,** however, since most of the attackers do not own botnets, their effectiveness will be low.

**Criminals will broaden their botnets using IoT devices,** also for subsequent use in DDoS-attacks. IoT devices will also be used in fraudulent schemes, for example, for the redirect to phishing websites, for search ads with hidden trojan downloads, for modified exploit servers, etc.

**There will be more incidents involving encryption-based ransomware.**

- Attacks on companies will be better targeted, which will increase the average ransom amount. Ransomware will become targeted at specific corporate sectors (such as call centers, outsourcing accounting firms at the day before the the reporting date, etc.), where it will be easier for attackers to encrypt sensitive information and demand a ransom.
- The number of incidents involving encryption of mobile devices will grow.
- The development of services to automate attacks will continue.
- New types of trojans capable of encrypting or blocking access to data on cloud services.
- When IoT-devices become popular on the market, the hunt for their security vulnerabilities will begin.

**Due to the dramatic expansion of the number of devices under attack, and to the increase of the encryption-based ransomware attacks on mobile devices, the segment of cyber insurance will be growing rapidly**. Such insurance will lead to an increase in cases where a victim will pay an attacker, which will only encourage attackers further, and this, in turn, will further stimulate the insurance market.

**The number of attacks on industrial sites will be growing, an attack on a critical infrastructure with significant damage (including human losses) is highly possible.**

- The solutions for SSL attacks and intercepting traffic are becoming more readily available. The new functionality of mobile trojans makes them increasingly better suitable for espionage. Both these factors will inevitably lead to an increase in the number of attacks for the purpose of espionage.
- The cyber-armies of various countries will continue attacking critical infrastructure facilities for both espionage purposes and to be able to use the control over them when needed.
- To hide the involvement of governments in the cyber-armies activity, hackers experienced in the targeted attacks on corporate segment will be actively recruited. Such hackers will use their tools, including tools that are legal and openly available, to gain access to systems with necessary information.
- Media coverage of successful attacks will draw cyber terrorists' attention to vulnerabilities in critical infrastructure, as attacks on it may cause public outcry and lead to human losses. Terrorists will be actively recruit hackers able to carry out targeted attacks. Attackers will be primarily interested in facilities like energy companies, transport infrastructure, airports, chemical plants, and water treatment units. Attack tactics in case of all these facilities will be very similar.

**The criminals will continue to use political differences to steal and attack in other countries**, unafraid of extradition (examples: Russia and Ukraine, Israel and Lebanon, Pakistan and India). Under the circumstances where intelligence services do not trust each other, hacker attacks can also be used to influence such political conflicts from within or without the conflicting countries.

# ABOUT GROUP-IB



Group-IB is one of the most innovative companies dedicated to preventing and investigating high-tech crimes and online fraud.

Since 2003, the company has been active in the field of computer forensics and information security, protecting the largest international companies against financial losses and reputational risks.

- The largest computer forensics laboratory in Eastern Europe with years of investigative experience
- CERT-GIB – a round-the-clock computer security incident response team
- Early warning system for proactive cyber defense

Official Europol partner

Recommended by the Organization for Security and Co-operation in Europe (OSCE)

Recognized by Gartner as a threat intelligence vendor

## PROPRIETARY INTELLIGENCE RELENTLESSLY GATHERED SINCE 2003

**High-tech infrastructure designed to collect threat data in key regions: Russia and Eastern Europe, Asia Pacific, Middle East**

### MONITORING

Network attack trackers
HoneyNet
Botnet analysis
Hacker forums
TDS Sensors
Behavioral analysis system

### HUMAN INTELLIGENCE

Forensics
Investigations
Malware analysis
Corporate security assessment
CERT-GIB activity

### INTERNATIONAL COOPERATION

Community Emergency Response Teams
Domain name registrars and hosting providers
Europol, Interpol and law enforcement agencies
Security vendors

## ADVANCED TECHNOLOGY AND EXPERIENCED SPECIALISTS

**Group-IB's solutions designed to extract data from secretive resources, monitor hacking platforms, perform forensic investigations, threat modelling and analysis:**

Detection of unknown threats using behavioral analysis algorithms and machine learning technology

Phishing detection and phish kit collection, prompt blockage of dangerous resources leveraging CERT-GIB reputation worldwide

Vast database of known cyber criminals and gangs that automatically identifies their intersections and analyzes social graphs

## EARLY WARNING SYSTEM FOR PROACTIVE CYBER DEFENCE

**Security ecosystem providing comprehensive protection for your IT infrastructure based on the cutting-edge cyber intelligence and deep analysis of actual attacks:**

### Threat Intelligence

Monitoring, analysis and forecasts of cyber threats

### TDS / TDS Polygon

Detection of targeted attacks and unknown malicious code

### Secure Bank / Secure Portal

Early fraud detection