HI-TECH CRIME TRENDS 2017

group-ib.com

HI-TECH CRIME TRENDS 2017

Contents

Key Findings

Ransomware

- Ransomware continued its march worldwide, confirming predictions outlined in 2016 Group-IB's annual report. Hackers acquired exploits and tools from the leaked NSA arsenals, which, combined with ransomware features for self-spreading in corporate networks, led to global outbreaks. Leading examples are WannaCry and NotPetya.

> Encryption-based ransomware is now used both by independent hacker groups and state-sponsored cybercriminals to cover the tracks of their attacks and distract attention from high-profile targeted attacks.

- Ransomware targeting personal computers and mobile devices has not changed greatly.

Attacks on Critical Infrastructure for Espionage and Sabotage

- Geopolitical disputes between the US and North Korea, India and China, Pakistan and India, Russia and Ukraine are being accompanied by an increase in cyber espionage and sabotage campaigns. We believe that it is not just the number of attacks that is rising, but these new conflicts have led to changes in the attackers' goals.
- In some countries, banks are considered a component of the national critical infrastructure. State-sponsored hackers have successfully attacked the banking sector for two purposes: to gather intelligence information, and disrupt the operation of target banks. For example, since the beginning of this year. Ukraine has experienced two attempts to destroy data at banks and disrupt their operations. The Lazarus North Korean hacker group targets the largest international banks and central banks worldwide for theft and espionage.

> BlackEnergy group continues to attack financial and energy companies. The group uses new tools that allow Remote terminal units (RTUs) responsible for the physical opening/closing of power grids to be remotely controlled. Test attacks on power generating companies in the UK and Ireland were tracked in the summer of 2017.

- The NotPetya attack launched in June 2017 and resulted in a disruption of internal processes in oil & gas companies and financial institutions. The attack temporarily shut down production at a number of refineries.
- Donald Trump's surprise election win has provoked animated discussions of the hackers' ability to influence the results of political campaigns. Despite the fact that attacks on politicians and state institutions as well as espionage and intelligence information collection have always existed, at the current time these attacks are linked in the media to potential attempts to affect elections and other political processes. This has prompted security specialists to thoroughly check the systems and technologies that are used to ensure the credibility and security of election processes.

Targeted Attacks on Banks and Payment Systems

- **All criminal groups that attacked Russian banks in the past have gradually turned their attention to other countries: the USA, Europe, Latin America, Asia and the Middle East, though we have witnessed continued successful attacks on financial institutions in Russia as well.**
- MoneyTaker (Carbanak related), a Russian-speaking hacker group that conducts targeted attacks on financial institutions across the world, has focused on small North American banks, one of which they robbed twice.
- Cobalt is the most aggressive and active hacker group. They attack a wide range of targets – banks, payment systems, and IT companies – constantly changing regions of interest. Following series of 'international' attacks, they focused on the CIS countries, but later continued their attacks with no obvious focus on a region.
- This year MoneyTaker and Cobalt primarily targeted ATMs and then later card processing systems. During their attacks they gained access to computers connected to SWIFT, but we did not detect any attempts to steal money through this interbank fund transfer system.
- One of the hacker groups developed an automated system to steal money through the AWS CBR (Automated Work Station Client of the Russian Central Bank), an interbank fund transfer system similar to SWIFT, but it was used only once, in Russia.
- To gain control over corporate networks, cybercriminals primarily use legitimate tools for penetration testing — Metasploit and Cobalt Strike.
- They often employed such legitimate tools as Plink and AmmyAdmin to establish these channels.
- **DNS protocol is now used more often to control malware as well as to deliver payloads, which allows cybercriminals to bypass network traffic analysis systems.**

Fileless malware using malicious scripts to launch an attack is a new and currently the primary attack method. To slip under the radar, hackers use fileless software that exists only in RAM until the system is rebooted. That said, malicious PowerShell, VBS, PHP scripts help them to ensure persistence in the system and automate some stages of their attacks.

- The processing systems of self-service payment terminals have become a new target for hackers involved in targeted attacks. They gain access to terminals' processing systems using the same proven techniques used in attacks on ATMs, card processing, and SWIFT workstations. However, they use different channels to launder money.
- Focusing on ATMs and card processing systems has reduced the average amount of loss from one cyber-attack, but it enables the attackers to carry out attacks that are safer for 'money mules' who deal with cash withdrawals. The attackers are located in one country, the attacked bank is in another and cash is withdrawn in a third locale.
- Email phishing remains the key infection vector for initial penetration into the networks of financial institutions.
- **Despite the fact that some banks use reliable anti-phishing tools, employees often check their personal email, which is not protected by corporate security tools, on workstations. This flaw has been leveraged by criminals. To attack a range of banks hackers gathered personal email addresses of bank employees to send them emails with malicious attachments during business hours.**
- Group-IB staff detected a new method to complicate investigations and incident response during targeted attacks on banks – this is where attackers use of ransomware to encrypt data on disks and cover their tracks.

Attacks on Bank Clients

- The number of groups and subsequently the number of attacks on companies in Russia aimed at committing theft has decreased by almost 50% compared to the previous period. However, the average loss has increased, and it shows that hackers are now choosing their victims more carefully.
- Corebot and Vawtrak (aka Neverquest) that were previously used in cyber-attacks on companies worldwide have left the market. The Corebot developer has simply stopped supporting it. As for Vawtrak, its main developer was arrested, after this, the malware dropped off the radar.
- **Every month, Russian-speaking hackers create 1-2 new malicious programs designed to steal money. Experts have detected 6 new PC Trojans. The best known among them is TrickBot.** 12 new banking Trojans for Android have appeared with no obvious leader among 'newcomers'. There are also 3 new Trojans for POS terminals, and old existing versions are still developed and extensively used with enhanced features.

> 20 (91%) out of 22 new malicious programs used to steal funds were created and are controlled by Russian-speaking hackers.

- **The beginning of this year saw the first cases of a new vector for theft using SS7 protocols, where during attacks on bank accounts in Germany, hackers bypassed two-factor authentication via SMS texts by exploiting call-forwarding features built into SS7.**
- In Russia, owners of banking botnets targeting legal entities have completely stopped using man-in-the-browser attacks in favour of remote control tools and automatic transfers via 1C accounting systems.
- Some hackers prefer forwarding traffic to their C&C servers in order to intercept and manipulate data to use web injects.
- Owners of the Buhtrap Trojan have delegated control over their botnet to other threat actors. After that, tactics of attackers changed and now their key infection vector is hacking legitimate websites, including financial and law firm resources, instead of spamming.
- **In Russia, the amount of loss caused by Android banking Trojans has increased by 136% and exceeded the loss caused by Trojans to personal computers by 30%.**
- Android banking Trojans are still attacking individuals. Attacks on companies have not been detected via this vector.

> Owners of Android botnets have started to use Apple Pay to steal money from bank accounts.

- **Phishing for banks and payment systems is automated and conducted in real time, which allows cybercriminals to bypass SMS confirmations for debiting money.** Every day over 900 bank clients become victims of financial phishing in Russia, which is three times the daily number of malware victims. However, the amount of loss caused by phishing is dozens of times lower than when it is caused by malware.
- On average, 10-15% of visitors of financial phishing websites enter their data.
- In 80% of cases phishers register accounts to collect compromised data in Gmail, while Russian search engines Yandex and Mail.ru account only for 6%.

Attacks on Cryptocurrency Services

- The hype around cryptocurrency and blockchain technology turning ICOs into the next digital gold rush has led to attacks by cyber criminals increasing exponentially. 2017 saw a series of successful attacks on cryptocurrency platforms and their users.
- **Attacks on cryptocurrency exchanges are conducted in the same way as targeted attacks on banks with similar or sometimes identical tools and tactics.**
- Cases when fraudsters create phishing websites copying content from websites belonging to companies launching ICOs have become more frequent. On such websites, users enter secret keys for their wallets, after that the money is stolen automatically.
- Startups launching ICOs do not pay enough attention to their website security. Attackers gain access to such websites, replace a wallet address with a fraudulent one and collect funds transferred as part of the ICO.
- We are seeing an increase in the number of incidents when hackers steal crypto wallet details using malware and withdraw money. The methods are identical to those used for attacks on users of banking applications.

> In addition to malware, cybercriminals actively compromise email addresses and use fake ID to get victim's SIM-card to recover passwords and gain control over accounts in cryptocurrency services.

- Cryptocurrency-mining Trojans have been used by cybercriminals for quite a long time. However, due to already significant emission, mining on hacked computers and servers yields increasingly lower results from year to year. That is why attackers are beginning to use them to mine new cryptocurrencies.

Development of Hacking Tools

- A number of criminal groups and state-sponsored hackers enriched their arsenals due to leaks from US government agencies. CIA and NSA toolkits published by WikiLeaks and The Shadow Brokers respectively were immediately added to malware and penetration testing tools to be further used in attacks worldwide.

> Many developers of malicious code have begun to publish the source code of their programs with increased frequency. During the reporting period, source code for a banking PC Trojan dubbed TinyNuke, an Android banking Trojan Maza-in, the RATAttack toolkit, that uses the Telegram protocol, and a DDoS Trojan named Mirai as well as various types of ransomware were made public.

- Last year it became obvious that hackers were interested not only in computers and mobile devices, but also in IoT devices and routers. **This year Android Trojans as well as ExploitKits were detected to have focused on gaining access to routers in local area networks and manipulating user traffic.** A little later, it became known that the CIA had used the Cherry Blossom tool for the same purpose.
- Through analysis of CopyCat, Gooligan, and DressCode Android Trojans security specialists have discovered that the largest botnets are located in Asia and are designed to display advertising.

Forecasts

Tools and Attacks on Critical Infrastructure

- The WannaCry and NotPetya attacks allegedly organized by state-sponsored hackers have shown the whole world how easy it is to make an effective ransomware that spreads itself within corporate networks. None of the financially motivated groups have ever conducted attacks in such a manner. The scale of the outbreak, the speed of infection and the damage done to the victims will most certainly lead to the appearance of imitators and successors and new attacks from traditional, financially motivated cybercrime. By changing the vector of initial network penetration, they can cause much more serious damage.
- NotPetya has demonstrated that creating a template can be enough to gain control over a corporate network. **In the future, we should expect many scripted cyber-attacks as well as ready-made simple tools that can gain control over corporate domains automatically**. If such tools are made publicly available or are sold among hackers, this can lead to an avalanche in the growth of attacks on the corporate sector. We primarily expect more incidents involving ransomware, theft of confidential information and extortion for non-disclosure, money theft, and incidents of public exposure by non-financially motivated hackers.

> increase in state-sponsored hacker activity and a lot of attention devoted to the topic of cyber-attacks, we may see more successors of The Shadow Brokers and insiders helping WikiLeaks in the near future.

- We expect malware developers to be more active in continuing to publish codes of their programs online. In addition, leaks published by The Shadow Brokers and their potential followers will also be immediately used for malware creation and improvement. This will give a powerful boost to the development of the cybercrime industry.
- Ransomware-related attacks will be primarily focused on countries imposing high fines for the disclosure of confidential information.

Targeted Attacks on Banks

- **Whereas in the past financial institutions were concerned about being attacked by financially motivated hackers, now they may have to face a new and more dangerous threat posed by state-sponsored hackers.** These hackers will be focused on monitoring cash flows, gathering compromising information about bank clients, as well as disrupting the performance of internal infrastructure. The latter objective is especially relevant for countries that accuse each other of cyber-attacks: they may use sabotage as a counter measure.

> In the next year, the main point of losses for banks from cyber-attacks will be not theft of money, but destruction of their IT infrastructure during the final stages of a targeted hacking attack

- One of the possible sabotage scenarios may be trading on exchanges on behalf of the victim bank in order to influence exchange rates and cause losses. This can lead to snowballing style flash crashes as HFT trading algorithms respond to fluctuations in exchange rates.

- Financially motivated hackers will remain focused on card processing systems because it is the safest area for attackers and the procedure for cash withdrawal is relatively simple and mule operations are low risk.
- Accordingly, this trend offers opportunities for less experienced attackers, because card processing attacks are safe for those engaged in cash withdrawal, it is simple to implement and does not require reliable money laundering contacts from the attackers, as opposed to SWIFT related attacks. That is why next year we may see some cyber attacks committed by entirely new groups.
- **Banks should pay special attention to connections of authorized partners to corporate networks because these partners have already been used in a number of attacks as a major vector for penetrating banking infrastructure.**
- The developer of a banking Trojan Vawtrak (aka Neverquest), which is used for cyber attacks on companies in various countries, has been arrested. However, his highly professional team with experience of large-scale theft and access to reliable money laundering schemes is still at large. We expect them to start conducting targeted attacks on banks and their clients.

Targeted Theft Attacks

- **If developers of banking and POS Trojans for personal computers add a function for self-spreading in corporate networks and automatic search for computers engaged in online banking, it will result in a significant growth of successful cyber attacks both on business and private bank accounts, because corporate network users conduct online banking from their workstations.**
- With the extensive use of mobile banking in the corporate sector, Android Trojans will start attacking users of these applications. Under these circumstances the method for distributing Trojans will remain the same.
- In Russia, the amount of loss caused by theft with the use of Android banking Trojans has already exceeded the loss caused by banking Trojans for personal computers. We expect a similar situation to develop in other countries where mobile banking services are widely used.
- To reduce costs and increase efficiency, hackers will continue to move away from using web injects in favour of traffic redirection to their servers with a view to intercepting and manipulating traffic data. This may result in a creation of services for automating traffic data process manipulation.
- Selling traffic from routers may create a new service that will allow cybercriminals to increase the number of phishing attacks significantly. Users will be simply redirected to phishing pages during specified periods of time. Under these circumstances, services offering higher quality victim will become especially popular.

Attacks on Cryptocurrency Services

- Android Trojans will allow hackers to carry out much more efficient attacks on cryptocurrency users. The methods for identifying crypto wallet owners and gaining access to crypto wallets will be identical to those used for cyber attacks on bank accounts. Android banking Trojans in their current form will most likely be adapted.
- In addition to Android Trojans, hackers attacking cryptocurrency users will be actively using PC Trojans. That said, universal Trojans will be used more often, including those that are publicly available instead of dedicated banking Trojans.
- **Targeted attacks on cryptocurrency exchanges will be carried out not only by financially motivated hackers but by state-sponsored attackers as well.**
- Phishing against cryptocurrency service will be the main problem for users of these services.

Continuous successful attacks will affect the trust level for services until they improve their security level and start actively countering phishing.

> Due to an easier money-laundering and less regulatory oversight, some groups specializing in targeted attacks on banks and payment systems will switch their attention to cryptocurrency exchanges.

- Anything related to cryptocurrency will become the main target for hackers specializing in web based attacks. Selling traffic from these websites will become their key driver due to the high demand from hackers controlling Android, PC Trojans, whereas compromised user contacts will be actively used in targeted attacks, phishing, vishing, including brute-force attacks.
- The finance industry has long been the main target of extortion attacks. At first, the number of attempts to extort money from owners of cryptocurrency services will grow due to both hackers posing a real threat and their imitators who are not capable of conducting sophisticated cyber attacks.
- A rise in the Bitcoin exchange rate, as well as the hype around new cryptocurrencies and ICOs have resulted in an increased interest to this topic in broader audiences. More and more people want to invest in cryptocurrencies. As a result, many fraudsters will bring back already inactive fraudulent schemes related to “investments“, “asset management“, “pyramid schemes“, etc.

Hi-Tech Crime Market Assessment

The growth in the number of attacks and the amounts stolen is a significant indicator of the hackers' financial activity, changes in their tactics and targets. The majority of attackers follow the money, and if they find more efficient and safer ways to earn it, they start investing in them, creating new tools, services, and attack schemes.

In Russia, the amount of loss caused by stealing from companies is still in decline, but the loss caused by Android banking Trojans is still on the increase. The number of targeted attacks on banks and payment systems is on the rise, but hackers have earned the majority of their profits outside Russia, as we predicted last year.

After phishing attacks on bank clients and payment systems were fully automated, the amount of loss from their activity in Russia became very significant. Every day they attack many more users than banking Trojans, but the net amount of loss is still smaller. However, due to the simplicity of the scheme, an increasing number of criminals are starting to use it.

Market Segment in Russia and CIS	Number of groups	Total number of successful attacks per day	Average amount stolen at a time USD	Amount stolen per day USD	H2 2016 — H1 2017 USD	H2 2015 — H1 2016 USD	Growth percentage vs. previous period
Money stolen from companies via online banking using malware	3	2	$20 833	$41 666	$10 375 000	$16 774 737	-35%
Money stolen from individuals via online banking using malware	1	1	$1 050	$1 050	$261 450	$112 705	144%
Money stolen from individuals using Android Trojans	10	300	$183	$55 000	$13 695 000	$6 115 789	136%
Targeted attacks on banks	2	—	—	—	$27 166 667	$43 859 649	-35%
Phishing	15	950	$16	$15 833	$3 942 500	—	—
Withdrawal of stolen money	—	—	—	$43 972	$23 174 153	$30 088 296	-19%
Total				**$113 550**	**$78 614 769**	**$96 951 177**	**-19%**

Key Trends and Facts of 2016 H2–2017 H1

Ransomware

Ransomware has acquired self-spreading features

Last year we predicted that Trojan ransomware would acquire features for self-spreading in local area networks on its own and be used for targeted infection of large companies with a view to receiving a ransom in exchange for recovered access to files. It could enable hackers to raise ransom amounts and increase their chances of receiving them. However, the opportunity attracted the attention of state-sponsored hackers rather than those who are financially-motivated.

On 14 April 2017, The Shadow Brokers hacker group posted information on the vulnerability and the executable code of EternalBlue exploiting a vulnerability in the Server Message Block (SMB) protocol v1 (SMB).

On 12 May 2017, the WannaCry ransomware appeared, and, on 27 June 2017, NotPetya ransomware began to spread on a massive scale.

Specialists associated the WannaCry attack with the pro-government North Korean Lazarus group and the NotPetya attack was attributed to the state-backed Black Energy group.

It is obvious that neither of the attacks was motivated by financial gain, although in both cases the victims were required to pay.

Loss caused by State-backed ransomware

The target aims of WannaCry distribution have not been detected. Considering that the attacks were carried out by state-sponsored hackers, the chances are that they were aimed at particular facilities whose performance had to be disrupted. All the other victims were hit incidentally. Only companies whose operating systems were not updated and were directly connected to the Internet suffered from the attack.

The NotPetya attack was more targeted. It struck only companies using M.E.Doc software, created by a Ukrainian document management system developer. Therefore, this can be seen to be targeting Ukrainian legal entities.

In both cases, it would have been sufficient to change the initial penetration vector and the number of victims in the segment concerned would have been much higher.

Covering tracks of attacks

We also predicted that ransomware would be used for covering tracks of targeted attacks. At the beginning of 2017, we detected the first cases of ransomware use to cover traces of a bank robbery during incident response. a robbery-motivated attack on a bank, the hackers gained control of its domain. After the robbery, they launched a modified version of Petya on behalf of the domain administrator on all the network computers. As a result, the majority of the computers were encrypted which made investigating the cyber attack significantly more difficult.

PC and Android Ransomware

Hackers that use ransomware are becoming increasingly focused on the corporate sector. We have not detected any new hacking techniques or unique tools used by financially motivated hackers. Locky

and Cerber have become the most popular ransomware. Both are distributed through a partner program by Russian-speaking hackers. Spam still remains the main vector of distribution. However, some partners have also used exploit kits to transfer ransomware to vulnerable computers.

Ransomware for mobile devices has become much less popular. Over the last 12 months no new offers for buying such programs were posted on Russian-speaking forums.

The forecasts for IoT ransomware attacks have failed to materialize, and so far there is no indication that hackers may be preparing to launch them next year. Attacking the corporate sector is still profitable, and the new feature used for self-spreading ransomware in local area networks opens wide opportunities for efforts in this particular area. That is why we expect the greatest losses to be caused by self-spreading ransomware creating disruption to business continuity. Unlike WannaCry and NotPetya attacks, these attacks will be more targeted.

NotPetya has demonstrated that scripting several simple steps is enough to gain control over a corporate network. In the future we should expect many more scripted cyber attacks as well as simple ready-made tools that will gain control over corporate domains automatically. If such tools become publicly available or are offered for purchase among hackers, this may lead to an avalanche in growth for all kinds of attacks on the corporate sector. We primarily expect more incidents with ransomware, theft of confidential information and non-disclosure extortion. These types of cyber attacks should be expected mainly in countries where there are high penalties for non-compliance with security measures, data leaks or disruption to services provided. It is especially relevant for the banking sector, insurance companies, and medical institutions.

Attacks on Critical Infrastructure

Development

Attacks on industrial facilities, detection of vulnerabilities, and remote access gained to control terminals of Industrial Control Systems (ICS) are being reported more and more often. But a successful attack leading to a physical disruption of IC systems requires a more than just a remote access and logins credentials. It requires a deep understanding of the physical processes in the IC systems to be able to have an impact on them and what is most important, to have an impact on these physical processes, this logic must be built into the attacker's tools.

The first malware program that was really able to affect physical processes and put equipment out of operation was Stuxnet virus used by the Equation Group (Five Eyes/Tilded Team). Stuxnet's key feature was the ability to have a destructive influence on Siemens equipment that was used to control the spinning rate of Iran's uranium enrichment centrifuges. By attacking Siemens equipment, Stuxnet would imperceptibly change the spinning rate of centrifuges in line with logic pre-determined by, which resulted in the destruction of this equipment. Stuxnet story broke in 2010 heralding a new era of cyber war and cyber security. This attack was followed by a lull that lasted several years during which hackers were seeking ways to impact ICS and disable them whenever needed. It was BlackEnergy group aka Sandworm who moved much closer towards this goal.

The Energetic Bear campaign (Dragonfly/ Crouching Yeti) targeting energy companies caused a bit of a stir when uncovered in 2014 using the Havex tool, which was purportedly installed in over 2,000 networks. However, Havex could not affect physical processes. It was an exploration stage, whose prime objective was to gather information on the equipment used in these energy companies; and to gather this information it would 'bug' the OPC (Open Platform Communications) protocol used to

control automation objects and technology flows. To put it simply, it would analyze the interactions between SCADA and hardware, and register what equipment was installed in each specific location. This process is of paramount significance for future attacks.

Another significant preparation stage was accessing SCADA Human Machine Interfaces (HMIs). The Black Energy 2 malware used by the same-named group (or Sandworm) was targeting HMIs of three vendors: General Electric's Cimplicity HMI, Siemens' SIMATIC WinCC and BroadWin's WebAccess. Black Energy 2 was installed on their servers taking advantage of vulnerabilities in these products.

In December 2015, a second attack, like-Stuxnet, was carried out at a critical infrastructure facility, which resulted in real damage and service impact. Black Energy 3 malware was used for the attack. The attackers used it to overload the network in three energy companies in Ukraine, substituting the firmware of Serial-to-Ethernet devices at sub-stations, which put them out of operation. Following this, they remotely disconnected uninterruptible power supplies, and disabled Windows computers, including those with HMIs, in the energy company network using a simple tool KillDisk.

Results of evolution

In December 2016, a test attack was carried out on a Ukrainian substation which plunged the city into darkness for 75 minutes. This barely noticeable attack demonstrated the capability of the new set of Black Energy tools, which was named Industroyer or CRASHOVERRIDE, as reported by ESET.

Industroyer is a full-fledged framework to attack ICS. Drawing on their past experience and investments in developments, the attackers automated a number of processes.

Like in the Havex case, the new malware leveraged legitimate functionality in the OPC protocol to map out the industrial equipment and devices on an ICS network.

Similar to Black Energy 2, this tool attacked HMI libraries and configuration files to better understand the environment, and be able to connect to other locations in the energy network.

As in the Black Energy 3 attack, they learned how to overload the energy network, and disable some of its elements in order to complicate the response and the restoration of power supply.

But on top of that, they came up with new modules to operate with such protocols as IEC 60870-5-101, IEC 60870-5-104 and IEC 61850. These protocols are used for remote control of Remote Terminal Units (RTU's) which are responsible for the physical connection / disconnection of the network. It is interesting to note that such elements are not only used by energy companies but also by other city services, such as water supply and gas supply systems.

Another addition was a module for exploiting the old vulnerability CVE-2015-5374 in Siemens SIPROTEC equipment, which initiates service denial and makes the device unavailable.

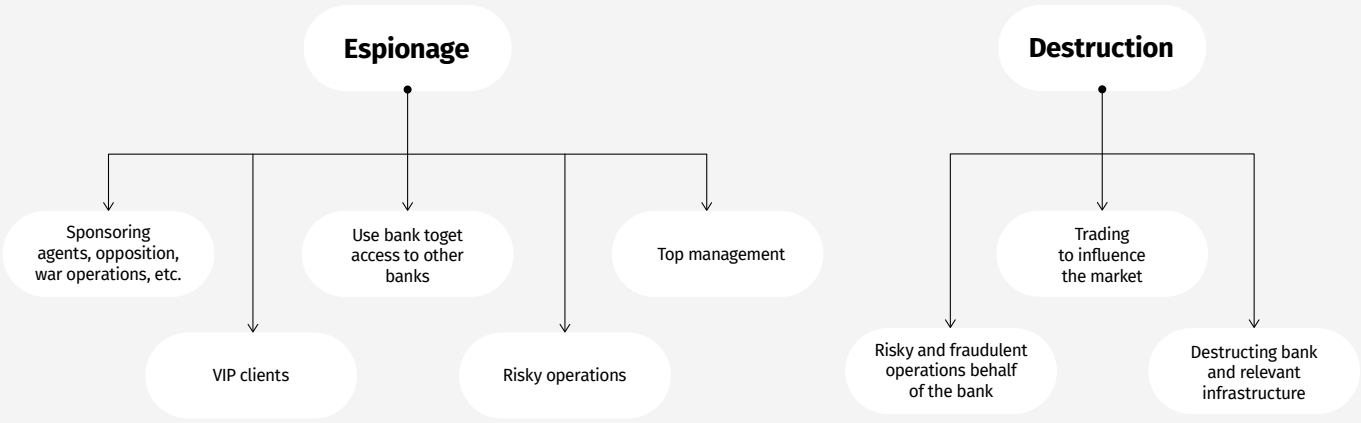
Other new developments from Black Energy

Black Energy is known for its attacks on energy companies. This year Group-IB confirmed they have stepped up their efforts in attacking banking infrastructure as well as.

Apart from the key Black Energy malware, they use a new backdoor that uses a secure Telegram protocol. There are two versions of it, one coded in Rust and the other in Python.

They previously used the unique utility application KillDisk, whereas now they have coded their own ransomware on the computers and servers of banking networks. The ransomware is identified as Win32/Filecoder.NKH, and encrypts files by using RSA-1024 and AES algorithms adding the extension .xcrypted to the files.

In June, they launched an attack with NotPetya. Both the unique ransomware and NotPetya were used to disable the local networks of commercial organizations.



Targeted Attacks on Banks and Payment Systems

State-sponsored hackers pose a new threat to banks

Some countries have recognized their banking system is an object of critical infrastructure. Hackers hired or sponsored by governments have successfully attacked the banking sector several times for two purposes — gathering intelligence information, and disrupting the performance of target banks.

Equation Group (US)

On April 15, hackers from The Shadow Brokers uploaded a new dump from a set of hacker tools from Equation Group that presumably operates out of the NSA. According to the leaked documents, they carried out two attacks on SWIFT Service Bureaus to access banking transactions data of a number of financial institutions of the Middle East and Latin America.

SWIFT Service Bureaus are third-party service providers organizing and allocating links to SWIFTNet for financial organizations that wish to be connected to the network but still prefer to outsource these transactions. According to SWIFT, the service package includes separation, allocation and exploitation of the components for connecting with SWIFT, as well as providing mechanisms for accessing the system, managing communication sessions, and ensuring the safety of SWIFT users.

SWIFT-associated archives are called JEEPFLEA, and include registration and architecture details of EastNets, the largest SWIFT service bureau in the Middle East. The second service bureau is presumably the Business Computer Group (BCG) in Panama.

Since the banking transactions are logged to the Oracle database based on SWIFT software, the leaked archives contain the description of the tools used by the NSA to retrieve data from the database, including a list of users and inquiries in the form of SWIFT messages.

The archive documents leaked by Shadow Brokers include identifiers, accounting records information and administrator account data.

Lazarus (North Korea)

In February 2016, an attempt to steal 1 billion USD was reported by the Bangladesh Bank. Analyzing the malware code, cyber security specialists identified some code fragments that had been previously used in other attacks. Based on the code similarity and a similar scheme of system deployment on infected computers, the specialists linked the attack to the Lazarus group.

As early as February 2017, it was reported that several banks in Poland had been compromised. The investigation revealed how the banking systems had been broken into and what malware had been used, also identifying some other regions and web resources that became targets. Through analysis of malicious code, specialists again linked the attacks to the Lazarus group. The

Lazarus group targets the largest international banks as well as central banks in various countries. But as opposed to the incident in Bangladesh, the attackers were not looking for money.

Kaspersky Lab published a report on responding to an incident that involved the Lazarus group. During the response operations, the tools for dealing with SWIFT were identified. One of the primary purposes of the tools was collecting data about transactions: Sender and Receiver, Account and Statement Numbers as well as some other data.

Moreover, in analyzing the activities of this Group, it was discovered that it had had access to the networks of several banks for months, but none of them had fallen victim to theft.

BlackEnergy

BlackEnergy Group has always focused on disrupting the performance of its attack targets, including banks. For example, since the beginning of this year Ukraine has experienced two attempts of destroying data in banks.

In late 2016, targeted attacks were identified on financial institutions in Ukraine. The TeleBot backdoor coded in Python was uploaded to target computers by using a downloader coded in RUST. **In January-February 2017, the criminal group managed to compromise the network of a large IT integrator in Ukraine. As a result, the criminals managed to access four Ukrainian banks and upload a Trojan similar to TeleBot, which was, however, coded in RUST.**

After gaining access, they would upload the Telegram backdoor and a self-coded RAT. They would later use Mimikatz to obtain the admin login and password to access other computers of the network. After getting hold of admin credentials for the domain controller, they would run ransomware to encrypt files on computers and servers of the banking network. The ransomware is identified as Win32/Filecoder.NKH, and encrypts files with RSA-1024 and AES algorithms, adding the extension of .xcrypted. It encrypts all files apart from the C:\Windows directory. Upon completing the encryption, the Trojan creates a file named !readme.txt with the following content: Please contact us: openy0urm1nd@protonmail.ch.

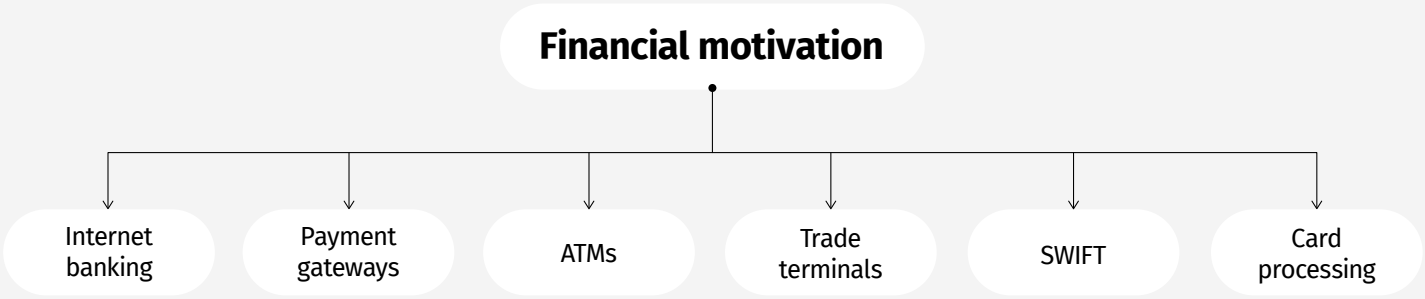
On 27 June 2017, the world learned about a massive attack carried out with the use of NotPetya ransomware. It targeted companies that were using M.E.Doc., accounting and document management software from a Ukrainian developer.

The attackers accessed the M.E.Doc. source code and update server that they used to distribute infected auto updates. After the launch of NotPetya, files were encrypted and the Trojan was distributed further through the corporate network with the use of the Eternalblue-like exploit and a legitimate remote-control tool PsExec.

To take full control over a corporate network, both state-sponsored and financially motivated hackers would often follow a simple scenario that we described in our previous report. It can be divided into the following stages:

1. Getting access to any computer within the network.
2. Getting logins and passwords from the first infected computer.
3. Connecting to neighbouring computers by using logins and passwords acquired and getting passwords from these computers to find the domain admin password.

In the NotPetya attack, the hackers just scripted this simple attack pattern, which enabled them not only to successfully attack companies using M.E.Doc, but also others that were connected to the infected ones. It is this strategy that opens Pandora's box. In the future, we should expect a large number of scripted attacks as well as ready-made simple tools that will automatically take control over corporate domains. If such tools are made publicly available or are easy to buy for hackers, this may lead to an avalanche in growth of all kinds of attacks on the corporate sector. Primarily, we expect more incidents with ransomware, theft of confidential information and extortion of non-disclosure, money theft, and public exposure carried out by non-financially motivated hackers.



Financially motivated hackers

As expected, financially motivated hackers have become more active in attacking financial institutions around the world. Phishing emails remains the main hacking method for penetrating banking networks regardless of the target region.

The attackers are aware that some banks use reliable security tools for protection against email phishing; however, bank employees in such institutions still check their personal emails at their work stations that are not protected by corporate security tools. That is why, to attack some banks, hackers gathered personal email addresses of bank employees to send them emails with malware attachments during work hours.

The most widely used tools for creating malicious attachments sent in phishing emails are Microsoft Word Intruder (MWI) by Objekt and OffensiveWare Multi Exploit Builder (OMEB).

The MoneyTaker group focused its efforts on small North American banks, one of which they robbed twice. In addition to North America, they actively attacked other regions, including Russia. It is worth noting that some MoneyTaker attacks on banks are related to Anunak (aka Carbanak, FIN7 Navigator, Teleport Crew, Digital Plagiarist), but we consider them as a separate group closely related to the members of the Anunak group.

The Cobalt group attacks financial organisations indiscriminately, experimenting in various regions. At different times they have focused on the CIS countries but later carried on attacking globally with no clear focus. Working with victim banks and those that have become a potential target, we see that these financial institutions prefer to mostly focus on the safety of SWIFT and ATMs, because successful attacks on these targets are widely covered by media. However, currently attackers seem to be more interested in a wider range of banking systems. In addition to incidents with ATMs and SWIFT, we have identified attacks on card processing systems, payment gateways and terminals, and stock trading terminals. Online banking seems to be the only system eluding attackers' attention; however, it has been frequently and successfully attacked and robbed in the past by other financially motivated groups.

Fileless attacks using scripts

Fileless attacks using malicious scripts are a new and currently the most popular attack method. Hackers try to stay as inconspicuous as possible, and therefore they use 'bodiless' malware which only exists in RAM and gets destroyed after rebooting. That said, PowerShell, VBS, PHP scripts help them to ensure persistence in the system and to automate some stages of their attacks.

Going fileless provides the following benefits for attackers:

- They cannot be easily detected by standard antivirus tools.
- They keep no files on the disk, leave fewer

traces of malicious activities, and severely complicate the response process and, consequently, future criminal investigations. Without files, you cannot see their attributes or understand when the malware penetrated into the system, how it got activated, what functions it has etc.

Scripts also provide a number advantages as well:

- Malicious scripts are also almost undetectable by antivirus tools. It is much more difficult to code a signature against a script without false-positive activation than to code a signature against a binary file.
- Scripts are easy to modify, which makes attackers' work much easier.
- It is easy to ensure persistence. Scripts are typically stored in the log, or activated by specific events via Windows Management Instrumentation (WMI), Group Policy Objects (GPOs), Scheduled tasks. These kinds of scripts are very simple, and usually their primary task is to upload the main software from an external or local source, and activate it.

  Imagine a situation that involves a bank theft. During the attack one of the computers retains a Scheduled Task to execute a script that just uploads a file from legal cloud storage and runs it. Detecting this task without a proper response is not easy, which is why we witnessed one situation where a bank was robbed twice in a nine-month period.

ATMs as the target

In July 2016, hackers conducted a series of successful attacks on ATMs of the Bank of Taiwan (First Bank). The attack was carried out in several cities, with the criminals eventually stealing $2.18 million. The people who withdrew the money were arrested, but it was never established who was actually behind the attack.

In December 2016, analysts from Group-IB found the malware that had been used to attack the Bank of Taiwan. It was much like ATMSpitter developed and used by the Cobalt group in other incidents. It is this group that was responsible for the majority of attacks involving ATM all over the world. The strategy and tools used by the group to attack ATMs are described in detail in a separate report https://www.group-ib.com/cobalt.html

European banks were attacked with the use of ATMSpitter implementation with the standard library MSXFS.dll. In Taiwan, the criminals used the implementation with the standard library CSCWCNG.dll. Further investigation fully confirmed that the attack had been carried out by the Cobalt group. At the time, the group was predominantly interested in ATM control network segments, with subsequent initiation of cash dispensing from the ATMs. Only after that they switched to other targets within the banks.

Both malicious programs are basically the same 'main' function that is executed sequentially without creating separate flows. Functions are sequentially called from financial libraries, and the command is given to dispense cash. Moreover, the two implementations have the following common elements:

- The majority of ATM-targeting malicious programs are equipped with advanced protection systems, such as session passwords and commercial protectors for complicating reverse engineering by other criminals, log clearing and temporary disconnection from the network for concealing their presence, recording into the alternative NFTS flows, and encryption of service files and logs. Neither of the ATMSpitter versions has any of this.
- They only use one protection technique — verification of the run month. If the current date does not coincide with July 2016 (Taiwan) or September 2016 (Europe), the programs will display a special error message. It looks as if it is impossible to connect to the device.

	Parameter	Europe ATMSpitter implementation with the standard library MSXFS.dll	Taiwan ATMSpitter implementation with the standard library CSCWCNG.dll	Notes from Group-IB analyst
1	Protection	Verification of the run month. If the current date does not coincide with September 2016, the malware displays an error message. It looks as if it is impossible to connect to the device. WFSOpen failed with error: **WFS_ERR_INTERNAL_ERROR** It corresponds to the month of the incident in the European bank, September 2016.	Verification of the run month. If the current date does not coincide with July 2016, the malware displays an error message. It looks as if it is impossible to connect to the device. Error message: CscCngOpen/CscCdmOpen failed with error: **System Failure** It corresponds to the month of the incidents in Taiwan, July 2016.	It corresponds to the dates of incidents (September 2016 in Europe, and July 2016 in Taiwan). In this case, a user running the software will not see the real cause of the failure that is known only to the developer.

2	Identical code chunks	int v1; // eax@1
		CHAR *v2; // ebx@1
		HANDLE v3; // esi@1
		int v4; // eax@1
		DWORD NumberOfBytesWritten; // [esp+2Ch] [ebp-Ch]@1
		va_list va; // [esp+44h] [ebp+Ch]@1
		
		va_start(va, a1);
		NumberOfBytesWritten = 0;
		v1 = lstrlenA(a1);
		v2 = (CHAR *)malloc(v1 + 10240);
		wvsprintfA(v2, a1, va);
		v3 = CreateFileA(«disp.txt», 0x120116u, 3u, 0, 4u, 0, 0);
		SetFilePointer(v3, 0, 0, 2u);
		v4 = lstrlenA(v2);
		WriteFile(v3, v2, v4, &NumberOfBytesWritten, 0);
		CloseHandle(v3);
		free(v2);
			int v1; // eax@1
			CHAR *v2; // esi@1
			HANDLE v3; // edi@1
			int v4; // eax@1
			DWORD NumberOfBytesWritten; // [esp+Ch] [ebp-4h]@1
			va_list va; // [esp+1Ch] [ebp+Ch]@1
			
			va_start(va, lpString);
			NumberOfBytesWritten = 0;
			v1 = lstrlenA(lpString);
			v2 = (CHAR *)malloc(v1 + 10240);
			wvsprintfA(v2, lpString, va);
			v3 = CreateFileA(«displog.txt», 0x120116u, 3u, 0, 4u, 0, 0);
			SetFilePointer(v3, 0, 0, 2u);
			v4 = lstrlenA(v2);
			WriteFile(v3, v2, v4, &NumberOfBytesWritten, 0);
			CloseHandle(v3);
			free(v2);
				Both instances have an identical code chunk which creates an unencrypted txt file with the results if dispensing cash (disp.txt in Europe and displog.txt in Taiwan)

3	An error notification in case of incorrect arguments	If any of the arguments are outside the pre-set range, an error message will be displayed: Error! Banknotes Count should be from 1 to 60 Error! Cassette number should be from 1 to 15 Error! Cassettes count should be from 1 to 15 Error! Dispenses Count should be from 1 to 500	If any of the arguments are outside the pre-set range, an error message will be displayed: Invalid parameter: Cassette slot number. Must be a digit from 1 to 9 Invalid parameter: Banknotes Count. Must be a digit from 1 to 60	Similar error messages connected with Cassette Number and Banknotes Count.

Table 1. Comparison of malicious programs used in Europe and Taiwan

The error message:

Europe: WFSOpen failed with error: WFS_ERR_INTERNAL_ERROR

Taiwan: CscCngOpen/CscCdmOpen failed with error: System Failure

Thus, the error message does not disclose the real cause of the failure to run the software, and only the software author is aware of this (see line 1 in Table 1).

Both versions contain an identical code chunk that creates an unencrypted txt file with results of cash withdrawals (disp.txt in Europe and displog.txt in Taiwan) — line 2 in Table 1.

Both ATMSpitter versions have no user interface and are controlled through the command line. The arguments are represented as transferred values: how many banknotes should be dispensed and from which ATM cassette. If a wrong number of arguments is given, ATMSpitter displays an error and required syntax message (see line 3 in Table 1).

At the same time, both versions use similar parameters for Cassette Number and Banknotes Count.

Payment gateways as the target

Attacks on payment gateways are rare but still occur every year. The Anunak group was the first to carry out this type of attacks, followed by independent hackers as well as the Cobalt group. So far, we are only aware of such attacks in Russia but, as practice shows, fraudulent schemes and attacks once tested in Russia are later "exported" for application in other countries. Not only banks become the targets but also companies that control payment terminals.

The attacking strategies only differ at the end stage:

- After gaining remote access to a bank's network, attackers look for payment gateways.
- They search for scripts and log files in the gateways to understand the standard format of message transfer used to perform transactions, and later create fraudulent messages.
- They run SOCKS proxy on local hosts to connect to payment gateways or use other remote access facilities.
- They code and launch a script in the local network and it automatically generates thousands of transactions with small amounts to be transferred to the attackers' cards and mobile phone accounts.
- Another script transfers cash from mobile phone accounts to bank cards, which is then followed by a standard money laundering procedure.

Cash withdrawal is the most challenging stage of this procedure. But as opposed to ATM attacks, the losses caused by one such attack is much more than $1-4 million USD.

This scheme has an advantage — many small transactions are carried out daily through such gateways, which is why the fraudulent transactions go undetected in the total flow. It complicates the identification of receivers' accounts, and makes it impossible to block the withdrawals in a timely manner.

SWIFT and AWS CBR as the target

SWIFT is a system allowing financial and non-financial institutions to send and receive information about financial transactions with 'financial messages'. The Russian analogue is AWS CBRC (Automated Workstation of the Central Bank of Russia's Customers). The underlying logic behind both systems is sending messages, which can be incoming and outgoing. Attackers have realized that they only need to manipulate these messages to steal money. This was later successfully carried out in attacks on banks:

- May 2016, attack on a bank in Hong Kong
- June 2016, attack on SWIFT workstation in Ukraine. 10 mln USD was stolen. Information about the attack became known to the media.
- November 2016, attack on AWS CBR.
- December 2016, attack on SWIFT workstation in Turkey. Information about the attack became known to the media. As a result, 4 mln USD was stolen.
- January 2017, attack on a bank in Latin America.

The attack scheme is simple:

- Detecting servers in a target bank with SWIFT or AWS CBR workstation
- Tracking outgoing messages.
- Substitution of payment details in outgoing messages.
- Transactions are confirmed by incoming messages, therefore they also need to be intercepted to have the fraudulent details substituted with the original ones that have been indicated by the system operator.

It is almost impossible to pull off such a scheme manually and special software must be used to perform this automatically.

Here are some examples of tools used for attacking the banks in Hong Kong and Russia.

A toolkit for AWS CBRC comprises the following:

Main module — runs other modules with parameters indicated in the main configuration file

AutoReplacer (XmlBin) — substitutes payment details in outgoing financial messages. The results are logged to Xml-Resultfile. The SUM field is not changed to prevent detection.

Hiding (EdBin) — verifies incoming / confirming messages. It verifies the PayeePersonalAcc. field and compares it with HackAcc in the Xml-Resultfile file. If the values match, the hidden module restores the initial PayeePersonalAcc. field.

The toolkit used in Hong Kong has not been recovered in full. One of its components performed the following activity:

- Searching outgoing message files in the directory D:\WIN32APP\SWIFT\ALLIANCE\SERVER\Batch\Outgoing\HK\HKAcksBak\
- If the file exceeds 102400 bites, it adds «Too big file : > 102400\r\n» to the file C:\\Temp\\Msg\\log.txt; otherwise it will open it in the reading mode to search for the sublines OTTC605384, OTTC605385, OTTC601386, OTTC601387, OTTC605381, OTTC605382.
- OTTC stands for «Outward Telegraphic Transfer Comm & Charges».
- If the file does contain this subline, it records the line 'Found file: %s with required token: subline>\r\n» into the log C:\\Temp\\Msg\\log.txt and copies the file into the directory C:\\Temp\\Msg\\
- It switches to the standby mode for 2.5 secs and then repeats the process of searching for the subline.

Card processing

Card processing has become the key target of hackers this year as this method has enabled criminals to steal large amounts easily and safely. The technique was first tested in Russia and used further in the countries of the former Soviet Union and USA by all major non-state sponsored cyber-criminal groups multiple times. Gaining access to card processing does not differ from gaining access to any other financial system in a bank in any real sense.

The scheme is extremely simple:

- After taking control over a bank network, the attackers checked if they could connect to the card processing system.
- They opened or bought legally available cards of the bank whose IT system they had hacked. They typically used around 30 cards per attack.
- Money mules – criminals who withdraw money from ATMs – with previously activated cards went abroad and waited for the operation to begin.
- After getting into the card processing system, the attackers removed or increased cash withdrawal limits for the cards held by the mules.
- They removed overdraft limits, which made it possible to go overdrawn even with debit cards.
- Using these cards, the mules withdrew cash from ATMs, one by one. The average loss caused by one attack was about $500 000 USD.

There are many advantages that have lead to the popularity of this scheme, including:

- Card processing systems are not as well protected as SWIFT, which is why attackers quite easily changed the limits while staying undetected. That said, the attack can be performed without any special programs, such as, for example, those used by Lazarus or MoneyTaker for attacks on SWIFT workstation.
- No need for complex cash-out and money laundering schemes. Attackers withdraw

pure cash at once.

- It is enough to obtain or buy some bankcards to withdraw cash.
- Withdrawing money in another country helped hackers to gain time since the bank's security service could not promptly contact the local police, obtain video records from surveillance cameras, nor arrest the perpetrators. As a comparison, when theft via logical attacks occurred in the same country where the attacked bank was located, money mules would often be arrested.

Concealing attack traces

After successful attacks on banks, the attackers have always tried to conceal any traces of their presence on corporate networks to complicate incident response and investigation as well as stay unnoticed as long as possible in future attacks. To cover up their tracks after thefts, they would use tools like SDelete, MBRKiller, and self-coded utility applications for removing data. It was obvious that using ransomware to conceal attack traces was only a matter of time.

Early in 2017, we detected the first cases of ransomware being used for concealing the traces of a bank theft. While attacking a bank with a view to rob it, hackers took control over its domain. After the robbery, they ran PetrWrap, a modified version of Petya – PetrWrap ransomware, on behalf of the domain administrator on all computers of the network.

PetrWrap is coded in C, and compiled in MS Visual Studio. It contains the Petya ransomware (version 3) used to infect target computers. Moreover, PetrWrap contains its own cryptographic algorithms, and changes the code of Petya during the operation, which allows the criminals to conceal the use of Petya in the process of infection.

Upon the completion of the encryption process, a message is displayed to say that encryption has been performed with a requirement to contact the criminal via email razlokyou@tutanota.com for further instructions. It is worth noting that the incident only involved the encryption of MFT (NTFS file table), which made it possible to recover the data. However, most computers of the bank's network were disabled, which complicated incident response to a certain extent.

Attacks on Bank Clients

PC Trojans

In Russia

Since mid-2012 we have been noting a continuous reduction in damage from banking Trojans used to target personal computers in Russia. During the last year no new banking Trojans targeting users in Russia were detected.

Since 2012 the owners of banking botnets have started to move away from using exploits and to use Spam for distribution. It is worth noting that during the previous period this was the main method for delivering banking Trojans in Russia. Now we can see that the situation is changing once again and the criminals are beginning to use Driveby methods again - i.e. hacking legitimate sites and redirecting users to servers with exploits.

Attacks on Companies

The number of groups and consequently the number of attacks on companies in Russia with the purpose of stealing funds has decreased by almost half compared to the previous period. This year attackers managed to steal only USD 10 mln., whereas last year this amount was USD 16 mln. However, the figures decreased only by 35% because the average amount of loss increased to USD 20k. It shows that the attackers have started to choose their victims more carefully.

There are only 3 criminal groups left in Russia who steal money from companies: Ranbyus, RTM, and Buhtrap2. It is worth noting that Buhtrap botnet is now used by another group and currently they are the most active. After control was delegated to other users (and the software sold off) a while later they changed their tactics and now the main distribution vector is not Spam, but hacked legitimate sites, including those in the financial sector. It is worthy of note that the financial sites hacked were the same those 5 years ago, when Carberp was distributed.

In Russia, owners of banking botnets targeting companies have completely moved away from the man-in-the-browser attacks and started to use either remote control or automatic transfers via 1C accounting systems. At the same time all the three groups have started to use a module for auto uploading via 1C (the Russian accounting software).

Attacks on Users

Only one criminal group – Proxy – continues attacking individuals with the use of banking Trojans targeting personal computers. This year they managed to steal USD 262k., compared to USD 106k last year. This loss is not considerable, but it has increased due to the fact that they were inactive for the most part of the last year.

This January Proxy started to attack customers of Kazakhstani banks alongside their attacks on clients of Russian banks. In April 2017 they completely stopped attacks within the Russian Federation.

On the Global Stage

The situation involving banking Trojans on the global state has undergone significant changes.

Corebot and Vawtrak (aka Neverquest), developed by Russian-speaking authors and used in global attacks on companies worldwide have left the market. The developer of Corebot simply stopped supporting it and as for Vawtrak, its author was arrested, which resulted in this activity being stopped.

But they have been replaced by new Trojans: Trickbot, Sphinx 2, TinyNuke, Portal, GNAEUS, and Plan2016. However, alongside with the new Trojans, some older ones have remained active: Dridex, Qadars, Gootkit, Panda, Jupiter, GozNym, Quakbot, Ramnit, Retefe, Atmos, Tinba, KINS, Citadel, Zeus, Sphinx, Shifu.

Out of 22 malicious programs designed for committing theft of funds, 20 (91%) were created and are controlled by Russian speakers.

This year Trickbot Trojan, described as the successor of Dyre, became the most remarkable player. It is worth noting that the Dyre botnet owners were arrested at the end of 2015.

Some attackers are moving away from using web injects in favour of traffic redirection to their servers in order to intercept and manipulate traffic data. These kinds of trojans include Trickbot, GNAEUS, Portal, Quakbot, Dridex, and Retefe. It is a very old method, but for some time it has not been popular among attackers. Now it is regaining its popularity.

Outside of Russia, Spam remains the main method of distribution in other regions globally. For some time GozNym, Gootkit, Vawtrak and Ramnit were all distributed with the use of Driveby methods, all the rest were spread via e-mail.

TinyNuke is one of most vivid examples of a new trend: malicious code developers have started to publish the source codes of their programs online more actively and on their own initiative. The author of TinyNuke has made the source code of this banking Trojan and its control system publicly available.

The beginning of this year saw the first

	Trickbot New	Sphinx 2 (zbot.ACB) New	TinyNuke New	Portal New	GNAEUS New	Plan2016 New	Dridex	Qadars	Gootkit	Panda	Jupiter (Midas, Bolek)	GozNym	Quakbot (Qbot)	Ramnit	Retefe (ProxyAdder)	Atmos	Tinba	KINS	Citadel	Zeus	Sphinx	Shifu	Total
Australia	●	●					●	●						●	●	●	●	●		●	●		11
Austria								●							●		●				●		4
Belgium								●															1
Bulgaria																				●			1
Brazil									●												●		2
United Kingdom	●						●	●	●	●		●		●	●	●	●	●		●	●	●	14
Germany	●							●	●	●		●		●		●	●	●	●	●	●		12
Spain							●	●	●							●	●	●		●			7
Italy								●	●	●						●	●	●		●		●	8
Kazakhstan															●								1
Canada	●	●						●	●	●		●	●	●		●	●	●	●	●	●		14
Colombia																					●		1
Netherlands									●	●			●			●	●						5
New Zealand	●																●				●		3
UAE																				●	●		2
Portugal																●							1
Poland							●	●		●	●	●							●				6
Russia															●					●			2
Romania							●																1
USA		●	●		●	●	●	●	●	●		●	●	●		●	●	●	●				15
Turkey																				●			1
Ukraine											●												1
France		●	●				●		●							●		●		●			7
Switzerland									●						●								2
Sweden									●														1
Japan																	●				●	●	3

cases of theft from bank accounts in Germany, where hackers bypassed two-factor authentication by intercepting an SMS code through an attack on CCS7 (SS7).

Android Trojans

As anticipated, the market for Android banking Trojans has proved to be the most dynamic and has the highest rates of growth. In Russia, the amount of loss caused by Android banking Trojans has gone up by 136% and exceeded the loss caused by Trojans for personal computers by 30%.

We are still not observing attacks on companies, but as attackers have all tools required — we expect attacks to happen in the near future.

Attackers managed to increase the average amount of loss caused by one attack and this is all due to the fact that new groups are more focused on obtaining bankcard data, and not on SMS banking as was previously the case.

Text messages still remain the main distribution channel. And currently are used in the following way

1. Bulk text messaging with a malicious link
2. They scan message boards and send text messages with malicious links to specified phone numbers making it look as a reply to an ad.
3. The android malware sends out text messages with a malicious link to all address book contact numbers.

A less popular channel is the distribution of infected applications in unofficial repositories. As a rule, this method of distribution implies the involvement of several people who are usually found on specialized forums.

Contextual advertising in search systems is less popular but it is the most effective targeted method widely in use.

The six methods of theft which we described in our previous report have remained the same with Apple Pay and other mobile payments services becoming a new vector:

- Stealing through SMS-banking
- Transfers from card to card
- Transfers via online-banking
- Interception of access to mobile banking.
- Fake mobile banking
- Purchases via Apple Pay

However, it is worth mentioning a reduction in the activity, particularly related to SMS banking. This has mainly been caused by arrests carried out by law enforcement agencies here in Russia. The organizers of the most active botnets using a theft scheme using SMS banking have been arrested - these are two groups using Cron Trojan and a group using Opfake Trojan.

We are still tracking SMS banking theft only in Russia. However, all the other schemes remain relevant.

Every month we have noted the appearance of a new banking Trojan for Android. During the last year the following malware has appeared: Limebot (and later its new version - Lipton), Easy, UfoBot, Rello, Loki, Red Alert, Vasya Bot, ExoBot (and later its new version - ExoBot 2.0), Instant VBV Grabber, Alien-bot, maza-in, and Catelites Android Bot. All the Android banking Trojans have been created by Russian-speaking hackers.

Late last year the authors of a Trojan called Catelites Android Bot announced that they had made a universal web-fake for 2,249 bank applications from Google Play. According to the author, 2249 applications were taken from Google Play with the use of parsing based on key words 'bank' and 'money'. The Trojan searches on the victim's telephone for one of these applications and displays a universal window where it places an icon and the bank name, taken from Google Play.

The publication of a banking Trojan called Maza-in by its developer was an major event of this year. Right afterwards numerous installations of this malware program with slight modifications began to appear.

Automatic theft using Android Trojans has achieved a huge growth in capacity and usage. Attackers use two scenarios for automatic thefts:

Total automation: After getting into the system the Trojan checks the state of a bank account and automatically makes moneytransfers, confirming them using the intercepted SMS codes. So far we have recorded fully automatic theft only on SMS banking.

"One-click" attack. The trojan also recognizes balances and collects bankcard data on a preliminary basis or login and password for online banking and automatically verifies their accuracy. Then the attackers select devices from which the transfer will be made, press a button in the botnet control system and the malware makes a transfer in accordance

with the scenario from card to card, or an online banking transfer and automatically confirms the transactions by SMS code, which it intercepts from the infected device.

Apple Pay / Samsung Pay

Samsung Pay and Apply Pay mobile payments were introduced in early 2017 and hackers were quick to take notice. Theft schemes against these systems are as follows:

1. Fraudsters infect an Android device and receive information about the bank card or login/password for online banking, as well as information about the current balance.
2. If the user's balance is of interest, fraudsters link the victim's bank account to Apple Pay on their iPhones. To do this, they need card data or login/password, obtained during the first step. They also need SMS confirmations, which are successfully intercepted by Android Trojan.
3. Apple Pay provides two main advantages: there is no need to carry the card around physically, and there are no limits for transactions. It is considered that if the user confirms the payment by his/her fingerprint during the payment process, the transaction must be executed, that is why it is very hard to stop such fraud.
4. The payment terminal may ask for a PIN-code for purchases involving large sums. However, some banks have a list of authorized venues where PIN-codes are not requested even for big-budget purchases. That is why fraudsters can make purchases just in these specific locations.

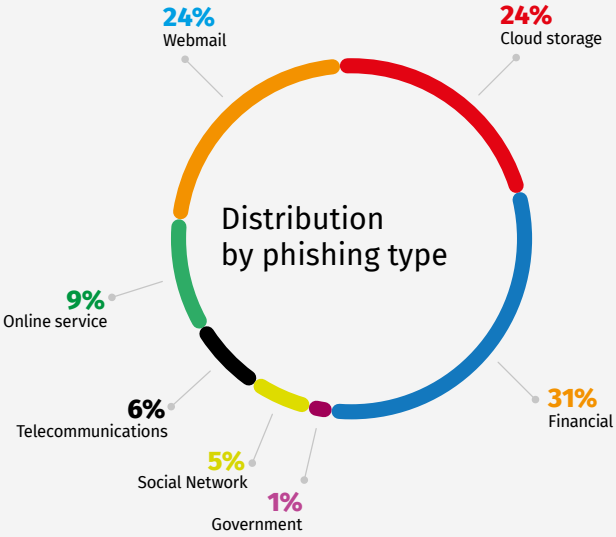
The Android banking Trojans landscape for the period described is as follows:

Trojans, attacking SMS banking (only in Russia)	Trojans using Web-fakes in Russia	Trojans using Web-fakes globally
Agent.SX	Limebot	Catelites Android Bot
Fakeinst.FB	Tiny.z	Maza-in
Opfake.A	Honli	Alien-bot
Flexnet	Asucub	Instant VBV Grabber
Granzy	Cron	Reich
Cron	Agent.BID	Marcher
Agent.BID	ApiMaps	Easy
		UfoBot
		Rello
		Loki
		Red Alert
		Vasya Bot
		ExoBot
		Skunk
		Abrvall
		Xbot
		GMbot
		Spy.agent.SI

Phishing

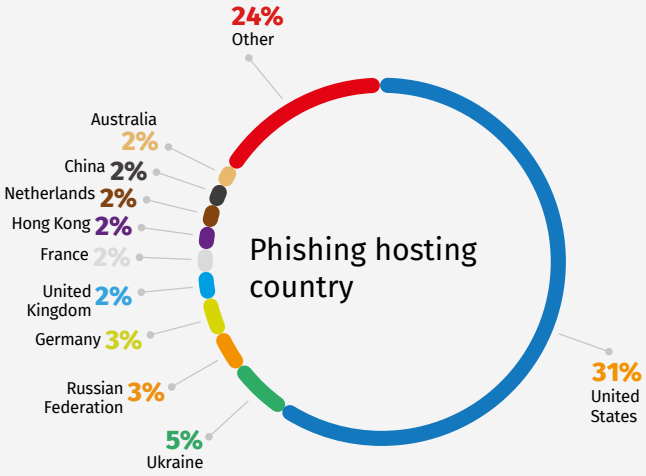
Group-IB specialists discovered and analyzed 1.4 mln unique phishing links on 657,000 domains. 5% of these links were using HTTPS.

Traditionally, financial institutions are the main target for fraudsters. Almost 80% of all phishing resources fall into the following three categories: financial (31%), cloud storage (24%) and mail services (24%).



The majority of phishing resources were hosted on hacked legitimate sites. The attackers were mainly exploiting well-known vulnerabilities in Joomla and WordPress content management systems. In Russia, the situation is slightly different. Hacked websites are used as a source of victims. When potential victims visited hacked websites, under certain circumstances they were re-directed to a phishing site, which is hosted on servers rented by the attacker or to free hosting services. 60% of all phishing sites were hosted in the USA, Ukraine ranks second (5%), and Russia and Germany share the third and fourth positions (3% each).

Phishing for banks and payment systems in Russia is automated and conducted in real time, which allows bypassing SMS confirmations for debiting funds. Every day over 900 bank clients become victims of financial phishing in Russia,

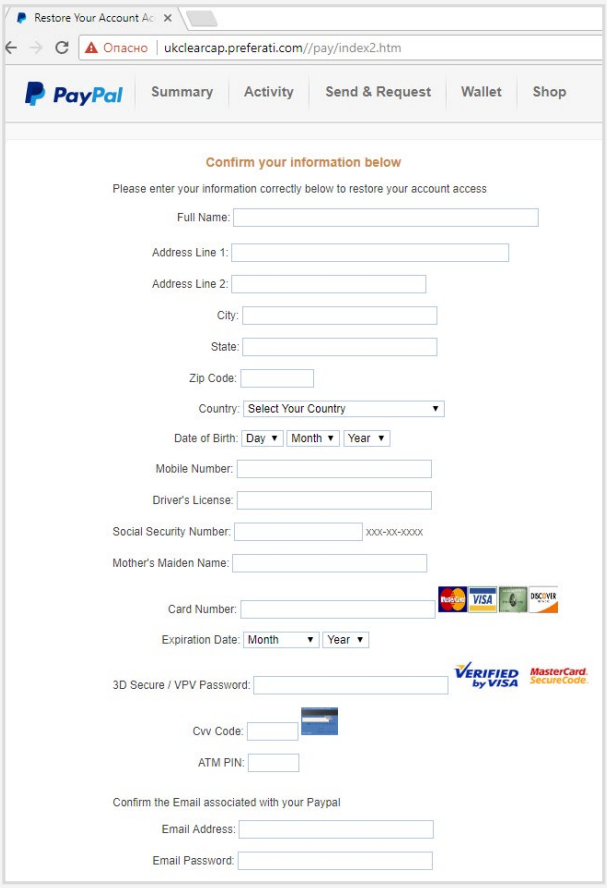


which is three times the number of malware victims. But the amount of loss caused by phishing is dozens of time less than that caused by malware. Last year we warned that phishing automation and the simplicity of its use would become the main cause of an increase in phishing attacks and losses incurred. In total, there are 15 groups in Russia that use phishing for financial institutions. The amount of damage is always quite small, but the number of victims that they daily lure to their sites amounts to thousands. Approximately 10-15% of visitors of financial phishing sites enter their data. Over the course of 12 months, attackers managed to steal USD 3.9 mln.

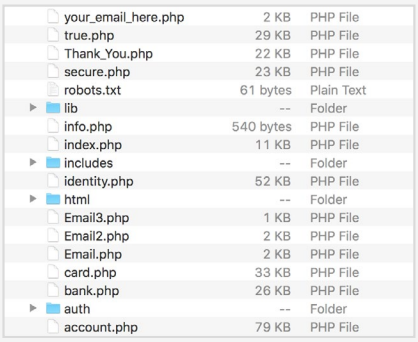
In other regions, we observe many cases of off-line phishing. This means that data collection is performed on a phishing site, it is stored locally or sent to a fraudster who later verifies its correctness and tries to use them some time later.

Hackers, who engage in this on a massive scale employ Phishing Kits, which are ready-to-use phishing websites with configuration files that determine the logic of the phishing site operation and where the compromised data should be sent. We have collected more than 12,000 unique Phishing Kits and analyzed their configuration files. In the overwhelming majority of cases the compromised data was sent to an email address. In 80% of cases

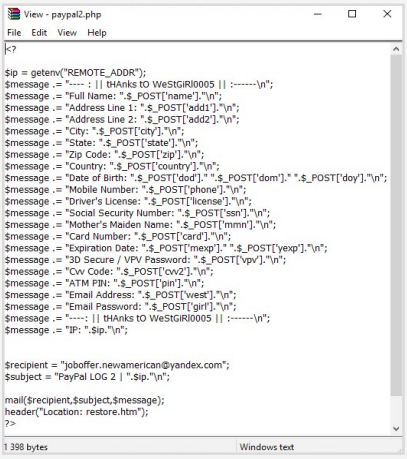
Phishing page

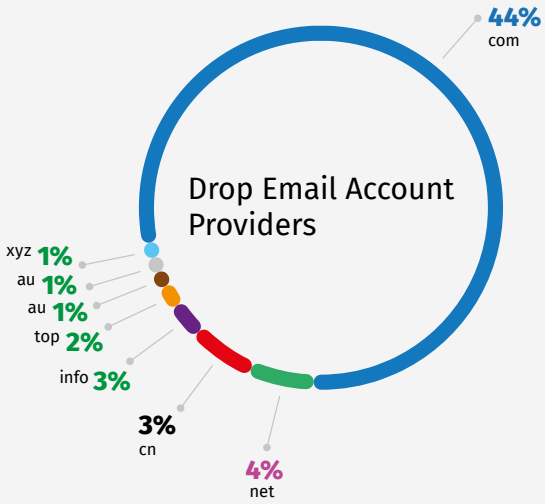


Phishing kit



Configuration file





phishers register email to collect compromised data in Gmail, while Yandex and Mail.ru account for only 6%.

Teamwork

Very often Russian-speaking cyber-criminals create and use partner programs, for example, for spreading malware, spamming, phone fraud etc. Team efforts towards a common goal enable organizers of criminal business to achieve it faster on a much wider scale, but they will have to pay a small amount of profit to their partners.

The situation involving phishing is similar. At the end of last year one of the criminals created 26 phishing sites imitating social networks, gaming resources, mail services and e-wallets. In addition, he created a site where he published links to his phishing web-resources and offered anyone who felt like attacking somebody to use these phishing resources. It meant that any attacker who could

not create a phishing site of their own, could use ready-made phishing resources. In return for such free use, the collected data was to all VIP users. VIP users got access not only to other people's data, but also received guarantees that any data they collected by phishing would not be made available to other users. VIP access for 30 days cost USD 3 only.

In this way the participants of this scheme compromised more than 90,000 logins and passwords in a matter of days.

This is an illustrative example of effective teamwork that enables people without relevant experience carry out simple attacks.

POS Trojans

When analyzing data on card-shops, one can draw the firm conclusion that the most in-demand commodity is not complete card details, which can be obtained with the use of Trojans, phishing, hacking of e-commerce sites, but data from magnetic stripes. POS Trojans are the main source of this data.

Attackers are still divided into two categories:

1. Those attacking a broad audience with a small amount of focus but on a massive scale, attempting to look for an opportunity to install a POS-Trojan.
2. Those purposefully targeting POS terminal vendors or large network organizations, to access their networks and in turn gain immediate infections on a large number of devices.

Just like with banking Trojans, during the reporting period new POS-Trojans were identified: LockPoS, MajikPOS, FlokiBot, ScanPOS, FastPOS.

These new Trojans have not introduced anything special. They keep functioning as RAM-scrapers and by analyzing core memory, they extract from it bankcard data, both from the magnetic stripe and the chip.

But in addition to new Trojans, the old ones are still active (PoSeidon, AbaddonPOS, Alina, etc.) having acquired a reputation as fairly efficient tools for bankcard data collection.

The attackers' tactics are usually as follows:

1. By using network scanners, a search for open ports conducted, using which it is possible to gain access by remote control to a device (with RDP and VNC among them).
2. Using various bruters and small dictionaries, password mining to detected devices is initiated. Dictionaries contain users' typical names and passwords for POS-terminals, for example,

various combinations of words POS, cash, payment etc.

3. If conducted correctly, the fraudster verifies what he/she has gained access to and whether this device is of interest to him/her. For example, if it is a restaurant's network.
4. Tools for password recovery Mimikatz, Fgdump, VNCPassView are uploaded to the device.
5. Backdoors which are usually public RAT (Remcos, Netwire, etc.) are installed on some computers and terminals, as well as legal remote access facilities such as Ammyy Admin, TeamViewer.
6. Using remote access, a POS-Trojan is installed manually.

Groups engaged in targeted attacks, do it in a much more challenging manner. At the same time, the losses caused and their profit are much higher.

	Company affected	Description
July 2017	**B&B Theatres**	A company that owns and manages the largest theatrical network in America was hacked in October 2015 and the card data kept leaking to attackers until April, 2017.
June 2017	**The Buckle Inc.**	The company operates more than 450 shops. It was hacked in October 2016 and card data kept attackers until April, 2017.
May 2017	**Kmart**	The US largest retailer was compromised once again. It was already hacked in 2014. In both cases POS terminals were the target.
May 2017	**Sabre Corp.**	Access was gained to the SynXis Central Reservations system, used by many hotels and containing payment details.
April 2017	**Shoney's**	A company that owns more than 150 restaurants. It was hacked in December 2016 and data kept leaking to attackers until March, 2017.
March 2017	**24×7 Hospitality Technology**	POS-vendor, processing transactions with credit and debit cards for thousands of hotels and restaurants. Card data was collected with the use of a Trojan called PoSeidon.
March 2017	**Verifone**	Verifone is the largest manufacturer of payment terminals. It was hacked in the middle of 2016 supposedly with the use of a MalumPOS Trojan.
February 2017	**Arby's**	A company that owns more than 1000 restaurants, part of which were infected. Card data kept leaking to attackers from October 2006 through January 2017.
December 2016	**InterContinental Hotels Group**	The parent company for more than 5000 hotels globally, including Holiday Inn. Data kept leaking to attackers from September 2016 through December 2016, from more than 1000 points.
August 2016	**Eddie Bauer**	A chain of more than 350 shops was hacked. In all the shops a Trojan was installed on tills and card data was leaked to attackers from January through July 2016.
August 2016	**Oracle**	MICROS – an Oracle business unit, sells POS-systems, which are used in more than 330,000 places.
July 2016	**Kimpton Hotels**	A chain of 62 boutique hotels was hacked and during the period from February through July 2016 card data was leaked to the attackers.

Attacks on Cryptocurrency Services

Cryptocurrencies and related services constitute a highly dynamic and profitable market. With such development, growth rate and money flow, security issues are often left by the wayside by startups. Hackers, knowing that, successfully take advantage of them

The more successful the fintech startup, the larger the ICO and the more attractive it is for attacks.

The number of threats to cryptocurrency and blockchain projects tracked by Group-IB's Threat Intelligence system has risen along with the Bitcoin exchange rate. Source code vulnerabilities in smart contracts have already been successfully exploited. Specialists have tracked incidents of keys to wallets on cryptocurrency trading platforms accessed by hackers. Multiple incidents related to leaks of user databases, and domain name hijacking have been detected. The owners of botnets monitor the infected devices for connections to web and mobile applications of wallets, exchanges, and funds. Creation and promotion of phishing websites to leak account information is becoming commonplace.

According to Chainalysis, a New York-based firm that analyzes transactions and provides anti-money laundering software, around 10% of all the money invested in initial coin offerings (ICOs) this year using cryptocurrency Ethereum has fallen into the hands of thieves.

Phishing scams have helped push up criminal losses to about $225 million this year. More than 30,000 people have fallen prey to ethereum-related cyber crime, losing an average of $7,500 each this year.

A similar spike in hacking activity was observed by Group-IB during the early stages of online banking in the Russian Federation. This is easy to explain – hackers always follow the money.

Vulnerabilities in Source Code

Vulnerabilities in source code is a nightmare for service developers.

June 17 2016, probably the largest attack in the history of crypto attacks took place - due to a code error in a promising project called THE DAO. This caused the loss of more than 60 million USD.

The theft was committed due to the vulnerability called 'recursive invocation' — it allowed endless withdrawals of DAO funds and their transfer to a DAO subsidiary via a multiple division of DAO, collecting ETH again and again as part of one transaction.

However, the gap for creating a subsidiary DAO was exactly 27 days, and it was, therefore, impossible to withdraw the funds from the wallet during that time. The community started to look for ways "to restore justice" and eventually settled upon Hardfork Ethereum. Thus, all DAO tokens, irrespective of DAO area were then frozen and token holders could withdraw. Therefore, this attack was to some extent resolved.

On July 19, 2017 due to a vulnerability in the code of the smart-contract Multisig Parity wallet (1.5 and later), the hacker managed to withdraw ETH 153,000, i.e. around USD 30,000,000 at the time.

The developers detected the attack almost immediately. Almost immediately a group of enthusiasts, calling themselves The White Hat Group used the same exploit to save the users' money, by transferring it to a bug-proof wallet.

The Parity developers informed that there were 596 vulnerable wallets and the criminals mainly attacked three on them - the ICO wallets:

- Edgeless Casino
- Swarm City
- æternity blockchain

Almost 40% of the entire investment portfolio of the satoshi.fund cryptocurrency fund - more than $7 000 000 USD was withdrawn to the White Hat Group wallet. Later the White Hat Group returned all the funds.

Targeted Attacks

Secret keys used to confirm transactions are the most valuable asset for any cryptocurrency service. Compromising the key means losing control over the account and, as a result, over all the funds.

And the opportunity to obtain these keys does not differ much from getting control over a critical system inside a bank, and in some cases it is much simpler. The main problem here is getting access to the company's local network, for which exactly the same methods are used as for attacks on banks.

On August 2, 2016, the third most popular Hong Kong cryptocurrency exchange Bitfinex (ranked No 3 among the most popular cryptocurrency exchanges in the world) was compromised and lost almost 120,000 bitcoins (some 72 000 000 USD at the exchange rate at the time), which provoked a considerable fluctuation in the cryptocurrency exchange rate. The accounts of the exchange clients were protected by multi-signature technology - two out of three keys were kept by the exchange itself (one - in a cold storage), and the third one - in BitGo. The successful withdrawal of funds indicates that control was gained over over the Bitfinex corporate infrastructure.

On October 13, 2016, about 2300 bitcoins amounting to about USD 1,5 mln were transferred in several transactions from one of the bitcoin addresses of the Polish cryptocurrency exchange Bitcurex. On the same day the administration reported that there was a server problem, arising as a result of updating a bitcoin client. A week later the exchange team delivered another statement, which mentioned current work on updating the network and measures to improve security. On October 27, yet another statement from the administration appeared on the exchange website where it admitted having sustained a hacker attack and loss of some funds. On November 30 2016 the exchange recommenced its operations, but at the beginning of 2017 the site went offline again and there were no more announcements and explanations, the exchange simply stopped working.

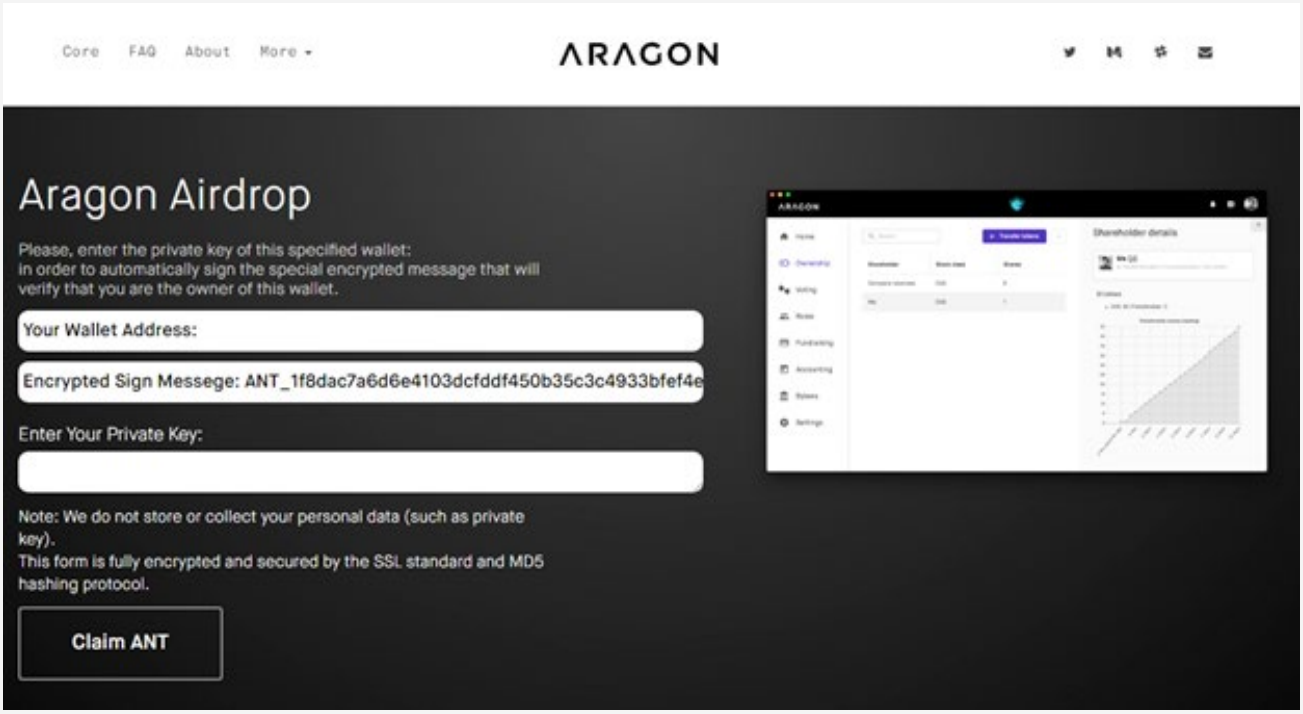
On July 16, 2017 the Israeli start-up CoinDash launched an ICO (Initial Coin Offering) procedure. Three minutes after the ICO, unknown criminals hacked the CoinDash site and substituted the address of the official Ethereum wallet by their own. During the first five minutes after the hack more than 6 000 000 USD was transferred to the hackers' wallet. The criminals have already received ETH 43.488, which at the exchange rate, which at that moment amounted to 8 300 000 USD.

On June 29, 2017 the South Korean cryptocurrency exchange Bithumb, which is the 4th largest in the world, announced it had been hacked. The attackers managed to compromise the computer of one of the exchange employees, after that they obtained access to information of around 31,800 users of the resource (around 3% of the entire customer database).

Domain hijacking

On October 12 2016 the administration of Blockchain.info, one of the most popular web-wallets on the Internet, warned about a DNS-hijacking attack: DNS data were changed: CloudFlare was substituted by a hosting-provider from Tulsa, USA. Website visitors ended up on completely different servers, where they were exposed to all kinds of attacks.

On June 30 2017, unknown criminals managed to gain control over the Classic Ether Wallet domain — the wallet for Ethereum Classic (ETC) cryptocurrency. After the malicious takeover of the domain, the hacker changed the website settings in such a way as to redirect users to his server. The malicious version of the website 'copied private keys, entered by users and sent them to hackers.' As a result, approximately USD 300,000 was stolen.



Phishing ICOs

This type of attack has become very popular among attackers due to its simplicity and efficiency.

The tactics of the attackers are as follows:

- They trace new projects launching an ICO
- They create a phishing page, its main distinctive feature is a request for a private key.
- All private keys are automatically connected to e-wallets of fraudsters and funds are automatically withdrawn to the accounts specified by fraudsters.

Tracing these wallets one can see that one group can earn up to USD 1.5 mln a month:

https://etherscan.io/address/0x68b0e0db7918c0211ea1fb78292a879839137dd0

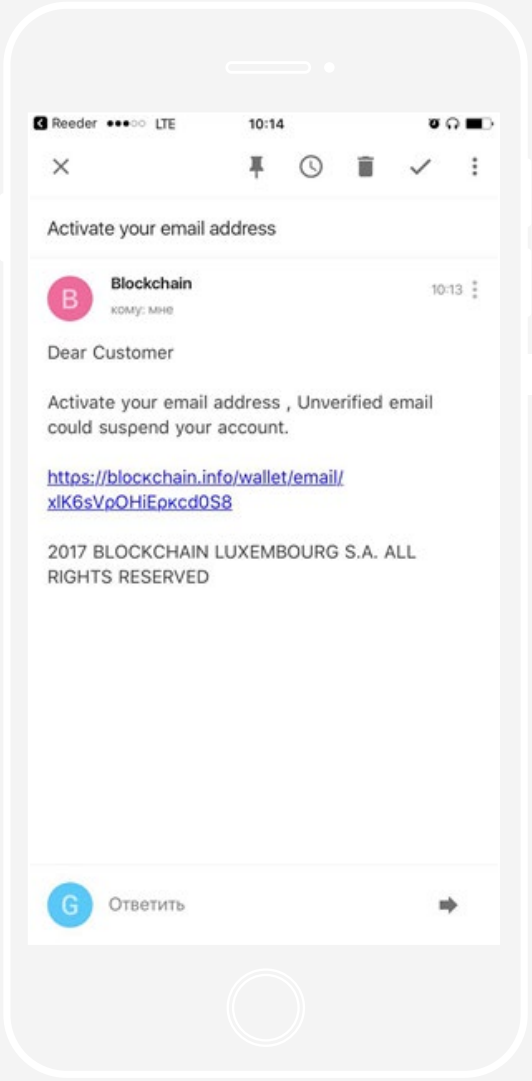
https://etherscan.io/address/0x0a5650aba6473c48898f3d9366b52c21a4eec37b

https://etherscan.io/address/0x1e80dad60d19fb8159af3f440a8ceaa0e5581847

https://etherscan.io/address/0x3681828DA105fC3C44E212f6c3Dc51a0a5A6F5C6

https://etherscan.io/address/0x4a0d27a1044dd871a93275de5109e5f5efc4d46e

https://etherscan.io/address/0x89C98CC6D9917B615257e5704e83906402f0f91f



Phishing

It is not necessary to create a phishing page for every single exchange to get access to a wallet. To recover access it may be enough to restore a password to an e-mail address or mobile telephone number.

To get access to e-mail boxes, phishing pages imitating popular mail service providers (Gmail, Yahoo, Outlook, etc) are used.

Use Restrictions

Group-IB hereby informs that:

- This report has been prepared by Group-IB specialists without funding from third parties.
- Assessment of the hi-tech crime market was made on the basis of proprietary internal methods developed by Group-IB.
- Technical details of cyber threats are described in this report are published only for use by information security staff with a view to prevent similar incidents in the future and to minimize the possible damage.
- Technical details of threats and attacks published in this report do not in any way support or provide advocacy of fraud and/or other illegal activities in hi-tech or other areas.
- All references to companies and trade marks in this report are made on the basis of approvals from such companies and/or on the basis of information already published in mass media.
- Information published in this report can be used by interested parties at their own discretion as long as the reference to Group-IB is given.

Company

Group-IB is one of the global leaders in providing high fidelity Threat Intelligence and best in class anti-fraud solutions.

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

EUROPOL INTERPOL

Official EUROPOL and INTERPOL partner

OSCE

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

WORLD ECONOMIC FORUM

Member of the World Economic Forum working group on cybersecurity

IDC Gartner Forrester

Group-IB Threat Intelligence has been recognized by top industry researcher reports

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 and HoneyNet

Botnet analysis

TDS Sensors

Hacker forums

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 manufacturers

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

Group-IB — one of the global leaders in providing high-fidelity Threat Intelligence and anti-fraud solutions

www.group-ib.com
blog.group-ib.com
info@group-ib.com
+7 495 984 33 64
twitter.com/groupib_gib
linkedin.com/organization/1382013