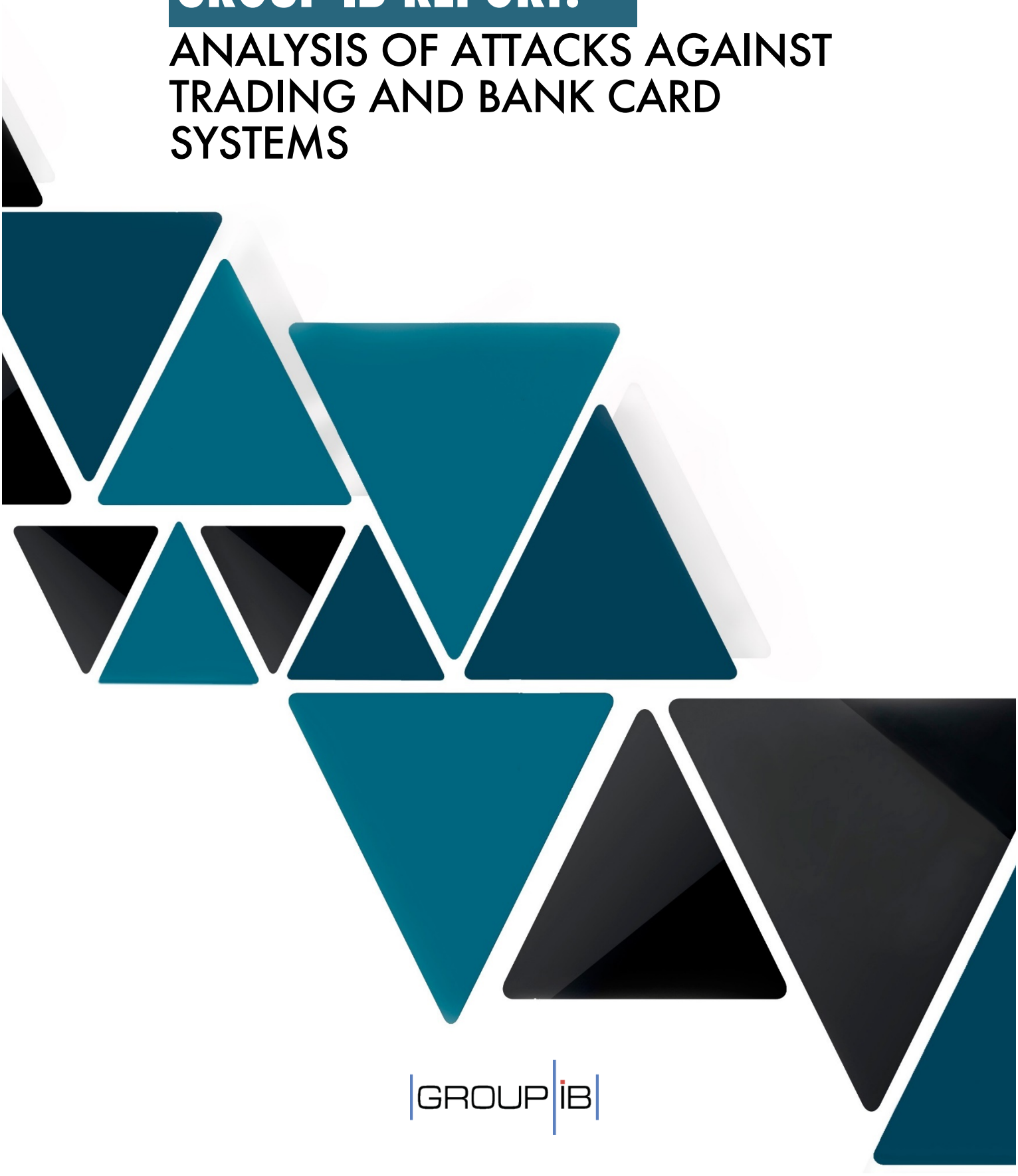
GROUP-IB REPORT:

ANALYSIS OF ATTACKS AGAINST TRADING AND BANK CARD SYSTEMS



GROUP IB

Executive summary

In February 2015 the first major successful attack on a Russian trading system took place, when hackers gained unsanctioned access to trading system terminals using a Trojan resulting in trades of more than $400 million.

The criminals made purchases and sales of US dollars in the Dollar/Ruble exchange program on behalf of a bank using malware. The attack itself lasted only 14 minutes, however, it managed to cause a high volatility in the exchange rate of between 55/62 (Buy/Sell) rubles per 1 dollar instead of the 60-62 stable range.

> Losses to financial institution were estimated in the millions.

To conduct the attack criminals used the Corkow malware, also known as Metel, containing specific modules designed to conduct thefts from trading systems, such as QUIK operated by ARQA Technologies and TRANSAQ from ZAO "Screen market systems". Corkow provided remote access to the ITS-Broker system terminal by «Platforma soft» Ltd., which enabled the fraud to be committed.

> This incident is believed to be a "test" to assess its ability to affect the market and earn money.

In August 2015 a new incident related to the Corkow (Metel) Trojan was detected. An attack on a bank card systems, which included about 250 banks which used the bank card system to service cash withdrawals from Visa and MasterCard cards under a special tariff. This attack resulted in the hundreds of millions of rubles being stolen via ATMs of the systems members.

Group-IB specialists use their unique Bot-Trek TDS threat detection system to identify Corkow and other threats to the corporate networks. According to our statistics, as of the beginning of 2015 this botnet encompassed over 250 000 infected devices worldwide including infecting more than 100 financial institutions with 80% of them from the top 20 list. The botnet is growing daily.

It is worth noting that the majority of computers that are infected have popular antivirus software

installed and the companies' internal networks are also highly protected.

Judging by the method of infecting devices and corporate networks, Group-IB can conclude that all infections were conducted on a random "non-targeted" basis. However, as our previous investigations on Anunak group displayed, access to any computer on a corporate network gives access to even the most highly protected banking systems. The attacks against the trading system and bank card system were conducted under the same scenario and thus we can forecast similar attacks against financial institutions in Russia, EU, the Middle East, Asia and the USA in the future.

Corkow is the second known Trojan to be used to collect information about trading systems. The interest among hackers in targeting trading systems is expected to grow.

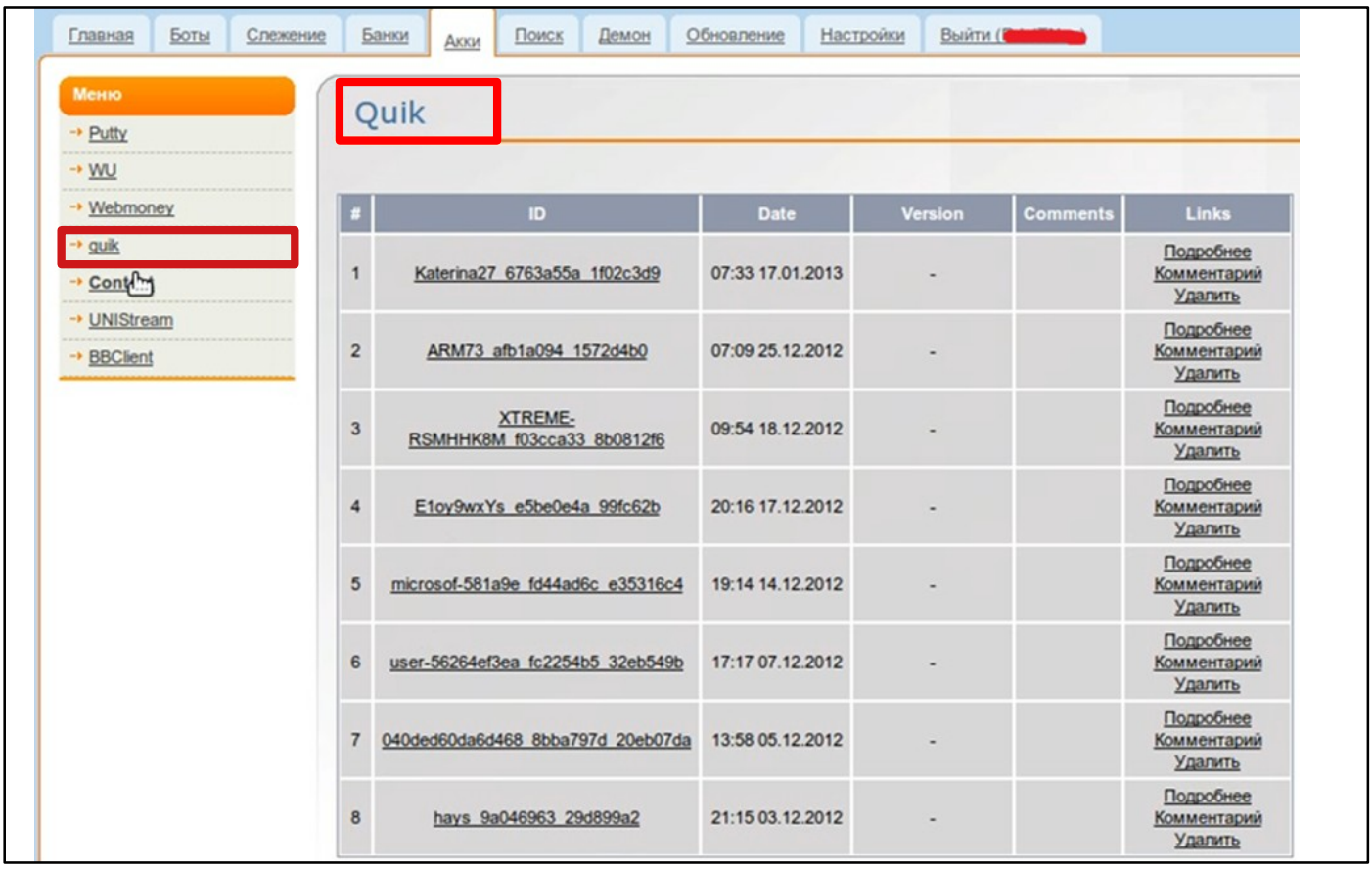
We would like to express our gratitude to Fox-IT, ESET and AVG companies for their support in performing this research.

Key findings

- In February 2015 the first successful attack on a trading system took place. The losses to this financial institution were estimated in the millions.
- It was a test attack aimed at demonstrating the malwares capabilities. In fact, many traders were those who used the exchange volatility to make good money, while hackers purportedly received nothing.
- The first targeted attack on a bank card system took place causing losses in the hundreds of millions of rubles.
- Russian-speaking hackers are believed to be responsible for these attacks and used the Corkow Trojan. No secret services involvement has been detected.
- Various hacker groups demonstrate increased interest towards trading and brokerage systems and their clients, which is evidenced by the specific modifications in malware they use.
- Hackers target primarily companies in Russia and CIS countries, though it is noticed that the amount of attacks targeting the USA has increased 5 times since 2011.
- Antiviruses are not capable of effectively preventing these threats. The majority of computers infected by this malware have antivirus installed and active. The Trojan can stay undetected in the system for more than 6 months.

Background

One of the first botnets specializing in targeting the trading software called Quik was "Ranbyus", created in 2012. Below are the examples of this botnet control panel interfaces. Each of them had separate sections designed to analyze computers with Quik installed.



Picture 1. Ranbyus control panel with a section for Quik users as of January 2013.

Picture 2. Ranbyus control panel with a section for Quik users as of May 2013.

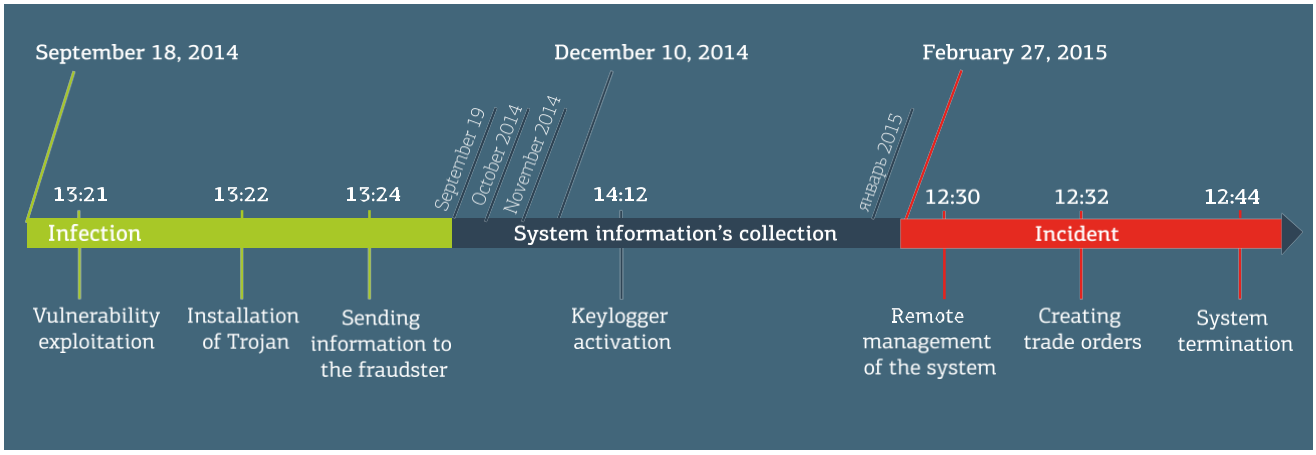
In 2014 Corkow had a QUIK v.1.0. module for collecting data from the Quik trading software developed by ARQA Technologies. In 2015 Corkow's developers updated the QUIK module to v.1.1. and released another module TRZQ v.1.0. to copy information from the trading system's application TRQNSAQ developed by ZAO «Screen market systems».

The re-development of the old QUIK module and development of the new TRANSAQ module show the Corkow group's continued interest in targeting trading systems.

Chronology of the Corkow attack against the trading system

The attack itself lasted only 14 minutes, during which all losses were sustained, however, the preparations for this intrusion took a much longer time.

Hackers gained access to a computer in the trading system in September 2014. From this time the Trojan was functional and constantly updated itself to avoid detection by antivirus software installed at the bank which was in functioning order. As of the Group-IB investigation of this malware program in March 2015, Corkow v.7.118.1.1 had not been detected by a single antivirus program.



Picture 3. Chronology of the Corkow attack on the trading system

Starting in December 2014, the criminal group began running keyloggers in the infected system.

On the 27th of February, 2015 Corkow provided remote access to the trading system which enabled the hackers to launch programs and enter data at the same time as the system operator did.

As a result of this unsanctioned access to the trading system terminal, the criminals made a total of seven purchases and sales of US dollars in the Dollar/Ruble exchange program. These operations were as follows:

- "Market" orders which provide requests to buy or sell a specified amount of lots (for fixed

amount of foreign exchange) at the best prices offered in the trading system.

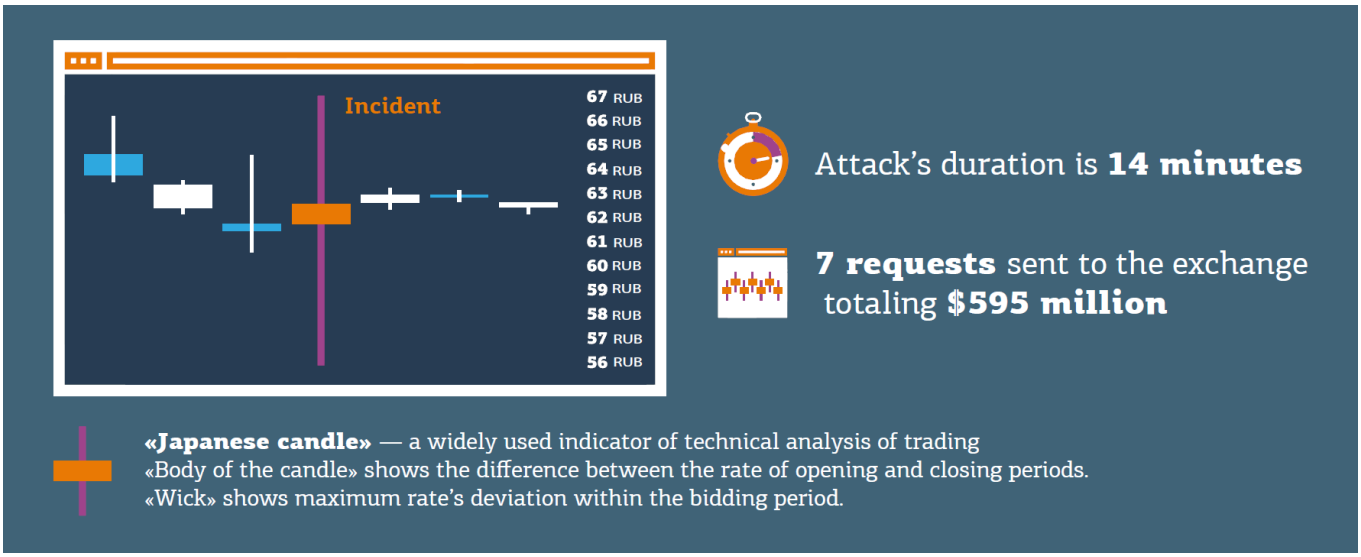
- "Removal" orders which provide a request to purchase the largest amount of currency possible immediately after their registration in the trading system, and the remainder was removed from the trading system.

Picture 4. Technical analysis of the trades

In total 5 trades were made for the purchase of $437 million and two trades for the sale of $97 million. However, only a small proportion of the trades were carried out in full, as a result $158 536 000 was purchased and $93 925 000 was sold.

In the graph for trades on that day, you can see a sudden hike, showing the volatility of the exchange from 55 to 66 Rubles.

14 minutes after the first trade request the hacker gave Corkow a command to delete itself from the system along with any traces of its activity.



Picture 5. Incident key facts

Attack results

The hacker attack provoked abnormal volatility which lasted 6 minutes and enabled buying dollars for 59,0660 rubles per dollar and in 51 seconds selling dollars for 62,3490 rubles per dollar.

To commercialize the difference in exchange rates hackers should have had a huge amount of money. For example, even if they had had **$22 million**, the profit would have been only **1.3 million Rubles**. This means the fraudsters likely conspired with some major brokerage clients to have that amount of money to buy/sell currency.

There was another potential opportunity to capitalize on the attack. With a limited amount of money at their disposal the hackers could have used the futures market where the multiplier for foreign exchange transactions could reach 1:20 to increase their profits 8 times. In this scheme, the criminals would not have needed to illegally cooperate with trading system clients.

In fact, many ordinary traders were those who used the exchange volatility to make good money, while hackers purportedly received nothing. It is also worth noting that ordinary clients of the trading system attract more attention while deals on futures market could remain unnoticed.

As a result of the attack, the compromised bank which terminal was used for intrusion, suffered a huge financial and reputational damage, since many players on the market didn't trust the hacking theory of the incident and tended to believe that a simple mistake had occurred. Experts

say that many companies that were trading at the time of the attack and successfully made profit while the attackers are believed to have received no money from the operation. This evidence leads us to believe that these hacker actions could be a test of the ability to influence the market and capitalize on future attacks.

Malware delivery method

To spread the Corkow malware criminals use a drive-by downloads method, when victims are infected while visiting compromised legitimate websites. Hackers use the exploits "Nitris Exploit Kit" (earlier known as CottonCastle), which is not available in open sources and sold only to trusted users. The exploits are described in details in the *Malware don't need Coffee* blog.

Group-IB specialists detected various sites used by criminals to spread the Trojan: mail tracking websites, news portals, electronic books, computer graphics resources, music portals, etc. The Wide range of websites used during the campaign shows that criminals target their attacks for maximum exposure, not limiting to corporate websites.

Group-IB Bot-trek TDS sensors are in place at a number of financial institutions and, unfortunately, we register that currently Corkow malware is present on 80% of protected corporate systems.

Considering the Trojan delivery method and through our analysis of infections on banks' networks, we can confirm that all infections were conducted on a random basis. However, as our previous investigations into the Anunak group have displayed, gaining access to any computer on a corporate network gives access to even the most highly protected banking systems.

The list of websites which were used to spread Corkow is presented below.

> Total traffic on these websites exceeds 800 000 users per day. An average infection rate of Nuclear Exploit Kit is 11%, which means hackers could infect up to 90 computers per day, significantly increasing the size of their botnet.

Website	Category	Average traffic per day
post-tracker.ru	Mail	38 478
zr.ru	Cars	112 271
business-gazeta.ru	News	68 746
proshkolu.ru	Education	47 249
opengost.ru	State standards	8 545
krokha.ru	Women's Portal	-
eurolab.ua	Medicine	156 552
newsdon.info	News	40 614
dirt.ru	Sport	7 100
anime-zone.ru	Cartoons	4 297
rus.kg	News	936
badger.ru	Shop	-
fedpress.ru	News	25 804
carsguru.net	Advertisement	52 157
findfood.ru	Cookery	56 307
beboss.ru	Advertisement	4 863
vidal.ru	Medicine	25 678
reghelp.ru	Advertisement	10 339
rabotagrad.ru	Advertisement	5 581
proshkolu.ru	Advertisement	-
muztorg.ru	Shop	26 332
mirf.ru	Magazine	5 226
medgorodok.ru	Medicine	8 696
dobrota.ru	Medicine	-
cooksa.ru	Cooking	19 929
consmed.ru	Medicine	32 712
buro247.ru	Fashion	-
3dmir.ru	Computer graphics	2 508
novorus.info	News	40 614
kidbe.ru	Women's Portal	14 778
eknigi.org	Electronic books	-
2x2.su	Advertisement	-

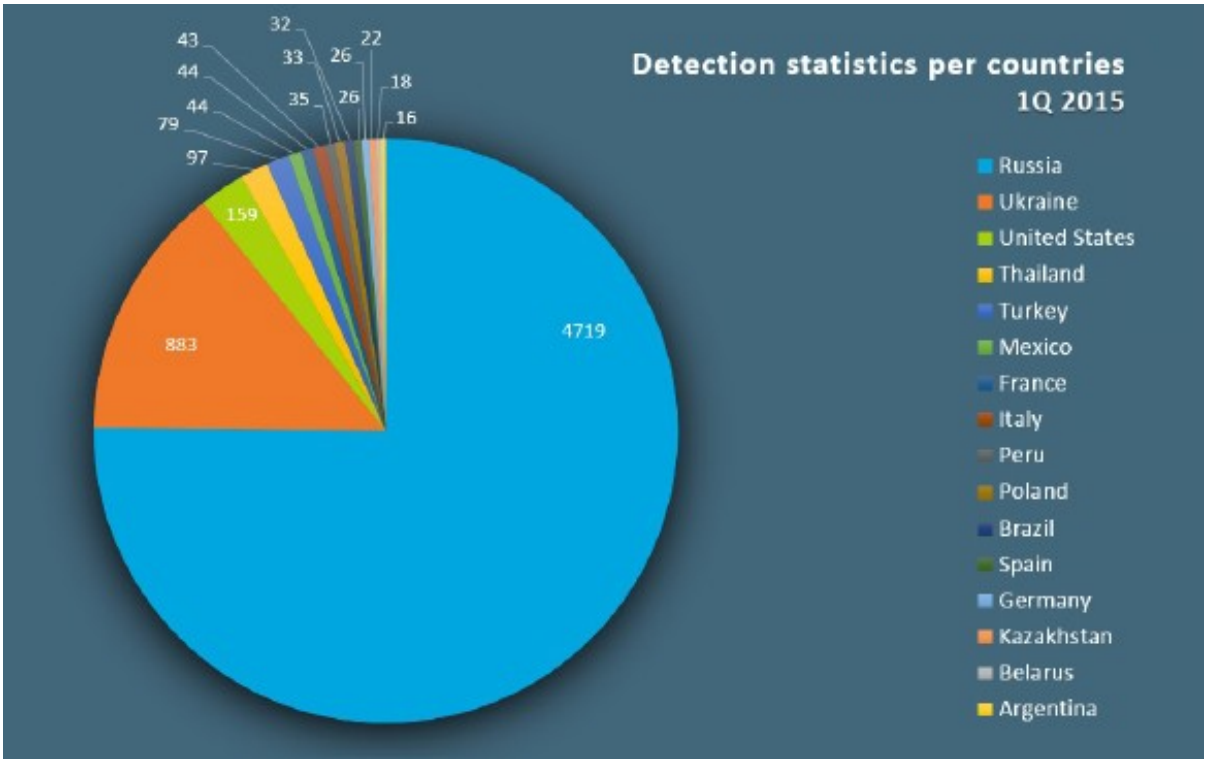
Table 1. List of websites used to spread Corkow

Area of attack

According to statistics, Corkow primarily targets users in Russia and the CIS, but it is worth noting that in 2014 the amount of attacks targeting the USA increased by 5 times, in comparison with 2011. Moreover, the number of Corkow incidents detected in Q1 2015 in the United States exceeds the number of those in the CIS countries.

Country	2011	2012	2013	2014	Q1 2015
Russia	61425	132327	19156	26493	4719
Ukraine	7076	9891	4558	6108	883
Belarus	2748	1892	584	82	18
Kazakhstan	1132	1997	254	43	22
Turkey	762	453	27	100	79
Spain	457	164	30	160	26
Italy	238	115	375	131	43
Mexico	209	362	33	82	44
Peru	191	167	5	123	35
Poland	181	86	28	94	33
United States	164	102	49	534	159
Chile	114	192	52	36	11
Thailand	114	51	8	204	97
Argentina	107	65	6	31	16
Germany	107	23	30	82	26
Greece	91	42	22	59	14
Brazil	89	69	10	43	32
France	81	65	10	79	44

Table 2. Incidents statistics per year by country



Picture 6. Geographical distribution of Corkow infections in Q1 2015

Attack tactics

Hackers first actively spread bots using the Niteris exploit, and then search for infected devices at banks amongst their bots by analyzing IP addresses, cracked passwords and results of the modules performance.

If a bot was installed on a network that was of interest to the hacking group, this bot was then used to upload one of the remote access programs. In addition to the legitimate AmmyAdmin tool, the hackers used Visconti Backdoor developed based on legitimate RMS (remote manipulator system) software. Visconti Backdoor is distributed on Russian-speaking hacker forums and delivers the following functionality:

- Secret installation on the targeted computers, retention in the system as legitimate software;
- Grabbing user desktop activity; actively recording onscreen audio and video (also can be performed according to established schedule);
- Keylogger;
- Remote access to the task manager, the system processes and services with application-blocking functionality;
- Receive data on technical parameters and the operating system of the victim's machine;
- Executing commands in CMD;
- Remote launch of files and applications on the victim's machine;
- Collect files and buffer exchange from the victim's machine;
- Secret remote access on behalf of the victim's account RDP);
- Remote registry editor;
- Capability to control computer state (shutdown/restart), set sleep mode, switch monitor off;
- Disabling the UAC (User Account Control) system;
- Can run on any version of Windows (from XP to 10), both 32-bit and 64-bit versions;
- Can uninstall itself from the victim's system.

Hackers used the remote access to detect servers of their interest in the internal network. To obtain logins and passwords they applied keyloggers built into Corkow, as well as a commonly used feature of Mimikatz, dumping clear text Windows credentials from LSA.

Also, the group used scanners aimed at searching for hosts with active VNC and Radmin services in the corporate network.

When they received access to a bank staff computer, Corkow malware was uploaded to their computer to spy on users through keylogging and transmission of screenshots.

Malware description

Each of Corkow's modules is implemented as a library capable of downloading and executing files from a remote server, deleting files, rebooting and disrupting the system, collecting data on the targeted PC and the victim's activity (keylogging, screenshots) and sending this information to various addresses. Also, the malware provides a server for remote access to the targeted PC.

The Corkow Trojan includes modules which are listed in table 3 below. The names of the modules and their versions were received through analysis of DRAM archives in infected system.

Module	Version	Description
MON	1.9.0	Collects information about the computer, accounts, OS and monitors processes
KLG	1.3.1	Keylogger
HVNC	2.0	Provides remote access to the computer
FG	2.0	Tracks websites visited by the user and collects authorization data
QUIK	1.1	Copies data from the Quik trading system application
IB2	1.3.1	Copies data from the «IBank2» application.
SBRF	1.3.8	Copies data from the «Wclnt.exe» application
AMY	1.4	Provides remote access to the computer using the Ammy Admin remote
iFOBS	1.6	Copies data from the «iFOBSClient.exe» application.
TRZQ	1.0	Copies data from the TRANSAQ trading system

Table 3. Corkow.dll modules

Basic functionality

The most important functions of the program are delivered in separate modules as described below:

- The tool decrypts and uploads extra modules to third-party processes. The search for appropriate process for intrusion is launched in a separate flow, which continuously monitors running processes.
  - The FG module can be injected into processes that have the following substrings inside their names: «firefox.exe», «iexplore.exe», «chrome.exe», «opera.exe», «browser.exe», «iTunes.exe»;
  - The QUIK module can be injected into processes that have the substring «info.exe» in the name;
  - The TRZQ module can be injected into processes that have the substring «transaq.exe» in the name;
  - The SBRF module can be injected into processes that have the substrings «wclnt.exe», «ip-client.exe» in the name;
  - The iFOBS module can be injected into processes that have the «iFOBSClient.exe» substring in the name;
  - The IB2 module can be injected into processes that have the substrings «java.exe», «javaw.exe» in the name;
- The MON module is unpacked inside the memory and launched as a separate flow; The HVNC module is also unpacked inside the memory and launched as a separate flow;
- The FG module intercepts functions and collects information on keys pressed, websites visited and credentials in the process. It encrypts information gathered and records it in the file specified in the "File System Interaction" section;
- The MON module collects information on running processes. It grabs file names, protection status (using the function "SfcIsFileProtected"), the username of the person who ran the process, the process ID, launch arguments and the last user input (using the function "GetLastInputInfo") and sends the information obtained to the remote server with the date stamp. It is also capable of taking screenshots;
- The iFOBS module collects information on the application for iFOBS Internet banking. It can take screenshots and copy key information;

- The SBRF module collects information on the application for Sberbank Online Internet banking system;

- The QUIK module can be injected into the process that has the substring «info.exe» in the name. This module is intended to collect data from the QUIK software, which interface provides access to various electronic stock exchanges. It copies the following files to send them to the server:

  - «Login.data»
  - «qrypto.cfg»
  - «ClientInfo.txt»
  - «limits.dat»
  - «ip.cfg»
  - «info.ini»
  - «ka_pr.ini»
  - «qcrypto.ini»
  - «randseed.bin»
  - «quik.txk»
  - «Pubring.txk»
  - «Secring.txk»

Also it copies file keys from the folder «/Keys» of the application directory.

- The HVNC module can provide remote access to a PC with the malicious program installed. It creates remote user session and extra desktop in OS Windows to provide remote management service. Thus, the actions of this module will be hidden from the PC user. After the module is unpacked and launched, it sends the information on PC, user, OS and module version to the C&C server.

- The AMY module can launch Ammy Admin software with –service and –nogui arguments and send the program configuration to the remote server. This data enables the hacker to connect to the PC and control it remotely.

- To get information about hardware electronic keys the Trojan reviews all the connected USB devices and searches for the following names among them:

Rutoken Magistra; USB Token Device; USB Token; USB_Token; USB-Token; Token; VPNKey; VPN Key; VPN-Key; VPN_Key; ICCD USB-Token; BIFIT ICCD; BIF IT-ICCD; BIFIT_ICCD; ICCD_USB_Token; EZCCID; Smart Card Reader.

- It downloads and then immediately removes files mentioned in Table 3. Purportedly it aims to disrupt the network analysis and hide requests to command servers.
- The malware sends collected information by modules to the C&C server.

- It can add a malicious file to the autostart through modifying the registry. You can find detailed description in the section “Registry modification”.

Network interactions

Corkow sends information on its status to the remote C&C server via HTTP POST requests. The list of C&C servers is established in each sample code. The malware sends the following string to C&C server:

<Machine GUID>.<Date of OS installation>.<disk serial number%SYSTEMDRIVE%><|><corkow.dll version><|><digit capacity of OS><|>1<|><OS version>

s=<current time>
tzb=<time zone>
cdi=<the difference between two API calls of time function> rsi=<the difference between two API calls of time function> on=<the difference between two API calls of time function>
lng=<OS langauge, returned by GetSystemDefaultUILanguage API> plds=<the list of modules and their versions>
hp=<the name of executed processes> un=<user account name>
clr=<.NET version>
svi=<disk serial number %SystemDrive %> mst=<time>
bst=<time>
hpid=<PID-process number>
hpst=<process creation tame, received by GetProcessTimes API> bts=<digit capacity>
dbgi=<setings with DebugInfo>
lbr=<settings with LastBadReply>

The server will then respond with one of the supported commands enlisted below.

Command	Arguments	Action
NOP	-	No operation
Reboot	-	Forced restart of the user's PC
Wipe	-	Wiping files beyond recovery
	Path	Path to the file to be deleted
	Mask	File mask to determine files to be deleted
SelfRemove	-	Removal of the Corkow program
	DestroySystem	This flag means disrupting the PC ability to operate after the Corkow program is removed. If active, the malware will try to remove files mentioned in the Table 1 and corrupt MBR
CfgWrite	-	Change to the configuration of the investigated program
	PayloadID	Library identification
	Section	Configuration section
	Param	Parameter name
	Value	Parameter value
Update	-	Update of the Corkow program
	Url	Network address of the update module to be downloaded
	Version	The version of the update module to be downloaded. If this version is older than the installed malware, the update process will be canceled
	LoadImmidiatly	This flag cancels the delay for update after the module is downloaded
DownloadAndExecuteEXE или DAMPDLL	-	Downloads file from the remote server and launches it. In case of «DAMPDLL», it also downloads dynamically linked library in PE format to the process memory space to run the Corkow
	Url	Network address of the file to be downloaded
	CommandLine	The arguments to be provided to the file, when executed.
	CryptMode	The value can be «Static» or «Dynamic». Encryption of the downloaded file uses the same algorithm as for sending data. In the first case the key is provided with argument «StaticKey» (see below). In the second case, the domain
	StaticKey	The key used to decrypt downloaded files.
ChangeURLs	CommandUrls	Replacing addresses of C&C servers.
	SendURLs	Replacing the addresses of the servers receiving data.

Table 4. Commands from C&C server.

Appendix – Compromised signatures

C&C Servers

CORE VERSION	PE time stamp
1.17.6.4	
1.19.9.0	
2.1.4.0	
2.5.7.0 2.6.4.0	
2.5.8.0 2.6.2.0	
3.0.6.0 3.3.0.0 3.6.0.0 3.6.2.0 3.7.8.0 3.8.9.0	
3.8.9.6 3.9.9.0 4.1.0.0 4.1.0.1 4.1.7.0 4.3.1.2 4.3.9.1 4.3.9.5	Dec 13 02:07:37 2011 Dec 23 00:02:04 2011 Jan 11 09:25:12 2012 Jan 11 09:35:46 2012 Feb 09 08:17:08 2012 Mar 01 04:36:57 2012
4.3.9.8	
4.4.7.0 4.4.7.1 4.4.7.2 4.4.7.7 4.7.5.0	Apr 12 04:39:33 2012

4.8.1.0	
4.8.7.0 4.9.3.0 5.5.1.0 5.5.1.2 5.7.6.0 5.7.9.1 5.9.3.1	Jul 12 13:43:51 2013
5.7.6.0 5.7.9.1 5.9.3.0 6.0.3.0	
6.0.6.0	
6.0.8.1 6.0.8.2 6.2.0.0 6.2.0.1 7.5.0.0 7.6.13.1 7.6.13.2 7.6.13.4 7.6.13.5 7.6.13.6 7.6.13.7 7.6.13.8 7.6.13.9	Sep 26 20:42:10 2013 Jan 16 17:49:55 2014 Jan 16 18:01:42 2014 Feb 19 21:17:36 2014
6.0.8.2 6.2.0.1 6.4.1.3 7.5.0.1 7.7.6.1	Sep 26 20:44:01 2013 Nov 18 19:07:10 2013 Dec 26 06:32:38 2013
6.0.8.4 6.2.0.1	Sep 27 12:06:51 2013 Oct 08 14:23:06 2013
7.9.0.1 7.9.0.5 7.9.1.1 7.10.0.1	May 28 18:08:09 2014 May 28 18:23:42 2014 Jun 11 21:14:26 2014
7.16.0.1 7.20.0.11	Jul 01 23:03:16 2014 Jul 21 22:02:08 2014

7.16.1.0 7.45.1.1 7.47.1.1 7.56.1.1 7.70.1.1 7.74.1.1	Jul 01 23:27:25 2014 Aug 07 05:40:04 2014 Sep 18 16:16:43 2014
7.78.1.1	
7.34.0.1 7.34.0.2 7.45.0.2 7.46.0.1 7.56.0.1 7.70.0.2 7.70.0.3 7.74.1.1	Aug 05 09:29:09 2014 Aug 05 09:30:00 2014 Aug 07 05:32:04 2014 Aug 13 10:34:35 2014 Aug 20 16:32:14 2014 Sep 09 19:01:42 2014
7.85.0.1 7.92.0.1 7.92.1.2	Nov 06 09:14:46 2014
7.85.1.1 7.92.1.2	Oct 20 21:37:36 2014 Nov 07 01:07:58 2014
7.102.0.1	
7.107.0.1 7.107.1.1	Dec 10 22:03:23 2014
7.107.1.1	Dec 10 22:03:23 2014
7.118.1.1	
7.120.0.11 7.120.0.32	

Mutexes

The mutex values are set up by the malicious program.

Mutex path
«Session\< id of desktop session for the injection process >\HighMemoryEvent_<id of
Global\TermSrvReadyEvent

Installation Paths

Corkow installs and runs in the following paths:

Possible Working Paths
«%Temp%\tmpXXXX.tmp
«%TEMP%

Yara rule

```
rule CorkowDLL
{
   meta:
      description = «Rule to detect the Corkow DLL
   files» strings:
      $mz = { 4d 5a }
      $binary1 = {60 [0-8] 9C [0-8] BB ?? ?? ?? ?? [0-8] 81 EB ?? ?? ?? ?? [0-8] E8 ?? 00 00 00 [0-
8] 58 [0-8] 2B C3}
      $binary2 = {(FF 75 ?? | 53) FF 75 10 FF 75 0C FF 75 08 E8 ?? ?? ?? ?? [3-9] C9 C2 0C  00}
      $export1 = «Control_RunDLL»
      $export2 = «ServiceMain»
      $export3 = «DllGetClassObject»

   condition:
      ($mz at 0) and ($binary1 and $binary2) and any of ($export*)
}
```

About Group-IB

Group-IB is one of the leading international companies specializing in high-tech cybercrimes, fraud prevention and investigation.

Since 2013, the company has offered a range of services in computer forensics, consulting and auditing of information security systems to prevent financial and reputational damages of the largest companies in Russia and worldwide.

Group-IB's extensive experience has resulted in the innovative Bot-Trek information security ecosystem – an array of highly sophisticated software and hardware solutions based on up-to-date cyber intelligence data and deep analysis of real hacker attacks to monitor, identify and prevent cyber threats.

The company's clients include over 60 financial institutions, light and heavy industry enterprises, energy and oil companies, software companies, telecommunications operators in Russia, Argentina, Australia, Brazil, Ecuador, UK, the EU, Canada and USA.

Group-IB team has uniquely qualified experts with solid practical experience. They are internationally certified by CISSP, CISA, CISM, CEH, CWSP, GCFA, SSCP and also have information security state certificates. The company's representatives are members of important advisory councils and speakers at major international information security conferences.

Group-IB's mission is to protect our clients in cyberspace by creating and using innovative products, solutions and services.

+7 (495) 984-33-64
www.group-ib.com
info@group-ib.com
facebook.com/groupib
youtube.com/groupib
twitter.com/groupib
linkedin/company/group-ib