BUHTRAP

The evolution of targeted attacks
against financial institutions

|GROUP|iB|

TABLE OF CONTENTS

In Group-IB's annual report "The High-Tech Crime Trends 2015" Group-IB noted the significant interest of hackers towards financial institutions and predicted an increase in targeted attacks for 2016.

We have published open reports on hacker groups, such as Anunak (also known as Carbanak), Corkow (also known as Metel), specializing in attacking financial institutions. The Buhtrap group covered in this report is a vivid example of a criminal team evolving from attacks against bank clients to attacks directly targeting financial institutions.

In many respects, this group's activity has led to the current situation where attacks against Russian banks causing direct losses in the hundreds of millions of rubles are no longer taken as something unusual.

The fundamental element of Buhtrap's success is **a general lack of awareness concerning targeted attacks against the financial sector**: the industry does not realize how exactly attacks are conducted, that's why they cannot develop adequate countermeasures.

Such lack of awareness also contributes to the second element of the hackers' success which is the **over-reliance on traditional security measures**, such as licensed and updated version of antivirus, the most recent operating system versions, firewall or Data Leak Prevention (DLP) systems which are mistakenly expected to stop criminals at the initial stages of attacks.

This report is intended to increase the banking communities' awareness about hacker tactics, provide indicators which enable banks to identify corporate network compromise incidents and develop recommendations which will help to combat cybercriminals.

Buhtrap has been active since 2014, however their first attacks against financial institutions were only detected in August 2015. Earlier, the group had only focused on targeting banking clients. At the moment, the group is known to target Russian and Ukrainian banks.

600 million ₽
the largest amount stolen from a Russian bank (2016)

25,6 million ₽
the smallest amount stolen from a Russian bank (2015)

143 million ₽
the average amount stolen from a bank

1 billion ₽
the amount of money which was prevented from being stolen in January 2016

Buhtrap attacks threaten the financial stability of their victims:

62%
the average amount of theft as it compares to the bank's charter capital

2,5 times
bank's charter capital was the loss to fraud in two separate cases

From August 2015 to February 2016 Buhtrap managed to conduct **13 successful attacks against Russian banks** for a total amount of **1.8 billion rubles ($25.7 mln)**. The number of successful attacks against Ukrainian banks has not been identified.

Buhtrap is the first hacker group using a network worm to infect the overall bank infrastructure that significantly increases the difficulty of removing all malicious functions from the network. As a result, banks have to shut down the whole infrastructure which provokes delay in servicing customers and additional losses.

Malicious programs intentionally scan for machines with an automated Bank-Customer system of the Central Bank of Russia (further referred to as BCS CBR). We have not identified incidents of attacks involving online money transfer systems, ATM machines or payment gates which are known to be of interest for other criminal groups.
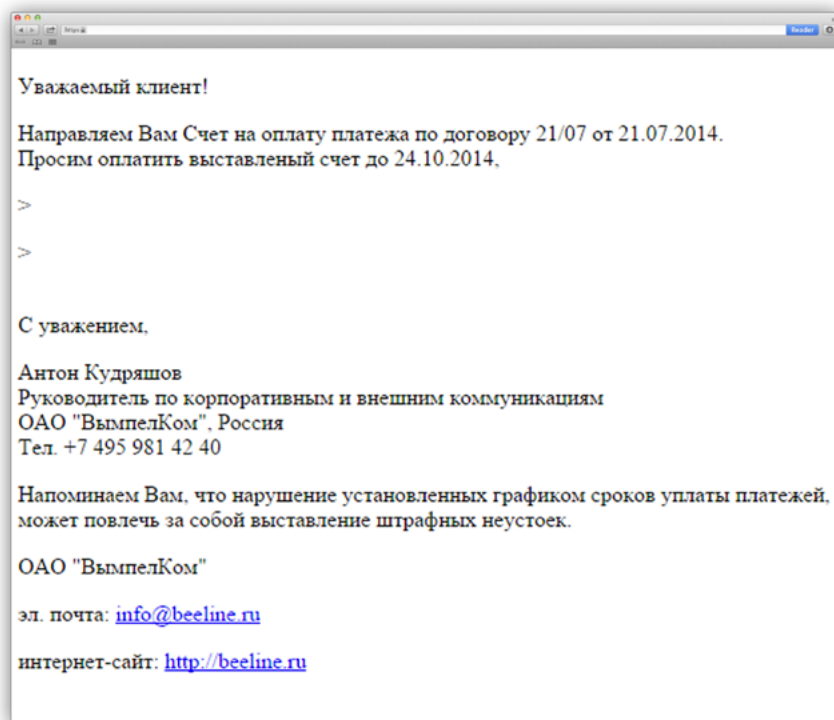
The main infection vector in corporate networks is phishing emails on behalf of the Central Bank of Russia or its representatives, however Group-IB specialists have also detected attacks by means of **distributing exploit kits** (using the infrastructure of Corkow (Metel) hacker group) and using **legal software distribution**.

In February 2016 sources codes of the malicious program were published in open resources which has led to its wide distribution. **Publishing source codes will provoke the appearance of new modifications for this malware** and increase in the amount of similar incidents.

Absolutely all incidents could have been easily prevented. Annual **expenditures for effective prevention tools are 28 times lower than the average direct loss** from one targeted attack.

On October 20, 2014 we notified Group-IB Bot-Trek Intelligence subscribers about phishing emails which were sent from the info@beeline-mail.ru address with the subject "Invoice No 522375-ФЛОРЛ-14-115" (pic. 1). The beeline-mail.ru domain name was also registered on October 20, 2014.

Уважаемый клиент!

Направляем Вам Счет на оплату платежа по договору 21/07 от 21.07.2014. Просим оплатить выставленый счет до 24.10.2014.

>

>

С уважением,

Антон Кудряшов
Руководитель по корпоративным и внешним коммуникациям
ОАО "ВымпелКом", Россия
Тел. +7 495 981 42 40

Напоминаем Вам, что нарушение установленных графиком сроков уплаты платежей, может повлечь за собой выставление штрафных неустоек.

ОАО "ВымпелКом"

эл. почта: info@beeline.ru

интернет-сайт: http://beeline.ru

Picture 1. *Screenshot of the phishing email sent on behalf of the VimpelCom company*

The email attachment contained a specifically modified **RTF file, exploiting the CVE-2012-0158 vulnerability in the MSCOMCTL.OCX library**. This malicious code can be activated in all MS Word versions, starting with MS Office 2003.

On the 21 November, 2014 a similar phishing attack was conducted from the info@extern-kontur.ru email address with the subject "Payment for SKBKontur Services" on behalf of the company SKBKontur (pic.2), specializing in developing software designed for electronic document flow, financial accounting and enterprise management.

INFECTION

If the user opens the RTF file the malware creates a file "ntxobj.exe" in the "%User%" directory which is then added to the startup folder and launched installing NSIS-packed Trojan downloader (Nullsoft Scriptable Install System is an open source system to create Windows installers) with various modules and scripts.

The malicious modules are 7z self-extracting password-protected archives. A lot of them are signed with a valid code-signing certificate.

The scripts check for evidence that the malware is run in a virtual machine, in a debugging environment or on a computer without the Russian Windows locale, exiting if it finds any. If not, the malware searches in files and folders by the following substrings: "iBank2", "amicon", "bifit", "bss", "ibank", "gpb", "inist", "mdm", "Aladdin", "Amicon", "Signal-COM", "bc.exe", "intpro.exe", "cft", "agava", "R-Style", "AKB", "Perm", "AKB Perm", "CLUNION.0QT", "ELBA". Also, **the Trojan checks if there are executable files related to bank applications** of various manufacturers (see the list on page 7).
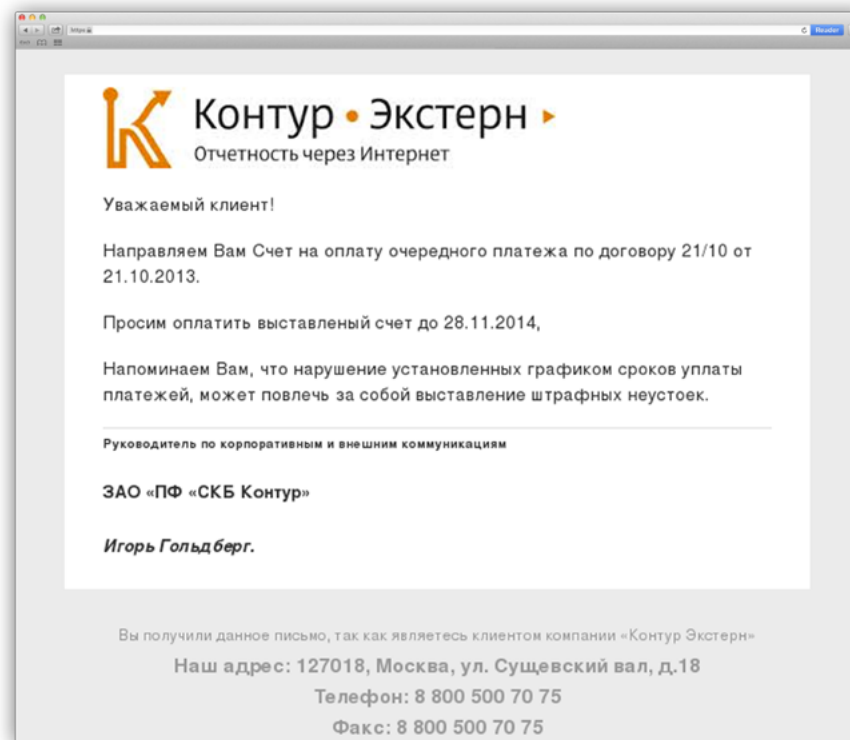
OBTAINING DATA

The main module with the executable file "pn_pack.exe" is responsible for stealing user credentials and communicating with the C&C. Hackers launch the module using **Yandex Punto Switcher** to spy on keystrokes and send them together with clipboard content to the C&C server, as well as to enumerate smart cards present on the system.

REMOTE CONTROL

If the malware detects banking applications present in the system, the module will then install **LiteManager,** a legitimate tool that allows remote control of a system.

To establish control over an infected PC, the malware uses executable files "mimi.exe" and "xtm.exe". They allow attackers to get or recover the password from all active Windows accounts for the whole period of operation, to create a new account on the operating system to enable the RDP (Remote Desktop Protocol) service.

Once successfully installed, the program creates fraudulent transfer orders and sends them to the bank for executing.

Picture 2. *Screen shot of the phishing email sent on behalf of SKBKontur*

EXECUTABLE FILES WHICH PRESENCE IS CHECKED BY BUHTRAP

ip-client.exe,
prclient.exe, rclient.exe,
saclient.exe,
SRCLBClient.exe,
twawebclient.exe,
vegaClient.exe,
dsstart.exe,
dtpaydesk.exe,
eelclnt.exe, elbank.exe,
etprops.exe, eTSrv.exe,
ibconsole.exe,
kb_cli.exe, KLBS.exe,
KlientBnk.exe,
lfcpaymentais.exe,
loadmain.exe, lpbos.exe,
mebiusbankxp.exe,
mmbank.exe,
pcbank.exe, pinpayr.exe,
Pionner.exe,
pkimonitor.exe,
pmodule.exe, pn.exe,
postmove.exe,

UpMaster.exe,
SGBClient.exe,
el_cli.exe,
MWClient32.exe,
ADirect.exe,
BClient.exe, bc.exe,
ant.exe, arm.exe,
arm_mt.exe,
ARMSH95.EXE,
asbank_lite.exe,
bank.exe, bank32.exe,
bbms.exe, bk.exe,
BK_KW32.EXE,
bnk.exe, CB.exe,
cb193w.exe, cbank.exe,
cbmain.ex,
CBSMAIN.exe,
CbShell.exe, clb.exe,
CliBank.exe,
CliBankOnlineEn.exe,
CliBankOnlineRu.exe,
CliBankOnlineUa.exe,

client2.exe, client6.exe,
clientbk.exe, clntstr.exe,
clntw32.exe,
contactng.exe, Core.exe,
cshell.exe,
cyberterm.exe,
client.exe, cncclient.exe,
bbclient.exe,
EximClient.exe,
fcclient.exe, iscc.exe,
kabinet.exe,
SrCLBStart.exe,
srcbclient.exe,
Upp_4.exe,
Bankline.EXE,
GeminiClientStation.exe,
ClientBank.exe,
ISClient.exe, cws.exe,
CLBANK.EXE,
IMBLink32.exe,
cbsmain.dll,
GpbClientSftcws.exe,

quickpay.exe, rclaunch.exe,
retail.exe, retail32.exe,
translink.exe, unistream.exe,
uralprom.exe, w32mkde.exe,
wclnt.exe, wfinist.exe,
winpost.exe, wupostagent.exe,
Zvit1DF.exe, BC_Loader.exe,
Client2008.exe,
IbcRemote31.exe, _ftcgpk.exe,
scardsvr.exe, CL_1070002.exe,
intpro.exe, Run.exe,
SGBClient.ex, sx_Doc_ni.exe,
icb_c.exe, Client32.exe,
BankCl.exe,
ICLTransportSystem.exe,
GPBClient.exe, CLMAIN.exe,
ONCBCLI.exe, rmclient.exe,
RkcLoader.exe, CLBank3.exe,
FColseOW.exe,
productprototype.exe,

TACTICS OF BUHTRAP ATTACKS AGAINST BANK CLIENTS

1. Hackers purchased domain names similar in spelling with legitimate companies' domains, which were planned to be used in attacks.

2. They rented a server where a mail server was correctly set up to send phishing emails on behalf of the legitimate company. Correct settings of a separate server and purchase of domains similar in spelling were necessary to reduce the probability of being filtered as spam and to increase the probability of opening the files attached by victims.

3. First looking for malware researcher tools or evidence that the malware is run in a virtual machine, exiting if it finds any.

4. After the malware was successfully launched as a result of vulnerabilities exploitation, it checked for the Russian Windows locale and signs of running in a virtual or debugging environment in order to reduce the risk of being detected by security tools and antivirus software.

5. The malware's basic module was responsible for collecting data and sending it to the attacker's remote server.

6. The malicious program searched for files and other traces typical to operations with banking applications. Their detailed list is presented above.

7. If operations with the banking applications were detected, the malware sent the command to download Lite Manager, a legitimate remote access tool. The operating system was configured in such a way that access via RDP was allowed.

8. Criminals used remote control tools to create fraudulent transfer orders and send them to the bank.

Observing the actions of phishing, checking environment and organizing remote access, one can't help that the Anunak group comes to mind, which successful targeted attacks against banks using similar tactics

The highest loss resulting from the Buhtrap attacks amounts to 40 million rubles, in contrast to the Anunak group which earned hundreds of millions directly attacking banks.
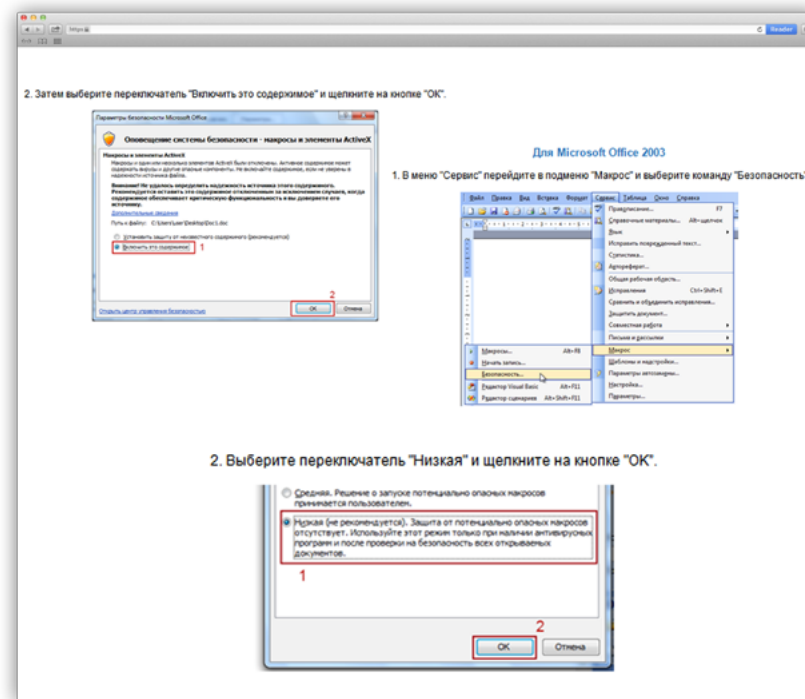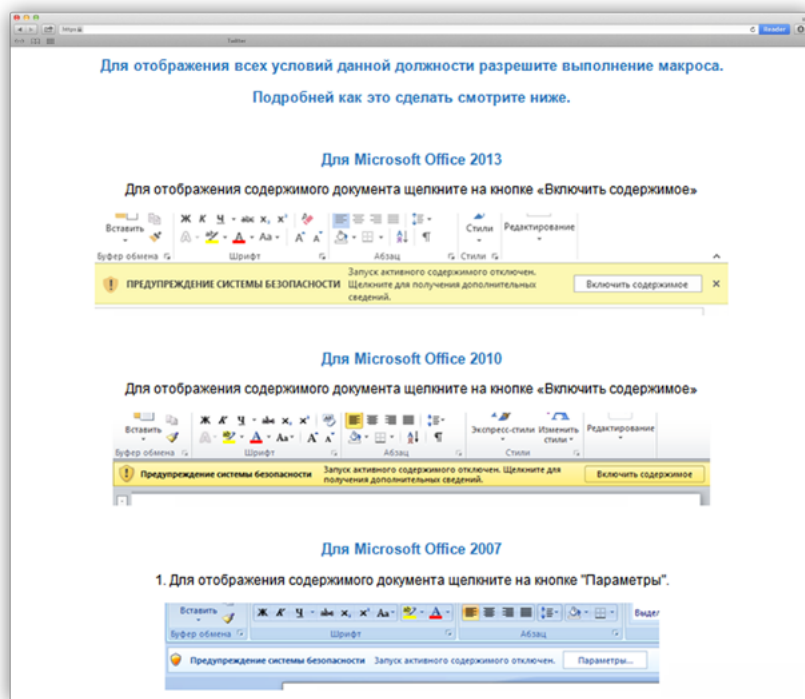
The group is believed to have actively attacked bank clients, trying to modify malware and search for more effective ways of spreading in corporate networks. We have identified 3 methods of Buhtrap distribution.

PHISHING MAILOUTS

Phishing attacks were the key tool used by the group to spread Buhtrap both in attacks against bank clients and in attacks against banks, which will be described further.

If the document was delivered with macros instead of exploits (CVE-2012-0158, CVE-2013-3906 or CVE-2014-1761), then the document contained instructions for enabling macros (pic. 3). In the event the user followed the instructions, Buhtrap was installed. Sometimes criminals spread the malicious executable files directly in encrypted archives.

Picture 3. *Instructions for enabling macros when opening a malicious document*

EXPLOIT KIT

We noticed that criminals were spreading Buhtrap using this method from May 2015 to August 2015. Attackers secretly redirected users from compromised legal resources to the malicious server hosting the exploit kit. In the event of successfully exploiting the vulnerability, the Buhtrap malware was then installed.

Compromised legal websites included accounting portals, specialized websites for registration of legal entities and construction websites.

It is worth noting that attackers used the same compromised websites to spread Buhtrap as those that had been used for the Corkow Trojan. Moreover, they used the same exploit kit Niteris (pic.4) as that in the Corkow case. This evidence leads us to believe that that members of these groups communicate with each other.

LEGAL SOFTWARE

In late October EsetNod32 analysts detected malicious activity on the **Ammyy** website, which belonged to the company specializing in developing the legitimate remote administrator software **Ammyy Admin**. Criminals managed to upload the malicious version of this software which contained the Buhtrap Trojan.

Also it should be noted that in various periods this website was used to spread modified Ammyy version with such Trojans as Lurk, CoreBot, Ranbyus, NetwireRAT.

Picture 4. *Control system for the Niterisexploit kit (also known CottonCastle)*

We managed to detect the first successful attacks against banks about one year after the first attacks had been conducted against banking clients.

The timeline of the Buhtrap group development

october · · · · · · august · october · december · february

2014 · 2015 · january · 2016

First attacks against bank clients

First attack against a bank
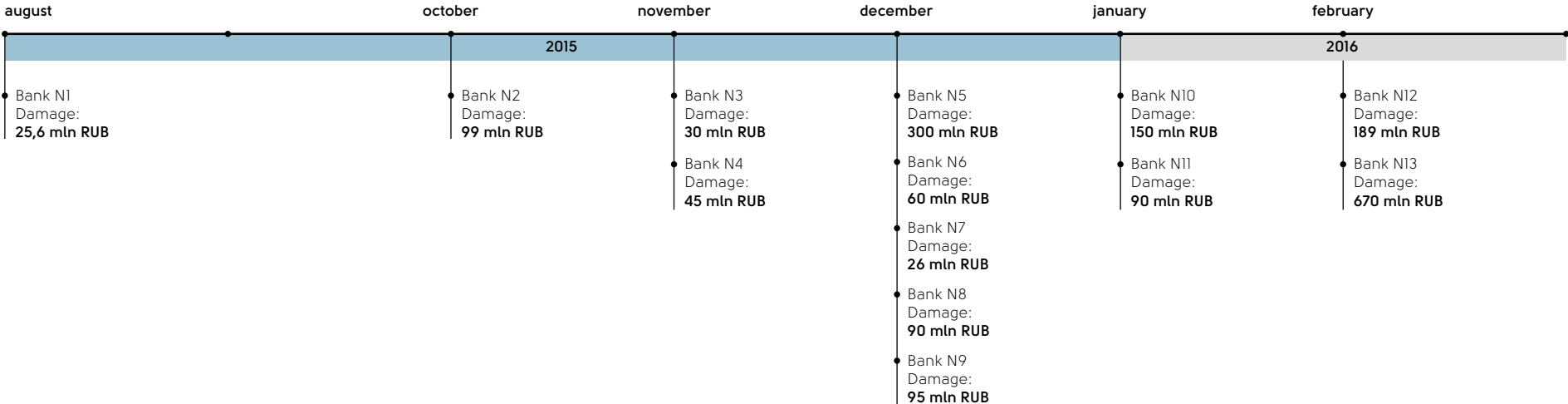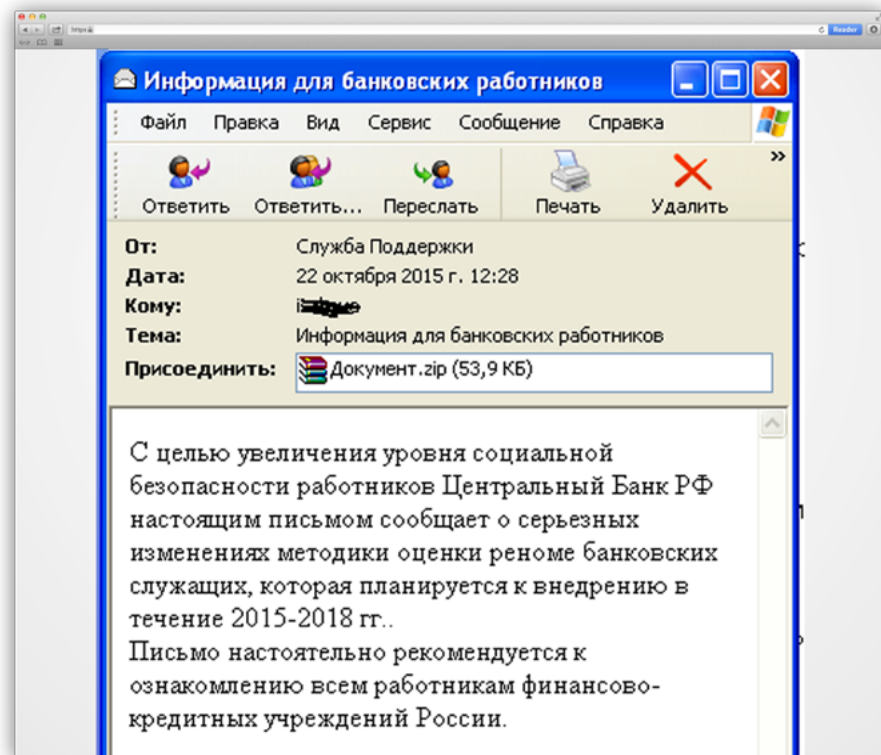
First spear-phishing attack against bank employees of the Central Bank

Distribution from the Ammyy admin website

Spear-phishing mailing to the anti-drop club mail list on behalf of Gazprombank

Money theft in several banks simultaneously

Spam emails with a new worms designed to infect the local network sent acting as the Central Bank

Hackers place Buhtrap source codes forums

From August 2015 to February 2016 Buhtrap conducted 13 successful attacks on Russian banks for a total amount of 1.8 billion rubles.
The amount of successful attacks against Ukrainian banks has not been identified.

Chronology of the successful attack against banks

august · october · november · december · january · february

2015 · 2016

Bank N1
Damage:
25,6 mln RUB

Bank N2
Damage:
99 mln RUB

Bank N3
Damage:
30 mln RUB

Bank N4
Damage:
45 mln RUB

Bank N5
Damage:
300 mln RUB

Bank N6
Damage:
60 mln RUB

Bank N7
Damage:
26 mln RUB

Bank N8
Damage:
90 mln RUB

Bank N9
Damage:
95 mln RUB

Bank N10
Damage:
150 mln RUB

Bank N11
Damage:
90 mln RUB

Bank N12
Damage:
189 mln RUB

Bank N13
Damage:
670 mln RUB

FIRST SPEAR-PHISHING ATTACK ACTING AS THE CENTRAL BANK

On October 22, 2015 we notified Bot-Trek Intelligence clients about spam being sent acting as the Central Bank of the Russian Federation from the support@cbr.ru.com inbox with the subject "Information for bank officials" (pic. 5). This was a mass-mailing attack with numerous Russian banks confirming they received this email.

The email attachment contained a ZIP archive with a MS Office document (pic. 6). If the user opened the document, a script was installed which then checked whether there were links to online banks and banking software in the web browsing history.

Picture 5. *Screenshot of the phishing email on behalf of the Central Bank*

Центральный Банк Российской Федерации доводит до сведения банковских сотрудников следующие меры, которые Банк намерен предпринять для сохранения комфортного уровня работы и жизнеобеспечения служащих финансово-кредитных учреждений нашей страны.

1. В ближайшие три года с 2015 по 2018 гг. все сотрудники банков должны будут пройти процедуру обязательной специальной оценки условий труда (СОУТ). По ее итогам каждому работнику будет присвоен персональный классификатор, согласно которому будет определяться размер полагающихся труженику заработной платы, компенсаций, бонусов, страховых выплат. Для снижения числа страховых случаев предусмотрено внедрение системы профилактических занятий, которые будут компенсироваться в соответствии с СОУТ.

2. Начиная с 1 января 2016 года, каждый банковский работник имеет право на ежегодный оплачиваемый отпуск в размере 42 рабочих дней. По желанию сотрудника любое количество из этих дней может быть заменено денежной компенсацией, превышающей должностную ставку трудящегося в 1,5 раза.

3. Банковские служащие, достигшие пенсионного возраста, могут рассчитывать на заключение бессрочного договора с работодателем. Для увольнения пожилого человека руководство финансового учреждения должно иметь веские мотивы, например, отсутствие штатного сотрудника на рабочем месте без уважительной причины. При этом каждый работник может оспорить увольнение в случае, если трудящийся считает, что с ним поступили незаконно или несправедливо.

4. В течение 2016 года ЦБ РФ намечает повышение размера районных коэффициентов и региональных надбавок к заработной плате от 10% до 25%. При этом каждый служащий имеет право на пересчет заработной платы за последний год исходя из квалификации, фактически отработанных часов и результатов СОУТ.

Эти меры, по мнению экспертов ЦБ РФ, будут способствовать сохранению ценных кадров в системе финансово-кредитной сферы экономики. Спрос на банковских служащих продолжает падать, и нет оснований, что в ближайшие годы тенденция изменится. Вместе с тем новая система переаттестации поможет обеспечить квалифицированных банковских работников достойной заработной платой, актуальными страховыми выплатами, полагающимися бонусами и гарантированным отдыхом. Сотрудники финансовых и кредитных учреждений страны должны понимать, что внедрение СОУТ направлено, прежде всего, на повышение объективности оценки уровня квалификации каждого служащего, адекватное распределение заработной платы и других денежных выплат, а также общее оздоровление морального микроклимата в каждом отдельном трудовом коллективе и обществе в целом.

Служба поддержки Центрального Банка Российской Федерации

Picture 6. *Unpacked document from the phishing email sent on behalf of the Central Bank of the Russian Federation*

If successful, the program uploaded the malicious malware from the Internet (remote control server LiteManager, keylogger and the main Buhtrap module) for its further installation.

It is worth noting that **the majority of antivirus programs do not identify the downloader as a malicious program** and all downloaded software had a valid digital signature.

SPEAR-PHISHING AGAINST MEMBERS OF THE "ANTI-DROP" CLUB

Phishing attacks when emails are sent on acting as the regulator have become standard practice. But Buhtrap members are believed to have gone a step beyond existing schemes. They learnt about the so-called "Anti-drop" club, which included security specialists from several hundred banks. These club members exchange information which enables them to detect and block fraudulent operations. Purportedly during one of the first attacks hackers intercepted the mailing list of the Anti-drop" club and created a specific phishing email for its members.

On December 18, 2015 the Buhtrap group started sending emails from the mironova.olga@gazprombank.com.ru address with the subjects "Urgent! Updated drop database" and "Updated drop database" (pic. 7). These emails contained a link to the malicious file hosted on a website with the fraudulent domain gazprombank.com.ru.

When the user followed the link, the document started loading, which, when opened, provoked a chain of processes with the similar scenario to that in the case of the Central Bank letters.

Banks security officers soon realized that these emails were fraudulent and had informed all club members about the incident, these actions reduced the attack efficiency to zero.

Picture 7. *Screenshot of the phishing email on behalf of the Gazprombank*

SECOND SPEAR-PHISHING ATTACK ACTING AS THE CENTRAL BANK

In January 2016 criminals returned to the scheme of sending emails acting as the Central Bank but with vacancies and offers included.

On January 29, 2016 Group-IB's Bot-Trek Intelligence system detected an email sent from the address vakansiya@cbr.ru.net with the subject "Vacancy in the Central Bank" (pic. 8). The email contained the MS Office "Vacancy_34" document attached with an instruction on how to enable macros. In case the macros run successfully, the vacancy text appeared. An example of such instruction is presented in the "Methods of distribution" section.

Once macros were enabled, the malware started checking the victim's system. If the system locale was Russian or Ukrainian and specific conditions were met, then the malware installed and launched the file form the Buhtrap archive.

The file then installed **LiteManager**, a tool that allows remote control of a system and the **Guide** program which was used to load the basic module. This module handles C&C communications, installs a keylogger and enumerates smart cards present on the system. The Guide program is legitimate software usually used to create documents.

Once at least one host was infected by a phishing email hackers launched the malware operating like a worm, which Group-IB dubbed **BuhtrapWorm**. This worm was the very tool which provided survivability of the Trojan in the system.

Picture 8. *Screenshot of the phishing email acting as the Central Bank*

TACTICS OF BUHTRAP ATTACKS AGAINST BANKS

1. After initial intrusion into the company's internal network criminals used remote access to install and launch the module responsible for the survivability of the Trojan and multiple infections of the host inside the bank.

2. Hackers collected credentials of domain accounts using a modified version of the Mimikatz program.

3. The malware searched for the systems with the AWS CBC software installed.

4. Once obtained access to AWS CBC, the malware replaced payment documents addressed to the Central Bank, which then processed them.

5. Infected working stations inside the bank were disabled to complicate collecting evidences.

In the Buhtrap case, we can observe that criminals always search for working stations with AWS CBC. We have not detected incidents involving online money transfer systems, ATM machines or payment gates which are known to be of interest for other criminal groups.

It is worth analyzing separately the process of transfer order replacement in AWS CBC, since a major part of banks do not pay sufficient attention to this software security.

Automated Working Station of the Central Bank Client (AWS CBC) is a complex software designed to deliver payment documents on behalf of the Central Bank according to Unified Formats of Electronic Bank Messages (UFEBM) in payment batches.

AWSCBC is freely available on the Central Bank official website, and any user can download it and test its functions.

The initial configuration procedure is performed during the first start of AWS. It includes installing storage options for payment documents and adding users. The storage parameters recorded in a file with a name like "< computer name > .cfg" in the subdirectory of the cfg directory where AWS CBC is installed. The configuration file in XML format is readable to anyone who connects to AWS CBC. While installing, the storage method for payment documents can be specified:

Picture 9. *Selection of the data storage type for UFEBM*

In the incidents investigated by Group-IB the "file type" of storage was used. This means that electronic messages sent in the UFEBM format (which description is also publicly available on the website of the Central Bank), are stored in the directory specified during the configuration procedure and automatically extracted to be processed in AWS CBC software. The example of payment batch is presented below:

Picture 10. *Example of the document in the UFEBM format*

Thus, to create a payment batch the criminal needs to know client credentials to gain access to the directory, from which AWS CBC takes files for processing. He can copy the content of the previous batch and change the content of the necessary fields. This way it happened in cases observed by Group-IB.

For other types of payment document storage, the criminal needs to know credentials to access the relevant database. The procedure of creating the payment batch is similar.

Also, the criminal can add his payment order to the already formed batch, changing content of the relevant file or a record in the database.

Following the Central Bank recommendations also published on the regulator's website, the bank can use the System of the electronic document cryptographic authorization "Signature" software, which checks the AWS CBC integrity and allows users to sign payment documents delivered in the Central Bank. However, it is not able to prevent such an attack: substitution of payment documents does not break the AWS CBC integrity and the software, in fact, it protects documents already changed by criminals.

The AWS CBC software itself does not verify the integrity of documents to be delivered as well as data validity for the payment sender and receiver. Thus, the payment batch is created by the criminal before its delivery to AWS CBC. Moreover, the criminal does not even need to provide reliable data.

Since August 2015 Group-IB specialists have detected incidents of new malware use in corporate networks infected by the Buhtrap malware operating as a worm which Group-IB analysts dubbed **BuhtrapWorm**.

STAGES OF THE BUHTRAPWORM DISTRIBUTION

1. Start distributing the software in the corporate network criminals need to run the main module on one of the network computers, which are connected under the domain administrator account.

   The main module is executed and stored in the computer memory. Through reading memory of the process "lsass.exe" it extracts logins and corresponding passwords for all client sessions on the current computer (the operation is similar to the functionality of the software **Mimikatz**).
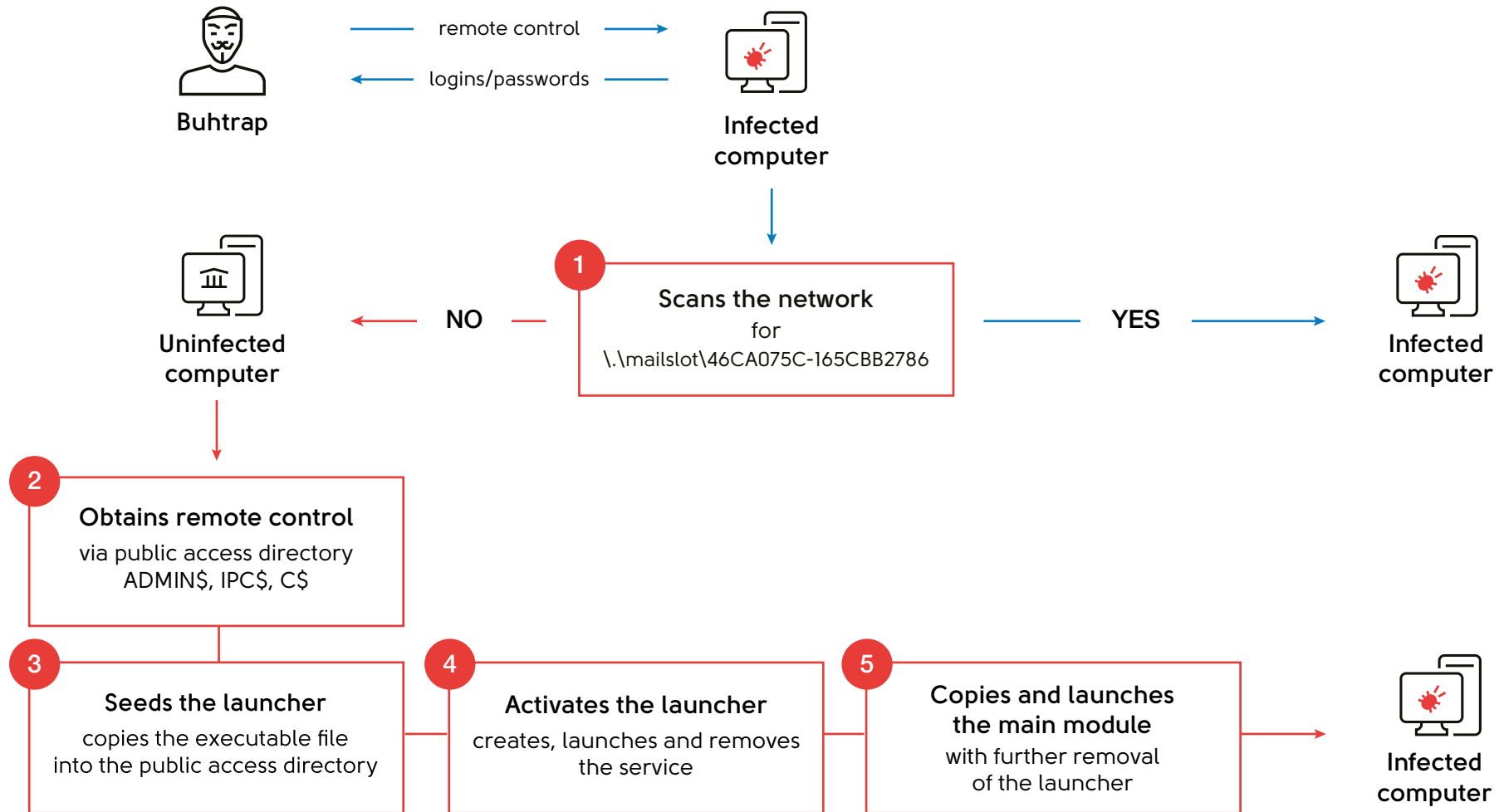
   The module scans the network for the mailslot object with the specified name "**\\.\mailslot\46CA075C165CBB2786**". The object with this name serves as an indicator of infection.

2. If this module is not present, the connection is carried out to the computer via a public access directory using the extracted login and password pairs "\ADMIN$", "\ipc$", "\C$" can be used as public access directories.

3. If the connection is successfully established, the launcher is copied in such directory (by default, this directory is "C: \ WINDOWS") in the form of an executable file.

4. Then a service with a random name is created on the uninfected computer with the path to the launcher set up. The malware sends a command from the infected computer to the uninfected computer to launch the service activating the module. After that this service is removed from the system.

5. The infected computer is used to copy the payload module in a "<launcher name> .dat" file or in a pipe object with the specified name (unique for each computer). The launcher copies and launches the main module. After that, the launcher is removed from the system with the file content overwritten.

After infecting a new computer, the malware is spread in the same way. Thus, **it takes a few minutes to create a self-maintaining botnet inside the corporate network**.
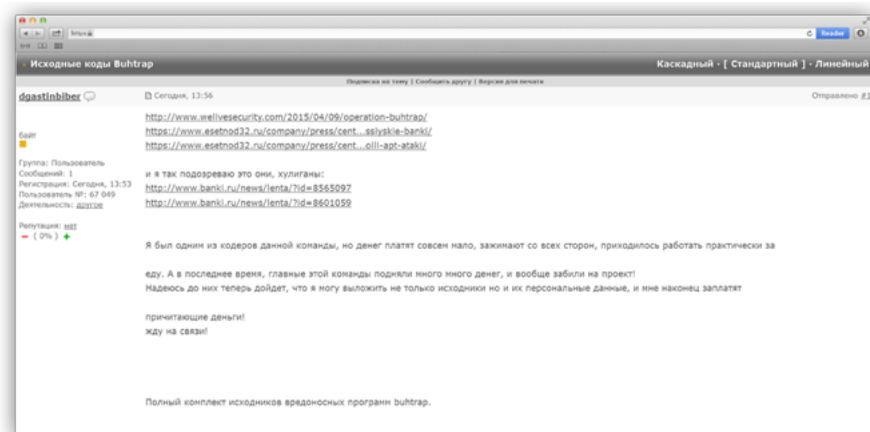
STAGES OF THE BUHTRAPWORM DISTRIBUTION

Buhtrap

remote control

logins/passwords

Infected computer

Uninfected computer

1

NO

Scans the network
for
\.\mailslot\46CA075C-165CBB2786

YES

Infected computer

2

Obtains remote control
via public access directory
ADMIN$, IPC$, C$

3

Seeds the launcher
copies the executable file
into the public access directory

4

Activates the launcher
creates, launches and removes
the service

5

**Copies and launches
the main module**
with further removal
of the launcher

Infected computer

The main module both contributes to spreading worm and exploits the operating system vulnerabilities to improve the rights and privileges in the system, as well as communicates with the control server providing the ability to remotely connect via RDP protocol to the infected computer. Each infected computer in the network is accessible from the outside via RDP.

At the moment antivirus software can detect only the launcher which itself is no threat. Moreover, its removal does not lead to removal of malicious program from the computer.

In case of malware operation errors, the service or the launcher may fail to stop or be removed, and then they can be stored in the infected system in a large amount.

After restarting the computer, the memory contents are erased together with the main module. Thus, if at least one computer in the company's network is infected by the BuhtrapWorm malware, all other computers will be infected again and again after the reboot.
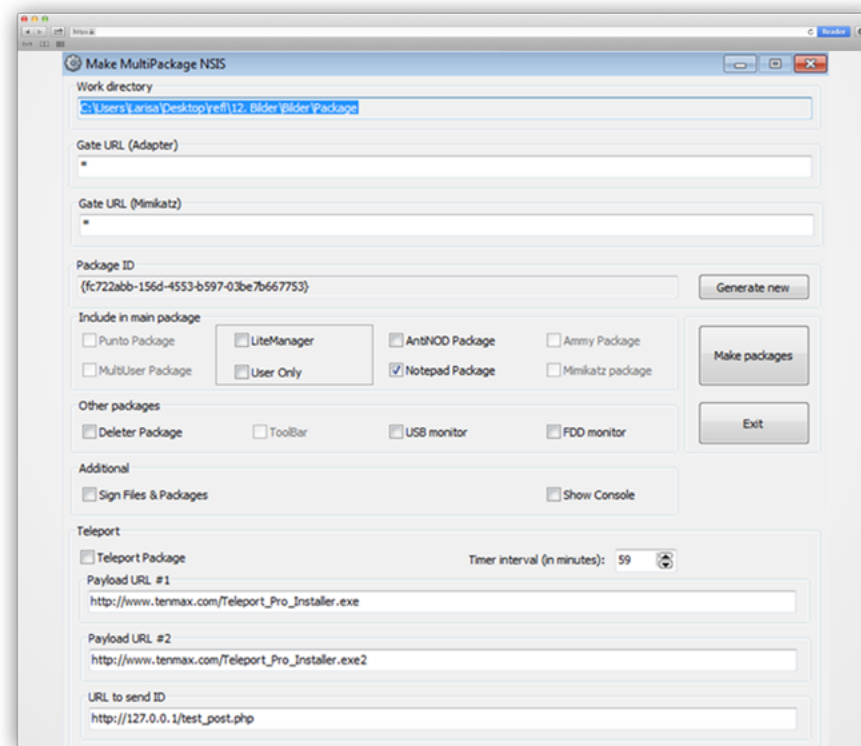
On February 5, 2016 a message with the link to Buhtrap source code download was published on the underground forum "exploit.in". The author claimed that he was a member of the Buhtrap group (pic. 11). However, since he allegedly hadn't been paid for developing the project, he decided to publish all source codes of the malware in open sources. The codes were packed in password protected RAR archive and placed on the file hosting Sendspace.

Picture 11. *Message on the hacker forum with Buhtrap source codes*

Based on the archive content, this version of source codes relates to the period from summer 2015 to early fall 2015. This is evidenced by absence of codes for the "psexec" module and other programs involved in the latest crimes of the Buhtrap group.

The published source codes are active. Their wide distribution may trigger the increase in the number of attacks using this malware conducted by other groups. The builder interface is presented below.

Picture 12. *Screenshot of the Buhtrap builder*

PUBLISHED MODULES

- **BHO** — a module designed to replace pages in the Internet Explorer browser.

- **Kill_os** — a module designed to delete the master boot record (MBR). There is an option of specific actions in the system.

- **«Damagewindow»** — a fake window which will run after the MBR record is damaged requiring the user to reboot the system due to the internal error.

- **Loaders** — builders of NSIS scripts designed to install malware. There is also an option of opening documents after successful command execution.

- **Mimimod** — a modified version of the mimikatz program, used to obtain user credentials in the system.

- **ID** — an algorithm for obtaining the unique number of the infected machine.

- **BSShide** — a module designed to hide payment orders in the BSS system. It modifies the page displayed to the user.

- **Antidetekt** — a module designed to detect virtual environment, "sandboxes".

- **UAC** — a module to bypass the UAC protection.

- **RDP** — it modifies the OS for potential simultaneous operation of several users in the system.

- **VNC** — remote PC control with backconnect.

- **DLL Side-Loading** — the basic module. It installs a keylogger, a smart card in the system, provides communication with control panel and enables installation and operation of other modules in the system. According to its author, it contains modules bypassing anti-virus software and firewalls.

- **Control panel**.

- **Builder** — a program designed to collect module in one executable file.

Also this archive contains a variety of the **MWI exploit kits**. Exploit kits are grouped by vulnerabilities they exploit:

- CVE-2012-0158, CVE-2010-3333
- CVE-2013-3906, CVE-2012-0158, CVE-2010-3333
- CVE-2014-1761, CVE-2013-3906, CVE-2012-0158, CVE-2010-3333

Absolutely all targeted attacks against banks could have been detected and stopped at any stage. Below you will find simple recommendations which enable you to prevent threats more effectively.

PREVENTION AT THE INTRUSION STAGE

The key method of intrusion into the bank's network is sending phishing email with an attachment containing the exploit, document with macros, or executable file in the password protected archive.

To prevent infection resulting from the exploit operation it is enough to update Microsoft software regularly. The Buhtrap group didn't use zero day vulnerabilities; moreover, their exploits were old. **That's why even standard software updates didn't allow attackers to gain access to the corporate network**. Some attacked banks are known not to have taken these security measures.

In cases when hackers faced with updated software they sent emails without exploits but with specific documents containing macros which designed to download and launch the malware.

In this event the infection was not conducted automatically and required participation of the bank employee. By default, execution of such macros is blocked by Word, Excel, PowerPoint and to enable them the user should allow their execution following instructions of the criminal.

To prevent such types of malware infection **it is sufficient to switch off execution and unlocking of macros in the settings using group police for specific user categories**. Also, it is necessary to notify users that enabling macros can result in a malware infection.

If the computers had necessary updates and users did not follow instructions of the hackers, the attackers sent attachments with the executable file in the password protected archive. Such **attacks are easy to block by quarantining such emails for further analysis**.

PREVENTION AT THE IMPLEMENTATION STAGE

Even if the criminals have managed to obtain access to the corporate network, the attack can still be successfully prevented. After intrusion into the company's network hackers still need to find systems of their interest, obtain access, and prepare the scheme of cashing money. It takes days and even months sometimes, and this time should be used to detect the malicious activity.

Criminals use malware which transmits data to the C&C server. These **network interconnections between the infected computer and the remote server can be identified by analyzing the network traffic**. There are specific solutions such as IDS/IPS and more complex systems designed for such identification.

If you don't have such solutions or use tools of the companies which do not monitor activity of such criminal groups, **it is essential to use the cyber intelligence data provided by various suppliers and perform monitoring by**

indicators. Indicators for the Buhtrap group you will find in the next section of this report.

In addition to the malware, the hackers use **remote control tools which can be identified by anti-virus software**.

And the most important thing: if you have detected trails of a targeted attack at any stage, you need to involve specialized companies for its analysis. Incorrect responses to the attack results in the attacker activity remaining partly undetected to enable criminals achieve their goal — to steal money.

Buhtrap NSIS
http://playback.savefrom.biz/video/video_1.cab
http://download.sendspace.biz/file/install.cab
http://194.58.100.211/install.cab
http://download.source-forge.name/file/program.cab
http://cams.web-filecab.info/cams/video2.cab
http://cache-datamart-windows.com/source/source.cab
http://check-mate7.com/kliko/res1.cab
http://new.pikabu-story.com/file/file2.cab
http://game.sport-box.org/dcim/install.cab
http://gazprombank.com.ru/dropi/baza_dropov.xls
http://cbr.com.ru/vacansiy/вакансия_No36.zip

Buhtrap C&C
http://google997.com/info/menu.php
http://autopiter.biz/info/menu.php
http://google9971.com/info/menu.php
http://microsoft7751.com/info/menu.php
http://compatexchange-cloudapp.net/help/menu.php
http://mp3.ucrazy.org/music/index.php
http://uchet.grandars.info/info/menu.php
http://ndfl.pravcons.biz/info/menu.php
http://rss.sport-express.biz/info/menu.php
http://forum.ru-tracker.net/info/menu.php
http://microsoft775.com/info/menu.php
http://icq.chatovod.info/info/menu.php
http://yaf.buhgalter911.biz/topics/menu.php
http://forum.zaycev.biz/info/menu.php
http://res.buhgalter911.info/info/menu.php

http://football.championat.biz/info/menu.php
http://tvit.live-journal.info/info/menu.php
http://rs-term.org /res1/menu.php

Mail servers
mail.cbr.ru.com
mail.cbr.ru.net
cbr.ru.com
cbr.com.ru
cbr.ru.net
gazprombank.com.ru
213.159.215.119

LiteManager C&C
forum.buhgalt.net
forum.buhnalog.org
forum.glavbukh.net
tv.hdkinomax.org
rus-gazeta.biz
setting-sandbox-microsoft.com
89.108.101.61
193.124.17.223
37.140.195.165
37.143.12.190
5.63.159.32
194.58.97.249
178.21.10.33
151.248.125.251

Bot-Trek Intelligence subscribers are always on the forefront and were made aware of the recent Buhtrap spear-phishing emails the same day they were sent. Additionally, reports included both mailings details and payload analysis. The data we provided proved vital in preventing attacks against clients exposed to Buhtrap risks.

We help to prevent and investigate cyber attacks at every stage, from reconnaissance or preparation to threat actors taking actions to achieve objectives. Furthermore, we prevent the spread of the attack and ensure that your infrastructure is clean of the presence of infection.

Bot-Trek Intelligence

Learn about threats, leakages, attacks, and hacking activity before they can harm your business

Bot-Trek TDS

Detect malicious incidents in your internal network to prevent attacks, intrusions, data leaks, and espionage

Incident Response

CERT-GIB – 24/7 emergency response and effective incident management

Computer Forensics and Investigations

The largest computer forensics laboratory in Easter Europe, with an experienced investigation team

ABOUT GROUP-IB

Group-IB is one of the global leaders in preventing and investigating high-tech crimes and online fraud. Since 2003, the company has been active in the field of computer forensics and information security, protecting the largest international companies against financial losses and reputation risks.

We are recognized by Gartner as a threat intelligence vendor with strong cyber security focus and the ability to provide leading insight to the Eastern European region and recommended by the Organization for Security and Co-operation in Europe (OSCE). Learn more on group-ib.com or get in touch now +7 495 984-33-64.