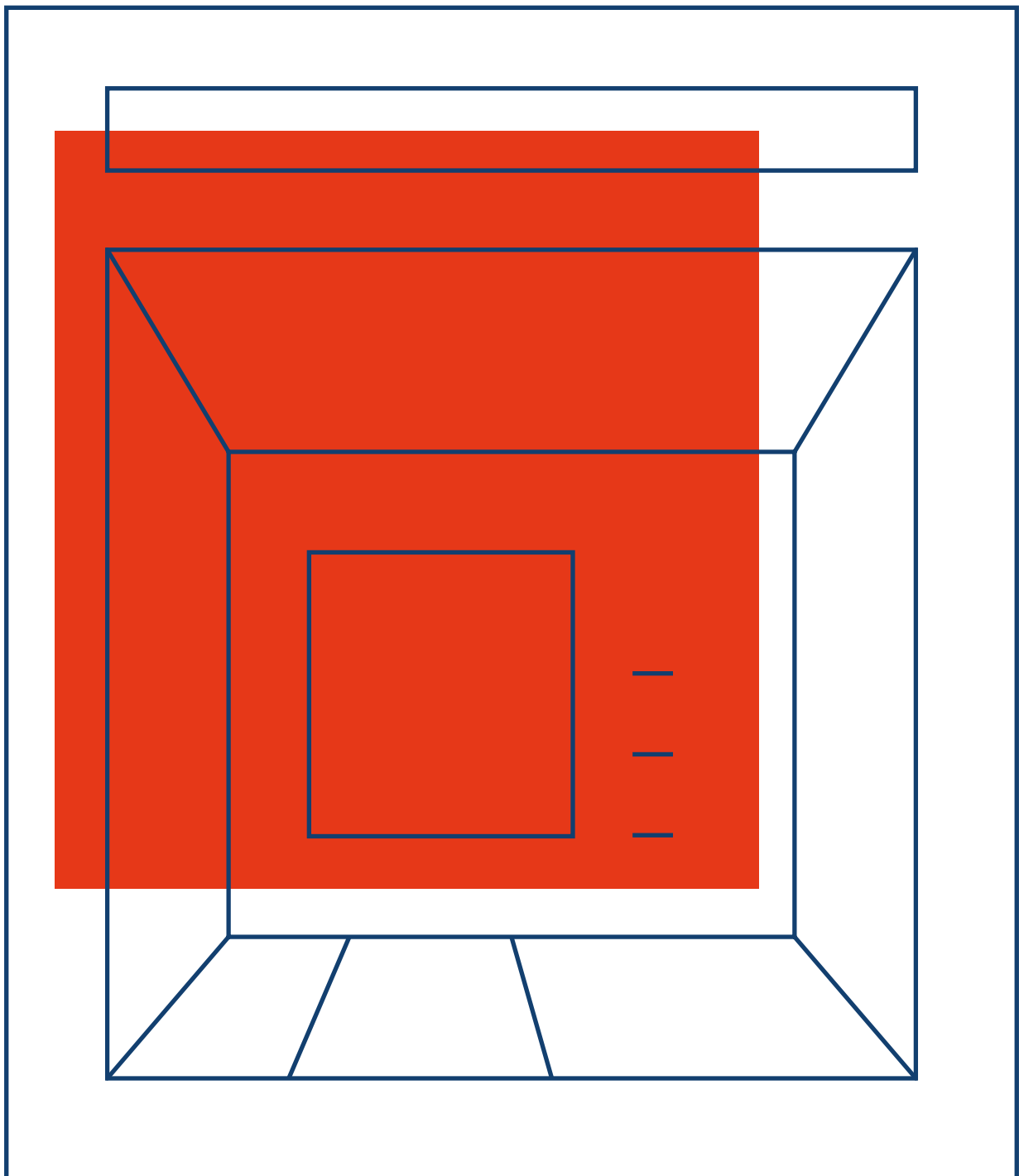


COBALT

Logical attacks on ATMs



Introduction	3
Key findings	5
Infection	9
Provision of the malware survivability	13
Gaining privileges	15
Consolidating control	20
Attack on ATMs	22
Links to Buhtrap	28
Recommendations.....	29
IOC	31

In July 2016, a group of masked cyber-criminals cashed out 34 ATMs operated by the First Bank, one of Taiwan's largest banks. The perpetrators stole T\$83.27 (over \$2m USD). **The criminals did not physically damage the ATMs, nor did they use skimmers or bank cards.** According to CCTV footage, the thieves used cellphones to trigger the ATMs to automatically dispense money.

Following this, criminals used a similar scheme in August to steal 12 million baht (around \$350,000 USD) from the Government Savings Bank ATMs in Thailand. In September, the same kind of attacks were detected in Europe; however, this fact was not made public.

Cybercriminals use a number of physical methods to conduct attacks on ATMs: skimming, shimmying, card trapping, ATM thefts and physical access have become common. However, these methods allow criminals to cash out only a single ATM and leave behind a large amount of evidence.



Criminals are actively seeking ways to reap ever-greater rewards and to lower risks: they have accordingly refocused their activity from physical threats to logical attacks.

To perform a logical attack, hackers access a bank's local network, which is further used to gain total control over ATMs in their system. Cash machines are then remotely triggered to dispense money, allowing criminals to steal large amounts with relative ease.

With full control over ATMs, criminals can choose the exact attack time to loot newly filled ATMs. This results in millions of dollars lost, as in the case of the First Bank. That said, such attacks do not require developing expensive advanced software – a significant amount of tools used by the hackers is widely available from public sources, as will be further covered later in this report.



This summer's wave of attacks appears to have been only a test to assess the potential of logical attacks on ATMs. This is expected to become one of the key vectors of targeted attacks on banks.

This report outlines how a currently active gang accesses cash machines by infecting internal banking infrastructure in Western and Eastern Europe, the CIS and the Asia-Pacific region.

A criminal group, which Group-IB has dubbed Cobalt because of the framework they use, has been **active since June 2016**. Their key target are ATM control systems.

Geographical distribution

As of September 2016, Cobalt has attacked banks in Russia, the UK, the Netherlands, Spain, Romania, Belorussia, Poland, Estonia, Bulgaria, Georgia, Moldova, Kyrgyzstan, Armenia, and Malaysia.

Infection vector

To get into the bank's internal network, hackers use spear phishing emails with a malicious attachment. **The emails purport to come from the European Central Bank, the ATM maker Wincor Nixdorf, or local banks.**

Criminals send emails with attachments containing exploits and password-protected archives with executable files. In the attacks, phishing emails were sent from virtual servers, which had installed an anonymous mailing script "yaPosylalka v.2.0" (another name of the service is "alexusMailer v2.0") developed by Russian-speaking cyber-criminals.

Intrusion

Instead of spending money to develop customized Trojans, criminals use **Cobalt Strike**, a legitimate program designed to perform penetration testing. To compromise domain and local accounts, hackers use the Mimikatz tool or exploit a domain controller configuration error.

The methods criminals use to deliver phishing emails and to obtain control over a domain controller are identical to those used by the Buhtrap group, which has conducted successful attacks against Russian banks, amounting to a total of 1.8 billion rubles (\$25m), from August 2015 to January 2016 (their activity was covered in Group-IB's report published in March 2016).

It takes anywhere between 10 minutes and a week to obtain complete control over a domain controller.

After the group's members were arrested in May 2016 while laundering money, the Buhtrap botnet was sold to other hackers, who are continuing attacks on Russian and Ukrainian companies.

Purportedly, at least a part of the Buhtrap group became Cobalt members, or more likely Buhtrap core members shifted their focus to attacks on ATMs.

An ATM attack

To make ATMs give out cash, criminals launch malware using Extensions for Financial Services (XFS) standard. On command from the bank's internal network, the program starts dispensing notes until machines are empty.

After each successful operation, the program records a specific log (a file named disp.txt) with information on the number of banknotes dispensed from the ATM cassette. The operator sends this log file to the organizer, who uses this data to control the 'jackpotting' chain.

Once these actions are complete, hackers erase all malware traces using **SDelete**, a legitimate free tool available on the Microsoft website. The criminals also knock out internal bank servers using the MBRkiller malware capable of removing MBR (master boot record). Such a careful approach significantly complicates further investigation.

The program that makes ATMs spit out cash on demand is unique and is believed to be used by one hacker group only.

The criminals are known to have other malicious programs for attacks on cash machines; however, specialists have not managed to recover them.



The criminals are known to have other malicious programs for attacks on cash machines; however, specialists have not managed to recover them.

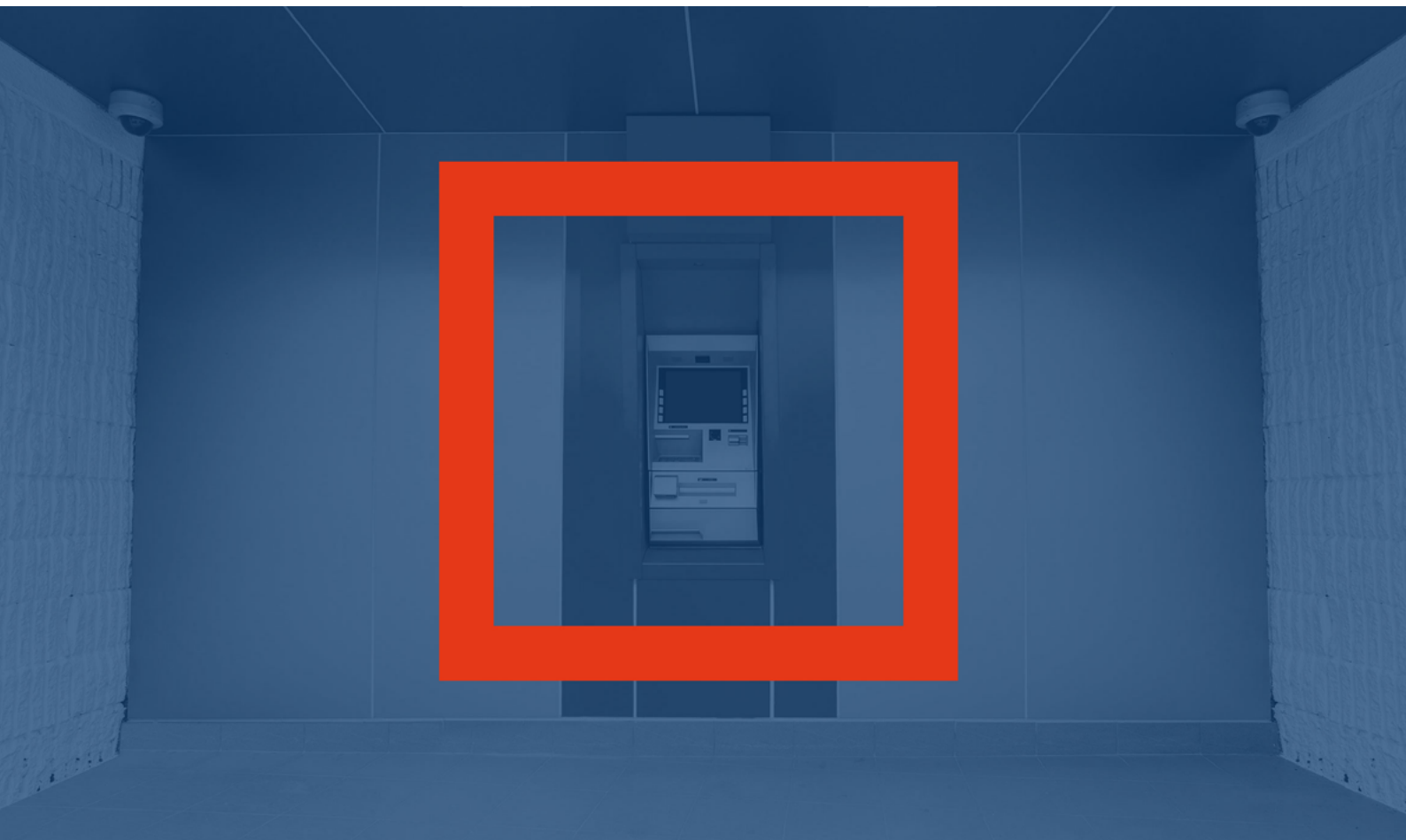
Recommendations

Logical attacks can be detected and prevented at any stage by following Group-IB's recommendations:

- use special systems designed to identify targeted attacks,
- send suspicious emails for dynamic analysis in an isolated environment,
- monitor new methods and attack tools using threat intelligence.

If you have detected trails of a targeted attack at any stage, you need to involve specialized companies for its analysis.

Incorrect responses to this type of attack will result in the bad actor activity remaining partly undetected allowing criminals achieve their goal – theft of cash.

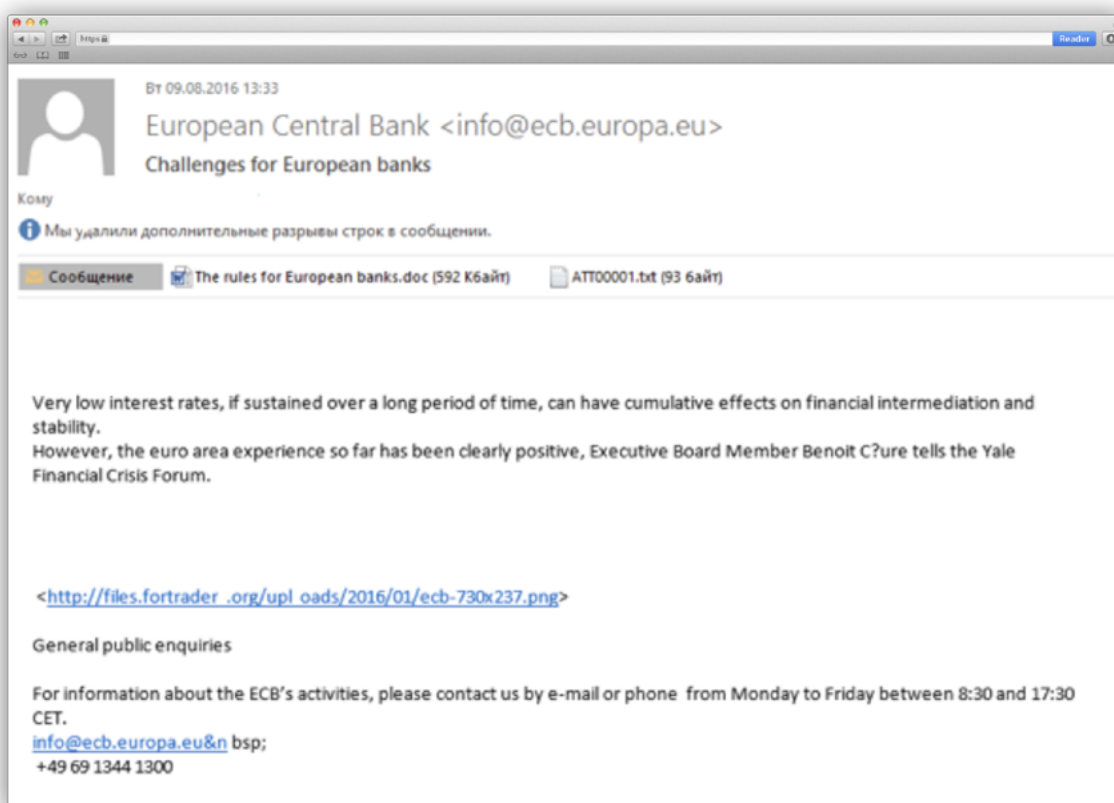


The main infection vector in bank networks are phishing emails with documents attached containing exploits and password-protected archives with executed files.

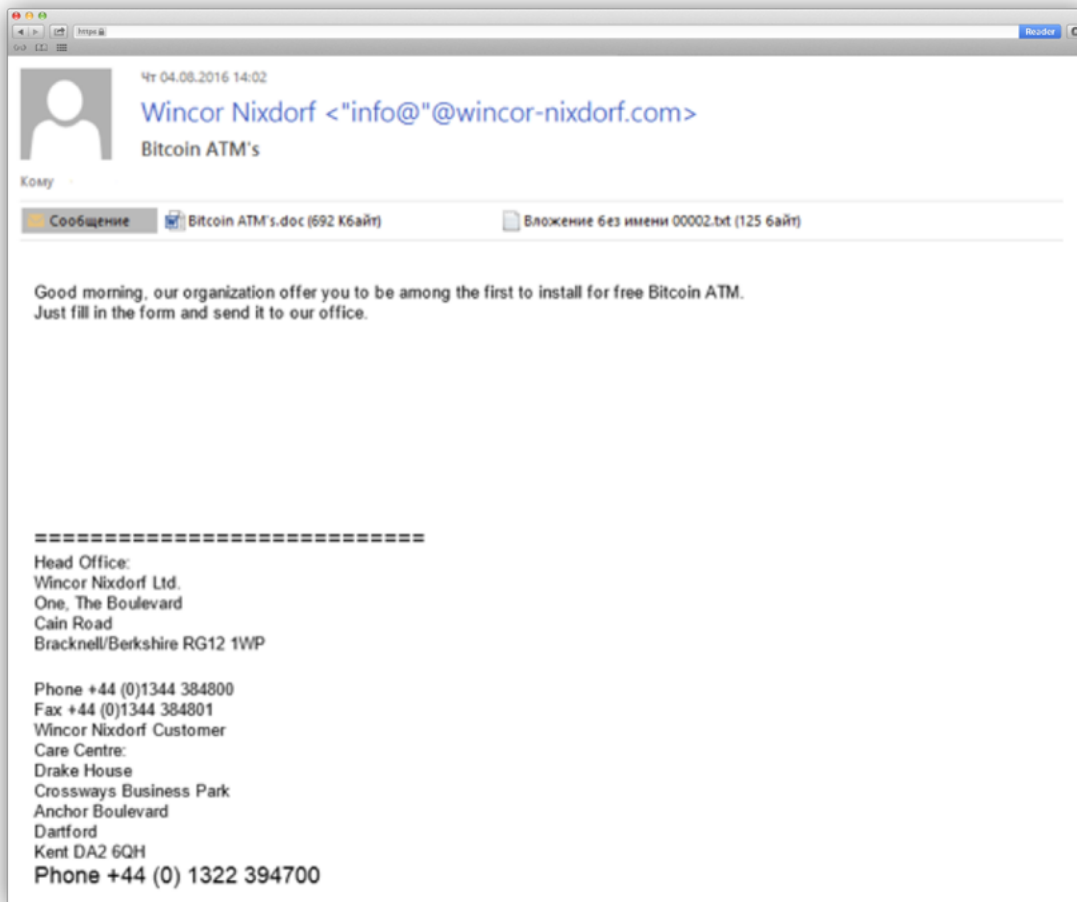
Criminals send emails acting as the European Central Bank, the ATM maker Wincor Nixdorf or local banks. Although the sender's address contains official domains, in fact the messages are sent from a server with a specific script changing the sender's address, while real banks and ATM manufacturers are not related to these mailouts.

In June phishing emails were sent from virtual servers with an installed anonymous mailing script "yaPosylalka v.2.0" (another name of the service is "alexusMailer v2.0") developed by Russian-speaking cyber-criminals.

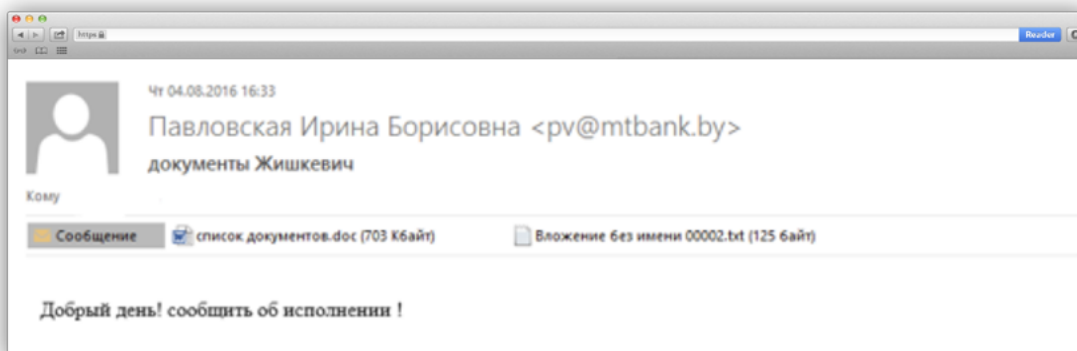
Then perpetrators started using Cobalt Strike software, as will be covered in this report.



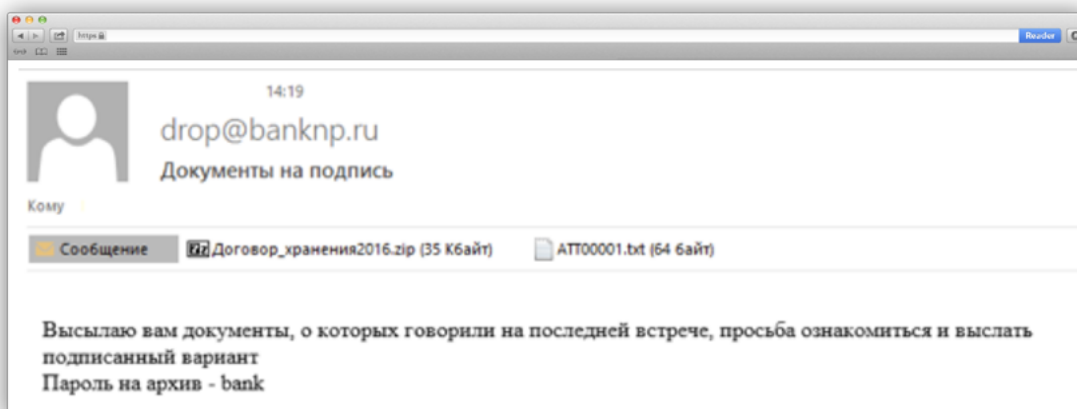
Picture 1. Phishing email posing as the European Central Bank



Picture 2.
Phishing email posing as
Wincor Nixdorf



Picture 3.
Phishing email posing as
a Belarusian bank



Picture 4.
Phishing email posing as
a Russian bank

Perpetrators sent emails from two servers with IP addresses 88.212.208.115 and 5.101.124.34. Both servers are located in Russia.

The methods used by criminals to deliver phishing emails are identical to those used by the Buhtrap group, which conducted successful attacks against Russian banks for a total amount of 1.8 billion rubles (\$25m) from August 2015 to January 2016.

2016



MARCH

The last confirmed attack on a bank conducted by the **Buhtrap group**



MAY

Arrest of the group laundering money for **Buhtrap**



JUNE

The first attack on a Russian bank using **Cobalt Strike**



JULY

Attacks on banks in Armenia, Belorussia, Poland, Germany



AUGUST

Attacks on banks in Georgia, Belorussia, Romania, Kyrgyzstan, Poland, Estonia, Spain, the Netherlands, the UK, Malaysia



SEPTEMBER

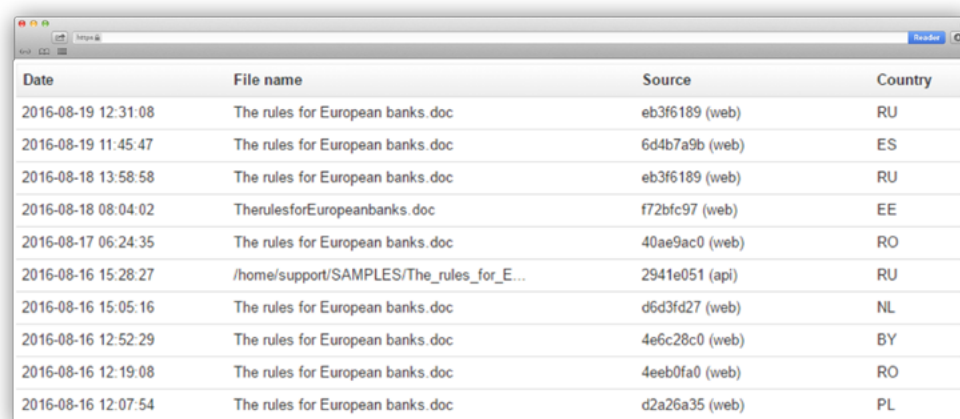
Confirmed thefts from ATMs outside Russia



Get a free copy of the report «Buhtrap. Evolution of targeted attacks on banks» on group-ib.com/reports

To distribute malware in the Russian-speaking bank segment, the criminals used attachments with the names “Договор_хранения2016.zip” (“Custodial_agreement2016.zip”) and “список документов.doc” (“document_list.doc”).

For phishing attacks in other countries they used the “The rules for European banks.doc” and “Bitcoin ATM’s.doc” files. The most widely-distributed file was a document sent acting as the European Central Bank in August 2016. An example of its upload to Virus Total is presented below.



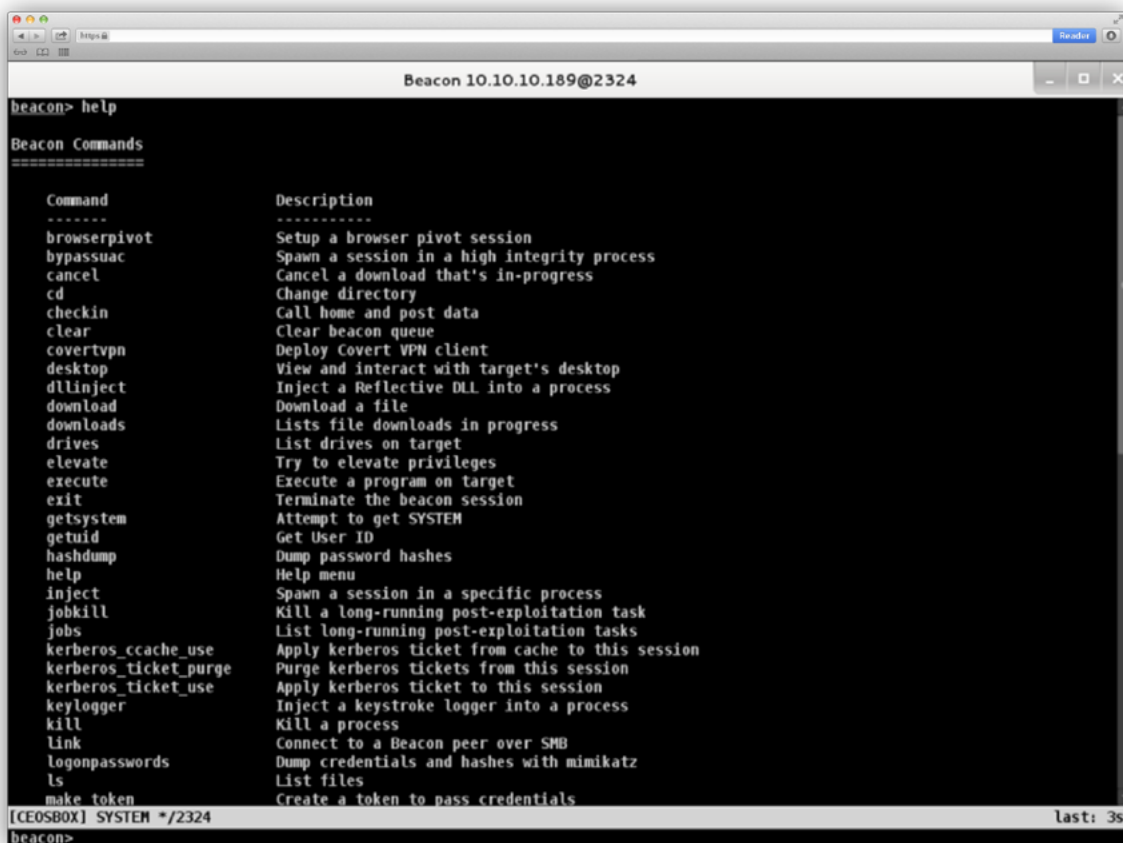
Date	File name	Source	Country
2016-08-19 12:31:08	The rules for European banks.doc	eb3f6189 (web)	RU
2016-08-19 11:45:47	The rules for European banks.doc	6d4b7a9b (web)	ES
2016-08-18 13:58:58	The rules for European banks.doc	eb3f6189 (web)	RU
2016-08-18 08:04:02	The rules for European banks.doc	f72bfc97 (web)	EE
2016-08-17 06:24:35	The rules for European banks.doc	40ae9ac0 (web)	RO
2016-08-16 15:28:27	/home/support/SAMPLES/The_rules_for_E...	2941e051 (api)	RU
2016-08-16 15:05:16	The rules for European banks.doc	d6d3fd27 (web)	NL
2016-08-16 12:52:29	The rules for European banks.doc	4e6c28c0 (web)	BY
2016-08-16 12:19:08	The rules for European banks.doc	4eeb0fa0 (web)	RO
2016-08-16 12:07:54	The rules for European banks.doc	d2a26a35 (web)	PL

We discovered a part of the emails sent from these servers and analyzed malicious attachments. Group-IB specialists also identified related malware samples and checked from where malicious files were being uploaded to Virus Total at the time of attack. That allowed us to identify the list of attack targets, which includes banks in Russia, the UK, the Netherlands, Spain, Romania, Poland, Estonia, Bulgaria, Belorussia, Moldova, Georgia, Armenia, Kyrgyzstan and Malaysia.

After the malicious attachment is launched, the malware starts providing for its survivability in the system, as outlined below:

1. The email attachment contains **malicious RTF files** exploiting the CVE-2015-1641 vulnerability. That said, criminals use a standard shellcode generated by such penetration testing tools as Metasploit and Cobalt Strike.
2. If the vulnerability is successfully exploited, the **malicious module will inject a payload named Beacon into memory**. Beacon is a part of Cobalt Strike, which is a multifunctional framework designed to perform penetration testing. The tool enables perpetrators to deliver the payload to the attacked machine and control it. .

To stay undetected by standard IDS/IPS systems, Beacon creates covert channels using DNS, HTTP, HTTPS protocols for communication with the C&C server over covert channels.



```
Beacon 10.10.10.189@2324
beacon> help
Beacon Commands
=====
Command      Description
-----
browserpivot  Setup a browser pivot session
bypassuac     Spawn a session in a high integrity process
cancel        Cancel a download that's in-progress
cd            Change directory
checkin       Call home and post data
clear         Clear beacon queue
covertvpn     Deploy Covert VPN client
desktop       View and interact with target's desktop
dllinject     Inject a Reflective DLL into a process
download      Download a file
downloads     Lists file downloads in progress
drives        List drives on target
elevate       Try to elevate privileges
execute       Execute a program on target
exit          Terminate the beacon session
getsystem     Attempt to get SYSTEM
getuid        Get User ID
hashdump      Dump password hashes
help          Help menu
inject        Spawn a session in a specific process
jobkill       Kill a long-running post-exploitation task
jobs          List long-running post-exploitation tasks
kerberos_ccache_use  Apply kerberos ticket from cache to this session
kerberos_ticket_purge  Purge kerberos tickets from this session
kerberos_ticket_use  Apply kerberos ticket to this session
keylogger     Inject a keystroke logger into a process
kill          Kill a process
link          Connect to a Beacon peer over SMB
logonpasswords  Dump credentials and hashes with mimikatz
ls            List files
make token    Create a token to pass credentials
[CEOSBOX] SYSTEM */2324
beacon>
```

Picture 6. A list of commands for Beacon

3. If an email with exploit fails to achieve its goals, the attackers send another letter with a password-protected archive containing the same Beacon payload.

The payload is not saved as a file on disk but only exists in memory, which means **it cannot run after the system is restarted**.

To keep permanent control over the infected system, a specific Beacon module automatically runs a scan for applications included in autorun to substitute them with executable files with the same names.

In real attacks we observed that criminals replaced files named iusb3mon.exe (Intel(R) USB 3.0 eXtensible Host Controller) and jusched.exe (Sun Java Update Scheduler). As a result of such replacement, services automatically launch malicious apps instead of legitimate programs.

4. Hackers copy a library named crss.dll to the same directory where substituted .EXE files are located. Each time when the operating system starts, the replaced applications download this library into memory. The main goal of the library is to download the Beacon module into memory from the Internet.

That is how the Trojan survivability is ensured. After each restart, the basic module of the operating system is removed. All the abovementioned steps are performed automatically once a malicious attachment is launched.

However, it is still necessary for bad actors to establish permanent access to the local network, should the victim shut down the infected computer or reinstall the operating system. This requires privilege escalation.

To perform continuous reconnaissance of the bank's local network and gain access to isolated network segments and its information systems, the attacker needs domain administrator privileges. The methods used by hackers to gain these privileges are 100% identical to those used by the Buhtrap group.

Method No1 Domain controller configuration error

Starting with Windows Server 2008 an addition functionality – **Group Policy Preferences (GPP)** – was added to group policies. GPP enables administrators to apply a variety of policies, such as to automatically assign a network drive when the user logs into his computer, update the default administrator account name, create new users, or change the registry, etc.

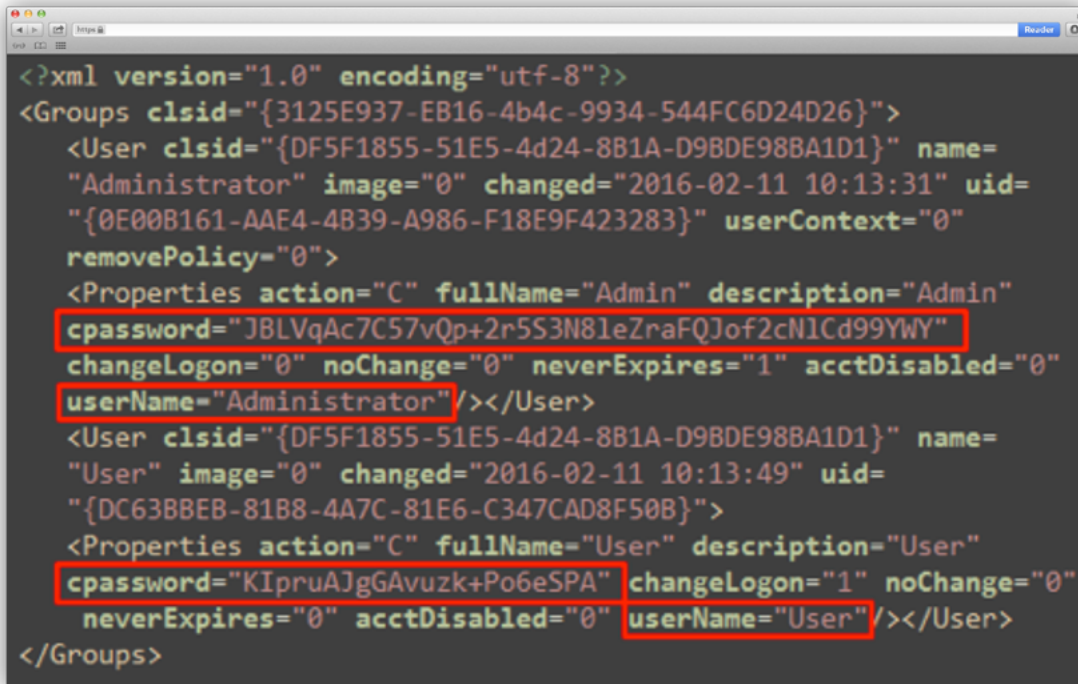
Actions such as adding a local user, connecting a network drive or printer may require a specified password. When such policies are added on a single computer, they will be loaded with the specified password. The password that is encrypted using the AES-256 algorithm and further coded using Base64 encoding, is stored in the GPP Groups.xml configuration file. This XML-file is created in specific cases, for example, when the default administrator account is created or modified.

The file is stored on the domain controller in a subdirectory of the "SYSVOL" directory and, like the directory, it is available to any user in the domain.

Attackers use Groups.xml to retrieve the domain administrator password as follows:

1. After obtaining access to the local network (the process is outlined in the previous section), the attackers detect domain controllers, which are specified in the computer settings.
2. When accessing the domain controllers, the hackers check the SYSVOL directory and the Groups.xml file, which is available via the following path: **«\\[server_name]\sysvol\[domain_name]\Policies\[group_policy_name]\Machine\Preferences\Groups\Groups.xml»**

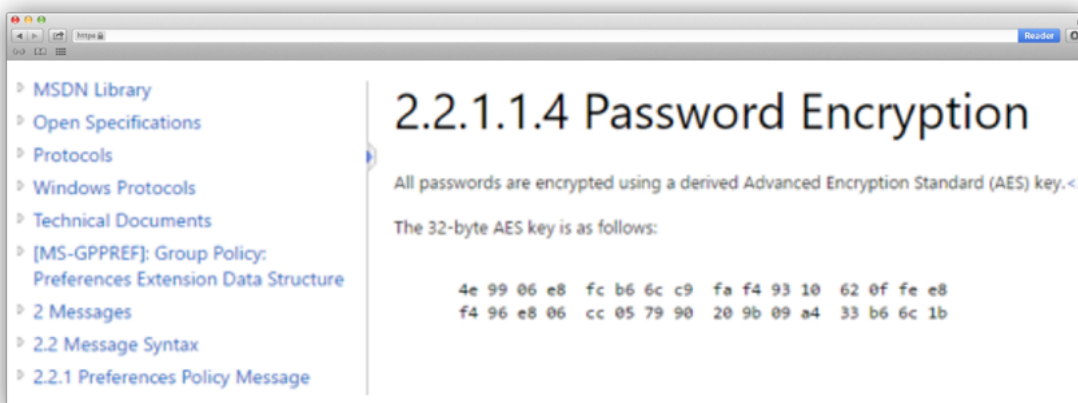
3. The perpetrators extract domain administrator credentials from the cpassword and userName fields in the Groups.xml file. The picture below shows how the encrypted password looks.



```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name=
  "Administrator" image="0" changed="2016-02-11 10:13:31" uid=
  "{0E00B161-AAE4-4B39-A986-F18E9F423283}" userContext="0"
  removePolicy="0">
    <Properties action="C" fullName="Admin" description="Admin"
    cpassword="JBLVqAc7C57vQp+2r5S3N81eZraFQJof2cN1Cd99YWY"
    changeLogon="0" noChange="0" neverExpires="1" acctDisabled="0"
    userName="Administrator"/></User>
  <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name=
  "User" image="0" changed="2016-02-11 10:13:49" uid=
  "{DC63BBEB-81B8-4A7C-81E6-C347CAD8F50B}">
    <Properties action="C" fullName="User" description="User"
    cpassword="KIpruAJgGAvuzk+Po6eSPA" changeLogon="1" noChange="0"
    neverExpires="0" acctDisabled="0" userName="User"/></User>
</Groups>
```

Picture 7. Fragment of the Groups.xml file

4. To obtain an unencrypted password the attackers decode it using Base64. They receive the following string **4e9906e8fcb66cc9faf49310620ffee8f496e806cc057990209b09a433b66c1b** – which is an AES-256 encrypted password.
5. This password is then decrypted using the key **4e9906e8fcb66cc9faf49310620ffee8f496e806cc057990209b09a433b66c1b**, published on the official website Microsoft MSDN.



Picture 8. Password encryption key published on Microsoft MSDN website

6. After the password is successfully decrypted, the hackers obtain access to the domain controller and using the method that is further covered in this report, they can access a password for any account.

With such configuration of the domain controller, it takes 10 minutes to access it.

Method No2 Mimikatz

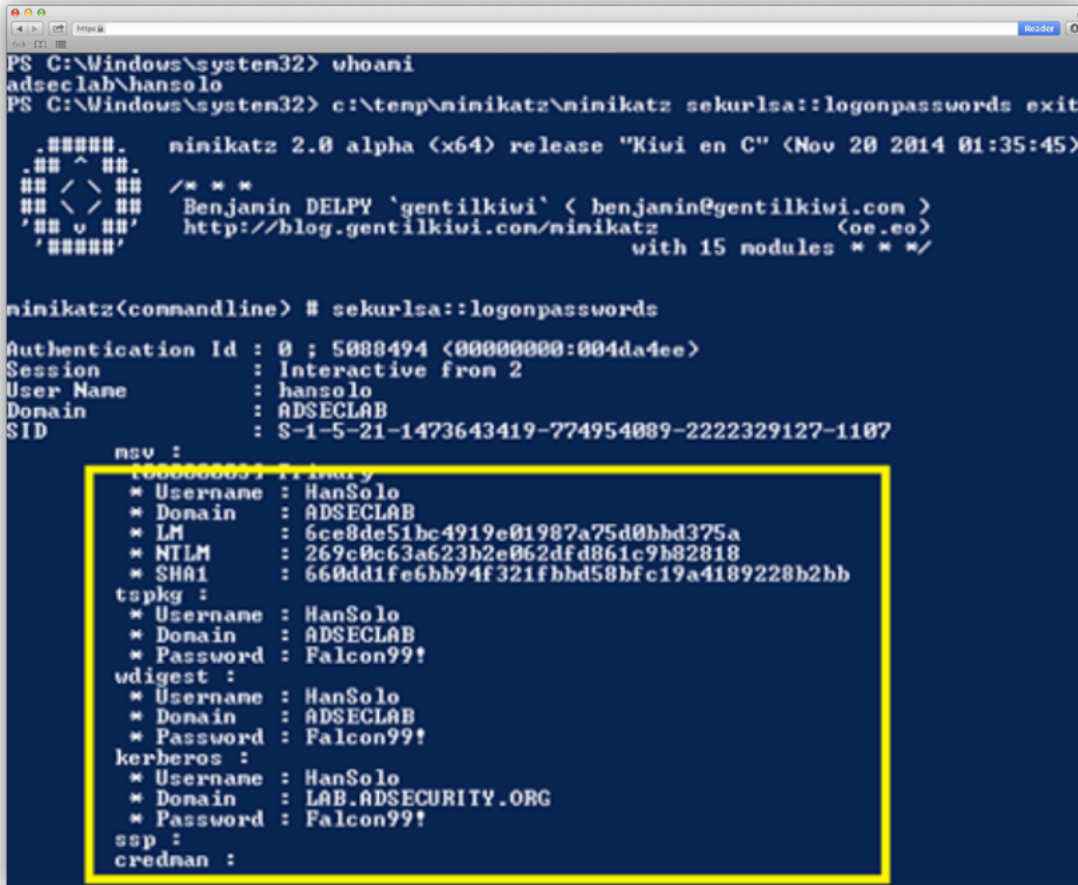
Mimikatz is a well-known tool designed to extract unencrypted Windows credentials for all client sessions through reading memory of the process "lsass.exe", which requires local administrator privileges. The Mimikatz source code is available on GitHub and built in to some penetration test tools, including Cobalt Strike.

If attackers have local administrator privileges and access to a domain controller

After attackers obtain access to a domain controller using method No.1, they launch Mimikatz on servers to collect unencrypted passwords for all administrators of a specific server. It was enough to run

mimikatz sekurlsa::logonpasswords

for all accounts and passwords to be displayed.



Picture 9.
Results of Mimikatz
operation

If the attackers already have local root privileges without access to a domain controller

When the attackers gets into the infected machine of an administrator, who does not have access to the domain controller, they connect to other workstations and servers with available account details and run Mimikatz until they find a user with necessary rights.

With local administrator privileges, attackers can access a domain controller within 1 working day.

If the attackers do not have local administrator rights

As mentioned before, to run Mimikatz criminals need to access the lsass.exe process, which requires local administrator rights. If initial access is obtained by compromising an account without local administrator privileges, the hackers start exploits to improve local privileges. When necessary updates and patches are installed on the operating system, the attackers connect to other hosts with this domain account and check them for vulnerabilities that would allow them to escalate privileges to local administrator level.

It takes from one day to one week to access a domain controller.

To improve the rights and privileges in the local system attackers exploit the operating system vulnerabilities CVE-2014-4113, CVE-2015-1701, CVE-2015-2363 and CVE-2015-2426, which enables the criminal to gain SYSTEM level privileges in x32 and x64 operating systems.

Mimikatz Golden Ticket

Group-IB specialists did not discover the use of the following method by Cobalt, because access to domain accounts solves all their problems, however **they might use it in future attacks**. The technique is to obtain a Golden Ticket, which gives maximum access to any domain account with minimum privileges.

Active Directory contains a system account krbtgt (Key Distribution Center Service Account). The KRBTGT account is disabled by default and cannot be renamed, removed or used to enter a domain.

With access to a domain controller, the attackers can copy the entire Active Directory database, for example, by running the command `mimikatz.exe "privilege::debug" "lsadump::samrpc /patch" exit` and extract NTLM hash of the krbtgt account.

With this hash and domain ID the criminals can use Mimikatz to create a file with a gold TGT ticket, which gives them access to any record in the domain.

After the abovementioned steps, the criminals have remote access to the network and privileges that allow them to perform any activity in the local network. The perpetrators then look for a way to consolidate their control of the local system to collect data and establish redundant access channels should their activity be detected and the security service take countermeasures.

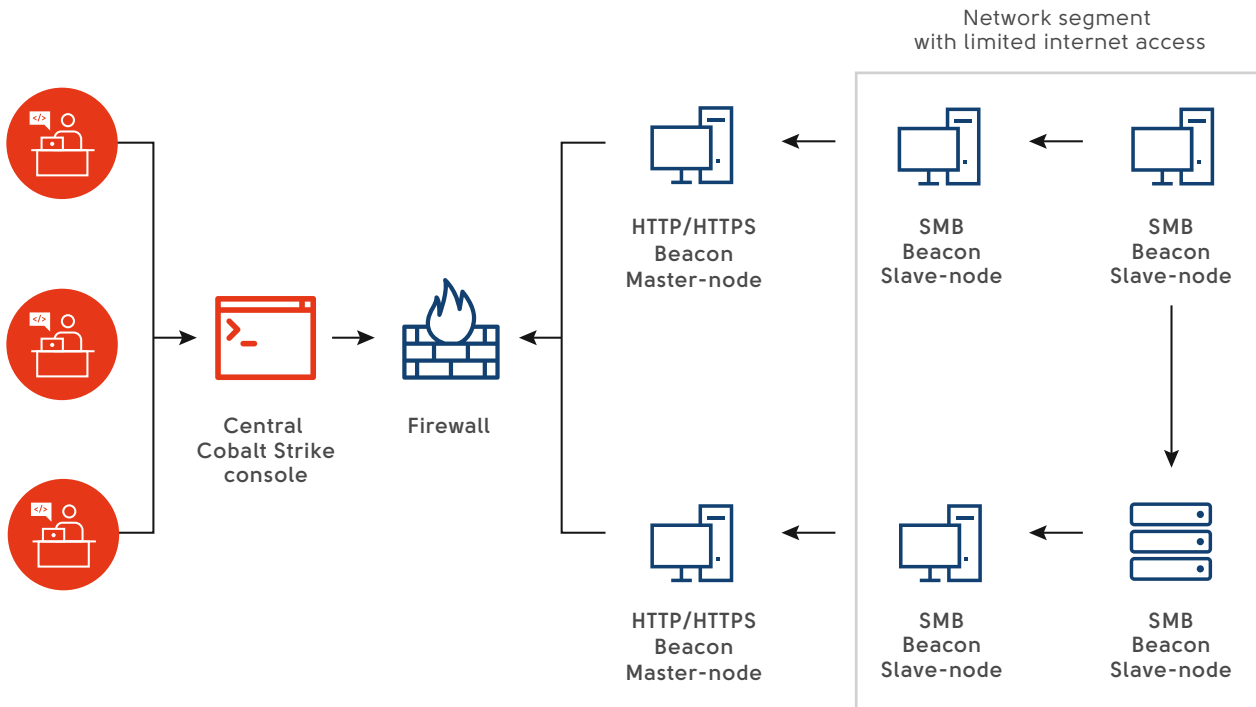
Consolidating control over the infected machine/server

Thus, the attackers have at least one host with Beacon. They need to have access to multiple computers, including those that do not have access to the Internet. To achieve this goal, they build their own mini-network of infected computers inside the bank's local network, which can be controlled through a single Cobalt Strike console installed on a remote server with the necessary functionality.

The process can be described as follows:

- Hackers launch a Beacon version on hosts with access to the Internet, which establishes a connection to the C&C server over a hidden channel. To prevent detection of these communications by standard IDS/IPS systems, Beacon uses DNS, HTTP, HTTPS protocols. They allow for interaction with other hosts in the local network. Let's call them **master-node**.
- Banks usually have isolated hosts without access to the Internet, these are of most interest to cybercriminals. Even if the host of a critical system has access to the web, any connections with a remote server will be suspicious for the security service. To control these kind of hosts without detection the attackers use a specifically modified version of Beacon, which can be controlled only over local network through SMB protocol via pipes. Let's call them **slave-node**.
- Cobalt Strike allows the attacker to connect the master-node and the slave-node through a dedicated channel over SMB protocol. Thus, the slave-node becomes available in the remote central control console of Cobalt Strike, which means that **isolated hosts gain access to the Internet through the master-node, which becomes a gateway for the slave-node**.

This scheme enables the criminals to build a sustainable mechanism of continuous access to the attacked local system while remaining undetected.



To kick the attackers off the network, the security service should at least identify all hosts that act as master-nodes, and remove them from the network simultaneously; **otherwise**, the criminals have a chance to restart their activity within a few minutes.

Creating a redundant access channel

After the local network and domain are successfully compromised, the attackers can use legitimate channels to remotely access the bank, for example, by connecting to terminal servers or via VPN acting as an administrator or a standard user.

Despite the fact that Cobalt Strike has a built-in VNC remote access module, the attackers try to secure their position further and download a modified version of the TeamViewer installer, which is a legitimate remote access tool. Group-IB specialists have not managed to recover a complete version of the installer. We believe that its key difference from the official app is hiding notifications of implemented remote connection to the computer, as in attacks conducted by other criminal groups in Russia.

According to video footage recorded by security cameras, the attack on ATMs was performed as follows:

- The thief came to ATMs with a mobile phone.
- He made a telephone call and prepared a bag.
- In a few minutes the ATM started to give out money in portions.
- When the ATM was empty, the criminal contacted partners and left the ATM.
- The ATM was then rebooted.

Money withdrawals were performed by small groups of individuals, who moved between predetermined ATMs to cash out money within a timeframe of a few hours.

This report will further outline the hacker activity performed beyond CCTV visibility.

Roles of group members

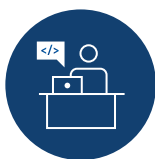
According to investigations of all incidents, hackers simultaneously attack several ATMs. It takes at least a few days to get inside the bank's system, compromise the entire network, understand from where ATMs can be accessed and evaluate how many cash mules are required to collect money. To support this process, the criminal group needs time and an organizational structure with roles and clear areas of responsibility.

ATTACK ORGANIZER



Attack organizers are the core of any group. Usually they consist of one or two criminals who develop the scheme, hire people, assign roles, and provide funding for the process. The most important task for the organizer is to control both operators and money mules, including the use of functional malware (see below).

OPERATORS



Are directly involved in breach of the bank's internal networks of banks. They send commands to ATMs to dispense money. Usually there are several operators, because they need to attack several banks simultaneously. Operators control the amount of dispensed money and report to the organizer.

CASH-OUT ORGANIZER

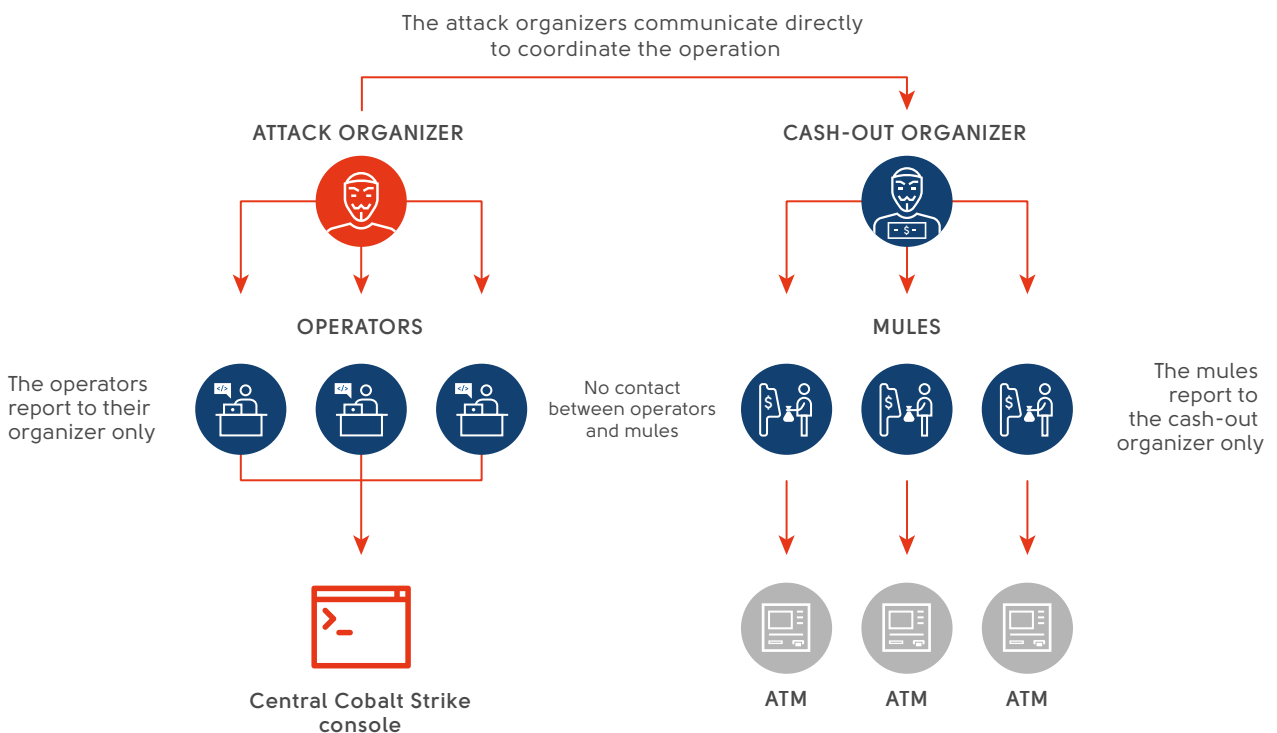


Interacts directly with the attack organizer without information about the operators. His task is to coordinate the actions of mules to withdraw money and control cashers. He is the person who money mules call to report on money received from the ATM. He then informs the attack organizer accordingly.

MONEY MULES (CASHERS)



Have with minimal technical skills and are not related to hacking banks. Their main aim is to withdraw money from ATMs and report to the cash-out organizer, who remotely controls their activity. It is the mules, who are arrested on evidence gathered from CCTV records.



A few days after the attacks on First Bank's ATMs, citizens of Latvia, Moldova and Romania were arrested in Taipei. At least 13 suspects including several Russian citizens managed to leave the island. Mules often visit a country using tourist visas specifically to perform an attack and then leave it as soon as the operation is over.

Gaining access to ATMs

After establishing control over the bank's internal network and creating redundant access channels, the criminals search network segments, from which they can gain access to ATMs, and workstations of bank employees who control ATMs.

With access to a necessary computer or server, the attackers use standard remote access tools applied in the bank. Usually, via Microsoft Remote Desktop Protocol.

Once access to ATMs is gained, they download a specific software to them, which allows criminals to control cash dispensers.

Software for attacks on ATMs

Once criminals obtain remote access to the ATMs, they upload three files:

- The del.bat script, which launches the SDelete program with required parameters.

Content of the del.bat script

```
sdelete.exe -accepteula -p 32 d2.exe  
sdelete.exe -accepteula -p 32 xtl.exe  
sdelete.exe -accepteula -p 32 *.txt  
sdelete.exe -accepteula -p 32 d2s.exe  
del sdelete.exe  
del del.bat
```

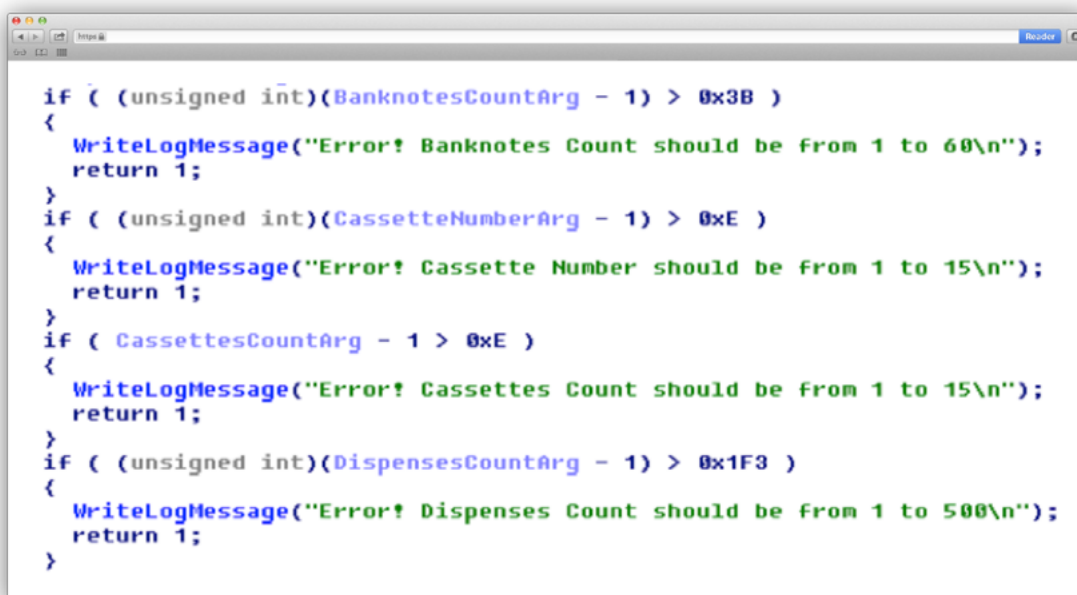
- A legitimate program, SDelete (available on the Microsoft website). This is designed to delete files in a special manner making it impossible to recover them with a forensic investigation.
- A malicious program that uses standard functions for the XFS interface via the XFS Manager (eXtensions for Financial Services). It is this program, which on command from the bank's internal network starts dispensing money.

The malware source code was not protected, which significantly simplifies its analysis and allows the criminal to adjust its operation. This means that the malware author did not plan its distribution and is likely a member of the attack group.

The malicious program allows the hacker to use XFS API in order to connect to an ATM dispenser and send commands to deplete cash cassettes. It operates in accordance with the arguments that are transmitted at startup. In total, there are five arguments, and the value for each of them should be specified.

Command line arguments should be added in the following order:

- **ServiceLogicalName** — a service name used as an argument for the WFSOpen function (for example, "Cash Dispenser Module").
- **Cassettes Count** — the total number of cassettes on the device. The value should be set in the interval from 1 to 15.
- **Cassette Number** — the number of the cassette, which should dispense cash. The value should be set in the interval from 1 to 15.
- **Banknotes Count** — the amount of banknotes to be dispensed from the cassette. The value should be set in the interval from 1 to 60.
- **Dispenses Count** — the number of times cash dispenses should be repeated. The value should be set in the interval from 1 to 60.

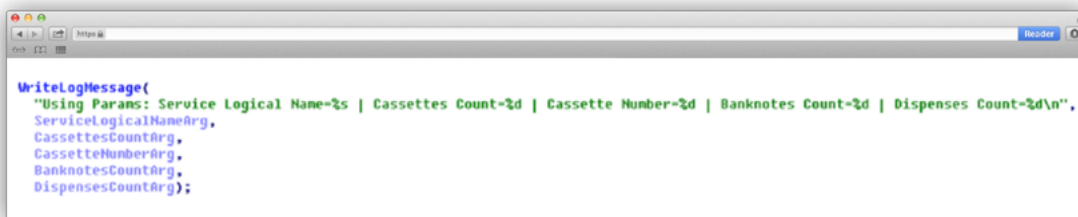


```
if ( (unsigned int)(BanknotesCountArg - 1) > 0x3B )
{
    WriteLogMessage("Error! Banknotes Count should be from 1 to 60\n");
    return 1;
}
if ( (unsigned int)(CassetteNumberArg - 1) > 0xE )
{
    WriteLogMessage("Error! Cassette Number should be from 1 to 15\n");
    return 1;
}
if ( CassettesCountArg - 1 > 0xE )
{
    WriteLogMessage("Error! Cassettes Count should be from 1 to 15\n");
    return 1;
}
if ( (unsigned int)(DispensesCountArg - 1) > 0x1F3 )
{
    WriteLogMessage("Error! Dispenses Count should be from 1 to 500\n");
    return 1;
}
```

Picture 10. A piece of code designed for parameter acceptance

All these values are indicated in the console by the operator, who is remotely connected to the ATM.

If these arguments are correctly transferred, a message with parameters of further actions will be displayed.

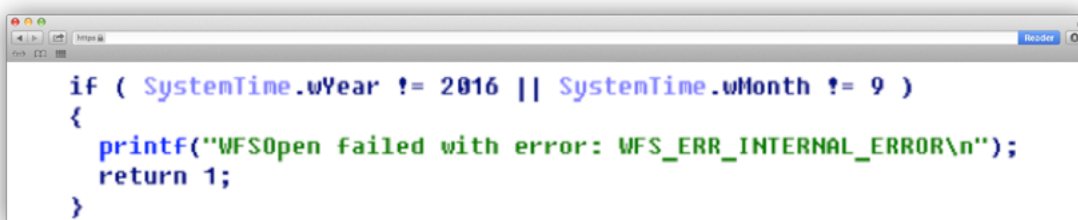


```
WriteLogMessage(
  "Using Params: Service Logical Name=%s | Cassettes Count=%d | Cassette Number=%d | Banknotes Count=%d | Dispenses Count=%d\n",
  ServiceLogicalNameArg,
  CassettesCountArg,
  CassetteNumberArg,
  BanknotesCountArg,
  DispensesCountArg);
```

Picture 11. A piece of code designed for log creation

Then an array is filled with each element corresponding to the cassette number on the device. The number of array elements should correspond to the total amount of cassettes. The value in each massive element means the number of banknotes that should be dispensed from a specific cassette. The counting of array elements starts from 1.

During its operation, the program receives information about system time. In the event it does not correspond to the time specified in the program code, the malware stops its activity.



```
if ( SystemTime.wYear != 2016 || SystemTime.wMonth != 9 )
{
  printf("WFSOpen failed with error: WFS_ERR_INTERNAL_ERROR\n");
  return 1;
}
```

Picture 12. A piece of code designed for fraud prevention

Following this, the program produces a number of standard actions that should be performed before cash dispenses, and if they are successful, the ATM gives out cash to the mule. This operation will be repeated as many times as specified in the "Dispenses Count" argument.

Upon successful completion of each operation, the program records the "Cassettes Count: Banknotes Count" text string in the file named "disp.txt" located in the same directory as the malware, where "CassettesCount" and "BanknotesCount" are values of the respective arguments.

Specialists have detected two versions of this program. One version is named d2.exe, and another one is d2sleep.exe. The only difference between them is that the second version makes ATMs dispense money with a small pause of 1 second.

Once an ATM is emptied, the operator launches the SDelete program, which removes files used with a special algorithm, which prevents information from being recovered. Thereafter, the ATM restarts. In addition, operators disable the bank's internal servers involved in the attack using the MBRkiller malware that removes MBR (master boot record). Such a careful approach significantly complicates further investigation.

The cellphones of arrested mules contained messages with six-digit codes. Normally, these codes are sent by the organizer to activate the malware on a particular ATM.



Purportedly, hackers have other malicious programs to attack ATMs.

Ensuring control over actors

In order to prevent operators from using the program to attack other ATMs without involvement of the organizer, its code contains built-in start time check. If the system time of the attacked ATM does not correspond to the month indicated in the code, the commands will not be executed. The program will not generate errors, and the operators will not likely learn about such a built-in check.

After each successful operation, the program records a specific log (a file named disp.txt) with information on the number of banknotes dispensed from the ATM cassette. The operator sends this log file to the organizer, who uses this data to control the 'jackpotting' chain.

Renewed attacks on companies using the Buhtrap botnet



MARCH

The last confirmed attack on a bank conducted by the **Buhtrap group**

In May 2016, Buhtrap members were arrested while laundering money. After that, thefts from accounts at banks using the Buhtrap Trojan stopped. However, the Buhtrap botnet continued its malicious activity: in May, several companies that had been infected with Buhtrap malware had money stolen.



MAY

Arrest of the group laundering money for **Buhtrap**

When investigating such incidents, we detected two versions of the Light Manager remote control in the infected networks: the first version had been installed for a long time (in some cases – more than a year) together with the main malicious program, and the second version was installed in June 2016.



JUNE



The first attack on a Russian bank using **Cobalt Strike**

Group-IB specialists believe that just after the arrest of the Buhtrap group in May their botnet was sold to other criminals who are continuing its use to steal money from corporate accounts.



JULY



Attacks on banks in Armenia, Belorussia, Poland, Germany

That said, according to our analysis of Cobalt attacks on ATMs of Russian and European banks, the methods used by criminals to deliver phishing emails and obtain control over a domain controller are identical to those used by the Buhtrap group.



AUGUST



Attacks on banks in Georgia, Belorussia, Romania, Kyrgyzstan, Poland, Estonia, Spain, the Netherlands, the UK, Malaysia

Purportedly, at least a part of the Buhtrap group became Cobalt members, or more likely Buhtrap core members shifted their focus to attacks on ATMs.



SEPTEMBER

Confirmed thefts from ATMs outside Russia

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.



Generally, these recommendations can help you prevent the attack, however, a bank can successfully minimize its financial risks only by tracking hacker group activity using threat intelligence and specialized solutions designed to detect targeted attacks.

Prevention at the intrusion stage

The key method of intrusion into the bank's network is sending phishing emails with an attachment containing the exploit, or executable file in a password protected archive. To prevent infection resulting from this exploit's operation it is enough to update Microsoft software regularly.

This 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 of the banks attacked are known not to have taken these security measures.

In cases when hackers were faced with updated software, they sent emails with documents attached containing password-protected archives with executed files. **Such attacks can be blocked by quarantining suspicious emails for further dynamic analysis in isolated environment.**

Prevention at the implementation stage

Even if the criminals have managed to obtain access to the bank's network, the attack can still be successfully prevented. It takes days and even months sometimes to implement all steps of the attack, and this time should be used to detect the malicious activity.

- Check configuration of domain controller and presence of the Groups.xml file in the SYSVOL directory with an encrypted password using a standard encryption key AES-256, as it is covered in the "Gaining privileges" section.
- Install integrity control software on ATMs.
- Check your systems by indicators of compromise presented in the next section.

If you have detected trails of a targeted attack at any stage, you need to involve specialized companies for its analysis.



Incorrect responses to this type of attack may result in the attacker activity remaining partly undetected which enables criminals achieve their goals – theft of cash.

IP addresses of the servers used to send phishing emails:

88.212.208.115
5.101.124.34

Names of malicious attachments:

The rules for European banks.doc
Bitcoin ATM's.doc
Договор_хранения2016.zip
список документов.doc

Links to download Cobalt Strike's Beacon:

hxxp://korolev-okna.ru/beacon.exe
hxxp://50.115.164.10/update.exe
hxxp://176.31.79.123/~tolipresorts/nig.exe
hxxp://durok.net/0x/1.exe
hxxp://www.sport7boxe.com/METOO.exe
hxxp://methninja.tk/private/hawkraw.exe
hxxps://23.152.0.210/GizS

IP addresses of the Cobalt Strike C&C servers:

188.214.129.65
94.130.120.179
23.152.0.210
95.215.45.221
84.200.84.241
95.183.51.24

MD5 of malicious files:

966cc404a4f6bf6d77565004a952b3e3	Cobalt Strike
db6a8169f55a20838c0ca6f383c11e23	Cobalt Strike
7falaf2adba39ef6efe0f870c057554d	Cobalt Strike
89889adb22c63186eb8c72323f34b1fd	Cobalt Strike
0d21832c171e817e947837bbfb67380e	Cobalt Strike
0c34ae326a8fd68d4a67ea3484b7cf81	Cobalt Strike
555399c93b5f01fd9fad5f903da768d3	Cobalt Strike
56487b799755f50c6e56c41870d43624	Cobalt Strike
fe44c14403f36c6e451bda391ald1ca7	Cobalt Strike
d529218495f0318b99e60477368bb55e	ATM malware program
f5aea645966319c96d4dbcadce2a10e0	ATM malware program
036faf1f7e39e44c0db25b9149b45786	MBR Killer
eb162cc34efaelcb621cc7157ef36514	Modified SDelete
c91658349005a2f1c92a20132de38486	Cobalt Strike launcher from autorun
3ea9ef46e89f07920d87255aef9261ba	Cobalt Strike launcher from autorun
cafab9cc40ad0bd1cbec2164e17c8216	Cobalt Strike beacon downloader
35e0449cbe9fbe43e95b920c246828b2	Cobalt Strike beacon downloader
bfb9688ac2747017c7975921ffe77be9	The rules for European banks.doc
b175140a52aca83833a8203ac81e7475	The rules for European banks.doc
712e11e5217ef06847ea96a83e952566	The rules for European banks.doc
5d11c7b17633332b787992ee617d3552	The rules for European banks.doc
9d443e225e21f160014e79b62c5aea3d	Bitcoin ATM's.doc
83dee40f12f67634c5da640f6d6f2efb	Договор_хранения2016.zip
1d07edbd16cbe529500c37245e613a47	Договор_хранения2016.exe
3b2b116db9569f50c9e7a272c7530b18	список документов.doc

GIB Threat Intelligence subscribers are always on the forefront and were made aware of the Cobalt activity in August 2016. Our reports included both phishing campaign details and payload analysis. The data we provided proved vital in preventing attacks against clients exposed to Cobalt 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.

Threat Intelligence



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

TDS + TDS Polygon



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 Eastern Europe, with an experienced investigation team



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 focus on high-tech crime investigation and the ability to provide leading insight to the Eastern European region. Group-IB is recommended by the Organization for the Security and Co-operation in Europe (OSCE).

Learn more on group-ib.com or get in touch now **+7 495 984 33 64**.