

Contents

Cobalt—a new trend or an old “friend”?	3
Opening an ATM from the inside out	4
Can the trend be changed?	5
Attack timeline	6
Who says criminals don’t have a sense of humor	8
Technical aspects	9
Cobalt: distinguishing traits	10
Conclusion	11

Cobalt—a new trend or an old “friend”?

Information about the so-called Cobalt group appeared quite recently, in a November 2016 report¹ from Group-IB. According to the report, Cobalt is associated with the previously known Buhtrap² campaign. Buhtrap is thought to have stolen around USD 28.5 million from Russian bank accounts in 2015 and 2016. It is suspected that either part of that group switched over to Cobalt, or that most of the Buhtrap creators redirected their efforts at ATMs.

At the same time, in the fall of 2016, Positive Technologies was independently investigating an incident at a bank in Eastern Europe. The bank had experienced phishing mailings as well as compromise of internal network resources and its ATM network. All the evidence indicated that the attack was targeted. Artifacts indicated the involvement of the same organized crime group that, according to Positive Technologies information, from August to October had performed similar successful attacks in Eastern Europe, and it's likely that this group may will soon become active in the West. Analysis confirmed that the Cobalt group was responsible.

This report includes the most important results of the investigation, including an example of a real-life advanced persistent threat (APT) attack that could occur at any bank. To implement the attack, the criminal group used easily available software to target some of the most common shortcomings and vulnerabilities in corporate systems, in which regard the financial sector is no exception (see the Positive Technologies report at www.ptsecurity.com/upload/iblock/2fe/corporate_vulnerability_2016_eng.pdf).

According to Group-IB, Buhtrap is the first criminal group to use a network worm to infect the entire infrastructure of a bank. The main vector for penetrating the bank's corporate network consisted of phishing messages, which claimed to be from the Bank of Russia or its representatives. Malware was planted in a number of attacks via exploits, notably including the infrastructure of the Metel³ group.

A trend has been seen in 2016 towards the use of publicly available software, legitimate penetration testing software, and standard operating system (OS) functions by attackers. One instructive example is the 2016 attacks by the Carbanak⁴ group in Eastern Europe. This group used similar tools, in addition to Metasploit. The same group is suspected in the recent hacking of PoS vendor Oracle MICROS⁵ and attacks on international banks recently reported by Symantec⁶.

By underestimating the abilities of cybercriminals, and assuming that attacks always happen to somebody else, companies fatally undermine their cybersecurity efforts. This can result in substantial financial losses.

Despite the wealth of information now known about methods, tools used, and indicators of compromise, the cybercriminals continue their attacks and are looking for new ways of monetizing their efforts. Targeted attacks on banks, retailers, and financial institutions around the world are covered with increasing regularity in the media. Total losses related to such cyber-crime, according to various estimates, run in the hundreds of millions of dollars. In 2017, we expect to see an increase both in the number of attacks and in related financial losses by banks—it would seem that the criminals are hitting their stride, while banks have barely even begun to play catch-up.

¹ <http://www.group-ib.com/cobalt.html>

² <http://www.group-ib.ru/brochures/gib-buhtrap-report.pdf>

³ <http://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf>

⁴ http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf

⁵ <https://krebsonsecurity.com/2016/08/data-breach-at-oracles-micros-point-of-sale-division>

⁶ <https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks>

Eastern European banks under threat

Who's the next target?

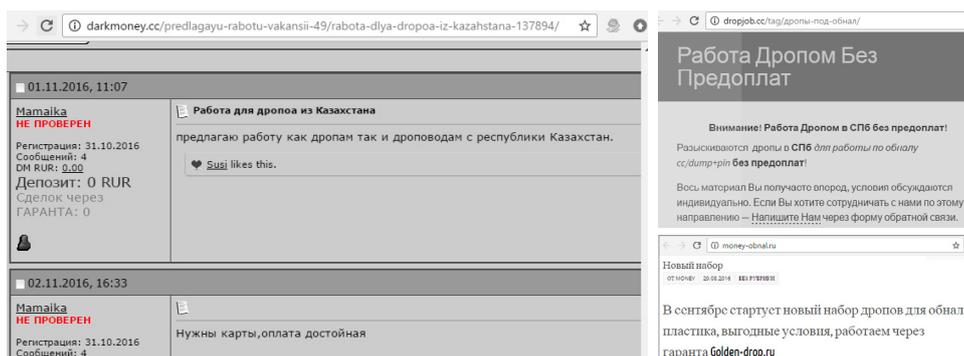
Opening an ATM from the inside out

In early October 2016, Positive Technologies learned from a bank in Eastern Europe of a security incident that resulted in funds being stolen from bank ATMs.

Total funds stolen, in the course of one night from six ATMs, were the equivalent of approximately \$35,000 in local currency. Rapid response by the bank and law enforcement prevented the losses from growing. Theoretically, had the attackers continued for a longer period, they could have stolen the equivalent of over \$156,000 over several days, with the amount limited only by the dispensing capabilities of the machines and number of compromised devices.

Individuals acting as cut-outs (“drops”) obtained cash from ATMs. One of these drops, a citizen of Moldova, was arrested by local law enforcement in the process of withdrawing money. These drops are used by criminal groups to minimize the risk to core group members. Drops do not know any of the core group members and work only with handlers, who are responsible for gathering the cash and delivering it to the organizers.

Cobalt uses so-called money mule services for laundering cash. These services attract the financially desperate with promises of easy earnings. Such services are plentiful online. Here are screenshots of a few examples:



The investigation performed by the Positive Technologies team showed that the theft occurred due to a compromise of the bank’s local network and installation of malware on ATMs from the bank’s internal infrastructure in August–September 2016. The malware installed on the ATMs was specialized, dispensing money from an ATM to a drop at the command of the attacker. Drops themselves did not need to perform any special manipulations of the ATM.

Cobalt Strike as an attack tool

Cobalt Strike functionality includes:

- + Module for phishing attacks
- + Module for drive-by web app attacks
- + Module for establishing a beachhead and spreading on the network (Beacon)
- + Hidden communication methods, including DNS tunneling and Peer-To-Peer SMB

More about Beacon:

- + Written in PowerShell
- + Resides in RAM
- + Advanced remote management capabilities (file downloading/uploading, privilege escalation, traffic proxy, keylogger, network scanner)

Detected by antivirus software

Antivirus software on the bank servers detected the infection. Rapid response by bank security personnel could have prevented the incident. However, employees often turn off the antivirus protection on their computers and antivirus logs were not checked at all.

Can the trend be changed?

Attacks on bank clients are starting to take a back seat to other methods that are every bit as effective—attacking the banks themselves, or more precisely, their network infrastructure. Criminals are aware that not all financial institutions make sufficient investments in their security and often concentrate on the bare minimum of compliance at the expense of actual security. In addition, attacks on clients are limited to how much money the client has in their account. But by taking over key servers and ATM controllers, hackers can strike a much more lucrative payday.

The last few years have seen a trend toward targeted attacks with social engineering and phishing messages. Most often, organizations (whether a bank, industrial concern, IT firm, or any other kind of company) concentrate on uptime in business processes, and when it comes to security, they buy and deploy various expensive solutions from outside vendors. But this approach has only middling results, closing a few of the most gaping holes in defense, while leaving untouched the weakest link in security: the human factor.

Attack groups are constantly modernizing their techniques and identifying new vulnerabilities. By staying at least one step ahead of defenders, attackers set the agenda for the entire security industry.

As shown by the experience of Positive Technologies, attackers tend to use commonplace tools, such as software for legitimate pentesting and built-in OS functionality. Cobalt is merely the most recent example of this trend.

This applies to the attack dissected in this report as well. Criminals used commercially available software, Cobalt Strike⁷, to perform penetration testing, including the use of the Beacon trojan. The Beacon agent is the main payload and is classified as a RAT (Remote Access Trojan).

Widely known legitimate Ammy Admin software, downloadable from the manufacturer's site, was used for remote administration.

Other common tools were used, including:

- + Mimikatz
- + PsExec
- + SoftPerfect Network Scanner
- + TeamViewer

A Pass-the-Hash attack was used for moving about the target infrastructure: OS authentication was bypassed by using a hash of the password, without even needing to know the password itself.

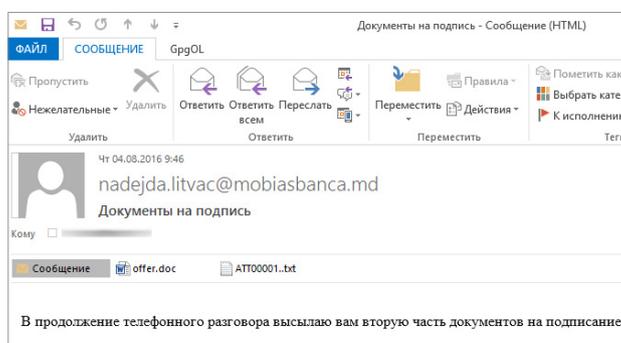
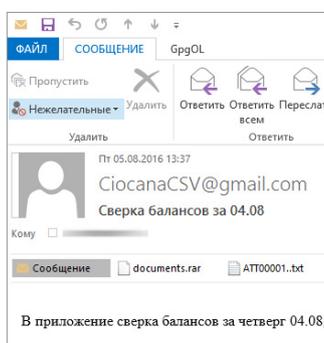
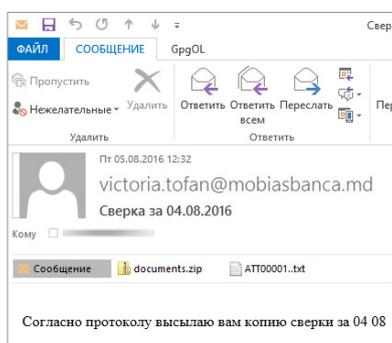
It should not be a surprise that criminals have switched to legitimate software for their attacks: modern remote administration tools for network infrastructure and servers are so powerful that there is simply no need to invent something else. And as a side benefit for attackers, identifying the use of such software is more difficult. The security of corporate infrastructure at most banks is poor, leaving an opening that cybercriminals are sure to exploit.

⁷ <https://cobaltstrike.com>

Attack timeline

The attack started in the first week of August. The initial infection vector started with a file named documents.exe; a RAR archive containing it was received in an email to a bank employee. If not for the employee being on vacation, the phishing message could have compromised the bank's entire infrastructure on that very same day. Instead, the attackers had to wait over two weeks for the workstation to be turned on again. As a consequence, the attackers had to repeat their actions for developing the attack and elevating privileges in the OS.

For one month, emails were sent to various bank addresses, containing malware while claiming to be from employees of various banks. Analysis showed that the sender addresses were forged. But the addresses themselves are real and most of them can be found on the official websites of the bank targeted, or online at curs.md/ru/lista_banci (a site dedicated to information about Moldovan banks).



Subject lines of phishing messages (translated):

- "Documents for signing"
- "Reconciliation for 04.08"
- "Balance reconciliation for 04.08"
- "Yesterday's meeting minutes"
- "Requirements for IT Security Staff"

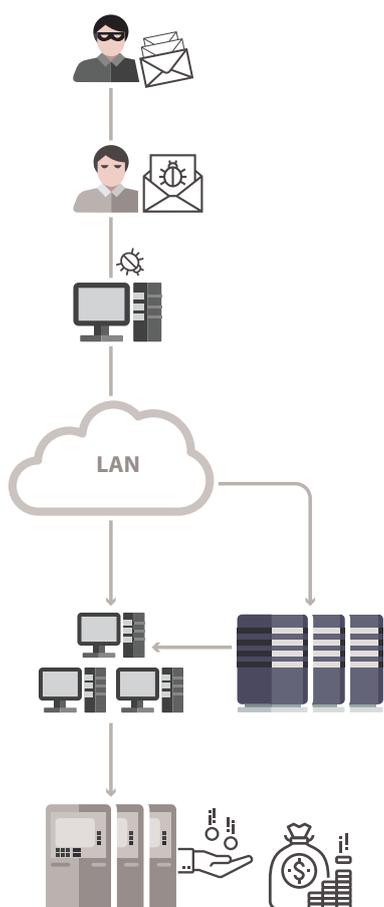
The mail server mail.peacedatamap.com was used to send the messages. Reply-to addresses were hosted on the domain temp-mail.ru, a site for temporary email addresses. The reply-to addresses in messages received by bank employees were sesati@lackmail.ru and foyup@lackmail.ru.

Investigation showed that several employees opened the file from the phishing messages at multiple times, indicating a poor level of security awareness at the organization.

Notably, antivirus software detected both the original malicious attachments and the actions of the attackers after the compromise—long before money was actually stolen. Suspicious activity by legitimate software (Ammyy Admin) was detected, and in some cases infection was prevented by the antivirus software. The original infection took place because the antivirus software was disabled, or had out-of-date databases, on the workstation of the employee who ran the malware from the phishing message.

The malware triggers the following verdicts by antivirus software:

ESET	SYMANTEC	KASPERSKY
Win32/Rozena	Trojan.Odinaff	RemoteAdmin.Win32.Ammyy
	Trojan.Odinaff!g1	Hacktool.Win32.Cobalt
	Trojan.Odinaff!gm	HEUR:Trojan.Win32.Generic
	Backdoor.Batel	
	Remacc.Ammyy	
	Backdoor.Gussdoor	



1 Spear phishing
(malicious attachments)

Penetration of local network

Message from untrusted source opened, attachment run

2 Infection of workstation

Foothold on local workstation

Excessive user privileges

3 Network reconnaissance and attack progression

Scanning of local network

Effective segmentation not present on network

4 Preparation for theft

Compromise of key resources

Identification of employee computers that interface with ATMs

5 Infection of ATMs

Theft from ATMs

Drops collect cash without performing any special actions at the ATM terminal

Warnings for banks

After similar attacks in 2016, FinCERT issued several bulletins (ATM-OTH-ML-JACKPOTTING-20160921-01, ATM-OTH-ML-JACKPOTTING-20161014-02 and BK-20160906-001) to alert banks to the risks and encourage them to take preventive measures (such as by looking for particular indicators of compromise on network infrastructure).

To reduce the likelihood of detection, attackers used various strategies:

- + Legitimate software and built-in OS functions were used.
- + Malware code was run only in RAM.
- + HTTPS was used for command and control.
- + A legitimate service, sendspace.com, was used for file exchange and download of the original malware.
- + Files were deleted, including with SDelete, to guarantee elimination of data.
- + Actions were performed primarily at night.

After gaining a foothold on the bank infrastructure, the Cobalt team did not rush to act. Only at the end of August did they substantially develop the attack across the bank's network. The attackers compromised the workstations of key employees and critical servers, including terminal server and domain controller. In addition, they stole the passwords of practically all company users, including administrator accounts, which allowed moving about the network at will.

To find and download various utilities (such as Mimikatz), Cobalt accessed legitimate sites and search engines directly from infected devices. Sites were chosen from the search results (for example, github.com) and software was downloaded from those sites to workstations and servers. To download files, the malware used the publicly available site sendspace.com for file exchange. By using legitimate services, the attackers attempted to mask their actions.

QA matters for criminals too

Errors in the malware prevented the criminals from taking money from NCR ATMs, although they tried to “troubleshoot” several times during their attack.

C2 server addresses:

23.249.164.26
149.56.115.70
142.91.104.135
173.254.204.67
23.152.0.210
185.82.202.232

It is important to note that using Mimikatz to get OS account credentials requires local administrator privileges. Key factors in the rapid spread of the attack across the network included the lack of network segmentation and overprivileged user accounts (the attacked user was a local administrator on all workstations on the local network). Therefore, the attackers did not need to use any additional exploits to escalate their privileges or look for methods of penetrating another network segment.

Another peak of activity occurred in early September, when the criminals actively attacked network resources in order to identify the workstations of employees responsible for ATMs and bank cards. These attacks consisted, in essence, of remotely connecting to workstations, running Mimikatz to collect credentials, surveying the file system and installed software, and moving on to the next workstation. After compromising the necessary devices, the attackers had the information needed for initiating the theft itself.

Security logs showed network movement by the attackers from compromised computers, including RAdmin sessions with ATMs. However, RAdmin is actively used by bank administrators to remotely access computers, including ATMs, and therefore this did not arouse suspicion.

Cobalt went about its plan with practically no special efforts to mask its activity – assuming that its actions would not be noticed. But the attackers did not hurry to cash in right away. They studied bank processes and waited for the maximum possible amount of cash to be present in ATMs.

The attackers waited until early October to load malware on ATMs and steal money. They acted at night in order to minimize possible attention. The operator sent a command to ATMs and the drops approached ATMs at a particular time and simply took all the money.

Due to an error in the malware code, the attackers were unable to steal money from ATMs manufactured by NCR. The malware generated errors in the ATM software. Despite attempts to fix this issue during the attack, including restarting the malware and ATMs multiple times over the course of two hours, the attackers were unsuccessful. In this case, luck helped the bank to curtail its losses.

Based on the incident investigation, Positive Technologies experts collected a long list of host- and network-based indicators of compromise, which were sent to the FinCERT of the Bank of Russia in order to alert banks and prevent similar attacks in the future.

Who says criminals don't have a sense of humor

During the investigation, Positive Technologies found a curious artifact: the email address used for downloading Ammyy Admin combined a Russian-language obscenity with the name of Kaspersky Lab.

```
2016-09-**T17:22:35.489000+06:00,Page Visited,WEBHIST,Firefox History,http://www.ammyy.com/AA_v3.exe?em=huy%40kasperskyc.com (AA_v3.exe) [count: 0] Host: www.ammyy.com visited from: http://www.ammyy.com/ru/ (www.ammyy.com) (URL not typed directly) Transition: DOWNLOAD,sqlite/firefox_history
```

In other words, Cobalt expected that Kaspersky Lab would be performing incident investigation. That assumption proved wrong, however, as shown by the work of the Positive Technologies team.

Technical aspects

Positive Technologies experts analyzed the detected malware. Here is a summary of the main modules:

winapma.exe	Stager for Beacon agent Downloads from 173.254.204.67:443/eHHr with the user agent string "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; Avant Browser)"
atm.exe	Stager for Beacon agent Downloads from 142.91.104.135:443/svVv with the user agent string "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)"
crss.exe	Downloads crss.dll Runs the run_shell function from crss.dll
crss.dll	Stager for Beacon agent Downloads from 173.254.204.67:443/eHHr with the user agent string "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; Avant Browser)"
artifact.exe	Stager for Beacon agent Downloads from 173.254.204.67:443 with the user agent string "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; NP08; MAAU; NP08)"
documents.exe	Stager for Beacon agent Downloads from 23.152.0.210:443/GizS with the user agent string "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
tkg.exe	Stager for Beacon agent Downloads from 185.82.202.232:443/xRdM with the user agent string "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)"
prikaz_08.08.2016.exe	Stager for Beacon agent Downloads from 23.152.0.210:443/GizS with the user agent string "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
offer.doc	RTF document with an exploit that runs stager for the Beacon agent Exploits vulnerability Word CVE-2015-1641 and contains exploit for Adobe Flash CVE-2016-4117. The exploits result in downloading Beacon agent from 23.152.0.210:443/GizS with the user agent string "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
jusched.exe	Stager for Beacon agent Downloads from 149.56.115.70:443/dDBr with the user agent string "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0; BOIE9;ENUS)"

CC323EA62B71E6 216A9ED830323B 18C8FAA03CB8.out	File restored from quarantine SMB Beacon Awaits commands via named pipe \\.\pipe\status_8443
netscan.exe	SoftPerfect Network Scanner

Cobalt: distinguishing traits

The attackers' phishing messages were written in Russian. This means that at least one of the criminals is a Russian speaker. The group knows a fair deal about the banking industry and has significant resources to support its activities.

A number of similar incidents also indicate that the Cobalt group is Russian-speaking. Performing such attacks is impossible without knowing internal bank processes, which requires an understanding of Russian.

Group	<ul style="list-style-type: none"> + Use of money mule services for moving cash + Resources for sustaining activity over non-trivial duration of time + Special focus on banks in Russia and Eastern European countries
Software	<ul style="list-style-type: none"> + Use of software intended for legitimate pentesting, such as Cobalt Strike + Use of legitimate Ammyy Admin remote administration software + Use of free, publicly available SoftPerfect Network Scanner + Use of Mimikatz + Use of built-in OS functions for moving about the network: PowerShell, PsExec, Runas
Theft method	<ul style="list-style-type: none"> + Cash received via ATMs. Specialized/malicious software used to manipulate the dispenser

Conclusion

As shown by this Positive Technologies investigation of a real-world attack by the Cobalt criminal group, media stories of billions in bank losses due to hacking are no tall tale—these attacks are already happening here and now. Banks must give serious thought to prevention in order to not become the next target.

More serious losses were avoided only thanks to the swift reaction of the bank, which brought in outside experts, and law enforcement, which caught one of the drops in the act of withdrawing money.

The criminals attempted to stay unnoticed on the bank network (hoping that use of legitimate software would not raise suspicions), but antivirus software noticed malicious activity at the host level. Thus proper security monitoring at the bank, had it been performed, could have prevented the incident entirely.

Targeted attacks have become a fact of life in recent years. And when choosing their targets, attackers bypass the little fish—that is, individual clients—in favor of the big fish, the banks themselves. Instead of elaborate zero-days, hackers use the most common vulnerabilities to target the weakest link in bank systems. APT attacks are not necessarily as complicated as they may seem. Banks need to make securing their infrastructure a priority, not just another checkbox to be completed at audit time. When the next attack occurs, will it be your bank that is targeted?

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

© 2016 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.