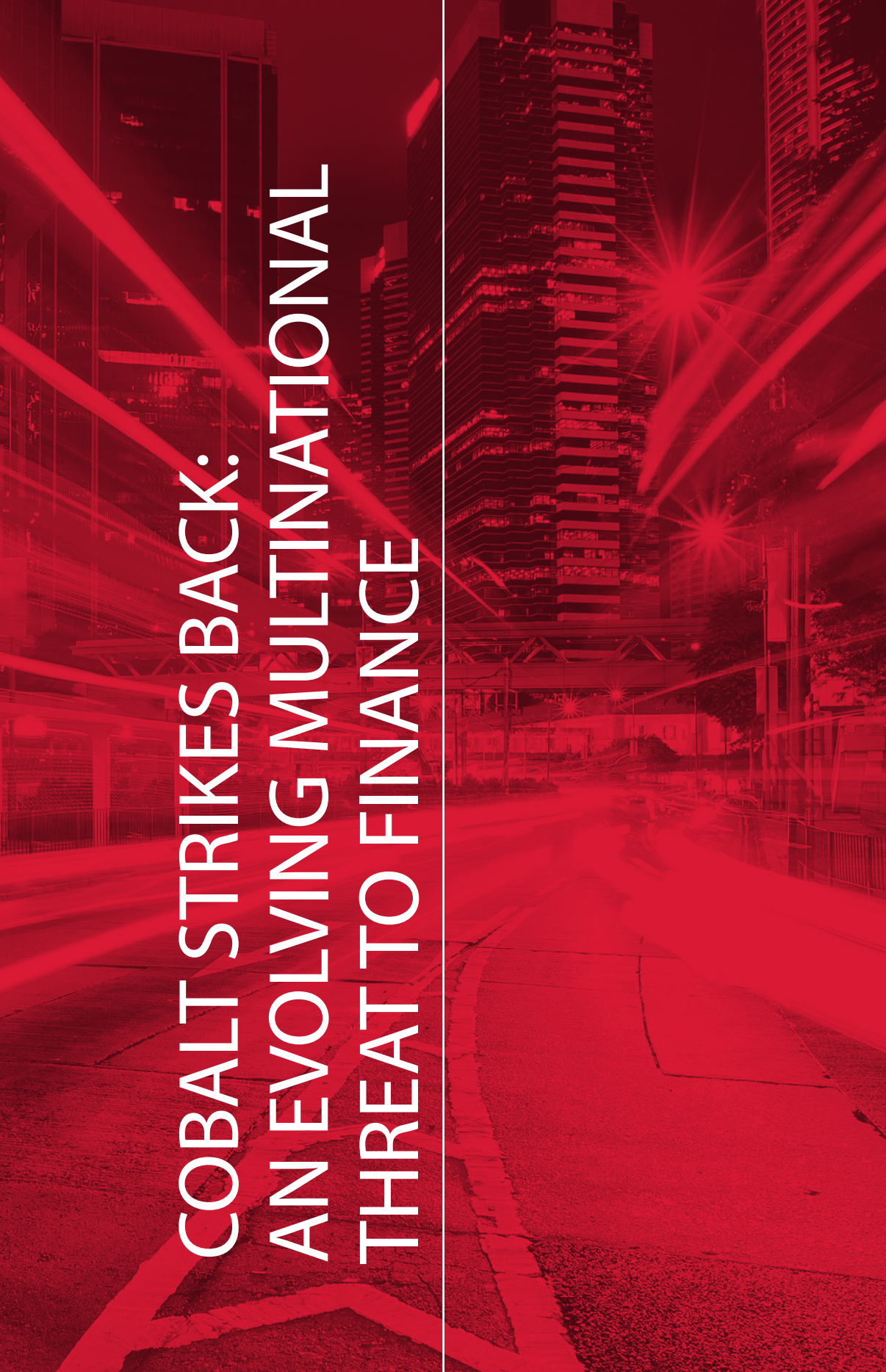


COBALT STRIKES BACK: AN EVOLVING MULTINATIONAL THREAT TO FINANCE



CONTENTS

Introduction.....	3
1. Executive summary.....	3
2. What we already knew about Cobalt.....	4
3. Cobalt targets and objectives.....	5
4. Chronology of Cobalt 2017 campaign.....	6
5. Cobalt attack methods.....	8
5.1. Partner phishing.....	9
5.2. Malicious attachments.....	13
5.3. Cobalt infrastructure.....	17
Conclusion.....	19

INTRODUCTION

Bank robbery is perhaps the quintessential crime. The promise of immense, instant riches has lured many a criminal to target banks. And while the methods, tools, and scale of robbery have all changed, two things have stayed the same: the enticement of a hefty payday and the fact that no system is perfectly secure.

In the modern digital economy, criminals are becoming ever more creative in ways to make off with millions without having to leave home. Despite enormous efforts, security is always a work in progress because of technical vulnerabilities and the human factor. Only a small fraction of banks today are able to withstand targeted attacks of the kind perpetrated by Cobalt, a cybercriminal group first described in 2016 that is currently active worldwide. Now the group has set its sights on more than just banks.

Researchers at Positive Technologies and other companies¹ have described the group's methods previously. In this report, we will describe the new techniques used by Cobalt in 2017, the changing target profile, and recommendations on how to avoid becoming their latest victim.

1. EXECUTIVE SUMMARY

The Cobalt group has been quick to react to banks' protective measures. When spam filters on mail servers began to block most of the group's phishing emails, which contained forged sender information, the attackers changed techniques. Now they actively use Supply Chain Attacks² to leverage the infrastructure and accounts of actual employees at one company, in order to forge convincing emails targeting a different partner organization. This tactic has already been used by other attackers, such as when the infrastructure of M.E.Doc was used to spread the NotPetya virus, which blocked workstations at a large number of major companies.³

Cobalt has attacked banks, financial exchanges, insurance companies, investment funds, and other financial organizations. The group is not afraid to use the names of regulatory authorities or security topics to trick recipients into opening phishing messages from illegitimate domains.



This year the Cobalt group:

- + **Actively attacks bank partners** in order to use partner infrastructure for sending phishing messages to banks.
- + **Sends phishing messages disguised as mailings from financial regulators.**
- + **Uses various types of malicious attachments:** document with an exploit (.doc, .xls, .rtf), archive with an executable dropper file (.scr, .exe), and archive with LNK file (.lnk).
- + **Appears among the first groups to get access to the latest version of the Microsoft Word Intruder 8 exploit builder**, which made it possible to create documents exploiting vulnerability CVE-2017-0199.
- + **Uses poorly protected public sites to upload files** and then download them to victim computers.
- + **Sends phishing messages to both corporate addresses and personal addresses of employees.**

¹ www.group-ib.com/cobalt.html

² www.sans.org/reading-room/whitepapers/analyst/combating-cyber-risks-supply-chain-36252

³ www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

2. WHAT WE ALREADY KNEW ABOUT COBALT



Group objective

Steal money



Main targets

Banks in Eastern Europe and Central Asia



Methods

Perform cyberattacks on a bank's information infrastructure.
Gain a foothold on bank local networks by tricking employees into opening phishing messages that contain malware.



Software used

Cobalt Strike, Ammy Admin, SoftPerfect Network Scanner, Mimikatz, and OS functions (PowerShell, PsExec, Runas)

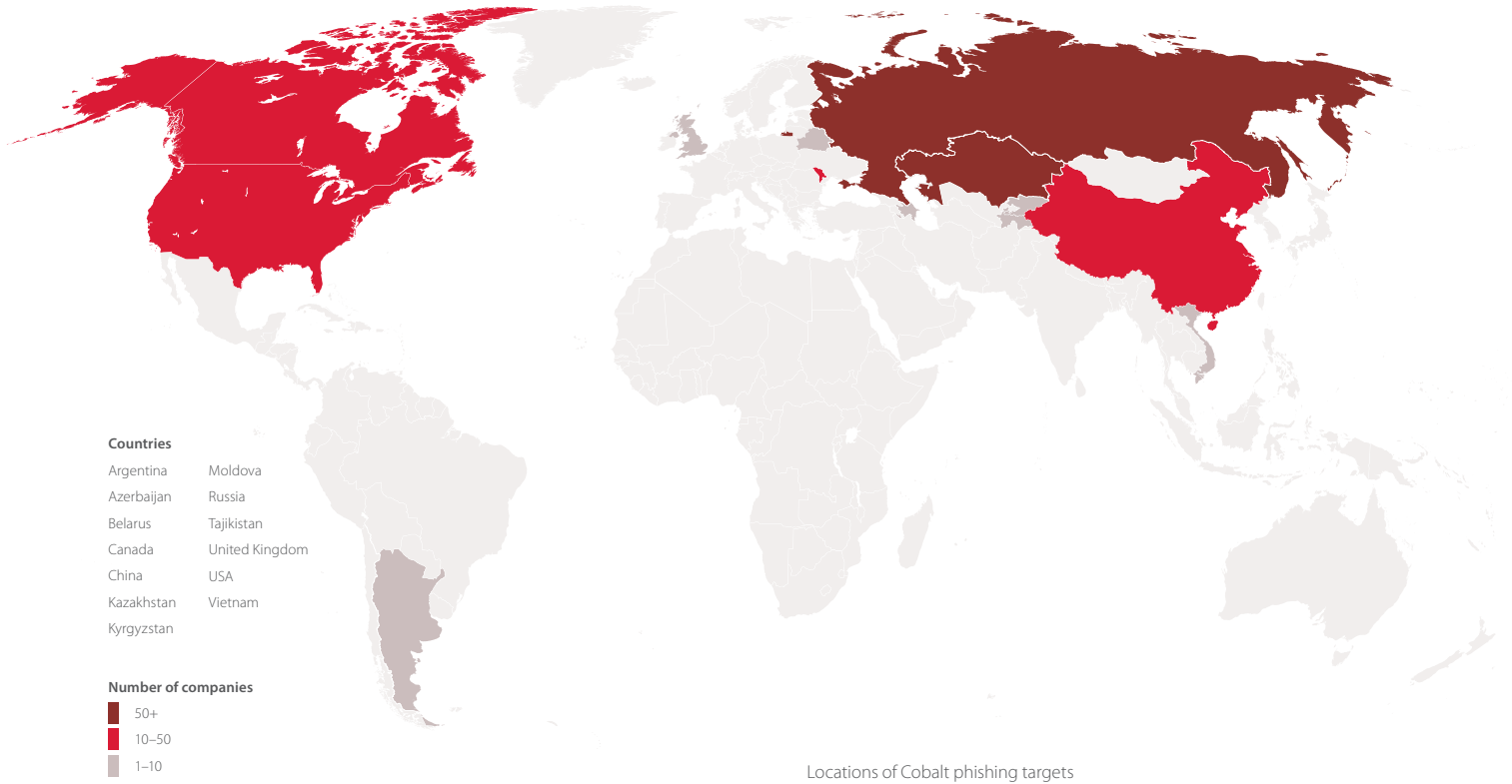


Outline of a typical attack

1. Spear phishing against bank employees
 2. Infection of the employee computer used to open an attachment
 3. Continuation of attack on the bank network; compromise of workstations used to administer bank ATMs
 4. Infection of ATMs and on-command dispensing of cash
 5. Cash withdrawal by willing cut-outs who receive a portion of the proceeds ("mules")
-

3. COBALT TARGETS AND OBJECTIVES

The Cobalt group's traditional "stomping grounds" are the Eastern Europe, Central Asia, and Southeast Asia. In 2017, attacks grew to include North America, Western Europe, and even South America (Argentina).



Of the companies targeted by Cobalt in phishing mailings, around 75 percent are in the financial sector. Most of these financial companies are banks (90%), but others include financial exchanges, investment funds, and lenders. This widening range of targets suggests that attacks on diverse companies with major financial flows are underway. This concurs with the forecast made by the FinCERT of the Russian Central Bank, which predicted increased interest by cybercriminals in financial exchanges in 2017.

By attacking a financial exchange, the Cobalt group can "pump" or "dump" stocks, incentivizing purchase or sale of shares in certain companies in a way that causes rapid fluctuations in share price. Stock manipulation can affect not just the welfare of a single company, but the economy of entire countries. These methods were employed by the Corkow group in their 2016 attack on Russia's Energobank, which caused a 15-percent change in the exchange rate of the ruble and caused bank losses of RUB 244 million (over USD 4 million).⁴

Since the beginning of 2017, our researchers have studied over 60 unique samples of phishing messages sent as part of Cobalt campaigns. These messages were sent to over 3,000 people in 13 countries. The addresses include corporate addresses but also personal addresses, since employees often can check their email on work computers.

Notably, Cobalt attacks government organizations and ministries in order to use them as a stepping stone for other targets.

The remaining 25 percent of targeted companies represent diverse industries:

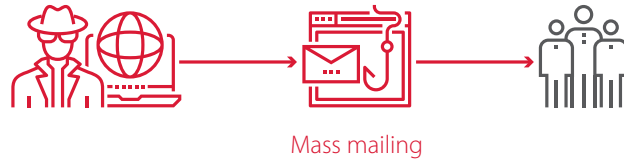
- + Government
- + Telecom/Internet
- + Service Providers
- + Manufacturing
- + Entertainment
- + Healthcare

⁴ fortune.com/2016/02/08/russian-hackers-currency-rate/

4. CHRONOLOGY OF COBALT 2017 CAMPAIGN

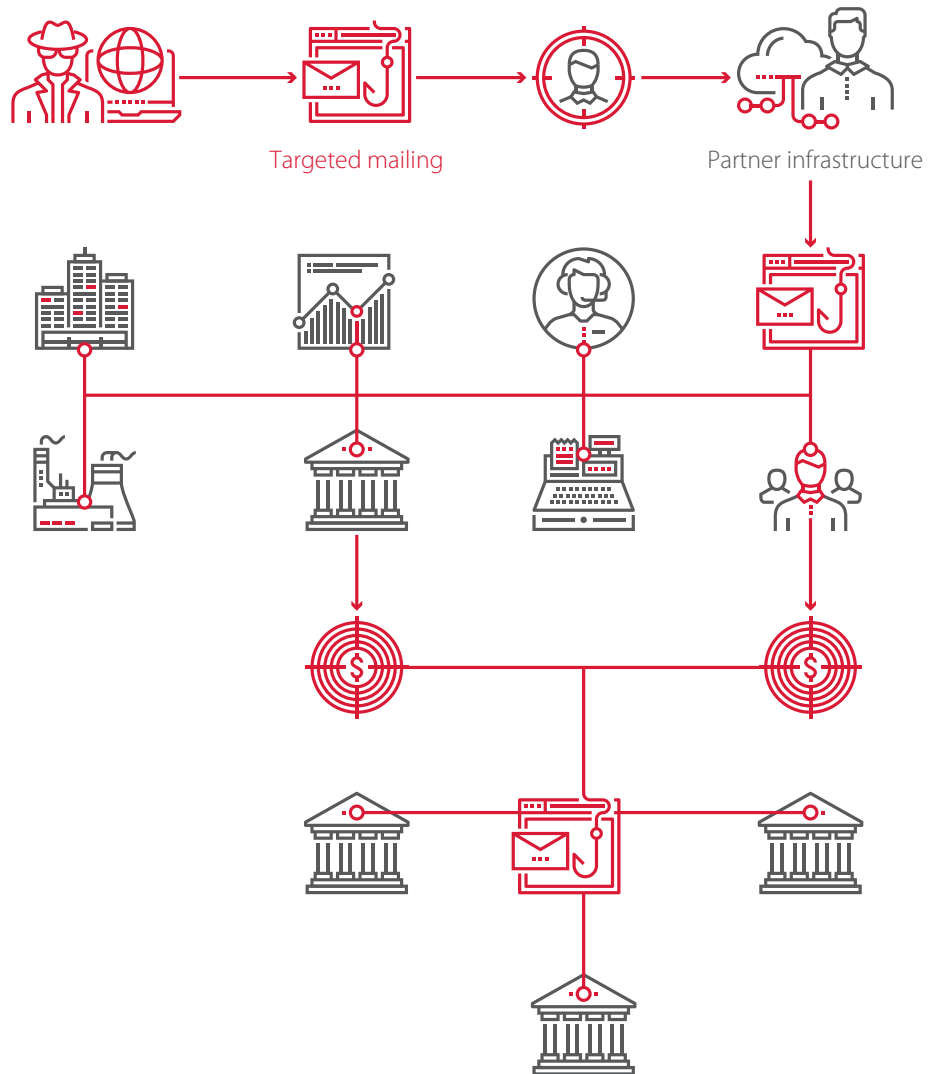
January

1. Registration of new phishing domains and configuration of DNS servers
2. Mass phishing mailings



February

3. Several successful targeted attacks on partners, with full compromise of partner infrastructure
4. Mailings sent from partners to companies in North America, Europe, USA, Southeast Asia, and South America

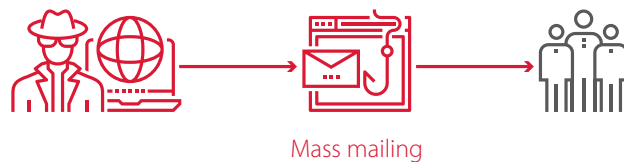


March

5. Compromise of several partners and banks
6. Continuation of mass phishing and attacks on other banks

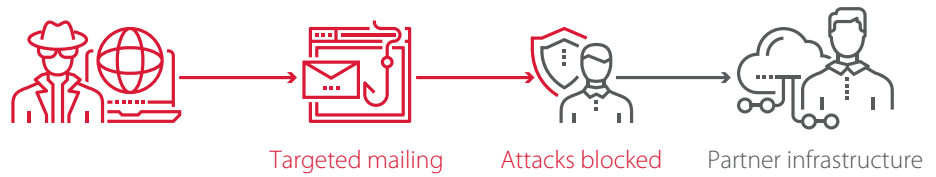
April

7. Registration of new phishing domains and configuration of DNS servers
8. Mass phishing mailings



May

- 9. MWI 8 update used to create documents exploiting vulnerability CVE-2017-0199
- 10. Registration of new phishing domains and configuration of DNS servers
- 11. Phishing mailings with new documents (CVE-2017-0199)
- 12. Repeat attempts to attack partners are blocked

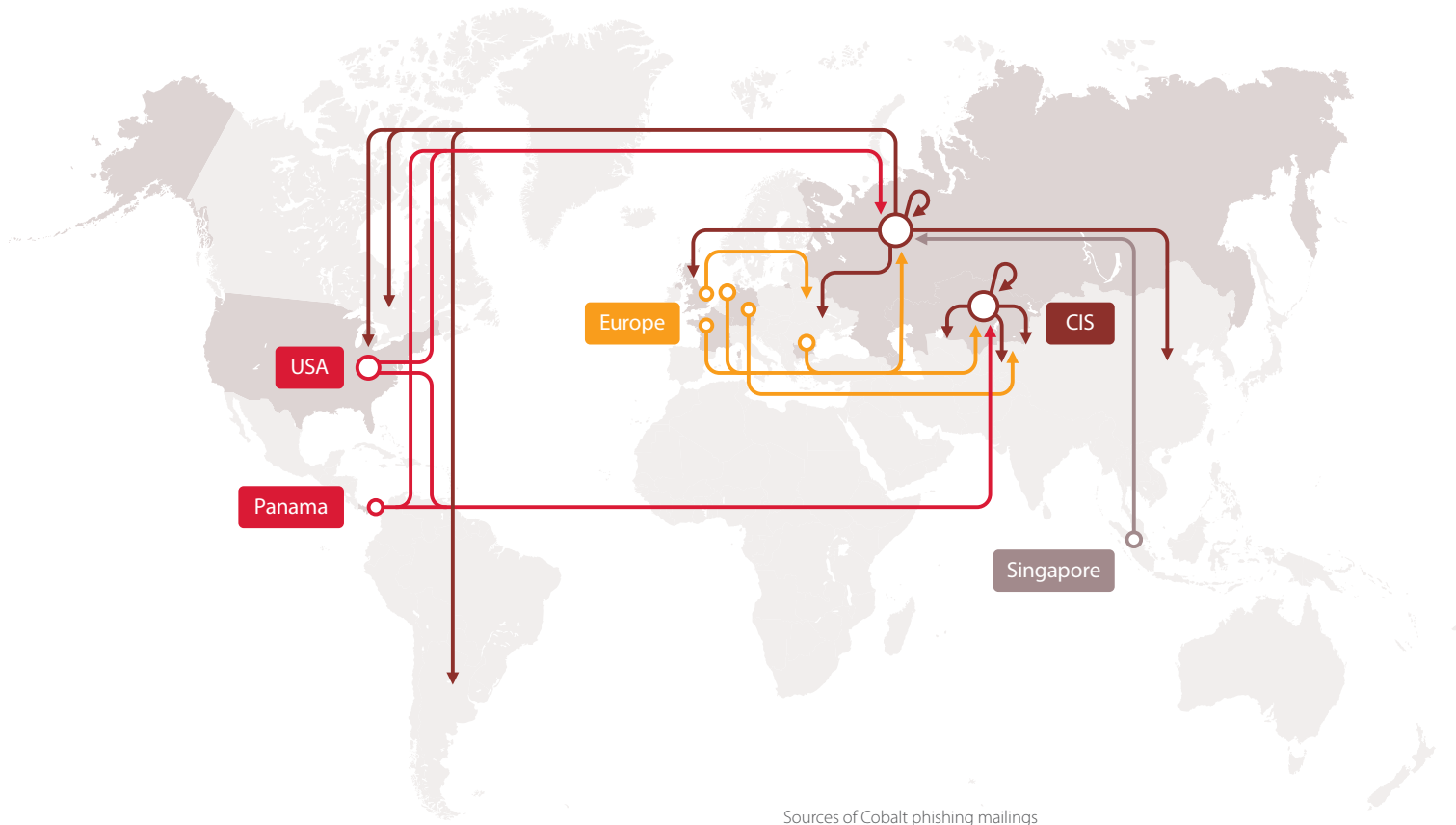


In early 2017, we noted that the Cobalt group was actively registering illegitimate domains. As soon as these domains were used to send phishing mailings, we notified the security departments of the targeted companies, as well as the FinCERT of the Russian Central Bank. Thanks to this timely intervention, the domains were blocked before the attackers could make use of them.

Positive Technologies has investigated incidents related to attacks by the Cobalt group at a number of companies in 2017. In several cases, the attackers compromised company infrastructure and employee accounts in order to send phishing messages to partner companies (i.e., companies that have a legitimate pre-existing business relationship with banks) in North and South America, Europe, CIS countries, and Central and Southeast Asia. Against targets in the CIS countries, the attackers also used their own infrastructure, which included rented dedicated servers located in North America, Europe, and Southeast Asia.

With the help of timely countermeasures, not only was it possible to detect and stop Cobalt attacks on partner infrastructures, but also to prevent repeat compromise when the attackers attempted to re-establish control on victim networks. Companies whose partners had been used to send phishing messages were warned of the danger.

Attacks on various organizations around the world were just an intermediate step for Cobalt. Having successfully implemented an attack on a bank or other partner organization, the group pressed on, sending phishing messages and attacking other banks.



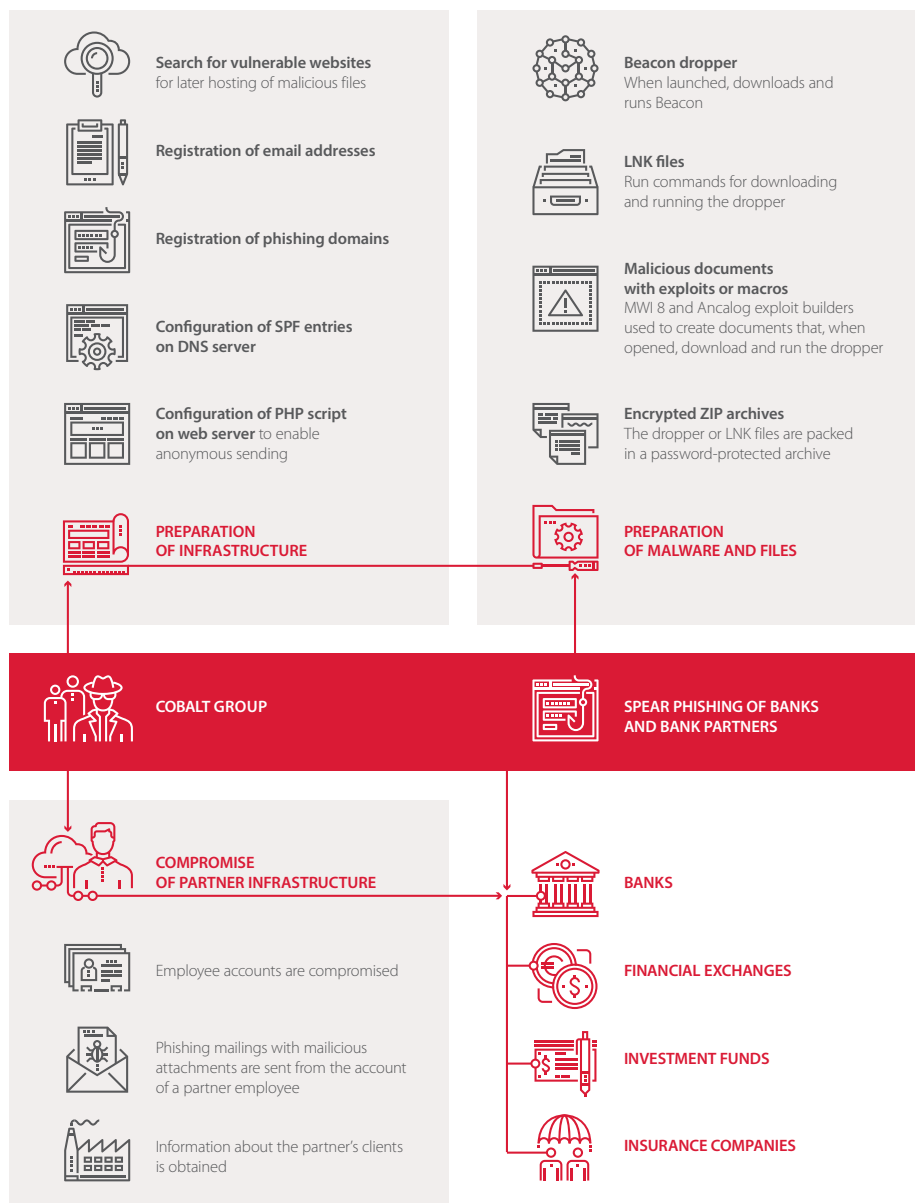
Sources of Cobalt phishing mailings

Several pieces of information suggest that the team responsible for the technical aspects of attacks consists of only a handful of people. When the attackers were at their most active inside target networks, the group would temporarily stop registering domain names and sending phishing mailings. Activity not aimed at the targeted infrastructure was not detected. The days and times of mailings are also suggestive in this regard, as described later in this report.

5. COBALT ATTACK METHODS

The Cobalt group relies on social engineering to penetrate networks—users open malicious attachments from phishing messages that are disguised by the attackers to resemble messages from legitimate companies and regulatory authorities. These attachments contain a document file, which downloads a dropper from a remote server or contains the dropper in a password-protected archive. Small in size, a dropper is used to download and run other malicious software (in the case of Cobalt, the Beacon Trojan).

Preparations and progression of a typical attack are illustrated below.



For information on the actions of Cobalt attackers inside the network of a targeted organization, please see our previous report.⁵

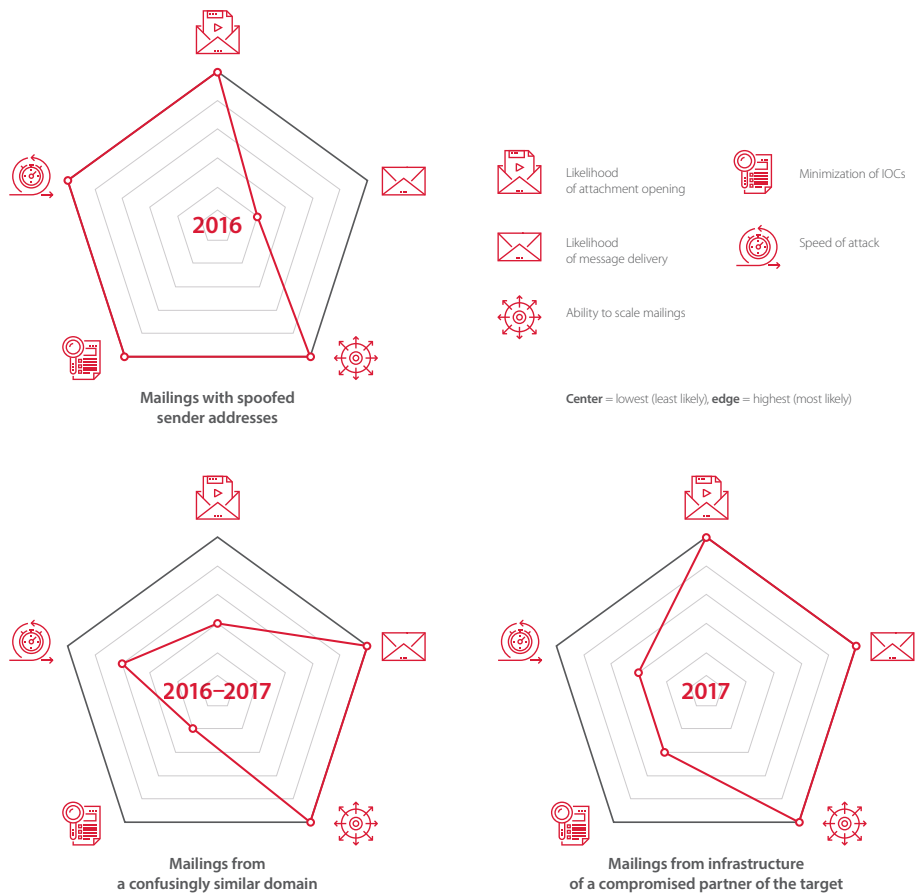
⁵ www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-Snatch-eng.pdf

5.1. Partner phishing

The Cobalt group's traditional method—sending messages with forged sender information—has fallen out of favor. Instead, the group has paid more attention to making sure that messages get delivered by dodging mail server filters.

For a targeted mailing ("spear phishing"), the criminals use previously registered domains. A domain name is chosen to be similar in meaning and spelling to the domain of the real company. For messages to make it through antispam and antivirus checks, the criminals correctly configure SPF entries on the DNS server and indicate the correct DKIM signatures for their messages. This approach allows bypassing verification of the address of the sender's mail server, but offers digital evidence for investigators.

Despite the increased complexity involved, in the first quarter of 2017 the Cobalt group also began to attack various companies that partner with banks, then send phishing messages from these partners' infrastructures using the hacked accounts and mail servers of real employees.



This approach ensures that recipients are likely to trust the sender and has a number of advantages:

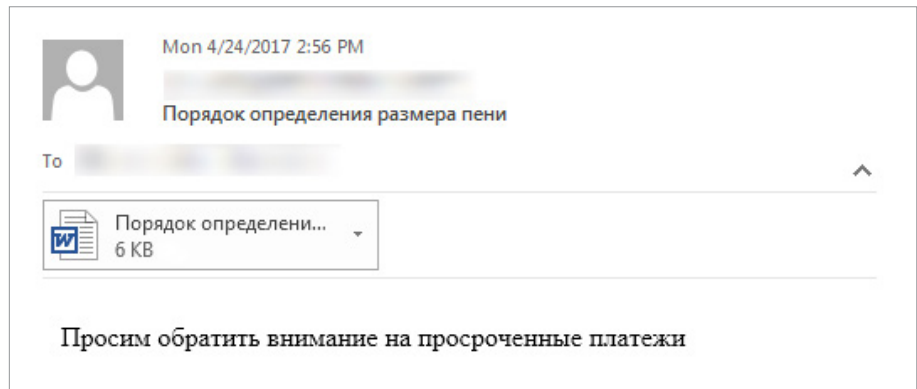
- + Attackers get information stored on the servers and in the databases of the compromised partner organization. This information can be used to create convincing phishing messages.
- + Attackers obtain access to employee accounts on workstations and mail servers, giving phishing messages a high degree of trust and plausibility among potential recipients.
- + Messages from partners are not blocked by mail server filters.



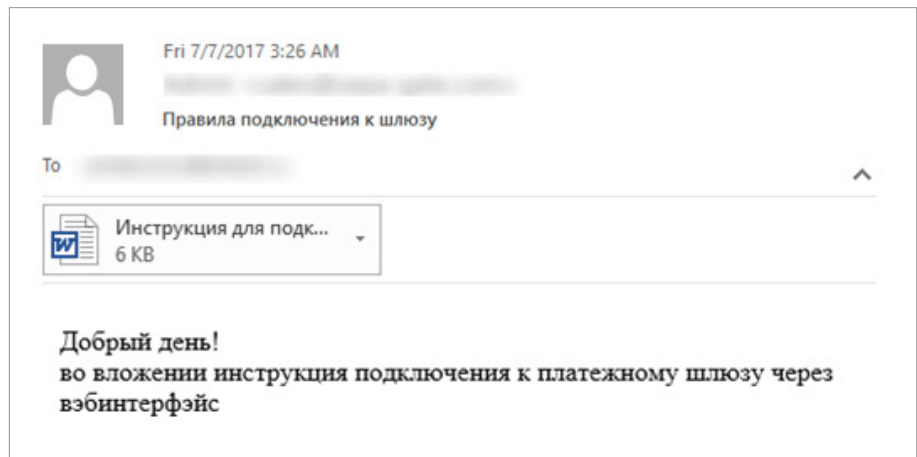
The attackers carefully choose subject lines, recipient addresses, and attachment names that will "fly below the radar" so that recipients open the attachments enclosed with phishing messages.

Today, Cobalt uses phishing mailings at practically all stages of targeted attacks on banks.

1. Initial compromise starts with one or more workstations at a partner organization, which have been infected via phishing.

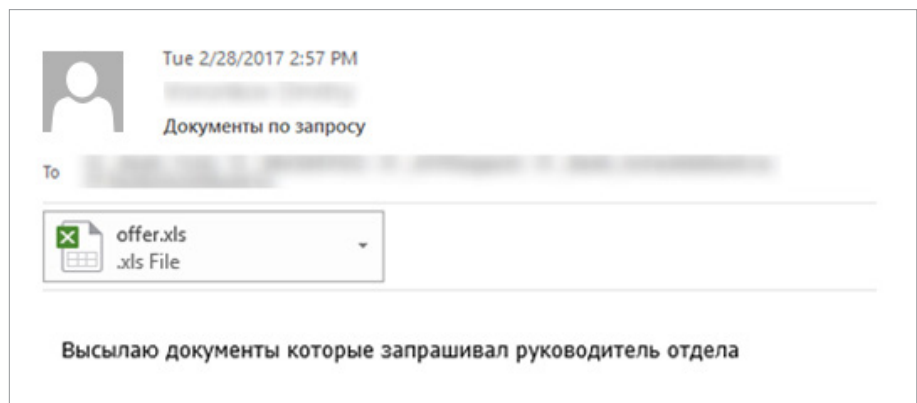


A message informing of "missed payments"

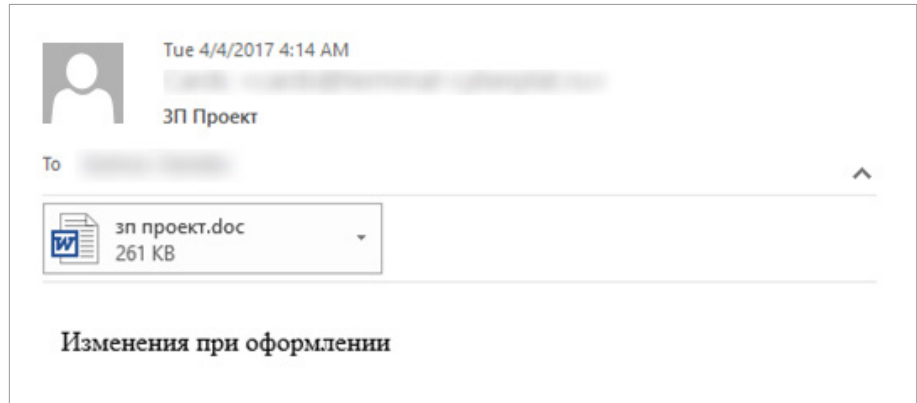


Instructions for connecting to a payment gateway—supposedly

2. The attack against the partner organization is then developed by means of internal mailings containing malicious documents supposedly from colleagues, management, or IT.

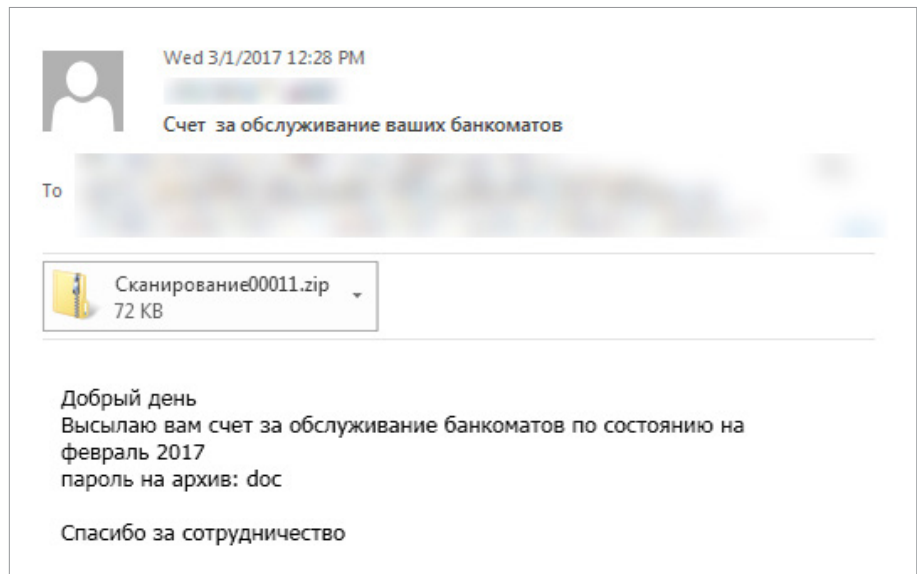


"Documents requested by the head of the department"



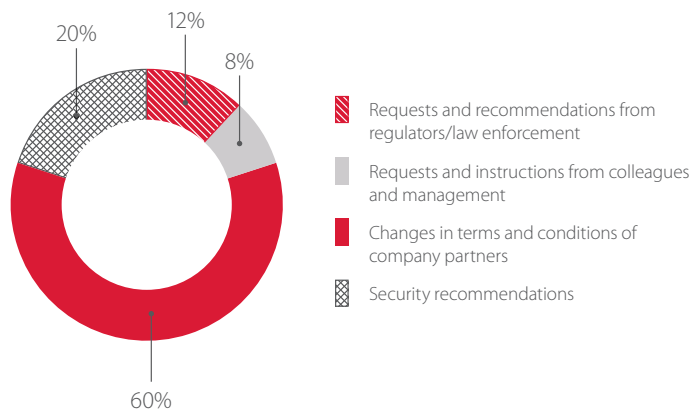
A message claiming to inform of payroll changes

3. Malicious messages are sent from the partner's infrastructure to banks and other financial organizations.



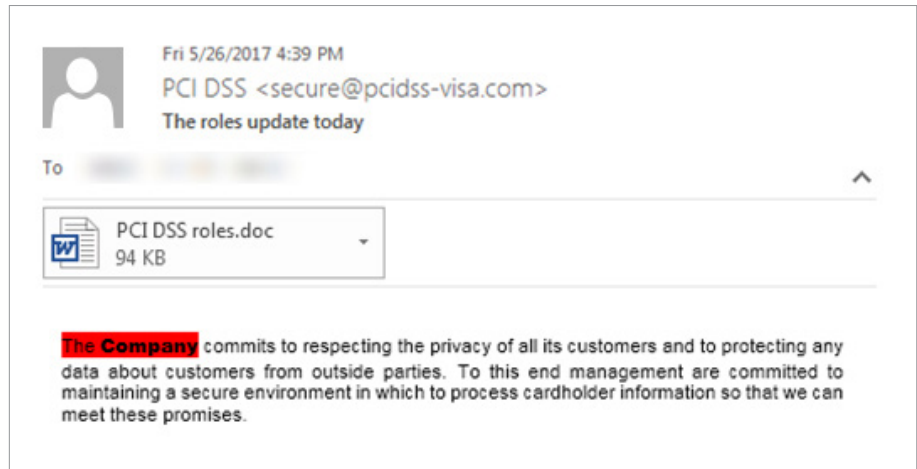
A password-protected archive (with the password "doc") supposedly containing an invoice for ATM maintenance

In early 2017, 60 percent of phishing messages from Cobalt related to cooperation and service terms between banks and their partners.

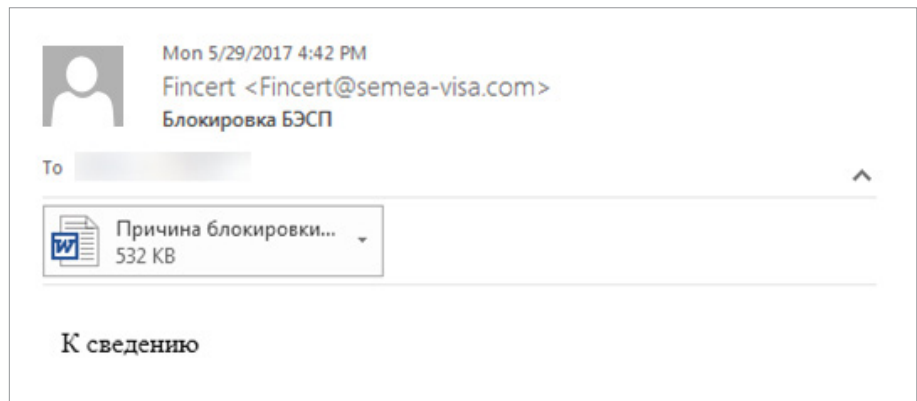


Subjects of phishing messages

In 2017 Cobalt began to use security anxieties as an attack vector. The group has sent messages from illegitimate domains posing as VISA, MasterCard, and FinCERT units of the Russian Central Bank and National Bank of the Republic of Kazakhstan.

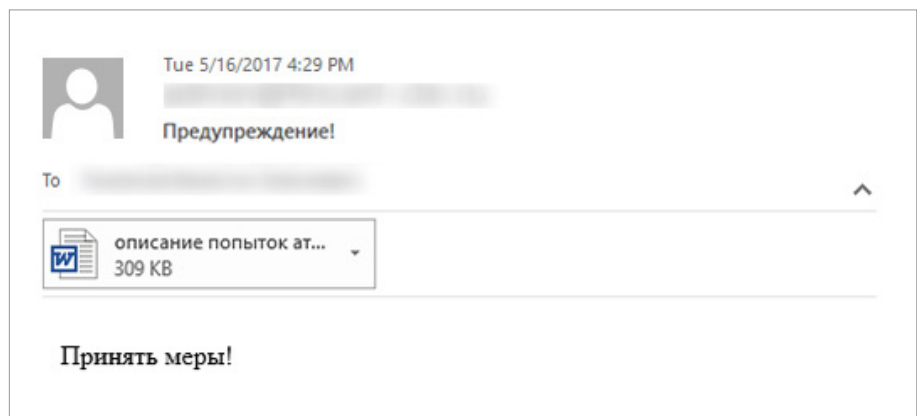


Broken English and copied boilerplate text can be convincing in the right circumstances



A fake FinCERT message

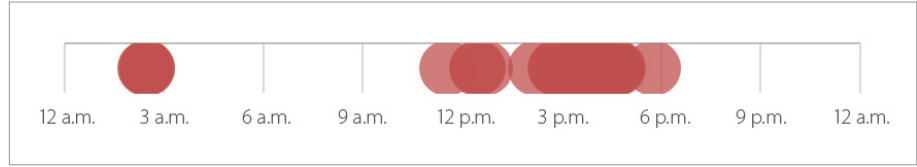
In Russia, this was a particularly ironic "twist" since FinCERT had been actively warning financial companies about the Cobalt threat. So the group took advantage of such anxiety to send messages to banks with malicious documents, supposedly on how to keep bank systems safe.



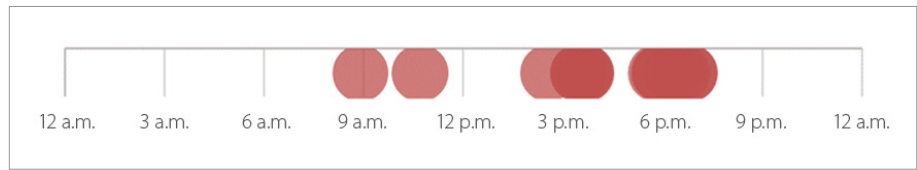
A vague warning that asks the user to act immediately

So by creating counterfeit domains superficially similar to those of real companies, the criminals use the imprimatur of well-known organizations to convince users to open dangerous attachments.

Since real messages from colleagues and partners usually arrive during working hours, the criminals structured the mailings so that employees would receive them during working hours (no matter in which time zone the attackers themselves were located).

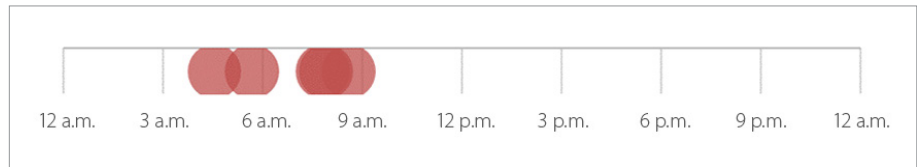


Time of message receipt for Eastern European companies (UTC+3)



Time of message receipt for Central and Southeast Asian companies (UTC+6)

Most messages were received in the afternoon—the reason being that employees tend to be less vigilant, and therefore more susceptible to phishing, as the evening approaches.

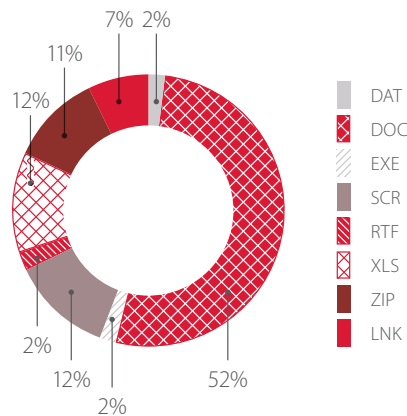


Time of message receipt for North American companies (UTC-4)

We noticed a slight variation in tactics against North American companies. Messages targeting U.S. and Canadian organizations were sent from the compromised infrastructure of a European partner. For the phishing messages to be plausibly European in origin, the criminals performed the mailing during European working hours, due to which the targets received emails in the early waking hours in the U.S. and Canada.

5.2. Malicious attachments

To ensure remote access to the workstation of an employee at a target organization, the Cobalt group (as in previous years) uses Beacon, a Trojan available as part of commercial penetration testing software Cobalt Strike.



Types of malicious files

The Trojan is delivered and run with the help of a special dropper. The dropper consists of .scr or .exe files that are placed on the victim's computer in one of the following ways:

- + In a password-protected ZIP archive, the password to which is given in the text of the phishing message
- + Downloaded from a hacked website when a malicious attachment (.doc, .xls, .rtf) is opened from the phishing message
- + Downloaded from a hacked website based on commands coded in a LNK file that is in a ZIP archive attached to the message

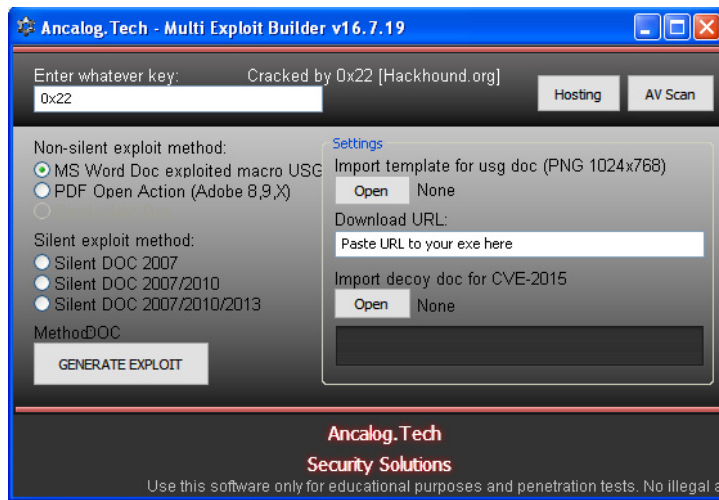
Poorly protected websites are compromised by the attackers and used, in essence, as file hosts for spreading malicious files in attacks against banks.

52 percent of the Cobalt phishing messages reviewed by our researchers contained Microsoft Word documents.

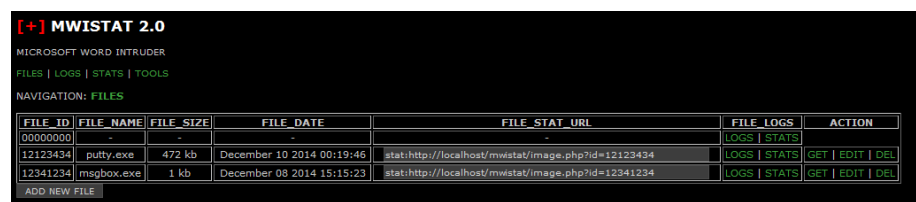


Poorly protected websites are compromised by the attackers and used, in essence, as file hosts for spreading malicious files in attacks against banks.

The malicious Microsoft Office documents that trigger download of the dropper are created using the Ancalog and Microsoft Word Intruder (MWI) exploit kits. With these kits, even a hacker without programming skills can create malicious Word documents and PDF files in an intuitive visual interface in just minutes.

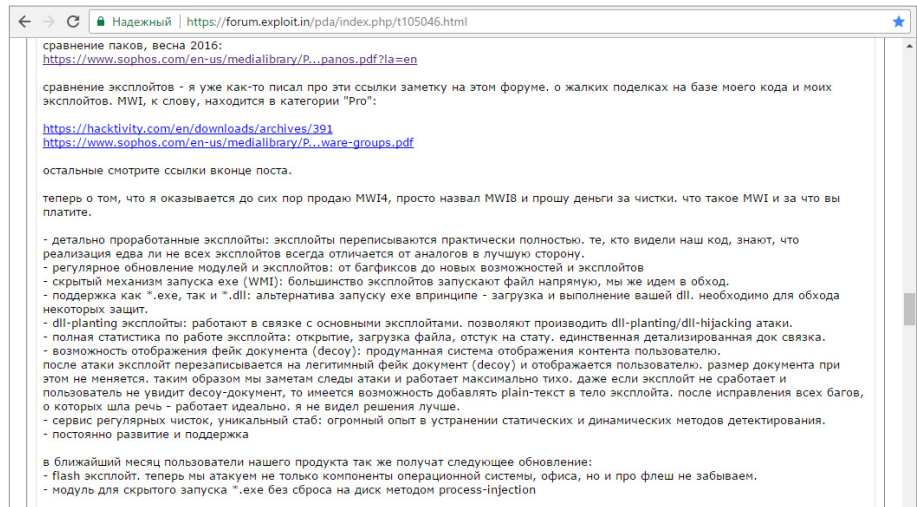


The Cobalt group was one of the first to get their hands on a restricted version of MWI that can create documents exploiting the critical vulnerability CVE-2017-0199. Since the version in question was sold on an individual basis to customers well known to the developer, there may be a relationship between the Cobalt group and developer of MWI. One instructive fact in this regard is that less than a week passed between announcement of a new MWI version and use by Cobalt of attachments exploiting vulnerability CVE-2017-0199.⁶



⁶ www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target

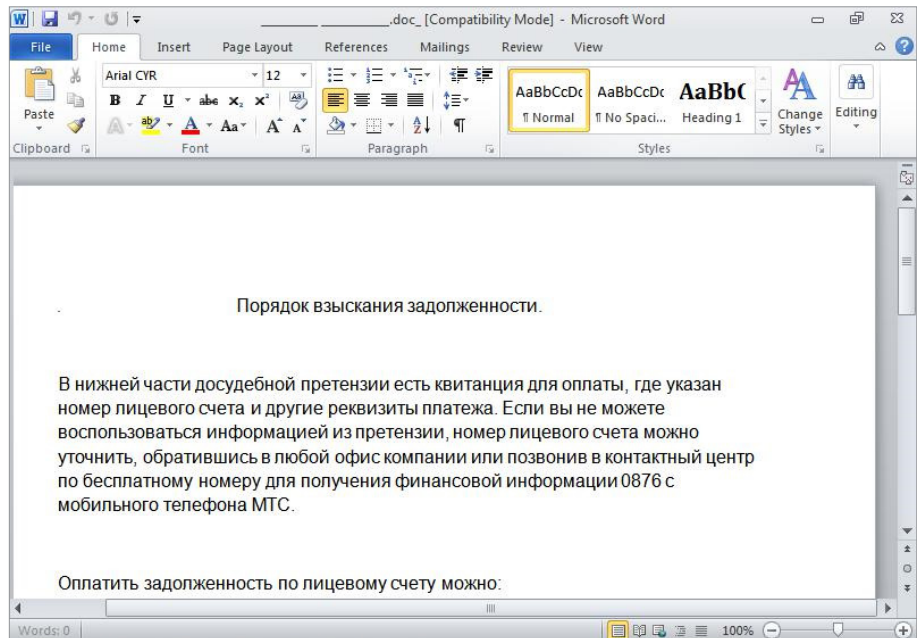
MWI is positioned by its developer as a tool for conducting APT; if the software is instead used to create files for mass spamming, the developer revokes the license. For users of the restricted version of MWI, the developer offers a sort of "scrubbing" so that files will not be flagged by currently available antivirus scanners.



The MWI developer boasting of the "product" online



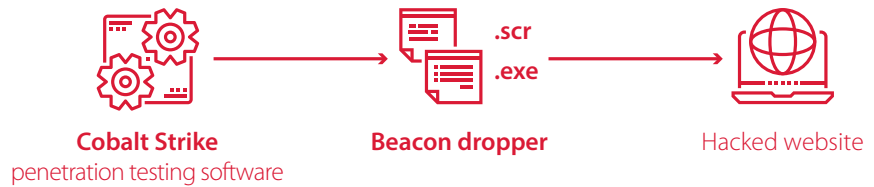
Malicious documents sent by Cobalt to banks and their partners use exploits for vulnerabilities CVE-2017-0199, CVE-2015-1641, and CVE-2012-0158 in order to download and run the dropper on the victim system.



An official-seeming document about how to pay overdue debts

When the attachment is opened, malicious code is run. This code takes advantage of vulnerabilities in Microsoft Office to download the dropper from a remote server and run it.⁷ After the code finishes running, a decoy document (such as shown in the screenshot above) is displayed.

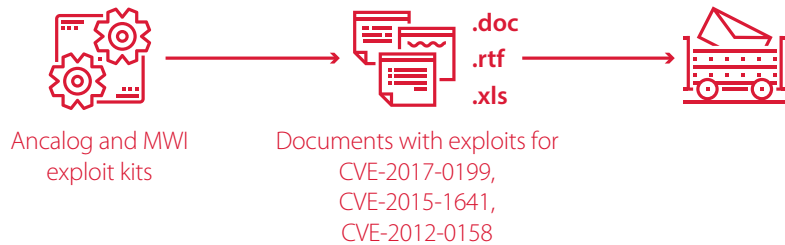
⁷ blog.fortinet.com/2017/05/30/spear-phishing-fileless-attack-with-cve-2017-0199



Upload of trojan to previously hacked site

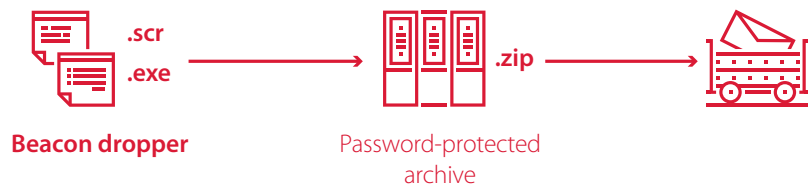
The attackers upload files to vulnerable sites in advance, from where the files can be later downloaded to victim systems during an attack. Therefore we urge website owners to be vigilant in securing their sites: if weak protections cause a site to become a staging ground for malware, regulators may block the site or law enforcement may seize server equipment as part of a criminal investigation. Public knowledge of such incidents is likely to cause severe damage to company reputation.

Usually Cobalt phishing messages are sent in several waves. In the first wave, the criminals send Microsoft Office documents created using the described exploit kits.



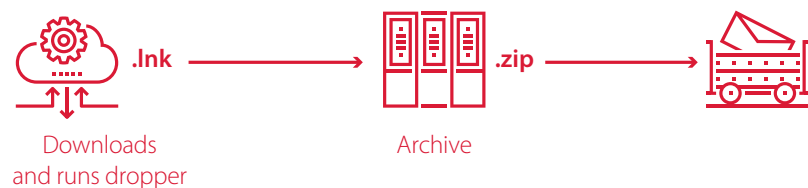
First wave of spear phishing

If there are no "hits" from targeted users within 24 hours of a mailing (this is possible if a company has up-to-date versions of Microsoft Office that are free of the vulnerabilities targeted by the exploit builders), the attackers send a second wave.



Second wave of spear phishing

Attached to the messages is a dropper, consisting of .exe or .scr executable files, in a password-protected archive. By placing the files in an archive, the attackers can bypass some filtering and antivirus systems. Solutions are available for real-time scanning of encrypted archives (when the password is indicated in the body of the message, as is the case here) but organizations making use of such software are few and far between.

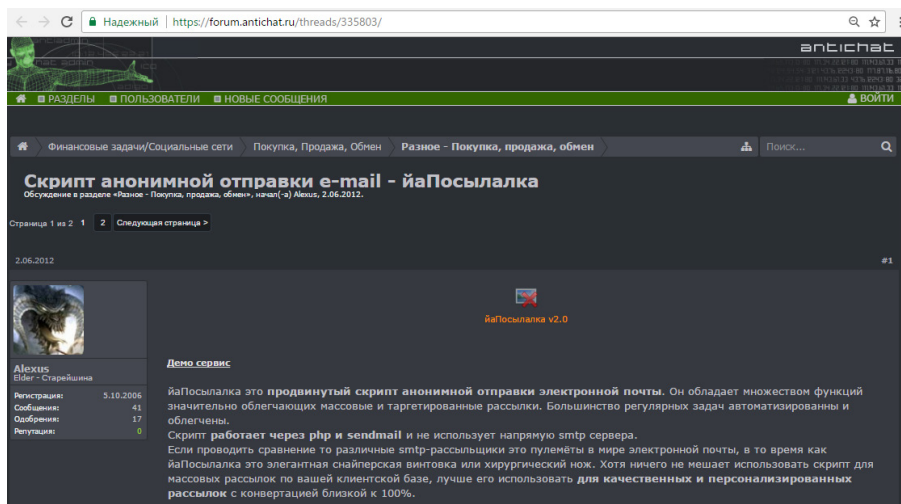


Spear phishing

In addition, we have observed a separate mailing in which the attached archives contained LNK files; as in all the other cases, these files are used to download the Beacon dropper.

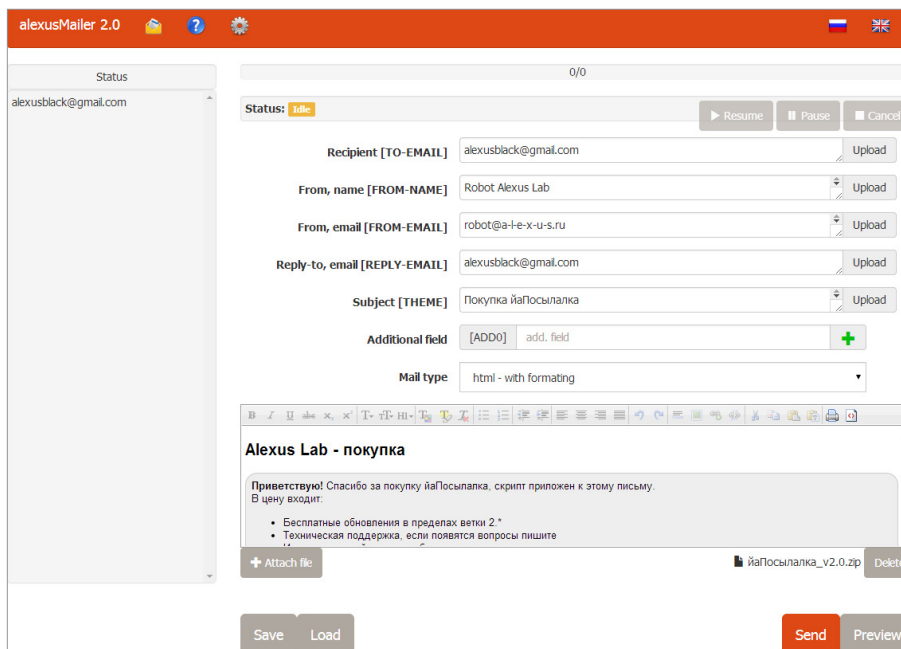
5.3. Cobalt infrastructure

Since a Cobalt mailing is sent to thousands of recipients, the group clearly is using some sort of automation. Based on analysis of the phishing messages, we believe that the messages are sent from phishing domains with the help of alexusMailer v2.0, a freely available PHP script used to send emails anonymously.⁸



alexusMailer and other scripts are available on forums

The script includes support for multithreaded sending, a visual editor for messages, import of recipient lists and other fields from files, templates, attaching any number of files to a message, and more. Users can distribute sending tasks over a number of servers and set a delay for message sending.



alexusMailer interface

However, when messages are sent with alexusMailer, the message header contains an artifact: the X-PHP-Originating-Script field contains the name of the file of the PHP script that was used to send the messages. This means that on servers used for sending, the php.ini configuration file is set to log outgoing mail.

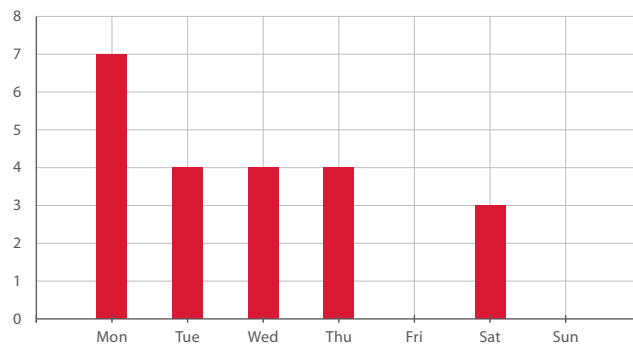
8 github.com/AlexusBlack

```
Received: from www-data by pcidss-visa.com with local (Exim 4.80)
(envelope-from <www-data@pcidss-visa.com>) id 1dEFNS-0004JT-EX for
Fri, 26 May 2017 13:34:28 +0000
To:
Subject: =?UTF-8?B?V6h1IHJvbGVzIHVwZGF0ZS00b2RheQ==?=
X-PHP-Originating-Script: 0:alexusMailer_v2.0.php
From: =?UTF-8?B?UENJIERTUw==?= <secure@pcidss-visa.com>
MIME-Version: 1.0;
Content-Type: multipart/mixed; boundary="--mPzo4To60J"
Reply-To: <secure@pcidss-visa.com>
Message-ID: <E1dEFNS-0004JT-EX@pcidss-visa.com>
Date: Fri, 26 May 2017 13:34:28 +0000
```

The Cobalt group uses widely available public mail services, as well as services that allow anonymous registration of temporary addresses. Some of the domains used for reply addresses in Cobalt mailings include: TempMail (@doanart.com, @rootfest.net), Mail.com (@mail.com), AT&T Mail (@att.net, @sbcglobal.net), and Yahoo! (@ymail.com). These same services were used by Cobalt to create email addresses when registering domains.

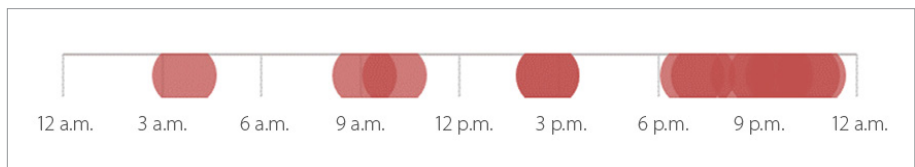
Based on the times at which the domains in the Cobalt infrastructure were registered, we found that the attackers tended to register domains towards the beginning of the week. This enables us to speculate on their working schedule:

- + On weekdays, the attackers actively register domains, prepare hacking tools, and (less often) send phishing mailings.



Days on which domains were registered

- + At the end of the week, the group concentrates on sending out mailings and advancing their attacks within the infrastructure of compromised organizations.
- + Since phishing mailings are sent out during working hours, domains are usually registered during the interval from 6:00 p.m. to 12:00 a.m. (UTC+0), which coincides with the end of the working day in European countries.



Time of domain registration (UTC+0)

It would seem that after registering a domain at the beginning of the week, the Cobalt group takes some time to prepare for their upcoming phishing campaign, which as noted usually comes at the end of the week. On average, the time from domain registration to the first phishing mailing with that same domain is four days.

Our researchers discovered a number of Cobalt phishing domains before the group was able to use them in its phishing campaigns. By acting quickly, it was possible to block the domains.

Working in cooperation with industry regulators in Russia and other countries, we have succeeded in disabling delegation for all .ru domains and most other top-level domains known to be associated with Cobalt.

CONCLUSION

The barrier to entry for would-be cybercriminals keeps falling every year. No longer do hackers need to look for zero-day vulnerabilities and expensive tools to perform attacks. Instead, all they require are basic programming skills, commercially available software, and instructions posted on the Internet.

Banks and other companies must realize that attackers are constantly refining the tools and techniques they use. In today's environment, a company can fall victim just by getting caught in the middle as attackers scout for stepping stones to reach their ultimate target. That's why responsible companies can no longer remain complacent about security and pretend that hackers go after only large companies and banks, or target only far-away areas of the world. No matter their industry or ownership—whether banks, state-owned organizations, or whatever else—companies must keep protection of their digital infrastructure current and proactively update their software and operating systems. Employees must be trained to increase their security awareness and resist phishing attempts. Moreover, scanning should go beyond just incoming messages and attachments to include outgoing messages, with retrospective analysis. Public-facing web applications must also be protected—if company infrastructure or sites are compromised by an attacker, this can wound company reputation, cause blocking of company servers, trigger a drop in search engine ratings, and drive away customers.

Information about the extent of losses caused by the Cobalt group in 2017 is not yet available. Perhaps warnings by bank regulators headed off some of the group's efforts. We will continue to monitor the Cobalt group and report new details as they become available. Judging by the scale of Cobalt campaigns worldwide, multimillion-dollar losses by banks are a real possibility. And if attacks on financial exchanges are successful, the consequences will include not only direct losses to individual companies, but rate turbulence on world currency markets.

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.

© 2017 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.