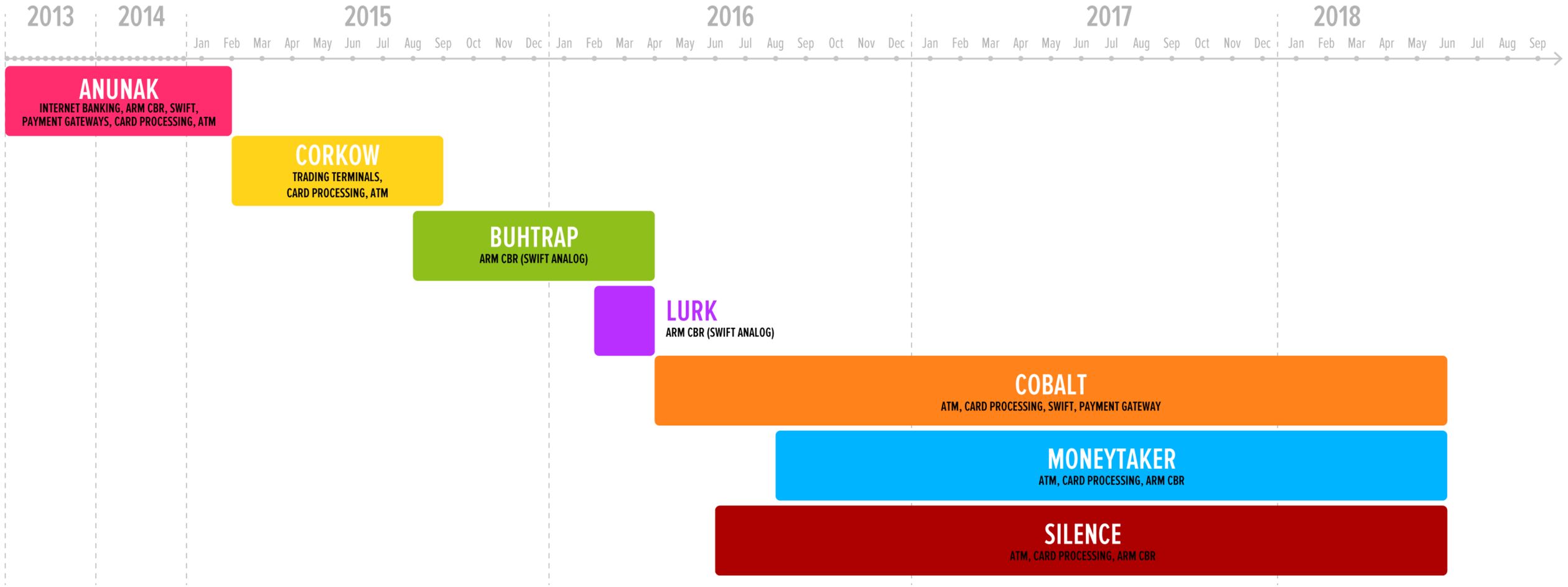
An Evolution of Targeted Attacks - Case Study “Cobalt”

- Tool, Techniques and Procedures
- Attribution

Camill Cebulla
Director EMEA
cebulla@group-ib.com

Advance Persistent Threat Groups



Case Study: The Evolution of Cobalt

Interbank systems, Card processing, ATMs, Payment gateways

Cobalt Timeline

2016

- **March** — Last confirmed attack by Buhtrap gang
- **April** — Arrest of ML group for Buhtrap
- **May** — First attack in Russia
- **June** — Attack on ATMs in Taiwan **First Bank**
- **August** — Begin preparation of attacks on **card processing**
- **September** — Public Group-IB report about logical **attacks on ATMs**
- **November** — The first successful attack on card processing **In Kazakhstan**

2017

- **January** — The first attack with ransomware: **PetrWrap**
- **January** — Attacks on Supply chain (**integrators and service providers)**
- **February** — Improving the quality of phishing
- **February** — Penetration into banks through **Supply chain**
- **April** — Start testing of a new **Reconnaissance backdoor** (test.dll)
- **April** — **First decoy** documents
- **May** — Active use of the new **JS-backdoor v2.0** in attacks with English language phishing emails
- **June** — First attack on **Telecoms company** In Russia
- **August** — Use of the new **InfoStealer v. 0.2**
- **September** — Instant adaptation of **1-day exploits**
- **September** — Start to use **SPF and DMIK**
- **November** — First theft through **SWIFT in Russia**
- **November** — New **Java-stager & 2-step infection**
- **November** — **ATM attack** after long pause in Russia

January | February | March | April | May | June | July | August | September | October | November | December

Cobalt Timeline – in cooperation with Anunak (Carbanak)

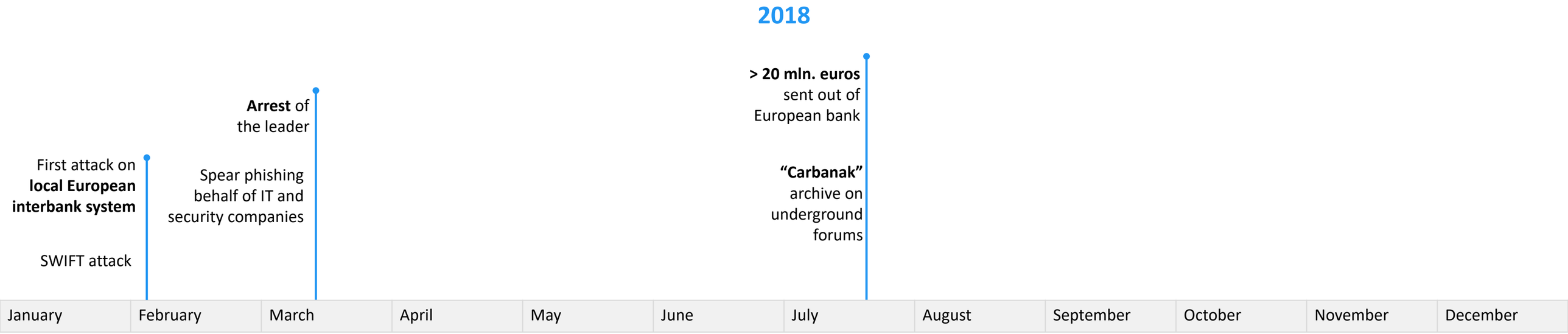
2016

- **January**
- **February**
  - Last confirmed attack by Buhtrap gang
  - Server activation & configuration used in SWIFT attack in Hong Kong
- **March**
  - **Joint operation** of theft through **SWIFT** in Hong Kong
  - **Joint operation** of theft through SWIFT in Ukraine **Credit Dnepr bank**
- **April**
- **May**
  - Arrest of ML group for Buhtrap
- **June**
  - First attack in Russia
- **July**
  - Attack on ATMs in Taiwan **First Bank**
- **August**
- **September**
  - Begin preparation of attacks on **card processing**
- **October**
  - Public Group-IB report about logical **attacks on ATMs**
- **November**
  - The first successful attack on card processing **In Kazakhstan**
- **December**

2017

- **January**
  - The first attack with ransomware: **PetrWrap**
  - Attacks on Supply chain (**integrators and service providers)**
- **February**
  - Attacks on companies **e-wallets and terminals**
  - Improving the quality of phishing
  - Penetration into banks through **Supply chain**
- **March**
  - The first attack on **Payment gateways (e-wallet company)** Using a unique program.
- **April**
- **May**
  - Start testing of a new **Reconnaissance backdoor** (test.dll)
  - **First decoy** documents
- **June**
  - Active use of the new **JS-backdoor v2.0** in attacks with English language phishing emails
- **July**
- **August**
  - First attack on **Telecoms company** In Russia
- **September**
  - **Joint operation with Anunak (Carbanak) tools** to steal through a payment gateway
  - Use of the new **InfoStealer v. 0.2**
- **October**
  - Instant adaptation of **1-day exploits**
  - Start to use **SPF and DMIK**
- **November**
- **December**
  - First theft through **SWIFT in Russia**
  - New **Java-stager & 2-step infection**
  - **ATM attack** after long pause in Russia

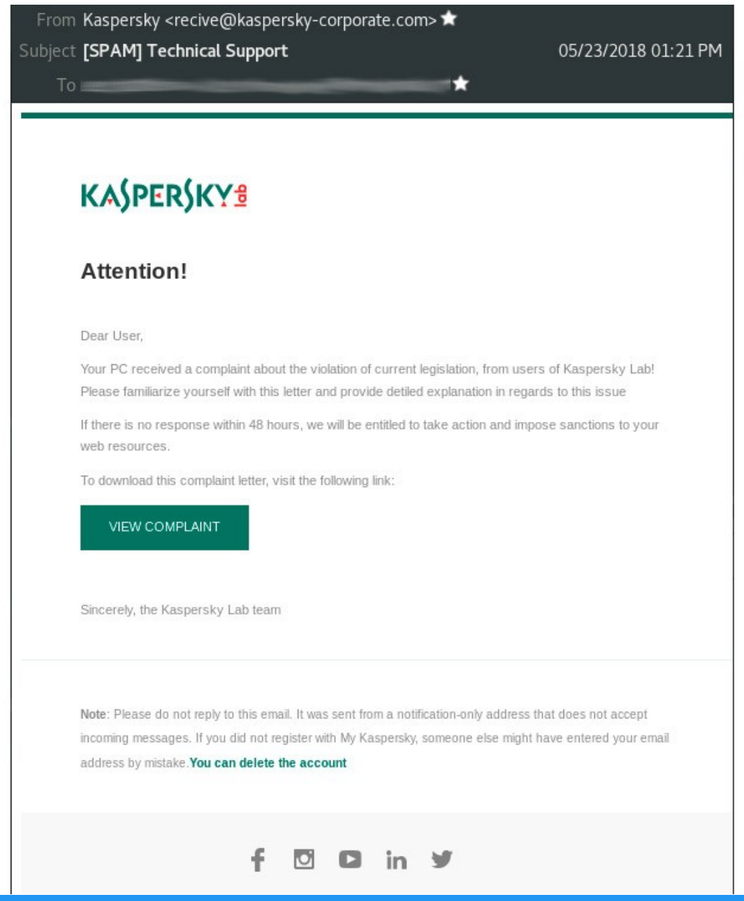
Cobalt Timeline



New Cobalt spring

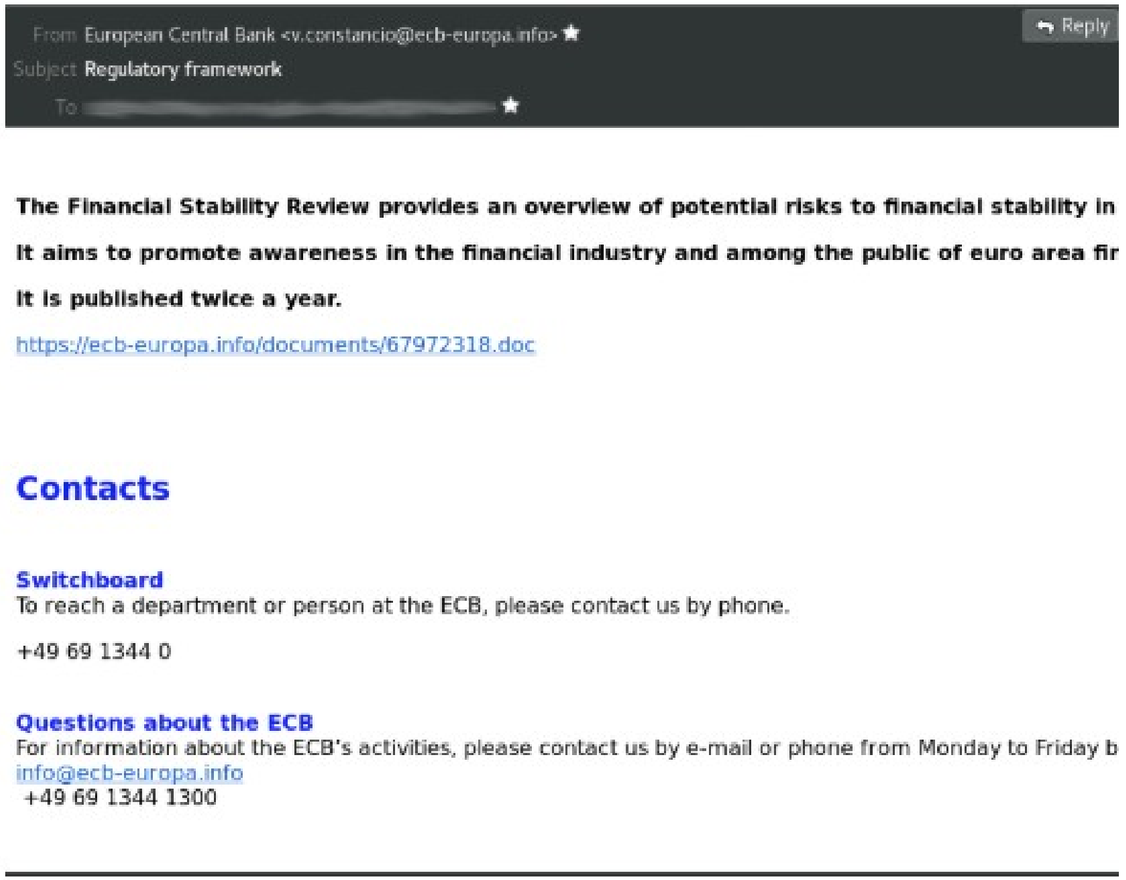
May, 23

Phishing emails were sent acting as a major anti-virus vendor, containing unique Trojan «CobInt»

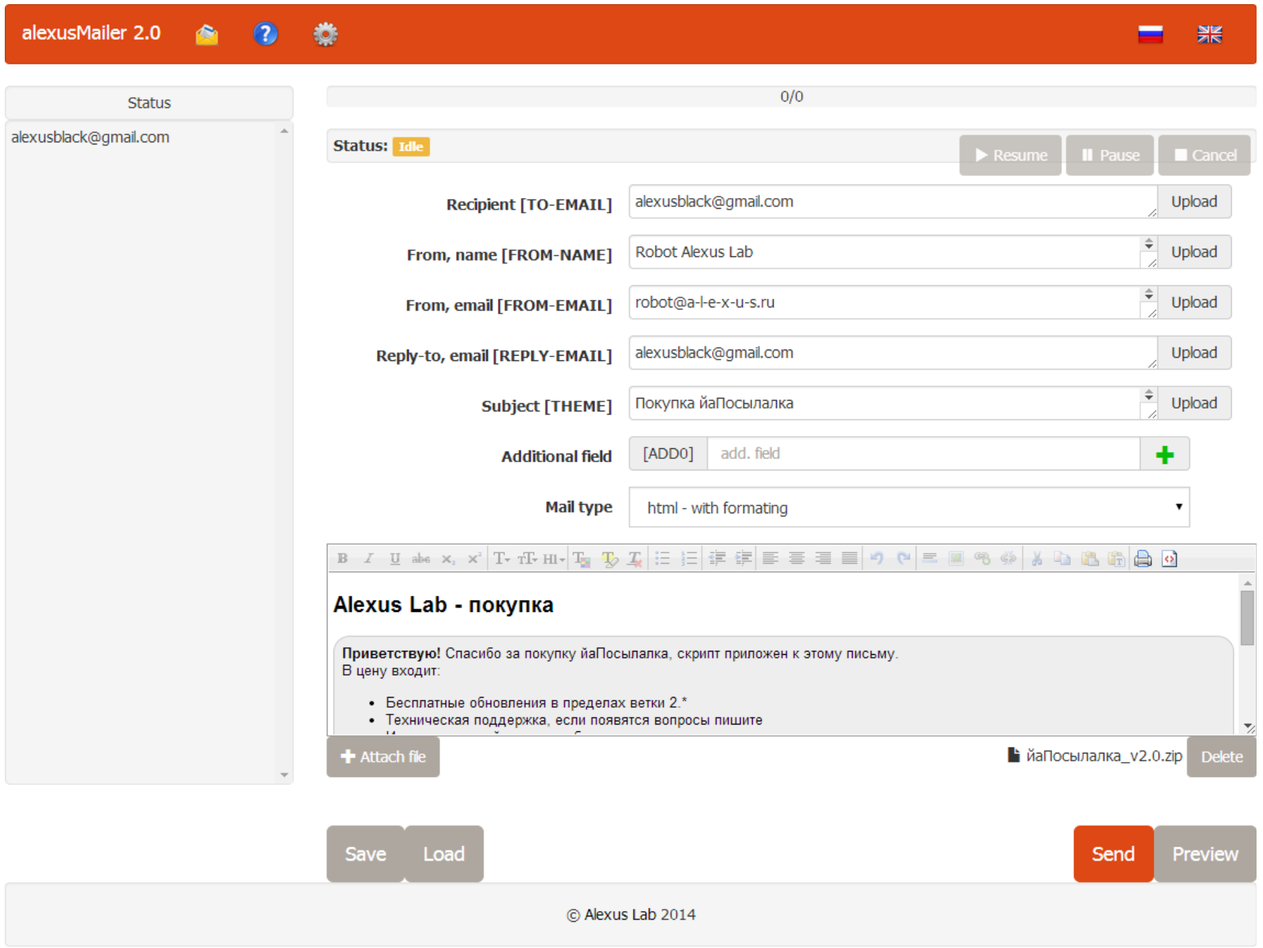


May, 28

Emails purporting to be from the European Central Bank contain a link to the file '67972318.doc', which triggers the exploitation of the CVE-2017-11882 vulnerability



Spear phishing



Mailing tool

- Since 2016 until present Cobalt uses the same tool to send emails – alexusMailer 2.0 aka iPosylka developed by Russian speaking developer in 2011. https://github.com/AlexusBlack/alexusMailer-2
- Only since November of 2017 have Cobalt started to configure SPF and DKIM on mail servers.

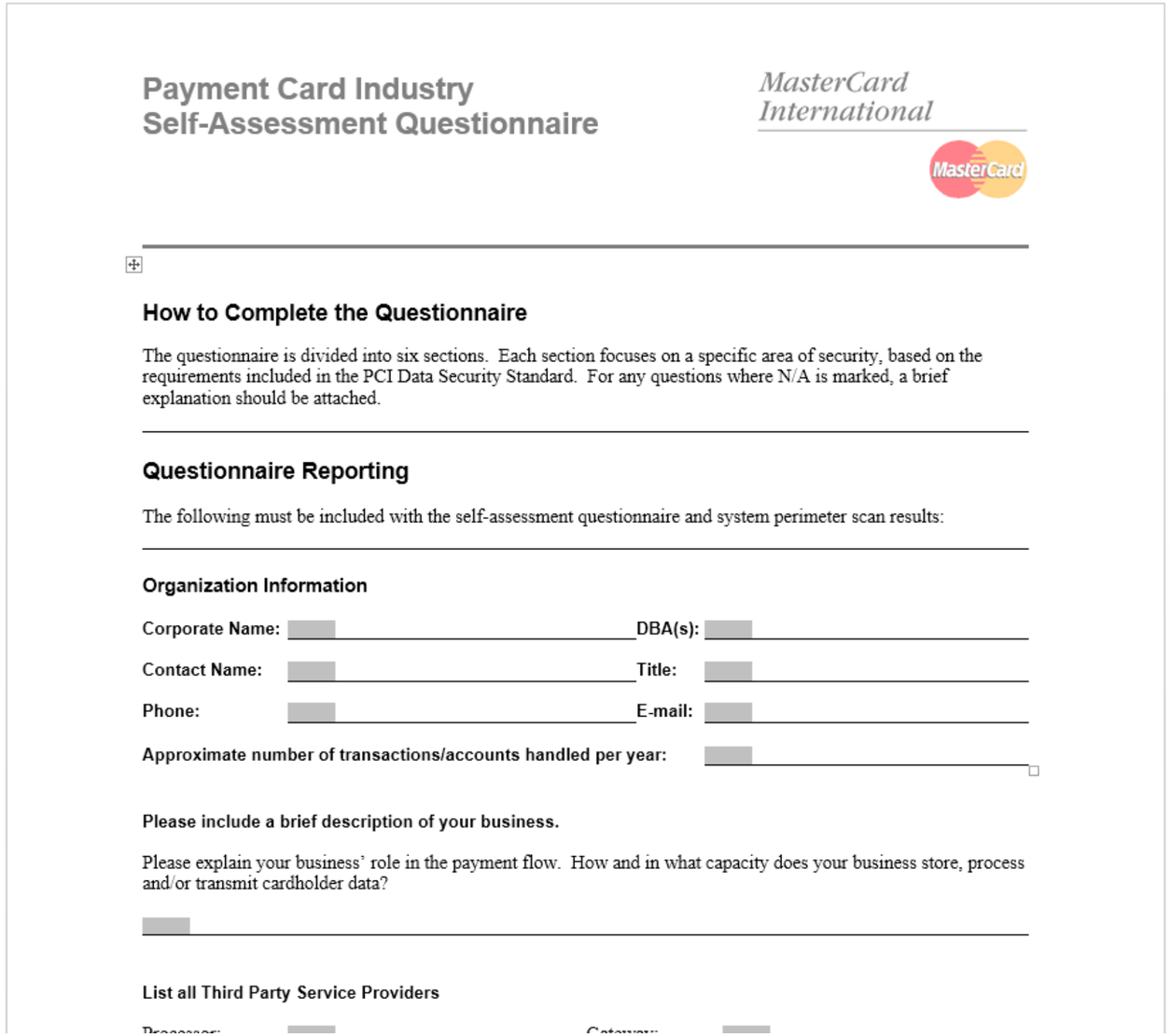
Attachments

- Documents: DOC, XLS, RTF, LNK, HTA
- Executables: EXE, SCR
- Documents and executables in archives with passwords and without them.
- Only in December 2017 they used email with link on malicious Java applet rather than attachment.

Exploit builder

- **Ancalog Exploit Builder** aka OffensiveWare Multi Exploit Builder (OMEB) – generates malicious files DOC, JS, HTA, PDF, VBS и CHM. Advertising on forums and sites like ancalog.tech, ancalog.win, offensiveware.com
- **Microsoft Word Intruder** (MWI) developed by Russian speaking developer with nickname Object since 2010. Generates DOC files that can contain up to 4 exploits at the same time.

Spear phishing



Payment Card Industry
Self-Assessment Questionnaire

MasterCard International

How to Complete the Questionnaire

The questionnaire is divided into six sections. Each section focuses on a specific area of security, based on the requirements included in the PCI Data Security Standard. For any questions where N/A is marked, a brief explanation should be attached.

Questionnaire Reporting

The following must be included with the self-assessment questionnaire and system perimeter scan results:

Organization Information

Corporate Name: DBA(s):

Contact Name: Title:

Phone: E-mail:

Approximate number of transactions/accounts handled per year:

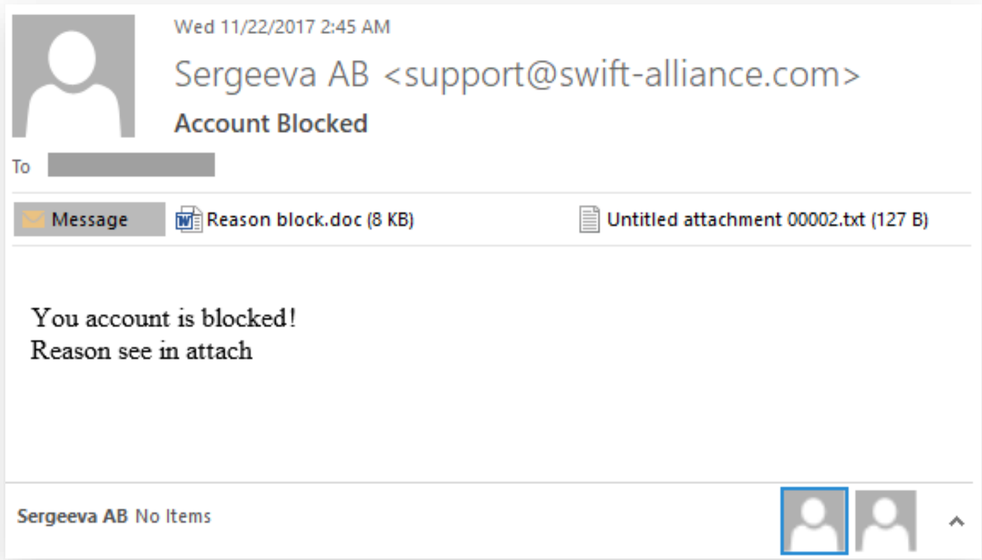
Please include a brief description of your business.

Please explain your business' role in the payment flow. How and in what capacity does your business store, process and/or transmit cardholder data?

List all Third Party Service Providers

Email body and the Decoy documents

- Only since May of 2017 Cobalt started to used well prepared decoy documents. Before that, if victims opened an attached document it would not display any content, which can be construed as suspicious.
- Absence of decoy documents helped Cobalt on occasion, because users resent malicious email to other users to check if document will open.
- In most cases the email body does not have a well written text. Usually it is one or two sentences and signature is absent.
- Only in Supply chain attacks did Cobalt copy original emails of compromised companies with well written text and signatures.



Wed 11/22/2017 2:45 AM

Sergeeva AB <support@swift-alliance.com>

Account Blocked

To

Message | Reason block.doc (8 KB) | Untitled attachment 00002.txt (127 B)

You account is blocked!
Reason see in attach

Sergeeva AB No Items

Attacks on Supply chain

Supply chain attack – infected system integrators, software vendors, service providers.

New vector to deliver malware

- In February 2017 Cobalt successfully compromised a Supply chain company (IT Integrator).
- They used their mail server to send spear phishing, targeting companies in Russia, Kazakhstan, Moldova, Azerbaijan, Tajikistan and their local offices in other counties (Turkey, Indonesia, Vietnam, Singapore).
- Within the next 9 months Cobalt compromised at least 3 more “Supply chain” companies. One of them in Ukraine and other in Russia.
- In August they compromised a Russian Telecom company. The attack was stopped and it is unclear what was the final goal of attackers.

Unused potential

- In all cases they used the mail server of the compromised company to send spear phishing against their clients.
- We did not detect any watering hole attacks, even when attackers compromised the victim network.
- Attackers did not use the software of the compromised vendor to deliver malware.
- Only in one instance did Cobalt use the infrastructure of the compromised IT integrator, (remote channels to their clients) to infect them.

Lateral movement & Persistence & Remote control

Lateral movement

- For network scanning they use: SoftPerfect Network Scanner, Eternal Blues, EternalPunch 0.3.0
- Manual dump of the network administrator's **keepass** database
- **Mimikatz** to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory.
- Searched for passwords stored in Active Directory group policies by exploiting the **MS14-025**: Vulnerability in Group Policy Preferences

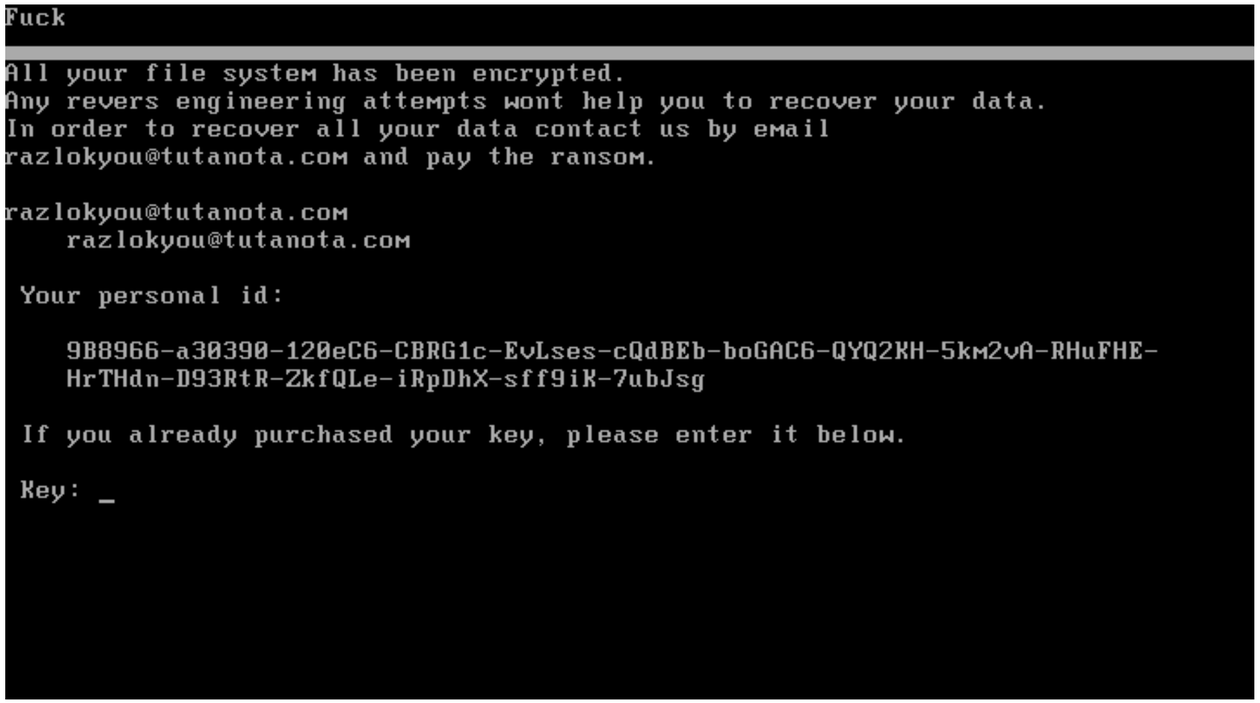
Persistence

- For persistence Cobalt use servers with long uptime.
- Creating services and autorun keys to launch powershell.exe and passing arguments to start CobaltStrike stager.
- Create local account **support452** with RDP permissions.
- Adding new C2 servers in the development of the attack.
- Create tasks in Windows Task Scheduler +3 weeks after thefts to launch CobaltStrike stager with future C2 server.

Remote control

- VNC built into CobaltSrike
- Radmin, AmmyAdmin, TeamViewer
- RPIVOT (reverse socks 4 proxy) precompiled with py2exe.
- Use of corporate RDP and VPN servers that allows remote.

PetrWrap



Ransomware to hide traces

- In February 2017 Cobalt compromised a small Russian bank. Using corporate antivirus management software, they launched file out.exe
- Out.exe – was the new ransomware PetrWrap. It is modified version of well known Petya ransomware later used in NotPetya attack (otherwise unrelated).
- After the encryption process was completed, a message is displayed that encryption was performed, with the requirement to contact the attacker via email razlokyou@tutanota.com

Reconnaissance & JS – backdoor 2.0

Reconnaissance – backdoor

- In May of 2017 Cobalt spear phishing with PCI DSS related attachments exploited CVE-2017-0199.
- After exploitation a new test backdoor launched on the system. Testing is also indicated by the internal name of the module test.dll.
- **Test.dll** is a reconnaissance module. It was able to collect information like:
  - Operating system
  - User
  - Active processes
  - List of files in %USER%\Desktop\
  - Create screenshots
  - Cookies and browser history
- Additionally it supported command:
  - Download files
  - Remove itself

JS – backdoor 2.0

- In July Cobalt use new JS-backdoor v2.0 in attacks on the English-speaking countries.
- After exploitation malicious DLL will download JS-backdoor. But prior to download this DLL will check if current year = 2017 and the process name that launched it. If checks fail, the JS-backdoor will not be downloaded.
- Execution scheme used by the malware is previously described by researcher Casey Smith @subTee and help them to successfully bypass whitelist protection.
- JS-backdoor supports these commands:

Command	Description
d&exec	Download and execute the file
more_eggs	Download the new SCT script
gtfo	Self remove from the system
more_onion	Run a new SCT script
more_power	Run an arbitrary command

InfoStealer v. 0.2

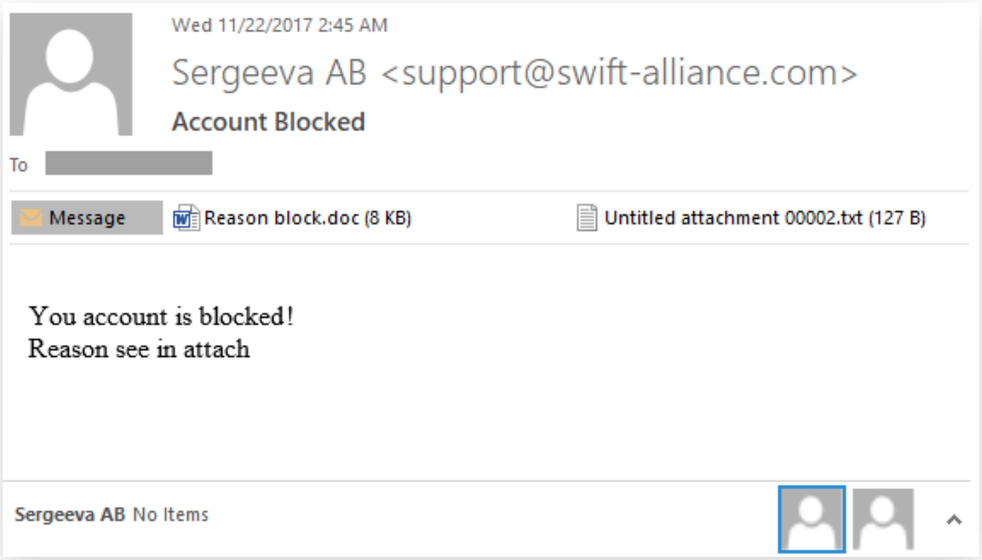
Short history

- In early September, Cobalt sends out the RTF document "New Business Venture.doc" with the vulnerability exploit CVE-2017-0199 in MS Word.
- As a result of the exploit the x1.db file was downloaded - the executable DLL.
- DLL implemented JS backdoor functionality in the executable, but without the ability to download and execute.
- This Info Stealer was version 0.2. It is completely memory-hosted and does not leave traces on the file system.

Functionality

- It is executed only if the file was started by the **odbcconf.exe** process.
- After start, start cycled delays to avoid sandbox detection. Total delay was about 10 minutes.
- Backdoor collects and sends data about the serial number of the system volume, PC name, user name, AV system availability, OS version, OS bit, malware version.
- Extract user data, including passwords from: Mail clients, Browsers, SSH/FTP clients.
- Collect data from the Address book.
- Collect from the system the list of visited web pages.

1-day exploits adaptation



Premium support with exploits

- On November 14, 2017, Embedi specialists published a technical report on the vulnerability CVE-2017-11882. The same day Microsoft patched this vulnerability.
- November 21, in the public GitHub repository Embedi published Proof of Concept for this vulnerability https://github.com/embedi/CVE-2017-11882
- Just few hours later, Cobalt began a massive phishing campaign to financial institutions that contained a malicious document that was not detected by antivirus solutions.
- A few hours later, anti-virus solutions began to detect the file as malicious.
- The same day, Cobalt modified document and continue spear phishing campaign behalf of Central bank of Russia and SWIFT Alliance.

Java applet and 2-step infection

PHISHING EMAIL → JAVA APPLET / DROPPER → DOWNLOADER → MAIN MODULE → MODULES → COBALT / BEACON

Spear phishing with link to **signed.jar**.

No attachments.

signed.jar – Dropper that extracts main.dll or main64.dll.

Then launch it in the context of JAVA machine.

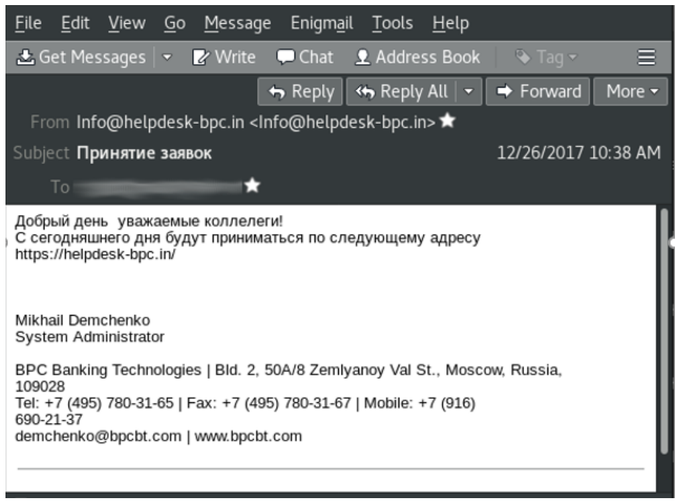
Main.dll – simple downloader. It download and launch main trojan – int.dll

Int.dll – download and launch another modules.

Get data from modules and send it on C2.

1. Screenshot module
2. Process info collection module

Main module can receive command to download and execute Cobalt Strike Beacon.



Infection process

- In December of 2017 Cobalt sent spear phishing with link to new malicious Java applet.
- Java-applet is the Dropper that extracts and launch files. In 2-step infection Dropper contains Downloader program. In later attacks, the Java applet immediately loaded and ran Cobalt beacon from C2 server.
- First Downloader downloads from remote host main module responsible for download Screenshotter and ProcessChecker and communication with C2 server.
- In February the stopped using Java.

Questions?

www.group-ib.com
info@group-ib.com
twitter.com/groupib
t.me/group_ib
group-ib.ru/blog
+44 2036085907
facebook.com/group-ib
instagram.com/group_ib