RSAConference2018

Singapore | 25–27 July | Marina Bay Sands

NOW MATTERS

#RSAC

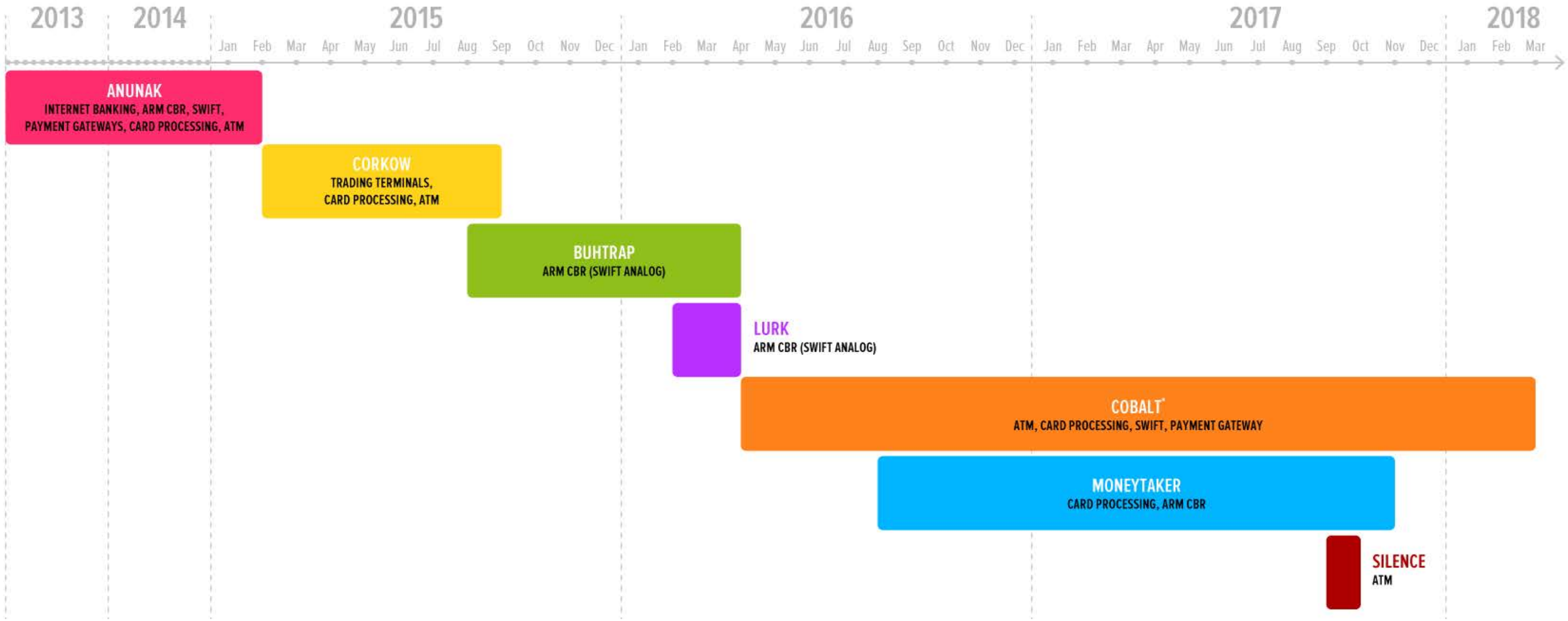
SESSION ID: FLE-R09

ANALYSIS OF COBALT ATTACKS ON FINANCIAL INSTITUTIONS: SWIFT, PROCESSING, ATMS

Tim Bobak

APAC Executive Director at Group-IB
Group-IB
@GroupIB_GIB

Cybercrime attacking financial institutions



ANUNAK
INTERNET BANKING, ARM CBR, SWIFT, PAYMENT GATEWAYS, CARD PROCESSING, ATM

CORKOW
TRADING TERMINALS, CARD PROCESSING, ATM

BUHTRAP
ARM CBR (SWIFT ANALOG)

LURK
ARM CBR (SWIFT ANALOG)

COBALT*
ATM, CARD PROCESSING, SWIFT, PAYMENT GATEWAY

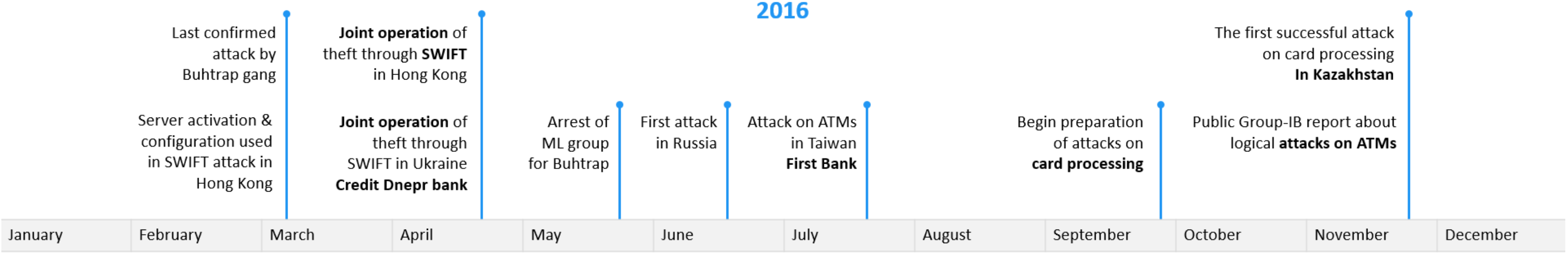
MONEYTAKER
CARD PROCESSING, ARM CBR

SILENCE
ATM

Cobalt Timeline

#RSAC

2016



Last confirmed attack by Buhtrap gang

Server activation & configuration used in SWIFT attack in Hong Kong

Joint operation of theft through **SWIFT** in Hong Kong

Joint operation of theft through SWIFT in Ukraine **Credit Dnepr bank**

Arrest of ML group for Buhtrap

First attack in Russia

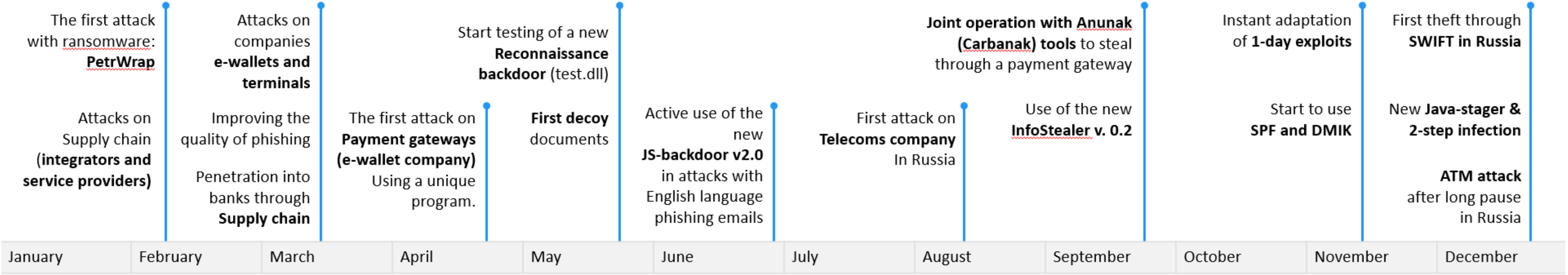
Attack on ATMs in Taiwan **First Bank**

Begin preparation of attacks on **card processing**

The first successful attack on card processing **In Kazakhstan**

Public Group-IB report about logical **attacks on ATMs**

2017



The first attack with ransomware: **PetrWrap**

Attacks on Supply chain **(integrators and service providers)**

Attacks on companies **e-wallets and terminals**

Improving the quality of phishing

Penetration into banks through **Supply chain**

The first attack on **Payment gateways (e-wallet company)** Using a unique program.

Start testing of a new **Reconnaissance backdoor** (test.dll)

First decoy documents

Active use of the new **JS-backdoor v2.0** in attacks with English language phishing emails

First attack on **Telecoms company** In Russia

Joint operation with Anunak (Carbanak) tools to steal through a payment gateway

Use of the new **InfoStealer v. 0.2**

Instant adaptation of **1-day exploits**

Start to use **SPF and DMIK**

First theft through **SWIFT in Russia**

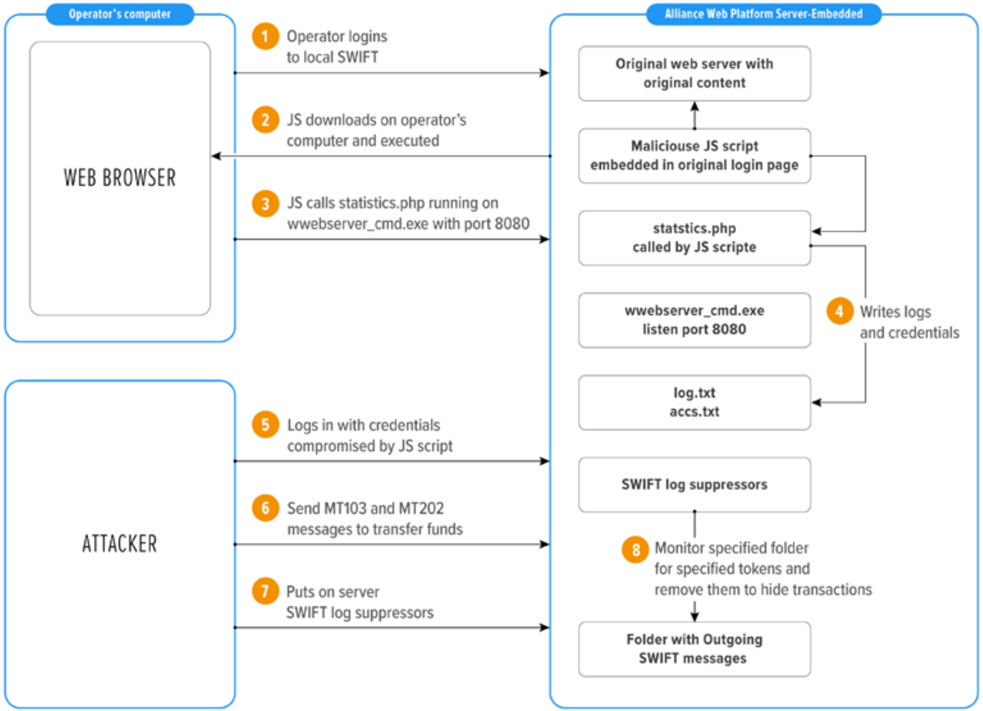
New **Java-stager & 2-step infection**

ATM attack after long pause in Russia

GROUP-IB

RSAConference2018 Asia Pacific & Japan

SWIFT attacks



Operator's computer

WEB BROWSER

1 Operator logins to local SWIFT

2 JS downloads on operator's computer and executed

3 JS calls statistics.php running on wwebserver_cmd.exe with port 8080

ATTACKER

5 Logs in with credentials compromised by JS script

6 Send MT103 and MT202 messages to transfer funds

7 Puts on server SWIFT log suppressors

Alliance Web Platform Server-Embedded

Original web server with original content

Maliciouse JS script embedded in original login page

statstics.php called by JS scripte

wwebserver_cmd.exe listen port 8080

4 Writes logs and credentials

log.txt accs.txt

SWIFT log suppressors

8 Monitor specified folder for specified tokens and remove them to hide transactions

Folder with Outgoing SWIFT messages

Hong Kong incident

- Attacker activated 2 servers on 20 March and 28 March
- 28 April 2016, unnamed bank in Hong Kong was robbed
- Bank used Customer-hosted SWIFT connectivity
- This took one month once inside the compromised bank for preparation and organization of money laundering
- Attack was sophisticated and to accomplish it attackers developed tools specifically for this bank

Ukraine incident

- April 2016, Credit Dnepr bank was robbed[1].
- Attackers sent out of the bank about **$10 mln.**
- Year later bank confirmed losses of **$950 000 USD**

Russian incident

- Globex bank - December 2017[2]
- Attackers sent out about **$6 mln**. (339,5 mln. rub)
- SWIFT-specific malware was not identified.

[1] https://ubr.ua/finances/banking-sector/hakeryi-ukrali-$1-mln-iz-banka-kredit-dnepr-a-obnalichili-ego-v-kitae-3858154

[2] https://www.reuters.com/article/us-russia-cyber-globex/russias-globex-bank-says-hackers-targeted-its-swift-computers

ATM attacks

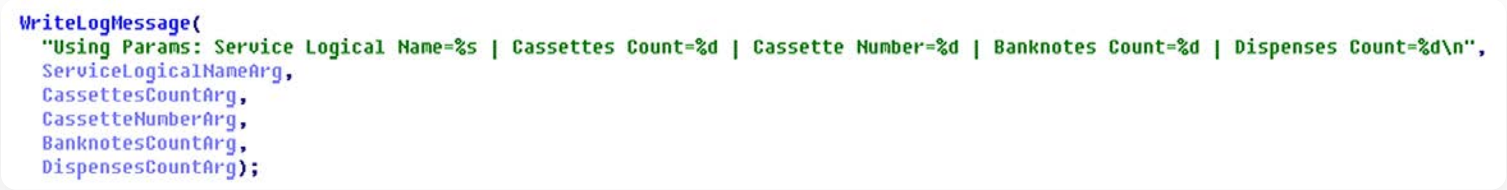
Malicious program using standard functions for the XFS interface via the XFS Manager (eXtensions for Financial Services).

ATM incidents

- First attack was in Russia in June 2016
- Second attack was in Taiwan with First Bank. Mules withdraw more than **$2 mln[1].**
- We attributed this attack to Cobalt only in the end of 2016 base on malware comparison.
- There were no any further ATM attacks after November 2016 until December 2017.

ATM malware parameters

- 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.



```
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);
```

ATM attacks

	Parameter	Europe (realization of ATMSpitter using standard library MSXFS.dll)	Taiwan (realization of ATMSpitter using standard library CSCWCNG.dll)	Group-IB Analyst Comments
1	**Protection Mechanisms**	Checking of launch month. If the current date does not coincide with September 2016, error message will be shown. Error message: WFSOpen failed with error: **WFS_ERR_INTERNAL_ERROR** It corresponds with month of incident in Europe – Sep 2016	Checking of launch month. If the current date does not coincide with July 2016, error message will be shown. Error message: CscCngOpen/CscCdmOpen failed with error: **System Failure** It corresponds with month of incident in Taiwan – July 2016	The protection mechanisms correspond with the months of the incidents (in Europe – September 2016, in Taiwan – July 2016). The person who launched program didn't know the real reason the program was not launched, only the developer knew and understands what this error means.

2	**Identical parts of code**	`int v1; // eax@1`
		`  CHAR *v2; // ebx@1`
		`  HANDLE v3; // esi@1`
		`  int v4; // eax@1`
		`  DWORD NumberOfBytesWritten; // [esp+2Ch] [ebp-Ch]@1`
		`  va_list va; // [esp+44h] [ebp+Ch]@1`
		
		`  va_start(va, a1);`
		`  NumberOfBytesWritten = 0;`
		`  v1 = lstrlenA(a1);`
		`  v2 = (CHAR *)malloc(v1 + 10240);`
		`  wvsprintfA(v2, a1, va);`
		`  v3 = CreateFileA("disp.txt", 0x120116u, 3u, 0, 4u, 0, 0);`
		`  SetFilePointer(v3, 0, 0, 2u);`
		`  v4 = lstrlenA(v2);`
		`  WriteFile(v3, v2, v4, &NumberOfBytesWritten, 0);`
		`  CloseHandle(v3);`
		`  free(v2);`
			`int v1; // eax@1`
			`  CHAR *v2; // esi@1`
			`  HANDLE v3; // edi@1`
			`  int v4; // eax@1`
			`  DWORD NumberOfBytesWritten; // [esp+Ch] [ebp-4h]@1`
			`  va_list va; // [esp+1Ch] [ebp+Ch]@1`
			
			`  va_start(va, lpString);`
			`  NumberOfBytesWritten = 0;`
			`  v1 = lstrlenA(lpString);`
			`  v2 = (CHAR *)malloc(v1 + 10240);`
			`  wvsprintfA(v2, lpString, va);`
			`  v3 = CreateFileA("displog.txt", 0x120116u, 3u, 0, 4u, 0, 0);`
			`  SetFilePointer(v3, 0, 0, 2u);`
			`  v4 = lstrlenA(v2);`
			`  WriteFile(v3, v2, v4, &NumberOfBytesWritten, 0);`
			`  CloseHandle(v3);`
			`  free(v2);`
				Both instances have identical code designed to record the dispensing results into an unencrypted file (disp.txt in European case, displog.txt in Taiwan). This is so that the exact amount of notes taken by money mules can be tracked during theft. This indicates the developer is using mules that they do not trust.

3	**Error messages in incorrect arguments passing**	If any of the arguments are outside the possible range, ATMSpitter displays error messages: *Error! Banknotes Count should be from 1 to 60* *Error! Cassette number should be from 1 to 15* *Error! Cassettes count should be from 1 to 15* *Error! Dispenses Count should be from 1 to 500*	If any of the arguments are outside the possible range, ATMSpitter displays error messages: *Invalid parameter: Cassette slot number. Must be a digit from 1 to 9* *Invalid parameter: Banknotes Count. Must be a digit from 1 to 60*	Analogous messages connected with «Cassette number» and «Banknotes Count»
4	**Language errors in code**	Developer uses words «cassettes», «banknotes»	Developer uses word «banknotes»	Typical usage by Russian-speaker

Card processing

Card processing – the easiest way to steal money

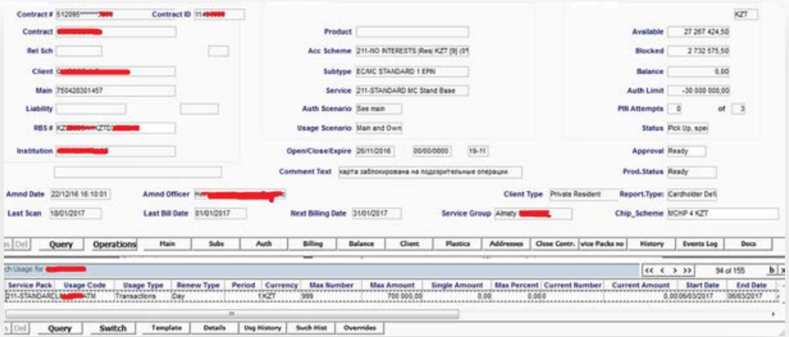
- It took 2 months to prepare first attack on card processing.
- First victim – bank in the Kazakhstan. Attackers withdraw **$600 thousand**.
- After first success they started to attack other clients of the card processing vendor as used in Kazakhstan bank.
- Cobalt attempted to steal **€25 mln** just in one attack on a Central European bank via Card processing. Infection was through Supply chain.

Scheme description

- Getting access to computers of Card processing operators in the bank.
- Legally open bank cards in the same bank or buy new cards on dark market (usually about 30 cards).
- Remove or increase withdraw limits.
- Remove overdraft limits (even for debit cards).
- Cash out using these cards in other countries

Reason to shift on Card processing

- After arrest of mules in Taiwan, Romania, Russia, the safety of mules became a priority for them.
- No need of complicated scheme of money laundering. Mules always get clean cash. Attacker need only several cards of attacked bank to accomplish fraud.
- Withdrawing money in another country provides time to mules. Bank's security service could not quickly contact the police, get records from video surveillance cameras.



Contract # 512095*******[redacted] Contract ID 11[redacted]
Contract [redacted]
Rel Sch
Client [redacted]
Main 750428301457
Liability
RBS # KZ[redacted]ZTO[redacted]
Institution [redacted]

Product
Acc Scheme 211-NO INTERESTS (Res) KZT [9] (0*
Subtype EC/MC STANDARD 1 EPN
Service 211-STANDARD MC Stand Base
Auth Scenario See main
Usage Scenario Main and Own
Open/Close/Expire 26/11/2016 00/00/0000 19-11
Comment Text карта заблокирована на подозрительные операции

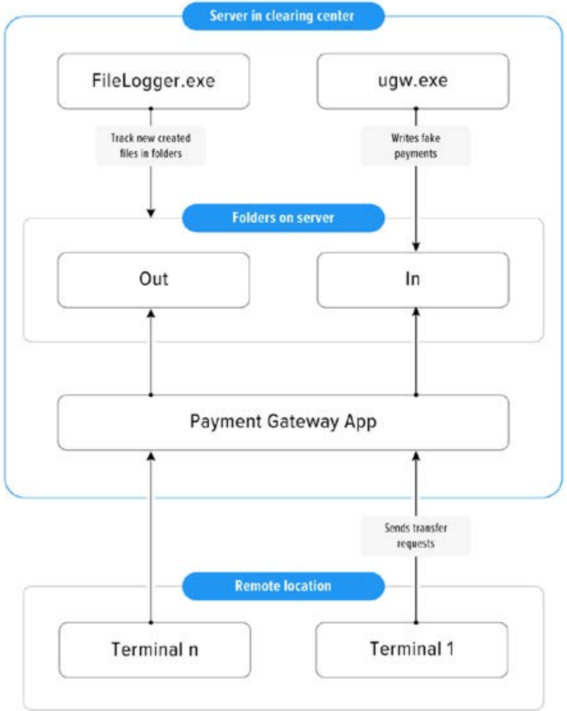
KZT
Available 27 267 424,50
Blocked 2 732 575,50
Balance 0,00
Auth Limit -30 000 000,00
PIN Attempts 0 of 3
Status Pick Up, spe
Approval Ready
Prod.Status Ready

Amnd Date 22/12/16 16:10:01 Amnd Officer H[redacted] Client Type Private Resident Report.Type: Cardholder Def
Last Scan 18/01/2017 Last Bill Date 01/01/2017 Next Billing Date 31/01/2017 Service Group Almaty [redacted] Chip_Scheme MCHP 4 KZT

ch Usage for [redacted]

Service Pack	Usage Code	Usage Type	Renew Type	Period	Currency	Max Number	Max Amount	Single Amount	Max Percent	Current Number	Current Amount	Start Date	End Date
211-STANDARD	L[redacted]ATM	Transactions	Day	1	KZT	999	700 000,00	0,00	0,000		0,00	06/03/2017	06/03/2017

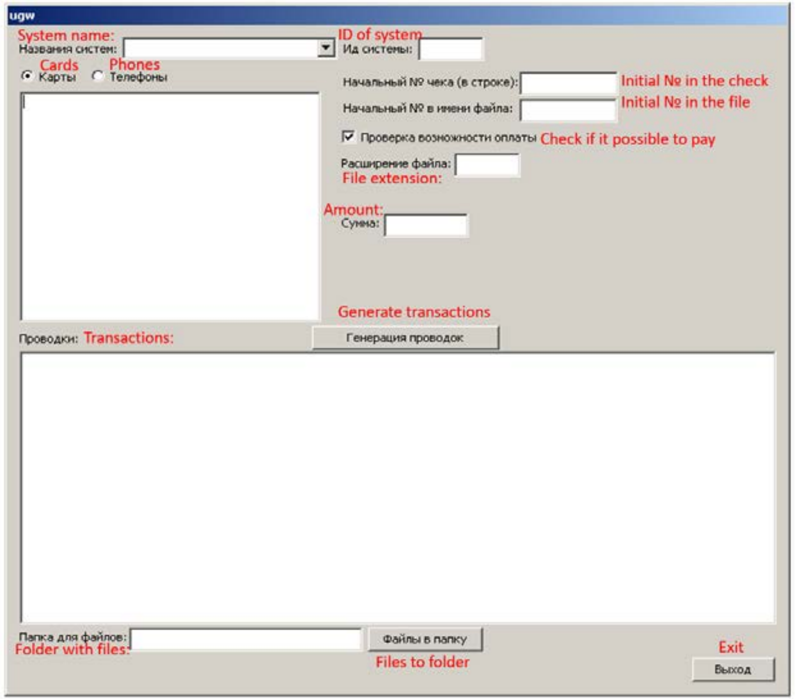
Payment gateways



First episode

- March 2017 first spear phishing campaign behalf of moneta.ru targeting 4 Russian and 4 Ukrainian e-wallet companies.
- To accomplish attack threat actors created 2 simple tools: FileLogger.exe and Ugw.exe.
- FileLogger.exe – track new files in the specified folder and copy content of new files into the log file.
- Ugw.exe – generate transactions to automate theft process.

Payment gateways



First episode

- To steal money the attacker needs to generate thousands of transactions for small sums. Very hard to stop without disrupting service and also hard to return stolen funds.
- Ugw.exe - generates transactions to automate the theft process.
- Ugw.exe reads file terminals.txt generated by the attackers. This file contains Terminal IDs, on behalf of whom requests for transfer are made.
- Here the attackers specified phone, cards numbers and the totals for transfers and press Generate transaction button.
- The output of Ugw.exe are files with transaction details in the right format. These files were put into the In folder and processed by the payment gateway.
- Total loss was about **$2 mln.**

Payment gateways: Cooperation with Anunak (Carbanak) gang

GROUP-IB AND FOX-IT

ANUNAK:
APT AGAINST FINANCIAL INSTITUTIONS

GROUP-IB FOX IT

Carbanak / Anunak

- First attack recorded payment gateway attack was conducted in 2014 by Anunak (Carbanak) gang.
- In that attack Anunak (Carnabak) used a SSH-backdoor that they compiled right on the compromised Linux servers.

Second episode

- In September 2017 another e-wallet company was hacked and robbed by Cobalt.
- The attack scheme was similar to the first episode with standard Cobalt toolkit.
- After successful theft the attack did not stop. The attacker got access to 2 development servers and installed the SSH-backdoor on them.
- SSH-backdoors had identical RSA private and public keys, but different C2 domains.
- The domain hagaipipko.net and RSA keys are identical to those we saw in 2014 during Carbanak incident response.
- SSH backdoor and Cobalt Strike beacon C2 addresses were in the same subnets 89.37.226.0/24 and 190.123.35.0/24 and 190.123.36.0/24

SSH backdoor C2-address	Registration date	Expiration date	SSH backdoor IP-address	Cobalt Strike C2-address
hagaipipko.net	2014-08-14	2018-08-14	190.123.36.162	190.123.35.177
javacdnupdate.com	2017-10-12	2018-10-12	89.37.226.10	89.37.226.131 89.35.178.108

Attacks on Supply chain

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

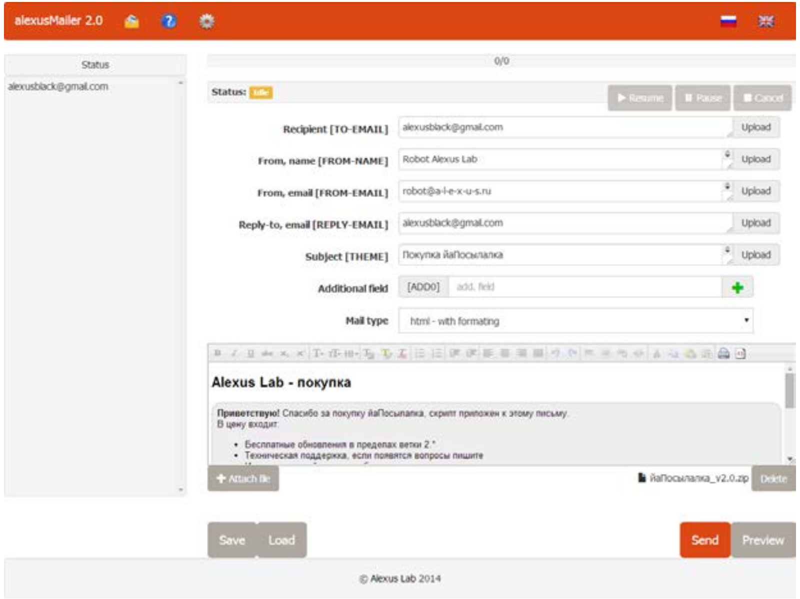
New vector to deliver malware

- 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.

Spear phishing



alexusblack@gmail.com

Status: Idle

Recipient [TO-EMAIL] alexusblack@gmail.com

From, name [FROM-NAME] Robot Alexus Lab

From, email [FROM-EMAIL] robot@a-l-e-x-u-s.ru

Reply-to, email [REPLY-EMAIL] alexusblack@gmail.com

Subject [THEME] Покупка йаПосылалка

Additional field [ADD0] add. field

Mail type html - with formating

Alexus Lab - покупка

Приветствую! Спасибо за покупку йаПосылалка, скрипт приложен к этому письму.
В цену входит:

- Бесплатные обновления в пределах ветки 2.*
- Техническая поддержка, если появятся вопросы пишите

йаПосылалка_v2.0.zip

© Alexus Lab 2014

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.

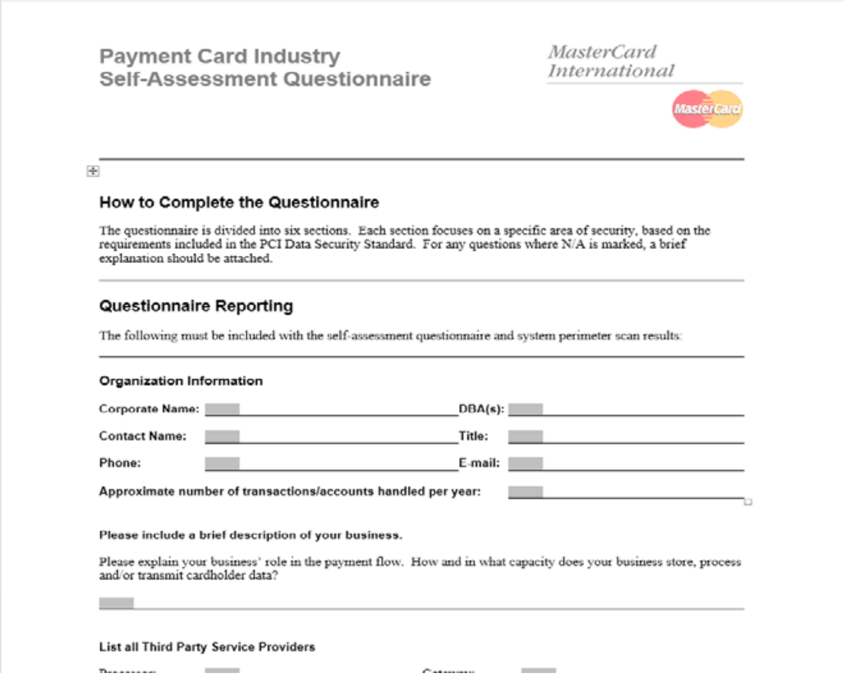
Attachments

- 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

MasterCard

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

Processor: Gateway:

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.

Lateral movement & Persistence & Remote control

Lateral movement

- For network scanning they use: SoftPerfect Network Scanner, Eternal Blues, EternalPunch 0.3.0
- Malware provisioning for corporate anti-virus management software
- 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

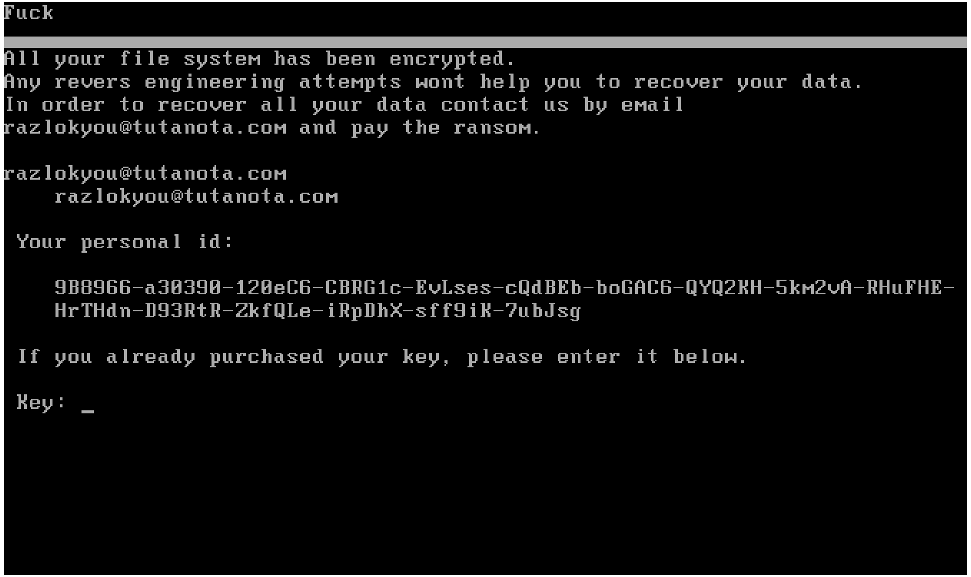
Persistence

- 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 access.

PetrWrap



```
Fuck

All your file system has been encrypted.
Any revers engineering attempts wont help you to recover your data.
In order to recover all your data contact us by email
razlokyou@tutanota.com and pay the ransom.

razlokyou@tutanota.com
    razlokyou@tutanota.com

 Your personal id:

    9B8966-a30390-120eC6-CBRG1c-EvLses-cQdBEb-boGAC6-QYQ2KH-5km2vA-RHuFHE-
    HrTHdn-D93RtR-ZkfQLe-iRpDhX-sff9iK-7ubJsg

 If you already purchased your key, please enter it below.

 Key: _
```

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

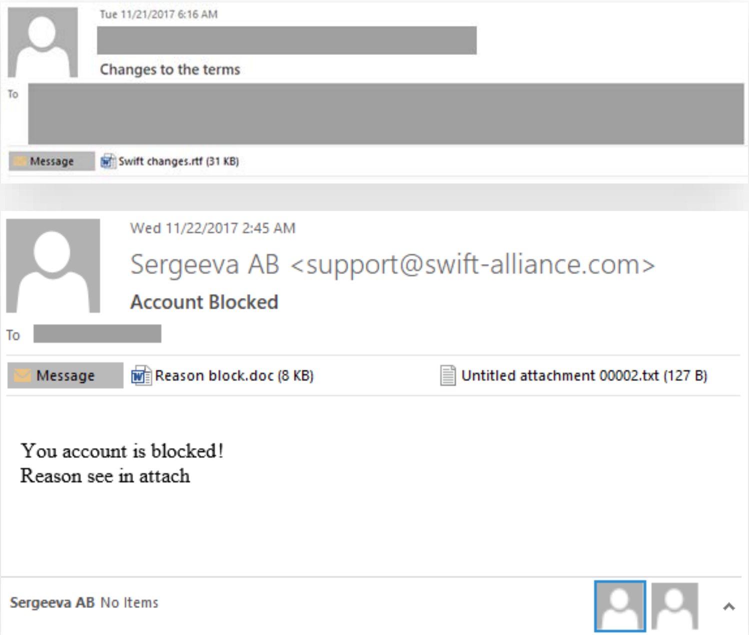
Short history

- 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



Tue 11/21/2017 6:16 AM

[redacted]

Changes to the terms

To [redacted]

Swift changes.rtf (31 KB)

Wed 11/22/2017 2:45 AM

Sergeeva AB <support@swift-alliance.com>

Account Blocked

To [redacted]

Reason block.doc (8 KB)

Untitled attachment 00002.txt (127 B)

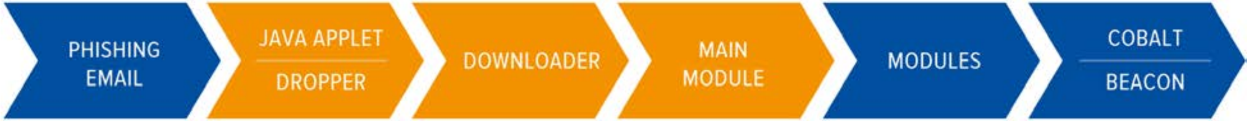
You account is blocked!
Reason see in attach

Sergeeva AB No Items

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



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.

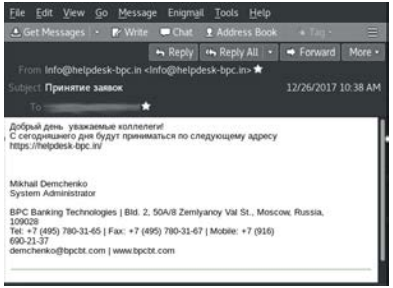
Main.dll – simple downloader. It download and launch main trojan – int.dll

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.



From Info@helpdesk-bpc.in <Info@helpdesk-bpc.in>

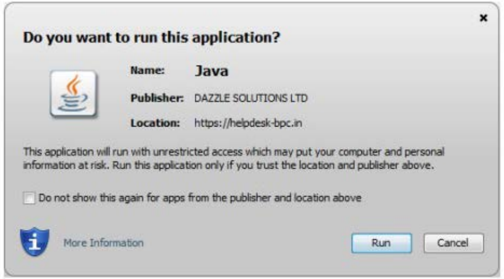
Subject **Принятие заявок** 12/26/2017 10:38 AM

To [redacted]

Добрый день уважаемые коллелеги!
С сегодняшнего дня будут приниматься по следующему адресу
https://helpdesk-bpc.in/

Mikhail Demchenko
System Administrator

BPC Banking Technologies | Bld. 2, 50A/8 Zemlyanoy Val St., Moscow, Russia, 109028
Tel: +7 (495) 780-31-65 | Fax: +7 (495) 780-31-67 | Mobile: +7 (916) 690-21-37
demchenko@bpcbt.com | www.bpcbt.com



Do you want to run this application?

Name: Java

Publisher: DAZZLE SOLUTIONS LTD

Location: https://helpdesk-bpc.in

This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

□ Do not show this again for apps from the publisher and location above

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 they 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