



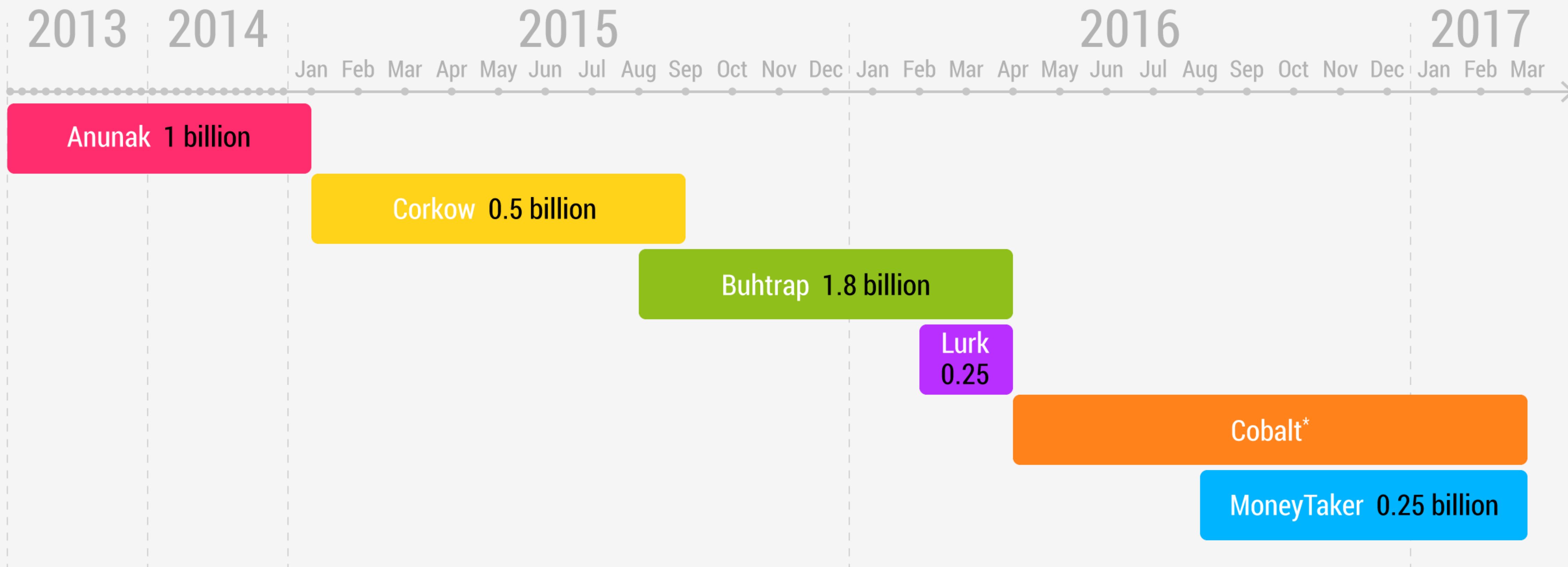
*The evolution of targeted
attacks on financial
institutions*



Who are the attackers?



Timeline



*Cobalt was detected in June



KNOWN TARGETED ATTACKERS

Cobalt

ATM, Card processing, SWIFT

Buhtrap

ARM CBR (SWIFT analog)

Corkow

Trading terminals,
Card processing, ATM

Lurk

ARM CBR (SWIFT analog)

Anunak

Internet banking, ARM CBR,
SWIFT, Payment gateways,
Card processing, ATM

FUTURE TARGETED ATTACKERS

- Toplel
- Ranbyus
- RTM
- Vawtrak
- Dridex

ID	Login info	Bank	IP	Last activity	Assigned	Action	Comment
551	[redacted]/le	RBS (Business)	62.[redacted]42	18:07:43 (10.07)	-	+	77k
582	[redacted]	HSBC (business)	[redacted]	18:07:18 (10.07)	-	+	
589	[redacted]	Natwest (Business)	[redacted]	18:07:23 (10.07)	-	+	
588	[redacted]	TSB (business)	[redacted]	18:07:43 (10.07)	-	+	
527	[redacted]	aibgb1.co.uk (Business)	[redacted]	18:07:41 (10.07)	-	+	-6k.skip
506	[redacted]	Bank of Scotland (corporate)	[redacted]	18:07:58 (10.07)	-	+	
514	176[redacted]h	RBS (Business)	8[redacted]4	17:07:39 (10.07)	-	+	500k balance. inter -UK. pod chaps dropov pod krupnoe net.skip poka
564	[redacted]	Natwest (Business)	[redacted]	17:07:57 (10.07)	-	+	
586	[redacted]	Natwest (Business)	[redacted]	17:07:13 (10.07)	-	+	
539	26[redacted]53	RBS (Business)	2[redacted]	17:07:27 (10.07)	-	+	акк для авторизации платежей. 2kk balance. skip
587	[redacted]	Santander (business)	[redacted]	17:07:14 (10.07)	-	+	
492	1[redacted]	RBS (Business)	[redacted].8	16:07:34 (10.07)	-	+	PIN:1357 Pass:Aegis12 TMS-Payment approval - %Password21 balance total 40kk. dual auth
585	[redacted]	Unity Trust	[redacted]	16:07:22 (10.07)	-	+	
584	[redacted]	Santander (business)	[redacted]	16:07:09 (10.07)	-	+	
583	86[redacted]tti	RBS (Business)	[redacted].194	14:07:15 (10.07)	-	+	нет функции подтверждения платежа. 18kk. poproboval 2kk slit' na china
579	[redacted]	Santander (business)	[redacted]	14:07:21 (10.07)	-	+	11,3k на toader cocier 202569 13208710(2PAC)
566	376[redacted]m	RBS (Business)	[redacted]0	14:07:05 (10.07)	-	+	7kk balance. dual auth-ON. lutsche prozvonom lit'
581	[redacted]	Santander (business)	[redacted]	14:07:03 (10.07)	-	+	slito 15k (2PAC) Josif Kasparovic 20-25-85. 90077186, веннулись обратно

Balance is 500 thousand pounds, inter-UK, for money mules (now such money mules now). Skip for now.

Account for authorization of payments, balance is 2 million pounds

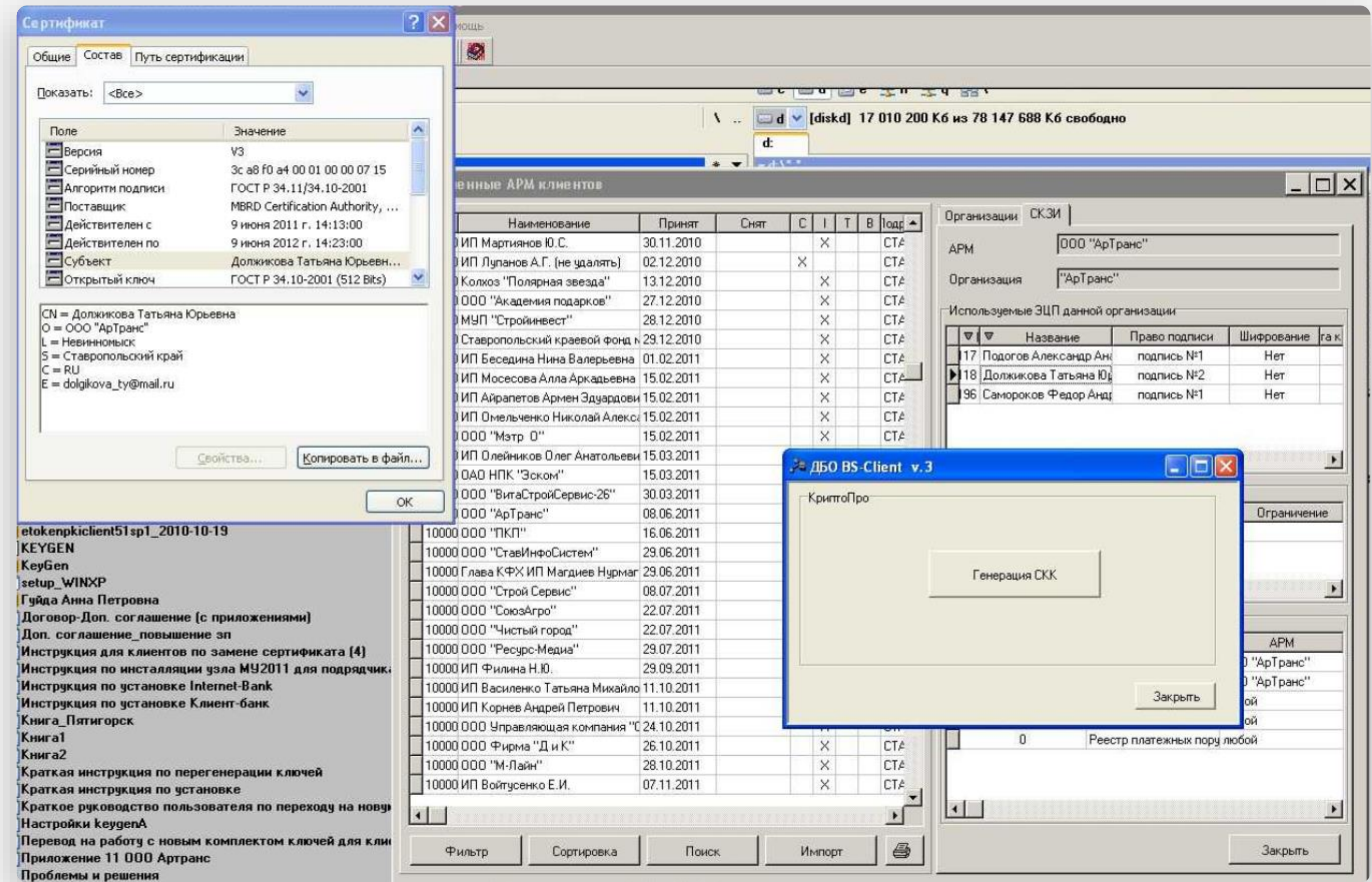
No function of payment approval. Balance is 18 million pounds. Tried to transfer 2 million to China

Balance is 15 million pounds, dual authorization off. No opportunity to establish sort code for transfer. It is better to ring out

What are the targets?

Access to corporate internet banking enables criminals to steal from TOP clients. Anunak used this method in 2013-2014.

- Compromise operator workstations of corporate accounts
- Listing companies with high balances
- Generating new digital signatures for each company
- Transactions from corporate accounts signed with new digital signatures



Payment gateways enables high frequency, low amount transfers. Very hard to stop and return money.

- Once inside, hackers search for payment gateways
- Obtain log files from payment gateways to understand the typical format of communication
- Start SOCKS proxies on internal hosts to enable communication with payment gateways
- Run scripts to replenish attacker's phone balances in thousands of transactions
- Transfer money from phones to cards and cash out

```
$ses = date("Ymdhis");  
$url = "http://ru-demo.cyberplat.com/cgi-bin/DealerSertification/de_pay.cgi";  
$data_string =  
"SD=XXXXXX&AP=XXXXXX&OP=XXXXX&SESSION=".$ses."&COMMENT=Test&NUMBER=9642065662&AMOUNT_ALL=10.0&AMOUNT=10.0";
```

```
$ch = curl_init();  
curl_setopt($ch,CURLOPT_URL, $url);  
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);  
curl_setopt($ch, CURLOPT_HTTPHEADER, array('Content-Type: application/x-www-form-urlencoded','Content-Length:'.strlen($data_string)));  
curl_setopt($ch, CURLOPT_POSTFIELDS,  
"inputmessage=0000038801SM000001270000012700000125&".$data_string);  
$result = curl_exec($ch);
```

```
var_dump($result);
```


Cobalt and ATM Heists

2016

Europe Case

- MARCH** - The last confirmed attack on a bank conducted by the **Buhtap group**
- MAY** - Arrest of the group laundering money for **Buhtap**
- JUNE** - The first attack on a Russian bank using **Cobalt Strike**
- JULY** - **Attacks on banks:** Armenia, Belorussia, Poland, Germany
- AUGUST** - **Attacks on banks:** in Georgia, Belorussia, Romania, Kyrgyzstan, Poland, Estonia, Spain, the Netherlands, the UK, Malaysia
- SEPTEMBER** - Confirmed thefts from ATMs outside Russia



Taiwan Case

```
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 = strlenA(a1);
v2 = malloc(v1 + 10240);
wvsprintfA(v2, a1, va);
v3 = CreateFileA("disp.txt", 0x120116u, 3u, 0, 4u, 0, 0);
SetFilePointer(v3, 0, 0, 2u);
v4 = strlenA(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 = strlenA(lpString);
v2 = malloc(v1 + 10240);
wvsprintfA(v2, lpString, va);
v3 = CreateFileA("displog.txt", 0x120116u, 3u, 0, 4u, 0, 0);
SetFilePointer(v3, 0, 0, 2u);
v4 = strlenA(v2);
WriteFile(v3, v2, v4, &NumberOfBytesWritten, 0);
CloseHandle(v3);
free(v2);
```

Corkow conducted the first successful attack on broker terminals in 2015.

- The attack lasted only 14 minutes
- \$437 million in purchases (5 trades)
- \$97 million sold (2 trades)
- 55 to 66 Rubles — volatility in exchange rate





SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

Circular

13 October 2016

SFC notifies the industry of cybersecurity review on internet/mobile trading systems

The Securities and Futures Commission (SFC) announced the commencement of a cybersecurity review in the fourth quarter with a focus on assessing the cybersecurity preparedness, compliance and resilience of brokers' internet/mobile trading systems.

The SFC has received an increasing number of reports from securities brokers that the security of some customers' internet/mobile trading accounts has been compromised and unauthorized securities trading transactions were conducted through these accounts. For the 12 months ended 30 September 2016, there were 16 reported hacking incidents which involved 7 securities brokers and total unauthorized trades in excess of \$100 million. While these hacking incidents are still under police investigation, there are indications that brokers and their clients may be able to do more to better protect online trading accounts.

- Identify working directory of SWIFT or ARM CBR application
- Replace payment details with fraudster's information
- Intercept confirmation messages to bypass identification of fraudulent transactions

Notice To Receive Required

Message Identification

TNum: [] Status: [] Sender's Ref: [] Related Ref: [] Template: []

Sender: SWBPBEHA | HA bank | Receiver: []

Internal Memo: []

Credit Account

Account Number: [] Name: [] Bank: []

Ordering Party

Ordering Party is a Financial Institution

Institution Code: SWIFT | []

Name: []

Address 1: []

Address 2: []

Address 3: [] Country: []

Intermediary Bank

Bank Code: SWIFT | []

Name: []

Address 1: []

Address 2: []

Address 3: [] Country: []

Amount & Date

Credit Amount: [] Value Date: 19/08/2010

Save | Save Incomplete | Template | Search | Reset

SWIFT

[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcm\in\
 [ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcm\out\

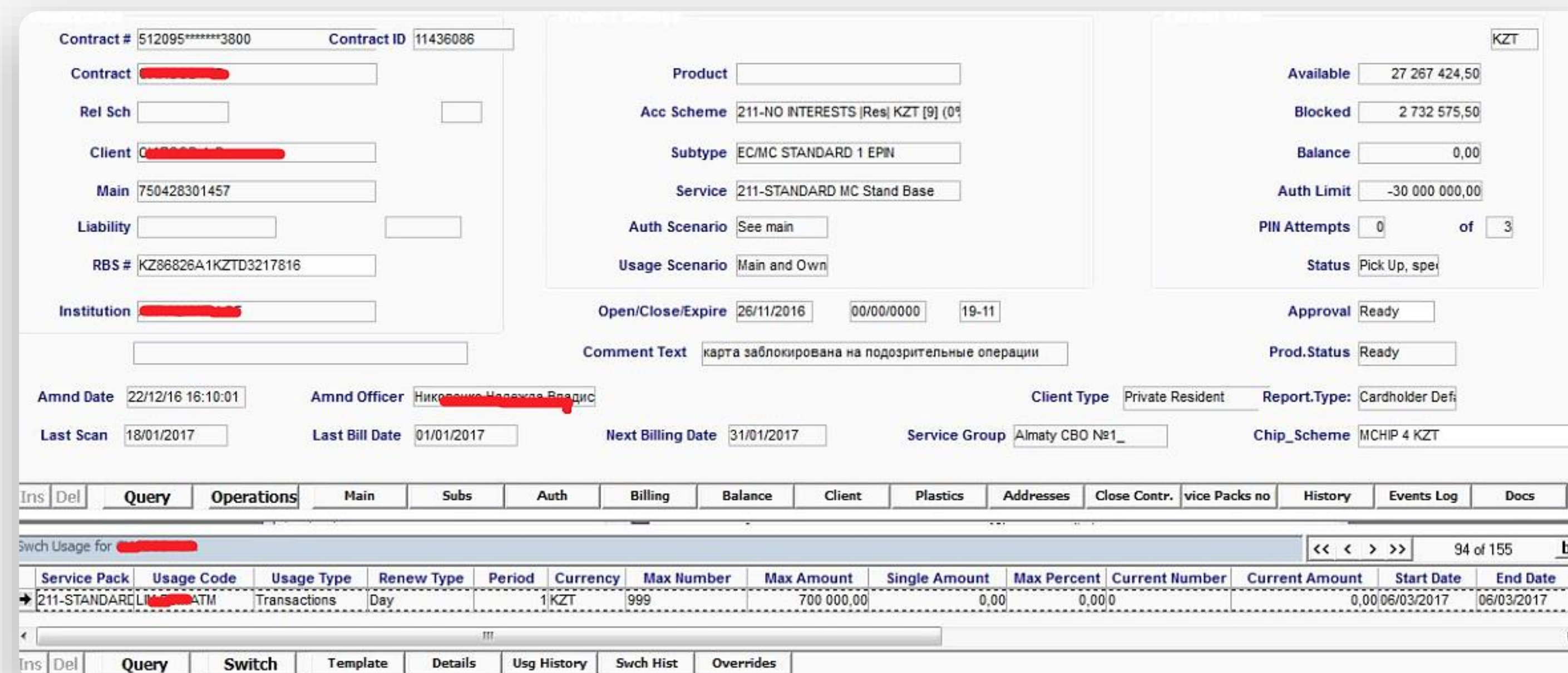
ARM CBR

[ROOT_DRIVE]:\uarm3\exq\inc\
 [ROOT_DRIVE]:\uarm3\exq\out\

Cobalt, Corkow, Anunak have been conducting these attacks since 2014.

It provides very important cash-out benefits.

- 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



The screenshot displays a banking system interface with the following details:

- Contract #:** 512095*****3800, **Contract ID:** 11436086
- Product:** (Empty field)
- Acc Scheme:** 211-NO INTERESTS [Res] KZT [9] (0%)
- Subtype:** EC/MC STANDARD 1 EPIN
- 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
- Amnd Date:** 22/12/16 16:10:01, **Amnd Officer:** Николаев, Александр Владимирович
- Last Scan:** 18/01/2017, **Last Bill Date:** 01/01/2017, **Next Billing Date:** 31/01/2017
- Client Type:** Private Resident, **Report.Type:** Cardholder Defi
- Service Group:** Almaty CBO №1_, **Chip_Scheme:** MCHIP 4 KZT
- Available:** 27 267 424,50 KZT
- Blocked:** 2 732 575,50
- Balance:** 0,00
- Auth Limit:** -30 000 000,00
- PIIN Attempts:** 0 of 3
- Status:** Pick Up, spe
- Approval:** Ready
- Prod.Status:** Ready

Navigation tabs include: Query, Operations, Main, Subs, Auth, Billing, Balance, Client, Plastics, Addresses, Close Contr., vice Packs no, History, Events Log, Docs.

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	ATM	Transactions	Day	1	KZT	999	700 000,00	0,00	0,000		0,00	06/03/2017	06/03/2017

Navigation tabs at the bottom: Query, Switch, Template, Details, Usg History, Swch Hist, Overrides.

What's next?

The screenshot displays the NGN Intelligence Threat List interface. The main threat entry is CP-1438-15: Cobalt's mass email sending from mail server of Russian company Lanit, dated 2017-03-02. The interface includes a sidebar with navigation options like Dashboard, Compromised data, Threats, Attacks, Hactivism, Suspicious IP, Targeted malware, and Brand abuse. The main content area is divided into sections: PERSONAL PROFILE, DESCRIPTION OF THREAT, and RECOMMENDATIONS. The PERSONAL PROFILE section shows an Admiralty Code of A1, a Threat type of Targeted attack, and a Detection date of 2017-02-27. The DESCRIPTION OF THREAT section contains a red-bordered text box stating: "In the previous notification CP-1438-14 we've already informed about compromising of IT-infrastructure of company Lanit by Cobalt. After that on 27/02/2017 Cobalt started to send malicious emails from Lanit's mail server. Now Group-IB specialists continue to detect malicious emails from this attack." The RECOMMENDATIONS section provides several bullet points for user action.

CP-1438-15: Cobalt's mass email sending from mail server of Russian company Lanit 2017-03-02

PERSONAL PROFILE

Admiralty Code A1 Completely reliable/Confirmed by other sources	Threat type Targeted attack Detection date 2017-02-27 Involved individuals	Notification type Cybercrime preparation Affected countries Azerbaijan, China, India, Indonesia, Kazakhstan, Moldova, Romania, Russian Federation, Tajikistan, Turkey, Viet Nam Related links	Target industry Banks, Telecom, Industry, Insurance Threat short name New attack of Cobalt cybercrime group	Malware used Cobalt Strike MWI Dissemination tools Email
---	--	---	--	--

DESCRIPTION OF THREAT

In the previous notification CP-1438-14 we've already informed about compromising of IT-infrastructure of company Lanit by Cobalt. After that on 27/02/2017 Cobalt started to send malicious emails from Lanit's mail server. Now Group-IB specialists continue to detect malicious emails from this attack.

Malicious attachment:
"договор на обслуживани.doc", hash 08fd104d0c5a65912efd699c213e48e446d1f5ad15df0cd3e367176708800d46, size 1777822 bytes.
This document drops Cobalt's downloader
%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRO7702.tmp, hash 56a3a4c857939ac9bed4f2e0084fb037, size 215040 bytes.
The same loader is available on the URL hxxp://185.82.216.94/lms.exe. It means that another documents with macros, which download it, are exist. Cobalt's C&C-server: 193.238.152.67.
Domail name cards-alfabank.ru was registered on 2017-02-20.

RECOMMENDATIONS

- Use indicators from the notifications to adjust your security systems and to check for potential incidents.
- When you see a new threat please make sure this information is shared with all people interested in it in your organization.
- If your compromised data is being sold we can secretly contact the seller to make a test purchase that will help to reveal the insider. Click "Request more information" to do that.
- If you want to know more about certain threat, please let us know. We can carry out an investigation and identify people behind it.

SCREENSHOTS

No items here yet

- Cobalt has been compromising companies and sending spear phishing emails with exploit to targets from the compromised e-mail server.
- In Feb 2017, Cobalt targeted companies in India, China, Kazakhstan, Turkey and Vietnam by compromising a Russian organizations servers.

INTELLIGENCE

History [Threat list](#)

CP-1438-9: Cobalt cybercrime group's money theft using payment processing system «Way4» 2017-02-03

PERSONAL PROFILE

Admiralty Code A1 Completely reliable/Confirmed by other sources	Threat type Targeted attack Detection date Involved individuals Brief description Cybercrime group Cobalt conducted successful attack against bank in Kazakhstan, obtained access to payment processing system «Way4» and successfully theft money as the result of manipulating with limits of bank cards	Notification type Cybercrime preparation Affected countries Kazakhstan Related links	Target industry Banks Threat short name Cobalt cybercrime group	Malware used Mimikatz Cobalt Strike Microsoft Windows Intruder Dissemination tools Email
---	---	--	--	---

BRIEF DESCRIPTION

Group-IB specialists have detected money theft from [REDACTED]

Infection was conducted using standard for Cobalt cybercrime group method – via malicious emails containing documents with exploits. Emails were sent in the beginning of September. As the result, attackers obtained access to the bank's network.

More than two months they conducted research of network and prepared to further money theft. As the result, they obtained administrative access to payment processing system Way4. There they have changed credit limits for bank cards. At the second half of December using these cards they cashed out more than 572 thousand of dollars.

- Cobalt begins to shift focus to payment processing systems.
- Successfully targeted a bank in Kazakhstan cashing out more than \$572,000
- Targeting payment processing systems will be an effective target for less experienced groups as the cashout infrastructure is not as complex.
- Leave Bearing Gifts... IOC Report for Way4 attack.



Web site

www.group-ib.com

Twitter

twitter.com/groupib_gib

E-mail

help@group-ib.com

Facebook

facebook.com/group-ib



+973 7728 8886

yawadhi@ngnintl.com