

Оценка защищенности:

Укрепление слабых звеньев систем защиты данных и предотвращение кибератак. Практика Group-IB



Андрей Брызгин

**Направление аудита и консалтинга,
Group-IB**

EMAIL

BRYZGIN@GROUP-IB.COM



9-10 октября



**CYBER
CRIME
CON/18**



2018.group-ib.ru

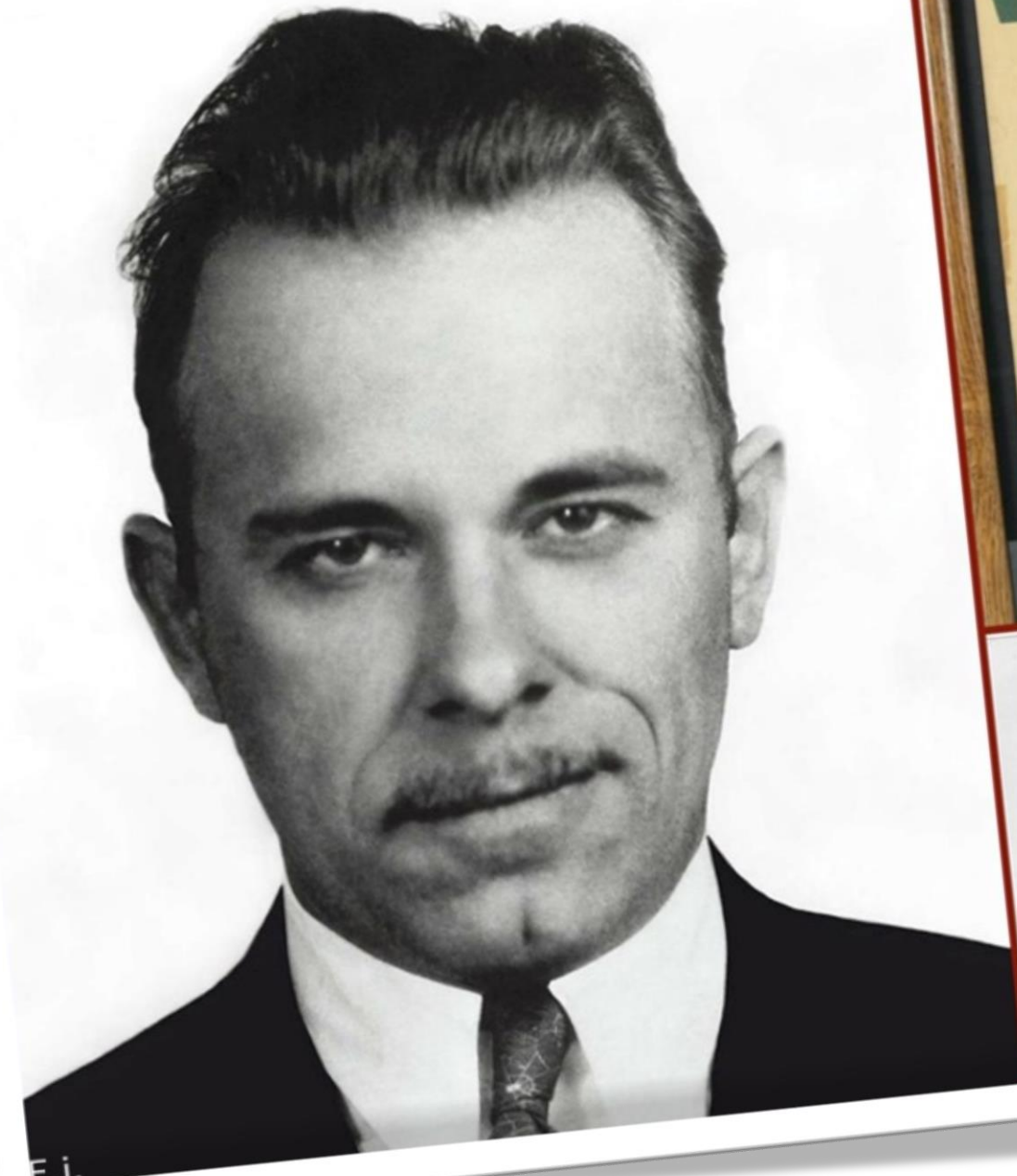
CyberCrimeCon — ключевое событие
в области предотвращения
и расследования киберпреступлений

2 ДНЯ — полное погружение в мир
киберугроз и технологий для защиты

Новая современная площадка —
«Центральное Деловое
Пространство»

Выбирайте свой формат
участия

РЕГИСТРАЦИЯ





Киберпреступность активно растёт

\$ 445млрд

годовой урон мировой экономике от киберпреступности
(Allianz)

38%

экономических преступлений в финансовой сфере
приходятся на киберпреступления (PWC)

3 место

занимают киберугрозы среди ключевых корпоративных рисков
(1 место – простой производства; 2 место – развитие рынков)
(Allianz Risk Barometer)

В 2 раза

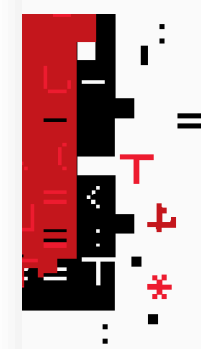
выросло количество атак с использованием вредоносных программ
(Dell)

5,5млрд руб

было похищено в 2016 году (GIB)

46 дней

в среднем занимает устранение киберугрозы, средняя стоимость
составляет таких атак составляет \$21,155 в день
(Ponemon Institute)

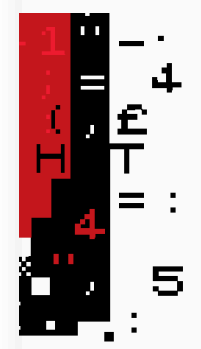


**АТАКУЮЩИЕ,
СПОНСИРУЕМЫЕ
ГОСУДАРСТВАМИ**

Рисковые и мошеннические операции от имени банка

Торги на биржах с целью влияния на курсы валют

Разрушение банковской и телеком-инфраструктуры



**ФИНАНСОВО
МОТИВИРОВАННЫЕ
АТАКУЮЩИЕ**

Уничтожение следов другой атаки

Монетизация неудачного ограбления

Вымогательство



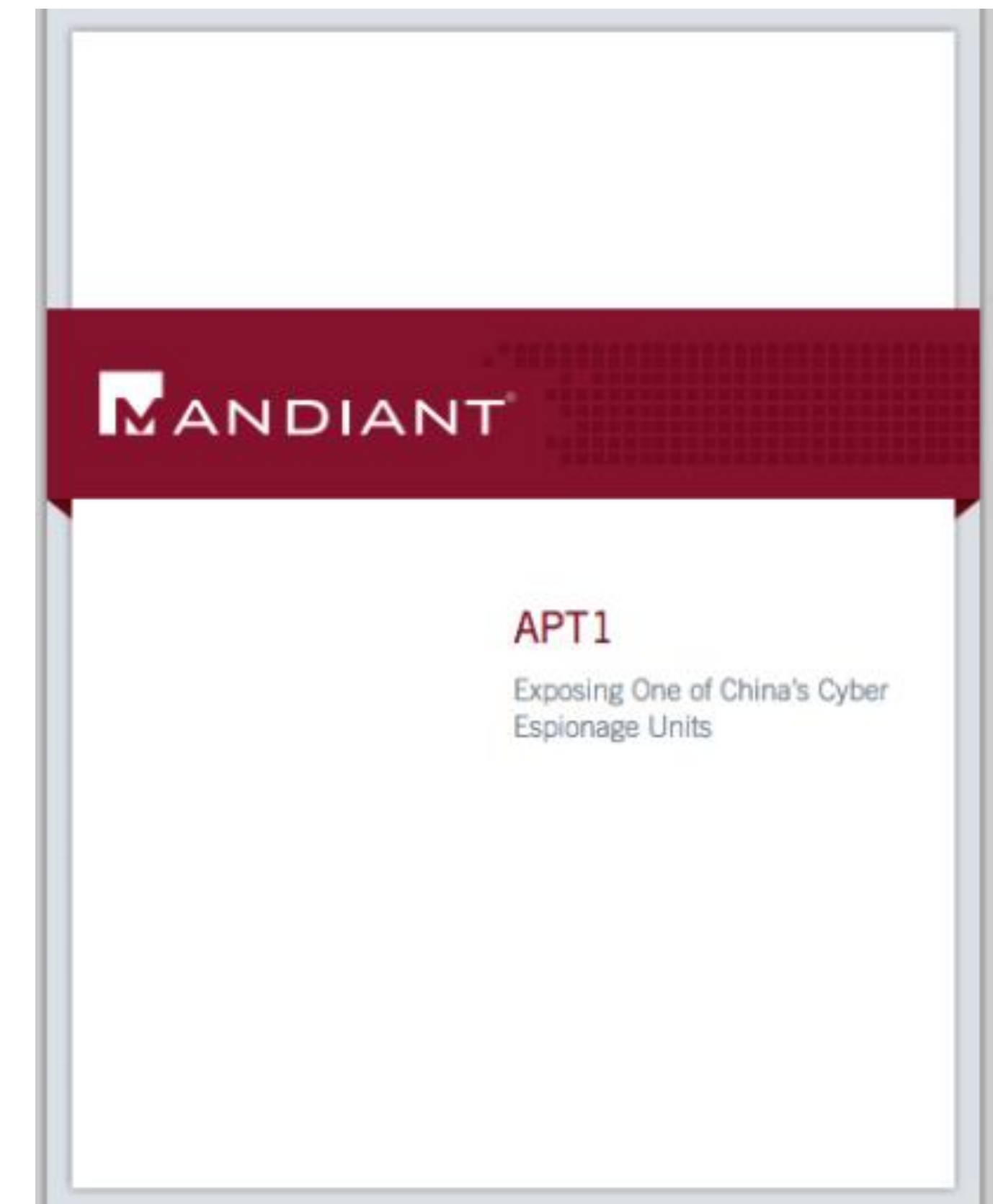
Узнайте больше
group-ib.ru/reports

2013 год. Компания Mandiant публикует отчёт по киберразведывательным операциям в отношении китайской хакерской группы APT1. Краткие выводы:

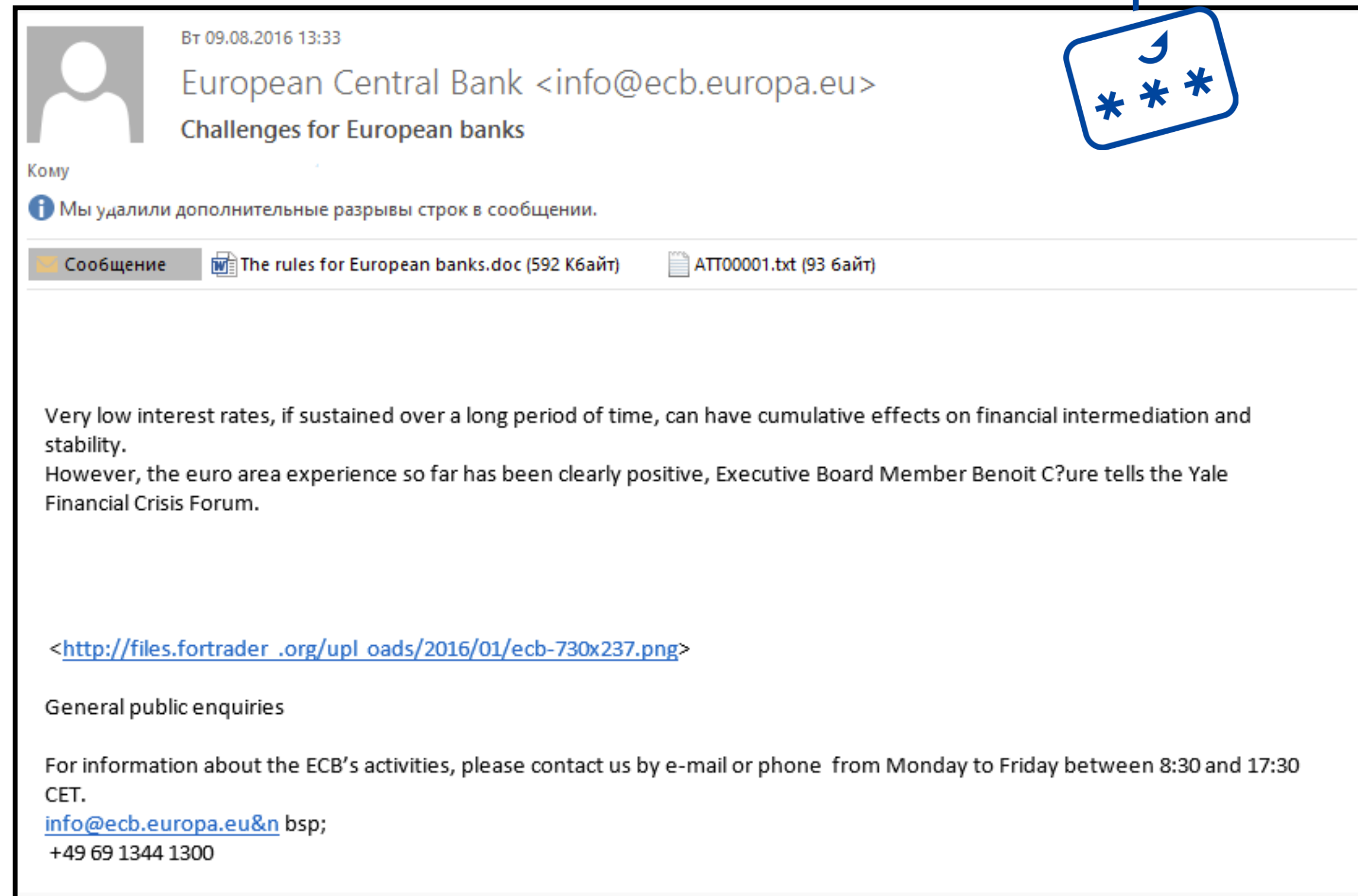
- Профиль группы – не разовые атаки, а длительное (от года), присутствие в атакуемых системах;
- Цели группы – технологические компании в сферах IT, финансов, медиа, энергетики и, конечно, военных разработок по всему миру;
- Группа насчитывает несколько тысяч участников, компактно расположенных в отдельном 12-этажном здании в центре Шанхая;
- Здание подключено к мощнейшим оптоволоконным магистралям.
- В компании, официально расположенные в здании APT1 идёт постоянный набор сотрудников по профилям IT, безопасность и лингвистика.

Основной вывод:

Речь идёт о кибервойсках КНР, получающих задания от правительства и поставляющих информацию для технологического рывка в рамках пятилетних планов развития государства.



Основное средство: Фишинг



Бестелесность и скрипты

- Сложное обнаружение стандартными средствами антивирусной защиты
- Затруднительный процесс реагирования на инцидент
- Легко обеспечить персистентность
- Возможность повторной атаки
- Легко модифицировать

Вымогатели | Прогосударственные группировки

США обвинили КНДР в атаке вируса-вымогателя WannaCry

19 декабря 2017

f t vk л Поделиться



```

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

1Mz7153HMuXtUR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail
w0nsm1th123456@posteo.net. Your personal installation key:

74f296-2Nx1Gm-yHQRWr-SBgaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-oBtizU-gUeUMa

If you already purchased your key, please enter it below.
Key: _
    
```

NotPetya
27 июня 2017

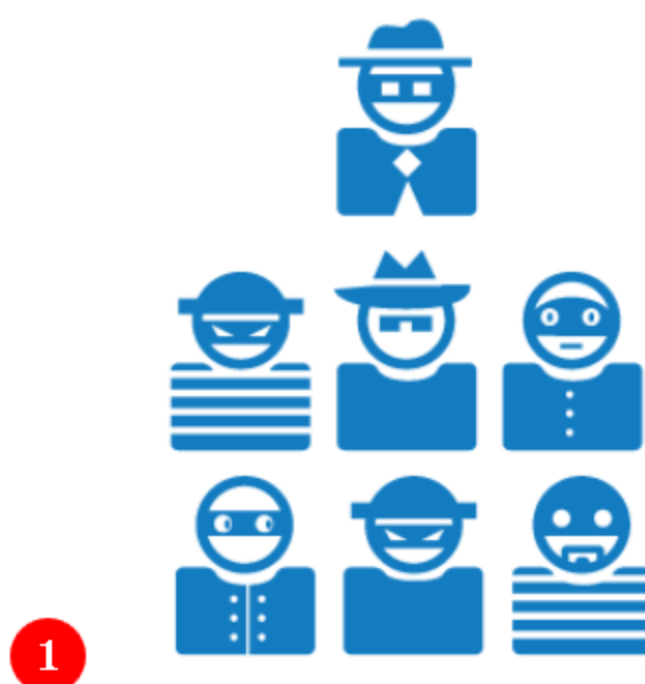


by **Lazarus**

by **Black Energy**



Примеры расследований: Группа Carberp



1

→ Самая большая в России организованная преступная группа онлайн-мошенников (на 2012 г.)



2

→ Расследование проведено в тесном сотрудничестве с ФСБ и МВД России при содействии Сбербанка России



3

→ Первый в российской правоохранительной практике случай задержания всех фигурантов группы онлайн-мошенников

ТЕХНОЛОГИИ И МЕДИА, 01 АВГ 2017, 07:01  88 947

Хакеры российской группировки Cobalt атаковали 250 компаний по всему миру

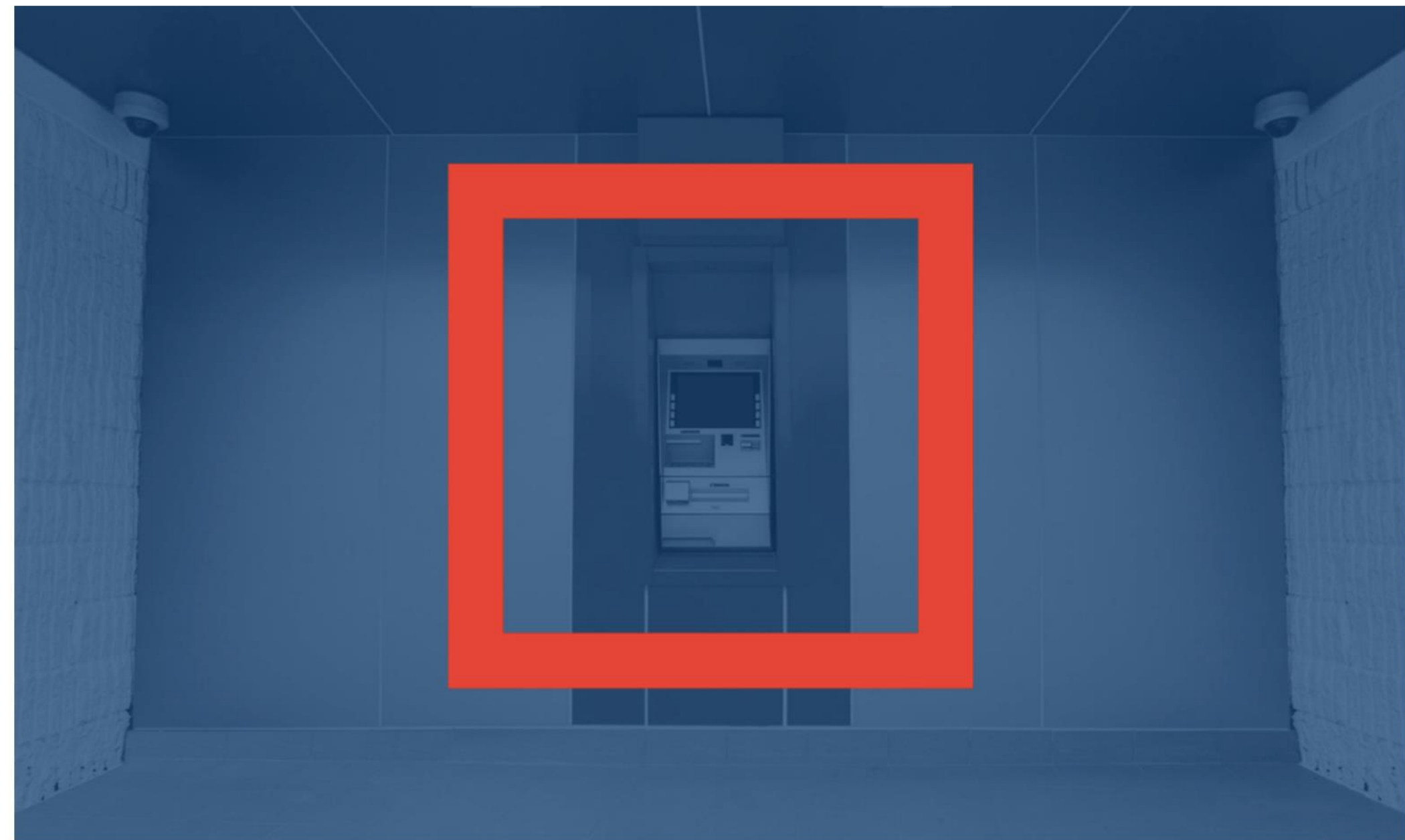
Хакеры из группировки Cobalt, летом 2016 года заставившие банкоматы на Тайване и в Таиланде выбрасывать деньги, в первой половине 2017 года атаковали более 250 организаций по всему миру, рассылая письма от имени Visa и MasterCard



 EditorGIB 16 марта 2017 в 10:58

По следу Cobalt: тактика логической атаки на банкоматы в расследовании Group-IB

Реверс-инжиниринг, Платежные системы, Информационная безопасность, Блог компании «Group-IB»



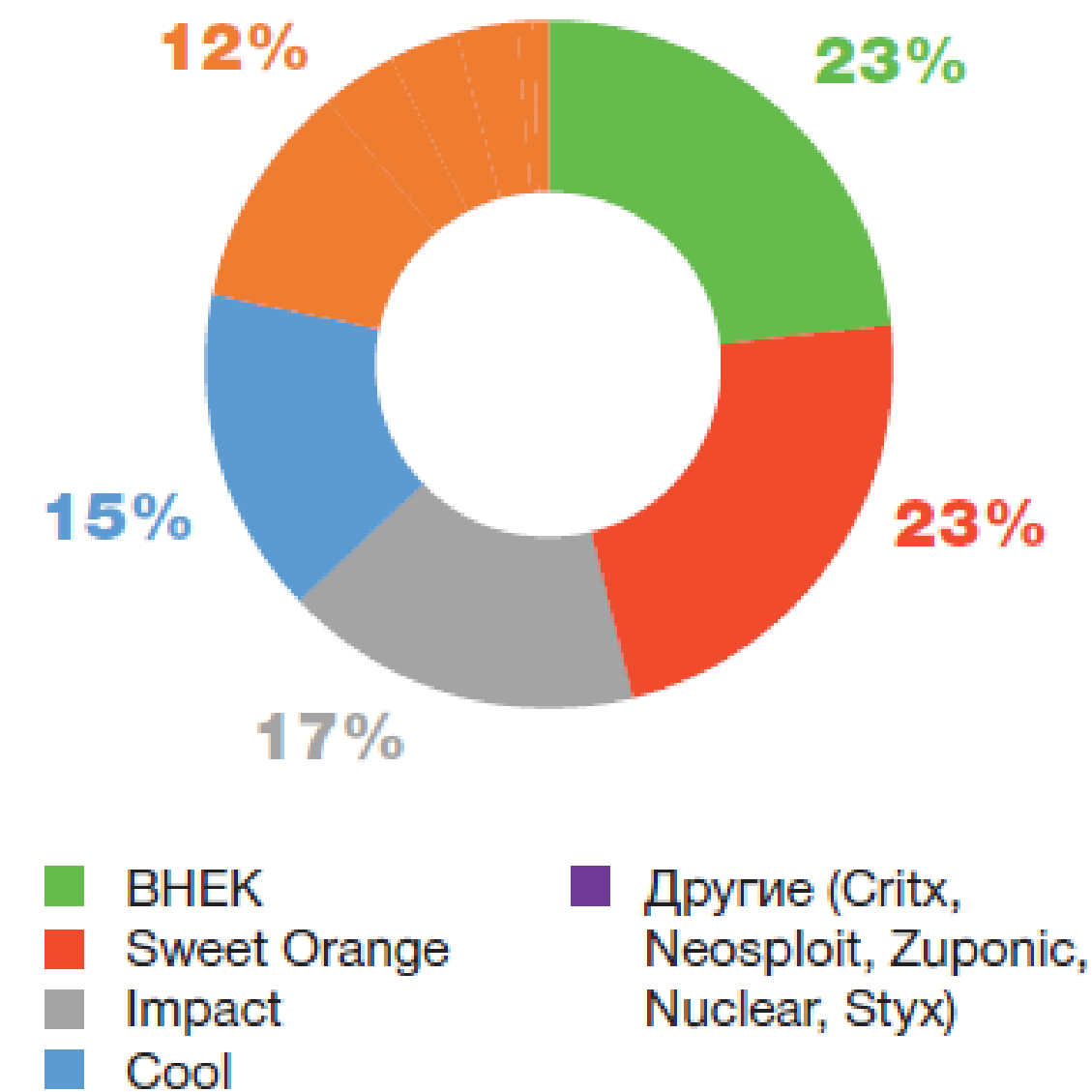
В июле 2016 года работа First Bank, одного из крупнейших банков Тайваня, была парализована. Банк столкнулся с масштабной атакой: люди в масках одновременно опустошили три десятка банкоматов на \$2 млн. Полиция терялась в догадках: на корпусах банкоматов не было ни следов взлома, ни накладных устройств — скиммеров. Злоумышленники даже не использовали банковские карты.

Задержание Raunch

- Автор Blackhole и Cool Exploit kits, сервиса crypt.am
- 40% заражений было сделано с использованием его эксплойтов
- Платил за эксплойты \$100 000 – \$200 000



Exploit Kits - January 2013



Атака на биржу

Компрометация РТС - Сообщение (HTML)

ФАЙЛ СООБЩЕНИЕ

Пн 20.01.2014 16:38

Dmitry Volkov <volkov@group-ib.ru>
Компрометация РТС

Кому 'Maxim Tkachenko'
Копия 'Ilya Sachkov'

Макс,

Вот три айпишника РТС, которые мы видели в бот-сети. Значит там хосты скомпрометированы

194.247.134.72 (rtsnet.ru)
91.208.232.203 (Moscow Interbank Currency Exchange)
91.208.232.124 (Moscow Interbank Currency Exchange)

Best regards,
Dmitry Volkov
Cyber crimes investigation division leader
Briot Head of CERT-GIB
Group-IB
+7 (495) 984-33-64 ext. 111
volkov@group-ib.ru
www.group-ib.ru

Global Cyber Security Company

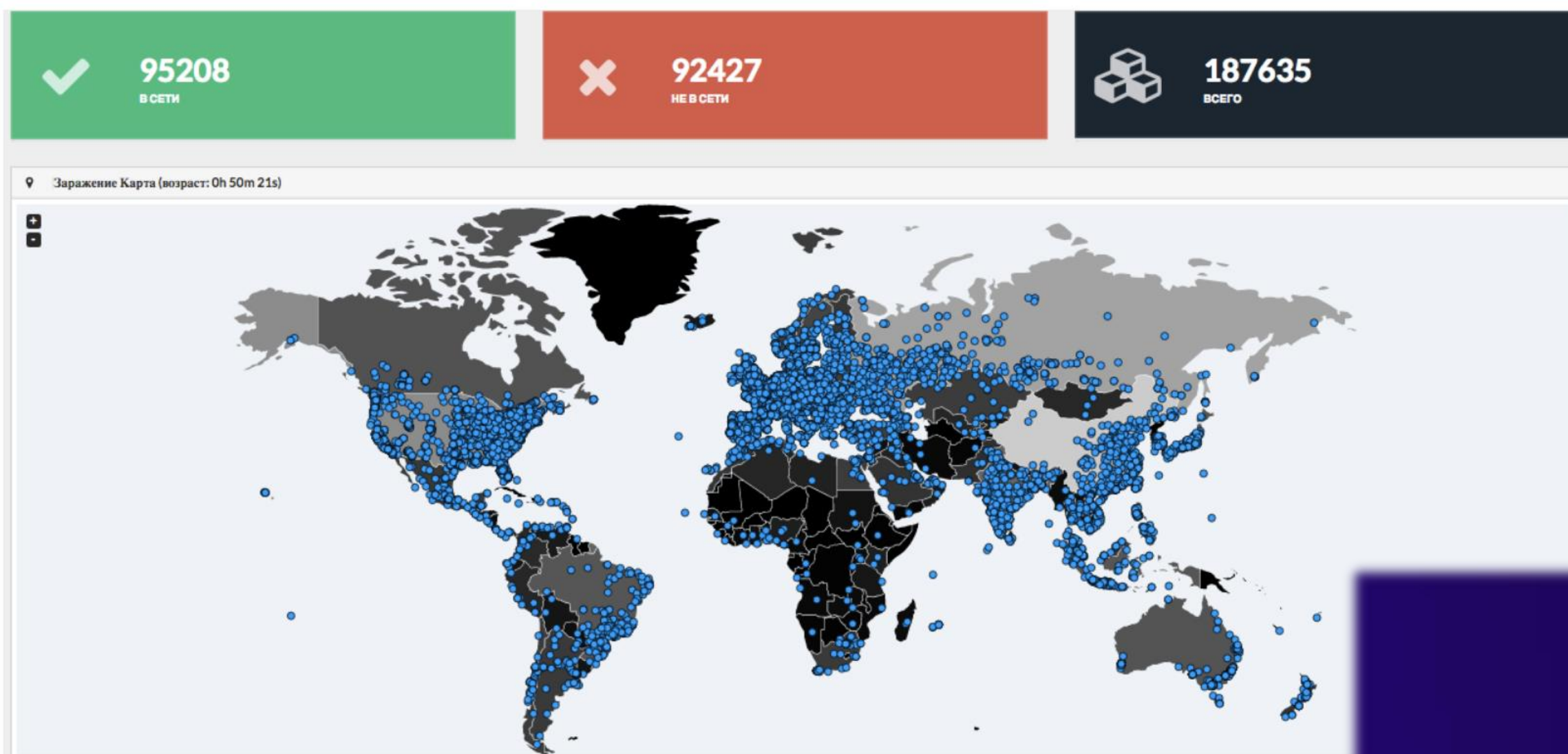
Подробнее о Dmitry Volkov.

1_filtered.pcap [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]

Filter: **ip.addr==194.247.134.72** Expression... Clear Apply >>

No.	Time	Source	Destination	Protocol	Length	Info
49	8.009727	194.247.134.72	217.23.3.201	TCP	66	24120→443 [SYN] Seq=0 w
50	8.009769	194.247.134.72	217.23.3.201	TCP	66	[TCP out-of-order] 2412
59	11.008770	194.247.134.72	217.23.3.201	TCP	66	[TCP Retransmission] 24
60	11.008800	194.247.134.72	217.23.3.201	TCP	66	[TCP Retransmission] 24
94	17.012182	194.247.134.72	217.23.3.201	TCP	62	[TCP Retransmission] 24
95	17.012201	194.247.134.72	217.23.3.201	TCP	62	[TCP Retransmission] 24
174	37.012067	194.247.134.72	217.23.3.201	TCP	66	36540→53 [SYN] Seq=0 wi
175	37.012104	194.247.134.72	217.23.3.201	TCP	66	[TCP out-of-order] 3654
178	40.015388	194.247.134.72	217.23.3.201	TCP	66	[TCP Retransmission] 36
179	40.015415	194.247.134.72	217.23.3.201	TCP	66	[TCP Retransmission] 36

File: "\\fs\\Investigation Department\\Пасследо" Packets: 16559 · Displayed: 762 (4,6%) ... Profile: Default



Атаки вируса-вымогателя Petya

Вирус-вымогатель атаковал нефтяные, телекоммуникационные и финансовые компании по всему миру.



В Севастополе рассказали, как удалось отразить новую атаку вируса Petya

Сюжет: [Атаки вируса-вымогателя Petya](#)

14:43 17.07.2017

0 1349



Минобразования Украины обратилось в киберполицию из-за взлома сайта

Сюжет: [Атаки вируса-вымогателя Petya](#)

12:33 11.07.2017

1 272

24.10.2017

BadRabbit прыгнул

Новая масштабная кибератака с использованием вируса-шифровальщика BadRabbit



МВД РФ начало проверку после хакерской атаки на "ПИР-банк" в Москве

Экономика и бизнес 18 июля, 16:43 UTC+3

Ранее сообщалось, что в ночь на 4 июля хакеры вывели с корреспондентского счета банка более 58 млн рублей

Поделиться



МОСКВА, 18 июля. /ТАСС/. Полицейские начали проверку обстоятельств хакерской атаки в столичном отделении "ПИР-банка". Как сообщили ТАСС в пресс-центре МВД, соответствующее заявление поступило в полицию 10 июля.

"Поступило обращение администрации ООО "ПИР-банк" о несанкционированных операциях с корреспондентским счетом кредитной организации, осуществленных неустановленными лицами", - сказал собеседник агентства.

По его словам, проведение проверки поручено Управлению внутренних дел по Центральному административному округу ГУМВД по Москве.

Ранее газета "Коммерсант" [сообщила](#), что в ночь на 4 июля хакеры вывели с корсчета банка более 58 млн рублей. Председатель правления банка Ольга Колосова сообщила изданию, что часть украденных денег удалось остановить, однако она отметила, что денежные средства выведены веерной рассылкой на пластиковые карты физлиц в 22 банках. По информации главы Сбербанка Германа Грефа, атаку на ПИР Банк совершила группировка Carbanak, использующая для проникновения в защищенный периметр компаний одноименный вирус.

Group-IB: ПИР Банк был атакован хакерской группой MoneyTaker

MONEYTAKER

БАНКИ

ВАЛЕРИЙ БАУЛИН

ДЕЛАЕМ

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

Group-IB, международная компания, специализирующаяся на предотвращении кибератак и разработке продуктов для информационной безопасности, установила, что за атакой на российский ПИР Банк и попыткой хищения нескольких десятков миллионов рублей стоит преступная группа [MoneyTaker](#). Инцидент произошел 3 июля с использованием АРМ КБР (автоматизированное рабочее место клиента Банка России). По заявлению банка, деньги выведены веерной рассылкой на пластиковые карты физических лиц в 17 банках из топ-50, большая часть денежных средств обналичена уже в ночь хищения. После этого злоумышленники попытались «закрепиться» в сети банка для подготовки последующих атак, однако вовремя были обнаружены специалистами Group-IB.

“

В рамках произошедшего инцидента специалисты компании Group-IB в максимально короткие сроки помогли установить предполагаемый источник атаки, выстроить цепочку событий, а также локализовать проблему. На данный момент Банк работает в штатном режиме, все рекомендации компании Group-IB применяются и будут применяться в работе банка, чтобы не допустить подобных инцидентов в будущем.



Ольга Колосова
Председатель Правления ООО ПИР Банк

Исследовав зараженные рабочие станции и сервера финансовой организации, криминалисты Group-IB собрали неопровержимые цифровые доказательства причастности к краже хакеров из MoneyTaker. В частности, экспертами были обнаружены инструменты, которые ранее уже

Tweets by @GroupIB



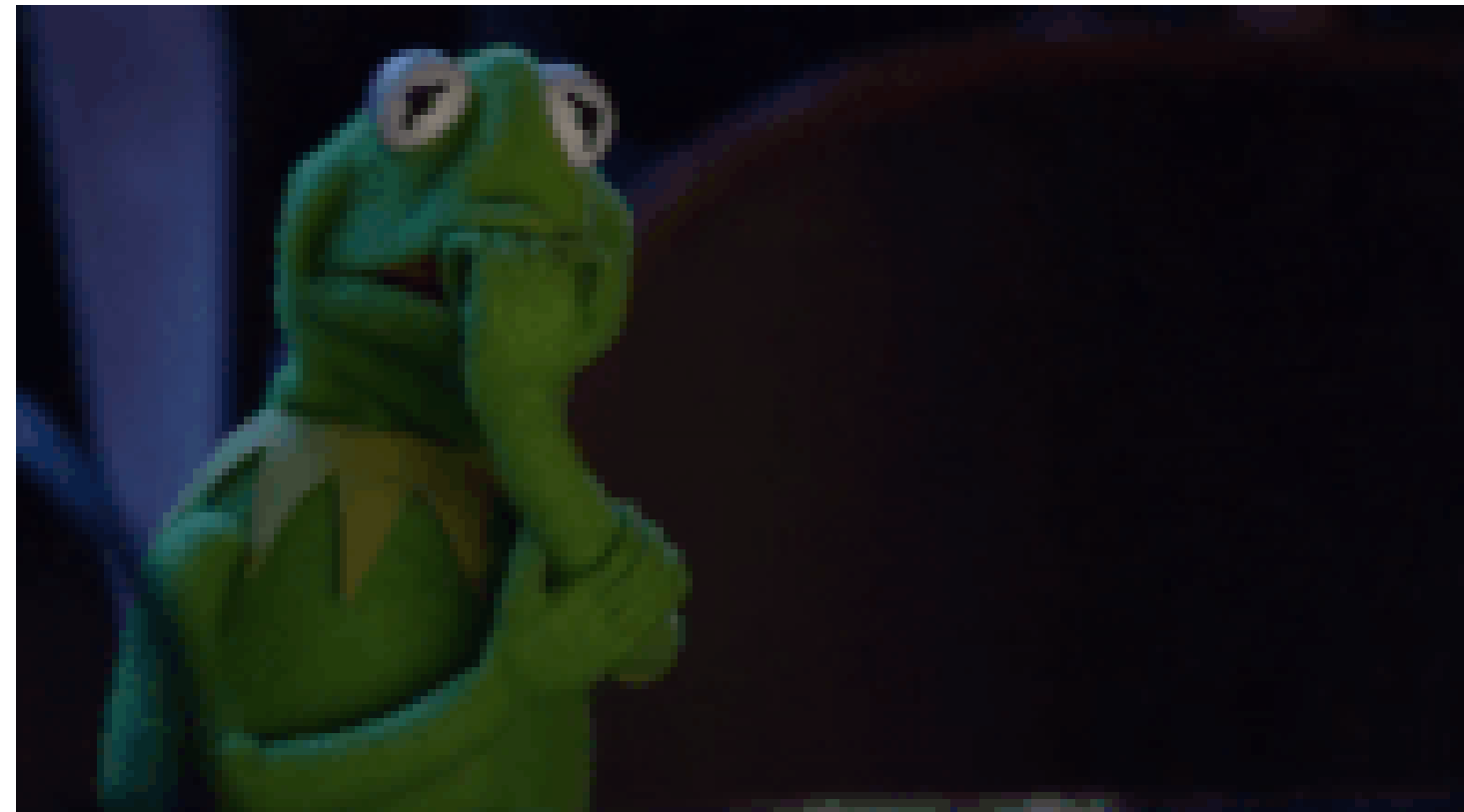
На **86%** зараженных компьютеров в ботнетах установлен антивирус

Main	Bots	Data	Commands	Service						
Filter: Prefix... Country... Apply Filter										
Total bots for botnet "40": 31989										
Bots with filter:										
All bots	ID	N	Prefix	Country	Uptime	A	CMD	CMD Status	DBO	Token
Online bots	a2b679184df7		main	RU	148:54:07	A			1C, Unk, SberBank_BO	
Bots with DBO	9bf386b51a53		main	RU	10:33:06	A			WinPost, Unk	
Bots with tokens	8b4bbc8d9a94		main	RU	2:23:50	A			iBank2, iBank2_PC	
	d36a200ce6a9		main	RU	9:55:21	A			BSS, Unk	
Bots with comments	4942d929ce31		main	RU	236:34:52	A			iBank2_PC, Unk	
Find bot	78f1ea791b8a		main	RU	53:41:35	A			BSS, SberBank_BO, 1C, Unk	
	f102c70baa7f		main	RU	100:28:55	A			BSS, Unk	
	d13508ab601f		main	RU	5:20:52	A			BSS, 1C, Unk	
	bf68f1954e92		main	RU	3:05:00	A			BSS_PC, Unk, SberBank_BO	
	76bb0431c664		bit3	RU	51:25:18	A		OK 1	Faktura, 1C, Unk	
	43e2e5c5b0de		bit3	RU	4:40:22	A			1C, Unk, BSS, iBank2_PC	
	2740f5894393		bit3	RU	5:29:44	A		OK 1	BSS, 1C, Unk	
	06ed4007e9ba		0.1.5	BY	1:36:02	A			1C, BSS_PC	
	9ae400c2e22b		bit3	RU	8:24:40	A			WinPost, Unk	
	a11b73148088		main	RU	22:57:24	A			iBank2_PC	
	95126e92f960		main	RU	3:21:52	A			iBank2_PC, 1C, Unk	
	d9e2fc48338d		bit3	RU	142:53:10	A			BSS, BSS_PC, 1C, Raiffeisen, Unk, SberBank_Fiz	
	d2a76c021fea		main	RU	5:45:54	A			BSS, 1C, Unk	
	435a42be64d2		main	RU	6:42:48	A		OK 1	Inter Pro, 1C, Unk	
	31a52b15dfcf		main	RU	3:52:50	A			BSS, 1C, Unk	
	495104d84bc0		bit3	RU	8:41:47	A			BSS, SBIS, 1C, Unk, SberBank_BO	
	1a2442f2c8a3		main	RU	7:50:36	A			BSS, 1C, Unk	
	be72ae17bd5b		main	RU	6:11:28	A			Unk	

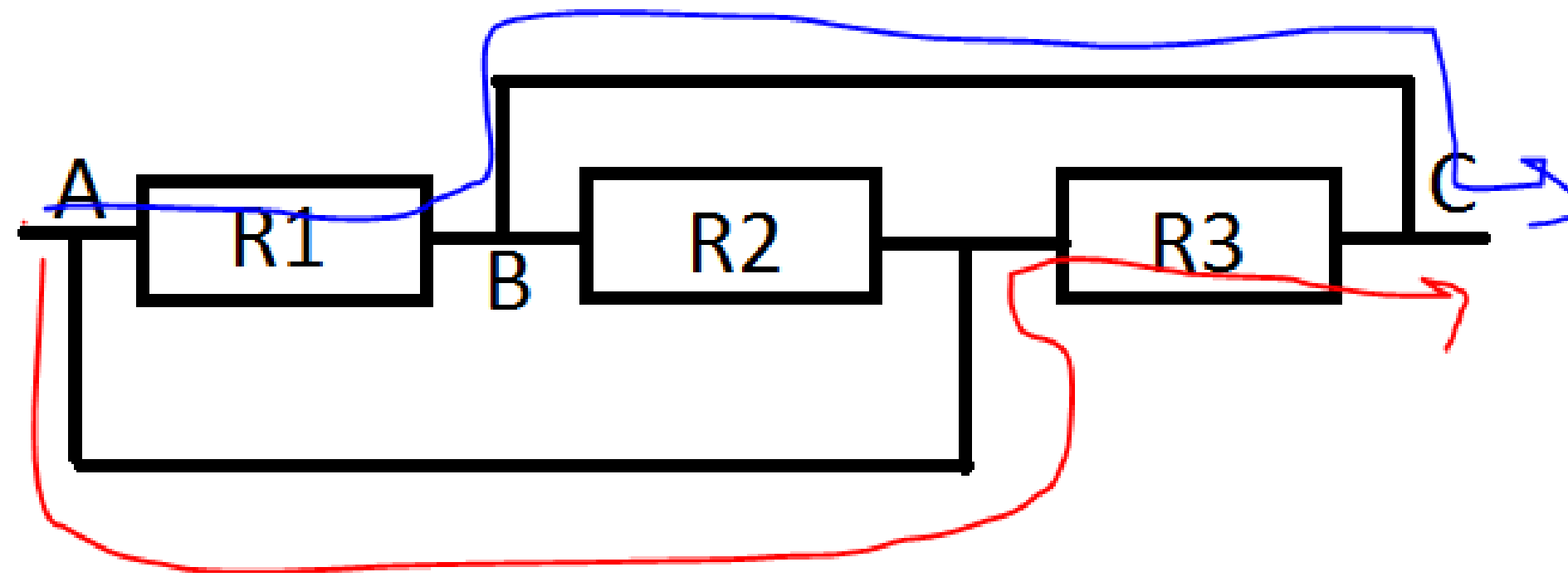
Logout
Core
Stats
AVStats
ProgramsStats
Bots
Loads
Backconnects
Updates
Campaigns
Jupiter
Webinjects

AV encounter success	Encounters	Bot installed [%]	AV not prevented bot [%]	Bot not installed [%]	AV prevented bot [%]
Avast	57	49 [85.96%]	41 [83.67%]	8 [14.04%]	8 [100.00%]
Bkav	1	1 [100.00%]	0 [0.00%]	0 [0.00%]	0 [0.00%]
ESET	20	20 [100.00%]	20 [100.00%]	0 [0.00%]	0 [0.00%]
Kaspersky	8	8 [100.00%]	4 [50.00%]	0 [0.00%]	0 [0.00%]
Ikarus	1	1 [100.00%]	1 [100.00%]	0 [0.00%]	0 [0.00%]
AVG	5	3 [60.00%]	2 [66.67%]	2 [40.00%]	2 [100.00%]
电脑管家系统防护	5	4 [80.00%]	4 [100.00%]	1 [20.00%]	1 [100.00%]
CMC Antivirus	1	1 [100.00%]	0 [0.00%]	0 [0.00%]	0 [0.00%]
McAfee	9	9 [100.00%]	6 [66.67%]	0 [0.00%]	0 [0.00%]
AntiVir Desktop	3	1 [33.33%]	1 [100.00%]	2 [66.67%]	2 [100.00%]
Microsoft	14	13 [92.86%]	12 [92.31%]	1 [7.14%]	1 [100.00%]
360 Total Security	3	3 [100.00%]	2 [66.67%]	0 [0.00%]	0 [0.00%]
Baidu Antivirus	5	5 [100.00%]	5 [100.00%]	0 [0.00%]	0 [0.00%]
Windows Defender	9	9 [100.00%]	2 [22.22%]	0 [0.00%]	0 [0.00%]
Антивирус Касперского Яндекс-версия	1	1 [100.00%]	0 [0.00%]	0 [0.00%]	0 [0.00%]
ZoneAlarm Antivirus	1	1 [100.00%]	1 [100.00%]	0 [0.00%]	0 [0.00%]
Avira	3	2 [66.67%]	1 [50.00%]	1 [33.33%]	0 [0.00%]
Norton	4	4 [100.00%]	0 [0.00%]	0 [0.00%]	0 [0.00%]
G Data AntiVirus	2	2 [100.00%]	2 [100.00%]	0 [0.00%]	0 [0.00%]
Quick Heal Total Security	1	1 [100.00%]	1 [100.00%]	0 [0.00%]	0 [0.00%]
IObit Malware Fighter	1	1 [100.00%]	0 [0.00%]	0 [0.00%]	0 [0.00%]

Сложно! Непонятно! Стрессово!

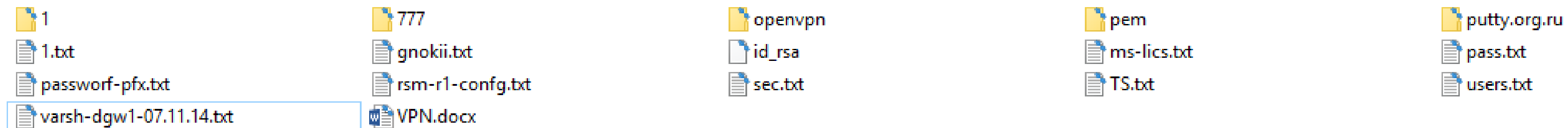


Нерабочие схемы защиты



Ключи под ковриком

- Времена года: Весна-2018, Лето-2018, Осень-2017, Зима-2017;
- qazWSX123; Qwerty123 и далее в том же духе;
- Универсальные и дефолтные пароли.



Содержимое файлов users.txt и pass.txt из скриншота выше:

```
sharepoint
(пароль)

search
(пароль)

crm. lan
root
(пароль)

MySQL
vtiger
(пароль)

https://crm. lan
admin
(пароль)

CA
web_ca
(пароль)
```

Листинг 2. Содержимое файла users.txt

Andrey

Ср 07.10.2015 11:34

пометить как непрочитанное

Кому: Dmitry

Копия: Vladimir

• Это сообщение отправлено с высокой важностью.

Привет!

Дима, с инженером договорились, что он будет в офисе завтра (четверг) с 10-00.

Нужно сделать перевод их стенда на наш «бой».

Я им скидывал следующие настройки .v2.Client.Host.exe.config:

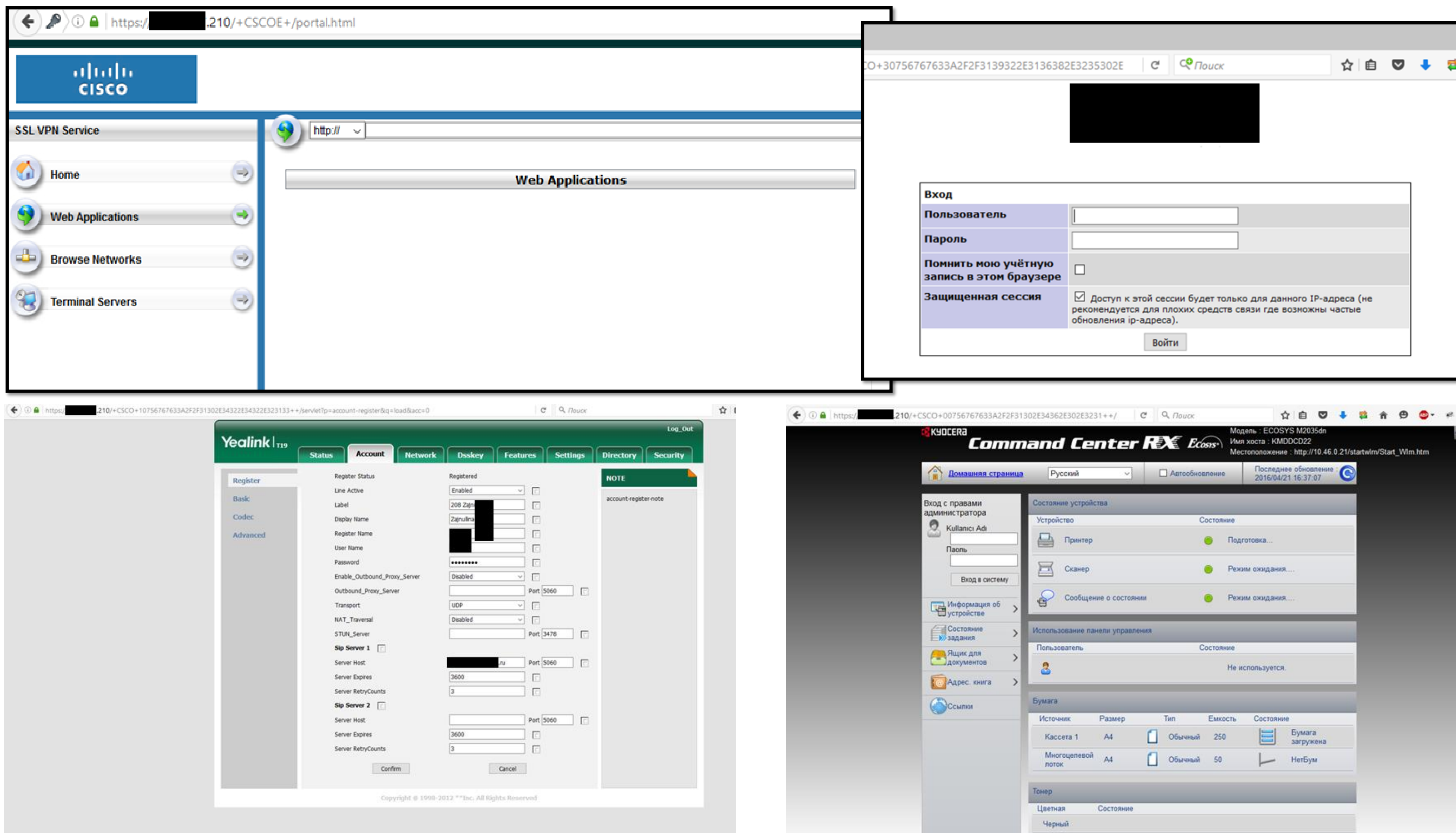
«1) Host: <https://api.>

2) Login: 0004

3) **Password:** 00040004

Если установлен на Windows7, то нужно открыть только 443 порт. Для Windows ниже чем win7, надо открыть порт 9010.»

Открытые двери



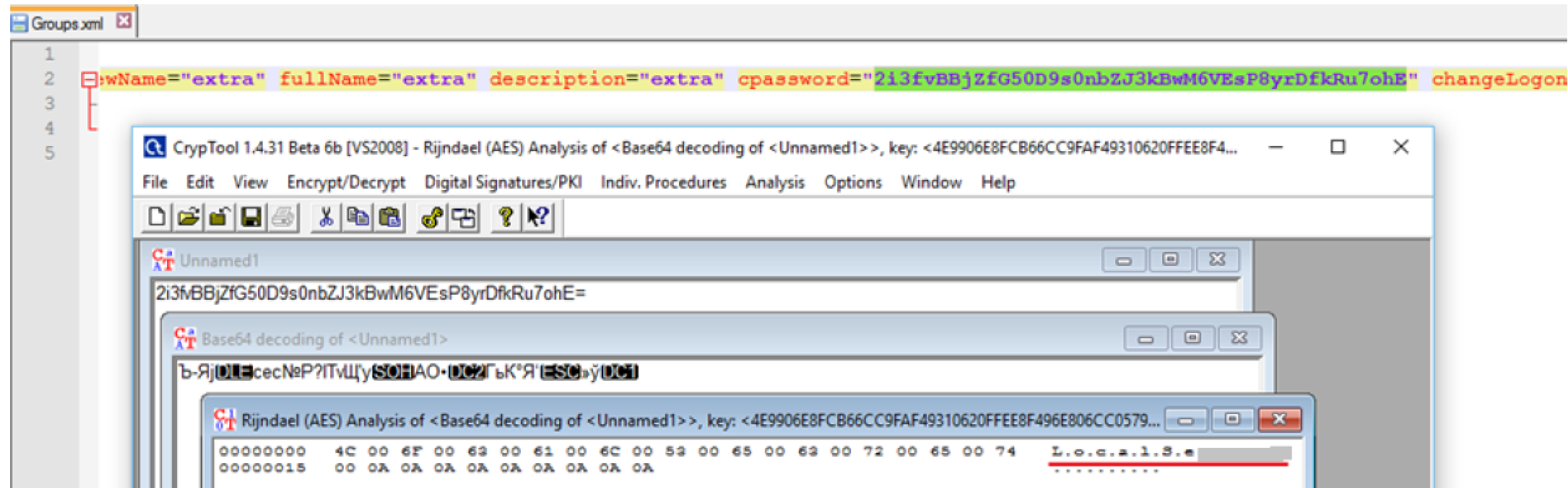


Рисунок 12. Расшифровка пароля.

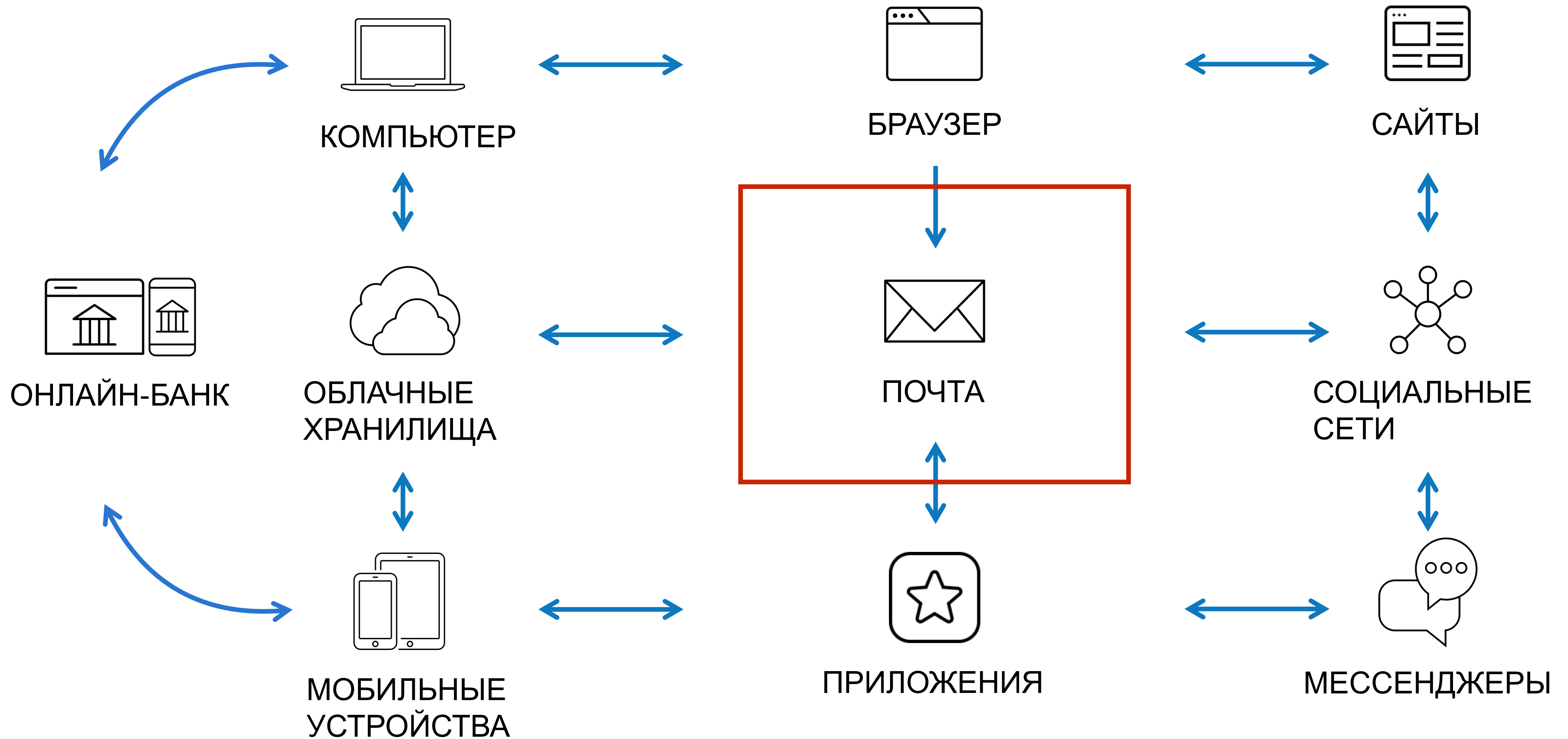
Получена учетная запись: extra с паролем LocalSe..... (вырезано), которая является локальным администратором на рабочих станциях.

CVSS v2 Vector (AV:A/AC:L/Au:S/C:C/I:C/A:C). Общий балл – 7.7 (высокий).

Опасность уязвимости в контексте теста – критическая.



Почта – объект особого внимания



[Features](#) [Business](#) [Explore](#) [Marketplace](#) [Pricing](#)

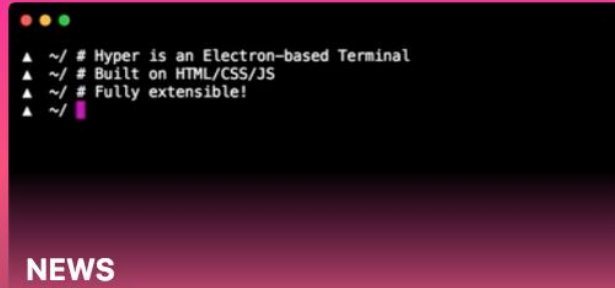
[Sign in](#) or [Sign up](#)



COLLECTION
Pixel art tools
Create some pixel art or animated sprites with your pick from the tools in this fun collection.



Congrats on 1 million users, Sam! 🎉
Join the next million composers to code music with Sonic Pi >



NEWS
@zeithq releases Hyper 2
The Electron-based Terminal, Hyper, graduates to Version 2.0 on Windows, macOS, and Linux.

Trending repositories

Date range: This week ▼

[adam-golab / react-developer-roadmap](#)
Roadmap to becoming a React developer in 2018
★ 4.4k 🍴 297

[phobal / ivideo](#)
一个可以观看国内主流视频平台所有视频的客户端 (Mac、Windows、Linux)，包括 VIP 资源
★ 3k 🍴 686

[browsh-org / browsh](#)
A fully-modern text-based browser, rendering to TTY and browsers
★ 3.1k 🍴 48

[nbedos / termtosvg](#)
Record terminal sessions as SVG animations
★ 3k 🍴 99

[serhii-londar / source-mac-os-applications](#)
🚀 Awesome list of open source applications for macOS
★ 2.4k 🍴 197

 Want Explore delivered to your inbox?

[Sign up for GitHub](#) or [Sign in](#)

sy,shu, suj, suudo, sudoi, etc

MAKE ME A SANDWICH.

SUDO MAKE ME
A SANDWICH.



WHAT? MAKE
IT YOURSELF.

OKAY.



```
manohar@mani: ~
manohar@mani:~$ sudo apt-get install mysql-server
[sudo] password for manohar:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libdbd-mysql-perl libdbi-perl libhtml-template-perl libnet-daemon-perl libplrpc-perl mysql-client-5.1 mysql-client-core-5.1 mysql-server-5.1
  mysql-server-core-5.1
Suggested packages:
  libipc-sharedcache-perl libterm-readkey-perl tinyca mailx
The following NEW packages will be installed:
  libdbd-mysql-perl libdbi-perl libhtml-template-perl libnet-daemon-perl libplrpc-perl mysql-client-5.1 mysql-client-core-5.1 mysql-server
  mysql-server-5.1 mysql-server-core-5.1
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 20.7 MB of archives.
After this operation, 50.3 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://in.archive.ubuntu.com/ubuntu/ oneiric/main libnet-daemon-perl all 0.48-1 [43.1 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu/ oneiric/main libplrpc-perl all 0.2020-2 [36.0 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu/ oneiric/main libdbi-perl i386 1.616-1build1 [852 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu/ oneiric/main libdbd-mysql-perl i386 4.019-1 [110 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu/ oneiric-updates/main mysql-client-core-5.1 i386 5.1.61-0ubuntu0.11.10.1 [88.5 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu/ oneiric-updates/main mysql-client-5.1 i386 5.1.61-0ubuntu0.11.10.1 [8,620 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu/ oneiric-updates/main mysql-server-core-5.1 i386 5.1.61-0ubuntu0.11.10.1 [4,634 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu/ oneiric-updates/main mysql-server-5.1 i386 5.1.61-0ubuntu0.11.10.1 [6,256 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu/ oneiric/main libhtml-template-perl all 2.10-1 [65.0 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu/ oneiric-updates/main mysql-server all 5.1.61-0ubuntu0.11.10.1 [6,452 B]
Fetched 20.7 MB in 7min 39s (45.1 kB/s)
Preconfiguring packages ...
Selecting previously deselected package libnet-daemon-perl.
(Reading database ... 168926 files and directories currently installed.)
Unpacking libnet-daemon-perl (from .../libnet-daemon-perl_0.48-1_all.deb) ...
Selecting previously deselected package libplrpc-perl.
Unpacking libplrpc-perl (from .../libplrpc-perl_0.2020-2_all.deb) ...
Selecting previously deselected package libdbi-perl.
Unpacking libdbi-perl (from .../libdbi-perl_1.616-1build1_i386.deb) ...
Selecting previously deselected package libdbd-mysql-perl.
Unpacking libdbd-mysql-perl (from .../libdbd-mysql-perl_4.019-1_i386.deb) ...
Selecting previously deselected package mysql-client-core-5.1.
Unpacking mysql-client-core-5.1 (from .../mysql-client-core-5.1_5.1.61-0ubuntu0.11.10.1_i386.deb) ...
Selecting previously deselected package mysql-client-5.1.
```

Хостинги как супермаркет сливов



- Режим ЗИ и инструктажи по его соблюдению
- Персональная ответственность

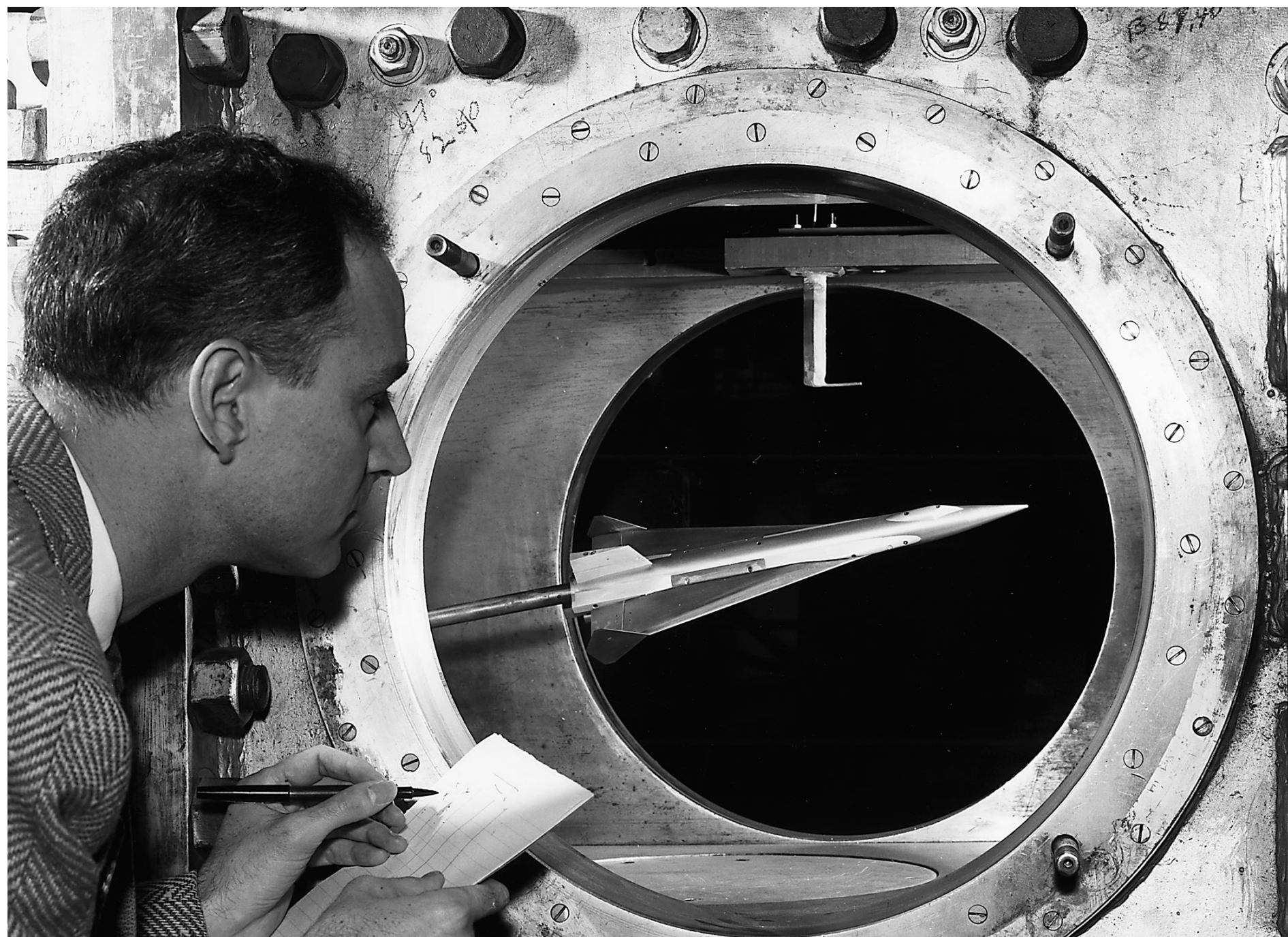


Ответственность за нарушение
законодательства о коммерческой
тайне

Что делать?

Что же делать?

Регулярные проверки защищённости



Обнаружение вторжений



Что делать?

Что же делать?

Регулярные проверки защищённости

Обнаружение вторжений



86%

веб-ресурсов, требующих идентификации, содержат как минимум одну критическую уязвимость

Многолетняя практика аудита крупных порталов, банковских и производственных систем показывает, что защищённость «на бумаге» оборачивается крайней беззащитностью перед реальными угрозами.

Формальный подход к обороне позволяет злоумышленникам месяцами контролировать самые критичные системы, подвергая риску конфиденциальность данных и сохранность счетов.

193

дня в среднем системы остаются беззащитными до устранения уязвимости

1

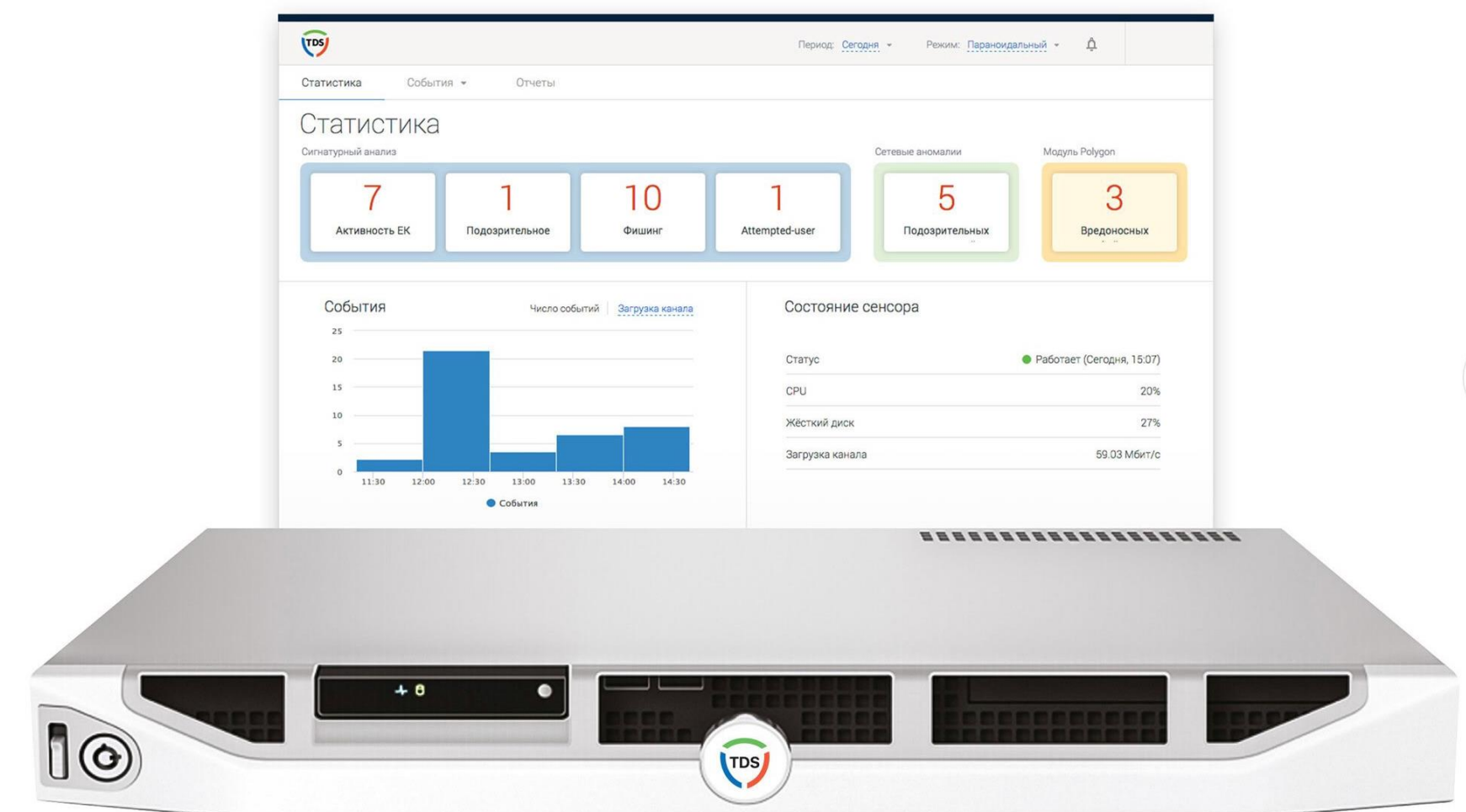
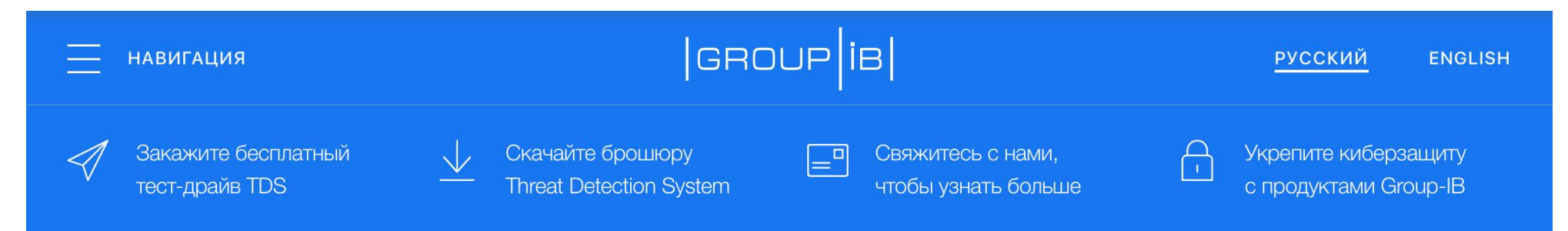
час и меньше требуется злоумышленнику для кражи информации и вывода денег

Мы не доверяем «бумажной безопасности», тщательно исследуя практическую защищённость бизнес-процессов. Хорошо понимая актуальные технологии киберпреступников, мы видим слабости ваших систем их глазами.

Результаты аудита предельно конкретны – мы даем объективное представление об уязвимостях и четкие рекомендации для подготовки к отражению реальных угроз.

1 500 000

мобильных телефонов в РФ заражены троянами и управляются злоумышленниками



СПАСИБО ЗА ВНИМАНИЕ!

ВЫ ВСЕГДА МОЖЕТЕ СО МНОЙ СВЯЗАТЬСЯ



Андрей Брызгин

**Направление аудита и консалтинга,
Group IB**

EMAIL

BRYZGIN@GROUP-IB.COM