SAS FORUM
RUSSIA 2017

Киберпреступность 2017
Вызовы и решения

О Group-IB

Group-IB — одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий

1000+

успешных расследований по всему миру, 150 особо сложных уголовных дел

$300 млн

возвращено клиентам Group-IB благодаря нашей работе

Официальный партнер Europol, полицейской службы Евросоюза

Рекомендована Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

Постоянный член Всемирного экономического форума

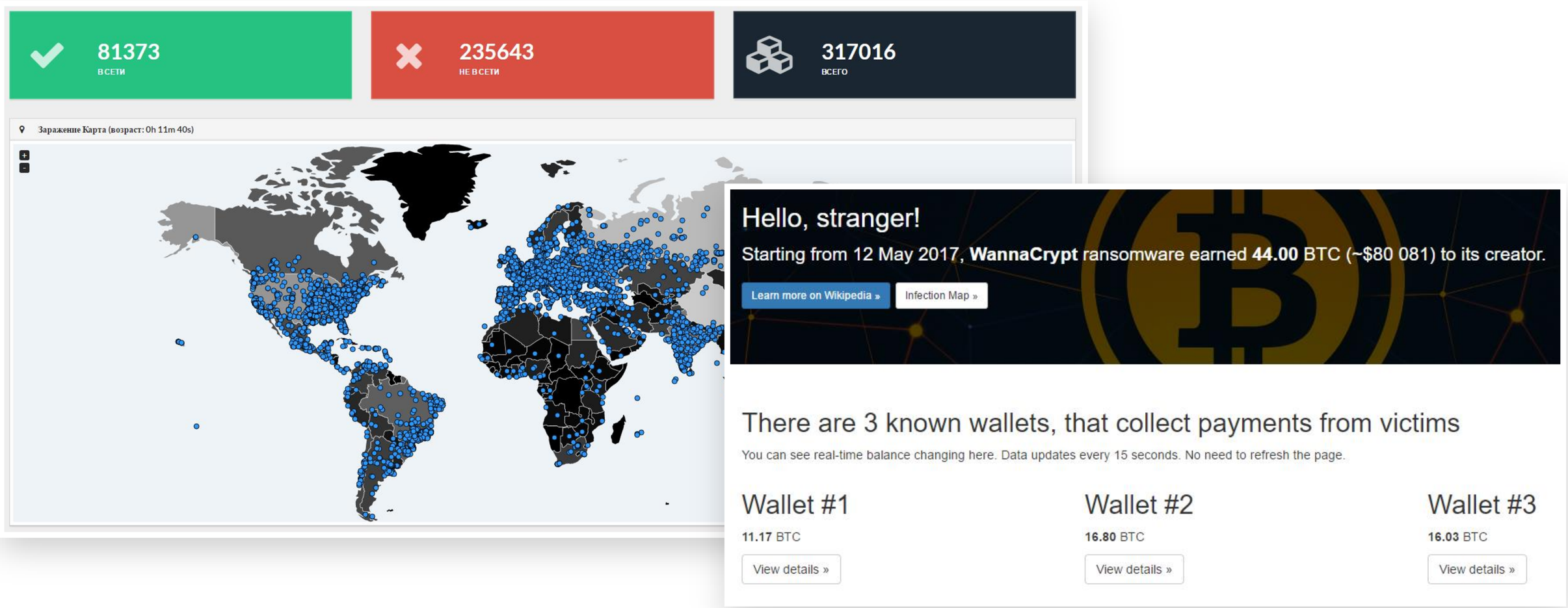
Threat Intelligence от Group-IB – в числе лучших мировых систем по оценке Forrester и Gartner

Одна из 7 самых влиятельных компаний в области кибербезопасности по версии Business Insider

Лидер российского рынка по исследованию киберугроз

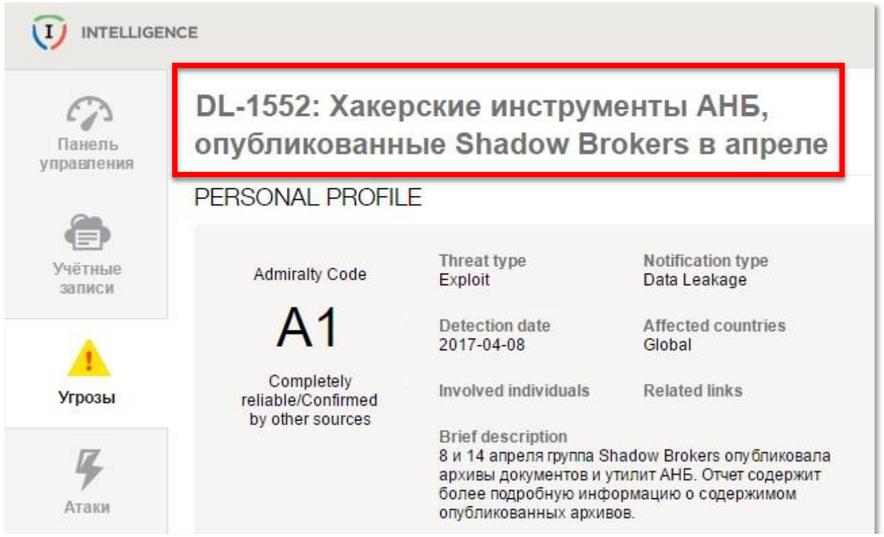
О нас говорят:

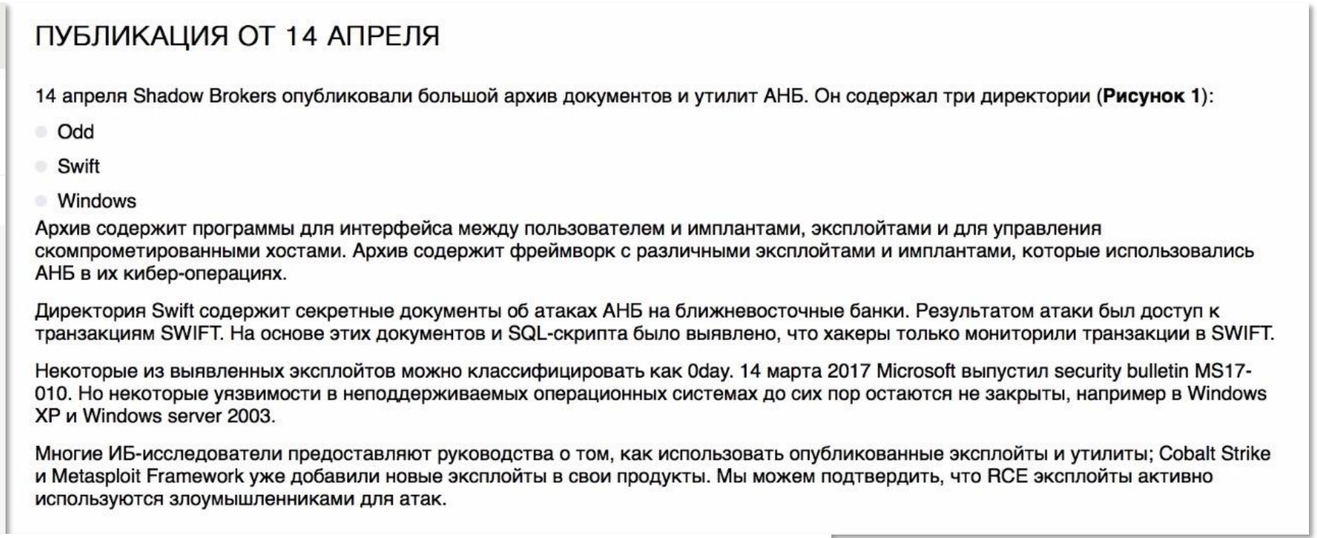
В мае весь мир следил за WannaCrypt



https://intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all
https://whitesunset.github.io/wannacrypt_balance/

Почему WannaCrypt стал глобальной эпидемией





ПУБЛИКАЦИЯ ОТ 14 АПРЕЛЯ

14 апреля Shadow Brokers опубликовали большой архив документов и утилит АНБ. Он содержал три директории (**Рисунок 1**):

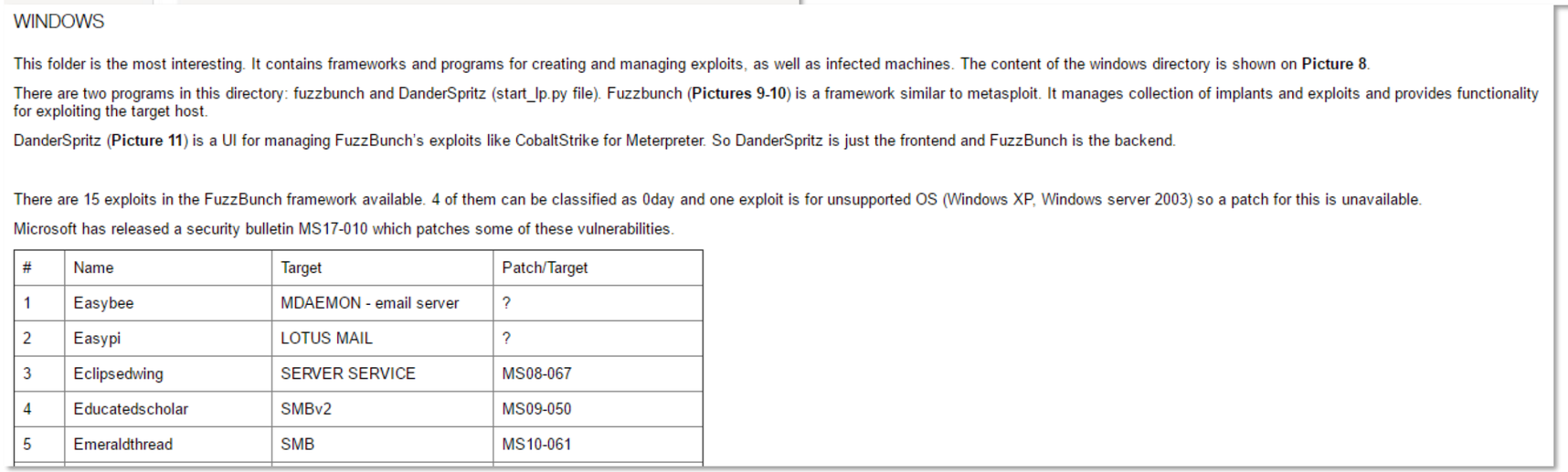
- Odd
- Swift
- Windows

Архив содержит программы для интерфейса между пользователем и имплантами, эксплойтами и для управления скомпрометированными хостами. Архив содержит фреймворк с различными эксплойтами и имплантами, которые использовались АНБ в их кибер-операциях.

Директория Swift содержит секретные документы об атаках АНБ на ближневосточные банки. Результатом атаки был доступ к транзакциям SWIFT. На основе этих документов и SQL-скрипта было выявлено, что хакеры только мониторили транзакции в SWIFT.

Некоторые из выявленных эксплойтов можно классифицировать как 0day. 14 марта 2017 Microsoft выпустил security bulletin MS17-010. Но некоторые уязвимости в неподдерживаемых операционных системах до сих пор остаются не закрыты, например в Windows XP и Windows server 2003.

Многие ИБ-исследователи предоставляют руководства о том, как использовать опубликованные эксплойты и утилиты; Cobalt Strike и Metasploit Framework уже добавили новые эксплойты в свои продукты. Мы можем подтвердить, что RCE эксплойты активно используются злоумышленниками для атак.



WINDOWS

This folder is the most interesting. It contains frameworks and programs for creating and managing exploits, as well as infected machines. The content of the windows directory is shown on **Picture 8**.

There are two programs in this directory: fuzzbunch and DanderSpritz (start_lp.py file). Fuzzbunch (**Pictures 9-10**) is a framework similar to metasploit. It manages collection of implants and exploits and provides functionality for exploiting the target host.

DanderSpritz (**Picture 11**) is a UI for managing FuzzBunch's exploits like CobaltStrike for Meterpreter. So DanderSpritz is just the frontend and FuzzBunch is the backend.

There are 15 exploits in the FuzzBunch framework available. 4 of them can be classified as 0day and one exploit is for unsupported OS (Windows XP, Windows server 2003) so a patch for this is unavailable.

Microsoft has released a security bulletin MS17-010 which patches some of these vulnerabilities.

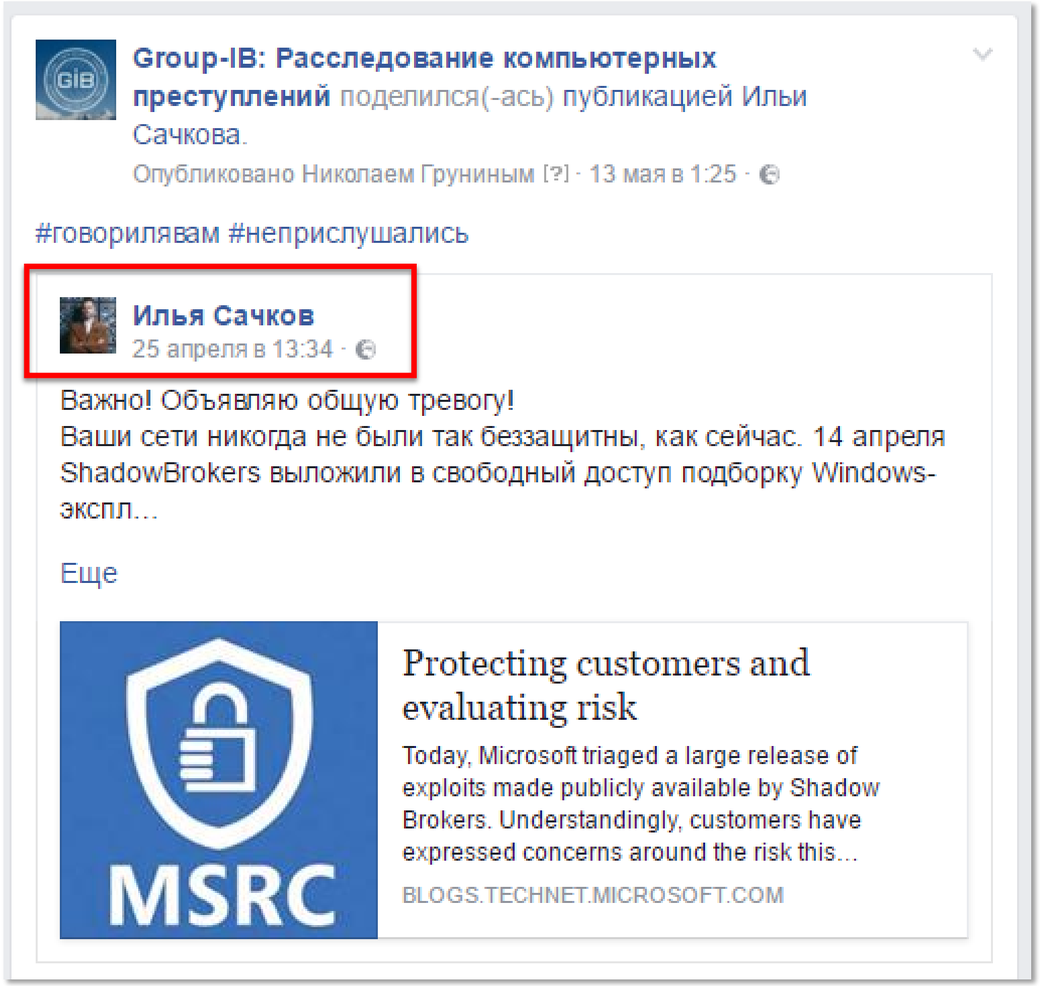
#	Name	Target	Patch/Target
1	Easybee	MDAEMON - email server	?
2	Easypi	LOTUS MAIL	?
3	Eclipsedwing	SERVER SERVICE	MS08-067
4	Educatedscholar	SMBv2	MS09-050
5	Emeraldthread	SMB	MS10-061

АПРЕЛЬ 2017

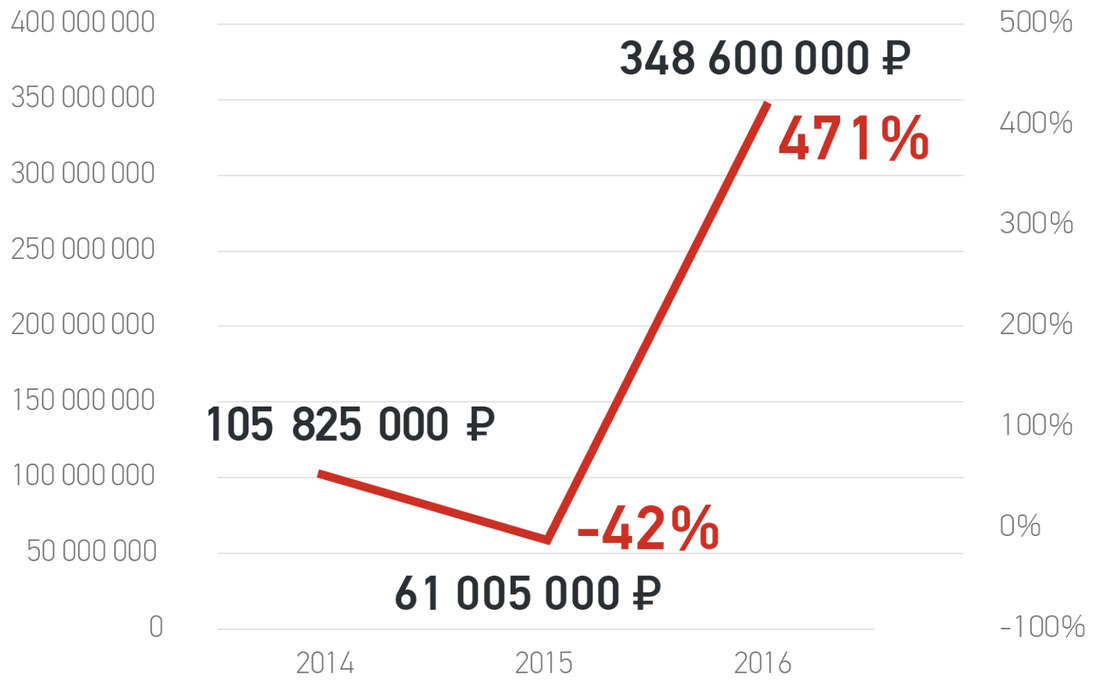
Клиенты Threat Intelligence получили уведомление об утечке еще в апреле.

Отчет содержал подробный разбор содержащихся в архиве документов, а также рекомендации по предотвращению угрозы

Можно ли было избежать заражения?



Все уходят на Android



РОССИЯ

Group 404
ApiMaps
Adabot
Cron1 (new)
FlexNet (new)
Agent.sx (new)
Agent.BID (new)
Honli (new)
Asucub (new)
FakeInst.ft (new)
GM bot (new)
Fake Marcher (new)
Cron2 (new)
Greff
March
Webmobil
Mikorta
MobiApps
Xruss
Tark
Sizeprofit

ЕВРОПА И США

Marcher 2.0 (new)
Xbot (new)
Abrvall (new)
Asacub (new)
Mbot 2.0 (new)
T00rb00r (new)
Marcher
GM-bot
Skunk
Bilal
Reich (Svpeng)

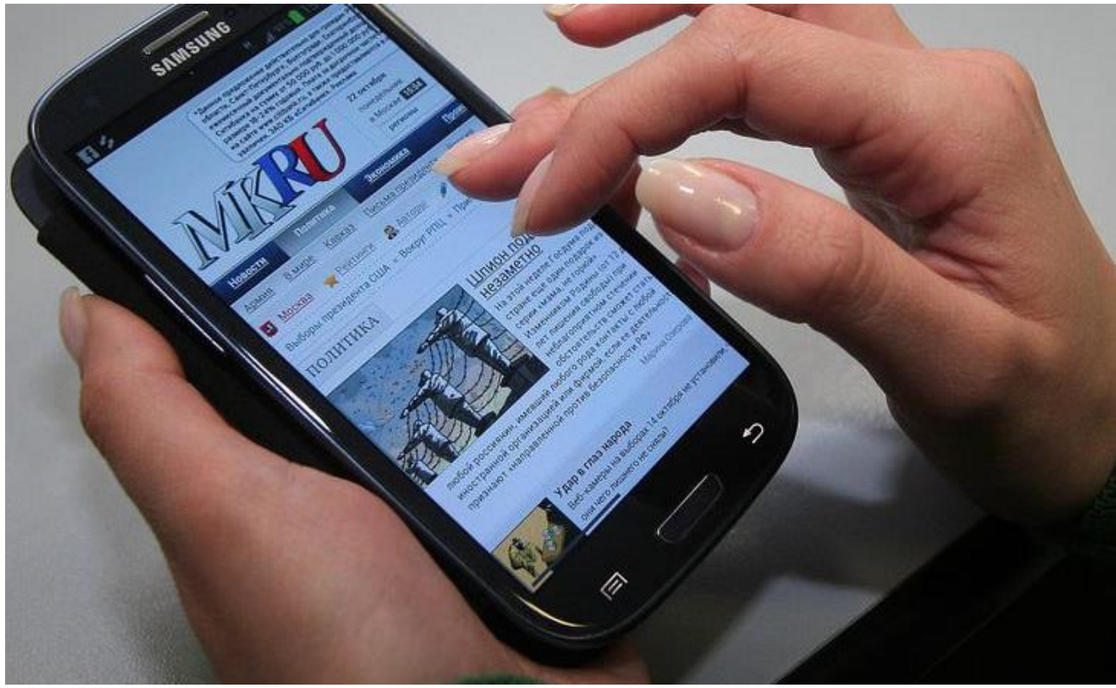
Падение CRON

МВД и Group-IB ликвидировали группу, заразившую миллион смартфонов

ANDROID ПОД ПРИЦЕЛОМ

Впервые мы услышали про Cron в марте 2015 года: система киберразведки Group-IB зафиксировала активность новой преступной группы, распространяющей на хакерских форумах вредоносные программы «viber.apk», «Google-Play.apk», «Google_Play.apk» для ОС Android.

Cron атаковал пользователей крупных российских банков из ТОП-50.



Как сработал CRON

1

Попадая на телефон жертвы, троян мог автоматически переводить деньги с банковского счета пользователя на счета, подконтрольные злоумышленникам. Для этого хакеры открыли более 6 000 счетов.

2

После установки программа помещалась в автозагрузку устройства и сама могла отправлять SMS-сообщения на указанные преступниками телефонные номера, пересылать текст получаемых жертвой SMS-сообщений на удаленные сервера, а также скрывать поступающие по SMS уведомления от банка.

Задержание CRON

К ноябрю 2016 года сотрудники МВД при участии Group-IB смогли установить 20 членов группы, собрать цифровые доказательства совершенных преступлений. Лидером группы был 30-летний житель г. Иваново.

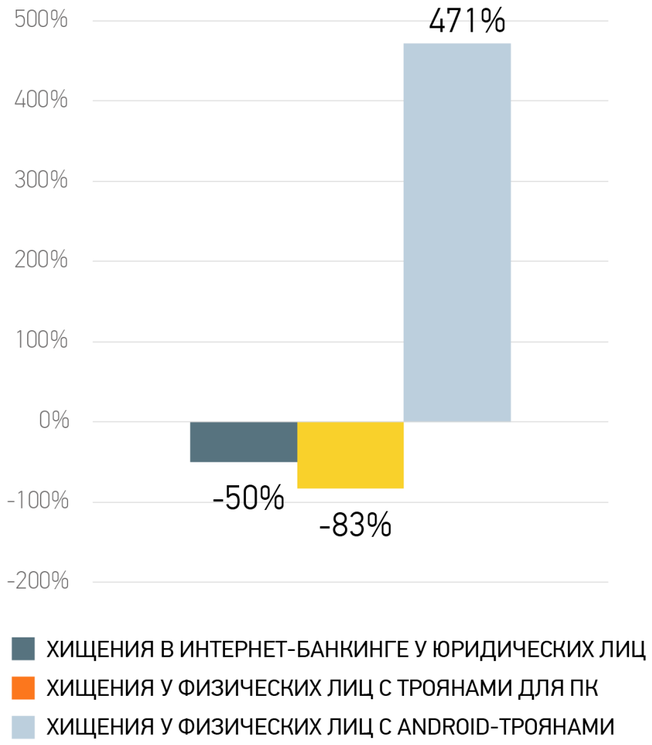
22 ноября 2016 года, в 6 регионах России была проведена масштабная операция: задержаны 16 участников группировки Cron. Последний активный участник группы был задержан в начале апреля 2017 года в Санкт-Петербурге.

Захват рынка вирусописания для ПК русскоязычными специалистами

РОССИЯ

Buhtrap
Toplel
Ranbyus
RTM (new)
Jupiter (new)

Lurk
Corkow
Yebot
Kronos
Chtonic



МИР

Panda Banker (new)
Shifu (new)
Midas bot (Jupiter) (new)
GozNym (new)
Sphinx (new)
Corebot (new)
Atmos (new)
Gozi (ISFB)
Dridex
Qadars
Gootkit
Vawtrak
Tinba
KINS (ZeusVM)
Citadel
Zeus
Quakbot (Qbot)
Retefe
Ramnit

A BRIEF GUIDE TO RUSSIAN-SPEAKING CYBERCRIME BY GROUP-IB

«85 per sent of [Europol's] cases are Russian-speaking organized cyber groups»

Troels Oerting, Head of Europol's European Cybercrime Centre (EC3)

16 из 19 троянских программ, наиболее активно используемых для кибератак, разработаны русскоязычными киберпреступниками

Уровни поведенческого анализа*

Big Data User and Entity Analytics
- Enable analysis of both linkages and relationships across users and other entities and their attributes using data in big data stores to detect fraud

User- and Entity-Centric for Multiple Channels and Products
- Analyzes and correlates users and other entity behavior across different channels and products, and prioritizes alerts using rules or statistical models

User- and Entity-Centric for Specific Channel
- Monitors and analyzes user and entity behavior, as well as identities anomalous behavior using rules or statistical models

Navigation- and Network-Centric
- Analyzes session or network behavior and compares it to what is expected

End-point centric
- Malware detection, end-point behavior and location correlation
- Device fingerprinting, phone printing and “bloprinting”

Поведение на разных ресурсах? Глобальный поведенческий профиль.

Какие совершает операции? Как? Кто?

Какие совершает операции в одном канале? Как? Кто?

Аномалии в сессии работы пользователя. Время, география операций, с каких устройств?

*https://www.gartner.com/doc/1646115/layers-fraud-prevention-using-beat

Соц. инженерия – драйвер мошенничества

Сбербанк фиксирует порядка 5 тыс. атак в неделю с использованием социальной инженерии

ПОДЕЛИТЬСЯ

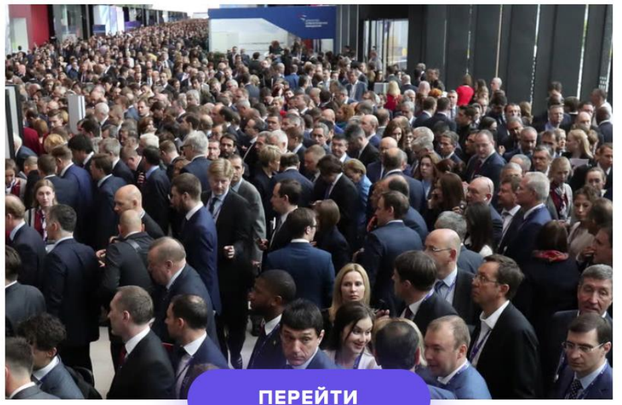
Потенциальный ущерб от этих покушений составляет около 700 млн рублей, отметил зампред правления банка Станислав Кузнецов

САНКТ-ПЕТЕРБУРГ, 3 июня. /ТАСС/. Сбербанк фиксирует порядка 5-5,5 тыс. атак на клиентов в неделю с использованием социальной инженерии. Об этом сообщил журналистам зампред правления банка Станислав Кузнецов в кулуарах Петербургского международного экономического форума.

"5-5,5 тысяч атак конкретно с использованием социальной инженерии", - сказал Кузнецов.

Активность мошенников усиливается, добавил он. Тем не менее, служба фрод-мониторинга Сбербанка минимизирует ущерб от их действий. "Потенциальный ущерб от этих покушений составляет около 700 млн рублей", - сообщил Кузнецов.

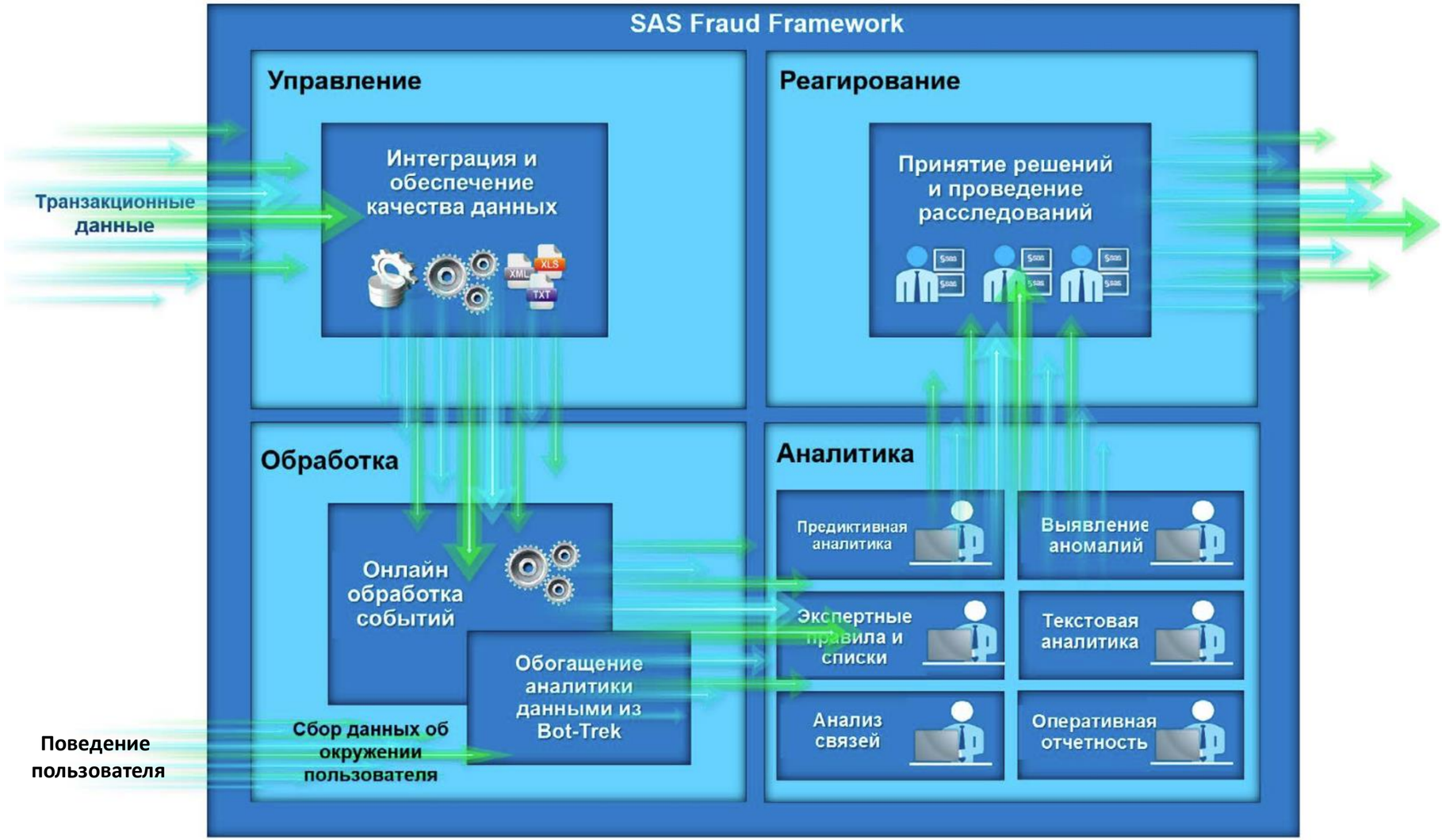
ФОТОБАНК



ВИДЕО

*http://tass.ru/pmef-2017/articles/4310476

sas + GROUP IB



Преимущества

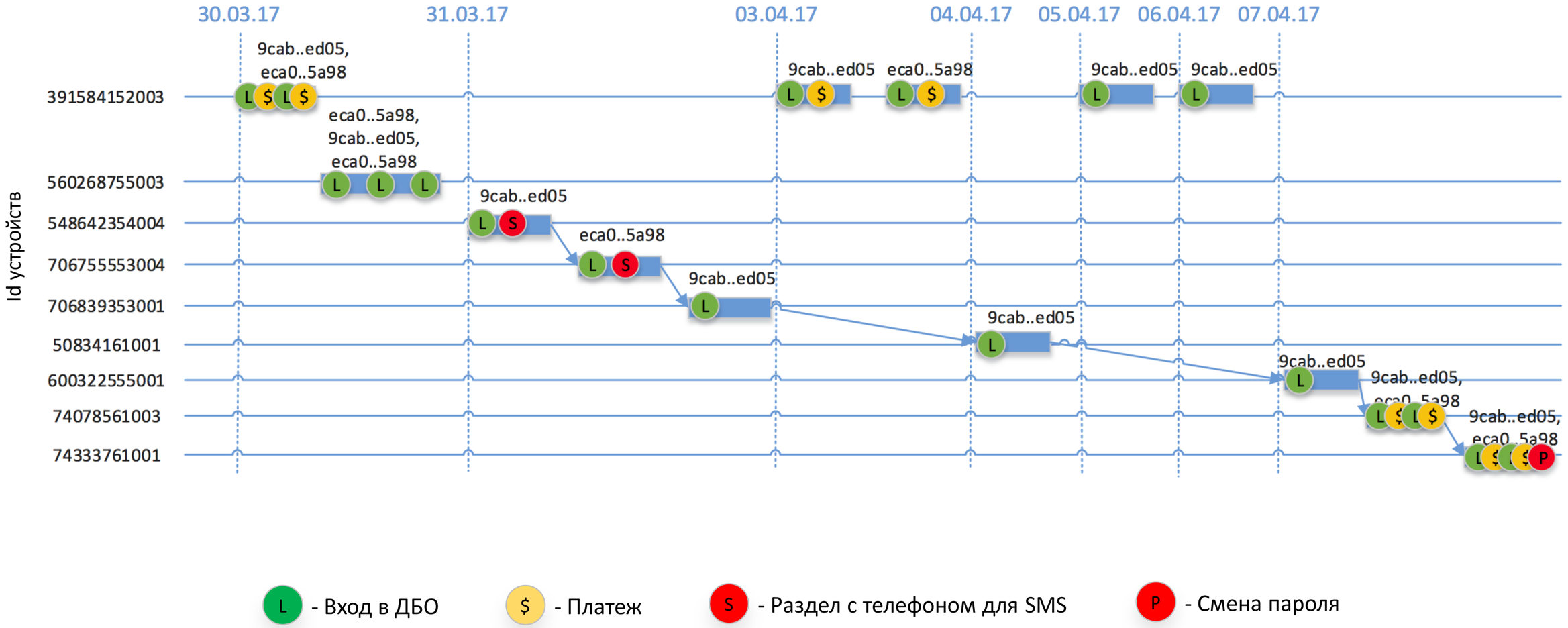
Увеличение предиктивной точности аналитических моделей

Детектирование угроз на стадии планирования и подготовки мошенничества

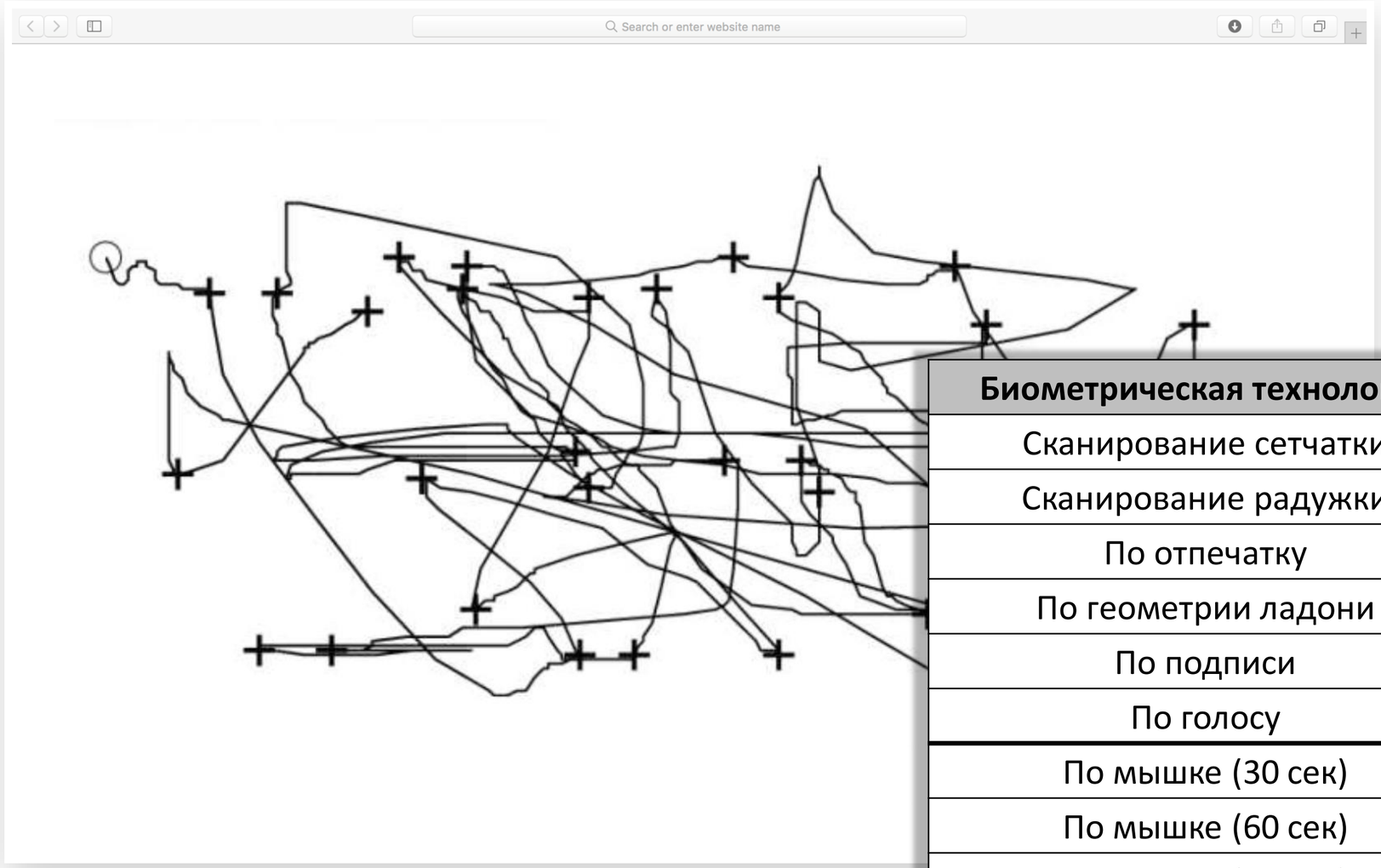
Перманентная осведомленность о новых схемах мошенничества и обновление черных списков

Простая интеграция и единая поддержка решения

Уровень 3: какие действия?



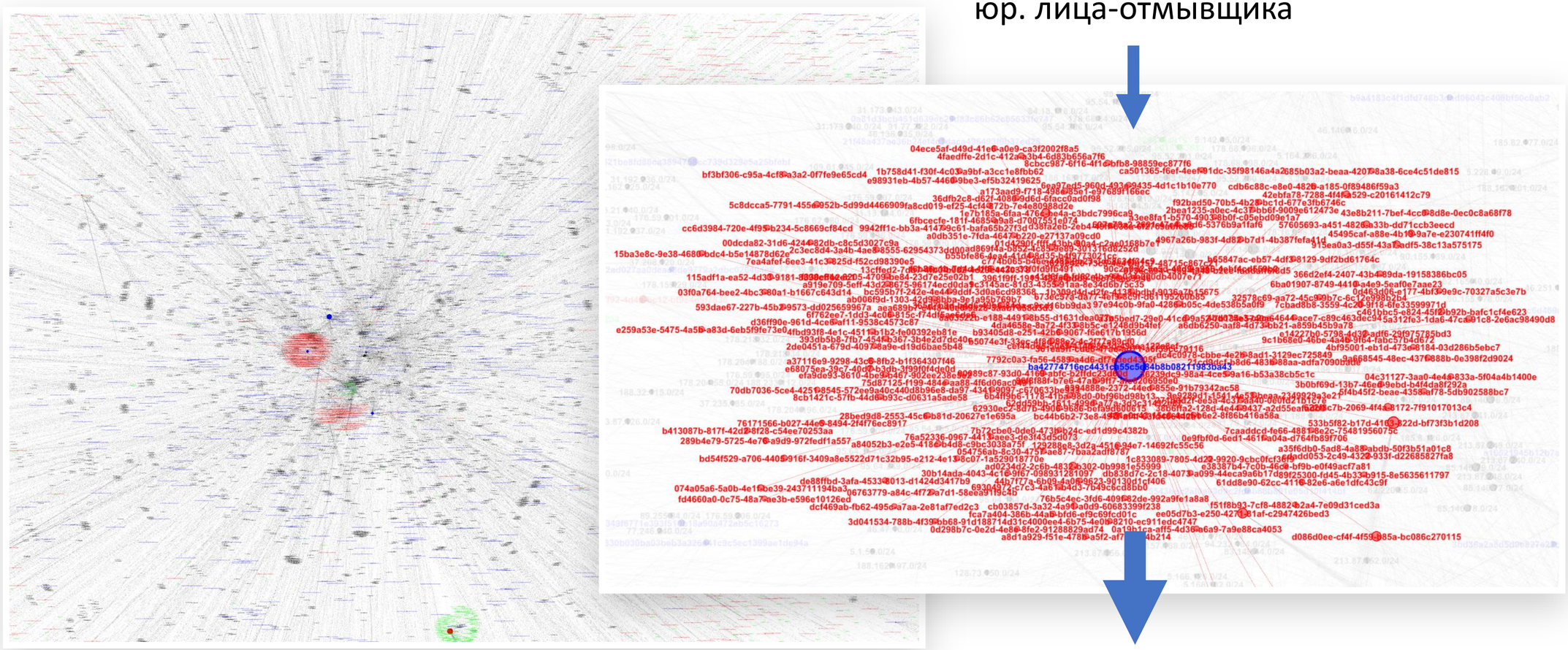
Уровень 3: кто делает? (UEBA)



Биометрическая технология	Equal Error Rate (EER)
Сканирование сетчатки	1:10 000 000
Сканирование радужки	1:131 000
По отпечатку	1:500
По геометрии ладони	1:500
По подписи	1:50
По голосу	1:50
По мышке (30 сек)	1:50
По мышке (60 сек)	1:100
По мышке (90 сек)	1:200

ПОД/ФТ (№18-МР от 21.07.2017 г.)

Граф связей устройств и учет. записей



Банк: идентификатор учет. записи
юр. лица-отмывщика

N учет. записей M юр. лиц,
«аффилированных» с исх. учет. записью

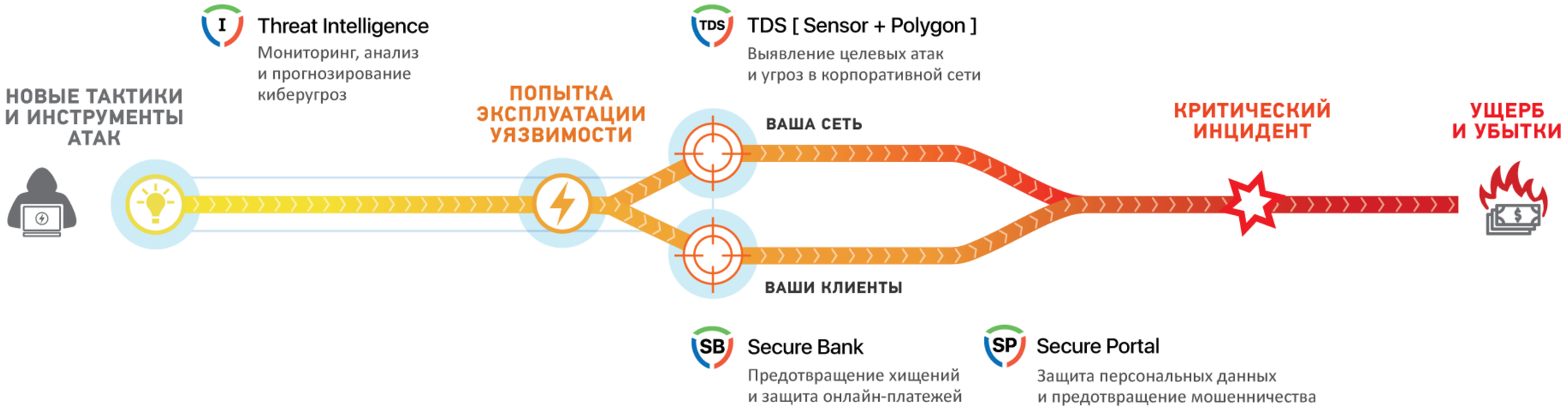
Что делать?

Мы даем вам самое важное — время для подготовки к инцидентам.

Система раннего предупреждения киберугроз Group-IB позволяет оперативно узнавать о новых угрозах и блокировать их появление на ваших рубежах обороны. Она основана на 14-летнем опыте нашей команды, глубоком анализе хакерских кампаний и актуальных разведданных из мира киберпреступности.

14 лет

опыта в сфере компьютерной криминалистики, консалтинга и аудита информ-безопасности



CyberCrimeCon — конференция о тенденциях развития киберпреступлений, технологиях проактивной защиты и реагирования на инциденты

Регистрация > 2017.group-ib.ru

Предотвращаем и расследуем киберпреступления с 2003 года.

www.group-ib.ru
group-ib.ru/blog
info@group-ib.ru
+7 495 984 33 64
twitter.com/groupib
facebook.com/group-ib
Крылов Павел
krylov@group-ib.ru