КИБЕРПРЕСТУПНОСТЬ В ЦИФРАХ И ТРЕНДАХ

Сергей Золотухин

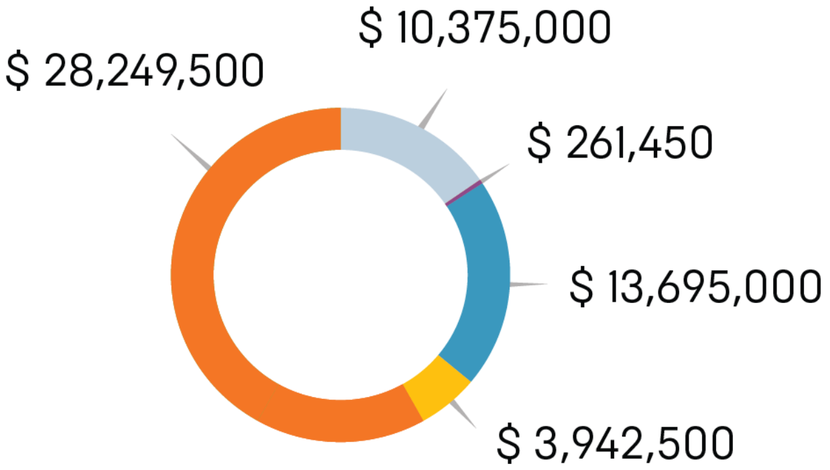
Менеджер по развитию бизнеса

Group-IB

Оценка рынка (Россия)

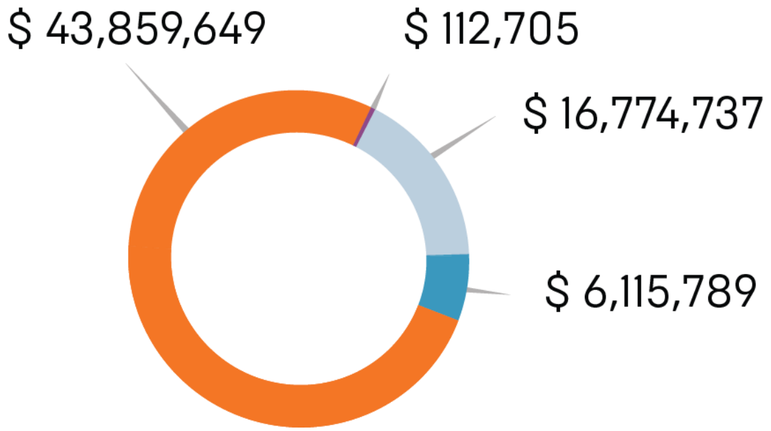
H2 2016 - H1 2017

$ 55,440,617

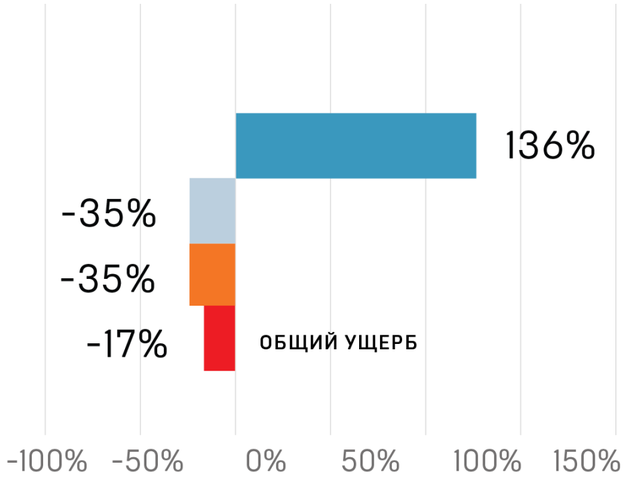


H2 2015 - H1 2016

$ 66,862,880



Изменения по отношению к предыдущему периоду



- ХИЩЕНИЯ В ИНТЕРНЕТ-БАНКИНГЕ У ФИЗИЧЕСКИХ ЛИЦ С ТРОЯНАМИ ДЛЯ ПК
- ХИЩЕНИЯ В ИНТЕРНЕТ-БАНКИНГЕ У ФИЗИЧЕСКИХ ЛИЦ С ANDROID ТРОЯНАМИ
- ХИЩЕНИЯ В ИНТЕРНЕТ-БАНКИНГЕ У ЮРИДИЧЕСКИХ ЛИЦ
- ЦЕЛЕВЫЕ АТАКИ НА БАНКИ
- ФИШИНГ
- ОБНАЛИЧИВАНИЕ ПОХИЩЕННЫХ СРЕДСТВ

ТРЕНД 1
Целевые атаки на банки – смена тактики

Опыт гос. хакеров

Стейджеры

Разведмодули

Взломы партнеров

Атаки на сотрудников банков

Более совершенные эксплойты и фишинг

Скрытые каналы

HTTPS

DNS

Легитимные инструменты

Меньше внимания SWIFT

Есть автозалив и под SWIFT, и под АРМ КБР

Единичные случаи успешных атак

Непубличные инциденты

Бестелесность

Легко обходить антивирусы

Работа только в оперативной памяти

Скрипты на PowerShell, VBS, PHP

Закрепление в системе через:
– Windows Management Instrumentation (WMI)
– Group Policy Objects (GPOs)
– Scheduled task

Карточный процессинг – основная цель

Менее защищен, чем SWIFT

Дешевая схема обнала

Снимается чистый кэш

Обналичивание в другой стране

Безопасность мулов

Связана с карточным процессингом

Обналичивание в другой стране

ТРЕНД 2
Диверсии – массовые атаки на инфраструктуру

При массовых атаках ущерб может быть колоссальным.

ФИНАНСОВО МОТИВИРОВАННЫЕ АТАКУЮЩИЕ

АТАКУЮЩИЕ, СПОНСИРУЕМЫЕ ГОСУДАРСТВАМИ

Массовые атаки, наносящие максимальный урон атакуемым компаниям

2017

Февраль

PetrWrap

Cobalt

Уничтожение следов атаки

Март

Filecoder.NHK

BlackEnergy

Точечные атаки, запуск шифрования «руками» с правами администраторов домена

Май

WannaCry

Lazarus

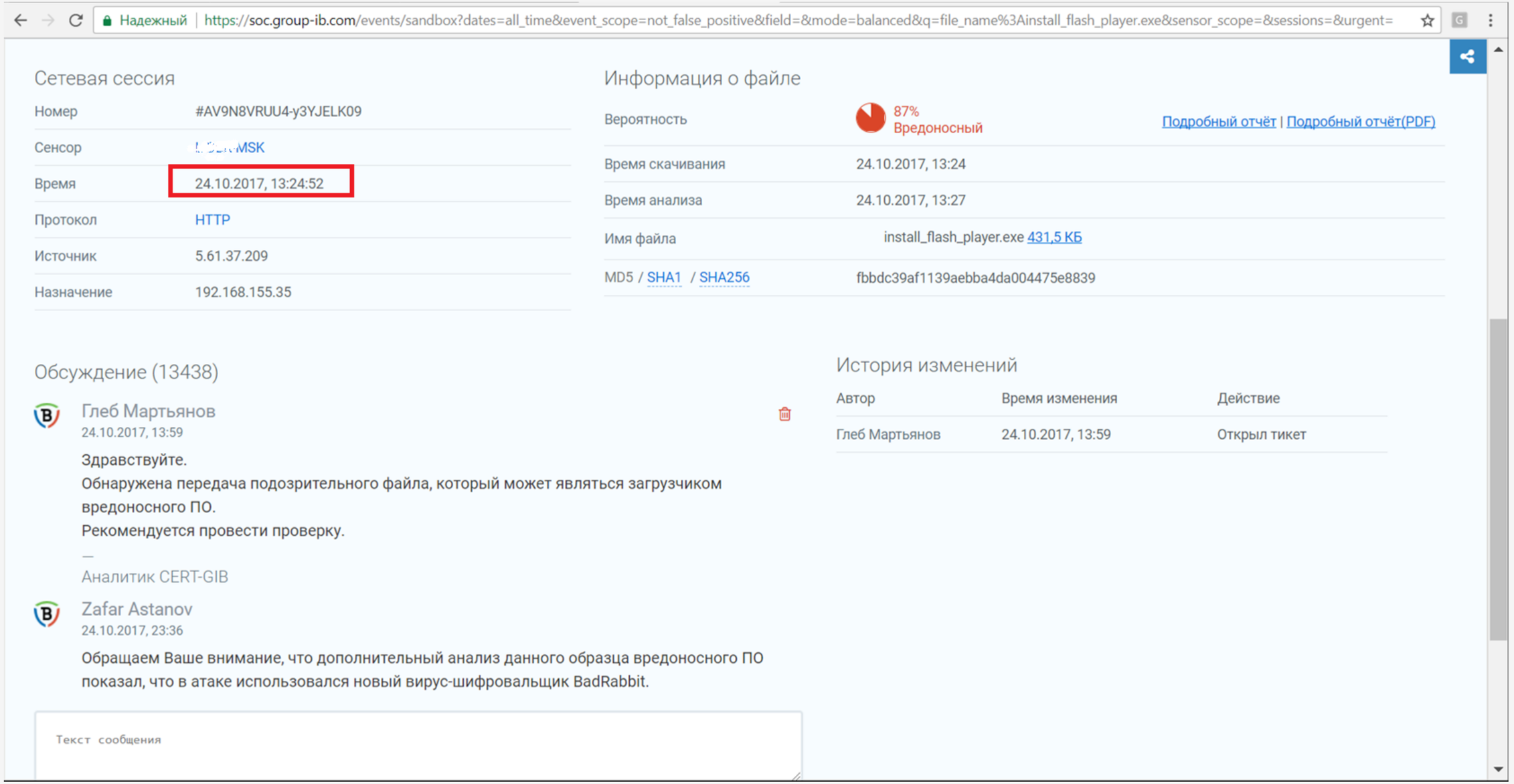
Июнь

NotPetya

BlackEnergy

Узнайте больше
group-ib.ru/blog

Октябрь 2017 #BadRabbit



#BadRabbit

GROUP-IB

Взломанный интернет-ресурс

Pop-Up окно с предложением обновить Flash Player

ДА

НЕТ

Скомпрометированные домены:

fontanka.ru
argumentiru.com
grupovo.bg
sinematurk.com
aica.co.jp
spbvoditel.ru
argumenti.ru
mediaport.ua
1dnscontrol.com
most-dnepr.info
osvitaportal.com.ua
otbrana.com
pensionhotel.cz
online812.ru
imer.ro
novayagazeta.spb.ru
i24.com.ua
an-crimea.ru
t.ks.ua

Вредоносный домен 1dnscontrol.com

Загрузка install_flash_player.exe

Извлечение и сохранение файла infpub.dat в директорию %WINDOWS%

- Mimikatz
  - %windows% \<4chars>.tmp
- Discoder driver
  - %windows% \cscc.dat
- MBR Encryptor
  - %windows% \discpi.exe

#BadRabbit

NOT PETYA

```
int result; // [esp+234h] [ebp-4h]@1

result = -1;
hSnapshot = CreateToolhelp32Snapshot(2u, 0);
if ( hSnapshot != (HANDLE)-1 )
{
  pe.dwSize = 556;
  if ( Process32FirstW(hSnapshot, &pe) )
  {
    do
    {
      hash = 0x12345678;
      counter = 0;
      len = wcslen(pe.szExeFile);
      do
      {
        curPos = 0;
        if ( len )
        {
          v3 = counter;
          do
          {
            v4 = (char *)&hash + (v3 & 3);
            v5 = (*v4 ^ LOBYTE(pe.szExeFile[curPos++])) - 1;
            ++v3;
            *v4 = v5;
          }
          while ( curPos < len );
        }
        ++counter;
      }
      while ( counter < 3 );
      if ( hash == 0x2E214844 )
      {
        result &= 0xFFFFFFF7;
      }
      else if ( hash == 0x6403527E || hash == 0x651B3805 )
      {
        result &= 0xFFFFFFFB;
      }
    }
    while ( Process32NextW(hSnapshot, &pe) );
  }
  CloseHandle(hSnapshot);
}
return result;
}
```

BAD RABBIT

```
int __stdcall GetHashFromUnicodeString(int str, unsigned int len)
{
  unsigned int counter; // edi@1
  unsigned int v3; // ecx@2
  unsigned int iter; // esi@3
  _BYTE *v5; // eax@4
  char v6; // dl@4
  int hash; // [esp+8h] [ebp-4h]@1

  hash = 0x87654321;
  counter = 0;
  do
  {
    v3 = 0;
    if ( len )
    {
      iter = counter;
      do
      {
        v5 = &hash + (iter & 3);
        v6 = (*v5 ^ *(str + 2 * v3++)) - 1;
        ++iter;
        *v5 = v6;
      }
      while ( v3 < len );
    }
    ++counter;
  }
  while ( counter < 3 );
  return hash;
}
```

```
signed int CheckProcessExistence()
{
  signed int result; // edi@1
  HANDLE processes; // esi@1
  BOOL i; // eax@2
  int hash; // eax@3
  PROCESSENTRY32W pe; // [esp+8h] [ebp-22Ch]@2

  result = -1;
  processes = CreateToolhelp32Snapshot(2u, 0);
  if ( processes != -1 )
  {
    pe.dwSize = 556;
    for ( i = Process32FirstW(processes, &pe); ; i = Process32NextW(processes, &pe) )
    {
      if ( !i )
      {
        CloseHandle(processes);
        return result;
      }
      hash = GetHashFromString(pe.szExeFile);
      if ( hash != 0x4A241C3E )
      {
        if ( hash == 0x923CA517 )
          goto LABEL_10;
        if ( hash != 0x966D0415 && hash != 0xAA331620 )
        {
          if ( hash == 0xC8F10976 )
            goto LABEL_10;
          if ( hash != 0xE2517A14 )
            break;
        }
      }
      result &= 0xFFFFFFEF;
LABEL_12:
      ;
    }
    if ( hash != 0xE5A05A80 )
      goto LABEL_12;
LABEL_10:
    result &= 0xFFFFFF8F;
    goto LABEL_12;
  }
  return result;
}
```

ТРЕНД 3
Заскриптованность – автоматизация любых атак

Заскриптованные шаги
– автоматизация, дающая мощный стимул к развитию средств нападения

NotPetya
3 простых шага открывают ящик Пандоры

1. Запуск Mimikatz
2. Распространение с помощью штатных средств (WMI and PsEXEC)
3. Параллельно – попытка запуска EternalBlue

Вымогатели
WannaCry, NotPetya, Uiwix, EternalRocks

Банковские трояны
Ramnit, Emotet, Trickbot, Qbot

Майнеры
Adylkuzz

ТРЕНД 4
Энергетика – полигон для испытания кибероружия

2014

HAVEX

Этап разведки

Установлен более чем в 2 000 сетей

Havex не мог влиять на физические процессы

Через OPC анализировал, какое оборудование установлено в конкретной локации

2014

Black Energy 2

Этап разведки

Поиск уязвимостей в SCADA Human machine interfaces (HMI)

Установка трояна на серверы с HMI

2015

Black Energy 3

Блэкаут в Украине

Перегрузка сети в трех энергетических компаниях

Замена прошивок

Отключение источников бесперебойного питания

Вывод из строя Windows машин операторов, включая HMI

2016

Idustroyer

Тестирование в Украине

Контроль OPC

Вызов перегрузки сети

Модули для работы с протоколами IEC 60870-5-101, IEC 60870-5-104, IEC 61850

Эти протоколы используются для удаленного управления Remote Terminal Unit (RTU)

DoS модуль для распределительного устройства высокого напряжения Siemens SIPROTEC

ТРЕНД 5
Android трояны – основная угроза для клиентов банков

Все новые банковские Android трояны созданы русскоговорящими разработчиками

Схемы хищений

- Хищение через SMS банкинг
- Переводы с карты на карту
- Переводы через интернет-банкинг
- Перехват доступа к мобильному банкингу
- Поддельный мобильный банкинг
- Покупки с помощью Apple Pay

Тотальная автоматизация

Либо полностью автоматизированное хищение, либо хищение «одной кнопкой»

Трояны под SMS банкинг (только в России)	Трояны с веб-фейками (Россия)	Трояны с веб-фейками (мир)
Agent.SX	Limebot	Maza-in
Flexnet	Honli	Alien-bot
Agent.BID	Asucub	Catelites Android Bot
Granzy	Agent.BID	Instant VBV Grabber
Cron	ApiMaps	Easy
Fakeinst.FB	Cron	UfoBot
Opfake.A	Tiny.z	Rello
		Loki
		Red Alert
		Vasya Bot
		ExoBot
		Reich
		Marcher
		Skunk
		Abrvall
		Xbot
		GMbot
		Spy.agent.SI

ТРЕНД 6
Криптоиндустрия – новый стимул для киберпреступников

Июнь 2016

THE DAO

Эксплуатация уязвимости в смарт-контракте

– $60 миллионов

Июль

Parity
Etherium кошелек

Эксплуатация уязвимости в коде

– $30 миллионов

Авг.

Bitfinex
Гонконгская биржа

– $72 миллиона

Окт.

Blockchain.info
Bitcoin кошелек

Перехват домена

Нояб.

Bitcurex
Польская биржа

– $1,5 миллиона, закрылась вскоре после инцидента

2017

Апр.

Yapizon
Южнокорейская биржа

– $5,3 миллиона

Июнь

Bithumb
Южнокорейская биржа

Предположительно, взлом персонального компьютера сотрудника

– "миллиарды вон"

Classic Ether Wallet

Перехват домена с помощью социальной инженерии

Банковские ПК и Android трояны

перепрофилируются для атак на пользователей криптовалют
– TrickBot, Vawtrak, Qadars, Triba, Marcher

Фишинг

– направленный на клиентов
Средний доход одной группы в месяц – более $1,5 миллионов

– направленный на сотрудников
Резко участились случаи атак

Целевые атаки

Атаки на биржи как киберпреступниками, так и проправительственными хакерами

ТРЕНД 7
Фишинг – самая массовая угроза с минимальным ущербом

80%

фишинга приходится
на следующие категории

- финансовые сервисы
- облачные хранилища
- почтовые сервисы

10 - 15%

посетителей финансовых
фишинговых сайтов
вводят на них свои данные

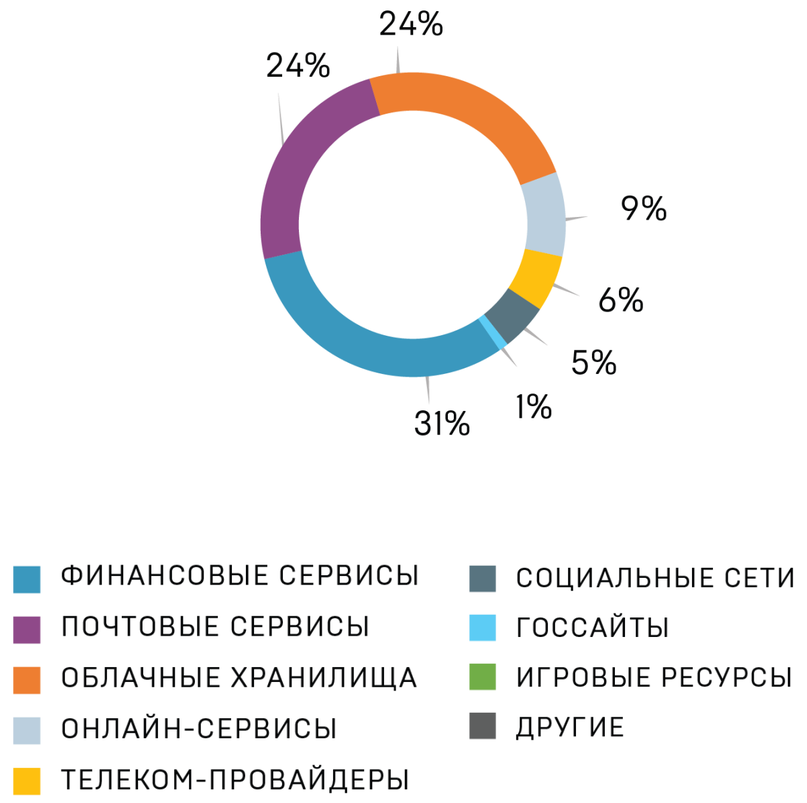
3 : 1

соотношение количества жертв
фишинга к количеству жертв
банковских ПК и Android троянов

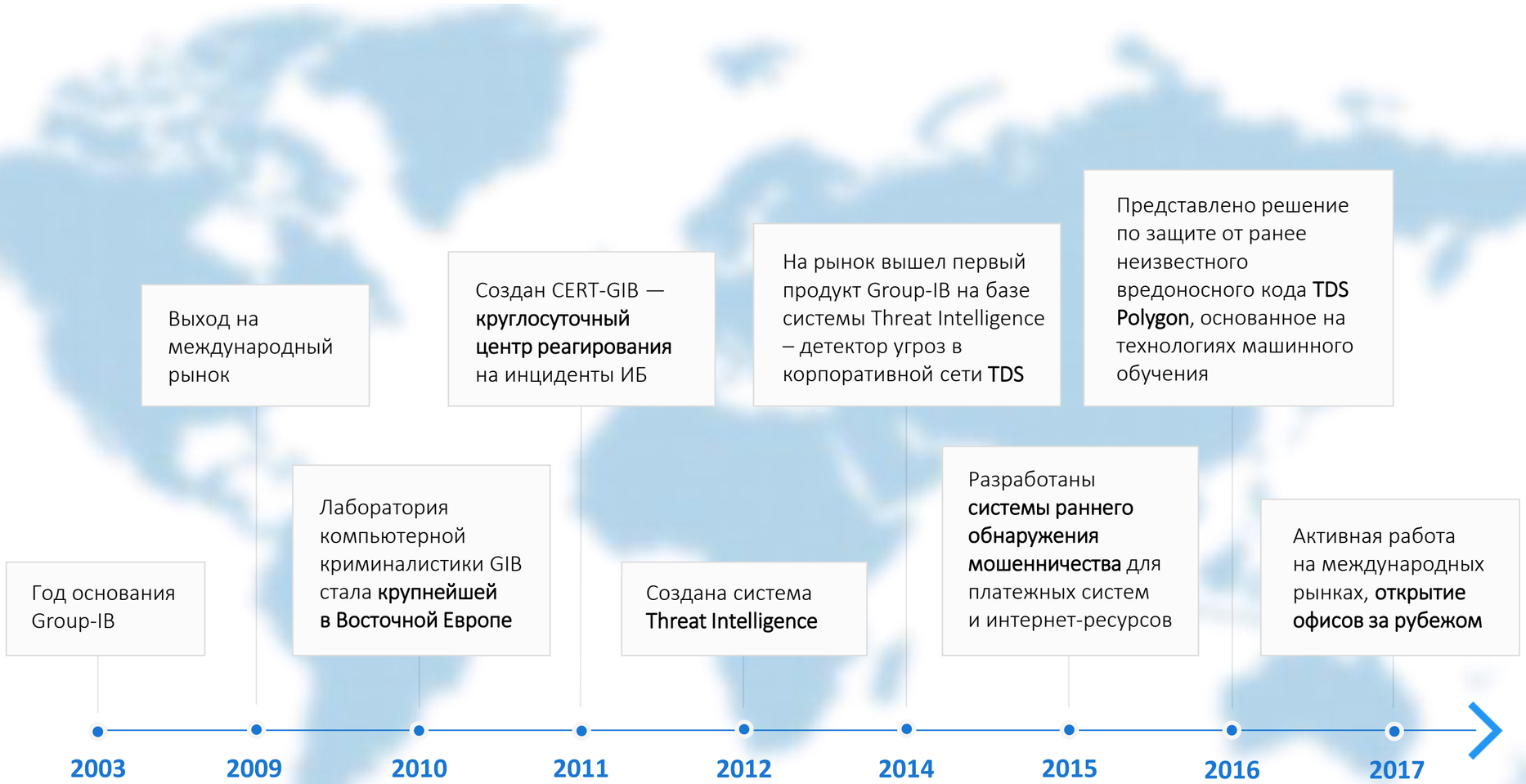
Адреса для сбора логинов и паролей

gmail.com	80%
yahoo.com	6%
yandex.com	5%
hotmail.com	3%
outlook.com	1%
mail.com	1%
aol.com	1%
mail.ru	1%
other	3%

Фишинговые сайты по категориям



История компании



Многолетний опыт Group-IB воплощен в системе раннего обнаружения киберугроз — линейке высокотехнологичных продуктов, основанной на самых актуальных данных и глубоком анализе реальных хакерских атак.

160+
сотрудников

40%
разработчиков

27
средний возраст

45 000
часов реагирования

Уникальная ресурсная база

Уникальная ресурсная база, накопленная за 14 лет работы

Мы создали высокотехнологичную инфраструктуру для мониторинга хакерской активности, слежения за ботсетями и извлечения данных, необходимых для предотвращения инцидентов. **90% данных поступает в систему из закрытых источников**, абсолютное большинство из них – уникально. Мы мониторим закрытые площадки, следим за изменениями бот-сетей, извлекая конфигурационные файлы вредоносных программ и информацию об украденных идентификаторах.

1 ТЕХНОЛОГИЧЕСКАЯ ИНФРАСТРУКТУРА

- Распределенная сеть мониторинга и HoneyNet-ловушек
- Аналитика бот-сетей
- Трекеры сетевых атак
- Мониторинг хакерских форумов и закрытых сетевых сообществ
- Данные сенсоров TDS

2 HUMAN INTELLIGENCE

- Результаты криминалистических экспертиз Лаборатории Group-IB
- Материалы расследований
- Мониторинг и анализ вредоного ПО
- База обращений и практика реагирования на инциденты CERT-GIB
- Результаты аудита
- Целевая аналитика Group-IB

3 ОБМЕН ДАННЫМИ

- Команды реагирования CERT
- Регистраторы и хостинг-провайдеры
- Производители средств защиты
- Организации и объединения по противодействию киберугрозам
- Europol, Interpol и правоохранительные органы

Системы раннего предупреждения киберугроз

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.

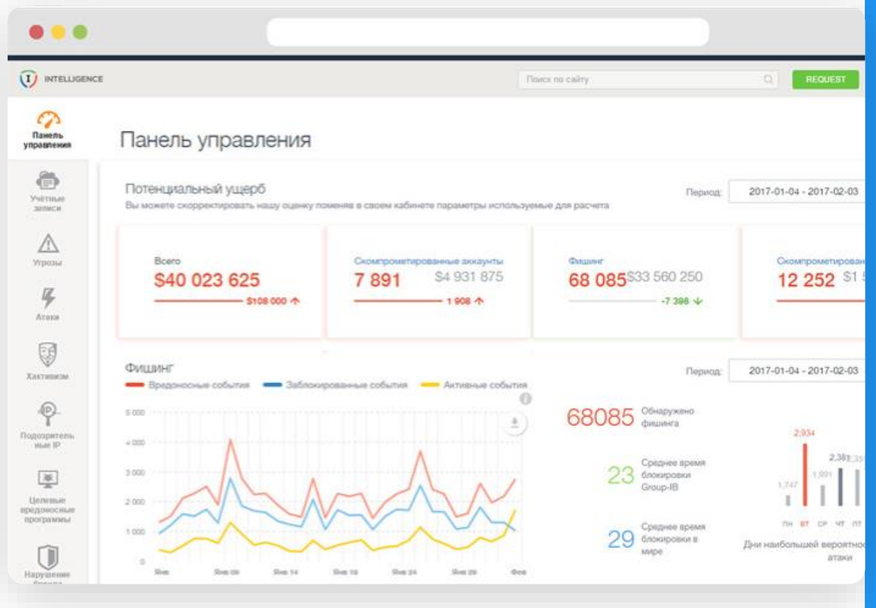
14 лет

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

Intelligence

Кибербразведка по подписке: мониторинг, анализ и прогнозирование угроз для компании, клиентов и партнеров

- Стратегическая информация для взвешенной оценки рисков и приоритизации угроз
- Оперативные данные для подготовки к атакам и настройки систем защиты
- Тактические индикаторы, минимизирующие время реагирования на инцидент



Gartner®

В 2015 году исследовательская компания Gartner включила Group-IB в число 7 лучших поставщиков threat intelligence в мире

«Базируясь в Восточной Европе, Group-IB лучше понимает угрозы, рождающиеся в регионе, и глубже внедрена в локальные хакерские сообщества. Участие в расследовании особо важных высокотехнологичных преступлений позволяет Group-IB получать эксклюзивную информацию о киберпреступниках, их взаимосвязях и другие разведданные».

Competitive Landscape: Threat Intelligence Services, Worldwide, 2015

GROUP-IB

- Оперативные уведомления об атаках и угрозах
- Наглядный веб-интерфейс
- Разбор инструментов и тактик атак, профайлы преступных групп
- Прямой доступ к скомпрометированным идентификаторам
- API для интеграции с SIEM, IPS, Firewall, Antiphraud
- Круглосуточная поддержка

Результаты использования Threat Intelligence

Аналитики и Incident Response команды

- Качественная приоритизация инцидентов на основании данных Threat Intelligence
- Ускорение процессов Incident Response
- Погружение в детализированный контекст угроз, знание тактик и инструментов преступных групп, потенциально интересующихся компанией

CEO и топ-менеджмент

- Максимизация ROI от инвестиций в системы безопасности, Incident Response команды и аналитиков
- Получение информации об угрозах, влияющей на принятие управленческих решений
- Предотвращение использования бренда компании в преступных целях, снижение репутационных рисков

CISO

- Построение стратегии ИБ на основании глубокого понимания эволюции киберугроз и анализе реальных атак в вашем секторе
- Взвешенный выбор технологических решений для защиты от актуальных угроз
- Увеличение эффективности и возможностей аналитиков и Incident Response команд

MSSP

- Предоставление клиентам сервиса, основанного на глубоком понимании контекста угроз
- Более качественное таргетирование предложений для клиентов исходя из данных об актуальных для них угрозах
- Прогнозирование развития угроз и средств противодействия им на основании глобальных данных threat intelligence

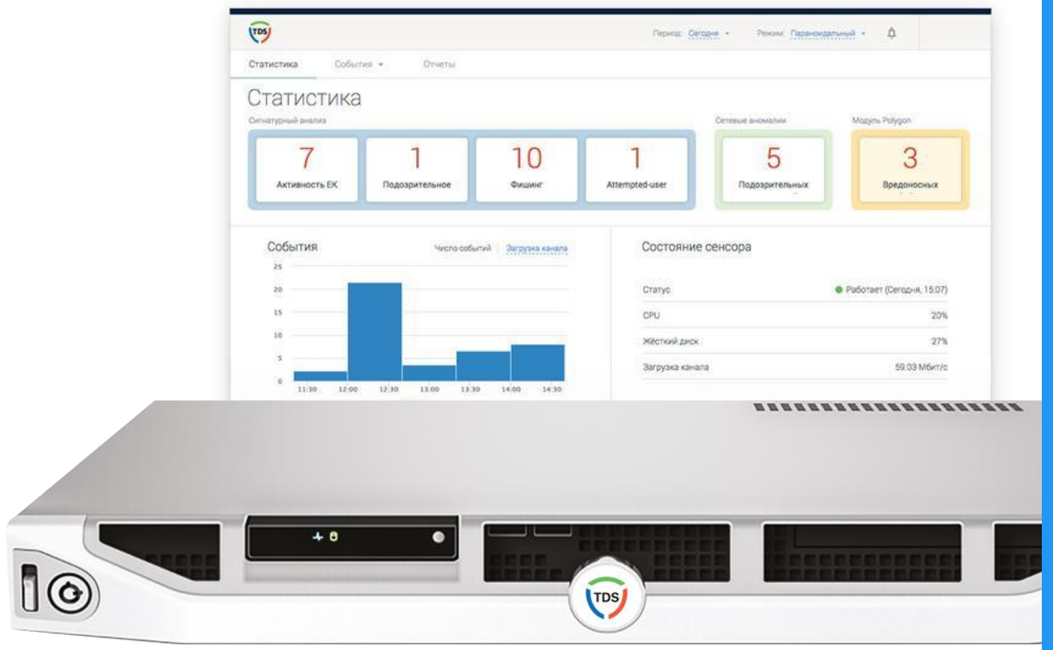
Threat Intelligence от Group-IB позволит вам:

- ✓ Сократить время реакции на инциденты до минимума
- ✓ Отслеживать появление новых инструментов и методов атак
- ✓ Получать персонализированные данные с закрытых хакерских площадок
- ✓ Оценивать эффективность выбранной стратегии инвестиций в информационную безопасность компании

TDS Sensor

TDS — обнаружение целевых атак

Выявляйте зараженные узлы.
Предотвращайте проникновения,
утечки, целевые атаки
и промышленный шпионаж



Благодаря глубокому понимаю специфики целевых атак и активности преступных групп в разных регионах мира мы выявляем угрозы, незаметные другим, в том числе:

- нежелательное и опасное сетевое взаимодействие
- опасные передаваемые объекты
- шпионское ПО
- средства удаленного управления
- попытки использования уязвимостей

Уникальные источники и авторские наработки для высокоточного выявления угроз:

1. Алгоритмы поведенческого анализа + машинное обучение
2. Сведения об атаках из Лаборатории компьютерной криминалистики
3. Данные системы Threat Intelligence от Group-IB

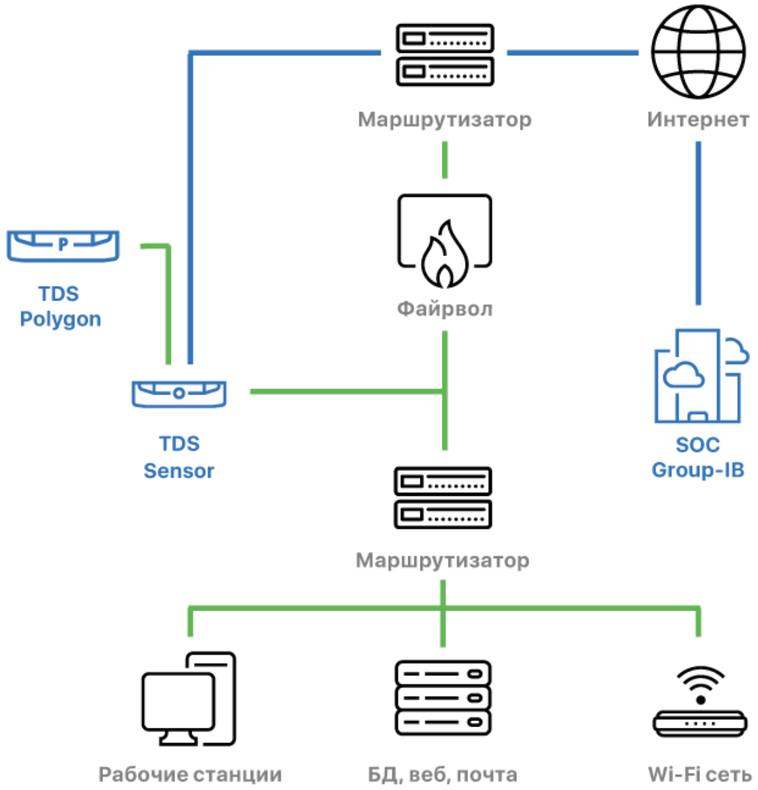
GROUP-IB

- Мгновенные уведомления о всех актуальных и ранее неизвестных семейств вредоносных программ
- Определение зараженных мобильных устройств в Wi-Fi сетях
- Круглосуточная поддержка и консультации
- Удобный веб-интерфейс и наглядные отчеты
- Ручной анализ логов и выделение критически важных инцидентов
- Регулярно обновляемый классификатор

Как работает TDS

СЕНСОР АНАЛИЗА ТРАФИКА

- Выявляет зараженные узлы, устанавливая их взаимодействия с командными центрами по признакам вредоносной активности, разрабатываемым на основе данных из уникальных источников.
- Детектирует сетевые аномалии, генерируемые вредоносными программами, при помощи алгоритмов машинного обучения.
- Интегрируется с системой поведенческого анализа TDS Polygon для выявления ранее неизвестного вредоносного кода.
- Передаёт информацию о выявленных инцидентах в SOC Group-IB по безопасному каналу либо в любую внутреннюю корпоративную систему учета событий ИБ.



SOC GROUP-IB

- Сведения об инцидентах, полученные от сенсора, классифицируются и коррелируются в Центре обработки данных.
- События анализируются квалифицированными специалистами Group-IB вручную.
- Эксперты SOC уведомят ваших специалистов о критичных угрозах по телефону и e-mail, а все результаты анализа будут доступны в удобном web-интерфейсе.

Опытные специалисты Group-IB берут на себя работу по выявлению критичных инцидентов, позволяя вашей службе ИБ сосредоточиться на реагировании.

Детектор угроз в корпоративной в сети Polygon

Polygon запускает файлы, полученные от TDS, в безопасной изолированной среде внутри вашего контура безопасности, анализирует их поведение и выносит объективное заключение о степени опасности объекта

TDS Sensor + TDS Polygon

ФЕРМА ВИРТ. МАШИН

Вызывающие подозрение файлы запускаются в тестовой среде, настраиваемой исходя из специфики вашего бизнеса и региона

СИСТЕМНЫЙ МОНИТОР

Не раскрывая своего присутствия, Polygon отслеживает поведение вредоносных объектов на самом низком уровне

ОБНОВЛЯЕМЫЙ КЛАССИФИКАТОР

Опасность объекта определяется с помощью Machine Mind и получающего новую информацию с заданной регулярностью классификатора

Почтовые вложения
Вредоносные файлы, получаемые в результате применения социальной инженерии

Скачиваемые файлы
Объекты, скачиваемые пользователями и/или их компьютерами в фоновом режиме

Целевые атаки
Вредоносное ПО, нацеленное эксклюзивно на вашу инфраструктуру

и другие
ранее неизвестные вредоносные объекты, не определяемые антивирусами и сигнатурным подходом

Group-IB & AIG CyberEdge

Первый в России комбинированный продукт по защите и страхованию от киберпреступлений

В отдельных случаях киберпреступники используют не только вредоносное ПО, но и социальную инженерию, обман, подкуп сотрудников. Благодаря нашему сотрудничеству с AIG клиенты Group-IB защищены и от таких сложных атак.

ЧТО ВХОДИТ В СТРАХОВОЕ ПОКРЫТИЕ

- Убытки в связи с нарушениями данных
- Административное расследование в отношении данных
- Расходы на реагирование при нарушении данных

Secure Bank

Система раннего обнаружения фрода для платежных систем, в режиме реального времени выявляющая мошеннические операции в личных кабинетах онлайн-банкинга еще на стадии подготовки.

Включена в реестр отечественного ПО

Наше решение:

- Предотвращает хищения за счет раннего детектирования мошенничеств
- Сокращает издержки на обработку ложных срабатываний и звонки клиентам
- Укрепляет вашу репутацию
- Повышает защищенность и привлекательность ваших систем онлайн-банкинга
- Укрепляет доверие к банку, давая возможность предупреждать клиентов о заражениях и атаках
- Сокращает количество инцидентов информационной безопасности

Secure Bank защищает «Сбербанк Онлайн»

- Установка на устройство клиента не требуется
- Выявляет мошеннические платежи и подготовку к их совершению
- Детектирует новые атаки и схемы мошенничества
- Ежедневное обновление правил и сигнатур
- API для интеграции с антифрод-системами
- Аналитическая поддержка и консультации

Secure Bank

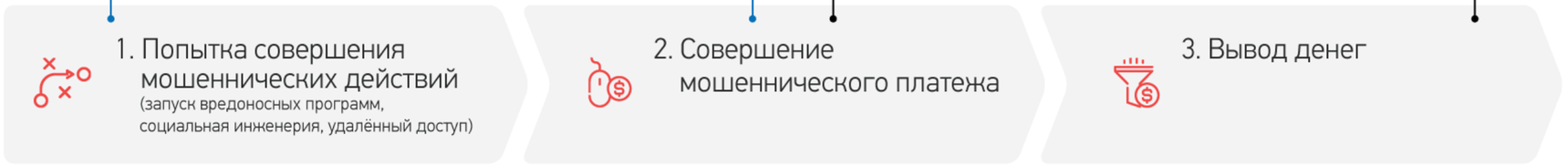
Загружаясь вместе с веб-страницами банка, Secure Bank дополняет антифрод-системы и помогает предотвратить хищение. Позволяет своевременно уведомить клиента о заражении или компрометации его устройства

Современные инструменты киберпреступников (удаленные подключения, веб-инжекты для «автозалива», трояны, позволяющие перехватывать SMS) делают традиционные средства защиты от фрода на стороне клиента неэффективными

Secure Bank использует расширенные средства обнаружения вредоносных программ и поведенческого анализа для выявления мошенничества до его возникновения

AF

Классические системы по противодействию мошенничеству анализируют транзакции, они не обнаруживают, заражено ли клиентское устройство вредоносным ПО, происходит ли что-то подозрительное на нём до совершения транзакции



Мошенничество может занять от нескольких секунд до нескольких месяцев

Готовая интеграция с инфраструктурой банка:

Система раннего предупреждения: Threat Intelligence TDS **Secure Bank** Secure Portal

Почему 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:

КИБЕРПРЕСТУПНОСТЬ В ЦИФРАХ И ТРЕНДАХ

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

Сергей Золотухин

Менеджер по развитию бизнеса