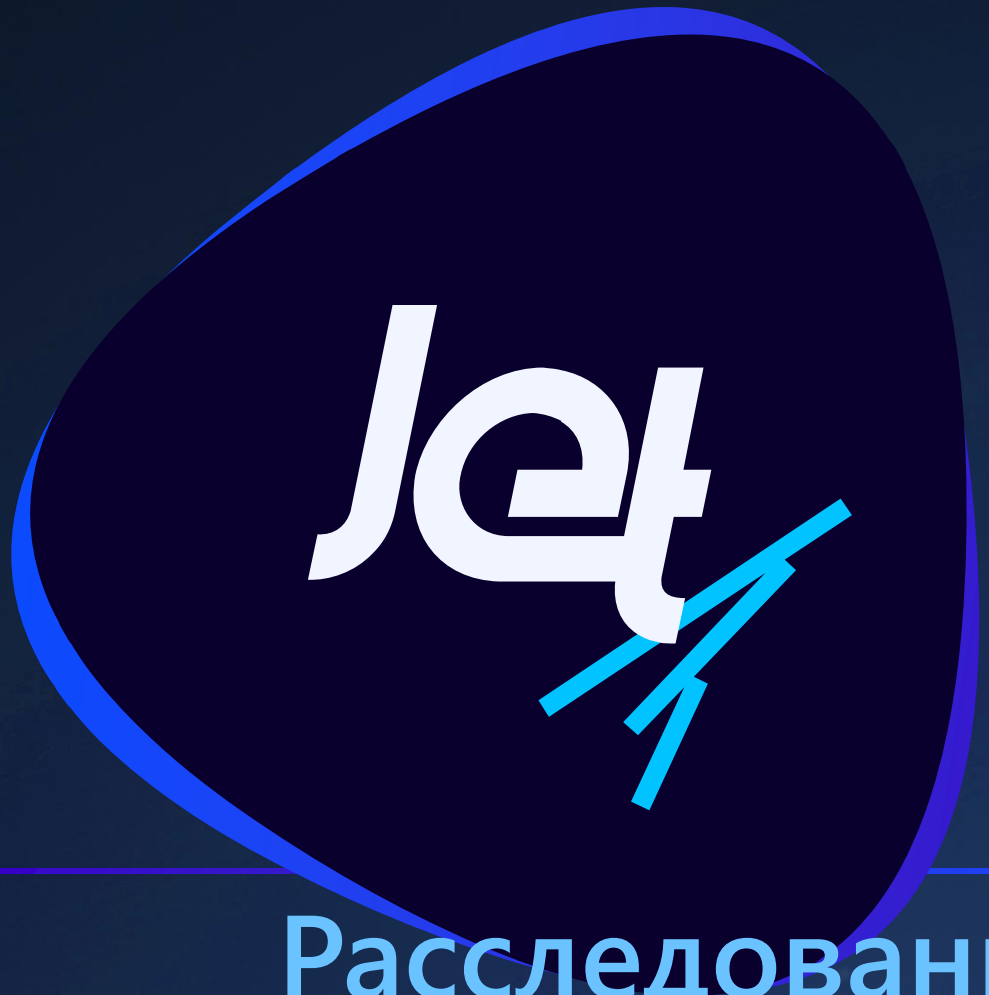


JET CONFERENCE

Расследования и криминалистика

Артёмов Артём
Ведущий специалист по компьютерной криминалистике
GROUP-IB

Какими бывают киберпреступления

СЕТЕВЫЕ АТАКИ

- Хищение в интернет-банкинге
- DDOS-атаки
- Взлом ip-телефонии
- Несанкционированный доступ (веб-сайт / бд / сервер / почта)
- Сетевой шантаж / вымогательство

ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ

- Мошенничество с использованием высоких технологий
- Вымогательство,
- Разглашение коммерческой тайны и конфиденциальной информации
- Незаконное использование товарного знака и бренда

ЦЕЛЕВЫЕ АТАКИ / ПРОМ ШПИОНАЖ

- Целевые вирусные атаки
- «Прослушка» сетевых каналов связи
- Установка программных закладок
- Организация цифровых «черных входов»

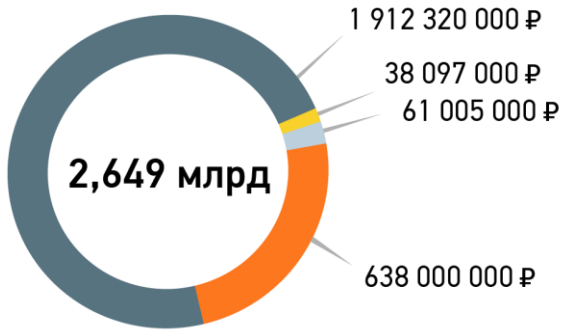
САБОТАЖ И ИНСАЙД

- Утечки информации
- Уничтожение информации
- Манипуляция данными с целью мошенничества
- Блокирование доступа

JET CONFERENCE

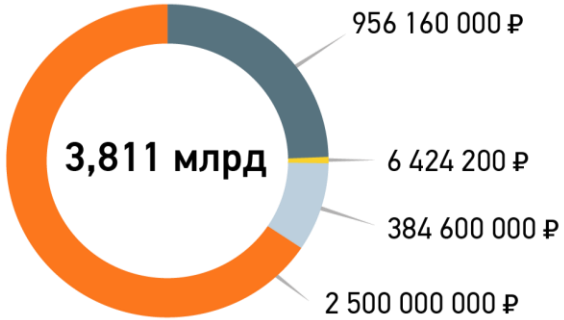
Оценка российского рынка хищений основной драйвер роста – целевые атаки

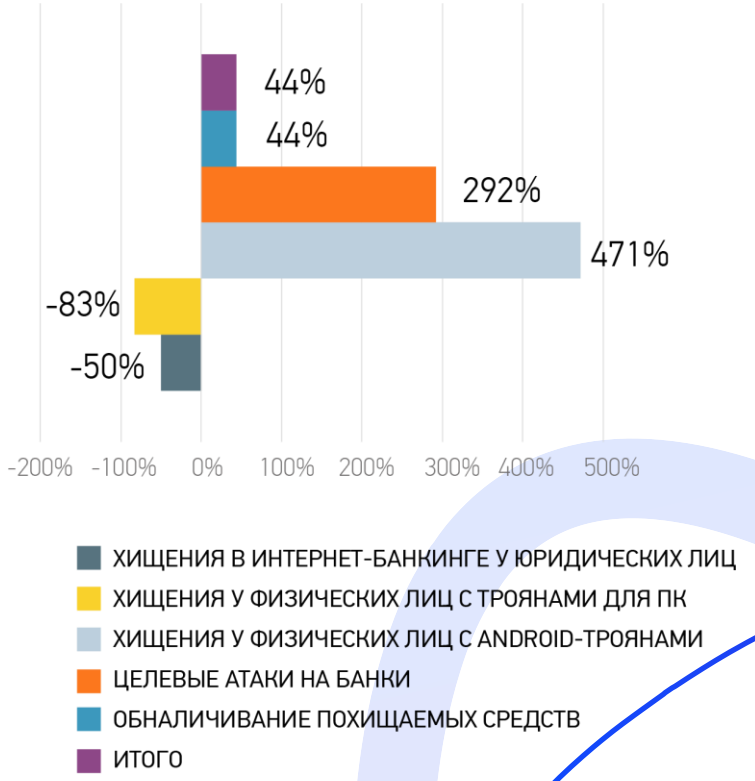
Q2 2014 - Q1 2015



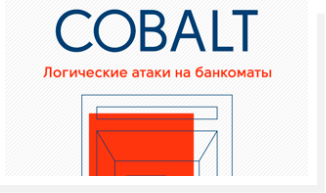
Изменение по отношению к предыдущему периоду

Q2 2015 - Q1 2016





Тренд №1 - те, кто атаковал клиентов, теперь атакует банки

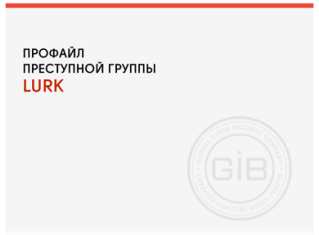


COBALT

Банкоматы и SWIFT

BUHTRAP

АРМ КБР



LURK

АРМ КБР

CORKOW

Карточный процессинг, банкоматы, биржевые терминалы

ANUNAK

АРМ КБР, SWIFT, банкоматы, платежные шлюзы, процессинг

www.group-ib.ru/media/category/analitycs/

JET CONFERENCE

Наборы утилит для целевых атак
Легальные утилиты

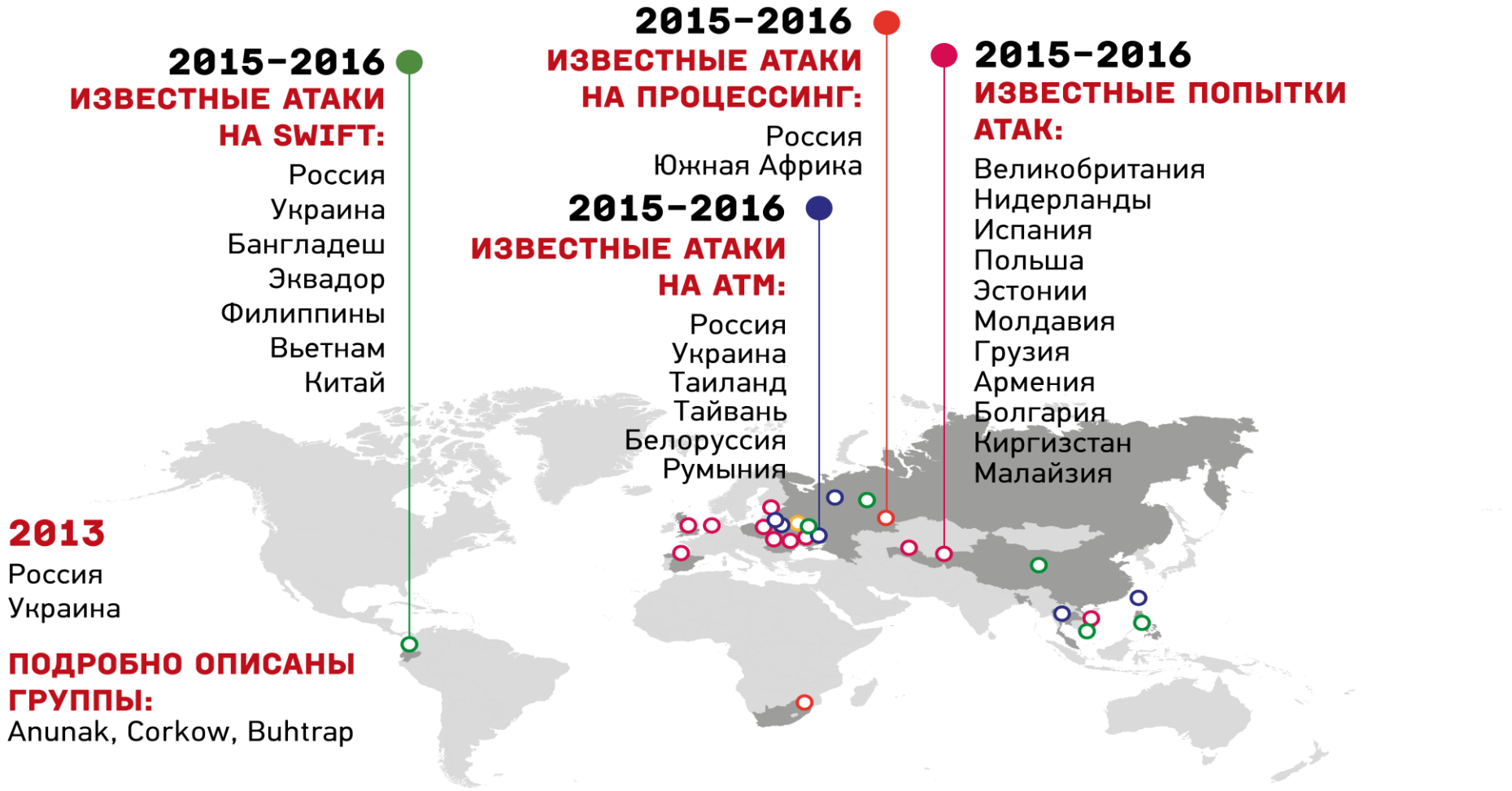
1) Удаленное управление
Ammyy Admin, Team Viewer, Lite Manager, RMS – Легальное ПО

2) Кража паролей
Mimikatz, Nirsoft, (group.xml sysvol)

3) Использование Meterpreter
SSL over DNS
HTTPS
SSH

4) Networks Worm
Admin share, built in mimikatz

Тренд №2 глобальность целевых атак



JET CONFERENCE

Пример расследования

Братья-близнецы

ФИНАНСЫ 02.06.2015, 10:01

Братья-близнецы украли со счетов российских банков более 11 млн руб.

Екатерина Метелица

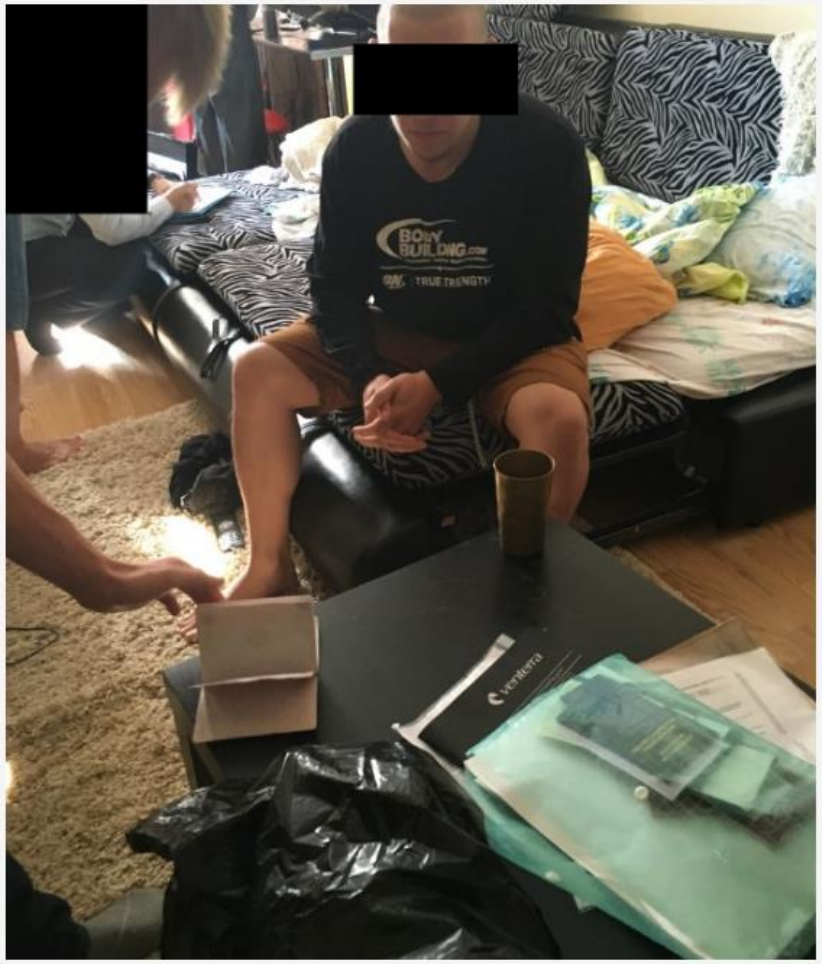
Полиция задержала хакеров, которые украли с банковских счетов более 11 млн руб. Жертвами киберпреступников стали клиенты крупных банков, включая Сбербанк и ВТБ24

Фото: AP

20 мая правоохранительные органы задержали киберпреступников, которые на протяжении почти четырех лет похищали с банковских счетов клиентские деньги, говорится в сообщении Group-IB (есть у РБК). Расследование преступлений и задержание происходили при содействии Group-IB и службы безопасности Сбербанка России.

Организаторами хакерских атак на банковские счета оказались два брата-близнеца из Санкт-Петербурга. Они уже были осуждены за подобные деяния и на момент совершения преступлений уже имели условный и испытательный сроки. Преступники

Задержание CRON



Пример расследования инсайдерской атаки

1. Система DLP компании фиксирует копирование чувствительной информации на которую распространяется режим КТ

2. Специалисты Group-IB выезжают на место и фиксируют цифровые доказательства, после чего проводят исследование накопителей информации и составляют отчёт

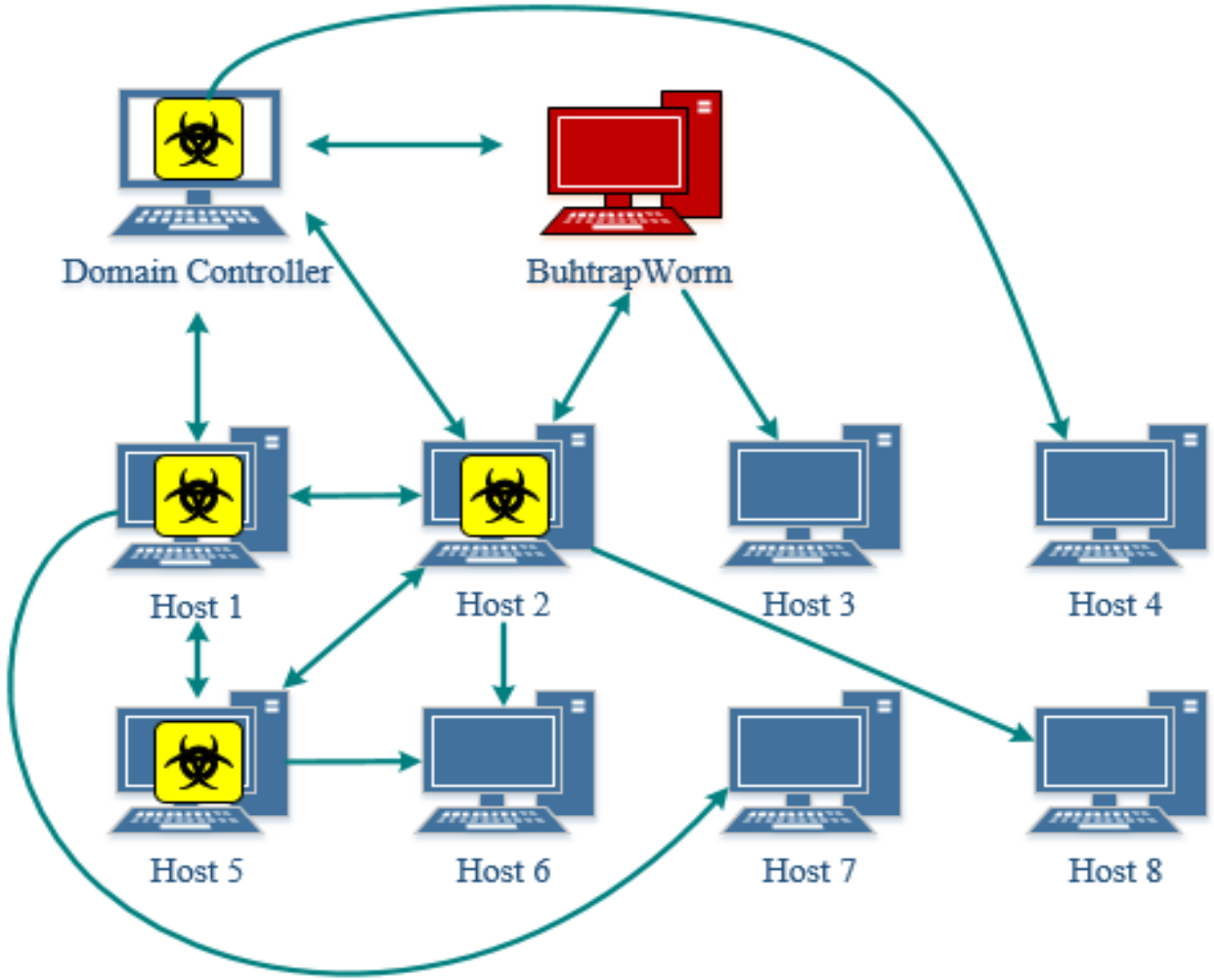
3. На основе заключения специалиста возбуждается уголовное дело. Сотрудник компании осужден

LAZARUS

- **knf.gov.pl** — Комиссия по финансовому надзору, Польша
- **cnvb.gob.mx** — Национальная банковская и фондовая комиссия Мексики
- **brou.com.uy** — Банк Восточной Республики Уругвай

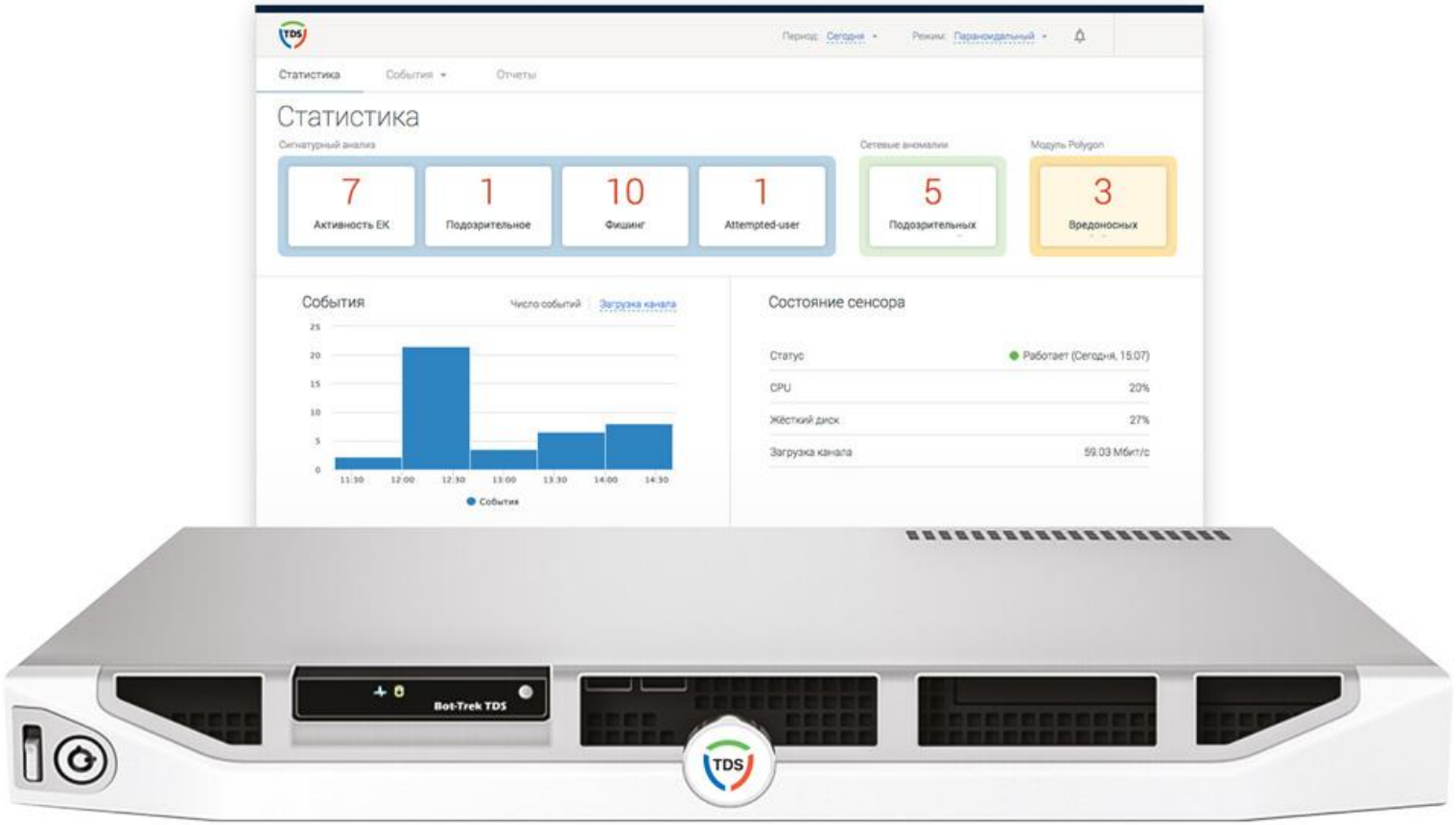
Трехуровневая структура командных серверов.

Something fileless



More fileless

TDS для обнаружение целевых атак
Система раннего предупреждения киберугроз



+ TDS POLYGON

SENSOR TDS

+ SOC GROUP-IB

JET CONFERENCE

JET CONFERENCE

01/06/2017

ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!