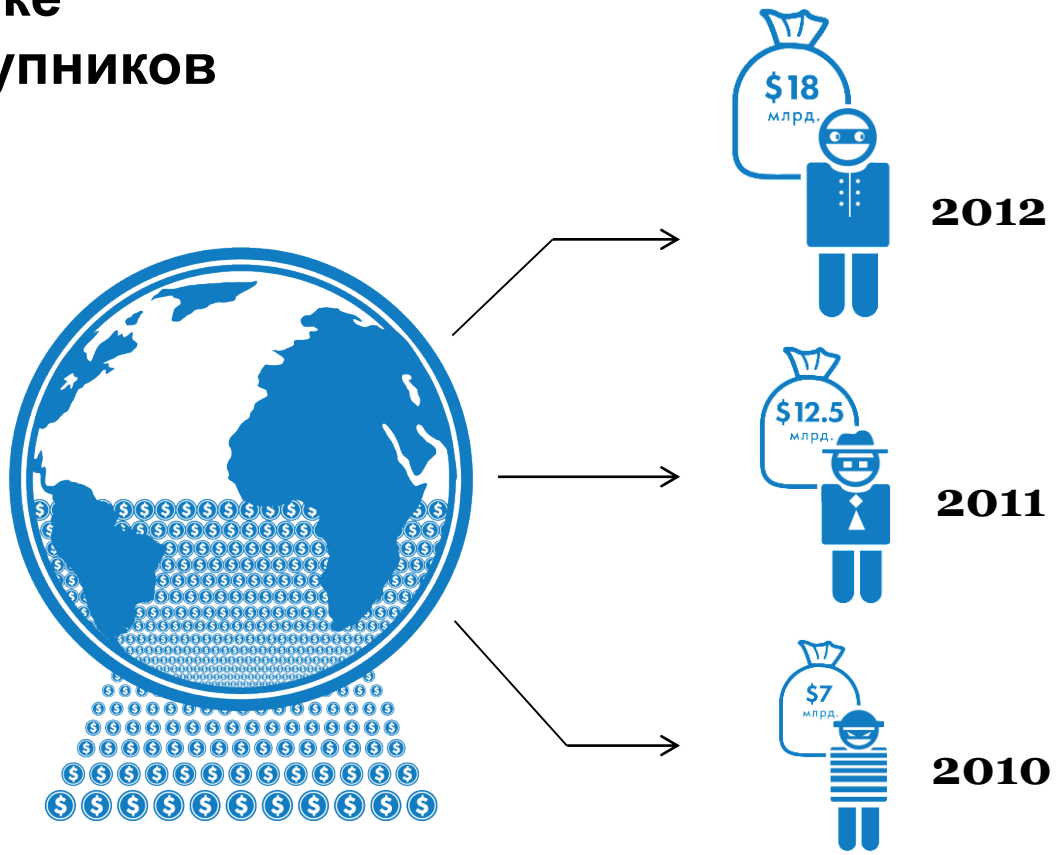
Записки о безопасности технологических процессов в РФ

Ущерб мировой экономике от действий киберпреступников

→ КЛАССИЧЕСКИЕ СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЖЕ ДАВНО НЕ СПОСОБНЫ ПРЕДОВТРАЩАТЬ ИНЦИДЕНТЫ



Group-IB

→ ОДНА ИЗ ВЕДУЩИХ МЕЖДУНАРОДНЫХ КОМПАНИЙ ПО ПРЕДОТВРАЩЕНИЮ И РАССЛЕДОВАНИЮ КИБЕРПРЕСТУПЛЕНИЙ И ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ

Основные направления деятельности:

1

→ Мониторинг и предотвращение киберугроз

2

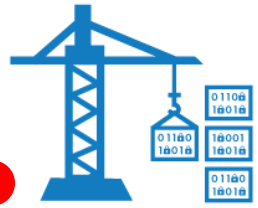
→ Расследование киберпреступлений и хищений, совершенных с использованием высоких технологий

3

→ Компьютерная криминалистика и экспертиза

4

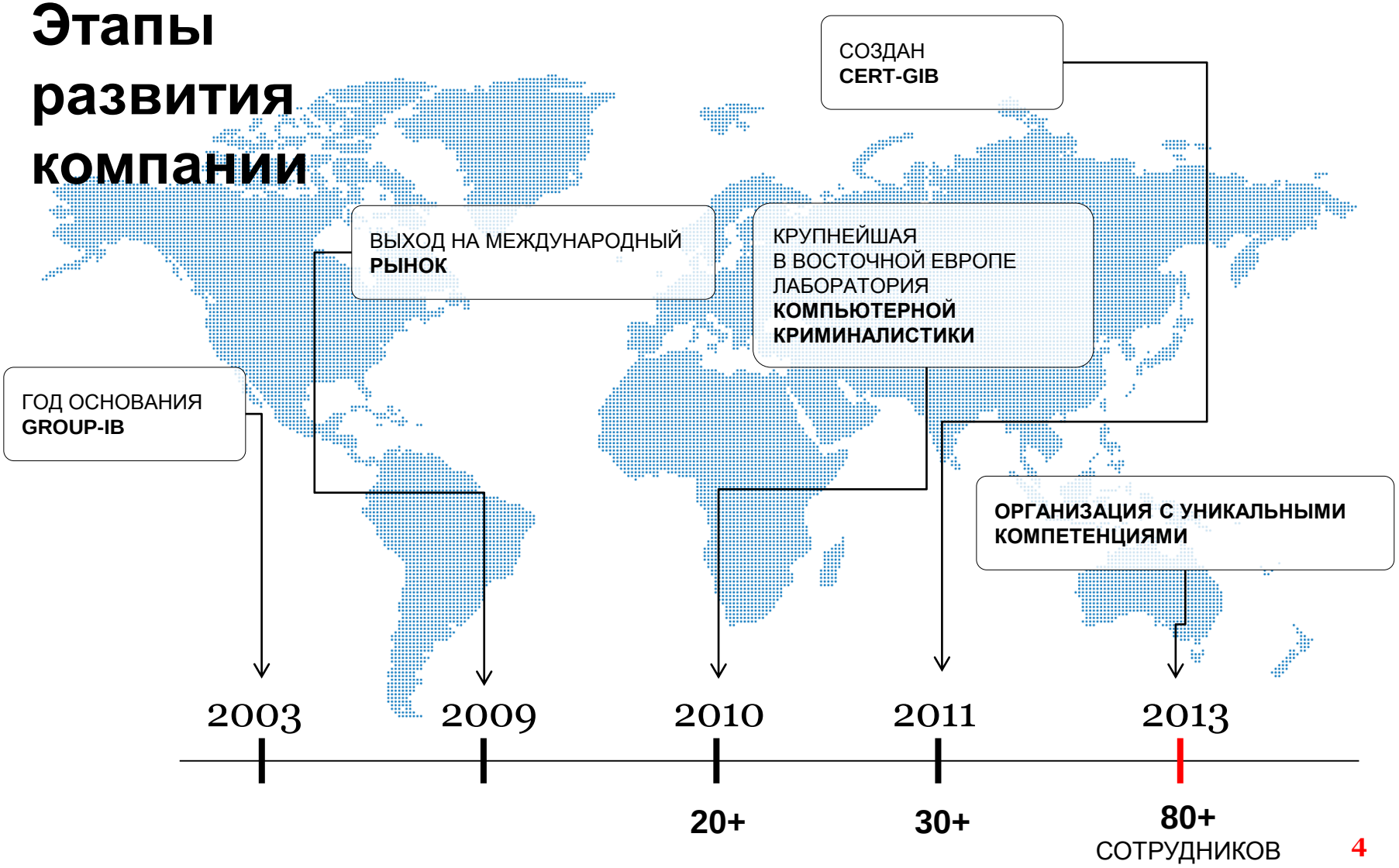
→ Аудит информационной безопасности и анализ защищенности



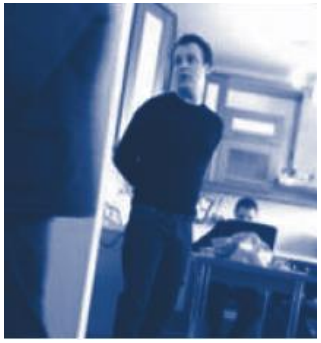
5

→ Разработка инновационных продуктов в области информационной безопасности

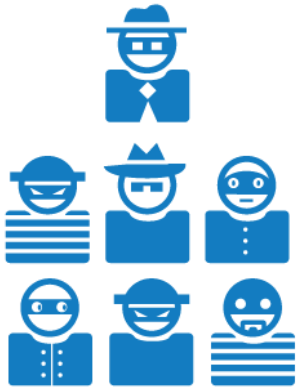
Этапы развития компании



Примеры расследований: Группа Carberp



1



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

2

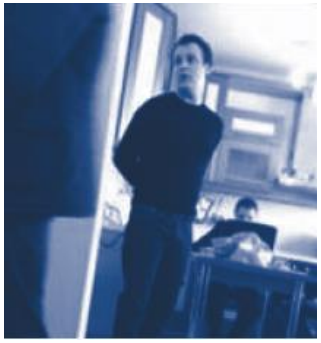
→ **Расследование проведено** в тесном сотрудничестве с ФСБ и МВД России при содействии Сбербанка России

3

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

Примеры расследований:
Группа Carberp

$250 000 000



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

Примеры расследований: Группа Hodprot

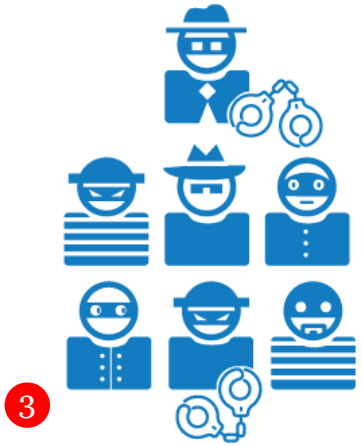
1

→ **Одна из старейших групп,** занимающихся хищениями в интернет-банкинге

2

→ **Мероприятия проводились** в нескольких регионах России и СНГ

3



→ **Результат расследования –** задержана преступная группа из 7 человек

Примеры расследований: Группа Hodprot

2 000 000 р.

1

→ **Одна из старейших групп,** занимающихся хищениями в интернет-банкинге

2

→ **Мероприятия проводились** в нескольких регионах России и СНГ

3

→ **Результат расследования –** задержана преступная группа из 7 человек

Примеры расследований: Группа Hodprot

1

→ **Одна из старейших групп,** занимающихся хищениями в интернет-банкинге

2

→ **Мероприятия проводились** в нескольких регионах России и СНГ

3

→ **Результат расследования –** задержана преступная группа из 7 человек

Примеры расследований: Группа Hodprot

В месяц!

1

→ **Одна из старейших групп,** занимающихся хищениями в интернет-банкинге

2

→ **Мероприятия проводились** в нескольких регионах России и СНГ

3

→ **Результат расследования –** задержана преступная группа из 7 человек

Вирус граббер (Платформа NCR)

1. Загрузка при доступе в банкомат. Модификация ПО банкомата (добавление функции в исполняемый файл в автозагрузке).
2. Запись тела вируса в библиотеку, в скрытый поток NTFS (ApplicationCore.exe:netncr.dll)
3. Перехват треков и пинов и запись их в зашифрованном виде в скрытый поток NTFS (autosave:descriptor).
4. Копирование данных на чип определенной карты, удаление вируса и следов работы после чтения определенной карты.

Вирус диспенсер (Платформа NCR)

1. Копирование исполняемого файла с загрузочного компакт диска. Добавление ярлыка в автозагрузку.

2. Внедрение в служебные процессы ПО банкомата.

3. Возможность вывода интерфейса по выбору кассеты и выдачи из нее купюр через диспенсер.

```
CASH OPERATION PERMITTED.

TO START DISPENSE OPERATION -

ENTER CASSETTE NUMBER AND PRESS ENTER
```

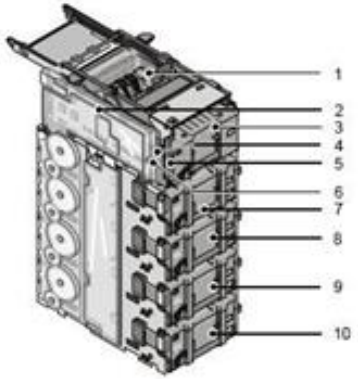
4. Отключение локальной сети и возможности самоудаления, «McAfee Solidcore for APTRA».

Подмена кассет (Платформа Wincor)

1. Загрузка при удаленном или физическом доступе в банкомат. Модификация ключей реестра.

HKEY_LOCAL_MACHINE\SOFTWARE\Wincor Nixdorf\ProTopas\CurrentVersion\LYNXPAR\CASH_DISPENSER\

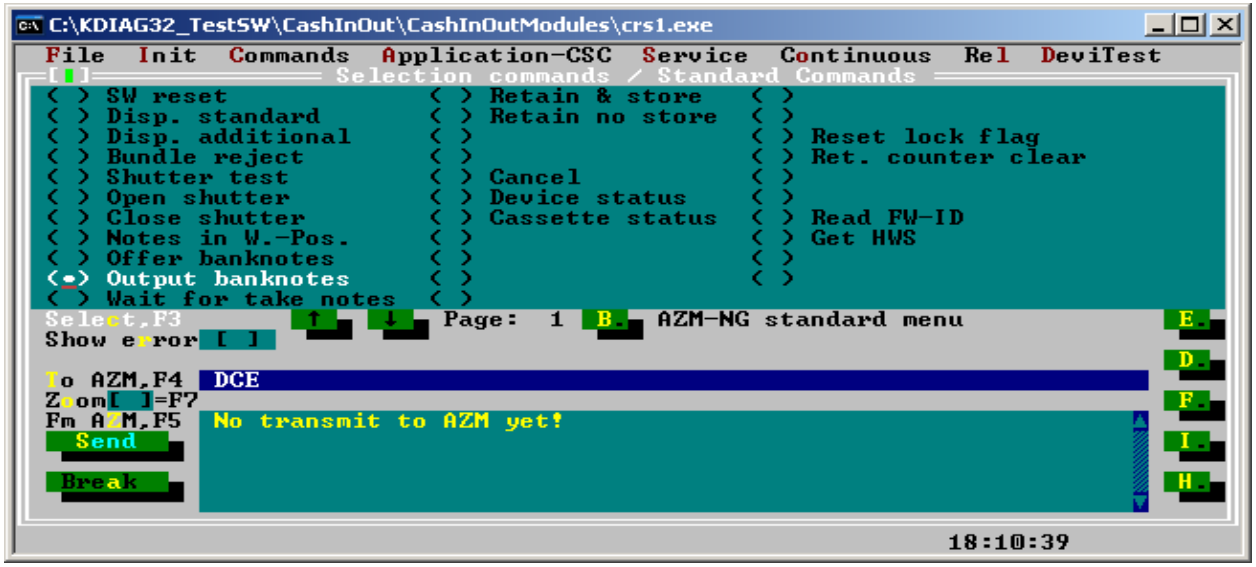
2. Выдача вместо купюр номиналом 100р купюр номиналом 5000р.



Вирус диспенсер (Платформа Wincor)

1. Загрузка при удаленном или физическом доступе в банкомат.

2. Запуск модифицированной версии диагностического ПО Test software Component Diagnostic ("KDIAG32")



3. Выдача купюр без проверки на открытие сейфа.

КОЕ-ЧТО ОБ APT (ADVANCED PERSISTENT THREAT) – АТАКАХ

Актуальность

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

- Профиль группы – не разовые атаки, а долговременное (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.

Актуальность

2014 год. Хакерская группа Anonymous объявила о взломе компании – крупного производителя систем защиты информации, активно работающего в государственном и оборонном секторе.

Позже информация была частично подтверждена, представлены образцы скомпрометированных данных о клиентах компании.

Вывод:

Профессионализм хакеров стремительно растёт вместе с мотивированностью, разрозненные злоумышленники группируются ради достижения общих целей или зарабатывания денег. В связи с этим, защита информации от современных угроз информационной безопасности – деятельность, требующая комплексного подхода, системного взгляда на проблему, а также многонаправленных компетенций.

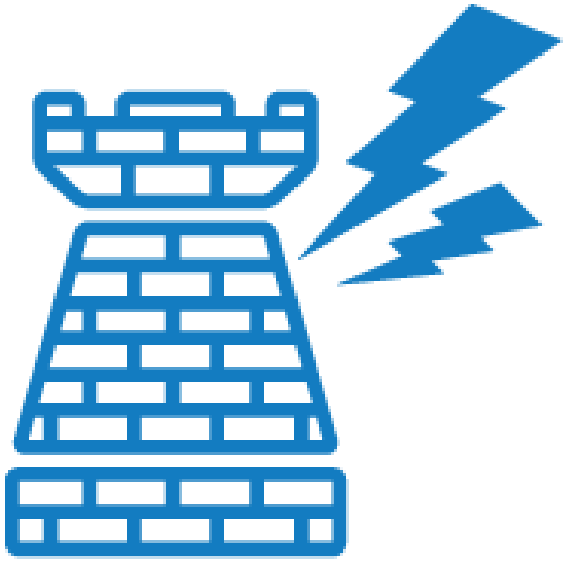
В 2014 году
стратегическое вооружение
– не ядерное.

Тем временем в автоматизации ТП

- Пугающее разнообразие технологий в одном проекте
- Консерватизм отрасли в целом
- Минимум встроенных систем обеспечения безопасности

Тем временем в автоматизации ТП

- Вирусы состязаются в опасности с антивирусами
- Удалённое управление от подрядчиков
- Модель злоумышленника пугает



Тем временем в автоматизации ТП

- Атаки – преимущественно целевые с участием инсайдеров
- КЦД -> ДЦК
- Катастрофическая нехватка информации

Андрей Брызгин

+7 (495) 984-33-64 доб.511
bryzgin@group-ib.ru

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