KASPERSKY lab

ЦЕЛЕВЫЕ АТАКИ НА КРЕДИТНО-ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

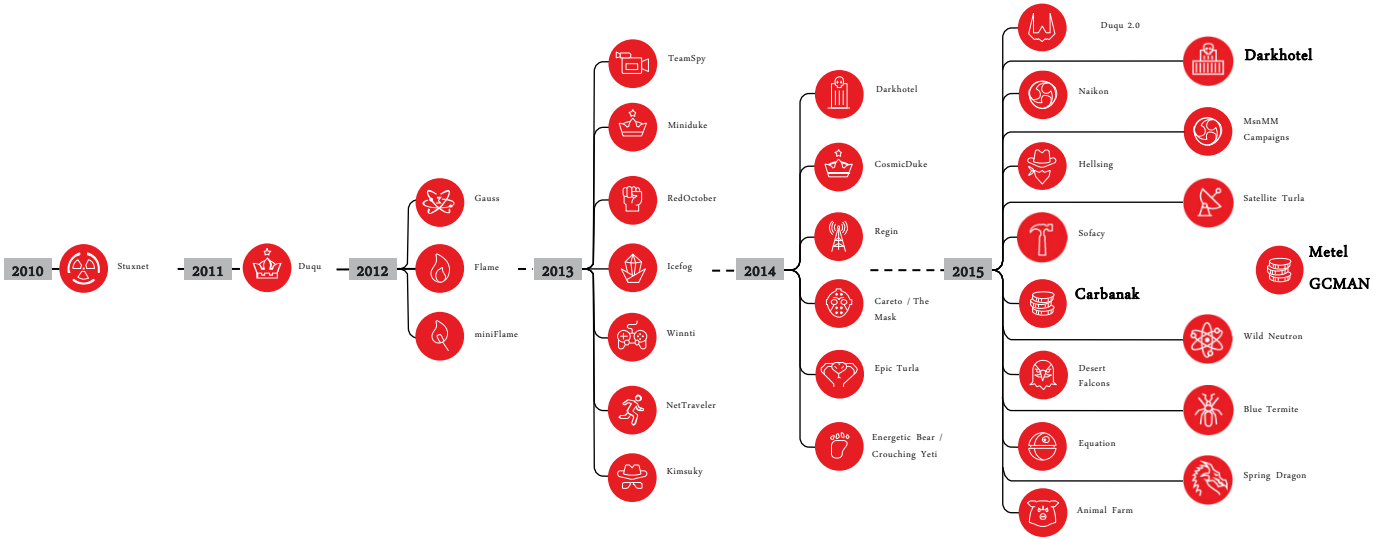
СПОСОБЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ФИНАНСОВЫХ ПОТЕРЬ

Кирилл Керценбаум
Лаборатория Касперского

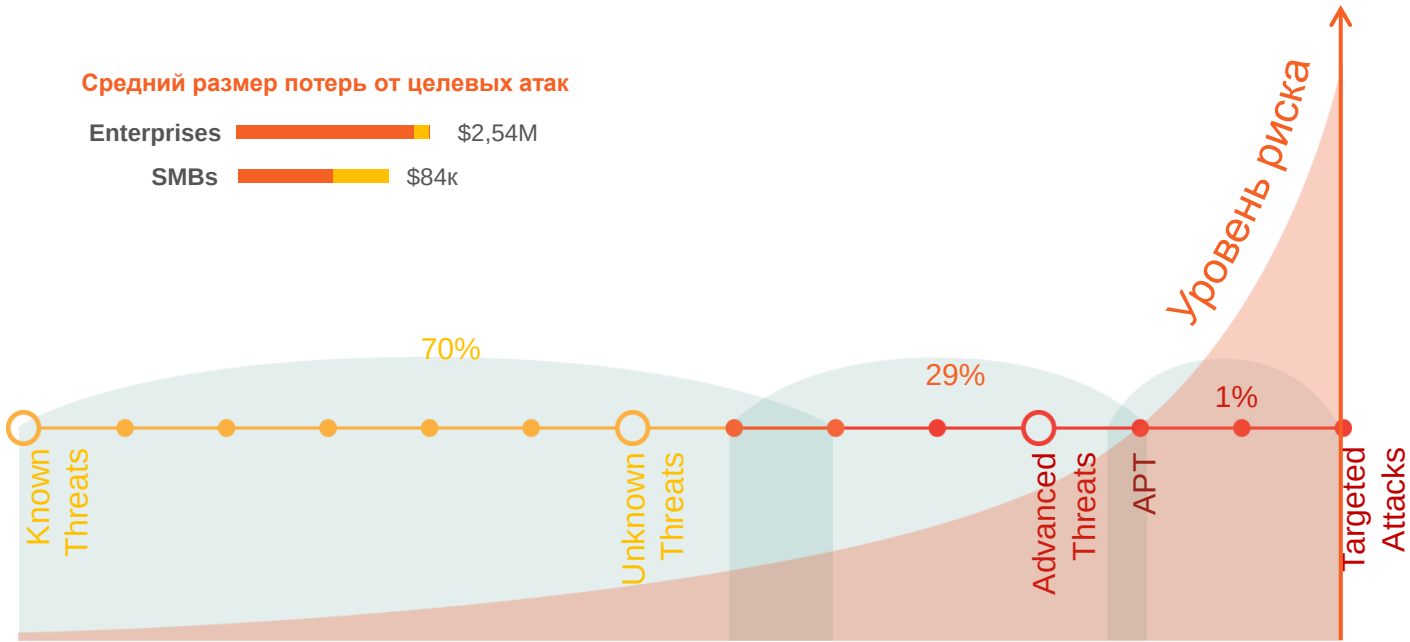
Магнитогорск, 17 февраля, 2016 года

ТРЕНДЫ И ПРОБЛЕМАТИКА

ЦЕЛЕВЫЕ АТАКИ: ВЧЕРА, СЕГОДНЯ И ЗАВТРА



РИСК ОТ ЦЕЛЕВЫХ АТАК И ВОЗВРАТ ИНВЕСТИЦИЙ



ТИПОВОЕ РАЗВИТИЕ ЦЕЛЕВОЙ АТАКИ

НЕГАТИВНОЕ ВОЗДЕЙСТВИЕ

- доступ к информации
- воздействие на бизнес процессы
- сокрытие следов
- тихий уход

ПОДГОТОВКА

- анализ цели
- подготовка стратегии
- создание/покупка тулсета

РАСПРОСТРАНЕНИЕ

- кража идентификационных данных
- повышение привилегий
- налаживание связей
- легитимизация действий
- получение контроля

ПРОНИКНОВЕНИЕ

- использование слабых мест
- проникновение внутрь инфраструктуры

KASPERSKY lab

Как преступник группировки Carbanak атакует финансовые организации

1. Заражение

Во вложении отправляется бэкдор Carbanak

Служащий банка

Письма с эксплойтами

Украденные учетные данные

В поисках ПК администратора заражены сотни компьютеров

2. Сбор сведений

Перехват экрана служащего

Системы денежных переводов

Запись

Администратор

3. Имитация действий сотрудника

Как были украдены деньги

Интернет-банк
Деньги были переведены на счета мошенников

Системы электронных платежей
Деньги переведены в банки Китая или США

«Раздувание» балансов счетов
Увеличение количества средств за счет мошеннических операций

Контроль над банкоматами
Команды на выдачу наличных в установленное время

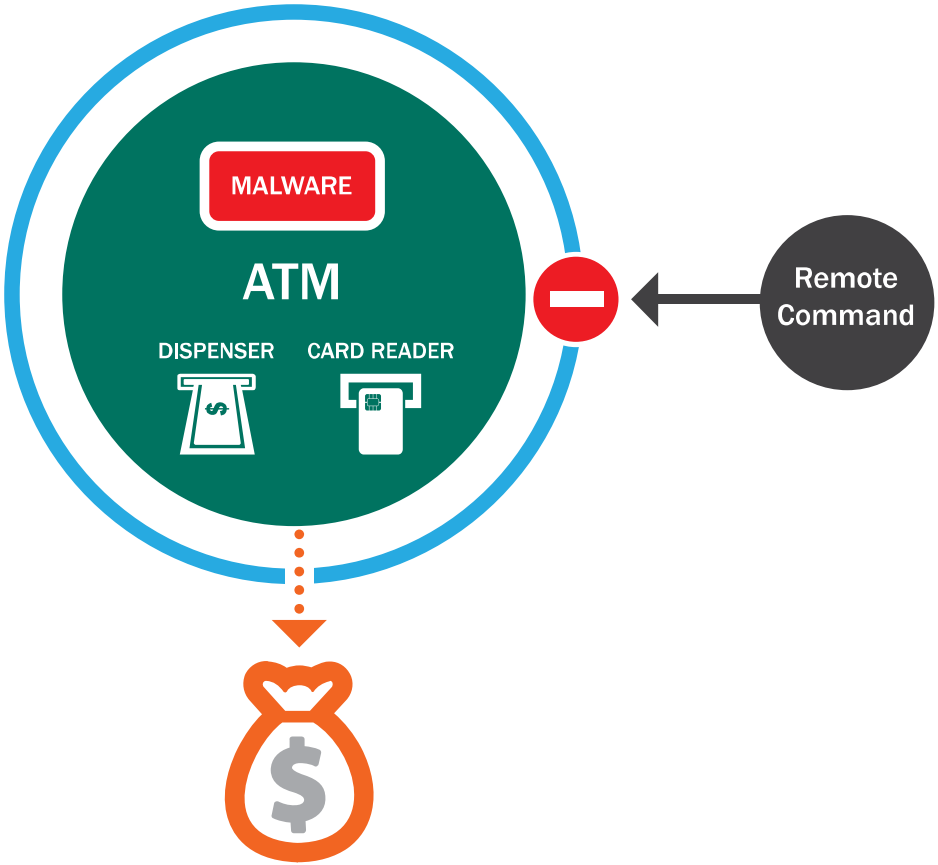
Манипуляции с базами данных
Изменения сведений о владельце счета

НОВИНКА!

GREAT

KASPERSKY lab

СХЕМА ТИПИЧНОЙ АТАКИ НА ATM С ИСПОЛЬЗОВАНИЕМ ВРЕДОНОСНОГО ПО



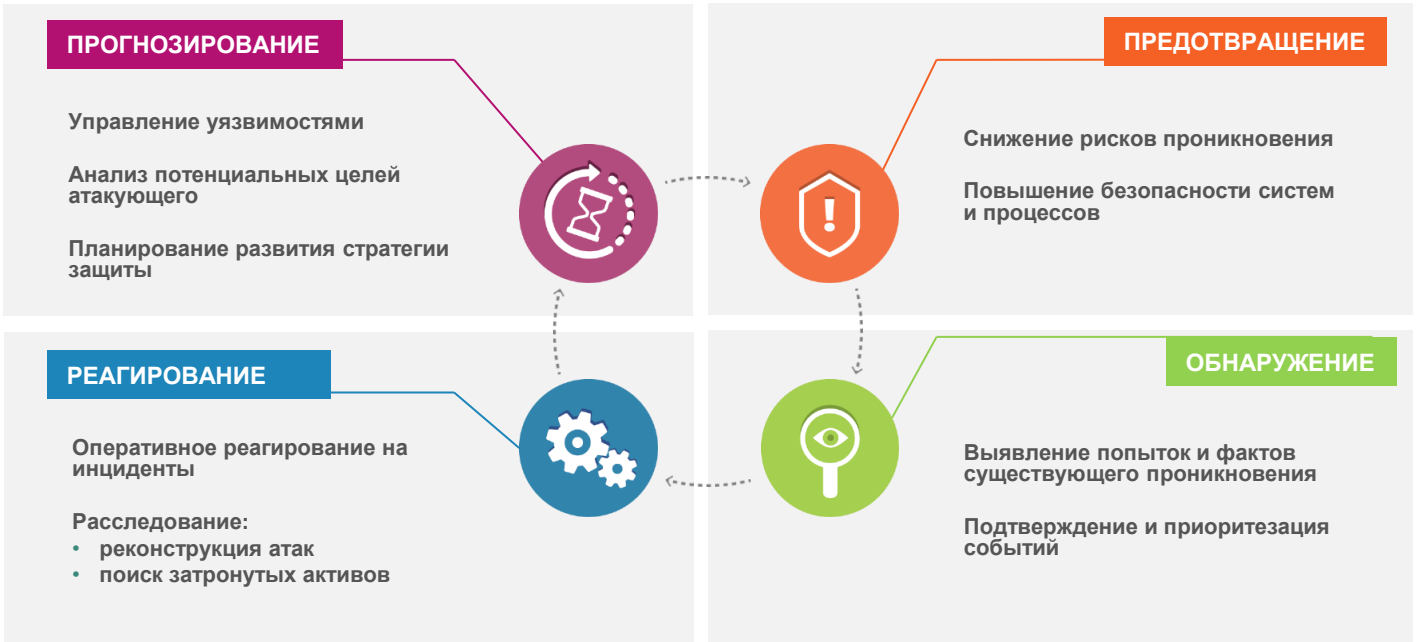
ВРЕДОНОСНЫЕ ПРОГРАММЫ ДЛЯ БАНКОМАТОВ

March 2009	**Backdoor.Win32.Skimer**
March 2012	**Trojan-Spy.Win32.SPSniffer**
October 2013	**Trojan-Banker.MSIL.Atmer (Ploutus)**
November 2013	**Trojan.Win32.Brob (Virus?)**
December 2013	**Backdoor.Win32.SkimerNC**
March 2014	**Backdoor.Win32.Tyupkin**
April 2014	**Backdoor.Win32.NeoPacket (VB.ww)**
December 2014	**Backdoor .Win32.Atmmng**
March 2015	**Backdoor.Win32.Atmdelf (Skimmer.w)**
September 2015	**Backdoor.Win32.Sucful.a**

KASPERSKY lab

СТРАТЕГИЯ ПРОТИВОДЕЙСТВИЯ ЦЕЛЕНАПРАВЛЕННЫМ АТАКАМ И ПЕРЕДОВЫМ УГРОЗАМ

АДАПТИВНАЯ МОДЕЛЬ ПРОТИВОДЕЙСТВИЯ ПЕРЕДОВЫМ УГРОЗАМ ИБ



ОБНАРУЖЕНИЕ ЦЕЛЕВЫХ АТАК ИМЕЮЩИМИСЯ СРЕДСТВАМИ

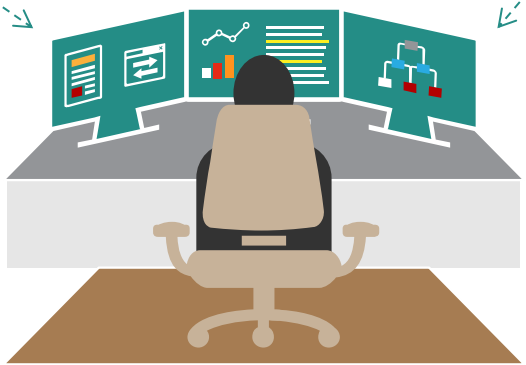
ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СУЩЕСТВУЮЩИХ РЕШЕНИЙ

Проактивное оповещение об угрозах безопасности

Повышение эффективности существующей SIEM-системы

- Malicious URLs
- Phishing URLs
- Botnet C&C URLs
- Malware Hashes
- Mobile Malware Hashes
- P-SMS Trojan Feed
- Mobile Botnet C&C URLs

splunk> QRadar® ArcSight An HP Company

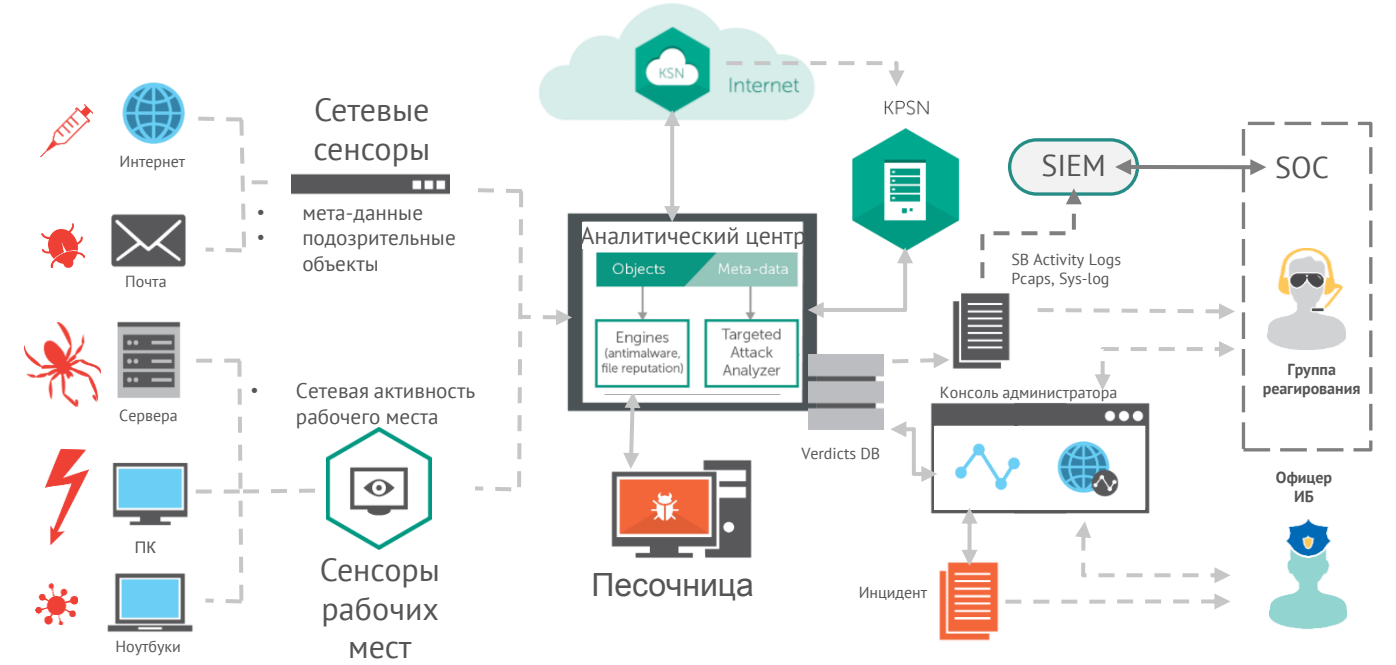


Оперативная информация о новых целевых атаках

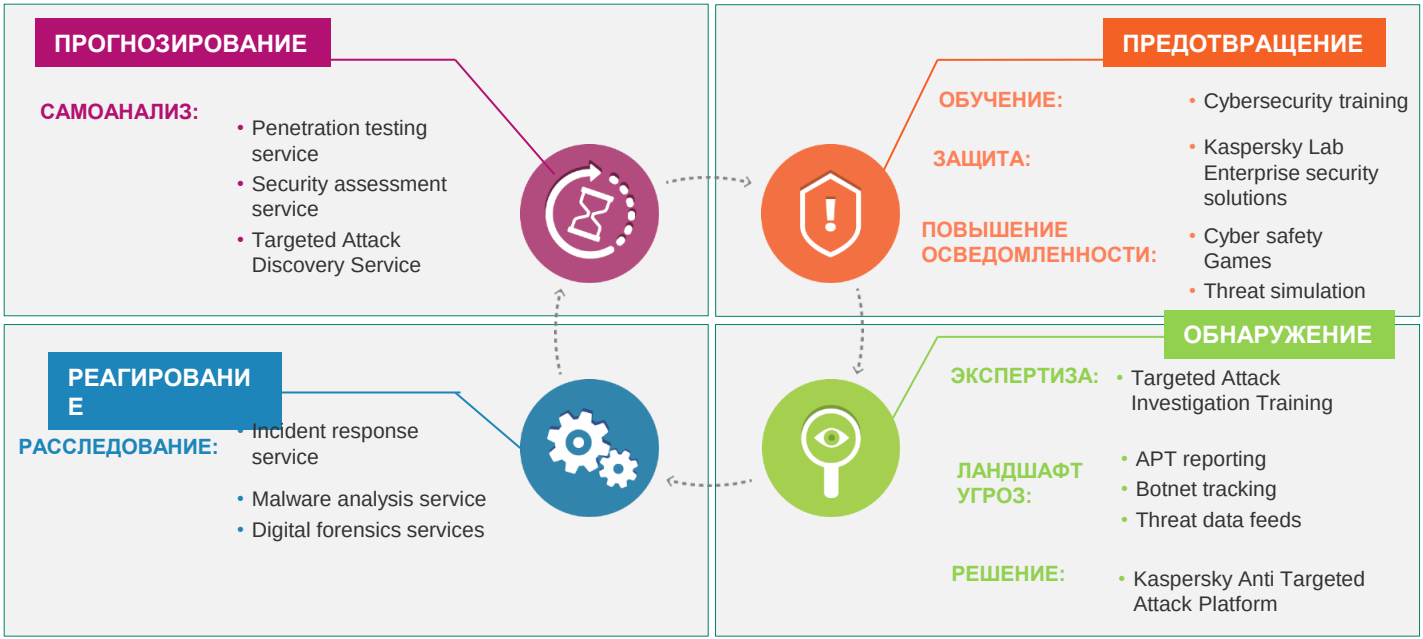
- Детальная информация как обнаружить угрозу внутри сети
- Обновление новой информацией по угрозе со временем
- Подписка на все выявленные целевые атаки ЛК (Global Targeted Attacks)

KASPERSKY lab

СПЕЦИАЛИЗИРОВАННОЕ РЕШЕНИЕ



СТРАТЕГИЯ АДАПТИВНОЙ КОРПОРАТИВНОЙ ИБ



СПАСИБО!

Kaspersky Lab

www.kaspersky.ru/enterprise

KASPERSKY lab