



# ЦЕЛЕВЫЕ АТАКИ НА КРЕДИТНО-ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

СПОСОБЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ  
ФИНАНСОВЫХ ПОТЕРЬ

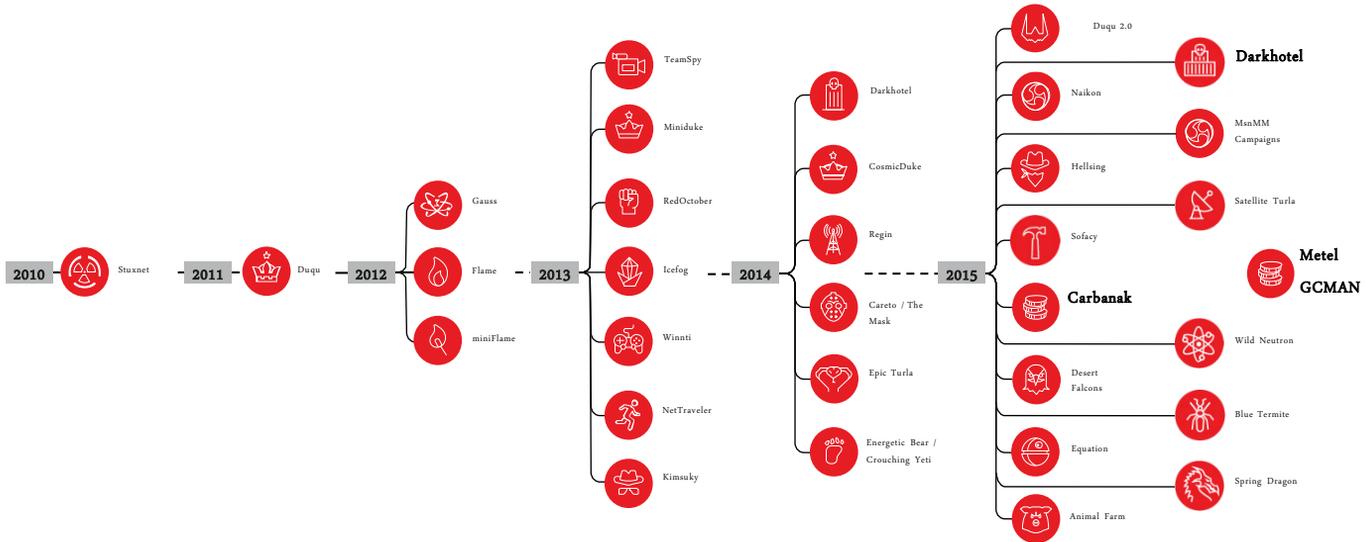
Кирилл Керценбаум  
Лаборатория Касперского

Магнитогорск, 17 февраля, 2016 года

---

## ТРЕНДЫ И ПРОБЛЕМАТИКА

# ЦЕЛЕВЫЕ АТАКИ: ВЧЕРА, СЕГОДНЯ И ЗАВТРА

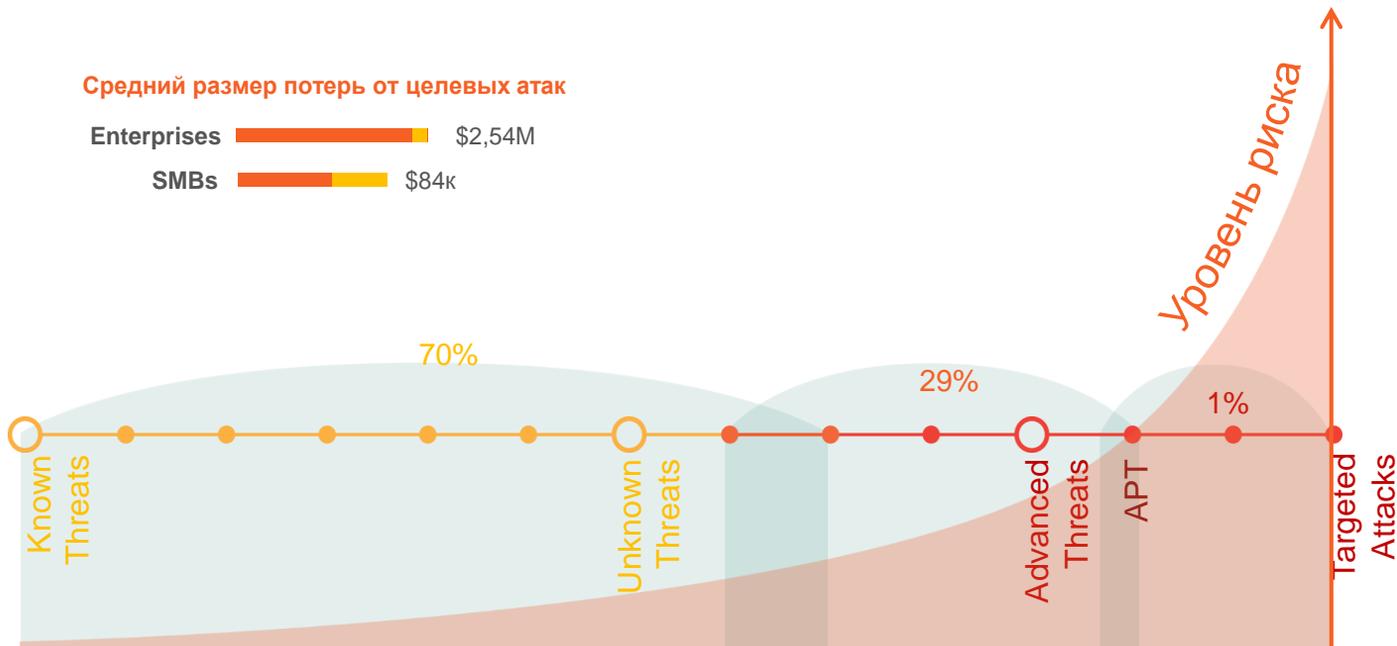


# РИСК ОТ ЦЕЛЕВЫХ АТАК И ВОЗВРАТ ИНВЕСТИЦИЙ

Средний размер потерь от целевых атак

Enterprises ██████████ \$2,54M

SMBs ██████████ \$84к



# ТИПОВОЕ РАЗВИТИЕ ЦЕЛЕВОЙ АТАКИ

## НЕГАТИВНОЕ ВОЗДЕЙСТВИЕ

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



ЦЕЛЕВАЯ АТАКА  
МОЖЕТ ДЛИТЬСЯ  
МЕСЯЦЫ... И  
ГОДАМИ  
ОСТАВАТЬСЯ  
НЕОБНАРУЖЕННОЙ

## 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





# Как преступник группировки Carbanak атакует финансовые организации

## 1. Заражение

 Во вложении отправляется бэкдор Carbanak

 Служащий банка

 Письма с эксплоитами  
 Украденные учетные данные

В поисках ПК администратора заражены сотни компьютеров



## 2. Сбор сведений

Перехват экрана служащего



 Hacker

 Системы денежных переводов

 Администратор



 Запись

## 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

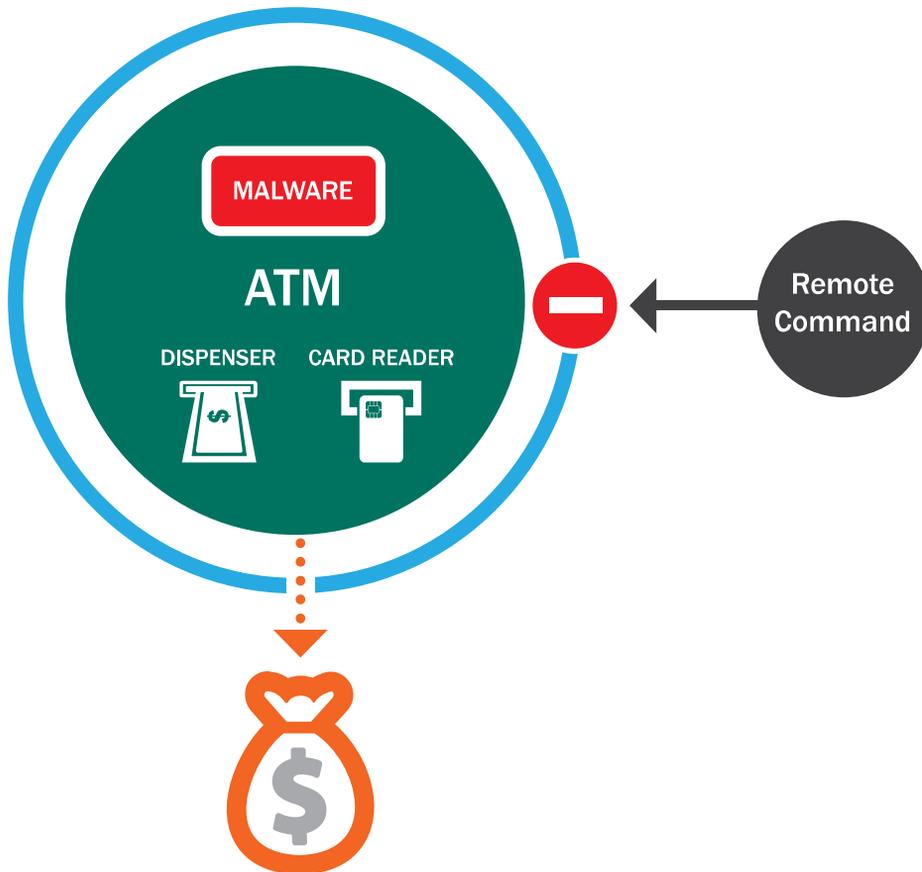
 «Раздувание» балансов счетов  
Увеличение количества средств за счет мошеннических операций

 Контроль над банкоматами  
Команды на выдачу наличных в установленное время

 Манипуляции с базами данных  
Измена сведений о владельце счета

**НОВИНКА!**

# СХЕМА ТИПИЧНОЙ АТАКИ НА АТМ С ИСПОЛЬЗОВАНИЕМ ВРЕДНОСНОГО ПО



# ВРЕДОНОСНЫЕ ПРОГРАММЫ ДЛЯ БАНКОМАТОВ



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

---

# СТРАТЕГИЯ ПРОТИВОДЕЙСТВИЯ ЦЕЛЕНАПРАВЛЕННЫМ АТАКАМ И ПЕРЕДОВЫМ УГРОЗАМ

# АДАПТИВНАЯ МОДЕЛЬ ПРОТИВОДЕЙСТВИЯ ПЕРЕДОВЫМ УГРОЗАМ ИБ

## ПРОГНОЗИРОВАНИЕ

Управление уязвимостями

Анализ потенциальных целей атакующего

Планирование развития стратегии защиты



## ПРЕДОТВРАЩЕНИЕ

Снижение рисков проникновения

Повышение безопасности систем и процессов



## РЕАГИРОВАНИЕ

Оперативное реагирование на инциденты

Расследование:

- реконструкция атак
- поиск затронутых активов



## ОБНАРУЖЕНИЕ

Выявление попыток и фактов существующего проникновения

Подтверждение и приоритезация событий



# 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> Radar®

ArcSight®  
An HP Company

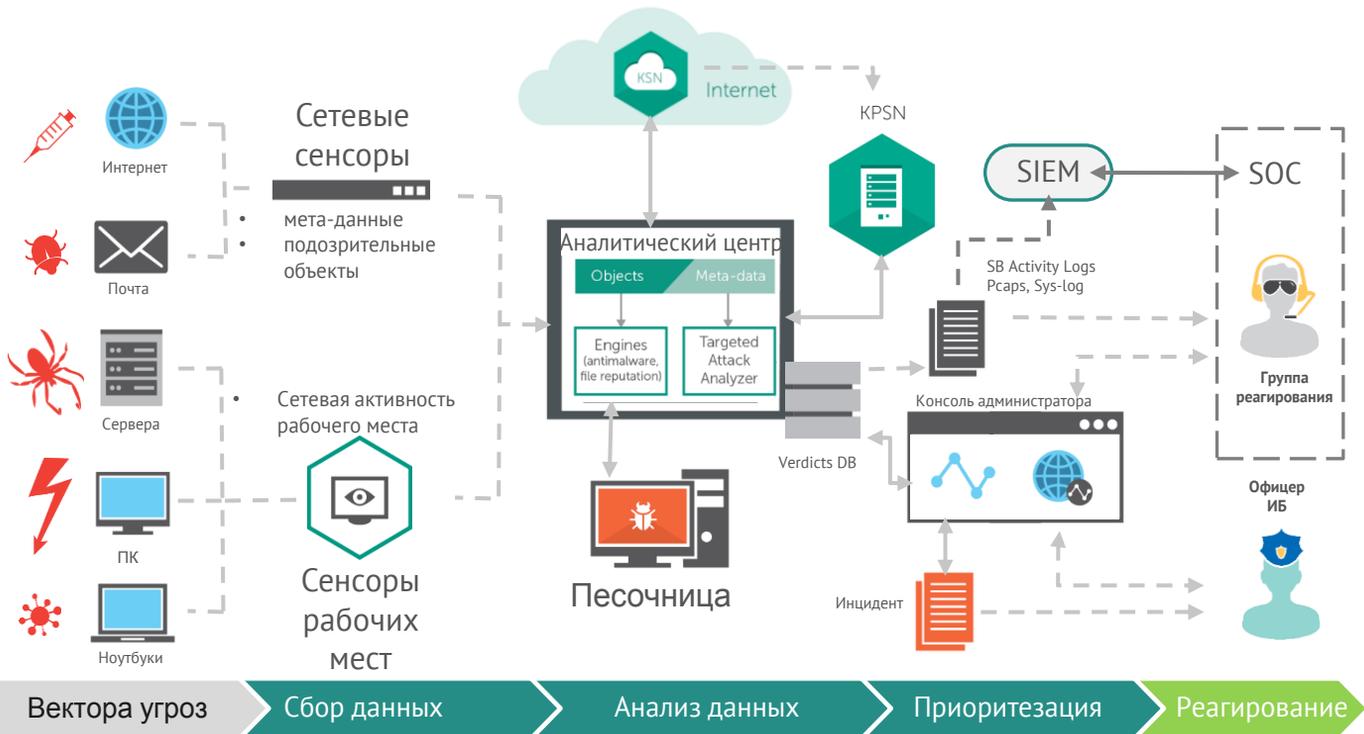


Оперативная  
информация о новых  
целевых атаках

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



# СПЕЦИАЛИЗИРОВАННОЕ РЕШЕНИЕ



# СТРАТЕГИЯ АДАПТИВНОЙ КОРПОРАТИВНОЙ ИБ

## ПРОГНОЗИРОВАНИЕ

### САМОАНАЛИЗ:

- Penetration testing service
- Security assessment service
- Targeted Attack Discovery Service



## ПРЕДОТВРАЩЕНИЕ

### ОБУЧЕНИЕ:

- Cybersecurity training

### ЗАЩИТА:

- Kaspersky Lab Enterprise security solutions

### ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ:

- Cyber safety Games
- Threat simulation



## РЕАГИРОВАНИЕ

### РАССЛЕДОВАНИЕ:

- Incident response service
- Malware analysis service
- Digital forensics services



## ОБНАРУЖЕНИЕ

### ЭКСПЕРТИЗА:

- Targeted Attack Investigation Training

### ЛАНДШАФТ УГРОЗ:

- APT reporting
- Botnet tracking
- Threat data feeds

### РЕШЕНИЕ:

- Kaspersky Anti Targeted Attack Platform



# СПАСИБО!

---

Kaspersky Lab

[www.kaspersky.ru/enterprise](http://www.kaspersky.ru/enterprise)

