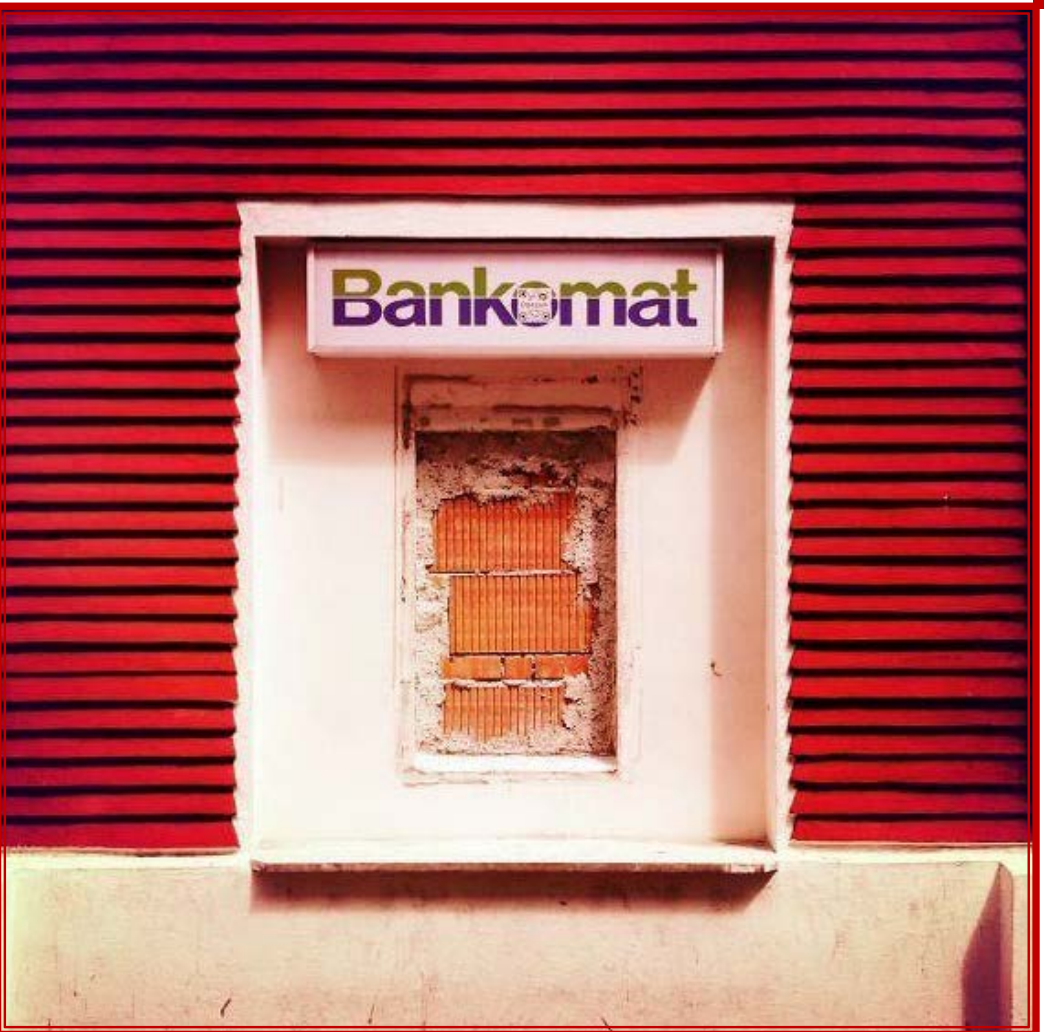
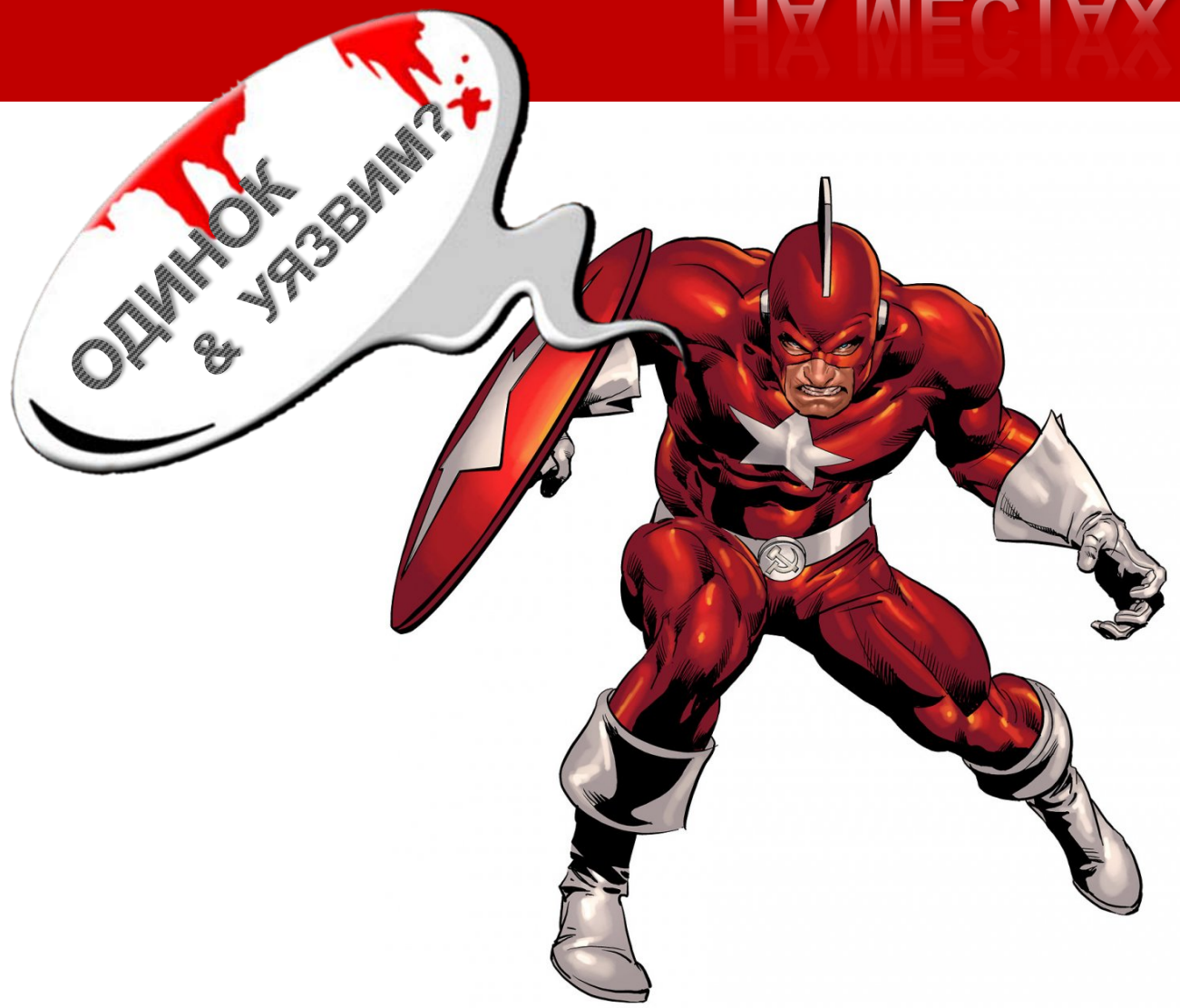
Оксана Пиргалина

Офицер информационной безопасности
департамента ИТ-безопасности
АО «Евразийский банк»

О ЗАЩИТЕ БАНКОМАТОВ НА МЕСТАХ





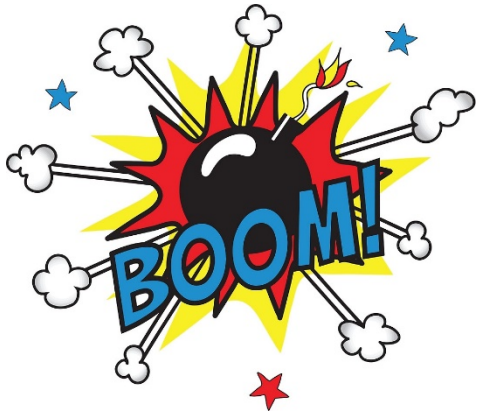
ДЛЯ ЧЕГО ЭТО НУЖНО?

ЧТО БЫ ИЗБЕЖАТЬ:

- ✓ Репутационного ущерба
- ✓ Прямых убытков
- ✓ Недополученной прибыли
- ✓ Претензий со стороны регуляторов

ЗАМЕТКИ НА ПОЛЯХ:

- ✓ *структура банкомата*
- ✓ *принцип взаимодействия с банком*
- ✓ *физическое расположение;*
- ✓ *место в сети.*



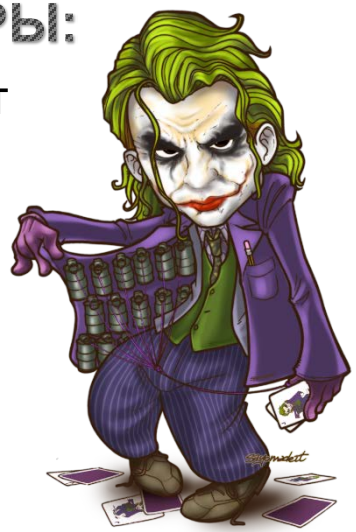
ПРИМЕРЫ:

кража данных пластиковых карт

выдача наличных денег злоумышленникам

выход из строй терминальной сети

нарушение требований НБРК, PCI DSS



АТАКИ ТИПА «BLACK BOX»

NCR Personas
Wincor ProCash

ИСТОЧНИК УГРОЗЫ: внешний злоумышленник, возможно участие инсайдера

ОПИСАНИЕ:

Злоумышленники получают свободный доступ к сервисной части банкомата,
затем разрывают соединение между диспенсером и USB-хабом, куда потом помещается «имитатор».
Далее злоумышленники подключают ноутбук или смартфон к оригинальному диспенсеру,
С помощью чего подают специальные управляющие команды на выдачу наличных денежных средств.

ПРЕДОТВРАЩЕНИЕ:

- ✓ включение шифрования команд, передающихся на диспенсер;
- ✓ «нестандартный» ключ, усиленный замок;
- ✓ ограничение доступа в помещение в темное время суток;
- ✓ установка банкоматов таким образом, что бы закрыть бесконтрольный доступ к сервисной части

ВЫЯВЛЕНИЕ:

- ✓ мониторинг событий по открытию сервисной части и
- ✓ механизм распознавания несанкционированного открытия;
- ✓ видеонаблюдение за сервисной частью;

АТАКИ ТИПА «KDIAG»

Wincor Nixdorf

ИСТОЧНИК УГРОЗЫ: инсайдер, возможно участия пособника из вне

ОПИСАНИЕ:

Инсайдер получает доступ к банкоматам через удаленное подключение, и размещает модифицированную версию утилиты для тестирования механизма выдачи денежных средств.
В модифицированной версии отсутствуют ограничения, связанные с нахождением банкомата в тестовом режиме и открытыми створками сейфа.
По расписанию утилита отрабатывает и происходит неограниченная выдача денежных средств.

ПРЕДОТВРАЩЕНИЕ:

- ✓ ограничение прав администраторов минимальным необходимым набором;
- ✓ использование системы контроля целостности критичных файлов (FIM);
- ✓ использование инструментов по контролю запуска приложений;
- ✓ использование инструментов по контролю за изменением реестра и т.д.

ВЫЯВЛЕНИЕ:

- ✓ логирование подключений и действий администраторов;
- ✓ дублирование логов банкоматов и систем мониторинга, FIM в SIEM;
- ✓ механизм распознавания несанкционированного входа до банкомата.

АТАКИ ТИПА «SKIMER»

Diebold

ИСТОЧНИК УГРОЗЫ: внешний злоумышленник

ОПИСАНИЕ:

Злоумышленники получают свободный доступ к сервисной части банкомата, затем загружаются с компакт-диска или флешки, и размещают на жестком диске вирус.
Вредоносной программой можно управлять при помощи специальные карты с магнитной полосой, на второй дорожке которой записаны инструкции для Skimer.
Другой тип карт позволяет злоумышленникам активировать одну из 21 известных трояну команд, пользуясь цифровой клавиатурой банкомата.

ПРЕДОТВРАЩЕНИЕ:

- ✓ установка пароля на BIOS, запрет загрузки с дисков, флешек;
- ✓ использование инструментов по контролю запуска приложений;
- ✓ использование системы контроля целостности критичных файлов;
- ✓ использование антивируса и т.д.

ВЫЯВЛЕНИЕ:

- ✓ логирование подключений по сети;
- ✓ дублирование логов банкоматов и систем мониторинга, FIM в SIEM;
- ✓ механизм распознавания несанкционированного открытия.

АТАКИ ТИПА «TYUPKIN»

Microsoft Windows XP

ИСТОЧНИК УГРОЗЫ: внешний злоумышленник, возможно участие инсайдера

ОПИСАНИЕ:

Злоумышленники получают свободный доступ к сервисной части банкомата, затем загружаются с компакт-диска или флешки, и размещают на жестком диске вирус.
Далее злоумышленники получают возможность управлять зараженным компьютером.
Вирус Tyupkin имеет несколько модификаций. Некоторые версии также занимаются скимингом, другие позволяют уничтожать следы Tyupkin и стирают видеозаписи.

ПРЕДОТВРАЩЕНИЕ:

- ✓ установка пароля на BIOS, запрет загрузки с дисков, флешек;
- ✓ использование инструментов по контролю запуска приложений;
- ✓ ограничение доступа к банкомату и от него на уровне сети;
- ✓ использование антивируса и т.д.

ВЫЯВЛЕНИЕ:

- ✓ логирование подключений по сети;
- ✓ дублирование логов банкоматов и систем мониторинга, FIM в SIEM;
- ✓ механизм распознавания несанкционированного открытия.

РЕКОМЕНДАЦИИ

- ✓ Установка пароля на BIOS (уникальность), запрет на загрузку не с жесткого диска
- ✓ Включение шифрования команд для диспенсера, при этом каждый ключ уникален
- ✓ Пароль от учетной записи администратора (сложный, меняющийся)
- ✓ Установка систем контроля целостности критичных файлов, запуска приложений и т.д.
- ✓ Обеспечение безопасности на уровне сети. Для gsm подключений отдельный APN.

Для внутренних сетей VLAN/шифрование данных на банкомате/программный VPN.

Изолировать сетевые розетки, исключить возможность подключения.

- ✓ Система удаленного управления (Radmin, DameWare, RDP и т.д.) – централизованная, персональные учетные записи, ограничение на подключение по сети, ограниченные права при подключении, шифрование.

РЕКОМЕНДАЦИИ

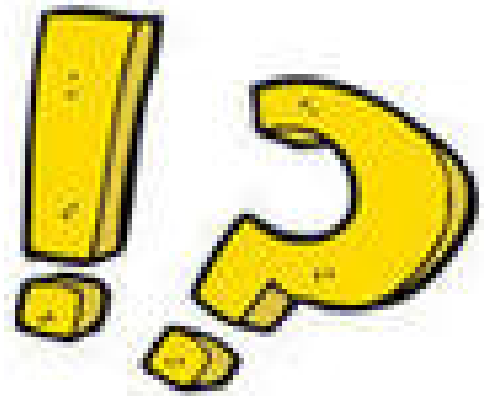
- ✓ Мониторинг за действиями пользователей и открытием сервисной части
- ✓ Надежные замки и нестандартные ключи от сервисной части банкомата
- ✓ Видеонаблюдение за сервисной частью банкоматов, сигнализация
- ✓ При размещении межстенных банкоматов ограничение доступа к сервисной части
- ✓ При наличие – установка патчей, обновлений. Обновление антивирусных баз и т.д.
- ✓ Получение и выполнение рекомендаций от вендеров и других надежных источников
- ✓ Повышение осведомленности работников и клиентов

БАНКОМАТЫ → Увеличение функций → Увеличение рисков

ОБСУДИМ?

ЗАМЕТКИ НА ПОЛЯХ:

Наличие антивируса – обязательное требование согласно дополнению от 28 января 2016 года к Инструкции по выпуску и использованию платежных карт



- ✓ Требования регуляторов: ставить ли антивирус? Есть ли альтернатива?
- ✓ Стоит ли вводить в домен? Плюсы и минусы
- ✓ Обновление ПО и железа. Игра стоит свеч?

СПАСИБО ЗА ВНИМАНИЕ!