Противостояние актуальным хакерским атакам. Взгляд из банки.

Алексей Плешков
Газпромбанк

Москва, ноябрь 2015


прямые
внешние
объективные
глобальные
потенциальные
непосредственные
локальные
косвенные
внутренние
субъективные
#угрозы_ИБ

#банковский_фишинг

«Whaling» (от англ. «whale» – кит)

- **Целевая атака на исполнителей**
- **Имитация письма/директивы менеджера**
- **Имитация отправки с телефона**

Цель: получение $$$

Источник: МПС VISA

#банковский_фишинг

обучение

анализ

пентесты

#вирусы_шифровальщики

- Скрытая установка вредоносного ПО в ОС рабочей станции или смартфона
- Шифрование чувствительных данных
- Предложение о «выкупе»

Цель: получение $$$

Источник: FinCERT ЦБ

#вирусы_шифровальщики

антивирус

резервирование

обучение

#операции_CNP

- Получение доступа к реквизитам карт
- Копирование реквизитов
- Совершение операций покупки на сайтах в Интернет (чаще - без поддержки схемы 3D-Secure)
- Продажа купленного товара

Цель: получение $$$

Источник: МПС VISA/MC

#операции_CNP

информирование

геофильтры

антифрод

#мобильный_фишинг

- Кибersквоттеринг
- Создание зараженной баннерной сети
- Массовая рассылка «приманок»
- Скрытая установка вредоносного ПО

Цель: создание бот-сети из смартфонов, получение персональных данных

Источник: securitylab.ru

#мобильный_фишинг

анализ

информирование

антивирус

#атаки ДБО

- Получение НСД удаленно к АРМ клиента ДБО
- Отслеживание операций
- Совершение несанкционированных переводов на счета дропперов
- Вывод из строя АРМ клиента
- Обналичивание денежных средств через банкоматы

Цель: получение $$$

Источник: Антидроп

#атаки ДБО

информирование

антифрод

объединение усилий

#шантаж

- Взлом «тематических» сайтов
- Получение персональных данных
- Поиск связей в социальных сетях / базах
- Целевая рассылка предложений

Цель: создание сети инсайдеров

Источник: FinCERT ЦБ

#шантаж

информирование

геофильтры

ограничения

#плацдарм

- Получение НСД к АРМ жертвы
- Мероприятия по закреплению / заражению
- Изучение и продажа «полезных» реквизитов
- ...
- Реализация/демаскировка бота

Цель: построение инфраструктуры для целевых атак

Источник: Антидроп

#плацдарм

антивирус

обучение

информирование

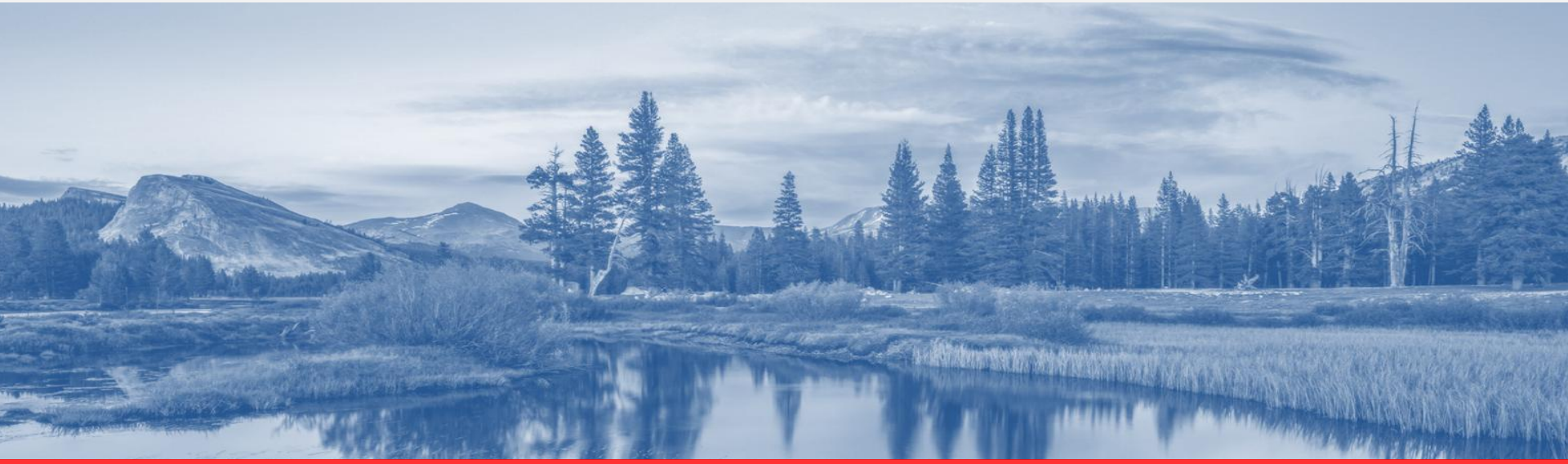
#контакты

Плешков Алексей Константинович

начальник Управления
режима информационной безопасности
Департамент защиты информации
Банк ГПБ (АО) г. Москва

e-mail: Alexey.Pleshkov@gazprombank.ru
тел: 8(495)-428-5045

Спасибо за внимание!



Готов ответить на Ваши вопросы