Целевые атаки – так ли они разнообразны, как мы привыкли считать?

Олег Котов - Региональный инженер CyberArk

Целевые атаки

banki.ru

Главная / Новости / Обзор прессы / Хакеры против банков

Хакеры против банков

22.12.2014 11:54

Хакеры из группы Anunak атакуют крупные банки, а не их клиентов, и уже похитили около 1 млрд рублей. Почему такие преступления считаются особо опасными в киберсреде?

Более пятидесяти банков и пять платежных систем на территории России и стран бывшего СССР подверглись атакам киберпреступников из группы Anunak, следует из отчета российской Group-IB, специализирующейся на расследовании киберпреступлений, и голландской Fox-IT, компании-эксперта в области технологий информационной безопасности.

https://www.fox-it.com/en/files/2014/12/Anunak_APT-against-financial-institutions2.pdf

http://www.cyber-berkut.org/traitors/0017.php

CYBERARK

Развитие атаки. Anunak

CYBERARK

Развитие атаки. КиберБеркут

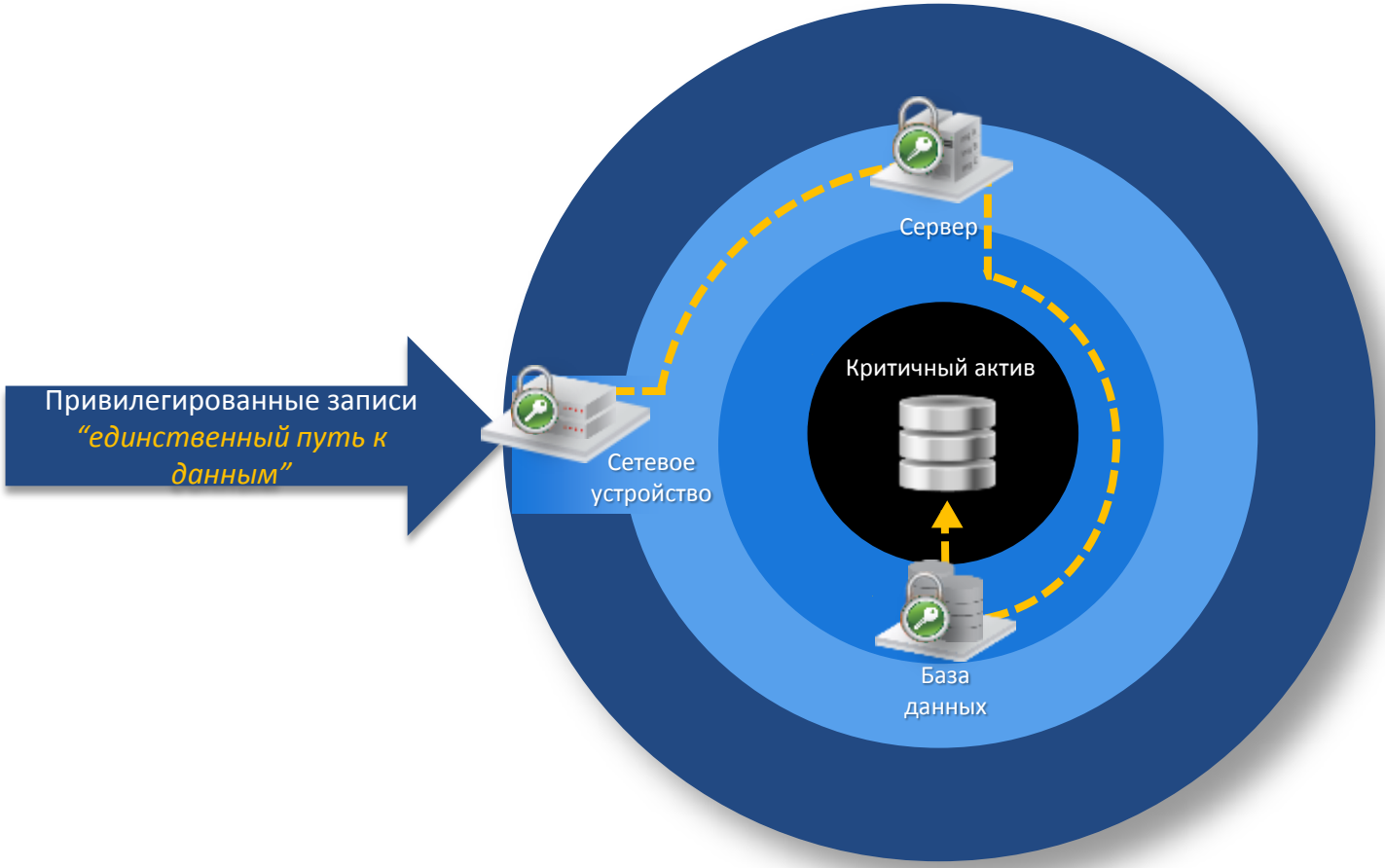
CYBERARK

Что общего?

- Проникновение
- Реализация сценария атаки
- …
- PROFIT !!!

CYBERARK®

«Все пути ведут...» к привилегированым записям



CYBERARK

Мнения экспертов

Не существует идеальной защиты

Нарушители профессиональны и меняют тактику все время.

Компании, уделяющие серьезное внимание ИБ и инвестирующие в ИТ, все равно подвергаются компрометации.

100%

Жертв обновляли антивирусы

94%

Вторжений были замечены 3-ми лицами

416

Дней (в среднем) атака в сети не замечена

100%

Вторжений использовали украденные УЗ

Mandiant, 2013

CYBERARK


CYBERARK

Эффективный контроль за привилегированными учётными записями

1. Обнаружение

2. Защита и управление доступом

3. Изоляция и полное фиксирование действий

4. Расследование в реальном времени

CYBERARK

CyberArk - Privileged Account Security

Поведенческий анализ

Контроль и мониторинг

Единая безопасная платформа

Privileged Threat Analytics

Management Portal/Web Access

Enterprise Password Vault®

SSH Key Manager

Privileged Session Manager®

Application Identity Manager™

On-Demand Privileges Manager™

Master Policy

Secure Digital Vault™

Защита

Детектирование

Ответная реакция

CYBERARK®

Сертификация

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3267

Выдан 24 ноября 2014 г.
Действителен до 24 ноября 2017 г.

Настоящий сертификат удостоверяет, что **программный комплекс управления привилегированными учетными записями и привилегированными сессиями: Cyber-Ark Privileged Identity Management and Session Management Suite 8.0**, разработанный компанией CyberArk Software Ltd. и производимый ООО «Сертифицированные информационные системы» в соответствии с техническими условиями ТУ 5090-003-82487552-13, функционирующий в средах операционных систем, указанных в формуляре 5090-003-82487552-13 ФО, является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации, управления доступом и регистрации событий безопасности, и соответствует требованиям технических условий при выполнении указаний по эксплуатации, приведенных в формуляре.

CYBERARK

Жизнь с CyberArk

"Борода" (диптих), Вася Ложкин.

CYBERARK

CYBERARK

Спасибо

Олег Котов - Региональный инженер CyberArk

Mobile +7 916 836 63 68 | Skype oleg_i_kotov
oleg.kotov@cyberark.com
www.cyberark.com