

# *ІНСОМ*



***Целевые  
кибератаки:  
причины,  
сценарии,  
последствия***

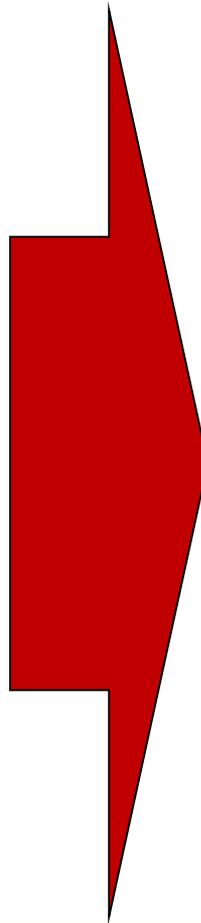
**Алексей Швачка,  
Инком Казахстан**

***Advanced Persistent Threat***  
**или**  
**Зачем нужна информационная  
безопасность**



# Advanced Persistent Threat

Смена парадигмы атак – от похищения к разрушению



# Advanced Persistent Threat

## Особенности реализации

- Перехват управления сетевым оборудованием и Active Directory
- Час «Ч» – Kill Disk, удаление бэкапов, конфигураций сетевого оборудования
- Выбор времени атак для максимального социального эффекта – последние дни года

## Соседи в Украине тоже пострадали

- Минфин, Казначейство, Укрзализныця (ж/д), Прикарпатьоблэнерго и многие др.

# Advanced Persistent Threat

- Целенаправленность
- Скрытность
- **Неотразимость**



# Целевая аудитория

- В организации «всё хорошо»:
  - стоимость активов не оценивали
  - анализ рисков не проводили
  - серьёзных инцидентов раньше не было
- В организации «всё есть»:
  - корпоративный антивирус
  - межсетевой экран, анти-СПАМ
  - резервное копирование

...но зачастую нету даже  
выделенной службы ИБ



# «Всё хорошо»



Периметр



Внутренняя  
сеть



Сервера и  
АРМы

# Начало



WEB



VPN

Периметр

Сегмент  
АРМов

CORE

Сегмент  
серверов

Внутренняя  
сеть

Admin    User

AD

Приложения,  
БД

Сервера и  
АРМы

# Начало



Периметр



Внутренняя  
сеть



Сервера и  
АРМы

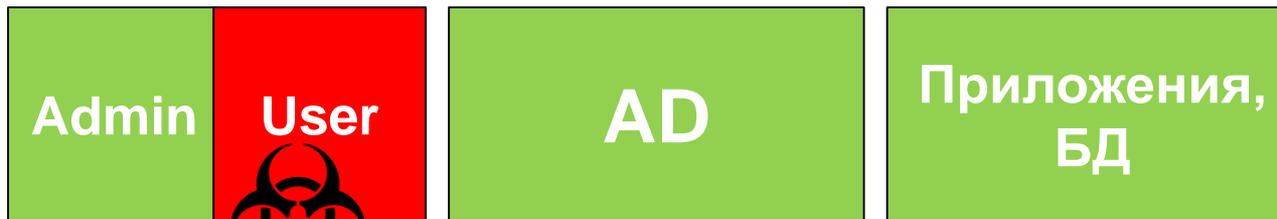
# Первое заражение



**Периметр**



**Внутренняя  
сеть**



**Сервера и  
АРМы**

# Контакт с С&С



**WEB**

**Mail**

**VPN**

**Периметр**

**Сегмент АРМов**

**CORE**

**Сегмент серверов**

**Внутренняя сеть**

**Admin** **User**

**AD**

**Приложения, БД**

**Сервера и АРМы**



# Discovering



**WEB**

**Mail**

**VPN**

**Периметр**

**Сегмент АРМов**

**CORE**

**Сегмент серверов**

**Внутренняя сеть**

**Admin**

**User**

**AD**

**Приложения, БД**

**Сервера и АРМы**



# «Root» получен!



**WEB**

**Mail**

**VPN**

**Периметр**

**Сегмент  
АРМов**

**CORE**

**Сегмент  
серверов**

**Внутренняя  
сеть**

**Admin**  

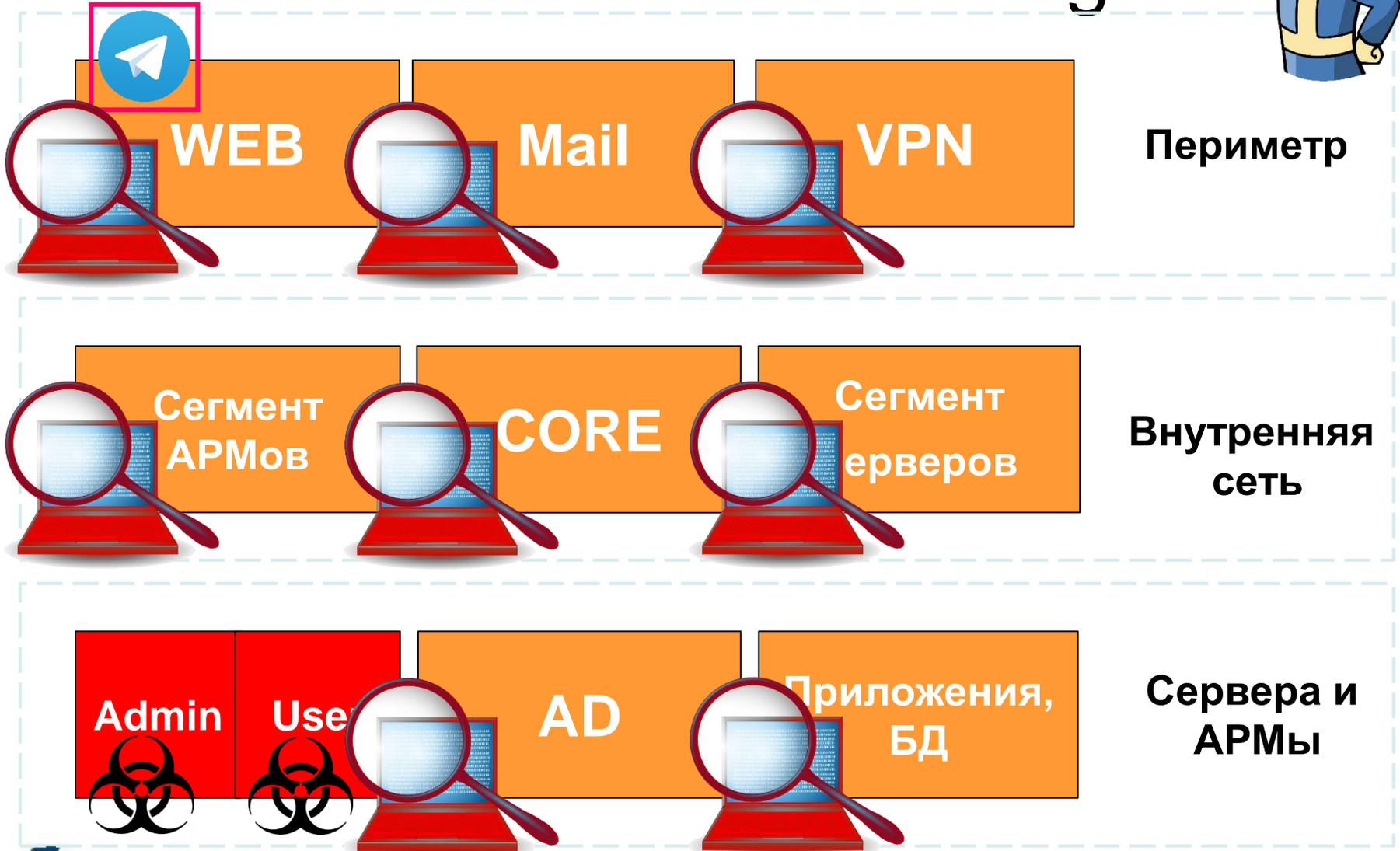

**User**  


**AD**

**Приложения,  
БД**

**Сервера и  
АРМы**

# Advanced Discovering



# AD скомпрометирована!



Периметр



Внутренняя  
сеть



Сервера и  
АРМы

# Контроль перехвачен!



Периметр



Внутренняя сеть

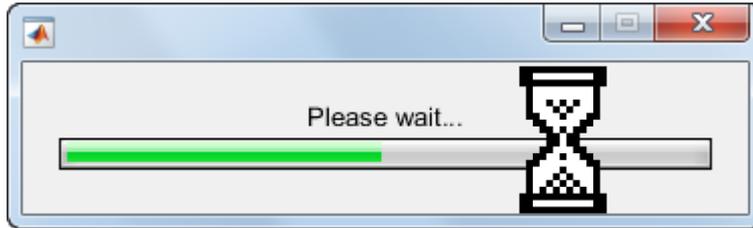


Сервера и АРМы

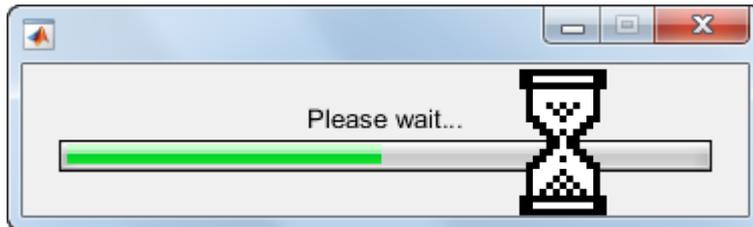
# Devastation



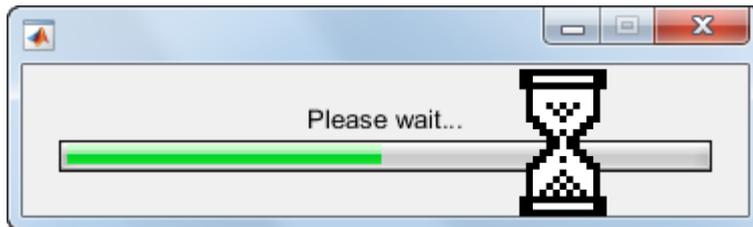
# Восстановление



Периметр



Внутренняя  
сеть



Сервера и  
АРМы

# «Всё хорошо» ?



WEB

Mail

VPN

Периметр

Сегмент  
АРМов

CORE

Сегмент  
серверов

Внутренняя  
сеть

Admin

User



AD

Приложения,  
БД

Сервера и  
АРМы

# Advanced Persistent Threat

- Бессистемность
- Беспечность
- **Беззащитность**



# Что делать ?

- Системный подход
- Комплексные меры
- **Защищённость**



# Как делать ?

- Лучшие мировые практики кибербезопасности
- Международные стандарты
- Отраслевые требования

## Framework for Improving Critical Infrastructure Cybersecurity

ISA99: Developing the ISA/IEC 62443 Series of Standards on  
*Industrial Automation and Control Systems (IACS) Security*

Version 1.0

Institute of Standards and Technology

Министерства энергетики

Республики Казахстан

от «25» октября 2016 года

№ 457

Политика информационной безопасности  
Министерства энергетики Республики Казахстан

# Как делать ?

## Акценты из опыта

- Не надейтесь на периметр – специально собранный для конкретной атаки malware пройдёт его
- Усиливайте защиту Active Directory – очень трудно восстанавливать службу после компрометации (в некоторых случаях невозможно)
- Создавайте выделенную сеть управления – с выносом в отдельный физ. сегмент и защитой по мотивам NIST SP 800-82

# Чем делать ?

IT-department responsibility

Mixed responsibility

Security Service responsibility

Tier 4: Adaptive



Tier 3: Repeatable



Tier 2: Risk Informed



Tier 1: Partial



Cybersecurity Framework Maturity Level

# С кем делать?

- Мы – знаем как восстанавливать
- Мы – знаем как предотвращать

***Пишите!***

***Звоните!***

***Спрашивайте!***

## Контакты:

Phone: +7 (727) 323 61 76

Email: [info@incom.com.kz](mailto:info@incom.com.kz)

Web: <http://incom.com.kz>



Incom.Kazakhstan

***INCOM***



# Спасибо за внимание!



## Контакты:

Phone: +7 (727) 323 61 76

Email: [info@incom.com.kz](mailto:info@incom.com.kz)

Web: <http://incom.com.kz>



Incom.Kazakhstan

# **INCOM**

