Информационная безопасность в 2023 году

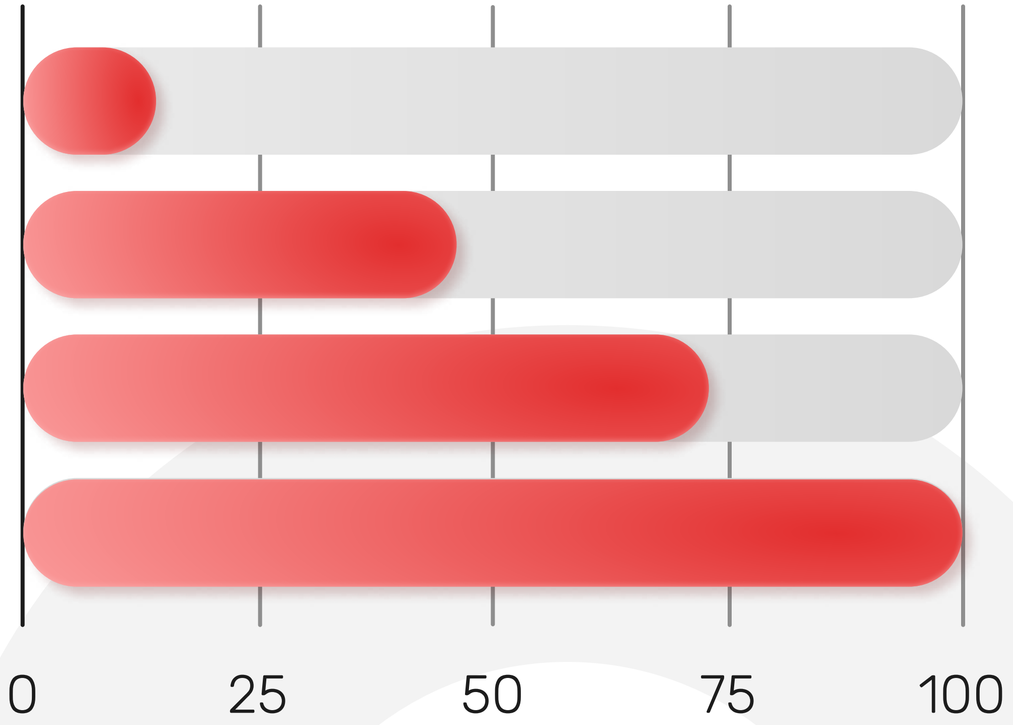
От кого и каким образом защищать информацию

Дмиртий Кибенко 12’2022

I Кто вас атакует?

Профиль нарушителя

- Вероятность и опасность успешной атаки



Сканы из интернета

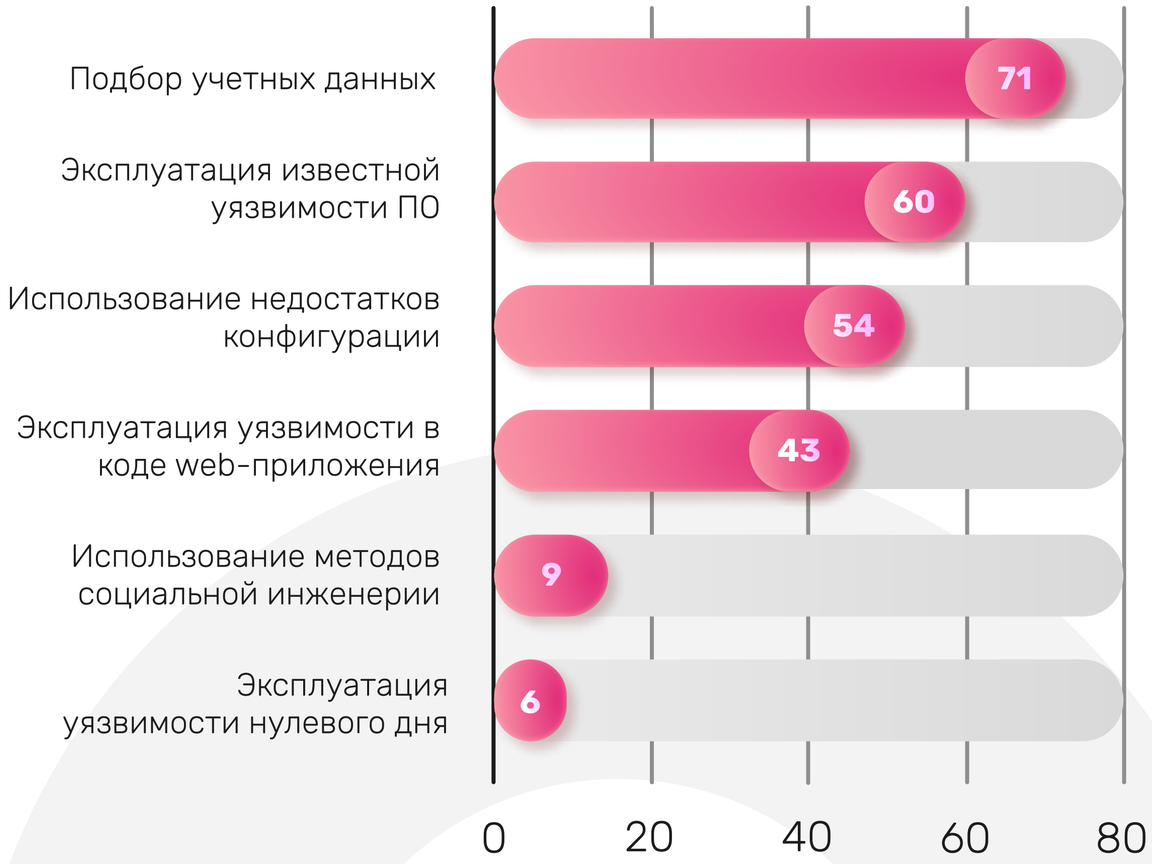
Небольшие группировки

Подготовленные команды хакеров

Штатные государственные команды хакеров

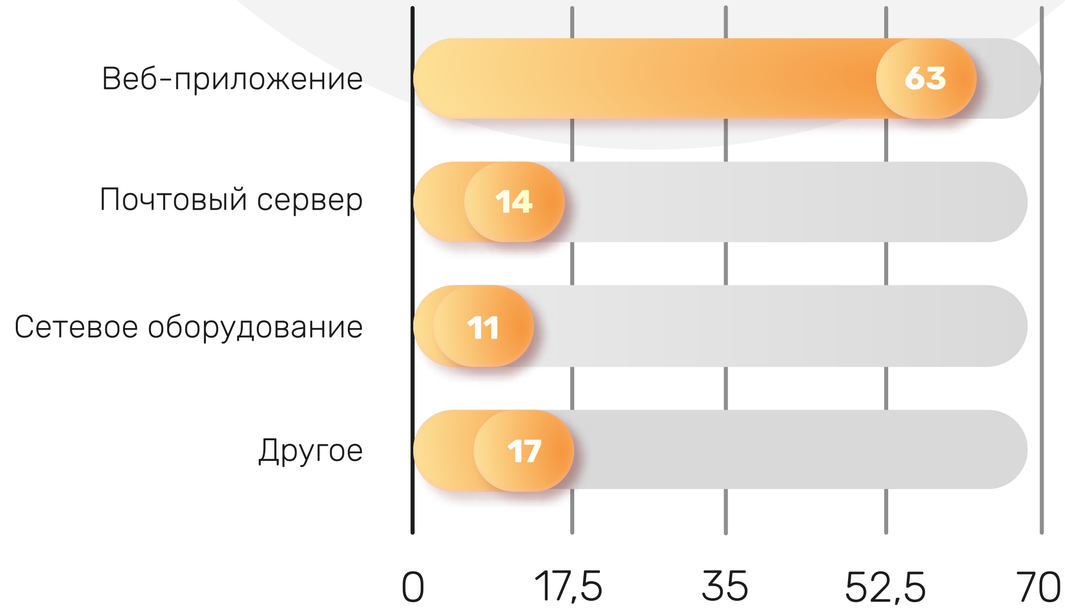
Статистика способов проникновения

Методы проникновения в локальную сеть (доля компаний)



вероятность эксплуатации уязвимости, %

Точки проникновения в корпоративную сеть компаний (доля компаний)



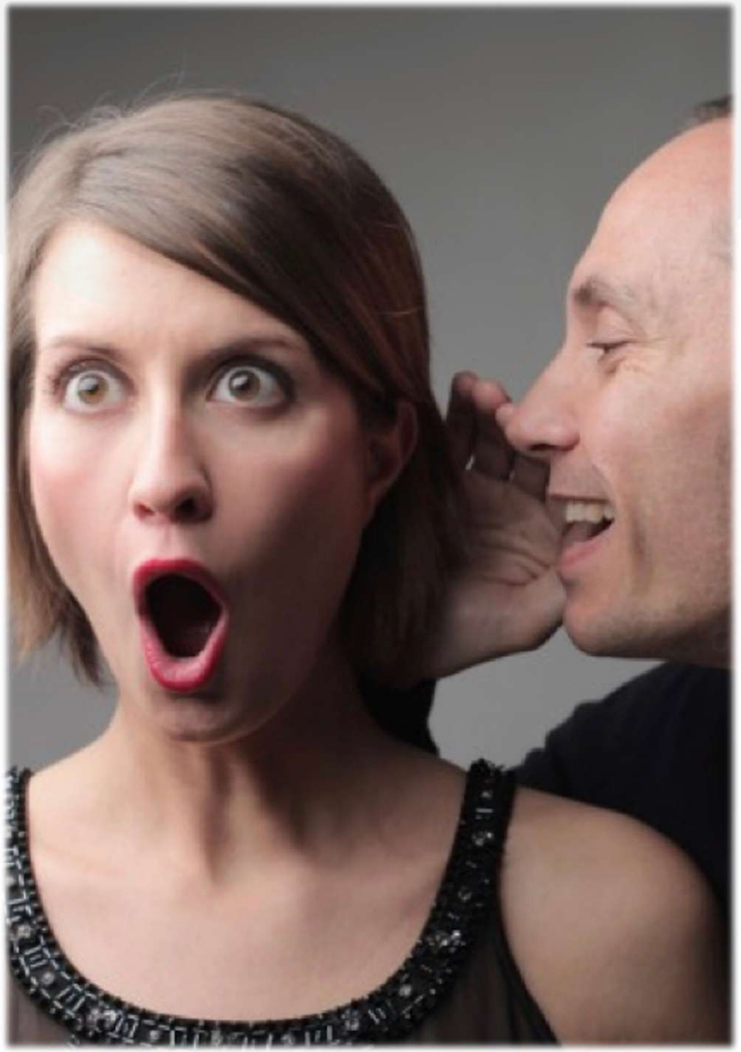
вероятность эксплуатации уязвимости, %

www.ptsecurity.com/ru-ru/research/analytics/pentests-2021-attack-scenarios/

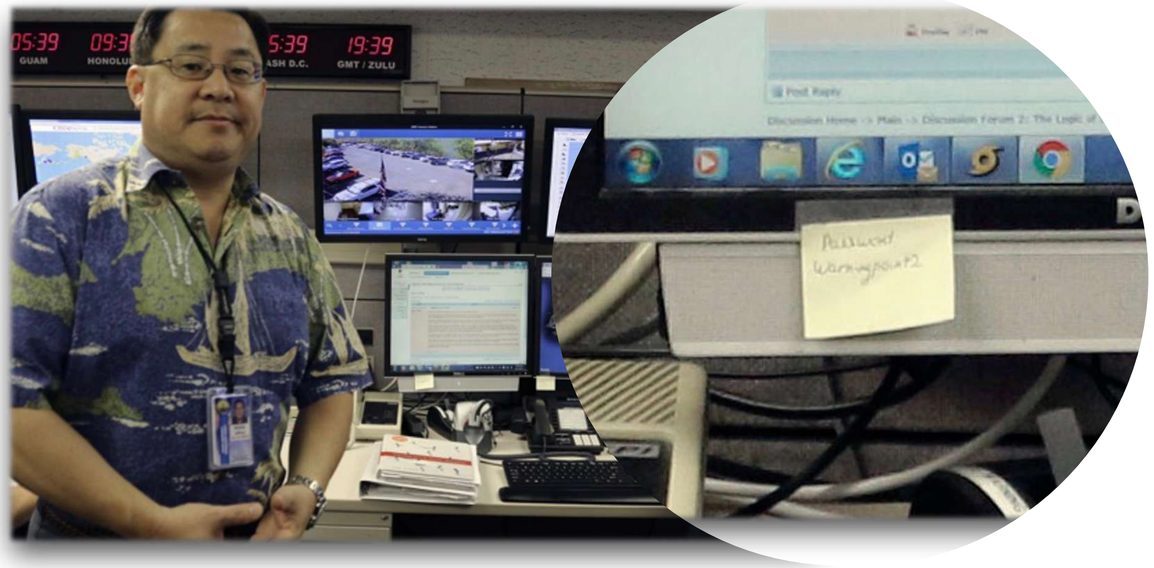
I Типовой сценарий атаки

Последовательность действий нарушителя
при проведении атаки на информационную систему

- **Сбор данных о системе**
- **Сканирование периметра сети**
- **Эксплуатация уязвимостей на периметре**
- **Социальная инженерия и фишинг**
- **Проникновение во внутренний контур**
- **Повышение привилегий**
- **Реализация атаки**



Разведка на основе открытых данных OSINT

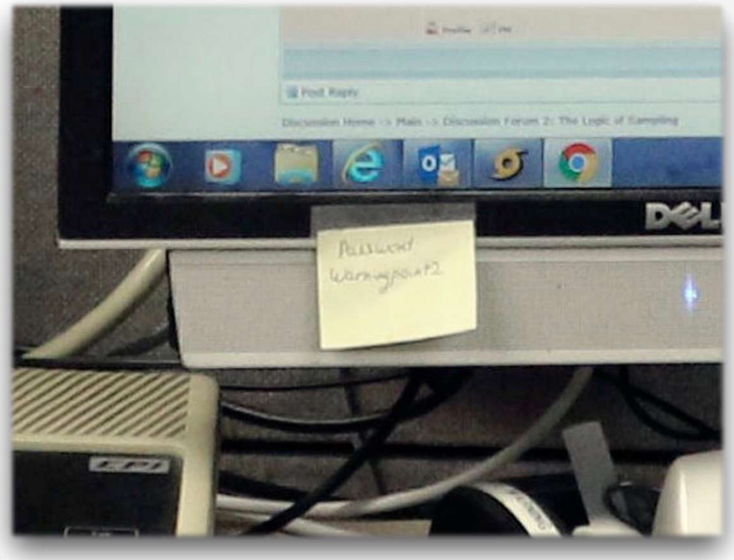


Google Dork

FEAR THE FOCA

GitHub

Разведка на основе открытых данных OSINT



GitHub

FEAR THE FOCA

Google Dork

Регулярный анализ открытой информации

Обучение и консультирование пользователей

I Сканирование периметра сети

I Сканирование периметра сети

Фильтрация ICMP

Архитектура с ДМЗ

Межсетевой экран + IPS

Авторизованные VPN

Эксплуатация уязвимостей на периметре

Cisco ASA CVE-2020-3452

Чтение произвольных файлов

ProxyLogon ProxyShell

Уязвимости в Microsoft Exchange остаются непропатченными годами

Bitrix 1 day CVE-2022-27228

RCE в модуле Bitrix Vote

Wireless

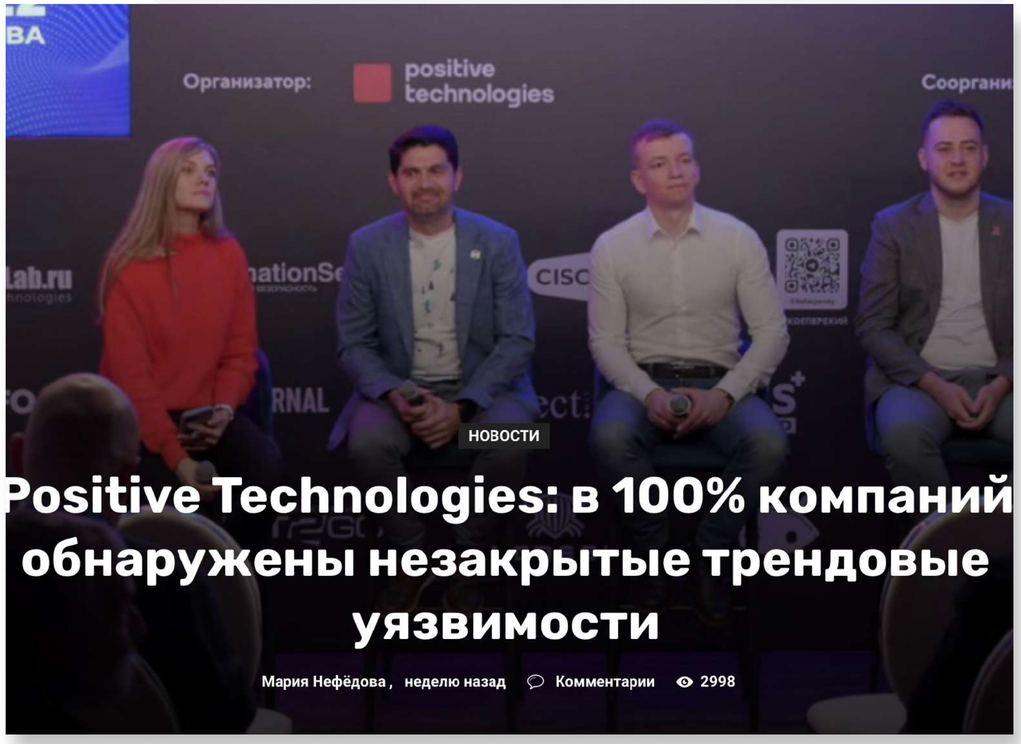
Слабая авторизация в беспроводной сети, доступ ко внутренней инфраструктуре из Wi-Fi

Log4Shell

Массовое сканирование спустя 10-20 часов после публикации

SQL/WEB 0day

Уязвимости собственных приложений



Эксплуатация уязвимостей на периметре

Cisco ASA CVE-2020-3452

Чтение произвольных файлов

ProxyLogon ProxyShell

Уязвимости в Microsoft Exchange остаются непропатченными годами

Bitrix 1 day CVE-2022-27228

RCE в модуле Bitrix Vote

Wireless

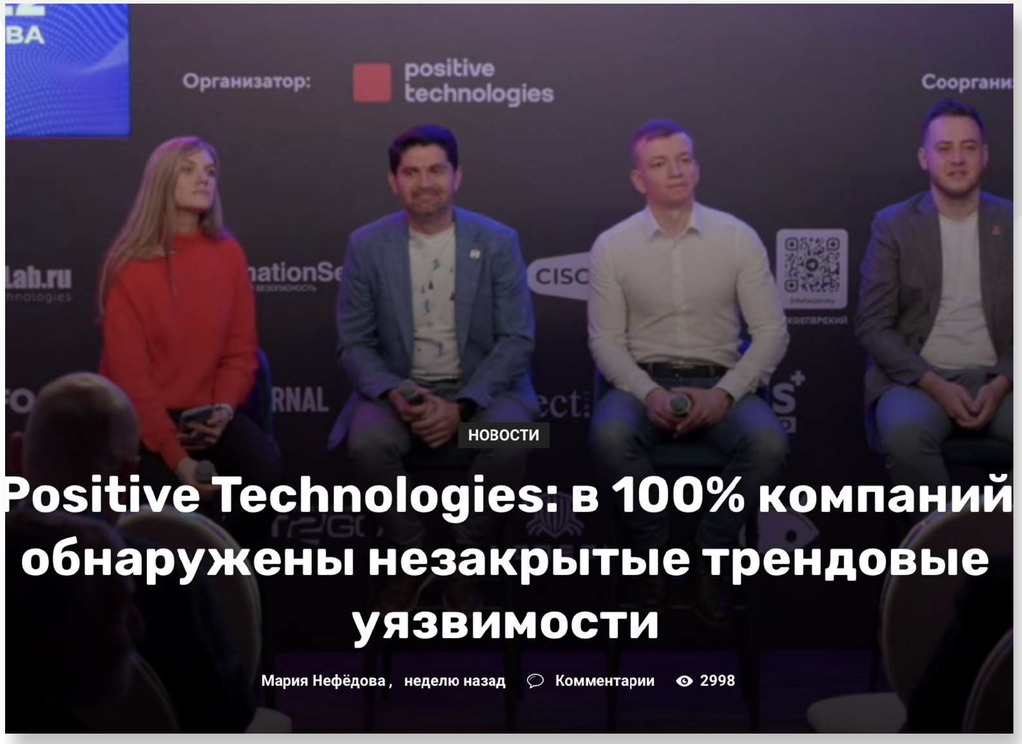
Слабая авторизация в беспроводной сети, доступ ко внутренней инфраструктуре из Wi-Fi

Log4Shell

Массовое сканирование спустя 10-20 часов после публикации

SQL/WEB 0day

Уязвимости собственных приложений



Регулярное сканирование ПО и кода на уязвимости

Оперативное обновление ПО при появлении CVE

NGFW/ Web Application FW Web - шлюзы

Социальная инженерия. Фишинг.

Вредоносные вложения

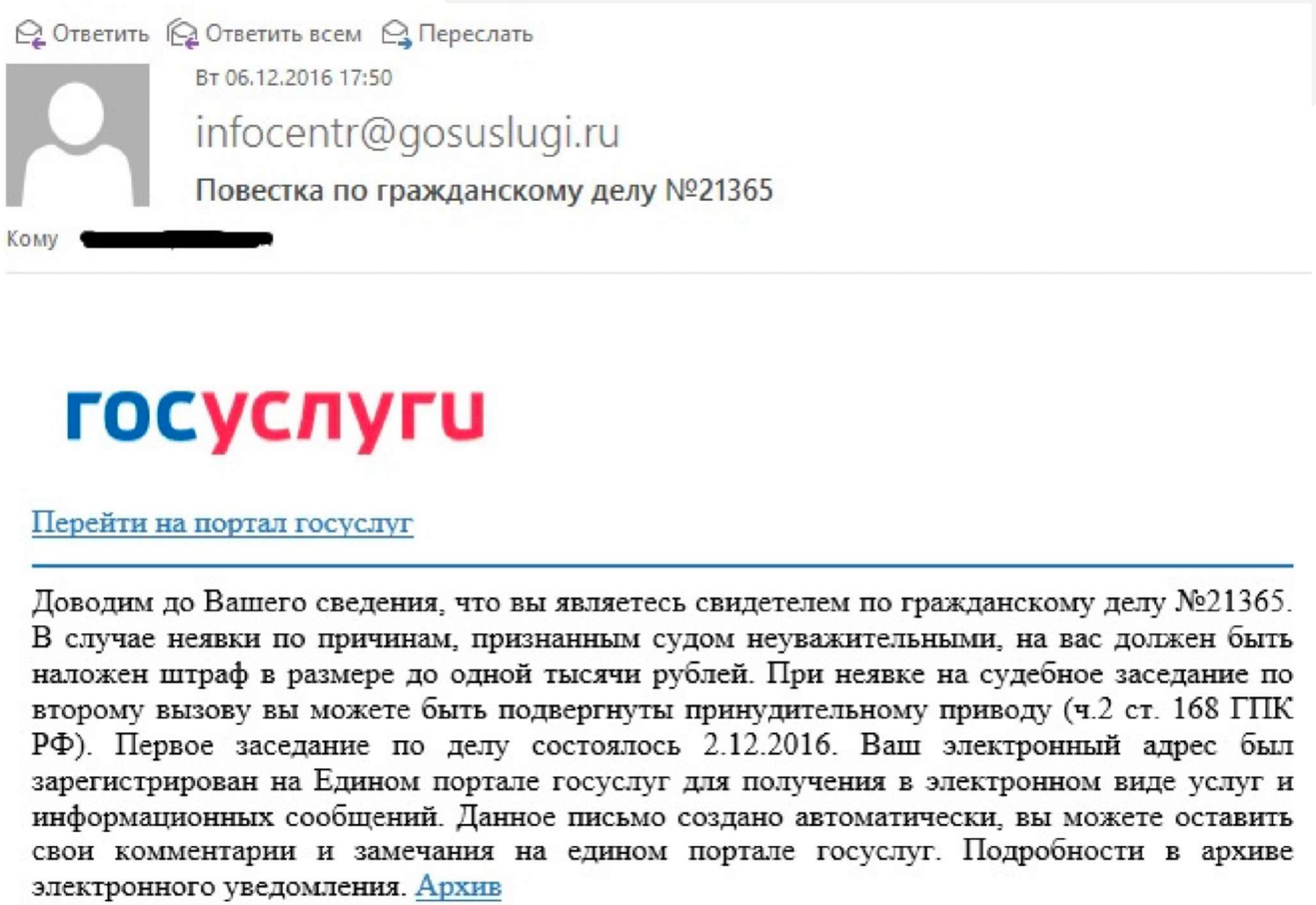
Вредоносное программное обеспечение, эксплойты для офисных приложений. Требуют большой подготовки и легко обнаруживаются

Вредоносные ссылки

Ссылки на вредоносные файлы и эксплойты. стилизованные под популярные сервисы и ПО. Используются для обхода антивирусных средств и почтовых шлюзов

Фишинг

Ссылки на формы аутентификации, стилизованные под сервисы компании. Используются для перехвата учетных данных.



Ответить Ответить всем Переслать

Вт 06.12.2016 17:50

infocentr@gosuslugi.ru

Повестка по гражданскому делу №21365

Кому [redacted]

госуслуги

Перейти на портал госуслуг

Доводим до Вашего сведения, что вы являетесь свидетелем по гражданскому делу №21365. В случае неявки по причинам, признанным судом неуважительными, на вас должен быть наложен штраф в размере до одной тысячи рублей. При неявке на судебное заседание по второму вызову вы можете быть подвергнуты принудительному приводу (ч.2 ст. 168 ГПК РФ). Первое заседание по делу состоялось 2.12.2016. Ваш электронный адрес был зарегистрирован на Едином портале госуслуг для получения в электронном виде услуг и информационных сообщений. Данное письмо создано автоматически, вы можете оставить свои комментарии и замечания на едином портале госуслуг. Подробности в архиве электронного уведомления. Архив

Социальная инженерия. Фишинг.

Вредоносные вложения

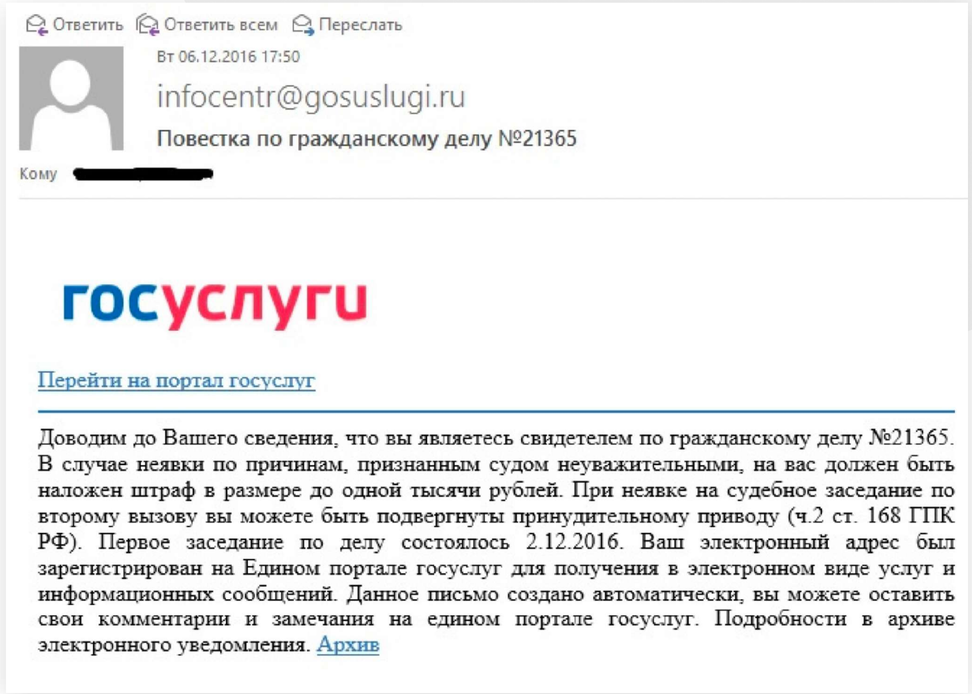
Вредоносное программное обеспечение, эксплойты для офисных приложений. Требуют большой подготовки и легко обнаруживаются

Вредоносные ссылки

Ссылки на вредоносные файлы и эксплойты. стилизованные под популярные сервисы и ПО. Используются для обхода антивирусных средств и почтовых шлюзов

Фишинг

Ссылки на формы аутентификации, стилизованные под сервисы компании. Используются для перехвата учетных данных.


Ответить Ответить всем Переслать

Вт 06.12.2016 17:50

infocentr@gosuslugi.ru

Повестка по гражданскому делу №21365

Кому [redacted]

госуслуги

Перейти на портал госуслуг

Доводим до Вашего сведения, что вы являетесь свидетелем по гражданскому делу №21365. В случае неявки по причинам, признанным судом неуважительными, на вас должен быть наложен штраф в размере до одной тысячи рублей. При неявке на судебное заседание по второму вызову вы можете быть подвергнуты принудительному приводу (ч.2 ст. 168 ГПК РФ). Первое заседание по делу состоялось 2.12.2016. Ваш электронный адрес был зарегистрирован на Едином портале госуслуг для получения в электронном виде услуг и информационных сообщений. Данное письмо создано автоматически, вы можете оставить свои комментарии и замечания на едином портале госуслуг. Подробности в архиве электронного уведомления. Архив

Антивирусное ПО

Web шлюзы

Настройка почтовых шлюзов

Песочницы

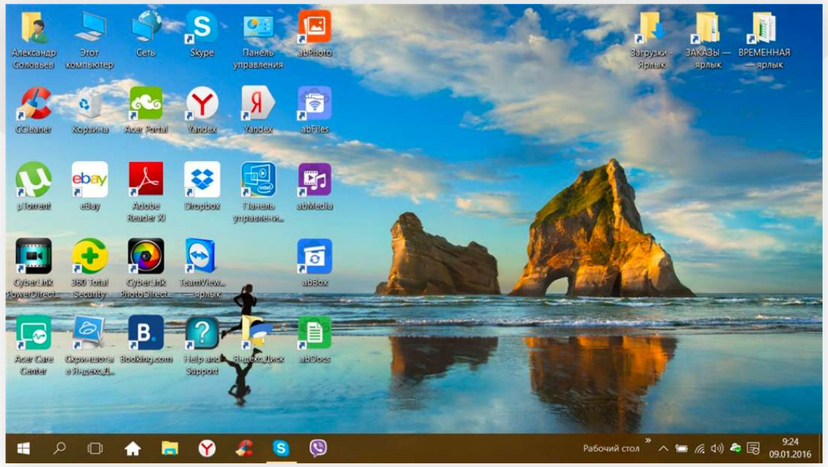
Специализированные программы обучения персонала

Проникновение во внутренний контур

```
Администратор: Windows PowerShell
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)

PS C:\Windows\system32> cd C:\Users\MiA1\Downloads\PSTools\
PS C:\Users\MiA1\Downloads\PSTools> .\psexec \\HACKWARE-SERVER -u Администратор -p Aa1 ipconfig

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Настройка протокола IP для Windows


Адаптер Ethernet Ethernet:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::58ff:c68d:cfc4:7428%13
   IPv4-адрес. . . . . . . . . . . . : 192.168.0.53
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . . . : 192.168.0.1
ipconfig exited on HACKWARE-SERVER with error code 0.
PS C:\Users\MiA1\Downloads\PSTools>
```

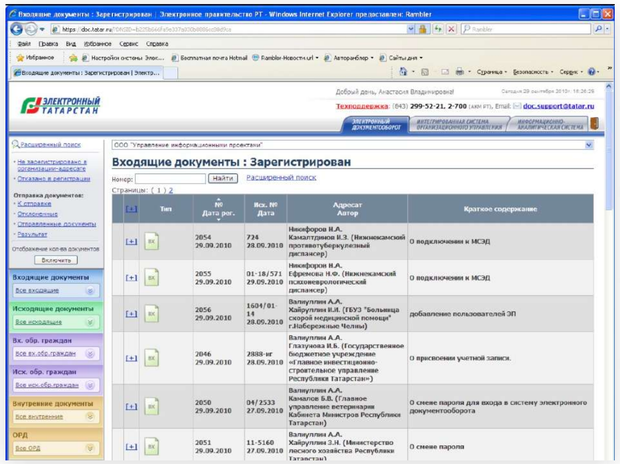
PSExec

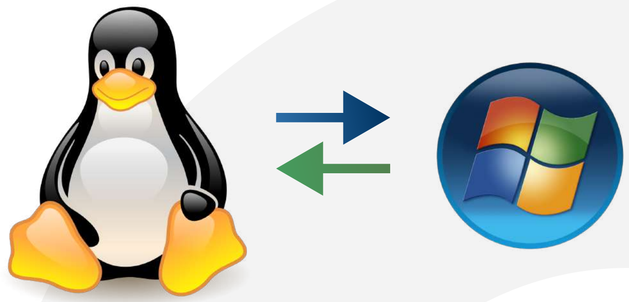
Ваши админы используют эту утилиту командной строки, с помощью нее можно запускать программы на удаленных Windows системах



RDP

Ваши админы и удаленные работники заходят на свои Windows ПК

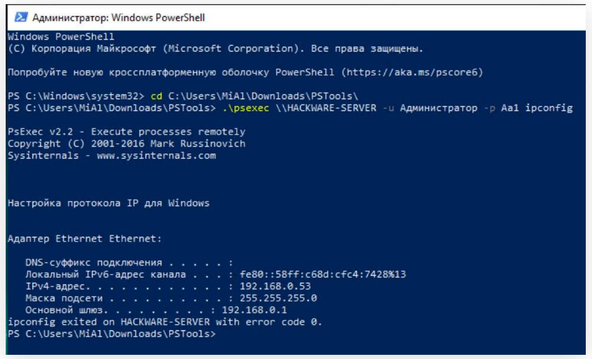




PSRemouting

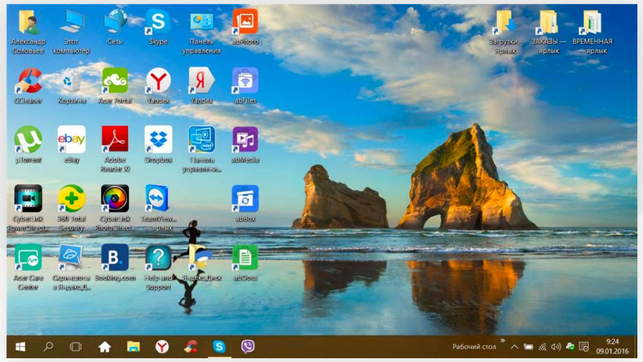
Логи и телеметрия могут отправляться через powershell remoting

Проникновение во внутренний контур



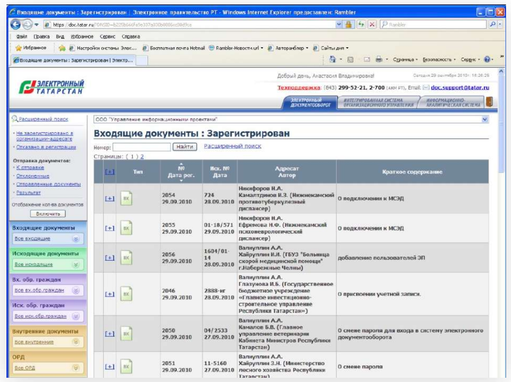
PSExec

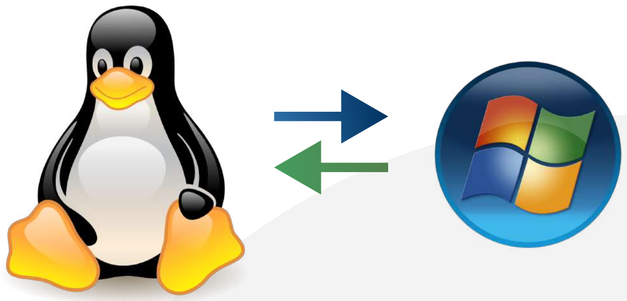
Ваши админы используют эту утилиту командной строки, с помощью нее можно запускать программы на удаленных Windows системах



RDP

Ваши админы и удаленные работники заходят на свои Windows ПК





PSRemouting

Логи и телеметрия могут отправляться через powershell remoting

Двухфакторная и/или многоступенчатая аутентификация

VPN | PAM | SIEM | UEBA | IPS | NAT

Проникновение во внутренний контур

Secure Socket Funnelling

Практически любые виды тоннелей внутри TLS соединения до соседнего хоста или сервера атакующих

SSH

Классика построение тоннелей

CnC

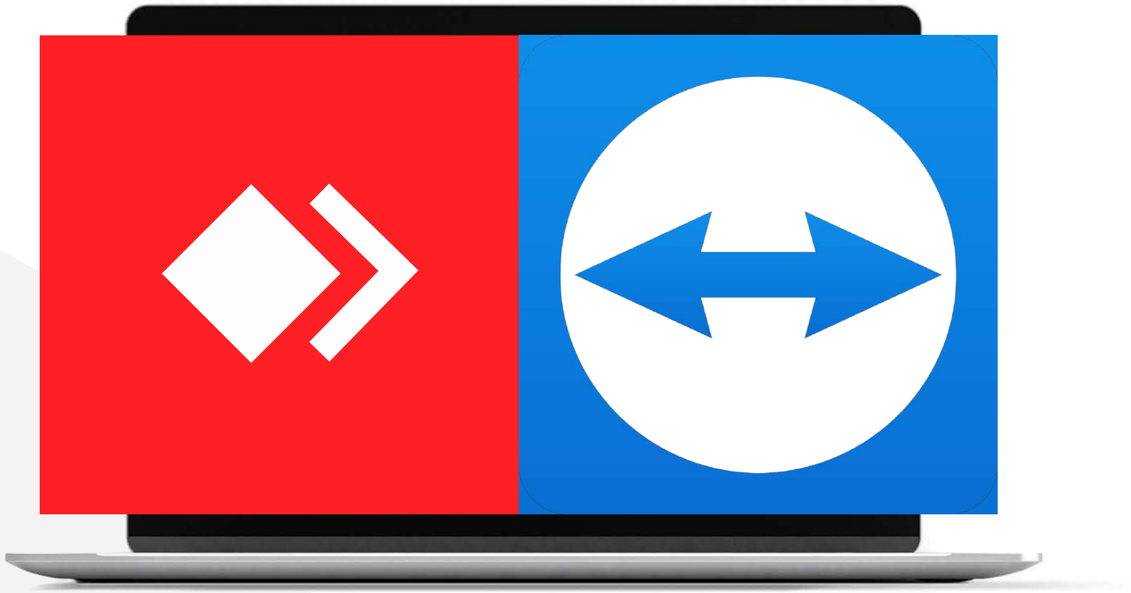
Фреймворки для построения цепочки атак и коммуникации с зараженными хостами. Cobalt Strike, Bruteratel

Teamviwer

AnyDesk, Ammyy и др.
Будут использованы против вас

DNS и ICMP

Туннелирование траффика внутри жизненно необходимых протоколов. Используется когда остальные протоколы запрещены



Проникновение во внутренний контур

Secure Socket Funnelling

Практически любые виды тоннелей внутри TLS соединения до соседнего хоста или сервера атакующих

SSH

Классика построение тоннелей

DNS и ICMP

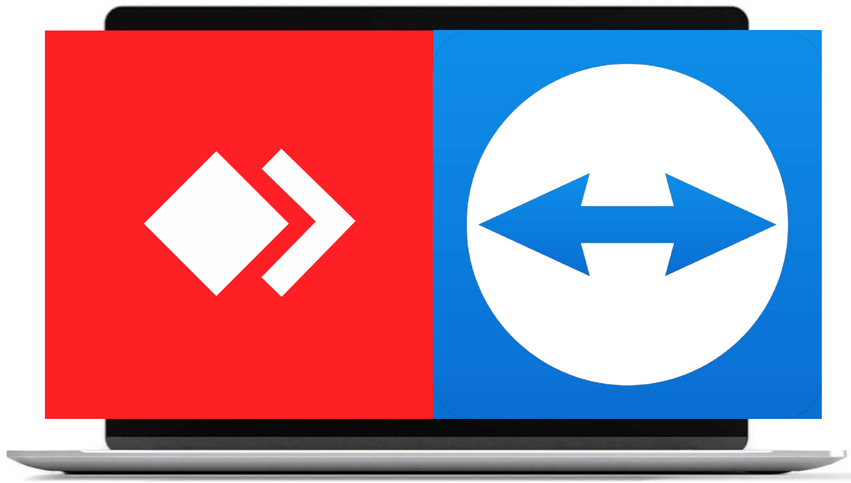
Туннелирование траффика внутри жизненно необходимых протоколов. Используется когда остальные протоколы запрещены

CnC

Фреймворки для построения цепочки атак и коммуникации с зараженными хостами. Cobalt Strike, Bruteratel

Teamviwer

AnyDesk, Ammyy и др.
Будут использованы против вас



Ограничение на установку нежелательного ПО

Двухфакторная и/или многоступенчатая аутентификация

VPN

SIEM

IPS

PAM

UEBA

NAT

Что сделано?

Единий контур информационной безопасности ГИС

Межсетевой экран + IPS

Крипто кластер VPN/TLS ГОСТ

Мониторинг

SIEM

Антивирусная защита

Сканирование на уязвимости

Архитектура с ДМЗ

Двухфакторная аутентификация

Web шлюзы

Что сделано?

Единий контур информационной безопасности ГИС

- Межсетевой экран + IPS
- Крипто кластер VPN/TLS ГОСТ
- Мониторинг
- SIEM
- Антивирусная защита
- Сканирование на уязвимости
- Архитектура с ДМЗ
- Двухфакторная аутентификация
- Web шлюзы

Что запланировано на 2023 год?

- Подключение новых ГИС к единому контуру ИБ
- Подключение пользователей к ГИС через единый контур безопасности

- WAF
- SandBOX
- PAM
- NAT
- IRP
- Обучение пользователей

Вопросы?

Дмиртий Кибенко 12’2022
(843) 2 100 488
vrca.ru