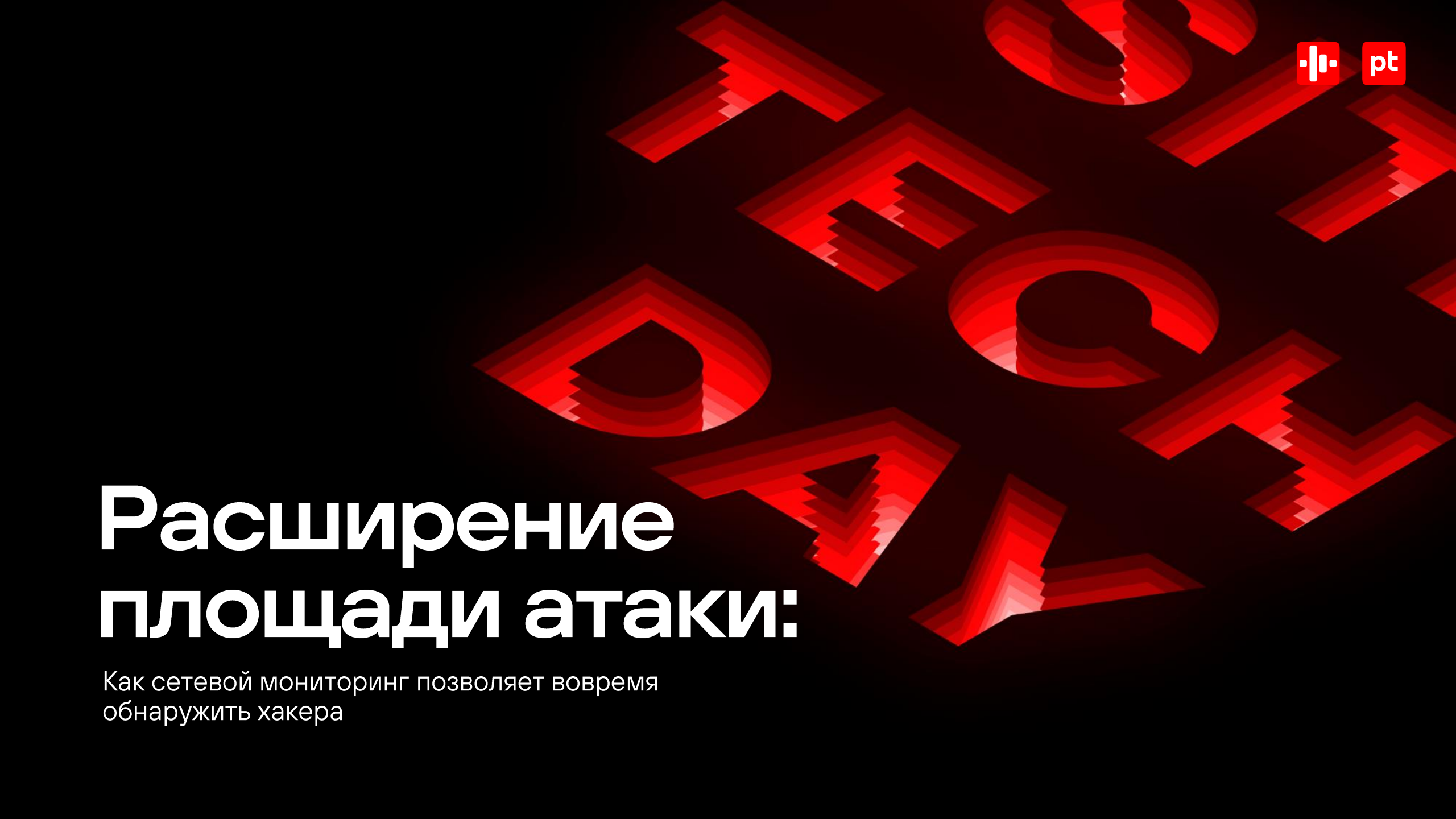


Расширение площади атаки:

Как сетевой мониторинг позволяет вовремя обнаружить хакера

Всем привет!

Игорь Тюкачев
Продаю PT NAD

+7 909 942 18 60

ityukachev@ptsecurity.com

Защиты периметра недостаточно

96%

компаний
не защищены
от внешних атак

От одного до семи дней

тратят
злоумышленники
на проникновение
во внутреннюю
сеть

в 100%

компаний
инсайдер может
контролировать
инфраструктуру

По данным исследования Positive Technologies «Итоги пентестов — 2023»

Как злоумышленник попадает в сеть

Сайты и приложения

В 50% случаев атакующие проникают в сеть через эксплуатацию уязвимостей сайта компании.
В 25% случаев — через эксплуатацию уязвимостей в почтовом сервисе

Легитимные действия

В компаниях **не контролируются** смена паролей, удаленное подключение к системе, сбор информации о сети, домене и пользователях, загрузка файла на сервер с помощью встроенных функций приложени

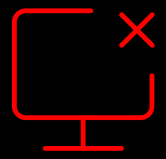
Подбор учетных данных

В 9 из 10 случаев атакующему удается подобрать пароль к учетной записи. Сотрудники компаний используют простые короткие и словарные пароли, нет двухфакторной аутентификации

По данным исследования Positive Technologies «Итоги пентестов — 2023»

Защита конечных узлов не помогает

Компании не всегда знают о своих активах: например, об оборудовании для тестирования, забытых виртуальных машинах и сетевых узлах



Не на все устройства можно установить защиту: незащищенными остаются принтеры, IoT, сетевое оборудование, BYOD-устройства, WinXP

Злоумышленники **научились скрываться** на конечных узлах и в некоторых случаях **отключать** средства защиты

Какие решения подходят

Системы анализа трафика

NTA-решения*

Разбирают трафик на периметре сети и в инфраструктуре

Предоставляют информацию, необходимую для расследования инцидентов

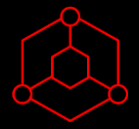
Выявляют атаки с помощью комбинации методов детектирования

* Network traffic analysis

PT NAD

Выявляет сложные сетевые атаки и сокращает время обнаружения хакеров в инфраструктуре

Упрощает расследование инцидентов и показывает слабые точки в сети



Сокращает время реагирования на приоритетные угрозы

РЕЗУЛЬТАТ

Сокращает время присутствия злоумышленника в сети **до считанных минут**

PT NAD позволяет предотвратить **недопустимое событие**

Недопустимые события

Недопустимое событие — событие, делающее невозможным достижение операционных и стратегических целей или приводящее к значительному нарушению основной деятельности организации в результате кибератаки.

Недопустимое событие	Порог ущерба
Остановка ключевого бизнес-процесса	Более 3% от годовой выручки
Остановка производственного процесса	Более чем на X часов
Вывод денежных средств	Более 15% от чистой прибыли
Утечка персональных данных клиентов	Неприменимо
Угроза жизни и здоровья людей	Неприменимо
Влияние на окружающую среду	Неприменимо

Чтобы
предотвратить
атаку, думай
как хакер!

План атаки/Kill chain — Разведка

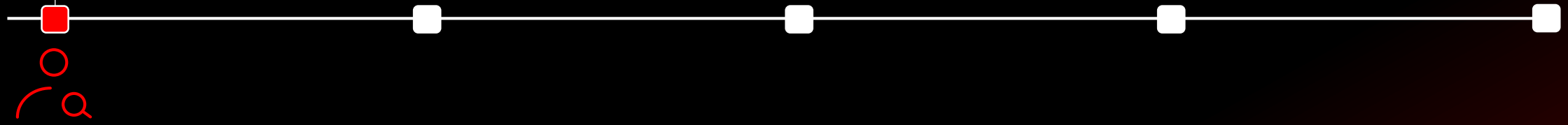
1 Разведка

Сбор данных о сотрудниках
e-mail, слитые пароли, открытые RDP, ФИО сотрудников и их данные

Сбор данных о компании
орг структура, график работы, бизнес-процессы, контрагенты

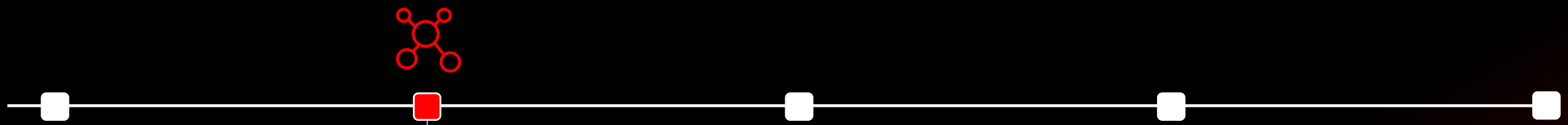
OSINT
Shoodan, maltego

Фишинг для сбора сведений



Это описание стандартных действий злоумышленников при атаке

План атаки/Kill chain — Подготовка



2 **Подготовка**

Найм экспертов
Ransomware as a service
Собственная разработка
Подготовка инфраструктуры

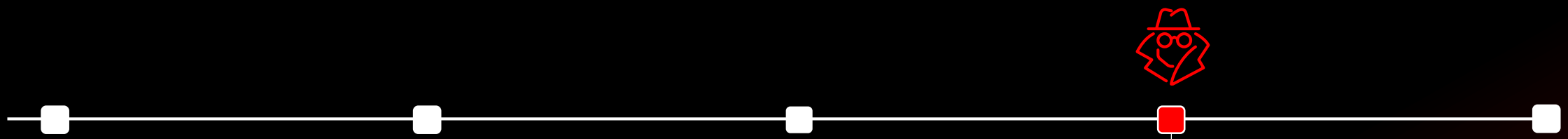
Это описание стандартных действий злоумышленников при атаке

План атаки/Kill chain — Первоначальный доступ

Фишинг
Уязвимости RDP и облачных хранилищ
Удаленное выполнение кода (RCE)
Уязвимости ПО
Взломанное веб-приложение
Брокеры доступа

Это описание стандартных действий злоумышленников при атаке

План атаки/Kill chain — Постэксплуатация



4 **Постэксплуатация**

Повышение привилегий
атака на контроллер домена (Metasploit, cobalt strike)

Обеспечение резервного доступа
распространение троянов и/или установка ПО удаленного управления — team viewer)

Горизонтальное перемещение
Исследование инфраструктуры

Кража данных
эксфильтрация, утечка (WinSCP, FileZilla и т.д.) в течение несколько месяцев

Это описание стандартных действий злоумышленников при атаке

План атаки/Kill chain — Развертывание ПО вымогателя

Удалить резервные копии

Остановить процесс резервного копирования

Обезвредить средства ИБ

Если средства ИБ это позволяют

Развернуть шифровальщика

на всех узлах с помощью групповых политик

5 **Развертывание ПО вымогателя**

Это описание стандартных действий злоумышленников при атаке

План атаки/Kill chain

1 Разведка

- Сбор данных о сотрудниках
- Сбор данных о компании
- OSINT
- Фишинг для сбора сведений

2 Подготовка

- Найм экспертов
- Ransomware as a service
- Собственная разработка
- Подготовка инфраструктуры

3 Первоначальный доступ

- Фишинг
- Уязвимости RDP и облачных хранилищ
- Удаленное выполнение кода (RCE)
- Уязвимости ПО
- Взломанное веб-
- приложение
- Брокеры доступа

4 Постэксплуатация

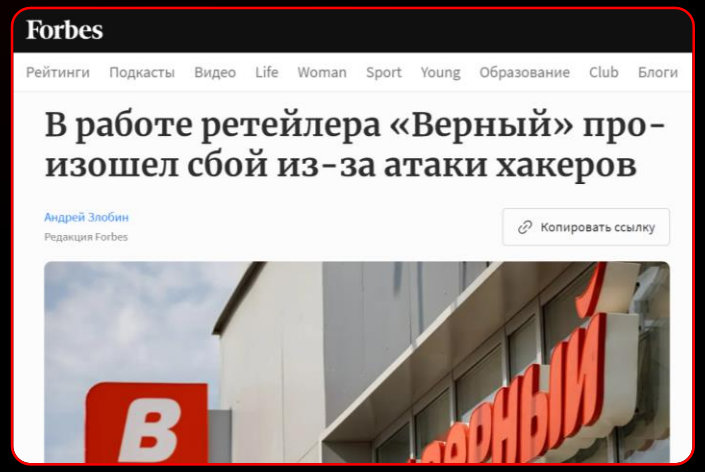
- Повышение привилегий
- Обеспечение резервного доступа
- Горизонтальное перемещение
- Кража данных

5 Развертывание ПО вымогателя

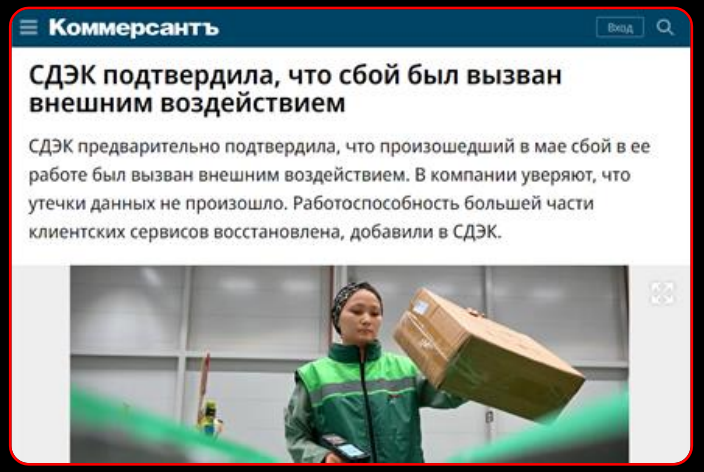
- Удалить резервные копии
- Обезвредить средства ИБ
- Развернуть шифровальщика

Это описание стандартных действий злоумышленников при атаке

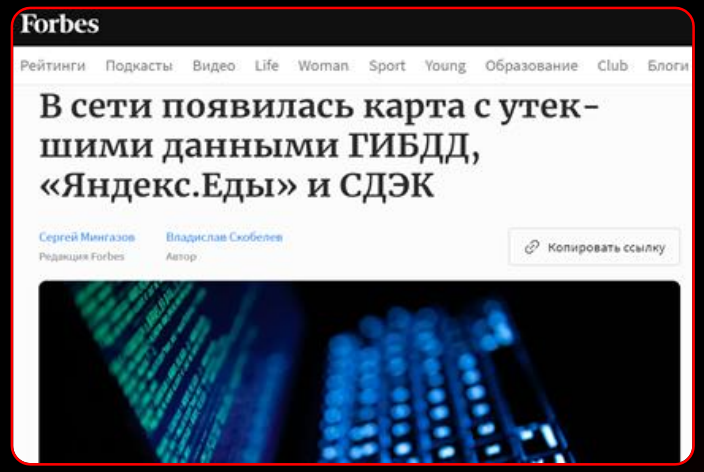
Последствия



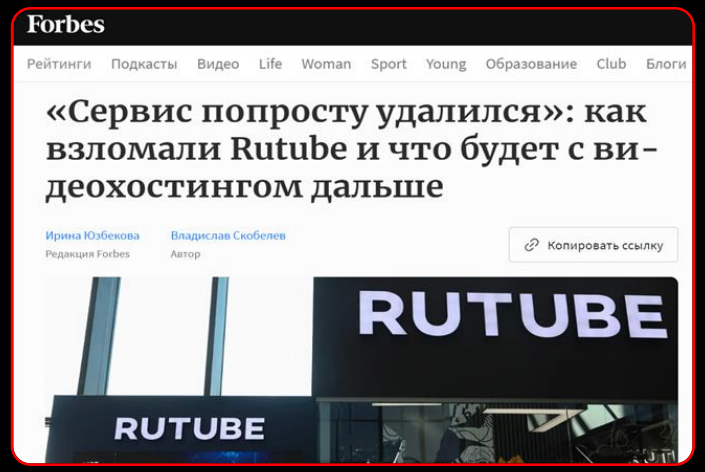
forbes.ru



kommersant.ru



forbes.ru



forbes.ru

bfm.ru

lenta.ru

Как обнаружить
с помощью PT NAD

План атаки/Kill chain — Первоначальный доступ

Фишинг

~~Уязвимости RDP и облачных хранилищ~~

~~Удаленное выполнение кода (RCE)~~

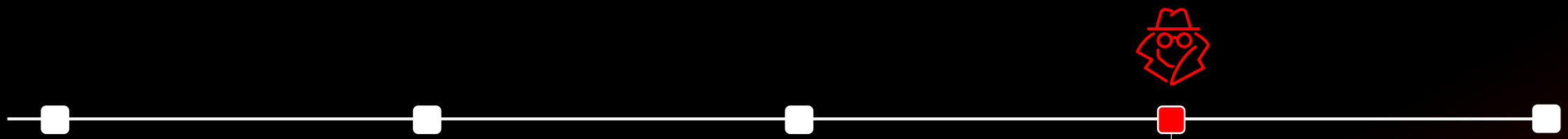
~~Уязвимости ПО~~

~~Взломанное веб-приложение~~

~~Брокеры доступа~~

Это описание стандартных действий злоумышленников при атаке

План атаки/Kill chain — Постэксплуатация



~~Повышение привилегий~~
атака на контроллер домена (Metasploit, cobalt strike)

~~Обеспечение резервного доступа~~
распространение троянов и/или установка ПО удаленного управления — team viewer)

~~Горизонтальное перемещение~~
Исследование инфраструктуры

~~Кража данных~~
эксфильтрация, утечка (WinSCP, FileZilla и т.д.) в течение несколько месяцев

4 **Постэксплуатация**

Это описание стандартных действий злоумышленников при атаке

План атаки/Kill chain — Развертывание ПО вымогателя

~~**Удалить резервные копии**~~

Остановить процесс резервного копирования

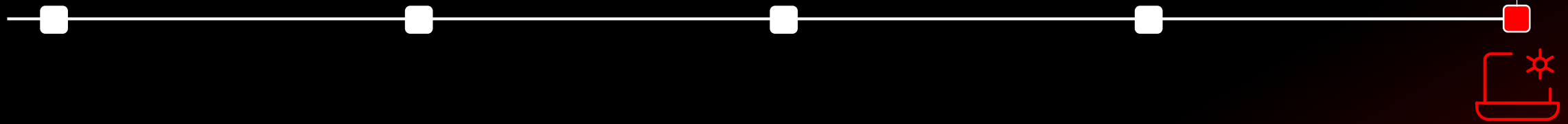
Обезвредить средства ИБ

Если средства ИБ это позволяют

~~**Развернуть шифровальщика**~~

на всех узлах с помощью групповых политик

5 **Развертывание ПО вымогателя**



Это описание стандартных действий злоумышленников при атаке

План атаки/Kill chain

1 Разведка

- Сбор данных о сотрудниках
- Сбор данных о компании
- OSINT
- Фишинг для сбора сведений

2 Подготовка

- Найм экспертов
- Ransomware as a service
- Собственная разработка
- Подготовка инфраструктуры

3 Первоначальный доступ PT NAD

- Фишинг
- Уязвимости RDP и облачных хранилищ
- RCE / Уязвимости ПО
- Взломанное веб-приложение
- Брокеры доступа

4 Постэксплуатация PT NAD

- Повышение привилегий
- Обеспечение резервного доступа
- Горизонтальное перемещение
- Кража данных

5 Развертывание ПО вымогателя PT NAD

- Удалить резервные копии
- Обезвредить средства ИБ
- Развернуть шифровальщика

Это описание стандартных действий злоумышленников при атаке

Отзывы

ОБЪЕДИНЕННАЯ ЭНЕРГЕТИЧЕСКАЯ КОМПАНИЯ

Антон Мельник,
начальник управления
ИБ АО «ОЭК»

PT NAD – полезный инструмент для мониторинга безопасности сети. После внедрения продукта мы почти моментально увидели первые результаты, которые помогли нам снизить риски безопасности и улучшить защищенность инфраструктуры

ГЕНБАНК

Дмитрий Ларин,
начальник управления
ИБ АО «ГЕНБАНК»

PT NAD – зафиксировал 5700 потенциальных угроз, включая 90 угроз высокой опасности. При этом результаты мониторинга сети «Генбанка» не выявили успешных проникновений в сеть организации.

Подробнее: ptsecurity.com/ru-ru/products/network-attack-discovery/#reviews

Полезные ссылки

Телеграм-чат
о PT NAD

t.me/PTNADChat

Дополнительные
материалы о PT NAD

clck.ru/33f7PP

Спасибо!