



**positive
security
day**



**Digital
Forensics and
Incident
Response**

**Почему хакеры сидят в сети
незамеченными 200 дней?
Мы пришли это исправить!**

Денис Батранков

руководитель направления сетевой безопасности



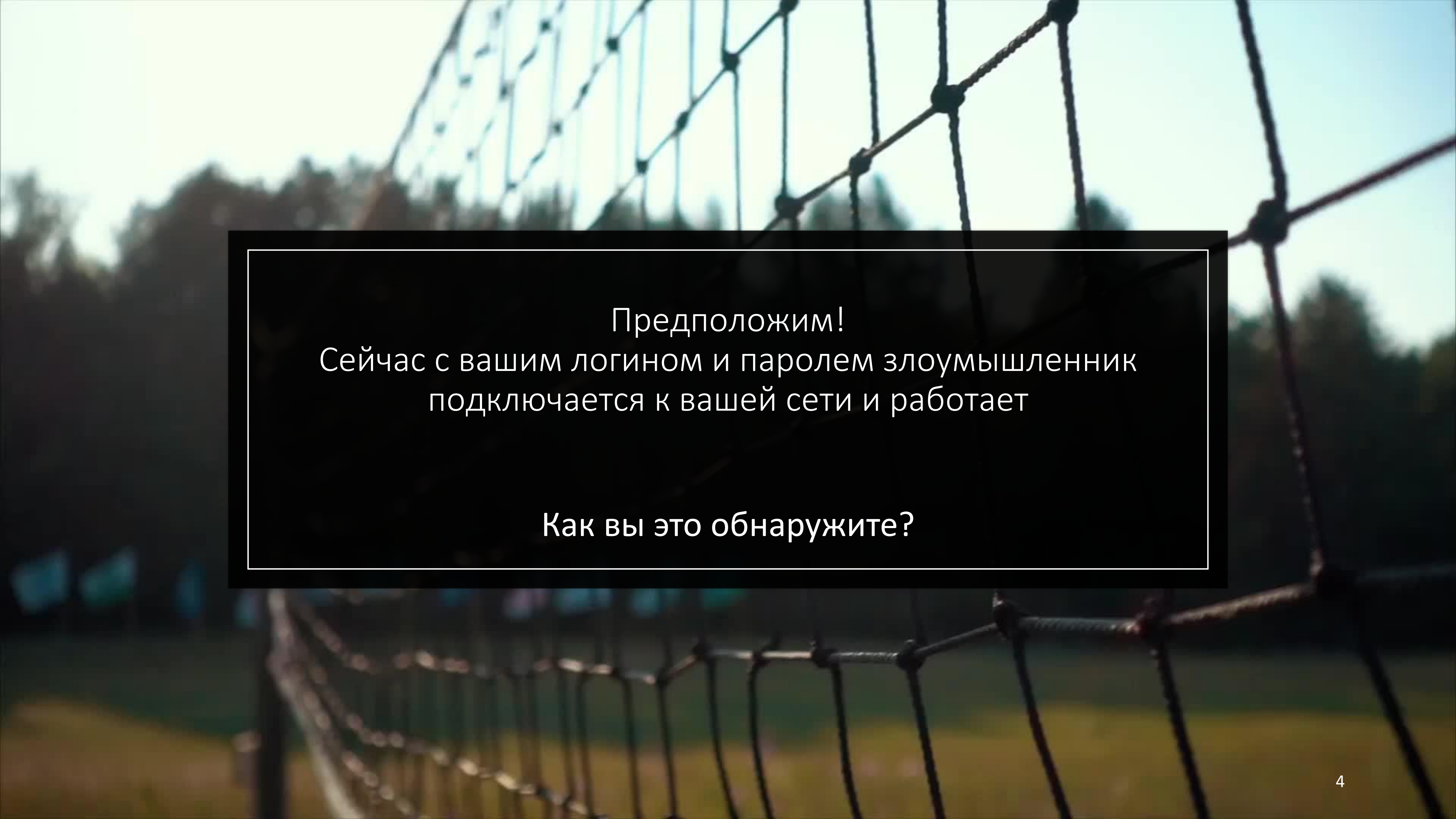
Результаты пентестов Positive Technologies 2021 и 2020 года

100%

Средства защиты работали!



У кого есть VPN доступ в
корпоративную сеть?



Предположим!
Сейчас с вашим логином и паролем злоумышленник
подключается к вашей сети и работает

Как вы это обнаружите?

Злоумышленники обнаружены внутри сети Cisco с правами администратора домена



- Проникли через кражу аккаунта Cisco VPN
- Проникли в мае, в августе опубликовали украденные данные
- Украдены инженерные чертежи (по сообщению BleepingComputer)
- Были обнаружены системой анализа внутреннего трафика (NTA)

From: [REDACTED]
Date: Saturday, July 30, 2022 at 8:51 AM
To: [REDACTED]
Subject: Re: Cisco incident 5/28

We are giving you a very good deal. no one will know about the incident and information leakage if you pay us.

June 13, 2022 7:17:02 PM CEST [REDACTED] wrote:
How are you?

June 3, 2022 9:27:46 AM CEST [REDACTED] wrote:

This is just the beginning, more to come.

01 Historical (Approved NDA Requests)	6/2/2022 12:20 PM
3DIT-Architecture Documents	6/2/2022 12:10 PM
Cisco AnyConnect Secure Mobility Client	6/2/2022 9:28 AM
Cisco Confidential Information Agree...	6/2/2022 12:07 PM
[REDACTED]	6/2/2022 11:51 AM
ECM Agile Data Governance Working Sp...	6/2/2022 12:05 PM
HW Playbook - IT Only	6/2/2022 12:06 PM
NDA_business_request_neslin.pptx	6/2/2022 12:09 PM
NDA_Solar	6/2/2022 12:17 PM
PLM Service Management	6/2/2022 12:06 PM
Schematic Modeling	6/2/2022 12:15 PM
[REDACTED]	6/2/2022 11:51 AM
[REDACTED]	6/2/2022 11:51 AM

19 способов проникновения в сеть компании

Каналы проникновения в организацию (примеры)



Электронная
почта

Веб-сервер

Уязвимости

Соседний
офис

Облачный
файлообменник

Облачные
ресурсы

USB флешки

Wi-Fi сеть

Взломанный
софт

Мобильные
устройства
и удаленные
рабочие места

Веб-
камеры и IoT

Контейнеризация
и вредоносные
контейнеры

Подрядчики

Watering Hole

Атаки на DNS

Среднее время проникновения
в сеть (результаты пентестов)

2 дня

Минимальное время

30 минут

Среднее время до обнаружения
(результаты исследований)

200 дней
2000–2022

Максимальное время

11 лет

9 из 10
компаний
взломаны

На протяжении
всего этого времени
хакеры имеют
доступ ко всей
корпоративной
информации

Портрет злоумышленников

➤ **Промышленный шпионаж**



➤ **Правительственные команды**



➤ **Хактивисты**



Проникнуть в инфраструктуру большинства компаний может даже низкоквалифицированный хакер.

В любую компанию можно проникнуть.

Служба безопасности Rutube не знала о хакерах в системе на протяжении двух месяцев

Хакеры взломали сервис еще в марте и два месяца изучали работу сервиса

Марина Тюняева (Бочкарёва) Анастасия Курашева

Прочту позже



Максим Стулов / Ведомости

Российский видеохостинг Rutube, массовый сбой которого произошел на 9 мая, взломали еще в марте, сообщил «Ведомостям» Денис Баранов, гендиректор компании Positive Technologies, которую Rutube привлек для расследования и устранения последствий инцидента.

Вы слышали про взлом RUTUBE?

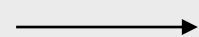
Хакеры взломали сервис и 2 месяца сидели внутри, а потом просто начали уничтожать их данные и виртуальные машины.

И это не единственный пример взломов этого года.

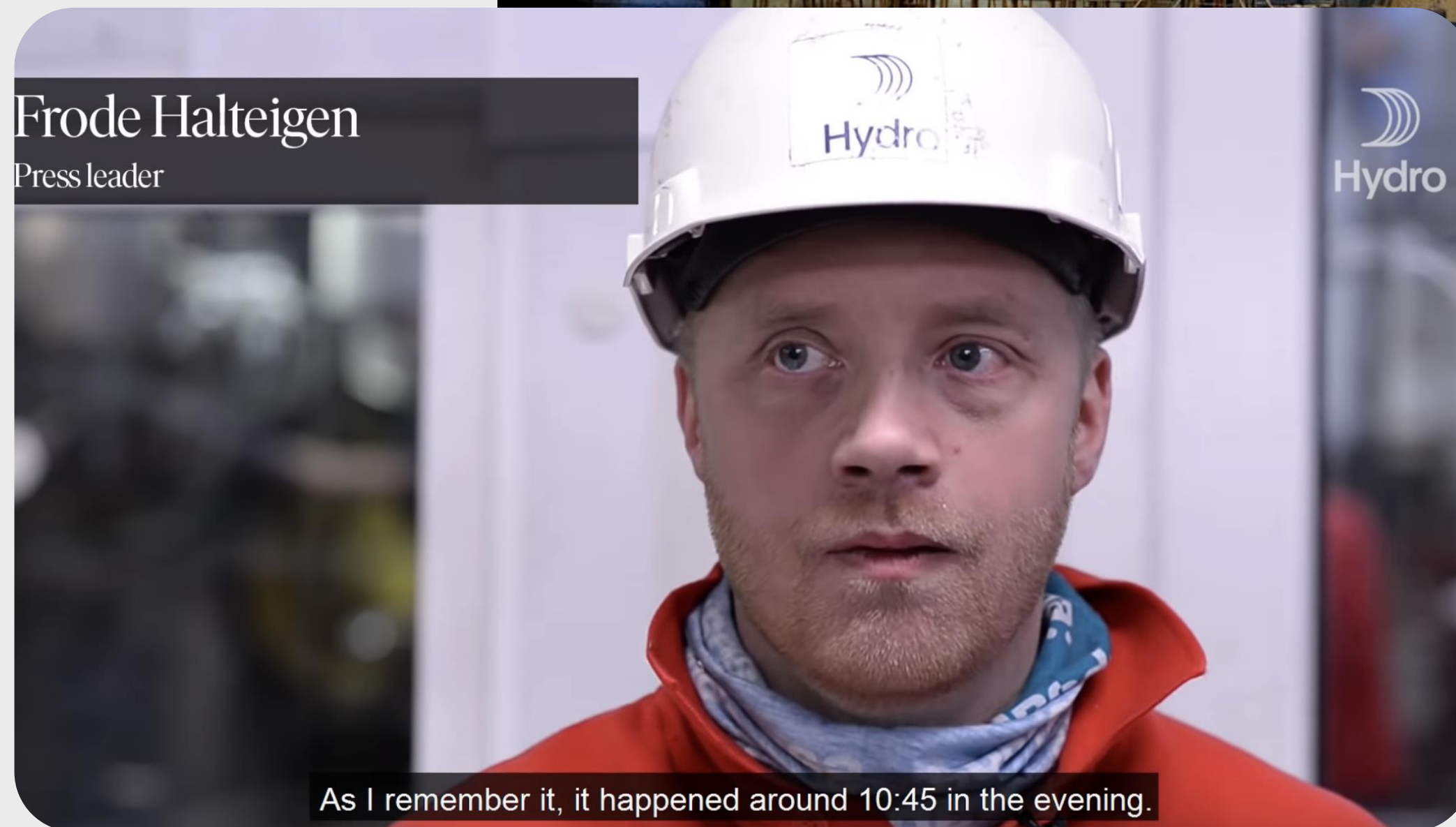
Норвежская
алюминиевая
компания атакована
18 марта 2019 в 22:45.

Вся компания с
35000 сотрудников
в **40 странах** по всем
160 адресам.

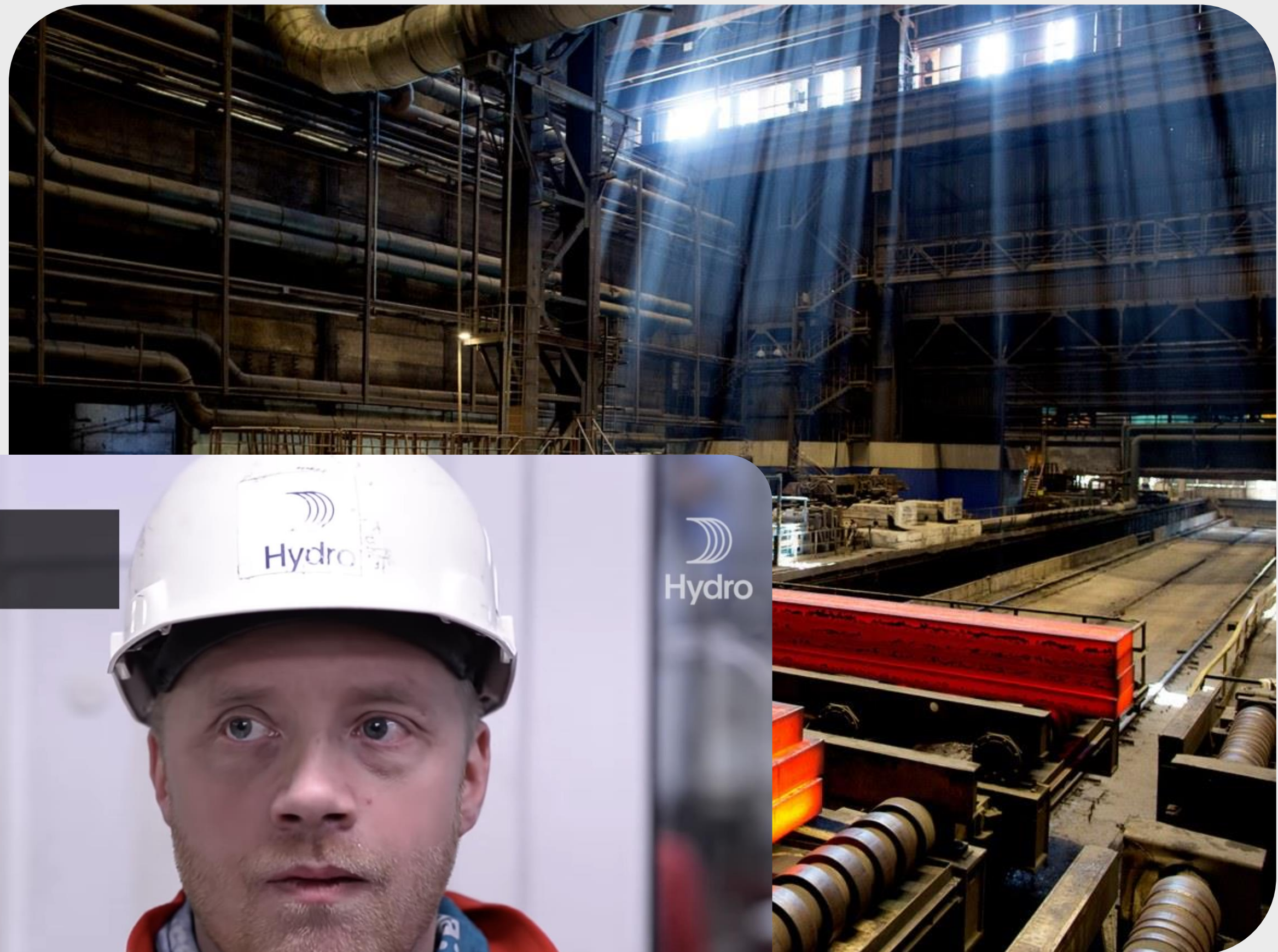
«Я помню,
что экран
системы
управления
погас в 22:45»



Frode Halteigen
Press leader



As I remember it, it happened around 10:45 in the evening.



Подробнее в видео самой компании:
youtube.com/watch?v=S-ZIVuM0we0

3 недели

**Хакеры находились в компании
до момента запуска криптолокера!**

Никто не заметил!

Почему молчали средства защиты?

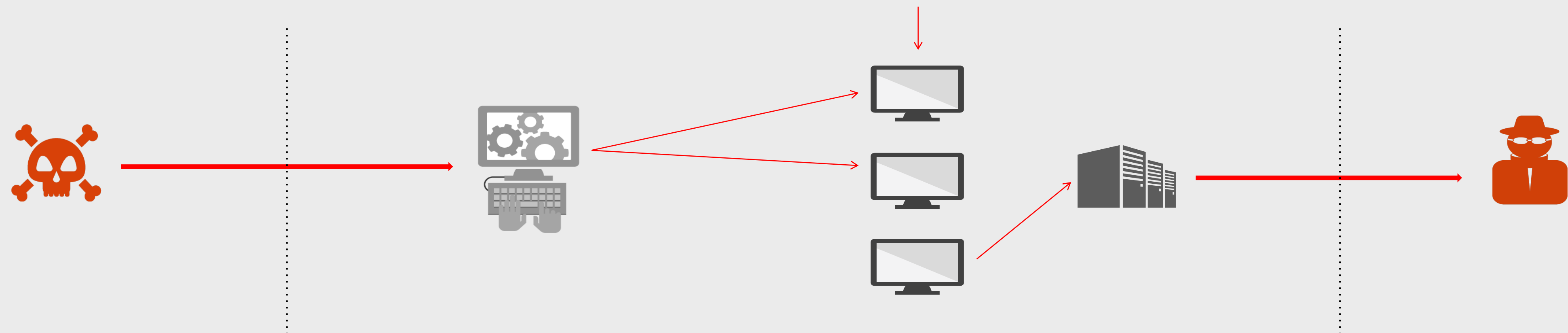


1 → Код LockerGoga был создан под конкретно эту компанию и у него было несколько вариантов. Активно противодействовал песочницам: в процессе запуска засыпал более 100 раз, не использовал сеть для распространения, не подключался к центру управления C&C

2 → **Взлом производится стандартными утилитами**

3 → Привилегии были повышены каким-то неизвестным способом. Можно предположить, что это Mimikatz и PathTheHash

Kill Chain или Пошаговый взлом





Покрываемые техники АТТ&СК

Разведка	Первоначальный доступ	Выполнение	Закрепление	Повышение привилегий	Предотвращение обнаружения	Получение учетных данных	Исследование	Перемещение внутри периметра	Сбор данных	Управление и контроль	Экспфильтрация данных	Воздействие
+ Активное сканирование (2/2)	Внешние службы удаленного доступа	+ Выполнение с участием пользователя (2/2)	Внешние службы удаленного доступа	+ Выполнение по событию (1/1)	+ Выполнение через подписанные бинарные файлы (2/2)	+ «Человек посередине» (1/1)	Запросы к реестру	+ Использование альтернативных данных для аутентификации (2/2)	+ «Человек посередине» (1/1)	+ Динамическое разрешение (1/1)	+ Экспфильтрация по альтернативному протоколу (1/1)	Несанкционированное использование ресурсов
Поиск уязвимостей	Доверительные отношения	Вредоносная ссылка	+ Выполнение по событию (1/1)	Подписка на события WMI	Установщик профилей диспетчера подключений (CMSTP)	Подмена LLMNR/NBT-NS-ответа и ретрансляция SMB	Исследование владельца или пользователей системы	Украденные хеш-значения учетных данных	Подмена LLMNR/NBT-NS-ответа и ретрансляция SMB	Алгоритмы генерирования доменных имен	Экспфильтрация по альтернативному протоколу без шифрования (с возможной обфускацией)	Остановка службы
Сканирование блоков IP-адресов	Недостатки в общедоступном приложении	Вредоносный файл	Подписка на события WMI	+ Запланированная задача (задание) (2/2)	Утилита mshta	+ Кража или подделка билетов Kerberos (4/4)	+ Исследование групп разрешений (1/1)	Украденный билет Kerberos	Данные с общих сетевых дисков	+ Зашифрованный канал (2/2)		
+ Сбор информации об атакуемых узлах (1/1)	+ Существующие учетные записи (3/3)	Планировщик заданий Windows	+ Запланированная задача (задание) (2/2)	Планировщик заданий Windows	+ Использование альтернативных данных для аутентификации (2/2)	«Прожарка» AS-REP	Доменные группы	+ Службы удаленного доступа (4/4)		Асимметричное шифрование	+ Экспфильтрация через веб-службу (2/2)	
Программное обеспечение	Доменные учетные записи	Утилита at (Windows)	Планировщик заданий Windows	Утилита at (Windows)	Украденные хеш-значения учетных данных	«Прожарка» Kerberos	Исследование доверительных отношений между доменами	SSH		Симметричное шифрование	Экспфильтрация в облачное хранилище	
	Локальные учетные записи	Инструментарий управления Windows	Утилита at (Windows)	+ Создание или изменение системных процессов (1/1)	Украденный билет Kerberos	Золотой билет Kerberos	Исследование конфигурации сети	VNC		+ Кодирование данных (0/0)	Экспфильтрация через репозиторий кода	
	Учетные записи по умолчанию	+ Использование интерпретаторов командной строки и сценариев (4/4)	+ Компонент серверного ПО (1/1)	Служба Windows	+ Обфусцированные файлы или данные (1/1)	Серебряный билет Kerberos	Исследование общих сетевых ресурсов	Общие SMB-ресурсы или ресурсы администраторов Windows		Нестандартный порт	Экспфильтрация через канал управления	
	Теневая (drive-by) загрузка	JavaScript/JScript	Веб-шелл	+ Существующие учетные записи (3/3)	Упаковка ПО	+ Метод перебора (0/0)	Исследование парольной политики	Протокол удаленного рабочего стола		Передача инструментов из внешней сети		
	+ Фишинг (2/2)	PowerShell	+ Манипуляции с учетной записью (0/0)	Доменные учетные записи	Поддельный контроллер домена	+ Незащищенные учетные данные (1/1)	Исследование процессов	Распределенная COM-модель		ПО для удаленного доступа		
	Целевой фишинг с вложением	Python	+ Создание или изменение системных процессов (1/1)	Локальные учетные записи	+ Существующие учетные записи (3/3)	Параметры групповой политики	Исследование системного времени	Служба удаленного управления Windows		+ Прокси-сервер (3/3)		
	Целевой фишинг со ссылкой	Visual Basic	Служба Windows	Учетные записи по умолчанию	Доменные учетные записи	+ Получение дампа учетных данных (4/4)	Исследование системных служб	Средства развертывания ПО		Внешний прокси-сервер		
		Командная оболочка Unix	+ Создание учетной записи (1/1)	Сценарии инициализации при загрузке или входе в систему (1/1)	Локальные учетные записи	DCSync	Исследование системы	Эксплуатация удаленных служб		Внутренний прокси-сервер		
		Командная оболочка Windows	Доменная учетная запись	+ Существующие учетные записи (3/3)	Учетные записи по умолчанию	Диспетчер учетных записей безопасности	Исследование удаленных систем			Цепочка прокси-серверов		
		+ Системные службы (1/1)	+ Существующие учетные записи (3/3)		Эксплуатация уязвимостей для предотвращения обнаружения	Секреты LSA	+ Исследование установленного ПО (1/1)			+ Протокол прикладного уровня (4/4)		
		Диспетчер управления службами	Доменные учетные записи			Содержимое файлов /etc/passwd и /etc/shadow	Исследование средств защиты			DNS		
		Средства развертывания ПО	Локальные учетные записи			Эксплуатация уязвимостей для получения учетных данных	+ Исследование учетных записей (1/1)			Веб-протоколы		
		Уязвимости в клиентском ПО	Учетные записи по умолчанию				Доменная учетная запись			Протоколы передачи файлов		
			Сценарии инициализации при загрузке или входе в систему (1/1)				Сканирование сетевых служб			Протоколы эл. почты		
			+ Сценарий входа в сеть							Протоколы (кроме прикладного уровня)		
										Туннелирование протокола		

PT NAD выявляет
117 различных действий
злоумышленников

Подробнее, какие техники покрывает PT NAD и как он их выявляет: mitre.ptsecurity.com

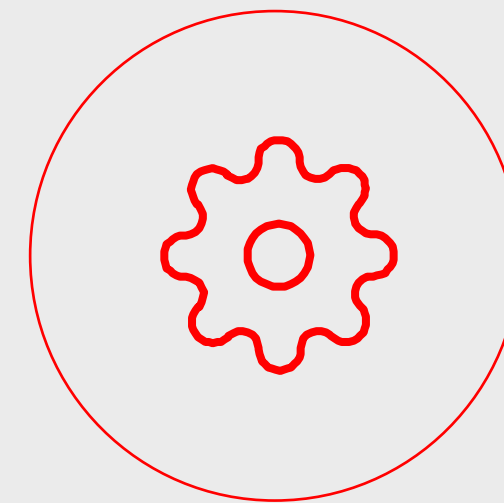
атакуют критичные ресурсы



Сегмент
бухгалтерии



Сегмент
топ-менеджеров



Сегмент
АСУТП

Что сделали хакеры

- Способ попадания в компанию неизвестен. Версия: фишинг и затем через политики AD. UPD: Может RDP (CVE-2019-0708) ?
- Получили пароль Администратора Домена
- Использовали кастомизированный криптолокер LockerGoga, который использовал недокументированные возможности Windows – продвинутые программисты
- По мере расследования цена на расшифрование росла

**Скорость
расследования
= деньги**

**Уничтожили
данные
на рабочих
станциях
и серверах**

**Заставили
компанию
выключить все
компьютеры
и отключить
их от сети**

**Вы не можете защищать то,
что вы не можете увидеть**



SHADOW IT

Shadow IT – несанкционированные
информационные ресурсы
и компоненты треть взломов в компании
приходится на shadow IT (GARTNER)

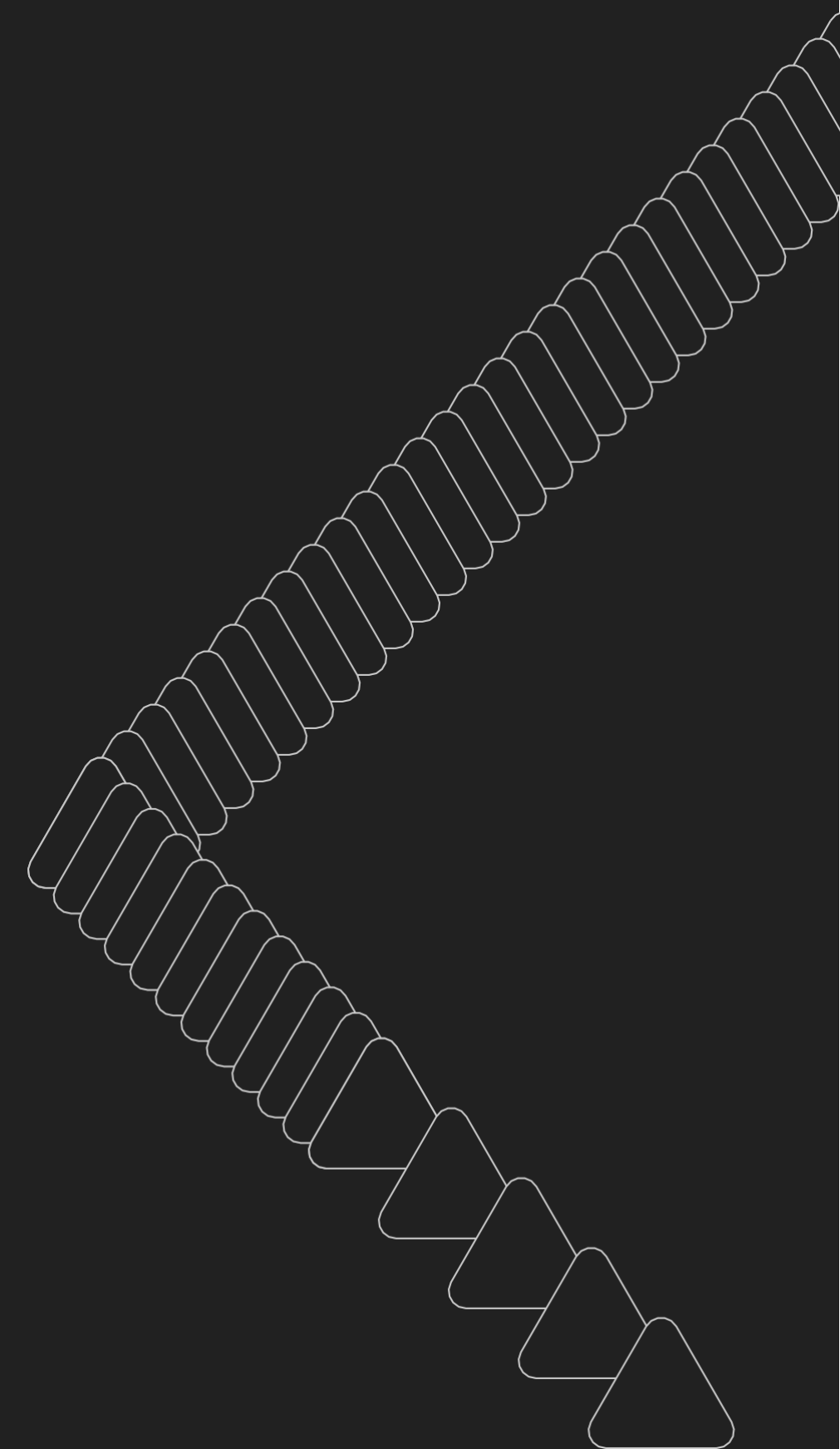
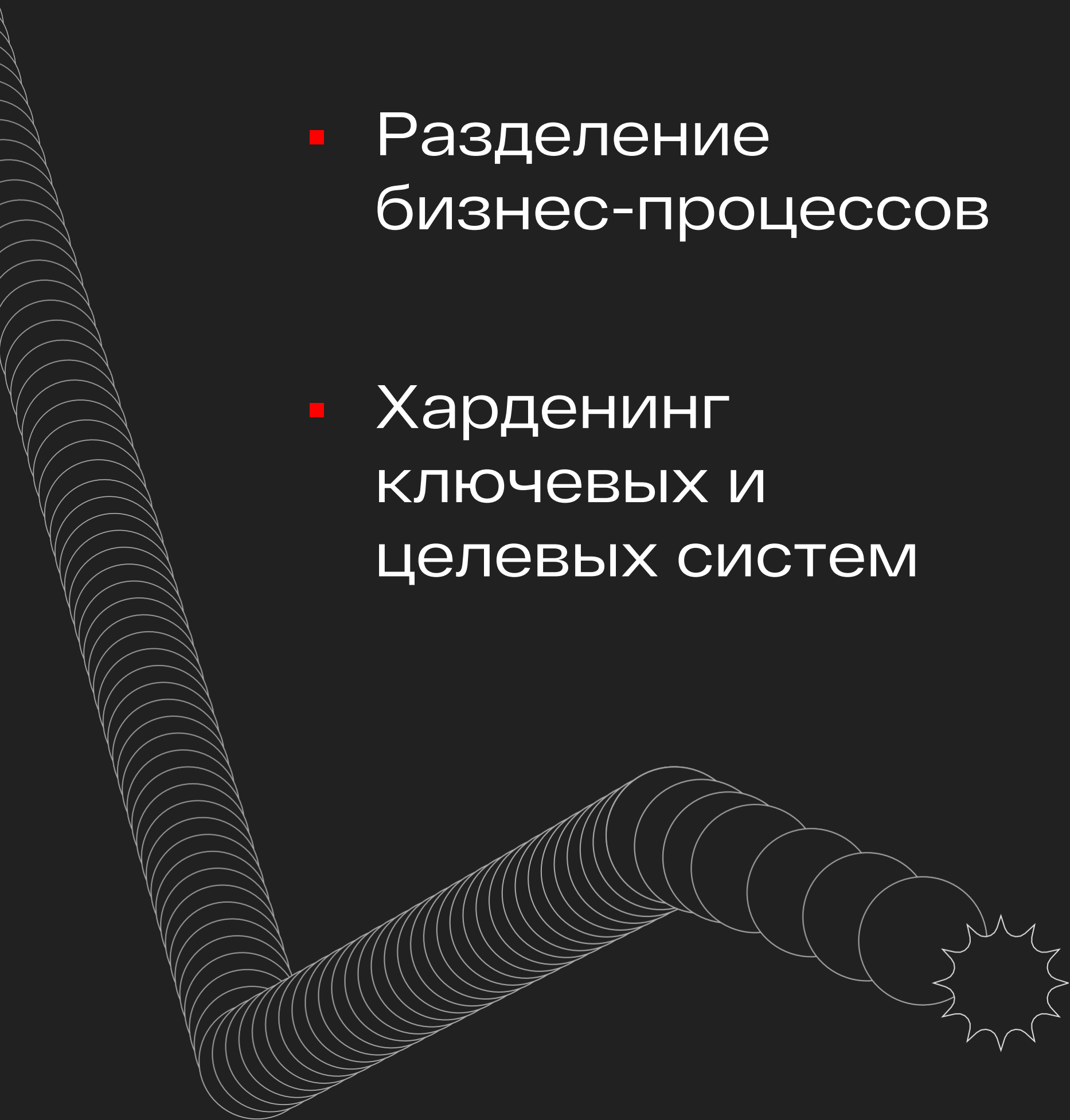


БЕСПЕЧНОСТЬ

У 9 из 10 инженеров на компьютере в открытом виде хранится документ с перечнем используемых систем, кратким описанием, IP-адресами и учетными данными для входа

Как вовремя обнаружить и остановить атаку

- Разделение бизнес-процессов
- Харденинг ключевых и целевых систем
- Мониторинг
- Удлинение цепочек атаки



Злоумышленник может скрыться на рабочей станции и сервере

- Множество устройств без хостовой защиты: новые узлы, тестовые машины, мобильные устройства, VPN шлюзы, сервера, сетевое оборудование, принтеры, видеокамеры, СКУД, датчики, системы управления, shadow IT



- На хосте есть возможность скрыться: руткиты и буткиты, вредоносный код создается уникальным под каждого человека

Ваша цель!

**Сокращение времени
скрытого присутствия
угрозы с 200 дней
до нескольких минут**



Продукты аналитические класса
Network Traffic Analysis (NTA)
должны сократить время
присутствия злоумышленника в
сети:

- выявляет целевые атаки на периметре и внутри сети на самых ранних этапах благодаря глубокому анализу сетевого трафика и файлов;
- обнаруживает атаки с хостов, которые не были выявлены в прошлом, благодаря регулярному ретроспективному анализу
- Обнаруживает зараженные хосты, на которых нет хостовой защиты.

Как минимум рекомендуем защищать критичные активы

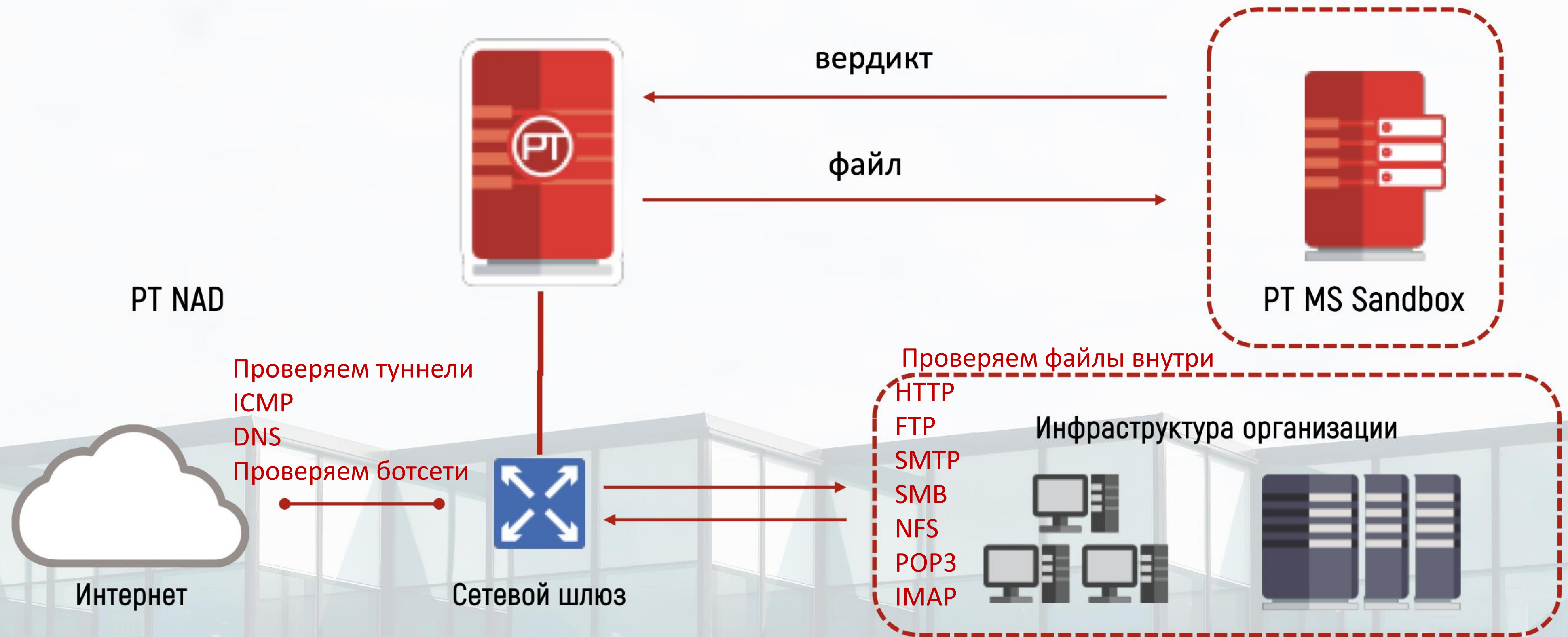


Комплексный подход: как это работает

- Детектирование угроз
- Поиск следов компрометации
- Хранение контекста атаки

- Выявление ВПО
- Локализация угроз
- Защита актуальных каналов

- Выявление скрытых и новых угроз



Как PT NAD дополняет NGFW



■ Обнаруживает внутренние сетевые атаки и инсайдеров

Обычно внутренний трафик никак не контролируется; обнаружить зараженные узлы и действия инсайдера невозможно без средств анализа внутреннего трафика (NTA).

■ Проводит ретроспективный анализ

После обновления базы знаний PT NAD автоматически проводит ретроспективный анализ, ищет скрытые угрозы в трафике и зараженные устройства.

■ Анализирует трафик по поведению

Обнаруживает появление новых сетевых узлов, атаки Kerberoasting, медленные сканирования, эксфильтрацию трафика с помощью вложенных друг в друга туннелей.

■ Помогает расследовать сетевые атаки

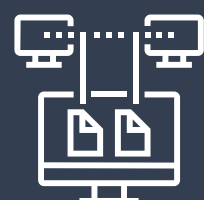
PT NAD хранит копию трафика и разбирает протоколы по 1200 параметрам. Это позволяет аналитикам SOC проводить threat hunting (проверять гипотезы) и расследовать сетевые атаки.

■ Хранит копию сетевого трафика и метаданные

Полностью записывает весь сетевой трафик, разбирает его структуру до файлов, хранит метаданные приложений для ретроспективного анализа и проактивного поиска угроз (threat hunting)

■ Разбирает метаданные протоколов и приложений

За счет технологии разбора трафика приложений (DPI) у PT NAD меньше ложных срабатываний и больше критериев для обнаружения злоумышленника в сети. Эксперты снабдили PT NAD правилами и несигнатурными методами обнаружения угроз: ML, статистика, корреляция разных сессий, поведение пользователей в сети.



Горизонтальное
перемещение
злоумышленника

Ретроспективный
анализ трафика



Угрозы
в зашифрованном
трафике



Активность
вредоносного ПО



Связь с автоматически
сгенерированными
доменами DGA



Признаки атак,
не обнаруженных ранее



Нарушения
регламентов ИБ



Соккрытие активности
от средств защиты



Хакерский
инструментарий



Эксплуатацию
уязвимостей в сети

**Решение
выявляет**

Продвинутый инструмент вашего ИТ отдела

Максимально быстро
обнаружить источник
проблемы в сети

Решаемые задачи:

- Кто грузит сеть или Интернет канал?
- Есть ли «левые» DHCP?
- Кто обходит средства удаленного подключения (TeamViewer, SSH туннели)
- Кто избежал правил по изоляции и сегментации? Например гостевой вай фай иногда становился внутренним, потому что админы косячат с правилами. Можно отследить когда там появляются подключения к внутренним адресам.
- Кто сливает данные? когда у тебя кто-то выкачивает все исходные коды или Wiki - это большой трафик
- Кто использует сервис, который надо ИТ службе отключить или переделать? Например хочешь отключить LDAP и перейти на LDAPS, вроде всех предупредил, системы переконфигурировал, а как быть уверенным? Заглянул, проверил, что таких подключений больше нет.



КГ НИЦ

«Калининградский государственный научно-исследовательский центр информационной и технической безопасности» (КГ НИЦ) использует систему анализа трафика и выявления атак PT Network Attack Discovery с 2018 года. Тогда мы начинали строить региональный центр безопасности (security operations center, SOC) для защиты органов государственной власти Калининградской области от хакерских атак. С 2020 года SOC функционирует как государственная информационная система «Центр управления безопасностью».

Незаменимой частью центра стал PT NAD. Он дает специалистам SOC около 70% полезной информации об инцидентах, выявленных в органах власти Калининградской области. Нам нравится, что он глубоко разбирает трафик и детально отображает, что происходит в подключенных к мониторингу сетях. Несколько серьезных инцидентов мы выявили благодаря сигналам в PT NAD о подозрительных соединениях.

Вместе со специалистами PT Expert Security Center мы оперативно расследовали сложные запутанные атаки на региональные органы власти и приняли меры по предотвращению их развития.



Уже в ходе пилотного проекта с помощью PT NAD специалистам ОЗИ ВГТРК удалось обнаружить в корпоративной сети **несколько действующих ботнетов** и другую скрытую вредоносную активность. Вскоре после перехода на боевую систему было выявлено и оперативно ликвидировано несколько программ-майнеров. В результате проекта ВГТРК получила удобный инструмент для контроля вредоносной активности в сетевом трафике и возможность для выполнения требований регуляторов — в частности, новых требований к операторам связи и интернет-проектам, предусмотренных Федеральным законом № 35-ФЗ «О противодействии терроризму».



«PT Network Attack Discovery (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».

Сотрудникам службы ИБ удалось вывести IT-ресурсы из тени. С помощью PT NAD они обнаружили несколько «теневых» приложений (shadow IT), установка которых не была одобрена IT-отделом.

Антон Мельник, начальник управления ИБ АО
«Объединенная энергетическая компания»

Какие цели заказчики достигли продуктом PT NAD



1. Храним копию трафика, что позволяет соответствовать 196 приказу ФСБ.
2. Позволил выявить внутренних злоумышленников
3. Позволил контролировать логины и пароли передающиеся в открытом виде в трафике
4. Позволил реализовать threat hunting и поиск различных IoC в трафике для аналитиков SOC
5. Позволили выявлять целевые атаки и вредоносный код в трафике, включая криптолокеры и майнеры
6. Позволил начать контролировать действия администраторов в сети
7. Позволил мониторить производительность сети и кто внутри сети ее нагружает
8. Позволил удобно разбирать инциденты и для ИТ и для ИБ служб, поскольку стандартные утилиты wireshark и встроенные в роутеры не умеют также
9. Позволил после взлома выявить какие машины заражены вредоносным ПО и выявить различные признаки компрометации
10. Получили сертифицированный ФСТЭК продукт класса COB
11. Позволил подменить функции NGFW от ушедшего иностранного производителя
12. DPI движок позволил собрать ИТ метрики.

РЕЗУЛЬТАТ ОДНОГО ПИЛОТА

Получение информации о парольной политике в домене

Перебор доменных служебных учетных записей

Запрос Kerberos со слабым набором шифров RC4

Сетевое сканирование Nmap

Перебор доменных пользователей

Подбор учетных данных к серверам

Подбор учетных данных SSH

Удаленное выполнение команд через механизм WMI

Создание копии домена через DCSync

Удаленное исполнение кода утилитой Impacket

Попытка эксплуатации уязвимости Path Traversal

Сканирование утилитой nmap

Атака класса MITM используя NTLM Relay

Передача логинов и паролей в открытом виде

Почта с вредоносными вложениями



NAD сетевая часть вашего
КОМПЛЕКСА РАННЕГО
ВЫЯВЛЕНИЯ СЛОЖНЫХ И
СКРЫТЫХ УГРОЗ И
РАССЛЕДОВАНИЯ
ИНЦИДЕНТОВ



Функционал PT NAD	Собственная база репутационных списков Threat Intelligence (IoC) с базой DNS, IP, хешей MD5
Глубокий анализ трафика и аналитика	Адреса бот-сетей
Анализ трафика и разбор 1200 служебных полей для следующих приложений и протоколов, например: IP (IPv4, IPv6), TCP, UDP, ICMP, HTTP, DNS, SSH, SMTP, POP3, IMAP, Telnet, FTP, TFTP, NTP, SIP, SNMP, DCE/RPC, Kerberos, LDAP, NFS, SMB, PGSQL, MySQL, RDP, RFB (VNC), IP-IP, GRE	Обнаружение атак на основе поставляемых в устройство из лаборатории PT ESC правил для их обнаружения
Ретроспективный анализ трафика по 1200 параметрам и по обогащенным данным: посчитанными хешами файлов, странам, именам пользователей и DNS адресам, IoC и IoA	Возможность загружать правила для обнаружения атак от сторонних производителей
Сбор и хранение выявленных атрибутов и метаданных сессий на основе разобранных протоколов, файлов, вердиктов песочницы и результат	Возможность добавлять самому правила для обнаружения атак
Обогащение журналов сетевых соединений дополнительной информацией: Geo-IP, хеш-суммы MD5, имени хоста, DNS адреса, обнаруженное ПО, баннеры и др.	Фиксация сессий связи на основе разбора протоколов сетевого взаимодействия
Выявление утилит удаленного управления	Фиксация атаки с разбором дополнительных параметров
Выявление туннелей и прокси	Выявление передачи учетных данных, словарных паролей и паролей по умолчанию
Разбор атак внутри трафика инкапсулированного в VLAN, MPLS, VXLAN, TEREDO, GRE, ERSPAN, GENEVE	Выявление майнеров и нежелательного ПО
Разбор протоколов приложений при частичной потере данных в соединениях	Выявление хакерского инструмента Impacket, CrackMapExec, Koadic и др.
Работа с файлами в трафике и интеграция с внешними системами безопасности	Выявление SGT и TGT тикетов для атак на AD
Выявление файлов и данных, передаваемых по протоколам прикладного уровня SMTP, POP3, IMAP, FTP, HTTP, SMB	Привязка сетевого трафика к аккаунтам, используемыми пользователями на основе запросов Kerberos и NTLM
Отправка выявленных файлов из SMTP, POP3, IMAP, FTP, HTTP, SMB, NFS по ICAP в любую внешнюю систему (антивирус, DLP, песочницу) по ICAP файлов без получения обратно вердикта о проверке	Запоминание DNS запросов и ответов в трафике и обогащение журнала сессий для сопоставления DNS с IP адресами
Отправка выявленных файлов из SMTP, POP3, IMAP, FTP, HTTP, SMB, NFS по ICAP для проверки в многопоточную антивирусную систему PT Multiscanner или в песочницу PT Sandbox, с получением вердикта о проверке файла	Возможность создавать пользовательские правила для обнаружения атак через интерфейс продукта
Запись и долговременное хранение захваченного трафика в сыром виде в формате PCAP	Обновление сигнатур в реальном времени для новых атак
Импорт и анализ файлов PCAP из сторонних источников	API для просмотра и редактирования пользовательских репутационных списков
Интеграция с SIEM	Функционал анализа сетевого трафика по поведению (NTA)
Интерфейс управления и его возможности	Обнаружение аномалий на основе экспертных правил, статистики и поведенческого анализа
Управление через веб-интерфейс для просмотра и анализа захваченной копии трафика, проведения расследований	Обнаружение медленных сканирований
Фильтрация анализа для захваченного трафика по: протоколам и портам транспортного уровня, IP-адресам, IP-подсетям фильтрами BPF	Обнаружение сканирований и DDoS
Автоматическое выполнение ретроспективного анализа индикаторами атак по сохраненным метаданным трафика	Обнаружение новых сетевых узлов и контроль используемых ими сетевых портов и протоколов
Лента активностей для упрощения работы аналитика	Корреляция событий из различных сессий: запросы DNS, запросы Kerberos, запросы HTTP
Возможность проведения Threat Hunting	Machine Learning для выявления автоматически сгенерированных доменов (DGA)
Возможность проиграть повторно трафик экспертными движками анализа	Обнаружение ВПО в SSL без расшифрования (для части атак)
Возможность расследования инцидентов на основе разобранного трафика	Определение ролей и типов устройств по их поведению
Выявление уязвимых мест в инфраструктуре	Machine Learning для Kerberoasting
Построение графа сетевых взаимодействий	Дополнительный функционал
Обогащение информации о каждом соединении на основе экспертизы Positive Technologies Expert Security Center	Уведомления ответственных лиц с помощью почтовых сообщений
Обнаружение вредоносных соединений на основе собственных репутационных списков с индикаторами компрометации на основе DNS, IP, URL и хешей MD5	Уведомлений о сбоях в работе сервисов и отображение состояния подсистемы в интерфейсе пользователя
Выявление APT и целевых атак на компанию на разных стадиях MITRE ATT&CK, включая 117 техник и тактик	Фильтрация захватываемого трафика правилами BPF по сетевым реквизитам: IP-адресам, протоколам и портам транспортного уровня, таким VLAN и др.



Проверьте, что в вашей сети нет хакеров!

Денис Батранков,
эксперт по информационной
безопасности, CISSP



bdv@ptsecurity.com



ptsecurity.com

ЧАТ
ПРОДУКТА В
ТЕЛЕГРАММ



t.me/PTNADChat

