

Шифрование корпоративной информации
и полная остановка бизнеса.

Насколько ваш контрагент уязвим? Актуальные сценарии хакерских атак



Директор департамента безопасности
Грунтов Антон

Eqvanta — группа компаний, работающих в сфере альтернативных финансов и финансовых технологий

Быстроденьги

на пути к лучшему

Онлайн-сервисы и розничная сеть.
Самый известный бренд МФО в России,
основоположник займов до зарплаты



IT-подразделение 200+ человек
с резидентством в Сколково



Онлайн-сервис мгновенных
займов на банковские карты



Онлайн-сервис мгновенных
займов на банковские карты



Альтернативные финансы
во Вьетнаме



**CISO, CESO
CFE, MBA (IT)**



**НАЦИОНАЛЬНОЕ ОБЪЕДИНЕНИЕ
СПЕЦИАЛИСТОВ ПО БЕЗОПАСНОСТИ БИЗНЕСА**

Работает полноценная «компания»

- Подразделение отбора «клиента»
- Подразделение вскрытия доступов
- Подразделение исследования инфраструктуры
- Подразделение внедрения шифровальщиков
- Подразделение переговорщиков
- Подразделение финансистов

?

```
ion () {  
k ready')  
l, document.title,  
state",function(e){  
https://credit.pod-
```

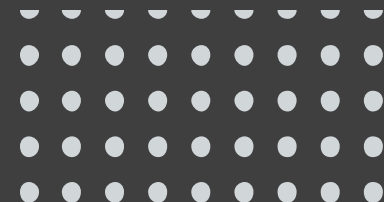


340				
	Табельный номер	Имеет отсрочку от мобилизации	Дата окончания отсрочки от мобилизации	Должность
19	Сергеевич 77001	Да	14.12.2022	Ведущий инженер
20	Иванович 77001	Да	13.12.2022	Профессор
21	Владимирович 77001	Да	22.11.2022	Доцент
22	Олегович 77001	Да	21.11.2022	Профессор
23	Иванович 77001	Да	17.01.2023	Заместитель начальника отдела
24	Иванович 77001	Да	23.11.2022	Преподаватель
25	Сергей Владимирович 77001	Да	09.12.2022	Профессор
26	Михайлович 77001	Да	23.12.2022	Заведующий центром
27	Андреевич (вн.) 77001	Да	21.11.2022	Преподаватель
28	Иванович 77001	Да	21.12.2022	Заместитель директора
29	Александрович 77001	Да	21.11.2022	Преподаватель
30	Курочкин 77001	Да	29.11.2022	Доцент
31	Сергеевич 77001	Да	17.11.2022	Ректор
32	Владимирович 77001	Да	22.11.2022	Доцент
33	Владимирович 77001	Да	25.11.2022	Профессор
34	Владимирович 77001	Да	21.11.2022	Ведущий инженер
35	Евгеньевич 77001	Да	26.12.2022	Заместитель директора
36	Александрович 77001	Да	21.11.2022	Начальник управления
37	Иванович 77001	Да	21.11.2022	Доцент
38	Канюкович 77001	Да	16.12.2022	Проректор
39	Сергеевич 77001	Да	21.11.2022	Профессор
40	Иванович 77001	Да	21.11.2022	Директор по эксплуатации и текущему ремонту зданий и сооружений



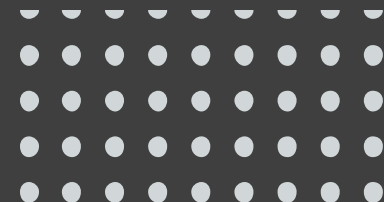
Сценарий реализации атаки. Часть 1. Доступы.

1. Отбор «клиента», т.е. компании - жертвы. Изучение его финансовых показателей, контактов персонала (иные приемы OSINT).
2. Изучение активных контрагентов и их контрагентов. Определение перечня предпочтительных доступов.
3. Официальная аренда сервера на территории РФ, чтобы не «светиться» с зарубежными IP.
4. Попытка проникновения в инфраструктуру «жертвы» напрямую через легальный доступ, полученный от ее персонала через фишинг или взлом личных рабочих станций (в т.ч. через незащищенный домашний WiFi - роутер).



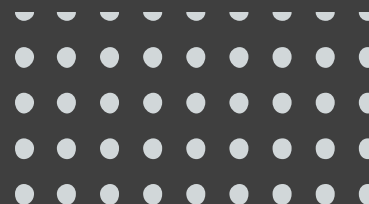
Сценарий реализации атаки. Часть 1. Доступы.

5. Попытка проникновения в инфраструктуру контрагента через легальный доступ, полученный от ее персонала. Изучение легальных каналов связи между контрагентом и «жертвой». Далее получение легальных доступов в инфраструктуру «жертвы».
6. Шантаж контрагента в случае выявления им факта опосредованной атаки.



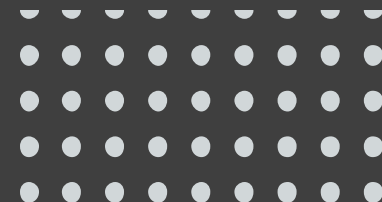
Сценарий реализации атаки. Часть 2. Шифрование.

7. Создание надежного прямого доступа - собственной учетной записи или использование легитимной, которая редко или беспорядочно используется владельцем. Организация доступов к серверам, тестовым контурам и пр. через учетные записи контрагентов или свои (вновь созданные) учетные записи. Получение доступов к системам других контрагентов «жертвы». Передача доступов инфраструктурщикам.
8. Тщательное изучение внутренней ИТ – инфраструктуры и ее описание. Выявление наиболее уязвимых мест, определение порядка резервного копирования и возможных сценариев восстановления системы.



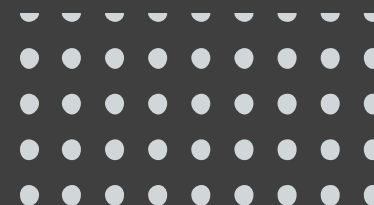
Сценарий реализации атаки. Часть 2. Шифрование.

9. Изучение иерархии и сотрудников подразделения защиты данных, руководства. Получение доступов к их перепискам, в т.ч. через мессенджеры (посредством компрометации веб - версий).
10. Внедрение программ – шифровальщиков в инфраструктуру.
11. Шифрование данных и через вирус – шифровальщик по ночам, в выходные и праздники. Обезвреживание подразделения защиты. Контроль коммуникаций внутри компании.



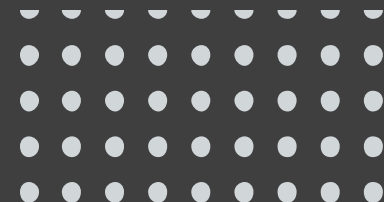
Сценарий реализации атаки. Часть 3. Выкуп.

12. Требование выкупа и вступление в переговорный процесс
13. Снятие реакции. Противодействие восстановлению. Модуляция переписки и формирование ложного следа, отвлечение на ложный объект.
14. Аргументация надежности в обратной передаче доступа к информации, ее дешифрования.
15. Достижение договоренности по сумме выкупа.
16. Передача данных «жертве» о нескольких криптокошельках. Прием средств и дальнейшая их трансграничная легализация.
17. Передача ключей для дешифрования.
18. Продолжение контроля «жертвы», зачистка следов в случае их наличия.
19. Противодействие расследованию, наведение на ложный след.
20. Сохранение доступов и их поддержка с целью дальнейших атак на «жертву».



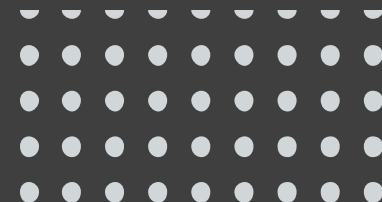
Что делать? ДО АТАКИ.

1. Средства защиты информации на личные АРМ для удаленщиков и для пользователей с привилегированным доступом (антивирус и др.).
2. Двухфакторная аутентификация на VPN и на подключение к серверам.
3. Запрет на подключение к контуру компании без средств защиты информации.
4. Менеджмент паролей локальных учетных записей, увеличение сложности администраторских паролей до минимального количества символов 18.



Что делать? ДО АТАКИ.

5. Запрет работы через прямое подключение для администраторов, только через прокси-устройство во внутреннем контуре (джамп).
6. Внедрение авторизации по сертификату взамен входа по паролю (Bluetooth токен, содержащий электронную подпись, по которой производится авторизация, может использоваться в т.ч. и на мобильных устройствах для доступа к электронной подписи).
7. Ограничение доступа к системам из - за пределов контура компании (только через VPN и джампы).
8. Авторизация в VPN по токену с ЭП + второй фактор (не пароль). При переходе в спящий режим рвем блютуз – соединение.



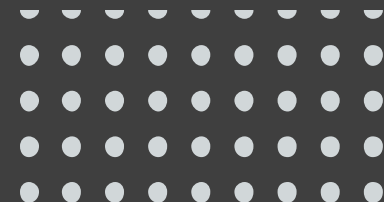
Что делать? ДО АТАКИ.

9. Ограничить срок жизни сессий, при переподключении нужно автоматически проверять наличие подключенного токена.
10. Учетные записи для решения общих рабочих вопросов делятся для привилегированных пользователей на 2 типа: пользовательскую (для почты/портала/джира и т.д.) и администраторскую для выполнения должностных задач.
11. Запрет на авторизацию в VPN через администраторские УЗ.
12. Проведение пентеста всего контура инфраструктуры не реже раза в год и аудита не реже раза в 2 года.
13. !!! Анкетирование контрагентов на предмет защищенности от киберугроз, которым предоставляется доступ в Ваши информационные системы или с которыми ведется обмен данными. Рекомендуется делать это еще на этапе закупочной процедуры.

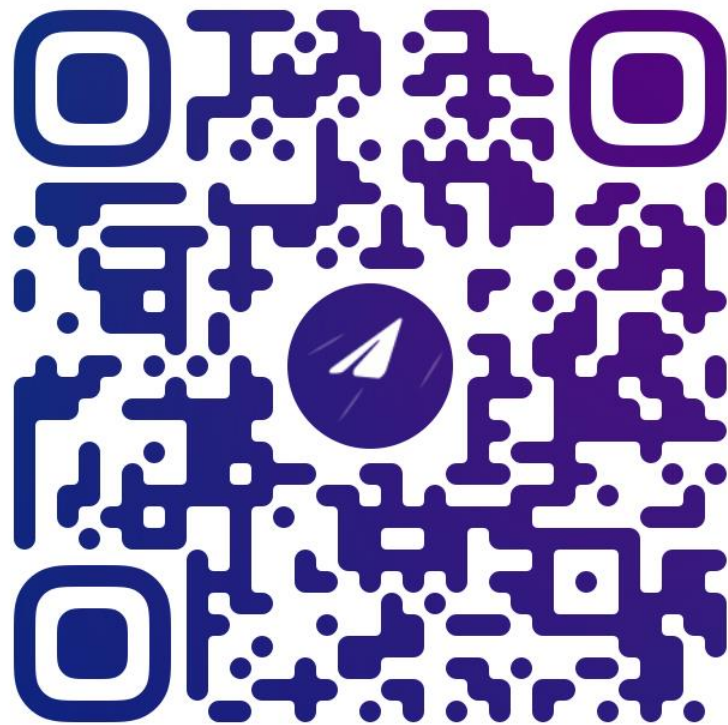


Что делать? ПОСЛЕ АТАКИ.

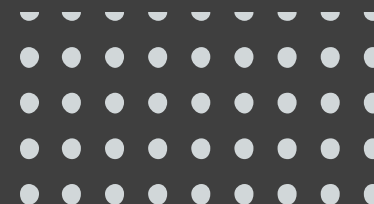
1. Привлечение специализированной организации для расследования атаки.
2. Ограничение доступов к ИС снаружи корпоративного периметра и разграничение пользовательской активности внутри.
3. Смена учетных записей и паролей.
4. Ограничение копирования информации пользователями на флэшки и т.п.
5. Полный аудит информационных систем, рабочих станций и носителей данных на предмет закладок.
6. Копирование журналов ИС и их анализ.
7. Исследование резервных копий.
8. Восстановление данных в ИС из резервных копий.
9. Контроль всей пользовательской активности.
10. Привлечение правоохранительных органов.



**Секретный неблокируемый
чат – бот для помощи в расследованиях.**



**@ASSISTANT_SECRET_
BOT**





Спасибо за внимание!

agruntov@eqvanta.ru

2024