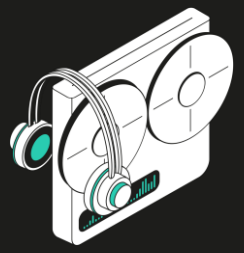
kaspersky

Значимые утечки данных в 2023

Игорь Фиц

Аналитик Digital Footprint Intelligence

Digital Footprint Intelligence



Мониторинг Даркнета

Поиск утечек данных

Исследование сетевого периметра

Защита репутации бренда

План вебинара

1. Как анализируют факты утечек пользовательских данных?

2. Статистика публичных инцидентов 2023 года

3. Анализ скомпрометированных паролей: количество и содержание

Инцидент информационной безопасности, при котором конфиденциальная информация становится доступной для посторонних лиц

Базы данных пользователей и сотрудников российских организаций, опубликованные в свободный доступ в Интернет

Инцидент информационной безопасности, при котором конфиденциальная информация становится доступной для посторонних лиц

Базы данных пользователей и сотрудников российских организаций, опубликованные в свободный доступ в Интернет

Приватные дампы / материалы выставленные на продажу

Базы данных с минимальной достоверностью

Базы менее 5 000 строк пользовательских данных

Для компаний

Репутационные риски

Регуляторные риски

Материальные риски

Для пользователей

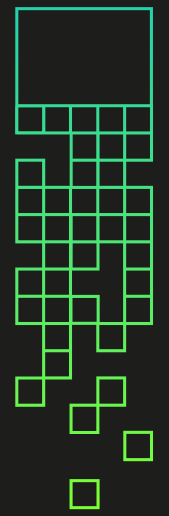
Приватная информация

Взлом аккаунтов

Мошеннические базы

Фейк?

Подтвердить факт утечки пользовательских данных может только компания владелец данных



Как анализируется утечка данных?

Уникальность

Адекватность

Структура

Источник публикации

Анализ ресурса

Комментарии сообщества

Зачем анализируют утечки данных?

Осведомленность

Векторы атак

Тренды

Парольная информация

Распространение утечек данных 2023

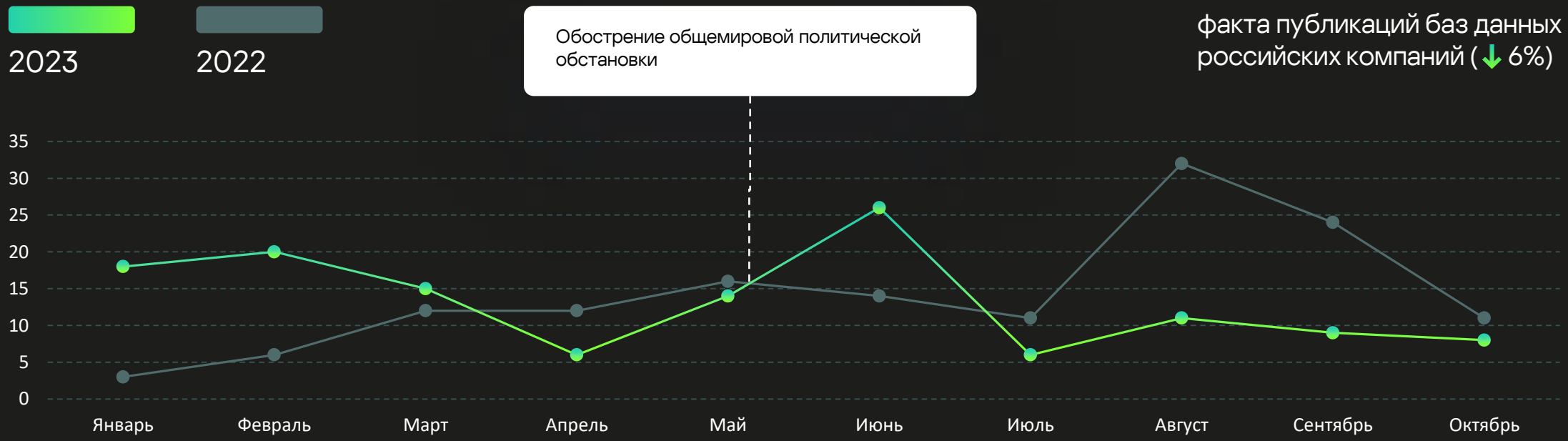
Факторы возможной активизации публикаций

Наличие громких публикаций у противоборствующих группировок

Обострение общемировой политической обстановки

133

факта публикаций баз данных российских компаний (↓ 6%)

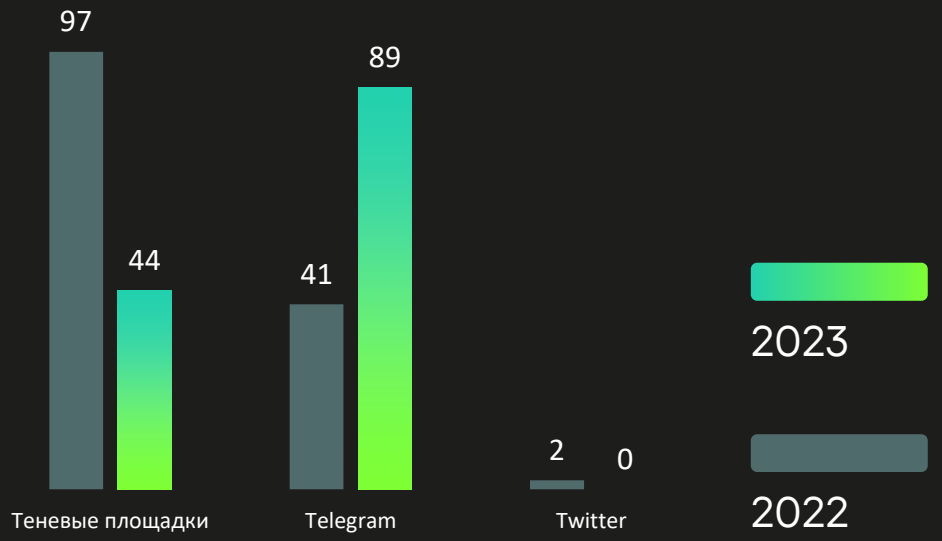


Распределение количества утечек по годам

Распространение утечек данных 2023

67%

публикаций пользовательских баз данных изначально размещены в Telegram (↑ x2)



Актуальность утечек данных 2023

>310M

пользовательских данных опубликовано (↑33%)

71%

утечек данных относятся к 2023 году

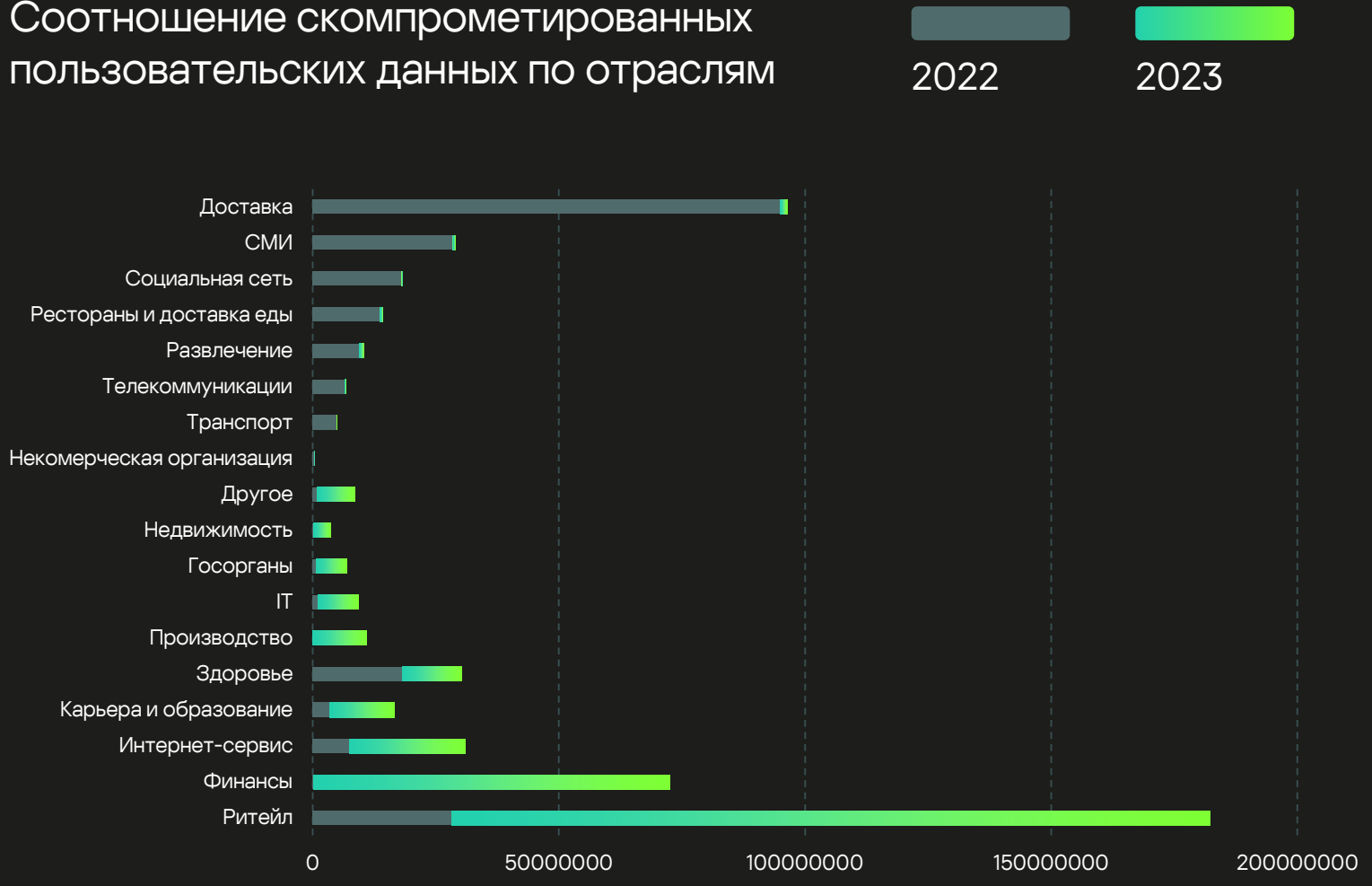
55%

утечек опубликованы в течение месяца после выгрузки данных из атакованной компании

Ритейл — лидер по количеству утечек данных

Профиль жертвы 2023

Соотношение скомпрометированных пользовательских данных по отраслям



Лидеры по объему скомпрометированных данных:

49%

Ритейл

23%

Финансы

Топ-10 утечек по объемам данных содержат в себе 74% всех скомпрометированных данных, опубликованных в 2023 году.

В каких сферах были самые крупные утечки?

- 4 Ритейл
- 2 Финансы
- 1 Интернет-сервисы
- 1 Здоровье
- 1 Карьера и образование
- 1 Производство

Смещение фокуса на публикацию данных компаний крупного бизнеса

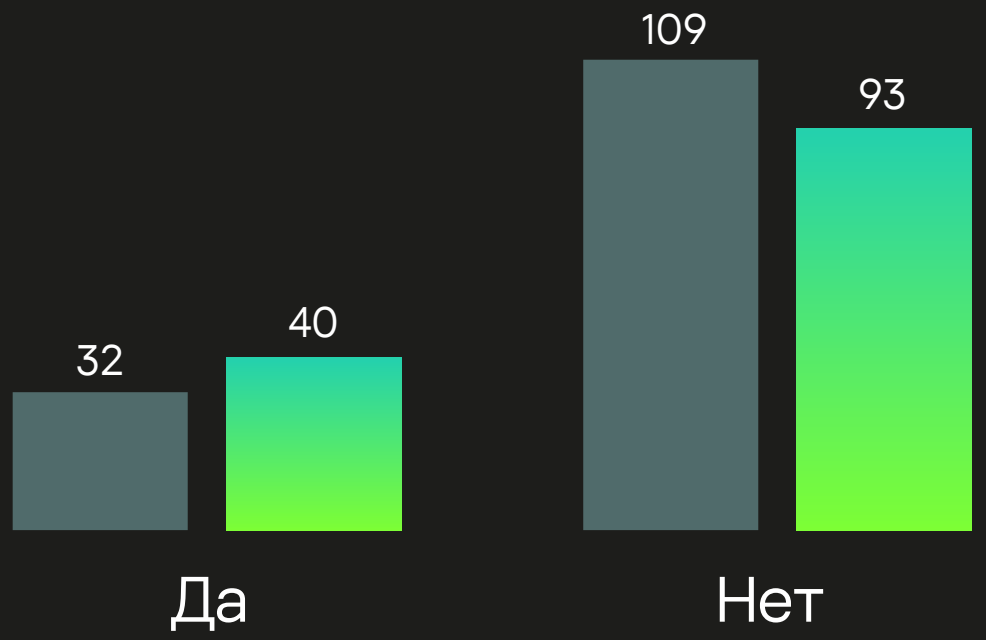
Количество утечек

Количество строк

	2022	2023
МСБ	74M	73M
Крупный бизнес	137M	220 M

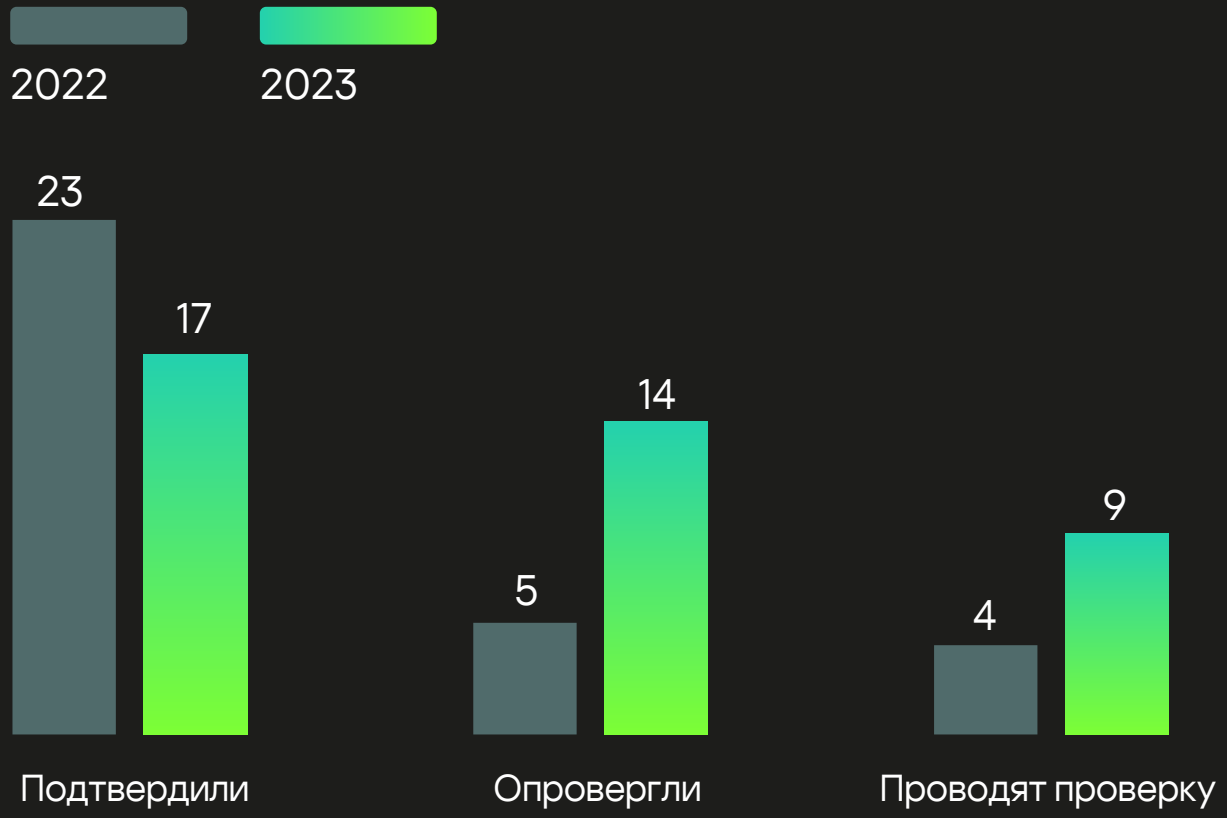
* МСБ – малый и средний бизнес

Наличие реакции компании-жертвы на утечку данных



В 2023 году наблюдается рост публичных реакций компаний на инцидент утечки данных, но.....

Реакция бизнеса на утечку данных



! увеличилось количество организаций, которые выбирают «осторожную» позицию либо полностью отрицают какой-либо факт утечки

- фейк
- причины утечки устранены
- подрядчик
- проходит проверка
- взлом админ панели
- атака на сайт
- компиляция
- сбоев не было

54%

баз данных содержали парольную информацию

>47м

парольной информации скомпрометировано

Алгоритмы хеширования паролей

35%

md5 (salt+pass)

18%

md5

13%

sha512-crypt

35%

md5 (salt+pass)

18%

md5

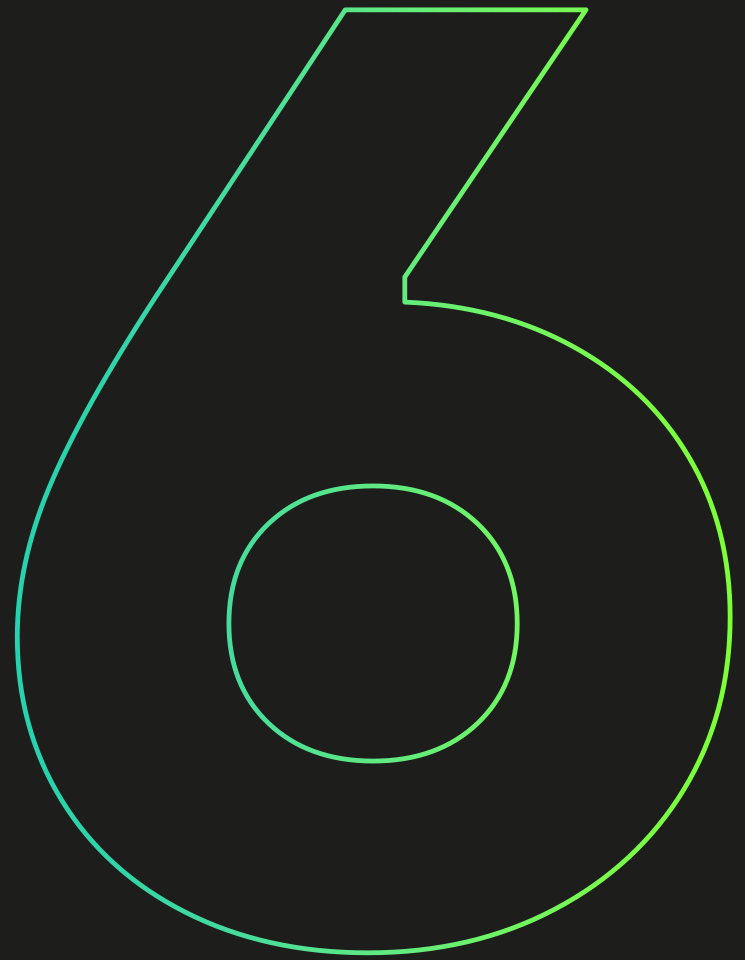
13%

sha512-crypt

md5 (salt+pass) и sha512-crypt используется в различных версиях CMS 1C-Bitrix

Сколько баз данных с паролями в открытом виде?

Сколько баз данных с паролями в открытом виде?



md5 (salt+pass)

hashcat -m 20 -a 0 e7ce7e469d4f129c91467ca4294bf674:U6x1Lk5M /home/kali/Desktop/tet.txt

Session: hashcat
Status.....: Cracked
Hash.Mode.....: 20 (md5($salt.$pass))

e7ce7e469d4f129c91467ca4294bf674:U6x1Lk5M :XXXX

Стоимость услуги расшифровки хешей

cmd5.ru

20 $	Расшифровка **100** хэшей Истекает через 3 лет	**0.2 $** за хэш
100 $	Расшифровка **10000** x Истекает через 3 лет	
200 $	Расшифровка **50000** x Истекает через 3 лет	

hashes.com

Paid Recovery Lists

NEW LIST | GENERATE MASS LEFT LIST | UPLOAD FOUNDS | VIEW AS JSON

Show 25 entries Search:

ID	Created At	Last Crack	Algorithm	Total Hashes	Hashes Found	Hashes Left	Price Per Hash Coin/(USD)	Currency	Maximum Cracks Needed	Progress	Download Left
44903	2023-11-22 13:15:11	2023-11-23 05:44:02	NTLM	3952	1215	2737	0.00001000 XMR (~$0.0017 USD)	XMR	3952	31 %	HASHES LEFT
44431	2023-11-13 12:16:15	2023-11-23 05:32:04	NTLM	2274084	2599	2271485	0.00001000 LTC (~$0.0007 USD)	LTC	900000	0 %	HASHES LEFT
44316	2023-11-11 08:24:43	2023-11-23 05:29:02	NTLM	1301	503	798	0.00001000 XMR (~$0.0017 USD)	XMR	1301	39 %	HASHES LEFT
44953	2023-11-23 04:54:58	2023-11-23 04:57:03	MD5	274	224	50	0.00000053 BTC (~$0.0198 USD)	BTC	274	82 %	HASHES LEFT
38117	2023-06-14 18:24:10	2023-11-23 04:47:15	NTLM	690648	36101	654547	0.00000010 LTC (~$0.0000 USD)	LTC	600000	6 %	HASHES LEFT
38101	2023-06-14 12:16:37	2023-11-23 04:46:57	NTLM	2389751	119742	2270009	0.00000010 LTC (~$0.0000 USD)	LTC	500000	24 %	HASHES LEFT
44937	2023-11-22 22:10:53	2023-11-23 04:41:01	NTLM	23	5	18	0.00000268 BTC (~$0.1000 USD)	BTC	23	22 %	HASHES LEFT

Что делать в случае утечки?

Идентификация инцидента

Определите источник

Верифицируйте

Проведите анализ

Коммуникации

Организуйте коммуникации с заинтересованными сторонами

- Топ-менеджмент компании
- Регуляторы
- СМИ
- Пользователи
- Партнеры

Устранение инцидента

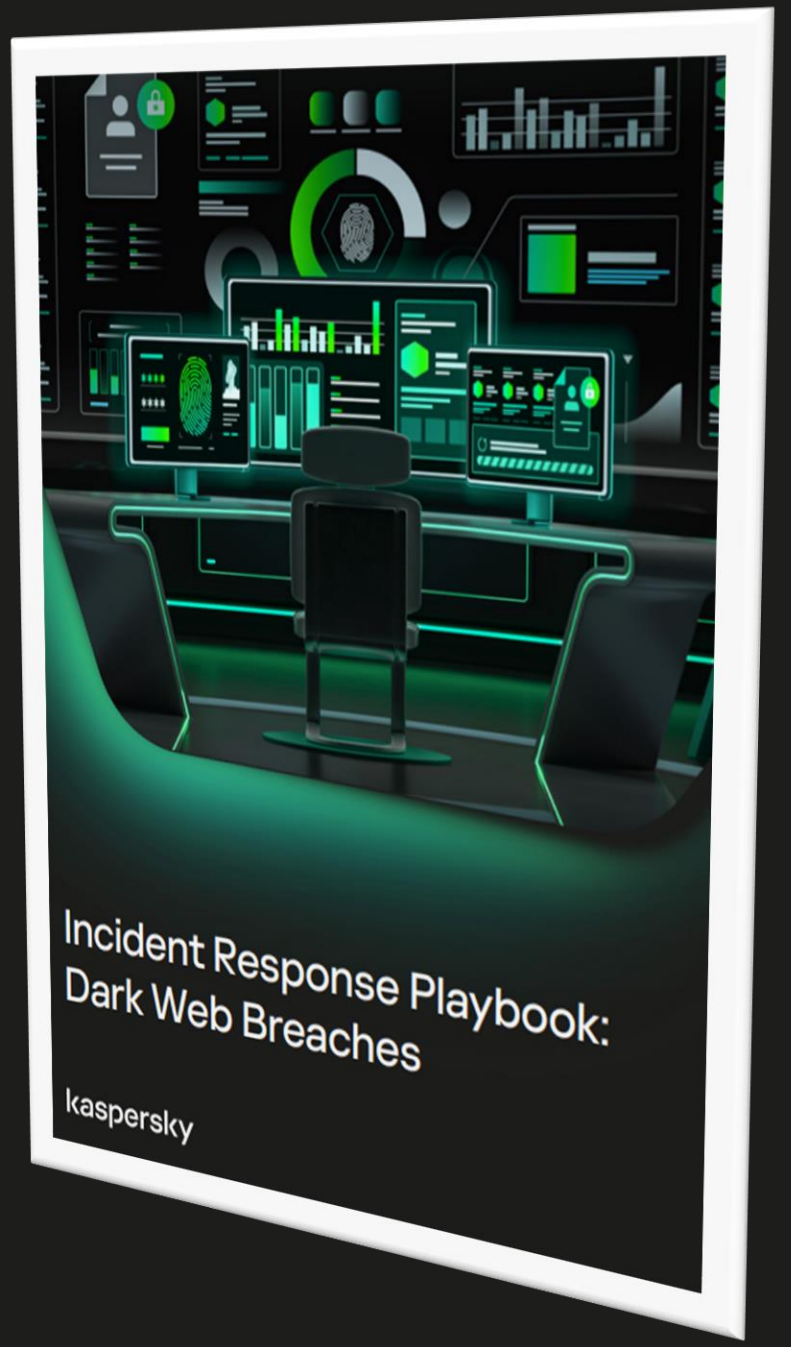
Проведите расследование

Устраните угрозу

Выучите уроки

Сценарии реагирования

Публикация утекших данных
Продажа доступа в инфраструктуру
Публикация скомпрометированного аккаунта



Спасибо!
Вопросы?

https://dfi.kaspersky.ru/