



АССОЦИАЦИЯ
БОЛЬШИХ ДАННЫХ

ЭКОНОМИКА
АНО «Цифровая экономика»

FIRST RUSSIAN DATA FORUM

Тренды киберугроз и утечки данных

Павлов Алексей,
Директор по развитию бизнеса SOC
Ростелеком-Солар

Тренды угроз

Q1 2022

- Массовые атаки на веб-ресурсы: **дефейс через взлом счетчиков и баннеров.**
- Необратимое **шифрование** данных **без возможности выкупа**
- **Проправительственные группировки** повысили активность в части **проникновения и закрепления в объектах КИИ и компаниях госсектора**

Q2 2022

- Событийные атаки на публичные сервисы
- Точечные взломы преимущественно через уязвимости периметра
- **Атаки через подрядчиков и цепочки поставок**

Q3-Q4 2022

- Снижение фона простых кибератак
- Усложнение подходов на фоне повышения защищенности
- **Появление фишинга и взлом сервисов с использованием публичных утечек**

Утечки

Небывалый
масштаб

Склейки
компиляции

PR-войны и фейки

Атрибуция и
идентификация
систем

Примеры фейков

Назад в будущее...

```
(1480045, '2018-06-05 12:53:08', '██████████ik@mail.ru', '██████████F9d3b364e6d1d5a4c0c05c444e9c606',
'qDpfeT1g8d9c403c231174911524d1600749ea3c', 'Y', '██████████ЮН', '██████████ГЯН', '██████████ik@mail.ru', NULL, '2018-
01-31 21:06:05', NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, '+7(930) 410-60-04', NULL, NULL, NULL, NULL, NU
LL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL,
NULL, NULL, NULL, NULL, NULL, NULL, '2023-11-28', NULL, '2018-01-31 21:09:43', '██████████ович', NUL
L, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL)
```

Утечка 2022 года....

ГУ МВД России по Московской Области в
городском поселении Мытищи.

Взлом Ростелекома...

54.60

Regular View Raw Data History

General Information

Country	Russian Federation
City	Krasnodar
Organization	OJSC Rostelecom Macroregional Branch South
ISP	PJSC Rostelecom
ASN	AS25490
Operating System	Linux