Тенденции развития угроз безопасности информации

Докладчик: Сердечный Алексей

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Источники исходных данных об угрозах безопасности информации

Информационная карта источников

Граф связей источников

Источники исходных данных об угрозах безопасности информации

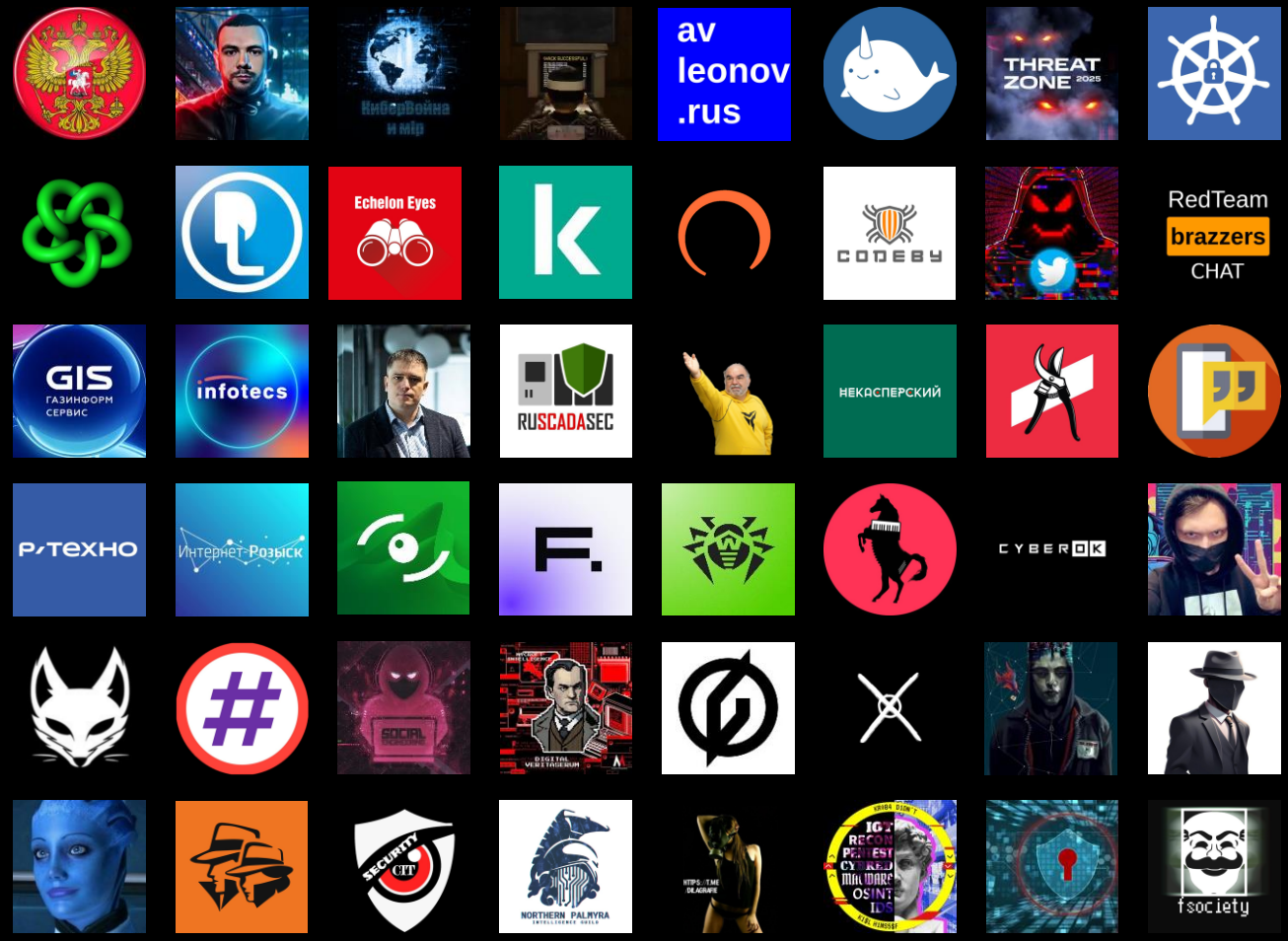
Информационная карта источников

Базы данных угроз, уязвимостей, эксплойтов, утечек, новостные источники

Источники исходных данных об угрозах безопасности информации

Информационная карта источников

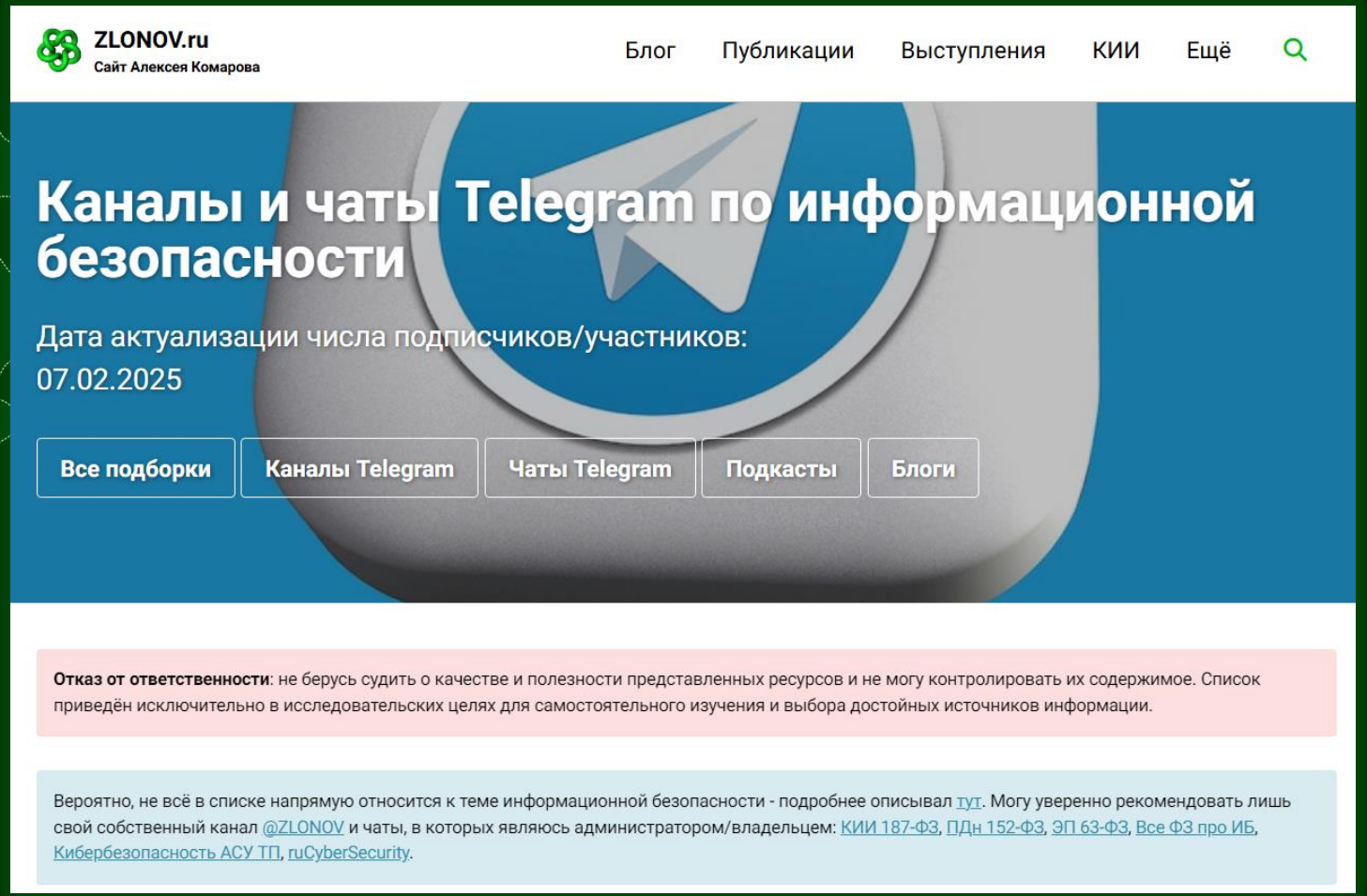
Отчёты, статьи и заметки исследователей



Источники исходных данных об угрозах безопасности информации

Информационная карта источников

Пример тематического анализа группы источников

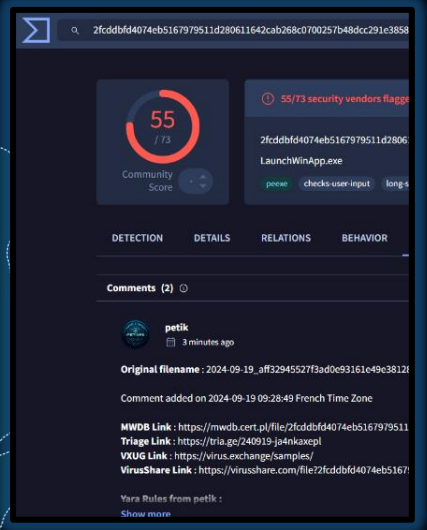


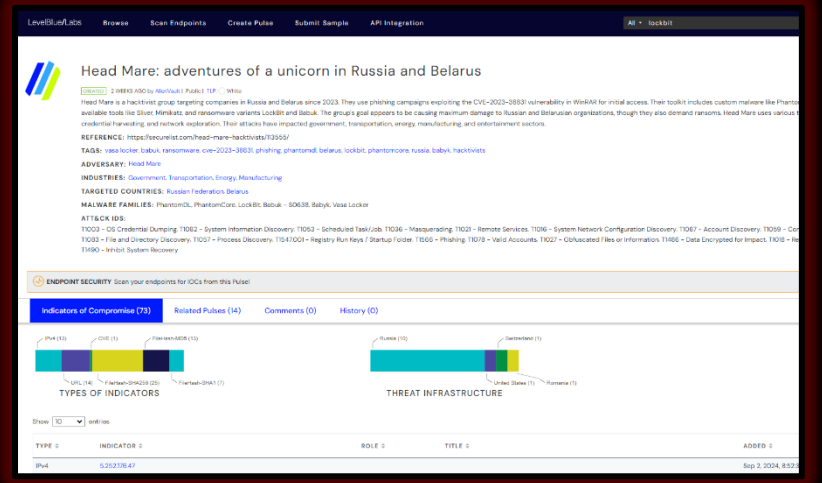
Подборка источников от Алексея Комарова: https://zlonov.ru/lists/telegram/

Источники исходных данных об угрозах безопасности информации

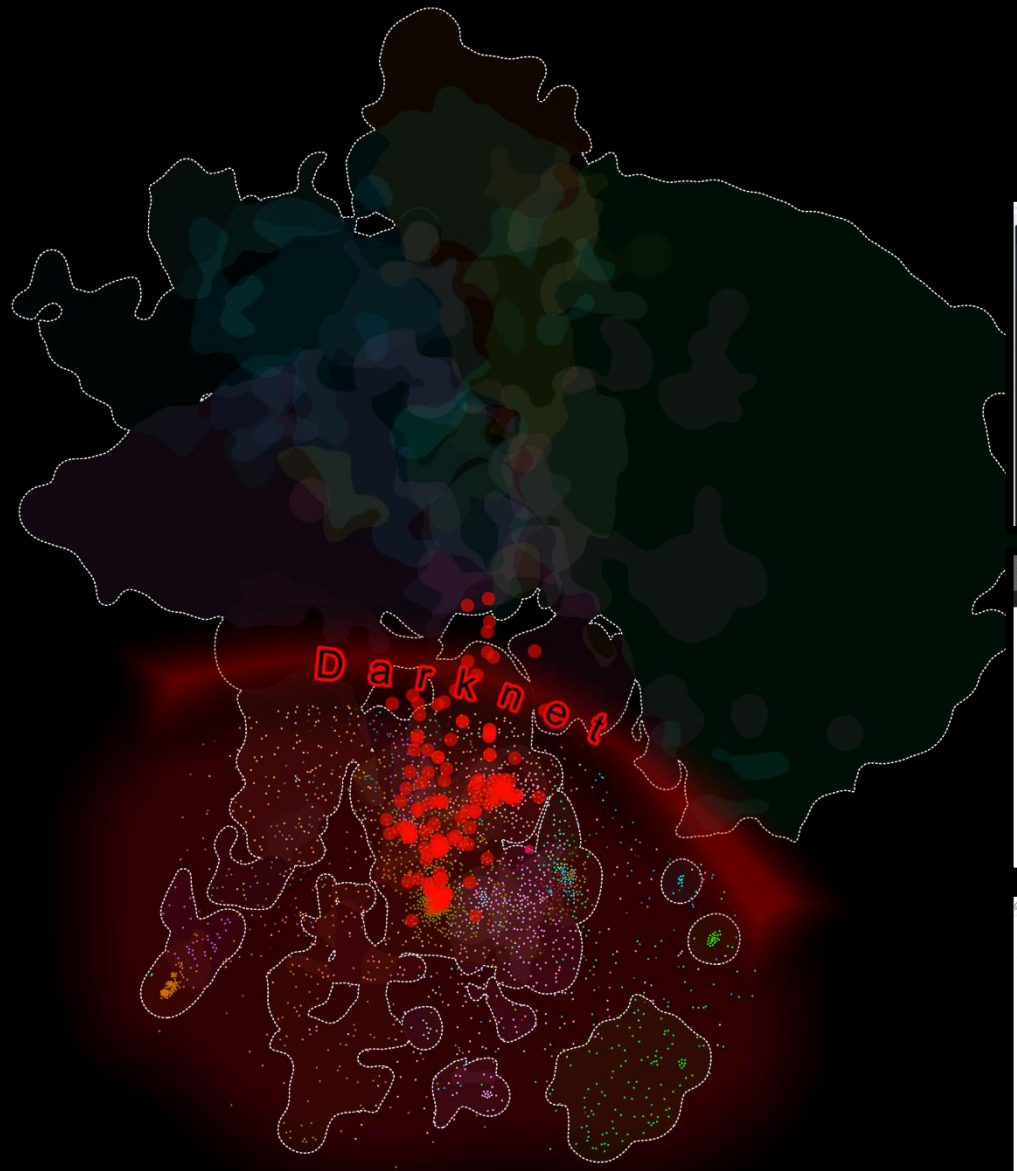
Информационная карта источников

TI-платформы



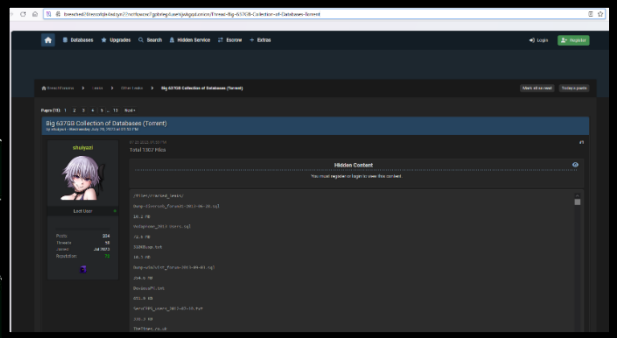


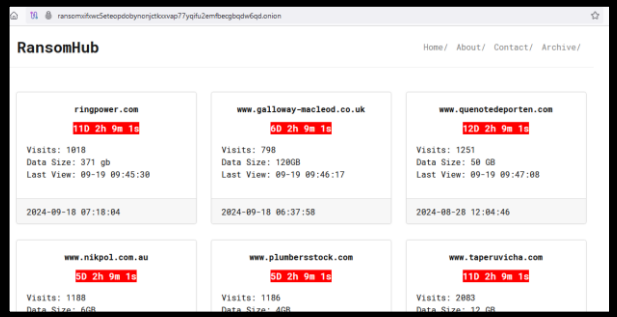
Источники исходных данных об угрозах безопасности информации

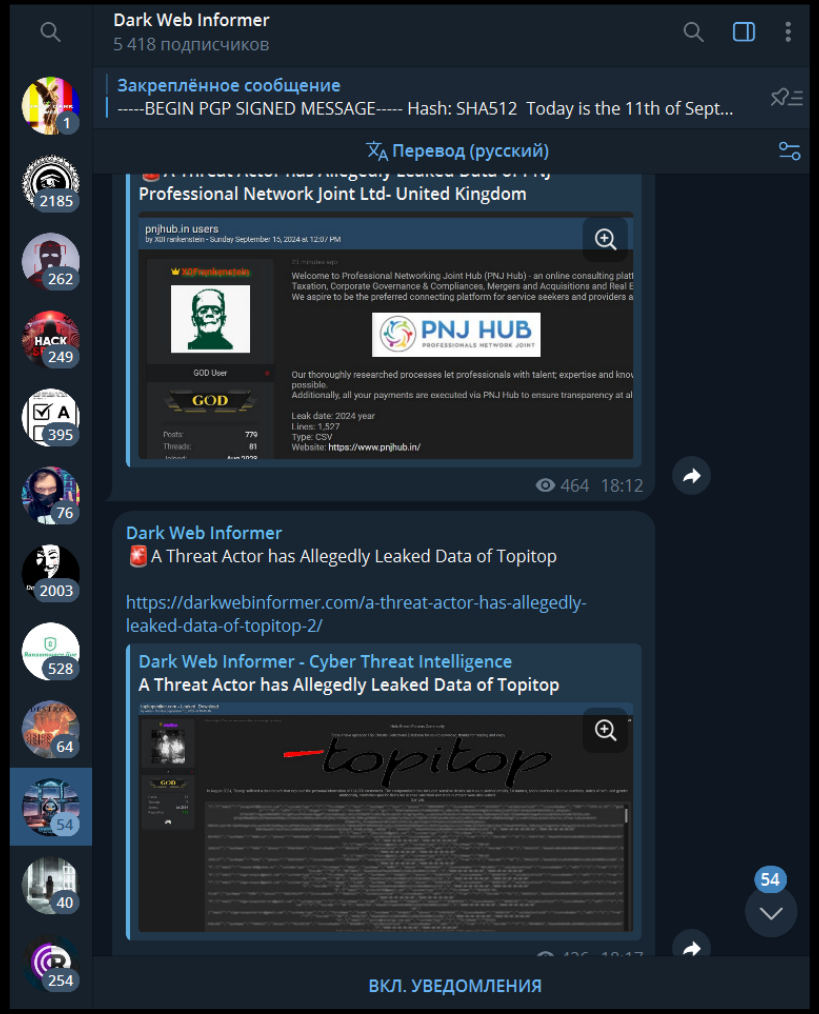


Информационная карта источников

Теневой интернет (Darknet)







Субъекты реализации угроз безопасности информации

Типы субъектов:

- **APT-группировки**
- Финансово-мотивированные группировки
- Кибернаёмники
- Хактивисты
- Низкоквалифицированные киберпреступники

Субъекты реализации угроз безопасности информации

Типы субъектов:

- APT-группировки
- **Финансово-мотивированные группировки**
- **Кибернаёмники**
- Хактивисты
- Низкоквалифицированные киберпреступники

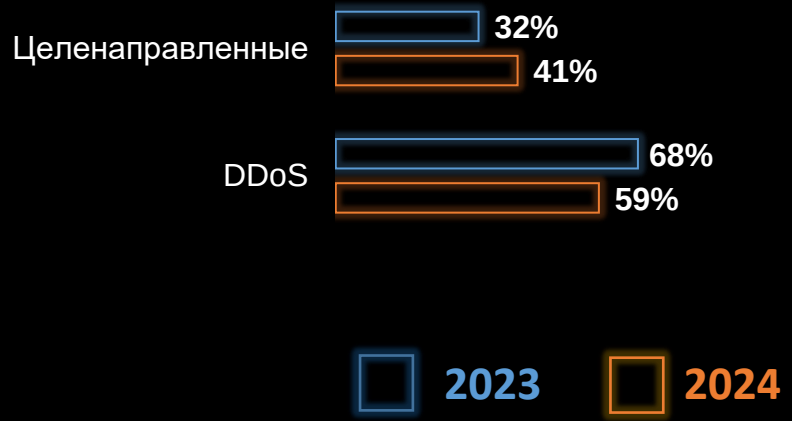
Субъекты реализации угроз безопасности информации

Типы субъектов:

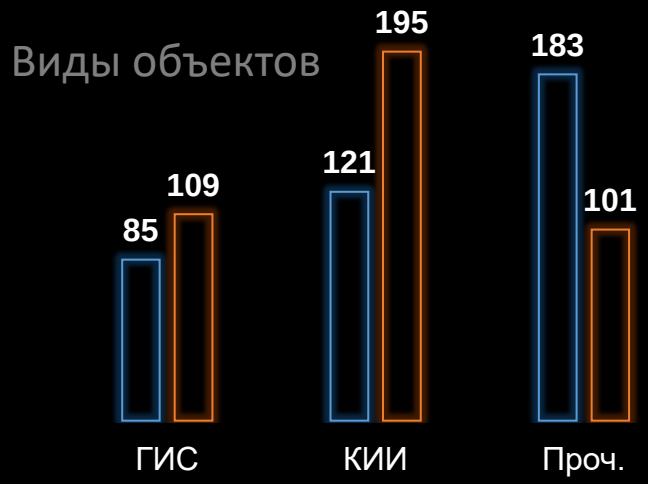
- APT-группировки
- Финансово-мотивированные группировки
- Кибернаёмники
- **Хактивисты**
- Низкоквалифицированные киберпреступники

Угрозы государственным информационным системам и объектам критической информационной инфраструктуры

Виды атак

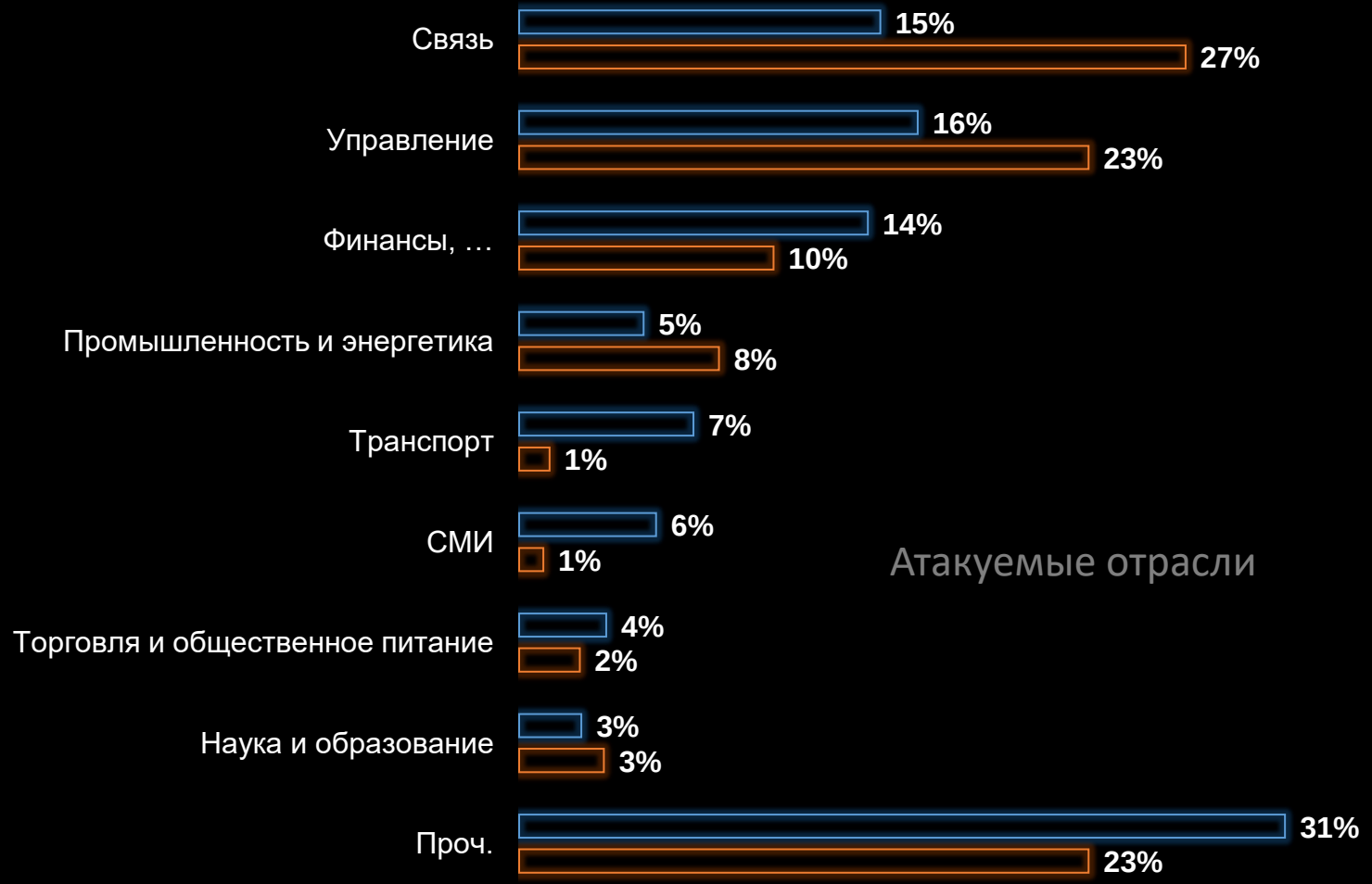


Виды объектов



зафиксировано упоминаний об инцидентах: **389** (2023 год), **405** (2024 год)

Атакуемые отрасли



Инструменты реализации угроз безопасности информации

Проникновение:

- массовое сканирование
- эксплойты
- подбор паролей
- фишинг

Закрепление и постэксплуатация:

- Cobalt Strike
- PowerSploit
- Impacket
  SecretsDump
- QuasarRAT
- Ngrok
- CrackMapExec
- AnyDesk

Проведение DDoS-атак:

- Gorgon Stress
- mhddos proxy

Основные источники данных

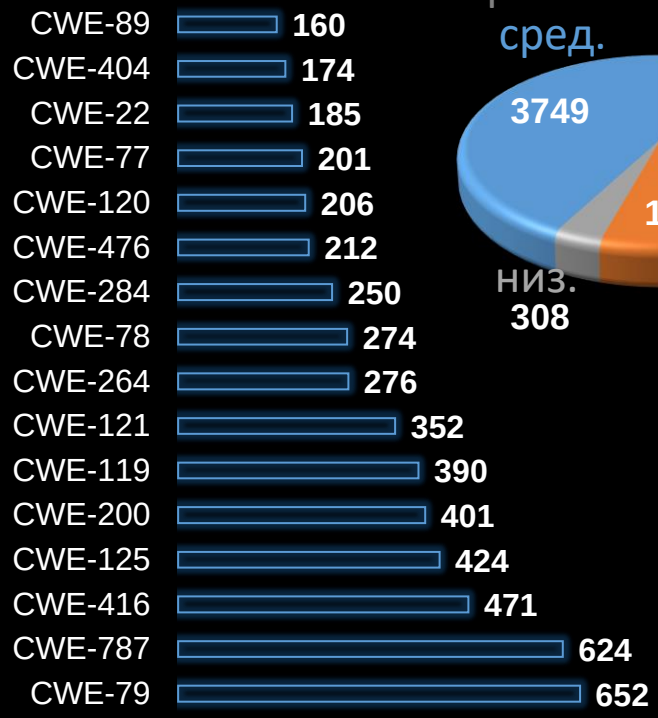
Взаимосвязь группировок, инструментов и объектов атаки

Уязвимости и эксплойты

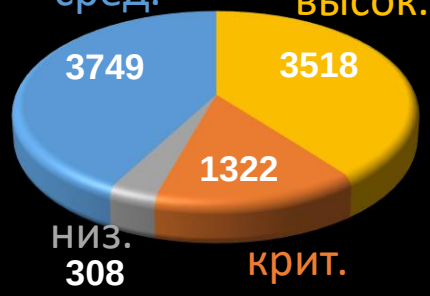
обнаружено и внесено в БДУ

2023

8897 шт.



Уровень опасности



1770 (2677)

с эксплойтами

Типы ошибок

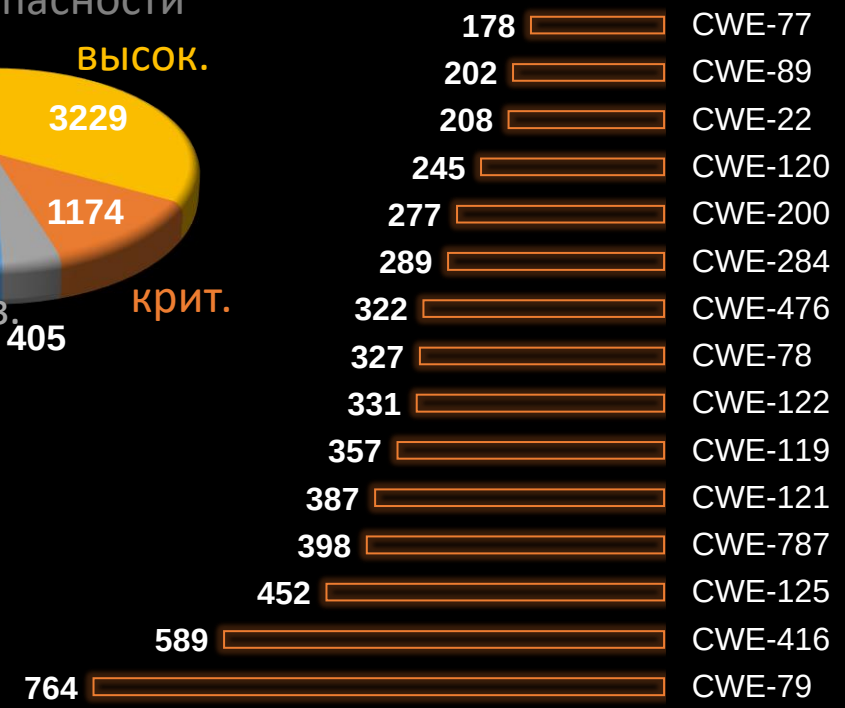
668

(отмечены в атаках)

Типы ПО

2024

9774 шт.



Уровень опасности

Типы ошибок

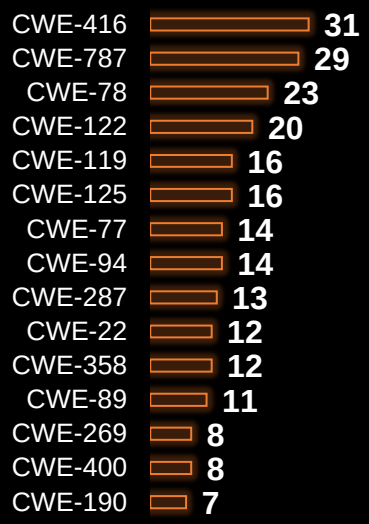
383

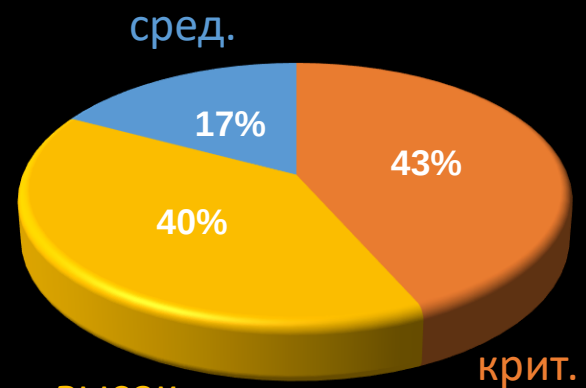
(отмечены в атаках)

1479 (2283)

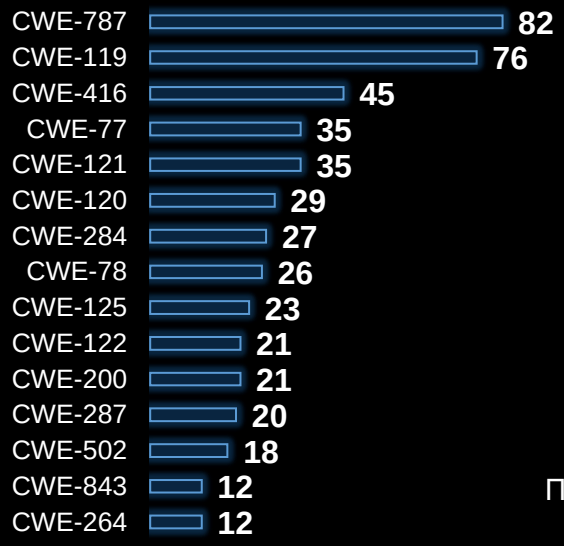
с эксплойтами

Тенденции эксплуатации уязвимостей. Связь с инцидентами ИБ



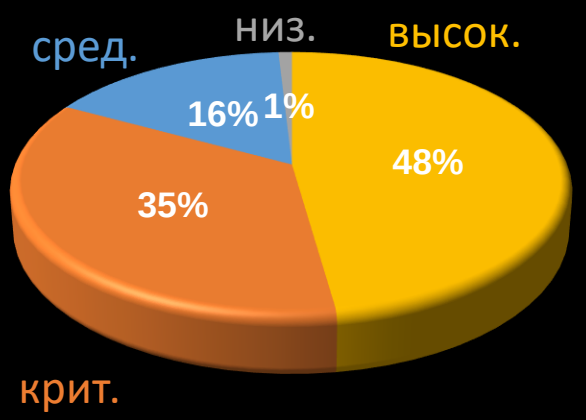


Типы ошибок

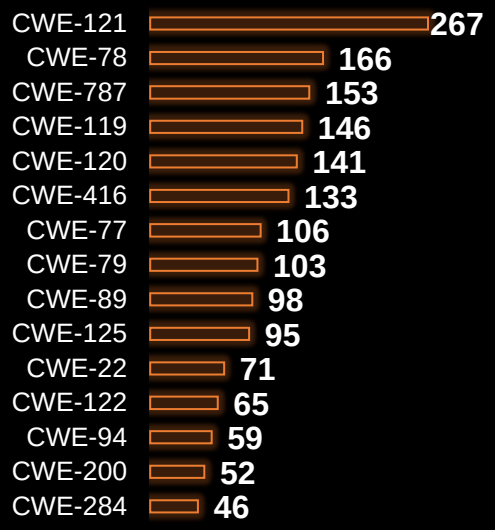


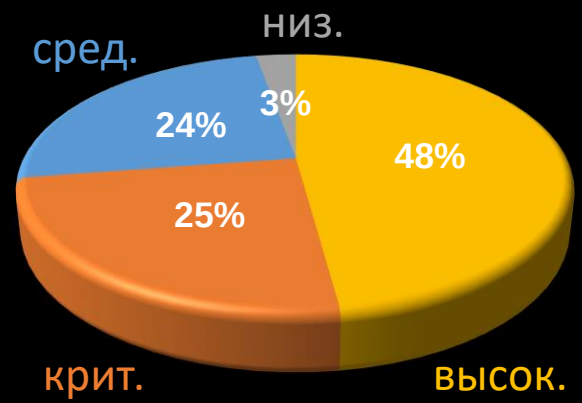
Типы ПО

Уровень опасности



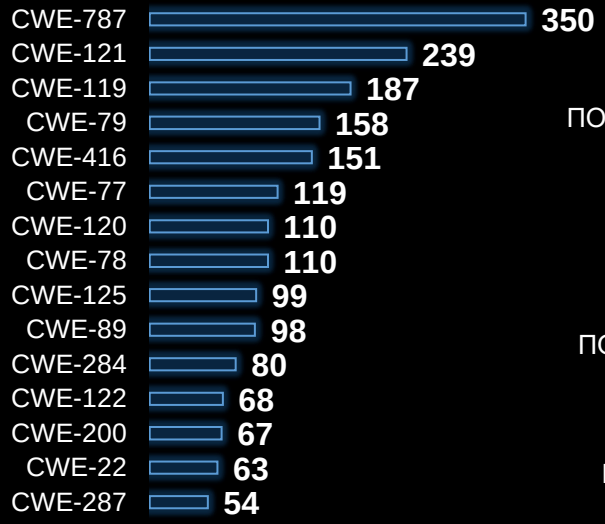
Тенденции эксплуатации уязвимостей. Наличие эксплойтов





2024

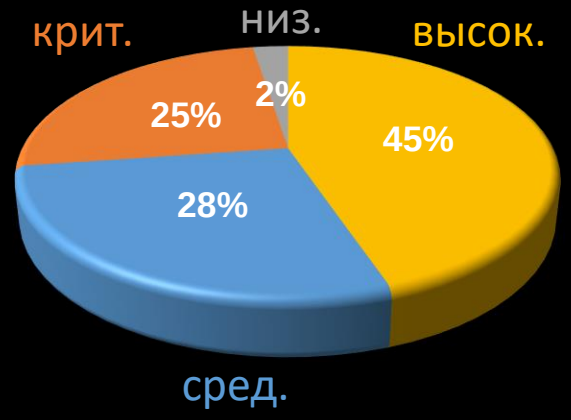
Типы ошибок



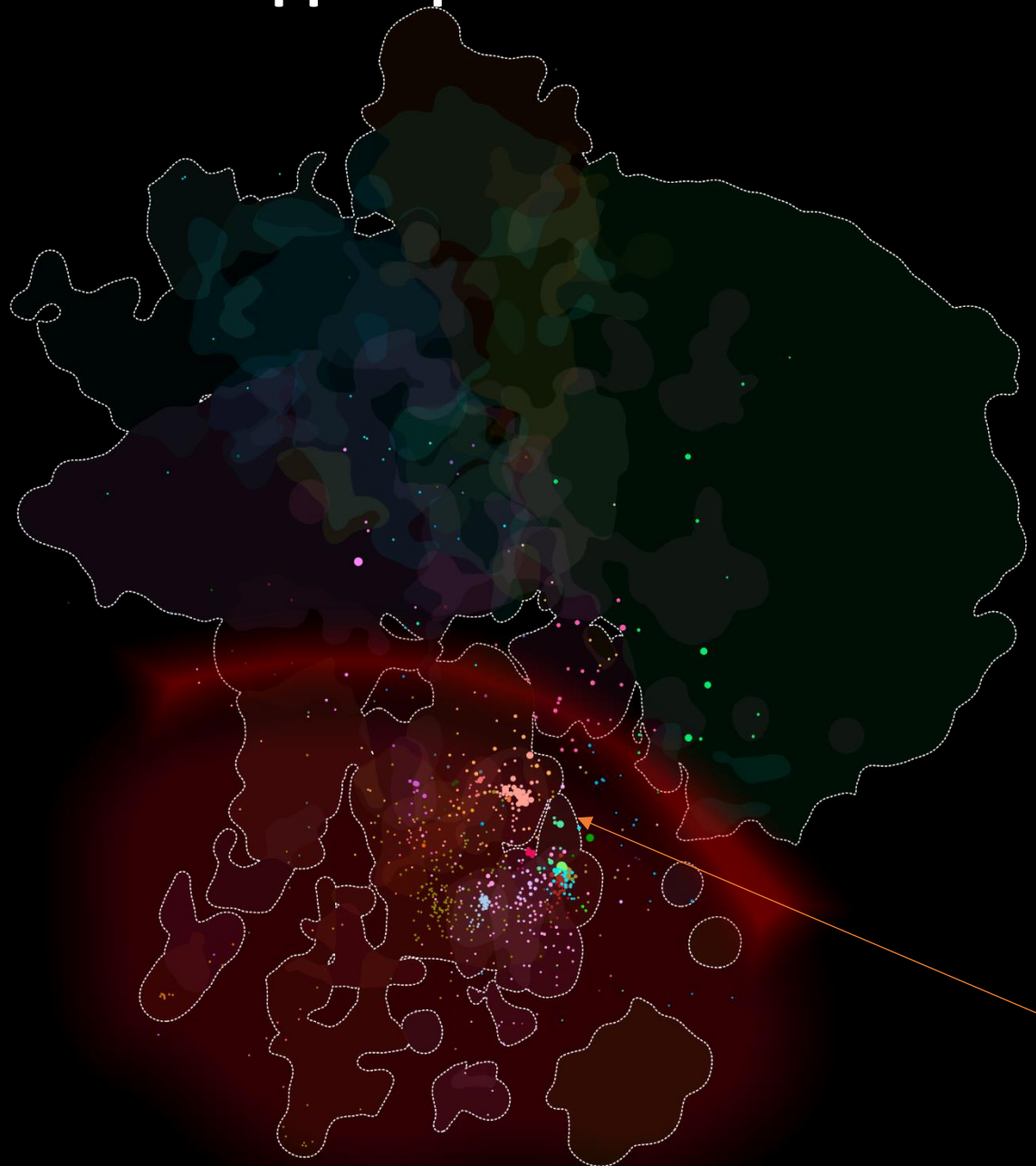
Типы ПО

Уровень опасности

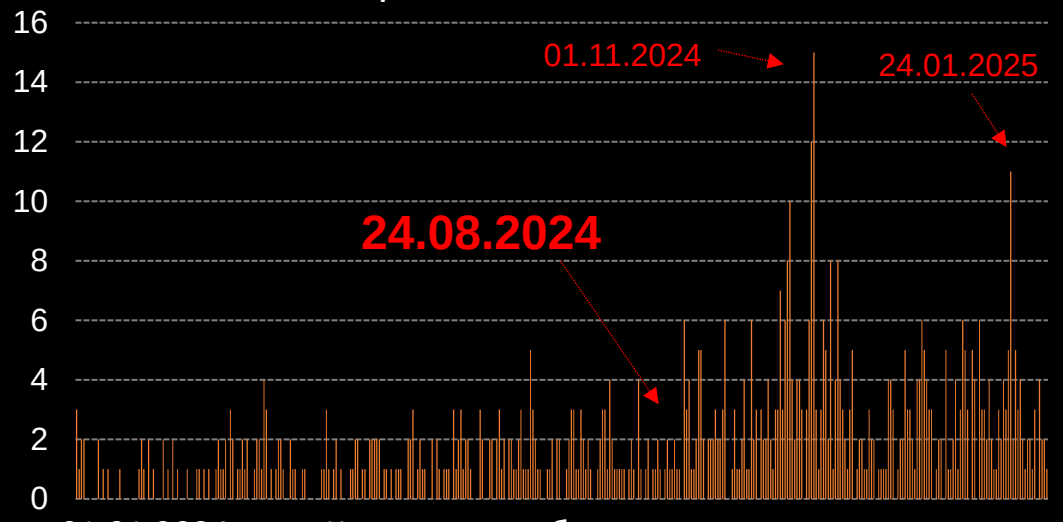
2023



Тенденции теневого сегмента сети Интернет (Darknet)



Усиление блокировок источников



Тенденции развития угроз безопасности информации

- угрозы центрам обработки данных и операторам связи
- угрозы промышленным информационным системам
- угрозы региональным государственным информационным системам
- автоматизация компьютерных атак с помощью машинного обучения

Меры защиты

Базовые меры

- идентификация и аутентификация
- управление доступом
- защита периметра и конечных точек
- устранение уязвимостей
- регистрация и учет
- повышение осведомленности сотрудников
- резервирование данных

Меры для защиты от нарушителей высокого уровня опасности

- разведка угроз
- SIEM
- ложные информационные системы
- другие усиливающие меры