

Тенденции развития угроз безопасности информации

Докладчик: Сердечный Алексей

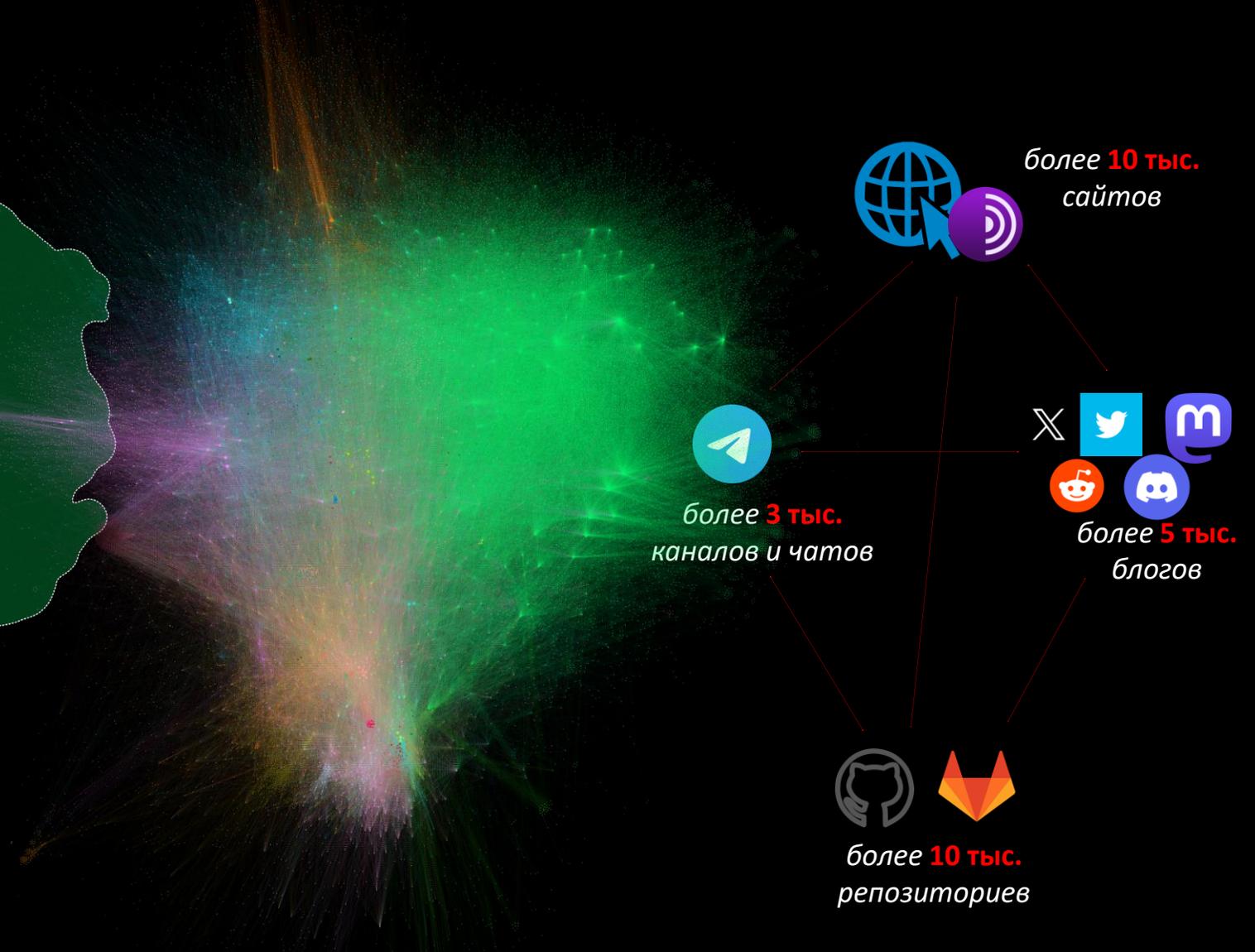


ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Источники исходных данных об угрозах безопасности информации



Информационная карта источников



Граф связей источников

Источники исходных данных об угрозах безопасности информации

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

bdu.fstec.ru
snyk.io
security.snyk.io
exploitify.haxx.it
cve.mitre.org
attack.mitre.org
misp-project.org
ransomlook.io
cisa.gov
exploit-db.com
capec.mitre.org
ransomfeed.it
web.nvd.nist.gov
nvd.nist.gov
cxsecurity.com
packetstormsecurity.com
ransomware.live
haveibeenpwned.com



Информационная карта источников

Источники исходных данных об угрозах безопасности информации

Пример тематического анализа группы источников



Информационная карта источников

ZLONOV.ru
Сайт Алексея Комарова

Блог Публикации Выступления КИИ Ещё

Каналы и чаты Telegram по информационной безопасности

Дата актуализации числа подписчиков/участников:
07.02.2025

Все подборки Каналы Telegram Чаты Telegram Подкасты Блоги

Отказ от ответственности: не берусь судить о качестве и полезности представленных ресурсов и не могу контролировать их содержимое. Список приведён исключительно в исследовательских целях для самостоятельного изучения и выбора достойных источников информации.

Вероятно, не всё в списке напрямую относится к теме информационной безопасности - подробнее описывал [тут](#). Могу уверенно рекомендовать лишь свой собственный канал [@ZLONOV](#) и чаты, в которых являюсь администратором/владельцем: [КИИ 187-ФЗ](#), [Пдн 152-ФЗ](#), [ЭП 63-ФЗ](#), [Все ФЗ про ИБ](#), [Кибербезопасность АСУ ТП](#), [ruCyberSecurity](#).

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

Источники исходных данных об угрозах безопасности информации

TI-платформы



Screenshot of a TI platform interface showing a file analysis page for LaunchWinApp.exe. The page displays a Community Score of 55/73, a list of vendors (peee, checks-user-input, long-s), and a list of comments. The original filename is 2024-09-19_a#32945527f3ad0e93161e49c38121. Comments include:

- petik: 3 minutes ago
- Original filename: 2024-09-19_a#32945527f3ad0e93161e49c38121
- Comment added on 2024-09-19 09:28:49 French Time Zone
- MWDB Link: <https://mwdb.com.pl/files/2fcddb64074eb5167979511d2806>
- Trigo Link: <https://trigo.ge/240919-j4n4kaxopl>
- VXUG Link: <https://virus.exchange/samples/>
- VirusShare Link: <https://virusshare.com/files/2fcddb64074eb5167979511d2806>

Screenshot of a TI platform interface showing a world map of APT organization distribution. The map is titled "APT组织分布全景图" and displays various APT groups across different regions. A bar chart on the right shows the "2022全年APT组织活动情况" (2022 Full Year APT Organization Activity Situation) with the following data:

Organization	Activity Count
Lockbit	8
Kimmyky	8
APT29	7
APT35	7
MuddyWater	6
海莲花	6
APT38	6
APT37	6
APT33	6
APT34	6
APT36	6
APT32	6
APT31	6
APT30	6
APT28	6
APT27	6
APT26	6
APT25	6
APT24	6
APT23	6
APT22	6
APT21	6
APT20	6
APT19	6
APT18	6
APT17	6
APT16	6
APT15	6
APT14	6
APT13	6
APT12	6
APT11	6
APT10	6
APT9	6
APT8	6
APT7	6
APT6	6
APT5	6
APT4	6
APT3	6
APT2	6
APT1	6

Screenshot of the Malpedia website showing a search for LockBit. The page displays the search results for LockBit, including a list of references and a "Propose Change" button. The references include:

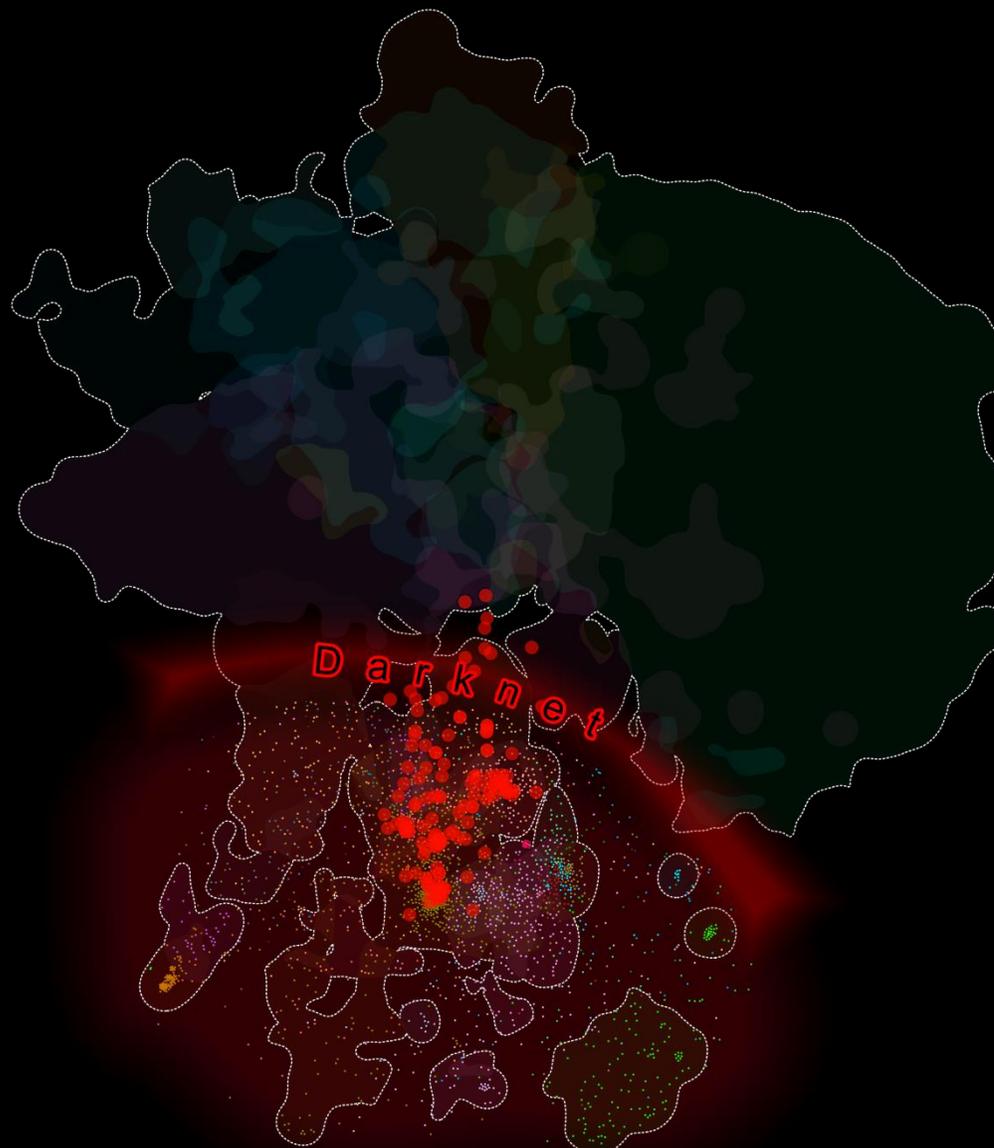
- 2024-02-29 - ANALYSIS - Anastasia Semsova, Jon DiMaggio: LockBit Takedown & Operation Cronos: A Long-Awaited PsyOps Against Ransomware
- 2024-02-28 - Washington Post - Leo Sands: World's most harmful' cybercriminal group disrupted in 11-nation operation
- 2024-02-28 - Eurapol - Eurapol: Law enforcement disrupt world's biggest ransomware operation
- 2024-02-29 - National Crime Agency - National Crime Agency (NCA): International investigation disrupts the world's most harmful cyber crime group
- 2023-10-03 - Luca Pella: Lighting the Exfiltration Infrastructure of a LockBit Affiliate (and more)
- 2023-09-07 - PROOFPOINT - PROOFPOINT: PIT-257 (ex-Wizard Spider) - IOCs

Screenshot of the Head Mare malware analysis page. The page displays the title "Head Mare: adventures of a unicorn in Russia and Belarus" and provides a detailed overview of the malware, including its capabilities, target countries, and industries. The page also includes a "Types of Indicators" section and a "Threat Infrastructure" section.

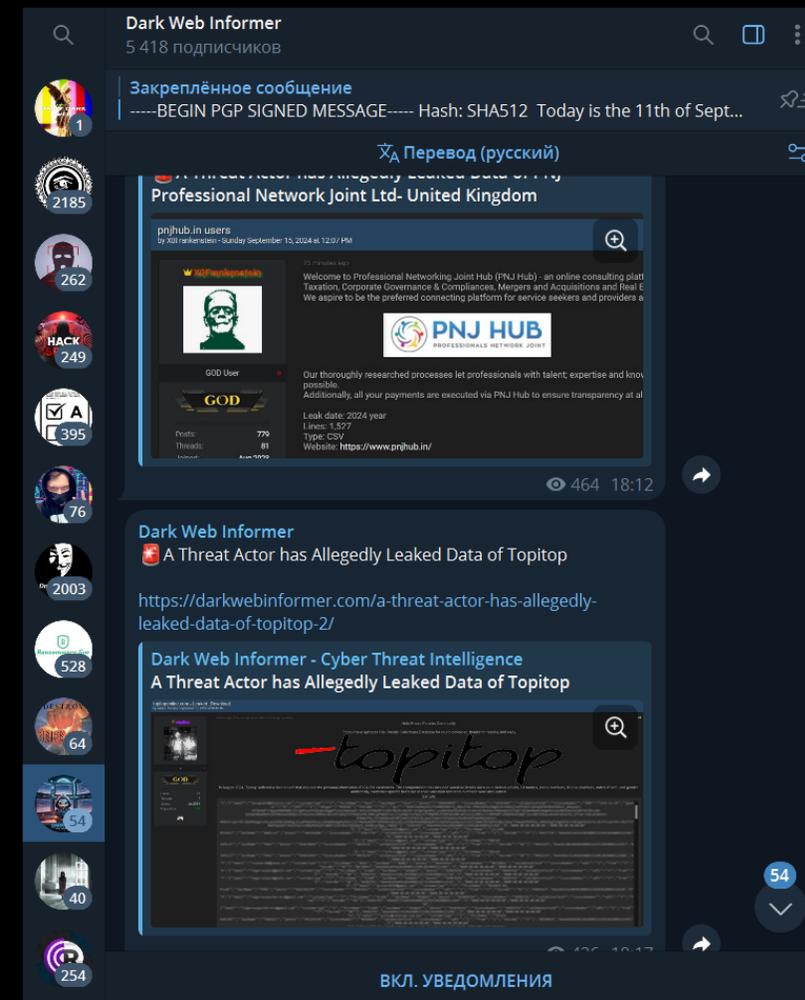
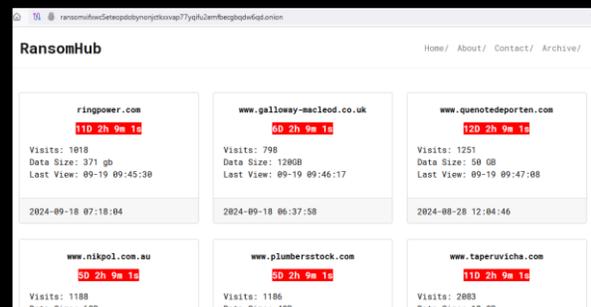
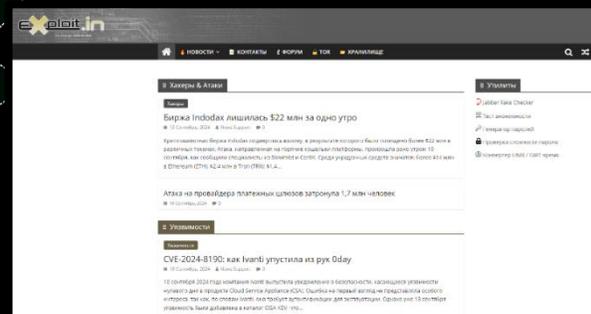
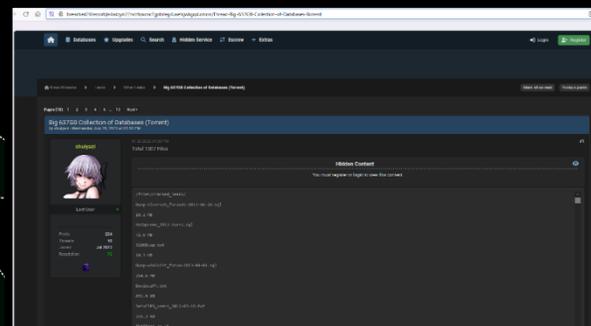
Информационная карта источников

Источники исходных данных об угрозах безопасности информации

Теневой интернет (Darknet)



Информационная карта источников



Субъекты реализации угроз безопасности информации

Типы субъектов:



■ АPT-группировки

■ Финансово-мотивированные группировки

■ Кибернаёмники

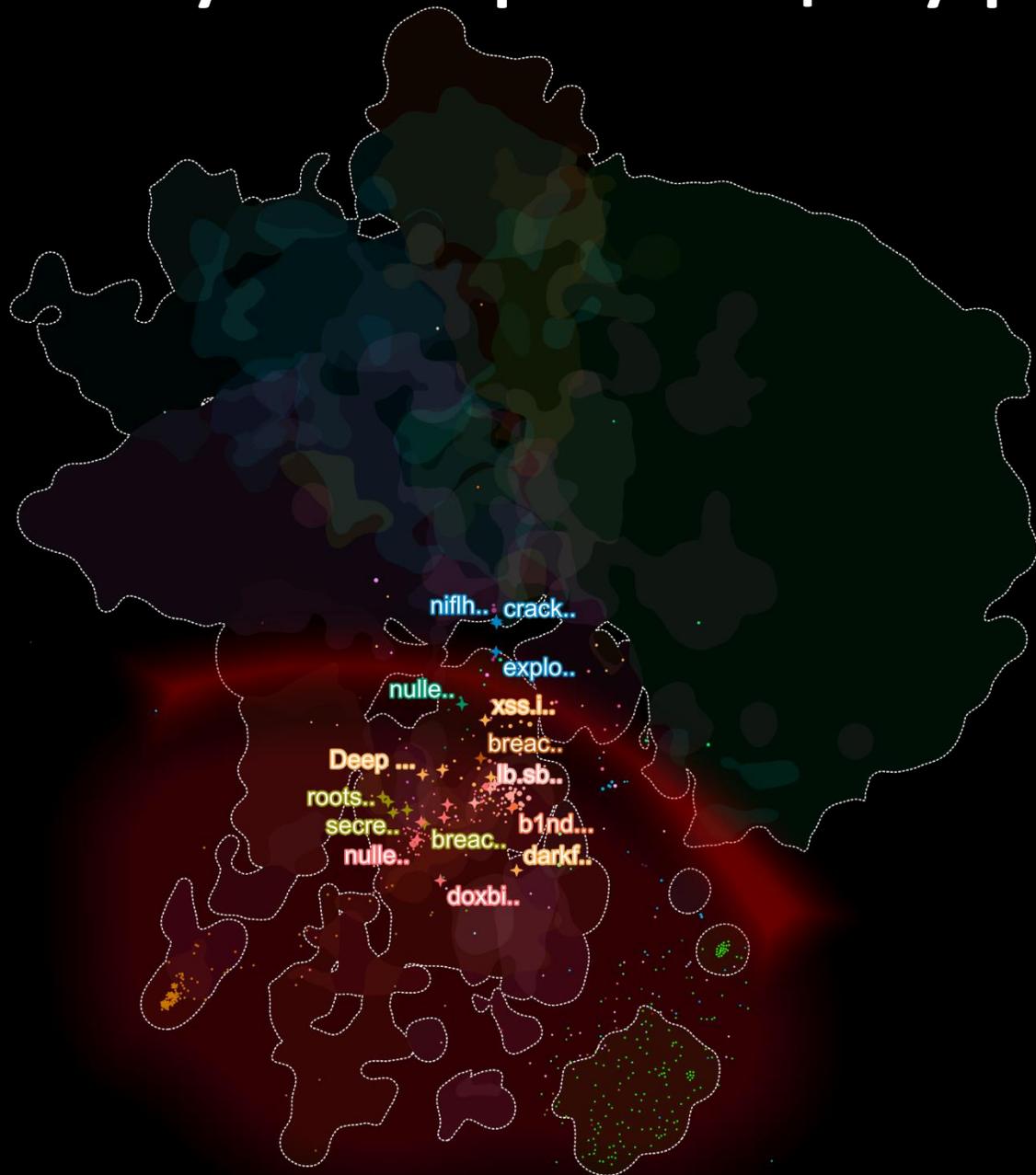
■ Хактивисты

■ Низкоквалифицированные киберпреступники

Субъекты реализации угроз безопасности информации

Типы субъектов:

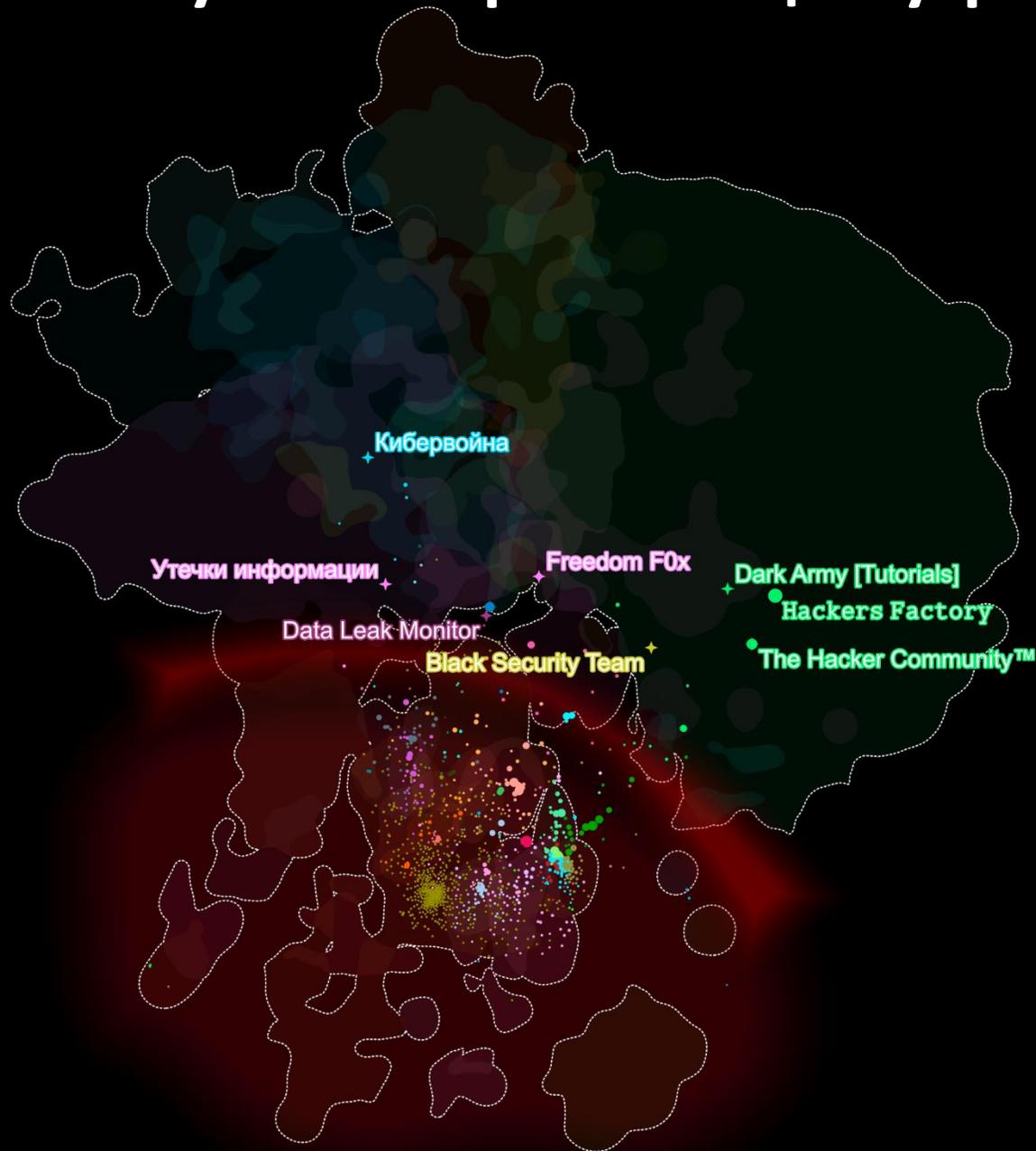
- АPT-группировки
- **Финансово-мотивированные группировки**
- **Кибернаёмники**
- Хактивисты
- Низкоквалифицированные киберпреступники



Субъекты реализации угроз безопасности информации

Типы субъектов:

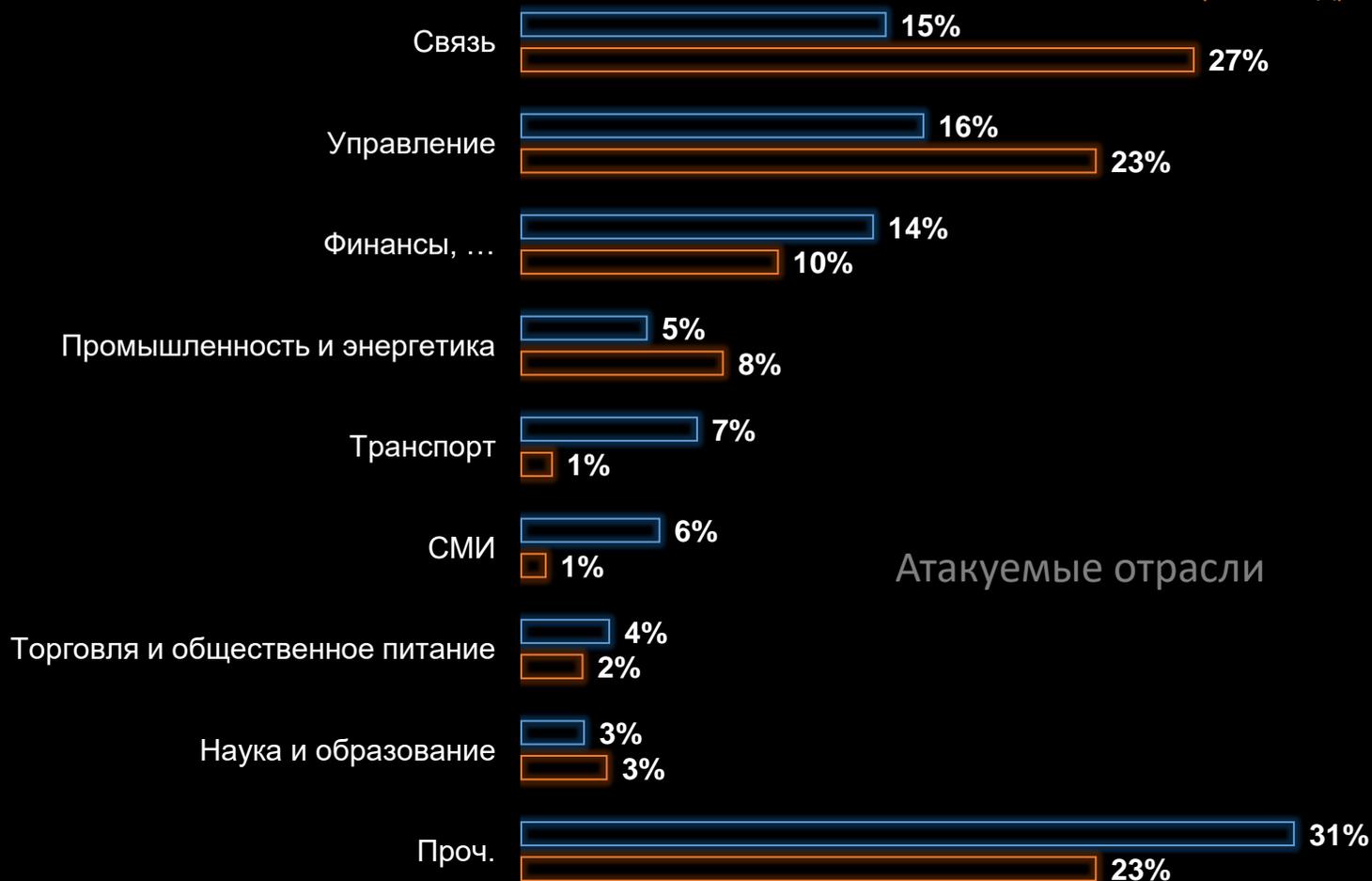
- АPT-группировки
- Финансово-мотивированные группировки
- Кибернаёмники
- **Хактивисты**
- Низкоквалифицированные киберпреступники



Угрозы государственным информационным системам и объектам критической информационной инфраструктуры



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



Инструменты реализации угроз безопасности информации

Проникновение:

- массовое сканирование
- подбор паролей
- эксплойты
- 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

8897 шт.

2023



CWE-89	160
CWE-404	174
CWE-22	185
CWE-77	201
CWE-120	206
CWE-476	212
CWE-284	250
CWE-78	274
CWE-264	276
CWE-121	352
CWE-119	390
CWE-200	401
CWE-125	424
CWE-416	471
CWE-787	624
CWE-79	652

Типы ПО

Средство защиты	166
ПО виртуализации	172
Средство АСУ ТП	269
СУБД	311

Микропрограммный код

Микропрограммный код	524
Сетевое (аппарат.)	990
Сетевое (программное)	1140
Операционная система	3497
Прикладное	4244

Сетевое (аппарат.)

Сетевое (аппарат.)	990
Сетевое (программное)	1140
Операционная система	3497
Прикладное	4244

Сетевое (программное)

Сетевое (аппарат.)	990
Сетевое (программное)	1140
Операционная система	3497
Прикладное	4244

Операционная система

Сетевое (аппарат.)	990
Сетевое (программное)	1140
Операционная система	3497
Прикладное	4244

Прикладное

Сетевое (аппарат.)	990
Сетевое (программное)	1140
Операционная система	3497
Прикладное	4244

2024

9774 шт.



CWE-77	178
CWE-89	202
CWE-22	208
CWE-120	245
CWE-200	277
CWE-284	289
CWE-476	322
CWE-78	327
CWE-122	331
CWE-119	357
CWE-121	387
CWE-787	398
CWE-125	452
CWE-416	589
CWE-79	764

Типы ошибок

383

(отмечены в атаках)

1770

(2677)

с эксплойтами

Типы ошибок

668

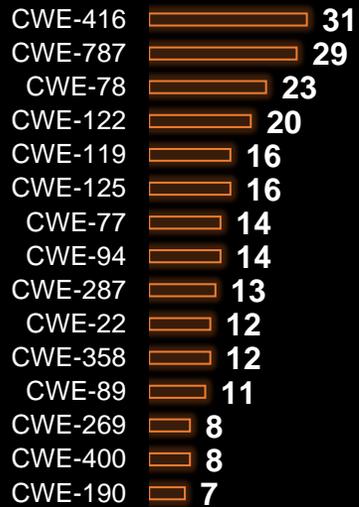
(отмечены в атаках)

1479

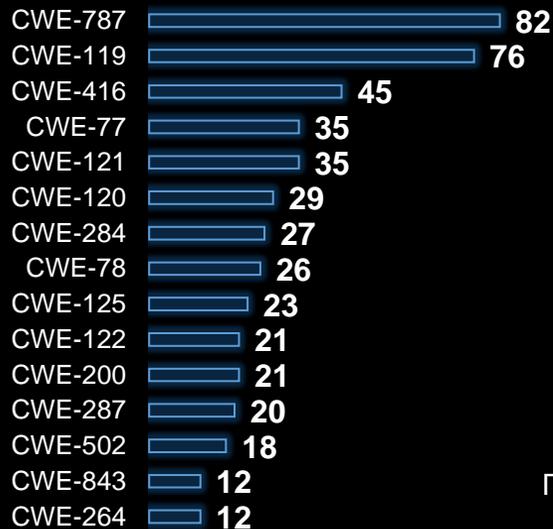
(2283)

с эксплойтами

Тенденции эксплуатации уязвимостей. Связь с инцидентами ИБ



Типы ошибок



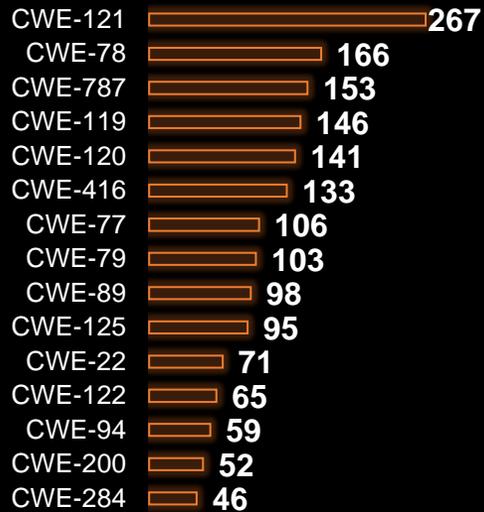
Типы ПО



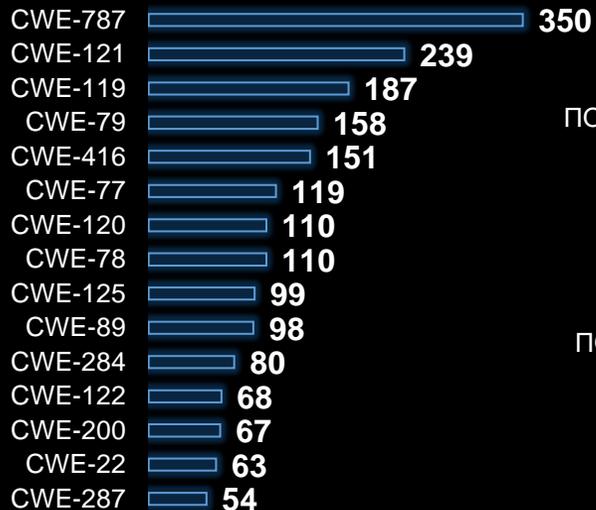
Уровень опасности



Тенденции эксплуатации уязвимостей. Наличие эксплойтов



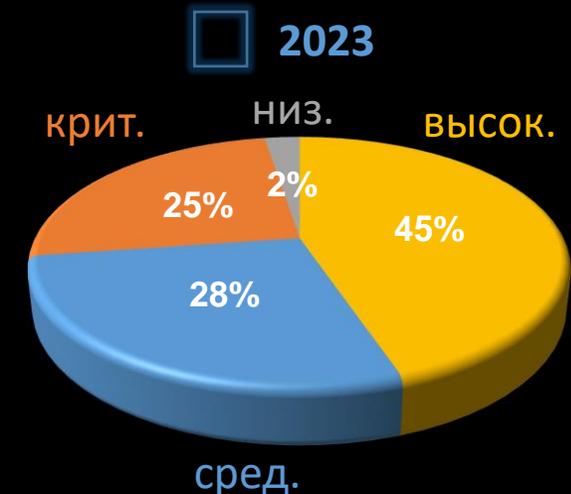
Типы ошибок



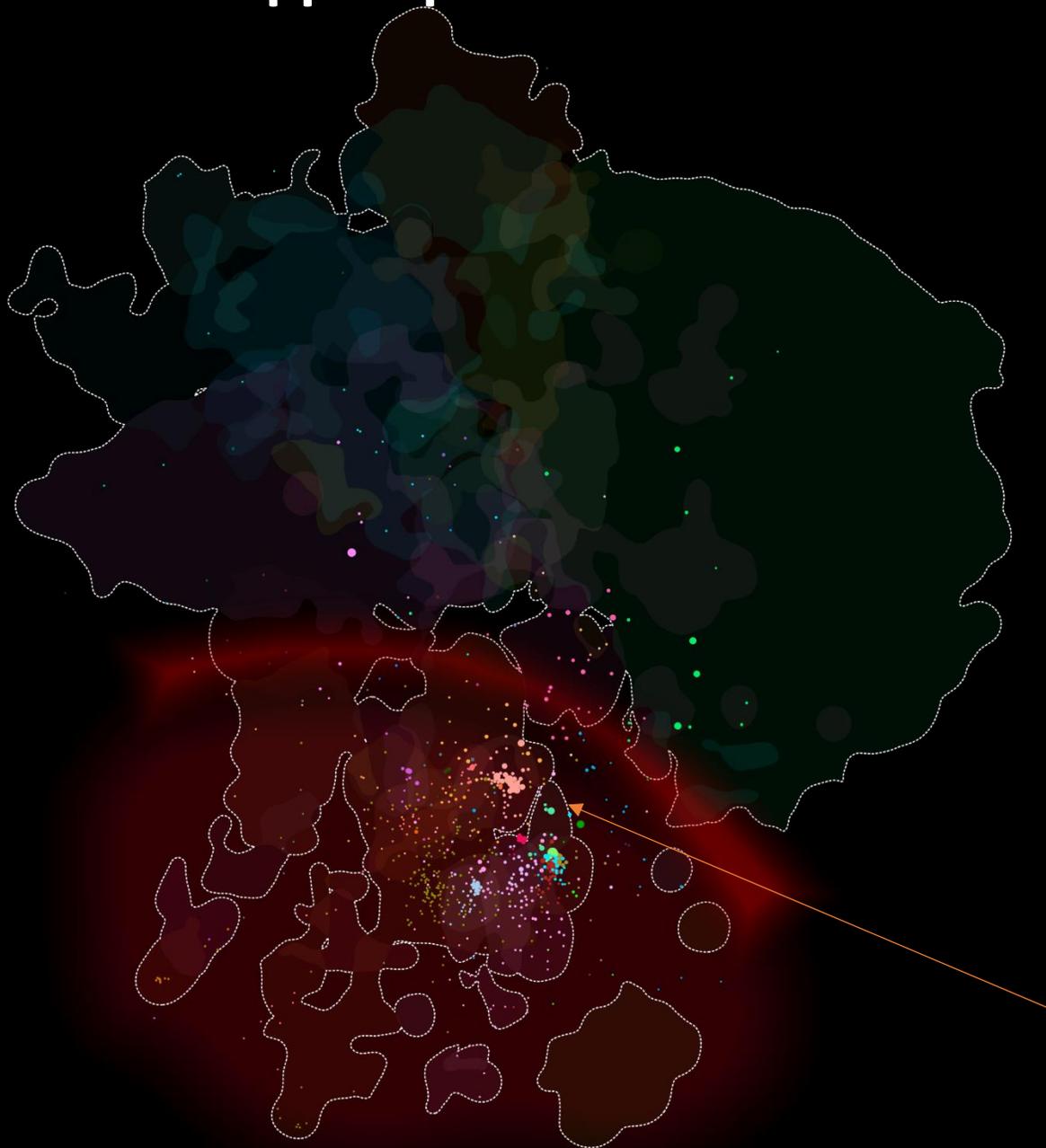
Типы ПО



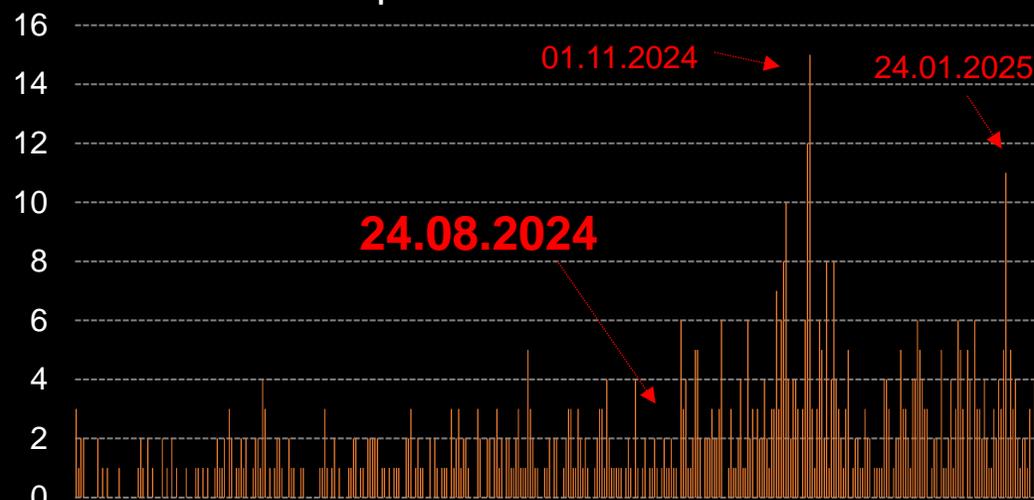
Уровень опасности



Тенденции теневого сегмента сети Интернет (Darknet)



Усиление блокировок источников



Количество заблокированных источников в день

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