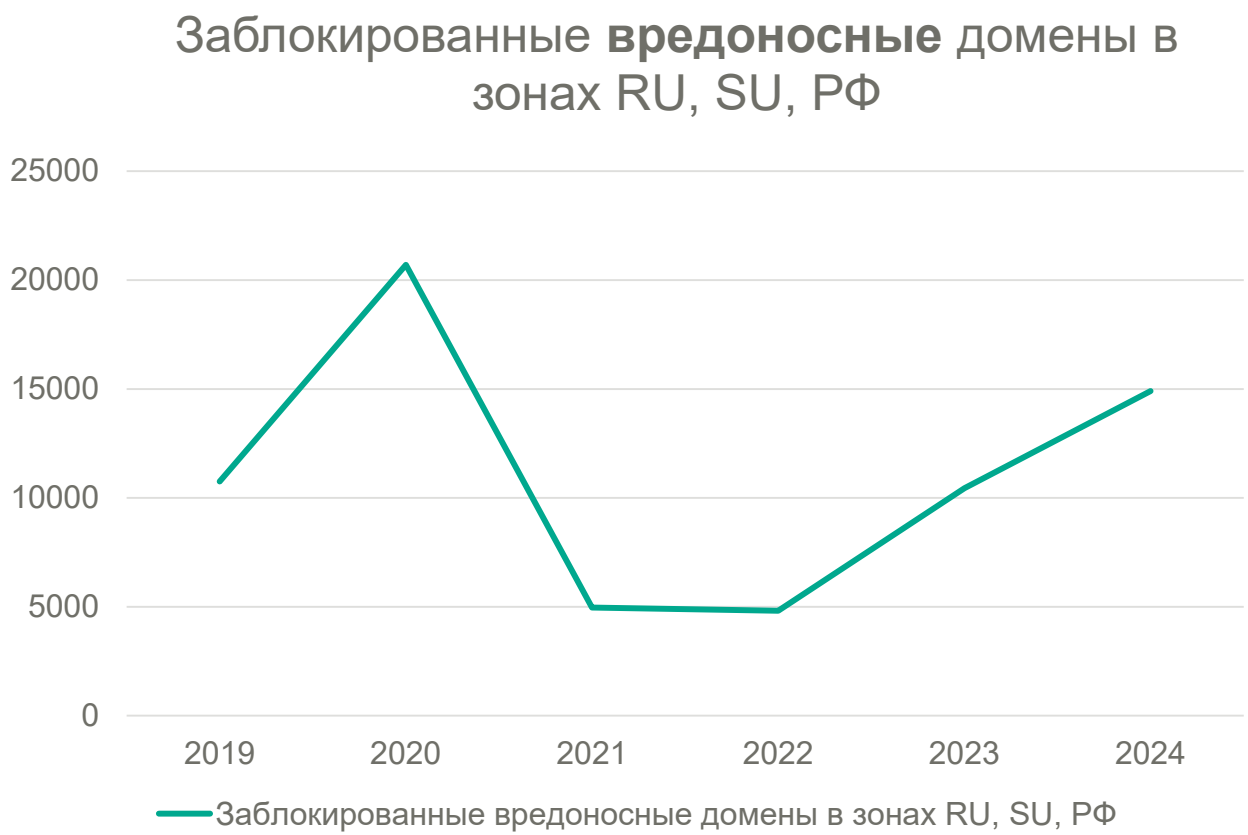
План

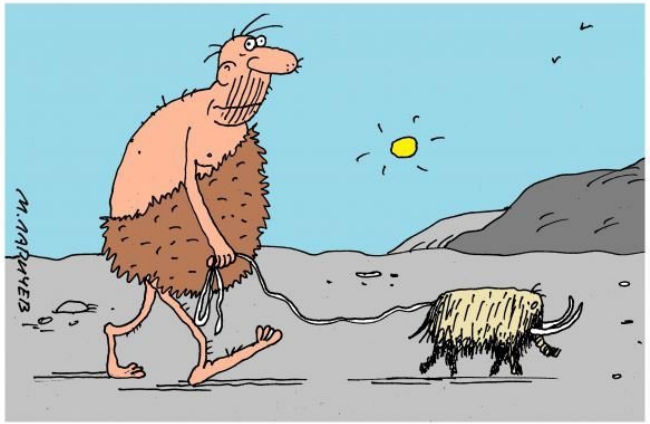
- **Немного статистики**
- **Как мы используем Netoscope**
- **Примеры угроз**
  - Mamont – AndroidOS Banker
  - Lumma stealer
  - DCRat backdoor

Немного статистики

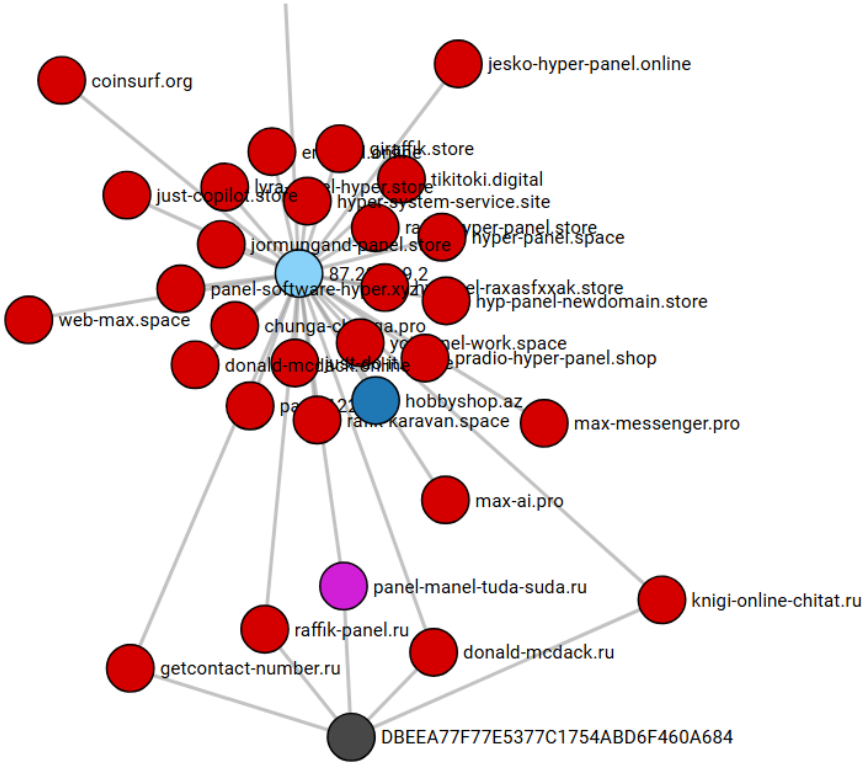


Период	Количество
H1 2025	5871
2024	14905
2023	10445
2022	4817
2021	4966
2020	20702
2019	10751

- Наиболее объемные источники поставляют данные об уже известных угрозах
- Для проактивного обнаружения – поиск похожего, построение связей



- Свыше 10К атак в месяц
- Распространяется через мессенджеры
- Перехватывает финансовые учетные данные, SMS-сообщения, пуш-уведомления, прочее.



DBEEA77F77E5377C1754ABD6F460A684

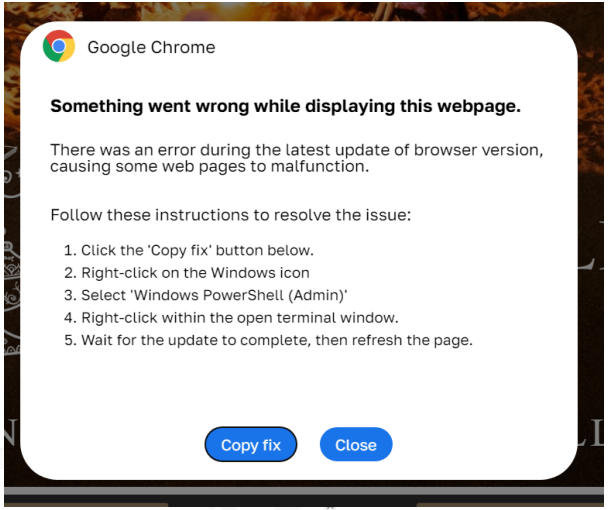
- panel-manel-tuda-suda.ru
- donald-mcdack.ru
- getcontact-number.ru
- knigi-online-chitat.ru
- raffik-panel.ru

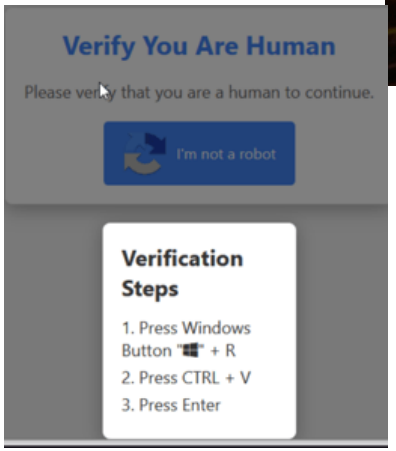
87.236.19.2

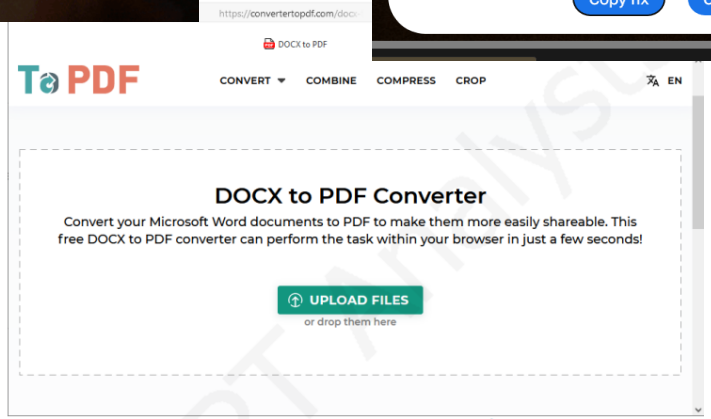
- max-messenger.pro
- max-ai.pro
- tikitoki.digital
- jeki-chan.xyz
- chunga-changa.pro
- serverconfig.ru
- …

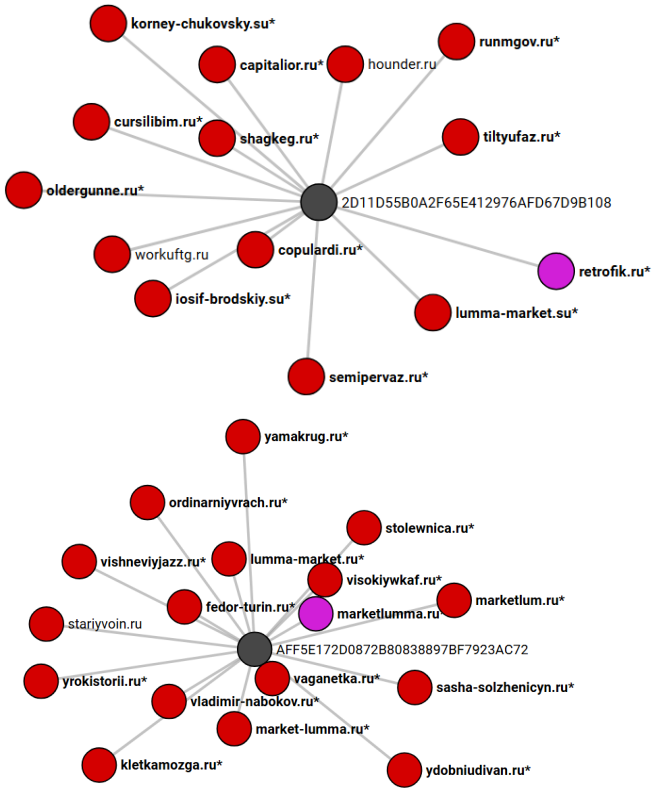
- Около 32К атакованных пользователей в 2024 (преимущественно Россия и Бразилия)
- Распространяется при помощи зараженных сайтов и под видом легитимного ПО
- Ворует данные криптокошельков, cookies и пароли из браузеров, данные из почтовых клиентов и прочего ПО

Способы распространения









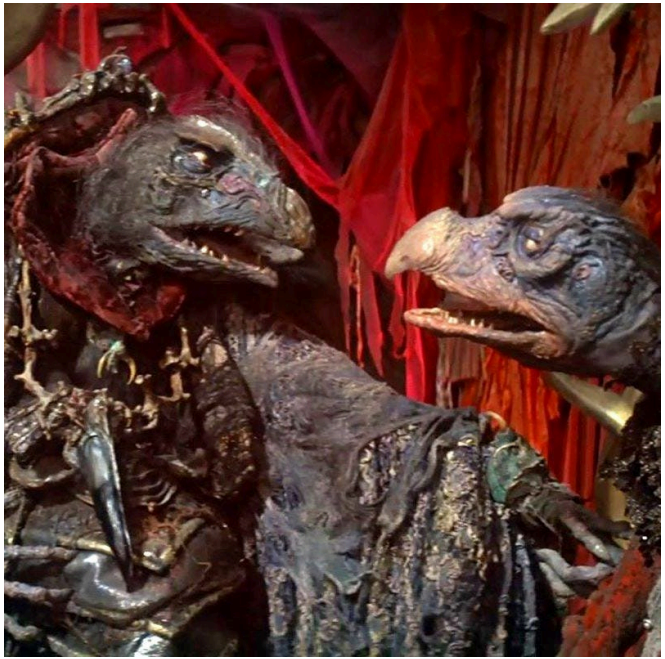
AFF5E172D0872B80838897BF7923AC72

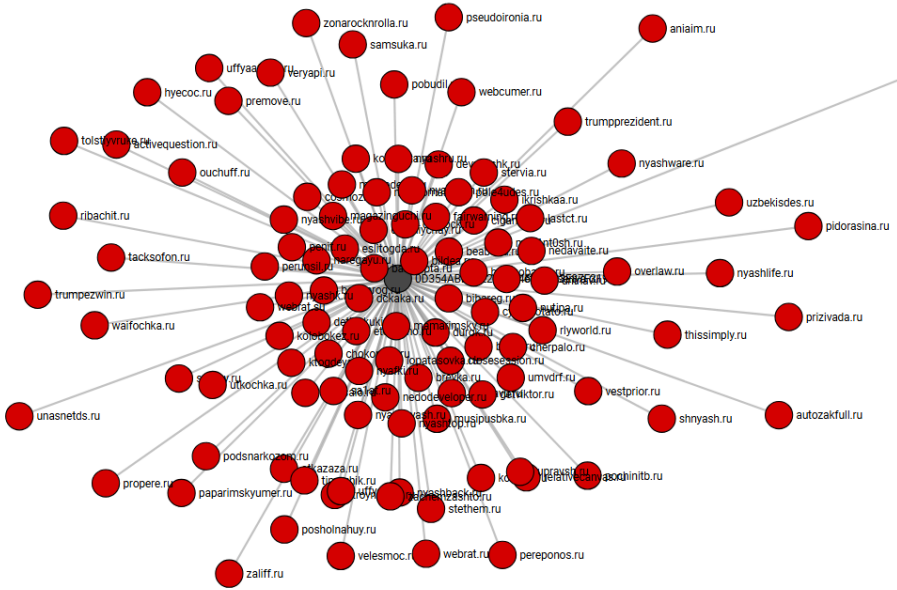
- sasha-solzhenicyn.ru
- vladimir-nabokov.ru
- ydobniudivan.ru
- lumma-market.ru
- …

2D11D55B0A2F65E412976AFD67D9B108

- iosif-brodskiy.su
- korney-chukovsky.su
- lumma-market.su
- …

- Dark Crystal Remote Access Tool
- Распространение: YouTube видео с рекомендациями читов и кряков
- Функционал: запись нажатий клавиш, доступ к веб-камере, кража паролей и другие модули





0d354abd94e251d846aacc3e87f3195d

- nyanyash.ru
- nyashback.ru
- nyashk.ru
- nyashlife.ru
- nyashnyash.ru
- nyashru.ru
- nyashtop.ru
- nyashvibe.ru
- nyashware.ru
- …
- zachemzashto.ru
- ktogdeya.ru
- gugugusi.ru
- cherniychay.ru
- …

Спасибо

Victoria.Vlasova@kaspersky.com