F6

TLDCON 2025

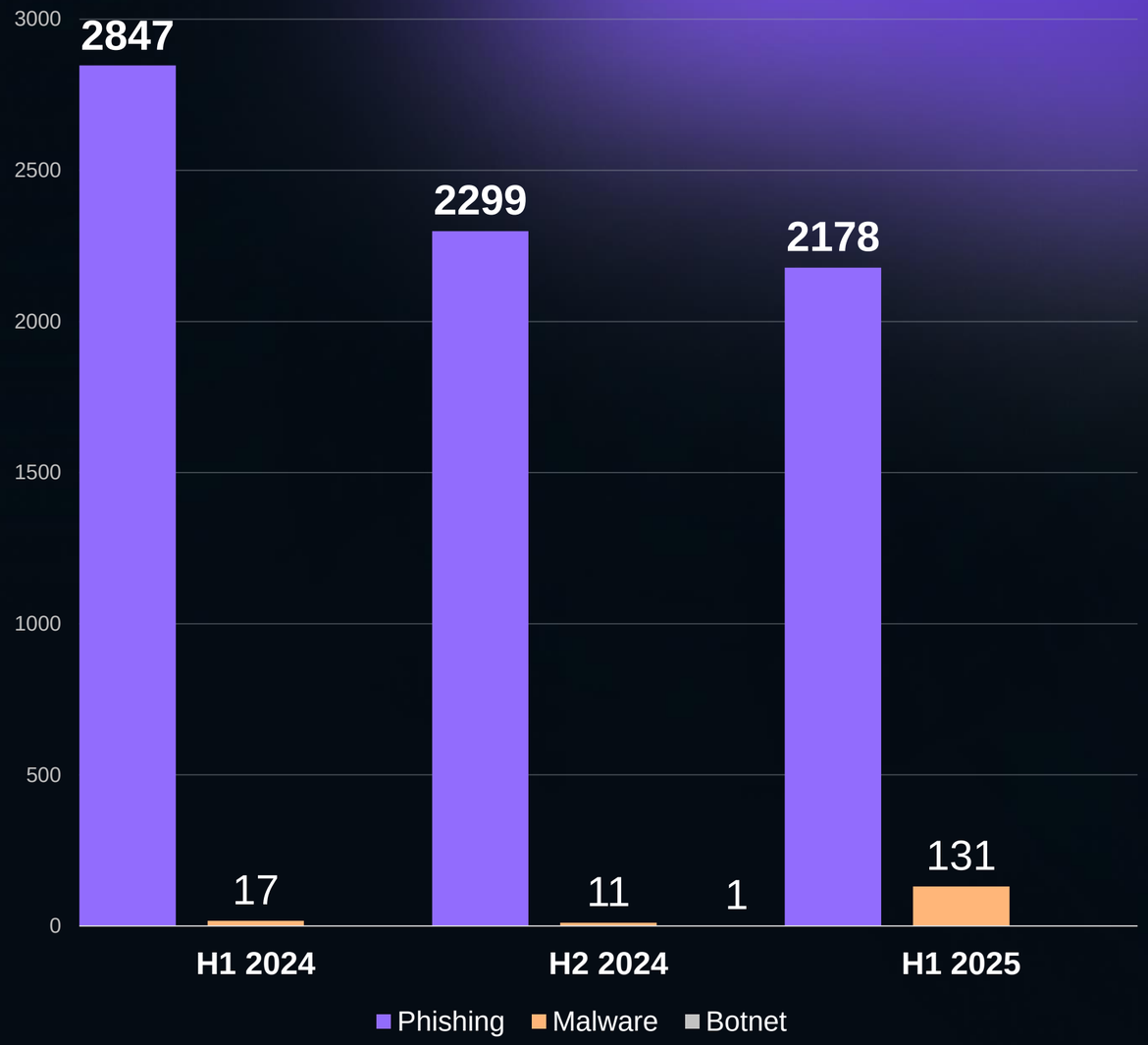
Станислав Гончаров

Руководитель DRP, Россия и СНГ

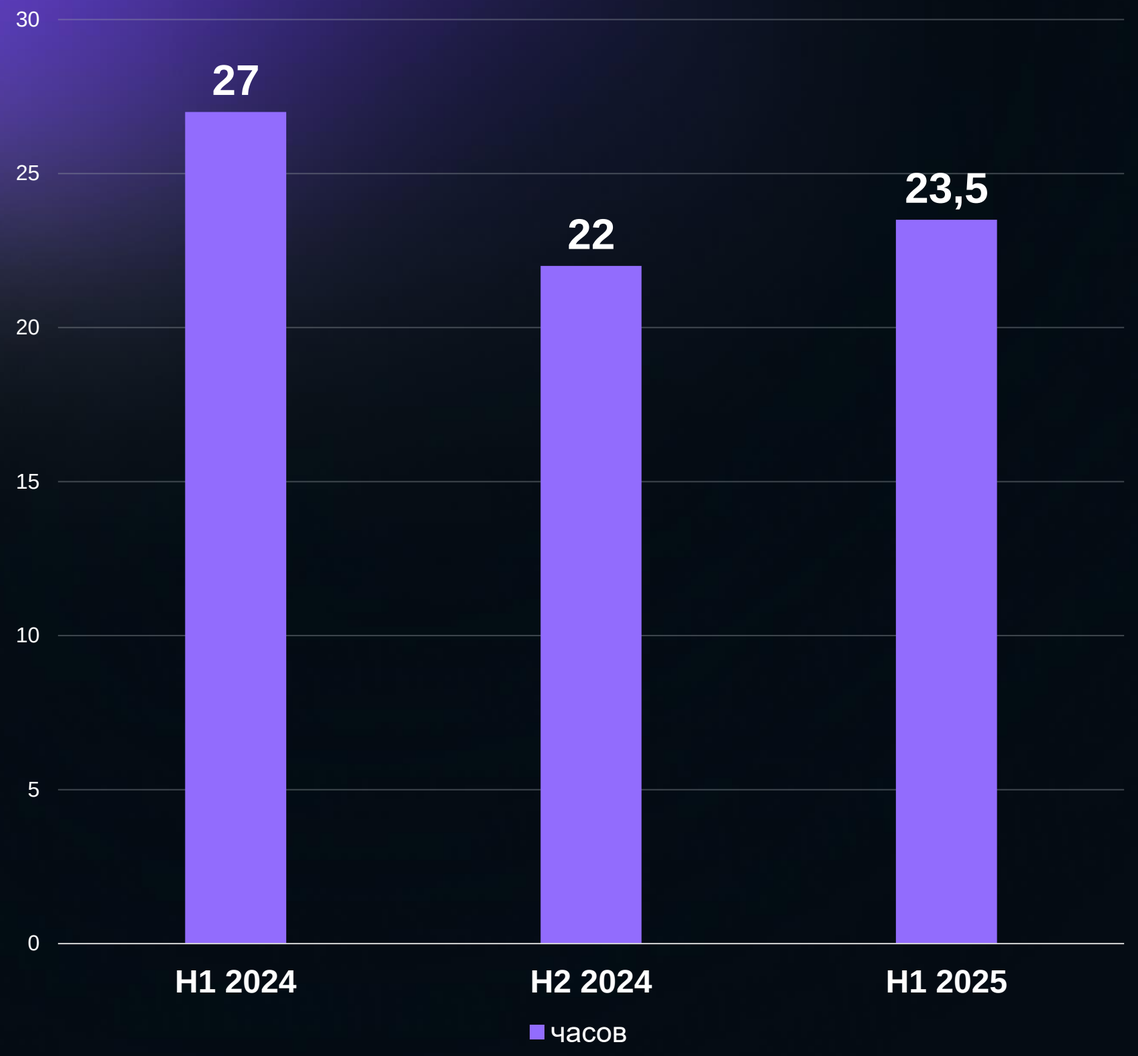
Доменный патруль

F6

Количество отправленных на блокировку ресурсов

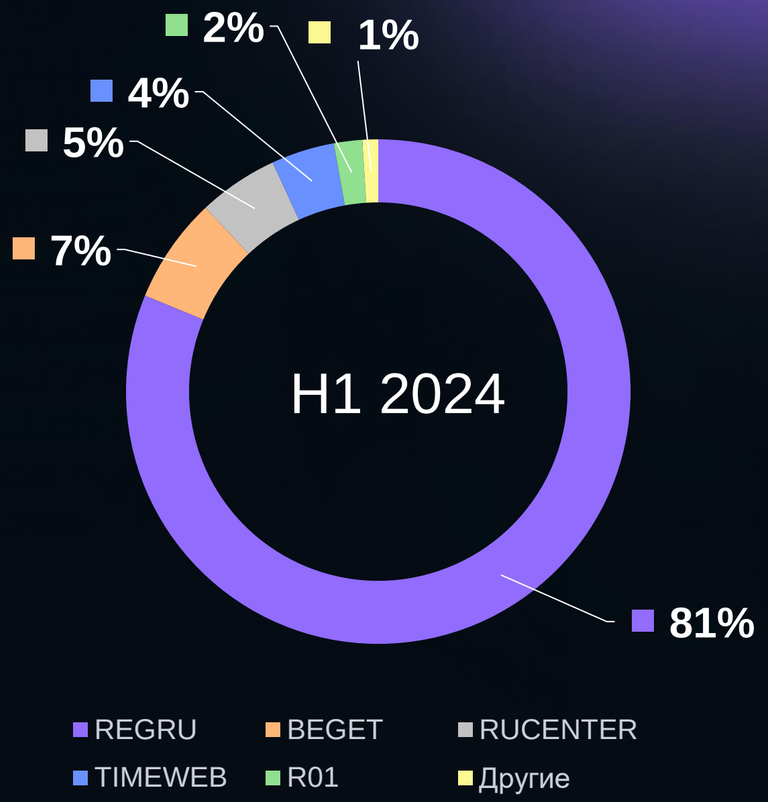


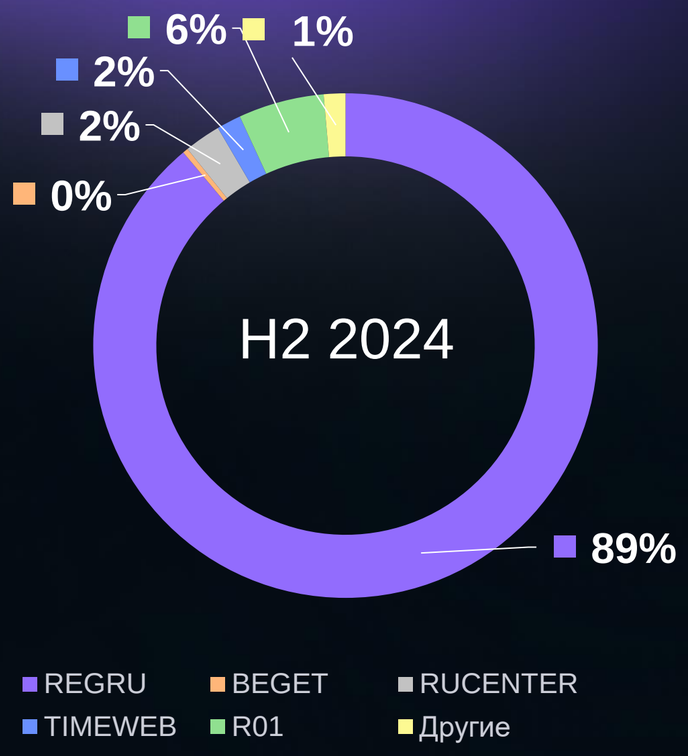
Среднее время обработки запроса

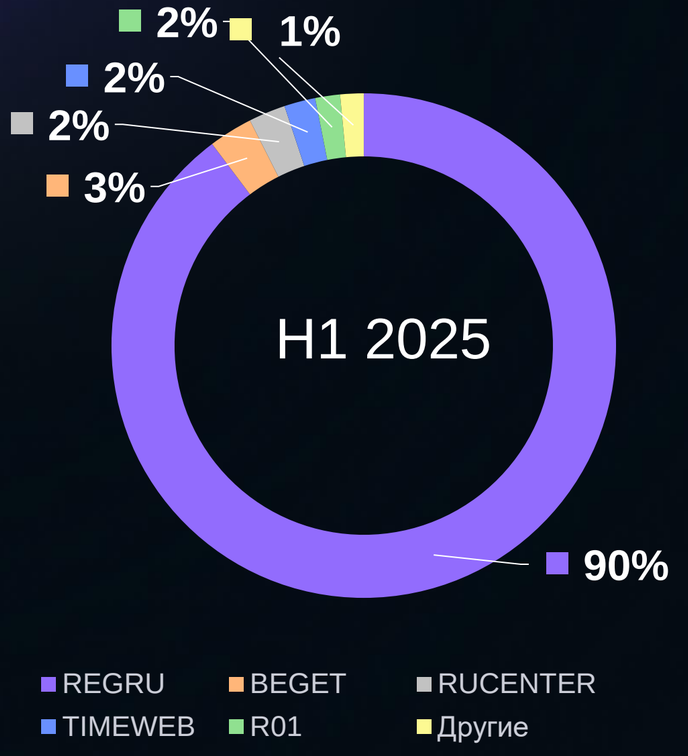


Доменный патруль

F6

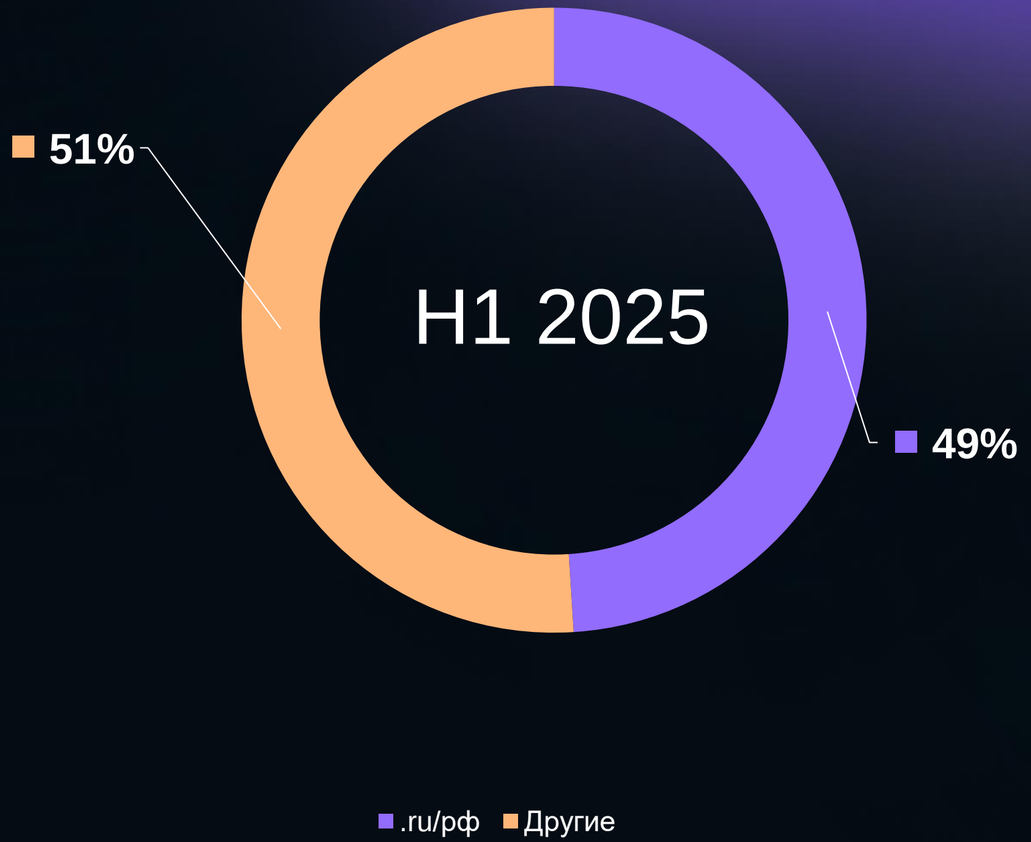






Фишинговые сайты

F6



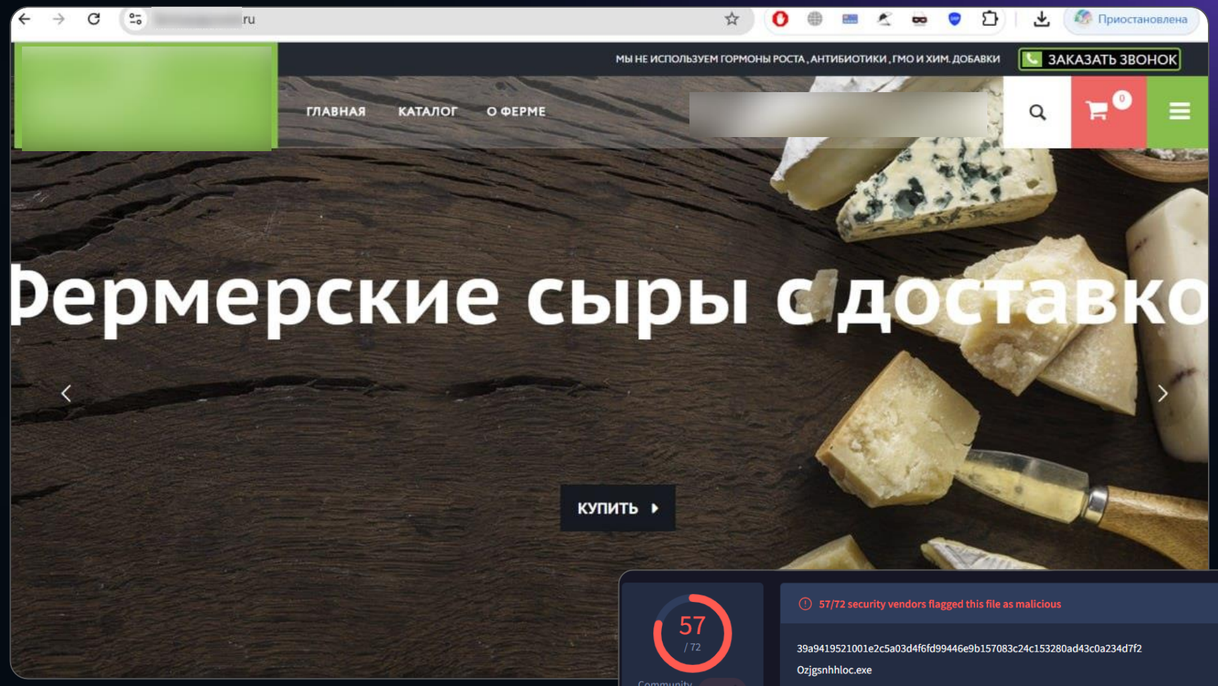
Про взломы – размещение ВПО

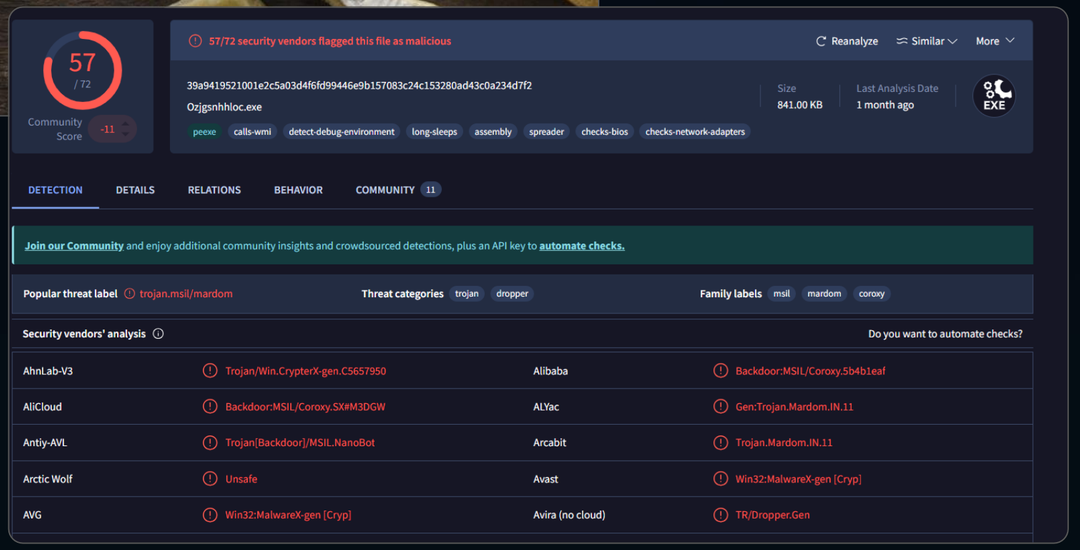
F6

https://*.ru/images/sys.exe**

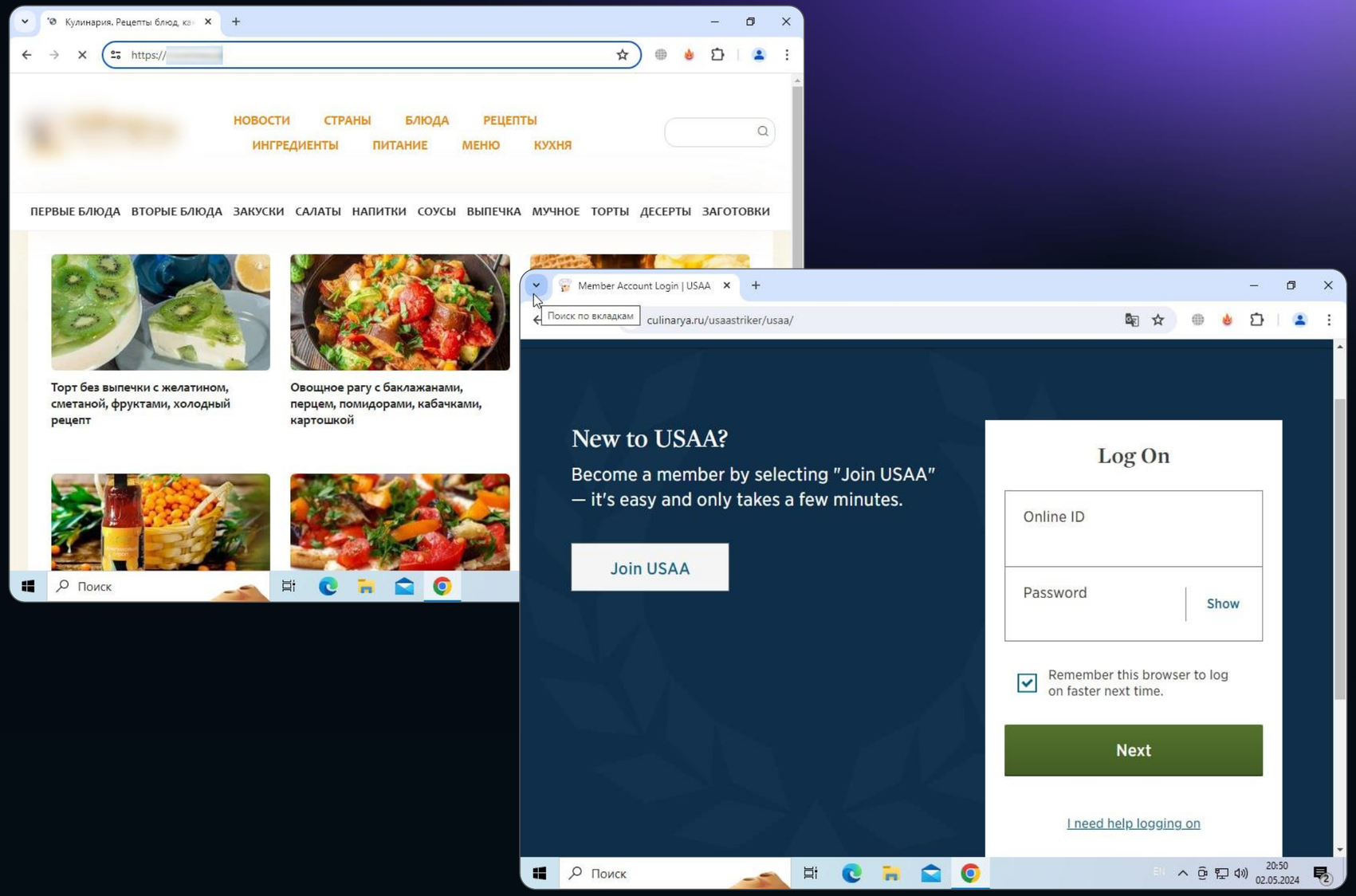
По данной ссылке в директориях сайта размещалось ВПО типа SpyWare, Stealer

Были предприняты многократные попытки связаться с владельцем ресурса для устранения нарушения, но данный метод не принес положительных результатов. В связи с чем домен был разделегирован в доменном патруле и позже восстановлен по нашему запросу, когда нарушение было устранено. Восстановлен был после звонка генерального директора, который уточнял информацию по разделегированному домену.





Про взломы – размещение фишинга



F6

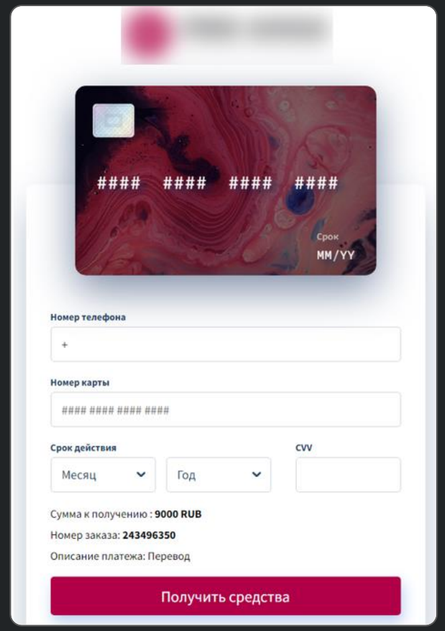
Директория с вредоносной фишинговой страницей, направленная на пользователей USAA (группа компаний диверсифицированных финансовых услуг. Базируется в штате Техас).

Нарушение устранено через доменный патруль. Доменный патруль связался с владельцем ресурса, нарушение было устранено.

Самые популярные способы взлома сайтов:

1. Уязвимости в CMS
2. Brute-force атаки на панель админа
3. SQL-инъекции
4. Загрузка вредоносных файлов
5. Cross-Site Scripting
6. Смена NS/DNS через взлом аккаунта у регистратора
7. Заражение зависимостей и библиотек
8. Доступ через уязвимости в панелях управления
9. Взлом FTP/SFTP через перехват логинов
10. Социальная инженерия (фишинг владельцев сайта)

Выявление и блокировка доменов по схеме «Мамонт»



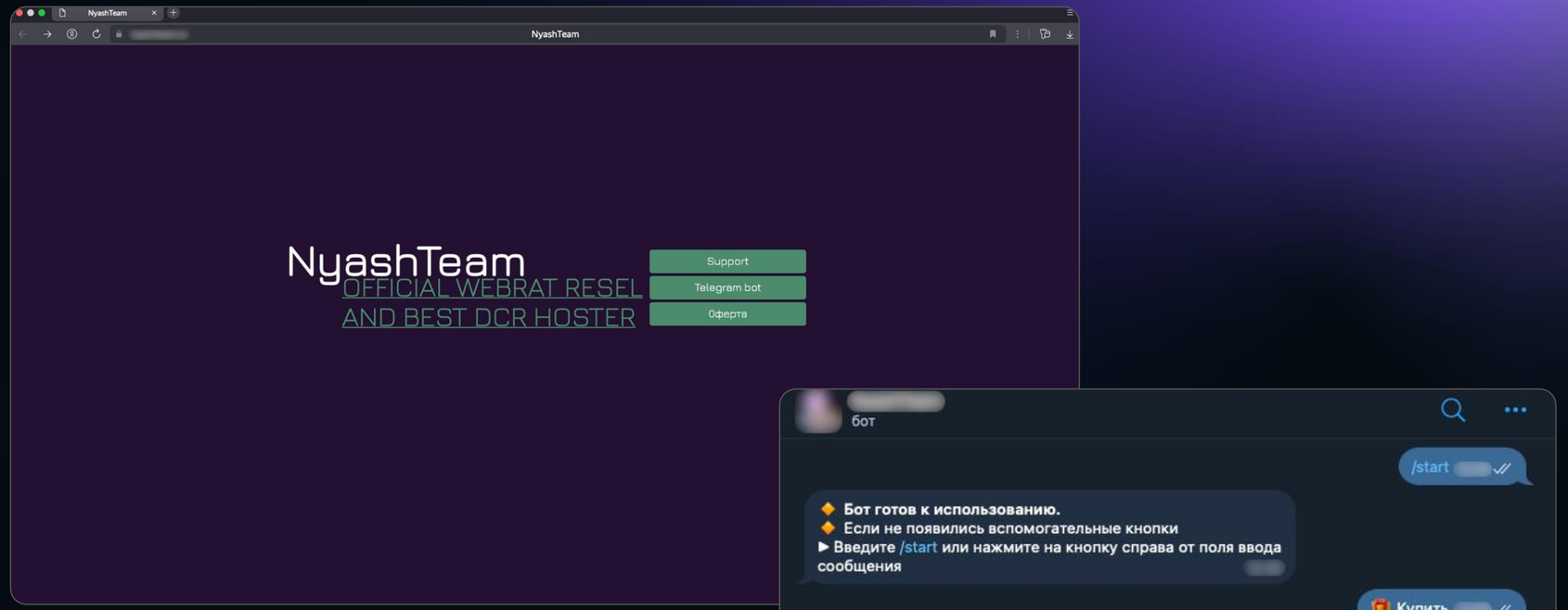
Персональная ссылка

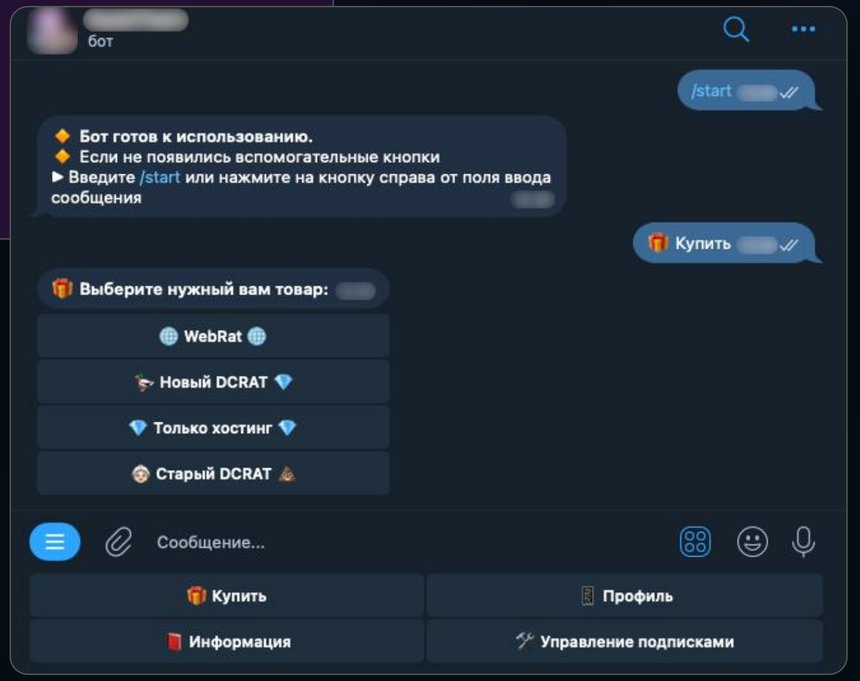
Вид ссылки: https://**.******.ru/?pay=24204417**

1. Выявление доменов второго уровня по паттернам в зоне .ru
2. Выявление доменов третьего уровня по паттернам наименований брендов
3. Обязательное наличие айпи у домена третьего уровня
4. IP-адрес скрыт под Cloudflare
5. Домен второго уровня не старше 7 суток
6. Владельцем домена должен быть Private Person
7. Домен должен быть Unverified

NyashTeam 1/2

F6





Чем занимаются?

Группировка NyashTeam с 2022 года проявляет активность на криминальном рынке MaaS (Malware-as-a-Service, вредоносное программное обеспечение как услуга). Предлагает приобретение вредоносного ПО и предоставление хостинг-услуг для его размещения.

Инфраструктура злоумышленников

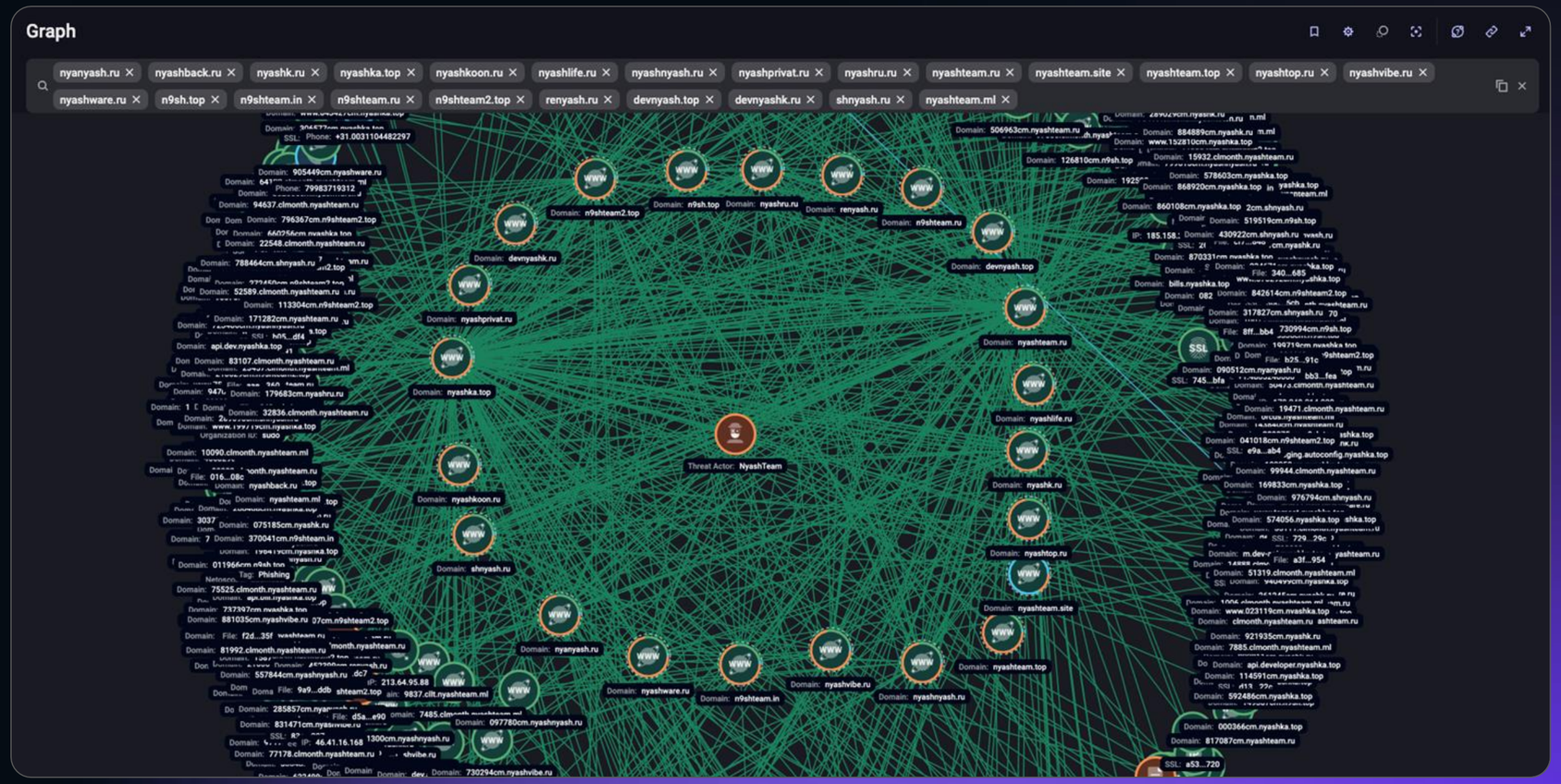
Продажа ВПО ведётся исключительно через Telegram-боты группировки. Также для своих клиентов NyashTeam предлагают мануалы для новичков, инструменты обработки данных, а также техническую поддержку, на случай возникновения вопросов

Распространение

В большинстве случаев для распространения ВПО клиенты NyashTeam использовали YouTube и GitHub

NyashTeam 2/2

F6



Домены

Для предоставления услуг хостинга под размещение ВПО NyashTeam активно регистрирует домены второго уровня в том числе в зоне .ru. В основном злоумышленники используют для доменов характерные названия, такие как «nyanyash[.]ru», «nyashback[.]ru» или имена, содержащие названия ВПО «webrat» и «dcrat», а на их основе создают домены третьего уровня

Объёмы

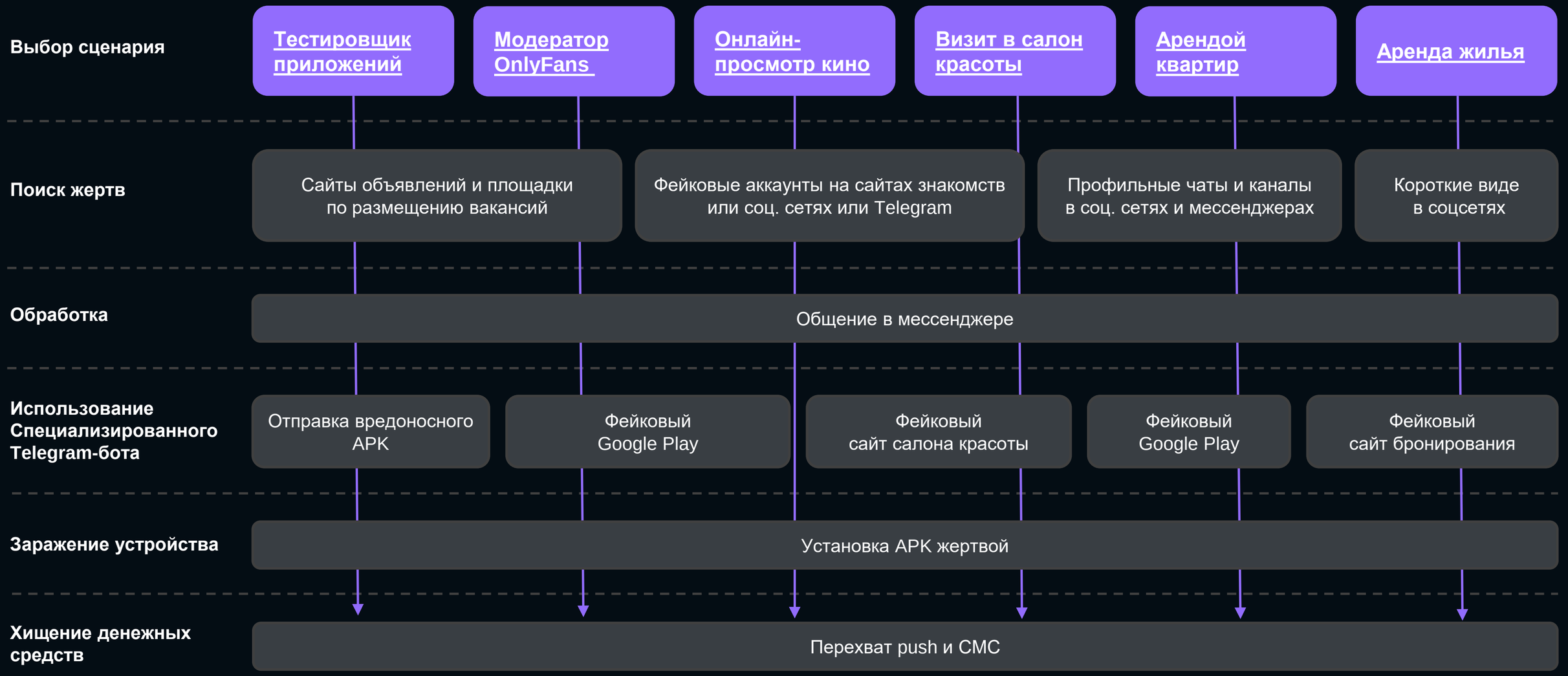
С 2022 года, момента начала активности группировки, было зафиксировано более 350 доменов второго уровня, некоторые из них связаны с более чем 100 доменами третьего уровня. На июль 2025 года уже заблокированы
более 110 доменов в зоне .ru.

Скорость блокировки

Среднее время блокировки доменов, которые использовались группировкой - 62 часа 39 минут

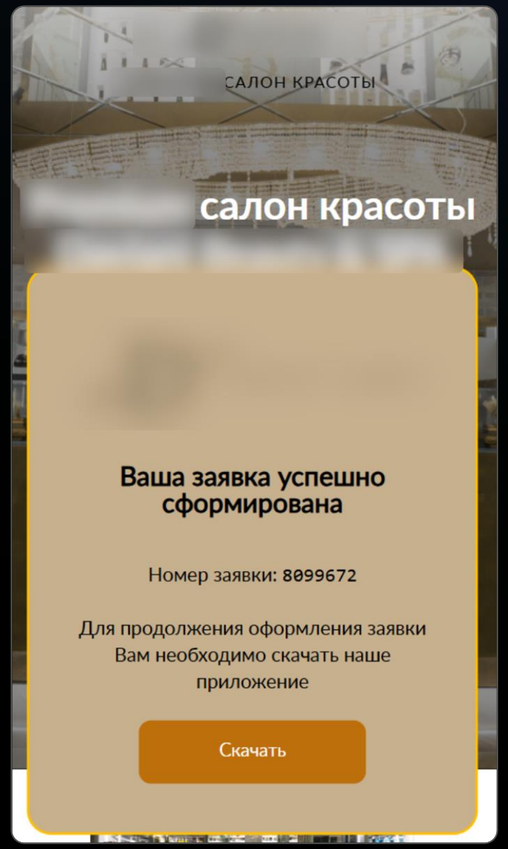
6 сценариев – одна цель

F6

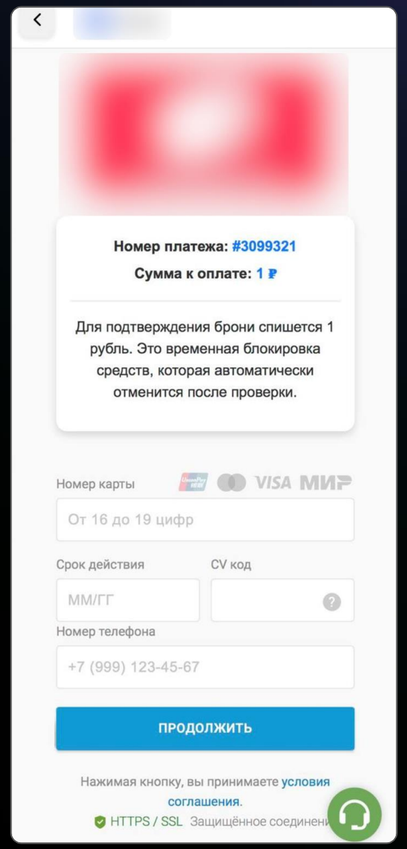


Атаки не только под Android

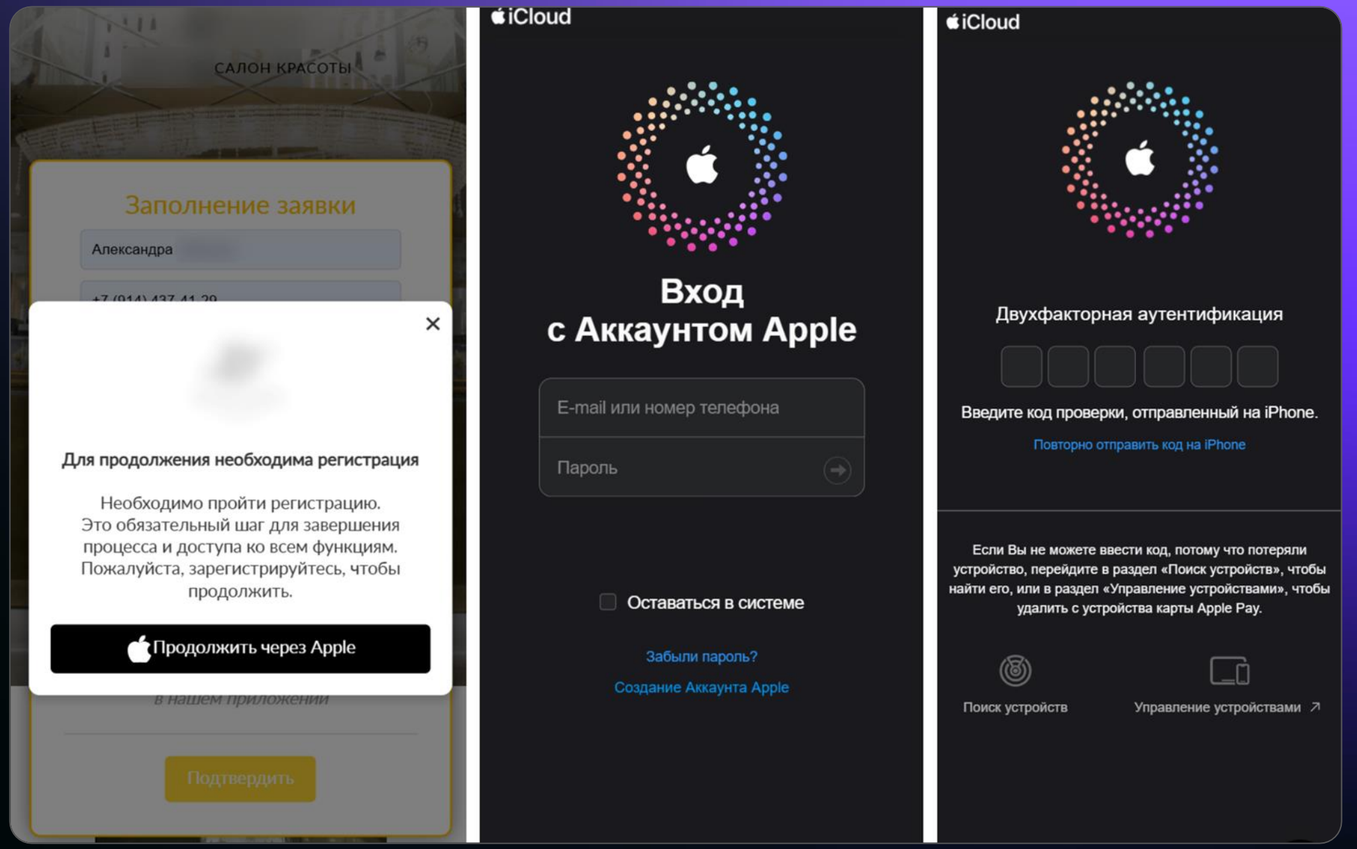
F6



Загрузка APK



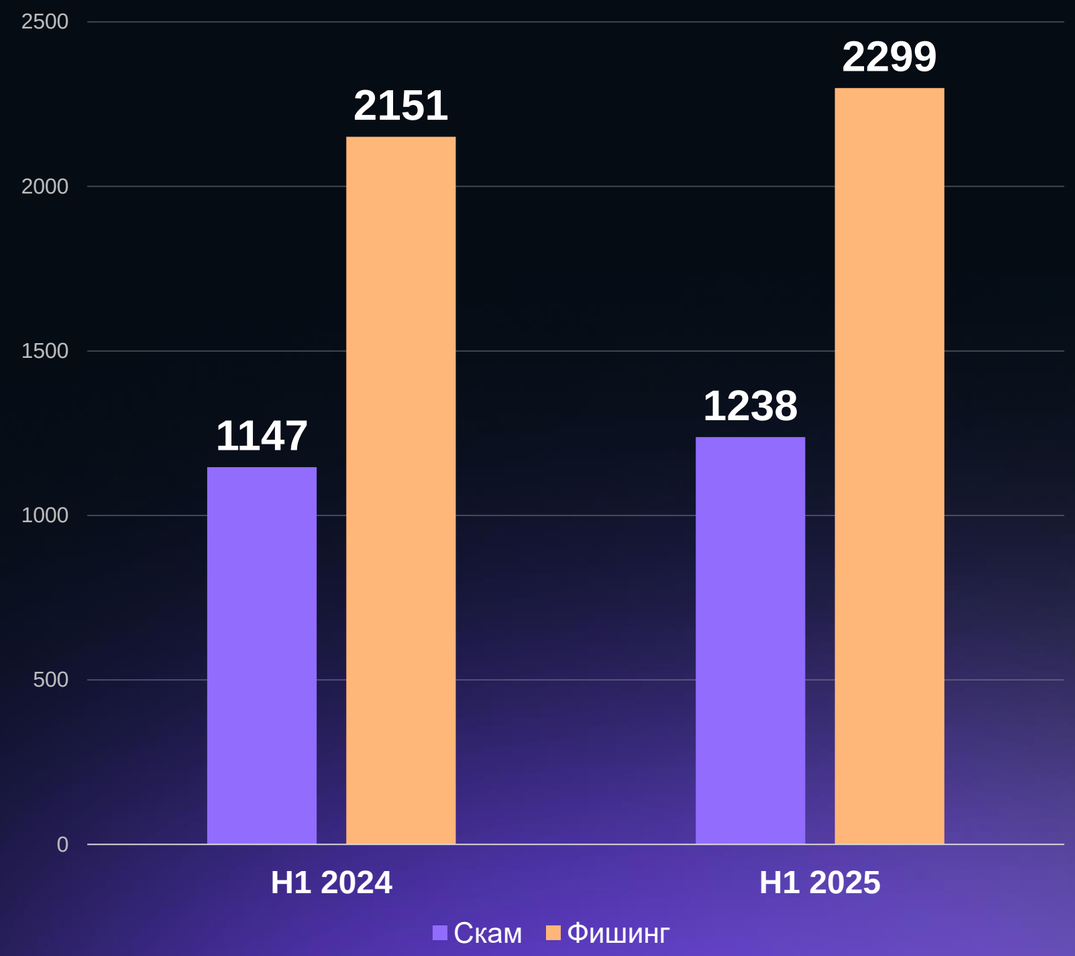
Фишинг данных карты

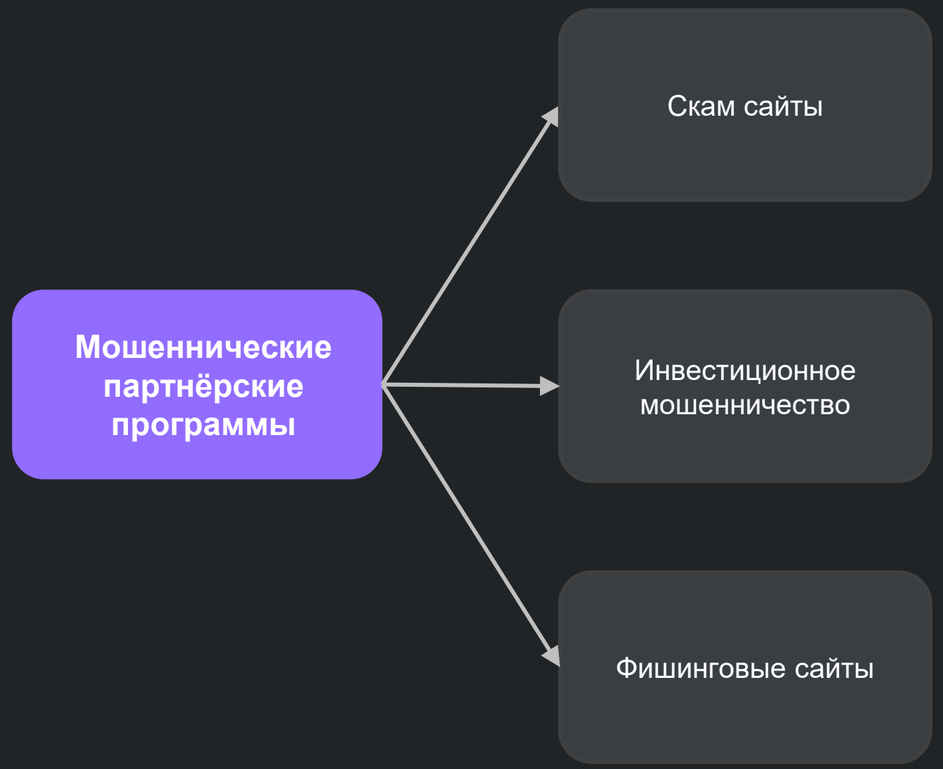


Фишинг iCloud

Не фишингом едины

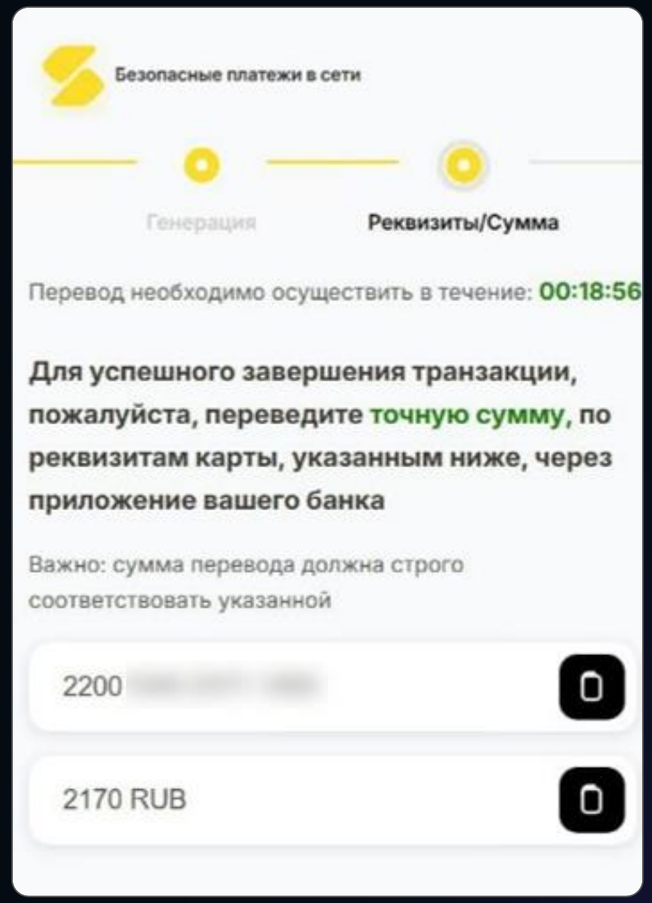
Среднее количество создаваемых фишинговых и мошеннических ресурсов на 1 бренд

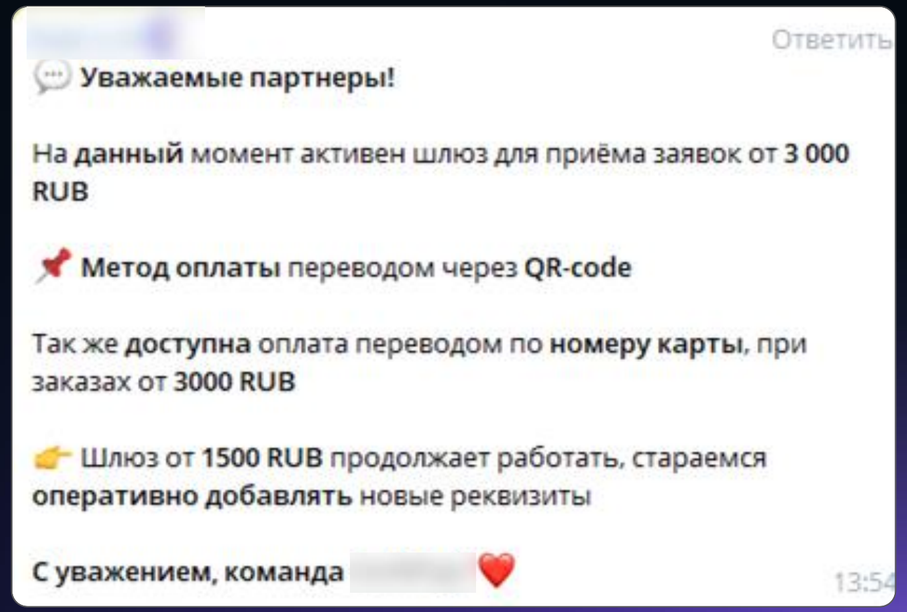




F6

Не фишингом едины





F6

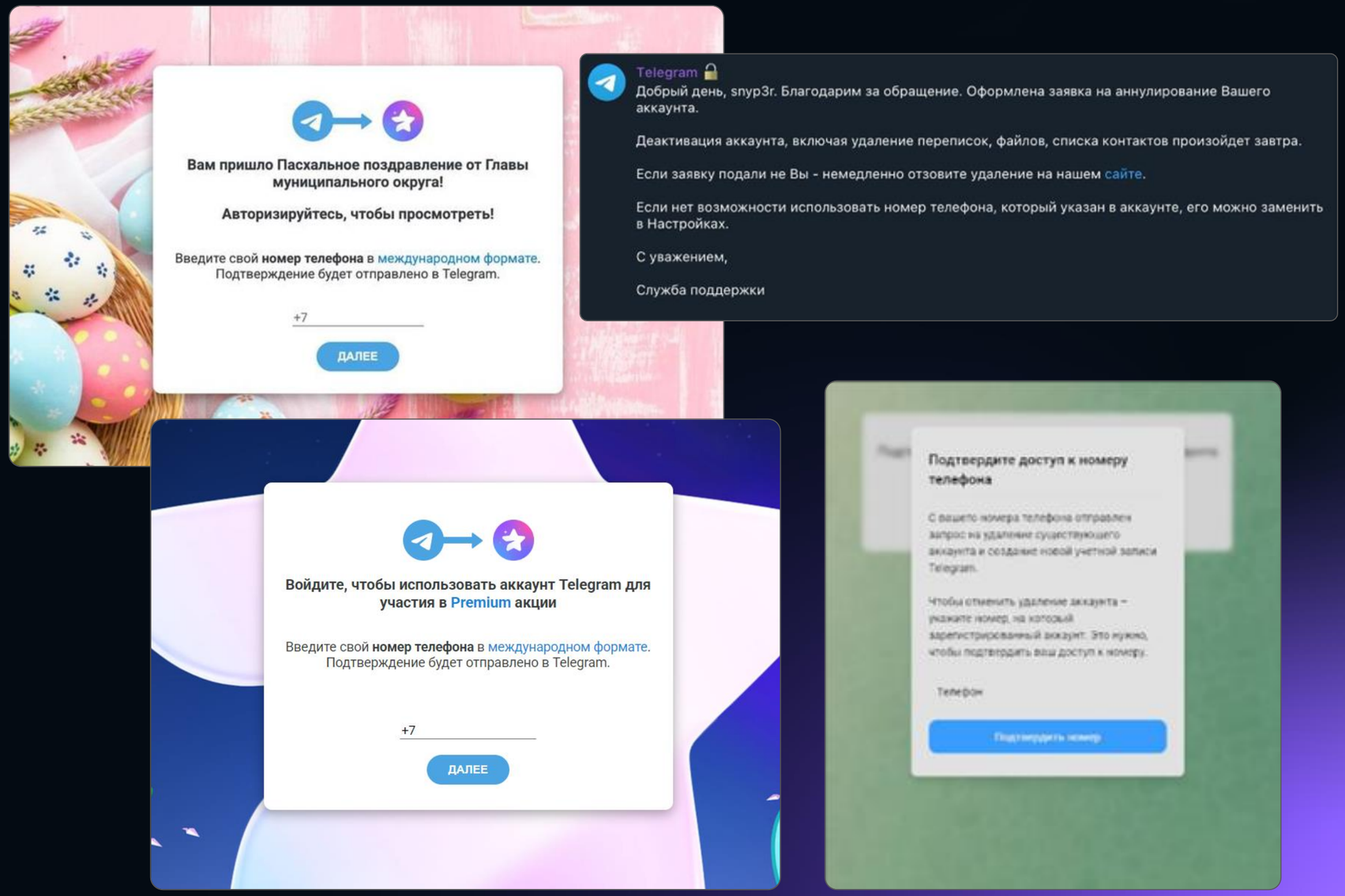
Тенденция ухода от фишинга

В партнёрских программах всё чаще используются прямые переводы на карту или оплата QR кодом.

Скорость блокировки

На данный момент домены со скамом блокируются значительно дольше, чем домены с фишингом – этим и пользуются злоумышленники.

Фишинг Telegram



F6

1 496 034 аккаунтов

похитила только одна из русскоязычных групп злоумышленников за январь-июнь 2025 года у пользователей из России и других стран. F6 зафиксировали не менее четырёх таких групп.

Ужесточение законодательства

В конце июня некоторые популярные у киберпреступников торговые площадки запретили продажу российских аккаунтов на своих ресурсах из-за новых законов по усилению борьбы с телефонным мошенничеством. Мошеннические группы, которые специализируются на краже учётных записей пользователей из России, оказались перед выбором: искать другие способы продаж или угонять зарубежные аккаунты.

Благодарим за внимание!

На связи 24/7

Технологии для борьбы
с киберугрозами