Рынок киберпреступных услуг в Telegram

Positive Technologies

ptsecurity.com

Рынок киберпреступных услуг в Telegram

Последние несколько лет мы видим, как крупные киберпреступные площадки прекращают свое существование или теряют доверие пользователей. Некоторые из форумов, к примеру RaidForums и DarkMarket, были закрыты в ходе действий правоохранительных органов. Другие, например BHF, Carding Mafia, Nulled и Maza, были взломаны конкурентами. Контроль над площадками переходит от одних администраторов к другим, как это произошло с форумом DarkMoney. Так или иначе, возникает угроза компрометации пользовательских данных, включая информацию о подключениях к преступным ресурсам. Это повышает шансы на раскрытие личности и местоположения киберпреступников.

Поскольку киберпреступные форумы как ресурсы для проведения сделок и привлечения клиентов вызывают сомнения с точки зрения анонимности, теневые площадки все чаще создают каналы и группы в Telegram. Мессенджер вызывает большее доверие у пользователей и удобен в использовании, а значит присутствие в нем позволяет увеличить аудиторию: это и среда общения, и площадка, удобная для покупки и продажи киберпреступных товаров и услуг.

В нашем исследовании мы проанализируем актуальное состояние рынка криминальных киберуслуг, сформировавшегося на базе каналов и групп в мессенджере Telegram, и проанализируем зрелость этого рынка.

Методика исследования

В ходе исследования мы проанализировали 323 публичных канала и группы в Telegram с общим количеством подписчиков более одного миллиона. В числе проанализированных источников не только каналы и группы с изначально криминальной направленностью, но и созданные IT-сообществом в легитимных целях, которыми тем не менее могут воспользоваться и злоумышленники.

Количество новых каналов и групп, содержащих сообщения на киберпреступную тематику, стало увеличиваться со второй половины 2019 года. Возраст большинства попавших в выборку каналов и групп (73%) составляет менее двух лет, что может свидетельствовать как о недавнем переходе криминальных коммуникаций в мессенджер, так и о недолговечности их существования.

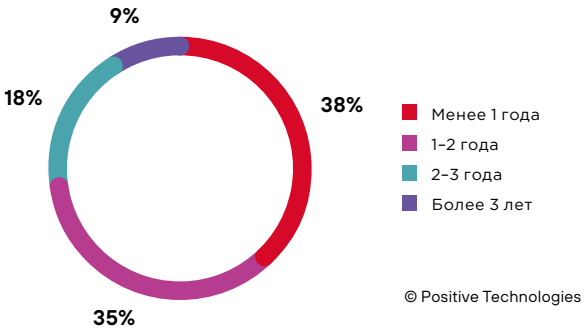


Рисунок 1. Возраст каналов и групп

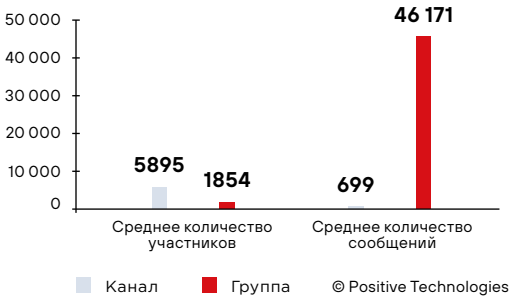


Рисунок 2. Средние значения по типам ресурсов

Для исследования мы выбрали сообщения, опубликованные в период с начала 2019 года по II квартал 2022 года включительно, в которых обсуждались вредоносное ПО, уязвимости и эксплойты, доступы к корпоративным сетям, данные пользователей и киберпреступные услуги: взлом ресурсов (в том числе сайтов, почтовых аккаунтов и аккаунтов в социальных сетях), обналичивание средств, распространение ВПО, спам-рассылки, услуги DDoS. В итоговую выборку вошли более 120 тысяч сообщений на русском и английском языках.

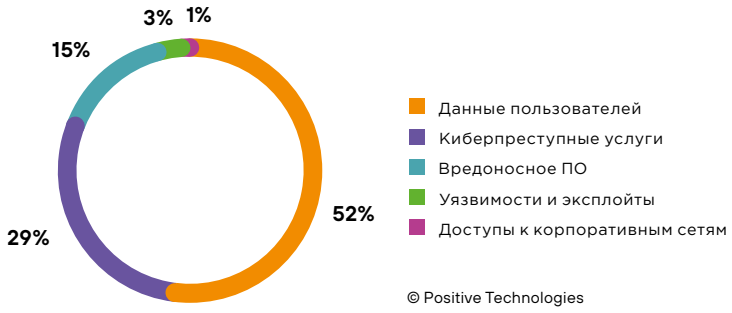


Рисунок 3. Распределение сообщений по темам

От криминальных форумов к мессенджерам

Удобство и простоту использования мессенджеров смогли оценить не только обычные пользователи, но и злоумышленники: достаточная степень анонимности, простой процесс регистрации и подключения позволяют масштабировать рынок киберпреступных услуг, создавать теневые каналы в мессенджерах.

Начиная со II квартала 2020 года мы можем наблюдать увеличение количества сообщений в Telegram; в 2021-м активность пользователей возросла в разы. Можно предположить причину массового перехода пользователей криминальных форумов в мессенджер именно в этот период: в 2020 году было выявлено множество критически опасных уязвимостей в форумных движках vBulletin, XenForo, IPB и других, а затем, в 2021 году, произошло несколько крупных взломов форумов. Это могло снизить доверие к форумам и предопределить переход пользователей в Telegram. В это время появилось большое количество рекламы новых каналов и групп, отдельных пользователей, предоставляющих различные преступные услуги. По этой причине в конце 2021 года существенно выросло общее число сообщений, но затем активность пользователей вернулась к прежним показателям.

К концу I квартала из-за массовых взломов и утечек снова возросло количество рекламы каналов и групп, киберпреступных услуг. И сейчас, во II квартале 2022 года, было отмечено рекордное количество сообщений — более 27 тысяч.

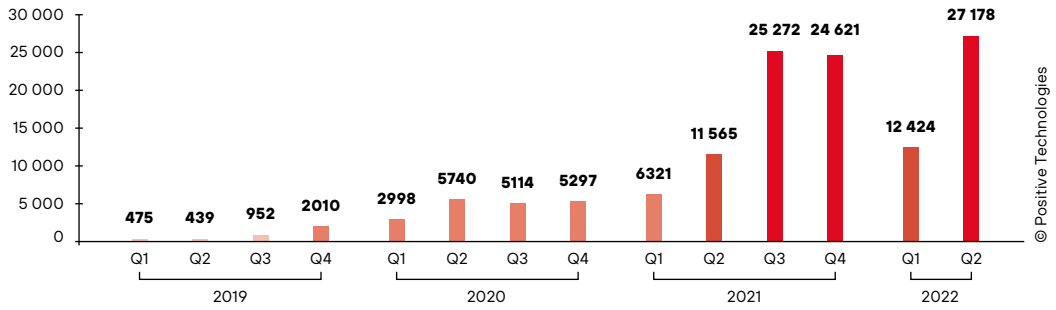


Рисунок 4. Общее количество сообщений

Вредоносное ПО

Среди всех проанализированных сообщений по теме вредоносного ПО самыми популярными оказались ПО для удаленного управления (remote access trojan — RAT), а также шпионское ПО — разнообразные стилеры.

Рисунок 5. Распределение сообщений по типам ВПО

Шифровальщики, на протяжении последних лет бьющие рекорды по количеству атак, упоминались всего в 8% сообщений. Возможно, это связано с тем, что распространение шифровальщиков происходит по большей части через партнерские программы, на специализированных сайтах и форумах в дарквебе и в закрытых группах. Поэтому на публичных просторах мессенджера встречается совсем немного объявлений о покупке и продаже, а сами ВПО достаточно простые и могут обойтись в 10 $.

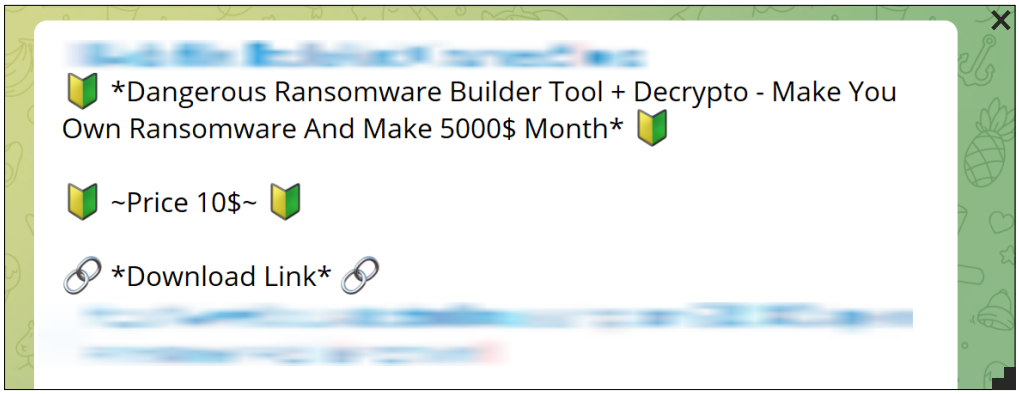


Рисунок 6. Объявление о продаже инструментов для шифрования

Несмотря на общее преобладание сообщений, предметом обсуждений которых является ВПО для удаленного управления, их доля среди всех сообщений о вредоносном ПО снизилась с начала 2021 года на целых 10 п. п. Если на период I квартала 2021 их доля составляла 42% от количества всех сообщений о ВПО, то к концу II квартала 2022 она составила 32%. Это падение частично связано с переключением интереса на другие категории: в III квартале 2021 года возросла популярность стилеров (23%) и ботнетов (22%), а в следующем, IV квартале одними из самых популярных оказались майнеры (19%).

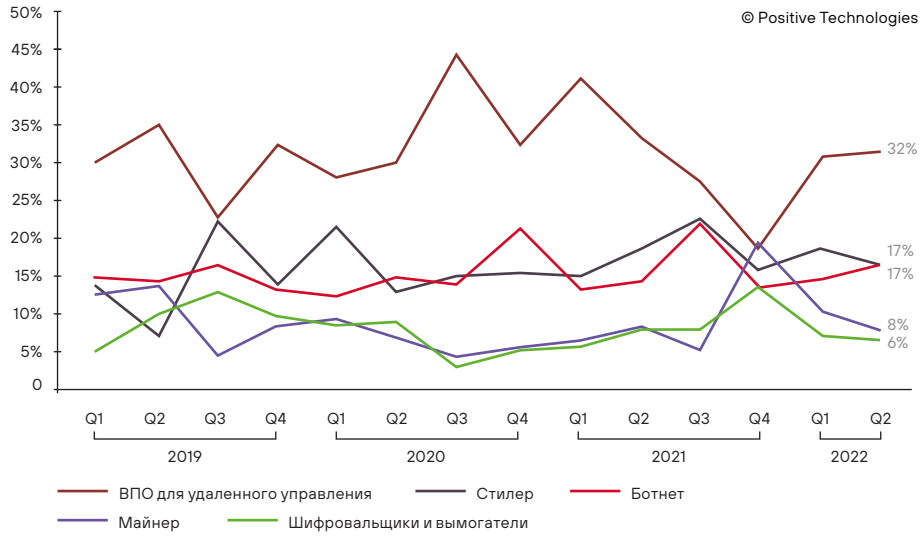


Рисунок 7. Наиболее популярные типы ВПО (доли сообщений)

Из всех сообщений 11% относились к объявлениям о продаже ВПО, 10% составляли сообщения о бесплатной раздаче вредоносов и 7% содержали запросы на покупку. Услуги разработки, а также сотрудничество в Telegram пользуются наименьшим спросом: для таких тем злоумышленники выбирают специализированные сайты и форумы. И это можно объяснить: в Telegram отсутствует рейтинговая система, и говорить о достаточном уровне доверия между пользователями невозможно. В этом мессенджере достаточно легко можно менять никнеймы, что дает мошенникам больше возможностей обмана: отследить «недобропорядочных» продавцов и покупателей становится сложнее. Поэтому в 31% сообщений, посвященных покупке и продаже ВПО, требовался или был заявлен гарант — лицо, которому доверяют покупатель и продавец и которое выступает как посредник при проведении сделки.

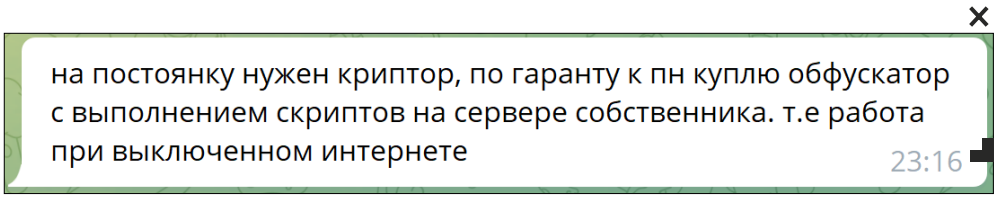


Рисунок 8. Объявление о покупке ВПО при участии гаранта

Обсуждения функций вредоносного ПО, способов его использования и распространения, новости о появлении и обновлении ВПО суммарно составили 70% сообщений.

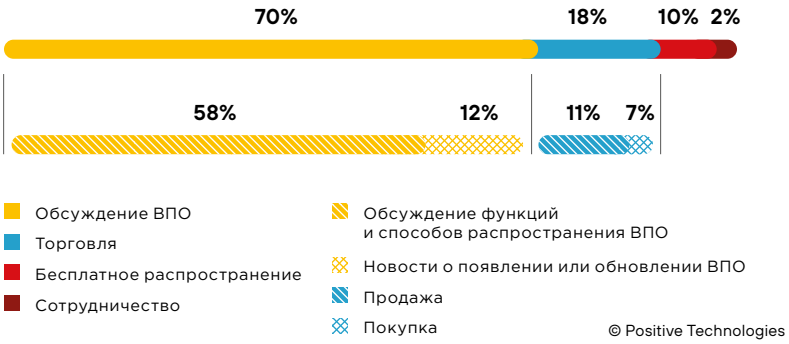


Рисунок 9. Категории сообщений на тему вредоносного ПО

Стоимость готового ВПО в сообщениях о продаже может варьироваться. На цену влияет тип вредоноса, его функциональные возможности (чем их больше, тем выше цена), а также сроки использования программы: ВПО часто предлагается как подписка с фиксированным временем доступа или поддержки. Например, инструменты для обфускации (запутывания кода) могут стоить от 20 $ до 100 $, а цена на ботнет или руководство по его созданию может доходить до 750 $.

При обсуждении майнеров была отмечена наибольшая доля сообщений о продаже (27%), чаще всего это были рекламные объявления. Цена может составлять от 10 $ до 1000 $: за 10 $ можно приобрести достаточно простое ВПО с ограниченными возможностями, а за 1000 $ — исходный код инструмента с широким набором функций, включая обход антивирусных программ и возможность заражения системы без привилегий администратора.

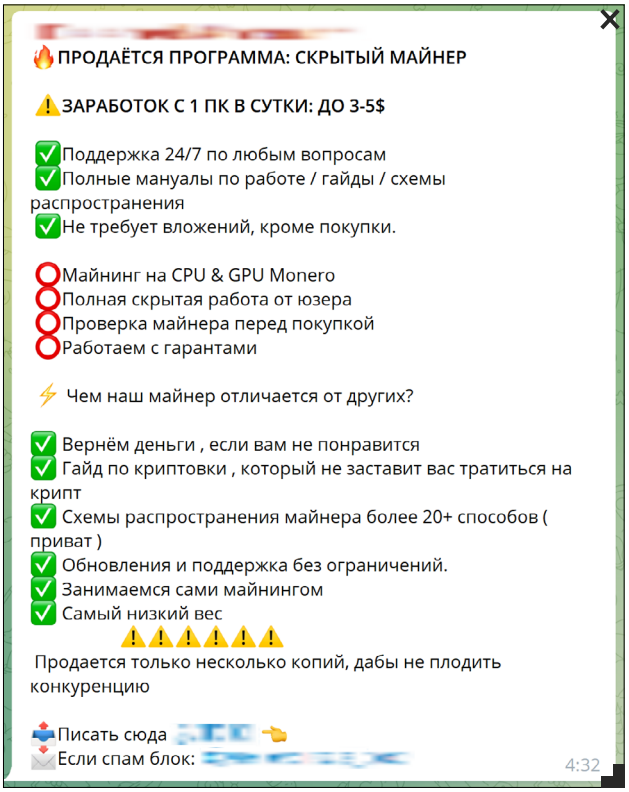


Рисунок 10. Объявление о продаже майнера

ВПО для удаленного управления и стилеры

Среди наиболее популярных инструментов для удаленного управления оказались SpyMax, обсуждения которого составляют 8% от всех сообщений в категории, SpyNote (5%) и Mobihok (4%). Все это ВПО предназначено для Android. Инструменты для удаленного управления для этой операционной системы пользуются высокой популярностью: около четверти всех сообщений этой категории посвящены RAT для Android. Цена готового инструмента зависит от набора функций и может составлять от 10 $ до 500 $.

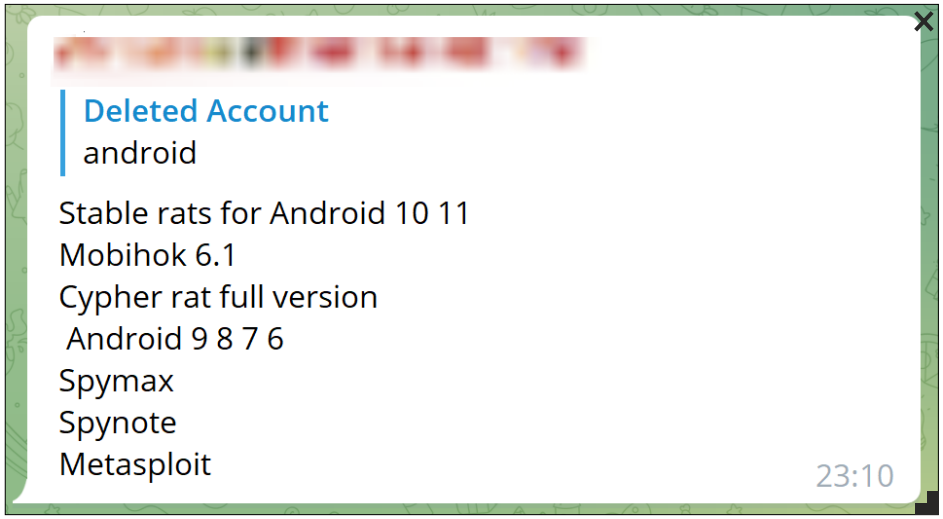


Рисунок 11. Обсуждение наиболее популярных RAT для Android

Самым популярным стилером оказался RedLine, о котором мы уже писали в исследовании актуальных киберугроз за I квартал 2022 года. Он упоминается более чем в 18% сообщений на эту тему: это многочисленные обсуждения функций, продажа и раздача исходного кода ВПО, а также информации, собранной с помощью стилера. Также в Telegram встречаются такие стилеры, как Anubis, SpiderMan, Oski Stealer, Loki Stealer. Стоимость может составлять от 10 $ до 3500 $.

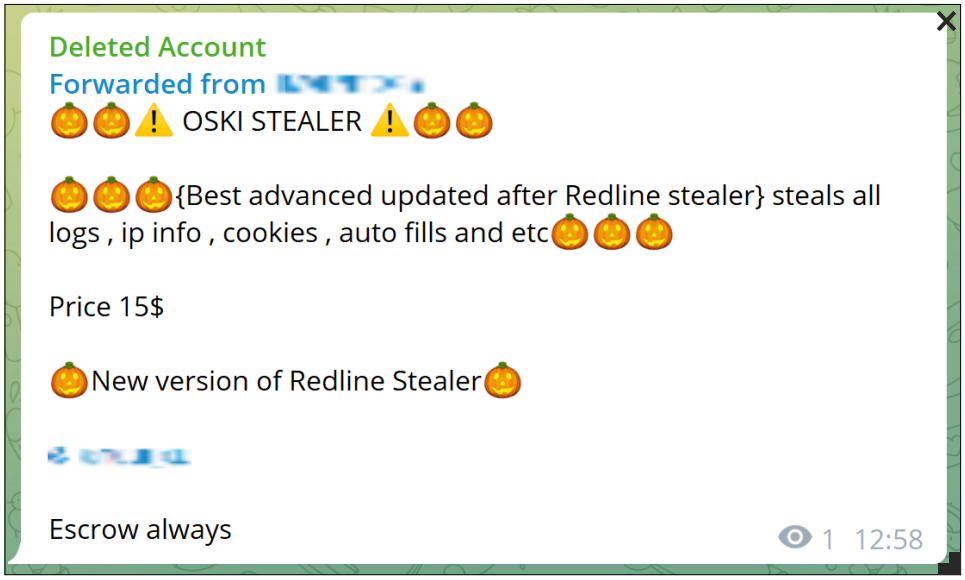


Рисунок 12. Объявление о продаже стилера

Обычно стилеры собирают с устройства жертвы информацию о пользователе: это учетные данные, банковская информация, записи с веб-камеры и микрофона, информация о местоположении. Большинство стилеров могут также собирать данные криптокошельков: учетные данные, закрытые ключи.

Уязвимости и эксплойты

Среди сообщений на тему эксплойтов 29% посвящены уязвимостям нулевого дня: это могут быть как сами эксплойты для новых уязвимостей, так и многочисленные обсуждения, новости. Четверть сообщений была посвящена уже опубликованным уязвимостям и способам их эксплуатации. В 24% обсуждений упоминались уязвимости типа RCE (Remote Code Execution — позволяет удаленно выполнить код) или LPE (Local Privilege Escalation — позволяет повысить привилегии в системе). Эти уязвимости являются наиболее опасными, и они чаще всего привлекают внимание злоумышленников.

Рисунок 13. Распределение сообщений об эксплойтах

Часть сообщений о различных уязвимостях и их эксплуатации посвящена определенным операционным системам. Как и ожидалось, наибольшую популярность имеют уязвимости в Windows, второе место занимает Linux. Третьей по популярности оказалась Android, для которой появляется и распространяется все больше вредоносного ПО.

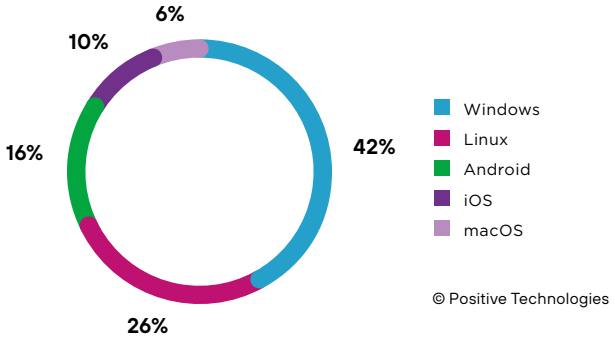


Рисунок 14. Сообщения об эксплойтах для различных ОС

Чаще всего эксплойты распространялись бесплатно (22%), в основном в виде ссылок на исходный код. Объявлений о покупке и продаже для этой темы намного меньше (4% и 3%); такие сообщения встречаются, например, при продаже или покупке эксплойтов, которые не так широко распространены в открытом доступе: в основном для уязвимостей нулевого дня, недавно опубликованных, или для уязвимостей наиболее опасных типов (RCE, LPE). Так, цены за RCE-уязвимость для определенного веб-сайта могут доходить до 4500 $, а в одном из сообщений за LPE нулевого дня для Windows пользователь предлагал заплатить 30 000 $.

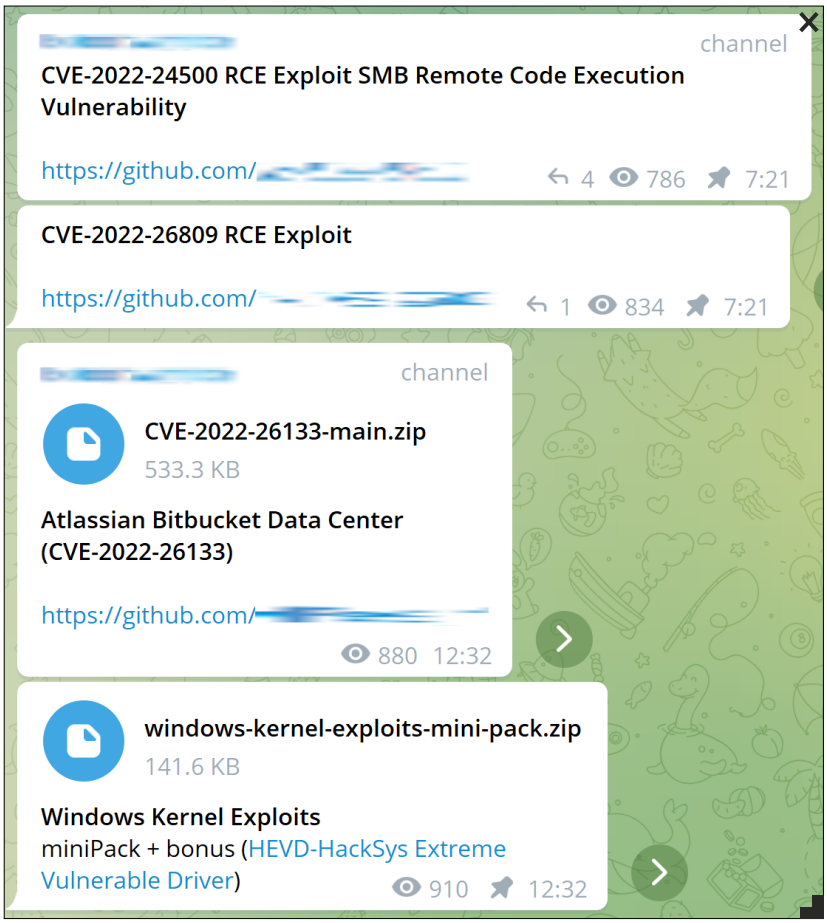


Рисунок 15. Раздача исходного кода для эксплуатации уязвимостей

Встречаются и комплексные инструменты для эксплуатации уязвимостей, предполагающие сканирование и эксплуатацию не одной, а целого набора уязвимостей. Как правило, они предназначены для определенного ПО или фреймворков. Например, особую популярность имеют инструменты для сканирования сайтов на базе фреймворка Laravel, который лежит в основе около 600 тысяч веб-приложений (9% сообщений по теме эксплойтов посвящены этому фреймворку).

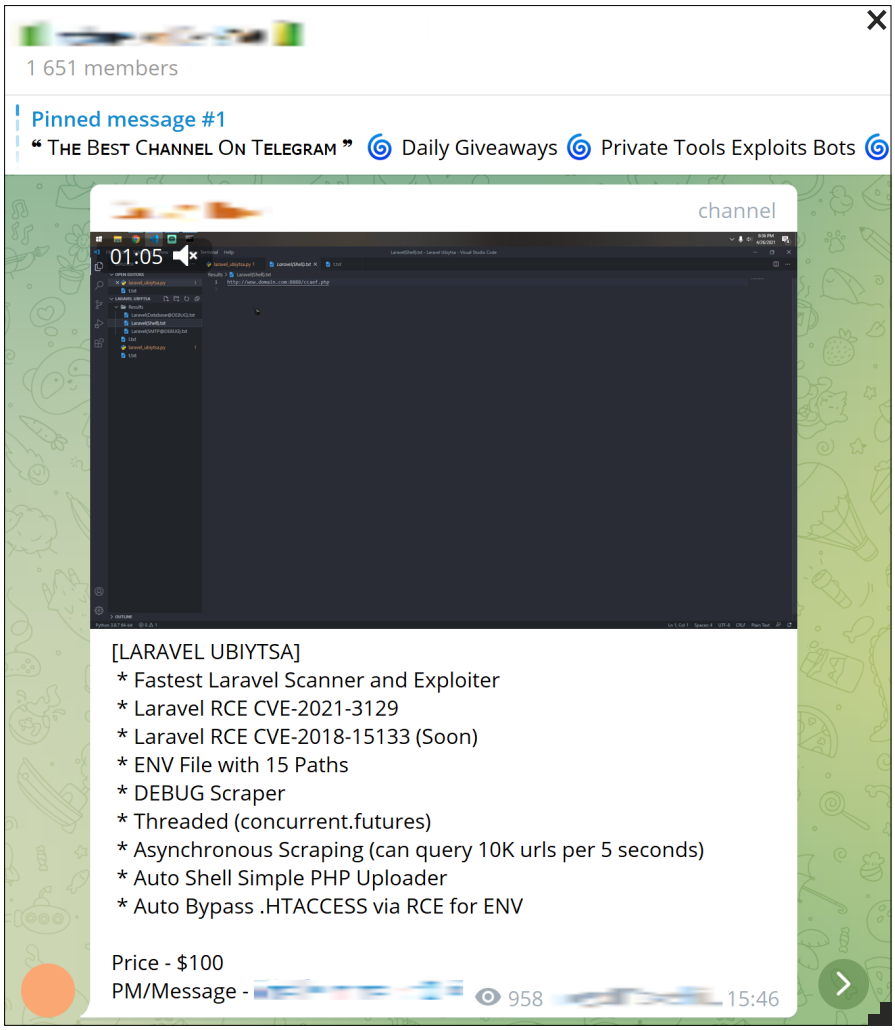


Рисунок 16. Продажа инструмента для эксплуатации уязвимостей

В 17% случаев эксплойты начинали распространяться в мессенджерах в течение суток после публикации информации об уязвимости; в среднем эксплойты для общеизвестных уязвимостей начинали появляться спустя 13 дней после публикации. Наиболее популярными уязвимостями в первой половине 2022 года оказались:

- CVE-2022-26809 в Microsoft RPC,
- CVE-2022-22965 (Spring4Shell) в Java Spring Framework,
- CVE-2022-0847 (Dirty Pipe) в Linux,
- CVE-2022-26134 в Atlassian Confluence,
- CVE-2022-26133 в Atlassian Bitbucket Data Center.

Кроме того, до сих пор популярны достаточно давно обнаруженные недостатки: например, в конце июня 2022 года активно распространялся инструмент для эксплуатации RCE-уязвимости CVE-2017-9841 в Laravel.

Данные

Значительная часть всех сообщений этой темы посвящены документам и персональным данным (43%), а также учетным данным пользователей (42%).

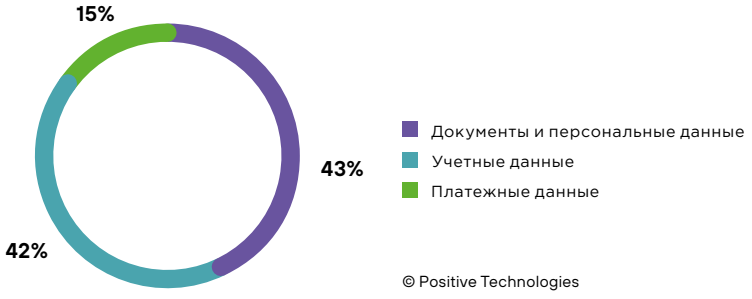


Рисунок 17. Сообщения о компрометации данных

В 2021 году учетные данные были предметом практически половины всех сообщений, но в первом полугодии 2022 года преобладающей стала тема документов, персональных данных и услуг, связанных с ними (71%). Значительный рост числа сообщений на эту тему произошел во II квартале: на фоне многочисленных атак и утечек данных, замеченных в I квартале 2022 года, возросло число услуг, связанных с предоставлением скомпрометированных копий документов из различных учреждений.

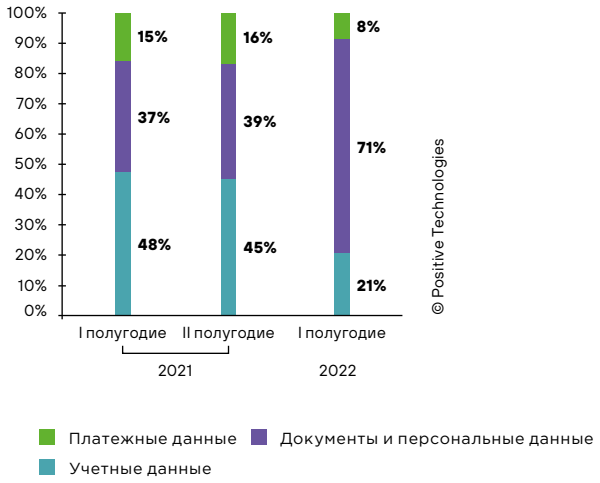


Рисунок 18. Сообщения о компрометации данных

Существенную часть всех сообщений на эту тему (28%) составляют объявления о продаже данных и предоставлении услуг, связанных с данными (например, о подделке документов, изготовлении электронной подписи), а каждое десятое сообщение посвящено покупке.

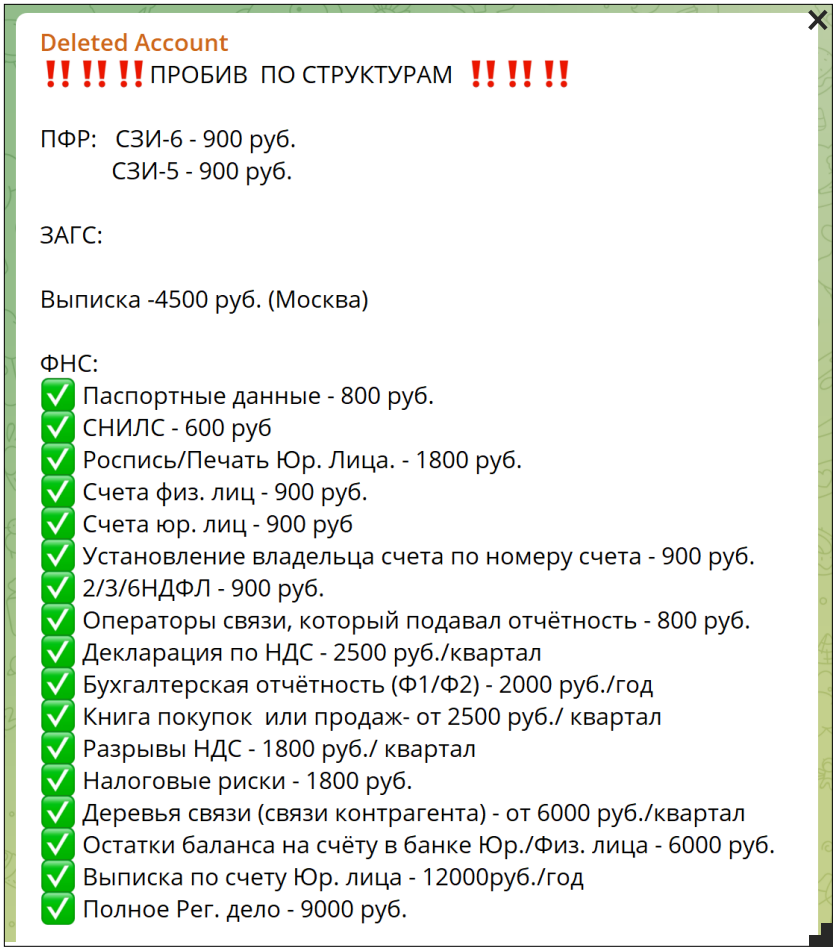


Рисунок 19. Сообщение о продаже документов и персональной информации

Услуги по обналичиванию средств набирают популярность, и при этом все больше распространяются услуги фальсификации документов (например, для создания и верификации аккаунтов, в том числе банковских и на различных биржах криптовалют). Массовое распространение этих услуг также может быть вызвано блокировкой и ограничением функций множества сервисов для российских пользователей.

🔶" [redacted] " - СЕРВИС ДЛЯ ОТРИСОВКИ ВАШИХ ДОКУМЕНТОВ🔶
———————————————————————

🖌️КОРОТКО О НАС:🖌️

✍️ *ТОЛЬКО ПРОВЕРЕННЫЕ СПЕЦИАЛИСТЫ СО СТАЖЕМ ОТ 2-Х ЛЕТ*

✅ *УСПЕШНО ПРОХОДИМ МОДЕРАЦИЮ НА БОЛЬШИНСТВЕ СЕРВИСАХ*

🧾 *В НАЛИЧИИ ШАБЛОНЫ 62-Х СТРАН*

📊 *СТРОГО РЫНОЧНЫЕ ЦЕНЫ*

📍 *СКИДКИ НА ОПТОВЫЕ ЗАКАЗЫ*

💼 *ОТКРЫТЫ НА 4-Х КРУПНЫХ ФОРУМАХ*
———————————————————————

📌ВЫПОЛНИМ ЛЮБУЮ РАБОТУ:📌

❎ *РЕДАКТИРОВАНИЕ ФОТО-СЕЛФИ*

❎ *СОЗДАНИЕ ПЕЧАТЕЙ*

❎ *ОТРИСОВКА DL(+barcodes)/ID/CC НА СПЕЦ. ПЛАСТИКЕ С МАТОВЫМ ПОКРЫТИЕМ*

❎ *СЕРТИФИКАТЫ, КВИТАНЦИИ, СЧЕТА*

❎ *ОТРИСОВКА ПАСПОРТОВ, В/У, ПЛАТЁЖНЫХ СИСТЕМ И Т.Д.*

Рисунок 20. Сообщение об услугах подделки документов

В теме учетных данных больше всего сообщений посвящено продаже аккаунтов различных сервисов: это могут быть стриминговые платформы, социальные сети, криптобиржи, букмекерские конторы. Так, аккаунт Spotify может стоить 5 $, а премиум-аккаунт на Netflix с подпиской на год — от 10 $. Аккаунты пользователей криптобирж и букмекерских компаний обойдутся намного дороже: для их верификации обычно требуются паспортные данные, а на внутреннем счете сервиса уже могут быть денежные средства.

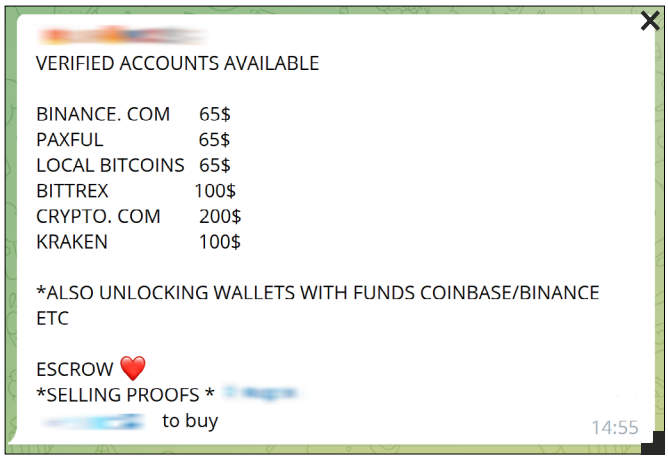


Рисунок 21. Сообщение о продаже аккаунтов криптовалютных бирж

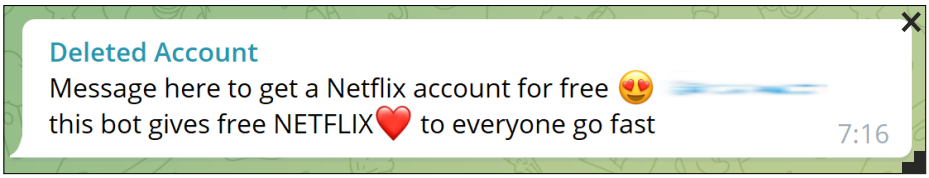


Рисунок 22. Сообщение о раздаче аккаунтов Netflix

В первом квартале мы упоминали об особом интересе к аккаунтам VPN-сервисов, и в мессенджерах эти данные также широко распространяются. Так, число сообщений, связанных с VPN, к 2022 году выросло более чем в три раза в сравнении с началом 2020 года. Чаще всего продают аккаунты NordVPN: эти же данные собирают стилеры, упомянутые в разделе о ВПО.

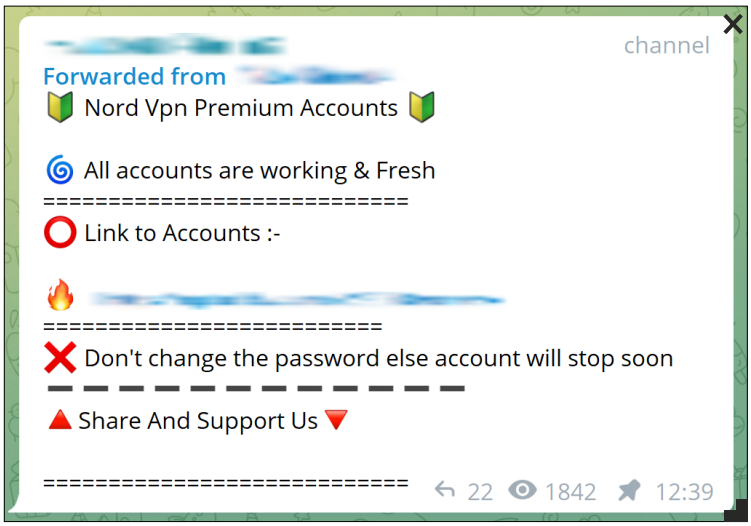


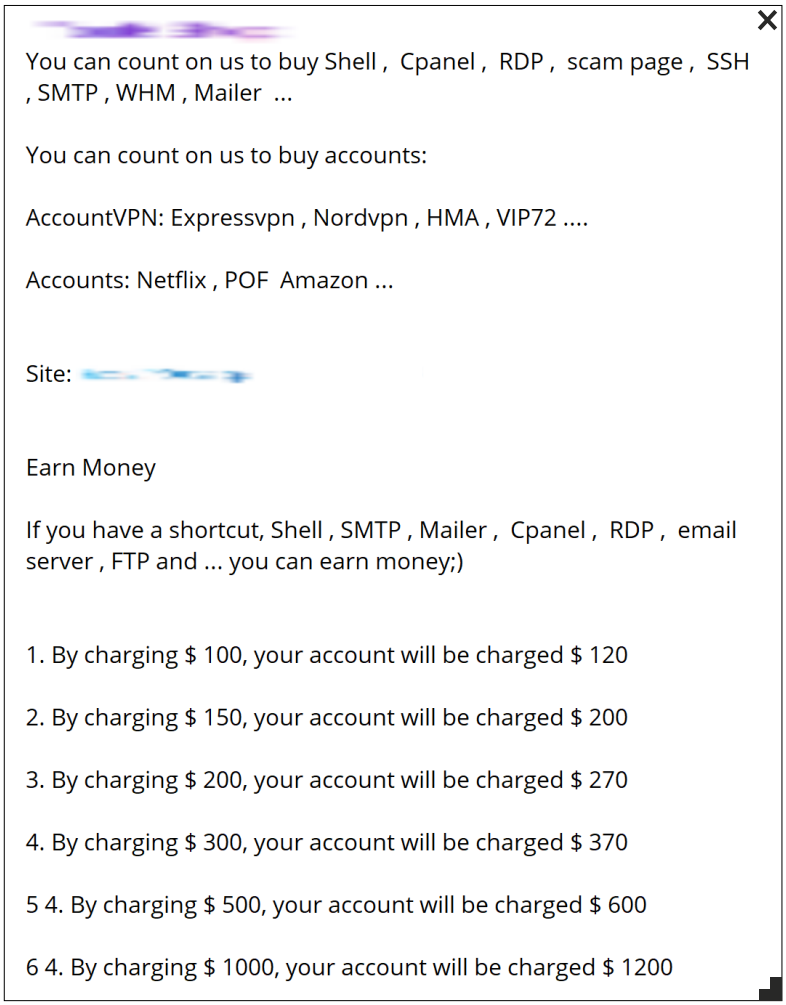
Рисунок 23. Сообщение о продаже аккаунтов VPN-сервисов

Доступы

[1]Веб-шелл — это загруженный на сервер файл, с помощью которого злоумышленник может выполнить команды ОС на сервере организации через веб-интерфейс и получить доступ к другим файлам.

К этой теме мы относим сообщения, где упоминаются доступы к корпоративным сетям организаций. Это могут быть, например, учетные данные для подключения к сети по протоколам удаленного доступа или доступ к веб-шеллу[1]. Сообщения на тему доступов составили всего 1% от проанализированных сообщений, но при этом в одном объявлении могли быть выставлены на продажу сразу несколько доступов к различным организациям. Покупка и продажа доступов пока не так распространены в мессенджерах, как на форумах, по крайней мере в публичных каналах и группах.

Чаще всего продаются учетные данные для доступа по RDP, VPN и через веб-шелл, а их цена может начинаться от 7 $.



You can count on us to buy Shell , Cpanel , RDP , scam page , SSH , SMTP , WHM , Mailer ...

You can count on us to buy accounts:

AccountVPN: Expressvpn , Nordvpn , HMA , VIP72 ....

Accounts: Netflix , POF Amazon ...

Site:

Earn Money

If you have a shortcut, Shell , SMTP , Mailer , Cpanel , RDP , email server , FTP and ... you can earn money;)

1. By charging $ 100, your account will be charged $ 120

2. By charging $ 150, your account will be charged $ 200

3. By charging $ 200, your account will be charged $ 270

4. By charging $ 300, your account will be charged $ 370

5 4. By charging $ 500, your account will be charged $ 600

6 4. By charging $ 1000, your account will be charged $ 1200

Рисунок 24. Объявление о продаже доступов и сотрудничестве

Услуги в мессенджерах

Две трети сообщений на тему киберпреступных услуг составляют обсуждения обналичивания денежных средств, например вывод криптовалют. DDoS-атаки оказались вторыми по популярности, набрав 16% от всех сообщений в этой теме. Еще около 9% сообщений — это предложения услуг по взлому ресурсов; они включают в себя компрометацию почтовых аккаунтов и аккаунтов в социальных сетях, а также взлом веб-сайтов и серверов.

Кроме того, в теневых каналах мессенджера встречаются услуги массовой установки ВПО (2%), услуги перенаправления трафика из рекламных сетей (1%), таргетированной рекламы и других каналов, которые могут быть использованы для перенаправления на фишинговые сайты или сайты, содержащие ВПО.

Услуга установки ВПО подразумевает установку программного обеспечения на компьютер или телефон жертвы, которая может быть осуществлена, например, с помощью рассылок с вредоносными вложениями, через ботнеты, путем атак типа watering hole. Эта услуга часто предоставляется дополнительно при продаже ВПО (например, стилеров и майнеров).

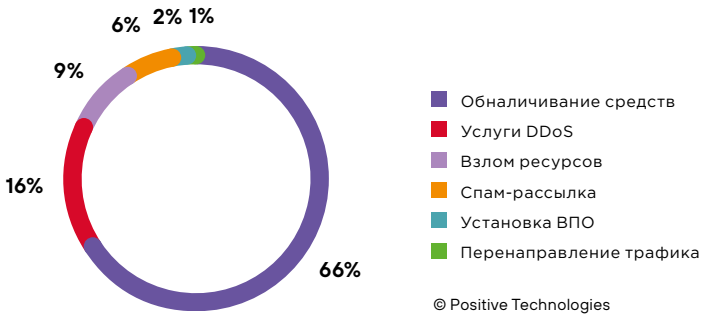


Рисунок 25. Сообщения на тему киберпреступных услуг

Проведение DDoS-атак

Каждое пятое сообщение на тему DDoS является объявлением о продаже услуг по проведению DDoS-атаки, их стоимость зависит от продолжительности атаки: за час цена составит 8 $, за сутки — 40 $, а неделя будет стоить не менее 200 $. Таким же образом распространяются и инструменты для проведения DDoS-атак.

Предоставляю DDOS услуги по устранению различных сайтов и серверов.

Наш сервис быстро и качественно решит ваши проблемы с конкурентами.

Особенности нашего DDOS SERVICE:
-Бесплатный тест до 10 минут
-Все анонимно
-Индивидуальный подход к каждому клиенту
-Во время атаки сайты не подают признаков жизни
-В нашем распоряжении практически все известные типы атак
-Постоянный мониторинг за атакуемой целью
-Подстраиваемся к бюджету клиента. Предложим оптимальный вариант
-Возврат денежных средств в случае неудачи.
-Сотрудничаем со всеми известными гарантами
-Предоставляем скидки постоянным клиентам
-Скидки при больших объёмах

Стоимость услуги зависит от атакуемой цели:
-час 8$ (выгоднее взять на сутки)
-от 75$ за сутки
-неделя, месяц обсуждается индивидуально.

Принимаем оплату только Биткоинами.
Контакт для заказа : [redacted]

12:57

Рисунок 26. Объявление о продаже услуг DDoS

Значительный рост числа сообщений на тему DDoS пришелся на I квартал 2022 года. В том же квартале мы наблюдали рост числа атак на веб-ресурсы различных организаций.

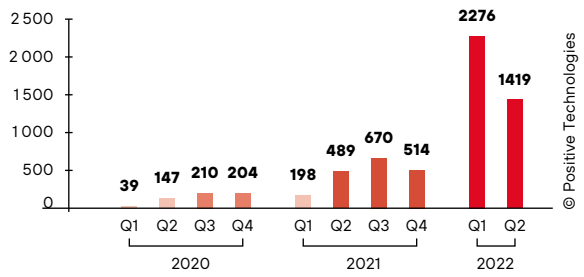


Рисунок 27. Количество сообщений на тему DDoS

Увеличению числа атак способствовал тот факт, что в I квартале стали активно распространяться бесплатные инструменты для их проведения. Часть сообщений в этот период содержала призывы к атакам на определенные серверы.

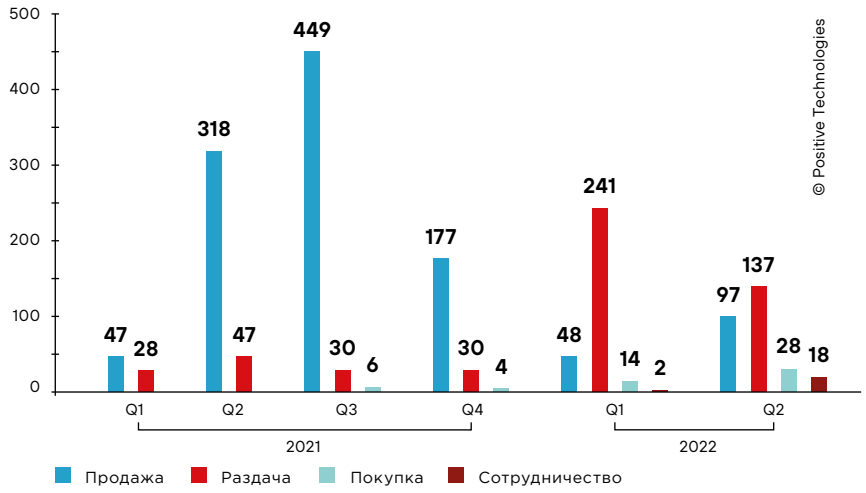


Рисунок 28. Сообщения различных категорий в теме DDoS

Ко второму кварталу мы видим снижение количества сообщений о раздаче инструментов для DDoS, однако наблюдается небольшой прирост числа сообщений о сотрудничестве: некоторые из группировок переходили от открытого распространения исходного кода среди подписчиков к поиску участников для своих команд.

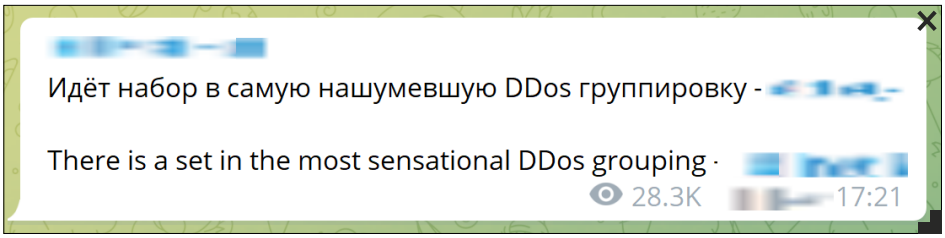


Рисунок 29. Объявление о наборе участников в группировку

Услуги взлома ресурсов

Наибольший интерес для злоумышленников представляют социальные сети и мессенджеры: сообщения об услугах по взлому аккаунтов «ВКонтакте», Telegram, WhatsApp, Viber и других социальных сетей и мессенджеров составляют 72% от общего числа сообщений в категории.

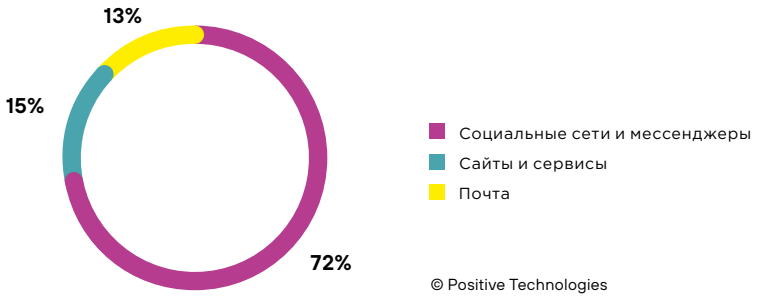


Рисунок 30. Сообщения на тему взлома ресурсов

Цены на компрометацию аккаунтов социальных сетей и мессенджеров различаются: например, взлом аккаунта «ВКонтакте» может обойтись от 10 $ до 50 $. Мессенджеры обойдутся дороже: например, взлом Telegram, Viber и WhatsApp может стоить от 350 $.

За компрометацию корпоративного аккаунта цены существенно выше: если за взлом личного почтового аккаунта берут 100 $, то за компрометацию корпоративного почтового аккаунта могут потребовать в два раза больше, не менее 200 $.

Взлом почт (только русскоязычный сегмент):

1️⃣
Mail.ru:

Взлом - вероятность успеха 75% (без смены пароля) ✉️

Взлом + зеркало - вероятность успеха 75% (без смены пароля) 📩

Зеркало без взлома – вероятность успеха 98% 📨

2️⃣
Yandex.ru / rambler.ru :

Взлом – вероятность успеха 75% (без смены пароля) 📥

Взлом + зеркало – вероятность успеха 75% (без смены пароля) 📥

Зеркало без взлома - вероятность успеха 99% 📥

Сроки : 5 - 30 суток 🕔
Возможна выкачка содержимого 📤
Цена и сроки на корпоративные почты могут отличаться ❗

Возможна работа по другим доменам - уточняйте (gmail) ⚠️

Рисунок 31. Объявление о взломе почтовых аккаунтов

Обналичивание средств

Обналичивание не только широко распространено, но и с каждым кварталом становится все более популярной услугой. Несмотря на общий спад количества сообщений в I квартале 2022 года, связанный с множественными блокировками групп с нелегальными материалами, во II квартале число сообщений на тему обналичивания средств вернулось к значениям 2021 года.

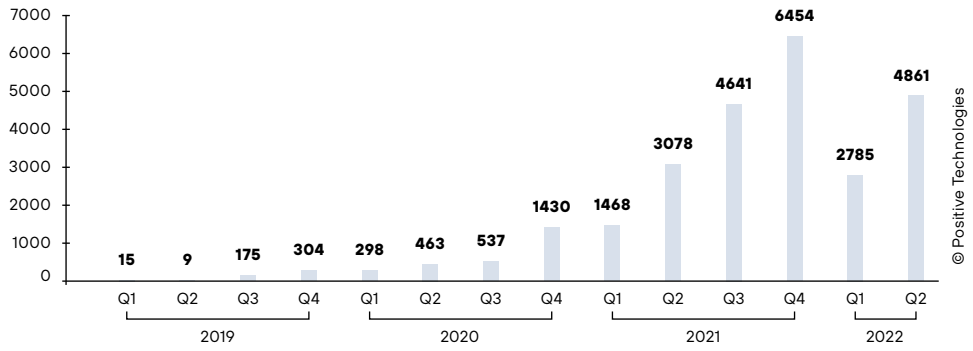


Рисунок 32. Количество сообщений на тему обналичивания средств

Шесть из каждых 10 сообщений на эту тему являются объявлениями о продаже и предоставлении услуг. Покупке посвящены 16% сообщений, а в 3% предлагается долгосрочное сотрудничество.

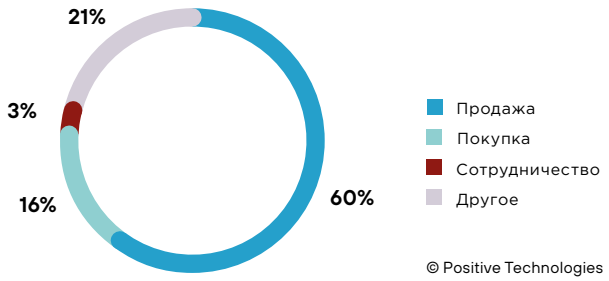


Рисунок 33. Категории услуг по обналичиванию средств

Принимаю платежи (обнал):
💰 карты и счета РФ
💰 3D мерч для карт (cc)
💰 с Moneygram, WU
💰 Unistream; Contact
💰 на счета Европы и США
💰 на карты Европы и США
💰 платеж по SWIFT, SEPA,
💰 на корр счета банков
💰 на расчётник ИП РФ
💰 на корпоративные карты
💰 на SEPA чернуху
💰 на Bpay

💶 Приму платежи на:
•Счет в Ирландии
•Счёт в Британии
•Счёт в Commerzbank AG
•Счёт в Литве
•Счёт в Бельгии
•Счёт в Словакии
•Счёт в Чехии
•Счет в Германии
•Счёт в Нидерландах
•Счёт на Мальте
•Счёт Молдовы
•Счёт в Канаде

Писать👉
Гарант +
16:52

Рисунок 34. Объявление об услугах обналичивания средств (продажа)

Ищем Обнал сервис из СНГ и восток европы.

Задача принимать крипту с Африканской биржи. IP и регистрация принимающего кошелька СНГ и восток европы обязательна. Объем от 300к $ день. Ваши 30%. Нам возврат чистыми!

Гарантии возврата обязательны! Гаранты форумов

Без гарантий и на тест не отправляем.
19:13

Рисунок 35. Объявление об услугах обналичивания средств (покупка)

Спам-рассылки

Услуги спама и массовой рассылки в Telegram достаточно популярны (6% от общего количества сообщений об услугах). Чаще всего предлагают спам по SMS (54% сообщений), немного реже — спам по электронной почте (32%).

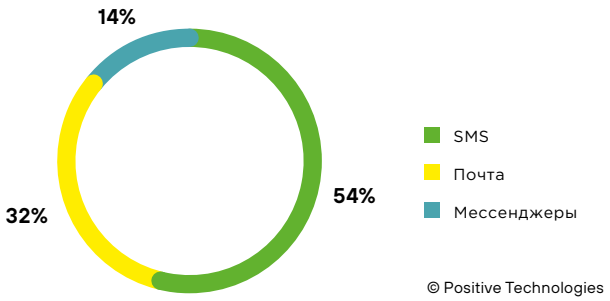


Рисунок 36. Инструменты для массовых рассылок (доля сообщений на тему спама)

Вместе с SMS-рассылками часто предлагаются и услуги массового обзвона. Среди мессенджеров самым популярным для распространения рассылок стал Telegram.

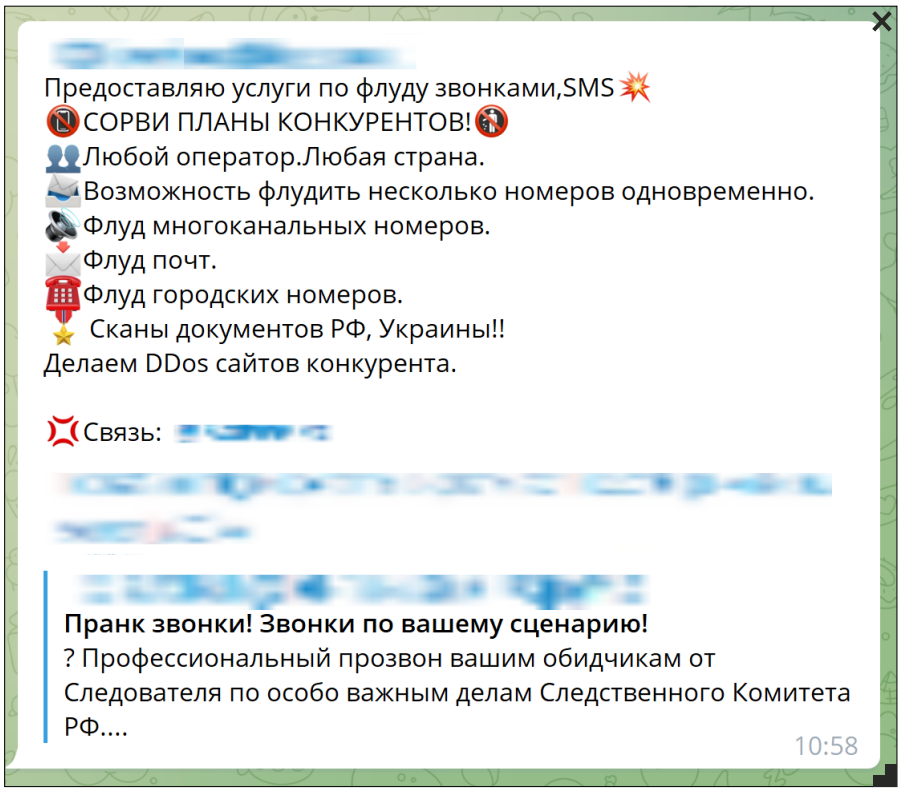


Рисунок 37. Объявление об услугах спама

Цены на рассылки обычно рассчитываются в зависимости от времени или от количества сообщений. Например, средняя стоимость для одного почтового адреса — около 1 $ за час спама или 1000 писем.

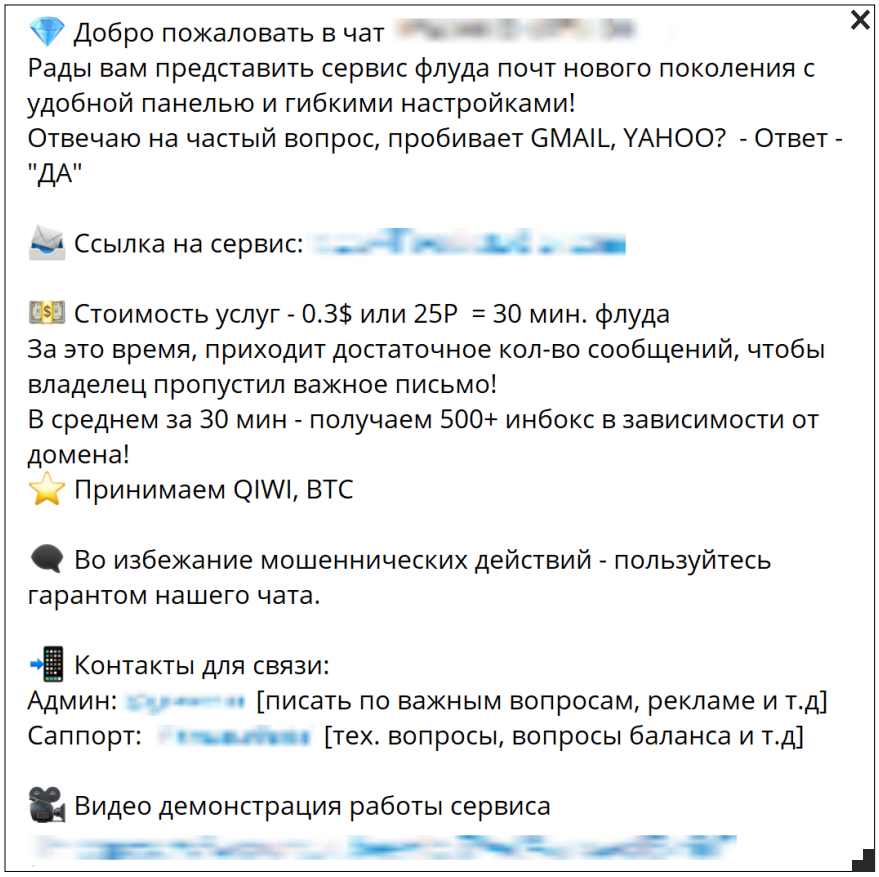


Рисунок 38. Объявление об услугах спама

Заключение

Количество уникальных кибератак постоянно растет, и теневой рынок также становится все более широким явлением, просачиваясь в обычные социальные сети и мессенджеры и тем самым существенно снижая порог входа для злоумышленников. Наше исследование показывает актуальное положение теневого рынка в Telegram и дает повод серьезно относиться к мессенджеру как источнику информации для киберразведки и прогнозирования киберугроз; анализ этой информации помогает выстраивать процессы информационной безопасности. Своевременное реагирование на сообщения о готовящихся атаках, например о DDoS-кампаниях, распространяющихся эксплойтах и скомпрометированных данных, поможет принять соответствующие меры защиты и предотвратить недопустимые для организаций события.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — ведущий разработчик решений для кибербезопасности. Наши технологии и сервисы используют более 2300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Уже 20 лет наша основная задача — предотвращать хакерские атаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.

Рынок_киберпреступных_услуг_в_Telegram_A4.RUS.0003.02.OCT.24.2022