GROUP-IB

ЭВОЛЮЦИЯ CLASSISCAM

Происхождение, принцип работы
и развитие схемы

THREAT REPORT

Дисклеймер

1. Отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью отчета является предоставление сведений о тактике, инструментах и особенностях инфраструктуры различных групп для минимизации риска дальнейшего совершения таких противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В отчете приведены рекомендации от экспертов Group-IB по превентивным мерам защиты от атак групп. Описание деталей угроз в отчете приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованная в отчете информация об угрозах не является пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Отчет подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления с отчетом, цитирования отчета в объеме, оправданном правомерной целью цитирования, при условии, что сам отчет, включая ссылку на сайт правообладателя, на котором он размещен, будет указан как источник цитаты.
4. Отчет и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав на отчет Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.

Содержание

Появление схемы Classiscam

На теневой стороне интернета давно существуют форумы киберпреступников, объединяющие на своей площадке людей, которые технически подкованы и могли бы своей деятельностью наносить существенный вред компаниям и государствам.

Однако сфера киберпреступлений — как и мир в целом — меняется. И на подобные площадки стали приходить люди с меньшими техническими знаниями или вовсе несовершеннолетние, ищущие способ подзаработать в интернете. Чаще всего это те, кто занимался какими-то мелкими махинациями в интернете и имел небольшой доход. К тому же на таких форумах царил хаос, не было никаких норм, правил поведения или элементарной модерации сообщества. Ущерб от деятельности подобных сообществ был небольшой и носил локальный характер. Происходившие инциденты практически не привлекали внимания со стороны атакуемых компаний и правоохранительных органов. Все это воспринималось как проблема конкретного пострадавшего человека, с которой он сам должен разбираться.

Со временем ситуация начала меняться. Сообщества низкоквалифицированных преступников продолжали расти, собирая все больше последователей. На форумах стали устанавливать правила, появилась модерация деятельности участников. Это позволило структурировать работу сообществ, и их прибыль начала увеличиваться. Желание заработать начало побеждать и рождать спрос на новые варианты заработка. Такие условия повлияли на появление квалифицированных специалистов в этой области.

Вначале нехватку средств для осуществления скам-атак компенсировали методами социальной инженерии, а недостаток хороших исполнителей — их числом. Первые организованные группы на аналогичных форумах занимались хищением учетных записей игровых площадок и социальных сетей. Но организация работы вышла на новый качественный уровень.

Появились организаторы, предоставляющие всем желающим ссылки на фишинговые сайты, имитирующие страницы социальных сетей или игровых платформ. Способы распространения ссылок и убеждения жертвы ввести свои реквизиты полностью делегировались исполнителю, и для понимания механики работы предоставлялись простые руководства (мануалы). Порог вхождения в мошеннические схемы значительно снизился за счет автоматизации работы инструментов для обмана — скамеры все чаще стали использовать административные панели.

Админпанели

Одними из первых инструментов воркеров стали админпанели. Они позволили снизить порог входа для новых мошенников, желающих поучаствовать в схеме, и значительно ускорили создание фишинговых страниц.

Воркер (с англ. «работник») — один из основных участников мошеннической схемы Classiscam, задача которого — привлечь трафик на фишинговый ресурс.

Админпанель — это сайт на отдельном домене или IP, доступ к которому предоставляется по логину/паролю или специальному токену после собеседования с лидером проекта.

Для использования админпанели не нужно обладать какими-то специальными техническими знаниями: интерфейс прост и интуитивно понятен (рис. 1–4).

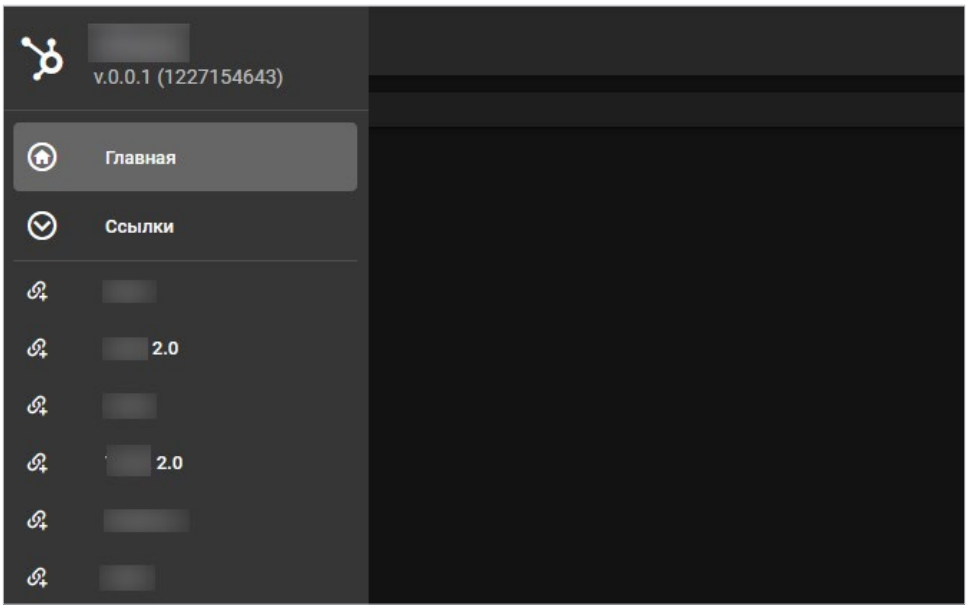


Рис. 1. Пример админпанели

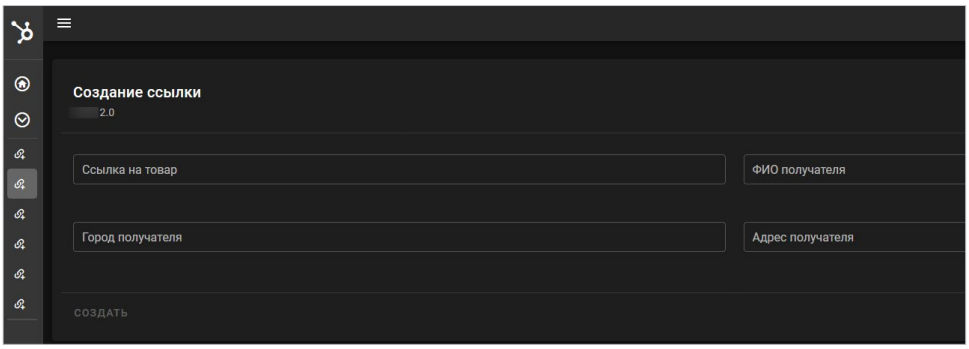


Рис. 2. Пример админпанели

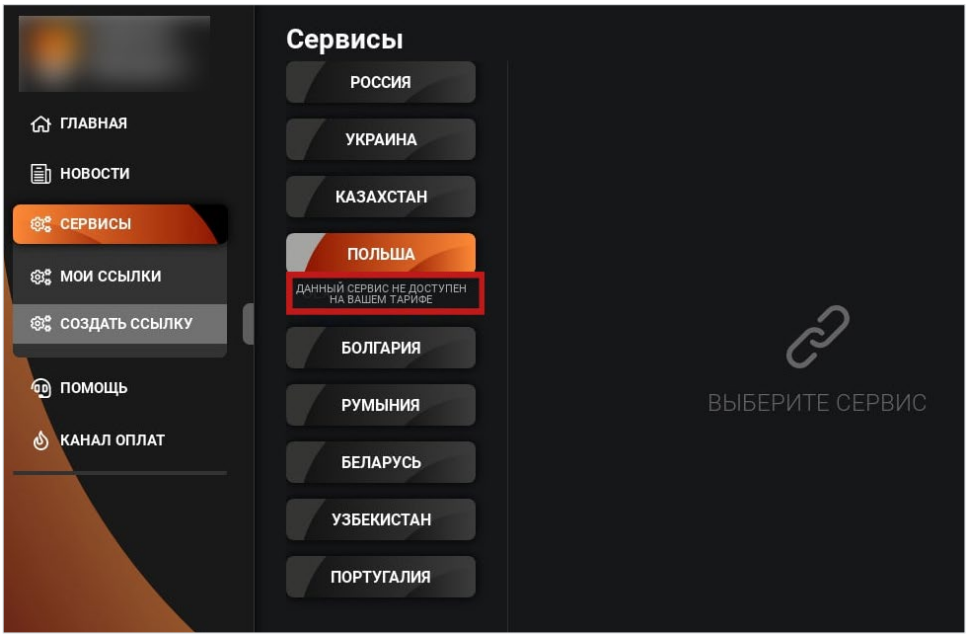


Рис. 3. Пример админпанели

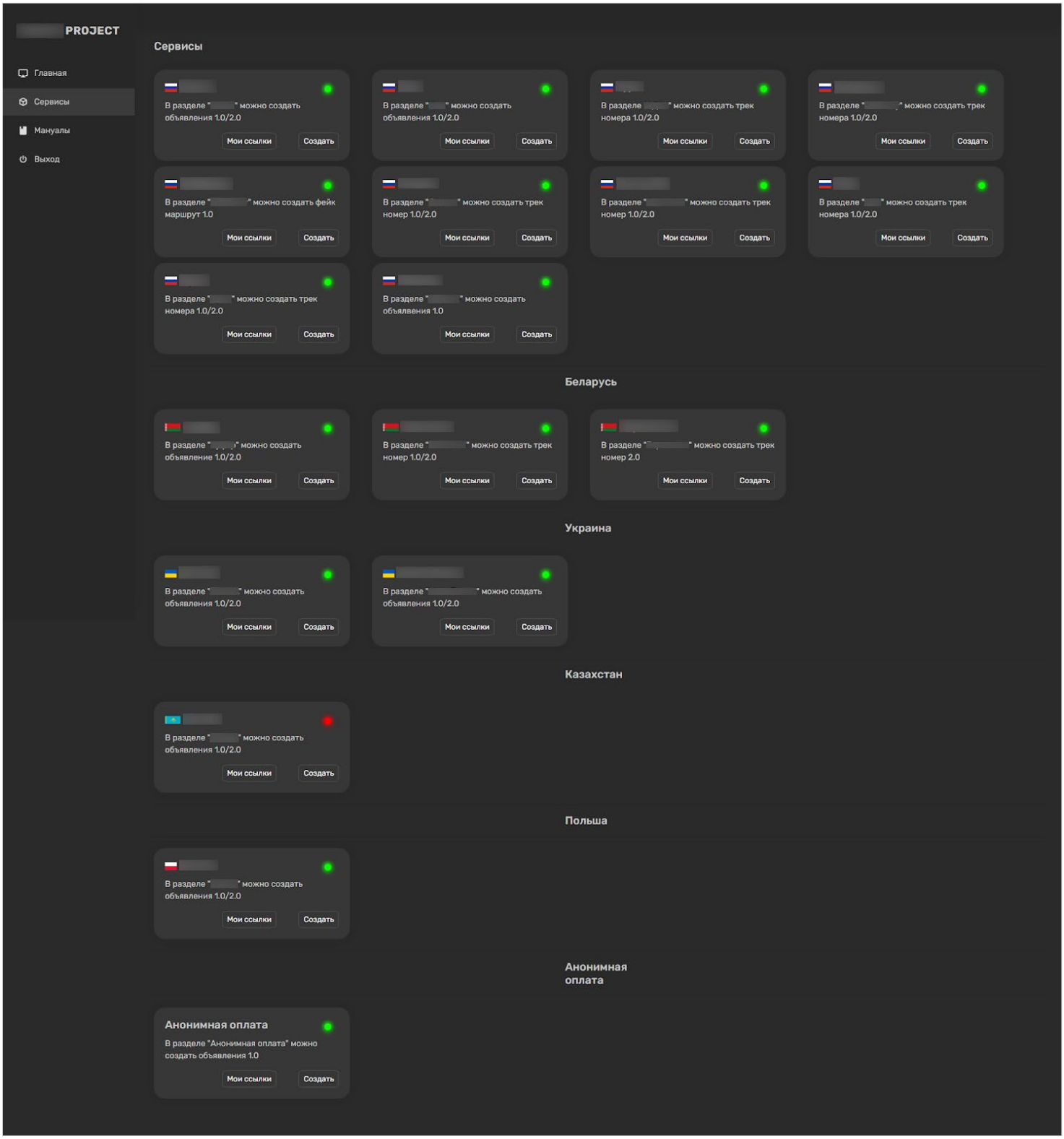


Рис. 4. Пример админпанели

Помимо создания фишинговых страниц, админпанель зачастую содержит раздел с мануалом — инструкцией, которая помогает новичкам в скаме.

Эволюция схемы Classiscam

В 2019 году схема Classiscam начинала свою работу на досках объявлений. Часто это было мошенничество даже без использования фишинг-страниц: пользователей просто уговаривали перевести деньги за товар на карту или телефон.

Мошенники выступали исключительно как продавцы. Приемы для привлечения покупателей были стандартными: низкая цена, ограничение времени на продажу, продажа эксклюзивных или дефицитных товаров.

Изначальная схема действий мошенников выглядела следующим образом.

1 Создание или поиск лота-приманки на сайте объявлений

Злоумышленники регистрируют новые аккаунты или используют взломанные аккаунты интернет-сервисов. Создают собственное предложение или обращаются к чужому в зависимости от выбранной схемы. Например, объявления, рассчитанные на разные целевые аудитории, о продаже товаров по заниженной цене: фотоаппаратов, игровых приставок, ноутбуков, смартфонов, бензопил, звуковых систем для авто, швейных машинок, коллекционных вещей, товаров для рыбалки, спортпитания и др.

Для удобства в поиске жертв воркеры используют сервисы по отслеживанию объявлений на атакуемых интернет-площадках. Это позволяет массово рассылать сообщения продавцам конкретного товара или услуги, увеличивая шанс найти пользователя, которого получится обмануть.

2 Контакт с жертвой

После того как пользователи сервисов выходят на контакт со злоумышленниками с помощью внутреннего чата на самой интернет-платформе, им предлагается перейти в мессенджеры WhatsApp или Viber для дальнейшего обсуждения покупки и доставки.

Внутренние сервисы переписок нередко предупреждают своих пользователей о подозрительных ссылках или даже блокируют их, а в мессенджерах такой проблемы у злоумышленников не возникает.

4 Подготовка к сделке

Уже в чатах мессенджеров злоумышленники делают все, чтобы показаться добросовестными покупателями/продавцами: запрашивают у жертвы ФИО, адрес и номер телефона якобы для заполнения формы доставки на ресурсах курьерской службы. Рассказывают или спрашивают о состоянии товара, просят показать чеки и так далее. На данном этапе отличить злоумышленника от настоящего продавца или покупателя очень сложно.

5 Оплата на фишинговом ресурсе

Далее жертву вынуждают перейти по заранее сгенерированной ссылке на фишинговый ресурс, который полностью копирует официальные страницы популярных курьерских служб. Здесь представляются указанные ранее данные жертвы для сверки и после этого там же происходит оплата покупки.

6 Повторный обман

Часть жертв мошенникам удается обмануть повторно — их убеждают сделать возврат. Через некоторое время после оплаты товара покупателю сообщают, что на почте произошло ЧП. Легенда может быть любой, например сотрудник почты якобы пойман на краже, а заказанный товар конфисковала полиция, поэтому для компенсации перечисленной суммы необходимо оформить возврат средств. Для этого жертве демонстрируется окно, в котором необходимо указать данные карты и CVV-код, а далее ввести пароль из СМС, после чего вместо возврата с карты повторно списывается та же сумма.

Переход на Telegram-ботов

Несмотря на то что генерация ссылок через админпанель до определенного времени занимала довольно много времени и имела скудную функциональность по сравнению с современными Telegram-ботами, схема уже тогда пользовалась определенной популярностью.

Руководство абсолютно всех преступных групп заинтересовано в масштабировании своего бизнеса и привлечении как можно большего количества новых участников. Учитывая популярность схемы, решение проблемы, связанной с ограниченными возможностями админпанели, было вопросом времени.

С развитием функциональности Telegram-ботов злоумышленники сразу нашли способы применения данной платформы в своих целях, что позволило обойти ограничения и выйти на новый уровень благодаря автоматизации и масштабированию.

Telegram-боты позволяют создавать ссылки, выводить средства, размещать предложения о работе, продавать необходимые инструменты и инструкции, размещать рекламу и даже оказывать юридические услуги. Примеры интерфейсов Telegram-ботов показаны на рис. 5–9.

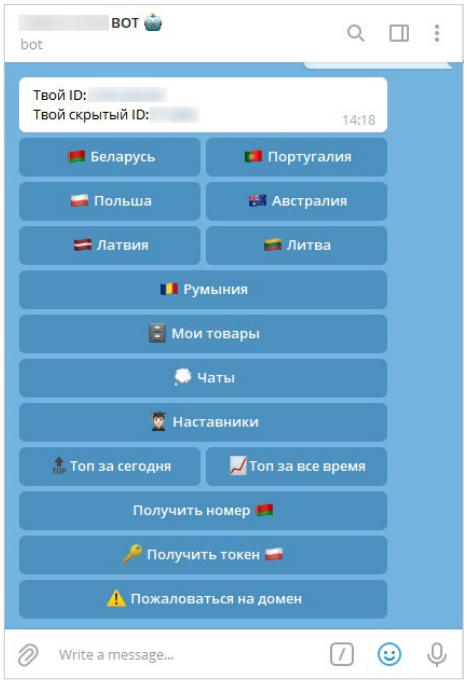


Рис. 5. Пример интерфейса Telegram-бота

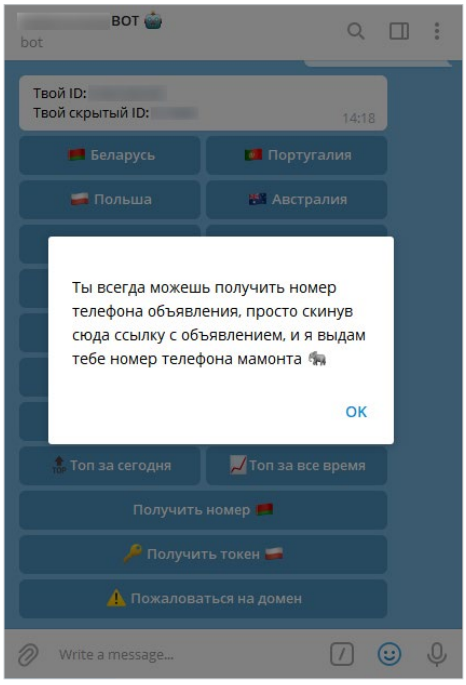


Рис. 6. Пример интерфейса Telegram-бота

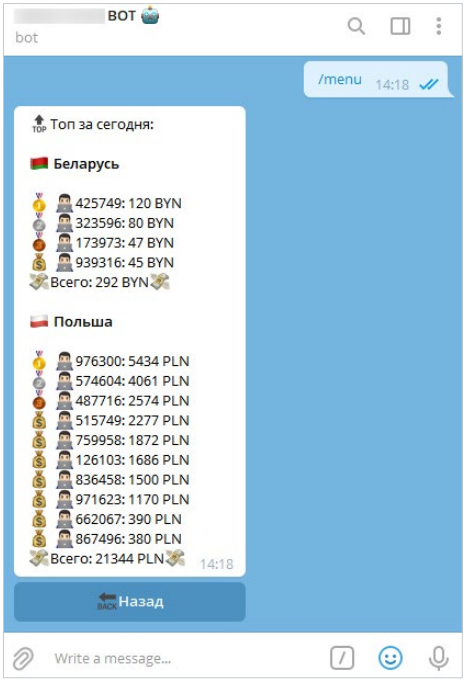


Рис. 7. Пример интерфейса Telegram-бота с разделом топ-воркеров

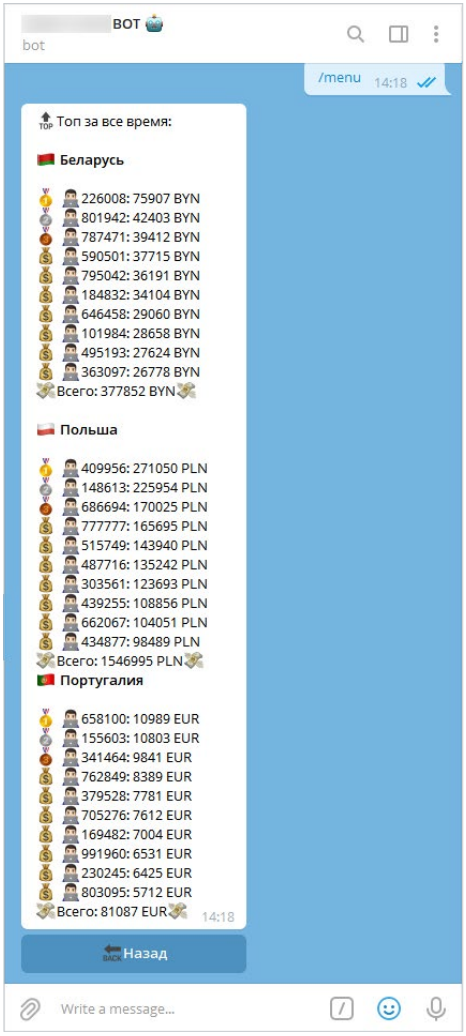


Рис. 8. Пример интерфейса Telegram-бота с разделом топ-воркеров

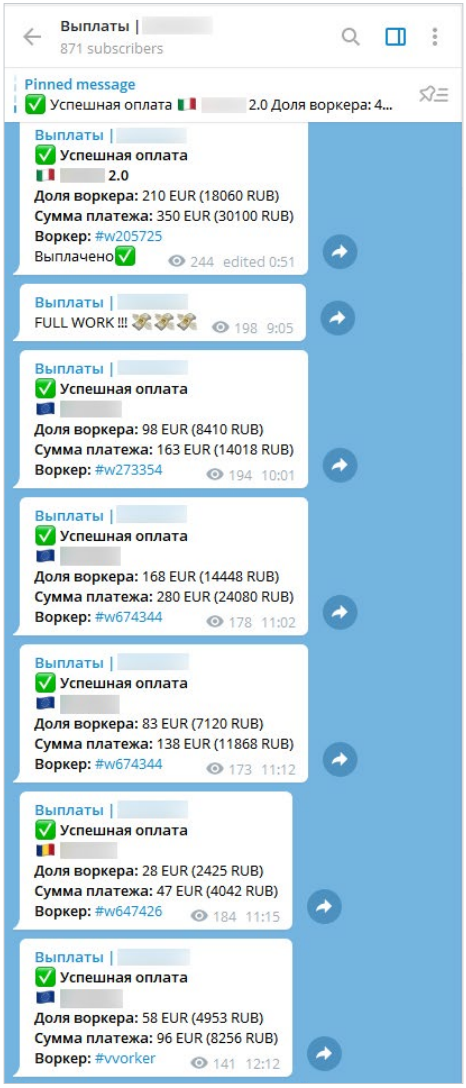


Рис. 9. Пример канала Telegram с выплатами воркерам

Telegram-боты чаще всего разрабатывают за фиксированную плату сторонние наемные специалисты, не принимавшие участия в работе схемы. Но в редких случаях все же разработкой ботов занимаются участники внутри группы. Иногда руководитель группы и разработчик — одно лицо.

Благодаря активному использованию функций Telegram количество задействованных брендов **увеличилось** более чем **в 4 раза**, а география мошенников существенно расширилась и вышла далеко за пределы СНГ — своего первоначального ареала.

Классический состав группы в целом не изменился при массовом переходе от админпанелей к Telegram-ботам. Владеет проектом лидер группы, или ТС (от англ. Topic Starter) – владелец скам-группы, занимающийся ее администрированием. Тем не менее сама роль ТС в период после появления Telegram-ботов 2019 года довольно сильно изменилась.

О масштабе распространения схемы Classiscam также хорошо говорит статистика количества участников. На данный момент это более **38 000 воркеров** занимающихся подобной деятельностью, а количество задействованных доменов превысило **5 000 единиц**.

Регистрация новых участников осуществляется через Telegram-бота, подпольные форумы или напрямую через лидеров групп (ТС). Бывают открытые и закрытые чаты группировок.

Как правило, при найме участников спрашивают про опыт работы в других проектах, какую роль они выполняли, есть ли знакомые в данном проекте, откуда узнали про проект, есть ли профили на подпольных форумах, просят представить доказательства реальной работы (рис. 10).

После того как воркер прошел процедуру регистрации, он получает доступ к трем чатам:

- с общей информацией, где рассказывают о нынешнем положении проекта, о будущем развитии и векторе действий, передают мануалы по мошенничеству и прочее;
- чату воркеров, где они общаются между собой, делятся опытом, обсуждают проекты;
- чату с выплатами — последнему на данном этапе. В нем бот показывает, какой воркер, на сколько, в какое время, через какой бренд/платформу обманул пользователя. Зачастую чаты с выплатами общедоступные. Возможно, это нужно для привлечения внимания к проекту других воркеров, для демонстрации, что проект живой.

Количество и структура чатов у каждой группировки могут различаться, примерная схема показана на рис. 11.

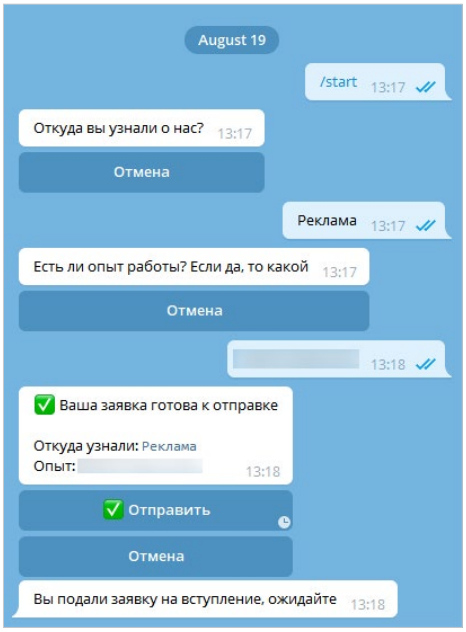


Рис. 10. Пример прохождения интервью для вступления в скам-группу в Telegram-боте

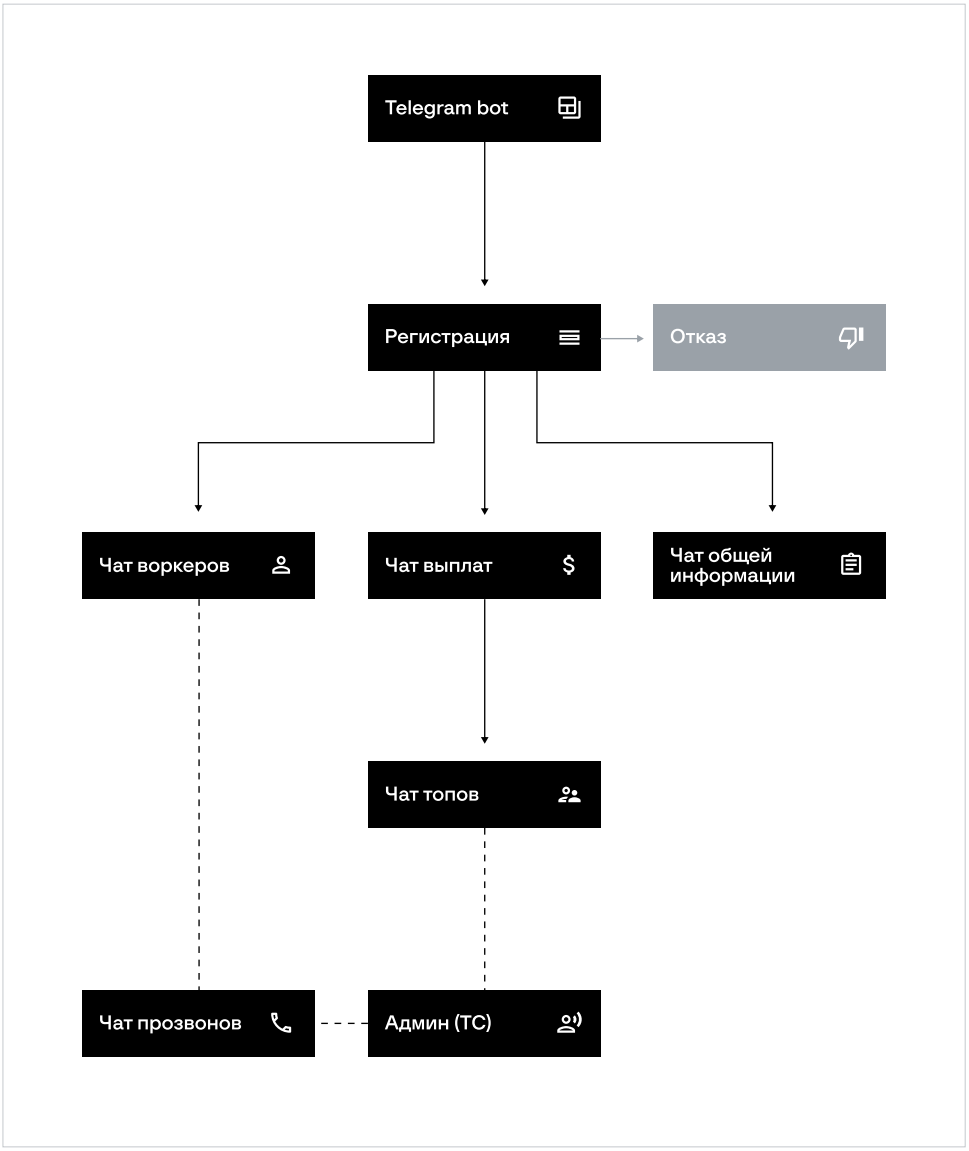


Рис. 11. Схема структуры мошеннической группировки и ее доступа к чатам

Существуют своеобразные конкурсы: лучшие воркеры добавляются в общедоступный список топов по выплатам (рис. 12). Это позволяет им получить доступ к так называемому VIP-чату, в котором топовые воркеры уже имеют влияние на проект и на его развитие и доступ к VIP-скриптам. Например, в одной из групп у топовых воркеров есть эксклюзивный доступ к мошенничеству в США, в то время как остальные мошенники не могут работать в этих регионах и иметь доступ к чату и соответствующие возможности.

Рис. 12. Пример прохождения интервью для вступления в скам-группу в Telegram-боте

Современная схема Classiscam

Актуальная версия мошеннической схемы Classiscam сформировалась благодаря развитию программного интерфейса и функциональности Telegram-ботов, что позволило мошенникам уйти от сайтов с панелями по созданию фишинговых страниц, начать вести все коммуникации и использовать необходимые инструменты для атаки в мессенджере.

Отличительной чертой новой схемы с использованием Telegram-ботов является высокий уровень автоматизации таких процессов, как создание фишинговых ссылок, распределение оплаты, учет и контроль работы воркеров, но самое главное, полностью ручной трафик, который генерируют рядовые участники группы, эти самые воркеры.

Простые и понятные интерфейсы Telegram-ботов и алгоритмы действий (мануалы) привели к тому, что требования к технической подготовке участников существенно снизились. Низкий порог вхождения для использования данной мошеннической схемы и хорошие проценты выплат за успешную атаку отразились на привлечении множества воркеров в скам-группы.

Также в отличии от классического фишинга, трафик на который привлекается полуавтоматически (спам-рассылка, SEO-продвижение фишинговых сайтов, создание аккаунтов в социальных сетях), в этой схеме скамеры привлекают трафик вручную, целенаправленно работая с жертвой.

Мошеннические ресурсы не работают на постоянной основе. Для каждого нового случая мошенничества генерируется новая уникальная ссылка с ограниченным временем работы. Ссылка прекращает работать по двум сценариям: удаляется вручную сразу после попытки мошенничества — неважно, удачной или нет, — либо автоматически через 24 часа.

Вспомогательные сервисы и услуги воздействия на жертву

Для успешной атаки могут привлекаться помощники, которые оказывают дополнительное воздействие на жертву для получения результата, а также используются различные методы. Это могут быть:

- **Помощники воркеров**

  Помощниками могут выступать прозвонщики или возвратеры, которые выдают себя за службу поддержки, бомберы — программы для массовой рассылки спама по СМС или звонков, вбиверы — мошенники, которые проводят платеж вручную. В случае успешной атаки помощники получают процент от выручки (рис. 13–16);

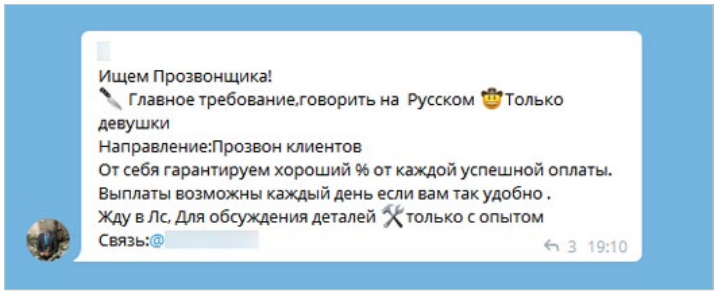


Рис. 13. Пример рекламного сообщения о наборе в прозвонщики

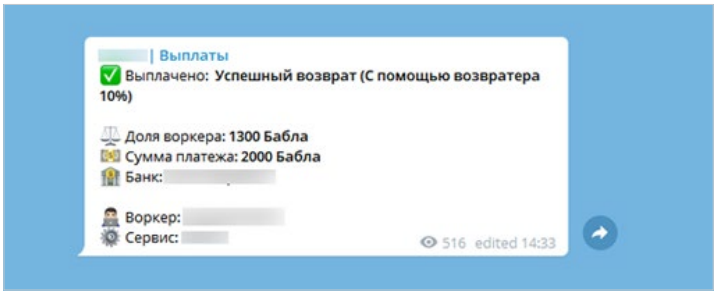


Рис. 14. Пример отчета о получении денег с использованием схемы возврата

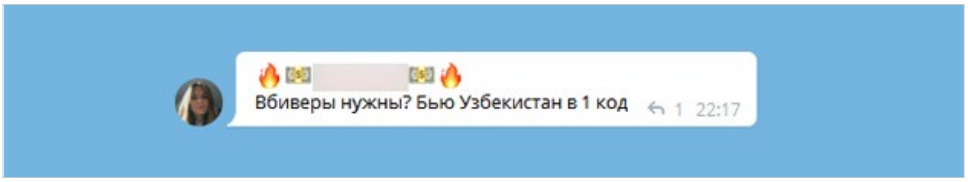


Рис. 15. Реклама оказания услуг по вбиву

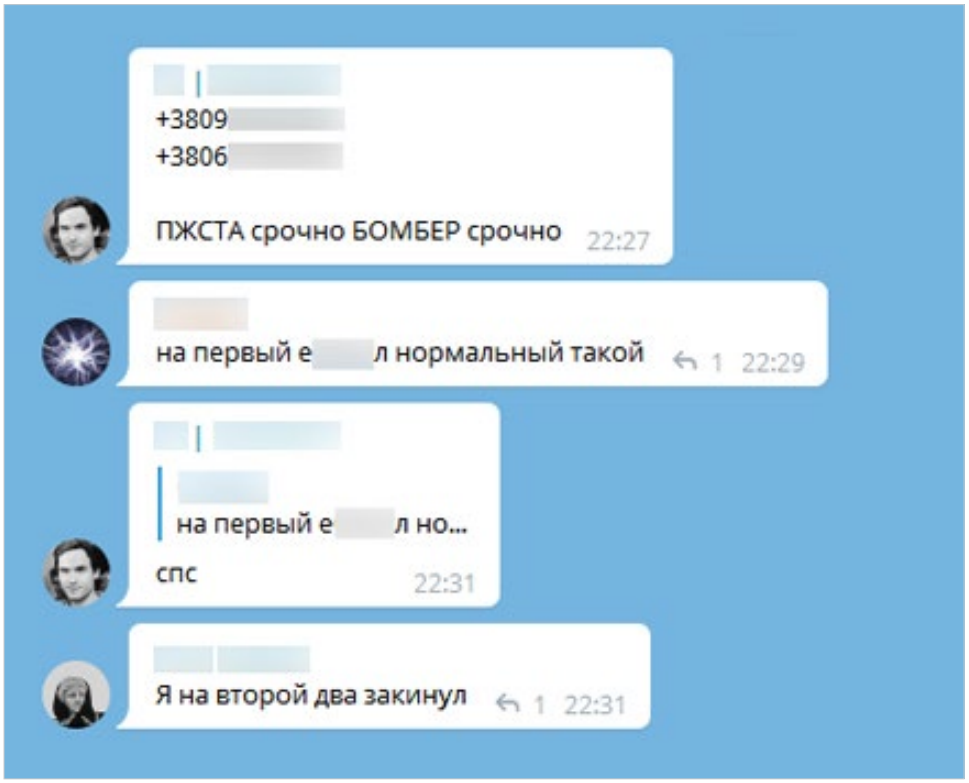


Рис. 16. Пример просьбы «забомбить» жертву

- **Отрисовка документов**
  Повышает доверие жертвы к планируемой сделке (рис. 17).

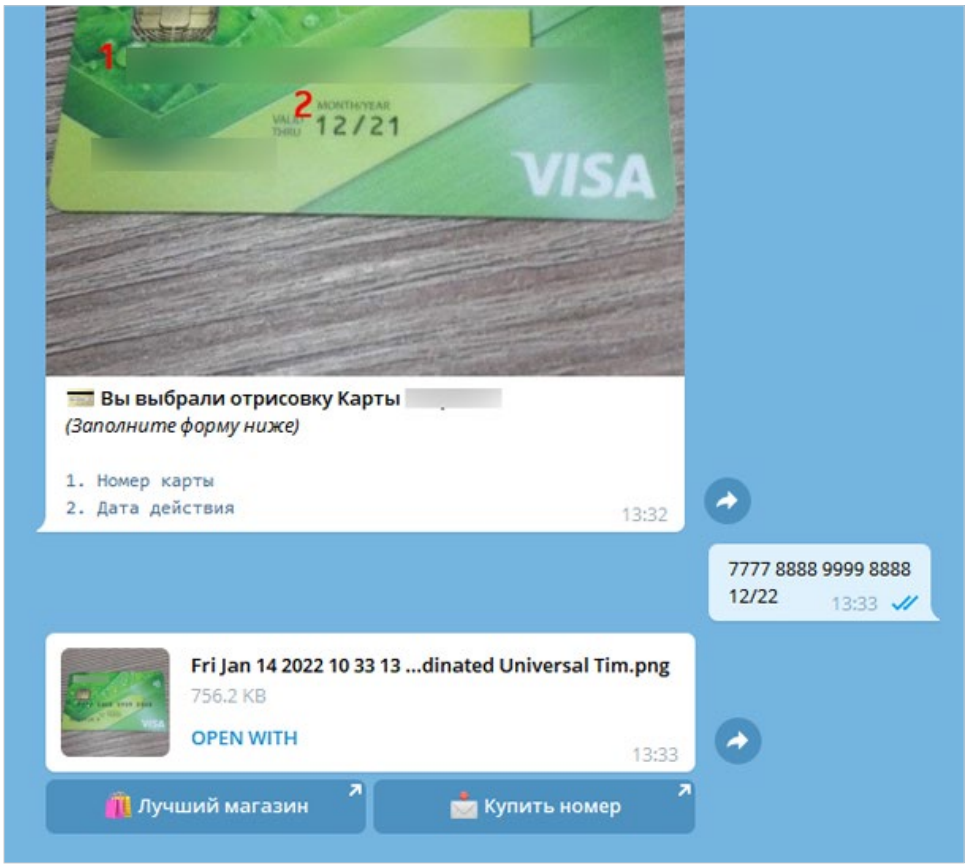


Рис. 17. Пример отрисовки банковской карты

- **Разработка и сдача в аренду Telegram-ботов**
  Аренда Telegram-ботов позволяет злоумышленникам единолично совершать скам-атаку и забирать себе все переводы от жертв, а также получать проценты с хищений воркеров, которые используют арендованный бот. На рис. 18 показан скриншот рекламы такой аренды.

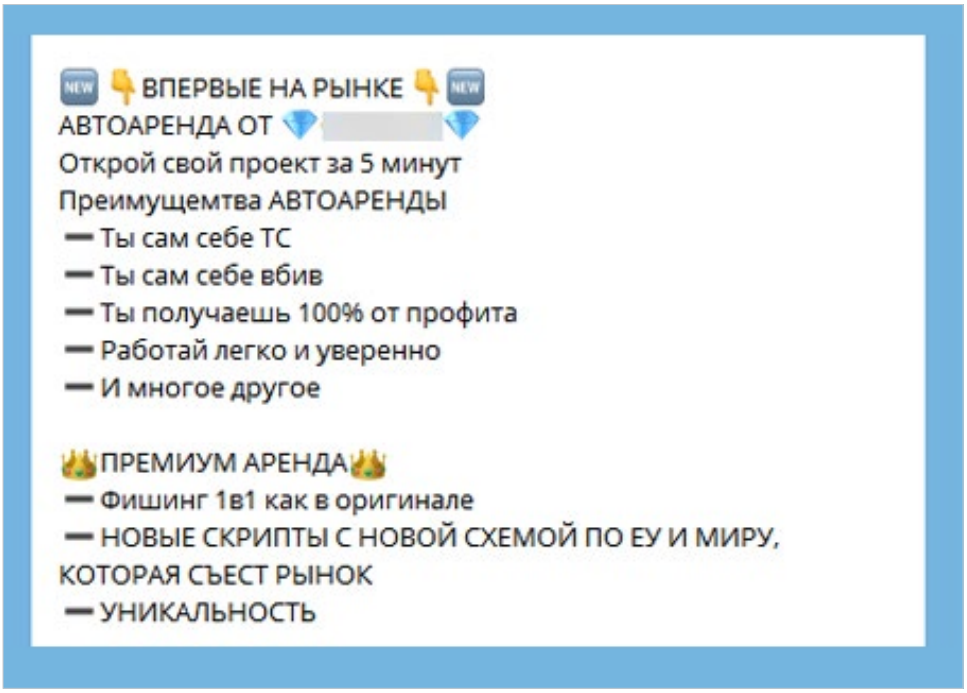


Рис. 18. Пример рекламы аренды проектов

Разновидности схемы Classiscam

У скамеров схемы разделены по версиям: 1.0, 2.0, 3.0, 4.0.

Они отличаются тем, какие именно действия совершает воркер: выдает себя за покупателя или продавца, арендодателя или арендатора.

1.0 — скам от лица продавца. Стандартный вид мошенничества с помощью схемы мамонта, когда покупатель получает сгенерированную фишинговую ссылку на оплату и теряет деньги.

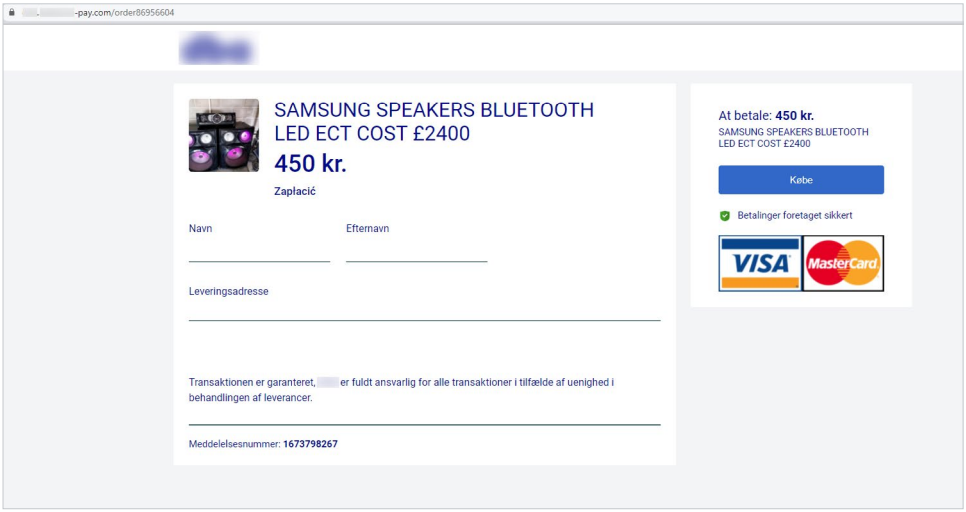


Рис. 19. Фишинговая страница по оплате товара

2.0 — скам от лица покупателя. Мошенники находят продавцов на сайтах объявлений и предлагают им сделку через доставку. Далее они генерируют фишинговую страницу для приема денег, которую отправляют продавцу якобы на проверку. На ней продавец вводит данные своей карты, но вместо получения деньги списываются с его счета.

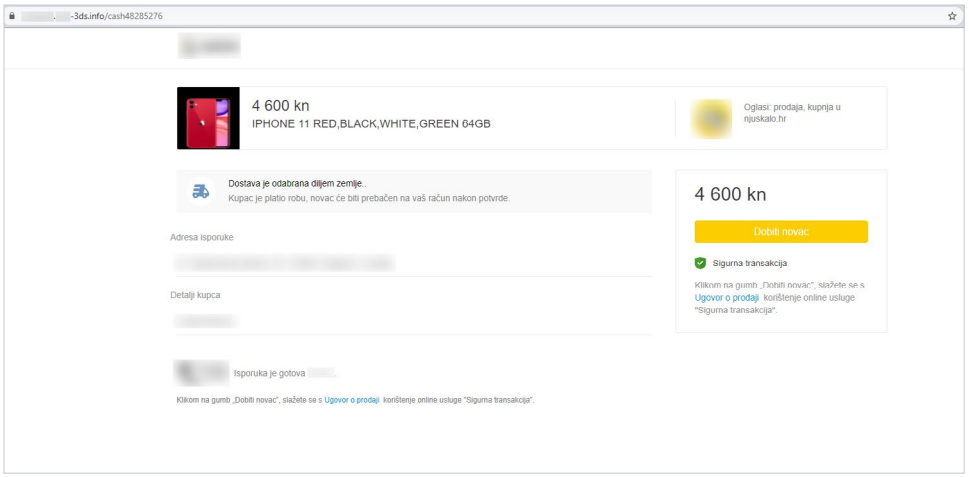


Рис. 20. Фишинговая страница по получению денежных средств за товар

3.0 — продавец публикует объявления с заранее активированной доставкой через сервис. Когда покупатель оплачивает товар, мошенник отправляет ему скриншот, на котором администрация сервиса якобы просит код подтверждения.

С помощью кода продавец заходит в аккаунт пользователя. В профиле покупателя мошенник отмечает галочкой, будто тот получил товар.

Таким образом покупатель остается и без товара, и без денег.

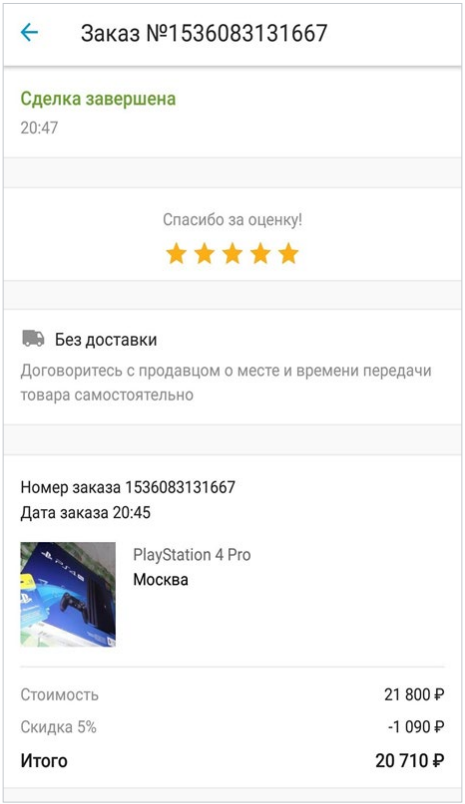
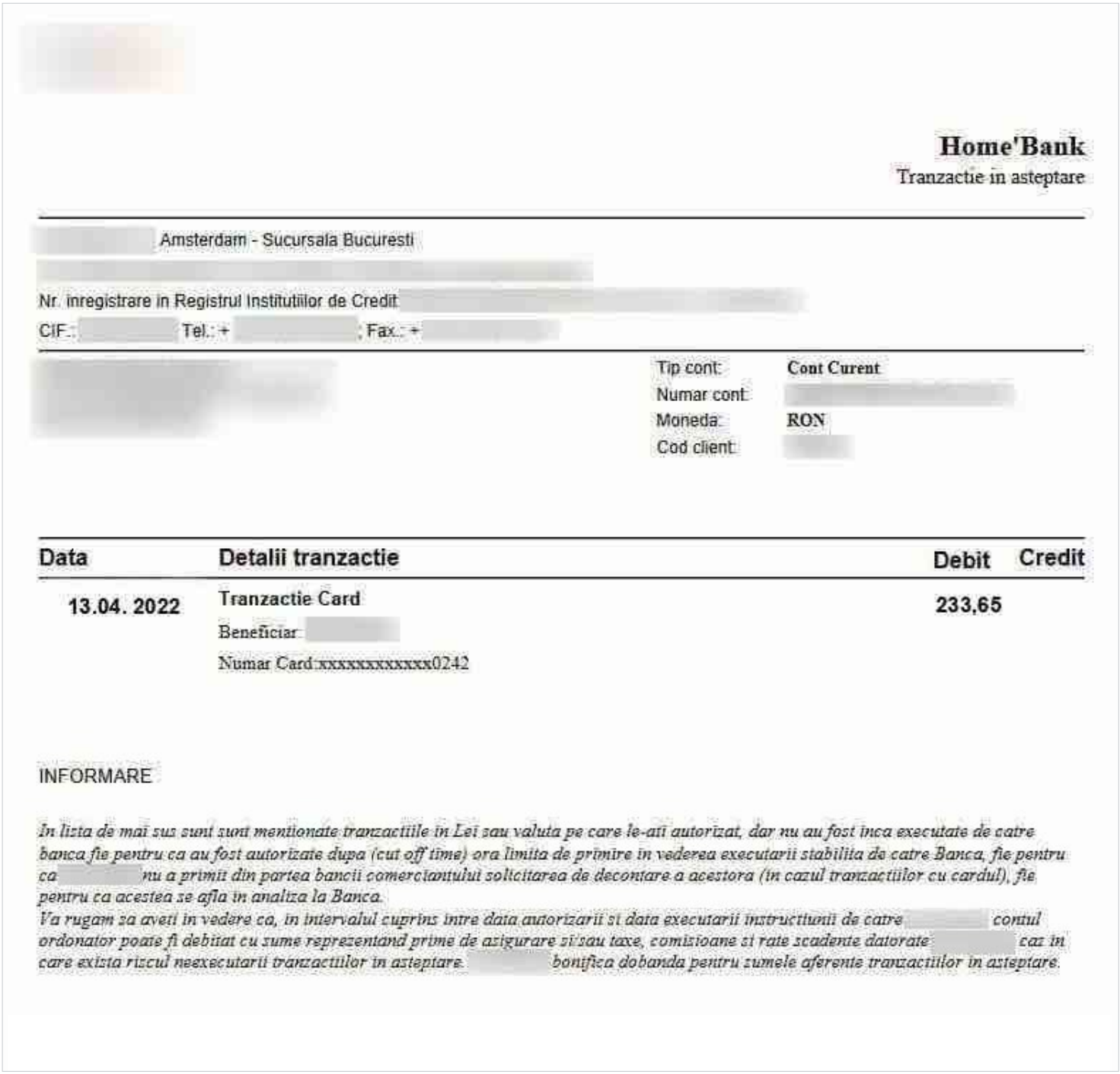


Рис. 21. Пример подтверждения получения товара мошенником

4.0 — покупатель создает видимость, что оплатил товар, и присылает поддельный чек. Продавцу приходит СМС, которое мимикрирует под зачисление из банка.

Через несколько минут покупатель пишет, что ему больше подойдет товар другого продавца, и просит вернуть деньги. Часто в ход идет аргумент «верните, вы же не мошенник». Продавец отправляет покупателю сумму, но из своего кармана, ведь никакого платежа не было.



Home'Bank
Tranzactie in asteptare

Amsterdam - Sucursala Bucuresti

Nr. inregistrare in Registrul Institutiilor de Credit

CIF.: Tel.: + ; Fax.: +

Tip cont:	Cont Curent
Numar cont:	
Moneda:	RON
Cod client:	

Data	Detalii tranzactie	Debit	Credit
13.04. 2022	Tranzactie Card Beneficiar: Numar Card:xxxxxxxxxxxx0242	233,65	

INFORMARE

In lista de mai sus sunt sunt mentionate tranzactiile in Lei sau valuta pe care le-ati autorizat, dar nu au fost inca executate de catre banca fie pentru ca au fost autorizate dupa (cut off time) ora limita de primire in vederea executarii stabilita de catre Banca, fie pentru ca nu a primit din partea bancii comerciantului solicitarea de decontare a acestora (in cazul tranzactiilor cu cardul), fie pentru ca acestea se afla in analiza la Banca.
Va rugam sa aveti in vedere ca, in intervalul cuprins intre data autorizarii si data executarii instructiunii de catre contul ordonator poate fi debitat cu sume reprezentand prime de asigurare si/sau taxe, comisioane si rate scadente datorate caz in care exista riscul neexecutarii tranzactiilor in asteptare. bonifica dobanda pentru sumele aferente tranzactiilor in asteptare.

Рис. 22. Пример поддельного чека об оплате

Вступление в скам-группу и создание фишинговой страницы с помощью Telegram-ботов

Вступление в скам-группу

Чтобы приступить к генерации фишинговых ссылок в Telegram-боте скам-группы, сначала необходимо пройти собеседование у администрации (рис. 23). Для этого необходимо просто запустить бота или в некоторых случаях нажать предложенную кнопку после запуска.

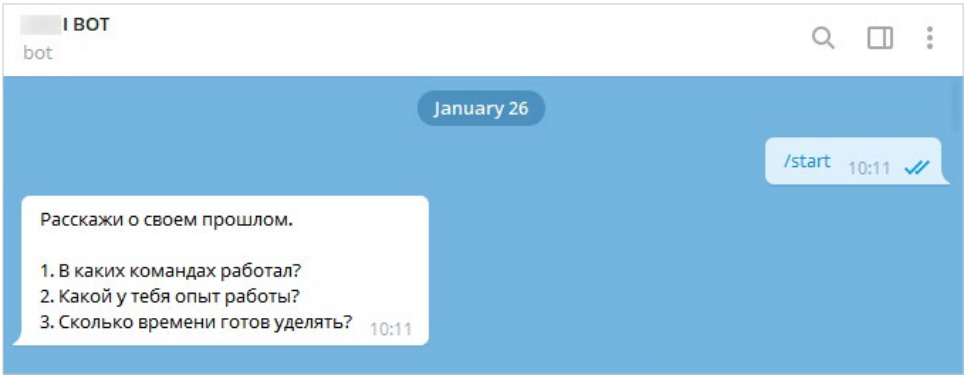


Рис. 23. Пример вопросов, которые запрашивают перед вступлением в скам-группу

Потенциальному участнику предлагается ответить на вопросы, которые помогут администраторам оценить его опыт работы по данной мошеннической схеме (рис. 24).

Чаще всего кандидата просят перечислить:

- **скам-группы**, на которых ранее работал или продолжает работать;
- **онлайн-площадки**, с которыми уже есть опыт скама;
- **время**, которое участник планирует уделять скаму.

Также нередко запрашивают **скриншот выплат** и **ID аккаунта** воркера, который пригласил в проект.

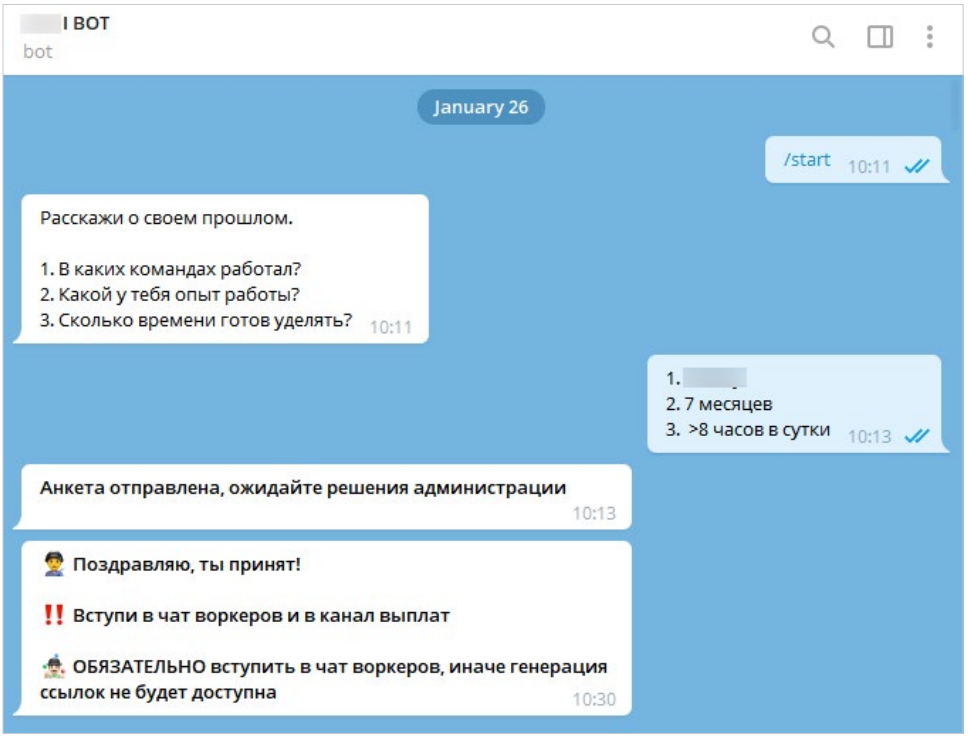


Рис. 24. Пример успешного принятия в скам-группу

Создание фишинговой ссылки

Для создания фишинговой ссылки существует специальный раздел в Telegram-ботах, который доступен в главном меню (рис. 25). Называться может по разному: «бренды», «генерация», «создать ссылку / создать трек-номер» (в зависимости от типа площадки) и т. д.

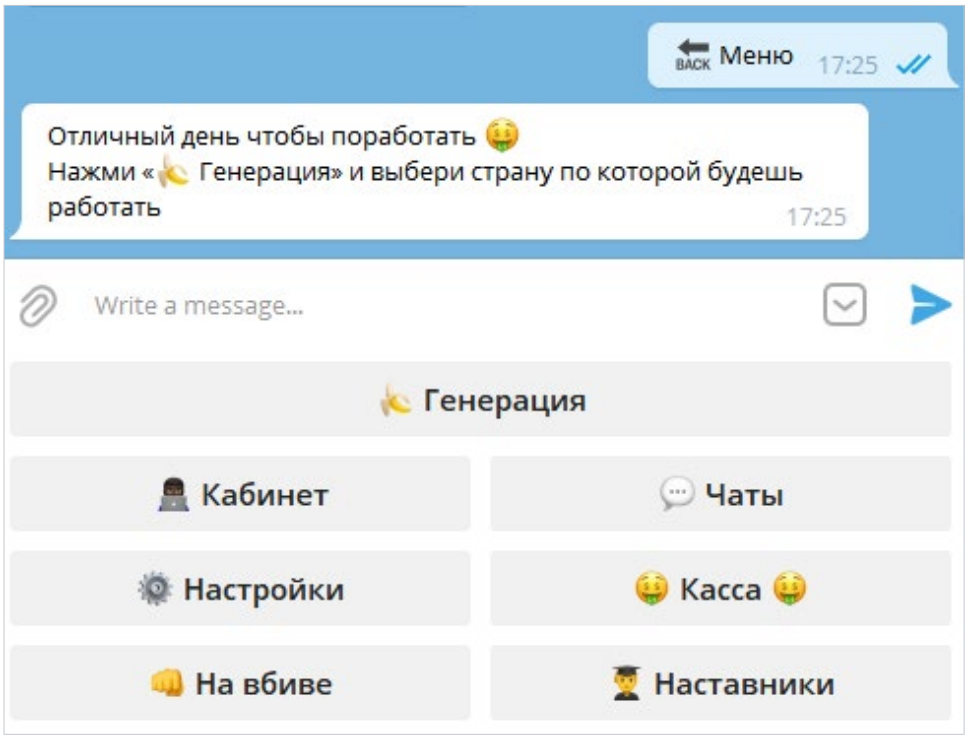


Рис. 25. Пример меню бота

Далее воркеру необходимо выбрать страну/бренд, под чей шаблон он хочет сгенерировать фишинговую ссылку (рис. 26).

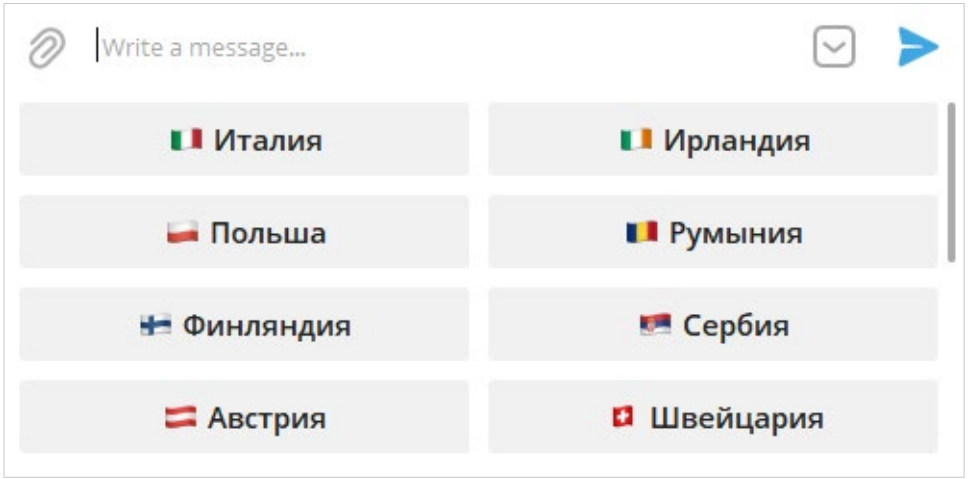


Рис. 26. Выбор страны

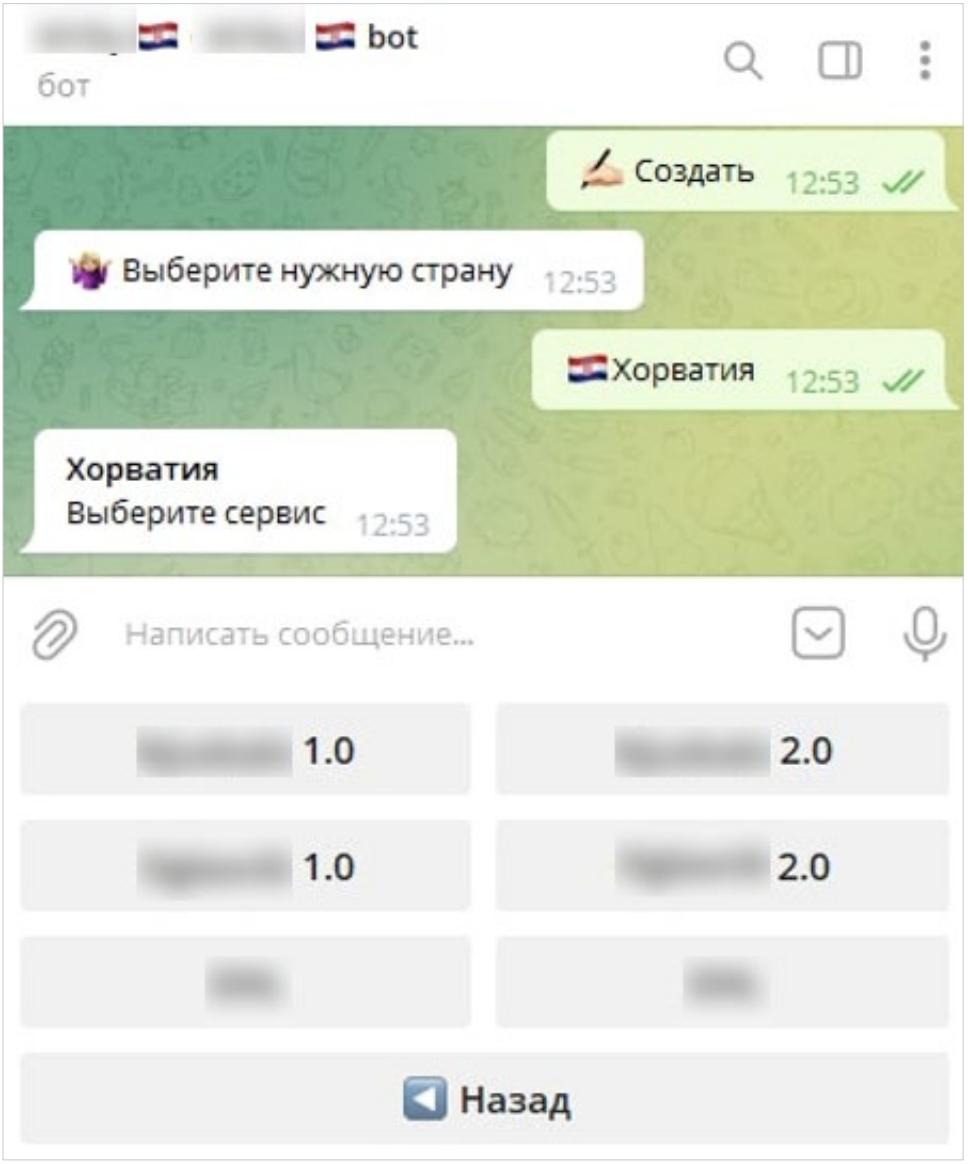


Рис. 27. Версии схемы Classiscam

При выборе площадки в некоторых ботах могут заранее проинформировать, по какой из версий схемы Classiscam (рис. 27) будет сгенерирована фишинговая ссылка. В остальных случаях версию можно выбрать после ввода параметров для генерации.

После того как был выбран атакуемый бренд, необходимо заполнить ключевые параметры, на основе которых будет сгенерирована фишинговая страница (рис. 28). Обычно это следующая информация:

- → Название товара/услуги.
- → Цена.
- → Фотография товара/услуги.
- → Имя получателя.
- → Мобильный номер получателя.
- → Адрес получателя.

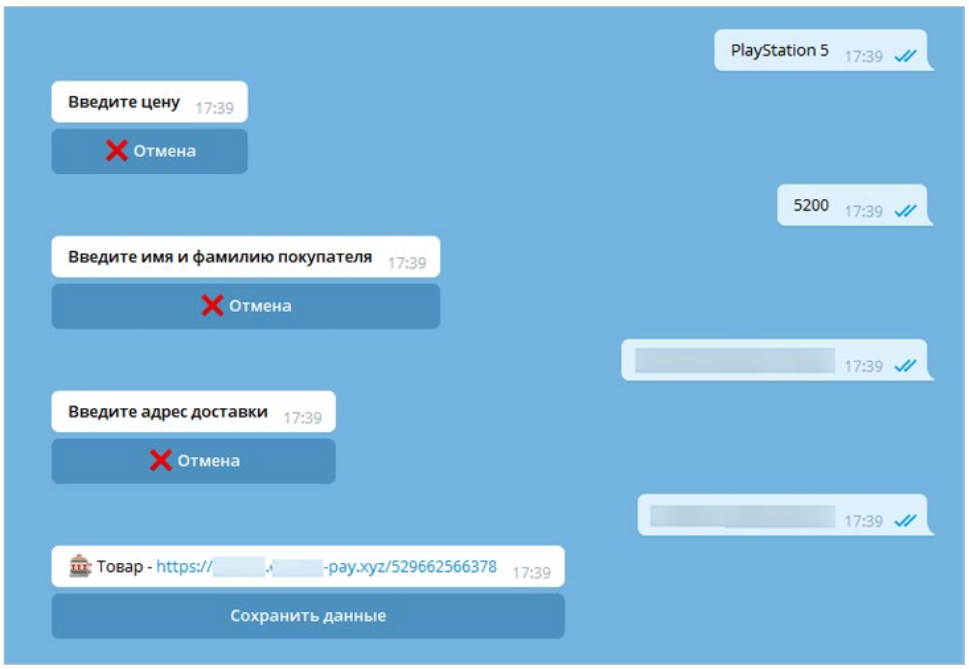


Рис. 28. Выбор ключевых параметров для фишинговой ссылки

Если воркер планирует создать фишинговую страницу транспортной компании, то дополнительно надо ввести имя и город отправителя, дату отправки/доставки посылки, а также ее вес (рис. 29).

В некоторых случаях достаточно только ввести ссылку на товар с официального ресурса, и на ее основе будет сгенерирована фишинговая ссылка с дублирующей информацией.

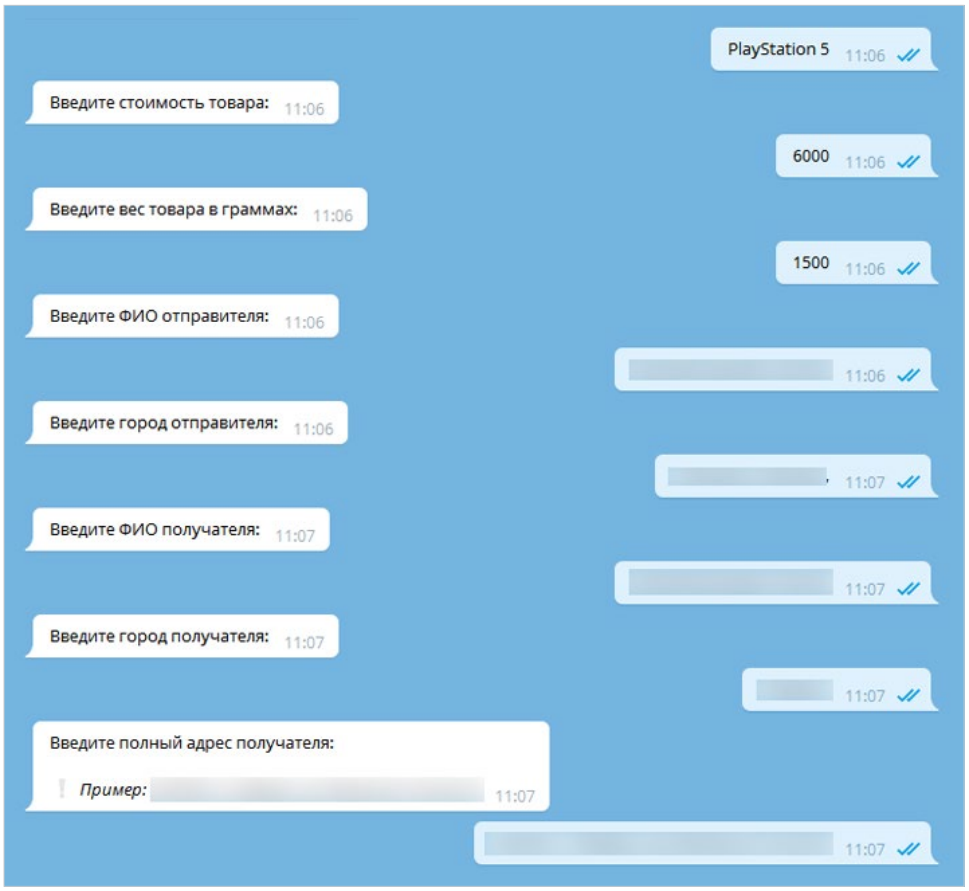


Рис. 29. Выбор ключевых параметров для фишинговой ссылки

После того как все вышеперечисленные данные будут введены воркером, бот может запросить возможность включить функцию проверки баланса жертвы (рис. 30). Если эта функция включена, на фишинговую страницу дополнительно будет добавлена форма ввода баланса банковской карты. Это делается для того, чтобы в дальнейшем списать весь денежный баланс с карты.

Далее Telegram-бот генерирует саму фишинговую ссылку, их может быть несколько, в зависимости от версии мошеннической схемы. В некоторых ботах генерируются ссылки сразу на несколько брендов.

Как будет выглядеть сгенерированная фишинговая страница, изображено на рис. 31.

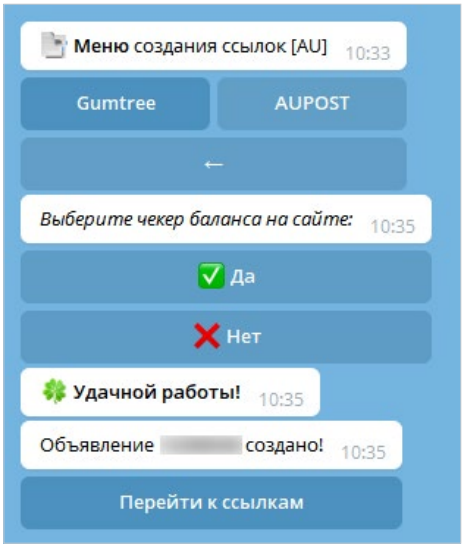


Рис. 30. Пример создания фишинговой ссылки

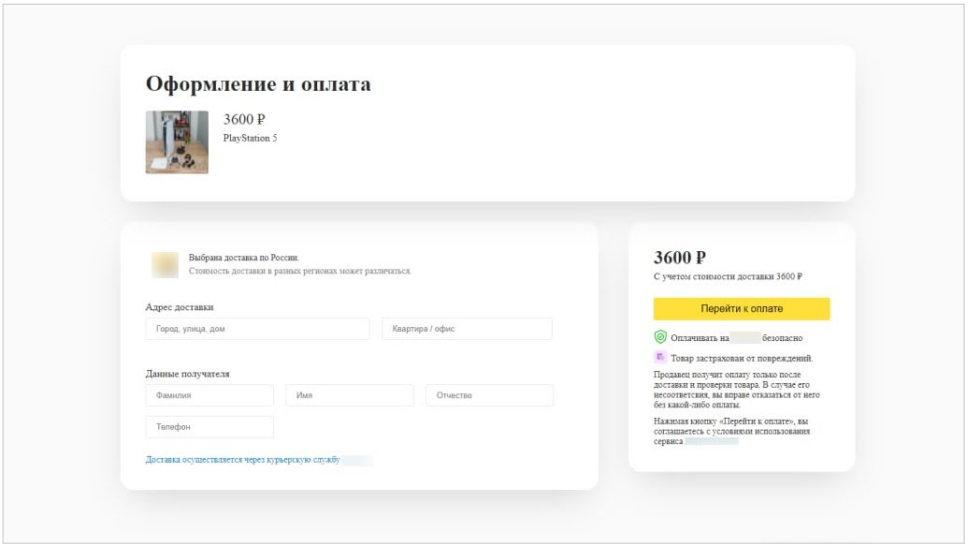


Рис. 31. Фишинговая страница

Переход на «партнерки»

После 2019 года ТС стал лишь менеджером среднего звена, над которым стояли настоящие организаторы, разработчики, админы. Некоторым из ТС позволяли регистрировать домены под фишинг. Другие же только следили за выплатами и деятельностью воркеров.

Роль ТС сильно снизилась, и они перестали быть отдельными организаторами, а стали ячейкой более крупных организаций.

Это привело к изменению организационной структуры сообщества и переходу схемы на партнерскую модель (рис. 32).

Рис. 32. Пример рекламы продажи партнерской программы

«Партнерка» представляет собой кооперацию организатора партнерской программы со знакомыми ему ТС, которые, в свою очередь, создавали свои команды с темами на форумах под арендованный Telegram-бот со фишинговыми доменами. При этом сервер со скриптом для генерации фишинговых страниц был общим для ТС и их команд, состоявших в «партнерке».

Новые ТС — это уже опытные воркеры с с большим доходом (т.н. профитом). Новый ТС должен хорошо представлять себе работу схемы, уметь привлекать воркеров и проводить обучение для новичков. Доля ТС в схеме небольшая. Около 80% от профитов он отдает воркерам, 10–15% платит организатору «партнерки», однако доход получает с каждого успешного хищения участниками его команды.

Состав участников партнерских программ нигде не фиксировался, но общая инфраструктура доменов и серверов, а также сообщения на тематических форумах указывают на формирование подобных организаций. Участники «партнерок» на теневых форумах активно комментируют профили друг друга и дают характеристику «порядочности» и «надежности».

Роли воркеров

Роль самой массовой группы участников — воркеров — не изменилась в процессе развития схемы.

Это рядовые сотрудники, которые общаются с потенциальной жертвой и пытаются убедить ее перейти по нужной ссылке и оставить свои данные.

У воркеров может быть разная специализация в зависимости от выполняемых задач:

- **прозвонщики** — это люди, которые разговаривают с жертвой по телефону, выдавая себя за службу поддержки, и просто помогают мошенникам, играя любую роль в соответствии с задействованной схемой;
- **возвратеры** — выдают себя за техническую поддержку сайта, общаются с жертвой через окно чата, которое обычно отображается внизу фишинговой страницы, или через специальную почту. Их роль заключается в помощи жертвам с фиктивным возвратом списанных денежных средств. В действительности вместо возврата происходит повторное списание с карты жертвы;
- **вбиверы** — это еще одна группа участников, которая занимается списанием средств средств с карты жертвы вручную, когда жертва испытывает трудности в самостоятельном проведении платежа мошенникам;
- **бомберы** — осуществляют массовую спам-атаку через СМС и звонки на номер жертвы. К подобной практике злоумышленники прибегают нечасто, и делается это для запугивания или мести за неудавшуюся попытку скама.

Выход на международный рынок

Долгое время мошенники атаковали исключительно бренды, работающие на территории СНГ. Так как мошенническая схема не нова, атака на русскоязычные ресурсы становится сложнее и опаснее. Бренды проводят рекламные кампании по информированию своих пользователей о мошенничестве и защищают свой бренд, активно удаляя фишинговые ресурсы.

В середине февраля 2020 года на теневых форумах начала появляться реклама Telegram-ботов со свободным доступом к использованию, где можно было генерировать фишинговые формы под украинскую версию сайта бесплатных объявлений OLX (рис. 33–35).

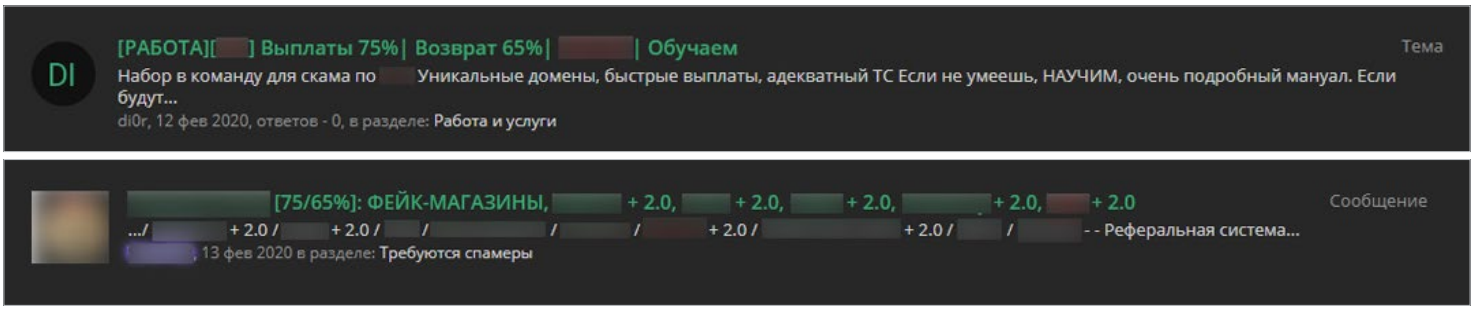


Рис. 33. Реклама скам-групп на теневых форумах

Рис. 34. Реклама скам-группы

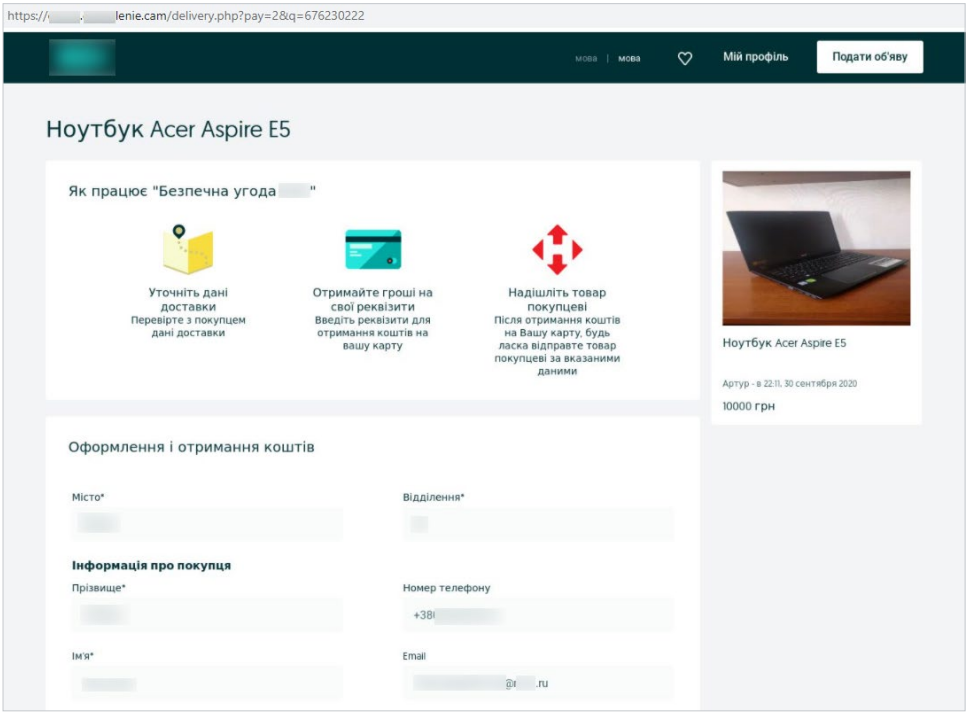


Рис. 35. Пример фишингового ресурса, использующего бренд OLX (Украина)

В апреле начали появляться предложения о новом виде скама — Kufar, белорусском сайте бесплатных объявлений (рис. 37).

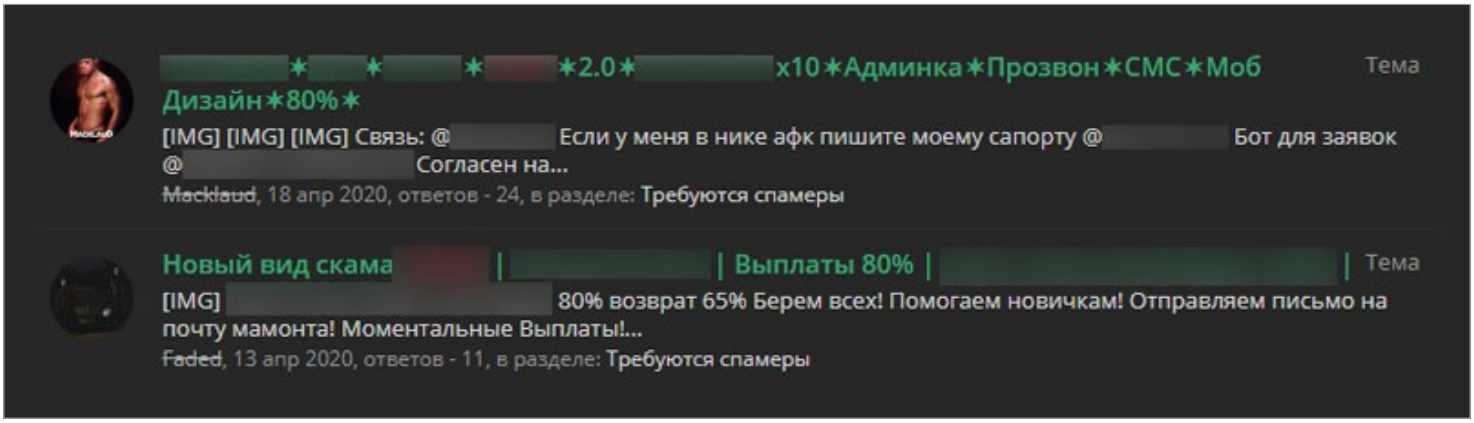


Рис. 36. Реклама скам-групп, в которых атакую пльзователей белорусского сайта бесплатных объявлений

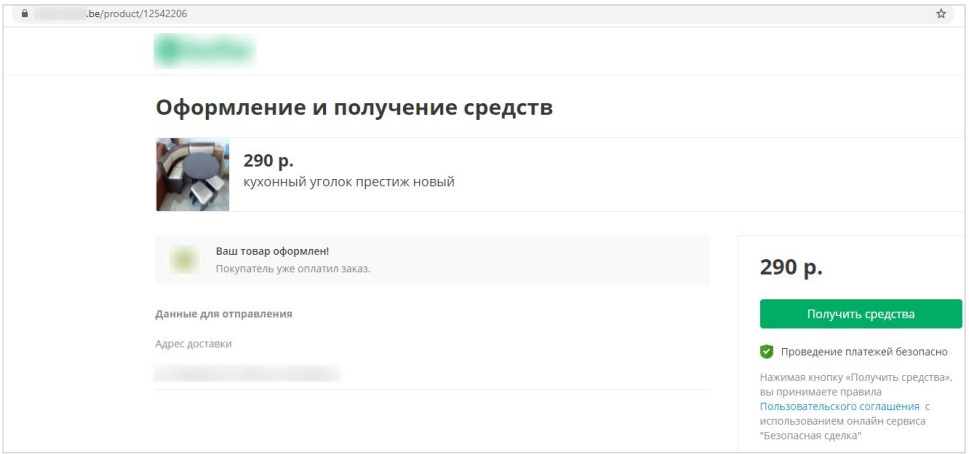


Рис. 37. Пример фишингового ресурса, использующего бренд Kufar

Белорусские транспортные компании также не обошли стороной. В скором времени добавились бренды CDEK в Беларуси (рис. 38) и Белпочта (рис. 39).

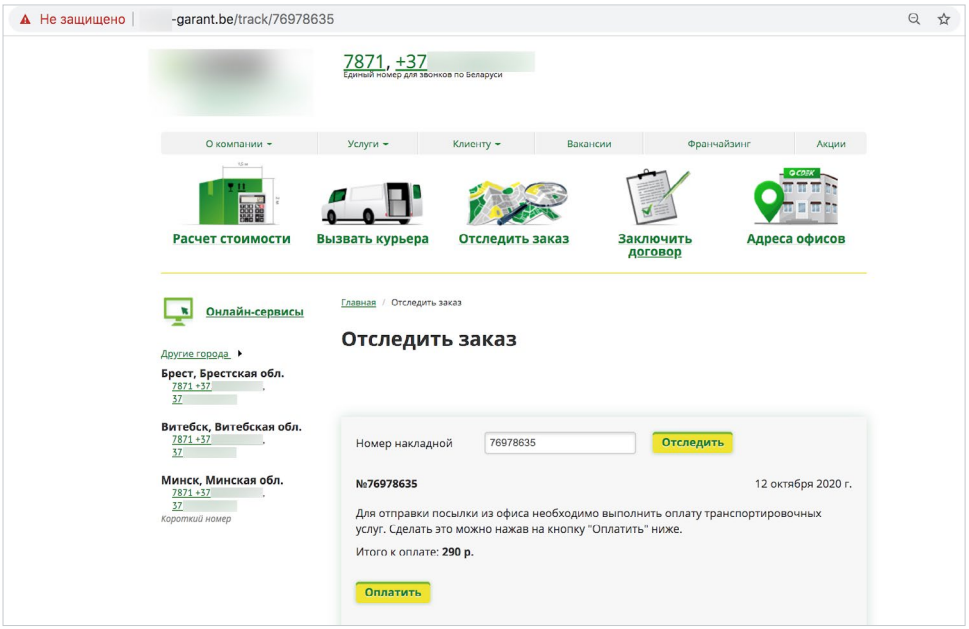


Рис. 38. Пример фишингового ресурса, использующего бренд CDEK (Беларусь)

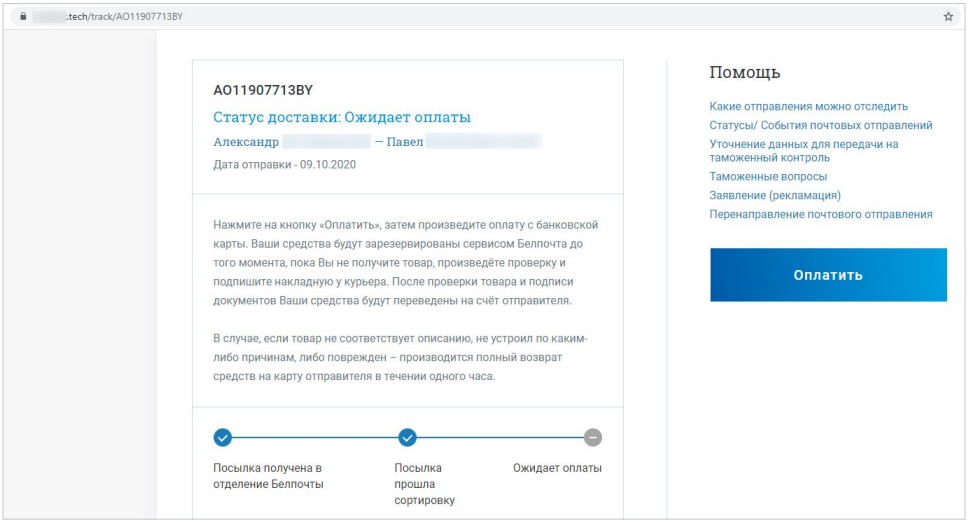


Рис. 39. Пример фишингового ресурса, использующего бренд Белпочта

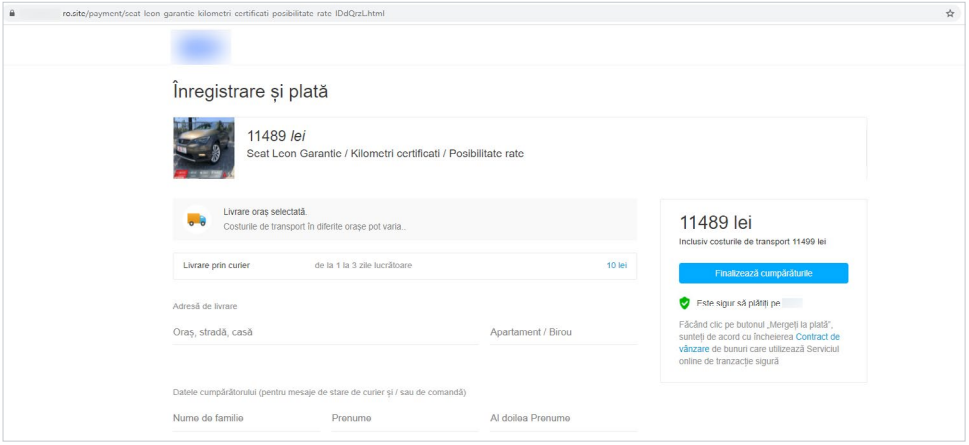


Рис. 40. Пример фишингового ресурса, использующего бренд OLX на румынском языке

Уже в начале августа на открытых Telegram-ботах появился скам болгарской (рис. 41) и казахской версии OLX (рис. 42).

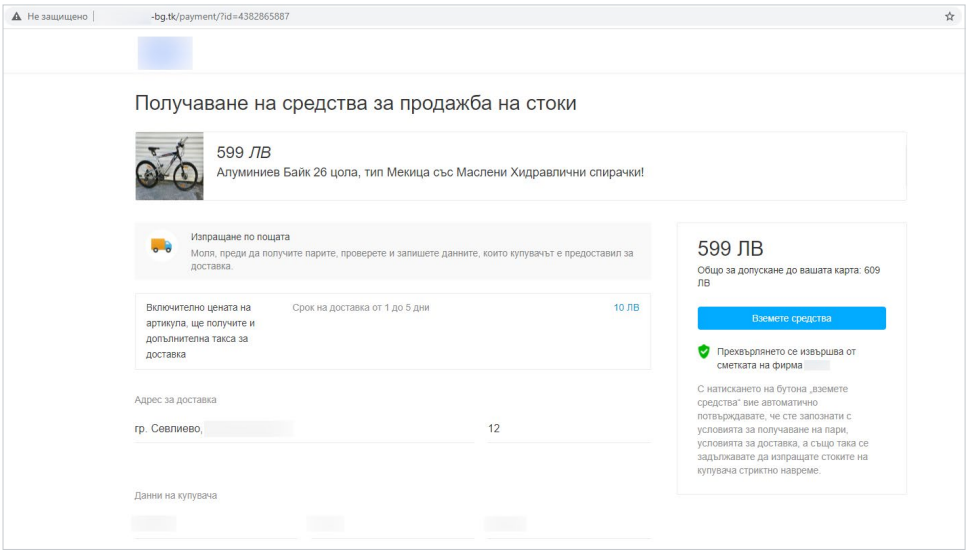


Рис. 41. Пример фишингового ресурса, использующего бренд OLX на болгарском языке

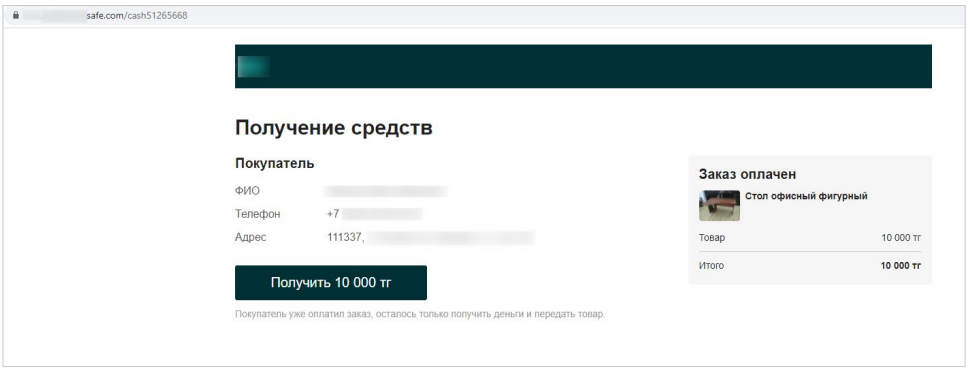


Рис. 42. Пример фишингового ресурса, использующего бренд OLX с казахской валютой

Скамеры не остановились на отработке схемы в странах СНГ. Так, в конце августа в популярных Telegram-ботах появился скам французского сайта бесплатных объявлений Leboncoin (рис. 43).

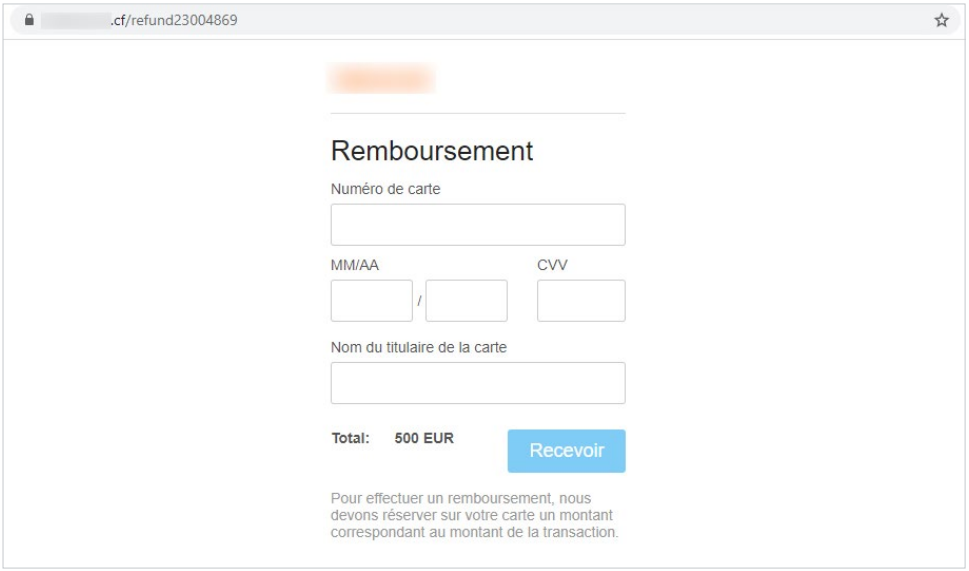


Рис. 43. Пример фишингового ресурса, использующего бренд Leboncoin

До 2020 года атаки на зарубежные бренды уже осуществлялись, но это были единичные случаи. Программное обеспечение для генерации фишинговых страниц было доступно в закрытых сообществах для скамеров с опытом работы. Развитие схемы Classiscam и масштабирование сообщества ускорило распространение схемы в мировом масштабе.

Стоит отметить, что скам европейских брендов более сложный с технической точки зрения. Мошенники сталкиваются с трудностями при верификации аккаунтов на сайтах, что вынуждает их покупать краденые личные документы, а также телефонные номера через теневые форумы и сообщества.

Для ТС появляется проблема с привязкой валютных кредитных карт к Telegram-ботам. Решается это привлечением опытных дропов (подставные лица для приема банковских переводов, получающие с них долю).

Под каждый бренд мошенниками-энтузиастами пишутся инструкции по скаму, помогающие новичкам авторизоваться на зарубежных площадках и вести диалог с жертвой.

Объемы атак

За все время исследования мошеннической схемы было обнаружено **384** Telegram-бота. На данный момент около 90 продолжают активно функционировать. Количество активных интернет-ботов постоянно меняется. В любой момент бот может прекратить свою работу по той или иной причине, и вся команда может быть распущена или перекочует на другой бот.

Сейчас Classiscam распространен в **64** странах в Европе, СНГ и на Ближнем Востоке. В схеме используется **169** брендов различных сервисов: досок объявлений, сервисов доставок, сервисов по продаже товаров и предоставлению услуг, банков, а также других локальных площадок, например, кинотеатров.

Заработок за последний оцениваемый период с апреля 2020 года по февраль 2022-го составил по самым минимальным оценкам не менее **$29 500 000.** Средняя сумма хищений — около **$83.**

Всего было найдено более 2000 тем, связанных с поиском воркеров для фишинговых партнерских программ на более чем 60 специализированных форумах.

Создаваемые мошенниками страницы довольно сложно обнаружить проактивно, так как время их существования очень ограничено, зачастую это несколько часов.

Распределение доходов от мошеннической схемы Classiscam по валютам списания позволяет сделать вывод о том, что чаще всего жертвами становятся граждане России (см. диаграмму на рис. 44).

Рис. 44. Диаграмма распределения сумм денежных средств в валюте списания

Рост предложений абузоустойчивого хостинга

Стоит отметить, что потребность групп в абузоустойчивых хостингах породила массу соответствующих предложений. Если до 2020 года в этой нише было преимущественно несколько крупных компаний, то буквально за год их стало значительно больше. Они не отличаются высоким качеством предоставления услуг: простое оформление диапазонов IP-адресов на собственные реквизиты для перехвата жалоб. Но они есть и затрудняют противодействие мошеннической активности. В конечном счете это сказывается как на киберпреступности в целом, так и на информационной безопасности.

SaaS как модель развития схемы

Учитывая иерархическое распределение ролей, переиспользование готовых шаблонов, методик, а также масштабирование за счет низкого порога входа для новых участников, можно сказать, что схема Classiscam работает по принципу SaaS (англ. scam as a service — «программное обеспечение как услуга»). В данном случае программным обеспечением является инструментарий по созданию ссылок, а пользователями выступают рядовые исполнители, которые создают ссылки и непосредственно контактируют с жертвой. Прибыль делится пропорционально между всеми участниками группы в зависимости от их роли (рис. 45–46).

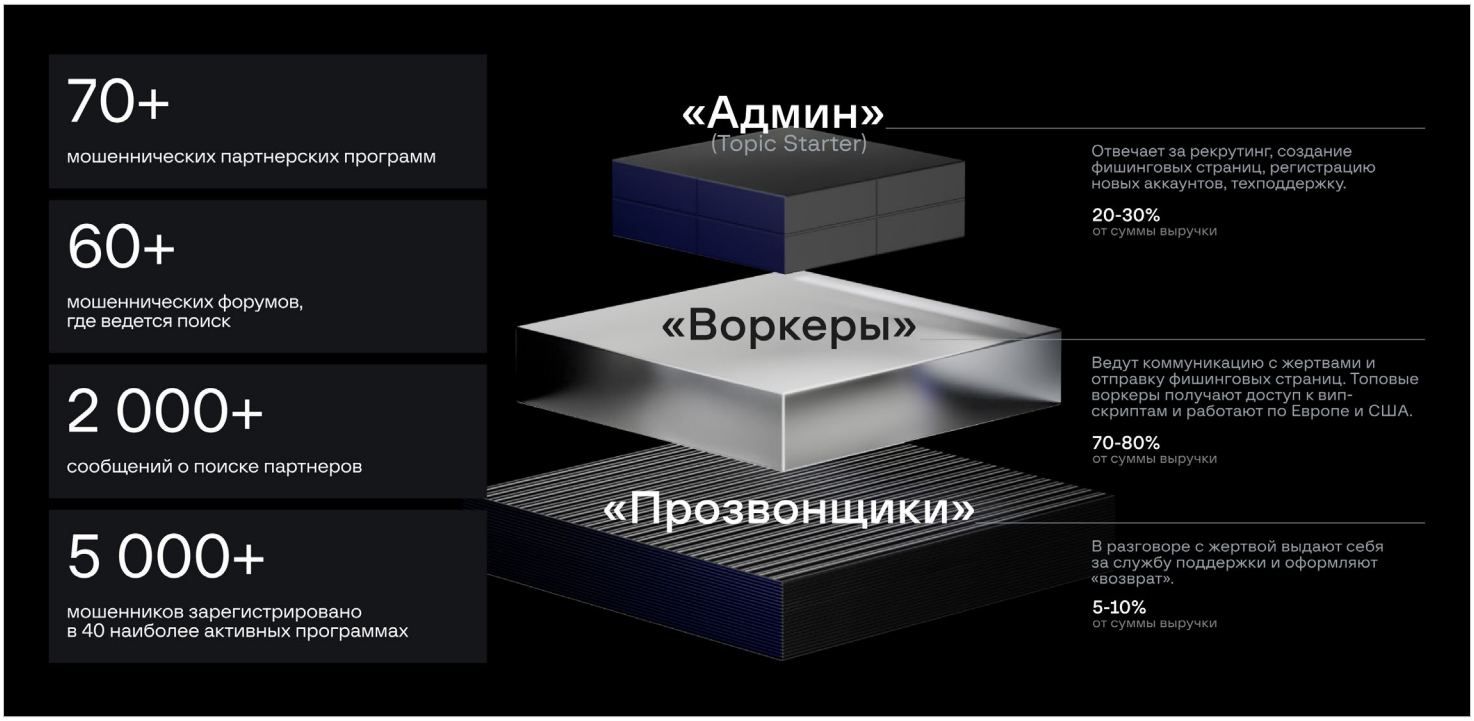


Рис. 45. Схема иерархии преступных групп

Также в чатах воркерам предоставляется помощь для обмана:

- смена домена на собственный;
- отправка писем и СМС от выбранных сервисов;
- генератор фейковых скриншотов поддержки;
- мануалы с алгоритмами действий мошенников (бывают платные);
- магазин с продажей баз для рассылок, аккаунтов, номеров и других разнообразных услуг.

Скриншоты создания ссылок, выбора доменов, мануалов

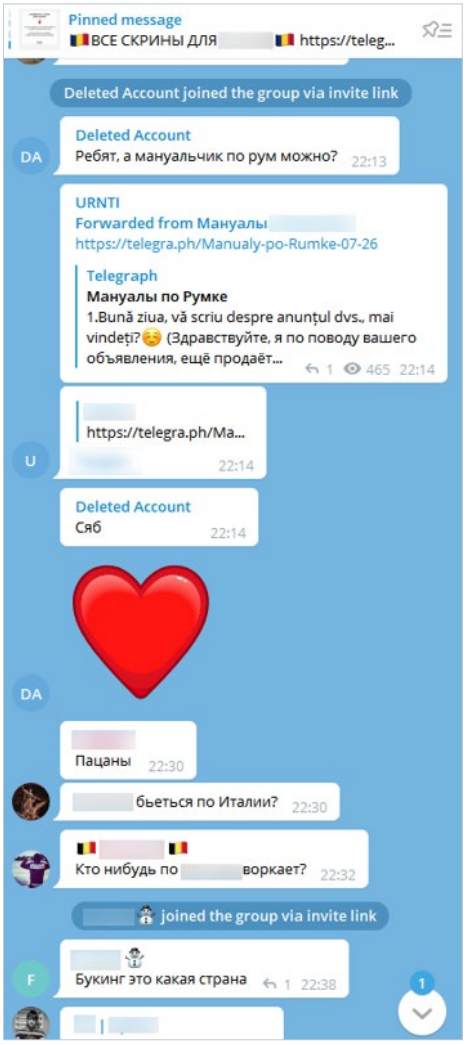


Рис. 46. Пример рассылки мануала в скам-группе по атаке на румынские онлайн-сервисы

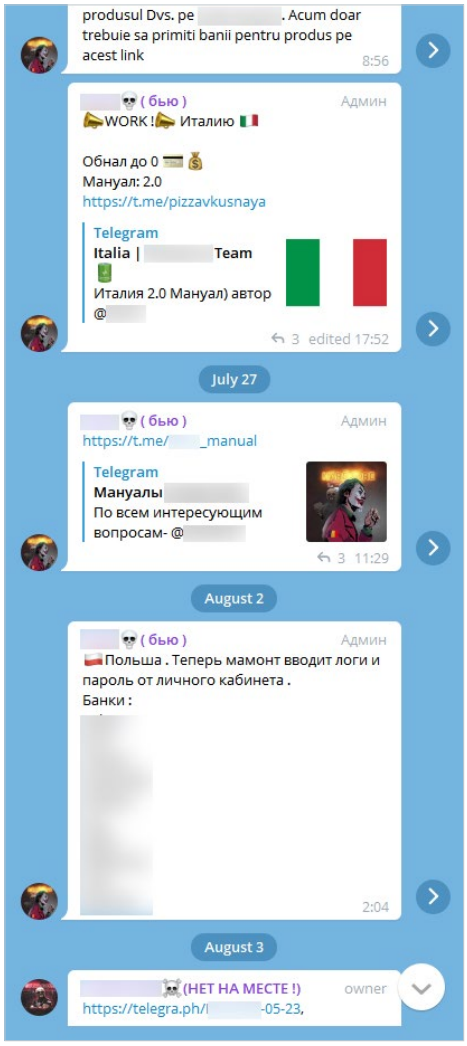


Рис. 47. Пример рассылки мануала в скам-группе по атаке на итальянские онлайн-сервисы

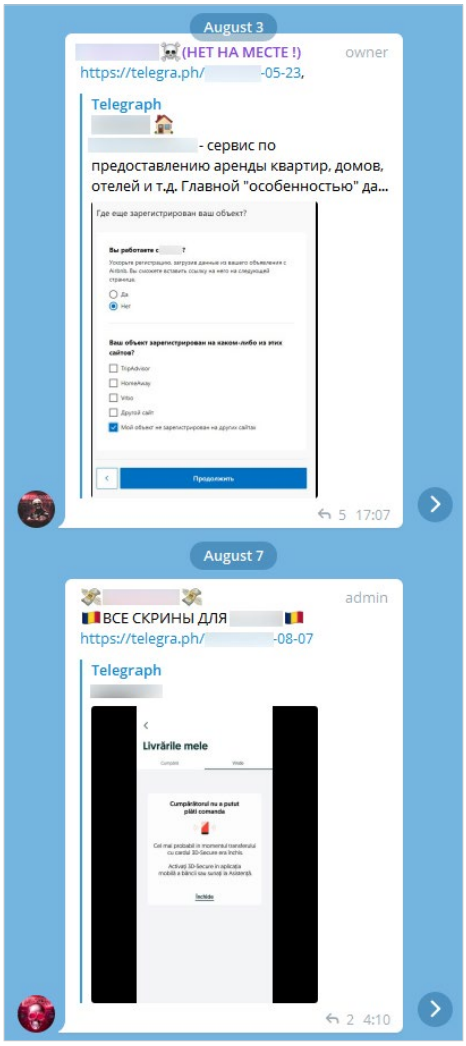


Рис. 48. Пример рассылки в скам-группе поддельных материалов для атак на румынских онлайн-сервисах

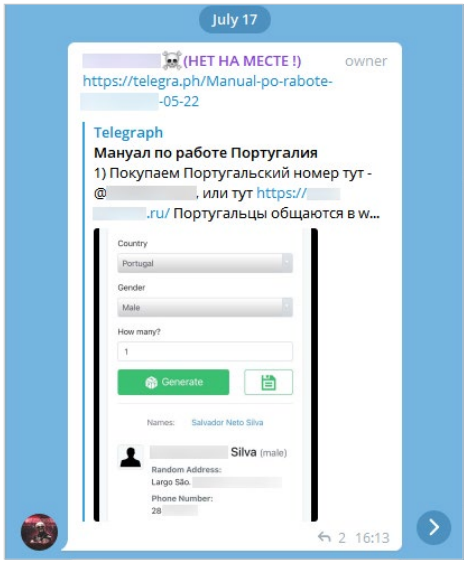


Рис. 49. Пример рассылки мануала в скам-группе по атаке на португальские онлайн-сервисы

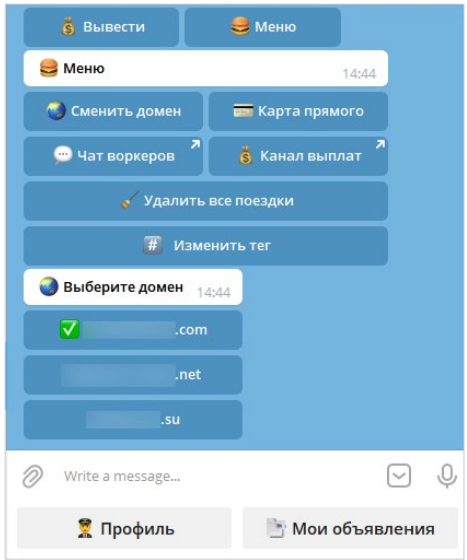


Рис. 50. Пример выбора доменов, на которых будет генерироваться фишинговая ссылка

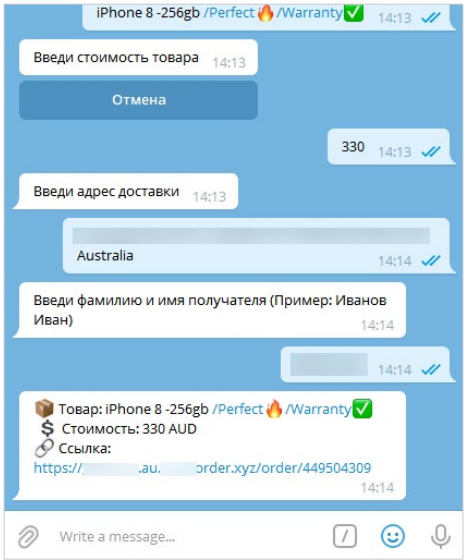


Рис. 51. Пример создания фишинговой ссылки

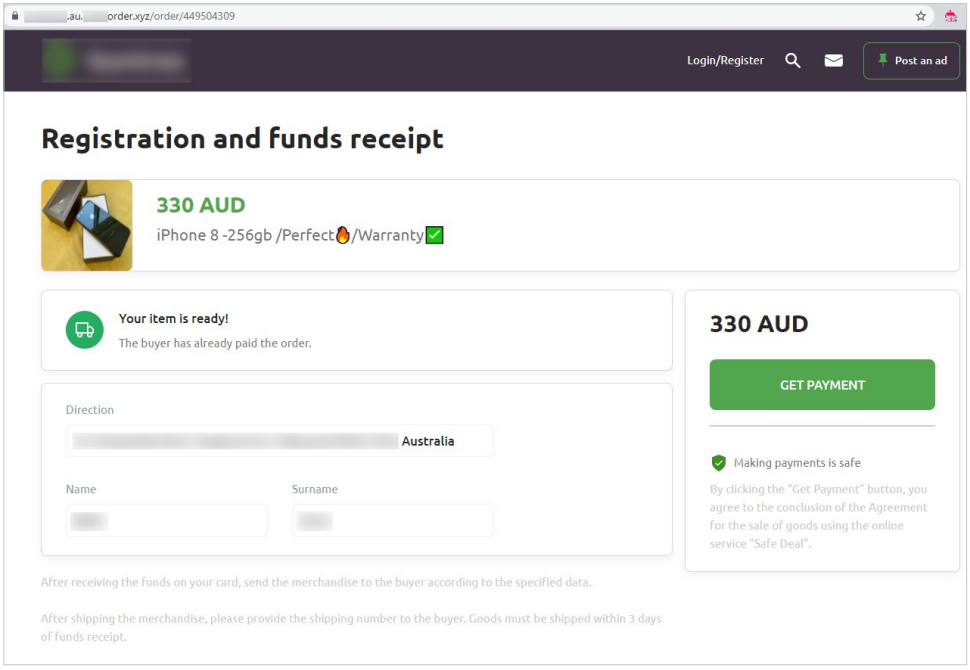


Рис. 53. Пример фишинговой страницы

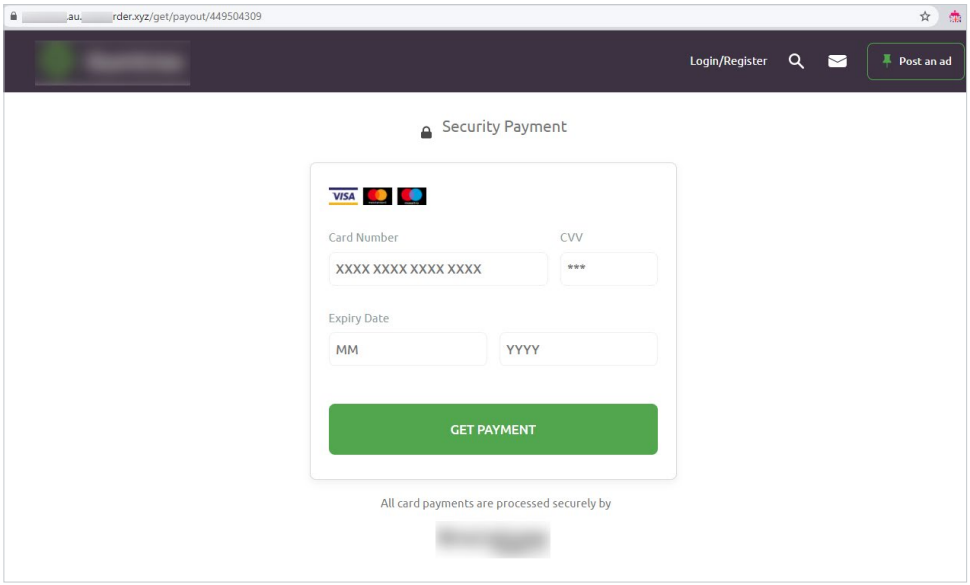


Рис. 54. Пример фишинговой формы

Новая роль админпанелей

С развитием схемы и увеличением ее масштабов мошенники стали использовать все больше брендов и стран. Уже стало сложно все это вмещать и хранить в Telegram-боте. Во второй половине 2021 года были выявлены предложения по продаже полноценных комплектов инструментов для скама, где покупатель может единолично выполнять все необходимые ему операции, обходиться без команды и становиться одновременно ТС, воркером, вбивером и возвратером в одном лице.

Для опытных скамеров это очень выгодное и удобное предложение, в отличие от работы в Telegram-боте. Мошенник просто разворачивает админпанель на своем сервере с инструментами скама и тем самым оперативно получает к ним доступ.

Основные выводы

Данная схема существует уже достаточно давно и успела сильно усовершенствоваться. Переход с админпанелей в Telegram-боты позволил облегчить коммуникацию среди мошенников и упростить создание фишинговых страниц. Успешные атаки популярных русскоязычных сервисов дали толчок к увеличению атакованных брендов, начиная от менее популярных русскоязычных и заканчивая зарубежными.

Всего было обнаружено более **384** групп, участвующих в схеме, а атака распространена в **64** странах в в Европе, СНГ, на Ближнем Востоке и в других регионах с использованием **169** брендов.

После внимательного изучения данных скам-групп стало очевидно, что их гораздо меньше, потому что преступные группировки не являются выделенными образованиями, как это принято в классической киберпреступности. Например, воркеры могут участвовать сразу в нескольких группировках.

На самом деле влияние в данной сфере принадлежит очень ограниченному кругу людей, объединенных в небольшие группы. И тут ТС стали не руководителями проекта, а просто наемными работниками, получающими процент от прибыли, в некоторых случаях — оклад с процентом. В рамках данного исследования такие скам-проекты мы назвали «партнерками».

Изменение иерархии сильно повлияло на сам подход к работе с подобными группами и понимание их возможностей, отразилось на методах противодействия этим группам и слежения за ними. Тогда и возникла сама мысль о том, что Intelligence-подход может дать гораздо более весомый результат, чем классическая блокировка конечных сайтов.

Так, например, у скам-групп были обнаружены целые диапазоны IP, собственные NS-серверы и собственные способы вывода денежных средств.

Все это позволило видеть все изменения в работе схемы и ее групп, а также купировать проблемы в самом начале их возникновения, наносить болезненные удары по всем векторам — от самих ботов до средств вывода денег.

На основании данной информации стало возможным наносить непоправимый урон этим группам, привлекая к уголовной ответственности настоящих руководителей группировок.

В начале развития групп в Telegram партнерки использовали неизменную инфраструктуру: одни и те же домены, выделенные серверы, платежные шлюзы, фиш-киты — это упрощало процесс объединения групп в партнерские программы.

Со временем SaaS поднялся совершенно на другой уровень. Теперь на вершине «пищевой цепи» были даже не руководители супергрупп (люди, владевшие несколькими группами), а те, кто оказывал подобные услуги для самих владельцев групп.

В результате любой человек мог прийти и зарегистрировать своего бота для мошенничества. За него решались все проблемы технического характера вплоть до вывода денег. Задачей руководителя стало лишь привлечение воркеров и распределение денег.

Для помощи в противодействии мошенничеству специалисты Group-IB представляют рекомендации по поиску и атрибуции.

Миссия Group-IB – борьба с киберпреступностью

Group-IB — один из ведущих мировых разработчиков решений для обнаружения и предотвращения кибератак, выявления мошенничества и защиты интеллектуальной собственности в сети.

19 лет практического опыта

1 300+ успешных расследований по всему миру

70 000+ часов реагирования

600+ специалистов и разработчиков

Партнер и участник совместных исследований

Интерпол

Европол

Решения Group-IB признаны мировыми агентствами

Forrester®

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN

Технологии и инновации

Кибербезопасность

- Threat Intelligence
- Управление поверхностью атаки
- Защита электронной почты
- Анализ сетевого трафика
- Детонация ВПО
- Защита конечных станций (EDR)
- XDR

Противодействие мошенничеству

- Противодействие мошенничеству client-side
- Адаптивная аутентификация
- Защита от ботов
- Выявление платежного мошенничества
- Поведенческий анализ

Защита бренда

- Антифишинг
- Антипиратство
- Антимошенничество
- Антиконтрафакт
- Выявление утечек данных
- Защита VIP-персон

Портфолио услуг

Аудит и консалтинг	• Анализ защищенности • Тестирование на проникновение • Red Teaming • Оценка соответствия и консалтинг	• Выявление следов компрометации • Проверка готовности к реагированию на инциденты
Обучающие программы	• Для технических специалистов • Для широкой аудитории	• Мастер-классы для детей
Реагирование на инциденты и цифровая криминалистика	• Реагирование на инциденты • Реагирование на инциденты по подписке	• Цифровая криминалистика • eDiscovery
Managed Services	• Managed Detection • Managed Threat Hunting	• Managed Response
Исследование высокотехнологичных преступлений	• Исследование киберпреступлений	

GROUP-IB

Предотвращаем и исследуем киберпреступления с 2003 года

БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ

GROUP-IB.RU
GROUP-IB.RU/BLOG
+7 495 984 33 64
INFO@GROUP-IB.COM