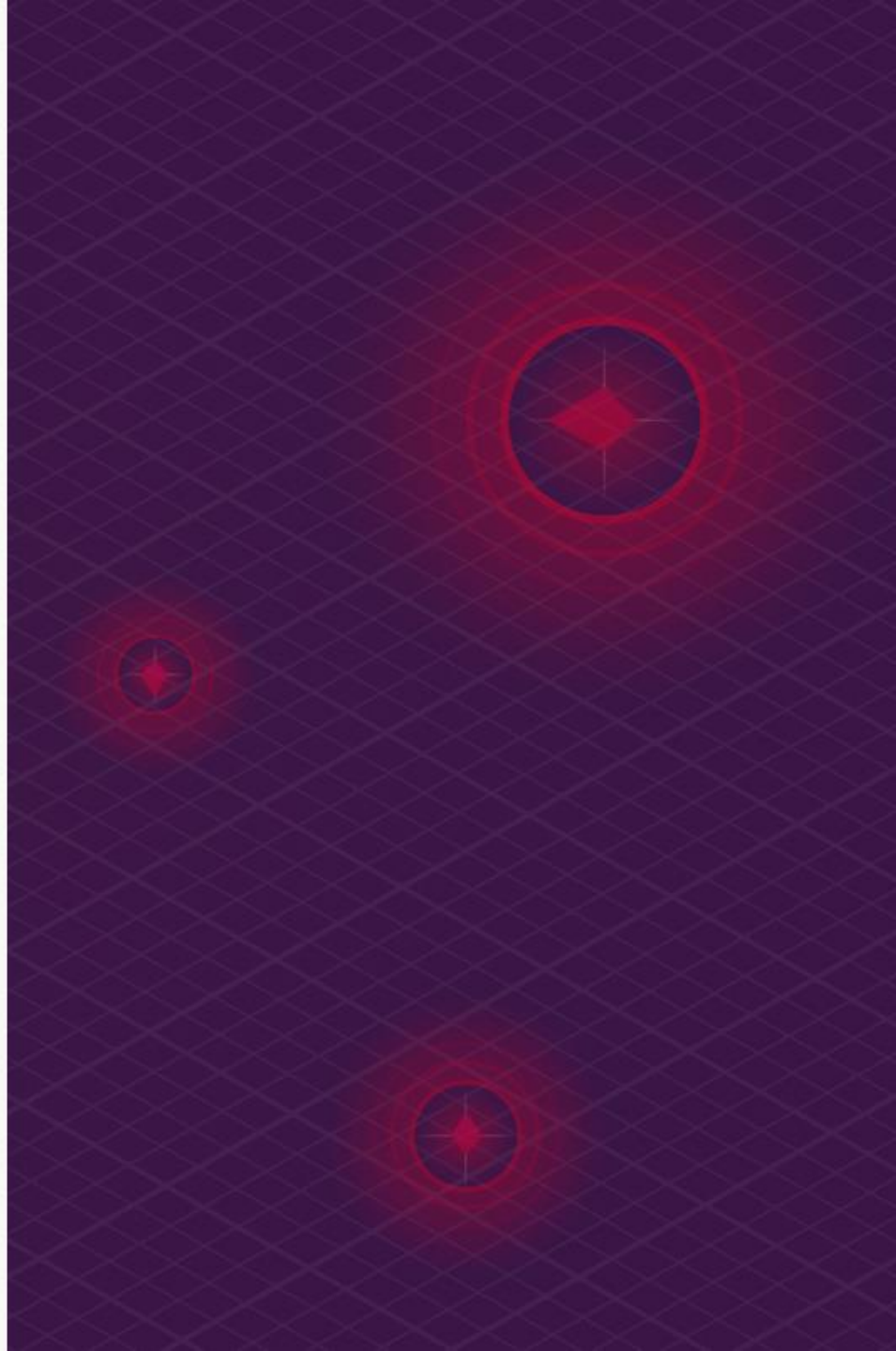
T.Hunter
атакующая безопасность

Основные тренды мошенничества в 2021 году

Макаров Владимир

Главный специалист отдела аудита ИБ
Компании «Ти Хантер»

Люди видят то, что хотят видеть. На этом их и ловят мошенники



Африканский футбол

Суть преступной аферы:

мошенничество с футбольным трансфером.

Злоумышленники умудрились обмануть итальянский футбольный клуб «Сампдория».

Спортивная структура перевела им 800 тысяч евро

Завязка

По данным из открытых источников, Миккель Дамсгор перешел из «Норшелланна» в «Сампдорию» 1 сентября 2020 года.

В таких случаях деньги обычно переводятся не сразу, а несколькими платежами.

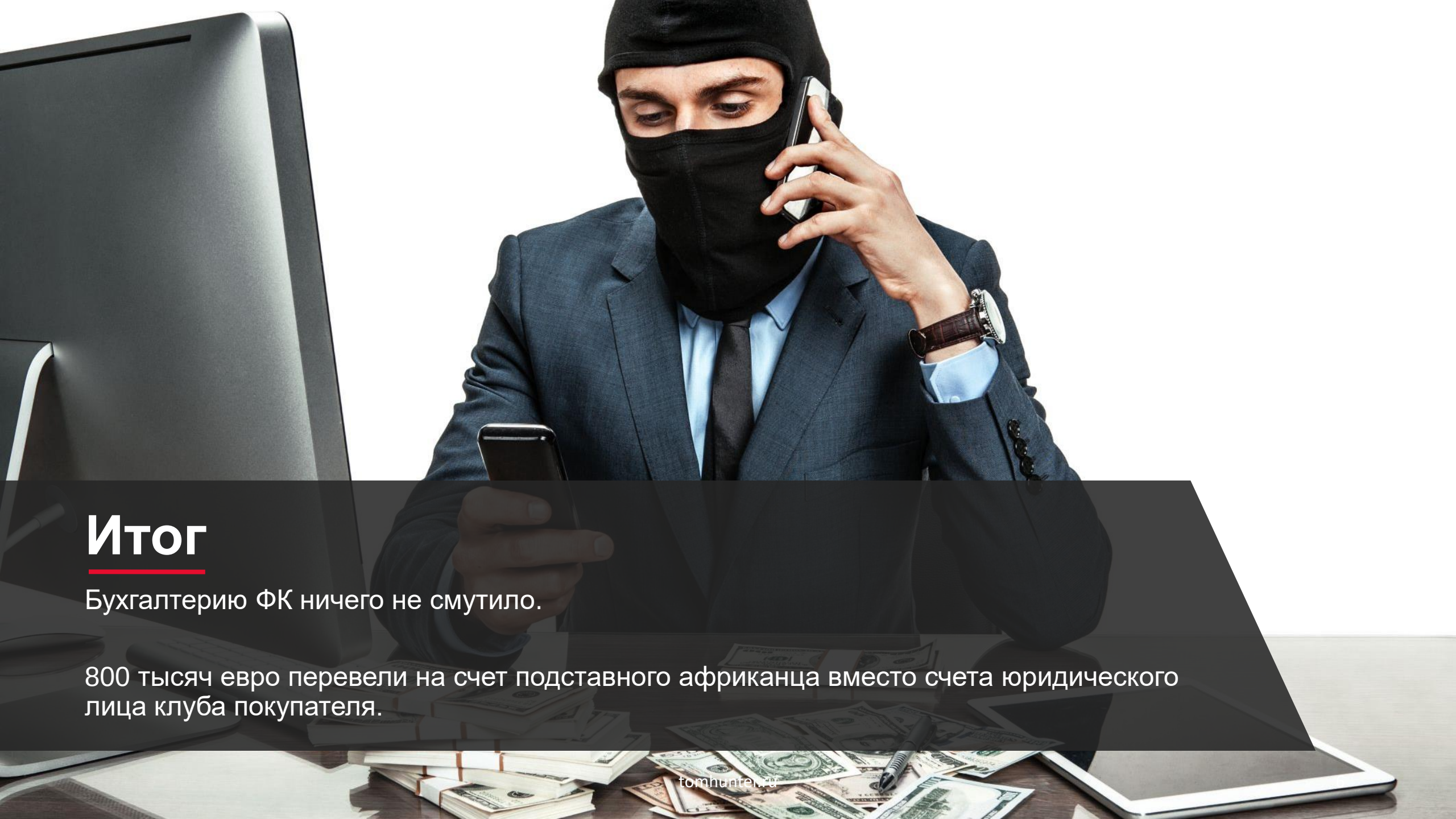
Один из таких переводов и стал объектом внимания африканских мошенников, которые смогли в итоге обмануть бухгалтерию итальянского клуба.

Как так-то?

В фальшивом документе в графе «имя» злоумышленники указали аббревиатуру FC SAMPDORIA

Изготовив поддельный паспорт на вымышленное имя, они открыли счет банке Санкт-Петербурга.

Отправили номер счета своему подельнику из Европы. Последний смог обманным путем изменить данные о клубе покупателе на данные гражданина FC, на счет которого и поступили денежные средства за покупку игрока.



Итог

Бухгалтерию ФК ничего не смутило.

800 тысяч евро перевели на счет подставного африканца вместо счета юридического лица клуба покупателя.

Задержание

В Ленинградской области, в городе Мурино, 23 сентября 2021 года были задержаны четверо выходцев из Западной Африки

Чему нас учит эта история?

Использование инфоповодов

Инфоповод – мощный заряд доверия

В июне 2020 года весь Twitter

Хакеры в 1998

Я написал вирус, который спалит твой BIOS, чисто по приколу

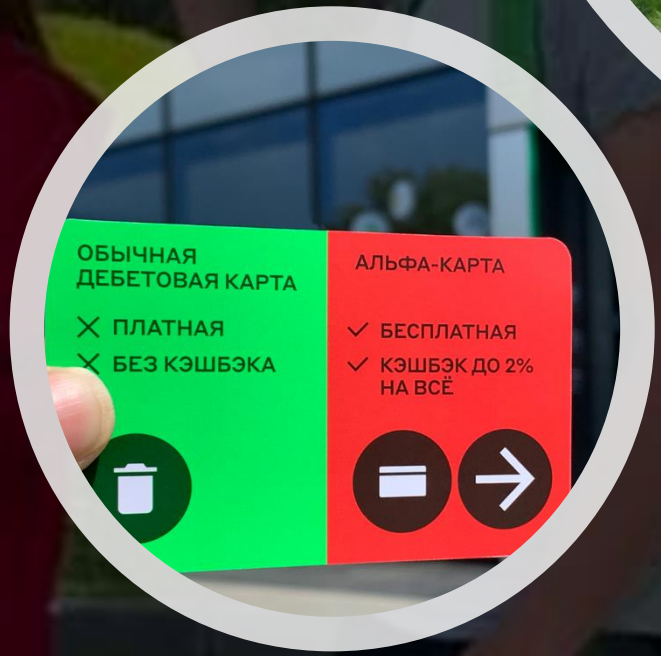
Хакеры в 2020

Я Илон Маск
Пришлите битки

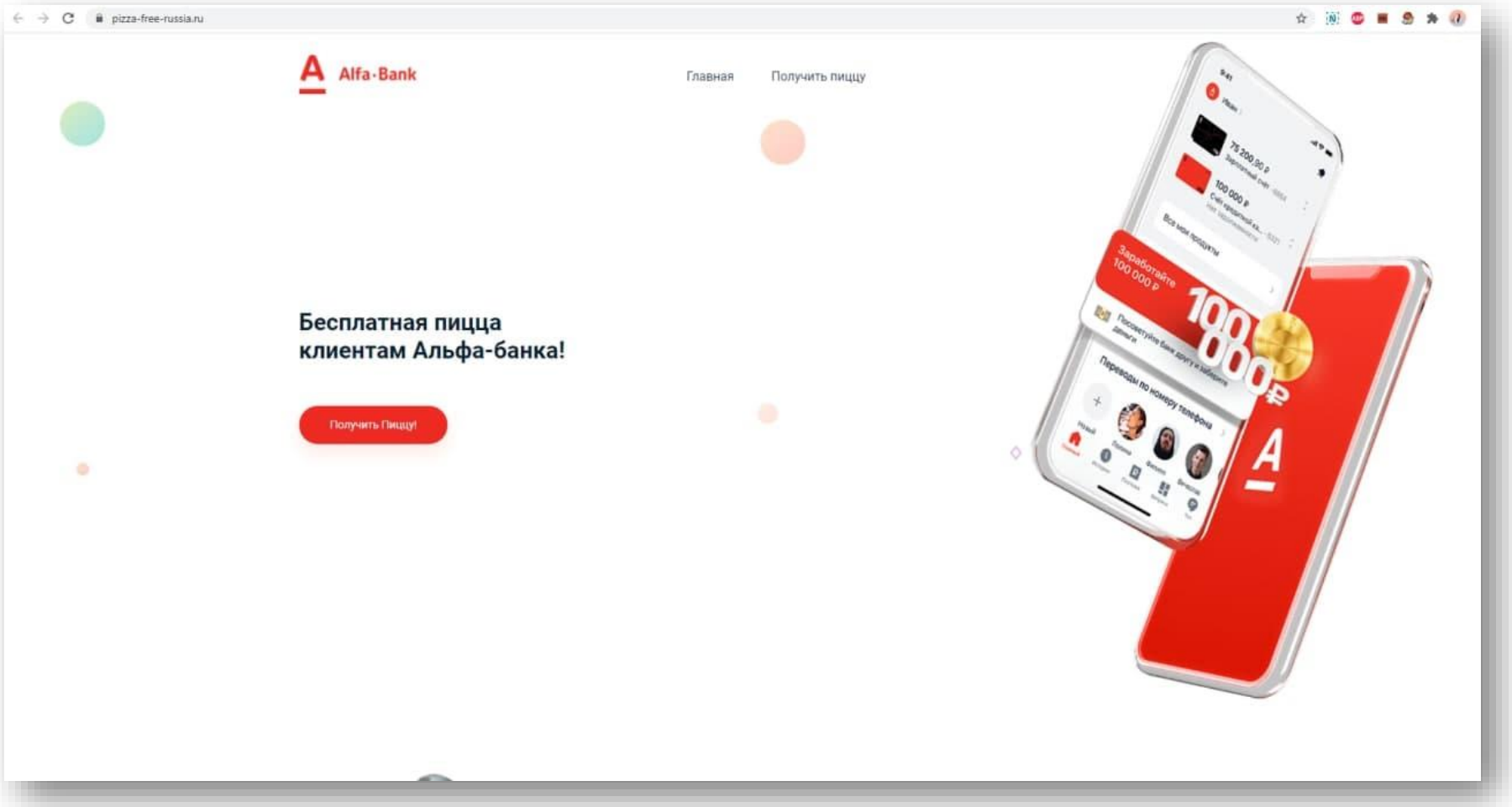
Россия в этом плане не исключение

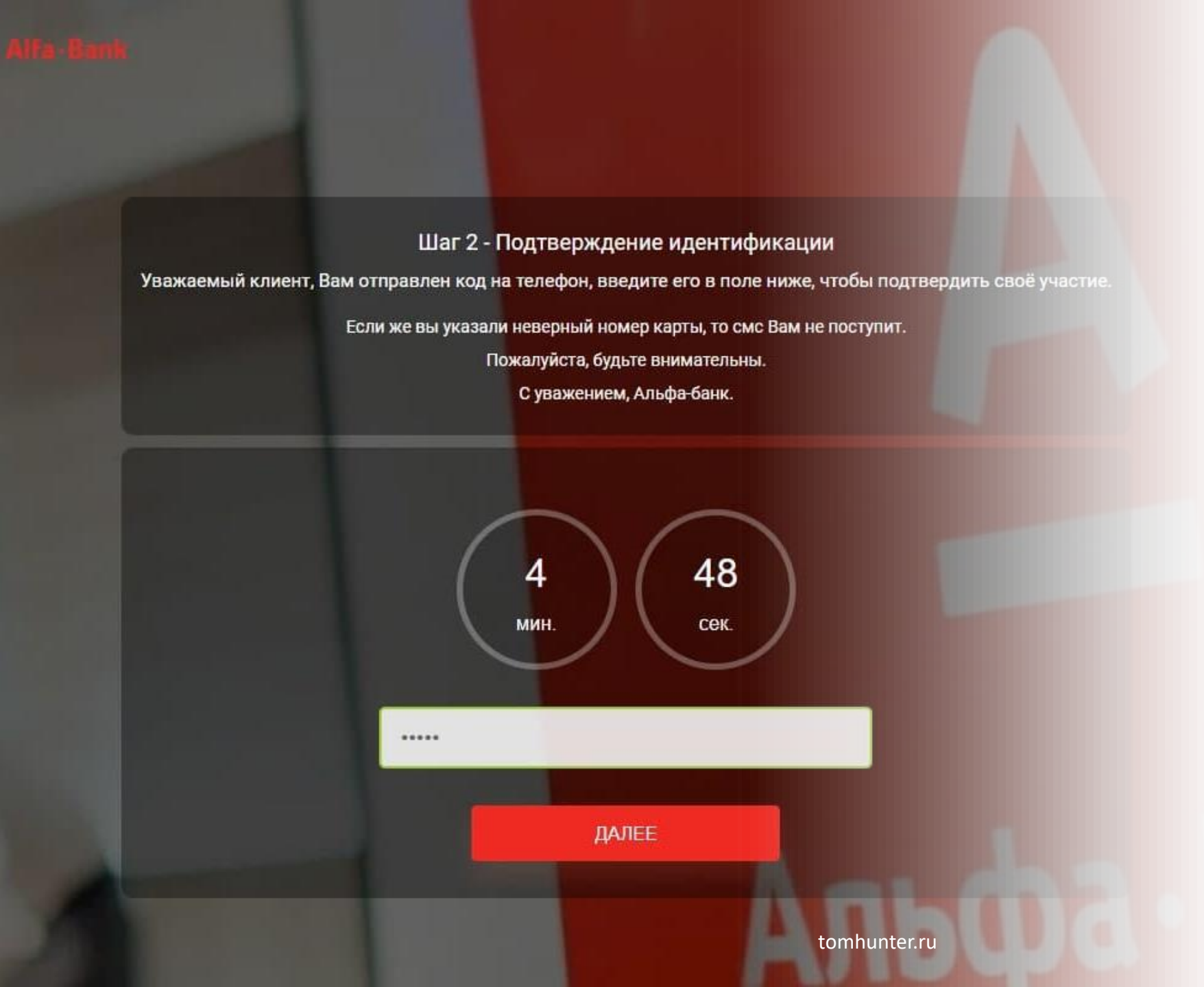
В мае «Сбер» угостил пиццей промоутеров «Альфа-Банка», раздававших листовки у входа в его офис.

Это событие не осталось незамеченным и упоминания о нем разлетелись по сети.



«Банк раздает пиццу… отличная мысль!» - решили мошенники





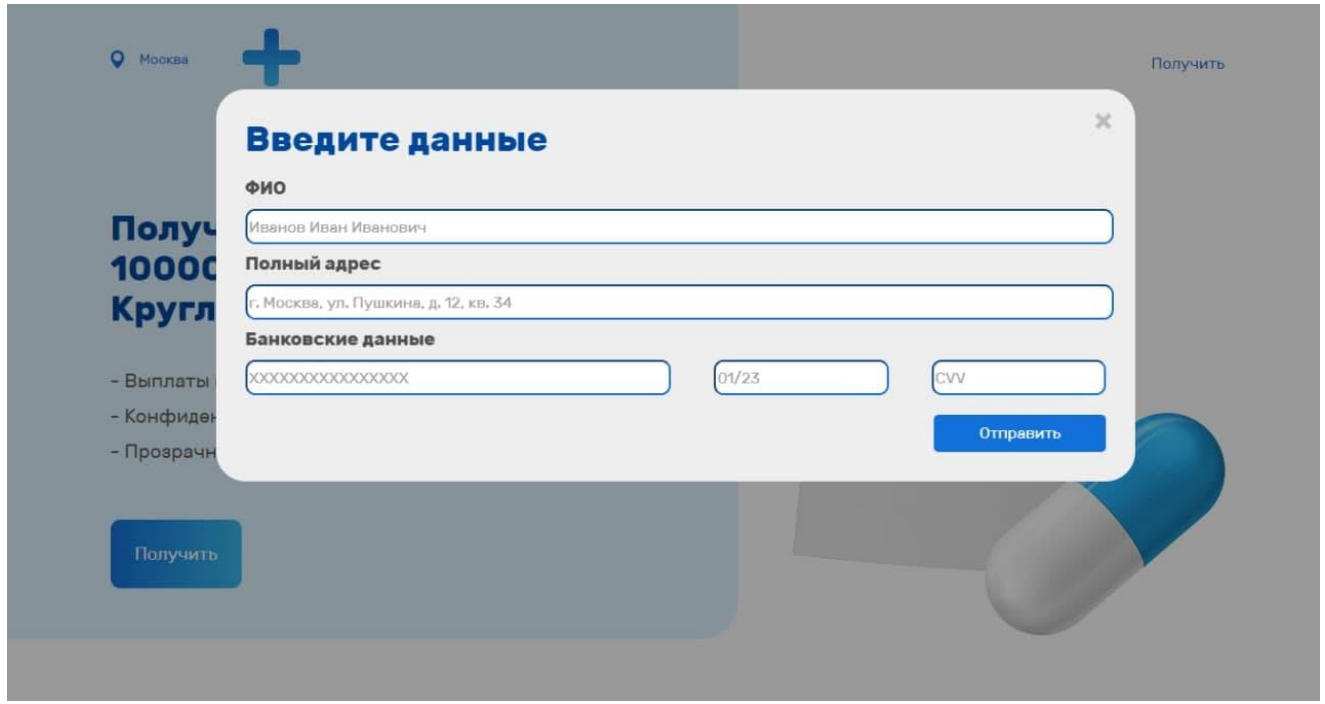
Желающему получить бесплатное угощение требовалось ввести ФИО, номер банковской карты и номер телефона.

А после этого передать злоумышленникам код из СМС.

Разумеется, сайт убеждает нас в том, что безопасность данных клиентов банка гарантируется, а акция направлена на повышение лояльности клиентов.

Опять COVID-19

Пока в России фиксируется очередной всплеск заболеваемости COVID-19, мошенники пытаются выжать из этой темы все возможное.



Основной тренд все еще ПАНДЕМИЯ

Основным видом мошенничества с применением инфоповода в 2021 году все еще остается продажа поддельных QR-кодов и справок.

КРУПНЫЙ БРЕНД – ЭТО НАДЕЖНОСТЬ!

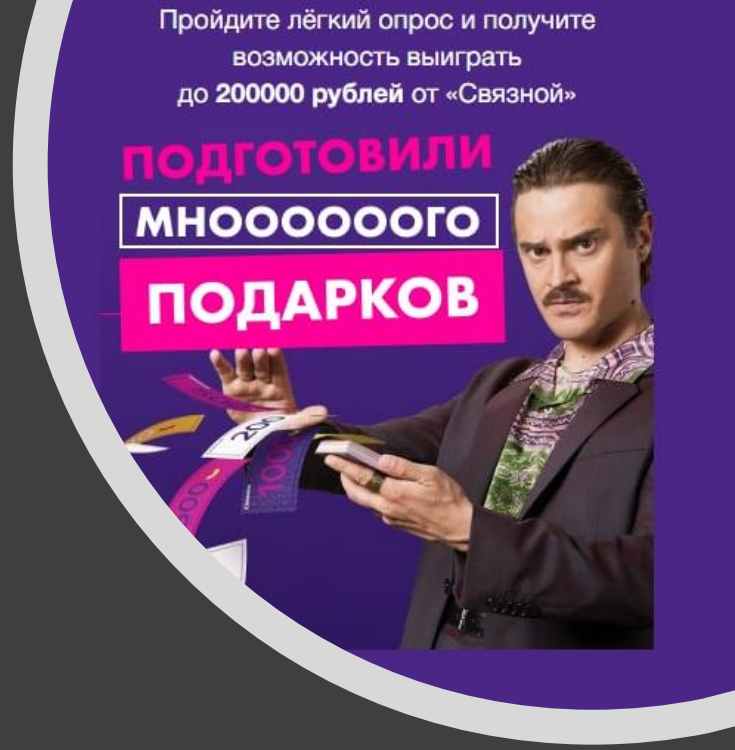
tomhunter.ru

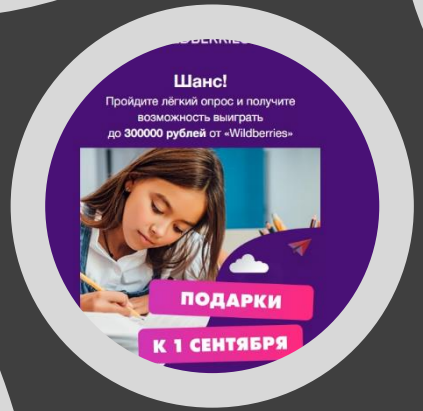
Основной упор на ритейл

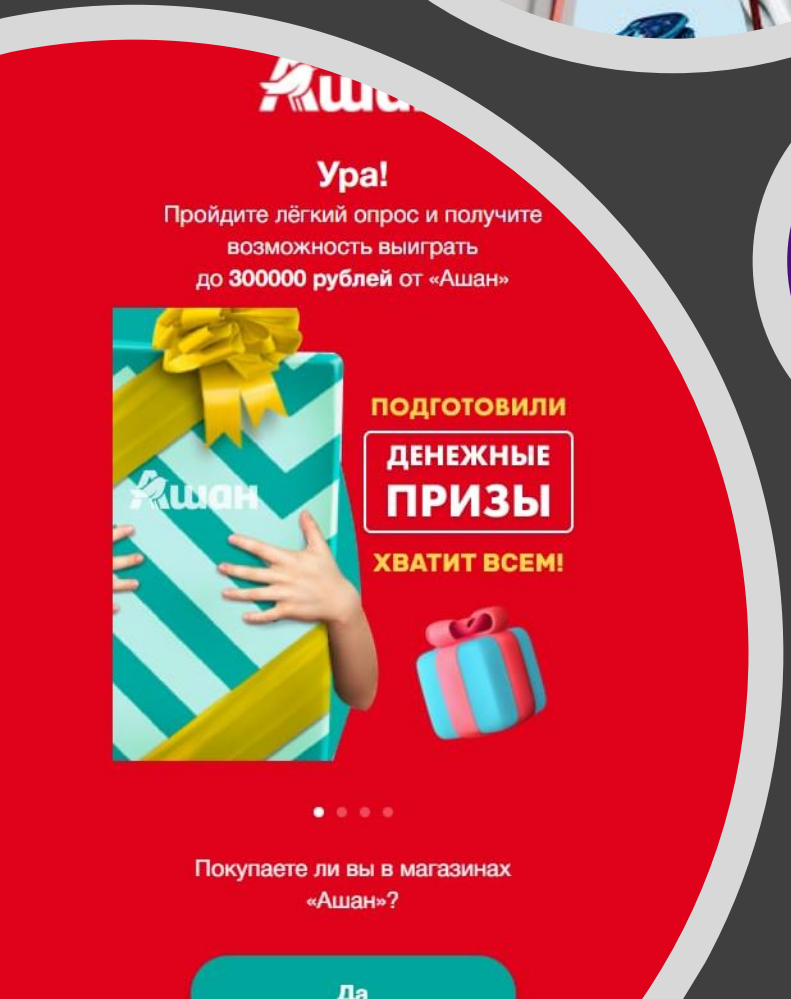
Российский ритейл снова под прицелом киберпреступников.

Начиная с последних чисел августа фиксируется интенсивная атака на российский ритейл-сектор.

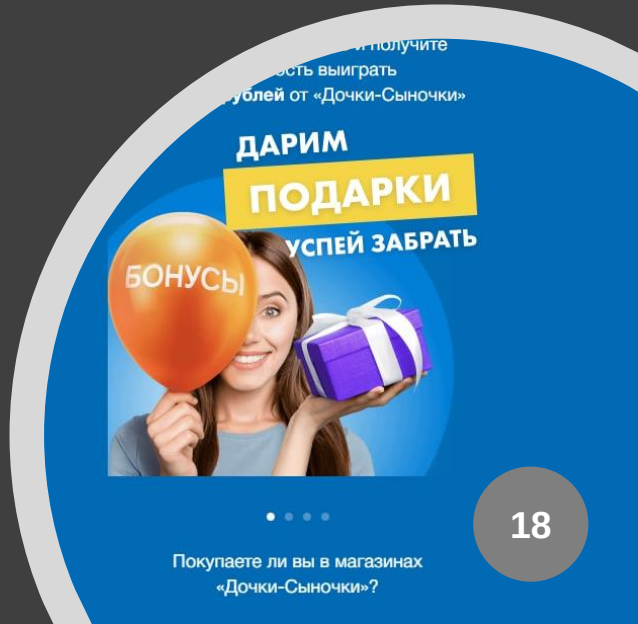
На сегодняшний день под ударом находится порядка 15 популярных российских брендов, в их числе «Дочки Сыночки», «Красное и белое», «Бристоль», «Дикси», «Ашан», «О’Кей», «Wildberries», «DNS», «Связной», «Ситилинк», «Татнефть», «Huawei», а также «Теле2».







Все сайты имеют схожий паттерн атаки



Как итог имеем самую массированную атаку в 2021 году на ритейл

Подобная схема позволяет обеспечить стремительное расширение аудитории без использования малоэффективных схем типа рассылки спама

Помимо этого, сам факт того, что человек получает ссылку на фейковый сайт от своего друга, заранее повышает шансы того, что он перейдет по ссылке и станет очередной жертвой и звеном в цепочке распространения

Исходя из количества задействованных брендов, можно говорить о том, что это самая массированная атака на клиентов ритейла в 2021 году.

Атака на Wildberries

В июне компания Wildberries направила заявление в полицию по факту хищения 385 миллионов рублей.

Злоумышленники открывали на площадке свой магазин, наполняли его несуществующими товарами по завышенным ценам.

Уязвимость оказалась на стороне Wildberries

После этого злоумышленники оформляли покупки своего товара, однако при оплате указывали платёжные данные карты с нулевым балансом.

Система оплаты Wildberries подтверждала покупку и переводила деньги на счёт продавцу со счетов Wildberries, игнорируя при этом ответ от банка об отмене транзакции ввиду недостаточного баланса на карте.

Как же Wildberries решил проблему?

Баним все подозрительные магазины и сразу переходим в фазу Damage control для репутации компании.

На все крики забаненых честных продавцов на платформе – не реагируем.

А ведь можно было просто отключить функционал оплаты товаров без фактической отгрузки…

Богатства страны чьи?

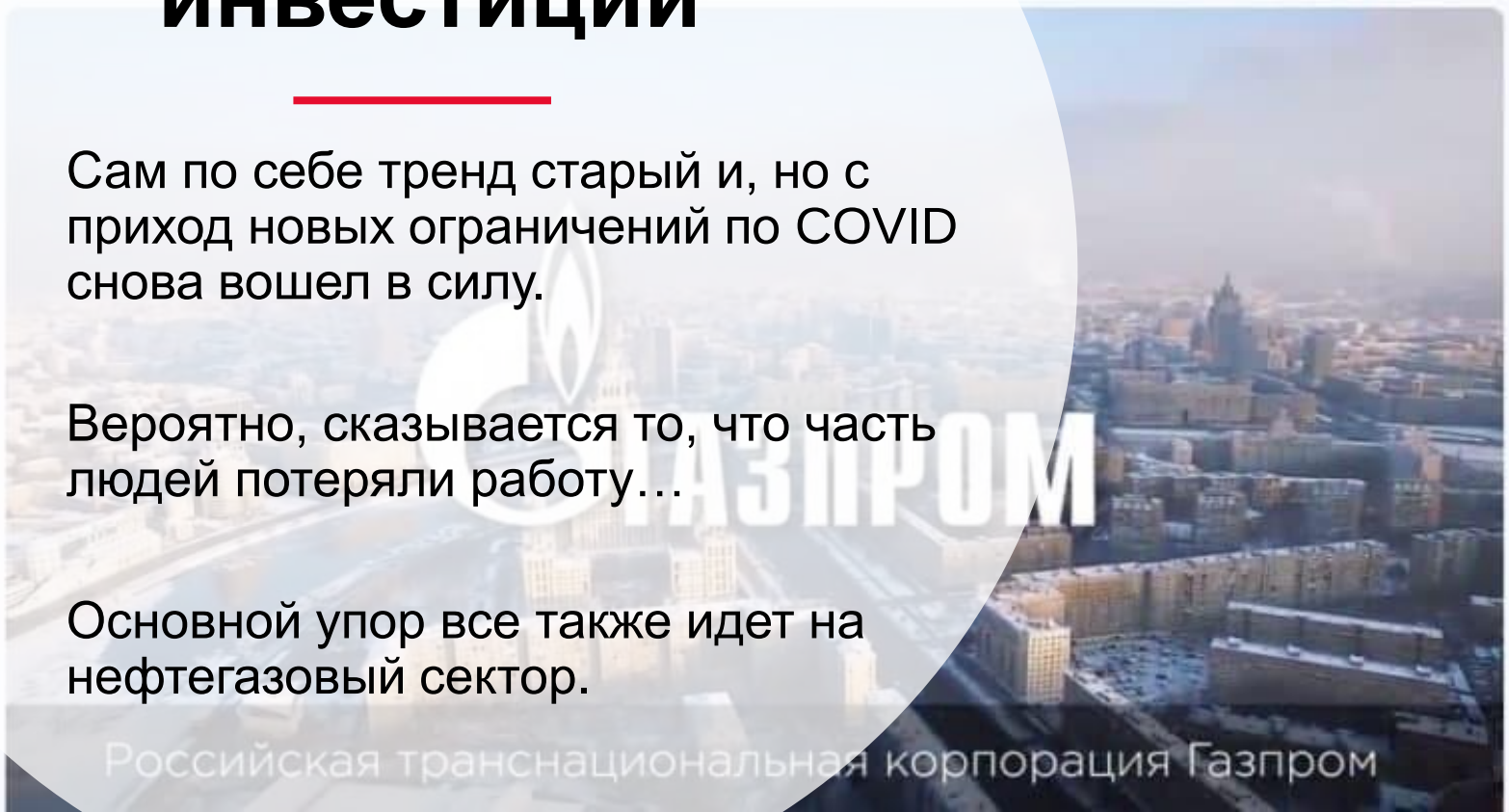
НАШИ!!!

Фейковые инвестиции

Сам по себе тренд старый и, но с приход новых ограничений по COVID снова вошел в силу.

Вероятно, сказывается то, что часть людей потеряли работу…

Основной упор все также идет на нефтегазовый сектор.

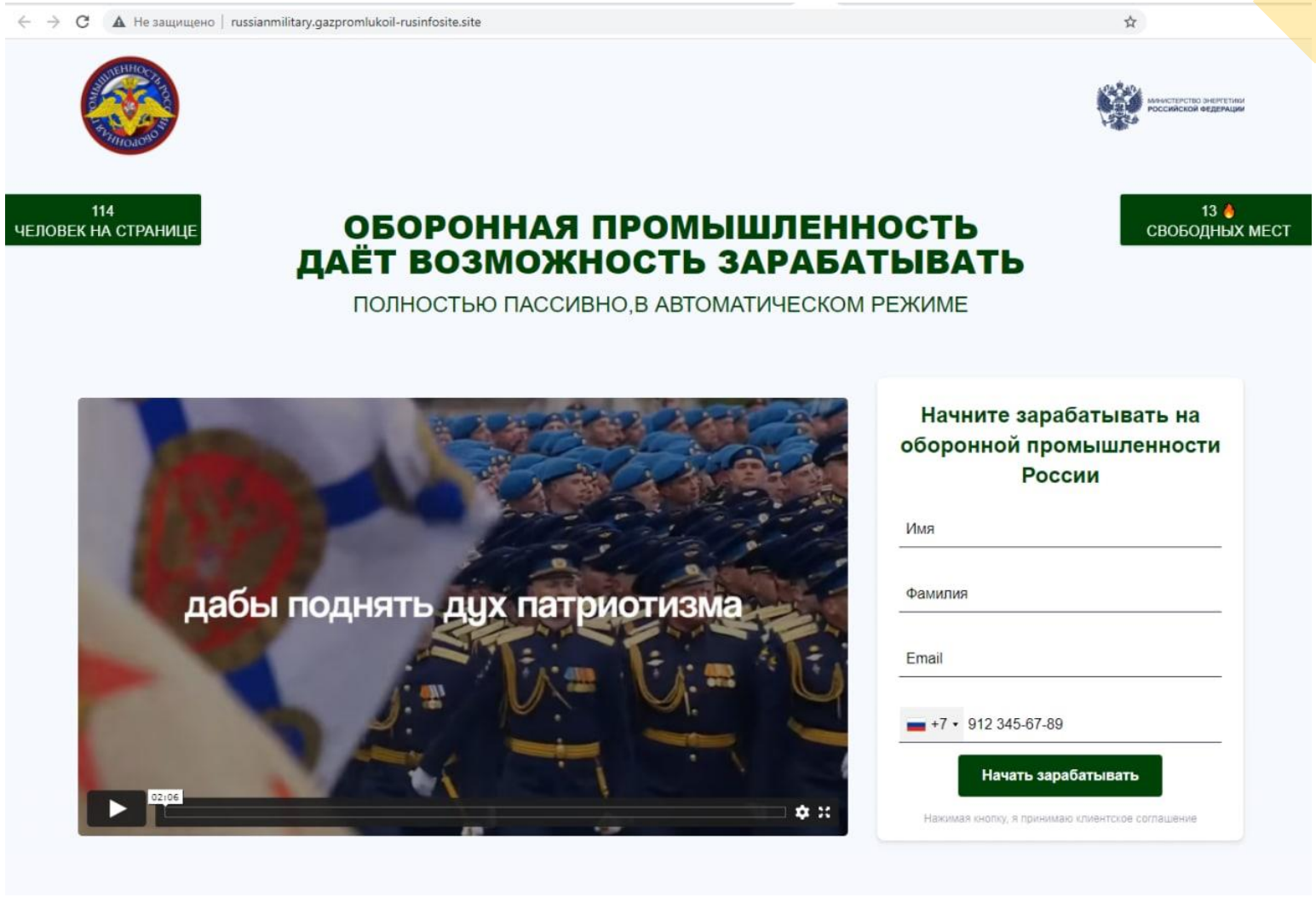


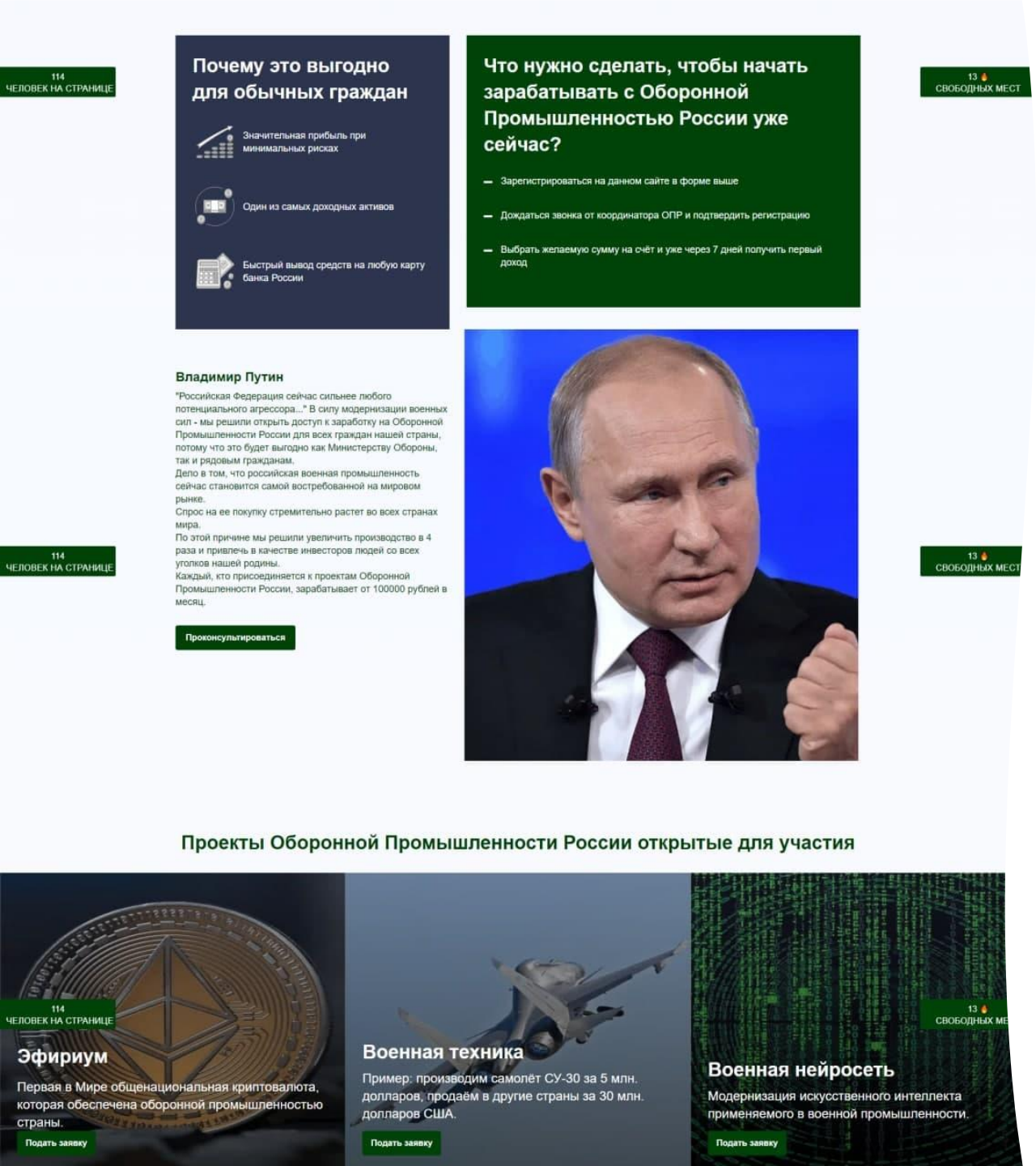
Для тех, кто считает, что торговать газом уже НЕ МОДНО

Теперь же в целях поднятия духа патриотизма предлагается инвестировать в ВПК.

Шаблон сайта, к слову, остался прежним, создатели поленились даже заменить надпись «Министерство энергетики» и для атаки используется домен:

gazpromlukoil-rusinfo.site





Чтобы поднять кредит доверия – фото Президента РФ

Для того, чтобы придать весомость предложению, на сайте размещена откровенно фейковая цитата Президента РФ

Ну и конечно невозможно не обратить внимание на проекты Оборонной промышленности России.

Набирающие силу тренды

Шантаж компаний через отзовики

Подавляющее большинство (93%) российских интернет-юзеров при выборе товаров и услуг ориентируются на отзывы.

В сентябре появилось более 100 доменов со словом «отзыв», причем многие из них явно были зарегистрированы одними и теми же людьми.

Вектор атаки – накрутка негативных отзывов в подконтрольные сайты отзовики с последующим предложением компании все убрать.

Безакцепное списание денежных средств с банковских карт

Никаких кодов подтверждения платежа в смс-сообщениях или push-уведомлениях при этом жертве не приходит.

Самое популярное мошенничество посредством этого метода сейчас происходит через сервис Stripe.

Дата операции / дата обработки[1] / код авторизации	Описание операции / категория	Сумма в валюте счёта[2] / сумма в валюте операции	Остаток по счёту в валюте счёта
23.12.2020 00:00 24.12.2020 / 243418	MARIA S Все для дома	5 484,79 (70,39 USD)	87 046,33
23.12.2020 00:00 24.12.2020 / 258961	MARIA S Все для дома	5 458,30 (70,05 USD)	92 531,12
23.12.2020 00:00 24.12.2020 / 218941	MARIA S Все для дома	5 504,27 (70,64 USD)	99 255,42
23.12.2020 00:00 24.12.2020 / 234226	MARIA S Все для дома	5 440,37 (69,82 USD)	104 759,69

T.Hunter
атакующая безопасность

СПАСИБО ЗА ВНИМАНИЕ

Макаров Владимир

Главный специалист отдела аудита ИБ
Компании «Ти Хантер»