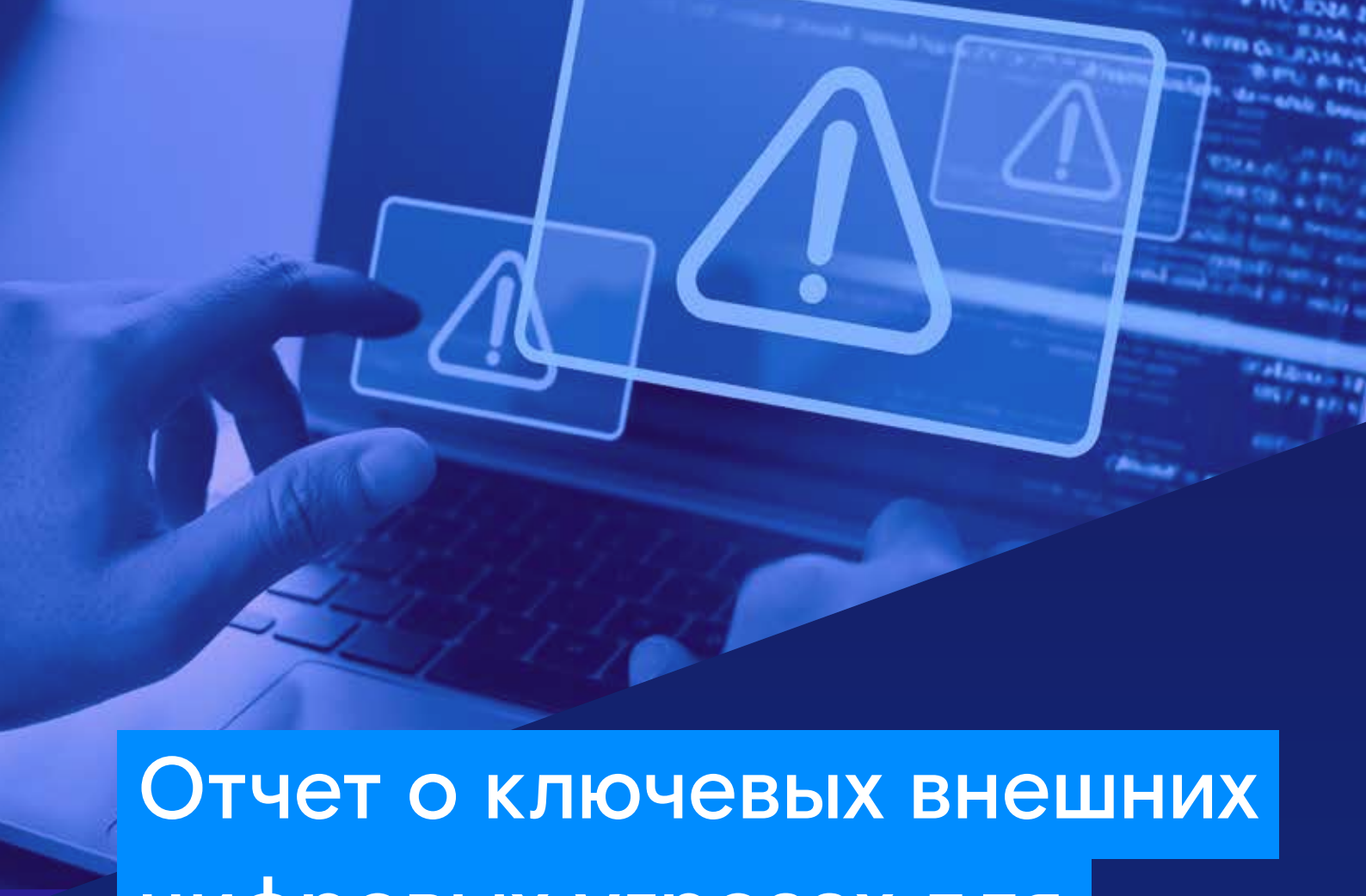


Отчет о ключевых внешних цифровых угрозах для российских компаний

(январь – апрель 2023)

rt-solar.ru
rt.ru

Ростелеком
Солар

Оглавление

Об отчете

Отчет составлен на основе данных DRP-сервиса мониторинга внешних цифровых угроз Solar AURA компании «РТК-Солар». Аналитика базируется на результатах мониторинга публичных и закрытых сегментов интернета:

1,2 млн+ **доменных имен и выданных SSL-сертификатов (пул источников динамически обновляется каждые сутки);**

более 2500 **Telegram-каналов противоправной тематики и даркнет-форумов;**

50 млн **DNS-запросов в сутки.**

Отчетный период включает январь – апрель 2023 года.

О сервисе Solar AURA

Сервис Solar AURA включает восемь модулей, которые могут подключаться отдельно или в комплексе:

«Антифишинг» — обеспечивает полный цикл противодействия фишингу: от выявления доменных имен и интернет-ресурсов, которые могут быть использованы в противоправных действиях в отношении заказчика или от его имени, и до реализации комплекса мер по оперативной блокировке подобных ресурсов.

«Утечки» — помогает оперативно выявлять факты компрометации чувствительной для компании информации в публичных источниках.

«Даркнет» — помогает оперативно выявлять в даркнете и на иных ресурсах признаки угроз, нацеленных на компанию, таких как случаи публикации в Сети документов ограниченного доступа, баз данных, сведений о скомпрометированных аккаунтах, а также различного рода нелегальных услугах и готовящихся кибератаках.

«Бренд компании» — выявляет широкий перечень нарушений, затрагивающих бренд компании: от фейковых страниц в соцсетях и мессенджерах до мобильных приложений, использующих название и логотип организации или её продукты.

«Личный бренд» — отслеживает появление фейковых личных аккаунтов в соцсетях, случаи компрометации личных и корпоративных учетных данных, оценивает информационный фон вокруг персоналий компании, фиксирует появление негативных или компрометирующих публикаций.

«Медиаполе» — выявляет в открытом доступе публикации, способные негативно повлиять на информационную или экономическую безопасность компании, в частности, сведения об используемых средствах защиты информации, регламентах работы, особенностях ИТ-инфраструктуры и т. п.

«Безопасность финансов» — обнаруживает факты использования интернет-эквайринга банка для оплаты запрещенных в РФ услуг; собирает сведения о банковских картах, используемых при отмывании или обналичивании нелегальных денег; мониторит сайты с интернет-эквайрингом защищаемого банка на соответствие заявленному виду деятельности; предоставляет сведения для проверки контрагентов.

«Мониторинг периметра» — сканирует корпоративные сервисы на наличие уязвимостей; ищет новые опубликованные в интернете ИТ-активы компании; контролирует контент сайта на предмет нелегитимных изменений.

Ключевые тезисы

- Изменение мотивации киберпреступников привело к существенному смещению ландшафта угроз. Атакам стали подвергаться даже те организации и отрасли, которые ранее не привлекали внимания злоумышленников.

- Киберпреступность быстро адаптировалась к санкционным условиям и уходу из России популярных сервисов и платежных систем.

- Ключевая угроза – утечки данных. С начала года в Сеть попало более 300 млн строк конфиденциальных сведений, а общий объем размещенных данных российских компаний составил 1,1 ТБ.

- Косвенные утечки также могут наносить прямой ущерб. Мы фиксируем значительное количество чувствительных корпоративных данных, фигурирующих в утечках из сторонних компаний, не имеющих прямого отношения к объекту мониторинга.

- В то же время появляется множество фейковых данных, выдаваемых за сведения, украденные из той или иной компании.

- Злоумышленники не брезгуют копаться в «мусоре»: даже отработанные логи с троянов-стилеров представляют интерес для ряда киберпреступников, выискивающих в них чувствительные корпоративные данные.

- Фишинговые атаки становятся все более массовыми и изощренными. Основные характеристики современного фишинга: высокий уровень автоматизации, защита от обнаружения, нацеленность на самые разные отрасли.

Изменение ландшафта угроз. Причины. Следствия

Минувший год произвел революцию в российском киберкриминальном мире. Число атак существенно увеличилось, а перечень атакуемых отраслей и компаний расширился. 2023 год стал достойным преемником 2022-го: все ключевые тенденции сохранились и получили свое эволюционное развитие. Можно выделить две основные причины, способствовавшие изменению ландшафта ИБ-угроз.

Во-первых, это **изменение мотивации киберпреступников**, которые затронули в первую очередь B2B и B2G. Даже множественные утечки персональных данных граждан стали следствием роста числа атак на организации, а не на физических лиц.

Ключевая мотивация атак на B2B и B2G до 2022 года: материальная выгода.

Ключевая мотивация атак на B2B и B2G в 2022–2023 годах: хактивизм, идеологически мотивированные атаки, преследующие своей целью нарушение функционирования российских организаций и предприятий.

Вторая причина – появление в открытом доступе многочисленных автоматизированных инструментов, облегчающих реализацию типовых кибератак. Это существенно снизило порог вхождения в преступный бизнес и позволило низкоквалифицированным злоумышленникам осуществлять технически сложные атаки даже при отсутствии должного опыта и понимания происходящих процессов.

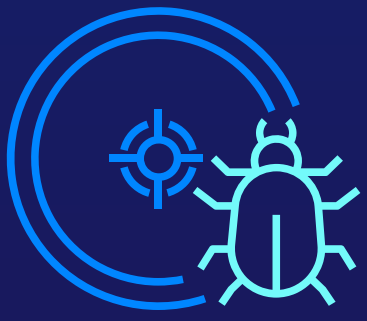
С одной стороны, бесплатная публикация инструментов, которые раньше были доступны узкому кругу лиц, дает возможность организовывать более массовые атаки на российский бизнес. С другой – позволяет замаскировать по-настоящему серьезные атаки за счет повышения нагрузки на ИБ-подразделения атакуемых компаний.

Последствия:

- **Увеличилось общее количество инцидентов.** Любой достаточно замотивированный человек, вооруженный вредоносными скриптами, получил возможность атаковать самые разные информационные ресурсы.

- **Существенно расширился перечень целей атак.** Любая российская организация автоматически становится предметом интереса злоумышленников вне зависимости от ее принадлежности к субъектам критической инфраструктуры или наличия у нее ценных информационных активов.

- **Чувствительные данные массово публикуются в открытом доступе.** Полученные в ходе атак сведения, которые раньше выставлялись на продажу и были доступны ограниченному кругу лиц, теперь становятся общедоступными.



Утечки данных – главная киберугроза в 2023 году

С января по апрель 2023 года в Сеть попали данные **123 российских организаций.** А общий объем опубликованных данных составил **1,1 терабайта.**

Что утекает

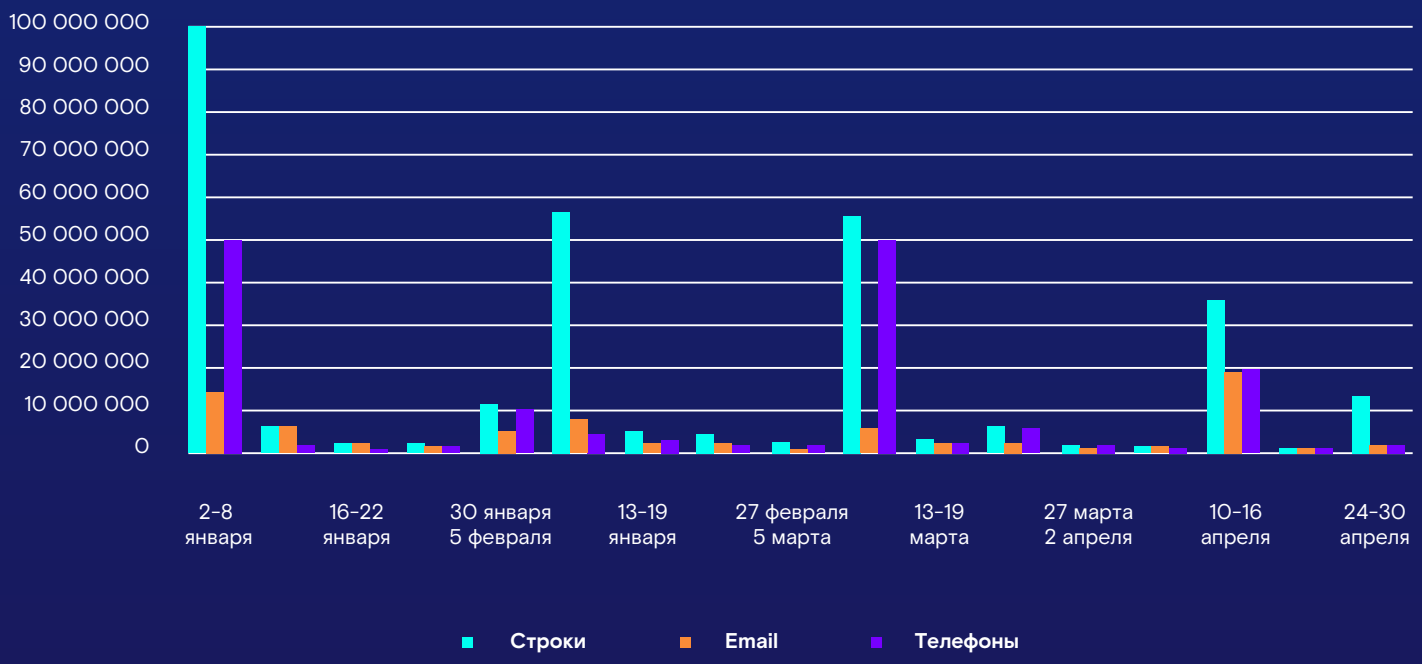
76% утечек составляют различные базы данных;

24% утечек – массивы документов, украденных с файловых серверов.

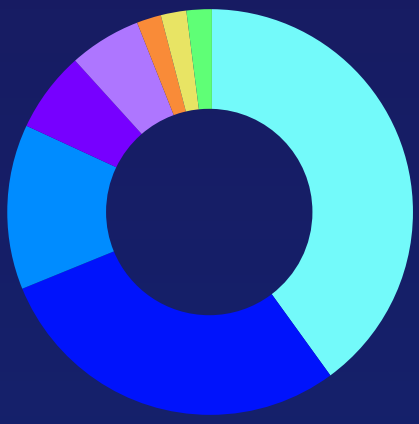
В **6%** случаев кража данных сопровождалась дефейсом сайта атакованной организации.

Размещенные с начала года в публичном доступе базы данных содержат в общей сложности **более 300 млн строк**, в том числе **61,1 млн** адресов электронной почты и **144,3 млн** телефонных номеров.

Утечки данных по неделям



Распределение утечек по отраслям



- 40% E-commerce
- 6% Соцсети
- 2% Госорганизации
- 29% Финансы
- 6% Наука и искусство
- 2% Услуги
- 13% Строительство и девелопмент
- 2% ИТ

Количество утекших сведений, опубликованных в открытом доступе за последний год, настолько велико, что к ним в полной мере применимы принципы анализа больших данных. Такая ситуация делает любую новую утечку значимой и потенциально опасной. Так, популярные в даркнете боты и сервисы по «пробиву» берут сведения из самых разных утечек и формируют на их основе комплексное досье на конкретную персону, обогащая одни сведения за счет других. Подобные приемы используются и в процессе подготовки социотехнических и иных атак на организации.

Пример инцидента

1. Злоумышленники взломали компанию «А», организатора конференции, и опубликовали в Сети список ее участников, содержащий их ФИО, должности, телефоны, адреса электронной почты и названия компаний, которые они представляли.

   Несмотря на то что размещенные сведения относятся к персональным данным, сами по себе они не несут прямой угрозы лицам и организациям, сотрудники которых фигурируют в указанной базе.

2. В утечке обнаруживаются данные Алексея М., сотрудника компании «Б».

3. Поиск по номеру телефона в ранее опубликованных утечках позволяет получить дополнительные сведения об Алексее: адрес проживания (из утечки службы доставки еды), серию и номер паспорта (из утечки курьерской службы), личный email и хеш пароля (из утечки интернет-магазина).

4. Поиск по личному и корпоративному адресам электронной почты позволяет получить ссылки на профили в социальных сетях, а также пароли, фигурировавшие в других публичных утечках.

5. Один из ранее утекших паролей подходит к корпоративной учетной записи Алексея М. и открывает злоумышленникам путь в инфраструктуру компании «Б».

Это всего лишь один частный пример того, как, отталкиваясь от минорной утечки, злоумышленники могут «раскрутить» ситуацию до серьезного инцидента. В реальности количество возможных сценариев значительно больше.

Утечки, которых не было

Информация о новых утечках данных публикуется ежедневно, но далеко не все они являются следствием реальных или актуальных атак. Публикации данных, полученных в ходе атак на малый бизнес, в **80%** случаев имеют признаки достоверности. Однако, когда речь заходит о крупном бизнесе и государственном секторе, вырисовывается прямо противоположная картина. Всему виной различная ценность информации, а чем ценнее данные, тем больше желающих их сфальсифицировать.

Основные мотивы фейковых публикаций об утечках:

- Желание хакеров заработать репутацию, поднять свой рейтинг в конкретном киберкриминальном сообществе.
- Желание продать незначительную информацию под видом более ценной.
- Создание негативного информационного фона вокруг организации.
- Демонстрация активности хакерской группировки в отсутствие реальных достижений.

Классификация фейковых публикаций об утечках информации:

- Компиляция сведений из разрозненных утечек, не имеющих отношения к упоминаемой в публикации компании.
- Публикация старой утечки под видом новой.
- Публикация сообщения якобы о взломе компании без предоставления каких-либо образцов информации или иных доказательств.
- Взятие на себя ответственности за реальный инцидент, произошедший ранее.

Параллельно с размещением откровенно фейковых данных участились и случаи публикации реальной информации, полученной в ходе атак, совершенных несколько месяцев, а иногда и лет назад. В ход идут те сведения, которые на момент атаки не вызвали интереса у злоумышленников и пылились в их архивах. Теперь же различные кибергруппы пытаются с их помощью подогреть интерес к своей деятельности или заработать дополнительные деньги.

Полезный «мусор»

Помимо громких утечек, затрагивающих конкретный бренд, существует отдельная прослойка неструктурированных данных. Они получены в результате компрометации компьютеров и мобильных устройств физических лиц, а не целевой атаки на компанию. Один из каналов получения подобных данных – трояны-стилеры, предназначенные для кражи с зараженного устройства учетных данных и иной потенциально полезной хакерам информации.

Данные со стилеров активно продаются на черном рынке. Как правило, покупатели логов используют их для поиска и последующей кражи аккаунтов, которые легко монетизировать. Например, это учетки от игровых платформ, стриминговых сервисов и других популярных ресурсов.

Отработанные логи, уже не представляющие ценности для покупателей, размещаются в открытом доступе. Нами было проанализировано более **338 млн** таких «мусорных» учетных данных от 10 тыс. различных сервисов (все данные были опубликованы с начала 2023 года).

В результате мы обнаружили:

- **134 406 аккаунтов** клиентов российских банков;
- **977 615 аккаунтов** пользователей российских социальных сетей;
- **887 707 аккаунтов** пользователей популярных российских почтовых сервисов.

Фишинговые атаки

Тренды

Основными характеристиками фишинговых атак начала 2023 года являются:

1. **Автоматизация.** Процесс развертывания современного фишингового сайта в значительной мере автоматизирован. Автоматизации подвергается все: от регистрации доменного имени и до формирования фишинговых ссылок, взаимодействия с жертвой и вывода похищенных денег.

2. **Скрытность.** Все больше фишинговых атак осуществляется с использованием различных методов защиты от обнаружения. Фейковые сайты демонстрируют вредоносный контент лишь в том случае, если они невидимы для стороннего наблюдателя (пример подобной маскировки приведем ниже), а жертва соответствует заданным злоумышленниками параметрам.

3. **Использование доменов, не связанных с конкретным брендом.** Все чаще в фишинговых схемах оказываются задействованы произвольно сгенерированные доменные имена. Это делает невозможным их обнаружение методом анализа файлов зон DNS, мониторингом SSL-сертификатов или просто перебором похожих на официальный домен слов.

4. **Снижение доли использования интернет-эквайринга на фишинговых сайтах.** Акцент смещается с разового списания платежа в сторону попытки получения доступа к личному кабинету в системе онлайн-банкинга.

Наличие в широком доступе готовых фишинговых китов (набор скриптов для создания фишинговых сайтов), а также распространение схемы cybercrime-as-a-service привело к массовому притоку в отрасль низкоквалифицированных злоумышленников, способных при этом осуществлять технически сложные атаки благодаря наличию продвинутых инструментов.

Топ-6 популярного фишинга в 2023 году:

1. **Взлом Telegram или социальных сетей.** Фишинговые сайты используют регулярно меняющиеся информационные поводы для привлечения потенциальных жертв: от онлайн-голосования или подписания петиции до получения бесплатного premium-аккаунта или социальных выплат.

2. **Банковский фишинг.** В данной сфере акцент ставится на получение доступа в личный кабинет клиента банка и кражу денег с его счета, что делает такие атаки предельно опасными.

3. **Фейковые банки.** Сайты несуществующих кредитных организаций появляются практически ежедневно. В дело идут как никогда не существовавшие бренды, так и реквизиты банков, чья лицензия была отозвана.

4. **Фейковые инвестиционные платформы.** Ежедневно мы фиксируем появление от 2 до 15 новых сайтов в рамках данной схемы. Несмотря на то что схема не меняется уже более трех лет, она все еще демонстрирует высокую эффективность за счет сочетания элементов фишинга, телефонных мошенничеств и технических средств, обеспечивающих доступ к компьютеру жертвы. Непосредственно фишинговые сайты используются лишь для получения контактов потенциальной жертвы, дальнейшее общение ведется с «индивидуальным менеджером», который координирует весь процесс взаимодействия. Более того, лжеброкеры часто заставляют жертву устанавливать программы удаленного администрирования на компьютер, чтобы якобы совершать действия на «бирже» от имени клиента. Информационная обертка сайтов-ловушек меняется ежемесячно. Помимо сайтов, нацеленных на россиян, мы фиксируем аналогичные ресурсы, предназначенные для атак на граждан других государств.

5. **Фейковые опросы от имени различных брендов.** Одна из самых технически сложных и интересных схем, активно развивающаяся с 2022 года. В ее основе лежит сценарий, который мы назвали «Хамелеон 2.0». Сообщения со ссылками на вредоносный ресурс распространяются в мессенджерах, причем отправляют их сами пользователи: для получения подарка необходимо поделиться информацией о розыгрыше с друзьями. Ссылка в сообщении ведет не на сам фишинговый сайт, а на один из произвольно сгенерированных доменов, и лишь после нескольких редиректов через такие же безликие домены пользователь оказывается непосредственно на сайте с опросом. При этом цепочка редиректов постоянно меняется, а фишинговый сайт откроется лишь тому, кто попадет на него через переадресацию с одного из промежуточных ресурсов. Это обеспечивает стабильность работы схемы и ее защиту от обнаружения. Динамика данного подвида фишинга крайне высока: за последний год для реализации такой схемы мошенники имитировали **более 40 российских брендов.**

6. **Мошенничества на маркетплейсах.** Схема постоянно развивается в сторону повышения автоматизации. Несмотря на то что пик ее пришелся на 2020-2021 годы, такое мошенничество рано списывать со счетов.

Отдельно стоит отметить фишинг, нацеленный на клиентов российских промышленных и производственных предприятий. Подобные фишинговые атаки можно поделить на сезонные и круглогодичные. К последним, например, относятся фейковые сайты, имитирующие ресурсы российских предприятий нефтегазовой отрасли. С начала года нами было зафиксировано **более 270 инцидентов**, попадающих под категорию Russian Oil Scam. Особенностью схемы является то, что злоумышленники не просто копируют легитимные сайты предприятий, но и создают с нуля фейковые сайты компаний, не имеющих собственного веб-ресурса. Основными жертвами здесь являются зарубежные покупатели, поэтому большая часть таких сайтов является англоязычными.

К сезонному фишингу можно отнести, например, фейковые сайты производителей минеральных удобрений, количество которых резко возросло с началом посевного сезона 2023 года.

Промышленный фишинг практически всегда используется в связке с почтовыми рассылками. Де-факто сайт в этой схеме не играет существенной роли, являясь всего лишь ширмой для домена, используемого для общения по электронной почте.

Важной характеристикой такого фишинга в отличие от фишинговых атак, нацеленных на физических лиц, является его живучесть, ведь он менее массовый, а сами организации могут не сразу среагировать на атаку. Многие фейковые сайты функционируют на протяжении нескольких месяцев. В ряде случаев нами фиксировались фейковые сайты, существующие более года и даже более пяти лет.

Рекорды

В 2023 году наибольший рост в контексте использования в фишинговых кампаниях показала доменная зона **.TOP**. Только в марте этого года в ней было зарегистрировано чуть более **126 тысяч** доменов. Из них 95% составили доменные имена, представляющие собой произвольно сгенерированные буквенно-цифровые комбинации или шаблонные домены, задействованные в популярных фишинговых кампаниях. Такой же процент фиксировался нами и в феврале.

Причина кроется в появлении общедоступных инструментов и сервисов, позволяющих максимально автоматизировать процесс организации массового фишинга (автоматическая регистрация доменов, конструкторы фишинговых страниц, сервисы вывода похищенных денег и др.).

В 2023 году доменные имена в зоне **.TOP** активно использовались в наиболее высокотехнологичных и массовых фишинговых атаках, таких как сценарии вокруг маркетплейсов и «Хамелеон 2.0», для реализации которых требуется ежедневно регистрировать десятки и сотни новых доменов.

По сути, зона **.TOP** повторила судьбу любимых злоумышленниками африканских доменных зон .CF, .MD, .GA и т. п., скрипты для автоматической регистрации в которых лежат в даркнете уже более двух лет.

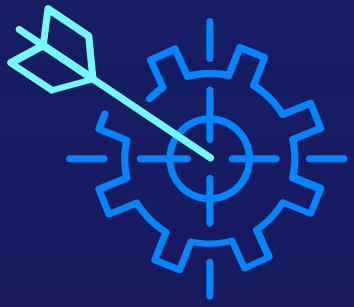
В целом же в топе доменных зон, используемых для фишинга, ориентированного на российскую аудиторию, остаются .COM, .RU, .SITE, .XYZ.

Выводы

- События, не оставляющие следов внутри инфраструктуры компании и зарождающиеся за ее пределами, могут наносить реальный ущерб. Чаще всего подобные инциденты влекут за собой комбинированные негативные последствия, выражающиеся в прямом или косвенном финансовом ущербе, репутационных рисках или санкциях со стороны регуляторов. Любой достаточно крупный инцидент в наши дни становится достоянием общественности и остается пятном на репутации организации.

- Задачи по самостоятельному мониторингу Глобальной сети и обнаружению признаков самых разноплановых угроз крайне сложны и труднореализуемы силами какой-то одной организации, так как требуют сочетания усилий работающего в режиме 24/7 коллектива высококвалифицированных аналитиков и целого комплекса разнообразных узкоспециализированных программных инструментов, многие из которых недоступны на широком рынке. Задача осложняется и тем, что для эффективного обнаружения признаков внешних инцидентов необходимо иметь доступ к всевозможным информационным источникам, перечень которых должен корректироваться и актуализироваться ежедневно.

- Сервис мониторинга внешних цифровых угроз Solar AURA компании «РТК-Солар» призван решить эти проблемы. Благодаря широкому функционалу решения и многовекторному мониторингу, компании станет доступен максимально полный набор данных, которые в Сети может найти потенциальный киберпреступник, и на их основе построить надежную ИБ-защиту.



Ростелеком
Солар

rt.ru
rt-solar.ru

Email:
solar@rt-solar.ru

Телефон:
+7 (499) 755-07-70

Устойчивость криминальных схем

Западные санкции и уход из России платежных систем Visa и Mastercard ударили в том числе и по киберпреступникам, нарушив привычные и хорошо отлаженные схемы вывода похищенных денег и оплаты зарубежных сервисов. В итоге в марте 2022 года количество фишинговых атак и кибермошенничеств **сократилось на 85%** по сравнению с показателями января-февраля того же года.

Но всего **за месяц** злоумышленники смогли перестроить схемы работы, адаптировав их к новым условиям. И к середине апреля количество фишинговых атак и социальных мошенничеств вернулось к прежним показателям.

Сейчас, в апреле 2023 года, количество подобных инцидентов на **26%** превышает показатели аналогичного периода 2022 года.