SOLAR

ОТЧЕТ

КЛЮЧЕВЫЕ ВНЕШНИЕ ЦИФРОВЫЕ УГРОЗЫ

для российских компаний в 2023 году

W: RT-SOLAR.RU

МОСКВА 2024

СОДЕРЖАНИЕ

ОБ ОТЧЕТЕ

Отчет составлен на основе данных DRP-сервиса мониторинга внешних цифровых угроз Solar AURA ГК «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)

2500

Telegram-каналов противоправной тематики и даркнет-форумов

50 МЛН

DNS-запросов в сутки

Отчетный период включает январь – декабрь 2023 года.

О СЕРВИСЕ SOLAR AURA

Сервис Solar AURA содержит 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 ее 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

Всего за год было выставлено на продаже в даркнете 1844 российские компании, при этом число подобных объявлений в сравнении с 2022 годом выросло на 42%

- Прошедший 2023 год стал рекордным по уровню фишинговой активности и количеству утечек данных. На протяжении всего года сервис Solar AURA регистрировал и обрабатывал десятки инцидентов ежедневно.
- Злоумышленники для проведения фишинговых атак стали чаще использовать домены второго и третьего уровня – причем домены второго уровня не связаны ни с каким популярным брендом, из-за чего теперь их невозможно найти автоматизированными средствами обнаружения.
- Больше всего фишинговых сайтов было найдено в сфере электронной коммерции, на втором месте – кредитно-банковская отрасль.
- В 2023 году начался резкий рост фишинговых атак на продавцов маркетплейсов с целью получить доступ в личный кабинет предпринимателя на торговых онлайн-площадках.
- Самые популярные фишинговые атаки в 2023 году – взлом соцсетей и мессенджеров, фейковые акции от популярных брендов и банковский фишинг.
- Сферы услуг и электронной коммерции стали лидерами по утечкам – отчасти это связано со слабой защищенностью отраслей ввиду того, что на протяжении долгого времени злоумышленники не интересовались данными секторами.

13 ТЫС.

предложений нелегальных услуг было найдено в даркнете и Telegram-каналах. Больше всего злоумышленники интересовались предложениями по продаже аккаунтов, пробиву данных и вербовке сотрудников для совершения кибератак на крупные российские организации и ведомства.

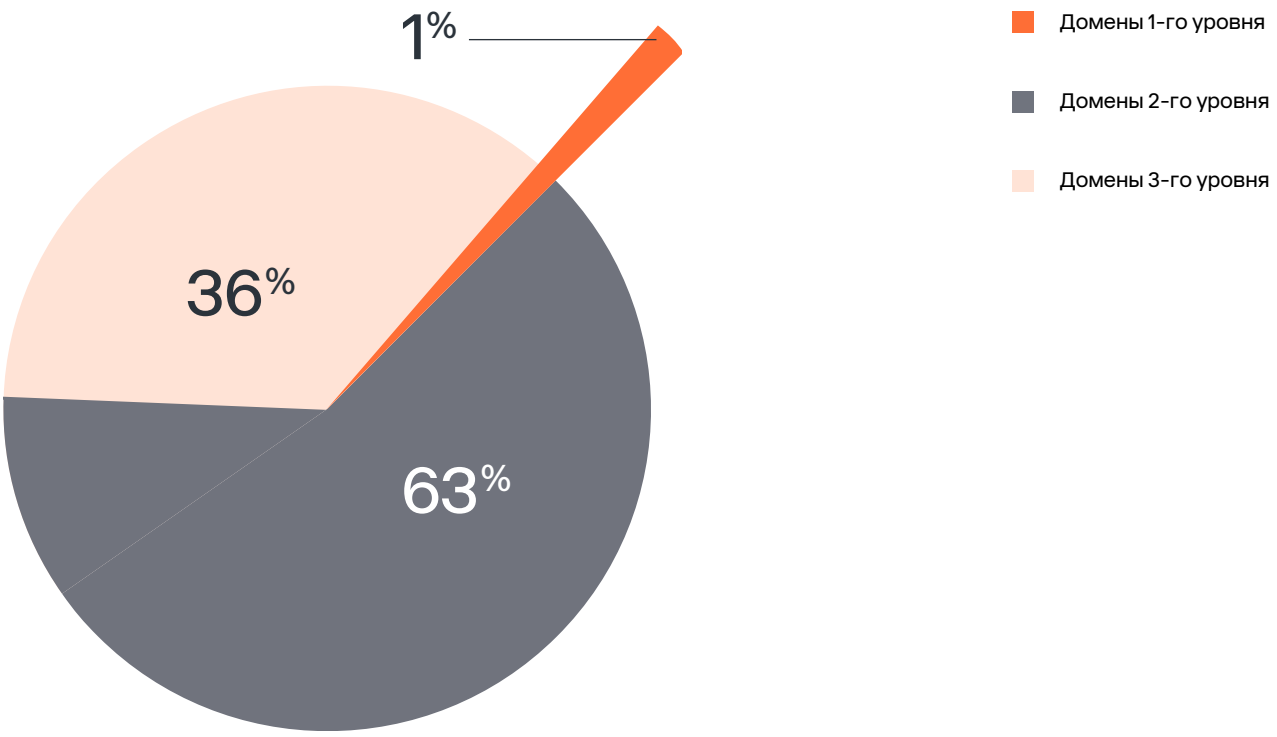
АНТИФИШИНГ

В течение 2023 года было выявлено более 40 тысяч доменных имен и веб-ресурсов, которые потенциально могут использовать популярные российские бренды для организации фишинговых атак. Подтвержденные факты фишинга были отмечены в 17% случаев. Рост числа выявленных фишинговых ресурсов составил 21% по сравнению с 2022 годом.

Любопытной особенностью последнего времени является то, что количество фишинговых доменов третьего уровня, которые невозможно обнаружить обычными автоматизированными средствами поиска, вплотную приблизилось к количеству доменов второго уровня.

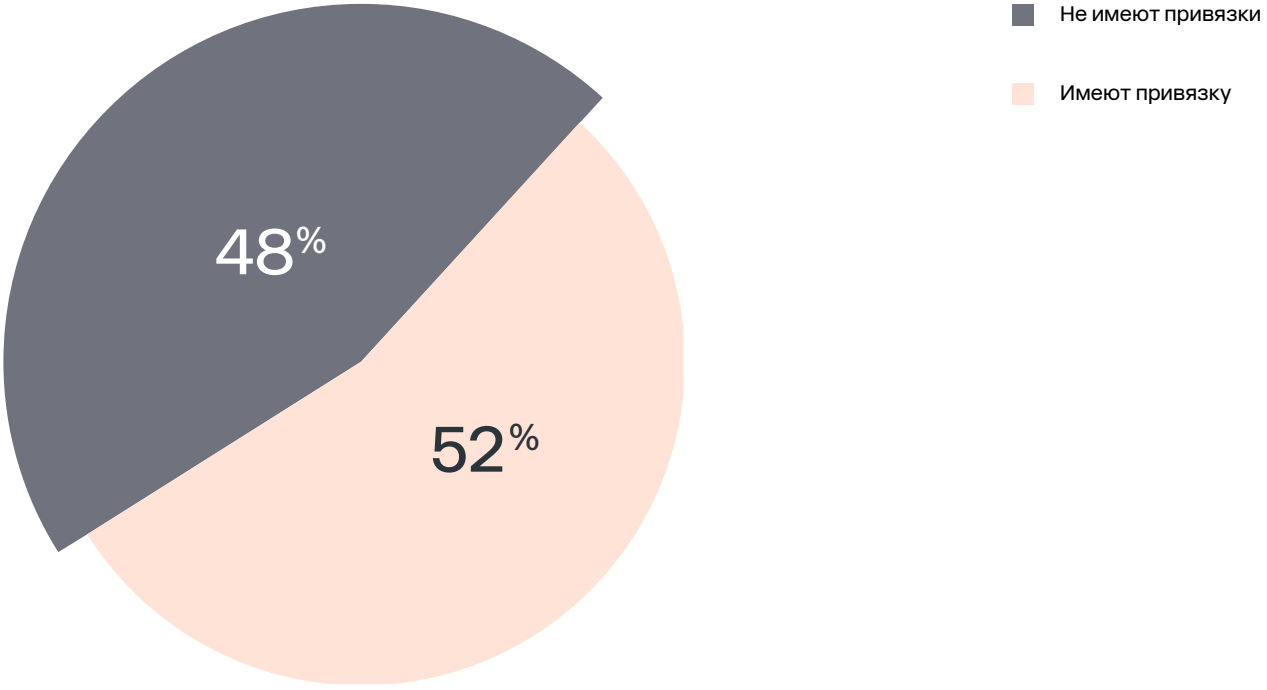
Это обусловлено массовостью и популярностью таких фишинговых схем, как «Хамелеон 2.0», а также широким распространением мошенничеств на маркетплейсах. Подобные сценарии зачастую используют в рамках одной атаки десятки, а то и сотни доменов второго уровня, каждый из которых содержит десятки поддоменов – это позволяет схеме работать беспрерывно даже в случае блокировки большинства доменов.

Распределение доменов для фишинговых атак, 2023 год



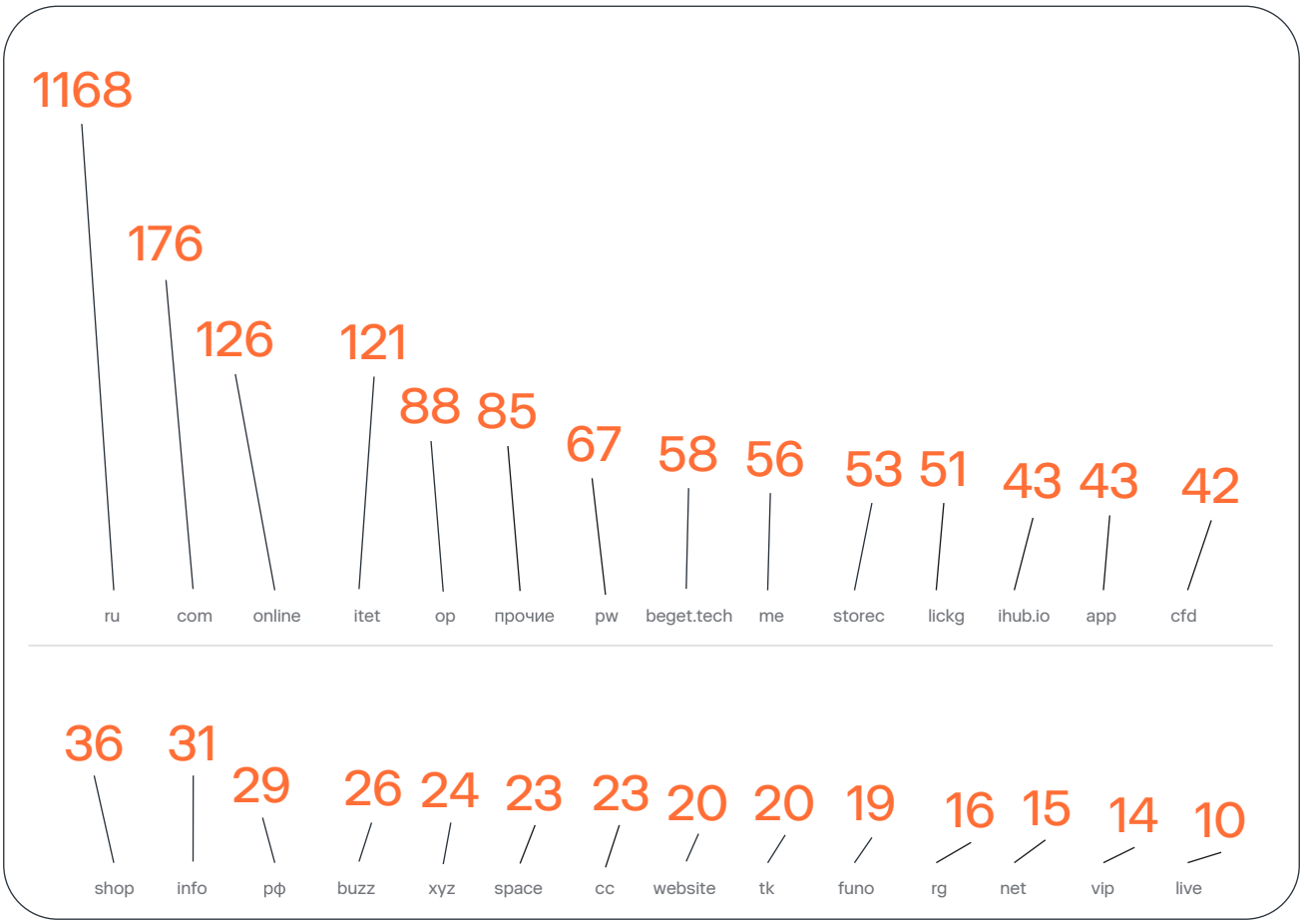
При этом 48% доменов второго уровня не связаны ни с каким брендом или вовсе сгенерированы случайно, что не позволяет искать их по автоматическим шаблонам и требует применения продвинутых механизмов мониторинга и возможностей киберразведки.

Привязка к бренду



Анализ последних 2500 заблокированных сервисом Solar AURA фишинговых ресурсов показал, что 46% сайтов располагались в зоне .RU, второе, третье и четвертое места с большим отрывом поделили доменные зоны .COM, .ONLINE и .SITE

Доменные зоны заблокированных фишинговых ресурсов



САМЫЕ ПОПУЛЯРНЫЕ ФИШИНГОВЫЕ АТАКИ 2023 ГОДА

Взлом соцсетей и мессенджеров. Фишинговые сайты используют различные информационные поводы для привлечения потенциальных жертв: от онлайн-голосования за детские рисунки в конкурсах или подписания петиции до получения бесплатного premium-аккаунта или социальных выплат. Как только пользователь заходит по фишинговой ссылке из рассылки, ему предлагается авторизоваться через социальные сети, такие как Telegram, WhatsApp, «ВКонтакте». После авторизации злоумышленники получают доступ к аккаунту и начинают рассылать вредоносные сообщения его контактам.

Фейковые акции и опросы от различных брендов. Популярная схема, основанная на сценарии «Хамелеон 2.0». Как правило, «приманка» представляет собой предложение в соцсети или мессенджере получить подарок от известного бренда — для этого ему необходимо поделиться информацией о розыгрыше с друзьями. При этом 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 или акцией. При этом цепочка редиректов постоянно меняется, а фишинговый сайт откроется лишь тому, кто попадет на него через переадресацию с одного из промежуточных ресурсов.

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. Если раньше фейковый сайт банка пытался выведать у жертвы номер банковской карты и код из СМС для единичного списания денег или оформления платной подписки, то теперь в большинстве случаев помимо номера карты от жертвы требуется ввести номер телефона или другую информацию, которая может послужить входом в личный кабинет клиента банка. При этом сам код из СМС-сообщения нужен уже не для подтверждения покупки, а для входа в ЛК или изменения пароля. Соответственно, растут и риски для клиентов банка — получив доступ в личный кабинет, злоумышленники могут свободно распоряжаться всеми счетами жертвы и даже оформлять на ее имя кредит.

Наиболее подверженной фишинговым атакам отраслью в 2023 году стала электронная коммерция — на эту отрасль пришлось 17,4% от общего числа выявленных фишинговых ресурсов.

Также в 2023 году наблюдался резкий рост атак на продавцов маркетплейсов. С середины июля прошлого года мы фиксируем массовое появление фейковых сайтов, целью которых является получение неправомерного доступа в личный кабинет продавца на крупных торговых площадках. Данная тенденция продолжается и в 2024 году — новые фейковые сайты появляются каждый день, причем характер атак свидетельствует о том, что все они являются делом рук одной преступной группы.

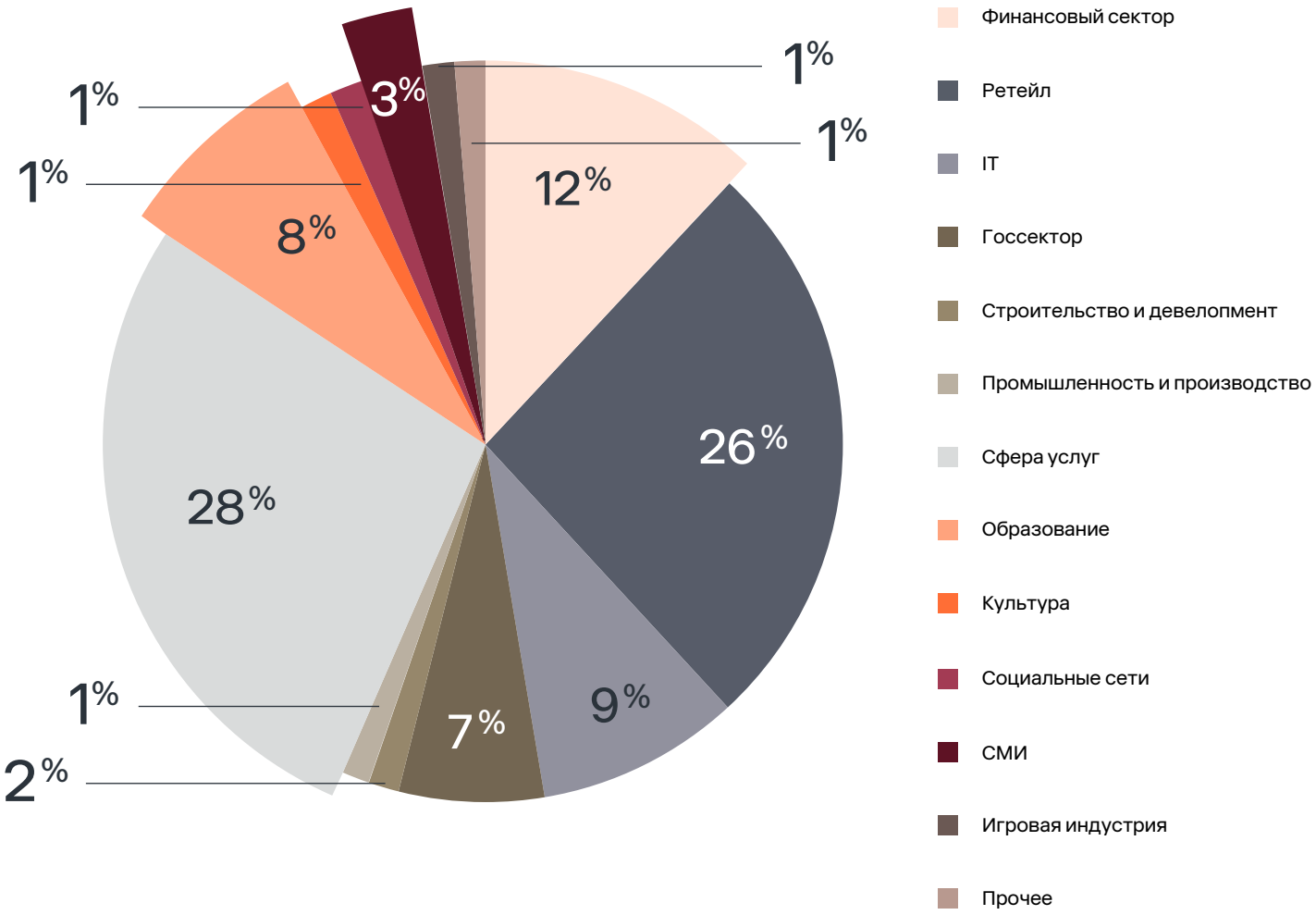
На втором месте по числу фишинговых ресурсов расположилась кредитно-финансовая сфера. В 2023 году в этой отрасли основной акцент злоумышленников сместился с получения данных банковской карты на получение доступа в личный кабинет клиента банка. При этом 8% выявленных фишинговых сайтов в банковском секторе использовались для распространения вредоносного программного обеспечения — программ удаленного администрирования компьютера, закамуфлированных под программы техподдержки банка. Такого рода сайты в последние годы активно используют телефонные мошенники.

УТЕЧКИ ДАННЫХ

В минувшем году нами было зафиксировано 420 инцидентов, связанных с утечками конфиденциальной информации российских компаний в формате баз данных.

Безусловными лидерами по количеству инцидентов являются представители электронной коммерции и сферы услуг (83 и 89 инцидентов соответственно), что обусловлено большим количеством организаций и слабой защищенностью в среднем по данным отраслям, так как на протяжении долгого времени подобные организации были мало интересны злоумышленникам.

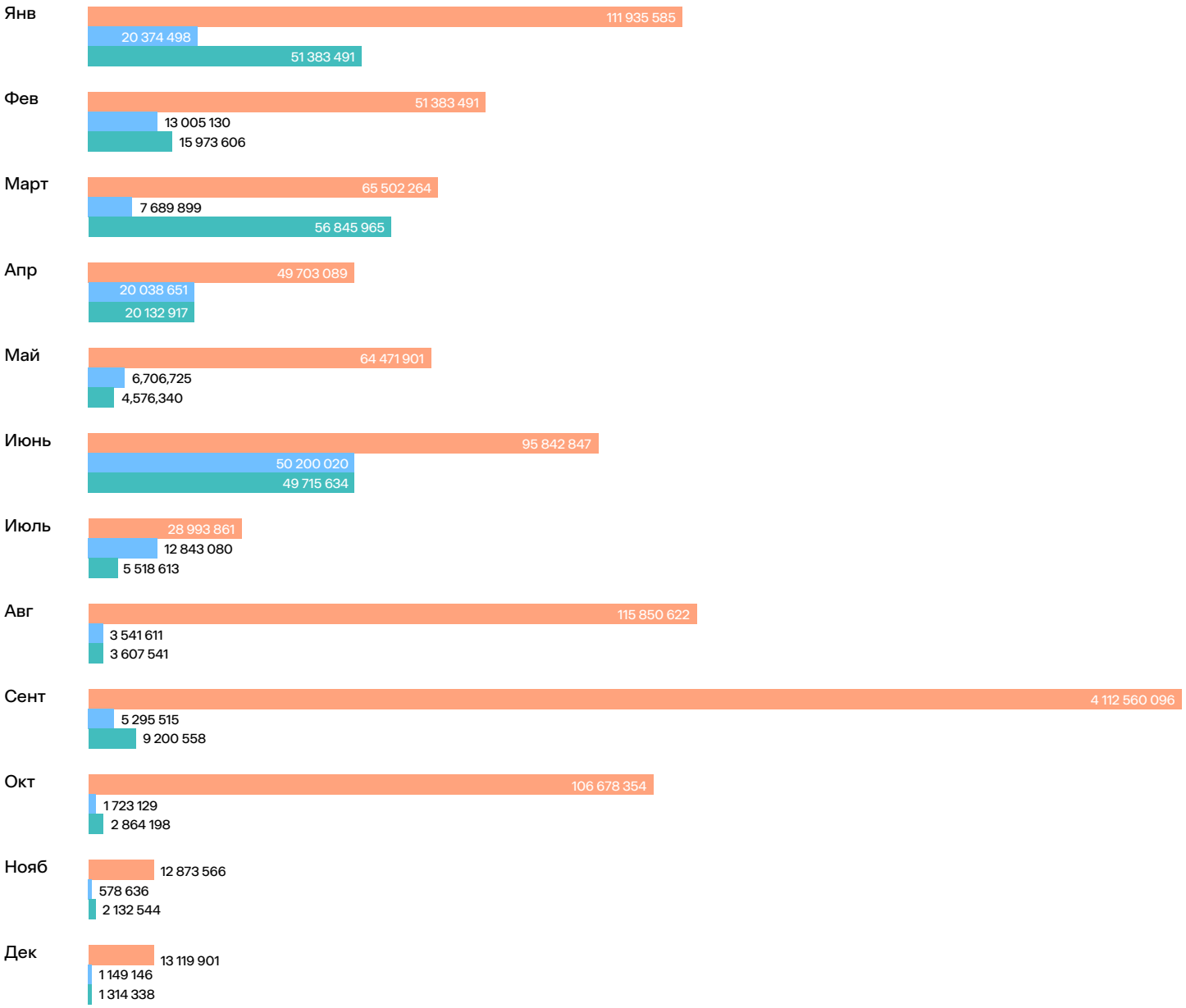
Распределение инцидентов по отраслям



Общий объем утекших данных оценивается в 103,4 терабайта.

Попавшие в общий доступ базы данных совокупно содержат 4,8 миллиарда строк, в том числе 225 миллионов номеров телефонов и 145 миллионов адресов электронной почты.

Российские утечки по месяцам: строки, почты, телефоны



В рамках работы с текущими клиентами и пилотных проектов сервисом в различных внешних источниках было зафиксировано 1976 инцидентов, связанных с попаданием в открытый доступ конфиденциальной информации о компаниях, являющихся клиентами Solar AURA. Речь идет как об обнаружении единичных документов или их массивов, так и о случаях, когда данные сотрудников организации фигурировали в сторонних утечках данных.

Также анализ публичных утечек за последние 6 лет позволил выявить 94 тысячи скомпрометированных и потенциально скомпрометированных корпоративных аккаунтов, имеющих отношение к нашим заказчикам и компаниям, для которых осуществлялось пилотное подключение в 2023 году. Отметим, что резкий рост числа этих скомпрометированных аккаунтов начался именно после начала СВО.

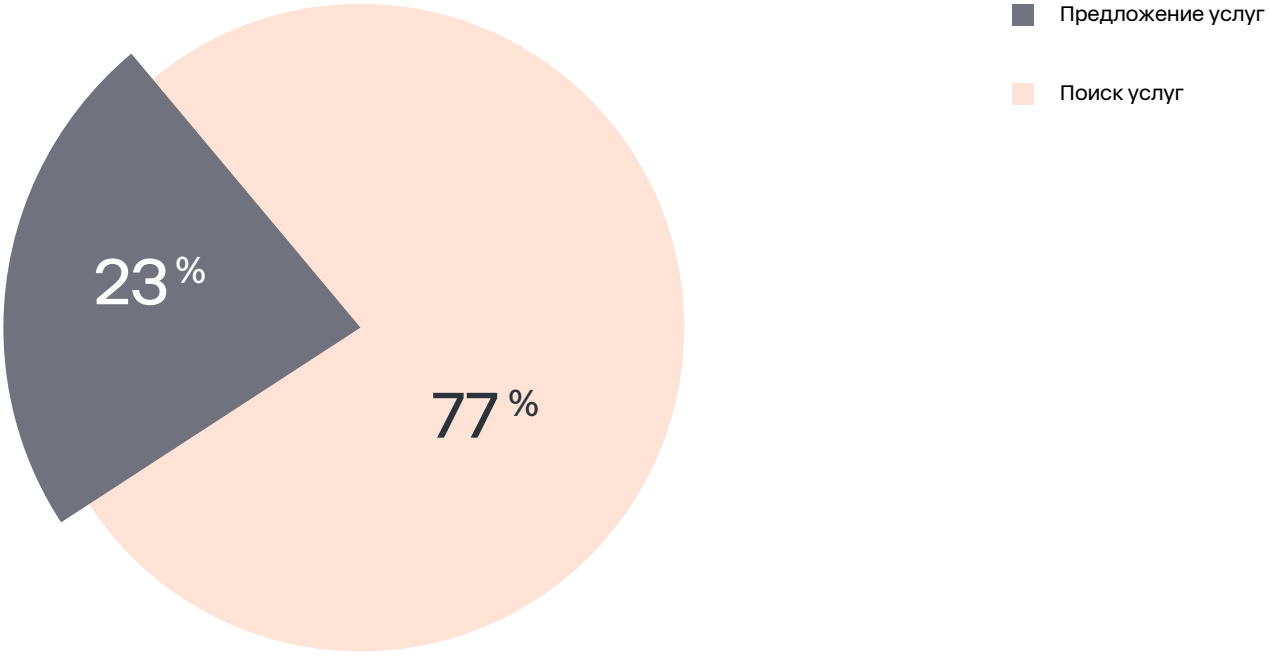
НЕЛЕГАЛЬНЫЕ УСЛУГИ

В ходе мониторинга даркнета и Telegram-каналов в поле зрения сервиса попало 13,3 тысячи объявлений с предложением различного рода нелегальных услуг (продажа взломанных аккаунтов, и продажа продукции в обход официальных каналов и т. д.).

На первом месте по уровню интереса со стороны злоумышленников располагается государственный сектор – на него пришлось 5089 инцидентов. Ключевые векторы: продажа аккаунтов, пробив данных, вербовка сотрудников.

На втором месте финансовый сектор – 4170 публикаций. Первые два места по услугам заняли продажа банковских карт и доступов в личный кабинет клиента банка, а также помощь в оформлении банковских счетов без визита в банк.

Привязка к бренду



ИНТЕРНЕТ-ЭКВАЙРИНГ

В 2023 году сервис Solar AURA зафиксировал 5376 вредоносных интернет-ресурсов, принимающих электронную оплату от своих пользователей. В целом в копилке сервиса имеются сведения о 13 тысячах банковских карт и мерчантов, задействованных в противоправной активности.

Большинство выявляемых сервисом сайтов связано с незаконным игорным бизнесом (96%), оставшиеся 4% приходятся на фишинг, различного рода мошеннические ресурсы, а также фейковые криптообменники.

Выявленные ресурсы можно разделить на две категории:

12%

инцидентов – сайты, использующие интернет-эквайринг для приема платежей от клиентов

88%

инцидентов – сайты, использующие карты дропов для приема платежей

Процесс работы с картами дропов автоматизирован: для этого используются автоматизированные «карусели» – платежные шлюзы, выдающие клиенту из имеющейся базы индивидуальную карту под конкретную транзакцию. Популярность данного метода проведения операций объясняется его технической простотой и отсутствием необходимости регистрации или покупки номинального бизнеса под интернет-эквайринг. Кроме того, если банк заметит подозрительную активность и заблокирует карту, это не вызовет остановки бизнеса, в отличие от отключения интернет-эквайринга.

ЮРИДИЧЕСКИЕ ЛИЦА

Фирма-однодневка легко вычисляется, ее обнаружит любая, даже самая поверхностная проверка, поэтому в трендах черного рынка – покупка готовых юридических лиц под нелегальную активность (фейковое партнерство, обналичивание и отмывание средств и т. д.). Именно поэтому эксперты Solar AURA отслеживают объявления о продаже компаний и формируют базу потенциально неблагонадежных контрагентов. Опасность таких компаний заключается в том, что при внешней благонадежности, например отличных финансовых и иных показателях, взаимодействие с ними может нести серьезные риски для бизнеса.

В 2023 году нами в России было обнаружено 1844 выставленных на продажу организаций на черном рынке, а это – 5 компаний в день. Также это подтверждает тенденцию к увеличению числа продаваемых компаний, число подобных объявлений увеличилось на 42% по сравнению с 2022 годом. Полученные сведения используются заказчиками при проверке контрагентов и планировании сделок, что позволяет им выявить скрытые риски и снизить вероятность наступления негативных последствий. На сегодняшний день общая база сервиса насчитывает сведения о 6781 организации, которые были выставлены на продажу на черном рынке за последние пять лет.

Уникальность данного инструмента заключается в том, что он дает возможность выявлять скрытые факторы риска, не учитываемые традиционными инструментами проверки контрагентов. Зачастую продаваемые компании имеют безупречную репутацию и хорошую финансовую отчетность, что позволяет им без проблем проходить комплайенс-проверки, в то же время факт продажи организации в даркнете или Telegram является своеобразным «скелетом в шкафу» и зачастую свидетельствует о том, что дела у организации не так уж хороши, как это выглядит на бумаге.

Для чего же используются такого рода компании и какие риски могут возникать, если вступить с ними в деловые отношения? Сценариев достаточно много. Во-первых, подобные фирмы используются для обналичивания или отмывания денежных средств – во многих случаях компании продаются вместе с банковскими счетами и номинальным генеральным директором, что несет риски для банков, обслуживающих продаваемые таким способом организации. Во-вторых, компании могут быть задействованы в атаках на цепочки поставок или сценариях, связанных с ложным партнерством. В-третьих, это различные варианты на тему фирм-однодневок, только куда опаснее, ведь появившаяся неделю назад компания, желающая стать контрагентом, сразу же станет красным маячком в глазах любого специалиста в области экономической безопасности, а вот тайно купленная организация с многолетней историей может и не вызвать подозрений.

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 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 всевозможных 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 разного рода информационным источникам, перечень которых должен корректироваться и актуализироваться ежедневно.

Сервис Solar AURA компании ГК «Солар», являясь сервисом полного цикла, сочетающим в себе мониторинг, работу с источниками, классификацию событий, оповещение и реагирование, призван решить все эти задачи.

SOLAR

W: RT-SOLAR.RU
W: RT.RU

T +7 (499) 755-07-70
E solar@rt-solar.ru

Центральный офис, 125009, Москва,
Никитский переулок, 7с1