

Исследователи фиксируют 230% рост предложений за последний год.

По информации компании Resecurity – это компания, которая занимается информационной безопасностью. Она предоставляет решения для защиты от цифровых угроз и кибератак, а также помогает компаниям и организациям сохранять конфиденциальность информации. Компания предлагают ряд услуг, таких как мониторинг угроз, обнаружение инцидентов, анализ и реагирование на киберугрозы." data-html="true" data-original-title="Resecurity" >Resecurity, специализирующейся на кибербезопасности, количество предложений украденных личных данных жителей Сингапура увеличилось на 230% за последний год. Эти данные, продающиеся на даркнет-площадках, активно используются для мошенничества, включая создание поддельных документов и Deepfake – это технология, использующая глубокое обучение для создания фотографий и видео с искусственно созданными лицами и голосами. В частности, можно вставить лицо известного человека в видео или изменить голос в аудиозаписи. Такая технология может использоваться для создания шоу и комедий, однако она также может применяться для распространения ложной информации и дезинформации." data-html="true" data-original-title="Deepfake" >deepfake-контента.

В апреле этого года было зафиксировано рекордное количество новых утечек, когда тысячи записей сингапурцев оказались в продаже на тёмных форумах. Помимо простого мошенничества, эти данные также могут использоваться иностранными правительствами для сбора разведывательной информации.

Одним из основных источников этих утечек является известный подпольный форум XSS. Анализ Resecurity показывает, что многие утечки данных не были обнародованы пострадавшими организациями, в результате чего потерпевшие лица оставались неосведомлёнными о компрометации своих документов. Киберпреступники также торгуют шаблонами поддельных документов, которые крайне трудно отличить от настоящих благодаря внедрению сложных защитных элементов, таких как голограммы.

На тёмных площадках также выявлены аккаунты Singpass (Сингпасс) – это электронная система идентификации и аутентификации, используемая в Сингапуре. Она предоставляет гражданам, резидентам и предпринимателям удобный и безопасный способ получения доступа к различным государственным онлайн-службам и приложениям." data-html="true" data-original-title="Singpass" >Singpass — системы, обеспечивающей доступ к услугам правительства и частного сектора в Сингапуре. Несмотря на использование двухфакторной аутентификации, уязвимости в процессах Проверка KYC (Know Your Customer) – это процесс, который финансовые учреждения, компании и организации осуществляют для идентификации и верификации своих

клиентов. Целью этой процедуры является предотвращение финансовых преступлений, таких как отмывание денег, финансирование терроризма и мошенничество.

 В рамках проверки KYC клиент обязан предоставить определенные документы и информацию, которые позволят установить его личность и подтвердить его законность и надежность как потенциального клиента. Это могут быть паспортные данные, адрес проживания, реквизиты банковских счетов и другая информация, зависящая от требований конкретной компании или законодательства." data-html="true" data-original-title="KYC" >KYC часто эксплуатируются с участием инсайдеров, что приводит к мошенничеству, отмыванию денег и краже личности.

Только в июне 2024 года было обнаружено 2377 скомпрометированных аккаунтов Singpass, о чём компания Resecurity самостоятельно уведомила пострадавших. Основной причиной компрометации являются программы-вымогатели, похищающие информацию.

Для минимизации рисков жителям Сингапура рекомендуется немедленно сообщать о краже своих аккаунтов Singpass, активировать двухфакторную аутентификацию, регулярно менять пароли и внимательно следить за активностью своих аккаунтов. Компаниям, в свою очередь, следует разработать и реализовать более мощные программы защиты цифровой идентификации для обеспечения безопасности сотрудников и клиентов от захвата аккаунтов и кражи личности.

На перекрестке науки и фантазии — наш канал