ступлений, которые автоматизированы и происходят полностью в виртуальной среде.

Пользователи-люди часто представляют собой самое слабое звено в компьютерной безопасности, и их слабости, в зависимости от типа киберпреступности, могут использоваться различными способами, превращая жертв в инструменты собственной виктимизации. Средства эксплуатации включают социальную инженерию и обман, манипулирование процессами принятия решений посредством предполагаемой срочности или авторитета, а также использование предсказуемых привычек, связанных с использованием веб-сайтов, паролей, загрузками и социальными или профессиональными сетями. Таким образом, жертвы могут винить себя или испытывать вину со стороны других, помимо потенциально разрушительных последствий, таких как финансовые потери или ущерб репутации и карьере.

Жертвы киберпреступлений могут страдать от долгосрочных психологических и эмоциональных последствий, включая посттравматическое стрессовое расстройство (ПТСР), с соответствующими последствиями для физического здоровья. Жертвы также могут чувствовать стыд или оскорбление ввиду вторжения в их частную жизнь или переживать разрыв отношений из-за финансовых потерь, утечки информации, сексуального вымогательства или мошенничества при использовании ресурсов знакомств.

Сексуальная эксплуатация в Интернете и торговля людьми являются другими примерами серьезных преступлений, увеличению и развитию которых способствовал Интернет, поскольку преступники могут легче получить доступ к жертвам и вербовать других правонарушителей, анонимно распространять материалы и получать доступ к гораздо большему числу потенциальных клиентов, что приводит к способствованию совершению этих преступлений.

Таким образом, можно сформулировать основные тезисы, необходимые при раскрытии и расследовании киберпреступлений.

1. Из-за ощущения анонимности и удаленности от офлайн-мира пользователи Интернета испытывают ложное чувство безопасности, а онлайн-преступники психологически, социально и физически отдаляются от своих преступлений и жертв, сталкиваются с меньшим количеством и / или менее серьезными последствиями своего поведения.

2. Жертвы киберпреступлений занижают информацию о своей виктимизации по сравнению с традиционными преступлениями, что, как предполагается, связано с предполагаемым недостатком понимания и готовности в полиции, и как жертвы, так и полиция выражают замешательство по поводу того, в какую организацию следует сообщать.

3. Обучение для повышения уровня знаний и предоставления стандартизированных ответов на сообщения о киберпреступлениях, а также более активное участие общественности и размещение обучающих материалов на большинстве посещаемых ресурсов могут помочь улучшить качество противодействия подобным преступлениям и защищенность граждан.

4. Расширение знаний о киберпреступлениях и причастных к ним лицах может также повысить готовность к расследованиям и повысить способность сопереживать жертвам и подозреваемым, чтобы получить лучшие результаты на допросе, генерировать более точные версии и выявлять соответствующие доказательства.

Шерстяных А.С.,

кандидат технических наук, доцент
Сибирский юридический институт МВД России (г. Красноярск)

Браузерные расширения – киберугроза 2023 года

Многие из нас помнят время, когда для того, чтобы просматривать видео, слушать музыку или общаться с друзьями, требовалось специальное программное обеспечение. Сейчас для этого достаточно иметь браузер. Чем больше информации люди передают через браузер, тем более он привлекателен для мошенников. Вмешаться в работу браузера можно разными способами. Один из них – браузерные расширения.

Поскольку у браузерных расширений достаточно широкие полномочия, они могут иметь доступ к данным, которыми обмениваются пользователь и сайт (следить за действиями пользователя, собирать и / или воровать чувствительную информацию), могут влиять на отображение страниц (например, добавлять или изменять содержимое), подменять запрашиваемую страницу собственной (фишинговой или рекламной), подменять ссылки в поисковой выдаче (вставлять в верхние позиции нужные злоумышленнику ресурсы) и др. При этом данный класс программ не вмешивается в работу операционной системы (все действия происходят внутри браузера), поэтому вполне возможно, что на него не отреагирует обычная система антивирусной защиты.

Поговорим о самых нашумевших случаях 2023 года, когда пользователи сталкивались с опасными вредоносными расширениями. Один из них – расширения с названием SearchBlox, RoFinder и RoTracker (размещались в Chrome Web Store) для игроков Roblox[1]. Официально они были предназначены для поиска любого игрока на серверах Roblox. На самом деле с их помощью злоумышленники воровали аккаунты игроков и, как следствие, все, чем они владели внутри игры. Только после соответствующих публикаций на Bleeping Computers (известный сайт о кибербезопасности) эти расширения были убраны из Chrome Web Store и также автоматически удалены с устройств тех пользователей, которые их установили.

В марте 2023 года в том же Chrome Web Store были обнаружены два опасных расширения, связанных с ChatGPT (ChatGPT For Google и Quick access to Chat GPT). Оба расширения позволяли общаться с ChatGPT, но основной задачей была кража сессионных куки-файлов Facebook. При этом для популяризации своего расширения злоумышленники использовали рекламу в Facebook, которую оплатили за счет тех угнанных аккаунтов.

В 2023 году в официальном магазине расширений для браузера Google Chrome Web Store были обнаружены несколько десятков опасных плагинов (суммарная загрузка из магазина превысила 87 млн раз)[2]. Эти браузерные расширения носили различную направленность: расширения для работы с сервисом YouTube, PDF-конвертеры, переводчики, блокировщики рекламы, VPN и прочее.

Кроме размещения на официальных площадках, злоумышленники распространяют опасные плагины под видом различного пиратского контента: музыки, фильмов, взломанных игр и др.

Например, в начале 2023 года исследователи обратили внимание на активность зловреда ChromeLoader[3]. Этот троян является перехватчиком браузера и позволяет злоумышленникам организовать подмену поисковой выдачи таким образом, чтобы на первых страницах отображались ссылки на фишинговые страницы в зависимости от запроса пользователя. Это могут быть мошеннические розыгрыши призов, фейковые сайты знакомств, фишинговые страницы маркет-плейсов и т.п.

Внимательный пользователь, скорее всего, может заподозрить, что с поисковой выдачей что-то происходит. Но избавиться от опасного браузерного расширения простым удалением не получится. Дело в том, что ChromeLoader добавляет автоматическую установку браузерного расширения при каждой перезагрузке системы (вмешиваясь в работу планировщика заданий Windows).

Помимо всего прочего, кибермошенники не смогли обойти вниманием и операции с криптовалютой. В апреле 2023 года впервые было обнаружено опасное расширение Rilide[4], позволяющего злоумышленникам следить за действиями пользователя зараженного браузера в Интернете. В случае если жертва заходит на сайты, связанные с криптовалютой (либо из списка, заданного

[1] Опасные браузерные расширения // Kaspersky daily : официальный сайт. URL: https://www.kaspersky.ru/blog/dangerous-browser-extensions-2023/36712/ (дата обращения: 03.01.2024).

[2] Десятки вредоносных расширений в Chrome Web Store // Kaspersky daily : официальный сайт. URL: https://www.kaspersky.ru/blog/dangerous-chrome-extensions-87-million/35676/ (дата обращения: 03.01.2024).

[3] Перехватчик браузеров ChromeLoader атакует пользователей по всему миру // Securitylab.ru : сайт. URL: https://www.securitylab.ru/news/531889.php (дата обращения: 07.02.2024).

[4] Вредонос Rilide ориентирован на Chromium-браузеры // Xakep.ru : сайт. URL: https://xakep.ru/2023/04/05/rilide/ (дата обращения: 07.02.2024).

злоумышленниками), Rilide копирует конфиденциальную информацию. Расширение также содержит код, который позволяет генерировать поддельную страницу для ввода кода подтверждения криптовалютной транзакции (что позволяет злоумышленникам обойти двухфакторную аутентификацию). При этом кошелек получателя криптовалюты подменяется кошельком мошенников. Благодаря украденному коду-подтверждению оператор расширения Rilide может подтвердить транзакцию от имени пользователя. Также зловред способен вмешиваться в работу электронного ящика жертвы, скрывая оповещение по e-mail о выводе средств.

Кроме того, указанное расширение собирает и отправляет оператору историю браузера (включая куки-файлы), а также (по команде злоумышленников) может сделать и отправить снимки экрана.

Вредоносное расширение маскируется под обычное браузерное расширение для Google-диска и может быть встроено в браузеры Opera, Edge, Chrome и Brave.

Способов распространения этого опасного расширения обнаружено достаточно много – от вредоносных сайтов и электронных писем до зараженных установщиков криптоигр. Одним из наиболее интересных является распространение поддельной PowerPoint-презентации, созданной для сотрудников Zendesk. Презентация представляла собой предупреждение о безопасности, но на самом деле являлась пошаговой инструкцией по установке браузерного расширения Rilide.

Также в прошлом году стало известно об опасном расширении для браузеров Google Chrome, Microsoft Edge, а также южнокорейского браузера Naver Whale, позволяющего злоумышленникам читать переписку пользователей почтовой службы Gmail[1].

Все это говорит о том, что даже официальные площадки не являются абсолютно надежными. Для того чтобы модераторы заметили опасные расширения и убрали их из магазина, как правило, не достаточно отзывов пользователей. Чаще всего необходимы публикации исследователей безопасности, и лучше на крупном медиаресурсе.

Для того чтобы не попасться на уловку мошенников, не спешите устанавливать новые плагины. Если все же решили установить, то делайте это с официального сайта (там хотя бы есть служба безопасности), предварительно прочитав отзывы (бдительные граждане могут вас предупредить, что с плагином что-то не так). Хоть иногда просматривайте список установленных расширений и удаляйте ненужные (особенно если не можете вспомнить, что его устанавливали). И обязательно используйте надежную защиту на всех ваших устройствах.

Ущекин С.Н.

Академия управления МВД России (г. Москва)

Виды виктимности жертв хищений, совершаемых с использованием электронных средств платежа

В настоящее время, в период активного развития современного общества, отмечается явная тенденция к цифровизации экономических отношений. Этот процесс привлекает особое внимание научного сообщества, которое придает большую значимость изучению и анализу данной тенденции. В связи с этим возрастает интерес к проблеме роста качественных и количественных показателей преступности, связанной с использованием информационных технологий.

Исследователи обращают внимание на появление новых разновидностей средств платежа, которые, в свою очередь, становятся потенциальной угрозой для совершения хищения чужого имущества. Это вызы-

[1] Joint Cyber Security Advisory // The German domestic in-tel-li-gence ser-vices : сайт. URL: https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/prevention/2023-03-20-joint-cyber-security-advisory-korean.html (дата обращения: 03.01.2024).