Столыпинский вестник

Научная статья
Original article
УДК 004.424

ШПИОНСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

SPY SOFTWARE SPY SOFTWARE

Крыгин Никита Дмитриевич, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), krigginnn@rambler.ru

Krygin Nikita Dmitrievich, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), krigginnn@rambler.ru

Аннотации: Шпионское ПО — это тип вредоносного ПО, которое регистрирует информацию о пользователе вычислительного устройства и передает ее третьим лицам.

Annotations: Spyware is a type of malware that logs information about the user of a computing device and shares it with third parties.

Ключевые слова: шпионское ПО, уязвимость, информационная безопасность, злоумышленник.

Key words: spyware, vulnerability, information security, intruder.

Некоторые типы шпионских программ упакованы с, казалось бы, законными приложениями, установленными пользователем. Некоторые

вредоносные программы развертываются без ведома пользователя через вредоносные веб-сайты, зараженную электронную почту или другие методы, используемые другими типами вредоносных программ. Файлы cookie также могут служить одним из видов вредоносных программ, если они позволяют веб-сайтам отслеживать действия пользователя без его согласия или незаконным образом.

Удаление и предотвращение шпионских программ аналогичны другим типам вредоносных программ: пользователям следует избегать перехода по подозрительным ссылкам или посещения неизвестных веб-сайтов, а также следует установить защиту от вредоносных программ. Еще одной важной профилактической мерой для шпионского ПО являются решения для кибербезопасности, которые осуществляют мониторинг устройства в режиме реального времени для обнаружения сообщений, которые могут исходить от шпионского ПО.

Как шпионское ПО заражает устройства

Шпионское ПО использует различные методы, чтобы скрыть себя, чтобы оно могло работать, не предупреждая пользователя. Он часто скрыт на, казалось бы, законных веб-сайтах или в загрузках. Шпионское ПО может быть внедрено в легитимные программы и веб-сайты посредством эксплуатации без ведома поставщика исходного программного обеспечения или издателя веб-сайта. В других случаях поставщики вредоносного программного обеспечения или издатели веб-сайтов намеренно доставляют своим пользователям шпионское ПО.

Связанные пакеты программного обеспечения (известные как пакетное ПО) являются распространенным методом доставки шпионского ПО. В этом случае шпионское ПО намеренно прикрепляется к другим законным программам, которые пользователь загружает и устанавливает. Некоторые комплектные шпионские программы устанавливаются тайно, а в других случаях лицензионное соглашение может действительно упоминать шпионское ПО, но описывать его другими терминами. Это вынуждает

пользователей соглашаться на полный пакет, включающий шпионское ПО, тем самым заражая себя.

Шпионское ПО также может заражать пользовательские устройства теми же способами, что и другие типы вредоносных программ: например, когда пользователь посещает зараженный веб-сайт или открывает вредоносное вложение электронной почты.

Вредоносное рекламное ПО часто поставляется с бесплатными программами, условно-бесплатными программами и утилитами, которые загружаются из Интернета или автоматически устанавливаются, когда пользователь посещает зараженные веб-сайты. Он отображает нежелательную рекламу на устройстве пользователя и может замедлять или иным образом мешать работе устройства. В некоторых случаях отображаемая реклама содержит вредоносные ссылки, ведущие к развертыванию других типов вредоносных программ.

Интернет-куки

Файлы cookie, которые отслеживают и регистрируют личную информацию (PII) и привычки просмотра Интернета, являются одним из наиболее распространенных типов рекламного ПО. Рекламодатели могут использовать отслеживающие файлы cookie, чтобы отслеживать, какие веб-страницы посещают пользователи, чтобы нацеливать рекламу в маркетинговых кампаниях. В некоторых случаях рекламодатели могут отслеживать историю браузера и загрузок пользователя для отображения всплывающих окон или рекламных баннеров.

Поскольку данные, собранные шпионским ПО, часто продаются третьим лицам, для защиты личных данных посетителей веб-сайтов были приняты такие правила, как Общий регламент ЕС по защите данных (GDPR).

Клавиатурные регистраторы (кейлоггеры)

Кейлоггер — это тип шпионского ПО, используемого киберпреступниками для кражи персональных данных, учетных данных для входа и конфиденциальных корпоративных данных. Есть некоторые законные

пользователи клавиатурных шпионов — например, работодатели могут использовать клавиатурные шпионы для мониторинга компьютерной активности сотрудников, владельцы устройств могут использовать их для отслеживания нежелательной активности на своих собственных устройствах, или правоохранительные органы могут использовать их для расследования компьютерных преступлений.

Существует два основных типа кейлоггеров:

Аппаратный кейлоггер похож на флешку. Он действует как физический соединитель между компьютерной клавиатурой и компьютером, но помимо передачи сигналов клавиатуры на устройство, он сохраняет их или передает третьему лицу.

Программный кейлоггер — это программа, которая сохраняет или передает действия клавиатуры, не требуя физического доступа к устройству. Программные кейлоггеры могут быть преднамеренно установлены третьими лицами, заинтересованными в мониторинге устройства, или загружены пользователем по незнанию. В других случаях кейлоггеры развертываются как часть руткита или троянской программы, уже запущенной на устройстве.

Банковские трояны

Банковский троян — это тип шпионского ПО, которое получает доступ и записывает конфиденциальную информацию, обрабатываемую или хранящуюся в системах онлайн-банкинга. Обычно он маскируется под законное программное обеспечение при выполнении вредоносных действий, таких как:

Изменение веб-страниц на сайте онлайн-банкинга

Добавление транзакций в интересах злоумышленника

Изменение значений транзакций

Банковские трояны включают в себя бэкдор, который позволяет программе отправлять все собранные данные на удаленный сервер. Этот тип шпионского ПО часто нацелен на финансовые учреждения, такие как банки, брокерские конторы, поставщиков электронных кошельков и финансовые

онлайн-сервисы. Изощренный дизайн банковских троянов затрудняет их обнаружение даже самыми современными системами безопасности.

Мобильные шпионские программы опасны, потому что они могут быть доставлены с помощью SMS или MMS-сообщений и обычно не требуют взаимодействия с пользователем для развертывания на устройстве. Если смартфон или планшет заражен мобильным шпионским ПО, оно может выполнять ряд действий, в том числе:

Из-за личного характера мобильных устройств мобильные шпионские программы могут представлять серьезную опасность для конфиденциальности и личной безопасности пользователя. Например, преступники могут использовать его для вымогательства у пользователя или планирования других преступлений, таких как кража со взломом и физическое насилие.

Шпионское ПО является распространенной проблемой для пользователей Интернета. Если вы подозреваете, что устройство заражено, выполните следующие действия по устранению проблемы.

Если вы подозреваете, что настольный компьютер или ноутбук заражен шпионским ПО, попробуйте выполнить следующие действия:

Просканируйте устройство с помощью антивирусного программного обеспечения и, если угроза будет обнаружена, удалите ее.

Рассмотрите возможность развертывания антишпионского инструмента, который может постоянно контролировать систему и предотвращать доступ шпионских программ к личным данным владельца устройства или их изменение.

Удалить шпионское ПО с мобильного телефона

Если вы видите какие-либо признаки заражения мобильного телефона шпионским ПО, попробуйте выполнить следующие действия:

Удалите незнакомые приложения.

Просканируйте устройство с помощью мобильного приложения для защиты от вредоносных программ.

Если ничего не помогло, создайте резервную копию данных телефона и сбросьте настройки телефона до заводских.

Защита и предотвращение шпионского ПО

Следующие рекомендации могут помочь пользователям защитить свои устройства от шпионских программ:

Открывайте письма только из известных источников.

Скачивайте файлы только из надежных источников.

Просмотрите ссылки, прежде чем нажимать на них, наведя на них курсор, чтобы убедиться, что они верны.

Используйте только проверенные решения в области кибербезопасности для защиты от вредоносных и шпионских программ — многие программы, замаскированные под антишпионские решения, сами являются шпионскими программами.

Важной мерой защиты от программ-шпионов является защита в режиме реального времени. Шпионское ПО обычно использует сеть для передачи частной информации третьим лицам. Решения по кибербезопасности с мониторингом в режиме реального времени могут идентифицировать эти сообщения и обнаруживать шпионское ПО, даже если оно не может быть обнаружено другими методами.

Литература

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.
2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 400 с.
4. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 476 с.

5. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
6. Баранова, Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М.: Риор, 2008. - 400 с.
7. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
8. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.

References

1. Babash, A.V. Information security: Laboratory workshop / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2019. - 432 p.
2. Babash, A.V. Information Security. Laboratory workshop: Textbook / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2013. - 136 p.
3. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 400 p.
4. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 476 p.
5. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2018. - 400 p.
6. Baranova, E.K. Information Security. History of special methods of cryptographic activity: Textbook / E.K. Baranova, A.V. Babash, D.A. Larin. - M.: Rior, 2008. - 400 p.
7. Biryukov, A.A. Information security: protection and attack / A.A. Biryukov. - M.: DMK Press, 2013. - 474 p.
8. Gafner, V.V. Information Security: Textbook / V.V. Gafner. - Rn / D: Phoenix, 2010. - 324 p.

Для цитирования: Крыгин Н.Д. Шпионское программное обеспечение Научный сетевой журнал «Столыпинский вестник», номер 4/2022.