Бютнер С.И. Вирусы, использующие уязвимости в механизме PREFETCH И SUPERFETCH в WINDOWS // Международный журнал информационных технологий и энергоэффективности.– 2025. – Т. 10 № 3(53) с. 86–89

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.736

ВИРУСЫ, ИСПОЛЬЗУЮЩИЕ УЯЗВИМОСТИ В МЕХАНИЗМЕ PREFETCH И SUPERFETCH В WINDOWS

Бютнер С.И.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: serafimkavasaki@gmail.com

Механизмы Prefetch и Superfetch в операционных системах Windows предназначены для ускорения работы приложений за счет предварительной загрузки часто используемых данных в память. Однако, эти функции также могут быть использованы злоумышленниками для распространения вирусов и выполнения произвольного кода. В статье рассматриваются уязвимости, связанные с этими механизмами, способы их эксплуатации вредоносными программами, а также методы защиты, такие как обновления системы, настройка безопасности и ограничение прав доступа.

Ключевые слова: Вирусы, Prefetch, Superfetch, уязвимости, Windows, безопасность, защита, эксплуатация, обновления.

VIRUSES EXPLOITING VULNERABILITIES IN PREFETCH AND SUPERFETCH IN WINDOWS

Buetner S.I.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: serafimkavasaki@gmail.com

The Prefetch and Superfetch mechanisms in Windows operating systems are designed to speed up application performance by preloading frequently used data into memory. However, these features can also be exploited by attackers to spread viruses and execute arbitrary code. The article discusses vulnerabilities related to these mechanisms, how malicious software exploits them, and protection methods such as system updates, security configuration, and access control restrictions.

Keywords: Viruses, Prefetch, Superfetch, vulnerabilities, Windows, security, protection, exploitation, updates.

Введение

Механизмы Prefetch и Superfetch в операционных системах Windows играют ключевую роль в оптимизации производительности системы. Эти функции позволяют ускорить загрузку приложений, предзагружая в память файлы и данные, которые наиболее часто используются пользователем. Однако, несмотря на их пользу, в этих механизмах были обнаружены уязвимости, которые могут быть использованы злоумышленниками для выполнения вредоносного кода. В последние годы возникли случаи эксплуатации этих уязвимостей вирусами и другими вредоносными программами, что делает их важной темой для обсуждения в контексте информационной безопасности.

Суть проблемы заключается в том, что механизм Prefetch, предназначенный для ускорения запуска программ, хранит в себе информацию о том, какие файлы и компоненты использовались при запуске приложений. Эта информация сохраняется в специальных файлах с расширением .pf, что делает систему уязвимой к атакующим, которые могут создать вредоносный файл, использующий такую же структуру данных. Механизм Superfetch, в свою очередь, пытается предсказать, какие данные будут использоваться в будущем, и заранее загружает их в память. Злоумышленники могут использовать эти механизмы для внедрения вредоносных программ, которые могут скрыться от традиционных методов обнаружения или использовать их для выполнения кода на уязвимых системах.

Вирусы использующие уязвимости в механизме Prefetch и Superfetch в Windows

Механизм Prefetch в Windows был разработан для того, чтобы повысить производительность системы за счет кэширования и загрузки в память часто используемых файлов и компонентов. Однако его структура хранит важную информацию о процессе запуска приложений. Эти файлы с расширением .pf, в которых содержатся записи о запуске программ, также могут быть использованы для хранения данных, которые злоумышленники могут эксплуатировать. Вредоносное ПО может воспользоваться этими записями и внедрить свой код в файлы, которые обычно не проверяются антивирусными программами. Такой подход позволяет вирусам скрываться в системе, не привлекая внимания[1].

Кроме того, механизм Superfetch, который анализирует поведение пользователя и заранее подготавливает данные для более быстрого их использования, может быть использован для распространения вредоносных программ. Когда пользователи запускают приложение, которое было подготовлено Superfetch, возможно, что приложение будет пытаться загрузить данные или файлы, созданные злоумышленниками. В результате вирус может быть загружен на систему, если она подвержена уязвимостям, связанным с управлением памятью или с другими компонентами операционной системы[2].

Эксплуатация этих механизмов вирусами чаще всего происходит через социальную инженерию, когда злоумышленники подготавливают вредоносные файлы, которые имитируют нормальные операционные процессы. Например, вирус может сгенерировать файл Prefetch, который будет выглядеть как запись о запуске популярной программы, и при этом содержать скрытый вредоносный код. Когда система запускает этот файл, вирус может активироваться, что позволяет ему получить доступ к системным файлам или даже установить дополнительные компоненты, которые могут быть использованы для дальнейших атак[3].

Одной из угроз, связанных с использованием уязвимостей Prefetch и Superfetch, является возможность распространения вирусов через локальные и удаленные сети. Вредоносные файлы, связанные с этими механизмами, могут быть размещены в сети, и при доступе к ним на других устройствах система может заражаться. Сложность заключается в том, что такой вирус может быть трудно обнаружить, поскольку он не требует явного взаимодействия с пользователем и может активно использовать функции операционной системы для скрытности[4].

Существует несколько методов защиты от уязвимостей в механизмах Prefetch и Superfetch, которые можно внедрить на уровне настройки операционной системы и безопасности. Одним из самых простых и эффективных способов защиты является регулярное обновление операционной системы. Microsoft активно устраняет уязвимости в различных

компонентах Windows, и установление последних патчей является важной мерой профилактики.

Другим важным шагом является настройка безопасности с использованием групповых политик и ограничение доступа к определённым системным файлам и папкам. Например, можно отключить функции Prefetch и Superfetch, если они не являются критически важными для производительности системы. Это можно сделать через настройки реестра или с помощью инструментов администрирования Windows, что поможет минимизировать риски, связанные с использованием уязвимостей.

Кроме того, важно использовать антивирусные программы с поддержкой анализа поведения, которые способны обнаружить подозрительные активности в процессе работы системы. Такие программы могут отслеживать действия вредоносных файлов, которые пытаются внедрить код в систему через Prefetch или Superfetch, и заблокировать их до того, как они смогут нанести вред[5].

Для защиты от вирусов, использующих уязвимости в этих механизмах, следует также применять сегментацию сети и минимизацию прав доступа. Вредоносные программы чаще всего нацелены на слабые места, связанные с высокими правами доступа. Путём ограничения прав пользователей можно предотвратить заражение системы даже в случае эксплуатации уязвимости.

Заключение

Механизмы Prefetch и Superfetch в Windows являются полезными функциями для повышения производительности системы, но они также представляют собой уязвимости, которые могут быть использованы для распространения вирусов и выполнения произвольного кода. Злоумышленники могут эксплуатировать эти уязвимости для внедрения вредоносных программ в систему, что ставит под угрозу безопасность как индивидуальных пользователей, так и организаций.

Для защиты от таких угроз важно регулярно обновлять операционную систему, отключать ненужные функции, использовать антивирусное ПО с поддержкой анализа поведения и настраивать правильные параметры безопасности в системе. Эти меры помогут минимизировать риски и защитить систему от вирусов, которые используют уязвимости в Prefetch и Superfetch.

Список литературы

1. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
2. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.
3. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 61-65.

4. Кушнир Д. В., Шемякин С. Н., Орлов Г. А. Представление некоторых аспектов отсеивания составных чисел для криптографических приложений //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 1. – С. 25-28.
5. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения //Интеллектуальные технологии на транспорте. – 2018. – №. 3 (15). – С. 47-54.

References

1. Petrova T. V. and others. Approaches to detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
2. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment //Actual problems of infotelec communications in science and education. - 2021. – pp. 409-414.
3. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions with the best characteristics in the class of 4 variables //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. 2020. No. 4. pp. 61-65.
4. Kushnir D. V., Shemyakin S. N., Orlov G. A. Presentation of some aspects of screening composite numbers for cryptographic applications //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 1. – pp. 25-28.
5. Kalinin M. O., Shterenberg S. I. Analysis of information security of an enterprise based on monitoring of information resources using machine learning //Intelligent technologies in transport. – 2018. – №. 3 (15). – pp. 47-54.