аттестационных мероприятий для сотрудников субъектов КИИ, появление стандартов технического регулирования сферы, а также новые изменения в апреле 2025 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» направлены на реагирование и выстраивание комплексного подхода к обеспечению информационной безопасности объектов КИИ.

Литература

1. Введение в «Цифровую» экономику / А. В. Кешелава В. Г. Буданов, В. Ю. Румянцев и др.; под общ. ред. А. В. Кешелава; гл. «цифр.» конс. И. А. Зимненко. – ВНИИГеосистем, 2017. – 28 с. (На пороге «цифрового будущего». Книга первая).
2. В России появится новый нацпроект – «Экономика данных» https://digital.gov.ru/ru/events/45686/.
3. А. О. Рукосуев Роль органов государственного управления в цифровой трансформации экономики региона // Экономика: вчера, сегодня, завтра. 2023. Т. 9. № 7А. С. 237.
4. Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ.
5. Демин С. С., Джамай Е. В., Сазонов А. А. Трансформация пространства корпоративной информационной системы при реализации высокотехнологичными предприятиями концепции «Индустрия 4.0» // Экономика: вчера, сегодня, завтра. 2019. Т. 9. № 7А. С. 237.
6. Морозова О. В. Цифровая экономика: учебник/ Морозова О. В., Немова А. В. – М.: Феникс, 2016. – 398 с.

УДК 004.056.57

О НЕЙТРАЛИЗАЦИИ ПРОГРАММ-ВЫМОГАТЕЛЕЙ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS

И. Б. БЕРЕЖНОЙ

НИИ прикладных проблем математики и информатики,
Белорусский государственный университет,
г. Минск, Беларусь

Программа-вымогатель (англ. ransomware, от слов ransom – выкуп и software – программное обеспечение) – тип вредоносного программного обеспечения (ВПО), который используется в целях вымогательства путем зашифровывания данных, ценных для пользователя компьютерной системы, и последующего требования выкупа за их восстановление. Концепция программы-вымогателя, шифрующей пользовательские файлы, была представлена еще в 1996 году на конференции IEEE Security & Privacy conference [1], однако наибольшее распространение данный тип ВПО получил после 2013 года в связи с развитием криптовалют как трудноотслеживаемых способов платежей [2]. По данным компании Chainanalysis суммарный ежегодный объем платежей на криптовалютные кошельки вымогателей с 2020 года превышает 500 миллионов долларов США, а за 2024 год превысил 800 миллионов долларов США [3].

Программы-вымогатели разных семейств отличаются способами проникновения, особенностями горизонтального распространения и закрепления в системе, некоторым дополнительным функционалом. Для выявления работы программ-вымогателей на конкретном компьютере системы класса MDR (Managed Detection and Response) используют ряд правил детектирования, к наиболее распространенным из которых относятся [4]:

активная работа с реестром,

наличие в оперативной памяти вредоносного кода,

запуск подозрительных сервисов и программ, особенно удаленным пользователем,

доступ к подозрительным узлам и URL,

получение дампов памяти, связанных с сервисом безопасности LSASS,

добавление пользователей и повышение их привилегий,

работа с сетевыми устройствами.

Следует отметить, что применение таких правил требует предварительной настройки на конкретный образец ВПО и мало эффективно в случае использования в ВПО уязвимостей нулевого дня.

Основные рекомендации для борьбы с программами-вымогателями, предлагаемые на текущий момент, представляют собой только общие рекомендации по борьбе с ВПО произвольного типа с повышенным акцентом на необходимость регулярного резервного копирования информации [5]. Другими словами, в качестве общей стратегии вместо способов защиты предлагается рассматривать способы минимизации последствий. То есть эффективной защиты на текущий момент не имеется.

В качестве основной компоненты программ-вымогателей выступает блок шифрования пользовательских данных на псевдослучайных ключах шифрования, генерируемых в ВПО. Источником таких псевдослучайных значений могут выступать как самостоятельно разработанные хакерами генераторы псевдослучайных чисел (ГПСЧ), так и ГПСЧ, реализованные в операционной системе.

В случае самостоятельной реализации ГПСЧ в программе-вымогателе исходный код ВПО часто содержит ошибки, приводящие к понижению энтропии начальных значений ГПСЧ и, как результат, к возможности восстановления зашифрованных данных без необходимости уплаты выкупа [6].

Поэтому у самых эффективных семейств программ-вымогателей криптографические ядра, непосредственно отвечающие за шифрование файлов, соответствуют следующей схеме [7]:

1) злоумышленник генерирует пару открытого и личного ключей для асимметричного шифрования и загружает в ВПО (криптер) открытый ключ, после чего криптер некоторым образом доставляется на компьютер-жертву;

2) при запуске криптер осуществляет поиск файлов, предположительно представляющих ценность для владельца компьютера, по определенным признакам, чаще всего – по расширению имен файлов;

3) для каждого найденного файла с помощью криптографически сильного ГПСЧ, реализованного в операционной системе, генерируется ключ симметричного шифрования, затем с помощью этого ключа файл зашифровывается (либо полностью, либо частично – в случае большого объема файла), после чего к нему дописывается блок с использованным ключом, зашифрованный на открытом ключе злоумышленника;

4) жертва после оплаты выкупа получает программное обеспечение для расшифрования файлов, содержащее личный ключ злоумышленника (декриптер);

5) декриптер для каждого файла расшифровывает на личном ключе злоумышленника дописанный блок, извлекает из него ключ симметричного шифрования и с его помощью расшифровывает исходный файл.

Указанная схема обладает следующими преимуществами для злоумышленника:

1) ни при каких обстоятельствах закрытый ключ злоумышленника не передается жертве до оплаты выкупа;

2) злоумышленнику не требуется от жертвы никаких дополнительных данных, кроме идентификатора использованной ключевой пары;

3) жертве от злоумышленника требуется один файл фиксированного размера вне зависимости от размера зашифрованных данных;

4) при соблюдении известных требований на размер ключа восстановление личного ключа по открытому для жертвы невозможно;

5) при симметричном шифровании разных файлов использованные ключи не могут совпадать; как следствие, существенно затруднен криптоанализ алгоритма шифрования файлов либо процесс восстановления личного ключа.

Основное тонкое место описанной схемы действий криптографического ядра программы-вымогателя – получение данных от системного ГПСЧ. Во время работы вымогателя случайный ключ размером не менее 16 байтов требуется для каждого подходящего файла. А так как количество таких файлов, подходящих по шаблоны поиска, обычно исчисляется тысячами, то, соответственно, и случайная последовательность, которая требуется за короткий промежуток времени с ГПСЧ, будет большого размера.

В актуальных операционных системах семейства Windows начиная с Windows 10 все системные ГПСЧ построены в соответствии с рекомендациями NIST SP 800-90 на базе алгоритма AES-256 в режиме счетчика [8]. При этом реализована буферизация в 128-байтном состоянии, позволяющая сократить нагрузку на процессор при запросах на генерацию псевдослучайных данных малого размера. После запроса данных из буфера соответствующие байты буфера зануляются в целях конфиденциальности.

Сами ГПСЧ в ОС семейства Windows организованы в иерархию [8]:

1) корневой ГПСЧ, определяющий все псевдослучайные числа, выдаваемые ОС;

2) процессорные ГПСЧ режима ядра – набор из нескольких буферизованных состояний ГПСЧ по количеству логических процессоров для режима ядра, обслуживаемый драйвером CNG.SYS;

3) базовый ГПСЧ для процесса в пользовательском режиме;

4) набор процессорных ГПСЧ для каждого процесса в пользовательском режиме, реализованный с использованием библиотеки BcryptPrimitives.dll.

Корневой ГПСЧ инициализируется при запуске операционной системы на основе набора источников энтропии с использованием хэш-функции SHA-512. Переинициализация корневого ГПСЧ происходит по расписанию. Остальные системные ГПСЧ инициализируются по запросу на основе начального значения, получаемого из нижележащего ГПСЧ.

Согласно иерархии ГПСЧ, при известном состоянии некоторого ГПСЧ можно вычислить выходные последовательности вышележащих процессорных ГПСЧ, которые будут передаваться в ВПО при запросе случайных значений для ключей шифрования.

Если имеется возможность наблюдения 128-байтного состояния базового ГПСЧ для процесса программы-вымогателя, то становится возможно вычислить все ключи, использованные для шифрования пользовательских данных. Другими словами, нейтрализовать сработавшую программу-вымогателя без выплаты выкупа.

Вопрос наблюдения состояния базового ГПСЧ подозрительного процесса можно решить средствами мониторинга оперативной памяти на этапе запуска приложения либо путем мониторинга и сохранения состояний корневого ГПСЧ.

Литература

1. Young A. Cryptovirology: extortion-based security threats and countermeasures / A. Young, M. Yung. // *Proceedings 1996 IEEE Symposium on Security and Privacy.* – Oakland, CA, USA, 1996. – P. 129–140.

2. Fruhlinger J. Ransomware explained: How it works and how to remove it. / J. Fruhlinger // CSO Online. – URL: https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html. – Дата публ.: 02.10.2024.

3. 35 % Year-over-Year Decrease in Ransomware Payments, Less than Half of Recorded Incidents Resulted in Victim Payments. // Chainalysis Team. – URL: https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/ (дата обращения: 17.04.2025).

4. Managed detection and response in 2024 // Kaspersky Security Services. – URL: https://securelist.com/kaspersky-managed-detection-and-response-report-2024/115635/ (дата обращения: 17.04.2025).

5. Ransomware protection: How to keep your data safe in 2025 // Kaspersky Resource Center. – URL: https://www.kaspersky.com/resource-center/threats/how-to-prevent-ransomware (дата обращения: 17.04.2025).

6. Nugroho Y. Decrypting Encrypted files from Akira Ransomware (Linux/ESXI variant 2024) using a bunch of GPUs / Y. Nugroho // TinyHack.com – URL: https://tinyhack.com/2025/03/13/decrypting-encrypted-files-from-akira-ransomware-linux-esxi-variant-2024-using-a-bunch-of-gpus – Дата публ.: 13.03.2025.

7. Full source of the Conti Ransomware. // Github. – URL: https://github.com/gharty03/Conti-Ransomware. (дата обращения: 17.04.2025).

8. Ferguson N. The Windows 10 random number generation infrastructure / N. Ferguson // Microsoft. – URL: https://aka.ms/win10rng. – Дата публ.: 02.10.2019.