ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК004. 056.57

DOI: 10.21822/2073-6185-2024-51-1-79-86 Оригинальная статья/ Original article

Обнаружение вируса «Telegram Rat»

А.И. Дубровина[1,2], Мустафа Х. Алкорди[1]
[1] Донской государственный технический университет,
[1]344000, г. Ростов-на-Дону, пл. Гагарина, 1, Россия,
[2]Частное образовательное учреждение высшего образования
«Южный университет» (Институт управления, бизнеса и права),
[2]344000, г. Ростов-на-Дону, ул. Мечникова, 130, Россия

Резюме. Цель. Целью исследования является анализ вируса «Telegram Rat», подчеркивая важность информирования для эффективной борьбы с киберугрозами и обеспечения безопасности в цифровой эпохе. **Методы.** В статье использовался анализ характеристик и распространения вирусов «Telegram Rat». Приведен пример анализа технических механизмов вымогательства на примере «WAGNER GROUP» и сформулированы этапы ликвидации вируса. **Результаты.** Рассмотрена акуальность проблемы вируса «Telegram Rat» и пути его передачи. Представлены практические методы выявления и нейтрализации угрозы. Метод обнаружения угроз вируса «Telegram Rat» основан на анализе активных процессов, сетевой активности и файловой системы. Выявлено, что основным уязвимым местом на устройствах, зараженных вирусом, является неосторожное поведение пользователей. **Вывод.** В содержании настоящей работы подчеркивается важность бдительности при скачивании файлов и переходах по неизвестным ссылкам. Недостаточная осторожность может привести к утрате данных и утечке информации, подчеркивая необходимость сознательного поведения в цифровой среде.

Ключевые слова: «Telegram Rat», киберугрозы, информационная безопасность
Для цитирования: А.И. Дубровина, Мустафа Х. Алкорди. Обнаружение вируса «Telegram Rat». Вестник Дагестанского государственного техническо-го университета. Технические науки. 2024; 51(1):79-86. DOI:10.21822/2073-6185-2024-51-1- 79-86

Detection of «Telegram Rat» virus

A.I. Dubrovina[1,2], Mustafa H. Alcordi[1]
[1]Don State Technical University,
[1] 1 Gagarin Square, Rostov-on-Don 344000, Russia
[2]Southern University (Institute of Management, Business and Law),
[2] 130 Mechnikova St., Rostov-on-Don 344000, Russia

Abstract. Objective. The aim of this study is to analyze the «Telegram Rat» virus, emphasizing the importance of awareness to effectively combat cyber threats and ensure security in the digital age. **Methods.** This paper used an analysis of the characteristics and distribution of «Telegram Rat» viruses. An example of analyzing the technical mechanisms of extortion on the example of «WAGNER GROUP» was given and the steps of virus elimination were formulated. **Results.** The acuality of the «Telegram Rat» virus problem and ways of its transmission are considered. Practical methods of threat detection and neutralization are stipulated. The method of «Telegram Rat» virus threat detection is based on the analysis of active processes, network activity and file system. It is revealed that the main vulnerability on devices infected with the virus is careless user behavior. **Conclusion.** The contents of this paper emphasize the importance of vigilance when downloading files and clicking on links. Lack of caution can lead to data loss and information leakage, emphasizing the need for conscious behavior in the digital environment.

Keywords: «Telegram Rat», cyber threats, information security

For citation: A.I. Dubrovina, Mustafa H. Alcordi. Detection of «Telegram Rat» virus. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(1):79-86. DOI:10.21822/2073-6185-2024-51-1-79-86

Введение. В наше время, с развитием цифровых технологий и распространением интернета, кибербезопасность стала одним из наиболее актуальных вопросов. Киберугрозы и вирусы, такие как «Telegram Rat», стали серьезной угрозой для информационной безопасности, ведь они способны нанести значительный ущерб как отдельным пользователям, так и организациям. Обнаружение и изучение вируса «Telegram Rat» имеют решающее значение для разработки эффективных методов противодействия и обеспечения кибербезопасности, поскольку пользователей.

Постановка задачи. Исследование на тему обнаружения вируса особенно актуально в свете массового использования приложения Telegram в странах СНГ и даже за их пределами.

Целью данного исследования является обнаружение и анализ вируса «Telegram Rat» с целью понимания его структуры, распространения и механизмов действия, а также разработка стратегий для борьбы с данной киберугрозой.

Для достижения цели исследования были поставлены следующие задачи:

1. Идентификация вируса: Первым этапом является идентификация вируса «Telegram Rat». Это включает анализ характеристик вредоносного программного обеспечения, определение его целевой аудитории и способов распространения.

2. Анализ распространения: Изучение механизмов распространения вируса «Telegram Rat» включает анализ методов заражения, путей передачи и внедрения в целевую систему.

3. Разработка мер по борьбе: На основе полученных данных разрабатываются стратегии и методы борьбы с вирусом.

Это может включать разработку антивирусных программ, обучение пользователей правилам безопасности и рекомендации по предотвращению атак.

Методы исследования. «Telegram Rat» - (RAT - Remote Access Trojan), вирус, который представляет собой тип вредоносного программного обеспечения удаленного доступа, способного захватывать и передавать хакеру контроль над зараженным устройством с использованием мессенджера Telegram [1] для связи с удаленным хакером и передачи украденных данных [2]. И хотя сам Telegram можно использовать для злонамеренных действий, мы обнаружили, что поддельная версия приложения является частью большой волны поддельных приложений Telegram [3]. Согласно последним сообщениям, Telegram столкнулся с недавней волной подражателей приложения, которые используют репутацию приложения для распространения вредоносного ПО, которое тайно продвигает бесконечный поток вредоносных сайтов.

Эти сайты имеют неприятную способность вести к еще более опасным киберпространствам, таким как: мошенничество с техподдержкой;поддельные опросы; фишинговые страницы, предназначенные для кражи ваших личных данных; мошеннические сайты или страницы; вредоносные URL-адреса, содержащие вредоносное ПО [4]. «Telegram Rat» представляет собой определенный вид программного обеспечения, которое, однажды проникнув на компьютер, способно активировать скрытые процессы, получая при этом привилегии администратора.

Такая характеристика обеспечивает данному трояну возможность осуществления весьма неблагоприятных действий на устройстве, таких как:

1. Кража и последующая отправка документов на серверы хакеров.
2. Отправка информации о текущих активных процессах.
3. Управление состоянием Mac, включая включение или выключение.
4. Инициирование установки или удаления приложений.
5. Открытие и закрытие файлов на устройстве.

6. Сбор информации о конфигурации macOS.
7. Прекращение выполнения определенных процессов через инструмент «Монитор активности».
8. Использование встроенной микрофонной и камерной техники.

Это основная причина, по которой следует подумать об удалении этой вредоносной программы и прибегнуть к навыкам кибербезопасности в сети как можно скорее [5].

Обсуждение результатов. «Telegram Rat» использует методы социальной инженерии и манипуляции пользователем через приложение Telegram для внедрения и заражения целевой системы. Это манипулятивные методы внутри «мессенджера», чтобы убедить пользователей перейти к скачиванию (в большинстве случаев, человек не понимает, что вредоносный файл загружен на устройство) [6].

Пути передачи:

1. Ссылки: Злоумышленники могут размещать обманчивые ссылки в чатах или каналах Telegram, привлекая внимание пользователей. При переходе по такой ссылке пользователь может быть перенаправлен на страницу, представленную как легитимный ресурс, и попросить скачать какой-либо файл [7].

2. Файлы или документы: Вирус может быть передан через загрузку вредоносных файлов или документов, которые могут быть отправлены пользователями в чатах или каналах [8-9].

3. Сторонние приложения: Злоумышленники могут создавать и распространять в Telegram вредоносные приложения, представляющиеся как легитимные. Пользователи, устанавливая такие приложения, могут случайно заразить свои устройства [10-11].

4. Боты: Злоумышленники могут использовать ботов в Telegram для распространения вируса. Пользователи могут получить ссылку или инструкции от бота, которые в итоге приведут к установке «Telegram Rat» [12].

5. Поддельное приложение Telegram: Злоумышленники могут создавать поддельные версии официального приложения Telegram, которые содержат в себе вирус. Они могут распространять эти поддельное приложение через сторонние источники или недоверенные интернет-ресурсы.

Для обнаружения вируса «Telegram Rat» рекомендуется провести более глубокий анализ системы. Вот три основных пункта, которые можно использовать:

1. Анализ процессов и служб: Провести детальный анализ активных процессов и служб в системе [13-14]. Это включает:
   Использование инструментов, таких как диспетчер задач в Windows или команды в терминале в Linux, чтобы выявить подозрительные процессы или службы [15].
   Исследование поведения процессов, таких как их связь с интернетом, чтение/запись файлов или изменение системных настроек.
   Проверку подписей и авторства процессов для выявления потенциальных «фейковых» или подмененных компонентов.
2. Анализ сетевой активности: Изучить сетевую активность системы, чтобы обнаружить связь с удаленными серверами и подозрительные запросы:
   Использование сетевых мониторов, таких как Wireshark, для анализа трафика и выявления необычных или незнакомых подключений.
   Оценку активности по определенным портам и протоколам, которые могут быть связаны с «Telegram Rat».
   Выявление ненормально большого объема сетевого трафика или активности в ночное время, что может указывать на скрытую передачу данных.
3. Анализ файловой системы: Исследовать файловую систему на наличие вредоносных файлов и изменений:
   Сканирование всех файлов на предмет наличия подозрительных расширений или изменений в датах создания/изменения.

Использование антивирусных программ и антишпионских инструментов для поиска и обнаружения вредоносных файлов.

Проверку автозагрузки и изменений в реестре, которые могут быть связаны с «Telegram Rat».

Помимо этих пунктов, важно понимать, что вирусы могут использовать разные методы для маскировки и обхода обнаружения. Поэтому специалист по кибербезопасности должен иметь опыт и экспертизу, чтобы провести комплексный и адаптированный анализ системы и выявить потенциальные угрозы, включая «Telegram Rat».

Чтобы обнаружить все вирусные компоненты и файлы, принадлежащие вирусу, мы настоятельно рекомендуем вам выполнить следующие шаги по удалению. Если вы хотите полностью обнаружить и удалить вредоносное ПО Telegram, а также любые другие вирусы, которые оно могло занести на ваш компьютер в результате его наличия, мы предлагаем запустить сканирование вашего компьютера, загрузив передовое программное обеспечение для защиты от вредоносных программ. Такой инструмент специально создан, чтобы помочь вам автоматически удалить вредоносное ПО, а также защитить автоматизированное рабочее место в будущем [16].

Подготовка и удаление «Telegram Rat». Прежде чем приступить к фактическому процессу удаления, мы рекомендуем выполнить следующие подготовительные шаги.

1. Необходимо провести анализ, что инструкции сигнатур вирусных заражений актуальны, в связи с тем, что под вирусным заражением может определяться ошибка в отработке антивирусного ПО.
2. Необходимо делать резервную копию всех ваших файлов, даже если они могут быть повреждены. Необходимо сделать резервную копию своих данных с помощью облачного решения для резервного копирования и застраховать свои файлы от любой потери, даже от самых серьезных угроз.

Инструкция по удалению:

1. Необходимо загрузить компьютер в безопасном режиме, чтобы изолировать и удалить вирус Telegram. Откройте окно «Выполнить» «Win + R» (рис. 1).

Рис. 1. Windows + R
Fig. 1. Windows + R

2. В появившемся окне введите «msconfig» и нажмите «ОК» (рис. 2).

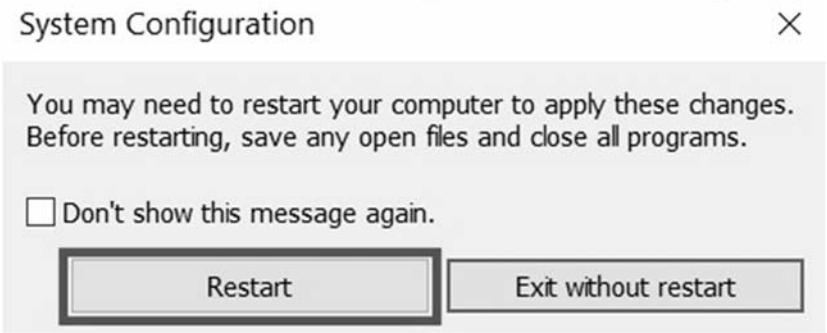

Рис. 2. Командная строка и безопасная загрузка
Fig. 2. Command Line and Secure Boot

3. Перейдите на вкладку «Загрузка». Там выберите «Безопасная загрузка», а затем нажмите «Применить» и «ОК» (рис. 2).

4. При появлении запроса необходимо нажать «Перезагрузить», чтобы перейти в безопасный режим (рис. 3).

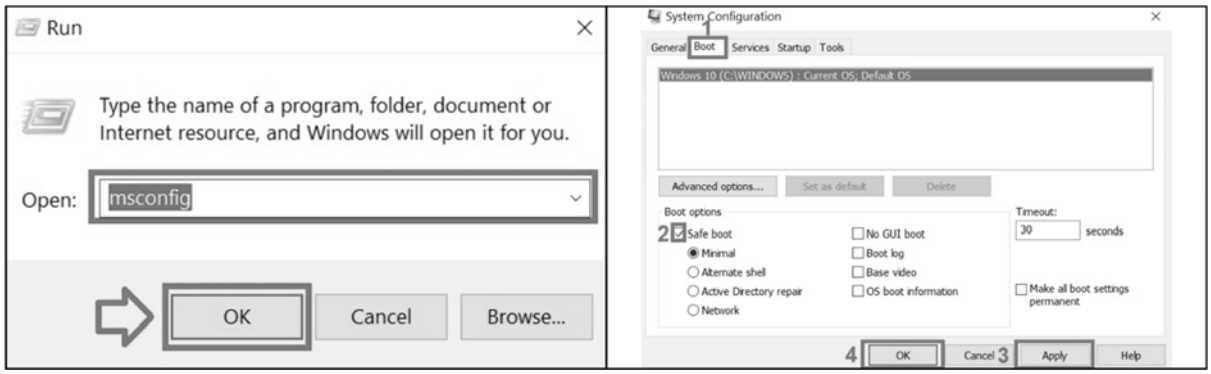

Рис. 3. Рестарт в безопасном режиме
Fig. 3. Restart in safe mode

Следуя этим шагам, возможно подготовиться к удалению «Telegram Rat» и обеспечить максимальную эффективность в процессе борьбы с вирусом. Анализ технических механизмов вируса на конкретном примере. Вымогательство Вагнера - хитроумная программа, нацеленная на операционную систему Windows.

Рассмотрим подробно технические аспекты этой угрозы, а также особенности ее обнаружения на примере реального случая использования в телеграм-группе «WAGNER GROUP» [1].

SHA256:1238ab3dd3ed620536969ee438e99a33a418ba20f5e691962ed07904e075b2a4 - вирус-вымогатель «Вагнер» представляет собой 32-разрядный двоичный файл, нацеленный на операционную систему Windows. На рис. 4 показаны детали файла.

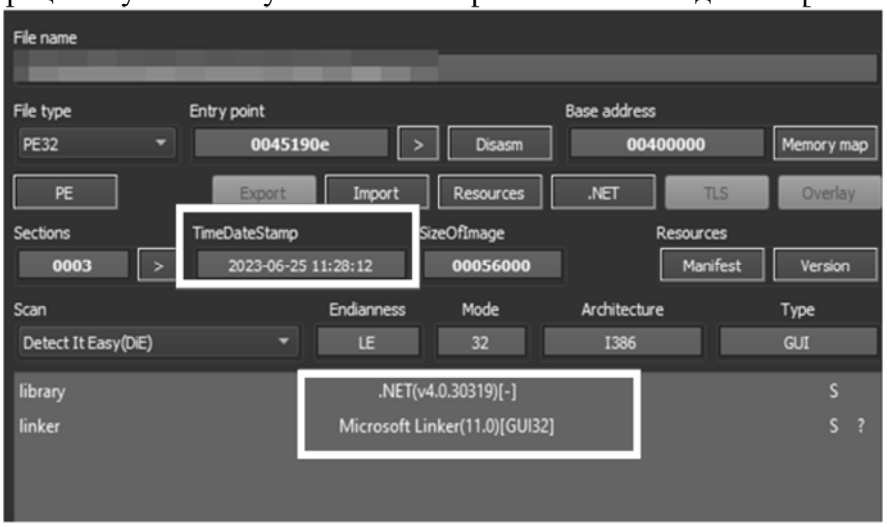

Рис. 4. Детали вируса «Вагнер»
Fig. 4. Details of the Wagner virus

Инициализация и Проверка Угрозы. После активации, программа-вымогатель Вагнера начинает свою деятельность с инициализации разнообразных переменных, которые служат ориентирами для дальнейших шагов. Однако перед тем как начать свое воздействие, она проводит первичную проверку, чтобы гарантировать, что в системе запущен только один экземпляр этой программы. Для этой цели она изучает список всех текущих процессов, используя метод GetProcesses(), после чего проводит поиск процесса с тем же именем, что и сама программа.

Если такой процесс обнаружен, программа автоматически завершает свою работу, исключая возможность запуска нескольких экземпляров одновременно. На рис. 5 можем ви-

деть визуальное представление этой проверки, гарантирующей наличие только одного экземпляра вымогательства (рис. 5).

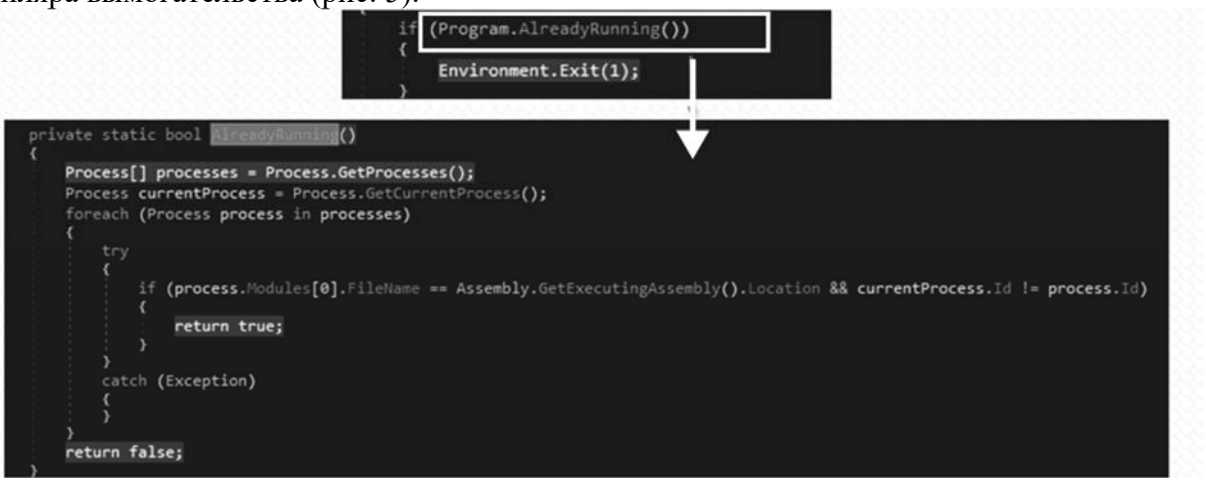

Рис. 5. Один экземпляр программы
Fig. 5. One copy of the program

После успешной проверки на наличие множественных экземпляров, программа вымогательства Вагнера переходит к анализу значения переменной «checkSleep».

Если эта переменная установлена в значение true, программа начинает проверять, запущена ли она из папки «%APPDATA%». Если запуск происходит из другой директории, программа переходит в режим «сна» на заданный период времени, определенный Исполнителем Угроз (ТА). На рис. 6 наглядно продемонстрирован механизм состояния сна в программе-вымогателе «Вагнер» (рис. 6).

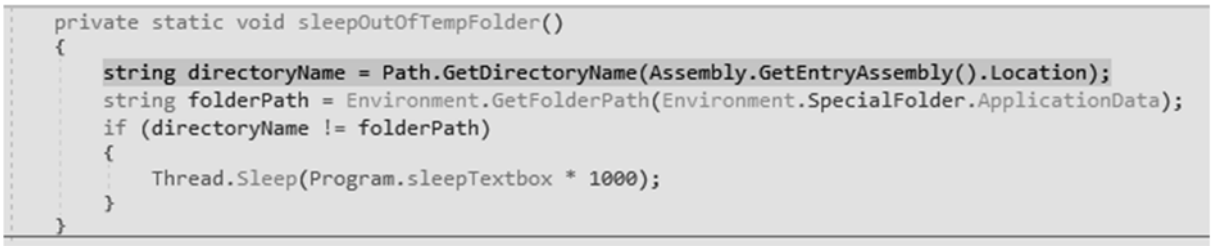

Рис. 6. Состояние сна как защита от обнаружения
Fig. 6. Sleep state as protection from detection

Анализ технических характеристик программы-вымогателя «Вагнер» раскрывает сложную сеть механизмов, созданных для обеспечения незаметности и эффективности ее действий. Обнаружение таких угроз, как вымогательство Вагнера, становится ключевым этапом в обеспечении кибербезопасности [17]. Понимание и анализ технических деталей позволяют нам эффективно бороться с угрозами и защищать нашу цифровую сферу от потенциальных атак.

Обсуждение методов анализа и обнаружения угроз, сосредотачивается на комплексном подходе. Это включает анализ активных процессов, сетевой активности и файловой системы для выявления характерных аномалий. Особое внимание уделяется обучению пользователей узнавать подозрительные действия и улучшать «кибергигиену». Это включает в себя умение различать подозрительные ссылки и файлы, регулярное обновление программ и операционных систем, использование надежных паролей и двухфакторной аутентификации, а также осведомленность о текущих кибертенденциях [18-20].

Вывод. В данной статье мы достаточно глубоко исследовали вирус «Telegram Rat» и проследили его пути передачи, методы заражения, а также технические характеристики. Мы рассмотрели разнообразные пути передачи вируса, начиная от загрузки вредоносных файлов до использования злоумышленных ботов в Telegram. Это подчеркивает сложность и многообразие методов, которыми киберпреступники могут распространять вредоносные программы.

Обнаружение и анализ вируса «Telegram Rat» играют критическую роль в обеспечении

кибербезопасности. Понимание его характеристик позволяет разрабатывать эффективные стратегии борьбы с этой угрозой. Важно помнить, что киберпреступники постоянно совершенствуют свои методы, и регулярное обновление знаний и технических навыков специалистов по кибербезопасности является неотъемлемой частью защиты от подобных угроз.

Выводы, сделанные на основе анализа вируса «Telegram Rat» и его распространения, подчеркивают важность обучения пользователей основам кибербезопасности, актуализации антивирусных программ и постоянной внимательности к собственной цифровой безопасности. Только путем совместных усилий экспертов и пользователей возможно сделать виртуальное пространство более безопасным и защищенным для всех его участников.

Библиографический список:

1. DrKLO. 2013. Telegram messenger for Android. (Oct. 2013). https://github.com/DrKLO/Telegram.
2. Кара И., Айдос М. Призрак в системе: технический анализ трояна удаленного доступа //International Journal on Information Technologies & Security. – 2019. – Т. 11. – No 1. – С. 73-84.
3. Li X. et al. An Android Malicious Application Detection Method with Decision Mechanism in the Operating Environment of Blockchain//Security and Communication Networks. – 2022. – Т. 2022. https://www.hindawi.com/journals/scn/2022/3111540/
4. Luo X. et al. Social engineering: The neglected human factor for information security management //Information Resources Management Journal (IRMJ). – 2011. – Т. 24. – №. 3. – С. 1-8.
5. Chislova O., Sokolova M. Cybersecurity in Russia //International Cybersecurity Law Review. – 2021. – Т. 2. – №. 2. – С. 245-251.
6. Govender I., Watson B. W. W., Amra J. Global virus lockdown and cybercrime rate trends: A routine activity approach //Journal of Physics: Conference Series. – IOP Publishing, 2021. – Т. 1828. – №. 1. – С. 012107.
7. Peeters S., Willaert T. Telegram and digital methods: Mapping networked conspiracy theories through platform affordances //M/C Journal.–2022.–Т.25.–№.1 https://journal.media-culture.org.au/index.php/mcjournal/article/view/2878.
8. Koutsokostas V. et al. Invoice# 31415 attached: Automated analysis of malicious Microsoft Office documents //Computers & Security. – 2022. – Т. 114. – С. 102582. https://www.mdpi.com/2076-3417/12/8/4088
9. Dubin R. Content Disarm and Reconstruction of RTF Files a Zero File Trust Methodology //IEEE Transactions on Information Forensics and Security. – 2023. – Т. 18. – С. 1461-1472. https://ieeexplore.ieee.org/abstract/document/10034674/
10. Balikcioglu P. G. et al. Malicious code detection in android: the role of sequence characteristics and disassembling methods //International Journal of Information Security. – 2023. – Т. 22. – №. 1. – С. 107-118. https://link.springer.com/article/10.1007/s10207-022-00626-2
11. Acharya S., Rawat U., Bhatnagar R. A comprehensive review of android security: Threats, vulnerabilities, malware detection, and analysis //Security and Communication Networks. – 2022. – Т. 2022. https://www.hindawi.com/journals/scn/2022/7775917/
12. https://www.mdpi.com/2075-4698/12/6/164 Herrero-Solana V., Castro-Castro C. Telegram channels and bots: A ranking of media outlets based in Spain //Societies. – 2022. – Т. 12. – №. 6. – С. 164.
13. Haagman D., Ghavalas B. Trojan defence: A forensic view //Digital Investigation. – 2005. – Т. 2. – №. 1. – С. 23-30.
14. Warrender C., Forrest S., Pearlmutter B. Detecting intrusions using system calls: Alternative data models //Proceedings of the 1999 IEEE symposium on security and privacy (Cat. No. 99CB36344). – IEEE, 1999. – С. 133-145.
15. Wu N., Qian Y., Chen G. A novel approach to trojan horse detection by process tracing //2006 IEEE International Conference on Networking, Sensing and Control. – IEEE, 2006. – С. 721-726.
16. Ciubotariu M. What next? trojan. linkoptimizer //Virus Bulletin. – 2006. – С. 6-10.
17. Mustafa Alkordi (2023). Ransomware Campaign Urges Resistance Against Russian Officials. URL: https://www.linkedin.com/pulse/ransomware-campaign-urges-resistance-against-russian-alkordi.
18. Kok S. et al. Ransomware, threat and detection techniques: A review //Int. J. Comput. Sci. Netw. Secur. – 2019. – Т. 19. – №. 2. – С. 136.https://seap.taylors.edu.my/file/rems/publication/105055_5256_1.pdf.
19. Tuma K., Calikli G., Scandariato R. Threat analysis of software systems: A systematic literature review // Journal of Systems and Software. – 2018. – Т. 144. – С. 275-294. https://www.sciencedirect.com/science/article/abs/pii/S0164121218301304
20. Zengy J. et al. Shadewatcher: Recommendation-guided cyber threat analysis using system audit records // 2022 IEEE Symposium on Security and Privacy (SP). – IEEE, 2022. – С. 489-506. https://www.sciencedirect.com/science/article/pii/S1319157821003621.

References

1. DrKLO. 2013. Telegram messenger for Android. (Oct. 2013). https://github.com/DrKLO/Telegram.
2. Kara I., Aidos M. A ghost in the system: technical analysis of a remote access Trojan. *International Journal on Information Technologies & Security*. 2019; 11(1): 73-84.
3. Li X. et al. An Android Malicious Application Detection Method with Decision Mechanism in the Operating Environment of Blockchain. *Security and Communication Networks*. 2022;2022. https://www.hindawi.com/journals/scn/2022/3111540/
4. Luo X. et al. Social engineering: The neglected human factor for information security management. *Information Resources Management Journal (IRMJ)*. 2011; 24(3):1-8.
5. Chislova O., Sokolova M. Cybersecurity in Russia. *International Cybersecurity Law Review*. 2021; 2(2): 245-251.
6. Govender I., Watson B. W. W., Amra J. Global virus lockdown and cybercrime rate trends: A routine activity approach. *Journal of Physics: Conference Series*. IOP Publishing, 2021; 1828(1): 012107.
7. Peeters S., Willaert T. Telegram and digital methods: Mapping networked conspiracy theories through platform affordances. *M/C Journal.* 2022;25(1): https://journal.media-culture.org.au/index.php/mcjournal/article/view/2878.
8. Koutsokostas V. et al. Invoice# 31415 attached: Automated analysis of malicious Microsoft Office documents. *Computers & Security*. 2022;114:102582.https://www.mdpi.com/2076-3417/12/8/4088
9. Dubin R. Content Disarm and Reconstruction of RTF Files a Zero File Trust Methodology. *IEEE Transactions on Information Forensics and Security.*2023;18:1461-1472. https://ieeexplore.ieee.org/abstract/document/10034674/
10. Balikcioglu P. G. et al. Malicious code detection in android: the role of sequence characteristics and disassembling methods. *International Journal of Information Security*. 2023; 22 (1):107-118.https://link.springer.com/article/10.1007/s10207-022-00626-2
11. Acharya S., Rawat U., Bhatnagar R. A comprehensive review of android security: Threats, vulnerabilities, malware detection, and analysis. *Security and Communication Networks.* 2022;2022. https://www.hindawi.com/journals/scn/2022/7775917/
12. https://www.mdpi.com/2075-4698/12/6/164 Herrero-Solana V., Castro-Castro C. Telegram channels and bots: A ranking of media outlets based in Spain. *Societies*. 2022; 12(6):164.
13. Haagman D., Ghavalas B. Trojan defence: A forensic view. *Digital Investigation*. 2005; 2(1): 23-30.
14. Warrender C., Forrest S., Pearlmutter B. Detecting intrusions using system calls: Alternative data models. *Proceedings of the 1999 IEEE symposium on security and privacy* (Cat. No. 99CB36344). IEEE, 1999; 133-145.
15. Wu N., Qian Y., Chen G. A novel approach to trojan horse detection by process tracing. *2006 IEEE International Conference on Networking, Sensing and Control.* IEEE, 2006: 721-726.
16. Ciubotariu M. What next? trojan. Linkoptimizer.*Virus Bulletin*. 2006: 6-10.
17. Mustafa Alkordi (2023). Ransomware Campaign Urges Resistance Against Russian Officials. URL: https://www.linkedin.com/pulse/ransomware-campaign-urges-resistance-against-russian-alkordi.
18. Kok S. et al. Ransomware, threat and detection techniques: A review //Int. J. Comput. Sci. Netw. Secur. – 2019;19(2): 136.https://seap.taylors.edu.my/file/rems/publication/105055_5256_1.pdf.
19. Tuma K., Calikli G., Scandariato R. Threat analysis of software systems: A systematic literature review. *Journal of Systems and Software*. 2018; 144: 275-294. . https://www.sciencedirect.com/science/article/abs/pii/S0164121218301304
20. Zengy J. et al. Shadewatcher: Recommendation-guided cyber threat analysis using system audit records // *2022 IEEE Symposium on Security and Privacy (SP).* IEEE, 2022;489-506. https://www.sciencedirect.com/science/article/pii/S1319157821003621.

Сведения об авторах:

Дубровина Ангелина Игоревна, ассистент, кафедра «Вычислительные системы и информационная безопасность»; adubrovina@yug.gkovd.ru

Алкорди Мустафа Хельми Муса, студент, кафедра «Вычислительные системы и информационная безопасность»; ministrelia69@yandex.ru.

Information about authors:

Angelina I. Dubrovina, Assistant, Department of Computer Systems and Information Security; adubrovina@yug.gkovd.ru

Mustafa Helmi Musa Alkordi, Student, Department of Computer Systems and Information Security; ministrelia69@yandex.ru.

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 25.12.2023.

Одобрена после рецензирования/ Reviced 16.01.2024.

Принята в печать/ Accepted for publication 16.01.2024.