ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2023-50-3-66-71 Оригинальная статья /Original article

Практический анализ вредоносного программного обеспечения

Д. А. Елизаров, А. В. Катков
Омский государственный университет путей сообщения,
644046, г. Омск, пр. Маркса, 35, Россия

Резюме. Цель. В настоящее время главным способом атак на организации является вредоносное ПО (ВПО). Проблема усиления защиты от такого способа атаки остается актуальной и требует новых подходов. Основная задача – анализ ВПО для оценки угроз и своевременное обнаружение и принятия мер. **Метод.** Для анализа следует использовать изолированную среду с настроенным окружением и ПО. **Результат.** В данной работе описан процесс создания изолированного стенда для анализа ВПО и проведен практический анализ файла malware.bin, взятого с учебного ресурса cyberdefenders.org. Для предотвращения воздействия на сеть, которая связывает две виртуальные машины, сконфигурированы сетевые интерфейсы. В результате анализа техник и особенностей, используемых в данном вредоносном ПО, было выявлено, что оно принадлежит к семейству банковских троянов Dridex. Для получения информации из данного семейства можно использовать инструмент AppGate Lab Dridex Toolkit. **Вывод.** Основываясь на проведенном анализе с применением статических и динамических методов, можно разработать правила детектирования для дальнейшего определения ВПО.

Ключевые слова: кибератака, вредоносное программное обеспечение, расследование инцидентов, анализ, информационная безопасность.

Для цитирования: Д. А. Елизаров, А. В. Катков. Практический анализ вредоносного программного обеспечения. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(3):66-71. DOI:10.21822/2073-6185-2023-50-3-66-71

Practical Malware Analysis

D. A. Elizarov, A.V. Katkov
Omsk State University of Railways,
35 Marx Ave., Omsk 644046, Russia

Abstract. Objective. Currently, the main method of attack on organizations is malware. The problem of strengthening protection against this type of attack remains relevant and requires new approaches. The main task is to analyze malware to assess threats and timely detection and take action. **Method.** For analysis, you should use an isolated environment with a customized environment and software. **Result.** This paper describes the process of creating an isolated stand for malware analysis and conducted a practical analysis of the malware.bin file taken from the cyberdefenders.org educational resource. Network interfaces are configured to prevent impact to the network that connects the two virtual machines. As a result of the analysis of the techniques and features used in this malware, it was revealed that it belongs to the Dridex family of banking Trojans. To obtain information from this family, you can use the AppGate Lab Dridex Toolkit. **Conclusion.** Based on the analysis performed using static and dynamic methods, detection rules can be developed for further identification of malware.

Keywords: cyberattacks, malware, incident investigation, analysis, information security.

For citation: D.A. Elizarov, A.V. Katkov. Practical Malware Analysis. Herald of Daghestan State Technical University. Technical Science. 2023; 50 (3): 66-71. DOI: 10.21822 /2073-6185-2023-50-3-66-71

Введение. В настоящее время наблюдается рост количества кибератак, что ставит под угрозу информационную безопасность организаций.

Согласно исследованию компании Positive Technologies, проведенному в 2022 году, лидирующим методом атак на организации является вредоносное программное обеспечение (ВПО) [1]. Этот факт подтверждается статистическими данными, представленными на рис. 1.

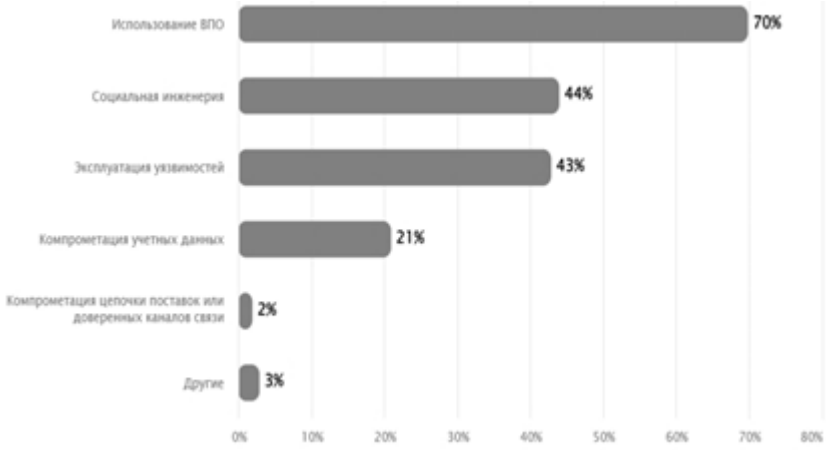


Рис. 1. Доля методов атак, используемых злоумышленниками, в 2022 году
Fig. 1. The share of attack methods used by attackers in 2022

Однако, не только организации, но и государство подвержено угрозе киберпреступлений. Компания RTM Group провела исследование, в рамках которого был выявлен общий ущерб преступных действий с использованием компьютерных технологий в России в 2021 году, который превысил 150 миллиардов рублей [2].

Эта оценка была основана на возбужденных уголовных делах, связанных с использованием технологий [3, 5-10]. Исходя из приведенных статистических данных, можно сделать вывод, что вопрос повышения уровня защиты от ВПО является актуальным, требует внимательного рассмотрения и принятия соответствующих мер.

Постановка задачи. Построение изолированного стенда для анализа ВПО. При расследовании инцидентов информационной безопасности, специалисты часто вынуждены производить анализ ВПО и изучать его взаимодействие с сетью и файловой системой. В результате этого анализа выделяются индикаторы компрометации и сигнатуры.

Для безопасного проведения подобного анализа необходимо использовать изолированную среду с настроенным окружением и программным обеспечением.

Стоит отметить, что многие вредоносные программы могут получать и отправлять информацию на командный сервер с помощью протокола HTTPS, который использует шифрование, что затрудняет обнаружение команд управления и выводимой из системы информации.

Методы исследования. Для решения данной задачи необходимо использовать специально подготовленный стенд, который позволяет анализировать происходящее и возвращаться к исходной точке до заражения системы.

Для создания стенда были использованы две виртуальные машины: ОС Kali Linux с установленным ПО Inetsim и BurpSuite и ОС Windows 10 со сконфигурированным ПО для проведения мониторинга системы и обратной разработки. Выбор ОС Windows 10 обусловлен ее популярностью в корпоративном сегменте и повышенной уязвимостью для атак.

В свою очередь, виртуальная машина Kali Linux будет использоваться для обеспечения работы интернет-служб, а виртуальная машина Windows – для изучения вредоносных программ. Схема виртуального стенда представлена на рис. 2.

В рамках исследования было проведено построение изолированного стенда, на основе выполнения шести этапов. На первом этапе был установлен гипервизор и созданы виртуальные машины на базе операционных систем Kali Linux и Windows 10.

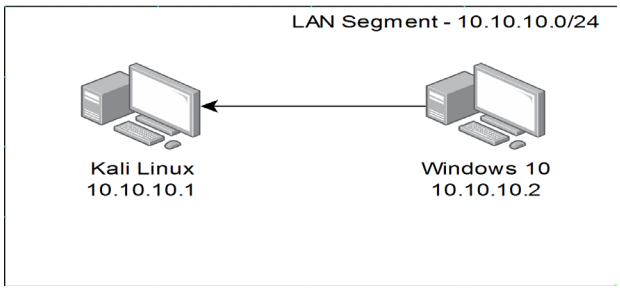


Рис. 2. Схема стенда для анализа ВПО
Fig. 2. Diagram of a stand for malware analysis

Далее была выполнена установка и настройка необходимого программного обеспечения на виртуальную машину Kali Linux и произведена настройка окружения и установка необходимого ПО на виртуальную машину Windows 10.

На следующем этапе была настроена изолированная виртуальная сеть и сетевые компоненты, а затем настроено ПО Inetsim для имитации работы соединения HTTP/HTTPS. На заключительном этапе была проведена итоговая проверка работоспособности стенда.

Для проведения анализа вредоносных файлов на виртуальную машину Windows, необходимо было установить программные инструменты – набор инструментов для статического и динамического анализа вредоносных программ FLARE VM. Для проведения статического анализа вредоносного программного обеспечения был использован фреймворк Ghidra-SRE. Данное ПО позволяет дизассемблировать и декомпилировать образцы с целью изучения их исходного кода и функционала.

Для разработки мер противодействия вредоносному программному обеспечению было использовано ПО Yara. Yara позволяет строить правила детектирования и противодействия на основе данных, полученных при статическом и динамическом анализе. Исследуемое вредоносное программное обеспечение может оказать воздействие на сеть, которая связывает две виртуальные машины.

Для предотвращения подобного воздействия необходимо сконфигурировать сетевые интерфейсы. Настройки по умолчанию в Inetsim нацелены на прослушивание только локального хоста. Первоочередная задача состоит в том, чтобы сделать его доступным для всех запросов в виртуальной сети.

Для этого необходимо изменить значение строки service_bind_address на 0.0.0.0 в конфигурационном файле. DNS-порт 53 (dns_bind_port 53) указывается в конфигурационном файле, а DNS конфигурируется по адресу 10.10.10.1 (dns_default_ip 10.10.10.1). Inetsim имеет ограниченную поддержку SSL и не может генерировать сертификаты для каждого хоста сразу.

Он имеет только один готовый сертификат для хоста inetsim.org. Для настройки SSL необходимо использовать Burp Suite на порте 443 в режиме прозрачного прокси. Для этого в файле конфигураций устанавливается порт 8443 для службы HTTPS (http_bind_port 8443).

Затем следует настроить Burp Suite в режиме прокси-сервера и на Windows-машину установить сертификат Burp Suite. Для настройки маршрутизации на Windows-машине требуется создать маршрут, направляющий весь сетевой трафик на IP-адрес Inetsim, а на машине Kali с Inetsim перенаправить входящий трафик на интерфейс eth0 (10.10.10.1). Необходимо также учитывать вопрос файлов-заглушек Inetsim при работе со стендом. Эти страницы распределены по протоколам и находятся в папке /var/lib/inetsim/. В файле конфигурации inetsim.conf можно отредактировать список.

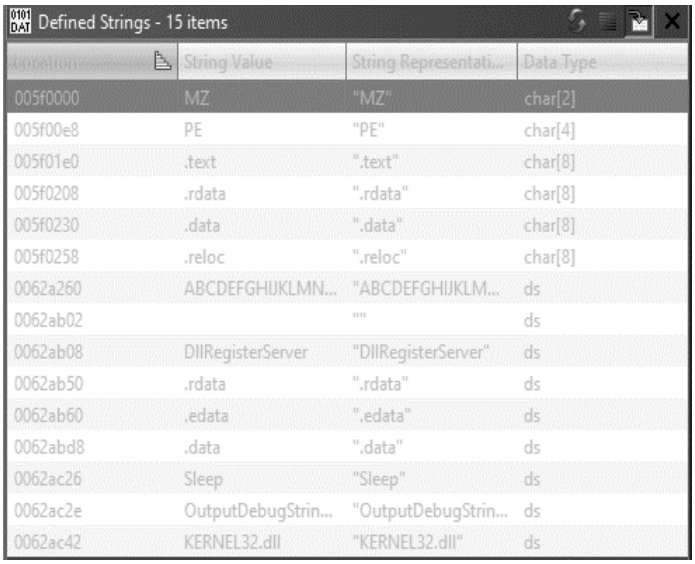
Обсуждение результатов. С целью проведения практического анализа в данном исследовании был выбран файл malware.bin с учебного ресурса cyberdefenders.org.

В процессе косвенного анализа был изучен заголовок данного файла, который позволил установить его формат (PE32), дату создания (11.11.21), а также хэш-суммы (SHA-1:FDD07C89C8ED656964DFA1A6CFF271E170EDA0C2,SHA-256: F9495E968F9A1610C0CF9383053E5B5696ECC85CA3CA2A338C24C7204CC93881).

Также было выявлено количество секций – 4, импортируемые библиотеки – 1 (Kernel. dll), импортируемые функции – 2 (OutputDebugStringA, Sleep) и экспортируемая функция – 1 (DllRegisterServer).

Анализ позволил установить, что файл не был сжат с помощью UPX. Кроме того, обнаружена строка, содержащая буквы английского алфавита в верхнем и нижнем регистре, цифры и символы ‘+’ и ‘/’, что может свидетельствовать об использовании кодирования base64.

Также в процессе извлечения строк были выделены ранее найденные импортируемые функции и библиотеки, экспортируемая функция, а также повторное использование сегментов .rdata, .edata, .data. Результат извлечения строк представлен на рис. 3.


Defined Strings - 15 items

Location	String Value	String Representati...	Data Type
005f0000	MZ	"MZ"	char[2]
005f00e8	PE	"PE"	char[4]
005f01e0	.text	".text"	char[8]
005f0208	.rdata	".rdata"	char[8]
005f0230	.data	".data"	char[8]
005f0258	.reloc	".reloc"	char[8]
0062a260	ABCDEFGHIJKLMN...	"ABCDEFGHIJKLM...	ds
0062ab02		""	ds
0062ab08	DllRegisterServer	"DllRegisterServer"	ds
0062ab50	.rdata	".rdata"	ds
0062ab60	.edata	".edata"	ds
0062abd8	.data	".data"	ds
0062ac26	Sleep	"Sleep"	ds
0062ac2e	OutputDebugStrin...	"OutputDebugStrin...	ds
0062ac42	KERNEL32.dll	"KERNEL32.dll"	ds

Рис. 3. Извлечение строк
Fig. 3. String extraction

Особое внимание следует уделить импортируемой функции OutputDebugStringA, которая может свидетельствовать об использовании метода противодействия отладке. Обнаружение данной функции указывает на необходимость дополнительного анализа для определения конкретных методов защиты, используемых в файле malware.bin.

Предположение о возможном использовании обфускации или сжатия в исполняемом файле может быть подтверждено путем анализа энтропии файла.

Высокие значения энтропии на определенном участке могут указывать на наличие шифрования сегмента. Для определения энтропии файла был использован инструмент binwalk, как показано на рис. 4.

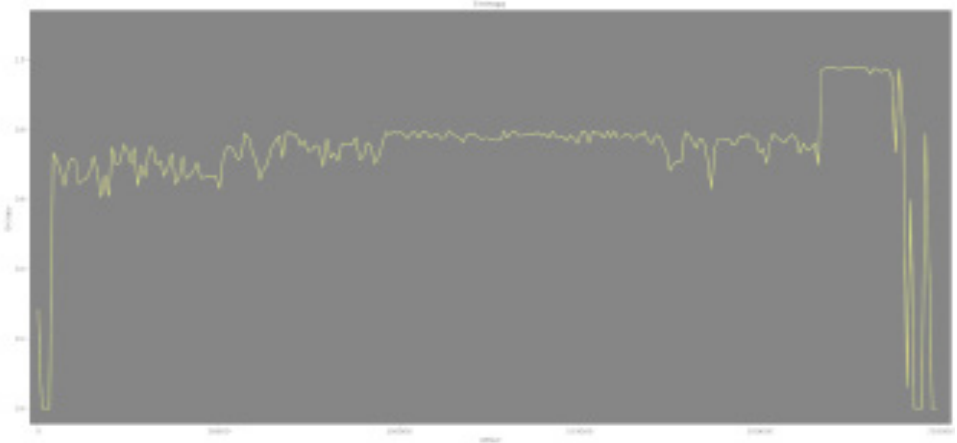


Рис. 4. Результат подсчета энтропии
Fig. 4. Entropy calculation result

Следует отметить, что сжатие наблюдается в интервале от 217000 до 234000 байт.

В процессе исследования бинарного файла с использованием программного

обеспечения Ghidra было выявлено отсутствие функции main или ее аналога, при этом код начинает исполняться с функции entry.

В ходе анализа данной функции было обнаружено взаимодействие с неинициализированными областями памяти в стеке, а также вызов других функций. Кроме того, были выявлены функции CRC32 хэширования, нахождения DLL, нахождения WinAPI и обнаружения WinAPI по табличным спискам.

В строке кода uVar10 = (local_420[0] >> 1 ^ 0xedb88320) & uVar10 | ~uVar10 & local_420[0] >> 1 впервые встречается значение 0xedb88320, которое является реверсированным представлением для CRC-32 (IEEE 802.3).

Также была обнаружена функция шифрования и расшифровывания, осуществляемая с помощью алгоритма RC4. Ключ для этого алгоритма расположен в секции .rdata и представляет собой поток байтов.

Среди информации, выделенной в ходе анализа, можно отметить наличие расширенной библиотеки API Windows (AdvApi32), API состояния процесса (PsApi), API программы оболочки Windows (shlwapi), API рабочего интерфейса Windows (shell32) и API для сетевого взаимодействия Windows (WinInet) [4].

В результате анализа были выделены следующие техники, используемые в исследуемом ВПО: использование системного API (T1106), обфусцированные файлы или конфигурации (T1027), изучение информации об установленном ПО (T1518), зашифрованные каналы связи: симметричные алгоритмы шифрования (T1573) и изучение информации о конфигурации системы (T1082).

Кроме того, отличительной особенностью может являться использование CRC32 хэширования для сокрытия информации об используемых библиотеках, использование OutputDebugString для анти-отладки и использование RC4 для шифрования конфигурации.

В результате анализа техник и особенностей, используемых в данном вредоносном ПО, было выявлено, что оно принадлежит к семейству банковских троянов Dridex. Для получения информации из данного семейства можно использовать инструмент AppGate Lab Dridex Toolkit. Результат извлечения адресов представлен на рис. 5.

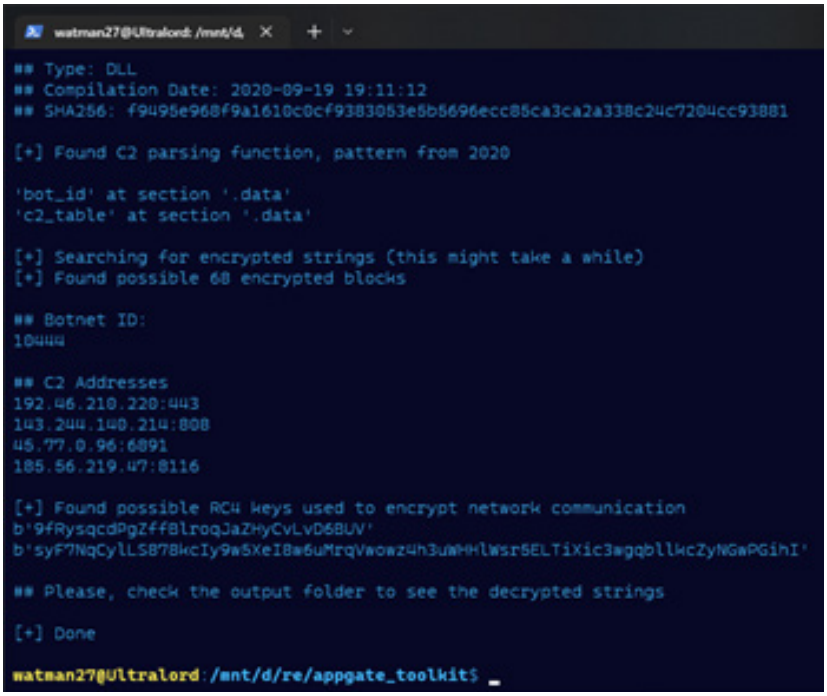


Рис. 5. Результат извлечения адресов C2, botnet ID и RC4 ключа для шифрования трафика
Fig. 5. The result of extracting the addresses of C2, botnet ID and RC4 key for traffic encryption

Результаты проверки на сайте VirusTotal подтверждают предположения об обнаружении банковской троянской программы Dridex в большинстве антивирусных программ (рис. 6).

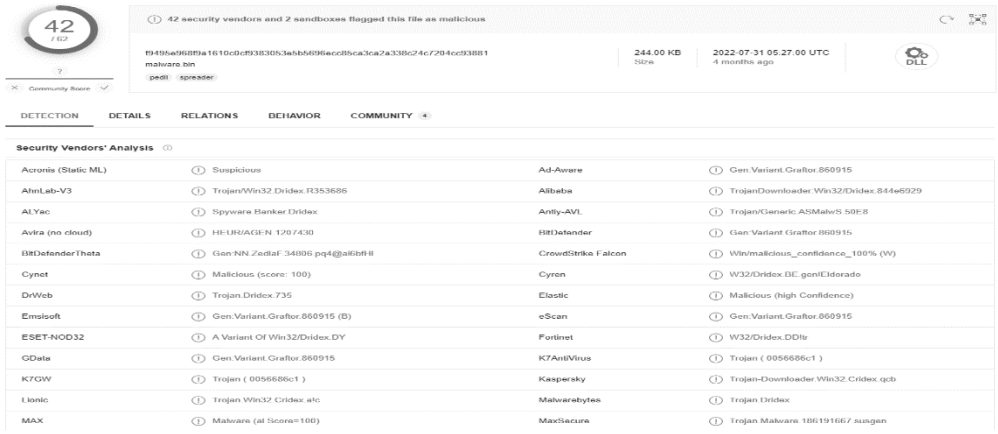


Рис. 6. Результат проверки на VirusTotal
Fig. 6. The result of checking for VirusTotal

Вывод. Результат подтверждается как при проверке исходного файла, так и при проверке хэш-суммы файла по алгоритму SHA-256, что свидетельствует о том, что это известный образец вредоносного программного обеспечения.

На основе проведенного анализа можно разработать правила для обнаружения вредоносного программного обеспечения этого семейства в будущем.

Библиографический список:

1. Актуальные киберугрозы для промышленных организаций: итоги 2022 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/industrial-cybersecurity-threatscape-2022/ (дата обращения: 25.03.2023).
2. Годовой ущерб от киберпреступлений может составить 165 млрд рублей. URL: https://www.banki.ru/news/lenta/?id=10961269 (дата обращения: 25.03.2023).
3. Ghidra. URL: https://xakep.ru/2019/03/20/nsa-ghidra/ (дата обращения: 25.03.2023).
4. Ионеску А. Внутреннее устройство Windows. СПб: Питер, 2022. 563 с.
5. https://www.kaspersky.com/blog
6. https://habr.com/
7. https://www.anti-malware.ru/
8. https://krebsonsecurity.com/
9. https://edu.ptsecurity.com/mira/
10. https://partners.kaspersky.com/

References

1. Current cyber threats for industrial organizations: results of 2022. URL: https://www.ptsecurity.com/ru-ru/research/analytics/industrial-cybersecurity-threatscape-2022/ (accessed date: 25.03.2023).
2. The annual damage from cybercrime may amount to 165 billion rubles. URL: https://www.banki.ru/news/lenta/?id=10961269 (accessed date: 25.03.2023).
3. Ghidra. URL: https://xakep.ru/2019/03/20/nsa-ghidra/ (accessed date: 25.03.2023).
4. Ionescu A. Windows internals. St. Petersburg: Peter, 2022. 563 p.
5. https://www.kaspersky.com/blog
6. https://habr.com/ (общая информация по ИБ тематике)
7. https://www.anti-malware.ru/
8. https://krebsonsecurity.com/
9. https://edu.ptsecurity.com/mira/
10. https://partners.kaspersky.com/

Сведения об авторах:

Елизаров Дмитрий Александрович, кандидат технических наук, доцент; доцент кафедры «Информационная безопасность»; elizarovda@gmail.com.

Алексей Викторович Катков, студент; elizarovda@gmail.com.

Information about authors:

Dmitry A. Elizarov, Cand. Sci.(Eng.), Assoc. Prof., Department «Information security»; elizarovda@gmail.com.

Alexey V. Katkov, student; elizarovda@gmail.com

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/Received 04.07.2023.

Одобрена после рецензирования/ Reviced 30.07.2023.

Принята в печать/Accepted for publication 30.07.2023.