УДК 004.056

Аминев Б.Р., Бурангулов Д.Б.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Фатхелисламов А.Ф.
Уфимский университет науки и технологий, Уфа

ВЫЯВЛЕНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СБОРА ИНФОРМАЦИИ В ОПЕРАЦИОННОЙ СИСТЕМЕ КОМПЬЮТЕРА

Аннотация. В статье рассмотрено программное обеспечение LanAgent, представляющее собой кейлоггер, и его анализ с помощью Wireshark.

Исследованы методы выявления и удаления подобных программ, а также их влияние на локальную сеть. Особое внимание уделено скрытности работы кейлоггеров и способам защиты от них.
Ключевые слова: кейлоггер, сетевой трафик, шпионское ПО, информационная безопасность, анализ данных.

В наше время киберугрозы становятся все более распространенными и могут причинить серьезный вред как индивидуальным пользователям, так и компаниям. Одна из таких киберугроз это кейлоггеры.

Кейлоггеры – это программное или аппаратное средство, предназначенное для фиксации и сохранения всех нажатий клавиш на клавиатуре компьютера или другого устройства. Это может включать пароли, логины, личные сообщения, тексты документов и другие данные, которые пользователь вводит с клавиатуры.

Программы такого типа могут использоваться как в рамках закона, например, в корпоративной среде для мониторинга сотрудников, так и с нарушением законодательства, когда они используются для кражи личной информации. В данной научной статье рассматривается программное обеспечение для мониторинга за сотрудниками и то, как это программное обеспечение может использоваться злоумышленниками.

LanAgent – это программное обеспечение, предназначенное для скрытого мониторинга работы сотрудников внутри организаций. Он предназначен для отслеживания действий пользователей в сети, анализа их активности и обеспечения контроля над рабочими процессами. Программа часто используется администраторами и руководителями для повышения производительности труда сотрудников и оптимизации трудовых ресурсов.

Чтобы провести анализ работы кейлоггеров была скачена и установлена программа LanAgent на два ноутбука подключенные к локальной сети. Один из них был ноутбук простого пользователя. Второй ноутбук был администратора, который следил за пользователем. Предварительно на ноутбук пользователя был установлен анализатор сетевого трафика Wireshark и пользовательская версия программы LanAgent. Первое что бросается в глаза это то, что после установки пользовательской версии LanAgent нет никаких ярлыков приложения, создается только папка в каталоге C:\Windows\SysWOW64\LASys. На первый взгляд нет никаких отклонений в работе операционной системы, все работает так же, как и работало до этого. На устройство администратора была установлена административная версия программного обеспечения LanAgent. После установки программы на рабочем столе появилась не посредственно сама программа. LanAgent простейшее программное обеспечение, открыв программу можно легко добавить нового пользователя по его локальному IP адресу и сразу же начать отслеживать его действия. В программе можно применить настройки для

каждого пользователя отдельно. К примеру, у одного пользователя периодичность снимка экрана будет 5 минут, а у другого минута.

На ноутбуке пользователя это никак уведомлений о том, что за ним следят не будет. На работу операционной системы так же ничего не влияет, все работает в штатном режиме. Однако действия администратора в приложение можно отследить с помощью анализатора трафика Wireshark. Wireshark – это мощное и широко используемое программное обеспечение предназначенное для анализа сетевого трафика. Он позволяет изучать детали передачи данных в реальном времени. Данная программа может использоваться для анализа как проводных, так и беспроводных сетей. Это позволяет применять его в самых разных областях: от локальных офисных сетей до глобальных подключений через интернет.

При каждом изменение настроек или запрашивание «логов» со стороны администратора отслеживается подозрительная активность сетевого трафика. На работу это никак не влияет, но с помощью Wireshark можно заметить отравление и получение множества пакетов со стороны администратора пользователю и от пользователя администратору. С использованием анализатора сетевого трафика было установлено, что все собранные данные, включая текстовую информацию и снимки экрана, сохраняются локально на устройстве пользователя. Так информация на ноутбук администратора поступала не постоянно, он ее получал при обновление «логов» и сразу же после этого начинается отправка пакетов на ноутбук администратора.

Исходя из работы с Wireshark было установлено, что наличие кейлоггера можно выявить по следующим причинам: большие объемы исходящего трафика, подозрительные пакеты, отправляемые на неизвестные IP-адреса, используемые протоколы. Кейлоггер использовал такие протоколы, как HTTP/HTTPS (для отправки данных на удаленные серверы), TCP/UDP (для связи), FTP/SFTP (для загрузки файлов), SMTP (для отправки данных на электронную почту).

Другим способом выявления LanAgent является анализ всех активных приложений и системных процессов на пользовательском ноутбуке. Обычно такие процессы имеют необычные названия или не являются стандартными для операционной системы. При их анализе стоит обращать внимание на расположение исполняемого файла, его версию и информацию о разработчике. К тому же нужно учитывать показатели использования центрального процессор, памяти и сетевой активности. При обнаружении подозрительного процесса, выполнить поиск в интернете по его имени, чтобы проверить является ли он вредоносным ПО.

На ряду с этим для выявления кейлоггера можно использовать специальные утилиты для дополнительного поиска шпионского ПО. Использование обычных антивирусных программ может не дать желаемого результата, так как LanAgent будет рассматриваться ими как обычное приложение, не являющееся вредоносным ПО.

Избавиться от кейлоггера в нашем случае можно через пакет установщика. Проводится вся таже процедура с установкой, но только при повторном открытие установщика программа сама предлагает удалить себя. В случае, когда нет доступа к пакету установщика стоит открыть диспетчер задач и в фоновых задачах искать подозрительные задачи. У нас эта задача system.exe (32 bit). Проведен анализ информации о данном процессе с использованием интернет-ресурсов, в результате которого был сделан вывод о его принадлежности к категории вредоносного программного обеспечения. Затем перешли в расположение папки, завершили задачу процесса и в безопасности папки выдали полный доступ пользователю. Впоследствии нам удалось удалить папку с кейлоггером.

В рамках проведенного исследования мы детально изучили функционал программы LanAgent, которая представляет собой кейлоггер. Особое внимание уделялось ее влиянию на локальную сеть и взаимодействию между устройствами пользователей и администраторов. Анализ показал, что данное программное обеспечение обладает высокой степенью скрытности: оно не отображается в списке активных приложений, не создает уведомлений для пользователя и работает в фоновом режиме, не оказывая заметного влияния на производительность системы.

Кроме того, исследование позволило определить способы обнаружения и удаления кейлоггеров. Один из подходов заключается в анализе процессов операционной системы, где ключевыми признаками являются нестандартные названия исполняемых файлов, их расположение и аномальная нагрузка на системные ресурсы. К тому же было установлено, что использование специализированных утилит для поиска шпионского ПО может быть более результативным, чем применение классических антивирусных решений, которые зачастую не распознают подобные программы как угрозу.

Список использованных источников:

1. Баланов А.Н. Кибербезопасность: учебное пособие для вузов. 2-е изд., стер. М.: Издательство «Лань», 2025. 680 с. ISBN 978-5-507-52709-0.

2. Голубцов И.С., Голубцова Е.С. Кейлоггеры: Электрон. версия. М.: Общество с ограниченной ответственностью «Интернаука», 2021. Студенческий вестник. № 17-6 (162). С. 56–57. URL: https://www.elibrary.ru/item.asp?id=45795122 (дата обращения: 05.04.2025)

3. Давидюк Н.В., Космачева И.М. Мониторинг безопасности информационных систем: практикум для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и направлений 10.03.01 «Информационная безопасность», 10.04.01 «Информационная безопасность». М.: ИЦ Интермедия, 2020. 116 с.

4. Николаева М.О. Информационная безопасность: современная картина проблемы информационной безопасности и защиты информации: Электрон. версия. Челябинск: Челябинский институт развития

профессионального образования, 2023. Т. 1, № 1. С. 51–57. URL: https://www.elibrary.ru/item.asp?id=54211958 (дата обращения: 06.04.2025).

5. Wireshark – подробное руководство по началу использования. URL: https://habr.com/ru/articles/735866/ (дата обращения: 10.04.2025).

6. Руководство пользователя LanAgent Terminal. URL: https://lanagent.ru/documents/manual_terminal.pdf (дата обращения: 04.04.2025).

7. Бабанов Н.Ю., Евстифеев А.А., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Основы защиты информации в современных информационных системах: учебное пособие. М.: Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики, 2022. 175 с.

8. Крыгин Н.Д. Шпионское программное обеспечение // Донской государственный технический университет, 2022. Столыпинский вестник. Т. 4, № 4. Порядковый номер 11. URL: https://www.elibrary.ru/item.asp?id=49403090 (дата обращения: 05.04.2025).

Aminev B.R., Burangulov D.B.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

IDENTIFICATION OF MALICIOUS SOFTWARE FOR COLLECTING INFORMATION IN THE COMPUTER'S OPERATING SYSTEM

Abstract. The article discusses LanAgent software, which is a keylogger, and its analysis using Wireshark. The methods of detecting and removing such programs, as well as their impact on the local network, are investigated. Special attention is paid to the secrecy of keyloggers and ways to protect against them.

Keywords: keylogger, network traffic, spyware, information security, data analysis.