УДК 004.491
DOI: 10.33764/2618-981X-2019-9-15-18

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И МЕТОДЫ БОРЬБЫ С НИМ

Тимофей Владимирович Таржанов
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, обучающийся

Вадим Евгеньевич Кудряшов
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, обучающийся

Диана Георгиевна Макарова
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: kaf.ib@ssga.ru

В статье рассматривается существующее вредоносное программное обеспечение. Для изучения особенностей построения вредоносного программного обеспечения были проанализированы самые распространенные компьютерные вирусы. Разработана программа по захвату нажатий клавиатуры средствами языка Python 3.7, а также реализована функция отправки на почту захваченных данных.

Ключевые слова: вирус, вредоносное программное обеспечение, средства защиты информации, антивирусное программное обеспечение.

DELETRIOUS SOFTWARE AND METHODS FOR COMBATING IT

Timofey V. Tarzhanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student

Vadim E. Kudryashov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student

Diana G. Makarova
Siberian State University of Geosystems and Technologies,10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (383)343-91-11, e-mail: kaf.ib@ssga.ru

The article discusses existing malware. To study the features of building deletrious software, the most common computer viruses were analyzed. A program for capturing keystrokes by means of the Python 3.7 language was developed, and a function for sending captured data to mail was implemented.

Key words: virus, malware, information security tools, antivirus software.

Компьютерный вирус – вид вредоносного программного обеспечения, способный внедряться в код других исполняемых программ, системные области памяти, загрузочные секторы, а также распространять свои копии, используя различные каналы связи.

Первые вирусные эпидемии относятся к 1986–1989 годам: Brain (вызвал крупнейшую эпидемию), Jerusalem (уничтожал программы при их запуске), червь Морриса (свыше 6200 компьютеров было заражено, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах). Тогда же оформились основные классы двоичных вирусов: сетевые черви (червь Морриса), «троянские кони» (AIDS), полиморфные вирусы (Chameleon), стелс-вирусы (Frodo, Whale) [1–3].

В настоящее время принято разделять следующие категории вирусов:

– по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);

– файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят зараженный файл, «спутники» идут отдельным файлом.

– по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Android);

– по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);

– по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);

– по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.)

В настоящее время наибольшее распространение получило следующее вредоносное программное обеспечение:

– вирус – программное обеспечение, которое дублирует себя множество раз и внедряет эти копии в другие программы и файлы;

– червь – то же, что и вирусы, но в отличие от них, у червей единицей заражения являются не файлы и документы, а компьютеры (иногда, сетевые устройства);

– логическая бомба – специфический вид вредоносных программ, который проявляет себя только при определенных действиях или событиях (наступление дат, открытие каких-либо файлов и прочее), а остальную часть времени бездействует;

– троян, или троянский конь – программное обеспечение, которое может не только выдавать себя за полезную программу, но и в реальности предоставлять полезные функции, в качестве прикрытия для деструктивных действий;

– клавиатурный шпион – особый вид трояна, который записывает все нажатия кнопок клавиатуры и/или действия мышки на вашем компьютере;

– руткит – скрытый тип вредоносного программного обеспечения, который выполняется на уровне ядра операционной системы. Основной опасностью руткитов является то, что, внедряясь на уровень ядра системы, руткиты могут выполнять любые действия и с легкостью обходить любые системы защиты, ведь для своего скрытия им достаточно отказать в доступе средствам безопасности.

Для отработки методики антивирусного программного обеспечения была смоделирована работа клавиатурного шпиона (кейлоггера).

Кейлоггер – программное обеспечение, регистрирующее различные действия пользователя, а именно, нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т.д. Кейлоггеры оказались самым распространенным способом кражи конфиденциальной информации, передвинув фишинг на второе место, и действуют все более избирательно: отслеживая веб-страницы, к которым обращается пользователь, они записывают нажатия клавиш только при заходе на сайты, интересующие злоумышленников [4].

Предложенный кейлоггер реализуется одним скриптом, в котором описаны следующие функции:

– функция addStartup() добавляет созданный кейлоггер в реестр, он будет запускаться автоматически при загрузке ОС;

– функция Hide() маскирует работу вируса, предотвращая появление командной строки (консоли);

– функция Mail_it() отвечает за отправку захваченной информации по почте;

– функция OnKeyboardEvent() отвечает за считывание нажатых клавиш и запись этой информации в текстовый файл.

Алгоритм работы предложенного кейлоггера следующий: пользователь запускает кейлоггер; программа перехватывает и записывает в текстовый файл нажатую клавишу, окно, в котором она была нажата, дату и время нажатия; затем происходит отправка захваченной информации на почту.

В работе кейлоггера возможны следующие варианты маскировки:

– с помощью утилиты pyinstaller создается exe-файл имеющегося скрипта. Создается его ярлык на рабочем столе рабочей станции, изменяется иконка и название, например на Skype. При запуске ярлыка ничего не открывается, но скрипт исполняется (в диспетчере задач процесс стал фоновым);

– из созданного exe-файла создается sfx-архив с помощью WinRAR. При открытии архива скрипт выполняется (в диспетчере задач процесс поменял название);

– через текстовый редактор создается bat-файл, который открывает одновременно браузер и exe-файл. Затем создается ярлык, прописав в объекте путь до имеющегося bat-файла (в диспетчере задач процесс скрыт);

– exe-файл маскируется под файл word, excel, или powerpoint с помощью утилиты backdoorppt. Этот вариант лучше остальных, так как он остается не-

замеченным антивирусным программным обеспечением, а в диспетчере задач процесс неотличим от исполнения процесса файлом word.

Наиболее актуальными методами защиты от кейлоггеров являются:

– использование одноразовых паролей;

– двухфакторная аутентификация;

– использование систем проактивной защиты, предназначенных для обнаружения программных кейлоггеров;

– использование виртуальных клавиатур.

Очевидно, что вредоносное программное обеспечение может быть использовано для кражи персональной информации и шпионажа. Компании, работающие в сфере компьютерной безопасности, фиксируют рост числа вредоносных программ, имеющих функциональность кейлоггера. В настоящее время кейлоггеры, наряду с фишингом и методами социальной инженерии, являются одним из главных методов электронного мошенничества. Все чаще в кейлоггеры добавляют rootkit-технологии, которые скрывают работу кейлоггера так, чтобы она не была видна ни пользователю, ни антивирусному программному обеспечению. Обнаружить и обезвредить такие кейлоггеры можно только с использованием специально разработанных средств защиты [5].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста / К. Е. Климентьев. – М. : ДМК Пресс, 2013. – 656 с. – ISBN 978-5-94074-885-4. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/63192.

2. Монаппа, К. А. Анализ вредоносных программ / К. А. Монаппа ; перевод с английского Д. А. Беликова. – М. : ДМК Пресс, 2019. – 452 с. – ISBN 978-5-97060-700-8. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/123709.

3. Нестеров С. А. Основы информационной безопасности : учеб. пособие. – 5-е изд., стер. – Санкт-Петербург : Лань, 2019. – 324 с. – ISBN 978-5-8114-4067-2. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/114688.

4. Жернаков, С.В. Система обнаружения вредоносных программ в операционной системе ANDROID / С.В. Жернаков, Г.Н. Гаврилов // Вестник Уфимского государственного авиационного технического университета. – 2016. – № 2. – С. 117-122. – ISSN 1992-6502. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/journal/issue/301803.

5. Keyloggers: How they work and how to detect them (Part 1) 2007. URL: https://securelist.com/analysis/publications/36138/keyloggers how they work and how to detect them part 1/.