УДК 681.3

АНАЛИЗ ВИДОВ, УГРОЗ И МЕТОДОВ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ ЧЕРВЕЙ

Р.Х. БАГДАСАРЯН, А.Д. ТЫРТЫШНЫЙ, А.В. ШВЕДЧИКОВА

Кубанский государственный технологический университет,
350072, Российская Федерация, г. Краснодар, ул. Московская, 2;
электронная почта: rafael_555@mail.ru

Защита информации всегда актуальна, и вопреки стремительным темпам развития информационных технологий всегда где-то скрывается уязвимость, которую рано или поздно использует злоумышленник. Одним из основных видов вредоносных программ являются компьютерные черви. Несмотря на то, что их история началась с 1978 года, программы-черви пользуются успехом у хакеров по сей день. В данной статье рассматривается понятие компьютерного червя, базовая функциональная структура, жизненный цикл программы-червя, виды, угрозы и методы защиты от данных вредоносных программ. Цель исследования состоит в реализации краткого и содержательного описания структуры, принципов работы и классификации компьютерных червей и рекомендаций по собственному обнаружению и защите компьютера от их воздействия. Материалы могут быть полезны для подготовки бакалавров, изучающих такие дисциплины, как «Сети и системы передачи информации» и «Основы информационной безопасности».
Ключевые слова: вредоносные программы, компьютерные черви, программы-черви

Компьютерные черви – один из видов вредоносных программ, способных самостоятельно проникать в компьютеры, распространять и запускать свои копии. Свое название компьютерный червь приобрел вследствие способности несанкционированно размножать свои дубликаты , т.е. «переползать» с одного компьютера на следующие. От классических вирусов их отличает использование сетевых ресурсов для дальнейшего распространения копий на удалённые компьютеры. Классический вирус не способен автономно внедряться в другие вычислительные устройства, он распространяется на локальных ресурсах компьютера. [1]

Всякий компьютерный червь в основе включает пару базовых функциональных сегментов. Функциональная структура сетевого червя представлена на рисунке 1.

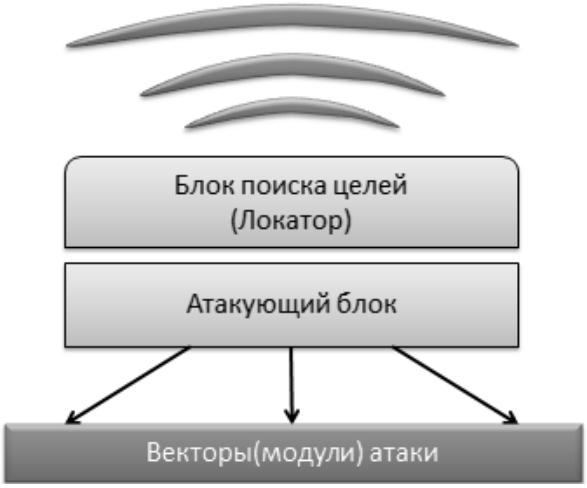

Рисунок 1 – Функциональная структура сетевого червя

Первый блок (локатор) собирает сведения об узлах сети компьютера (по ARP-таблицам, адресатам электронной почты, по UDP и TCP-портам и др.) и на их базе выводит диапазон узлов, на уязвимости которых имеются соответствующие механизмы атаки. Затем полученные данные применяет атакующий блок программы, состоящий из спектра механизмов (модулей) атаки. Модули атаки классифицируются по двум основным целям: ориентированные на уязвимости системы администрирования ПО и использующие средства социальной инженерии (путём убеждения самого пользователя к запуску зараженного файла). Некоторые сетевые черви могут быть расширены блоками удалённого регулирования и взаимодействия, управления жизненным циклом, фиксацией событий и другими. [2]

Жизненный цикл программы-червя представляет собой рекурсивный цикл и упрощённо выглядит следующим образом: сетевой червь активируется на компьютере, запускает локатор уязвимых целей, пересылает копии на выявленные уязвимые узлы через сеть, на которых затем копии запускаются и так же повторяют алгоритм. Лавинообразное распространение компьютерных червей представлено на рисунке 2.

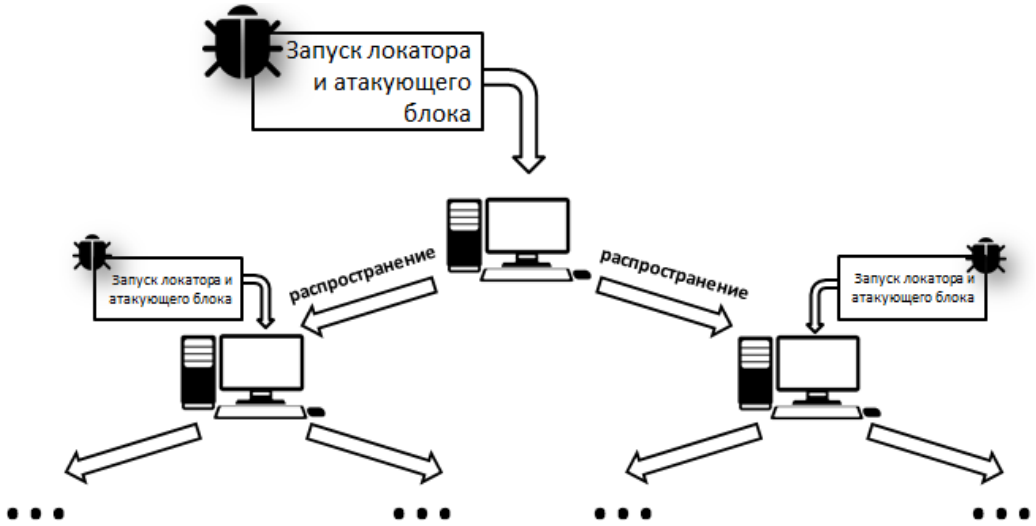

Рисунок 2 – Лавинообразное распространение компьютерных червей

Стоит отметить, что современные компьютерные черви редко стремятся как можно дольше и скрытно сохраниться на компьютере. Зачастую они имеют определенный временной период, а затем самоуничтожаются, разослав гигабайты спам-информации другим компьютерам. От вирусов их также отличает нацеленность на выполнение конкретных действий, например преодоление системы защиты от несанкционированного доступа.

Помимо своего вредоносного воздействия, атаки сетевых червей способны спровоцировать очаги атак типа отказ в обслуживании (DoS, Denial of Service), если в их функционировании не предусмотрено игнорирование подвергающихся атаке или заражённых узлов. [3]

В зависимости от среды распространения компьютерные черви подразделяются на почтовые, IM, IRC, P2P и Net-черви. [4]

Почтовые черви распространяются в виде вложения или ссылки в сообщениях электронной почты (например, Email-Worm.Win32.Zafi.d.). В некоторых случаях вложение может иметь «двойное» расширение с целью ввести в заблуждение пользователя и побудить его запустить файл (исполнительная программа под видом изображения с названием “открытка.jpg.exe” и т.п.). [4]

IM-черви используют тот же способ распространения, что и почтовые, только в системах мгновенного обмена сообщениями (instant messaging), таких, как ICQ, Skype, Viber и т.п. (например, IM-Worm.Win32.Kelvir.k) [4]

IRC-черви используют указанный выше способ распространения в сетях обмена сообщениями в реальном времени (Internet Relay Chat), таких, как mIRC, KVirc, XChat и других (например, червь IRC-Worm.Win32.Golember.a). [4]

P2P-черви циркулируют в файлообменных одноранговых (пиринговых) сетях, таких как RShare, DirectConnect, BitTorrent и подобных, где могут внедриться в каталог обмена файлами заражённого узла, а затем попасть вместе с файлами к новым узлам сети (например, червь Email-Worm.Win32.Netsky.q) Также существуют модификации данного вида червей, позволяющие формировать положительный ответ на поисковые запросы других пользователей пиринговой сети для передачи вредоносного файла, тем самым значительно ускоряя процесс заражения пользователей сети. [4]

Net-черви включают все прочие виды, такие как Web-черви, LAN-черви и другие (например, семейство Net-Worm.Win32.Sasser). [4]

Самой распространённой уязвимостью, которая активно применяется программами-червями является ошибка переполнения буфера. Для нормального функционирования программ большое значение имеет вместимость данных в диапазон выделенного им объема, т.к. иначе они будут сохраняться вместо команды возврата из процедуры. Суть атаки заключается в том, что атакующий сегмент передаёт узлу запрос длиной заведомо больше буфера, со сдвигом кода команды перехода к вредоносной программе, совпадающим с расположением команды возврата в процедуру приложения атакуемого узла. Ошибка переполнения буфера побуждает замену возврата из процедуры передачей управления программе-червю. Затем программа копирует недостающие программные модули на компьютер. Так, в ноябре 2016 года о себе вновь заявил известный ранее червь SQL Slammer, который использовал указанную выше уязвимость в продуктах Microsoft SQL Server и

Desktop Engine. Усугубил его влияние тот факт, что после исправления данной уязвимости не все пользователи посчитали нужным произвести обновление продуктов. Потому такая тривиальная процедура, как обновление ПО компьютера, является одним из наиболее эффективных методов защиты от компьютерных червей. [5]

Высокую угрозу для пользователя несут так называемые активные виды компьютерных червей, так как они способны автоматически запускать вредоносный скрипт через браузер. Чаще всего данные скрипты скрываются в баннерах и всплывающих окнах веб-страниц. Во избежание подобной ситуации можно запретить в браузере запуск скриптов, но это может повлиять на правильную работу некоторых веб-сайтов, использующих скрипты в благих целях. Потому оптимальнее использовать межсетевые экраны и модули проверки скриптов на наличие вредоносного кода, которые должны входить в состав Web-антивирусных программ. [6]

Также помимо перечисленных выше сред распространения, компьютерные черви могут под видом файла автозапуска (Autorun.inf), в съемных носителях, потому следует отключить функцию автозапуска носителей. Некоторые программы-черви внедряются в файлы программ Microsoft Office (*.doc, *. xls) в форме макроса, активируясь при запуске соответствующего заражённого документа. [6]

Некоторые усовершенствованные виды компьютерных червей способны противодействовать антивирусам, выгружая их из оперативной памяти и тем самым блокируя доступ к сайтам антивирусных компаний. Потому также важно выбирать антивирусное ПО с учётом не только его качества обнаружения вредоносных программ, но и активным противодействием их реализации. Все необходимые файлы и данные червь получает с управляющих серверов. Но, например, компьютерные черви вида Net-Worm.Bagle.n и Net-Worm.Bagle.p кроме своего распространения по почте и обмена файлами между сетями способны отключать большую часть антивирусов, а также могут заражать исполняемые файлы. [6]

В настоящее время имеют популярность резидентные черви, против которых использования антивирусного ПО с сигнатурами недостаточно для полноценной защиты. Такие виды компьютерных червей инфицируют рабочую программу и находятся в оперативной памяти компьютера, никак не воздействуя на жесткие диски. Их особенность заключается в том, что они не имеют загрузчик, а используют динамические библиотеки, загруженные в память имеющимися в компьютере программами. Основной метод защиты от данного вида червей на ранней стадии состоит в перезапуске компьютера, который соответственно приведёт к сбросу ОЗУ с размещённым на нём вирусом. Затем следует убедиться в отсутствии подозрительных программ в каталоге автозапуска.

Компьютерных червей объединяют некоторые признаки, по которым пользователь может самостоятельно определить их воздействие. В случае подозрения на заражение компьютерным червем стоит отключить доступ в интернет, используя его только при крайней необходимости.

В первую очередь, помимо возможной неработоспособности антивирусных программ, перестают функционировать системные службы Windows Update Service, Windows Defender, Windows Error Reporting Services, IPSec, отвечающие за безопасность компьютера и сети. Затем в большинстве случаев наблюдается значительное повышение использования ресурсов ЦП процессом для оперативной работы службами - svchost.exe, вплоть до предупреждения о стопроцентной нагрузке. Данные признаки можно обнаружить в окне диспетчера задач во вкладках «Процессы» и «Производительность», а проверка состояния системных служб возможна во вкладке «Службы». Если не удаётся перезапустить службы во вкладке (если они не выполняются), то велика вероятность активного заражения компьютерным червём. В некоторых случаях полезно использовать специализированные расширенные программы для просмотра активных процессов, так как современные компьютерные черви могут скрывать свои активные процессы от стандартных утилит Windows.

Некоторые компьютерные черви могут находиться в каталоге автозапуска, поэтому рекомендуется проверить их на наличие подозрительных файлов и отправить их на анализ компании-разработчику антивируса. Обычно данный каталог представляет собой адрес следующего вида: \%Documents and Settings%\%user name%\Start Menu\Programs\Startup\.

В большинстве случаев компьютерные черви располагаются в системных каталогах system и system32, windows. С помощью сортировки по времени в любом файловом менеджере можно проанализировать данные каталоги на наличие подозрительных файлов и также отправить их на проверку. Самостоятельное удаление подозрительных файлов с системных каталогов крайне нежелательно, так как имеется риск удалить необходимые для работы Windows файлы.

В заключение можно сделать вывод, что компьютерные черви перегружают и выводят из строя сети и организуют сетевые атаки, рассылают спам-сообщения. Путём анализа рекомендаций и собственного опыта были предложены признаки и методы защиты от компьютерных червей, представляющие собой обобщённый алгоритм для предотвращения негативных последствий вирусной программы в случае неработоспособности антивирусного ПО. Во избежание таких атак настоятельно рекомендуется комплексная защита, которая состоит из межсетевого экранирования, обеспечивающего проверку всех Web-страниц; проверки скриптов на языках JavaScript и VBScript; своевременного обновления приложений и операционной системы, а также осторожности с подозрительными вложенными файлами и ссылками.

ЛИТЕРАТУРА

1. Лекция 3: Классификация вирусов // Национальный открытый университет Интуит – URL: http://www.intuit.ru/studies/courses/1042/154/lecture/4277 Дата обращения: 29.03.2017

2. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010 – 944 с.

3. Евгения Вострякова. Сетевые черви и троянские программы. Распространение. Основные методы заражения. // Северный филиал инновационных технологий и управления - URL: http://www.in-nov.ru/node/900 Дата обращения: 28.03.2017

4. Типы сетевых червей // Компания Center-Soft – URL: http://center-soft.ru/state/tipy_setev_chervei.html Дата обращения: 28.03.2017

5. Олег Иванов. Check Point: Сетевой червь SQL Slammer возобновил свою активность. // Аналитический центр Anti-Malware.ru – URL: https://www.anti-malware.ru/news/2017-02-06/22099 Дата обращения: 29.03.2017

6. Павел Токарев. Сетевые черви и защита от них // Веб-сервис для ведения блогов Blogger – URL: http://talzashit.blogspot.ru/p/blog-page_9889.html Дата обращения: 28.03.2017

REFERENCES

1. Lekcija 3: Klassifikacija virusov // Nacional'nyj otkrytyj universitet Intuit – URL: http://www.intuit.ru/studies/courses/1042/154/lecture/4277 Data obrashhenija: 29.03.2017

2. Olifer V. G., Olifer N. A. Komp'juternye seti. Principy, tehnologii, protokoly: Uchebnik dlja vuzov. 4-e izd. – SPb.: Piter, 2010 – 944 s.

3. Evgenija Vostrjakova. Setevye chervi i trojanskie programmy. Rasprostranenie. Osnovnye metody zarazhenija. // Severnyj filial innovacionnyh tehnologij i upravlenija - URL: http://www.in-nov.ru/node/900 Data obrashhenija: 28.03.2017

4. Tipy setevyh chervej // Kompanija Center-Soft – URL: http://center-soft.ru/state/tipy_setev_chervei.html Data obrashhenija: 28.03.2017

5. Oleg Ivanov. Check Point: Setevoj cherv' SQL Slammer vozobnovil svoju aktivnost'. // Analiticheskij centr Anti-Malware.ru – URL: https://www.anti-malware.ru/news/2017-02-06/22099 Data obrashhenija: 29.03.2017

6. Pavel Tokarev. Setevye chervi i zashhita ot nih // Veb-servis dlja vedenija blogov Blogger – URL: http://talzashit.blogspot.ru/p/blog-page_9889.html Data obrashhenija: 28.03.2017

THE ANALYSIS OF TYPES, THREATS AND METHODS OF PROTECTION FROM COMPUTER WORMS

R.KH. BAGDASARYAN, A.D. TYRTYSHNY, A.V. SHVEDCHIKOVA

Kuban State Technological University,
2, Moskovskaya St., Krasnodar, Russian Federation, 350072,
e-mail: rafael_555@mail.ru

The protection of the information is always relevant, and despite the rapid pace of information technology development, there is always a vulnerability somewhere, which may be used by the malefactor. One of the main types of malicious programs are computer worms. Despite the fact that their history began in 1978, worm programs are still success for hackers now. This article discusses the concept of a computer worm, the basic functional structure, the life cycle of a worm program, the types, threats, and methods of protecting against these malicious programs. The purpose of the research is to implement a brief and meaningful description of the structure, principles of operation and classification of computer worms and recommendations for own detection and protection of the computer from their impact. The materials can be useful for the training of bachelors studying such disciplines as "Networks and Information Transfer Systems" and "Fundamentals of Information Security".
Key words: malware, computer worms, worm programs.