УДК 004.056.57

ПРОБЛЕМЫ ВОЗНИКНОВЕНИЯ И ОСОБЕННОСТИ ПРОЯВЛЕНИЯ КОМПЬЮТЕРНЫХ ЗАГРУЗОЧНЫХ ВИРУСОВ ПРОНИКНОВЕНИЯ

Вильский Г. Б., *к.т.н., доцент Херсонської державної морської академії, e-mail: g.vilsky@gmail.com*;
Радов А. А., *інженер Міжнародного технологічного університету «Миколаївська політехніка», e-mail: alexradovbulgar@gmail.com*

Рассмотрены результаты исследования опасностей троянских вирусов проникновения, проявляющихся в виде технического изменения файловых систем компьютеров, копирования информации по запросу, или выкачивания из интернет вредоносных кодов с их распаковкой и запуском с жесткого информационного диска компьютера. Обоснована сочетаемость проявлений троянского вируса и желания киберпреступников управлять компьютерами в системах и сетях на расстоянии. Предлагается оценочный подход к установлению уязвимости компьютерной системы и сети, основанный на теоретическом моделировании.
***Ключевые слова**: атака, вирус, вредоносная программа, информация, киберпреступность, компьютер, сайт, сервер, троян.*

Постановка проблемы. Глобализация международных отношений стимулирует переход на цифровую экономику. Эти процессы коснулись и морской критической инфраструктуры. Растет компьютерная инженерия стивидорных компаний, морских портов, судов и т.п. Учитывая эту тенденцию, сотрудники морской инфраструктуры отчётливо понимают, что информационная безопасность цифрового обмена данными находится под постоянной угрозой компьютерных вредоносных программ (ВП), наносящих в большинстве случаев серьёзный и значительный ущерб их основной деятельности. Входящие в ВП загрузочные троянские вирусы относятся к компьютерным вирусам проникновения. Множество их разновидностей способно глубоко укореняться в системах с целью хищения данных и других злоумышленных воздействий. Этот тип вирусов обладает уникальными возможностями при выполнении определённых компьютерных и сетевых процедур, реализовывать свой код, что в конечном итоге приводит к нанесению вреда информационной безопасности компании. Описанная проблематика и связанное с ней решение актуальных задач по развитию современных информационных, коммуникационных технологий, отражено в Постановлении КМУ от 18.10.2017 № 980 «Некоторые вопросы определения среднесрочных приоритетных направлений инновационной деятельности общегосударственного уровня на 2017–2021 годы».

Анализ последних публикаций и постановка задачи исследования. Кибер защищённость цифровой коммуникативной среды, объектов критической информационной инфраструктуры, систем цифрового управления и коммерции достаточно широко освещается в специализированных научных журналах и трудах конференций, а законодательно представлено в документе [1]. Ретроспектива возникновения и совершенствования вирусных ВП, описанная в учебном пособии [2], отражается с акцентом на глобальный негативный охват систем и сетей. Классическая теория формирования и обнаружения вредоносного программного кода достаточно полно приведена в работе [3]. Большинство публикаций о троянских вирусах проникновения отмечают их способность к репродуцированию и реализации функции нанесения ущерба путем запуска программ уничтожения доступной информации, переформатирования жёстких дисков и изменения конфигурации компьютеров, что детально отмечается в работах [2, 4]. О настоящем состоянии кибер эпидемии ВП говорится в работе [5]. Ближайшее будущее прогнозируется ускоренным развитием таких эпидемий, с целью нанесения беспримерных, существенных ущербов. Такое состояние станет реальным благодаря масштабным результатам изучения и предварительного анализа состояния сетей передачи данных, оформленного в виде списка наиболее уязвимых компьютеров для лавинообразного вирусного заражения других компьютеров. Инструментом противодействия созданию и распространению вирусных ВП

представляется разработка методов предсказания заражённостей и моделирование мер противодействия с устранением уязвимостей компьютеров [6]. Возможные и основные математические модели прогнозирования возникновения и распространения ВП в информационных базах вычислительных систем приводятся в [7]. Рассмотренные публикации позволяют сделать вывод о том, что защищённость компьютеров и сетей зависит от чёткости представления условий возникновения и особенностей проявления особо опасных троянских вирусов проникновения. Для выявления научно-практических подходов устранения проблемы требуется выполнение исследований, направленных на решение задач существенной минимизации угроз и рисков ВП компьютерным мощностям производственно-экономических систем.

Цель статьи. Представление полученных результатов исследований по оценке проблем возникновения и особенностям проявления вирусов проникновения в компьютерных системах семейства Windows и сетях.

Изложение материалов исследования. В настоящей работе будут рассмотрены троянские вирусы проникновения в ВП, наносящие ущерб кибернетическому оснащению морской критической инфраструктуре. Исследование проводилось методами экспертных оценок, дескриптивного анализа и обобщения собственной экспериментальной практики защитных мер по предупреждению кибератак и вредоносного воздействия таких троянских вирусов проникновения, как Backdoor, Trojan-PSW, LNK/Agent, Rootkit, Krepper. Структура и функциональное соответствие этих троянских вирусов отвечает большей части современных вредоносных программ.

Понимая, что каждый троянский вирус пишется специально для выполнения конкретной зловредной функции, проведенная работа позволила сформулировать и систематизировать основные цели и задачи создания и распространения ВП с троянскими вирусами проникновения.

В зловредных, корыстных целях хакеры стремятся к изменению количественного и качественного состояния информационного контента, хранящегося в киберпространстве морской инфраструктуры. Также ставятся задачи доступа третьих лиц к базам данных (БД) с информацией конфиденциального характера, с целью её использования и/или изменения. Это включает организацию несанкционированного рассмотрения личной информации, сбор конфиденциальных данных, налоговых номеров и банковских счетов и др. При этом хакеры, как правило, стремятся реализовать дистанционное управление взломанными компьютерными средствами. На рис.1 показана простейшая хакерская схема реализации ВП с троянским вирусом проникновения.

Рисунок 1 – Реализационная схема ВП с троянским вирусом проникновения

На 1-м этапе заказчик киберпреступления (КП) ставит задачу сообщнику-разработчику и финансирует создание вирусной программы, которую намерен продвигать посредством сайтов своих соучастников. Это могут быть продукты, ссылки или другие вирусы. На 2-м этапе размещают продукты, ссылки и другие вирусы на сайте, распространяющем вирусы, для постоянного открытия и представления к реагированию на данную ссылку.

На 3-м этапе пользователь компьютера поражения при скачивании информации или переходя по ссылкам, попадает на сайт с заранее запрограммированным зловредным действием, и начинается процесс заражения.

На 4-м этапе пользователь заражённого компьютера, не подозревая о том, что он реализует функциональные задания ВП, включая выкачивание следующих вирусов и выдачу личных данных. Выдача данных, по количеству сайтовых переходов и эффективности ВП, передаётся заказчику КП на 5 этапе. Благодаря работе сайтов соучастников КП их собственники получают коммерческую выгоду (этап 5), с её завершением на 6 этапе.

Особенности проявления троянских вирусов проникновения характеризуются высокой результативностью и жизнеспособностью. Такая вирусная программа, как правило, находящаяся внутри другой внешне безобидной программы, при запуске инсталлируется в систему. Кроме скачивания конфиденциальной информации, троянский вирус также использоваться в процессе так называемых DoS-атак, для блокирования работы компьютерных сетей противника, выполнения роли шпионской программы, при отправлении конфиденциальной информации третьей стороне.

Одна из основных особенностей проявления троянских ВП состоит в том, что сами они не размножаются, а потому инфицирование компьютерной системы возможно только при запуске вручную. Другая отличительная особенность этих вирусов «троянов» заключается в том, что после активизации они продолжают поддерживать связь с разработчиком, в то время как вирусы других типов функционируют обособленно. Данная особенность позволяет разработчику улучшать и обновлять вредоносную программу, делая ее еще опаснее. Отмеченные особенности затрудняют их обнаружение для антивирусного противодействия. Существующее множество разновидностей троянских ВП способно глубоко укореняться в компьютерных системах для хищения необходимых данных. В операционной системе Windows одним из признаков вирусного поражения файлов является появление ярлыков вместо существовавших ранее папок. Стоит только их запустить, и угроза начнет распространяться по компьютеру. Проявления троянских ВП разнообразны, а именно: диски начинают заполняться оставшимися фрагментами других файлов; появляются лишние процессы, потребляющие оперативную память; вводимая с клавиатуры информация отправляется на удаленные серверы злоумышленников.

Для бизнеса морской критической инфраструктуры под угрозой автоматически становится безопасность БД. Изменяются уровни доступа для всех клиентов, от неограниченных возможностей, до выборочного блокирования.

На распределенных компьютерных телекоммуникациях судоходной отрасли, включая и бортовые электронные средства морских судов, проверяются новейшие модели атак и отрабатываются способы противодействия. Рассмотрение кибербезопасности морских компьютерных телекоммуникаций, подобно тому, как это проводиться в классическом выполнении [2], предусматривает наличие в системах определённого числа уязвимых и поражённых компьютеров, которые осуществляют преднамеренные информационные воздействия-атаки. Предполагается, что с течением времени при отсутствии атак поврежденная система восстанавливается, с некоторой скоростью прироста уязвимых компьютеров. Таким образом подразумевается достижение отсутствия уязвимых компьютеров, и система становится неуязвимой для атаки. При этом понижается скорость уменьшения числа атакующих компьютеров. Учёт отражения текущих потерь от атак ВП, с оценкой прироста количества успешно атакованных компьютеров за конкретный

временной период, представляется математической моделью уязвимости в виде системы уравнений:

$$\begin{cases} \dfrac{dy_1(t)}{dt} = \dfrac{1-\mu(t)}{N}(a-(N_j\mu\, p_j + (1-p_j)(N-N_j)\mu\, y_2(t))y_1(t), \\ \dfrac{dy_2(t)}{dt} = (-c+dy_1(t))y_2(t), \end{cases} \quad (1)$$

где N – число потенциально уязвимых к атакам компьютеров; a – скорость прироста уязвимых компьютеров; c – скорость уменьшения. числа атакующих компьютеров; $y1(t)$ – уязвимые компьютеры; $y2(t)$ – пораженные компьютеры; $\mu(t)$ – доля компьютеров успешно атакованных.

С целью повышения корректности расчётных результатов уязвимости будем считать, что постоянная доля уязвимых компьютеров, которые были успешно атакованы в любой телекоммуникационной подсети, связана с вероятностью того, что захваченный компьютер в подсети будет атаковать компьютеры в этой же подсети, а также с существованием состояния, когда атакуемый компьютер находится вне этой подсети. Поскольку отработка системы информационной защиты выполняется с задержкой, (т.е. с момента начала атаки проходит некоторое время), в математическую модель вводится коэффициент осцилляции, который выражает задержку в срабатывании системы безопасности. С учётом приведенных выше вероятностных усложнений система уравнений, описывающая уязвимость телекоммуникационных компьютеров, представляется в виде:

$$\begin{cases} \dfrac{dy_1(t)}{dt} = (a-(s_j\mu\, p_j + (1-p_j)(1-s_j)\mu(1-\mu)\, y_2(t))\; y_1(t) - \lambda\, y_1^2(t), \\ \dfrac{dy_2(t)}{dt} = (d\; y_1(t) - c)\, y_2(t) - \lambda\, y_1^2(t). \end{cases} \quad (2)$$

где $sj = Nj\ /N$; d – коэффициентом уязвимости; $p\ j$ – вероятность захвата компьютера в подсети из Nj компьютеров; λ – коэффициент осцилляции (задержки срабатывания системы безопасности).

Усложнение математической модели уязвимости компьютерной телекоммуникации должно учитывать ряд особенных обстоятельств. Так, например, если компьютерная сеть содержит N потенциально уязвимых к атакам компьютеров считается, что модель противостояния можно упростить, так как один и тот же компьютер не может быть атакован дважды. При этом доля уязвимых компьютеров, которые были успешно атакованы представляется общим количеством успешно атакованных компьютеров, каждый из которых может быть использован для проведения среднего количества последующих атак. Поскольку часть компьютеров уже была успешно атакована, каждым новым захваченным компьютером будет произведено определённое количество новых успешных атак. В усложнённой модели учитывается тот факт, что система телекоммуникации состоит из нескольких автономных подсетей, в которых каждый компьютер может взаимодействовать в любой момент времени с любым другим произвольным количеством компьютеров вне системы, например, в Интернете. Поскольку мгновенное выявление троянских ВП невозможно, то сетевая защита может обеспечивается серверами безопасности с облачным принципом действия. При запуске все файлы целиком проверяются несколькими системами безопасности, а вся эвристика компьютеров сети настраивается с такими возможностями: сканирования файлов только целиком; обработка файлов, находящихся

как в статическом, так и в динамическом состоянии; копирования файлов сначала на сервер безопасности и последующего распаковывания, сканирования и диагностирования.

Говорить о надлежащей безопасности от большинства вирусов можно только после использования не менее 3–8 видов сканирования и проверок. Даже отсканированный компьютер антивирусной программой не может считаться в безопасности, поскольку система безопасности вычисляет сначала активные и самостоятельно копирующийся вирус, а спящие или скрытые обнаруживаются в лучшем случае через 2–3 дня и только после запуска. Полное проявление угрозы от троянских ВП можно увидеть лишь в процессе их действий.

Среди отмеченных выше троянских вирусов проникновения очень опасным и чрезвычайно разрушительным считается вредоносный паразит Krepper, который вызывает серьезные проблемы, связанные со стабильностью компьютера. В систему он попадает через ненадежные интернет ресурсы, сети общего доступа или онлайн чатов, работает в скрытном режиме в ожидании указанной даты запуска. В указанную дату, вирус Krepper поражает системный реестр Windows, удаляя несколько критических системных папок и инициируя другие деструктивные действия по обнаружению и полному прекращению работы антивирусных программ в компьютерах. Кроме того, этот вирус способен подключить систему к другим вредоносным серверам и способствовать загрузке других подобных вирусных программ. Его проявление отражается в постоянном замедлении работы компьютерной системы или некоторых программ, их сбой без какой-либо видимой причины. Однако проблемы идут глубже, чем может показаться в начале, так как этот троянский ВП будет потреблять много системных ресурсов и уменьшать его производительность. Вирус будет собирать различную конфиденциальную информацию о пользователе, например, его идентификационный номер, банковские счета и другие данные, которые могут быть использованы для вредоносных целей. Эта вредоносная программа создана таким образом, что её очень сложно обнаружить и удалить с компьютера раз и навсегда, поскольку она, по-видимому, постоянно обновляется. Более того, ВП Krepper подключается к Интернету без разрешения и обращается к веб-сайтам, которые могут быть вредными, и т.о. продолжает заражать компьютер.

Троянский ВП Krepper повреждает любую папку или файл, на которые он нацелен, и автоматически удаляет их. Поэтому легко теряется важная информация, повреждаются некоторые аппаратные компоненты, например, звук или изображения. Кроме того, собранные конфиденциальные данные он может несанкционированно передавать третьим лицам. Он распространяется через зараженные вложения электронной почты, с зараженного USB-накопителя или другого устройства, а также путём связывания различных программных средств вместе с некоторыми бесплатными приложениями в виде приманок. При этом, загружаются различные потенциально нежелательные программы, такие как браузеры, рекламные продукты, а также другие вредоносные программы. Это происходит при недостаточном внимании пользователей, когда не проверяется каждый шаг процесса установки и не избегаются подозрительные сторонние менеджеры загрузки. Поскольку данный вирус является опасным и постоянным приложением, то для поддержания компьютера в безопасном состоянии, средством надежной защиты являются антивирусные программы узконаправленного действия.

Значительную помощь может оказать и проектный подход, при котором во время проектирования задач сети и доступов учитываются задачи защиты от вирусов проникновения. Необходим только один подход – строить сети на предприятиях таким образом, чтобы любая ее часть легко сканировалась антивирусными приложениями в удаленном режиме, оставаясь при этом недоступной для пользователей с более низким уровнем допуска.

Выводы и предложения. Выполненное исследование показало проблематику структуры и принципов действия вирусов проникновения, и раскрыло некоторые особенности компьютерной уязвимости. Вирус проникновения троян несёт огромную

опасность и крайне пагубно влияет на работу компьютерных систем и сетей морской критической инфраструктуры. Полученные результаты оценки проблем возникновения вирусов связываются с желанием сообщников КП управлять компьютерными средствами на расстоянии. Особенности проявления троянских вирусов проникновения проявляются в виде технического изменения файловых систем компьютеров, копирования информации по запросу, заложенному в программном коде ВП, или выкачивания из интернет вредоносных кодов с их распаковкой и запуском с жесткого информационного диска компьютера**.** Предлагается устанавливать уязвимость компьютерной системы и сети с использованием оценочного подхода основанного на теоретическом моделировании.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Закон України «Про основні засади забезпечення кібербезпеки України», Київ, 5 жовтня 2017 року № 2163-VIII.

2. Монахов, Ю.М. Вредоносные программы в компьютерных сетях: учеб. пособие / Ю.М. Монахов, Л.М. Груздева, М.Ю. Монахов; Владим. гос. ун-т. – Владимир: Изд-во Владим. гос. ун-та, 2010. – 72 с.

3. Брэгг Р. Безопасность сетей. Полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг. – М. : Эком, 2006. – 912с.

4. Гошко С.В. Энциклопедия по защите от вирусов / С.В. Гошко. – М. : СОЛОН-Р, 2005. – 352 с.

5. Касперский К. Компьютерные вирусы: изнутри и снаружи / К. Касперский. – СПб. : Питер, 2005. – 528с.

6. Козлов Д.А. Энциклопедия компьютерных вирусов / Д.А. Козлов, А.А. Парандовский, А.К. Парандовский. – М. : СОЛОН-Р, 2001. – 464с.

7. Собейкис В.Г. Азбука хакера 3. Компьютерная вирусология / В.Г. Собейкис. – М : Майор, 2006. – 512 с.

REFERENCES

1. The Law of Ukraine «On the Basic Principles of Cyber Security of Ukraine», Kyiv, 5 October 2017 No. 2163-VIII.

2. Monakhov, Yu.M. Malicious programs in computer networks: training. allowance / Yu.M. Monakhov, LM Gruzdeva, M.Yu. Monakhov; Vladimir. state. un-t. Vladimir: Publishing house of Vladimir. state. University, 2010. 72 s.

3. Bragg R. Network Security. Full leadership / R. Bragg, M. Rhodes-Ousley, C. Strassberg. M .: 2006. – 912 c.

4. Goshko S.V. Encyclopedia on protection from viruses / S.V. Goshko. M.: SOLON-R, 2005. 352 p.

5. Kaspersky K. Computer viruses: inside and out / K. Kaspersky. St. Petersburg. : Peter, 2005. 528 s.

6. Kozlov D.A. Encyclopedia of computer viruses / D.A. Kozlov, A.A. Parandovsky, A.K. The Parandovsky. M. : SOLON-R, 2001. 464 p.

7. Sobeykis V.G. The ABC of the hacker 3. Computer virology / V.G. Sobeykis. M. : Major, 2006. 512 s.

Вільський Г. Б., Радов А. А. ПРОБЛЕМИ ВИНИКНЕННЯ І ОСОБЛИВОСТІ ПРОЯВУ КОМП'ЮТЕРНИХ ЗАВАНТАЖУВАЛЬНИХ ВІРУСІВ ПРОНИКНЕННЯ

Розглянуто результати дослідження небезпек троянських вірусів проникнення, що проявляються у вигляді технічної зміни файлових систем комп'ютерів, копіювання інформації за запитом, або викачування з інтернет шкідливих кодів з їх розпакуванням і запуском з жорсткого інформаційного диска комп'ютера. Обґрунтовано поєднуваність проявів троянського вірусу і бажання кіберзлочинців управляти комп'ютерами в системах і мережах на відстані. Пропонується оцінювальний підхід до встановлення уразливості комп'ютерної системи і мережі, заснований на теоретичному моделюванні.

***Ключові слова**: атака, вірус, шкідлива програма, інформація, кіберзлочинність, комп'ютер, сайт, сервер, троян.*

Vilsky G. B., Radov A. A. PROBLEMS OF VINICNENIYA AND THE OBOBLIVOSTS I WILL EXPERIENCE THE COMPUTERS OF THE VOLUNTARY PROTECTIVE VIRUSES

The results of a study of the dangers of Trojan penetration viruses appearing in the form of a technical change in computer file systems, copying information on demand, or downloading malicious codes from the Internet with their unpacking and launching from a hard information disk of a computer are examined. The compatibility of manifestations of the Trojan virus and the desire of cybercriminals to control computers in systems and networks at a distance is grounded. An evaluative approach is proposed to establish the vulnerability of a computer system and network, based on theoretical modeling..

***Keywords:** attack, virus, malware, information, cybercrime, computer, site, server, Trojan.*

Статтю прийнято
до редакції 15.05.18