ИССЛЕДОВАНИЕ БЭКДОРОВ: АЛГОРИТМЫ ДЕЙСТВИЯ, УДАЛЕНИЯ

К. А. Ахрамеева, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича, oklaba@mail.ru;*
Е. Ю. Герлинг, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича, gerlingeu@gmail.com;*
Д. В. Юркин*, к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича, доцент, dvyurkin@ya.ru;*
Д. Ю. Мицковский, *Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича, denism1111198@gmail.com.*

УДК 004.056

Аннотация. В статье рассматриваются наиболее популярные в настоящее время бэкдоры, а также вирус, который использовал бэкдор для проникновения в систему, а именно *WannaCry*. В рамках статьи освещена история обнаружения вирусов, алгоритм действия вирусов и методы противодействия вирусу. Также дана характеристика вирусам *Glupteba-AFJK, DoublePulsar.*

Ключевые слова: бэкдор; эксплойт; *WannaCry; Glupteba.*

BACKDOOR STUDY: ACTION AND REMOVAL ALGORITHMS

K. Akhrameeva, *associate professor, Ph.D., St. Petersburg state university of telecommunications named after prof. M.A. Bonch-Bruevich;*
E. Gerling, *associate professor, Ph.D., St. Petersburg state university of telecommunications named after prof. M.A. Bonch-Bruevich;*
D. Yurkin, *associate professor, Ph.D., St. Petersburg state university of telecommunications named after prof. M.A. Bonch-Bruevich;*
D. Mitskovsky, *St. Petersburg state university of telecommunications named after prof. M.A. Bonch-Bruevich.*

Annotation. The article discusses the most popular backdoors at present as well as the virus that used the backdoor to penetrate the system, namely WannaCry. The article gives the history of virus detection, the algorithm of the action of viruses and methods of countering the virus. Also the Glupteba-AFJK and DoublePulsar viruses are characterized.

Keywords: backdoor; exploit WannaCry; Glupteba.

Введение

Бэкдоры (вредоносное ПО, внедряемое в системы для намеренного создания уязвимостей) в последнее время становятся одной из наиболее часто встречаемых угроз. В первую очередь, это обусловлено тем, что многие вирусы-шифровальщики проникают в устройства с помощью бэкдора. Наиболее известным примером такого вируса является *WannaCry*. При этом наибольшая опасность бэкдоров заключается в том, что их действие крайне трудно обнаружить, поэтому важно знать алгоритмы действия бэкдоров, а также методы их удаления.

Характеристика действия бэкдора и методов противодействия ему

Важно отметить, что не все бэкдоры являются вирусами, поскольку не все бэкдоры способны самореплицироваться в системах. *Glupteba-AFJK* один из классических представителей бэкдоров-вирусов, который относительно недавно дал о себе знать (в сентябре 2019 г.) и до сих пор продолжает заражать системы во многих странах мира [1]. *Glupteba-AFJK* является одной из версий трояна *Glupteba*, который по своей сути являлся вирусом-вымогателем. Однако данная версия вируса была переработана в бэкдор, который является вредоносной программой, которая используется злоумышленниками для получения несанкционированного удаленного доступа к компьютерной системе или внедрения другого вредоносного ПО за счет уязвимости в системе безопасности. Зачастую бэкдор нельзя просто так удалить, даже если обнаружить файлы вируса. Чаще всего бэкдоры внедряются в автозагрузку системы и повторно загружаются вместе с системой. Данный вирус не является исключением. Такие вирусы также называются резидентными, то есть находящимися в памяти и активными не только в момент работы зараженной программы, но и после того, как программа закончила свою работу. Копии данных вирусов остаются активными вплоть до перезагрузки, даже если уничтожены все зараженные файлы. Резидентная копия вируса остается активной и заново заражает систему. Данное свойство реализуется за счет изменения значений регистров системы, поэтому для полного удаления вируса необходимо найти активный процесс вируса, остановить его, восстановить измененные значения регистра (а также удалить значения, созданные вирусом) и только потом удалить зараженные файлы.

Вирус «прячется» в исполняемом *CL.exe*. *CL.exe* – это средство, которое управляет *Microsoft C++* компиляторами и компоновщиком. *CL.exe* может выполняться только в операционных системах, поддерживающих *Microsoft Visual Studio* для *Windows*. То есть, как и все трояны, вирус прячется под видом системного исполняемого файла, как до этого делали и его предшествующие версии. На самом деле многие бэкдоры являются переработанными старыми версиями вирусов-предшественников, которые утратили многие функции вируса, на основе которого были созданы, но при этом не избавились от характерных его черт. Например, данная версия вируса использует тот же исполняемый файл для распространения, что и предшественник и при этом использует схожие механизмы распространения [2].

Также необходимо отметить, что основной целью поражения вируса являются сами алгоритмы работы системы, а точнее основной целью вируса является встраивание «дефектов» в работу алгоритма для проникновения других вредоносных программ.

Данный вирус является ярчайшим примером того, какую опасность могут представлять бэкдоры. *WannaCry* является сетевым червем-вымогателем, шифрующим почти все данные на устройстве при заражении. Данный вирус поразил сотни тысяч компьютеров в 150 странах мира и до сих пор продолжает наносить вред [3]. На данный момент экономический ущерб от деятельности данного вируса составлял на конец мая 2017 г. около 1 млрд долларов. Самой интересной особенностью данного вируса является то, что он использовал бэкдор *DoublePulsar* для проникновения в устройства жертв. При этом прямого участия пользователя совсем не требовалось. Самым страшным моментом является то, что вирус получает доступ не при нажатии ссылки, ведущей к скачиванию вируса и не при загрузке программ. Достаточно было просто не обновлять собственную ОС и иметь доступ к интернету. Вирус закачивался, используя уязвимость, создаваемую бэкдором *DoublePulsar*.

Бэкдор *DoublePulsar* имеет возможность подключать удаленные хосты и выполнять действия против взломанных систем. *DoublePulsar* поддерживает протоколы *SMB* и *RDP*. *DoublePulsar* предоставляет злоумышленникам высокий уровень контроля над компьютерной системой. После установки становятся доступны три команды: *ping, kill* и *exec*. Команда *exec* как раз и используется для внедрения вредоносов [4, 5].

В первую неделю апреля 2017 г. неизвестная хакерская группа под названием *Shadow Brokers* просочилась в систему эксплуатации, называемую *FuzzBunch* из группы *Equation* (одна из самых сложных атакующих групп в мире и подозреваемая в широких связях с Агентством национальной безопасности США (АНБ)) [4]. Этот фреймворк состоял из нескольких, не прошедших проверку удаленных эксплойтов для *Windows* (таких как эксплойты под кодовым названием *EternalBlue, EternalRomance и EternalSynergy*), и других хакерских инструментов. Одним из таких хакерских инструментов является бэкдор под кодовым названием *DoublePulsar*. Это бэкдор, используемый для введения и запуска вредоносного кода на зараженной системе, и он устанавливается и используется *EternalBlue*. *EternalBlue* – это эксплойт *SMBv1* (*Server Message Block* 1.0), который может вызвать *RCE* и атаковать службы обмена файлами *SMB* [4]. Считается, что он возник с АНБ.

DoublePulsar [5] – это очень сложная, основанная на памяти многоархитектурная полезная нагрузка ядра, которая подключается к *x*86 и 64-разрядным системам и позволяет злоумышленнику выполнять любые необработанные полезные данные шелл-код. Это полная полезная нагрузка ядра, дающая полный контроль над системой. Он не открывает новые порты, но использует тот же порт, на котором работает служба *SMB*. Эта вредоносная программа заражает компьютеры под управлением *Windows* и он открывает черный ход, через который другие вредоносные программы могут быть загружены на зараженных компьютерах. *DoublePulsar* может делать любую из четырех следующих действий:

- отвечает на определенный запрос *ping,*
- может удалить себя,
- загрузить шелл-код,
- запустить *DLL* на хосте.

Это единственная цель программы.

DoublePulsar существует как скрытый канал, который использует функции *SMB,* которые до сих пор не использовались, в частности, функцию *«Trans2».*

Как проверить – заражена ли система *DoublePulsar*? С помощью программы *Wireshark* можно проверить заражение системы на основании ответа порта 445 на конкретный *ping*-запрос. Система, запускающая эксплойт, отправляет запрос *«trans2 SESSION_SETUP»* на компьютер для проверки наличия бэкдора. Целью этого запроса является проверка заражения системы. В любом случае, система ответит сообщением *«Not Implemented»*, как показано на рис. 1. Но в качестве части сообщения возвращается «мультиплексный идентификатор», который равен 65 (0x41) для нормальных систем и 81 (0x51) для зараженных систем. Если система заражена, то *SMB* может использоваться в качестве скрытого канала для фильтрации данных или запуска удаленных команд.

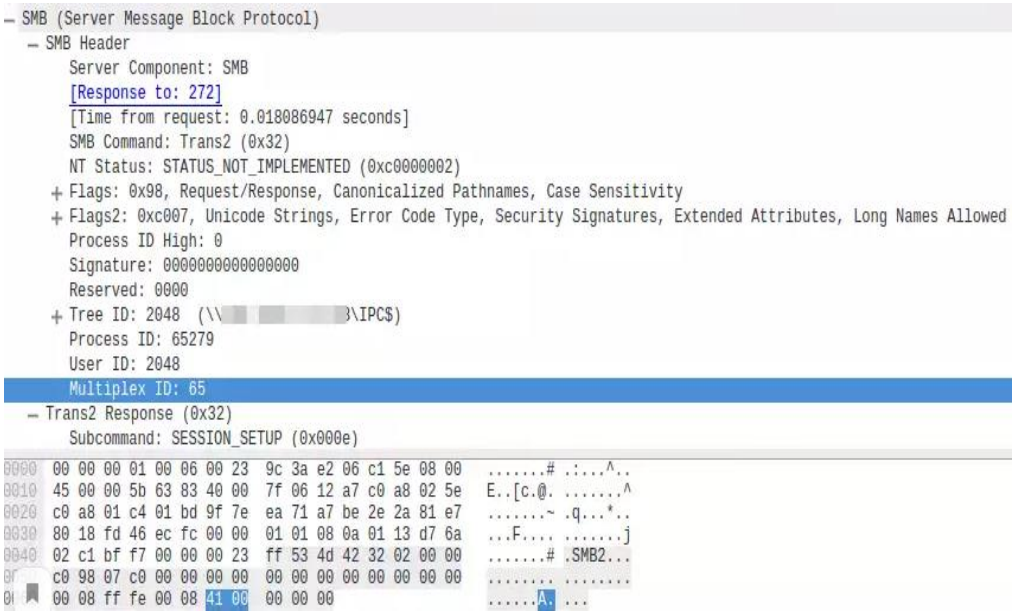

Рисунок 1

Несмотря на всю опасность данного бэкдора, удаляется он очень просто. Это нерезидентный вирус, сохраняющийся в *RAM*, то есть бэкдор живет в памяти. Как только машина перезагружается, он исчезает. В данном случае вопрос заключается скорее в предотвращении заражения, чем в самом удалении. Чтобы предотвратить заражение данным бэкдором, достаточно лишь закрыть или ограничить порт 445. Данный порт используется *TCP/IP* протоколами и является одним из самых атакуемых. Большая часть устройств, зараженных данным вирусом, имела открытый порт 445.

Заключение

В заключение следует отметить, что, на самом деле, бэкдоры зачастую не ищут особо замысловатые пути проникновения в систему. Вместо этого бэкдоры используют банальную неосторожность пользователей, поэтому самые банальные меры защиты, такие как мониторинг и ограничение потока трафика, проходящего через порт, помогут предотвратить заражение системы бэкдором.

Литература

1. Meskauskas, T. How to prevent installation of the Glupteba Trojan, 2020, [электронный ресурс]: https://www.pcrisk.com/removal-guides/15782-glupteba-trojan, доступ свободный (дата обращения: 15.04.2020).
2. База знаний ESET [электронный ресурс]: https://www.esetnod32.ru/support/knowledge_base, доступ свободный, (дата обращения: 15.04.2020).
3. Checkpoint.com, brokers in the shadows: Analyzing vulnerabilities and attacks spawned by the leaked NSA hacking tools, 2017, [электронный ресурс]: https://blog.checkpoint.com/2017/05/25/brokers-shadows-analyzing-vulnerabilities-attacks-spawned-leaked-nsa-hacking-tools/, доступ свободный, (дата обращения: 15.04.2020).
4. Pradeep Kulkarni, Sameer Patil, Prashant Kadam & Aniruddha Dolas, EternalBlue: A prominent threat actor of 2017-2018, [электронный ресурс]: https://www.virusbulletin.com/virusbulletin/2018/06/eternalblue-prominent-threat-actor-20172018/ доступ свободный, (дата обращения: 15.04.2020).

5. Shakeel Bhat, DoublePulsar – A Very Sophisticated Payload for Window, 2017 [электронный ресурс]: https://www.secpod.com/blog/doublepulsar-a-very-sophisticated-payload-for-windows/, доступ свободный, (дата обращения: 15.04.2020).
6. Василишин Н.С., Ушаков И.А., Котенко И.В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // в сборнике: Информационные технологии в управлении (ИТУ-2016) Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В.Г. Пешехонов, 2016. – С. 670-675.