Научная статья
Original article
УДК 004.424

МЕТОДЫ ЗАРАЖЕНИЯ ВИРУСНОЙ ПРОГРАММЫ

VIRUS INFECTION METHODS

Казарян Каторина Камоевна студент специалитета, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kazaryan_katorina@mail.ru

Белан Виктория Вадимовна магистрант, Донской государственный технический университет, г. Ростов-на-Дону, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), viktoriyabelan2018@gmail.com

Kazaryan Katorina Kamoevna specialty student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kazaryan_katorina@mail.ru

Belan Victoria Vadimovna Master student, Don State Technical University, Rostov-on-Don, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), viktoriyabelan2018@gmail.com

Аннотация Современные информационные системы представляют собой сложные и большие по размерам комплексы программно-аппаратных средств, решающие широкий спектр задач хранения и обработки данных в самых разнообразных отраслях деятельности. Применение информационных технологий позволяет значительно повысить эффективность работы предприятий, в том числе, за счёт организации совместной работы сотрудников и предоставления им общего доступа к данным.

Annotation Modern information systems are complex and large-sized software and hardware complexes that solve a wide range of data storage and processing tasks in a wide variety of industries. The use of information technologies can significantly improve the efficiency of enterprises, including through the organization of joint work of employees and providing them with shared access to data.

Ключевые слова: информационная безопасность, TBT, компьютерная безопасность

Keywords: information security, TVT, computer security

TBTTrojan (TBT) — это троян, который заражает устройства конечных пользователей и пытается взломать их финансовые счета и украсть средства.

Обнаруженный в 2012 году, троянец сначала заразил тысячи турецких компьютеров. После обнаружения исходный код вредоносного ПО просочился в сеть и с тех пор претерпел различные изменения, что значительно усложнило обнаружение финансовыми учреждениями.

TBT — это модифицированная версия троянца ZeuS, в котором использовался аналогичный механизм атаки, но главное отличие в том, что TBT намного меньше по размеру. Меньшие вредоносные программы намного сложнее обнаружить. TBT - самый маленький из известных троянцев размером всего 20 КБ.

Воздействие троянца TBT

TBT создал серьезную проблему для систем, зараженных этим вредоносным ПО. Он заразил более 20 крупных банковских учреждений США.

TBT заражает системы и браузеры различными способами и хранит данные, отправляемые на банковские сайты и с них. Когда пользователь входит на веб-сайт банка, появляется вредоносное всплывающее окно с запросом учетных данных с использованием оригинального логотипа и названия фактического сайта.

Исходный код TBT опубликован в Интернете, и продолжают появляться новые версии вредоносных программ. С момента своего пика в 2016 году он

считается одним из самых разрушительных штаммов вредоносных программ, влияющих на банковскую отрасль, и с тех пор повлиял на работу онлайн-банкинга.

Как работает банковский троян TBT

Зараженные веб-сайты могут распространять TBT, а жертвы заманиваются с помощью фишинговых писем и мошеннического рекламного контента. Когда уязвимая система запускает TBT, она реплицирует его под именем bin.exe в папку% AppData%.

Различные версии TBT оказывались в разных папках - варианты создавали папки со случайно сгенерированными именами на основе информации о зараженной системе. TBT шифрует использование памяти, чтобы избежать обнаружения.

Когда зараженная система перезагружается, запускается bin.exe и TBT остается на компьютере. TBT может изменять веб-браузеры, такие как Explorer и Firefox, отключая предупреждающие сообщения и разрешая отображение содержимого HTTP на веб-сайтах HTTPS без подсказок. TBT нацелен на такие процессы, как explorer.exe и svchost.exe в Windows, а также на другие запущенные процессы.

TBT шифрует свою связь с серверами управления и контроля и поддерживает доступность с помощью четырех доменов C&C. У него есть локальные файлы конфигурации, которые он может использовать, когда не может подключиться к серверу.

Как TBT ведет себя при атаках на человека в браузере

Атаки Man-in-the-Browser используют захват форм для перехвата нажатий клавиш, прежде чем они будут переданы на веб-сайт по зашифрованному протоколу HTTPS. Это эффективно обходит HTTPS и позволяет злоумышленнику украсть данные пользователя.

TBT поставляется с компонентом веб-инъекций, содержащим вредоносный код JavaScript. Это вредоносное ПО, которое может применять динамическую веб-инъекцию ко многим веб-сайтам онлайн-банкинга.

Компонент веб-инъекции адаптируется к точному внешнему виду исходного веб-сайта, что затрудняет его обнаружение пользователями.

Механизм веб-инъекции отображает вводящие в заблуждение сообщения для пользователя, например, о том, что финансовому учреждению необходимо, чтобы они повторно вводили данные своей учетной записи, и предлагает им ввести конфиденциальные данные для подтверждения своей личности. У пользователей запрашивается не только финансовая информация, такая как данные банковского счета или кредитной карты, но также идентификационная информация, такая как номера социального страхования. Кроме того, пользователей просят предоставить информацию об общих вопросах безопасности, таких как девичья фамилия их матери.

Затем злоумышленник может использовать атакующий посредник (MitM), чтобы передать доступный баланс жертвы так называемым «кассовым мулам». Это третьи стороны, которые снимают средства и отправляют их злоумышленникам без возможности отслеживания в обмен на комиссию.

Удаление троянца TBT

Если в системе присутствует TBT, это может вызвать проблемы с браузером или привести к сбою системы. Обычно всплывающее сообщение, которое якобы пришло из банка, просит пользователя предпринять необычные действия, например ввести конфиденциальную информацию. Он также может сообщить пользователю, что средства были зачислены на его счет по ошибке, и он должен немедленно вернуть средства.

Чаще всего TBT заражает систему, когда пользователи загружают бесплатное программное обеспечение с незнакомых веб-сайтов, нажимают на зараженные ссылки или вложения в фишинговых письмах, щелкают всплывающие окна с рекламой или загружают контент из даркнета или торрент-файлов.

Очистить TBT может быть сложно, потому что он внедряет вредоносный код в законные процессы. Есть два основных варианта удаления трояна:

1. Большинство крупных компаний, занимающихся защитой от вредоносных программ, предлагают очистители ТВТ.

Вы можете использовать полную резервную копию состояния системы, чтобы восстановить время до заражения. Однако это рискованный путь - выбор точки восстановления может быть трудным, поскольку заражение ТВТ может быть не сразу очевидным. Кроме того, любые изменения, внесенные с момента восстановления, будут потеряны.

Обучение пользователей: как пользователи могут предотвратить банковские трояны

Банковские трояны - это чрезвычайно скрытая форма вредоносного ПО. Когда банковский троян заражает компьютер или веб-браузер пользователя, он бездействует и ожидает, пока он получит доступ к веб-сайту онлайн-банкинга. Когда пользователь делает это, троянец активируется, использует кейлоггер для кражи имени пользователя и пароля учетной записи и тайно отправляет их злоумышленникам.

Поскольку угроза кражи с помощью банковских троянов возрастает, пользователи могут защитить себя несколькими способами:

- Остерегайтесь фишинговых писем - при открытии письма из ненадежного источника или писем из надежного источника, которые содержат необычный контент или запросы, пользователи не должны щелкать ссылки, запускать файлы или открывать документы Microsoft Office.
- Использование решений безопасности на локальном устройстве - современные решения безопасности могут защитить пользователей от вредоносных программ и других векторов атак. Хорошее решение безопасности может эффективно обнаруживать и блокировать банковских троянов, обнаруживая и блокируя вредоносный контент в файлах или фишинговых сообщениях. Даже если пользователи просматривают Интернет на личном устройстве, им следует развернуть хорошо известные и эффективные решения для защиты от вредоносных программ.

- Необычное поведение на банковских сайтах - пользователям следует остерегаться подозрительной активности на сайтах банковских и финансовых услуг. Им следует обратить особое внимание на новые поля для входа в систему, которых они раньше не видели, особенно когда они запрашивают личные данные. Пользователи должны учитывать то, о чем банк обычно не просит, и искать небольшие недостатки или изменения в дизайне или отображении веб-сайта.
- Устанавливайте мобильные приложения из проверенных источников - это особенно важно для банковских приложений. Загрузка приложений из известных и надежных источников, таких как Google Play и Apple App Store, не гарантирует, что пользователи не будут загружать вредоносные приложения, но защитит их от большинства угроз.
- Резервное копирование важных файлов - пользователи должны делать автономные копии своих самых важных файлов на внешних устройствах или в облачных хранилищах. Распространенные сегодня банковские трояны распространяют другое вредоносное ПО, такое как программы-вымогатели, после начальной фазы, что может лишить пользователей доступа к их файлам.

Литература

1. «Объём HTTP-трафика впервые превысил P2P» - net.compulenta.ru/322974/ — Компьюлента, 22 июня 2007. (Официальный документ от Ellacoya Networks - www.ellacoya.com/news/pdf/2007/NXTcommEllacoyaMediaAlert.pdf)
2. «HTTP-NG — объектно-ориентированный протокол передачи гипертекста» - www.osp.ru/cw/1998/20/29525/, «Открытые системы», 29 мая 1998 г. «(Proposed) HTTP-NG Working Group» - www.w3.org/Protocols/HTTP-NG/ — официальная страница W3C по разработке протокола HTTP-NG.
3. HTTP/1.1: Method Definitions - www.w3.org/Protocols/rfc2616/rfc2616-sec9.html (англ.). W3C.
4. См. первое предложение раздела «6.1.1 Status Code and Reason Phrase - tools.ietf.org/html/rfc2068#section-6.1.1» в RFC 2068. На стр. 40 -

tools.ietf.org/html/rfc2068#page-40 есть также объявление в формате расширенной БНФ-формы (Augmented BNF) «extension-code = 3DIGIT» для кодов расширений.

5. HTTP errors - www.flickr.com/photos/apelad/sets/72157594388426362/detail/

References

a. "The volume of HTTP traffic exceeded P2P for the first time" - net.compulenta.ru/322974/ - Compulenta, June 22, 2007. (White paper from Ellacoya Networks - www.ellacoya.com/news/pdf/2007/NXTcommEllacoyaMediaAlert.pdf)

b. "HTTP-NG - Object-Oriented Hypertext Transfer Protocol" - www.osp.ru/cw/1998/20/29525/, "Open Systems", May 29, 1998

2. The (Proposed) HTTP-NG Working Group - www.w3.org/Protocols/HTTP-NG/ is the official W3C HTTP-NG protocol development page.

3. HTTP / 1.1: Method Definitions - www.w3.org/Protocols/rfc2616/rfc2616-sec9.html (English). W3C.

4. See the first sentence of "6.1.1 Status Code and Reason Phrase - tools.ietf.org/html/rfc2068#section-6.1.1" in RFC 2068. On page 40 - tools.ietf.org/html/ rfc2068 # page-40 there is also an Augmented BNF "extension-code = 3DIGIT" declaration for extension codes.

5. HTTP errors - www.flickr.com/photos/apelad/sets/72157594388426362/detail/

© Казарян К.К., Белан В.В., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Казарян К.К., Белан В.В. МЕТОДЫ ЗАРАЖЕНИЯ ВИРУСНОЙ ПРОГРАММЫ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.