2. Артем'єва А. В. Захист інформації від витоку по електромагнітним каналам. *Сенергія наук*. 2019. № 33. С. 1006–1012.

3. Кірєєва Н. В. Виток інформації по каналам ПЕМВ та способи її захисту. *Міжнародний журнал прикладних та фундаментальних досліджень*. 2016. № 8. С. 499–504.

Ключові слова: електромагнітні канали, конструкторсько-технологічні рішення, заземлення, екранування.

Ключевые слова: электромагнитные каналы, конструкторско-технологические решения, заземление, экранирование.

Keywords: electromagnetic channels, design and technological solutions, filtration, grounding, shielding.

Науковий керівник: *к.т.н. доц. Кухаренко С. В.*

Сафонов Камиль Муханнадович
Национальный университет «Одесская юридическая академия»,
студент 2 группы факультету кибербезопасности
и информационных технологий

ЗАЩИТА УСТРОЙСТВ КОММУНИКАЦИИ ПОЛЬЗОВАТЕЛЯ ОТ RAT ВИРУСОВ

В современном мире актуализирована проблема вирусного поражения цифровых устройств пользователей. К их числу относятся самые опасные шпионские RAT вирусы (Remote Access Trojan – Троян удаленного доступа) [1].

Алгоритм работы этого вируса позволяет злоумышленнику получить полный удаленный доступ к устройству пользователя жертвы, а следовательно к его файлам, личным данным, видеокамере, геолокации, данным банковских карт и т.д.

Структурно, RAT вирус состоит из двух частей: клиентской и серверной. С помощью клиентской части, которая установлена на устройство злоумышленника, и серверной, которую, ничего не подозревая, запускает пользователь на своем устройстве коммуникации. После запуска серверной части RAT вируса, на устройстве коммуникации пользователя, в клиентской части

на устройстве злоумышленника появляется удаленный хост. В результате злоумышленник получает полный доступ к данным пользователя.

Отличительной особенностью рассматриваемого класса RAT вирусов является криптографическая обработка извлекаемых данных из устройства пользователя. Из-за этого антивирусное программное обеспечение не может определить сам факт передачи извлеченных данных на устройство злоумышленника [2]. Для защиты от последствий внедрения RAT вирусов на устройство пользователя существуют сложные решения, которые являются эффективными, однако в при использовании, обладают рядом недостатков.

Например, к их числу относится создание «виртуальной машины» на своем устройстве. Это позволяет выполнять любые действия в браузере или с файлами в пределах изолированной среды – «виртуальной машины», а не своего устройства [3]. Однако у такого решения есть существенный недостаток «виртуальная машина» потребляет значительное количество вычислительных ресурсов устройства. Следовательно, пользователь в этом случае будет терять время и аппаратные ресурсы из-за использования виртуальной и оперативной памяти «виртуальной машиной», которая, по сути, представляет собой дополнительную операционную систему. Также установка «виртуальной машины» требует много времени и знаний, которые есть не у каждого пользователя. Самым большим недостатком использования «виртуальной машины» является то, что многие вредоносное программное обеспечение, включая RAT вирусы, имеет возможность определить, что программа запущена в виртуальной среде, а не на реальном устройстве и таким образом, даже «виртуальная машина» не всегда предоставит полную безопасность пользователю. Однако, даже полностью подготовленный пользователь, с установленной на своё устройство «виртуальной машиной», всё равно имеет шанс стать жертвой внедрения RAT вируса.

Помимо самого вируса, угрозу несет и злоумышленник, который, прибегая к социальной инженерии, заставляет жертву совершить определенные действия, в том числе и установку вируса на своё устройство коммуникации. Для того чтобы защитить себя от последствий воздействия социальной инженерии достаточно понять основные типы и методы защиты от них [4].

Ведь помимо самого вируса, угрозу несет и злоумышленник, который, прибегая к приемам социальной инженерии, заставляет жертву совершить определенные действия, в том числе и установку вируса на своё устройство. Для того чтобы защитить себя от воздействия социальной инженерии достаточно понять основные ее методы воздействия на человека.

В основном фишинговые атаки выполняются благодаря поддельным сообщениям на почту или через профили в социальных сетях. В самом сообщении содержится форма для ввода персональных данных.

Также возможен и другой вариант развития событий, когда мошенник работает по заранее готовому плану действий, в результате которого он узнает от пользователя, любую нужную ему информацию.

И последний популярный вариант мошенничества с помощью социальной инженерии – «троянский конь». В этом случае мошенник ориентируется на эмоции жертвы, такие как страх, ненависть или жадность, манипулируя или угрожая пользователю, мошенник также с легкостью может получить всю необходимую ему информацию от пользователя.

Таким образом, любые защитные меры, включая антивирус, или «виртуальная машина» не всегда защитят пользователя от потери или утечки данных.

Самым эффективным вариантом решения рассматриваемой проблемы, является применение сетевого экрана. Его суть заключается в организации контроля за абсолютно всеми входящими и исходящими сетевыми соединениями устройства пользователя. Понятно, что в этом случае запросы

RAT клиента с компьютера злоумышленника на RAT сервер пользователя будут зафиксированы и обнаружены пользователем.

Понятно, что в этом случае злоумышленник не сможет удаленно подключиться к устройству пользователя, а значит и не сможет извлечь данные, хоть и сама серверная часть RAT вируса будет установлена и готова к выполнению поставленной задачи.

Таким образом, применение сетевого экрана не может исключить возможность попадания RAT вируса на устройство пользователя, но исключит возможность эксплуатации его серверной части злоумышленником.

Следует отметить, что правильная настройка и эксплуатация сетевого экрана является не самой простой для обычного пользователя задачей. Однако существует большое множество готовых решений с заранее установленными настройками, благодаря которым пользователь сможет легко фильтровать свой трафик, и тем самым обеспечить себе защиту от программ шпионов [5].

Несмотря на наличие этого решения, проблема защиты от RAT вирусов остается актуальной, так как малое число пользователей могут защитить себя от этого типа вирусов.

Именно это обстоятельство обуславливает устойчивую тенденцию массового использования злоумышленниками шпионского программного обеспечения RAT класса.

Список используемых источников:

1. Что такое RAT? Всё про шпионские RAT-трояны. [Електронний документ]. – URL: https://spy-soft.net/chto-takoe-rat/.

2. What is RAT Malware and How to Protect? [Электронный документ]. – URL: https://www.malwarefox.com/rat-malware/.

3. Вишняков В.А., Моздурани Шираз М. Г. Модели и реализация обнаружения вторжений в корпоративной информационной системе предприятия с использованием интеллектуального подхода. *Доклады БГУИР*. 2017. № 8 (110). [Электронный документ]. URL: https://cyberleninka.ru/article/n/modeli-i-realizatsiya-

obnaruzheniya-vtorzheniy-v-korporativnoy-informatsionnoy-sisteme-predpriyatiya-s-ispolzovaniem.

4. Соціальна інженерія в інтернет-просторі. [Електронний документ]. – URL: http://chtei-knteu.cv.ua/herald_ru/content/download/archive/2016/v3–4/NV-2016-v3–4_13.pdf.

5. Мохаммед Ф. О. Межсетевые экраны. *Доклады БГУИР*. 2009. № 5 (43). [Электронный документ]. URL: https://cyberleninka.ru/article/n/mezhsetevye-ekrany.

Ключові слова: RAT вірус, структура RAT вірусу, віртуальна машина, мережевий екран, захист від RAT вірусів.

Ключевые слова: RAT вирус, структура RAT вируса, виртуальная машина, сетевой экран, защита от RAT вирусов.

Keywords: RAT virus, RAT virus structure, virtual machine, firewall, protection against RAT viruses.

***Научный руководитель**: доцент Задерейко А. В.*

Соловйов Артем Сергійович
Національний університет «Одеська юридична академія»,
студент 3 курсу факультету кібербезпеки
та інформаційних технологій

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕРНЕТЕ

В настоящие время существует проблема кражи персональных данных. В условиях глобализации пользования человека всё больше приобретает связь с глобальной сетью Интернет. За последние десятилетие количество пользователей возросло. Работая в интернете человек получает множество полезной информации, но иногда он может не заметить то как его персональные данные оказываются под большой угрозой. Вопрос о защите персональных данных является очень актуальным, особенно является актуальной информация защита персональных данных, попавшая в интернет. Личные данные – это любые данные, идентифицирующие человека. Ваше имя, адрес электронной почты, местоположение, биометрические данные, логин [1].