МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01-1Спец
_____ Макаренко О.Р.
(подпись)

Отчет защищен с оценкой

_____

_____ С.С. Зотов
(подпись) (И.О. Фамилия)

« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН

_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____

« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.

на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Содержание

Задание на практику

- Проведение исследования в области мошенничества и киберпреступности
- Написание отчета по практике о проделанной работе.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1.Ознакомиться с понятием киберпреступности.

2.Теоретически ознакомиться с методами предотвращения мошенничества и киберпреступности.

3.На основе полученных знаний написать отчет по практике о проделанной работе.

Противодействие мошенничеству и киберпреступности

Аннотация:

Киберпреступность является глобальной проблемой, приобретающей все более широкие масштабы. Неважно, владеете ли вы малым предприятием или компанией из списка 500 ведущих компаний журнала «Форчун», покупаете ли вы ваш первый смартфон или становитесь экспертом в области кибербезопасности, вам необходимо знать о существовании киберпреступности. Интернет предоставляет беспрецедентные возможности в сфере образования и предпринимательства. Однако в то же время он предоставляет также беспрецедентные возможности для причинения вреда. Злоупотребляя технологиями, киберпреступники разрушают предприятия и даже жизни.

Ключевые слова: киберпреступность, типы киберпреступлений, вирусы-шифровальщики, вирус-шифровальщик Netwalker.

Введение:

Киберпреступность - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Большинство киберпреступлений совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организациями.

Типы киберпреступлений

- Мошенничество с электронной почтой и интернет-мошенничество
- Мошенничество с использованием личных данных
- Кража финансовых данных или данных банковских карт
- Кража и продажа корпоративных данных
- Кибершантаж
- Атаки программ-вымогателей

- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)

Вирусы-Шифровальщики

Программы-шифровальщики относятся к классу троянцев-вымогателей — это вредоносное ПО, которое вносит несанкционированные изменения в пользовательские данные или блокирует нормальную работу компьютера. Для расшифровки данных и разблокировки компьютера злоумышленники обычно требуют денежного перевода (выкупа).

Классификация вирусов-шифровальщиков

Поскольку шифровальщики относятся к вредоносным программам, для них справедливы те же типовые классификационные основания, что и для других образцов опасного кода. Например, можно подразделять их по способу распространения: через фишинговые или спам-рассылки, загрузку зараженных файлов, использование файлообменных сервисов и т.д. Преобразовав файлы пользователя, вирус-шифровальщик (virus-encoder) обычно оставляет инструкцию: в виде фона рабочего стола, как текстовый документ на рабочем столе или в каждой папке с зашифрованными файлами.

Источник угрозы

Вирусы-шифровальщики распространяются так же, как и любые другие программы-вымогатели. Методы и способы их доставки жертве постепенно усложняются: злоумышленники маскируют их под официальное приложение банка, новую версию известного ПО (зафиксированы даже случаи, когда шифровальщики устанавливались под видом обновления Adobe Flash). Однако самым популярным способом распространения шифровальщиков остается спам.

Как защититься от шифровальщиков?

- Регулярно делать резервные копии данных, чтобы их можно было восстановить в случае инцидента.

- Использовать инструменты для автоматического обнаружения уязвимостей и установки исправлений.

- Своевременно обновлять приложения и операционные системы на всех устройствах.

- Не открывать подозрительные файлы или ссылки в электронных письмах.

- Установить на компьютер антивирус

- Скачивать программы только с сайта разработчика или с проверенных ресурсов.

Вирус-шифровальщик Netwalker

Netwalker — это быстро набирающая масштабы программа-вымогатель, созданная в 2019 году группой киберпреступников, известной как Circus Spider. На первый взгляд Netwalker действует, как и большинство других разновидностей программ-вымогателей: проникает в систему через фишинговые письма, извлекает и шифрует конфиденциальные данные, а затем удерживает их для получения выкупа.

Но Netwalker способен на большее, чем просто удержание захваченных данных. Чтобы продемонстрировать серьезность своих намерений, Circus Spider публикует образец украденных данных в интернете, заявляя, что, если жертва не выполнит их требования вовремя, то в даркнет попадут и остальные данные. Circus Spider выкладывает конфиденциальные данные жертвы в даркнете в защищенной паролем папке и публикует пароль в интернете.

На кого и на что нацелена программа-вымогатель Netwalker?

С момента первого крупного результата в марте 2020 года наблюдается всплеск атак программы-вымогателя Netwalker. В первую очередь, ее целями стали учреждения здравоохранения и образования. Они провели одну из своих наиболее публично освещенных кампаний против крупного университета, специализирующегося на медицинских исследованиях. Программа-вымогатель похитила конфиденциальные данные этого университета, и, чтобы показать серьезность намерений, злоумышленники выложили образец украденных данных в открытый доступ. Эти данные включали студенческие приложения, содержащие такую информацию, как номера социального страхования и другие конфиденциальные данные. Это нарушение привело к тому, что университет заплатил злоумышленникам выкуп в размере 1,14 миллиона долларов за расшифровку их данных.

Злоумышленники, стоящие за Netwalker, предприняли серьезную попытку извлечь выгоду из хаоса эпидемии коронавируса. Они рассылали фишинговые электронные письма на тему пандемии, выбрав целью медицинские учреждения, которые уже перегружены пострадавшими от пандемии. Сайт одной из первых жертв в сфере здравоохранения был заблокирован программой-вымогателем как раз в тот момент, когда люди начали обращаться к ним за советом во время пандемии. Эта атака вынудила их запустить второй сайт и направить пользователей на новый, вызвав беспокойство и замешательство у всех участников. В течение года Netwalker и другие группы программ-вымогателей продолжали атаковать медицинские учреждения, пользуясь тем, что они уделяют мало внимания информационной безопасности.

Помимо сфер здравоохранения и образования, Netwalker атакует организации в других отраслях, в том числе:

- производство;
- управление бизнесом;
- управление потребительским опытом и качеством обслуживания;
- электромобили и решения для накопления электричества;
- образование;
- и многие другие.

Как работает Netwalker?

Шаг 1: фишинг и проникновение

Netwalker в значительной степени полагается на фишинг и адресный фишинг как методы проникновения. Если сравнивать с другими программами-вымогателями, рассылки фишинговых писем у Netwalker происходят часто. Эти письма выглядят вполне легитимно, что легко вводит в заблуждение жертв. Обычно Netwalker прикрепляет сценарий VBS с названием CORONAVIRUS_COVID-19.vbs, который запускает программу-вымогатель, если получатель откроет вложенный текстовый документ с вредоносным сценарием.

Шаг 2: эксфильтрация и шифрование данных

Если сценарий открывается и запускается в вашей системе, значит Netwalker начал проникать в вашу сеть. С этого момента начинается отсчет времени до шифрования. Попав в систему, программа-вымогатель превращается в не вызывающий подозрений процесс, обычно в виде исполняемого файла

Microsoft. Это достигается за счет удаления кода из исполняемого файла и внедрения в него собственного вредоносного кода для доступа к process.exe. Этот метод известен как Process Hollowing. Он дает программе-вымогателю возможность находиться в сети достаточно долго для извлечения и шифрования данных, удаления резервных копий и создания лазеек на случай, если кто-либо заметит, что что-то не так.

Шаг 3: вымогательство и восстановление (или потеря) данных

Как только Netwalker закончит эксфильтрацию и шифрование данных, жертва обнаружит, что данные украдены, и найдет записку с требованием выкупа. Записка с требованием выкупа Netwalker относительно стандартна: в ней объясняется произошедшее и что пользователь должен делать, если хочет вернуть свои данные в целости и сохранности. Затем Circus Spider потребует определенную сумму денег для оплаты в биткойнах, используя портал браузера TOR.

Как только жертва удовлетворяет выдвинутые требования, она получает доступ к своему индивидуальному инструменту дешифрования и может безопасно расшифровать свои данные.
Если жертва не выполнит требования вовремя, злоумышленники увеличат размер выкупа или опубликуют в даркнете все украденные данные либо их часть.

Советы по защите от программы-вымогателя Netwalker:

- Выполнять резервное копирование важных данных на локальные хранилища данных;
- Убедиться, что копии критически важных данных хранятся в облаке, на внешнем жестком диске или устройстве хранения;
- Защитить свои резервные копии и убедиться, что данные невозможно изменить или удалить из системы, в которой они хранятся;
- Установить и регулярно обновлять антивирусное программное обеспечение на всех компьютерах;
- Использовать только безопасные сети и избегайте общедоступных сетей Wi-Fi. По возможности используйте VPN;
- Использовать двухфакторную аутентификацию с надежными паролями;
- Регулярно обновлять компьютеры, устройства и приложения. Netwalker, как и другие программы-вымогатели, использует уязвимости в системах и инфраструктуре, чтобы взять под контроль

компьютеры пользователей и целые сети, а затем удерживает ваши данные в зашифрованном виде, пока вы не заплатите выкуп.

Вывод:

В ходе изучения различных статей можно сделать вывод, что вопрос киберпреступности и мошенничества в наше время имеет огромное значение. Стать жертвами мошенников могут не только крупные компании, но и рядовые пользователи. Существует множество способов предотвращения деятельности мошенников, которыми должны пользоваться все пользователи сети чтобы не попадать в неприятные ситуации.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики познакомился с рекомендациями и мерами защиты информации при удаленной работе. Познакомился с DLP-системами, их функциями, составом, способами работы. Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1. Номоконов В. А. Киберпреступность как новая криминальная угроза
2. Згадзай О. Э. Киберпреступность: факторы риска и проблемы борьбы
3. Чекунов И.Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы
4. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение
5. Пархоменко С.В. Предупреждение компьютерной преступности в Российской федерации: интегративный и комплексный подходы / С.В. Пархоменко, К.Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права.