Батчаева З.Б., Дауров Р.Т., Салпагарова М.У., Болурова М.И.
Расследование преступлений в компьютерной сфере

СКГА
(Россия, Черкесск)

doi: 10.18411/lj-12-2019-11

idsp: ljjournal-12-2019-11

Аннотация

В настоящее время проблема компьютерных вирусов и хакерских атак набирает огромные обороты. По мере усовершенствования разработчиками защиты своих продуктов растет и изобретательность хакеров. В статье рассматриваются основные виды преступлений в компьютерной сфере и каким образом ведется борьба с ними.

Ключевые слова: хакер, вирус, антивирусная программа, кража личных данных, DDOS-атака, информационная безопасность

Abstract

Problem of computer viruses and hacker attacks is becoming very serious nowadays. As developers improve the security of their products as the ingenuity of hackers grows. The article deals with the main types of crimes in the computer sphere and how to combat them.

Keywords: hacker, virus, antivirus software, theft of personal data, DDOS-attack, information security

Преступления, совершаемые с использованием компьютерных средств и систем принято называть компьютерными преступлениями.

Пока мы пользуемся своими ноутбуками, смартфонами, за нашей личной информацией ведется непрерывная охота. Хакеры придумывают все более сложные и изощренные вирусы, а те, кто с ними борются, наращивают все более сложную защиту. Рассмотрим это на примере пирамиды. Внизу находятся самые массовые угрозы, с которыми мы сталкиваемся каждый день это «черви», «трояны», «фишинговые письма» и большинство интернет атак. Чуть выше находятся целевые кибератаки, т.е. нацеленные на конкретных людей или организаций, а на самом верху расположилась новинка нашего столетия - кибероружие. Каждый хакер сам решает, какую нишу ему занять, после чего начинается настоящая война со специалистами в кибербезопасности.

С каждым годом ее темпы растут, все что происходило раньше игрушки по сравнению с новейшими атаками и расследованиями. Для начала стоит отметить что большая часть атак ни на кого конкретно не нацелена, это обычно «трояны», или «фишинговые письма» которые просто так «гуляют» по сети. Их жертвами как правило становятся те, кто не позаботился о своей интернет безопасности или можно сказать по-другому, о своей киберграмотности. Например, на почту приходит такое письмо: «Привет, Макс! Вчера классно оттянулись. Особенно когда ты стал голым танцевать в клубе. Прикрепила фотки с голым тобой, обязательно посмотри». К этому письму прикрепляют файл. И соответственно те, у кого на днях была вечеринка не усомнятся в том, что это письмо адресовано именно им. Человек открывает письмо, скачивает архив, открывает файл и ничего не происходит, а «зараженный» думает, что это какая то ошибка и просто закрывает письмо и забывает о нем. Через какое то время он обнаруживает, что на карте стало меньше денег или вообще все деньги исчезли. Все попытки понять, как это произошло тщетны. Это как в фильмах про зомби где главный герой в конце оказывается заражен, а вот когда его «укусили» не понятно. Но на самой деле все произошло от небольшой строчки кода, которая содержалась в скаченном файле, она и запустила зловердный вирус.

Раньше браузеры были менее защищены. Есть атаки построенные на невнимательность и называются «Homograph attack». Такая атака направлена на то, что бы подменить URL настоящего сайта на фэйковый и заходя в него, пользователь попадает на совершенно другую страницу. Есть даже специальные программы для генерирования фальшивых URL, которые подставляются в настоящие сайты. Вводишь нужный сайт и вот, у тебя уже хитрая копия URL.

Сейчас браузеры сами определяют настоящую опасность. Но это помогает не всегда. Всего пару лет назад, не составило бы никакого труда взломать страницу Instagram любого пользователя, достаточно было узнать его логин, а дальше все делала программа по подбору паролей. Но хорошая новость заключается в том, что киберграмотность растет, сейчас уже не каждый будет кликать на сомнительные ссылки из писем или смс. Но плохая новость в том, что это понимают и хакеры и теперь они начали действовать по-другому. «Drive-by download» это новый тип кибератак, теперь не нужно ничего скачивать, ты просто заходишь на WEB страницу и ты уже «заражен». Так происходит, если у вас не обновлены программы на компьютере. Например браузеры, хакеры используют ошибки в них что бы незаметно запустить свой вирус.

Пользоваться приложениями куда безопаснее, чем сайтами, разработчики закладывают в них сразу ряд проверок. Но чем больше людей используют это приложение, тем больше соблазна для хакера атаковать его, несмотря на все сложности. Сегодня не каждый человек может обойтись без телефона, это первое что мы видим утром и последнее перед сном. Мы отдали смартфону все свои функции, это раньше мошенники могли снять со счета телефона рублей 300, благодаря звонкам и смс, под предлогом проблем в семье и т.д. Но теперь, когда у всех установлены банковские приложения, можно вывести гораздо больше денег, а это в свою очередь заманчивое предложение для хакеров.

Есть множество вариантов как это можно сделать, одним из них являются фэйковые приложения, чаще всего фэйки выдают себя за популярные приложения, мессенджеры, музыки или даже за настоящую игру. Google Pay или App Store - для многих гарант качества и безопасности, эта видимость позволяет мошенникам придумывать более законные схемы мошенничества.

Для примера приложение «Ancestry» она якобы помогает найти своих предков, вводишь имя, дату и место рождения, и приложение просит тебя поднести палец, и люди не задумываясь просто касаются сканера, тем самым приобретая платную подписку для этого приложения, и это всего лишь одна программа из множества которые находятся в «безопасных» Google Play или App Store.

Порой ты просто скачиваешь приложение и спустя несколько дней оно начинает списывать деньги за подписку. Казалось бы, мы никуда не подписывались, но это все было в пользовательском соглашении, которое 99% людей никогда не читают. Поэтому не стоит доверять сомнительным приложениям, хоть у него будет пять звезд, скорее всего все комментарии и оценки фэйковые.

Приложения готовы списывать у вас деньги не так страшны, по сравнению с теми которому пользователь отдает рут права от своего телефона, т.е. приложение получает полный доступ к глубинным функциям смартфона и очистить его будет уже невозможно. Хакер сможет незаметно снимать вас на вашу же камеру, сможет перехватывать смс, записывать речь с диктофона, следить за вашей геолокацией.

Вспомнить хотя бы приложение Getcontact, всем было интересно узнать как их записали в телефоне другие, как результат - миллионы слитых телефонных номеров с именами. Это можно назвать самой гениальной аферой из последних, где каждый человек слил как минимум 100 своих контактов. И все это потом оказывается в

телефонных базах, и потом все удивляются, почему звонят незнакомые номера и предлагают ненужные услуги.

Личные данные это не все что нужно хакеру, после того как он получает все что ему нужно, вы все еще остаетесь для него полезными. Хакер встраивает ваш телефон в армию ботов «BOTNET» и вы становитесь его марионеткой, даже сами этого не подозревая. Если ваш «Хозяин» крупный хакер, вы становитесь «солдатом» в «DDOS» атаках. Грубо говоря, в любой момент хакер может приказать своей «Армии ботов» обрушить какой-либо сайт. Он через командный центр «приказывает» всем устройствам зайти на этот сайт, так как они это делают одновременно, сайт не выдерживает такого наплыва пользователей и просто «рушится». Чем больше армия хакера, тем больше денег стоят его услуги. Из-за BOTNET «Mirai» обрушилось множество сайтов включая даже Twitter, этот бот объединил более 300тыс. устройств по всему миру в 2016 году, это были не только смартфоны и компьютеры, но так же видеорегистраторы, камеры и даже тостеры. Такими вирусами легко заразиться, если скачивать пиратские программы из файлообменников.

Современные антивирусные программы способны эффективно обнаруживать вредоносные объекты внутри файлов, программ и документов. «Лаборатория Касперского», признанный лидер в области разработки решений для обеспечения IT-безопасности, теперь предлагает услуги по расследованию компьютерных инцидентов. Ведущие эксперты в сфере анализа вредоносного ПО в сотрудничестве со специалистами, имеющими большой опыт работы в правоохранительных органах. Перед специалистами «Лаборатории Касперского» стоит задача помочь организации взять ситуацию под контроль, восстановить возможную картину происшедшего, определить использованные злоумышленниками инструменты и методы, а также по возможности идентифицировать вовлеченные в инцидент компьютеры и мобильные устройства.

В ходе предварительной консультации по телефону специалисты «Лаборатории Касперского» проинструктируют вас о том, какие действия необходимо немедленно предпринять для локализации и сдерживания инцидента, а также для минимизации возможного ущерба.

Затем специалисты «Лаборатории Касперского» выезжают на место происшествия для выявления затронутых инцидентом устройств и носителей информации, корректного копирования данных для их последующего анализа, а также для оформления документов, необходимых правоохранительным органам для проведения дальнейшего расследования и возбуждения уголовного дела.

Собранные данные тщательно анализируются и проверяются на наличие вредоносного ПО. В случае его обнаружения исследуется способ распространения вредоносного ПО, совершаемые им в системе действия и возможные пути заражения. После этого специалисты «Лаборатории Касперского» составляют рекомендации по удалению вредоносного ПО и ликвидации последствий заражения.

В некоторых случаях для возбуждения уголовного дела необходимо провести дополнительное расследование, чтобы понять, откуда и как было произведено вторжение, а также установить лиц, причастных к инциденту.

Аналитики «Лаборатории Касперского» работают одновременно по всем направлениям, которые могут помочь расследованию, – от поиска финансовых следов и исследования технических аспектов инцидента до сбора информации в хакерских сообществах и сопоставления ее с фактами, обнаруженными в ходе расследования. Специалисты «Лаборатории Касперского» регулярно обсуждают с клиентом текущие результаты расследования и его дальнейшие перспективы.

По результатам расследования клиент получает итоговый отчет, который отражает результаты всех этапов проведенного расследования, содержит подробную схему инцидента и заключение о выявленном источнике атаки. Как правило, материалов, содержащихся в этом отчете, достаточно для возбуждения правоохранительными органами уголовного дела в отношении конкретных лиц, стоящих за инцидентом. Кроме того, четкое понимание сценария и механизмов атаки позволяет выстроить правильную стратегию защиты от подобных атак в будущем.

После возбуждения правоохранительными органами уголовного дела специалисты «Лаборатории Касперского» могут участвовать в его расследовании в качестве официальных представителей клиента. Это позволяет ускорить расследование уголовного дела и повысить вероятность его успешного завершения.

В рамках сервиса «Расследование компьютерных инцидентов» осуществляется аналитическая и информационно-техническая поддержка правоохранительных и следственных органов, подача ходатайств о производстве необходимых следственных мероприятий, участие в них и выполнение других действий, предусмотренных законодательством.

Сотрудничая с «Лабораторией Касперского» на этапе ведения уголовного дела, ваша организация не тратит лишнее время на общение с правоохранительными органами и может быть уверена в том, что наши опытейшие эксперты используют все имеющиеся в их распоряжении возможности для сбора необходимых доказательств. Вынесение по уголовному делу обвинительного приговора дает возможность обратиться с гражданским иском о компенсации ущерба.

Из всего вышесказанного можно смело сделать вывод, что необходимость защиты от компьютерных вирусов на данный момент стоит на первом месте.

Для предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.

1. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/10677.html> (дата обращения: 21.12.2019). — Режим доступа: для авторизир. Пользователей
2. Основы информационной безопасности : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2017. — 287 с. — ISBN 978-5-238-02857-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/72444.html> (дата обращения: 21.12.2019). — Режим доступа: для авторизир. Пользователей
3. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 с. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/72341.html> (дата обращения: 21.12.2019). — Режим доступа: для авторизир. Пользователей
4. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 с. — ISBN 978-5-4487-0298-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/77320.html> (дата обращения: 21.12.2019). — Режим доступа: для авторизир. Пользователей