Литература

1. Язык телодвижений: как читать мысли окружающих по их жестам / Аллан и Барбара Пиз; [пер. с англ. Т. Новиковой]. - Москва: Эксмо, 2018. - 448 с.: ил.

2. Экман П., Фризен У. Узнай лжеца по выражению лица / Пер. с англ. — СПб: Питер, 2010. — 272с.: с ил.

3. Библия языка телодвижений / Десмонд Моррис; (пер. с англ. Н. Караева). — М.: Эксмо, 2010. — 672 с.: ил.

УДК 004.056

СПАМ КАК АТАКА ТЕЛЕФОНА. МЕТОДЫ БОРЬБЫ.

Гаро В.А., Лозовик К.В.
Научный руководитель: ст. преподаватель Галай Т.А
Белорусский национальный технический университет

Спам сообщения – нескончаемое количество сообщений с бессмысленным содержанием, угрозами или вирусами. Они могут приходить с различных номеров или контактов. Отличие такой атаки заключается в формате контактов, с которых идут сообщения. Вред такой атаки состоит в том, что рассылка приходит слишком часто, и попытки очистить телефон будут напрасны. В некоторых случаях лучшим способом может быть смена номера или выключение телефона.

Такие атаки могут быть произведены по ряду причин: от шутки до мести. Действия злоумышленников могут перегрузить коммуникационную инфраструктуру и привести к негативному исходу из-за плохой меры безопасности, особенно на страницах регистрации. Осуществляются СМС-атаки при помощи вредящих ботов и специальных программ-сервисов, которые имеют огромную базу номеров телефонов.

СМС-атаки сопряжены с различными высокими рисками. Некоторыми из них являются:

1. Финансовые потери. Пока СМС-атаки не будут обнаружены и не будут приняты меры по ее обезвреживанию, месячный бюджет компании на СМС-рассылку может быть значительно израсходован, а при объемной атаке — даже закончен. СМС-атаки существенно перегружают формы верификации. Из-за высокой нагрузки клиенты не смогут зайти в свой личный кабинет и сделать покупку.

2. Ущерб репутации. Такое происшествие как СМС-атака может лишить компанию большой части её клиентской базы из-за возрастающего

количества недовольных клиентов, которое после может отразиться в СМИ и иных социальных сетях.

3. Нарушение персональных данных. Украденная база данных контактов может быть со временем использована в злоумышленных целях. Следовательно, клиентская база компании оказывается под угрозой. Это приведет к тем же ущербам, о которых говорилось раньше.

Существует три главных вида рассыльщиков: мошенники, роботы, операторы кол-центров.

Возможность реализовать злонамеренные действия появилась по причине слабой защиты смс-шлюзов, которые используются для обмена сообщениями владельцы смартфонов. Вы могли встречать примеры работы шлюзов на примере сайтов, позволяющих отправлять бесплатно короткие сообщения с использованием виртуального номера.

Шлюзы иногда используют в коммерческих целях. К ним подключают специальный софт для массовых отправок SMS. Подобные приложения позволят:

– организовать обратную связь с коллегами или партнёрами

– быстро сообщить важную информацию своим сотрудникам, в том числе и удалённым

– проинформировать клиентов о новинках, скидках и акциях.

Интерфейс шлюзов довольно прост и этим пользуются злоумышленники. При этом спам приходит и на линии IP-телефонии. Спамеру достаточно создать учётную запись, и он может отправлять бесчисленное количество SMS. Такой метод вреда пользователям имеет сравнительно низкую стоимость и высокую эффективность.

По различным причинам количество нежелательных звонков от спамеров и мошенников может внезапно возрасти, достигая нескольких десятков за сутки. Иногда это происходит из-за действий самого владельца номера, например, в результате размещения его контактных данных в сети или по попаданию номера в базу мошенников. Часто одни и те же списки номеров передаются между различными спам-центрами и мошенническими группировками. Если внезапно начинаются частые звонки, вероятно, номер попал в руки ещё одной группировки злоумышленников. Часто мошенники проявляют особую активность по отношению к новым жертвам, продолжая беспокоить их до тех пор, пока те не столкнутся с обманом или не раскроют его. Похожим образом могут действовать рекламные агенты и другие спамеры, продолжая звонить абоненту до тех пор, пока он не ответит на звонок и не выслушает их предложение

Существует несколько видов спама на телефоне, которые могут быть опасными:

1. SMS-спам. Злоумышленники могут отправлять SMS-сообщения с ссылками на вредоносные веб-сайты или просить вас отправить личные данные.

2. Звонки с мошеннической целью Злоумышленники могут звонить, представляясь сотрудниками банка, службы безопасности или других организаций с целью получить ваши личные данные или совершить финансовое мошенничество.

3. Vishing (голосовой фишинг). Это форма мошенничества, при которой злоумышленники используют звонки, чтобы выманивать личные данные, например, номера карты или пароли.

Чтобы защитить себя от спама на телефоне как от атаки, следует применять следующие меры:

4. Блокировка номеров. Многие современные телефоны имеют функцию блокировки номеров. Вы можете заблокировать номера, с которых приходит спам.

5. Использовать приложения, которые блокируют спам. Эти программы могут автоматически вычислять и останавливать ненужные сообщения и звонки.

6. Не отвечать на странные звонки. Если вы не уверены в источнике звонка, лучше не отвечайте на него. Это может помочь избежать попадания в список активных номеров для спамеров.

7. Сообщите о спаме провайдеру услуг. Если вы получаете массовые спам-звонки от определенного номера или оператора, сообщите об этом своему провайдеру услуг.

8. Запрет на массовую SMS-рассылку. Вы можете запросить у своего оператора услугу, которая блокирует массовую SMS-рассылку на ваш номер.

9. Будьте осторожны с предоставлением своего номер. При заполнении анкет, регистрации на сайтах или участии в акциях убедитесь, что ваш номер не будет использован для рассылки спама.

10. Поддерживайте список "не звонить". Регистрация вашего номера в списке "не звонить" может помочь снизить количество спам-звонков.

11. Используйте функцию фильтрации звонков. Некоторые телефоны имеют функцию фильтрации звонков, позволяющую настроить параметры принятия звонков от определенных номеров или групп номеров.

Таким образом, спам-атаки являются одними из серьёзных проблем в нашем цифровом мире. Они создают неудобства, нарушают конфиденциальность и могут представлять угрозу для систем и данных. Способы борьбы со спамом требуют внимания и активных действий от пользователей, компаний-провайдеров почты и их клиентов.

Литература

1. СМС-бомбинг: как защитить свои сервисы от атак [Электронный ресурс]. – Режим доступа: https://kontur.ru/articles/48471-sms_bombing_kak_zashhitit_svoi_servisy_ot_atak Дата доступа: 26.01.2024

2. Спам-атаки на смартфон: что это и как с ней бороться? [Электронный ресурс]. – Режим доступа: https://www.mtt.ru/support/blog/spam-ataki-na-smartfon/ Дата доступа: 26.03.2019

3. Как избавиться от спам-звонков: рассматриваем доступные варианты [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/spam-calls-blocking/30186/ Дата доступа: 05.03.2021

УДК 004.73

СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ТАМОЖЕННЫЕ ТЕХНОЛОГИИ ПРИМЕНЯЕМЫЕ В ТАМОЖЕННЫХ ОРГАНАХ

Авторы: Панасюк В.Д., Коминч А.В.
Научный руководитель: ст. преподаватель Галай Т.А.
Белорусский национальный технический университет

Сетевые информационные таможенные технологии представляют собой совокупность методов и средств, используемых таможенными органами для обработки, хранения и передачи информации в рамках таможенных процедур. Они позволяют обеспечить эффективное управление таможенным контролем, улучшить качество обработки и анализа данных, а также обеспечить безопасность и конфиденциальность информации.

Основные характеристики сетевых информационных таможенных технологий:

1. Автоматизация процессов. Сетевые технологии позволяют автоматизировать многие таможенные процедуры, что ускоряет и облегчает работу таможенных служб.

2. Централизованное управление. Сетевые технологии позволяют централизованно управлять информационными ресурсами таможенных органов, обеспечивая единый доступ к данным, контроль и мониторинг процессов.

3. Интеграция систем. Сетевые технологии позволяют интегрировать различные информационные системы таможенных органов, обеспечивая обмен информацией между ними и совместное использование данных.