Вредоносные ссылки в электронных письмах

Как защититься от фишинга, кибермошенничества и других угроз

cisco

Содержание

Введение

В прошлом году понятию «спам» исполнилось 40 лет. Именно в 1978 году Гари Туерк, менеджер по маркетингу компании Digital Equipment Corporation, отправил первое спам-сообщение на почту 393 пользователей через сеть ARPANET, чтобы представить новый продукт. Получатели были так же «рады» такому посланию, как и современные пользователи. Туерк получил строгий выговор, и ему запретили впредь совершать что-либо подобное.

К сожалению, на сегодняшний день все намного сложнее. За последние 40 лет количество спама возросло в геометрической прогрессии, а наши почтовые ящики переполнены ненужной рекламой фармацевтических препаратов, диетических продуктов и вакансиями. И не стоит забывать про более опасных «родственников» спама: фишинг и вредоносное ПО. Первый случай фишинга был зафиксирован более 30 лет назад, а распространение вредоносного ПО через электронную почту продолжается уже около 10 лет.

На сегодняшний день, как ни печально это признавать, многие электронные письма содержат ненужный спам, а часто и вещи похуже. Размах бедствия просто ужасает: по сообщению Talos Intelligence 85 процентов всех электронных писем, полученных в апреле 2019 года, относились к спаму. Объем нежелательных сообщений также вырос: в апреле количество спама достигло своего максимума за последние 15 месяцев.

Отправитель vs. получатель

Можно утверждать, что формат электронных писем идеально подходит для мошенников. Получатель должен ознакомиться с письмом, оценить полученную информацию, а затем решить, следует ли открыть предлагаемый файл или перейти по ссылке. Заставить выполнить нужное действие можно лишь используя социальную инженерию, основанную на природе людей.

Именно подобные социотехники делают мошеннические схемы такими привлекательными, а также столь сложными для систематической защиты. Чаще всего атаки на электронную почту оказываются успешными. Прекрасно известна уловка, когда URL-адрес в письме ведет на мошеннический или вредоносный веб-сайт с использованием эксплойт-наборов. Однако пользователи все равно переходят по вредоносным ссылкам.

Значение для бизнеса

Неудивительно, что защита электронной почты стала ключевой проблемой руководителей отделов информационной безопасности. В недавнем опросе руководителей отделов информационной безопасности выяснилось, что 56 % опрошенных считают очень сложным или чрезвычайно трудным делом защиту от поведения пользователей, которое включает в себя переход по вредоносным ссылкам из электронных писем. То есть главной проблемой безопасности руководители считают защиту электронной почты по сравнению с другими киберугрозами, включая защиту данных в общедоступном облаке и использование мобильных устройств.

Во многом это связано с высокой частотой таких атак. Например, 42 % опрошенных руководителей отделов ИБ сталкивались с инцидентами, вызванными переходом по вредоносной ссылке из спам-письма. У 36 % респондентов результатом фишинговых атак стала кража данных. Согласно данным нашего опроса руководители считают атаки на электронную почту главной угрозой безопасности своих организаций.

В отдельном исследовании, заказанном Cisco и выполненном компанией ESG, 70 % респондентов сообщили, что становится все сложнее защититься от угроз, связанных с мошенническими ссылками в электронных письмах. Если говорить о последствиях атак, связанных с электронными сообщениями, 75 % опрошенных сообщили о серьезном отрицательном воздействии на работу компании, а 47 % респондентов заявили о значительных финансовых последствиях.

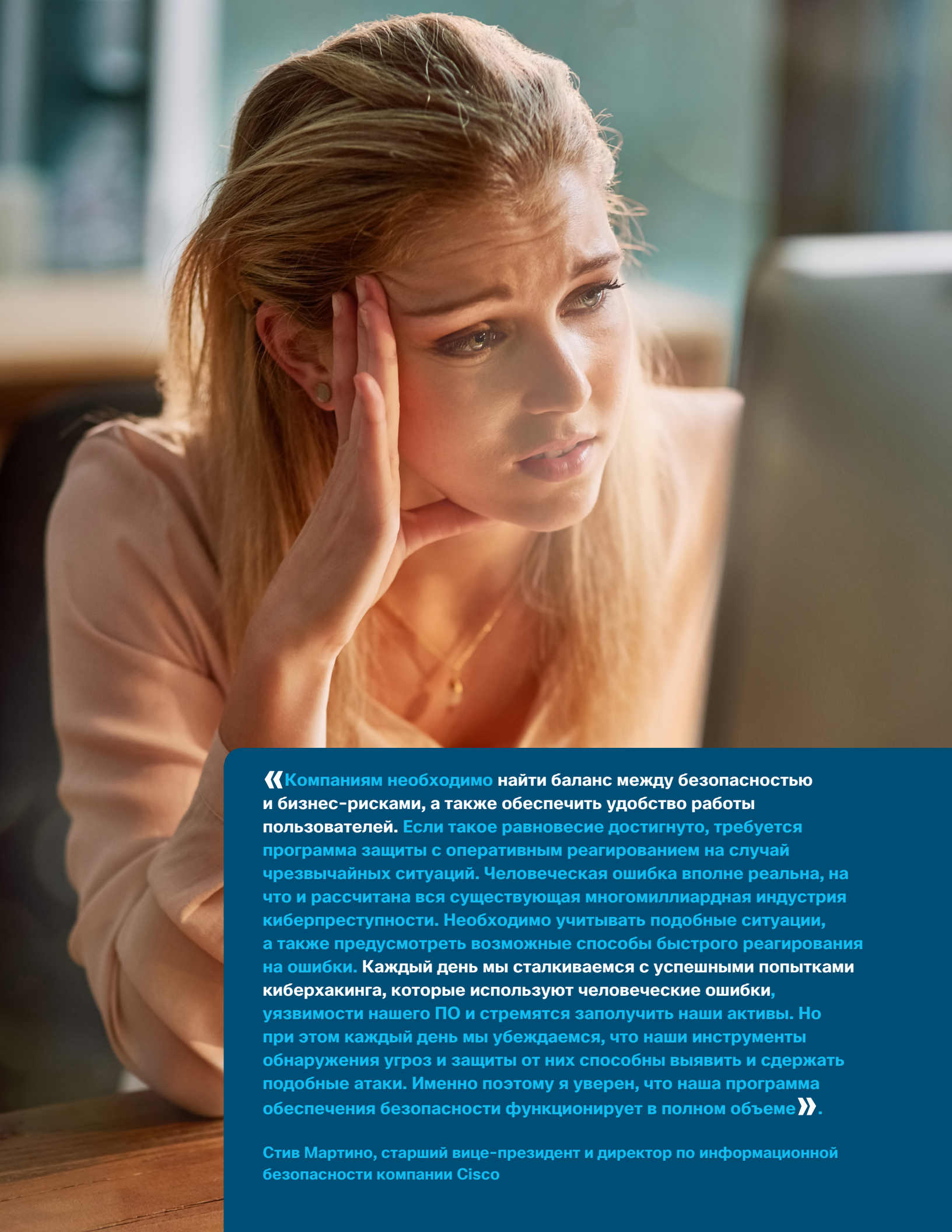
Требуется ответ

Как защитить то, что абсолютно необходимо, но при этом представляет угрозу? Для многих организаций решением стал переход на облачные технологии. Однако эту технологию нельзя назвать панацеей от опасностей, связанных с электронной почтой. В большинстве случаев это всего лишь полумеры, которые не решают проблему, а лишь усугубляют ее.

Существует несколько способов свести к минимуму последствия атак на электронную почту. В этом документе мы расскажем о текущей ситуации с угрозами, представив обзор наиболее распространенных в настоящее время типов атак на электронную почту. Мы опишем сценарии угроз, их задачи и используемую инфраструктуру. Также мы расскажем, как можно защитить свой бизнес и идентифицировать угрозы, связанные с мошенническими ссылками в электронных письмах

«В среднем мы получаем около 412 тысяч электронных сообщений в день, из которых 266 тысяч сообщений даже не доходят до SMTP, поскольку Talos блокирует их на основе глобальной аналитики угроз».

Милинд Самант, директор по информационной безопасности SUNY Old Westbury



«Компаниям необходимо найти баланс между безопасностью и бизнес-рисками, а также обеспечить удобство работы пользователей. Если такое равновесие достигнуто, требуется программа защиты с оперативным реагированием на случай чрезвычайных ситуаций. Человеческая ошибка вполне реальна, на что и рассчитана вся существующая многомиллиардная индустрия киберпреступности. Необходимо учитывать подобные ситуации, а также предусмотреть возможные способы быстрого реагирования на ошибки. Каждый день мы сталкиваемся с успешными попытками киберхакинга, которые используют человеческие ошибки, уязвимости нашего ПО и стремятся заполучить наши активы. Но при этом каждый день мы убеждаемся, что наши инструменты обнаружения угроз и защиты от них способны выявить и сдержать подобные атаки. Именно поэтому я уверен, что наша программа обеспечения безопасности функционирует в полном объеме».

Стив Мартино, старший вице-президент и директор по информационной безопасности компании Cisco

Фишинг и электронная почта. Текущая ситуация

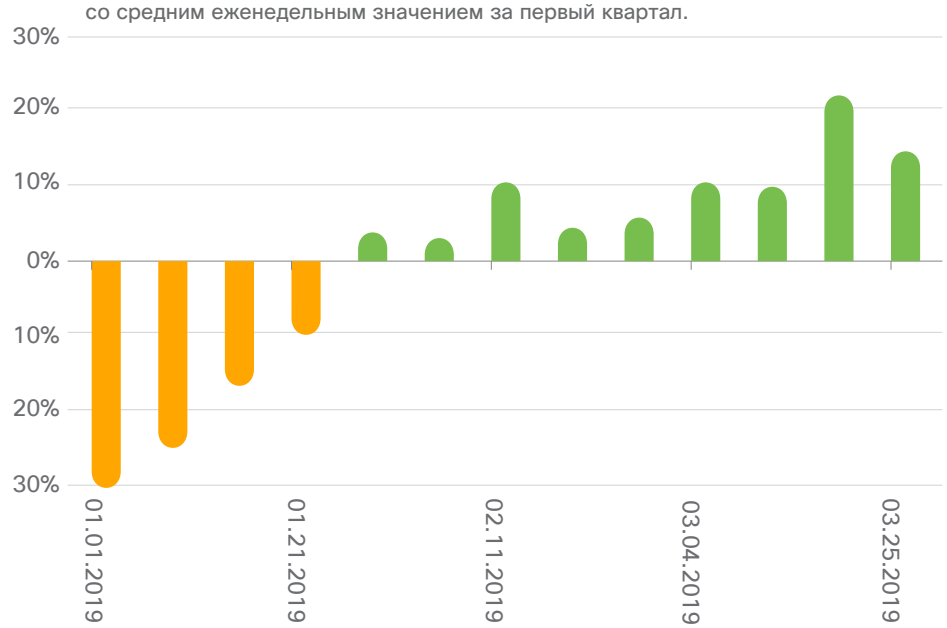
Огромное количество угроз связано с сообщениями электронной почты. Согласно отчету о расследованиях утечки данных Verizon 2018, участие в которых принимала компания Cisco, электронная почта – это самый популярный инструмент как для распространения вредоносного ПО (92,4%), так и для фишинга (96%). В результате выполнения инструкций из спамовых сообщений можно стать жертвой майнинга криптовалют, потерять все свои учетные данные или, поддавшись психологической атаке, лишиться значительной суммы денег. Сделайте поправку на масштабы предприятия и поймете, какой непоправимый вред могут нанести киберпреступники, используя сообщения электронной почты.

Как часто пользователи попадаются на крючок мошеннических ссылок в электронных письмах? Спросите об этом сотрудников Duo Security. Несколько лет назад команда разработала бесплатный инструментарий Free Duo Insight для создания фальшивых фишинговых кампаний, которые затем тестируются в собственных организациях. Таким образом можно выявить людей, которые могут стать жертвами подобной атаки.

К сожалению, многие люди не проходят это тестирование. Согласно отчету о доверенном доступе Duo за 2018 г., в результате 62 % кампаний по имитации фишинга был захвачен как минимум один набор учетных данных пользователей. Почти четверть получателей сообщений перешли по фишинговой ссылке в электронном письме. А половина из них ввела учетные данные на мошенническом веб-сайте.

С такими показателями неудивительно, что электронная почта – самый популярный инструмент для запуска фишинговых кампаний. В связи с ростом количества новых фишинговых доменов, обнаруженных Cisco Umbrella, можно ожидать целого шквала фишинговых атак. На основании данных за первый квартал 2019 года мы вывели средние показатели за неделю, которые затем сравнивали с последующими значениями. Результаты, представленные на Рис. 1, показывают, что, несмотря на низкие темпы роста на начало года, количество доменов увеличилось к последней неделе квартала на 64 % в сравнении с первоначальными показателями.

Рис. 1 Количество новых фишинговых доменов, появившихся за неделю, по сравнению со средним еженедельным значением за первый квартал.



Источник: Cisco Umbrella

Распространенные типы атак на электронную почту

Далее вкратце описаны наиболее распространенные в настоящее время атаки на электронную почту. Возьмите ноутбук, откройте папку «Входящие» и представьте, что вас ждут следующие непрочитанные сообщения.

Аналогичные фишинговые атаки наблюдались в отношении других облачных почтовых сервисов, таких как Gmail и G Suite.

Фишинг в Office 365

Кажется, что сообщение пришло от корпорации Microsoft. В нем говорится, что ваш адрес электронной почты Office 365 будет отключен из-за ошибок или нарушений политик. Единственный способ предотвратить это — подтвердить адрес по предоставленной ссылке.

Это попытка захватить ваши учетные данные Office 365. Используемые адреса и ссылки могут выглядеть вполне невинно: например, micros0ftsupport@hotmail.com. При переходе по ссылке откроется страница входа в систему, напоминающая официальную, где необходимо указать адрес электронной почты и пароль.

Тем не менее этот сайт является мошенническим. Как только хакеры получат учетные данные, они могут попытаться войти в другие службы Microsoft, а также собрать информацию о ваших контактах.

Один из распространенных методов обмана — выполнить вход в учетную запись электронной почты и отправить от вашего имени неофициальное письмо всем контактам (с возможной темой письма: FYI), содержащее другую вредоносную ссылку.

Этот метод атаки сейчас пользуется большой популярностью. Согласно данным, опубликованным нашими партнерами из Agari в отчете о тенденциях мошеннических действий, связанных с электронной почтой и кражей личных данных, за второй квартал 2019 г., 27 % современных атак на электронную почту запускаются через взломанные учетные записи. Это на 7 процентных пунктов выше, чем в последнем квартале 2018 г., когда уровень фишинговых атак, поступающих через взломанные учетные записи составил 20 %.

Кроме того, нападениям подвергается не только Office 365. Подобные же атаки были направлены против других облачных почтовых сервисов, включая облачные решения Google: Gmail и G Suite. С учетом распространенности учетных записей Google и их повсеместного использования для входа на различные сайты неудивительно, что хакеры создали фишинговые узлы и в этой области.

Рис. 2 Фишинговый сайт, который специально разработан так, чтобы быть похожим на страницу входа в Microsoft.

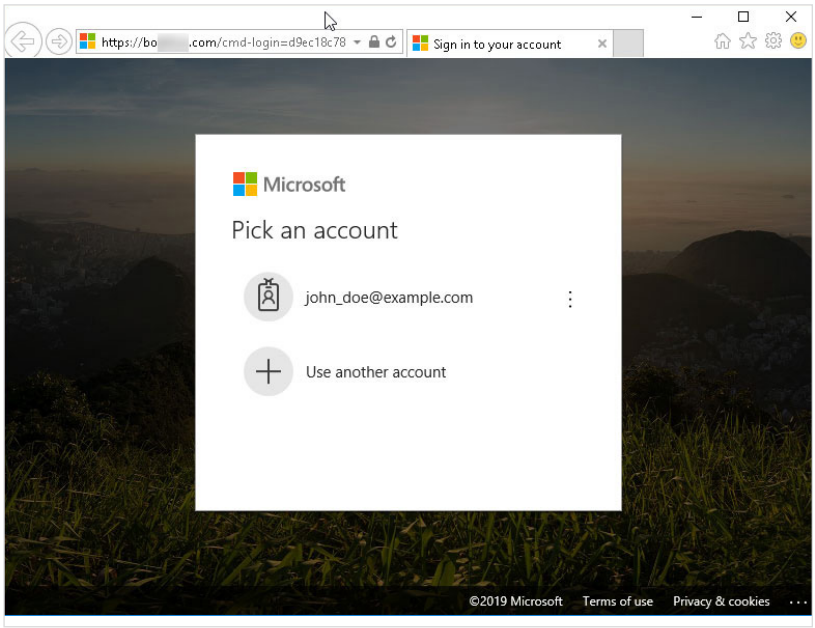
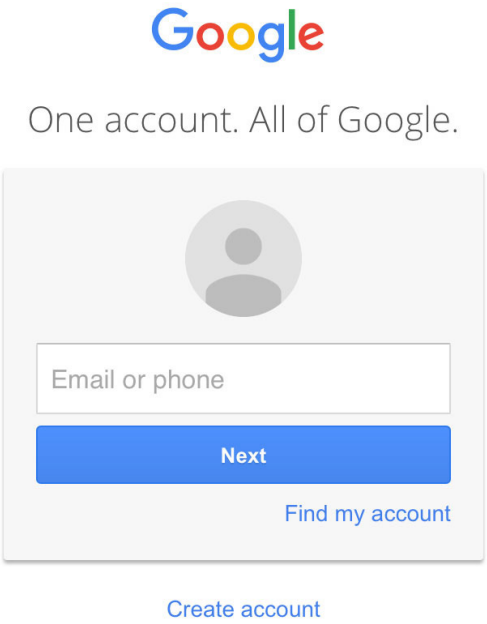


Рис. 3 Пример страницы входа в учетную запись Google. Легко ли отличить реальный сайт от подделки?



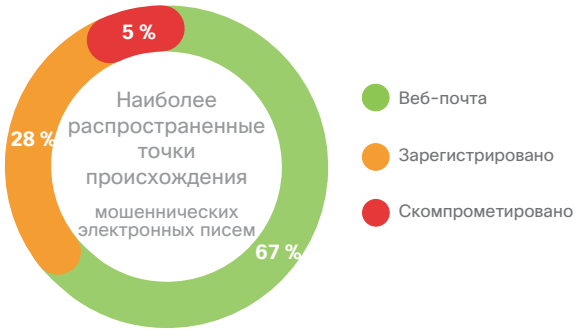
Утечка деловой переписки

На этой неделе происходит встреча глав компании, поэтому в офисе осталось лишь несколько сотрудников, которые следят за выполнением критически важных функций. Вы работаете в финансовом отделе и следите за функционированием сайта. Внезапно в папку «Входящие» приходит электронное письмо, которое, по-видимому, поступило от финансового директора с темой «Пропущенные платежи». В электронном письме объясняется, что платеж, который должен был поступить на прошлой неделе, был просрочен, что может привести к сбоям в цепочке поставок компании. В приложении находятся инструкции по совершению перевода. Отправитель заявляет, что свяжется с вами в течение часа.

Перед вами классический пример утечки деловой переписки. Подобного рода аферы – это разновидность мошеннических действий по электронной почте, когда киберпреступник притворяется руководителем высшего звена и пытается обманом заставить получателя выполнить свои рабочие обязанности, включая, к примеру, перевод денежных средств. Иногда мошенники и в самом деле звонят сотруднику и изображают начальника. И это часто срабатывает. По данным Центра приема жалоб на мошенничество в Интернете в 2018 году в результате утечки деловой переписки было украдено 1 300 000 000 долл. США.

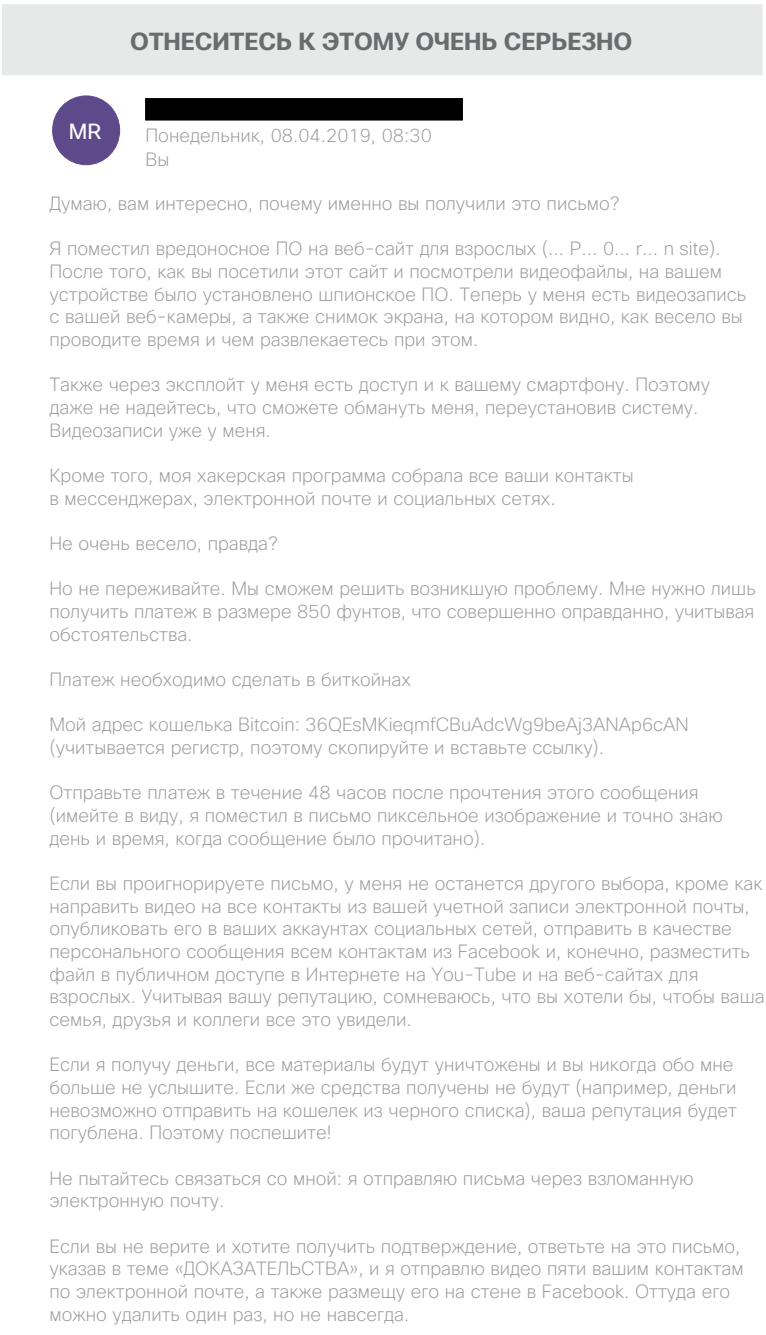
Можно предположить, что, как и в случае с фишинговыми атаками в Office 365, хакеры используют скомпрометированные учетные записи. Однако, согласно данным отчета компании Agari о тенденциях мошеннических действий, связанных с электронной почтой и кражей личных данных, за второй квартал 2019 г., этим приемом пользуются лишь около 5 % мошенников. В двух третях таких атак по-прежнему используются бесплатные учетные записи веб-сервисов, а оставшиеся 28 % запускают атаки через зарегистрированные домены. В последнем случае мошенники используют личные обращения даже в теле письма: согласно данным Agari к получателям обращаются по имени в одном из каждых пяти сообщений.

Рис. 4 Происхождение мошеннических электронных писем.



Источник: Agari Data, Inc.

Рис. 5 Пример недавнего случая цифрового вымогательства.



ОТНЕСИТЕСЬ К ЭТОМУ ОЧЕНЬ СЕРЬЕЗНО

MR [redacted]
Понедельник, 08.04.2019, 08:30
Вы

Думаю, вам интересно, почему именно вы получили это письмо?

Я поместил вредоносное ПО на веб-сайт для взрослых (... P... 0... r... n site). После того, как вы посетили этот сайт и посмотрели видеофайлы, на вашем устройстве было установлено шпионское ПО. Теперь у меня есть видеозапись с вашей веб-камеры, а также снимок экрана, на котором видно, как весело вы проводите время и чем развлекаетесь при этом.

Также через эксплойт у меня есть доступ и к вашему смартфону. Поэтому даже не надейтесь, что сможете обмануть меня, переустановив систему. Видеозаписи уже у меня.

Кроме того, моя хакерская программа собрала все ваши контакты в мессенджерах, электронной почте и социальных сетях.

Не очень весело, правда?

Но не переживайте. Мы сможем решить возникшую проблему. Мне нужно лишь получить платеж в размере 850 фунтов, что совершенно оправданно, учитывая обстоятельства.

Платеж необходимо сделать в биткойнах

Мой адрес кошелька Bitcoin: 36QEsMKieqmfCBuAdcWg9beAj3ANAp6cAN (учитывается регистр, поэтому скопируйте и вставьте ссылку).

Отправьте платеж в течение 48 часов после прочтения этого сообщения (имейте в виду, я поместил в письмо пиксельное изображение и точно знаю день и время, когда сообщение было прочитано).

Если вы проигнорируете письмо, у меня не останется другого выбора, кроме как направить видео на все контакты из вашей учетной записи электронной почты, опубликовать его в ваших аккаунтах социальных сетей, отправить в качестве персонального сообщения всем контактам из Facebook и, конечно, разместить файл в публичном доступе в Интернете на You-Tube и на веб-сайтах для взрослых. Учитывая вашу репутацию, сомневаюсь, что вы хотели бы, чтобы ваша семья, друзья и коллеги все это увидели.

Если я получу деньги, все материалы будут уничтожены и вы никогда обо мне больше не услышите. Если же средства получены не будут (например, деньги невозможно отправить на кошелек из черного списка), ваша репутация будет погублена. Поэтому поспешите!

Не пытайтесь связаться со мной: я отправляю письма через взломанную электронную почту.

Если вы не верите и хотите получить подтверждение, ответьте на это письмо, указав в теме «ДОКАЗАТЕЛЬСТВА», и я отправлю видео пяти вашим контактам по электронной почте, а также размещу его на стене в Facebook. Оттуда его можно удалить один раз, но не навсегда.

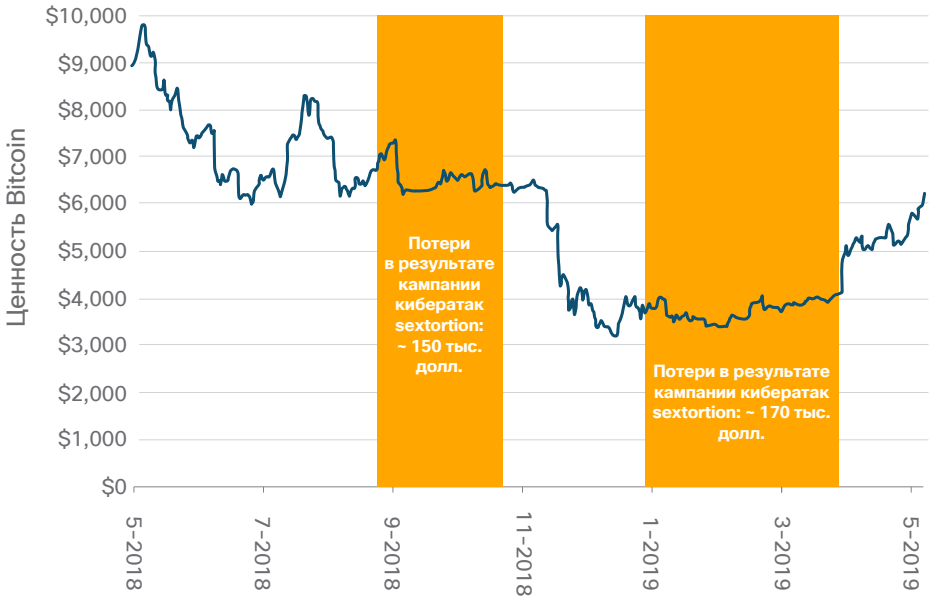
Цифровое вымогательство

В папку «Входящие» поступает электронное сообщение с темой **«ОТНЕСИТЕСЬ К ЭТОМУ ОЧЕНЬ СЕРЬЕЗНО».** Отправитель утверждает, что взломал веб-сайт для взрослых, куда якобы заходил получатель. У него есть видеозапись, на которой видно получателя и видео, которые он просматривал. Кроме того, по заверениям мошенника, он получил доступ ко всем контактам получателя и готов отправить имеющиеся записи, если получатель не выплатит сумму в сотни, а то и тысячи долларов в биткойнах.

Это пример цифрового вымогательства. Единственное, что отличает ту ситуацию от более традиционных случаев шантажа, – полностью сфабрикованные заявления мошенника. Хакеры на самом деле не взламывали веб-сайт, не делали записи и у них нет вашего списка контактов. Они лишь пытаются вас в этом убедить.

Подобные и многие другие примеры писем кибермошенников мы рассматриваем в нашей публикации в блоге «Угроза месяца» «Кошелек или жизнь: цифровое мошенничество».

Рис. 6 Сравнение стоимости биткойнов (долл. США) с прибылью от кампаний sextortion.



Источник: Cisco Talos

Это очень любопытный и прибыльный тип мошенничества: к концу 2018 года доходы киберпреступников достигли шестизначных цифр. Однако, согласно недавнему анализу, проведенному группой Cisco Talos, за период с января по март 2019 года, прибыль хакеров упала. Тем не менее, несмотря на заметный спад в этой сфере, сложно дать точную оценку взлетам и снижениям из-за особенностей стоимости биткойнов. В настоящее время стоимость биткойнов растет, но пока неясно, будет ли та же тенденция наблюдаться с цифровыми выплатами за вымогательство.

Мошеннические письма относительно доставки и счетов

Возможно, вы не можете вспомнить, как была приобретена подписка на это мобильное приложение. По крайней мере именно это указано в полученном электронном сообщении: вам предоставлена пожизненная подписка на киноклуб, к примеру. Подождите-ка, но ведь в счете в качестве местоположения указана Шри-Ланка, а вы не живёте в Шри-Ланке. «Должно быть, это ошибка», — вы говорите себе и быстренько открываете вложенный PDF-файл.

К сожалению, в этом файле находился эксплойт, который немедленно загрузил Emotet на ваше устройство. Схема мошенничества может меняться, однако обычно это связано с посылкой, которую получатель не заказывал, или счетом на товар, который получатель не приобретал, а иногда и с ежемесячной оплатой за подписку или услугу, о которой получатель даже не знает. Подобные злонамеренные действия могут привести к практически любому результату: от украденных банковских реквизитов до майнинга криптовалют.

Рис. 7 Мошенническое электронное письмо Emotet, которое якобы поступило из службы UPS.

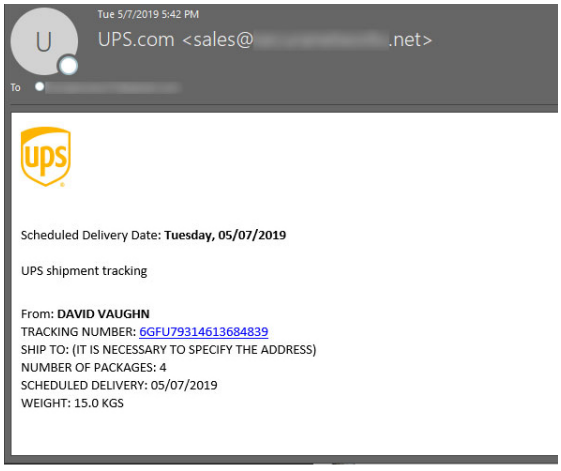


Рис. 8 Пример недавнего мошенничества с авансовым платежом.

Г-н Кристофер А. Рэй

CW

Директор Федерального бюро расследований (ФБР)

Кому: [redacted]

Ответить: [redacted]

Вниманию: получателя.

Вводная информация, пример которой показан далее, чрезвычайно важна в соответствии с правилами деловой переписки. Я г-н Кристофер А. Рэй, директор Федерального бюро расследований (ФБР). В этом официальном меморандуме мы хотим сообщить о противоправных действиях некоторых должностных лиц, работающих под руководством правительства Соединенных Штатов, которые попытались перенаправить ваши средства через резервный канал. Мы выяснили это сегодня через наших секретных агентов в дисциплинарном отделе Федерального бюро расследований (ФБР) после ареста подозреваемого.

Вышеупомянутый подозреваемый был задержан в международном аэропорту Далласа сегодня утром при попытке вывезти огромную сумму денег за пределы США. В соответствии с указом Соединенных Штатов о борьбе с отмыванием денег такая сумма не может вывозиться за пределы США, что рассматривается как попытка уголовного правонарушения и подлежит наказанию в соответствии с законом о борьбе с отмыванием денег от 1982 г. Соединенных Штатов Америки. Этот закон применяется в большинстве развитых стран с целью предотвращения террористических действий и отмывания денег.

На основании информации, собранной подразделением, мы обнаружили, что средства, о которых идет речь, принадлежат вам. Произошла их намеренная задержка, вызванная нарушениями ответственных должностных лиц, что полностью противоречит правилам любого платежного учреждения. В настоящее время эти средства находятся на ответственном хранении в банке-плательщике, и будут незамедлительно переведены вам при условии вашего честного сотрудничества с нами по этому вопросу. Нам необходима ваша поддержка на каждом этапе транзакции, чтобы убедиться в полном отсутствии мошеннических операций.

Сегодня, 9 мая 2019 г., мы поручили административному руководству банка-плательщика перевести вам указанные средства, поскольку у нас есть ценная информация/свидетельства подлинности, которые подтверждают, что вы действительно являетесь владельцем. Однако вы должны предоставить нам указанную ниже информацию (для официальной проверки).

1. Имя, отчество и фамилия.
2. Возраст.
3. Род занятий.
4. Семейное положение.
5. Прямой номер телефона/факса.
6. Адрес места проживания.

Мы ждем от вас немедленной отправки указанной информации, чтобы вы могли получить оплату от авторизованного банка-плательщика.

Официальная печать.

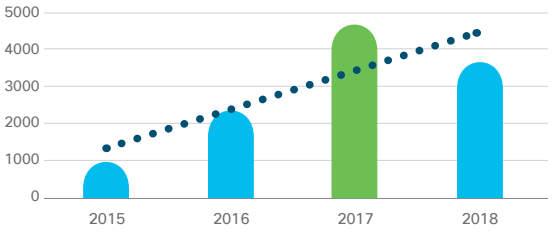
Г-н Кристофер А. Рэй
Директор Федерального бюро расследований (ФБР)

Мошенничество с авансовыми платежами

Не каждый день на ваш адрес приходит письмо из ФБР. А еще неожиданнее узнать, что вас ожидает перевод на сумму 10 500 000 долларов США! Все, что нужно сделать, — ответить на письмо, после чего будет получена инструкция по получению платежа.

Это классическая схема кибермошенничества с авансовыми платежами. Как следует из названия, мошенники запросят плату, прежде чем отправить обещанные деньги — деньги, которые никогда не появятся. Кроме того, это вариант одной из старых афер, которая претерпела различные видоизменения за прошедшие годы. В указанной схеме иностранный принц желал поделиться своими богатствами, чтобы люди с плохой кредитной историей могли получить заем. Тем не менее хакеры все еще используют подобные приемы, рассылая тысячи мошеннических писем каждый год, согласно данным Бюро по улучшению деловой практики (Better Business Bureau; BBB) США.

Рис. 9 Данные по авансовым мошенническим платежам по годам в соответствии с информацией BBB.
(Общая сумма авансовых платежей, категории мошеннических действий: нигерийские письма/обмен иностранной валюты, романтические письма, реструктуризация кредитов/списание долга, инвестиции и путешествия/каникулы.)



Источник: Better Business Bureau

Вредоносное ПО в электронных письмах

Значительная часть вредоносного ПО по-прежнему доставляется по электронной почте. Раньше такие программы сразу были видны: они поступали в виде вложений с расширением .exe. Но, когда пользователи поняли, что открывать исполняемые файлы небезопасно, хакеры изменили тактику.

В настоящее время вредоносное ПО лучше маскируется: оно приходит в виде менее подозрительных вложений (например, обычные бизнес-документы) или URL-адресов в теле письма. Все это вполне похоже на стандартную, ежедневную деловую переписку. Смысл в том, чтобы пройти традиционное сканирование электронной почты, которое вылавливает и помещает в карантин двоичные файлы и другие редко используемые вложения.

Чтобы лучше понять указанные принципы, достаточно взглянуть на помеченные вложения электронной почты, выявленные этом году (январь-апрель 2019 г.). Двоичные файлы составляют менее 2 % всех вредоносных вложений, включая не только exe-файлы, а все двоичные данные. Эти изменения произошли уже в прошлые годы, когда регулярно возникали исполняемые файлы, Java и Flash. На самом деле в последнее время Java и Flash перестали пользоваться популярностью, поэтому при добавлении их к двоичным файлам речь будет идти всего лишь о 1,99 % вложений.

Почти треть всех вредоносных вложений – это архивы (включая ZIP-файлы), на долю которых приходится четыре из десяти самых популярных форматов, которыми пользуются мошенники.

Таблица 1. Типы вредоносных вложений.

Тип	Процент
Офисные документы	42,8 %
Архив	31,2%
Сценарий	14,1 %
PDF	9,9 %
Двоичные файлы	1,77 %
Java	0,22 %
Flash	0,0003 %

Источник: Talos Intelligence

Наиболее распространенные типы вложений – самые обычные файлы, которыми ежедневно обмениваются офисные работники. Два из пяти вредоносных файлов – это документы Microsoft Office.

Так какие виды вложений чаще всего используют хакеры? Почти треть всех вложений – это архивы (включая ZIP-файлы), на долю которых приходится четыре из десяти самых популярных форматов мошеннических файлов. Скрипты (как, например, JS-файлы) составляют 14,1 %. По сравнению со статистикой, представленной в прошлом Ежегодном отчете по информационной безопасности за 2018 г. (ACR), когда количество используемых JS-файлов наряду с файлами XML и HTML составляло лишь 1 % от всех расширений вредоносных файлов, в настоящее время мы наблюдаем настоящий скачок популярности таких вложений.

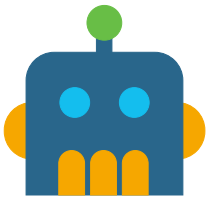
С момента выхода отчета за 2018 год частота использования этих вложений выросла на 5 процентных пунктов. Если добавить к этой подборке (которая составляет половину от всех вредоносных файлов) PDF-документы, мы получим наиболее распространенные вредоносные вложения, которые являются стандартными типами документов, повсеместно используемыми в работе.

Таблица 2. 10 основных вредоносных расширений в мошеннических электронных письмах.

Расширение	Процент
DOC	41,8 %
.zip	26,3 %
. js	14,0 %
PDF	9,9 %
RAR	3,9 %
.exe	1.7 %
.docx	0,8 %
ACE	0,5 %
GZ	0,5 %
XLSX	0,2 %

Источник: Talos Intelligence

Инфраструктура доставки электронной почты



Давайте отвлечемся от типов мошеннических электронных писем и полезной нагрузки и рассмотрим способы распространения таких сообщений. Для запуска спам-кампаний хакеры используют два основных метода: ботнеты и инструменты массовой рассылки электронной почты.

Ботнеты

Наибольшей популярностью на сегодняшний день пользуются, конечно, ботнеты. Ниже представлены некоторые из ключевых игроков в сфере рассылки спама через ботнетов.

Necurs

Ботнет Necurs появился в 2012 году и прославился распространением целого ряда угроз: начиная от троянов Zeus и заканчивая программами-вымогателями. В прошлом использование этого ботнета широко освещалось в прессе, но сейчас ситуация несколько изменилась, и его популярность снизилась. Тем не менее этот ботнет по-прежнему очень активен. По сути, ботнет Necurs является основным средством распространения различных видов мошеннических схем, включая цифровое вымогательство.

Для получения дополнительной информации о Necurs ознакомьтесь с анализом от компании Cisco Talos: «Многочисленные щупальца ботнета Necurs».

Emotet

Большая часть спама, которая отправляется через Emotet, посвящена вопросам получения товаров и счетам. Emotet – это модульное вредоносное ПО, которое включает в себя плагин Spambot. Мошенники используют Emotet в качестве канала для распространения других угроз. То есть модуль Spambot стремится заразить как можно больше систем и увеличить охват вредоносного канала распространения.

Поскольку Emotet крадет информцию из почты жертв, программа может отправлять мошеннические сообщения, которые очень похожи на настоящие и создают у получателей впечатление, что они просто продолжают начатую переписку. Emotet также получает доступ к учетным данным SMTP и использует серверы исходящей почты жертв для рассылки спама.

Для получения дополнительной информации о вредоносном ПО Emotet ознакомьтесь с нашим предыдущим отчетом из серии публикаций по информационной безопасности: «Защита от современных критически опасных угроз».

«Решение для защиты электронной почты Cisco Email Security сократило время, затрачиваемое на обнаружение и снижение количества спама, примерно на 80 %».

Жаклин Хеммерич, сотрудник по информационной безопасности, город Сарасота, Флорида

Gamut

Ботнет Gamut ориентирован на рассылку романтических и дружеских сообщений, в первую очередь, пользователям в указанном регионе. В рамках других кампаний мошенники отправляют письма с предложениями лекарственных препаратов или вакансий (см. Рис. 10).

Хакеры регистрируют множество доменов с относительно простой инфраструктурой, в рамках которой один домен включает в себя несколько субдоменов, часто под одним и тем же IP-адресом. Хотя компания Cisco не подтвердила, что предлагаемые услуги являются законными, в процессе регистрации, по-видимому, осуществляется попытка получения фишинговой персональной информации.

Рис. 10 Спам-письмо, отправленное ботнетом Gamut.

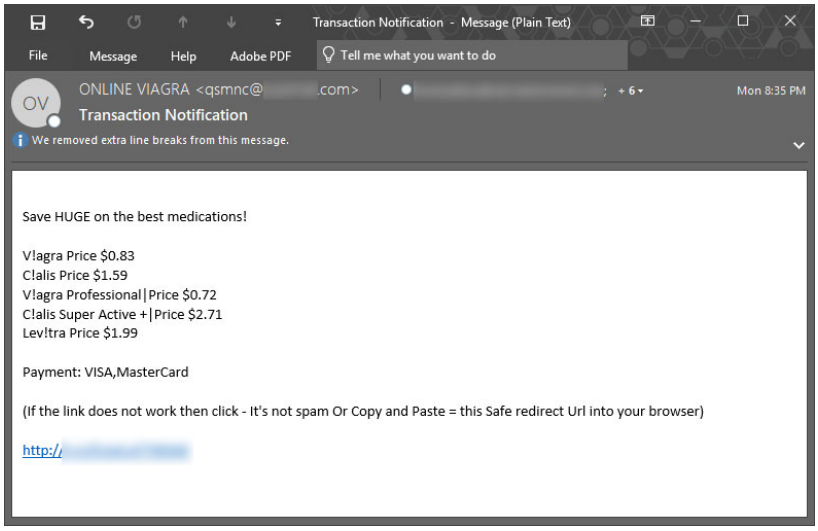
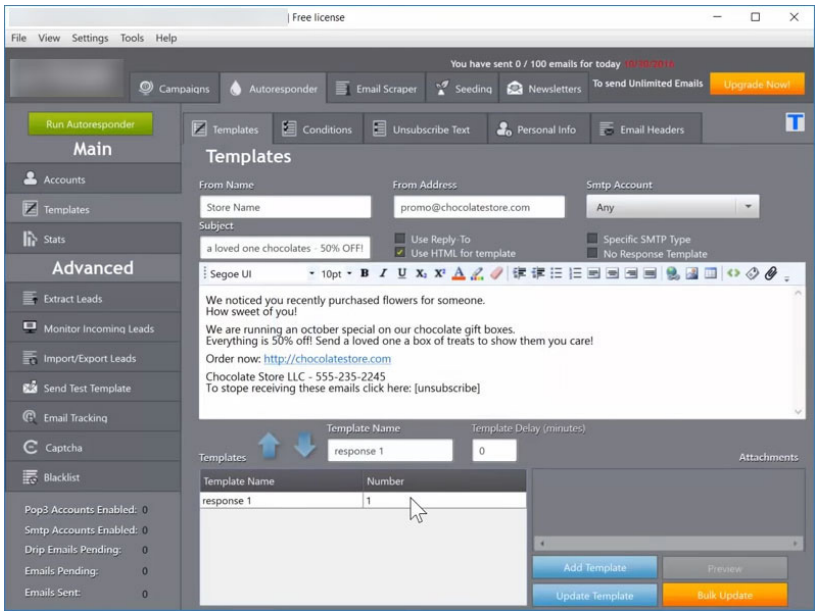


Рис. 11 Пример набора инструментов для рассылки спама.



Инструментальные средства массовой рассылки электронных писем

Многие мошенники используют альтернативный подход: покупают специальный инструментарий для рассылки большого количества электронных писем. Многие из этих инструментов могут использоваться вполне законным образом: например, для повышения узнаваемости собственного бренда (скажем, собственноручно изготовленных занавесок для душа) можно сделать массовую рассылку по своему списку адресов. Однако некоторые функции, включенные в такие наборы, как, например, механизм ротации IP-адресов отправителя или персональная перенастройка вложений для создания уникальных хеш-значений, вряд ли можно использовать в описанном сценарии.

В последнее время инженеры Cisco Talos обнаружили группы Facebook, в которых хакеры продавали средства массовой рассылки, а также обширные списки адресов электронной почты, которые, скорее всего, были получены в результате утечки данных. В подобных случаях покупатели явно используют эти инструменты в преступных целях.

Методы мошенничества

Если электронную почту можно назвать самой распространенной средой обмана, то самым популярным методом обмана является мошенничество (особенно со стороны организованной преступности).

Если электронную почту можно назвать самой распространенной средой обмана, то самым популярным методом обмана является мошенничество (особенно со стороны организованной преступности). Хакеры, замешанные в утечках деловой переписки, грабят компании на тысячи долларов. Цифровые вымогатели обманом заставляют пользователей перечислять им деньги в биткоинах. А в отношении мошенничества с авансовыми платежами все становится ясно из самого названия.

В принципе, ничего нового в этом нет. Электронная почта — лишь один из новейших инструментов, которые хакеры использовали для совершения мошеннических действий. Исторически сложилось так, что с появлением каждого нового поколения технологий преступники всегда стараются извлечь из этого максимум незаконной прибыли.

Согласно данным немецкой федеральной полиции (Bundeskriminalamt BKA) и ФБР, более 80 % всех зарегистрированных потерь в результате кибермошенничества приходится на расследование преступлений. Обратите особое внимание на слово «зарегистрированных», что подразумевает, что потери могут быть и нематериальными, т.е. такими, которые трудно точно оценить и зафиксировать То есть, имеющаяся статистика не слишком достоверна.

Следовательно, можно утверждать, что мошенничество является основным инструментом киберпреступности. Если оценить ущерб от двух методов мошенничества, отраженных в статистических данных ФБР, а именно утечка деловой переписки и взлом электронной почты, окажется, что общая сумма убытков за 2018 год составила 1 300 000 000 долл. США. Для сравнения: аналогичные потери в результате применения программ-вымогателей, которые являются достаточно распространенным и учитываемым методом кибермошенничества, составили 3 600 000 долл. США. И при этом все свидетельствует о том, что убытки, связанные с невыявленными киберпреступлениями, будут продолжать расти, поскольку уровень потерь в результате утечки деловой переписки и взлома электронной почты увеличился на 78 % лишь за период с 2016 по 2017 гг.

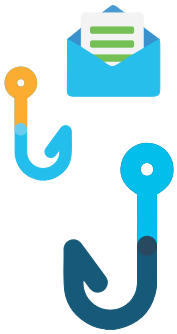
«Благодаря решению безопасности электронной почты Cisco Email Security мы практически забыли о проблемах с защитой электронных сообщений, что позволило нам сосредоточиться на других областях. Мимо него не проскользнет и муха! Мы приняли идеальное решение: теперь электронная почта надежно защищена!»

Стивен Вуджек, старший ИТ-архитектор, компания Technology Concepts & Design, Inc.

Для получения дополнительной информации о мошенничестве и убытках в результате киберпреступлений ознакомьтесь с серией блог-публикаций, посвященных киберпреступности и мошенничеству.

«Целостный подход к обеспечению безопасности – это не просто вопрос решения защиты или требование компании. Речь идет о работе с людьми, процессами и технологиями во всех сферах бизнеса. В компании Cisco мы ориентируемся на людей, на те обязанности, которые они выполняют; и наша задача – помочь им безопасно делать свою работу. Среди прочего мы даем нашим сотрудникам практические советы, как распознать подозрительные сообщения электронной почты, о которых необходимо немедленно сообщить, а не открывать их».

Стив Мартино, старший вице-президент и директор по информационной безопасности компании Cisco



Как защититься от атак на электронную почту

Явные признаки фишингового письма

Обычно письма, отправляемые киберпреступниками, содержат явные несоответствия, которые указывают на их мошенническую природу. Вот некоторые примеры: Подробные сведения о каждом из них см. на следующей странице.

Кому: you@youremail.com

1 От: Amazon Shipping <amz@123fnord.com>

Тема: Ваши недавний заказ

Здравствуйте!

2 Спасибо за ваш заказ. Ниже представлены подробные сведения.

Покупка: подписка на ежемесячную доставку еды для щенков Puppy Food™

Ежемесячная стоимость: 121 долл. США

Дата и время: 3 мая, 2019 г. 10:21

IP-адрес: 254.189.234.159.01

Страна приобретения: Гватемала

3 Если вы хотите отменить подписку, незамедлительно следуйте инструкциям в приложении или введите данные вашей кредитной карты далее:

4

5 http://badphishingsite.com/dontgothere.html

С уважением,

Отдел доставки Amazon

FILE

6 **dontopenthisis.bad**

Рис. 12 Предупреждение Microsoft Office о макросах в открытом документе.

1. **Кому: адрес** Совпадает ли адрес из поля «Кому» с адресом электронной почты?
2. **Многочисленные орфографические и грамматические ошибки или нечеткие логотипы.** Если письмо составлено с большим количеством ошибок, возможно, оно мошенническое.
3. **Срочность.** Если в письме от вас требуются незамедлительные срочные действия или в вас разжигают любопытство, будьте очень бдительны.
4. **Запрос на личную или конфиденциальную информацию.** Никогда не отвечайте на незапрошенное электронное письмо с просьбой предоставить личную, финансовую или конфиденциальную информацию.
5. **URL-адрес необычного вида.** Многие URL-адреса, используемые в фишинговых кампаниях, выглядят при более внимательном рассмотрении необычными. Открывать такие ссылки не следует. Если URL-адрес скрыт в текстовой ссылке, наведите на него указатель мыши и ознакомьтесь с информацией в нижней части браузера. При возникновении каких-либо сомнений, не открывайте ссылку.
6. **Нераспознаваемый тип файла.** В большинстве случаев в рамках деловой переписки по электронной почте отправляется лишь несколько стандартных типов файлов. Если файл выглядит необычно, не открывайте его.

Кроме того:

- **Не торопитесь.** В среднем человек тратит 8-10 секунд на знакомство с электронным письмом до выполнения каких-либо действий. Остановитесь и поищите признаки фишинговой атаки.
- **Если предложение слишком привлекательно, скорее всего, это обман.** В письме вам сулят миллионы долларов? Угрожают опозорить или нанести непоправимый вред? Большая вероятность, что послание сфабриковано от начала до конца.
- **Обратите особое внимание на предупреждения.** Если вы узнали отправителя и открыли вложение, обратите особое внимание на предупреждения баннеров о том, какие расширения или макросы необходимо включить (Рис. 12). Такие действия необходимы лишь в крайних случаях.

Стратегии предотвращения атак

Существует несколько подходов к снижению риска, связанного с угрозами электронной почты.

Регулярно проводите тренинги по распознаванию фишинговых атак. Ваши сотрудники — самая большая защита от угрозы фишинга, особенно учитывая персонализированный характер этого вида атак. Сотрудники, которые умеют мгновенно распознавать попытки фишинга, смогут устранить наиболее уязвимое место таких атак: человеческий фактор.

Чтобы повысить осведомленность, проводите регулярные корпоративные тренировки, которые позволят проверить и обучить пользователей. Моделируйте новейшие схемы мошенничества, чтобы сотрудники были в курсе возможных угроз. Компания Cisco предлагает выполнять такие тренировки ежемесячно, начиная с простых в обнаружении фишинговых кампаний и постепенно повышая сложность. Пользователи, которые не смогли распознать смоделированную фишинговую атаку, должны незамедлительно пройти соответствующее обучение (например, можно отправить проверочный «вредоносный» URL-адрес, который позволит получить дополнительную информацию о фишинге). Для наименее осторожных пользователей, чьи действия могут привести к значительному ущербу, необходимо проводить специальные антифишинговые тренировки.

Многофакторная аутентификация. В случае кражи учетных данных корпоративной электронной почты многофакторная проверка подлинности может помешать мошенникам получить доступ к учетной записи и нанести вред компании.

Красота многофакторной аутентификации заключается в ее простоте. Предположим, что кто-то смог получить доступ к вашим учетным данным или данным другого сотрудника из вашей сети и пытается войти в систему. При многофакторной проверке подлинности сообщение автоматически отправляется лицу, владеющему учетными данными, чтобы выяснить, кто именно предпринял попытку входа. В этом случае пользователь, который не в курсе попытки входа, отклоняет запрос. Это позволит успешно отразить атаку.

Регулярно обновляйте программное обеспечение. В некоторых случаях электронные сообщения с вредоносными ссылками могут привести пользователей на страницы с эксплойтами. Обновление браузеров и программного обеспечения, а также всех плагинов помогает снизить риски, связанные с такими атаками.

Никогда не отправляйте деньги незнакомцам. Это относится к мошенничеству с авансовыми платежами и утечке деловой переписки. В случае каких-либо подозрений просто не отвечайте на запрос. В частности для атак, связанных с утечкой деловой переписки, необходимо установить строгие правила, требующие авторизации банковского перевода со стороны высшего руководства компании, а также назначить представителя с правом второй подписи.

Внимательно изучайте запросы на вход в систему. Хакеры, нацеленные на кражу учетных данных, могут пойти на любые ухищрения, чтобы сделать свои страницы похожими на знакомые страницы входа. При получении запроса на вход в систему проверьте URL-адрес, чтобы убедиться, что он отправлен с официального сайта. Если появляется всплывающее окно, разверните его, чтобы убедиться, что виден полный URL-адрес (или по крайней мере полный домен).

Убедитесь, что электронное письмо выглядит достоверно. В случае цифрового вымогательства и мошенничества с авансовыми платежами хакеры часто придумывают сложнейшие истории, чтобы убедить вас в правдивости сообщения. Есть ли какой-либо смысл в описанной ситуации? Есть ли какие-либо пробелы в самой истории, с точки зрения технической стороны, финансовых процессов или других аспектов? Если да, то не доверяйте полученному письму.

Будьте готовы

Существует множество способов, с помощью которых мошенники пытаются обмануть пользователей или заставить их ответить на письмо, перейти по вредоносной ссылке или открыть вложение. Именно для этого следует использовать ПО обеспечения безопасности электронной почты, которое может захватить и изолировать вредоносные сообщения, а также отфильтровать спам.

К сожалению, мы обнаружили тревожную тенденцию: процент организаций, которые используют продукты защиты электронной почты, сокращается. Согласно нашему последнему опросу директоров по информационной безопасности, только 41 % опрошенных в настоящее время используют систему защиты электронной почты в рамках защиты от угроз, несмотря на тот факт, что организации подвергаются огромной опасности в результате атак подобного рода. Эта цифра приводится в сравнении с показателем 2014 г., когда 56 % организаций использовали системы защиты электронной почты.

Возможно, это вызвано несколькими причинами. Во-первых, произошел переход на облачные технологии. В недавнем исследовании, проведенном компанией ESG от имени компании Cisco, более 80 % респондентов сообщили, что их организация использует облачные сервисы электронной почты. По мере роста популярности облачной среды для размещения сервисов электронной почты специальные решения в этой области уже не кажутся столь необходимыми. Поэтому некоторые ИТ-специалисты считают, что смогут обойтись и без этого.

Однако базовые функции защиты, которые поддерживают многие облачные сервисы электронной почты, не могут сравниться с многоуровневыми решениями обеспечения безопасности. В том же опросе, проведенном ESG, 43 % респондентов выяснили, что им требуется дополнительная защита электронной почты после перехода на облачные технологии. В конце концов, ИТ-специалистам все еще необходимо иметь возможность устанавливать политики, отслеживать и контролировать процессы, использовать песочницы и внешние средства блокировки.

Еще одна проблема, с которой сталкиваются группы по обеспечению информационной безопасности в настоящее время, – это больший охват атак, что, естественно, приводит к увеличению количества областей, требующих защиты. При ограниченном бюджете таким группам приходится сокращать некоторые ресурсы, чтобы защитить большее количество уязвимостей.

С учетом того, что электронная почта является наиболее популярным направлением для атак, нельзя недооценивать важность ее защиты. При проведении любой оценки киберрисков важно определить наиболее важные точки входа, по отношению к которым должны быть развернуты максимальные меры защиты и применены системы управления рисками. Это позволит снизить отрицательные последствия для организации если произойдет проникновение. Затем следует выделить ресурсы, соизмеримые с уровнем возможных потерь.

Кроме того, по мнению Gartner, менеджеры по безопасности и рискам (SRM) должны применять трехсторонний подход к улучшению защиты от фишинговых атак:

1. Обновите защищенный шлюз электронной почты и другие средства контроля, чтобы улучшить защиту от фишинга.
2. Обеспечьте интеграцию сотрудников в решения и создайте возможности для обнаружения подозрительных атак и реагирования на них.
3. Совместно с руководителями бизнес-подразделений разрабатывайте стандартные операционные процедуры для обработки конфиденциальных данных и финансовых транзакций.

Как защитить электронную почту

Мы рассмотрели явные признаки фишинговой атаки на электронную почту и стратегии предотвращения атак. Теперь давайте оценим перспективы развития технологий обеспечения безопасности электронной почты в 2019 г.

Как и ранее, основная ставка в защите организаций от атак на электронную почту делается на многоуровневый подход к обеспечению безопасности. Существует несколько проверенных и протестированных функций защиты электронной почты, которые сохранили свою актуальность.

Например:

- Следует и дальше использовать решения защиты от спама, чтобы не допускать нежелательную электронную почту и вредоносный спам до входящих сообщений.
- Защита электронной почты от таких угроз, как вредоносное ПО, а также возможности блокировки URL-адресов используются для блокирования вредоносного ПО, защиты от фишинга, программ-вымогателей и майнинга криптовалют во вложениях, а также для борьбы с вредоносными ссылками в электронных письмах.
- Все новые файлы, приходящие на электронную почту, должны автоматически помещаться в песочницу в фоновом режиме. Это позволит быстро понять, являются ли они вредоносными.

Однако нельзя забывать о том, что ситуация с угрозами постоянно меняется, а мошенники все время ищут новые способы обмана.

В дополнение к уже проверенным и протестированным технологиям можно использовать следующие технологии обеспечения безопасности:

- Усовершенствованные средства защиты от фишинга с использованием машинного обучения для анализа и аутентификации идентификационных данных электронной почты и поведенческих отношений для блокировки сложных фишинговых атак.
- Теперь можно активировать решения защиты доменов DMARC, которые позволяют защитить бренд компании, не давая хакерам использовать легальный корпоративный домен в фишинговых кампаниях.
- Функция карантина применяется для хранения сообщений во время анализа вложений. Это позволяет удалить вредоносные вложения или все сообщение полностью.
- Функция устранения угрозы применяется, если вредоносный файл был обнаружен уже после доставки сообщения получателю. Это позволяет вернуться и поместить в карантин сообщение с вредоносным вложением в почтовом ящике.
- Внешние каналы угрозы в STIX в настоящее время успешно контролируются продуктами для обеспечения безопасности электронной почты. Это удобно в тех случаях, когда организация хочет использовать канал защиты от вертикальных угроз помимо встроенной аналитики угроз.
- Интеграция решений защиты электронной почты с более обширным портфелем решений безопасности также становится все более популярной. Это позволяет обнаружить сложное вредоносное ПО или сообщение, если они уже были доставлены определенным пользователям или получены на почту.

«Решение защиты корпоративной электронной почты Cisco занимает лидирующие позиции в обзоре Forrester Wave за 2019 г. Оно получило самые высокие оценки по следующим направлениям: поддерживаемые варианты развертывания, защита от атак и проверка подлинности электронной почты, производительность и работа (включая масштабируемость и надежность), а также технологическое превосходство».

Forrester Wave™. Защита корпоративной электронной почты, 2 квартал 2019 г.

О серии публикаций Cisco по кибербезопасности

За прошедшее десятилетие Cisco опубликовала множество материалов с исчерпывающей информацией по безопасности и анализу угроз для специалистов в данной области, которые интересуются состоянием глобальной кибербезопасности. В этих комплексных отчетах содержатся подробные сведения о сфере угроз и их влиянии на работу организации, а также рекомендации по защите от негативных последствий утечки данных.

В рамках нашего нового подхода к интеллектуальному лидерству Cisco Security публикует серию основанных на результатах исследований публикаций под заголовком «Серия публикаций Cisco по информационной безопасности». Мы расширили коллекцию публикаций, включив различные отчеты для специалистов по безопасности с разными интересами. Серия отчетов за 2019 г. хаактеризуется глубиной исследования и обширным опытом в сфере анализа угроз и инновационных достижений безопасности. Она включает в себя сравнительный анализ в области конфиденциальности данных, отчет об угрозах и опрос директоров по информационной безопасности. В течение года будут добавляться и другие публикации.

Для получения дополнительной информации и доступа ко всем отчетам и архивным копиям посетите страницу www.cisco.com/go/securityreports.

Штаб-квартира в Северной и Южной Америке
Cisco Systems, Inc.
Сан-Хосе, шт. Калифорния (США)

Штаб-квартира в Азиатско-Тихоокеанском регионе
Cisco Systems (USA), Pte. Ltd.
Сингапур

Штаб-квартира в Европе
Cisco Systems International BV Амстердам, Нидерланды

Компания Cisco насчитывает более 200 офисов и представительств по всему миру. Адреса, номера телефонов и факсов приведены на веб-сайте Cisco по адресу www.cisco.com/go/offices.

Опубликовано в июне 2019 г.

THRT_02_0519_r1