О вопросе профилактики преступлений, совершаемых с использованием глобальной компьютерной сети

В условиях становления общества информация обретает особую ценность, а вопросы безопасности становятся все более актуальными. Несмотря на преимущества и блага, которые создаются за счет цифровизации общества, в этом процессе есть и негативная сторона – неправомочное завладение злоумышленниками финансовыми активами предприятий или организаций с использованием так называемых BEC-атак (Business Email Compromise).

BEC - это атака, при которой злоумышленники начинают переписку с сотрудником предприятия или организации с целью завоевать его доверие и убедить выполнить действия, идущие во вред интересам субъекта хозяйствования или его клиентов. Зачастую используются взломанные аккаунты сотрудников или адреса, которые визуально похожи на официальные домены или адреса интернет сайтов как субъекта хозяйствования, так и его партнеров, но отличаются на несколько символов (к примеру: «kula@telliko.com», вместо «kula@teliko.com»). Заметить такое отличие очень сложно. Черты таких атак - высокий уровень подготовки, наличие знаний о структуре субъекта хозяйствования и ее процессах, использование приемов социальной инженерии.

Для проведения подобной атаки проводится подготовительная работа. В ходе которой злоумышленники при помощи фишинга похищают учетные данные рядового сотрудника, имея конечную цель - его более высокопоставленный коллега. Чаще всего атакующих интересуют деньги субъекта хозяйствавания, но бывает и так, что их цель - получить доступ к конфиденциальной информации, например, к клиентским базам или разработкам.

Справочно: для проведения BEC-атакн злоумышленники всегда тщательно собирают данные о жертве и позднее используют их, чтобы завоевать ее доверие. Некоторые такие атаки становятся возможными из-за того, что атакующие легко находят в открытом доступе имена и позиции сотрудников, их местоположение, даты отпусков, списки контактов и другие данные. Используется достаточно широкий арсенал технических приемов и методов социальной инженерии, чтобы войти в доверие к жертве и совершить мошеннические операции.

В июне 2021 года на электронный почтовый ящик сотрудника одного из предприятий г. Минска поступило электронное письмо от контрагента иностранного государства, содержащее требование оплатить доставку товара на новый расчетный счет. В последующем данный сотрудник подготовил дополнительное соглашение, содержащее измененные реквизиты счета для оплаты товара, а после его подписания руководством (без изучения и анализа) денежные средства в сумме более 200 ООО Евро зачислены на расчетный счет злоумышленника, открытый в иностранном банковском учреждении.

Также имели место случаи, когда к электронному письму, сообщающему об изменении реквизитов расчетного счета для оплаты, поступали вложения с приложением договора с печатью и подписью руководителя контрагента (зачастую могут содержать вредоносное программное обеспечение). В 2021 г. сотрудник одной из столичных организаций посредством переписки по электронной почте вел переговоры с представителем иностранной компании

(партнера) по вопросам оплаты за поставку оборудования. При этом представитель иностранного партнера направил электронное письмо, сообщив об изменении реквизитов расчетного счета для оплаты. В ходе переписки сотрудник белорусской организации, не убедившись в принадлежности нового счета фактическому поставщику, подготовил приложение к договору с измененными реквизитами для оплаты и направил его в адрес иностранной компании. В последующем от контрагента поступило отсканированное приложение к договору с печатью и подписью руководителя иностранной компании (поддельное), на основании которого произведен платеж на расчетный счет злоумышленника. Однако указанные денежные средства были возвращены банковским учреждением, поскольку наименование бенефициара не соответствовало действительности. После этого сотрудник сообщил об этом злоумышленнику, который, в свою очередь, отправил новый договор, содержащий иные реквизиты для оплаты, на который в последующем и были зачислены денежные средства в сумме более 10 ООО Евро.

Установлено, что сотрудник организации никакой переписки по факту заключения дополнительного соглашения с партнером не вел, а общался в сети Интернет с неизвестным пользователем, использующим адрес электронной почты, непринадлежащий иностранной компании, отличающийся на 1 букву в доменном имени. При этом имя пользователя электронного почтового ящика в обоих случаях в почтовом клиенте отображалось идентично (одинаково).

Совершению указанных преступлений способствовали компьютерная неграмотность сотрудников субъектов хозяйствования, отсутствие механизмов контроля и проверки электронной информации, поступающей от контрагентов, конкретных лиц, ответственных за соответствующие направления служебной деятельности, а также несоблюдение требований законодательства, в том числе, Директивы Президента от 11.03.2004 № 1 «О мерах по укреплению общественной безопасности и дисциплины», Закона от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» и Указа Президента от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации».

Анализ деятельности злоумышленников на территории Республики Беларусь показал, что они маскируются под бренды различных субъектов хозяйствования, их партнеров и контрагентов, используют массовые фишинговые рассылки для доставки популярных вредоносных программ под видом заказов, запросов данных о товарах и необходимости их оплаты и даже предложений помощи в борьбе с коронавирусом.

Обычно такие письма содержат призывы к активным действиям пользователя (представить адресату конфиденциальные данные, произвести оплату за услуги и товар, как правило, на новый расчетный счет по ранее заключенным договорам поставки).

Для рассылки фишинговых писем злоумышленники используют инструменты Gammadyne Mailer и Turbo-Mailer, платформу MailChimp, в том числе для того чтобы узнать, открывалось ли жертвой полученное письмо. Также применяются ранее взломанные электронные почтовые ящики для осуществления новых фишинговых атак, в том числе на партнеров конкретных субъектов хозяйствования.

По информации компании «Лаборатория Касперского» за май - август 2021 года значительно увеличилось число целевых BEC-атак на российские компании. Как следствие, в ближайшее время прогнозируется значительное увеличение указанных атак на субъекты хозяйствования Республики Беларусь.

Основная масса случаев хищения денежных средств субъектов хозяйствования в Республики

Беларусь связана с человеческими ошибками, поскольку совершение атаки происходит постепенно.

Злоумышленник сначала изучает предполагаемую жертву, собирает необходимые справочные данные. Затем переходит к завоеванию доверия, вынуждая жертву неосознанно нарушить правила безопасности: предоставить доступ к компьютерным сетям, хранилищам данных, раскрыть конфиденциальную информацию.

Справочно: социальная инженерия особенно опасна, поскольку она использует человеческие ошибки, а не уязвимость ПО, которые гораздо менее предсказуемы, чем угрозы вредоносных программ.

Основными способами совершения указанных преступлений являются.

1. Ложные ссылки в электронном ящике. Письма тщательно продумываются, оформляются по образцу той организации, с адреса которой якобы оно поступает. В письме злоумышленники представляются сотрудниками организаций, сообщают о рассылке спама с аккаунта, скрытых сообщениях в личном кабинете, о специальном суперпредложении - в ход идут любые уловки. Имеют место случаи, когда в письме требуется перейти по ссылке, в ходе перехода на которую на компьютер загружается вредоносный код, либо ссылка ведет на фишинговый сайт, неотличимый от оригинала, где необходимо ввести пароль, логин, телефон и другую информацию.
2. Фишинг-рассылки от гигантов Интернета, например, Google и Dropbox. В письме поступает просьба подтвердить электронный адрес, кликнув на фишинговую гиперссылку, и снова происходит утечка данных, но теперь не просто логина и пароля, а файлов, которые хранятся на облачных дисках: фотографии, документы, презентации.

Справочно: фишинг богат не только ложными ссылками, но и прикрепленными файлами к электронному письму, которые содержат вирусное ПО для заражения компьютера и получения доступа к информации с него.

3. Целенаправленная атака с целью получения личных данных. Злоумышленники ищут информацию на профилях в социальных сетях, где все стараются подробно написать о себе, дублируют ее в письме: когда обращаются по имени, с указанием должности и прочего, это вызывает доверие и желание дополнить свою информацию.
4. Атака на крупные организации с целью получения доступа ко всей информации, которая в дальнейшем позволит одобрять переводы на мошеннические счета, совершать иные действия.

Перенаправление на обманные сайты-двойники. Это самый опасный вид, потому что обнаружить его очень сложно. Компьютер заражается «трояном», который ждет своего часа. Когда пользователь заходит на страницы платежных систем или банков, выполняется подмена оригинального сайта на фишинговый, с помощью которого собираются данные. Происходит это из-за изменения кэша DNS.

6. Взлом по номеру телефона. Суть метода заключается в том, что злоумышленнику нужно знать номер телефона жертвы, указанный при регистрации электронного почтового ящика. При сбросе пароля почтовая служба требует ввести последние символы номера телефона. На этот номер отправляется SMS-сообщение с кодом подтверждения сброса пароля. Затем злоумышленник отправляет второе SMS-сообщение с неизвестного номера с требованием указать код из первого SMS-сообщения. Успех этого метода зависит от невнимательности жертвы.

С целью предотвращения мошеннических действий злоумышленников необходимо:

- постоянно обновлять браузеры, чтобы получать защиту от новых угроз;
- устанавливать почтовые спам-фильтры (умеют распознавать спам, в том числе графический, и блокируют появление нежелательной почты);
- использовать антивирусные программы;
- быть внимательными (бесплатный инструмент для защиты от злоумышленников);
- обновлять операционную систему. В обновлениях содержатся пакеты для исправления уязвимостей, через которые злоумышленники могут получить доступ к компьютеру;
- помнить, что банки не отправляют письма с просьбой повторно ввести логин или пароль;
- проверять адреса сайтов и электронных писем на правильность. Следует обращать внимание на URL-адрес ресурса, поскольку при фишинге адрес сайта отличается на 1-2 буквы, цифры или символа. Получая электронные письма, подлежит анализу не только содержимое, но и имя отправителя и электронный почтовый ящик, с которого оно поступило;
- проверять протокол. Https - это защищенное соединение, даже если злоумышленник перехватит данные, то получит бессмысленный набор символов, который не сможет расшифровать. Интернет-страницы с http должны насторожить в первую очередь;
- использовать несколько электронных почтовых ящиков (для личных и деловых переписок отдельно);
- проверять тщательно каждое письмо, особенно со ссылками и вложенными файлами. Если письмо поступило со знакомого почтового ящика, это еще не гарантия безопасности - почтовый ящик мог быть взломан;
- удалять письма с требованиями пин-кода или пароля. Это личная информация, и никто не имеет права ее просматривать;
- обращать внимание на отправителя письма и его содержимое. В письме может использоваться автоподстановка из почтового адреса, которая не всегда является именем;
- подключить двухфакторную аутентификацию для аккаунтов всех электронных почтовых ящиков и социальных сетей. Это спасет в том случае, если пароль стал известен злоумышленнику;
- регулярно, не реже 1 раза в неделю, проверять аккаунты всех электронных почтовых ящиков на предмет осуществления к ним несанкционированного доступа.

Также необходимо понимать, что злоумышленник не сможет достичь своей цели и похитить денежные средства, если атака будет своевременно выявлена и остановлена, а это возможно на любом ее этапе, при принятии соответствующих мер защиты, направленных на сохранение благосостояния субъекта хозяйствования, в том числе при соблюдении следующих правил:

1. никогда не доверять отправителю электронного письма.
2. всегда проверять основные идентификационные данные и служебные заголовки электронных писем (можно узнать и проанализировать IP-адрес отправителя письма и иную необходимую информацию), прежде чем ответить на письмо.
3. Не переходить по ссылкам и не открывать вложения, если отправитель письма не тот, кем он представился.
4. Тщательно проверять адрес сайта на наличие «опечаток» — это может быть копия официального ресурса, зарегистрированного специально для введения в заблуждение;
5. Перепроверять происхождение сайта, прежде чем ввести свои персональные данные (имя, адрес, реквизиты доступа, финансовые сведения).
6. В случае введения реквизитов доступа на подозрительном сайте немедленно сменить пароль.