ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ

Как не стать жертвой преступлений в социальных сетях

На сегодняшний день в молодёжной среде мы вряд ли найдем тех, кто не был бы зарегистрирован «ВКонтакте», «Фейсбуке», «Инстаграмм», каких-либо тематических форумах или иных площадках для виртуального общения. Однако некоторая неопытность, наивность и доверчивость порой приводят к негативным последствиям.

Социальные сети, форумы, блоги - это среда с практически мгновенной скоростью распространения информации и довольно сильным эффектом памяти (содержимое многих социальных ресурсов индексируется и доступно из поисковиков). Кроме того, растет индекс доверия к этим источникам информации.

Основная проблема социальных сетей - это доверие к тем, кто внесен в список «друзей». Бездумное предложение «дружбы» от неизвестных или малоизвестных людей может привести к драматическим последствиям. Очевидно, что уровень доверия к тем, кто находится в списке «друзей», по определению всегда будет выше, чем к случайным людям. С одной стороны, это хорошо, так как формирует лояльную аудиторию вокруг человека, но с другой стороны, открывает двери для злоумышленников.

«Дружеский» стиль общения, распространенный в социальных сетях, обманчив. Он может создать ложное ощущение, что вокруг только друзья и доброжелатели, с которыми можно делиться любой информацией.

В настоящее время актуальны следующие виды киберугроз, с которыми могут столкнуться физические лица:

Вишинг — это один из методов мошенничества с использованием социальной инженерии *(социальная инженерия — это совокупность способов психологического воздействия на поведение человека с целью получения выгоды),* который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль, под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию, или побуждают, убеждают вероятную жертву к совершению определенных действий со своей банковской платежной картой;

Фишинг — вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам, паролям, данным лицевых счетов и банковских карт с использованием поддельных интернет-ресурсов, контролируемых злоумышленниками, внешне схожих с настоящими (например,

поддельные страницы услуги «Интернет-банкинг» различных банков);

Заражение вирусным и вредоносным программным обеспечением - внедрение злоумышленниками специализированного программного обеспечения (далее по тексту ПО) в компьютерную систему пользователя для хищения его конфиденциальных данных, завладения ценной информацией, шифрования данных с требованием выкупа, использования компьютера или иного устройства в специализируемых сетях с целью совершения иных преступлений.

Структура преступных групп

В рамках проводимой работы было установлено, что рассматриваемый вид преступной деятельности осуществляется не одиночками, а как правило в составе групп, имеющих отдельные признаки организованных, члены которых обычно лично не знакомы друг с другом. (Такие группы имеют некоторое сходство с интернет-магазинами по торговле наркотиками и психотропами).

Разделение функций в таких группах может осуществляться по следующим категориям участников (названия подобраны условно):

1) Веб-разработчики. Обладая навыками программирования, создают основу фишинговых сайтов с заложенным механизмом динамического добавления в них веб-страниц, а также программы для автоматизации и интерактивности процесса создания таких веб-страниц. Веб-разработчики могут не являться непосредственными участниками преступных групп, а только инициативно или под заказ разрабатывать скрипты и продавать их иным заинтересованным лицам.

2) **Администраторы.** Осуществляют регистрацию доменных имен и подбор хостинга для новых сайтов; обеспечивают их оплату, загружают на хостинг файлы фишинговых сайтов, настройку сайтов их и взаимодействие с Telegram-ботами; контролируют функционирование указанных ресурсов; обеспечивают систему вывода денежных средств с карт-счетов граждан посредством создания (подыскания зарегистрированных на подставных лиц) карт-счетов, электронных кошельков, криптокошельков и управления данными средствами платежей; обеспечивают функционирования системы подсчета заработка и выплаты вознаграждения исполнителям.

3) **Операторы.** Осуществляют администрирование форумов, Telegram-чатов, Telegram-каналов, чат-ботов, ориентированных на данный способ хищения денежных средств; обеспечивают набор новых исполнителей; их обучение навыкам создания фишинговых вебстраниц, обмана потерпевших, обеспечения анонимности, вывода похищенных денежных средств; разрешают споры с исполнителями по поводу выплат.

4) Исполнители. Как правило, обладают низким уровнем образования и ориентированы на получение быстрых и легких заработков. Именно они подбирают объявление на «kufar.by», используя предоставленный им инструментарий, создают фишинговую веб-страницу; по абонентскому номеру автора объявления находят его в одном из мессенджеров; вступают в общение с потерпевшим под предлогом желания купить выставленный на продажу товар и убеждают в необходимости перехода на фишинговую веб-страницу и ввода необходимых данных. Посредством чат-бота они получают сведения о действиях потерпевшего на фишинговом сайте, сумме похищенных средств и своей доли в ней.

Содействовать совершению преступлений могут и иные лица, осуществляющие незаконную деятельность: осуществляющие регистрацию на подставных лиц абонентских номеров, электронных кошельков, банковских счетов (карт); оказывающие содействие в транзите похищаемых безналичных денежных средств через управляемые ими банковские счета и электронные кошельки; с использованием вредоносного ПО или социальной инженерии завладевающие аккаунтами пользователей «kufar.by», мессенджеров с целью их использовании в переписке с потерпевшими.

Порядок действий преступника

Здесь рассматривается порядок действий преступников в иерархии преступных групп:

1) на площадке объявлений «kufar.by» выбирает объявление и узнает абонентский номер разместившего его лица;

2) создает веб-страницу или несколько веб-страниц, визуально схожих с официальными сайтами известных сервисов (ЕРИП, Беларусбанк, Куфар, Белпочта и т.д.), содержащих формы ввода реквизитов, позволяющих осуществить доступ к банковскому счету, БПК потерпевших. Созданную фишинговую веб-страницу (вебстраницы) размещает на специально созданном сайте (опять же с использованием бота), буквосочетание доменного имени которого похоже на доменное имя соответствующего легального сервиса (например, kufar-pay.online, bel-post.biz, cdec.zyx, belarusbank-oplata.ru, erip-24.by);

4) используя абонентский номер автора объявления, устанавливает, не является ли он пользователем одного из мессенджеров: Viber, Telegram, WhatsApp;с аккаунта в мессенджере, связывается с потерпевшим и заявляет о намерении купить выставленный на продажу товар;

5) в ходе переписки или голосового общения с потерпевшим под

разными убедительными предлогами (например, заполнить форму для получения якобы уже перечисленных денег) предлагает перейти по гиперссылке, ведущей на фишинговую страницу и заполнить соответствующие данные;

6) потерпевший, перейдя по гиперссылке, на загрузившейся веб-странице (или на нескольких веб-страницах, загружаемых пошагово) вводит реквизиты банковской карты либо доступа к своему банковскому счету либо данные, предусмотренные межбанковской системой идентификации (МСИ). При этом формами ввода могут быть предусмотрены разные данные: номер карты, срок действия, CVC-код, номер абонентского номера, личный номер, пароль для входа в личный кабинет, получаемое sms-сообщение или код с карты кодов и т.д.;

7) вводимые потерпевшим данные отсылаются на сервер либо в мессенджер Telegram и обрабатываются специальным программным обеспечением, либо непосредственно преступником;

8) с использованием полученных данных осуществляется хищение денежных средств с карт-счета потерпевшего: либо путем несанкционированного доступа в кабинет удаленного управления банковским счетом (Интернет-банкинг, мобильный банкинг), либо посредством списания денежных средств с карт-счета через ввод на специальных онлайн-сервисах (например, perevod.mtbank.by), известных реквизитов банковской карты.

Сватинг - заведомо ложный вызов полиции, аварийно-спасательных служб, путем фальшивых сообщений о минировании, убийствах, захвате заложников и т.п.

Этот термин происходит от названия штурмовой группы «SWAT» (special weapons and tactics) - специализированной полицейской единицы в США и многих других странах. Если есть угроза, при которой необходимо вмешательство этой единицы, последствиями иногда становится эвакуация школ, деловых учреждений. В западных странах «сватинг» расценивается как разновидность терроризма, поскольку его используют для запугивания и создание риска получения телесных повреждений или даже смерти.

Сваттинг в первую очередь свойственен среде, где люди (чаще всего молодые) объединяются по каким-то целям. Например, в онлайн-играх. У них есть термин «вызвать милицию на дом» - когда для того, чтобы, к примеру, досадить обидчику, ему на дом вызывают правоохранителей, либо сообщают о заминировании какого-либо объекта.

В последние годы «сватинг» из забавы любителей онлайн-игр и хакеров превратился в массовое явление и большую проблему для правоохранительных органов различных стран. Жертвами хулиганов

становятся как обычные люди, так и знаменитости.

В Республике Беларусь за период 2020-2021 многократно возросло количество случаев поступления сообщений на электронную почту о ложном минировании объектов. Подобные «шалости» дорого обходятся государству, а для виновных чреваты весьма нешуточными последствиями.

Возраст привлечения к административной ответственности по статье 19.6 «Заведомо ложное сообщение» Кодекса Республики Беларусь об административных правонарушениях наступает с 16 лет. Санкция статьи предусматривает наложение штрафа в размере до 30 базовых величин.

Кроме того, предусмотрена уголовная ответственность (с 16 лет) предусмотренной статьей 340 «Заведомо ложное сообщение об опасности». Санкция статьи предусматривает наказание в виде лишения свободы на срок до 7 лет.