31 августа 2021

Боты наступают: как защититься от ИИ-обманщиков в соцсетях

Технологии искусственного интеллекта (ИИ), которые помогают бизнесу упростить взаимодействие с клиентами в Сети, все чаще применяют в мошеннических целях. Растет число плохих ботов, которые вводят пользователей в заблуждение. По количеству фейковых инструментов в интернет-среде лидируют США. По мнению аналитиков, во время COVID-19 виртуальные помощники спровоцировали своеобразную интернет-пандемию.

ФАЛЬШИВАЯ АКТИВНОСТЬ «ВКОНТАКТЕ»

В августе 2021 года Роскачество обнаружило новую схему мошенничества с рекламой игровых ботов во «ВКонтакте». В сообществах соцсети, где зарегистрированы большей частью несовершеннолетние, распространялись якобы реальные диалоги пользователей о быстрых заработках. Игрокам предлагалось добывать виртуальные «алмазы», которые можно обменивать на настоящие деньги.

Далее бот требовал пригласить друзей или оплатить VIP-доступ, а для вывода заработанных средств – внести комиссию за конвертацию. После совершения операции аккаунт жертвы блокировался и деньги пропадали.

Название ботов может меняться, но самый актуальный во «ВКонтакте» – GameBot, уточнили в Роскачестве. В ведомстве подчеркнули, что большинство школьников не читает пользовательского соглашения в игровых сервисах, где разработчики зачастую снимают с себя ответственность за выплату вознаграждения

В документе GameBot, в частности, говорится:

- сервис может, но не обязуется производить вывод средств на электронные счета самым активным юзерам;
- сумма вознаграждения определяется владельцем сервиса исходя из активности пользователя, величины его добровольных пожертвований, а также из своего личного субъективно-оценочного мнения.

Роскачество направило информацию по факту выявления злоумышленников в Роскомнадзор и администрацию социальной сети.

Описанная схема, как и многие другие, по сути, сводится к использованию мошенниками приемов социальной инженерии, отметил в беседе с RSpectr ведущий контент-аналитик «Лаборатории Касперского» Михаил Сытник. По его словам, в результате подобных действий хакеров человек чаще всего рискует определенной суммой или сохранностью своих данных.

Как сообщили RSpectr в пресс-службе «ВКонтакте», по факту проводится проверка, а указанное сообщество заблокировано. В компании подчеркнули, что серьезно относятся к задаче ограждения пользователей от злоумышленников и стараются обеспечить предельно справедливый подход к модерации контента.

«ВКонтакте», пресс-служба:

– Мы уже много лет используем максимально эффективный комплекс мер – гибридный метод модерации. Не только оперативно реагируем на обращения пользователей, общественных организаций и официальные запросы госрегуляторов, но и проводим проактивный внутренний мониторинг. Наша команда тщательно проверяет каждую жалобу и удаляет материалы, которые нарушают правила «ВКонтакте» или требования законодательства, а также блокирует сообщества и профили злоумышленников.

Адаптация под мошенничества

Эксперт по информационной безопасности, CEO компании AtreIdea Сергей Белов в разговоре с RSpectr констатировал, что использование ботов в мессенджерах, социальных сетях и прочих ресурсах – это удобный инструмент для оказания поддержки клиентам в любых областях, где требуется хотя бы минимальное интерактивное взаимодействие по четким паттернам.

66% запросов в финансовой сфере, ритейле и телекоме уже решают роботы, следует из исследования Markswebb.

Однако, говорит эксперт, использование автоматизированных средств в преступной деятельности –

ИСПОЛЬЗОВАНИЕ АВТОМАТИЗИРОВАННЫХ СРЕДСТВ В ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ – ЭТО ТРЕНД, КОТОРЫЙ НАБИРАЕТ ОБОРОТЫ ПОСЛЕДНИЕ ДЕСЯТЬ ЛЕТ

Сергей Белов, AtreIdea:

– Как только бизнес начинает применять какие-либо технологии, призванные упростить взаимодействие с клиентом, мошенники адаптируют наиболее популярные из них для своих целей.

Например, в конце ноября 2020 года пользователи по всему миру столкнулись с тем, что анонсированные новые поколения игровых консолей PlayStation 5 от Sony и Xbox Series X от Microsoft невозможно приобрести. Так называемые гринч-боты* – виртуальные перекупщики – заранее забронировали товар, чтобы потом продать его с наценкой. Подобный софт мошенники постоянно применяют в периоды крупных распродаж.

В Лаборатории исследования угроз Imperva посчитали, что осенью в преддверии «черной пятницы» количество плохого бот-трафика на розничные веб-сайты увеличилось на 788 процентов.

Боты лишь предлог для обмана доверчивых пользователей, не стоит демонизировать саму технологию интернет-помощников, говорит инженер по безопасности хостинг-провайдера и регистратора доменов REG.RU Артем Мышенков. В беседе с RSpectr он рассказал, что, помимо обнаруженной Роскачеством мошеннической уловки с выращиванием «алмазов», на просторах интернета существует огромное количество преступных схем.

Артем Мышенков, REG.RU:

– Это фейковые инвестиции в криптовалюты, торговля опционами, продажа прогнозов на ставки на спорт, большой «выигрыш» в лотерею. Даже выплаты от американского правительства и заработок на поиске внеземных цивилизаций. Фантазия мошенников безгранична.

В июле 2021 года Сбербанк раскрыл схему с участием ботов по рассылке пользователям мессенджеров писем о конкурсах с денежными призами в иностранной валюте. Чтобы конвертировать выигрыш в рубли, победитель должен был заплатить комиссию, а для этого сообщить мнимому онлайн-собеседнику данные банковской карты.

В апреле 2021 года число фейковых постов в Facebook, предлагающих установить «последнее обновление» мессенджера, достигло 5,7 тысячи. В сообщении содержалась короткая ссылка, перейдя по которой пользователи попадали на фишинговый сайт с фиктивной формой для авторизации. В итоге жертва рисковала потерять доступ к своему аккаунту, а также персональные данные (ПД), которые злоумышленники используют для вымогательства и рассылки спама, продают в даркнете.

Участились случаи мошенничества с помощью голосовых ботов: они запрашивают ПД, которые мошенники используют для оформления кредитов

На эту тенденцию в разговоре с RSpectr указал **менеджер по работе с корпоративными клиентами ГК «КОРУС Консалтинг» Тимофей Зайцев**.

Директор по маркетингу компании Epicstars (российская b2b-платформа для работы с блогерами) Лейла Салиева рассказала RSpectr, что если взять большое количество ботов, то можно искусственно вывести в тренды заказные темы или хэштеги.

Лейла Салиева, Epicstars:

– Речь идет как о всплеске упоминания какого-то товара, то есть, по сути, о рекламе, где боты выступают в роли блогеров, так и о более серьезных вещах – вовлечение в мошеннические схемы, травля, дезинформация на глобальные темы.

Методы киберпреступников почти не отличаются от тех, что были ранее, просто работают с ними ненастоящие люди – бот-аккаунты, согласилась с мнением собеседников RSpectr Л.Салиева.

В конце августа Общество защиты интернета сообщило об исследовании рынка продажи ботов. Выяснилось, что раскрутить паблик в соцсетях до нескольких десятков тысяч подписчиков может человек с любым уровнем технической грамотности за небольшие деньги.

РОСТ И ПРОНИКНОВЕНИЕ

Основная опасность фейкового чат-бота состоит в том, что часто его сложно отличить от настоящего, рассказал Т.Зайцев. По его словам, злоумышленники делают ссылку на виртуального собеседника максимально похожей на реальную, ставят подходящие аватарки, и его легко принять за представителей конкретной компании. Другая опасность, по мнению

эксперта, кроется в использовании игровых механик, которые заставляют пользователя проще идти на контакт.

Тимофей Зайцев, ГК «КОРУС Консалтинг»:

– Боты полностью автоматизированы, и мошенникам не приходится тратить время на общение с пользователем. Это позволяет прикладывать меньше усилий для привлечения новых жертв. Ими часто становятся дети и подростки, которые не знакомы с распространенными схемами обмана и не могут критически оценить ситуацию.

Активность ботов резко возросла во время пандемии, в частности, в Twitter. По оценкам экспертов Carnegie Mellon University, они могут составлять от 45 до 60% аккаунтов, в которых обсуждается COVID-19. Такой вывод ученые сделали на основе изучения более 200 млн твитов. В ходе анализа они также выявили больше 100 типов неточных историй о коронавирусе и обнаружили, что боты составляли 82% из 50 лучших и 62% из 1 тыс. влиятельных ретвитеров. Imperva зафиксировала рост плохого трафика на 372% на веб-сайтах здравоохранения по всему миру с сентября 2020 года.

Эта лаборатория угроз также посчитала проникновение фейковых программ в мире – плохих и хороших: 40,8% всех запросов в Сети в прошлом году исходило не от людей, полагают аналитики. Настоящие виртуальные помощники аккумулировали 15,2% трафика, фейковые – 25,6 процента. В целом пользовательский поиск от реальных аккаунтов уменьшился в 2020 году на 5,7 процента.

КАК РАСПОЗНАТЬ ЛОЖНОГО АССИСТЕНТА?

Ботов можно вычислить, внимательно изучив профиль.

Лейла Салиева, Epicstars:

– Обычно там мало личной информации, недавняя дата создания, аватар – чаще картинка, а не фото, и ненормально повышенная активность в какой-то из соцсетей на одну тему: будь то политика, компьютерные игры, некое инвестирование и так далее.

«Лаборатория Касперского» рекомендует пользователям прежде всего критически относиться ко всему, что предлагают в интернете, говорит М.Сытник. Особенно если речь идет о крайне щедрых предложениях или действиях, которые нужно выполнить незамедлительно.

Михаил Сытник, «Лаборатория Касперского»:

– Не стоит переходить по ссылкам из подозрительных писем, сообщений в мессенджерах и социальных сетей, даже если их прислали знакомые. К тому же нелишним будет использовать надежное защитное решение, которое не даст перейти на фишинговый или скам-сайт.

Эксперты рекомендуют сервисы комплексной аналитики показателей на коммуникационных платформах, например, Live Dune, он работает на всех онлайн-площадках.

Стоит отметить созданный в августе 2021 года метод по выявлению вредоносных ботов в соцсетях с помощью искусственного интеллекта. Решение придумано в Санкт-Петербургском федеральном

исследовательском центре РАН. Разработка поможет не только определять ботов, но и оценивать их качество, примерно рассчитывать стоимость атаки и понимать ее специфику.

Артем Мышенков, REG.RU:

– Целью мошенников могут быть не только сами денежные средства, но и данные банковских карт и пароли. Поэтому нужно обращать внимание на то, на каком сайте вы вводите ваши данные, смотреть на доменное имя ресурса – у поддельных веб-страниц оно может отличаться всего на одну букву от оригинала. Также стоит проверить безопасность соединения: подключен ли протокол SSL (Secure Sockets Layer), который обеспечивает безопасную передачу данных между браузером и сайтом.

Тимофей Зайцев, ГК «КОРУС Консалтинг»:

– Проверяйте ссылки на ботов на официальном сайте и не сообщайте им свои ПД. Предупредите пожилых родственников и детей о схемах мошенничества в интернете. Если вы все-таки попали на уловки мошенника – немедленно обратитесь в правоохранительные органы и в организацию, от имени которой осуществлялось мошенничество. В некоторых случаях компания может приостановить транзакцию и вернуть деньги.

Сергей Белов, AtreIdea:

– Основной защитой является активная работа платформ по выявлению и пресечению подобных активностей (автоматическим образом и в ответ на жалобы пользователей), а также активное обучение цифровой гигиене еще в школах. Подобные мероприятия уже проводятся в ряде школ, зачастую по

инициативе коммерческих организаций.

Нужно запомнить простую истину: никто в интернете не даст вам деньги просто так и не поделится секретным способом заработка, который он мог бы использовать сам, напоминают эксперты.

*Гринч-боты – названы так по имени сказочного персонажа книги Доктора Сьюза «Как Гринч Рождество украл».

Источник: RSpectr.com