В киберпространстве, на большой дороге

Интернет – самая большая, сложная и надежная машина, созданная человечеством. Она возникла совсем недавно, удваивается в размерах каждые несколько лет и быстро эволюционирует. Мы не представляем, какой она станет даже через десятилетие и как изменит мир. Сеть подарила нам доступ ко всей мировой культуре и любой информации, небывалые возможности для работы, общения и творчества. Но возникли и новые опасности. О некоторых из них рассказывают эксперты белорусского представительства Kaspersky.

Стилер *(от английского to steal – воровать)* – определенный класс троянов (малвари, вирусов – как хотите), функционал которых полностью состоит из кражи сохраненных в системе паролей и отправка их «автору»). После того как вы установили мод со стилером при входе в игру, вы введете пароль и он успешно перейдет в руки вору.

В 2022 году зафиксировано почти 90 тысяч атак с использованием троянцев-стилеров в Беларуси*. Это вредоносные программы, которые крадут логины и пароли от аккаунтов в различных сервисах. В их числе банковские, игровые аккаунты, учетные записи в мессенджерах, социальных сетях, сохраненные пароли в программах и браузерах. Стилеры ищут необходимую информацию в системных файлах, которые хранят конфиденциальные данные, или в реестре. Затем отсылают ее злоумышленникам. С такой угрозой сталкиваются в том числе авторы Telegram-каналов и блогеры.

Один из самых распространенных троянцев для кражи паролей и учетных данных из браузеров и десктоп-мессенджеров – RedLine. В 2022 году в Беларуси зафиксировано более 1,5 тысяч атак* с использованием этого вредоносного ПО. Он умеет красть данные от учетной записи в Telegram, токены Discord, данные для входа в криптокошельки, а также сохраненные пароли и файлы cookie из браузеров. Кроме того, стилер может скачивать и запускать сторонние программы, выполнять команды в cmd.exe (файл командной строки Windows) и открывать ссылки в браузере. Распространяется он разными способами, в том числе при помощи вредоносных спам-рассылок и сторонних загрузчиков. RedLine

* Данные на основе анонимизированной статистики срабатывания решений Kaspersky за январь – сентябрь 2022 г.

продается в даркнете и стоит несколько сотен долларов США.

– Мы видим, что стилеры по-прежнему актуальная угроза, – говорит Олег Купреев, эксперт по кибербезопасности Kaspersky. – Пользователям, особенно владельцам популярных каналов в мессенджерах и соцсетях, блогерам, стоит быть внимательными. Важно критически относиться к крайне щедрым или пугающим сообщениям и проверять с помощью защитных решений файлы, которые приходят от незнакомых контактов или вызывают подозрение. Так, например, нередки случаи, когда злоумышленники распространяют зловреды под видом рекламных предложений. Для защиты аккаунтов мы рекомендуем использовать двухфакторную аутентификацию, а также периодически проверять список активных сеансов. Если среди устройств появится такое, с которого человек не заходил в аккаунт, следует завершить сеанс и сменить пароль. Важно также пользоваться защитным решением – оно убережет от загрузки и установки вредоносного ПО и не даст перейти по фишинговой ссылке.

Нередко преступники прибегают к искусственным проблемам с Windows и обманом вынуждают русскоязычных пользователей перезвонить им. В сентябре эксперты Kaspersky зафиксировали почти 600 000 попыток перехода пользователей по всему миру на фишинговые ресурсы, эксплуатирующие тему продуктов Microsoft**. На одних сайтах предлагали скачать операционную систему Windows 10 или Windows 11. На других злоумышленники пытались выманить данные для входа в учетную запись (адрес электронной почты и пароль) в сервисах Microsoft, в том числе Outlook. Если человек вводил эти данные на фальшивом ресурсе, они доставались злоумышленникам.

Как уточняют эксперты, мошенническая схема нацелена на русскоязычную аудиторию. Поэтому не исключается, что с действиями злоумышленников могут столкнуться пользователи в разных странах СНГ.

Кибермошенники также используют вишинг – голосовой фишинг, то есть пытаются побудить человека позвонить им по указанному номеру. Если жертва попадается на крючок и перезванивает, ее начинают «обрабатывать». Обычно мошенники пытаются выманить конфиденциальные данные либо убедить перевести деньги на указанные реквизиты или установить потенциально опасное ПО. Одна из схем выглядела так: человек заходил на сомнительный ресурс или его перенаправляли на него из спам-письма, внезапно на экране появлялся баннер с сообщением: «Windows заблокирован из-за подозрительной активности». Якобы на устройстве пользователя была обнаружена угроза – шпионский троянец. В том же сообщении человека просили немедленно связаться с технической поддержкой по указанному телефону, чтобы избежать «полной неисправности компьютера». В реальности злоумышленники просто показывали баннер в полноэкранном режиме. Так они пытались убедить человека, что у него действительно заблокирован компьютер.

По словам представителя Kaspersky в Беларуси Дмитрия Кудревича, названия известных брендов часто используются злоумышленниками, которые всеми возможными способами стремятся усыпить бдительность и выманить деньги пользователей. Поэтому важно критически оценивать любую информацию в Сети. Особенно внимательными следует быть в том случае, если происходит что-то нетипичное: например, кто-то пытается привлечь внимание слишком заманчивым онлайн-предложением или запугивает и требует немедленно совершить какое-либо действие – перейти по ссылке, ввести свои данные или перезвонить по телефону.

– Важно соблюдать базовые правила безопасности в Сети и использовать надежное защитное решение, которое предотвратит попытку перейти на фишинговый или скам-сайт, – объясняет эксперт.

** Анонимизированные данные на основе срабатывания решений Kaspersky за сентябрь 2022 года.