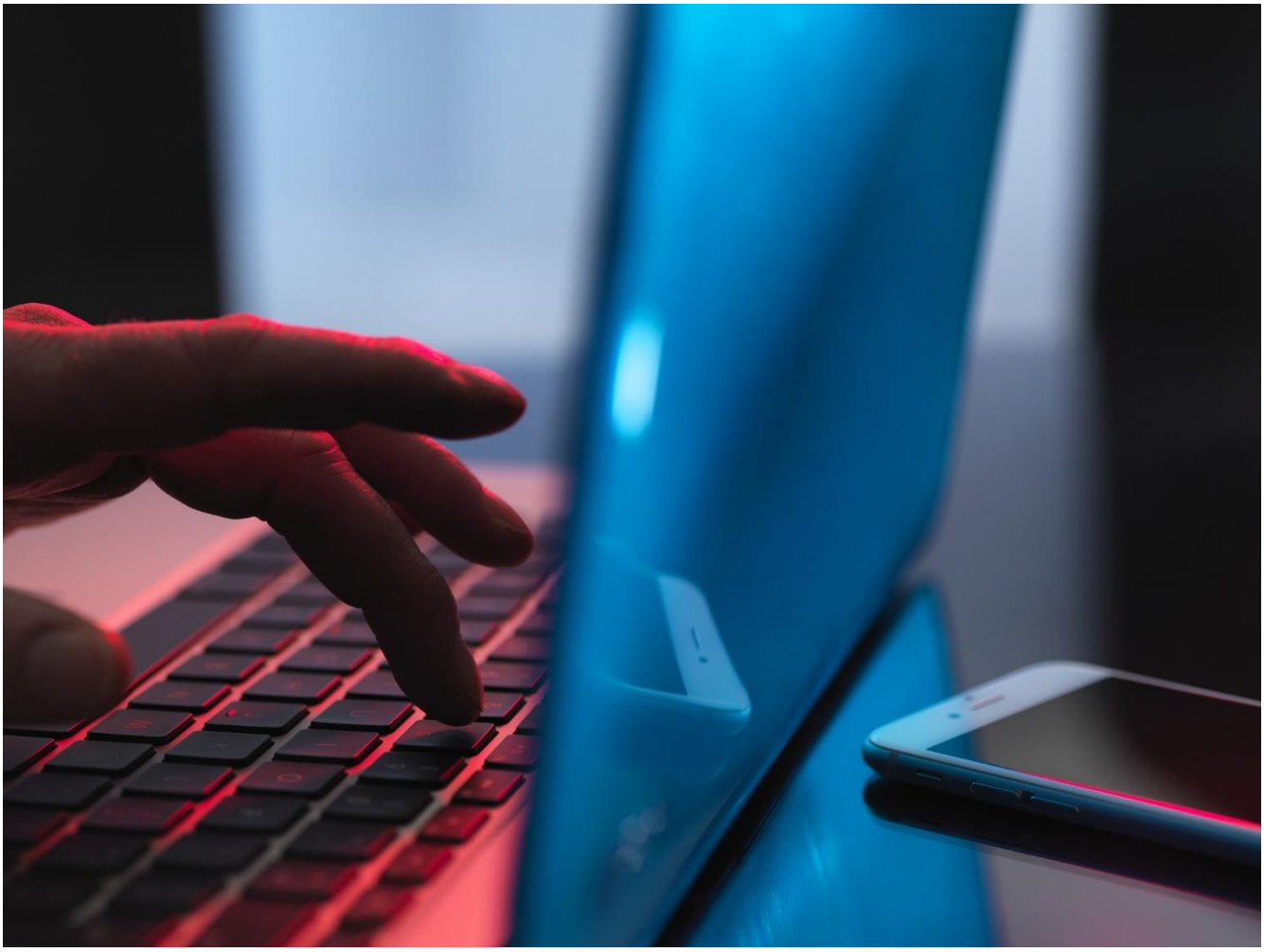


Узбекистан: новые случаи фишинга и кибератак на правозащитников

Amnesty International
EUR 62/1971/2020
12 March 2020

AMNESTY INTERNATIONAL

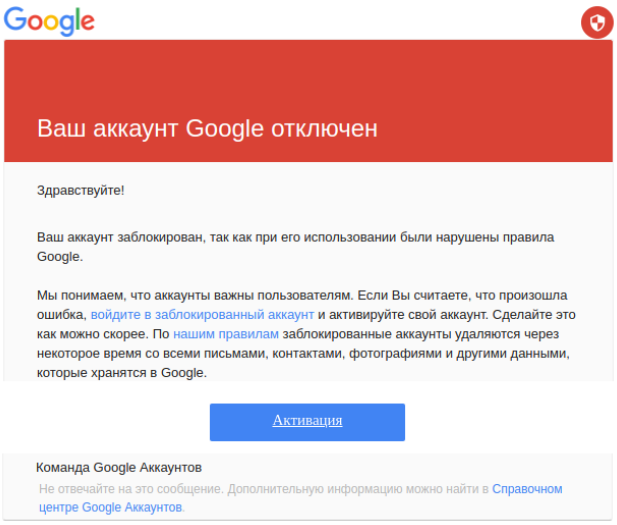
В ходе недавнего исследования Amnesty International стало известно о новой волне кибератак на правозащитников и журналистов из Узбекистана, в том числе о рассылке фишинговых сообщений и программ-шпионов для устройств на Windows и Android ОС.

В опубликованном сегодня докладе сообщается о кампании по рассылке вредоносных электронных сообщений со ссылками на фальшивые сайты, а также программ-шпионов для устройств на Windows и Android ОС, встроенных в легальное ПО. Пик кампании пришёлся на период с мая по август 2019 года, целью являлись правозащитники из Узбекистана. Личность того или тех, кто стоял за организацией кибератак, осталась неизвестной, однако выявленные в последнее время случаи можно считать частью масштабной кампании кибератак на активистов и журналистов из Узбекистана, о которой Amnesty International сообщала в 2017 году.

Новые методы фишинга

Что такое фишинг
Фишинг конфиденциальных данных пользователей (фишинг с целью кражи пароля) – это создание сайтов, имитирующих окно входа в учётную запись тех или иных интернет-сервисов, например Gmail или Facebook, с целью заманить пользователя на вредоносную страницу, где пользователь вводит имя и пароль, передавая тем самым злоумышленникам доступ к конфиденциальным данным.

В ходе расследования организация установила, что злоумышленник рассылал фишинговые сообщения в форме фальшивых уведомлений от Google и Mail.ru со ссылками на сайты, имитирующими настоящие сайты интернет-сервисов. Amnesty International выявила лиц, против которых была направлена кибератака, хотя и не всех, и подтвердила, что среди них были правозащитники и журналисты из Узбекистана.



Скриншот фишингового сообщения, отправленного злоумышленниками

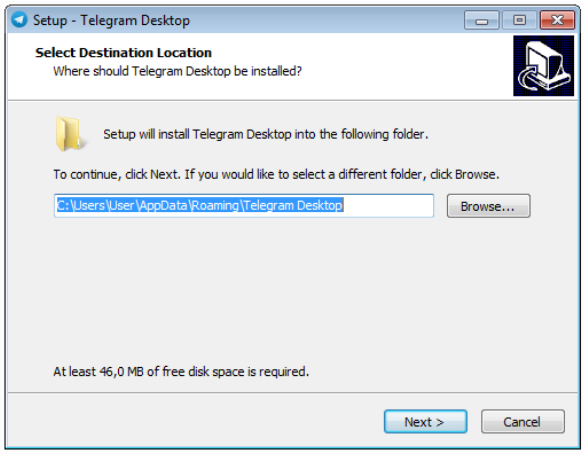
До настоящего времени злоумышленники создавали клоны страниц легальных сайтов, заманивающих пользователей, и так крали конфиденциальные данные. Теперь, как утверждается в докладе, злоумышленники начали пользоваться более продвинутой технологией под названием «перехват сеанса», в результате которого осуществляется подмена настоящего сайта фишинговым, для того чтобы максимально обойти двухфакторную аутентификацию.

Что такое двухфакторная аутентификация
Двухфакторная аутентификация – аутентификация, предусматривающая ещё один этап в дополнение к введению пароля. Часто таким вторым фактором аутентификации служит СМС-код, временный код, генерируемый приложением смартфона (например FreeOTP или Google Authenticator) либо код, генерируемый аппаратным ключом безопасности (таким как Yubikey или Solo Key).

По наблюдениям организации, злоумышленники впервые прибегли к данному методу, подтверждая значение рекомендаций, представленных Amnesty International в недавних докладах, в том числе в предыдущем докладе под названием When Best Practice Isn't Good Enough («Передовых методов может оказаться недостаточно»), опубликованном в декабре 2018 года. В докладе организация рекомендовала правозащитникам усилить меры защиты учётных записей, например с помощью ключей безопасности.

Программы-шпионы для устройств на Android и Windows ОС

В ходе расследования организация выяснила, что злоумышленники разработали программы-шпионы для устройств, работающих на Windows и Android ОС. Программы-шпионы для устройств на Windows ОС скрывались в установщике мессенджера Telegram для настольных ПК и в установщике Adobe Flash Player и были модифицированы так, чтобы одновременно с легальным ПО устанавливать программы-шпионы. После установки такое шпионское ПО использовалось для кражи паролей, записывало нажатие клавиш и регулярно делало скриншоты экрана.



Скриншот установщика Telegram Desktop, модифицированного для установки шпионского ПО

Шпионское ПО для устройств на Android ОС было разработано на базе приложения Droid-Watcher с открытым исходным кодом, поддержку которого разработчик прекратил ещё несколько лет назад. С помощью шпионского ПО злоумышленник мог удалённо следить за взломанным телефоном на Android ОС, записывать разговоры, СМС и переписку из чатов таких приложений, как «ВКонтакте», Telegram и WhatsApp. Помимо прочего, злоумышленник мог отслеживать точную геолокацию такого телефона в реальном времени.

Средства кибербезопасности для правозащитников

Правозащитников всё чаще подстерегает опасность в интернете, что подтверждается в докладе. Причём предпочтительным методом кибернаступления является фишинг конфиденциальных данных и методы, позволяющие злоумышленникам обходить стандартные виды двухфакторной аутентификации.

По данным Amnesty International, в декабре 2018 года были отмечены аналогичные кибератаки. В последнем докладе говорится об ужесточении давления на правозащитников в том, что касается безопасности информации в сети. На сегодняшний день самое надёжное средство защиты от фишинга – использование аппаратных ключей безопасности (например Yubikey или Solo Keys).

Примеры аппаратных ключей: SoloKeys и Yubikeys

В случае если почтовый сервис или социальная сеть не поддерживают аппаратные ключи безопасности, другие формы двухфакторной аутентификации (хотя и с меньшей надёжностью) остаются полезным базовым средством профилактики, способным по крайней мере помешать случайным злоумышленникам и снизить риск повторного применения пароля.

Дополнительную информацию о фишинге и методах защиты от фишинга см. в руководстве по фишингу Security Without Borders.

Слежка: правозащитники Узбекистана в постоянной опасности

Amnesty International зафиксировала в Узбекистане грубые нарушения прав человека, в том числе повсеместное применение пыток сотрудниками правоохранительных органов и произвольные задержания. Несмотря на недавнюю реформу системы уголовного правосудия и закрытие нескольких мест лишения свободы, где широко применялись пытки, безнаказанность прошлых нарушений сохраняется. И хотя в Узбекистане сейчас функционирует больше независимых СМИ, свобода выражения мнений, свобода объединений и свобода мирных собраний по-прежнему находятся под жёстким контролем и продолжается преследование активистов гражданского общества за мирную деятельность.

В докладе 2017 года «Мы найдём тебя везде» организация рассказала о последствиях аналогичного кибернаступления на активистов и журналистов в Узбекистане, в результате которого многие из них подверглись опасности, а некоторым даже пришлось уехать из страны.

Настоящий доклад подтверждает, что в Узбекистане сохраняется целенаправленная слежка за правозащитниками. Специальный докладчик ООН по вопросам свободы слова Дэвид Кайе призвал государства незамедлительно ввести мораторий на экспорт, продажу, передачу, использование и обслуживание разработанных частным образом средств слежения до тех пор, пока не будут установлены строгие правозащитные гарантии, регулирующие применение подобных средств. Amnesty International полностью согласна с данным требованием. Как отметил Специальный докладчик: «Недостаточно сказать, что комплексная система контроля и использования технологий целенаправленного слежения не работает. На деле ее практически не существует».

Если, по вашему мнению, вы подверглись кибератаке, аналогичной упомянутым в докладе, пожалуйста, свяжитесь с нами по адресу:

share@amnesty.tech