Кириллические доменные имена и адреса электронной почты реже используются для совершения противоправных действий в сети интернет

Проект Поддерживаю.РФ провел исследование использования омоглифов в интернет-идентификаторах. В отчете по результатам исследования представлена теоретическая база, приведены примеры вредоносного использования омоглифов, статистика омоглифических атак в различных доменных зонах, а также лучшие практики противодействия таким атакам от международных организаций, разработчиков ПО, регистратур и регистраторов доменных имен и других представителей экспертного сообщества.

Слово «омоглиф» в современном его значении означает графически схожие или одинаковые символы, имеющие разное значение. Например, латинская буква «o» (U+006F), кириллическая буква «о» (U+043E) и греческая буква омикрон «ο» (U+03BF). Несмотря на то, что символы выглядят одинаково – это совершенно разные буквы, имеющие разную машинную кодировку.

Более того, к омоглифам относят и буквы с диактрическими символами, например, кириллические буквы «е» (U+0435) и «ё» (U+0451), латинские «a» (U+0061) и «a» с акутом «á» (U+00E1). Существуют также составные омоглифы, состоящие из нескольких символов. Так, сочетание латинских букв «rn» (U+0072 и U+006E) визуально похоже на латинскую букву «m» (U+006D).

Подобная визуальная схожесть символов в интернет-идентификаторах (в частности, в доменных именах и адресах электронной почты) может привести не только к случайным ошибкам в адресации, но и к целенаправленной подмене адресов в противоправных целях.

Основной угрозой так называемых омоглифических атак является создание фишинговых ресурсов на доменных именах, максимально схожих с легитимными. Простой пользователь сети в поисках нужного ресурса может случайно попасть на фишинговый сайт, который мошенники постарались сделать похожим на оригинальный. Таким образом, злоумышленники могут получить конфиденциальную информацию и личные данные пользователя.

При этом использование омоглифов во вредоносных целях характерно не только для интернационализированных доменных имен и адресов электронной почты, но для доменов и почты на латинице. Согласно представленной в исследовании статистике, случаев омоглифических атак с использованием доменных имен в интернационализированных доменных зонах, в частности в кириллической зоне .РФ, установлено значительно меньше, чем в традиционных латинских, таких как .COM.

Появление интернационализированных доменных имен и адресов электронной почты расширило сценарии использования омоглифов в противоправных целях, но одновременно стало стимулом для выработки новых механизмов защиты, стандартов и рекомендаций для всего мирового интернет-сообщества.

«Пользователям удобнее пользоваться электронной почтой и доменами на родном языке, а продолжающийся рост языкового разнообразия в глобальной сети дает основания полагать, что интернационализация интернет-адресации только продолжит свое развитие. При этом пользователям стоит учиться соблюдать онлайн-гигиену и быть более подкованными в цифровом плане, в том числе и в отношении различных мошеннических схем с использованием омоглифов. Надеемся, что результаты нашего исследования помогут пользователям обезопасить себя при работе в интернете, а интернет-сообществу - обратить внимание на аспекты кибербезопасности, связанные с омоглифами», – отметил **технический консультант проекта Поддерживаю.РФ, автор исследования Вадим Михайлов.**

Проект Поддерживаю.РФ создан Координационным центром доменов .RU/.РФ в 2020 году в ознаменование десятилетнего юбилея российского домена верхнего уровня .РФ. Он призван помочь разработчикам программного обеспечения реализовать полноценную поддержку кириллических доменных имен и адресов электронной почты в их продуктах, а системным администраторам – правильно выбрать и настроить ПО, имеющее такой функционал. На сайте проекта собрана русскоязычная документация по работе с интернационализированными доменными именами (IDN) и почтовыми адресами (EAI), включая стандарты и лучшие практики по их обработке в программном обеспечении, а также постоянно обновляемый каталог программных продуктов с указанием их текущего статуса поддержки IDN и EAI.

Информационные партнеры проекта: интернет-портал D-Russia.ru, интернет-портал Digital-Report.ru, MSKIT.ru, «Мобильные телекоммуникации»,общественно-государственное объединение «Ассоциация документальной электросвязи», журнал «БИТ.Бизнес&Информационные технологии» и журнал «Системный администратор».