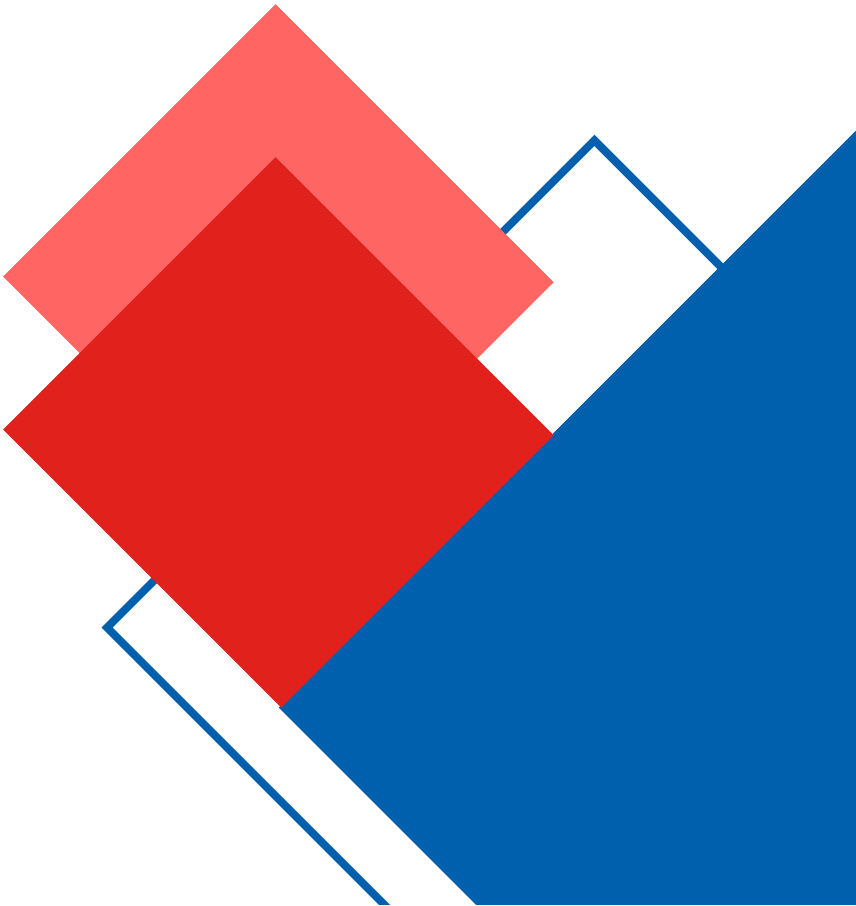
КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Поддерживаю .РФ

ИССЛЕДОВАНИЕ ИСПОЛЬЗОВАНИЯ ОМОГЛИФОВ В ИНТЕРНЕТ-ИДЕНТИФИКАТОРАХ



2022

Настоящее исследование посвящено проблеме ошибочного или злонамеренного использования визуально схожих символов или целых строк в интернет-идентификаторах (доменных именах и адресах электронной почты), примерам последствий такого использования и анализу стандартов, рекомендаций и лучших практик противодействия вредоносному использованию омоглифов, применяемых на уровне экспертных сообществ, международных организаций, разработчиков программного обеспечения, регистратур и регистраторов доменных имен.

Целью исследования является подготовка обзора актуальных примеров вредоносного применения омоглифов в доменных именах и адресах электронной почты, в первую очередь в интернационализированной их части, как наиболее уязвимой к такого рода атакам, а также разработанных средств противодействия и ведущейся в настоящее время работы в различных профессиональных объединениях по снижению рисков, возникающих в результате этой проблемы.

Содержание

1. Введение

Визуальная схожесть как отдельных символов различных алфавитов, так и целых строк в пространстве интернет-идентификаторов, в частности в пространстве доменных имен и адресов электронной почты, способна привести к ошибкам в адресации или даже к злонамеренной подмене адресантов. Для того чтобы снизить риски подобных ситуаций интернет сообществом выработан ряд методик, правил и лучших практик на различных уровнях информационного обмена в сети интернет, среди различных его участников. Что же представляет из себя такая схожесть и как классифицируется? Как она может быть использована в злонамеренных целях и как этому противодействовать? Рассмотрим эти и другие вопросы, начав с базовых понятий, примеров использования и далее, двигаясь от простого к сложному.

2. Понятие омоглифов

Понятие «омоглиф» произошло от древнегреческого ὁμός – «одинаковый», и γλυφή – «знак». В современности это слово является орфографическим и типографическим термином, обозначающим графически схожие или одинаковые символы, имеющие различное значение. Например, латинская буква «o» (U+006F), кириллическая буква «о» (U+043E) и греческая буква омикрон «ο» (U+03BF) выглядят абсолютно одинаково, однако это разные буквы, которые имеют совершенно разную машинную кодировку. Латинская строчная буква *дум* «ԁ» (U+A771) выглядит очень похоже на классическую латинскую строчную букву *ди* «d» (U+0064) и при беглом взгляде на строку, содержащую эти буквы, их легко принять за одну и ту же букву. Кроме того, к омоглифам относят и буквы с диактрическими символами, например, кириллические буквы «е» (U+0435) и «ё» (U+0451). Еще пример, латинская «a» (U+0061) и латинская а с акутом «á» (U+00E1) или латинская «a» с грависом «à» (U+00E0) или латинская «a» с диэризисом «ä» (U+00E4) или латинская «a» с циркумфлексом «â» (U+00E2) или латинская а с макроном «ā» (U+0101) и т.д.

Стоит заметить, что понятие омоглифа относят не только к отдельным символам, но и к их сочетанию, так называемые составные или многобуквенные омоглифы. Например, сочетание латинских букв «rn» (U+0072 и U+006E) визуально похоже на латинскую букву «m» (U+006D) или сочетание латинских букв «vv» (U+0076 и U+0076) легко спутать с латинской «w» (U+0077). К этой же группе можно отнести и лигатуры – символы, образованные путем соединения двух и более графем. Например, кириллическая буква «љ» (U+0459) представляет собой соединение букв «л» (U+043B) и «ь» (U+044C). Или латинская лигатура

«ffl» (U+FB04) является соединением букв «f» (U+0066), «f» (U+0066) и «l» (U+006C).

Понятие омографа схоже по смыслу с омоглифом, но относится к целым словам, ὁμός – «одинаковый» и γράφω – «писать», т.е. разные слова, которые одинаково или похоже написаны. Например, *pay* – английский глагол «платить» и *pay* – сочетание кириллических букв «р», «а» и «у». Если разложить на буквы, то этот пример омографа, является сочетанием трех омоглифов. Другой пример – это латинское слово в верхнем регистре *MAMA* и кириллическое *МАМА* или курсивом в нижнем регистре английское *mama* и кириллическое *мама*.

3. Доменная адресация

Доменная адресация в сети интернет была придумана для того, чтобы людям было проще запоминать адреса сетевых ресурсов и вводить их в адресной строке браузера. При помощи системы доменных имен (DNS), каждое делегированное доменное имя сопоставлено с IP-адресом, т.е. с идентификатором ресурса в сети. Так вот, основная угроза омоглифических атак – это создание вредоносных фишинговых ресурсов и привязка к ним доменных имен максимально похожих на легитимные. Пользователь, переходя по ссылке с таким доменным именем, убежден, что обращается к нужному ему ресурсу, например, своего банка и вводит там данные доступа к личному кабинету или кредитной карты. Фактически же он работает с подделкой под легитимный ресурс и отдает злоумышленникам критическую конфиденциальную информацию, которая может им позволить от лица этого пользователя и без его ведома, совершать мошеннические финансовые операции. Сочетание таких омоглифических доменных имен с фишинговыми схемами и методами социальной инженерии позволяет злоумышленникам получать и использовать во вредоносных целях различную конфиденциальную информацию пользователей сети интернет: реквизиты доступа от личных кабинетов различных ресурсов, данные крипто-кошельков платежных систем, данные банковских карт и т.д.

При помощи подобной схемы может быть обмануто значительное число пользователей, потому как злоумышленники стараются подобрать такие условия функционирования вредоносных ресурсов, при которых регуляторам и правоохранительным органам крайне сложно их ликвидировать. Например, злоумышленники обычно стараются производить атаки на граждан одной страны, размещая ресурсы и регистрируя омоглифические доменные имена в тех странах, с которыми у целевой страны максимально сложные взаимоотношения, что позволяет таким вредоносным ресурсам существовать длительный период

времени. Кроме того, для размещения вредоносных ресурсов регистрируются доменные имена в национальных доменах стран со слабой законодательной базой в области противодействия таким видам атак.

4. Электронная почта

Самая популярная атака с использованием омоглифов в области электронной почты – это BEC-атака, тип фишинговой атаки, направленной на компрометацию в основном корпоративной электронной почты (BEC – Business Email Compromise). По данным Федерального бюро расследований США в 2019 году этот тип атаки нанес наибольший финансовый урон, который составил порядка 50% от общих финансовых потерь от киберпреступлений, всего же с 2016 года урон от такого рода атак составил порядка 26 миллионов долларов [1]. Причем жертвами подобных атак становились как сотрудники крупных корпораций, так и представители малого и среднего бизнеса.

Основная схема BEC-атаки основана на рассылке сотрудникам компании писем с содержанием, побуждающим к различного рода компрометирующим конфиденциальные данные действиям, с адресов визуально похожих на адреса персон, которым сотрудники этой компании должны доверять. Если сотрудник, уверенный в том, что общается с доверенным лицом, вступает в переписку, то злоумышленник будет пытаться выманить у него некие критические конфиденциальные данные, заставить пройти по вредоносной ссылке, установить вредоносное ПО и т.д. Например, сотрудник бухгалтерии получает письмо от якобы директора компании с визуально похожего на адрес директора адреса электронной почты, в котором директор просит срочно прислать ему реквизиты доступа к банковскому аккаунту, оплатить некий товар или услугу со счета компании и т.д. Это упрощенная схема, в реальности схемы социальной инженерии зачастую куда более многоуровневые и сложные, направленные на то, чтобы у жертвы не возникло и тени сомнения, что она переписывается с доверенным лицом, а не с мошенником.

Подобная схема атаки требует от злоумышленника определенной подготовки: необходимо выяснить примерную структуру компании, кто является ее ключевыми фигурами, выбрать наиболее подходящие для подделки почтовые адреса и разработать схему социальной инженерии. Использование омоглифов в поддельных адресах электронной почты возможно как в локальной части (до знака @), так и в доменной (после знака @). В первом случае злоумышленнику надо иметь доступ к тому же почтовому серверу, который используется в компании. Это несложно, если компания использует общедоступные почтовые

сервисы для корпоративной переписки, например, Yandex, Mail.ru, Gmail и т.д. Например, martin.bowl@gmail.com может быть подделан как rnartin.bowl@gmail.com или как martin.bovvl@gmail.com. Конечно, локальная часть адреса может быть подделана и с использованием символов, отличных от латиницы, например, с помощью кириллических букв «а» или «о», если почтовый сервис позволяет регистрацию таких адресов.

Однако, в большинстве случаев для размещения почтового сервиса компании используют свой корпоративный домен, и в этом случае злоумышленнику либо нужно иметь возможность создавать на нем новые аккаунты, например, предварительно взломав его или получив еще каким-то способом реквизиты доступа администратора, либо попытаться подделать доменную часть адреса электронной почты, зарегистрировав визуально схожее доменное имя и делегировав его на свой почтовый сервер. Например, если у некой компании корпоративный почтовый домен com.org, то злоумышленник регистрирует схожий домен corn.org, или C0M.ORG, или же вообще домен на кириллице сом.org, и отправляет письма сотрудникам компании с адреса, у которого локальная часть идентична адресу руководителя компании, а доменная – это принадлежащий злоумышленнику домен почтового сервера, визуально схожий с корпоративным доменом электронной почты, например, martin.bowl@corn.org.

5. Примеры

Безусловно, существует множество прецедентов использования мошенниками омоглифов. В подавляющем большинстве своем это различные фишинговые схемы, направленные на подмену легитимных страниц ввода конфиденциальной информации. Однако, есть и любопытные примеры вредоносного использования омоглифов несколько иным образом.

В августе 2017 года независимым исследователем Ankit Anubhav был обнаружен домен adoḅe.com (обратите внимание на латинскую строчную букву «ḅ» (U+1E05) с точкой снизу), который в соответствии с данными сервиса whois был зарегистрирован регистратором GoDaddy в апреле 2017[2]. Домен использовался для распространения под видом Adobe Flash Player трояна Beta Bot, который отключал ПО, предназначенное для обеспечения безопасности, и препятствовал получению доступа к популярным сайтам разработчиков такого ПО. Домен был снят с делегирования, его регистрация была удалена, однако на момент проведения исследования, согласно официальному сайту GoDaddy домен снова стал доступен для регистрации любым желающим.

Ярким примером ошибки разработчиков, служит обнаруженная в ноябре 2018 года специалистом компании Tencent Security уязвимость (CVE-2018-4277) в программных продуктах компании Apple, связанная с отображением строчной латинской буквы дум «ԁ» (U+A771), которая отображалась абсолютно идентично латинской строчной букве ди «d» (U+0064)[3,4]. Таким образом, например, браузер Safari не отображал единственное различие между этими буквами – маленькую черточку в нижней части буквы дум. В результате у злоумышленников была возможность использовать эту букву из набора символов расширенной латиницы для проведения различных омоглифических атак. Специалисты Tencent Security уведомили компанию Apple о найденной уязвимости, и в новых релизах программных продуктов этот баг был исправлен, однако, угроза была весьма существенна, т.к. немало популярных ресурсов, которые могут быть потенциальной целью для омоглифических атак, имеют в составе своих доменных имен букву «d».

Еще один пример, хотя и относящийся больше к правовому пространству и формированию судебной практики, чем к особенностям технической реализации омоглифических атак, несомненно, тоже достоин упоминания. В июле 2019 года Microsoft Digital Crimes Unit, международное объединение экспертов компании Microsoft в области IT, юриспруденции, бизнеса и т.д., противостоящее киберпреступлениям с 2008 года, добилось решения суда Восточного округа Вирджинии об удалении 17 доменных имен, содержащих омоглифические схожести с легитимными доменами компании[5]. Злоумышленники использовали эти домены для BEC-атак, похищения конфиденциальных данных, в том числе и различных реквизитов доступа, для распространения программ-вымогателей и прочего ВПО. Это решение стало значимым примером в судебной практике США, на который опираются в судах и в настоящее время.

6. Статистика

Для того чтобы оценить специфику использования омоглифов во вредоносных целях, обратимся к статистике. По данным отчета об угрозах компьютерной безопасности компании ESET основные направления атак с использования омоглифов – это сервисы обмена криптовалюты, социальные и финансовые сервисы[6,7]. Если в середине 2020 года лидерами по числу направленных на них омоглифических атак являлись такие ресурсы, как blockchain.com и binance.com, то к концу 2021 года в тройку лидеров вошли ресурсы двух польских банков: mBank и Getin Bank. Самым распространенным

поддельным ресурсом стал online.mbąnk.com, а secure.getinbąnk.com занял третье место. Также австралийская криптовалютная биржа Coin Spot стала весьма популярной целью мошенников, использовавших поддельный домен coınspot.com. Помимо вышеперечисленных ресурсов в топ 10 целей омоглифических атак вошли такие бренды как чешский банк Equa bank, польский банк Pekao, международная банковская группа Santander, банк UniCredit, почтовый сервис Hotmail и сервис Microsoft для работы с электронными документами Office.

Если взглянуть на количественные показатели использования омоглифических атак в доменах верхнего уровня, то по данным «Центра реагирования CERT-GIB»[8] за 2021 год и первый квартал 2022 года, наиболее популярной доменной зоной в этом плане закономерно является .com, в ней было выявлено 77 случаев вредоносного использования омоглифов. Среди национальных доменов лидирует зона .de – 6 случаев, в российском национальном домене было обнаружено только 3 таких случая за указанный выше период (Рис. 1).

Рис. 1

Согласно тому же исследованию CERT-GIB, наиболее популярными символами, используемыми в омоглифических доменных именах являются такие символы расширенной латиницы как символ «é» (U+00E9) – латинская маленькая «е» с акутом, символ «á» (U+00E1) – латинская маленькая «а» с акутом и символ «ı» (U+0131) – латинская маленькая «i» без точки. Единственный символ

кириллического скрипта – маленькая «о» (U+043E) – занимает в этом рейтинге 17 место (Рис. 2).

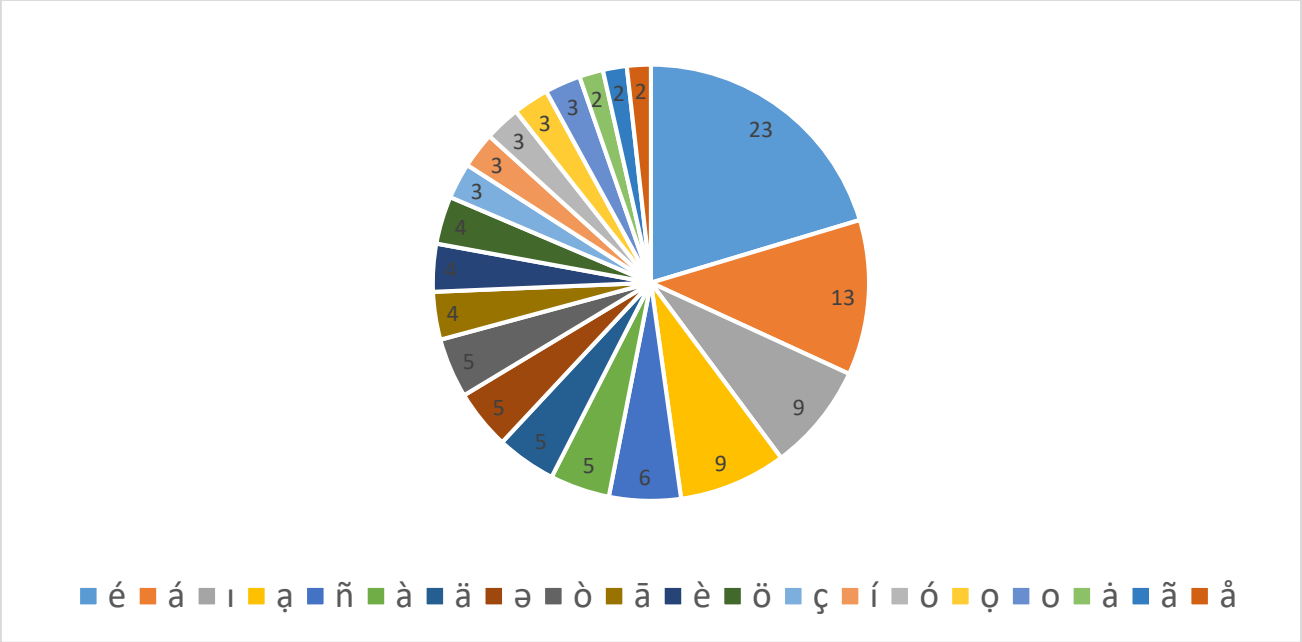


Рис. 2

Согласно данным проекта Координационного центра доменов .RU/.РФ «Доменный патруль»[9] за минувший год было зарегистрировано около 180 обращений от компетентных организаций, связанных с кириллическими доменами в зоне .РФ. Из них только три домена можно отнести к попыткам подделок легитимных ресурсов при помощи схожих доменных имен: госуслути.рф, целью очевидно была площадка государственных услуг, гэмотест.рф – ресурс медицинской лаборатории «Гемотест» и наложкаа.рф – сервис сделок для покупки товаров в сети интернет. Необходимо заметить, что два последних ресурса нельзя полностью отнести к омоглифическим атакам, поскольку один из них использует замену символа созвучным, а второй просто добавляет дополнительный дублирующий символ в конце домена второго уровня в расчете на невнимательность пользователей. Однако, эти вредоносные ресурсы используют тот же принцип схожести с атакуемыми доменными именами, что и при омоглифических атаках.

7. Ответные инициативы

С момента появление интернационализированных доменных имен, а затем и интернационализированных адресов электронной почты, эксперты интернет индустрии пытались оценить риски их использования и выработать соответствующие этим рискам ответные, а зачастую и упредительные меры. Эта

работа и по сей день ведется в различных экспертных сообществах, в профессиональных объединениях разработчиков программных решений, на уровне регистратур доменов верхнего уровня и регистраторов, предоставляющих услуги регистрации доменных имен конечным пользователям. Надо отметить, что противостояние «снаряда и брони» становится все сложнее, действия злоумышленников все запутаннее и изощреннее, что требует от противостоящих им специалистов организации комплексного подхода к проблеме омоглифов и выработки соответствующих ответных мер как на уровне отдельных организаций, так и на уровне глобальных экспертных объединений.

7.1. Профессиональные сообщества

Существует множество профессиональных сообществ, объединяющих независимых экспертов, представителей бизнеса, государства, гражданского общества и других организаций, заинтересованных в вопросах информационной безопасности, в том числе и в противодействии использованию омоглифов в различных противоправных и вредоносных целях. Рассмотрим некоторые из них.

Unicode Consortium

Консорциум Юникод – некоммерческая организация, основная цель деятельности которой состоит в публикации, поддержке и развитие стандарта Юникод, предназначенного для последовательного кодирования, представления и обработки текста большинства мировых систем письма. В рамках своей деятельности консорциум Юникод ведет активную работу по исследованию возможностей использования символов Юникод злоумышленниками в различных противоправных схемах, в том числе и для омоглифических атак, а также по выработке рекомендаций, как такому использованию противостоять.

В частности, еще в 2014 году был создан отчет о проведенном исследовании некорректного или злонамеренного использования многообразия символов Юникода, которое может привести к возникновению различных уязвимостей безопасности информационных систем или их компонентов. В исследование внесло свой вклад более десятка экспертов IT-отрасли, а его итогом стал отчет UTR#36 «Unicode Security Considerations»[10], одобренный техническим комитетом консорциума Юникод. Отчет описывает ряд специфических для интернационализации аспектов информационной безопасности, рассчитанных, в первую очередь, на аудиторию программистов, системных аналитиков и разработчиков стандартов. Он содержит целый ряд рекомендаций, направленных на снижение рисков, связанных с использованием Юникода. Отчет состоит из двух основных разделов: первый посвящен вопросам

безопасности, связанным с визуальным аспектом использования символов Юникод, к ним относятся и проблемы, связанные использованием омоглифов, второй раздел посвящен проблемам, не связанным с визуальной составляющей Юникода.

На основе этого отчета экспертами консорциума Юникод был создан документ UTS#39 «Unicode Security Mechanisms»[11], описывающий прикладные механизмы, позволяющие выявить потенциальные проблемные места в информационных системах или их компонентах. Речь, конечно, идет о проблемах в области информационной безопасности, связанных с использованием символов Юникод. Документ пересматривался и дополнялся множество раз, на момент проведения исследования актуальна 14-я версия от августа 2021 года[12]. В его составе есть описание механизмов определения степени схожести строк как в случае использования одного языкового скрипта, так и при их смешивании.

Internet Corporation for Assigned Names and Numbers

Интернет корпорация по управлению доменными именами и IP-адресами (ICANN) – некоммерческая общественная корпорация, объединяющая множество организаций и экспертов с целью обеспечения безопасного, стабильного и отказоустойчивого функционирования интернета.

Сообществом ICANN ведется активная работа, направленная на снижение рисков использования интернационализированных доменных имен, в том числе и рисков, связанных с использованием омоглифов. Одной из важных инициатив в этой области является разработка Правил генерации меток (Label Generation Rules) [1] – механизма, призванного определить правила создания корректного интернационализированного доменного имени с использованием определенного языкового скрипта. С появлением интернационализированных доменных имен верхнего уровня в 2010 году началась разработка правил генерации меток корневой зоны Root Zone Label Generation Rules (RZ-LGR), первый релиз которых состоялся в 2012 году. Четвертая версия RZ-LGR-4 опубликована в ноябре 2020 года и включает в себя 18 языковых скриптов. Предложение правил генерации меток для кириллического скрипта[13] планируется к внедрению в ожидаемую пятую версию RZ-LGR-5 и содержит помимо перечней символов различных алфавитов, относящихся к кириллическому скрипту, еще и перечень омоглифов из других языковых скриптов, таких как латинский базовый и расширенный латинский, армянский, грузинский и греческий[14].

[1] Метки в данном контексте – это разделенные точками строки, , из которых состоит доменное имя.

Кроме того, нельзя не отметить усилия рабочей группы IDNGWG (IDN Guidelines Working Group) по созданию «Руководящих принципов по внедрению интернационализированных доменных имен» (Guidelines for the Implementation of Internationalized Domain Names), в которые входят и рекомендации по минимизации рисков, связанных с использованием омоглифов в метках доменных имен. А также стоит упомянуть работу Security and Stability Advisory Committee (SSAC), комитета экспертов в области безопасности и целостности доменного и адресного пространства интернета, который в своих отчетах также уделяет внимание проблеме использования омоглифов.

Отдельного внимания заслуживает инициатива Универсального принятия (Universal Acceptance) – состояния, когда все домены, включая интернационализированные доменные имена (IDN) и новые общие домены верхнего уровня (New gTLD), и все адреса электронной почты одинаково воспринимаются всеми системами, устройствами, интернет-приложениями и т.д. Данная инициатива включает в себя большую подборку практической информации, в том числе направленной на помощь разработчикам во внедрении поддержки интернационализированных доменов и адресов электронной почты с учетом лучших практик противодействия использованию омоглифов во вредоносных целях.

Конечно, это далеко не полный перечень профессиональных сообществ, которые так или иначе затрагивают в своей работе тематику противоправного использования омоглифов. Ряд стандартов RFC разработан экспертами Инженерного совета интернета (Internet Engineering Task Force) с учетом принятых подходов работы с омоглифами, например, стандарт IDNA 2008. Да и в грядущих разработках стандартов, связанных с многоязычием интернет-идентификаторов, эта проблема, безусловно, будет учтена. World Wide Web Consortium (W3C), организация, разрабатывающая и внедряющая технологические стандарты для глобальной сети, Web Hypertext Application Technology Working Group (WHATWG), международная рабочая группа по технологиям гипертекстовых веб-приложений, Международный союз электросвязи (ITU), различные сообщества экспертов и организаций, занимающихся аналитикой в области информационной безопасности и реагированием на компьютерные инциденты CERT/CSIRT – все они стараются в своей работе учитывать существующие стандарты, рекомендации и лучшие практики работы с символами, схожими до степени смешения, или ведут разработку новых стандартов.

7.2. Регистратуры доменов верхнего уровня

Регистратура домена верхнего уровня – это организация, определяющая правила использования доменных имен в том домене верхнего уровня, за который эта организация отвечает в соответствии с соглашением с ICANN, в случае общих доменов верхнего уровня, или в соответствии с поручением конкретного государства в случае страновых доменов верхнего уровня.

Большинство регистратур предусматривают в своих регламентирующих документах меры противодействия противоправному использованию омоглифов в доменных именах в своих зонах.

Одной из распространенных мер регистратур является запрет на смешивания языковых скриптов в одной метке, который устанавливается в правилах регистрации доменных имен в этой зоне. Таким образом нельзя зарегистрировать доменное имя, содержащее кириллический и латинский символы в одном домене второго уровня, и при попытке регистрации такого имени будет получен отказ на уровне системы контроля реестра.

Более того, многие регистратуры страновых доменов специально регистрируют IDN домены верхнего уровня, чтобы разнести латинский и национальный языковые скрипты по соответствующим доменным зонам. В частности, в российской национальной доменной зоне .RU разрешена регистрация доменных имен только на латинице, а в зоне .РФ – только на кириллице, что, например, делает невозможным регистрацию домена cop.ru, где «cop» написано на кириллице и визуально идентично вполне легитимному латинскому домену cop.ru. Аналогично запрещен к регистрации домен cop.рф, где «cop» состоит из латинских символов.

Кроме того, большинство регистратур тесно взаимодействуют с экспертными организациями в области информационной безопасности, например, с CERT/CSIRT. Эти организации помогают выявлять различные противоправные действия с доменными именами, в том числе и связанные с использованием омоглифов. К примеру, Координационным центром доменов .RU/.РФ создан и развивается институт компетентных организаций, в который на момент проведения исследования входят 12 ведущих российских компаний в области информационной безопасности. В соответствии с «Правилами регистрации доменных имен в доменах .RU и .РФ» аккредитованные в этих зонах регистраторы наделены правом при получении мотивированного запроса от компетентных организаций снимать используемый для противоправных действий домен с делегирования.

7.3. Регистраторы

Регистратор – это организация, аккредитованная одной или несколькими регистратурами доменов верхнего уровня предоставлять услуги по регистрации доменных имен в этих доменных зонах. Регистраторы осуществляют непосредственное взаимодействие с администраторами доменных имен, т.е. лицами, регистрирующими доменные имена для своих целей, например, для создания веб-ресурса, лэндинг-страницы, почтового сервиса или даже для последующей перепродажи зарегистрированных доменных имен. Для защиты своих клиентов некоторые крупные регистраторы разрабатывают и развивают сервисы противодействия использованию омоглифов во вредоносных целях. Например, процедура генерации связанного с регистрируемым доменным именем набора схожих доменных имен (bundle), которые потенциально могут использоваться злоумышленниками. Эта процедура получила название homoglyph bundling, а полученные в результате наборы позволяют пользователю оценить уровень риска омоглифических атак на выбранное им доменное имя и, при необходимости, зарегистрировать этот дополнительный набор доменных имен, схожих с целевым именем, который зачастую предлагается регистраторами по сниженной цене.

Кроме того, как уже было упомянуто выше, регистраторы взаимодействуют с экспертными организациями, компетентными в области информационной безопасности, по запросам которых осуществляют проверку доменных имен и их администраторов и, при необходимости, снимают эти доменные имена с делегирования или вовсе их удаляют.

7.4. Разработчики программных продуктов

Немалую роль в противодействии злонамеренному использованию омоглифов играют разработчики программного обеспечения, осуществляющего работу с доменными именами и адресами электронной почты. От разработчиков зависит, например, каким шрифтом в их продуктах будут отображаться доменные имена и адреса электронной почты, и позволяет ли этот шрифт перепутать похожие символы или наоборот подчеркивает их разницу.

Когда происходит смешение языковых скриптов в одной метке, разработчик может заложить в свой программный продукт способ обратить на это внимание пользователя. В частности, в большинстве браузеров в случае, если доменное имя в адресной строке содержит смесь различных языковых скриптов,

такое доменное имя отображается в представлении punycode[2], которое характерно визуально хорошо заметным ACE префиксом «xn--», что позволяет пользователю перепроверить, к тому ли ресурсу он обращается. Например, доменное имя pay.com состоящее из латинских символов и кириллической буквы «а» будет отображено как xn--py-7kc.com.

Соблюдение требований актуальных стандартов в области работы с интернационализированными доменными именами и адресами электронной почты, использование лучших практик и экспертных рекомендаций также крайне важно при разработке программного продукта.

8. Заключение

Новые возможности почти всегда несут новые риски, однако это не повод их упускать. Проблема использования схожих доменных имен и адресов электронной почты в мошеннических целях появилась достаточно давно, еще до внедрения в систему адресации возможностей их интернационализации. Появление интернационализированных доменных имен и адресов электронной почты безусловно способствовало расширению разнообразия сценариев использования омоглифов во вредоносных целях. Однако, это позволило мировому интернет-сообществу выработать соответствующие механизмы защиты, стандарты, рекомендации и лучшие практики, следуя которым можно существенно снизить уровень таких рисков.

При этом удобство использования адресации в сети интернет на своем родном языке и продолжающийся рост языкового многообразия в доменных именах и адресах электронной почты позволяют сделать вывод, что интернационализация средств адресации в интернете уже вошла в нашу повседневную жизнь и продолжит свое развитие. В такой ситуации следует расширять навыки соблюдения цифровой гигиены и повышать уровень цифровой грамотности при работе в интернете, в том числе и в отношении различных омоглифических мошеннических схем.

[2] Punycode – алгоритм преобразования символов в кодировке Unicode в кодировку ASCII

Список источников

1. https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/business-email-uncompromised-part-one/ba-p/2159900
2. https://threatpost.com/idn-homograph-attack-spreading-betabot-backdoor/127839/
3. https://xakep.ru/2018/11/21/apple-homograph-attack/
4. https://xlab.tencent.com/en/2018/11/13/cve-2018-4277/
5. https://blogs.microsoft.com/on-the-issues/2021/07/19/cybercrime-homoglyphs-dcu-court-order/
6. https://www.welivesecurity.com/wp-content/uploads/2022/02/eset_threat_report_t32021.pdf
7. https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
8. https://www.group-ib.ru/cert.html
9. https://domainpatrol.ru/
10. https://www.unicode.org/reports/tr36/
11. https://www.unicode.org/reports/tr39/
12. https://www.unicode.org/reports/tr46/
13. https://www.icann.org/en/system/files/files/proposal-cyrillic-lgr-03apr18-en.pdf
14. https://www.icann.org/resources/pages/root-zone-lgr-2015-06-21-en
15. https://www.icann.org/resources/pages/implementation-guidelines-2012-02-25-en
16. https://www.icann.org/groups/ssac
17. https://www.w3.org/Consortium/
18. https://whatwg.org/