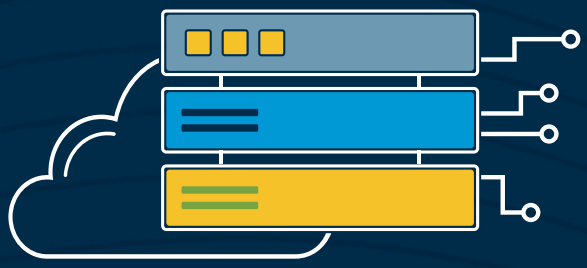
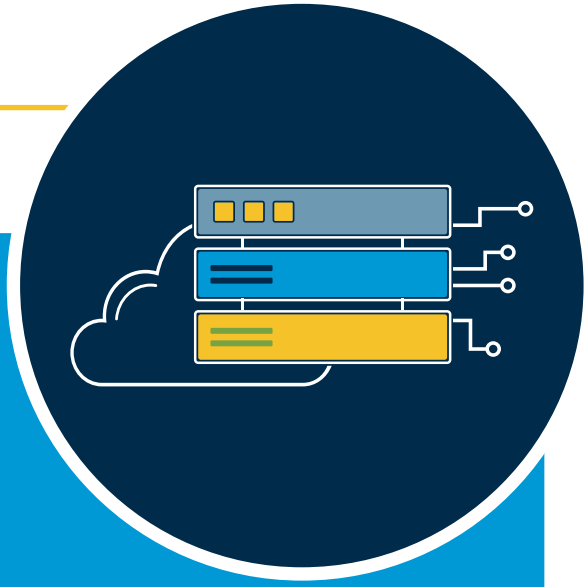


Инструмент сбора и регистрации информации об угрозах безопасности доменным именам (DNSTICR)

Январь 2022 года

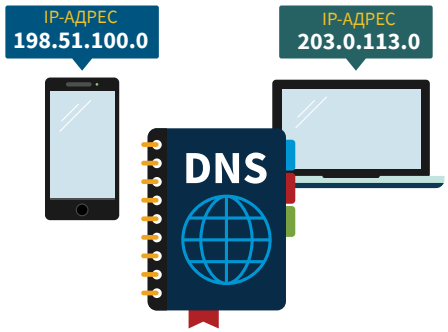
Интернет-корпорация по присвоению имен и номеров

ICANN



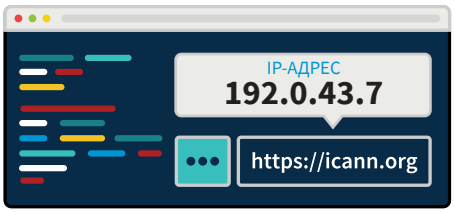
Содержание руководства

Что такое система доменных имен?



Система доменных имен (DNS) помогает пользователям ориентироваться в интернете. У каждого устройства или сайта в интернете есть уникальный адрес, аналогичный номеру телефона. Этот адрес, представляющий собой сложную последовательность цифр или цифр и букв, называется **IP-адресом.** IP — это интернет-протокол.

IP-адреса трудно запомнить.
DNS упрощает навигацию в интернете.



IP-адреса трудно запомнить. DNS упрощает навигацию в интернете, поскольку дает пользователям возможность вводить вместо **IP-адреса** привычные буквы — **доменное имя.** Например, чтобы попасть на сайт ICANN, необходимо всего лишь ввести **https://icann.org** вместо соответствующего **IP-адреса — 192.0.43.7**

Что такое угрозы безопасности DNS?

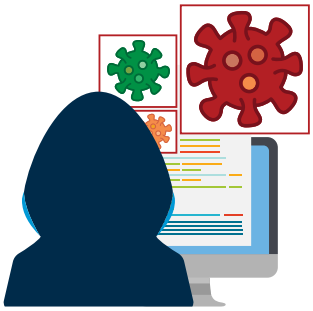
В интернет-пространстве имеют место различные виды **злоупотреблений**, связанных с контентом. К этим злоупотреблениям относятся сайты, предоставляющие платформу для незаконной деятельности, такой как эксплуатация детей и торговля людьми. Бывают также сайты, которые содействуют киберзапугиванию или являются цифровой площадкой для продажи несуществующих или поддельных товаров.

Однако регулирование интернет-контента не входит в сферу компетенции ICANN.

Усилия корпорации ICANN направлены на борьбу с конкретными **угрозами безопасности DNS**, имеющими более узкие рамки, чем злоупотребления, связанные с контентом. Так что же такое угрозы безопасности DNS?

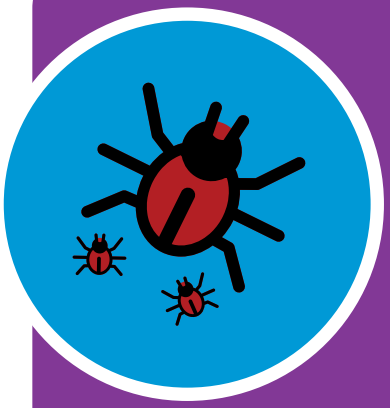
К угрозам безопасности DNS относится любая вредоносная деятельность, направленная на нарушение инфраструктуры или штатного режима работы DNS.

Инструмент сбора и регистрации информации об угрозах безопасности доменным именам (DNSTICR)



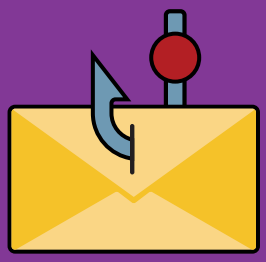
Проект **Инструмент сбора и регистрации информации об угрозах безопасности доменным именам (DNSTICR)** направлен на подготовку отчетов по недавно зарегистрированным доменам, которые, по мнению корпорации ICANN, используют тему пандемии COVID-19 для фишинговых кампаний и кампаний по распространению вредоносного ПО.

Эти отчеты содержат доказательства, которые приводят ICANN к мнению, что соответствующие домены используются в мошеннических целях. Наряду с другой вспомогательной информацией эти отчеты позволяют ответственным регистраторам определить правильный курс действий.



Проект DNSTICR предназначен для поиска попыток внедрения вредоносного ПО и фишинга.

Вредоносное ПО
Устанавливаемое на устройстве без согласия пользователя программное обеспечение, которое нарушает работу устройства, собирает конфиденциальные данные или получает доступ к частным компьютерным системам. К вредоносному ПО относятся вирусы, шпионские программы, программы-вымогатели и другое нежелательное программное обеспечение.



Фишинг
Происходит, когда злоумышленник обманом заставляет жертву раскрыть конфиденциальные личные, корпоративные или финансовые данные (номера счетов, идентификаторы входа, пароли и т. д.), отправляя мошеннические или похожие на подлинные электронные письма или заманивая пользователей на подложные сайты.

Проект DNSTICR не предназначен для поиска следующих вредоносных методов использования интернета:

Ботнеты

Группы подключенных к интернету компьютеров, которые заражены вредоносным ПО и находятся под управлением удаленного администратора.

Фарминг

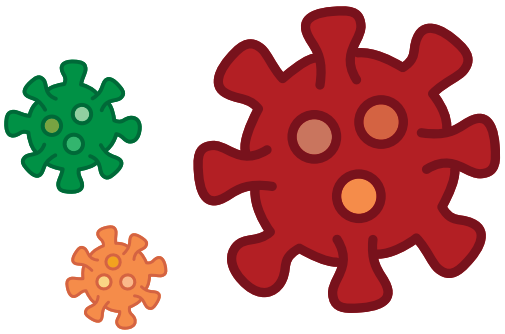
Перенаправление пользователей на мошеннические сайты или услуги, как правило, за счет перехвата или т. н. отравления кэша DNS.

- Перехват DNS происходит, когда злоумышленник с помощью вредоносного ПО перенаправляет своих жертв на собственный сайт вместо изначально запрошенного.
- Отравление кэша DNS приводит к тому, что DNS-сервер или резолвер в ответ на запрос отправляет ложный IP-адрес, являющийся источником вредоносного кода. Фишинг отличается от фарминга тем, что последний подразумевает изменение записей DNS, в то время как первый обманным путем заставляет пользователей ввести персональные данные.

Спам (когда он используется для распространения других угроз безопасности DNS)

Нежелательная массовая рассылка электронных писем лицам, не дававшим согласия на их получение, когда сообщение отправлено в составе группы сообщений, имеющих одинаковое по сути содержание. Типичная нежелательная электронная почта не представляет собой угрозу безопасности DNS за исключением ситуаций, когда эта электронная почта является частью фишинговой схемы.

Предпосылки создания проекта DNSTICR.



В период **пандемии COVID-19** целью фишинговых мошенников стали уязвимые, невнимательные, пожилые люди, дети и малоимущие. Эти преступники ищут своих жертв по всему миру и на многих языках, чтобы украсть деньги и персональные данные.

Преступники и мошенники звонят своим жертвам, отправляют им электронные письма или текстовые сообщения, чтобы обманом заставить раскрыть персональные данные или купить сфальсифицированные сертификаты вакцинации и результаты тестов на COVID-19 или поддельные лекарства.

Корпорация ICANN разработала проект **DNSTICR** для борьбы в интернете с фишингом и вредоносным ПО, связянными с COVID-19. Он предназначен для поиска потенциально злонамеренной деятельности в сфере доменных имен и передачи соответствующей информации регистраторам. Это создает дополнительную линию обороны в борьбе корпорации ICANN за защиту интернет-пользователей от угроз безопасности DNS.

По мере продолжения пандемии список терминов и тем для поиска в рамках проекта DNSTICR обновляется. Эти обновления — относительно простая техническая процедура. Например, были добавлены такие термины, как **паспорт** применительно к **иммунным паспортам**, выдаваемым в некоторых странах, и **ивермектин** — антипаразитарный препарат, который стал популярным в связи с пандемией.

Также могут употребляться и другие термины, такие как названия крупных финансируемых государствами программ, связанных с COVID-19 и предназначенных для оказания помощи нуждающимся. В базу данных включены также и более общие термины, такие как респираторы, маски N95 и антисептики.

Однако у корпорации ICANN недостаточно ресурсов или полномочий для проверки того, являются ли законными все сайты, предлагающие такие товары и услуги.

Помогите нам защитить интернет в вашем регионе мира от связанных с COVID-19 попыток фишинга и распространения вредоносного ПО.

Вы медицинский работник, финансовый менеджер, государственный чиновник, политик, сотрудник органов общественной безопасности или специалист по безопасности?

Мы нуждаемся в вас!

Вот как мы можем совместными усилиями защитить интернет-пользователей от угроз безопасности DNS:

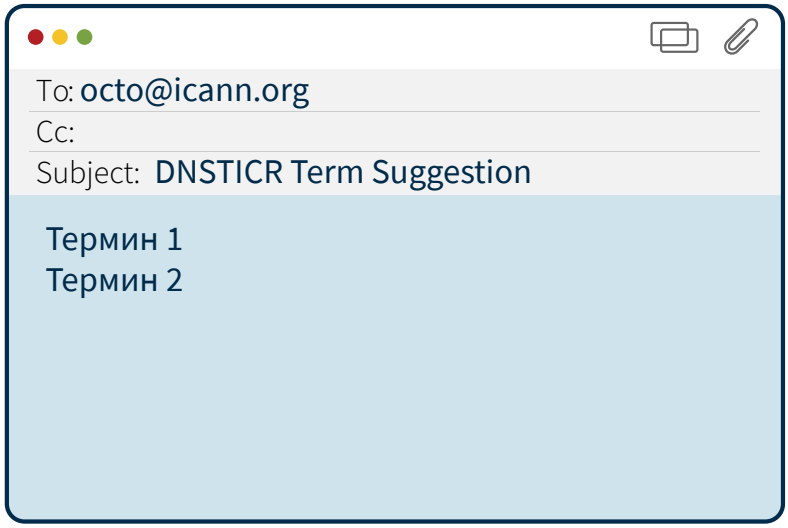
Шаг 1
Составьте на своем родном языке список связанных с пандемией COVID-19 слов, которые используются или могут использоваться в вашем регионе для атак на людей или организации.

Шаг 2
Отправьте этот список по адресу **octo@icann.org**, указав в строке темы сообщения: **DNSTICR Term Suggestion**

Предлагаемые термины должны быть представлены по одному в каждой строке текста электронного письма.

Например:
Термин 1
Термин 2

Если термины требуют пояснения, добавьте его в конце списка.



Ознакомьтесь с проектом «Инструмент сбора и регистрации информации об угрозах безопасности DNS» (DNSTICR) и узнайте, как вы можете внести свой вклад в повышение безопасности интернета!

Подробности
Посетите специальную веб-страницу DNSTICR:
https://www.icann.org/dnsticr

Обзор
Ознакомьтесь с усилиями корпорации ICANN по борьбе с угрозами безопасности DNS:
https://www.icann.org/dnsabuse

Аббревиатуры и термины
Нажмите на ссылки ниже, чтобы с помощью функции «Аббревиатуры и термины ICANN» подробнее узнать о терминах и аббревиатурах, используемых в настоящем руководстве:
https://go.icann.org/acronyms

Доменное имя
Метка доменного имени
Система доменных имен (DNS)
Интернет-протокол (IP)
Адрес интернет-протокола
Интернет-протокол 4-й версии (IPv4)
Интернет-протокол 6-й версии (IPv6)

МЫ В СОЦСЕТЯХ

https://icann.org
flickr.com/icann
@icann
linkedin.com/company/icann
facebook.com/icannorg
soundcloud.com/icann
youtube.com/icannnews
instagram.com/icannorg

или посетите наш портал соцсетей:
https://go.icann.org/socialmedia