Описание и условия использования Сервиса просмотра СТ-логов

Руководство пользователя

на 6 страницах

Информация о документе

Дата начала действия документа	03.03.2023
Версия	1.0

1. Введение

1.1. О документе

Настоящий документ разработан и выпущен Обществом с ограниченной ответственностью «Технический центр Интернет» (далее по тексту – ТЦИ, или Технический центр) и представляет собой руководство, регламентирующее порядок и условия использования пользователями программы для ЭВМ «Сервис просмотра CT-логов», являющейся модифицированной версией исходного программного обеспечения (https://github.com/crtsh) (далее по тексту – Программа). Программа позволяет проверить, выпускались ли сертификаты для доменного имени, в CT-логах Минцифры, Яндекса и VK.

Руководство содержит описание процесса поиска информации при помощи Программы.

1.2. Термины и сокращения

Доменное имя – зарегистрированное в базе данных (реестре) домена верхнего уровня символьное обозначение (обозначение символами), предназначенное для адресации сайтов в Интернете, где используется система доменных имен (DNS).

Минцифра – Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации — федеральный орган исполнительной власти.

Яндекс – ООО «Яндекс» (ОГРН 1027700229193).

VK – ООО «В КОНТАКТЕ» (ОГРН 1079847035179).

TLS-сертификат – сертификат открытого ключа, подтверждающий принадлежность открытого ключа доменному имени и позволяющий установить пользователю сети Интернет защищенное соединение с сайтом/ресурсом в сети Интернет по протоколу TLS.

Серийный номер TLS-сертификата — уникальный номер, присваиваемый каждым центром сертификации каждому выданному им TLS-сертификату.

Центр Сертификации (ЦС), или **Certification authority (CA)** – организация, осуществившая проверку права управлением доменным именем и выпустившая TLS-сертификат для данного доменного имени.

Certificate Transparency (CT) — набор технологий обеспечения публикации данных TLS-сертификатов доверенным способом и общедоступные системы, реализующие регистрацию и мониторинг выпуска TLS-сертификатов в соответствии с этими технологиями.

CT-лог — специальный лог-сервис, в котором регистрируется информация о выпущенных сертификатах.

SHA (Secure Hash Algorithm) — алгоритм криптографического хеширования.

2. Описание Программы и условия ее использования

Программа предназначена для поиска в CT-логах TLS-сертификатов, выпущенных одним из указанных в Таблице 2 Центров сертификации, в соответствии с параметрами поиска, заданными пользователем.

Право пользования Программой предоставляется на безвозмездной основе в рамках Пользовательского соглашения, размещенного на сайте ТЦИ по адресу: https://tcinet.ru/documents/user_agreement.pdf. Исходное программное обеспечение распространяется (https://github.com/crtsh) по открытой лицензии GNU General Public License v3.0 (https://www.gnu.org/licenses/gpl-3.0.en.html).

В случае наличия противоречий в условиях, установленных в GNU General Public License v3.0 и Пользовательском соглашении, применяются условия GNU General Public License v3.0.

2.1. Доступ к Программе

Пользование Программой осуществляется через браузер. Программа не требует установки на компьютере пользователя.

Доступ к Программе осуществляется по URL-адресу https://ct.tlscc.ru/.

2.2. Использование Программы

Программа проверяет сертификаты на доменные имена, выпущенные в Центрах сертификации, в CT-логах Минцифры, Яндекса и VK.

Для проверки необходимо ввести в поле поиска значение поиска и нажать кнопку «Найти».

В случае если искомый сертификат находится в CT-логах, он отобразится на странице.

В случае если искомый сертификат не найден в CT-логах, в результате поиска будет выведено сообщение «Сертификаты: Ничего не найдено».

Программа предоставляет возможность расширенного поиска сертификатов, доступного по активной ссылке «Расширенный поиск».

При расширенном поиске существует возможность указать дополнительные критерии поиска:

- Способ сравнения;
- Исключать истекшие сертификаты;
- Не дублировать сертификаты/пресертификаты;
- Показывать SQL.

Описание полей сертификата, по которым производится поиск, приведено в табл.1.

Табл. 1. Описание значений поиска

Поле	Описание
По сертификату	
CT Entry ID	Идентификтор записи CT-лога
Serial Number	Серийный номер сертификата
SHA-1 (SubjectPublicKeyInfo)	Открытый ключ, SHA-1
SHA-256 (SubjectPublicKeyInfo)	Открытый ключ, SHA-256
SHA-1 (Subject)	Имя субъекта
SHA-1 (Certificate)	Отпечаток сертификата, SHA-1
SHA-256 (Certificate)	Отпечаток сертификата, SHA-256
По Центру сертификации	
ID	Идентификатор издателя (Центра сертификации)
Name	Название организации издателя
По идентификатору	
commonName (Subject)	Имя субъекта, например, доменное имя или название Центра сертификации
emailAddress (Subject)	Адрес электронной почты
organizationalUnitName (Subject)	Наименование подразделения юридического лица
organizationName (Subject)	Наименование юридического лица
dNSName (SAN)	Доменное имя альтернативного имени субъекта
Rfc822Name (SAN)	Адрес электронной почты субъекта, которому выдан этот сертификат
IPAddress (SAN)	IP-адрес субъекта, которому выдан этот сертификат

Перечень Центров сертификации, по которым производится поиск, приведен в табл.2.

Табл. 2. Перечень Центров сертификации

Центр сертификации	URL-адрес сертификата Центра сертификации
Russian Trusted Root CA	http://company.rt.ru/cdp/rootca_ssl_rsa2022.crt
Russian Trusted Root CA	http://reestr-pki.ru/cdp/rootca_ssl_rsa2022.crt
Russian Trusted Root CA	http://rostelecom.ru/cdp/rootca_ssl_rsa2022.crt
Russian Trusted Sub CA	http://company.rt.ru/cdp/subca_ssl_rsa2022.crt
Russian Trusted Sub CA	http://reestr-pki.ru/cdp/subca_ssl_rsa2022.crt
Russian Trusted Sub CA	http://rostelecom.ru/cdp/subca_ssl_rsa2022.crt
TCI ECDSA B1 3-120 ECDSA	http://ca.cstls.ru/ecdsa-3-120.cer
TCI ECDSA B1 6-160	http://ca.cstls.ru/ecdsa-6-160.cer
TCI ECDSA ROOT A1	http://ca.cstls.ru/ecdsa-a1.crt

3. Условия использования

Пользователь обязан соблюдать приведенные ограничения при работе с Программой. ТЦИ оставляет за собой право изменить перечисленные ограничения в порядке, установленном в пользовательском соглашении.

Используя Программу, пользователь соглашается:

1. Использовать полученные данные только в законных целях;
2. Не допускать использования полученных данных в целях организации рассылки любой незапрашиваемой информации (спам) по адресам электронной почты, факсу, телефону;
3. Не производить массовых выборок информации.

Пользователю запрещено:

1. Изменять информацию, полученную с помощью Программы, в случае ее распространения в информационных целях;
2. Использовать полученную информацию с целью ее дальнейшего распространения в коммерческих целях.

3.1. Технические ограничения на использование

Ограничения количества запросов пользователя к Программе не установлены.

3.2. Ограничения на действия пользователей

Пользователь не вправе совершать действия, которые могут повлечь:

1. Нарушение функционирования оборудования и сети ТЦИ;
2. Нарушение предоставления ТЦИ услуг или ограничение возможности других пользователей сети Интернет в их получении;
3. Несанкционированный доступ к информационно-вычислительным и сетевым ресурсам ТЦИ;
4. Причинение либо угрозу причинения убытков иным пользователям и любым третьим лицам;
5. Введение в заблуждение третьих лиц относительно источника информации (отправителя сообщений любого характера, программ, запросов), если за источник информации выдается ТЦИ, коим он не является.

3.3. Квалификация действий пользователей и применяемые санкции

ТЦИ самостоятельно квалифицирует действия, совершаемые пользователем, как подпадающие или не подпадающие под ограничения, изложенные в п. 3.2 настоящего документа.

Техническая поддержка

Вопросы, возникающие в ходе работы с Программой, можно направлять по электронной почте на адрес: tech@mail.cstls.ru.