УТВЕРЖДЕН
RU.СГПВ.508110.001-01 93 01-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ СБОРА И ИССЛЕДОВАНИЯ ИНФОРМАЦИИ О ВЫДАВАЕМЫХ SSL-СЕРТИФИКАТАХ В СЕТИ ИНТЕРНЕТ

IoTSensor

Руководство пользователя

RU.СГПВ.508110.001-01 93 01

Листов 14

2021

Инв. № подл.	Подпись и дата	Взам. инв.№	Инв. № дубл.	Подпись и дата

АННОТАЦИЯ

Настоящий документ содержит сведения о назначении, условиях выполнения и порядке работы программного обеспечения для сбора и исследования информации о выдаваемых SSL-сертификатах в сети Интернет (далее – ПО IoTSensor, программа).

Операторы программы должны быть ознакомлены с настоящим руководством.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

Данный раздел содержит сведения о назначении, основных характеристиках и условиях применения ПО IoTSensor.

Программа предназначена для сбора сертификатов безопасности TLS. Сформированный объем данных в дальнейшем может использоваться для решения аналитических задач. Программа реализована на языке программирования Golang.

1.1. Сведения о назначении программы

Программа предназначена для сбора сертификатов безопасности, их хранения и поиска по базе данных.

Перечень функциональных возможностей программы:

- сбор сертификатов безопасности из открытых источников;
- сохранение сертификатов в СУБД ClickHouse;
- отображение web-интерфейса с функцией поиска по собранным данным.

Пользователь имеет возможность через web-интерфейс осуществлять просмотр сертификатов и поиск с использованием языка запросов SQL для СУБД ClickHouse.

Программа работает под управлением операционной системы Ubuntu Server версии 18.04 и выше.

1.2. Условия выполнения программы

Для работы с ПО IoTSensor необходимы следующие аппаратные и программные средства:

- операционная система Ubuntu Server версии 18.04 и выше;
- доступ к информационной сети Интернет;
- СУБД ClickHouse версии не ниже 20.12.3.3;
- 4 ядра центрального процессора (4 core CPU);
- 8 гигабайт оперативной памяти (8 GB RAM);
- 1 терабайт дискового пространства (1 TB HDD);

– 64-разрядная архитектура центрального процессора.

Климатические условия эксплуатации, при которых обеспечиваются заданные характеристики, должны удовлетворять требованиям, предъявляемым к техническим средствам в части условий их эксплуатации.

Конечный пользователь программы (оператор) должен обладать практическими навыками работы с графическим пользовательским интерфейсом операционной системы.

1.3. Ограничения области применения программы

Данная программа предназначена для работы в семействе операционных систем Ubuntu/Debian Server на вычислительных машинах серверного типа с 64-разрядной архитектурой. Программа не предназначена для работы под управлением Windows на персональных компьютерах, ноутбуках, планшетах.

Ограничения использования программы определяются требованиями, предъявляемыми при ее разработке программными средствами, а также требованиями компонентов, используемых для организации ее функционирования.

2. РАБОТА С ПРОГРАММОЙ

В настоящем разделе представлена последовательность действий, обеспечивающая запуск и работу программы.

ПО IoTSensor подключается к публичным реестрам сертификатов безопасности и собирает их с последующим сохранением в СУБД ClickHouse.

В программе присутствует web-интерфейс, с помощью которого оператор программы может производить поиск по базе данных сертификатов безопасности, в том числе с использованием синтаксиса языка запросов для СУБД ClickHouse.

2.1. Запуск программы

Функционал ПО IoTSensor предоставляется как web-сервис. Запуск программы не требуется.

2.2. Работа программы

ПО IoTSensor в непрерывном режиме вычитывает Certificate Transparency Log, накапливая буфер обмена с базой данных. При накоплении определенного количества записей в буфере обмена программа записывает их в базу данных, после чего буфер обмена очищается и цикл накопления и записи повторяется.

Пользователь может зайти в web-интерфейс программы и воспользоваться поиском по базе данных (см. рисунок 1).

Поиск осуществляется с использованием языка запросов СУБД ClickHouse.

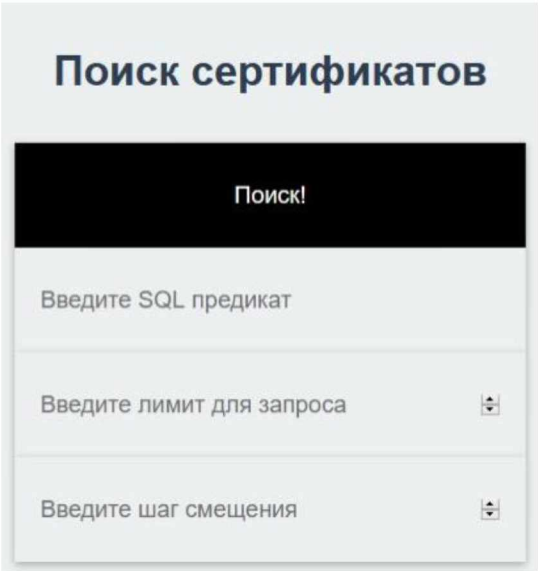

Рисунок 1 – Web-интерфейс программы

Сертификаты безопасности имеют определенную структуру данных, представляющую из себя набор пар ключ/значение. Описание полей приведено в таблице 1.

Таблица 1 – Описание полей сертификата безопасности для запросов

Наименование поля	Тип значения	Описание поля
Uuid	Строка	Уникальный идентификатор сертификата
cert_index	Целое число	Индекс сертификата в логе сертификатов
cert_link	Строка	Ссылка на необработанный сертификат
subject.cn	Строка	Имя сервера, защищенного с помощью сертификата
source.name	Строка	Имя лога, в котором был обнаружен сертификат
all_domains	Строка	Домены, принадлежащие данному сертификату
fingerprint	Строка	Уникальный отпечаток сертификата
not_after	Целое число	Верхняя граница времени действия сертификата (в миллисекундах)
not_before	Целое число	Нижняя граница времени действия сертификата (в миллисекундах)
subject.aggregated	Строка	Агрегированная информация о субъекте сертификата
timestamp	Временная метка (Timestamp)	Время сохранения сертификата в базу данных

Особое внимание необходимо уделить полям, в которых название состоит из двух слов, разделенных точкой. В запросе эти поля обрамляются двойными кавычками, например:

```
"extensions.basic_constraints"='CA:TRUE'
```

Далее перечислены примеры запросов, с помощью которых можно осуществлять поиск необходимой информации по этим данным.

Поиск сертификата для определенного домена (см. рисунок 2), к примеру "rem-ksa.com", осуществляется с помощью следующего запроса:

```
has(all_domains, 'rem-ksa.com')
```

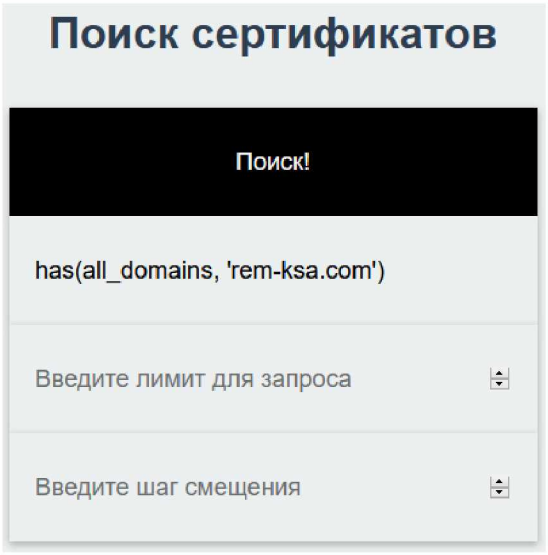

Рисунок 2 – Поиск сертификата для определенного домена

Результат выполнения запроса представлен на рисунке 3.

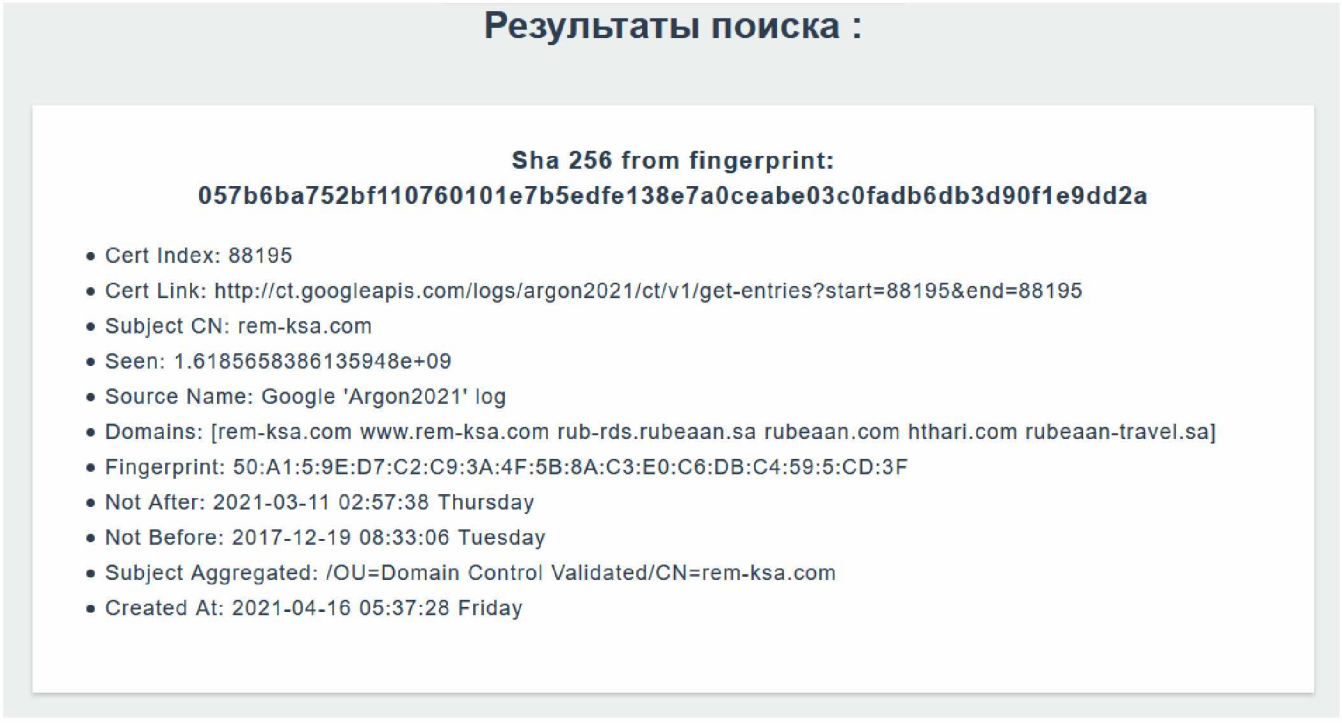

Рисунок 3 – Результат выполнения запроса "has(all_domains, ‘rem-ksa.com’)"

Просмотр всех корневых сертификатов (см. рисунок 4) реализуется запросом следующего вида:

```
"extensions.basic_constraints"='CA:TRUE'
```

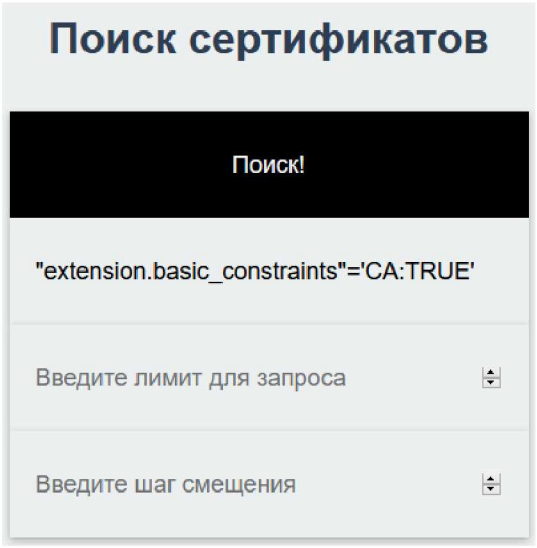

Рисунок 4 – Поиск всех корневых сертификатов

Для того чтобы получить список сертификатов, выданных субъектам определенной страны, к примеру США, необходимо выполнить следующий запрос:

```
"subject.c"='US'
```

Код страны указывается в соответствии с двухбуквенной международной системой обозначения стран ISO 3166-1 alpha-2 (см. рисунок 5).

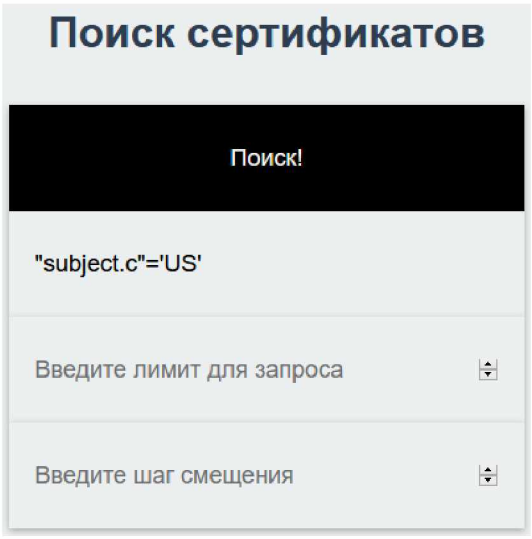

Рисунок 5 – Поиск сертификатов определенной страны

Фрагмент результата выполнения запроса приведен на рисунке 6.

Sha 256 from fingerprint: 00003e9ad9a1b97dc27532c8846e1142e56678b4eed6d3bb50561bb15a6295eb

- Cert Index: 52522
- Cert Link: http://ct.googleapis.com/logs/argon2021/ct/v1/get-entries?start=52522&end=52522
- Subject CN: 361d19f7-fae3-4702-a477-f2eb2258aa2b.cloudapp.net
- Seen: 1.6185657817427037e+09
- Source Name: Google 'Argon2021' log
- Domains: [361d19f7-fae3-4702-a477-f2eb2258aa2b.cloudapp.net azuregateway-361d19f7-fae3-4702-a477-f2eb2258aa2b-8ad9d7861c22.cloudapp.net]
- Fingerprint: 5C:F8:E3:11:DD:3F:1E:53:A6:72:1D:C8:57:80:97:7A:DB:88:4:DA
- Not After: 2021-01-09 07:00:00 Saturday
- Not Before: 2018-01-08 19:00:00 Monday
- Subject Aggregated: /C=US/ST=Washington/O=Microsoft Corporation/CN=361d19f7-fae3-4702-a477-f2eb2258aa2b.cloudapp.net
- Created At: 2021-04-16 05:36:30 Friday

Sha 256 from fingerprint: 0000a901e67fffbc7cd2d57d872786b68208b0a5c76222351c0cc02dc157d62c

- Cert Index: 98158
- Cert Link: http://ct.googleapis.com/logs/argon2021/ct/v1/get-entries?start=98158&end=98158
- Subject CN: cypress.calix.com
- Seen: 1.6185658504090629e+09
- Source Name: Google 'Argon2021' log
- Domains: [cypress.calix.com]
- Fingerprint: F9:FA:F0:CD:59:AF:91:A0:7A:A1:7A:F1:25:6B:ED:1B:C2:94:2D:6
- Not After: 2021-02-12 07:00:00 Friday
- Not Before: 2018-02-07 19:00:00 Wednesday
- Subject Aggregated: /C=US/ST=California/O=Calix, Inc./OU=IT/CN=cypress.calix.com
- Created At: 2021-04-16 05:37:33 Friday

Sha 256 from fingerprint: 00034b20e0dc5b7877b260960bf72076ba7463e4d072e4d53f8055c519ea482b

- Cert Index: 102981
- Cert Link: http://ct.googleapis.com/logs/argon2021/ct/v1/get-entries?start=102981&end=102981
- Subject CN: d50bb06f-7ba8-4223-8b43-764c95d61831.cloudapp.net
- Seen: 1.6185658565812373e+09
- Source Name: Google 'Argon2021' log
- Domains: [d50bb06f-7ba8-4223-8b43-764c95d61831.cloudapp.net azuregateway-d50bb06f-7ba8-4223-8b43-764c95d61831-352234d930b1.cloudapp.net]
- Fingerprint: C4:66:C:AF:73:4B:27:48:E0:5B:B5:DD:38:82:5C:87:55:1E:FC:A9
- Not After: 2021-02-04 07:00:00 Thursday
- Not Before: 2018-02-03 19:00:00 Saturday
- Subject Aggregated: /C=US/ST=Washington/O=Microsoft Corporation/CN=d50bb06f-7ba8-4223-8b43-764c95d61831.cloudapp.net
- Created At: 2021-04-16 05:37:47 Friday

Рисунок 6 – Фрагмент результата выполнения запроса "“subject.c”=’US’"

Получение информации о сертификатах, принадлежащих определенному субъекту, например компании Microsoft Corporation (см. рисунок 7), выполняется при помощи следующего запроса:

```
"subject.o"='Microsoft Corporation'
```

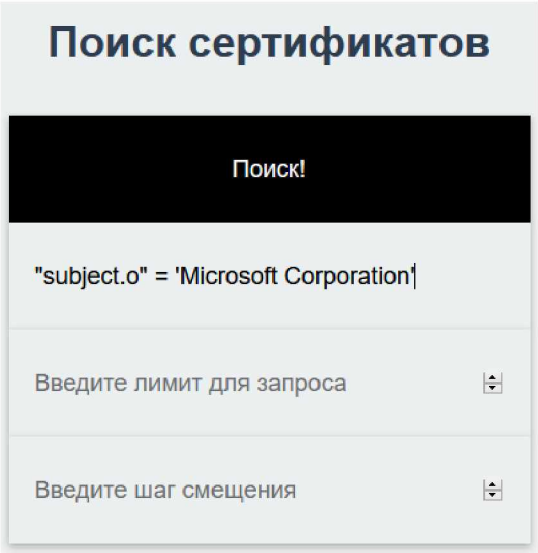

Рисунок 7 – Поиск сертификата, выданного определенной компании

Фрагмент результата выполнения запроса приведен на рисунке 8.

Результаты поиска :

Sha 256 from fingerprint:
0000d4526aed4858c18bd1e972294cb98b28809007d31e56a08cd5975db95733

- Cert Index: 401732
- Cert Link: http://ct.googleapis.com/logs/argon2021/ct/v1/get-entries?start=401732&end=401732
- Subject CN: enc.p.azurewebsites.windows.net
- Seen: 1.6185662167358701e+09
- Source Name: Google 'Argon2021' log
- Domains: [enc.p.azurewebsites.windows.net]
- Fingerprint: 2F:61:E5:99:73:EF:E8:62:CF:95:DA:73:54:BD:7E:C3:4:87:59:1E
- Not After: 2021-01-10 07:00:00 Sunday
- Not Before: 2019-01-09 19:00:00 Wednesday
- Subject Aggregated: /C=US/ST=Washington/O=Microsoft Corporation/CN=enc.p.azurewebsites.windows.net
- Created At: 2021-04-16 05:43:49 Friday

Sha 256 from fingerprint: 00019c87279dafe191c334ae68542b76c73f818e2f92659be09bd3d5d0cb33ab

- Cert Index: 561262
- Cert Link: http://ct.googleapis.com/logs/argon2021/ct/v1/get-entries?start=561262&end=561262
- Subject CN: a9b419b7-32d8-431f-8392-66ae7116b15d.vpn.azure.com
- Seen: 1.6185664127384e+09
- Source Name: Google 'Argon2021' log
- Domains: [a9b419b7-32d8-431f-8392-66ae7116b15d.vpn.azure.com azuregateway-a9b419b7-32d8-431f-8392-66ae7116b15d-7d467ab7be9a.vpn.azure.com]
- Fingerprint: F2:5:41:AC:91:96:21:D3:65:A9:89:63:C5:6A:9:1:FD:E9:CD:8E
- Not After: 2021-01-28 07:00:00 Thursday
- Not Before: 2019-01-27 19:00:00 Sunday
- Subject Aggregated: /C=US/ST=Washington/O=Microsoft Corporation/CN=a9b419b7-32d8-431f-8392-66ae7116b15d.vpn.azure.com
- Created At: 2021-04-16 05:46:56 Friday

Sha 256 from fingerprint:
00020a91dc1cead41605ebfd7d92bf8a54dbf5923e02a51c166c1628a1342455

- Cert Index: 469356
- Cert Link: http://ct.googleapis.com/logs/argon2021/ct/v1/get-entries?start=469356&end=469356
- Subject CN: enc.p.azurewebsites.windows.net
- Seen: 1.6185663000168 9e+09
- Source Name: Google 'Argon2021' log
- Domains: [enc.p.azurewebsites.windows.net]
- Fingerprint: F5:65:C9:5B:16:4D:E1:42:2B:2:FD:D1:1D:84:CE:A3:EF:A1:84:72
- Not After: 2021-01-16 07:00:00 Saturday
- Not Before: 2019-01-15 19:00:00 Tuesday
- Subject Aggregated: /C=US/ST=Washington/O=Microsoft Corporation/CN=enc.p.azurewebsites.windows.net
- Created At: 2021-04-16 05:45:01 Friday

Рисунок 8 – Фрагмент результата выполнения запроса

"“subject.o”=’Microsoft Corporation’"

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе приняты следующие сокращения:

IP	–	Internet Protocol;
TLS	–	Transport Layer Security;
ПО	–	программное обеспечение;
СУБД	–	система управления базами данных.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					