**Инструкция по эксплуатации**

**ПО "FINDLER"**

# **Аннотация**

Настоящий документ содержит информацию, необходимую для эксплуатации ПО "FINDLER", в том числе описание ПО, информацию о назначении ПО, описание основных компонентов платформы и действий, которые пользователь может выполнять при помощи платформы.

# **Содержание документа**

[Аннотация 2](#_6azvk1jd91d4)

[Содержание документа 3](#_ldxgxl3dcwxv)

[Описание и назначение ПО 4](#_n5qqbmh9pgg)

[Процесс запуска ПО 4](#_91iq87xx0qhn)

[Основные компоненты платформы 4](#_hhizzktu7zjp)

[Процесс завершения работы ПО 6](#_6r4guyfn0br4)

[Контакты 6](#_e42uovz4hwnc)

# **Описание и назначение ПО**

ПО “FINDLER” представляет собой ПО, позволяющее анализировать и выявлять уязвимые точки системы пользователя в реальном времени. ПО “FINDLER” представляет собой SaaS решение.

ПО позволяет:

- выявлять угрозы;

- изучать статистику уровня защищенности;

- анализировать информацию о текущих угрозах;

- выгружать информацию об угрозах;

- добавлять комментарии к угрозам;

- фильтровать угрозы;

- добавлять поддомены;

- работать с доверенными сетями;

- изучать отчеты и выгружать информацию по ним;

- осуществлять взаимодействие с ботом Findler через Телеграм.

# 

# **Процесс запуска ПО**

1. Для получения доступа к ПО потенциальный пользователь должен перейти на сайт https://new-lk.findlerbot.com/.
2. Ввести Email и пароль в соответствующие поля.
3. Нажать синюю кнопку “Войти”.

# **Основные компоненты платформы**

1. Окно авторизации.

С помощью окна авторизации (доступного по ссылке https://new-lk.findlerbot.com/) пользователь может войти в свой профиль. Для этого ему необходимо ввести свои логин и пароль и нажать кнопку “Войти”.

1. Главная страница.

На основной странице пользователь может перейти в разделы “Опасные ссылки по поддоменам”, “Опасные ссылки по ip”, “Опасные открытые порты”, “Хосты с CVE”, “Все хосты”.

Помимо этого, пользователь может изучить текущую статистику уровня защищенности - увидеть сколько обнаружено угроз и CVE, общую статистику уровня защищенности, CVE и показателей рисков по уровням (критический, высокий, средний, низкий, отсутствующий).

1. Меню настроек.

На главном экране, нажав на кнопку, расположенную в правом верхнем углу, пользователь может открыть меню настроек. С помощью него, пользователь может перейти в разделы “Доверенные сети” и “Отчет”, использовать функцию “Подключить Телеграм” или завершить работу ПО.

1. Раздел “Опасные ссылки по поддоменам”.

Перейти в данной раздел можно, нажав на ссылку “Опасные ссылки” и выбрав “По доменам”. В разделе “Опасные ссылки по поддоменам” пользователь может:

* изучить актуальные на сегодняшний день угрозы по ссылкам и оценить их уровень опасности;
* дать комментарии выбранным угрозам, нажав на кнопку с тремя точками справа от угрозы, введя комментарий в соответствующее поле и нажав после этого кнопку со стрелкой, направленной вверх;
* выгрузить список актуальных угроз, нажав на кнопку с изображением стрелки, направленной вниз;
* отфильтровать текущие угрозы, нажав на кнопку с ползунками и выбрав необходимые критерии.

1. Раздел “Опасные ссылки по IP”

Перейти в данной раздел можно, нажав на ссылку “Опасные ссылки” и выбрав “По IP” В разделе “Опасные ссылки по IP” пользователь может:

* изучить актуальные на сегодняшний день угрозы по ip и оценить их уровень опасности;
* дать комментарии выбранным угрозам, нажав на кнопку с тремя точками справа от угрозы, введя комментарий в соответствующее поле и нажав после этого кнопку со стрелкой, направленной вверх;
* выгрузить список актуальных угроз, нажав на кнопку с изображением стрелки, направленной вниз;
* отфильтровать текущие угрозы, нажав на кнопку с ползунками и выбрав необходимые критерии.

1. Раздел “Опасные открытые порты”.

В разделе Опасные открытые порты” пользователь может:

* изучить актуальные на сегодняшний день угрозы по открытым портам, поддоменам и серверам (и их ip) и оценить их уровень опасности;
* выгрузить список актуальных угроз, нажав на кнопку с изображением стрелки, направленной вниз;
* отфильтровать текущие угрозы, нажав на кнопку с ползунками и выбрав необходимые критерии.

1. Раздел “Хосты с CVE”.

В разделе “Обнаруженные CVE” пользователь может:

* изучить актуальные на сегодняшний день хосты с CVE и рекомендации по их устранению;
* дать комментарии CVE, нажав на кнопку с тремя точками справа от хоста и перейдя в подраздел “Комментарии”, введя комментарий в соответствующее поле и нажав после этого кнопку со стрелкой, направленной вверх;
* выгрузить список актуальных CVE, нажав на кнопку с изображением стрелки, направленной вниз;
* отфильтровать текущие CVE, нажав на кнопку с ползунками и выбрав необходимые критерии.

1. Раздел “Все хосты”.

В разделе “Все хосты” пользователь может:

* изучить актуальные на сегодняшний день хосты (по ip, поддоменам и портам);
* дать комментарии хосту, нажав на кнопку с тремя точками справа от хоста, введя комментарий в соответствующее поле и нажав после этого кнопку со стрелкой, направленной вверх;
* выгрузить список актуальных хостов, нажав на кнопку с изображением стрелки, направленной вниз;
* отфильтровать текущие хосты, нажав на кнопку с ползунками и выбрав необходимые критерии;
* нажав на “+” справа от раздела “Все хосты”, можно создать поддомен, введя в пустое поле поддомены и нажав синюю кнопку “Добавить”.

1. Раздел “Доверенные сети”.

В разделе “Доверенные сети” пользователь может:

* изучить существующие доверенные сети;
* удалять доверенные сети, нажав кнопку “крестик” справа от них;
* добавлять доверенные сети, нажав кнопку “Добавить” в разделе “Доверенные сети”, введя ip или подсеть и название и затем нажав кнопку “Добавить” снизу от поля.

1. Раздел “Отчет”.

В разделе “Отчет” пользователь может:

* изучать отчеты, содержащие информацию о возникших угрозах и CVE;
* выбирать временной период промежутка, нажав на поле “Период” и выбрав необходимый период времени;
* выгружать отчеты, нажав на кнопку со стрелкой вниз в перечне CVE.

1. Функция “Подключить Телеграм”

Функция “Подключить Телеграм” позволяет организовать взаимодействие с помощью мессенджера Телеграм.

# 

# **Процесс завершения работы ПО**

1. Пользователю необходимо перейти в меню настроек, а затем выбрать пункт “Выход” и нажать на него.
2. После чего Пользователь попадает в окно авторизации.

# **Контакты**

Контакты технической поддержки:

Email: [a.tomilov@rebrandy.co](mailto:a.tomilov@rebrandy.co);

[a.orlov@rebrandy.co](mailto:a.orlov@rebrandy.co);

[info@rebrandy.co](mailto:info@rebrandy.co).

Телефон: +79220020942