

FinalFrontier [Basisversion]

Nutzerdokumentation

31.01.2020

FinalFrontier ist ein Add-In für Outlook 2016 zur Verhinderung von (Spear-) Phishing Angriffen wie beispielsweise Emotet. Hierzu implementiert FinalFrontier verschiedene Ansätze zur Erkennung von schadhafte E-Mails, die vielen IT-Anwendern im Rahmen von Sensibilisierungsmaßnahmen nur schwer zu vermitteln sind.

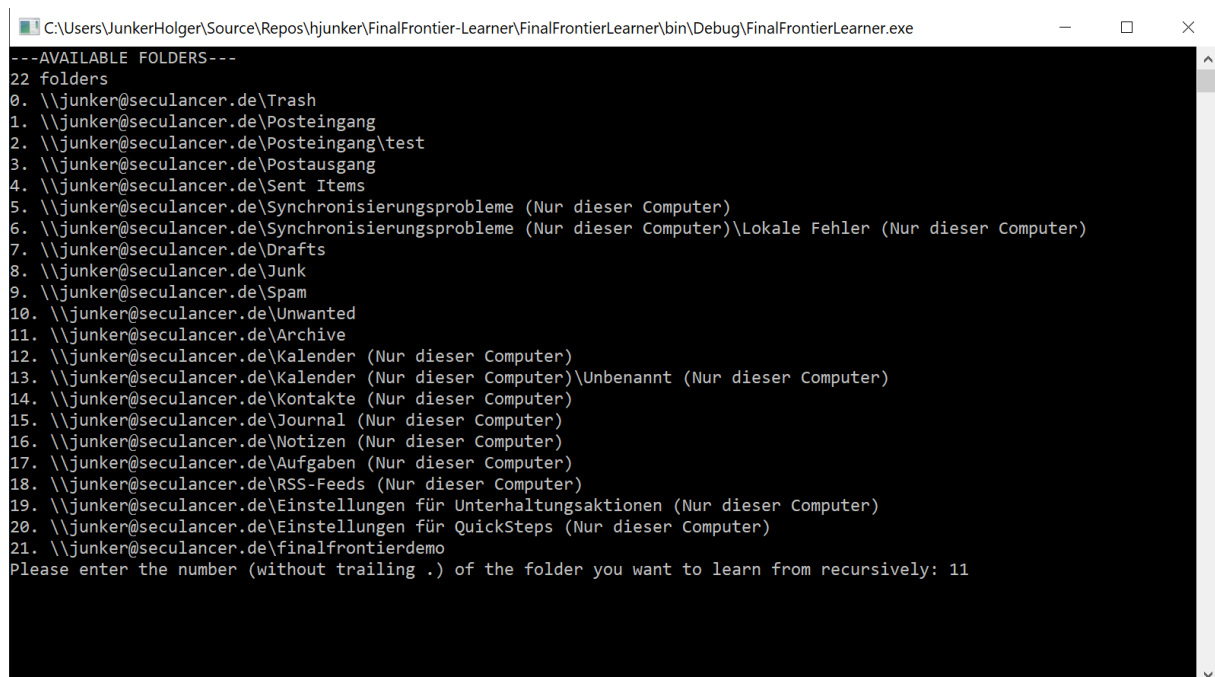
- Metadaten der E-Mail-Kommunikation, z.B. Absender (Name, Mailadresse)
- Links / URLs, z.B. bei verdächtigen Top Level Domains (TLD) oder Linkverkürzern
- Attachments / Dateianhänge, z.B. doppelte Dateierweiterungen (.doc.exe)

1 Anlernen der Kommunikationshistorie

Ein Teil der Detektionsmechanismen von FinalFrontier beruhen auf der Historie der E-Mail-Kommunikation. Hierzu werden statistische Auswertungen gemacht hinsichtlich der Absenderinformationen (Freitextname, Mailadresse aus Mail-Header, Mailadresse aus Envelope). Um dieses Feature zu nutzen, müssen Sie vor der Verwendung von FinalFrontier zunächst das Lerntool benutzen.

<https://github.com/hjunker/FinalFrontier-Learner>

Der Aufruf von FinalFrontierLearner.exe führt zunächst zu einer Übersicht der für den aktuellen Nutzer und FinalFrontier zugänglichen Mailstrukturen.



```
C:\Users\JunkerHolger\Source\Repos\hjunker\FinalFrontier-Learner\FinalFrontierLearner\bin\Debug\FinalFrontierLearner.exe
---AVAILABLE FOLDERS---
22 folders
0. \\junker@seculancer.de\Trash
1. \\junker@seculancer.de\Posteingang
2. \\junker@seculancer.de\Posteingang\test
3. \\junker@seculancer.de\Postausgang
4. \\junker@seculancer.de\Sent Items
5. \\junker@seculancer.de\Synchronisierungsprobleme (Nur dieser Computer)
6. \\junker@seculancer.de\Synchronisierungsprobleme (Nur dieser Computer)\Lokale Fehler (Nur dieser Computer)
7. \\junker@seculancer.de\Drafts
8. \\junker@seculancer.de\Junk
9. \\junker@seculancer.de\Spam
10. \\junker@seculancer.de\Unwanted
11. \\junker@seculancer.de\Archive
12. \\junker@seculancer.de\Kalender (Nur dieser Computer)
13. \\junker@seculancer.de\Kalender (Nur dieser Computer)\Unbenannt (Nur dieser Computer)
14. \\junker@seculancer.de\Kontakte (Nur dieser Computer)
15. \\junker@seculancer.de\Journal (Nur dieser Computer)
16. \\junker@seculancer.de\Notizen (Nur dieser Computer)
17. \\junker@seculancer.de\Aufgaben (Nur dieser Computer)
18. \\junker@seculancer.de\RSS-Feeds (Nur dieser Computer)
19. \\junker@seculancer.de\Einstellungen für Unterhaltungsaktionen (Nur dieser Computer)
20. \\junker@seculancer.de\Einstellungen für QuickSteps (Nur dieser Computer)
21. \\junker@seculancer.de\FinalFrontierdemo
Please enter the number (without trailing .) of the folder you want to learn from recursively: 11
```

Der gewählte Ordner (z.B. Mailablage) wird rekursiv gescannt, um eine statistische Datengrundlage für die Bewertung der Kommunikationshistorie zu erstellen.

Achtung: Bitte wählen Sie hier keine Ordner, die potentiell schadhafte Emails enthalten, also z.B. Posteingang, Spam-Ordner, Spam, Junk, etc. Einige dieser Ordner sind vom Lernprozess ausgenommen.

```
C:\Users\JunkerHolger\Source\Repos\hjunker\FinalFrontier-Learner\FinalFrontierLearner\bin\Debug\FinalFrontierLearner.exe
Skipping folder \\junker@seculancer.de\Posteingang\test
Skipping folder \\junker@seculancer.de\Postausgang
Skipping folder \\junker@seculancer.de\Sent Items
Skipping folder \\junker@seculancer.de\Synchronisierungsprobleme (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\Synchronisierungsprobleme (Nur dieser Computer)\Lokale Fehler (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\Drafts
Skipping folder \\junker@seculancer.de\Junk
Skipping folder \\junker@seculancer.de\Spam
Skipping folder \\junker@seculancer.de\Unwanted
learning from \\junker@seculancer.de\Archive
Skipping folder \\junker@seculancer.de\Kalender (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\Kalender (Nur dieser Computer)\Unbenannt (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\Kontakte (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\Journal (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\Notizen (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\Aufgaben (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\RSS-Feeds (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\Einstellungen für Unterhaltungsaktionen (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\Einstellungen für QuickSteps (Nur dieser Computer)
Skipping folder \\junker@seculancer.de\FinalFrontierdemo
learned 75 mails recursively from, starting in \\junker@seculancer.de\Archive.
dictionary files have been written to C:\Users\JunkerHolger\Documents... keep these files where they are so that FinalFrontier can find them.
---VERIFYING---
dict-sender-name.bin: 25 entries
dict-sender-email.bin: 25 entries
dict-sender-combo.bin: 28 entries
[hit key to exit]
```

Unter Dokumente (je nach Version ggfs. Unterordner FinalFrontier) finden sich nun die lokal gelernten Dateien.

Dieser PC > Dokumente			
<input type="checkbox"/>	Name	Änderungsdatum	Typ
	dict-sender-combo.bin	29.01.2020 13:11	Virtual CloneDrive
	dict-sender-email.bin	29.01.2020 13:11	Virtual CloneDrive
	dict-sender-name.bin	29.01.2020 13:11	Virtual CloneDrive

Diesen Lernprozess sollte man automatisiert – z.B. als scheduled task – regelmäßig erfolgen lassen. Zukünftige Versionen von FinalFrontier werden sukzessive lernen.

2 Installation

Ein fertiges Softwarepaket kann von der GitHub-Projektseite

<https://github.com/hjunker/FinalFrontier>

heruntergeladen werden. Alternativ kann auf Basis des öffentlichen Quellcodes eine individuelle Version erstellt werden.

Search or jump to... Pull requests Issues Marketplace Explore

hjunker / FinalFrontier Private

Unwatch 2 Star 0 Fork 1

Code Issues 0 Pull requests 0 Actions Projects 0 Security Insights Settings

Outlook Add-In to detect and prevent (spear-) phishing attacks such as e.g. emotet. Edit

Manage topics

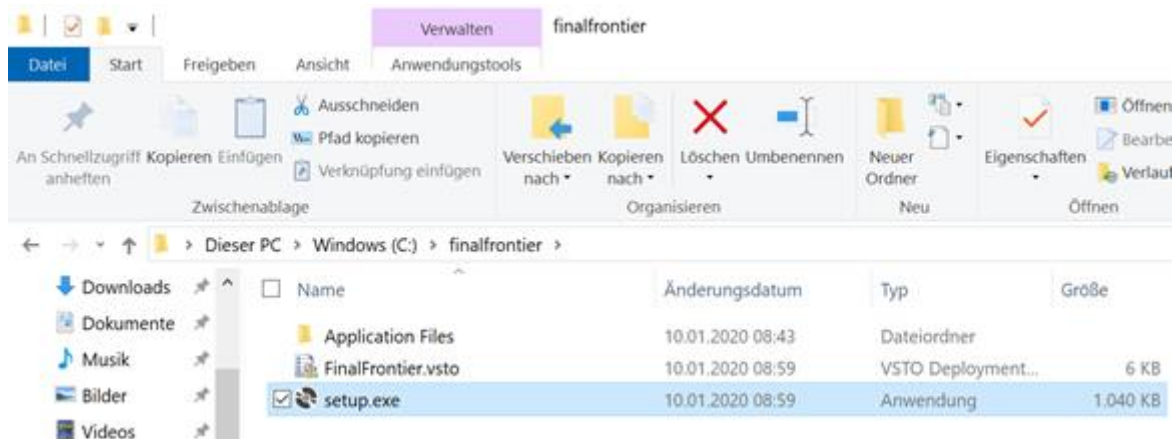
96 commits 2 branches 0 packages 0 releases

Branch: master New pull request Create new file Upload files Find file Clone or download

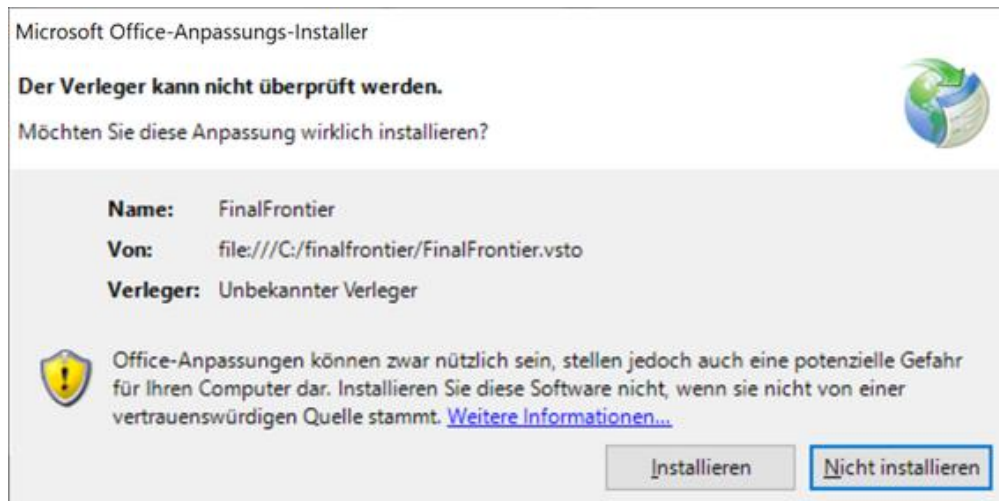
hjunker for testing only Latest commit 797f258 now

File	Commit Message	Time Ago
FinalFrontier	addition to message when app.config not readable; length of freemaile...	3 hours ago
FinalFrontierLearnLib	add external learning dll	19 hours ago
FinalFrontierUnitTest	Refactor CheckKeywords and CheckBadTld with Linq	3 days ago
.gitattributes	GITIGNORE und GITATTRIBUTES hinzufügen.	24 days ago
.gitignore	add external learning dll	19 hours ago
FinalFrontier.sln	add external learning dll	19 hours ago
README.md	Update README.md	2 minutes ago
finalfrontier-testbuild.zip	for testing only	now

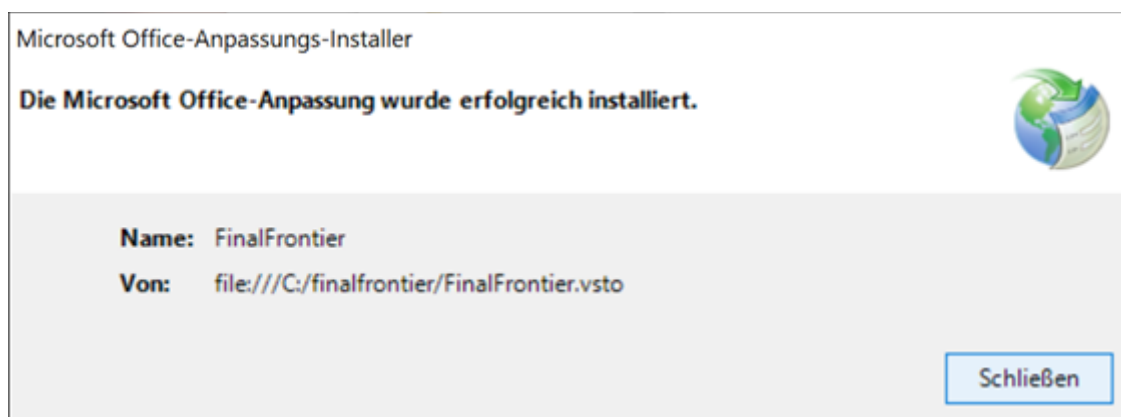
Entpacken Sie das zip-Archiv in einen Ordner Ihrer Wahl, z.B. C:\finalfrontier. Anschließend starten Sie die setup.exe mit einem Doppelklick



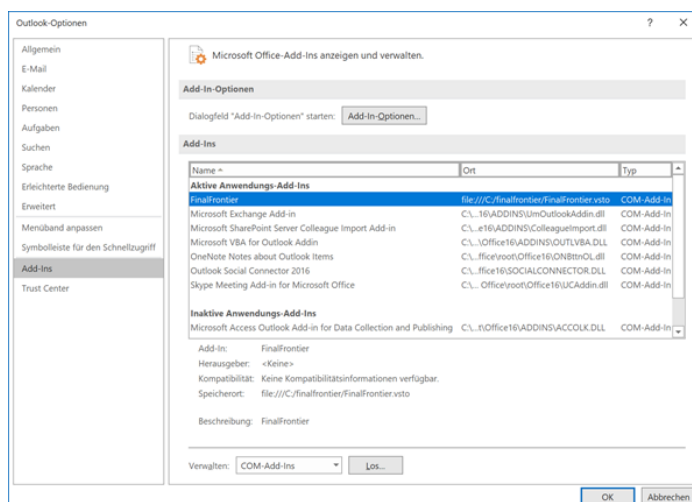
Nun müssen Sie die Installation durch Klick auf den Button "Installieren" bestätigen.



Die weitere Installation verläuft automatisch und sollte nur wenige Sekunden benötigen. Abschließend sollten Sie die folgende Meldung erhalten:



In Outlook sehen Sie unter Einstellungen nun auch das FinalFrontier AddIn.



3 Benutzung

Während Sie Outlook verwenden, prüft FinalFrontier kontinuierlich im Hintergrund auf verdächtige Emails. Dies wird immer dann initiiert, wenn Sie eine Mail anklicken bzw. öffnen. Wenn aufgrund der

geprüften Indikatoren der Verdacht auf eine schadhafte E-Mail vorliegt, wird eine Warnung angezeigt.

FinalFrontier - Security Info

Warnung!

Diese Mail könnte schadhafte sein.

Score: -130

-20

Receive-Freemailer

me.com

from cm-^

-40

Address-NotContained

Empfängermailadresse ist weder in den Empfängern noch im CC

junker@

-10

Meta-NameNew

Der Name (Freitext) des Absenders ist neu

Höhn, Al

< >

Header-Informationen

You have a problem?

Close

FinalFrontier - Security Info

Warnung!

Diese Mail könnte schadhafte sein.

Score: -190

-20

Link-Keyword

scan

<https://higashinakano->

-20

Receive-Freemailer

cs.com

from mail.c.flccebu-124

-20

Receive-Freemailer

cs.com

(202.218.155.1[...]

from sgp-smtp2.fastlog

Header-Informationen

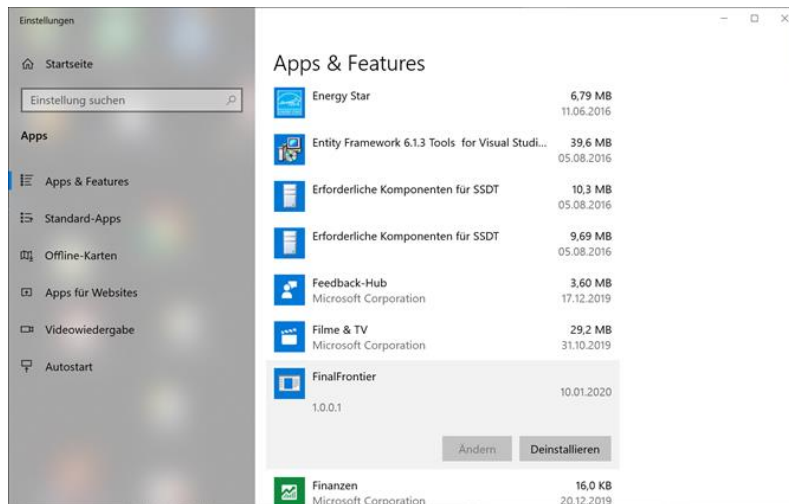
You have a problem?

Close

Bitte prüfen Sie im Falle einer solchen Warnung auf Grundlage der in der Warnung enthaltenen Ausführungen die E-Mail genau. Im Zweifelsfall kontaktieren Sie Ihren IT-Betrieb oder sonstige geeignete Dritte. Klicken Sie im Zweifelsfall weder auf Links / URLs in der E-Mail noch öffnen Sie an der E-Mail enthaltene Anhänge / Attachments.

4 Deinstallation

Die Deinstallation von FinalFrontier erfolgt auf die gleiche Weise wie bei anderen Programmen auch unter Systemsteuerung / Programme / Programm deinstallieren. Die dortige Suche ermöglicht ein schnelles Finden von FinalFrontier in der Liste der installierten Anwendungen.



Wählen Sie 'Deinstallieren' und bestätigen Sie wie folgt mit 'Ok'.



Die vollständige Deinstallation ist damit abgeschlossen. Prüfen Sie bitte, ob die Dateien mit Informationen zur Mail-Historie (Lernverfahren) gelöscht wurden. Diese befinden sich in ihrem persönlichen Ordner unter Dokumente. Löschen Sie die Dateien ggfs. manuell.

5 Datenschutzhinweise

Einige der Detektionsmechnismen verwenden statistische Daten über die Mailhistorie (vgl. Abschnitt 'Anlernen der Kommunikationshistorie'). Diese Daten werden ausschließlich unter ihrem Nutzerprofil verarbeitet und gespeichert. Es werden keine dieser Daten über das Netz übertragen.

Prinzipiell gilt: FinalFrontier kommuniziert nicht über das Internet.