



Anleitung ESET Bedrohung erkannt – in Log-Datei nachschauen

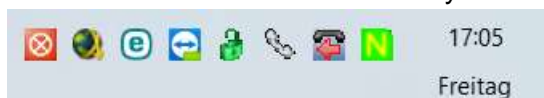
Der Virens Scanner ESET bringt von Zeit zu Zeit solche Meldungen am Bildschirm



Das ist z.B. die Information, dass Outlook eine Email empfangen hat, die eine infizierte Datei enthielt.

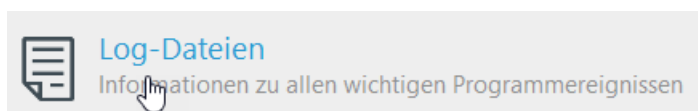
Diese Information kann man nachträglich nochmals anschauen.

Klicken Sie dazu zuerst auf das Symbol in der Taskleiste rechts bei der Uhr



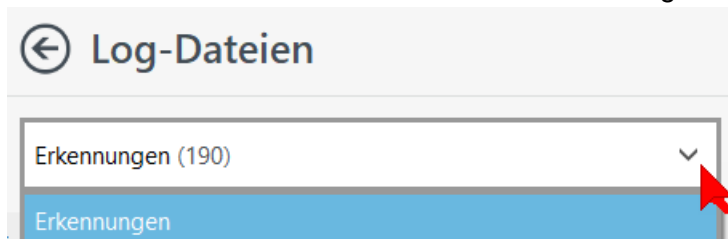
Hier klicken , dann im linken Menü auf  Tools

Dann noch  Weitere Tools und zuletzt auf



klicken

Nun sehen Sie eine Übersichtsliste aller Erkennungen





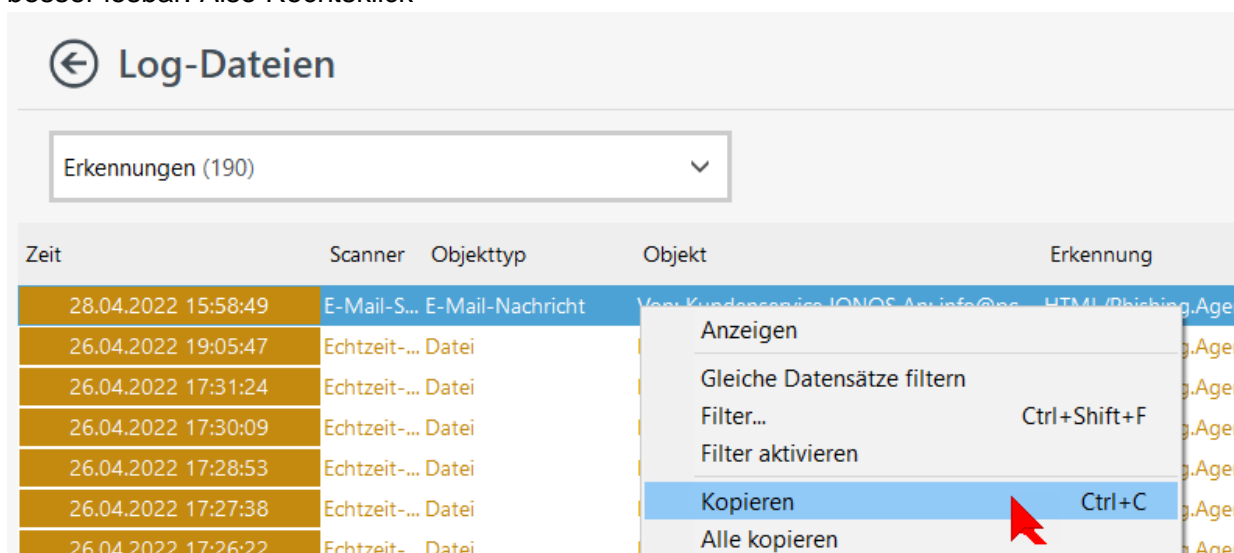
In unserem Beispiel



Zeit	28.04.2022 15:58:49
Scanner	E-Mail-Schutz - Outlook
Objekttyp	E-Mail-Nachricht
Objekt	Von: Kundenservice IONOS An: info@pc-blitzhelfer.de Betreff [SPAM] Ihre Vertragsbestätigung 17268944
Erkennung	HTML/Phishing.Agent.CJZ Trojaner
Aktion	Enthielt infizierte Datei(en)
Benutzer	PC-1-SSD-M2-BIG\PCB
Information	Ein Ereignis ist aufgetreten, als die folgende Anwendung eine E-Mail empfangen hat: C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE.
Hash	
Zuerst hier gesehen	

Von: Kundenservice IONOS An: info@pc-blitzhelfer.de
Betreff [SPAM] Ihre Vertragsbestätigung 17268944

Mit Rechtsklick kann man diese Information in die Zwischenablage kopieren, dann ist alles besser lesbar. Also Rechtsklick



Bringt diese Information in die Zwischenablage.



Zeit;Scanner;Objektyp;Objekt;Erkennung;Aktion;Benutzer;Information;Hash;Zuerst hier gesehen

28.04.2022 15:58:49;E-Mail-Schutz - Outlook;E-Mail-Nachricht;Von: Kundenservice IONOS

An: info@pc-blitzhelfer.de Betreff [SPAM] Ihre Vertragsbestätigung 17268944

;HTML/Phishing.Agent.CJZ Trojaner;Enthielt infizierte Datei(en);PC-1-SSD-M2-BIG\PCB;Ein Ereignis ist aufgetreten, als die folgende Anwendung eine E-Mail empfangen hat: C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE.;;

In der Liste sind evtl. weitere Einträge, z.B.

12.04.2022 09:50:59	IMAP-FIL... E-Mail-Nachricht	Von: EU Business Register <register@eb... PDF/EuBusiness potentiell unerwünschte... Enthielt infizierte Datei(en)
08.04.2022 22:51:54	HTTP-FIL... Datei	https://nippyshare.com/v/8604e7 HTML/ScriptInject.B Trojaner Verbindung getrennt
11.03.2022 13:48:25	IMAP-FIL... E-Mail-Nachricht	Von: pcblitzhelfer.de Security <appleid@... HTML/Phishing.Agent.AUW Trojaner Enthielt infizierte Datei(en)
08.03.2022 12:33:33	IMAP-FIL... E-Mail-Nachricht	Von: Adela Martinez Cespedes <cesadela... HTML/Fraud.CX Trojaner Enthielt infizierte Datei(en)

04.03.2022 04:25:07	HTTP-FIL... Datei	https://nippysshare.com/v/141190 HTML/ScriptInject.B Trojaner Verbindung getrennt
---------------------	-------------------	--

Z.B.

12.04.2022 09:50:59	IMAP-FIL... E-Mail-Nachricht	Von: EU Business Register <register@eb... PDF/EuBusiness potentiell unerwünschte... Enthielt infizierte Datei(en)
---------------------	------------------------------	---

Eine weitere infizierte Email

08.04.2022 22:51:54	HTTP-FIL... Datei	https://nippysshare.com/v/8604e7 HTML/ScriptInject.B Trojaner Verbindung getrennt
---------------------	-------------------	--

Hier wurde eine Webseite geblockt

11.03.2022 13:48:25	IMAP-FIL... E-Mail-Nachricht	Von: pcblitzhelfer.de Security <appleid@... HTML/Phishing.Agent.AUW Trojaner Enthielt infizierte Datei(en)
08.03.2022 12:33:33	IMAP-FIL... E-Mail-Nachricht	Von: Adela Martinez Cespedes <cesadela... HTML/Fraud.CX Trojaner Enthielt infizierte Datei(en)

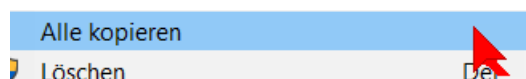
Nochmals 2 infizierte Emails

04.03.2022 04:25:07	HTTP-FIL... Datei	https://nippysshare.com/v/141190 HTML/ScriptInject.B Trojaner Verbindung getrennt
---------------------	-------------------	--

Nochmals die selbe Webseite

Man kann auch alle Inhalte in die Zwischenablage kopieren und von dort in den Editor.

Über den Rechtsklick



Die erkannten infizierten Daten werden von ESET in die Quarantäne verschoben.

Sie sind dort vor jeglichem Zugriff geschützt.

Diese Liste finden Sie dann dort mit

Hier klicken , dann im linken Menü auf  Tools

Dann noch  Weitere Tools und zuletzt auf  Quarantäne
Sicher gespeicherte infizierte Dateien

26.04.2022 14:34:12	E-Mail-Anlage: Rechnung_2022-04-25_100103020291_V36334466.html	Von: Rechnungsteile IONOS An: info@pc-blitzhelfer.de Betreff [SPAM] 39,7 kB
25.04.2022 19:05:57	D:\Eigene Dateien\Documents\Lockeeen\Dieter\Index\Attachments\637865103378276004_Rechnung_2022-04-25_100103020291_V3633...39,7 kB	