



Anleitung ESET Bedrohung erkannt – in Log-Datei nachschauen

Der VirensScanner ESET bringt von Zeit zu Zeit solche Meldungen am Bildschirm

The screenshot shows the ESET Internet Security software interface. A prominent red warning box on the left displays the message "Bedrohung entfernt" (Threat removed) in bold red text. Below it, it says "Eine Bedrohung (LNK/TrojanDownloader.Agent.FN) wurde in einer Datei gefunden, auf die Werbung Microsoft Outlook zugreift." (A threat (LNK/TrojanDownloader.Agent.FN) was found in a file that accesses Microsoft Outlook advertising.) To the right, there is a list of emails from various senders like "Manuel Klo", "KRAUS GHE", and "kimkarrer@". At the bottom of the main window, it says "Die Datei wurde gesäubert." (The file was cleaned.)

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

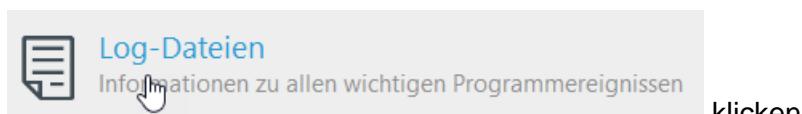
Diese Information kann man nachträglich nochmals anschauen.

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

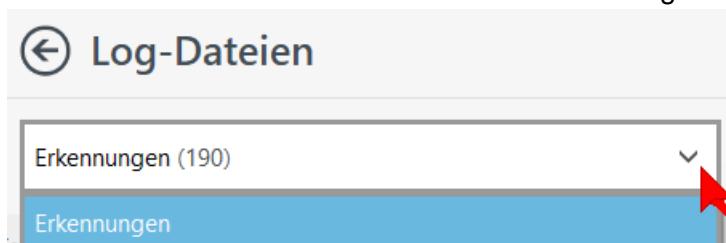


Hier klicken , dann im linken Menü auf Tools

Dann noch Weitere Tools und zuletzt auf



Nun sehen Sie eine Übersichtsliste aller Erkennungen





In unserem Beispiel

The screenshot shows the ESET Internet Security interface. In the center, there's a table titled "Log-Dateien" with columns: Zeit, Scanner, Objekttyp, Objekt, and Erkennung. One row is highlighted in yellow, representing the detected threat. A red arrow points to this row. To the right of the table, a detailed information pane displays the following details:

Zeit	28.04.2022 15:58:49
Scanner	E-Mail-Schutz - Outlook
Objekttyp	E-Mail-Nachricht
Objekt	Von: Kundenservice IONOS An: info@pc-blitzhelper.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-blitzhelper.de
Betreff [SPAM] Ihre Vertragsbestätigung 17268944

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

The screenshot shows the ESET Log-Dateien interface with a context menu open over the highlighted row. The menu items are: Anzeigen, Gleiche Datensätze filtern, Filter..., Filter aktivieren, Kopieren (selected), and Alle kopieren. A red arrow points to the "Kopieren" option. The menu has a blue background for the selected item.

Bringt diese Information in die Zwischenablage.



Zeit;Scanner;Objekttyp;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	Vom: EU Business Register <register@ebr... PDF/EuBusiness potenziell unerwünschte... Enthielt infizierte Dateien	
08.04.2022 22:51:54	HTTP-Fil... Datei	https://nippyshare.com/v/8604e7	HTML/Scinject.B Trojaner
			Verbindung getrennt
11.03.2022 15:48:28	IMAP-Fil... E-Mail-Nachricht	Vom: pcblitzhelfer.de Security <appleid@... HTML/Phishing.Agent.AUW Trojaner	Enthielt infizierte Dateien!
08.03.2022 12:33:33	IMAP-Fil... E-Mail-Nachricht	Von: Adela Martinez Cespedes <casadela... HTML/Fraud.CX Trojaner	Enthielt infizierte Dateien!
04.03.2022 04:25:07	HTTP-Fil... Datei	https://nippyshare.com/v/14f190	HTML/Scinject.B Trojaner
			Verbindung getrennt

Z.B.

12.04.2022 09:50:59 IMAP-Fil... E-Mail-Nachricht Vom: EU Business Register <register@ebr... PDF/EuBusiness potenziell unerwünschte... Enthielt infizierte Dateien)

Eine weitere infizierte Email

08.04.2022 22:51:54 HTTP-Fil... Datei <https://nippyshare.com/v/8604e7> HTML/Scinject.B Trojaner Verbindung getrennt

Hier wurde eine Webseite geblockt

11.03.2022 15:48:25 IMAP-Fil... E-Mail-Nachricht Von: pcblitzhelfer.de Security <appleid@... HTML/Phishing.Agent.AUW Trojaner

08.03.2022 12:33:33 IMAP-Fil... E-Mail-Nachricht Von: Adela Martinez Cespedes <casadela... HTML/Fraud.CX Trojaner

Nochmals 2 infizierte Emails

04.03.2022 04:25:07 HTTP-Fil... Datei <https://nippyshare.com/v/14f190> HTML/Scinject.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: Rechnungsstelle IONOS An: info@pc-blitzhelfer.de Betreff [SP... 39.7 kB
25.04.2022 19:05:37	D:\Eigene Dateien\Documents\Lockeen\Dieter\Index\Attachments\63786510337827604_Rechnung_2022-04-25_100103020291_V3633... 39.7 kB