STEP 01

エモテットの感染が発覚した場合、感染が疑われる 端末をネットワークから、また、感染が疑われる端末 が繋がっているネットワークを外部のインターネット から遮断しましょう。

発覚した時期が感染から間もない場合には、他の端末に感染を広げてしまうリスクを下げることができるため、確実に実施しましょう。



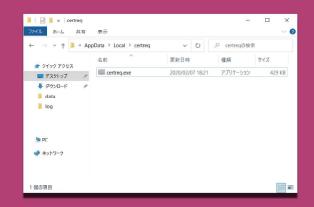
STEP 02

タスクマネージャーを起動し、詳細タブから実行結果に表示されている「プロセス ID」を選択し、 タスクの終了を選択します。

プロセス バフォーマンス アブリの履歴	スタートアツブ	ユーザー	詳細	サービス			
名前	PID	状態		CPU	メモリ (アクテ	UAC の仮想化	
 Аррисальні тата налажена 	5340	実行中		00	4,216 K	無効	
 Outdomnsteet 	6472	実行中		00	12,436 K	不許可	
Fill harrowsen_harrowsen	6184	実行中		00	3,208 K	無効	
@certreq.exe	8468	実行中		00	3,548 K	有効	
The state of the s	1696	実行中		00	504 K	無効	
■ Compat lellhærer eve.	960	実行中		00	80 K	不許可	
Conhasticka	9952	実行中		00	88 K	不許可	
Conhost exe	2892	実行中		00	6,936 K	無効	
wand notherne	1680	実行中		00	248 K	不許可	
The street rate	432	実行中		00	484 K	小計可	
The state of the s	520	実行中		00	680 K	不許可	
2 d lenerseve	5556	実行中		00	5,364 K	無効	
■ dilhostexe	7960	実行中		00	132 K	無効	
 dumpcsp.exe 	9996	実行中		00	476 K	不許可	
■ stvenses e	324	実行中		00	43,244 K	無効	
en dance enc	5876	実行中		01	36,876 K	無効	

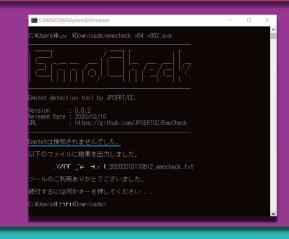
STEP 03

実行結果に表示されている「イメージパス」のうちフォルダ部をエクスプローラーで開き、表示されている exe を削除します。



STEP 04

再度 EmoCheck を実行し、Emotet を検知しない ことを確認ください。



STEP 05

感染した端末が利用していたメールアカウントなどのパスワード変更。

横断的侵害で組織内に感染を広げる能力を持っているため、添付ファイルを開いた端末だけでなく、他の端末も併せて調査を実施する。

