step 01 下記 GitHub の JPCERT/CC ページよりツール 「EmoCheck」をダウンロードし、感染が疑われる 端末へコピーしてください。使用している端末に応 じて emocheck_x86.exe または emocheck_x64.exe を使用ください (不明な場合は emocheck_x86.exe を使用ください)。

Jug lix	
Fixed a crash bug when executing with SYSTEM privileges	
emocheck_v2.1.1_x86.exe	
MD5 : 2092f131f615161187a4dd4446c3e654	
SHA256: 46beb191a16b752a9a5bebacf73ad1677fcf1d16e8d869f646957fd1218e9ee2	
emocheck_v2.1.1_x64.exe	
MDF - 367644-36-7-031-00-000-014440-3647	
MD5: df/611dfe/c21b50e606C5b1442adf1/	
SHA256: 1307b5c1da177de1b7fa0237a05813f883e60a936783a7e298f007fa64814ce0	
MUS : a1/01 l dte/c2 l b30e000C301442adt1/ SHA256: 1307b5c1da177de1b7fa0237a05813f883e60a936783a7e298f007fa64814ce0	
MID:::utrol:utr/cz.ubs/ebo0e501442/attr/ SHA256:1307b5c1da177de1b7fa0237a05813883660a936783a7e2981007fa64814ce0	
MD3: 01701 018722 10306000500 14424011/ SHA256: 1307b5c1da177de1b7fa0237a05813483e60a936783a7e2981007fa64814ce0	
NUD : dtr 0 i dter/cz i bosecoocso i 442.adti / SHA255: 1307b5c1da177de1b7ta0237a05813883e60a936783a7e298007fa64814ce0	2.25 N

https://github.com/JPCERTCC/EmoCheck/releases

step 02 感染が疑われる(主に通常その端末を使用してい るユーザ)でログインし、ツールをダブルクリック し実行してください。



STEP 03 感染してた場合 右のように「Emotet のプロセスが見つかりました」と表示されていた場合には、Emotet に感染しています。

C#WINDOWS¥system32¥cmd.exe	1	×
C:#Users##Downloads>emocheck_x64_v002.exe		^
Version : 0.0,2 Netesase Date : 2000/02/10 ReL : https://github.com/VPCERTCC/EmoCheck		
111 Emotet 1巻句 プロセス名 : certreq.exe プロケス11 : 8.468 イメージバス : C:Wibersternet WapDataWilcoslWcertreqYcertreq.exe		
motetのブロセスが見つかりました。 不蕾なイメージバスの表行ファイルを隔離/削除してください。		
以下のファイル(に結果を出力しました。		
.4 hostname20200207183150_emocheck.txt		
統行するには何かキーを押してください		
D: ¥Users¥		

STEP 03 イメージパスが表示されない場合は Emotet が管 理者権限で動作している可能性があります。 EmoCheck を管理者権限で実行してください。 確認結果は実行フォルダに txt ファイルとしても出 力されます。

	J: 2020-02-07 18:31:59		
結果] molelを検知しまし ****	tc.		
詳細」 プロセス名 プロセスID イメージパス	: certreq.exe : 8468 : C:¥Users¥ kı i ¥AppData¥Local¥certreq¥certreq.exe		



次のように「Emotet は検知されませんでした」 と表示されていた場合には、Emotet に感染してい ません。

