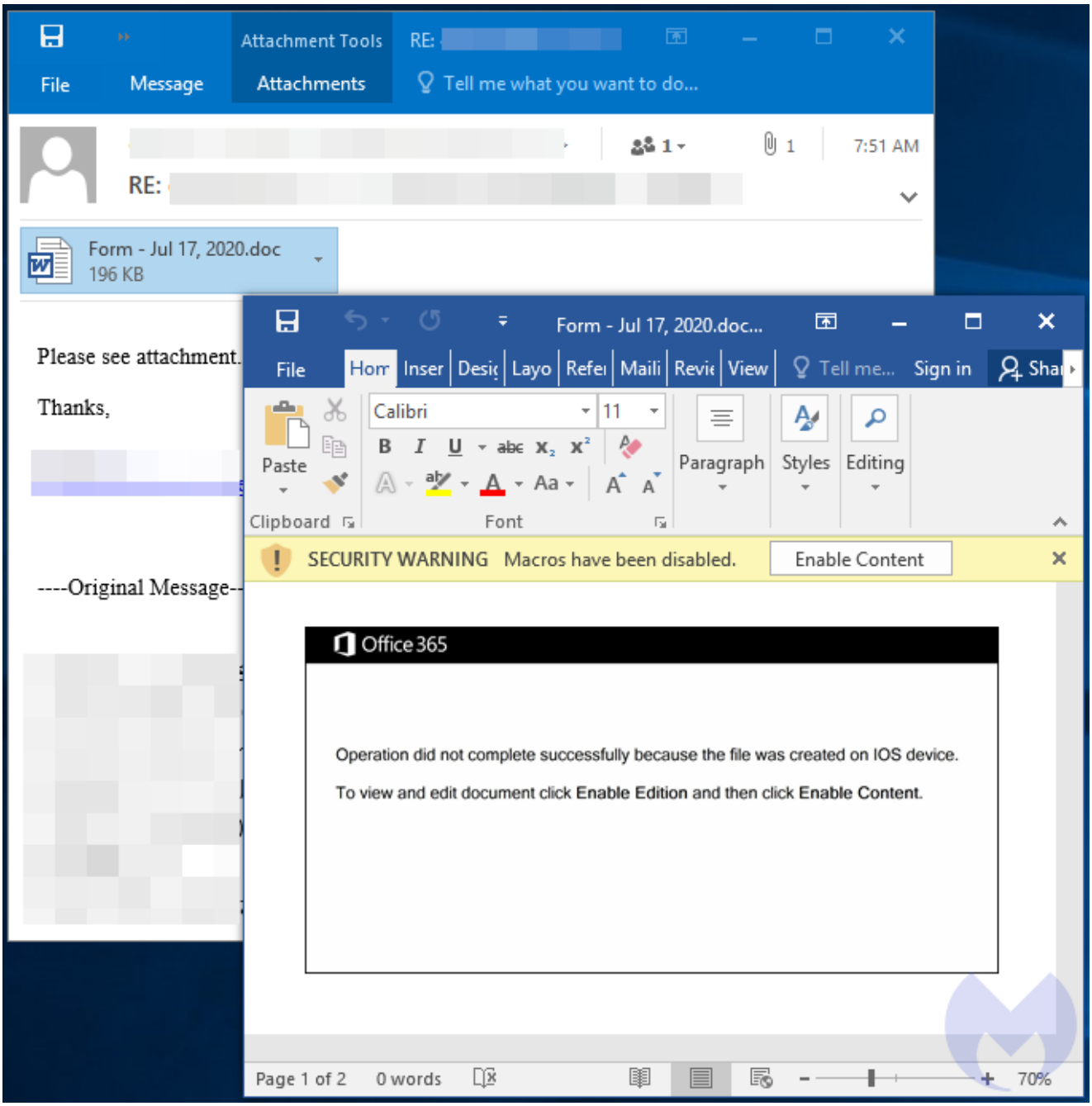
It’s baaaack: Public cyber enemy Emotet has returned

blog.malwarebytes.com/trojans/2020/07/long-dreaded-emotet-has-returned/

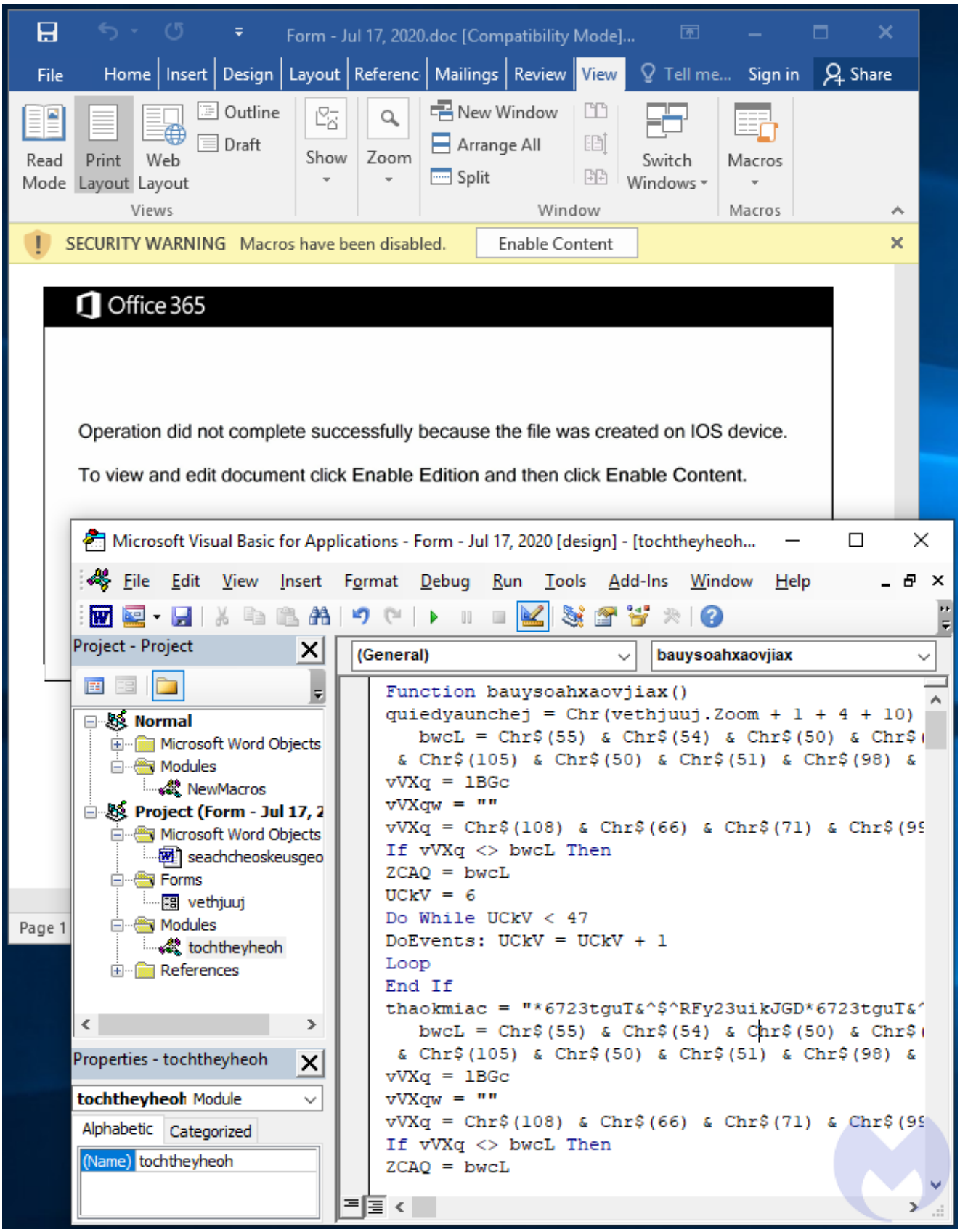
Threat Intelligence Team July 17, 2020

It was never a question of “if” but “when”. After five months of absence, the dreaded Emotet has returned. Following several false alarms over the last few weeks, a spam campaign was first spotted on July 13 showing signs of a likely comeback.

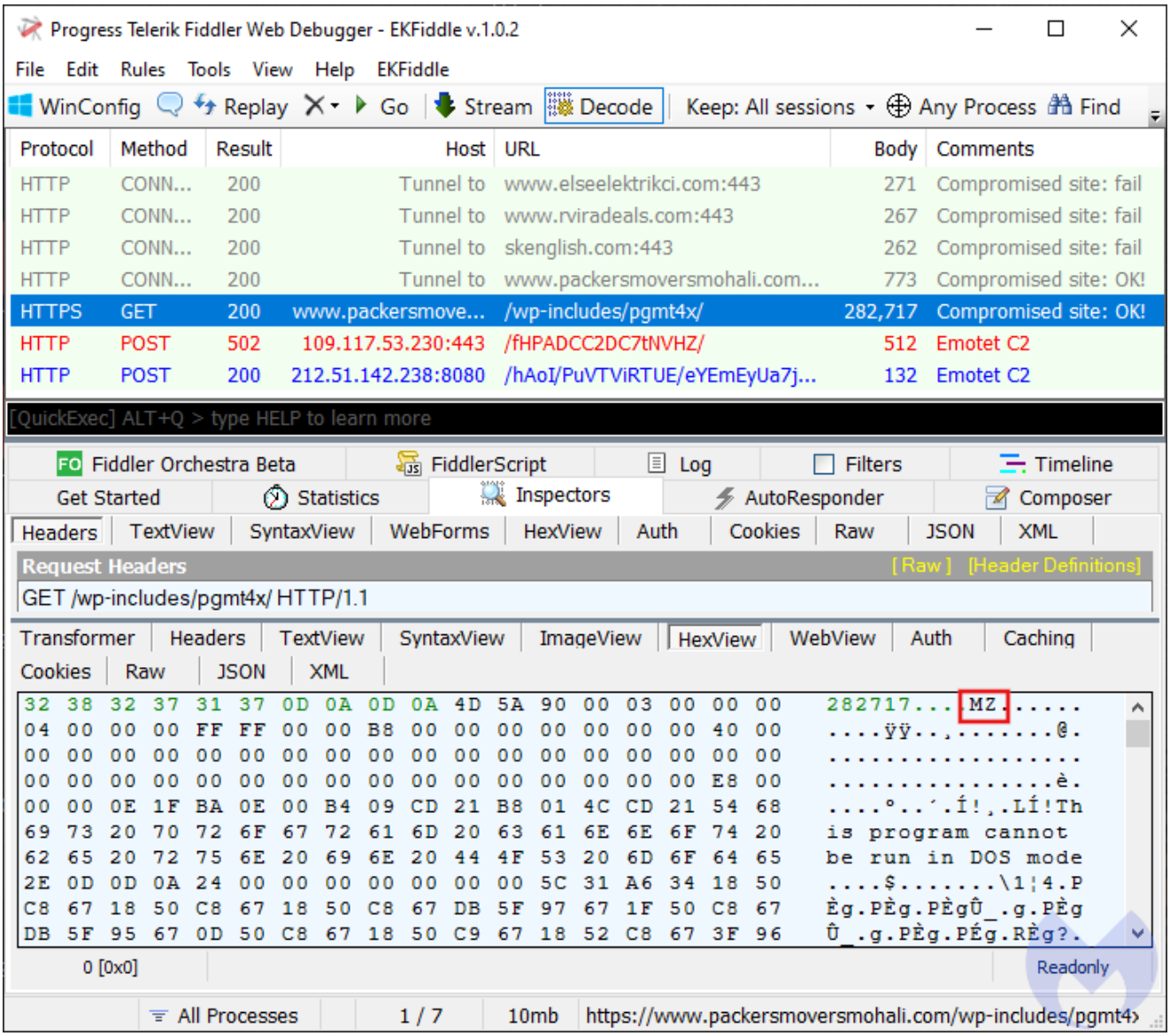
The Emotet botnets started pushing malspam actively on Friday, July 17, using the same techniques as employed in its last wave of activity. Malicious emails contain either a URL or an attachment that, once clicked on or opened, launches the Emotet payload. One familiar technique is for the document to be sent as a reply within existing email threads.



The document contains a heavily obfuscated macro:



Once the macro is enabled, WMI launches PowerShell to retrieve the Emotet binary from one of the remote compromised websites. It will iterate through a list until it identifies one that is responding.



Once the payload is executed, it will send a confirmation back to one of Emotet's command and control servers.

Emotet has returned with new tricks

Emotet was by far the most visible and active threat on our radars in 2018 and 2019—right up until the start of 2020, when it went into an extended break. One of the reasons why it was (and is) so successful is because of its constant evolution in attack techniques and threat partnerships.

For example, according to Bleeping Computer, Emotet now uses stolen email attachments to add credibility to the spam it generates to infect targeted systems. This is in addition to the aforementioned technique of hijacking email threads—a social engineering strategy employed to increase the likelihood of infection.

Emotet is used by cybercriminals as the initial entry point for infecting an organization, followed by a dwell time that can last days or weeks. In the meantime, it often drops secondary payloads to further penetrate its target's defenses. In its most recent incarnation, Emotet has been observed dropping secondary payloads, such as TrickBot and QakBot to spread laterally and steal credentials.

In fact, the real damage caused by an Emotet compromise happens when it forms alliances with other malware gangs—particularly with those threat actors interested in dropping ransomware, such as Ryuk, which was a constant partner of Emotet's in 2019. So far, a prevalent ransomware family has not yet been identified in Emotet's latest campaign.

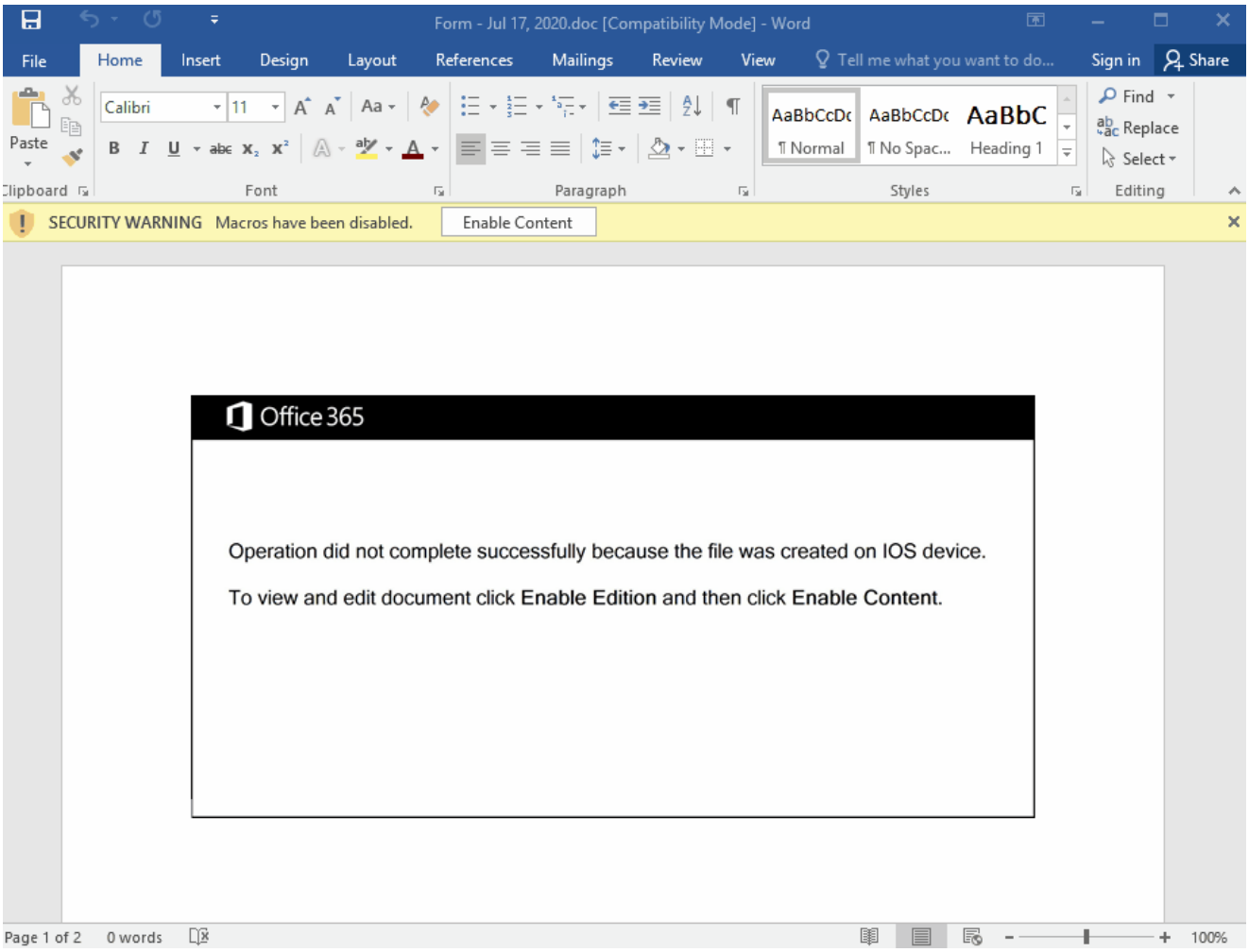
How to protect against Emotet

Users looking to protect against Emotet should first keep a wary eye out for phishing and/or spam emails—especially any emails with attachments. Even emails that appear to be from known contacts should be treated with suspicion.

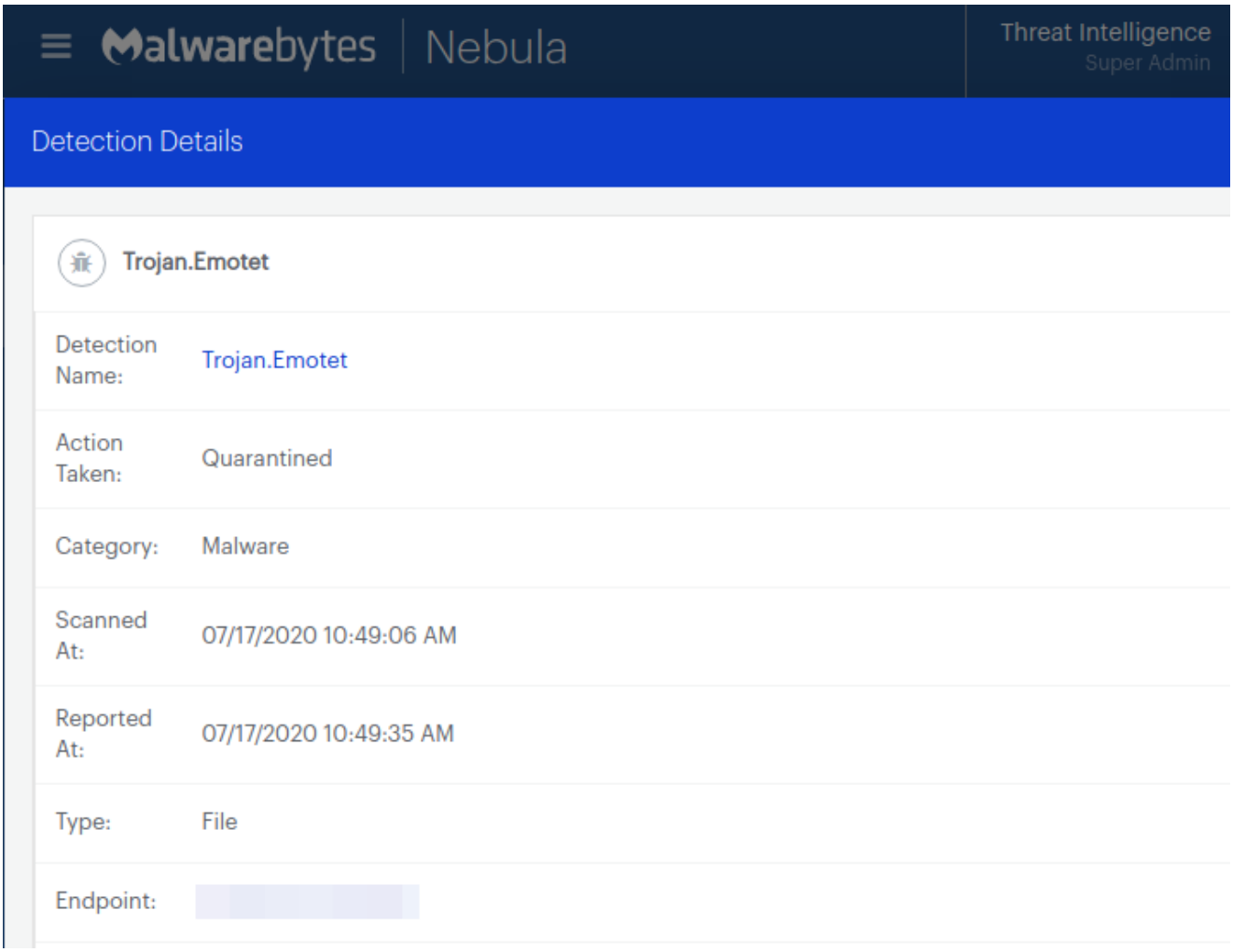
However, if unlucky users happen to click on a malicious URL or open an infected document, a good security program—especially one with anti-exploit technology—will block the malware from launching and keep computers free from infection.

For more information on how to protect against or remediate an Emotet infection, take a look at our emergency kit, which includes a summary of the threat and a checklist of tips.

Malwarebytes Premium and business users are already protected against Emotet, thanks to our signature-less anti-exploit technology.



We also detect the Emotet binary as a standalone file:



Indicators of Compromise

Malicious documents

```
5d2c6110f2ea87a6b7fe9256affbac0eebdeee18081d59e05df4b4a17417492b
4fdff0ebd50d37a32eb5c3a1b2009cb9764e679d8ee95ca7551815b7e8406206
bb5602ea74258ccad36d28f6a5315d07fbeb442a02d0c91b39ca6ba0a0fe71a2
6d86e68c160b25d25765a4f1a2f8f1f032b2d5cb0d1f39d1d504eeaa69492de0
18fab1420a6a968e88909793b3d87af2e8e1e968bf7279d981276a2aa8aa678e
d5213404d4cc40494af138f8051b01ec3f1856b72de3e24f75aca8c024783e89
```

Compromised sites

```
elseelektrikci[.]com
rviradeals[.]com
skenglish[.]com
packersmoversmohali[.]com
tri-comma[.]com
ramukakaonline[.]com
shubhinfoways[.]com
test2.cxyw[.]net
sustainableandorganicgarments[.]com
staging.icuskin[.]com
fivestarcleanerstx[.]com
bhandaraexpress[.]com
crm.shaayanpharma[.]com
zazabajouk[.]com
e2e-solution[.]com
topgameus[.]com
cpads[.]net
tyres2c[.]com
thesuperservice[.]com
ssuse[.]com
kdtphumy[.]com
lwzmy[.]com
innovertec[.]com
lawofattraction[.]work
bitvshe[.]club
```

Emotet binaries

```
454d3f0170a0aa750253d4bf697f9fa21b8d93c8ca6625c935b30e4b18835374
d51073eef56acf21e741c827b161c3925d9b45f701a9598ced41893c723ace23
1368a26328c15b6d204aef2b7d493738c83fced23f6b49fd8575944b94bcfbf4
7814f49b3d58b0633ea0a2cb44def98673aad07bd99744ec415534606a9ef314
f04388ca778ec86e83bf41aa6bfa1b163f42e916d0fbab7e50eaadc8b47caa50
2460d6cc6070933ec2e8c7b12e17a402d14546d7455aae293eefc085c4c76c7d
```

C2s

178[.]210[.]171[.]15
109[.]117[.]53[.]230
212[.]51[.]142[.]238
190[.]160[.]53[.]126
110[.]44[.]113[.]2:8080
113[.]160[.]180[.]109
113[.]161[.]148[.]81
115[.]79[.]195[.]246
139[.]59[.]12[.]63:8080
14[.]99[.]112[.]138
140[.]207[.]113[.]106:443
143[.]95[.]101[.]72:8080
144[.]139[.]91[.]187
157[.]7[.]164[.]178:8081
163[.]172[.]107[.]70:8080
177[.]0[.]241[.]28
177[.]144[.]130[.]105:443
178[.]33[.]167[.]120:8080
179[.]5[.]118[.]12
181[.]134[.]9[.]162
181[.]164[.]110[.]7
181[.]167[.]35[.]84
181[.]230[.]65[.]232
185[.]142[.]236[.]163:443
190[.]171[.]153[.]139
190[.]251[.]235[.]239
190[.]55[.]233[.]156
190[.]63[.]7[.]166:8080
192[.]163[.]221[.]191:8080
192[.]210[.]217[.]94:8080
192[.]241[.]220[.]183:8080
195[.]201[.]56[.]70:8080
201[.]212[.]78[.]182
203[.]153[.]216[.]178:7080
203[.]153[.]216[.]182:7080
211[.]20[.]154[.]102
212[.]112[.]113[.]235
216[.]75[.]37[.]196:8080
220[.]128[.]125[.]18
37[.]208[.]106[.]146:8080
37[.]46[.]129[.]215:8080
37[.]70[.]131[.]107
41[.]185[.]29[.]128:8080
45[.]118[.]136[.]92:8080
46[.]105[.]131[.]68:8080
46[.]32[.]229[.]152:8080
46[.]49[.]124[.]53
50[.]116[.]78[.]109:8080
51[.]38[.]201[.]19:7080
74[.]207[.]230[.]187:8080
74[.]208[.]173[.]91:8080
75[.]127[.]14[.]170:8080
77[.]74[.]78[.]80:443
78[.]188[.]170[.]128
80[.]211[.]32[.]88:8080

81[.]214[.]253[.]80:443
87[.]106[.]231[.]60:8080
91[.]83[.]93[.]103:443