


## Emotet malware strikes U.S. businesses with COVID-19 spam

By Lawrence Abrams

Published: 2020-08-14 · Archived: 2026-04-06 02:02:57 UTC

```
7701CFA0 C5CD FAR ECX LDS ECX,EBP
7701CFA2 FE OS DWORD PTR E??[EDI]
7701CFA3 FFE9 BYTE PTR DS:JMP FAR ECX
7701CFA5 ABD BYTE PTR DS:STOS DWORD PTR ES:[EDI]
7701CFA6 8402 SHORT ntdll TEST BYTE PTR DS:[EDX]
7701CFA8 00BF 23000000 ADD BYTE PTR DS:[EAX],BH
7701CFAE EB E9 EAX,38003000 JMP SHORT ntdll
7701CFB0 7B 00 BYTE PTR DS:JPO SHORT ntdll
7701CFB2 25 00300030 AND EAX,00003000
7701CFB7 006C 00 78 PTR DS:ADD BYTE PTR DS:[EAX+EAX-8],CH
7701CFBB 002D 00250030 ADD BYTE PTR DS:[EDI],A
7701CFC1 0034 00 X,30002500 ADD BYTE PTR DS:[EAX+EAX],A
7701CFC4 78 00 JS SHORT ntdll
7701CFC6 2D 00250030 SUB EAX,3000
7701CFB2 AND EAX,00003000
7701CFB7 ADD BYTE PTR DS:[EAX+EAX]
7701CFBB ADD BYTE PTR DS:[EDI+C0000000]
7701CFC1 JMP SHORT ntdll
7701CFB2 JPO SHORT ntdll
7701CFC4 AND EAX,00003000
7701CFC6 ADD BYTE PTR DS:[EAX+EAX]

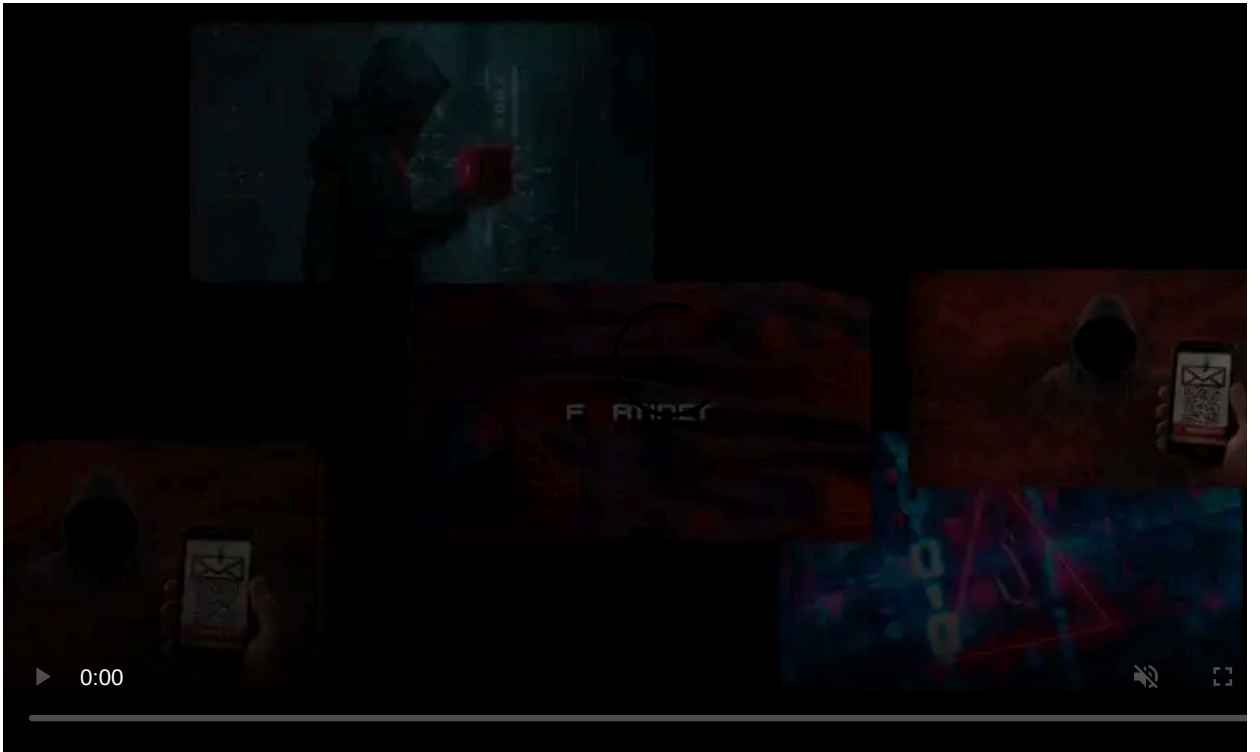
Address Hex dump
00408000 40 10 40 00 49 10 40 00 @@@@ 002D 00250030 ADD BYTE PTR DS:[30002500]
00408008 52 10 40 00 5B 10 40 00 @@@@ 003400 ADD BYTE PTR DS:[EAX+EAX]
```



The Emotet malware has begun to spam COVID-19 related emails to U.S. businesses after not being active for most of the USA pandemic.

Before going dark on Feb 7th, 2020, the Emotet malware was commonly spamming COVID-19 themed spam to [distribute malware in other countries](#) already affected by the pandemic.

As the start of the USA's pandemic was around March, Emotet never had the chance to target U.S. businesses with COVID-19 related spam.

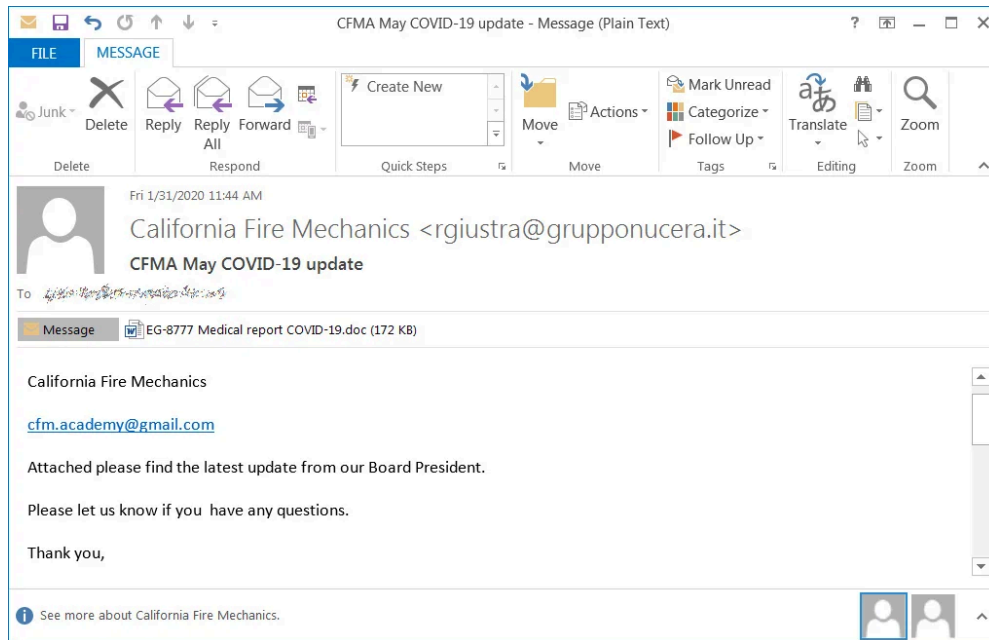


Visit Advertiser website [GO TO PAGE](#)

With Emotet's back in full swing again after awakening on July 17th, 2020, Emotet has started spewing out COVID-19 spam, and this time it's now targeting users in the USA.

## COVID-19 Emotet spam now targeting U.S. orgs

In a new spam email discovered by security researcher [Fate112](#), Emotet has been sending out a stolen email that pretends to be from the 'California Fire Mechanics' sending a 'May COVID-19 update'.

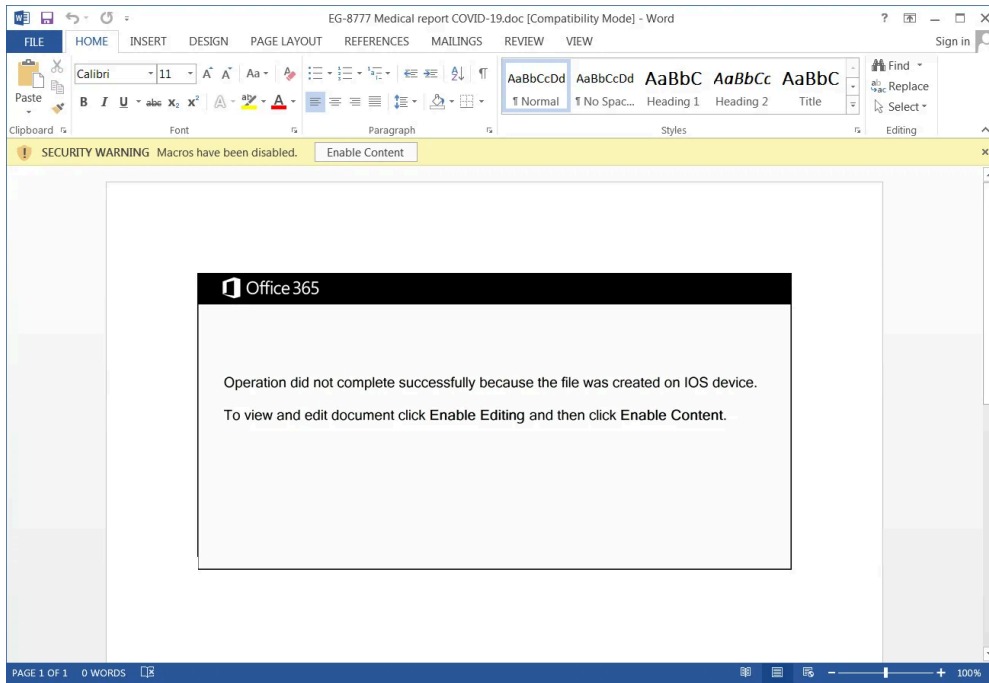


### COVID-19 themed Emotet spam

This email is not a template created by the Emotet actors, but rather an email stolen from an existing victim and adopted into the malware's spam campaigns.

Attached to the email is a malicious attachment titled 'EG-8777 Medical report COVID-19.doc', which uses a generic document template used in previous campaigns.

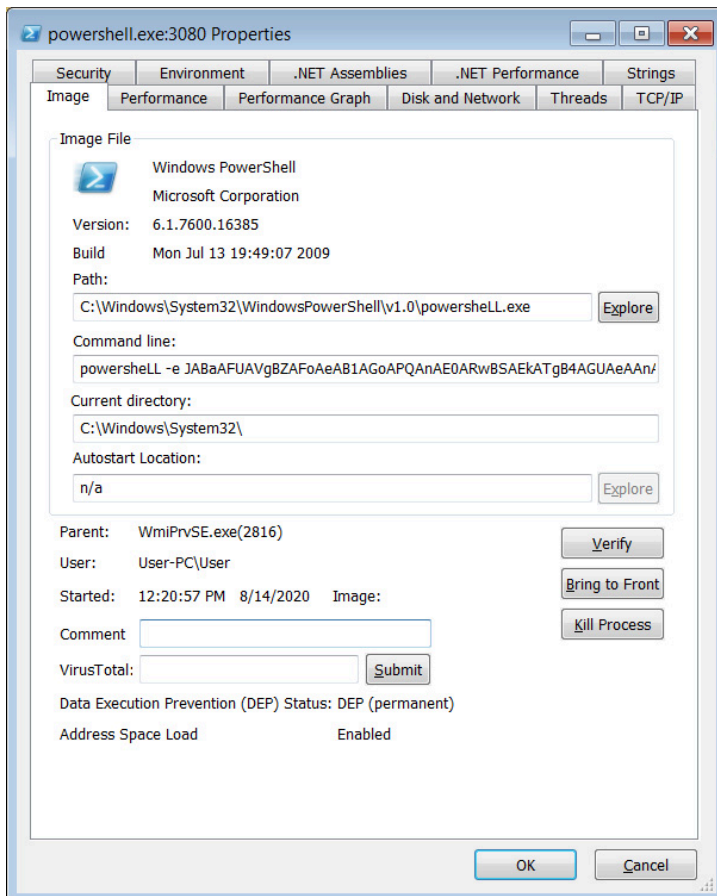
This template pretends to be created from an iOS device and requires users to click on 'Enable Content' to view it properly.



### Malicious Emotet document

Once a user clicks on the 'Enable Content' button, a PowerShell command will be executed that downloads the Emotet malware executable from one of three to four sites.

In this particular campaign, when downloaded, Emotet will be saved to the %UserProfile% folder and named as a three-digit number, such as 498.exe.



### Malicious PowerShell command

Once executed, a victim's computer will become part of the malware bot operation and spam out further malicious email.

Ultimately, Emotet will download and install other malware such as Qbot or TrickBot, which will be used to steal your data, passwords, and potentially lead to ransomware deployment.

In a conversation with Emotet expert [Joseph Roosen](#), BleepingComputer was told that other COVID-19 campaigns have recently been seen using reply-chain emails.

"So far we have only seen it as part of stolen reply chain emails. We have not seen it as a generic template yet but I am sure it is just around the corner hehe. There was one reply chain I saw yesterday that was sent to 100s of addresses that was referring to the closing of an organization because of covid-19. I would not be surprised if Ivan is filtering some of those reply chains to focus on ones that are involving covid-19," Roosen told BleepingComputer.

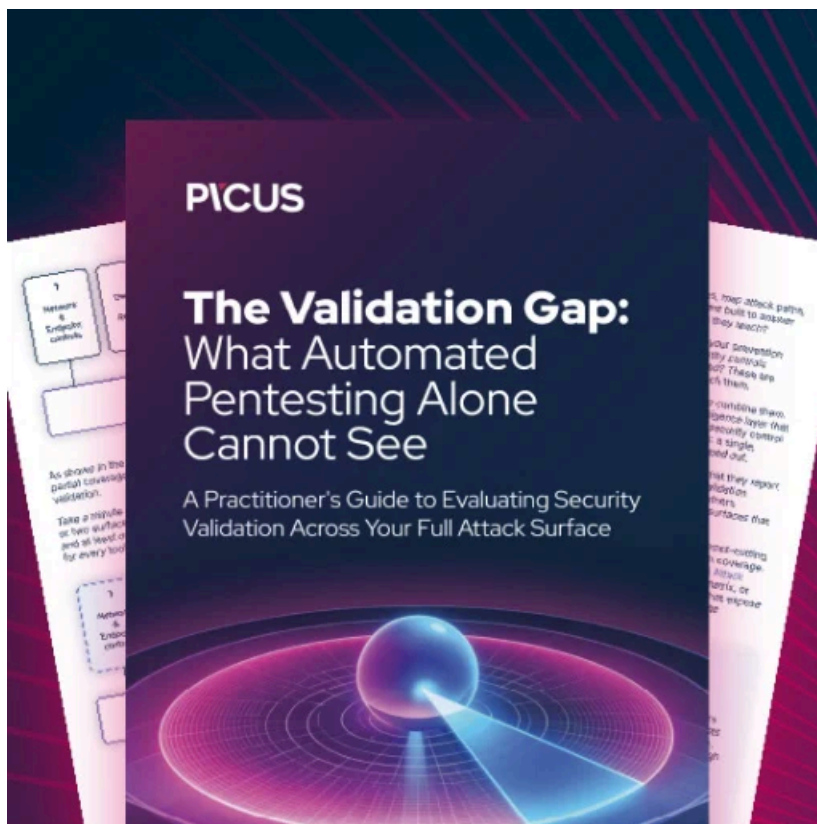
Ivan is Roosen's nickname for the Russian Emotet-malware operators.

Email security firm Cofense also told BleepingComputer that they have been seeing COVID-19 related spam recently that uses attachments named "COVID-19 report 08 12.doc" and similar.

Cofense states that the document date will change to the day of the campaign.

As Emotet is such a dangerous malware that can lead to a variety of risks, all home and corporate users must be cautious about opening documents that require you to 'Enable Content.'

If you receive these types of emails, first scan the attachment with an antivirus scanner to make sure it is safe to open. Even then, you should proceed with caution.



### **Automated Pentesting Covers Only 1 of 6 Surfaces.**

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/emotet-malware-strikes-us-businesses-with-covid-19-spam/>