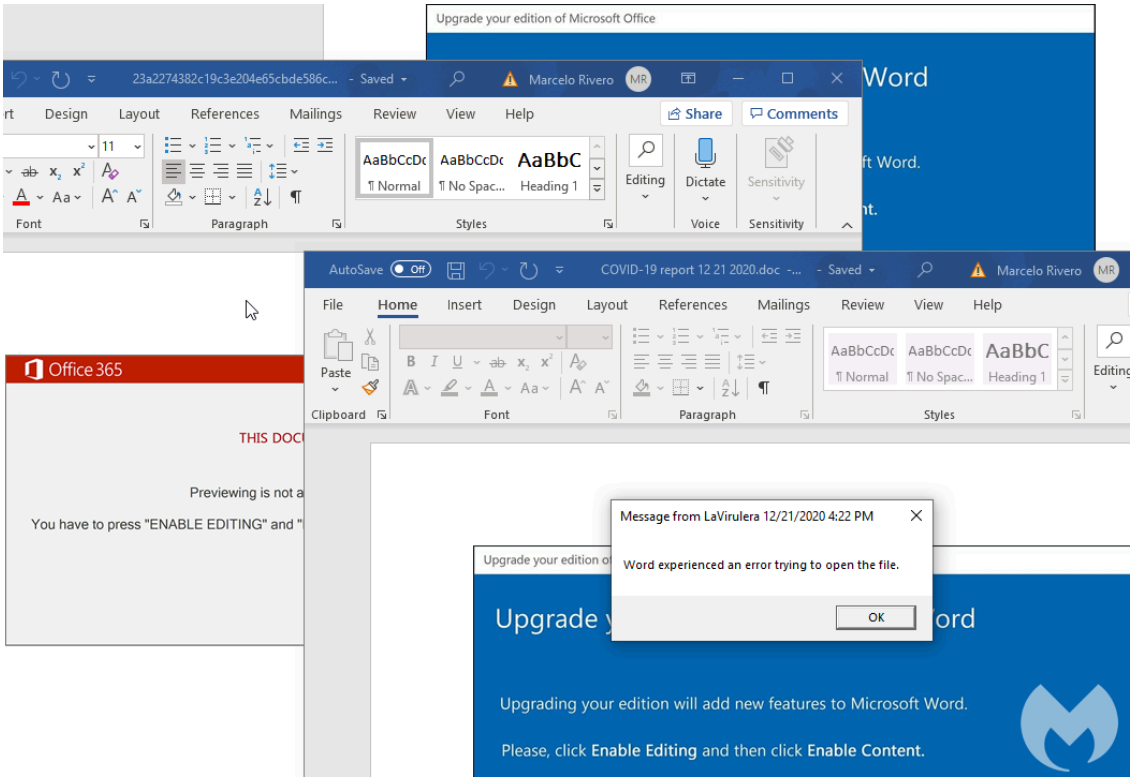
# Emotet returns just in time for Christmas

By Mark Stockley

Published: 2020-12-21 · Archived: 2026-04-05 21:25:55 UTC

December 22, 2020




Some of the malicious emails we collected used COVID-19 as a lure. This tactic was already seen in the spring but is still being leveraged, perhaps due to the massive second wave observed in the US as well as news about the

vaccine rollout.

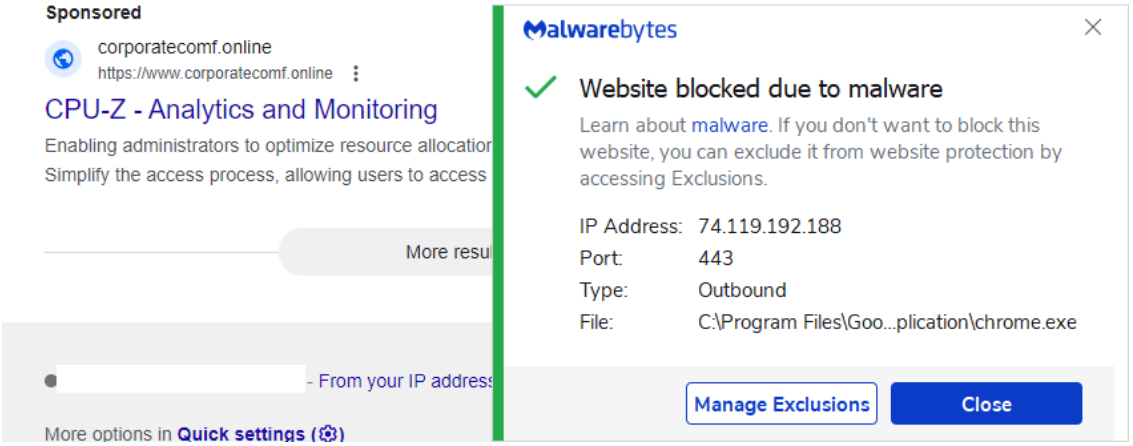
### Christmas campaign repeat?

Emotet is most feared for its alliances with other criminals, especially those in the ransomware business. The Emotet – TrickBot – Ryuk triad wreaked havoc around Christmas time in 2018.

While some threat actors observe holidays, it is also a golden opportunity to launch new attacks when many companies have limited staff available. This year is even more critical in light of the pandemic and the recent SolarWinds debacle.

We urge organizations to be particularly vigilant and continue to take steps to secure their networks, especially around security policies and access control.

Malwarebytes users were already protected against Emotet thanks to our signature-less Anti-Exploit protection.

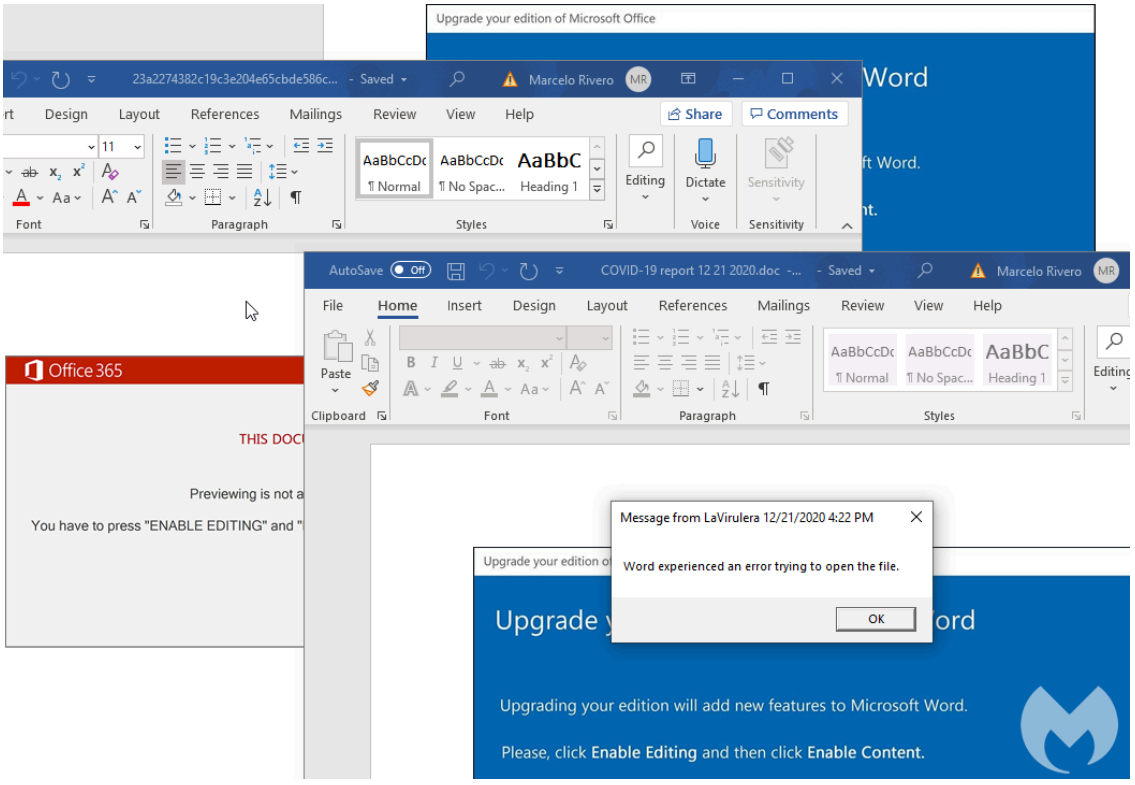



### Indicators of Compromise

You can downloads indicators of compromise related to Emotet's infrastructure on our GitHub page.

Emotet is a threat we have been tracking very closely throughout the year thanks to its large email distribution campaigns. Once again, and for about two months, the botnet stopped its malspam activity only to return days before Christmas.

In typical Emotet fashion, the threat actors continue to alternate between different phishing lures in order to social engineer users into enabling macros. However, in this latest iteration the Emotet gang is loading its payload as a DLL along with a fake error message.




Some of the malicious emails we collected used COVID-19 as a lure. This tactic was already seen in the spring but is still being leveraged, perhaps due to the massive second wave observed in the US as well as news about the vaccine rollout.

### Christmas campaign repeat?

Emotet is most feared for its alliances with other criminals, especially those in the ransomware business. The Emotet – TrickBot – Ryuk triad wreaked havoc around Christmas time in 2018.

While some threat actors observe holidays, it is also a golden opportunity to launch new attacks when many companies have limited staff available. This year is even more critical in light of the pandemic and the recent SolarWinds debacle.

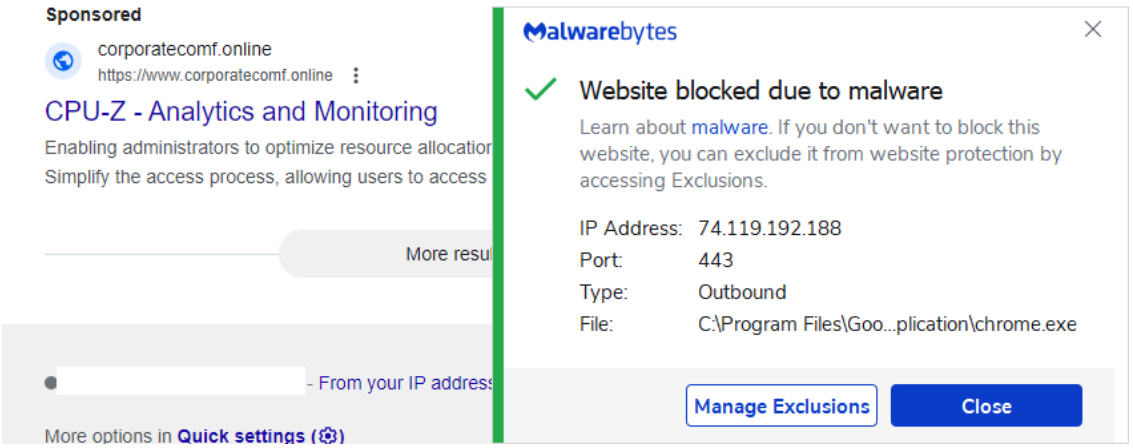
---



---

We urge organizations to be particularly vigilant and continue to take steps to secure their networks, especially around security policies and access control.

Malwarebytes users were already protected against Emotet thanks to our signature-less Anti-Exploit protection.




## Indicators of Compromise

You can downloads indicators of compromise related to Emotet's infrastructure on our GitHub page.

---

Source: https://blog.malwarebytes.com/cybercrime/2020/12/emotet-returns-just-in-time-for-christmas/