New Emotet delivery method spotted during downward detection trend

By David Ruiz

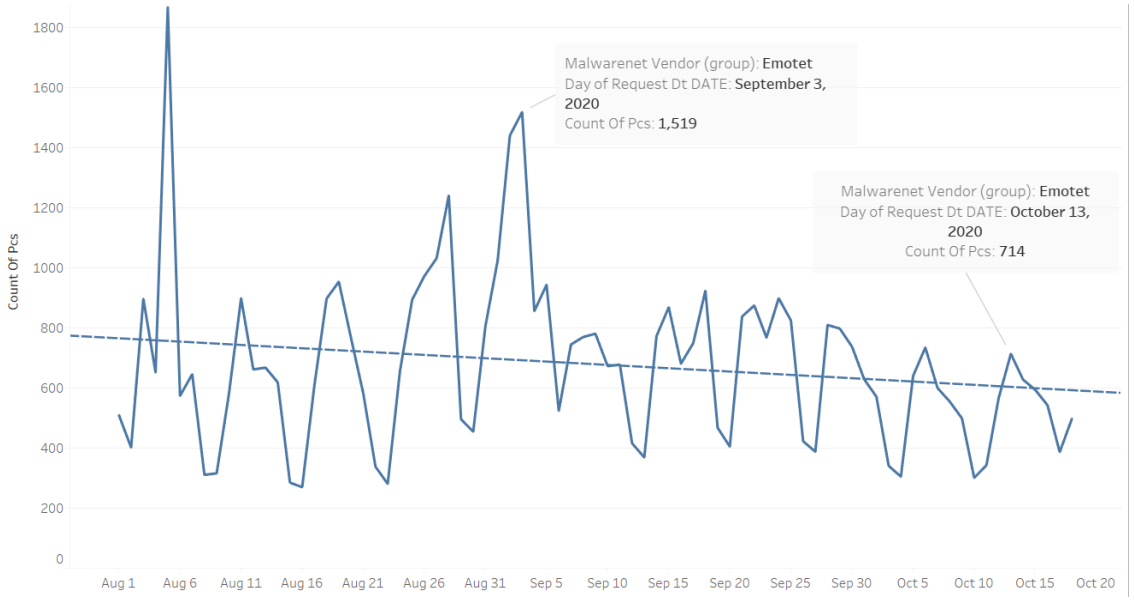
Published: 2020-10-27 · Archived: 2026-04-05 21:54:04 UTC

Emotet, one of cybersecurity's most-feared malware threats, got a superficial facelift this week, hiding itself within a fake Microsoft Office request that asks users to update Microsoft Word so that they can take advantage of new features.

This revamped presentation could point to internal efforts by threat actors to increase Emotet's hit rate—a possibility supported by Malwarebytes telemetry measured in the last few months.

Emotet spikes amid downward trend

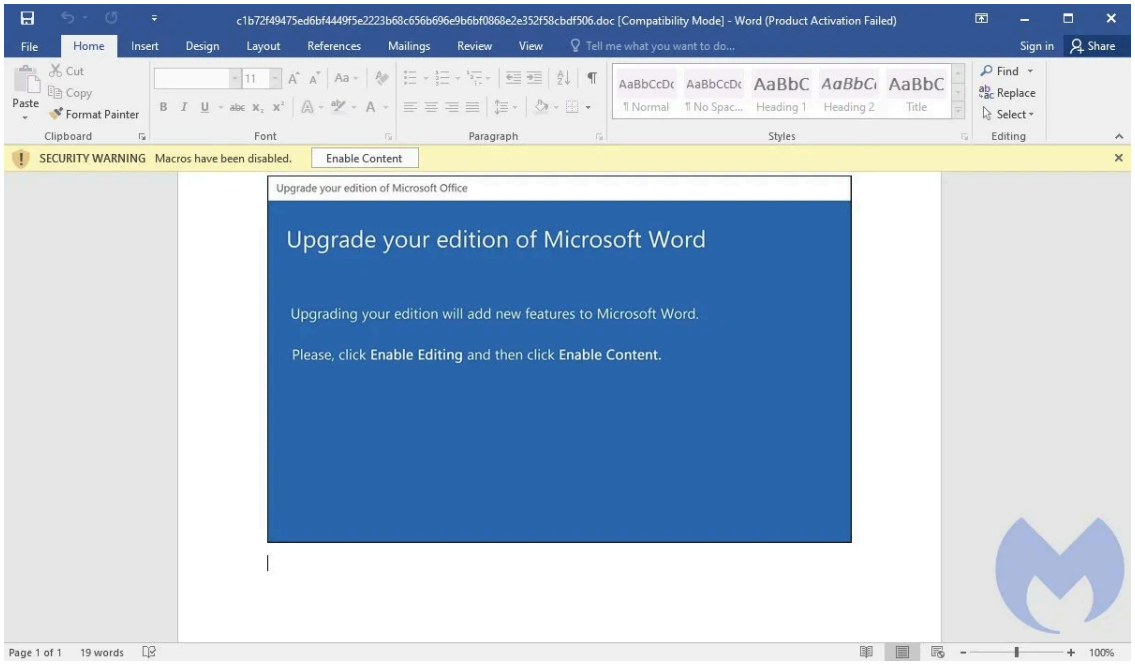
Since August 1, Malwarebytes has detected repeated weekly spikes in Emotet detections, with an August peak of roughly 1,800 detections in just one day. Those frequent spikes betray the malware's broader activity though—a slow and steady trend *downwards*, from an average of about 800 detections in early August to an average of about 600 detections by mid-October.



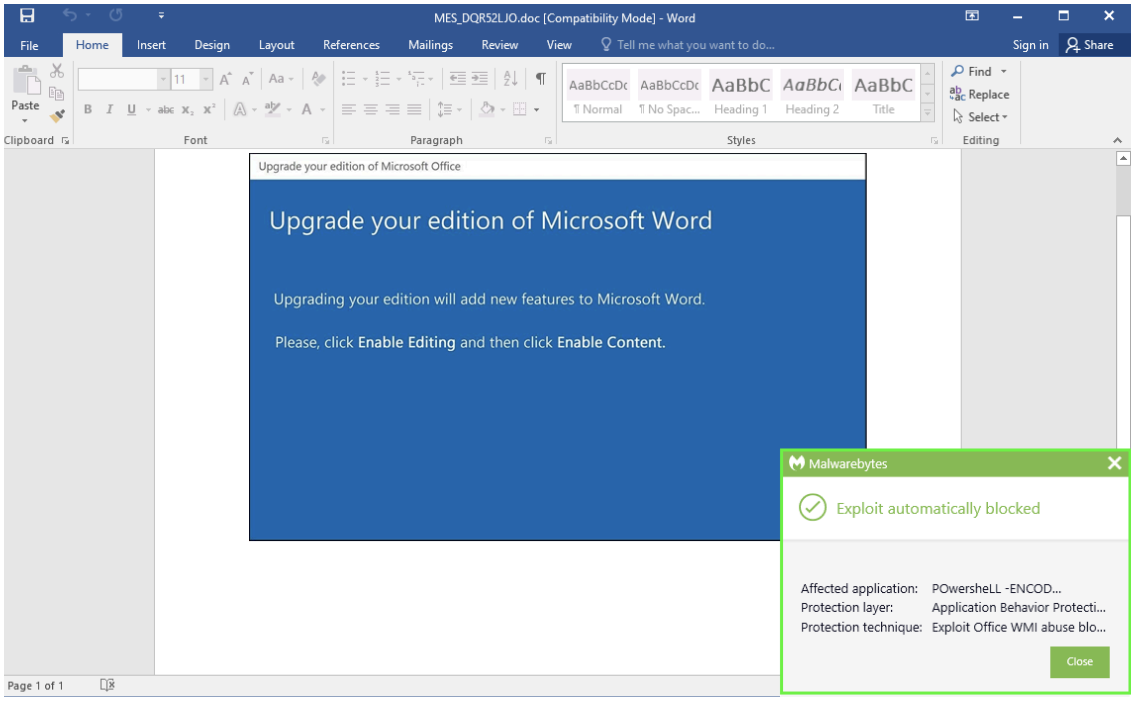
Caught by Malwarebytes on October 19, Emotet's new delivery method attempts to trick victims into thinking that they've received an update to Microsoft Word. The new template, shown below, includes the following text:

> "Upgrade your edition of Microsoft Word
>
> Upgrading your edition will add new features to Microsoft Word.
>
> Please, click **Enable Editing** and then click **Enable Content**."

If users follow these dangerous instructions, they will actually enable the malicious macros that are embedded into the "update request" itself, which will then be used as the primary vector to infect the machine with Emotet.



Malwarebytes protects users from Emotet and its latest trick, as shown below.



For those without cybersecurity protection, this new delivery method may appear frightening, and in a way, yes, it is. But when compared to Emotet's stealthy developments in recent years, this latest switch-up is rather ordinary.

In 2018, the cybersecurity industry spotted Emotet being spread through enormous volumes of email spam, in which potential victims received malicious email attachments supposedly containing information about "outstanding payments" and other invoices. In 2019, we spotted a botnet coming back to life to push out Emotet,

this time utilizing refined spearphishing techniques. Just weeks later, we found that threat actors were luring victims through the release of former NSA defense contractor Edward Snowden's book. And this year, Bleeping Computer reported that threat actors had managed to train the Emotet botnet to steal *legitimate* email attachments and to then include those attachments amongst other, *malicious* attachments as a way to legitimize them.

Threat actors have gone to such great lengths to deliver Emotet because of its destructive capabilities. Though the malware began as a simple banking Trojan to steal sensitive and private information, today it is often used in tandem to deliver other banking Trojans, like TrickBot, that can steal financial information and banking logins. This attack chain doesn't stop here, though, as threat actors also use Emotet and Trickbot to deliver the ransomware Ryuk.

Compounding the danger to an organization is Emotet's ability to spread itself through a network. Once this malware has taken root inside a network, it has derailed countless consumers, businesses, and even entire cities. In fact, according to the US Cybersecurity and Infrastructure Security Agency, governments have paid up to $1 million to remediate an Emotet attack.

How to protect your business from Emotet

Our advice to protect against Emotet remains the same. Users should look out for phishing emails, spam emails, and anything that includes attachments—even emails that appear to come from known contacts or colleagues.

For users who do make that risky click, the best defense is a cybersecurity solution that you've already got running. Remember, the best defense to an Emotet infection is to make sure it never happens in the first place. That requires constant protection, not just after-the-fact response.

About the author

Pro-privacy, pro-security editor. Former journalist turned advocate turned cybersecurity defender. Still a little bit of each. Failing book club member.
