Emotet Returns After Holiday Break with Major Campaigns | Proofpoint US

Published: 2020-01-16 · Archived: 2026-04-05 18:45:07 UTC

January 16, 2020

Threat actor group TA542, the group that's behind Emotet, is back from their Christmas holiday. Based on past activity and what we're seeing in just three days, one of the world's most disruptive threats is back to work and everyone around the world should take note and implement steps to protect themselves.

To understand how serious the potential threat of Emotet's latest return can be, it's helpful to look at the last break they took: May 2019 until late September 2019. Even though Emotet was on vacation for all but the last two weeks of Q3 (July – September), it still accounted for over **11% of all malicious** payloads we saw for that entire quarter. That statistic alone tells the story of what TA542 is capable of with Emotet. TA542 has massive sending infrastructure: nobody generates volumes like they do these days. Campaigns that TA542 unleash have big volumes and are widespread across verticals, languages and people. Even if they take 150 days off in a year, like they did in 2019, they can do lots of damage.

On Monday, we saw Emotet get back to work with a new campaign. In this campaign Proofpoint observed TA542 pursuing potential victims in the western hemisphere (U.S., Canada, and Mexico) in the pharmaceutical industry in particular. You can see an example from the latest Emotet campaign in Figure 1 below.

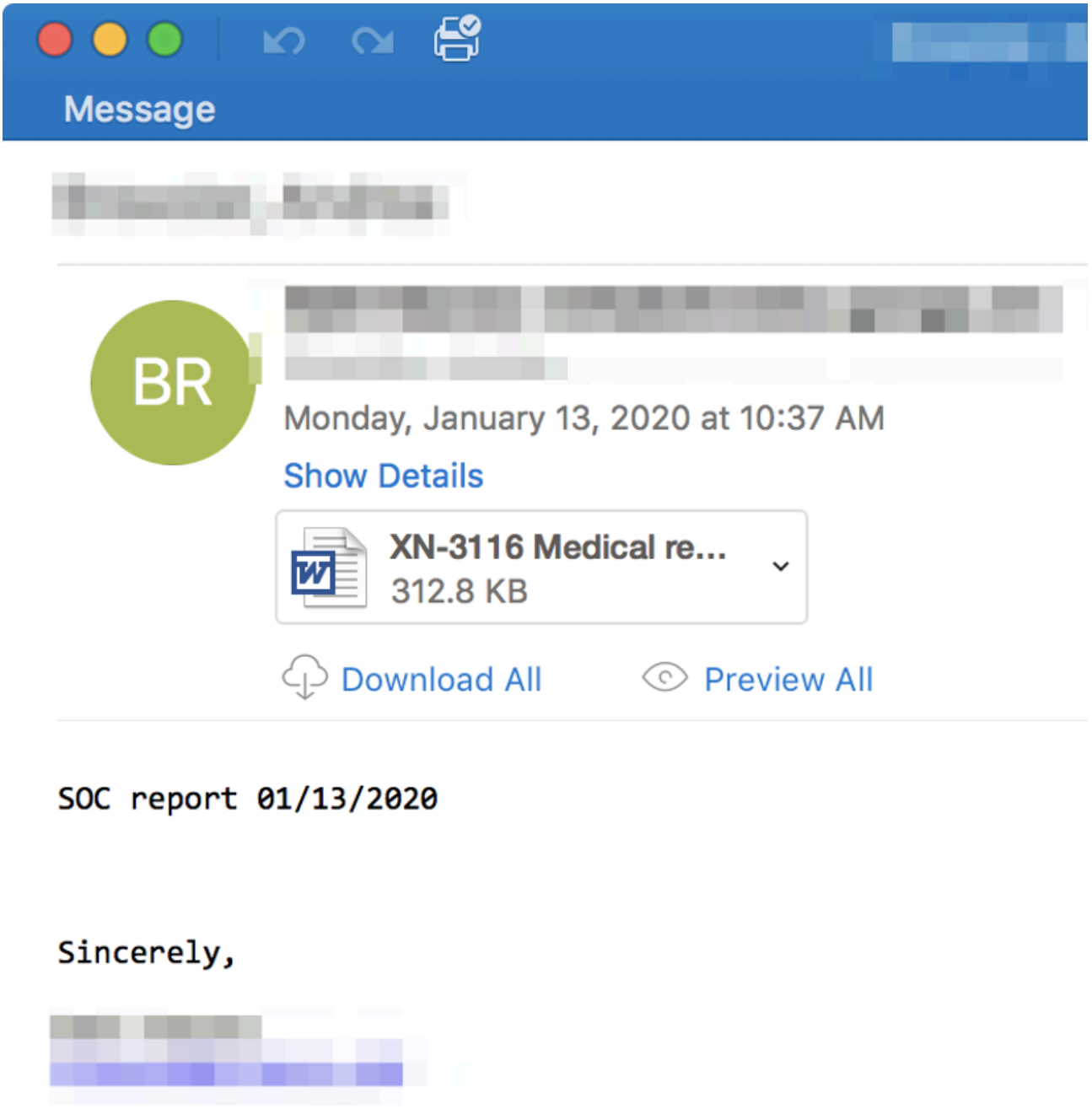

Figure 1 Sample from Latest Emotet Campaign

Then, on Tuesday, we saw the scope of the geographic expand significantly as they added over a dozen countries around the world. Countries being targeted now include:

1. Australia
2. Austria
3. Canada
4. Germany
5. Hong Kong
6. Italy
7. Japan
8. Mexico

9. Singapore
10. South Korea
11. Spain
12. Switzerland
13. Taiwan
14. United Arab Emirates
15. United States

At the same time, they expanded the languages used in their email lures from just English on Monday to English plus Chinese, German, Italian, Japanese and Spanish. As usual for this group, they've expanded to target a variety of industries.

We've mentioned that TA542 is capable of incredible volumes in a short period of time, that's one of the things that makes them such a significant threat. On Monday alone we saw nearly three quarters of a million messages and they're already fast approaching one million messages total. To give this context, this isn't the highest volume we've ever seen from this actor: that was over one million messages in one day. But Monday was the biggest volume since April 2019.

Based on past activity and what our researchers are seeing, organizations around the globe should take Emotet's return seriously. Throughout their career, TA542 has used widespread email campaigns on a huge, international scale that have affected North America, Central America, South America, Europe, Asia, and Australia. TA542's continued use of Emotet should cause concern as well: Emotet is a modular robust botnet, is capable of downloading and installing a range of additional malware, that often steal information and sends malicious email. Emotet can also spread across networks and use infected devices to launch further attacks. Emotet is a highly effective malware being used by a highly effective and sophisticated threat group with a large global infrastructure.

We recommend organizations take necessary steps to ensure email traffic is secure and warn users to be wary of emails that encourage urgent action, such as clicking on links or opening attachments. Layered defenses with protection at the email gateway will help prevent delivery of these messages and customized user training programs will help potential victims recognize malicious emails.

Subscribe to the Proofpoint Blog
