Emotet Makes Timely Adoption of Political and Elections Lures | Proofpoint US

By October 01, 2020 Axel F. and the Proofpoint Threat Research Team

Published: 2020-10-01 · Archived: 2026-04-05 16:27:38 UTC

During the 76 days since Emotet's return, researchers have observed activity reminiscent of past Emotet campaigns, like high message volumes and global distribution.

Emotet uses a variety of lure themes, some of which occasionally leverage current events or news items, like COVID-19 or Greta Thunberg. While TA542, the actor behind Emotet, has sent messages to local, state, and other government recipients, historically they have not directly leveraged political themes in their messaging.

On October 1, 2020, we observed thousands of Emotet email messages with the subject "Team Blue Take Action" sent to hundreds of organizations in the US. The message body is taken directly from a page on the Democratic National Committee's website, with the addition of a line requesting that the recipient open the attached document.

Attached is a malicious Word document, "Team Blue Take Action." The Word doc contains macros which, if enabled by the intended recipient, will download and install Emotet. The current second stage payload we've observed following Emotet is Qbot "partner01" and The Trick "morXXX" (e.g., "mor125").

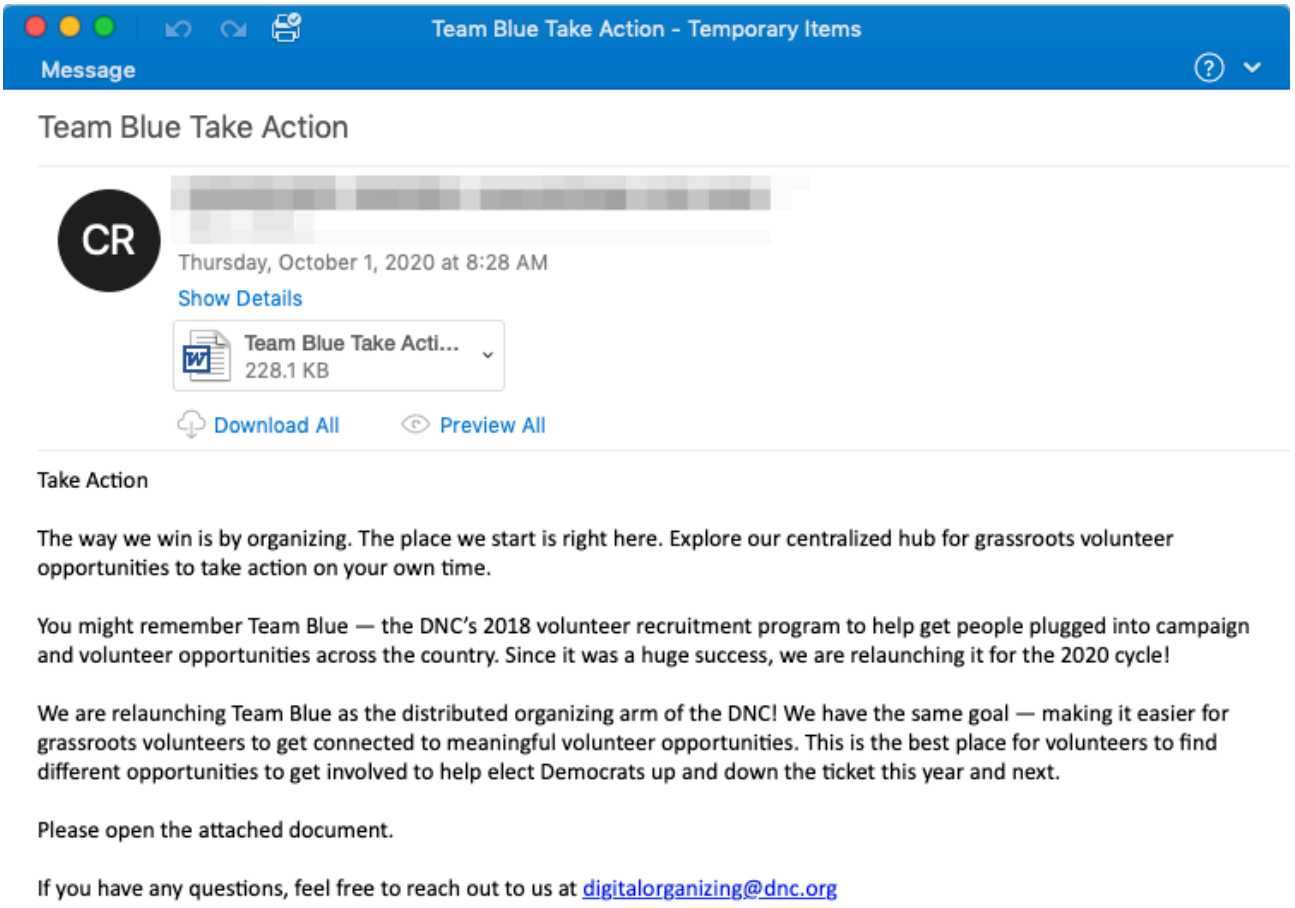

Figure 1: "Team Blue Take Action" lure containing malicious Word doc attachment

Sample of additional related subjects observed includes:

- Valanters 2020
- Detailed information
- List of works
- Volunteer
- Information

Sample of additional related filenames observed includes:

- Team Blue Take Action.doc
- List of works.doc
- Valanters 2020.doc
- Detailed information.doc

- Volunteer.doc

The shift to using politically themed lures comes days after the first of several 2020 US Presidential debates. The debate received widespread media coverage, and as Election Day draws nearer, many voters are likely feeling compelled to volunteer for political causes or for the election in some way. However, it's unlikely that this shift is driven by any specific political ideology. Like earlier use of COVID-19 or Greta Thunberg lure themes, TA542 is attempting to reach as many intended recipients as possible by capitalizing on a popular topic.

"Team Blue Take Action.doc" document SHA256:
21cda873bff60530ae094d7906219b5c0cc5d98e808f8608962886683fc37504

Subscribe to the Proofpoint Blog
