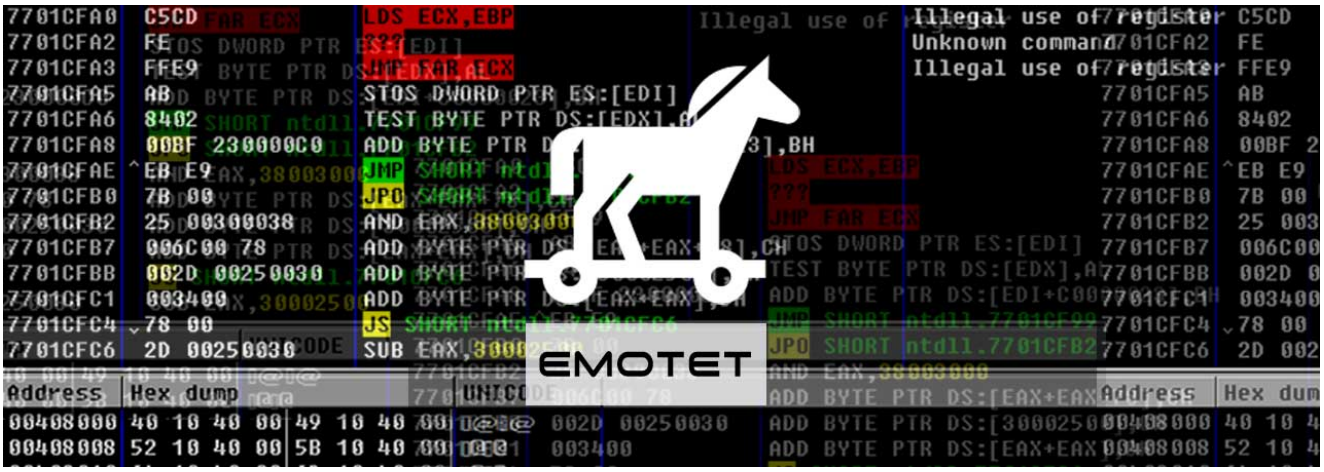
United Nations Targeted With Emotet Malware Phishing Attack

bleepingcomputer.com/news/security/united-nations-targeted-with-emotet-malware-phishing-attack/

Lawrence Abrams

By
Lawrence Abrams

- January 14, 2020
- 09:01 AM
- 0



Pretending to be the Permanent Mission of Norway, the Emotet operators performed a targeted phishing attack against email addresses associated with users at the United Nations.

Yesterday, the Emotet trojan roared back to life after a 3-week vacation with strong spam campaigns that targeted countries throughout the world.

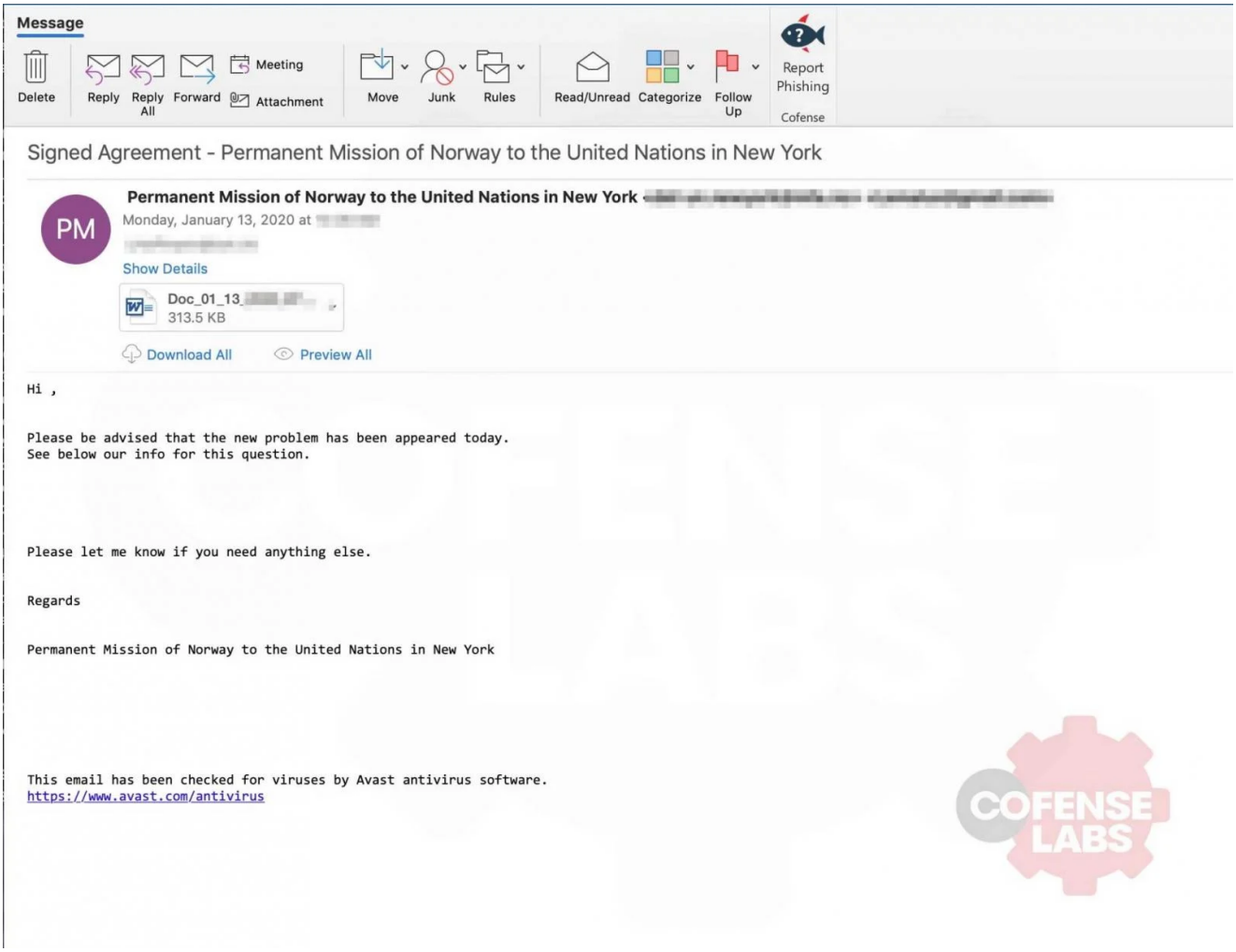
While Emotet's normal spam campaigns pretended to be fake accounting reports, delivery notices, and invoices, the malware operators had something special in mind for the United Nations.

Impersonating the "Permanent Mission of Norway"

In a sample of a phishing email shared with BleepingComputer by email security firm Cofense, the Emotet operators pretend to be representatives of Norway at the United Nations in New York, who state that there is a problem with an attached signed agreement.

According to Cofense, this phishing campaign had "highly specific targeting" and was seen being sent to 600 unique email addresses at the United Nations.

The email states that the representatives of Norway found a problem with a signed agreement and that the recipient should review it to learn the issue.



Emotet spam targeting the United Nations

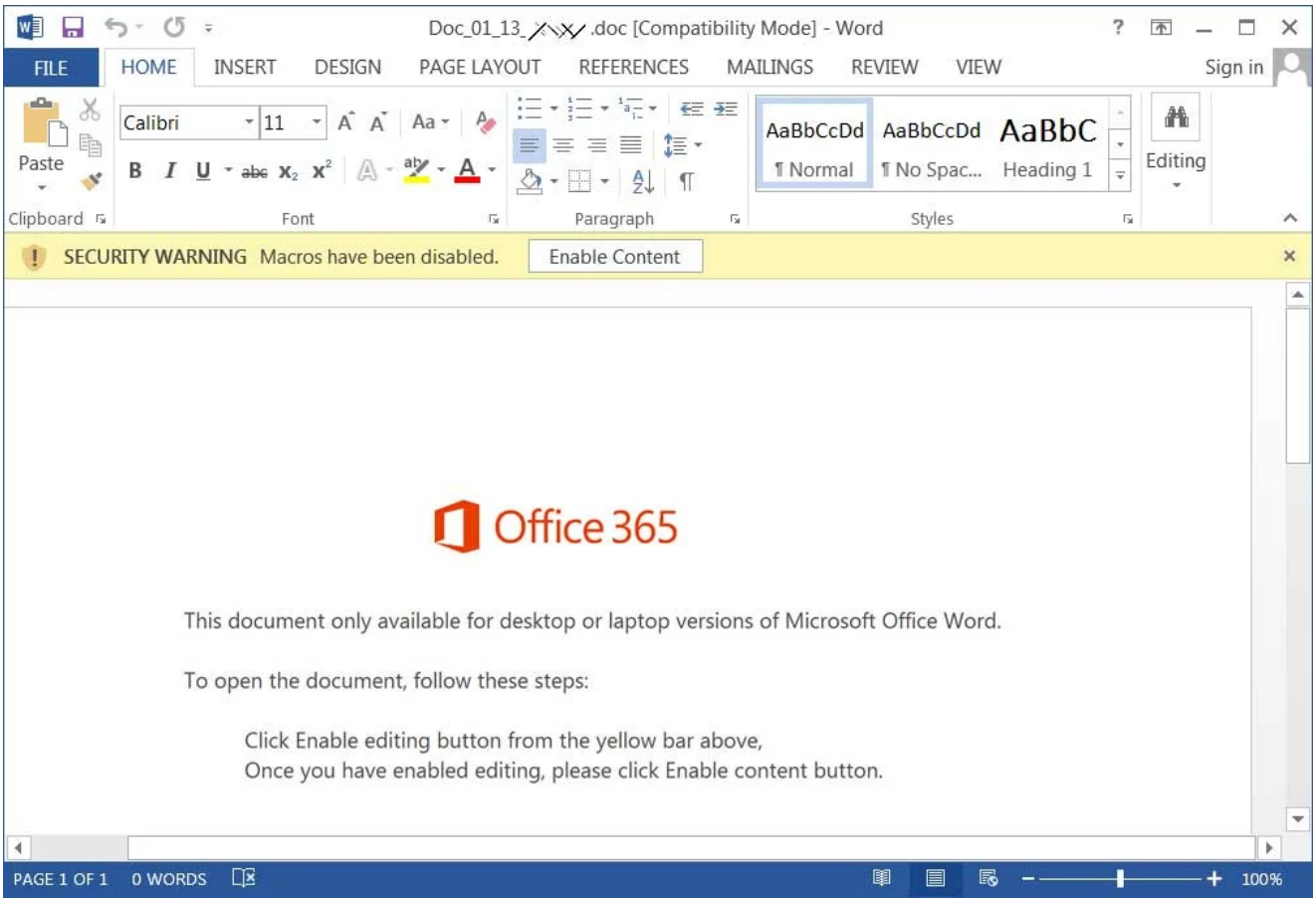
The full text of this targeted phishing email can be read below:

```
Hi,

Please be advised that the new problem has been appeared today.
See below our info for this question.

Please let me know if you need anything else.

Regards

Permanent Mission of Norway to the United Nations in New York
```

Attached to these emails is a Microsoft Word document that starts with "Doc_01_13" that pretends to be the signed agreement being sent by the Permanent Mission of Norway.

While there was room for Emotet to send a more convincing Word document template, they instead sent the same one that is used for all of the malspam campaigns.

This template pretends to be a warning that the "document only available for desktop or laptop versions of Microsoft Office Word." It then prompts the user to click on 'Enable editing' or 'Enable Content' to view the document.



Malicious Email Attachment

If a user opens the document and enables its content, malicious Word macros will be executed that downloads and installs Emotet on the computer.

Emotet will now run in the background while sending out spam emails to other victims.

Eventually, Emotet will also install other payloads such as Trickbot, which would be when things get really bad for the compromised UN workstation.

Emotet can lead to a full network compromise

When Emotet is installed on a machine, one of the malware payloads that is invariably installed is the TrickBot trojan.

The TrickBot trojan will attempt to harvest data from the computer such as cookies, login credentials, files from the computer, and possibly spread to other computers on the network.

After the harvesting of information is finished, TrickBot is known to open a reverse shell back to the operators of Ryuk Ransomware.

These operators will proceed to infiltrate the network, gain administrator credentials, and ultimately deploy Ryuk so that it encrypts every device on the network.

This is particularly worrisome for a UN network as ransomware operators are known to steal data before encrypting files, which could expose extremely sensitive diplomatic or government information.

While there are no known victims of this phishing attack, this targeted attack illustrates that bad actors are constantly trying to get access to the networks of organizations and government networks.

This is why it is imperative for all employees regardless of what sector they work in to be properly trained on how to recognize phishing emails.

Furthermore, before opening any attachments and enabling macros, users should notify their network administrator **and** contact the alleged user who sent the email to confirm its authenticity.

BleepingComputer has contacted the Permanent Mission of Norway about this attack but has not heard back at this time.

Related Articles:

Historic Hotel Stay, Complementary Emotet Exposure included

EmoCheck now detects new 64-bit versions of Emotet malware

Emotet botnet switches to 64-bit modules, increases activity

Emotet malware infects users again after fixing broken installer

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.