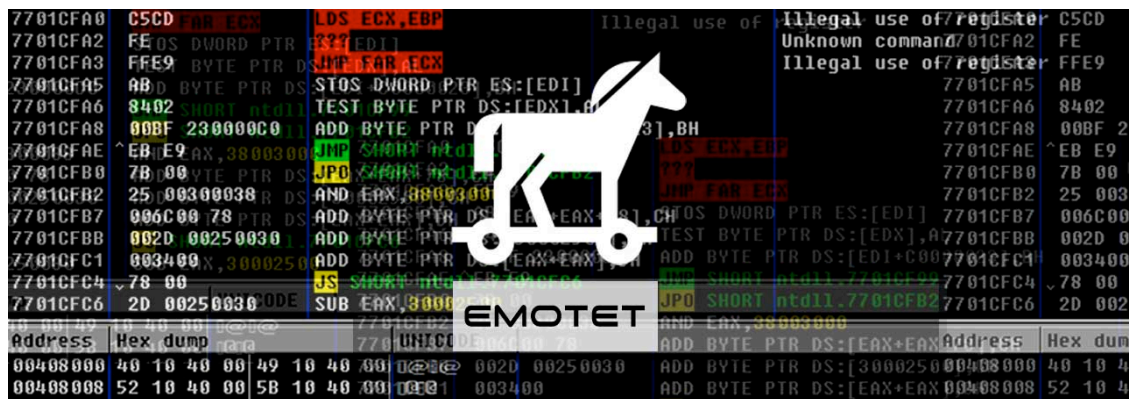


United Nations Targeted With Emotet Malware Phishing Attack

By Lawrence Abrams

Published: 2020-01-14 · Archived: 2026-04-05 16:21:43 UTC

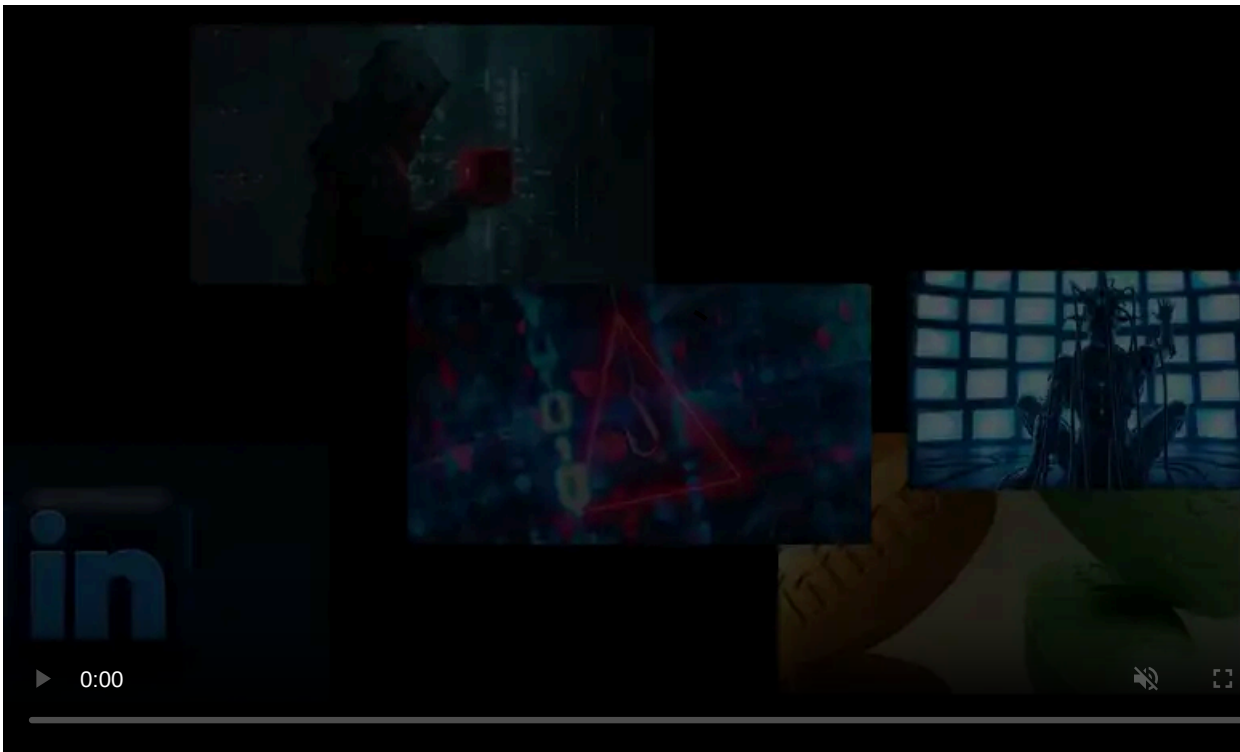


```
7701CFA0 C5CD LDS ECX,EBP Illegal use of register C5CD
7701CFA2 FE DS DWORD PTR DS:[EDI] Unknown command 701CFA2 FE
7701CFA3 FFE9 BYTE PTR DS:[EDI] Illegal use of register FFE9
7701CFA5 AB STOS DWORD PTR ES:[EDI] 7701CFA5 AB
7701CFA6 8402 TEST BYTE PTR DS:[EDX] 7701CFA6 8402
7701CFA8 00BF 23000000 ADD BYTE PTR DS:[EDI],BH 7701CFA8 00BF 2
7701CFAE EB E9 JMP FAR ECX 7701CFAE EB E9
7701CFB0 7B 00 JPO SHORT ntdd11 7701CFB0 7B 00
7701CFB2 25 00300038 AND EAX,80000000 7701CFB2 25 003
7701CFB7 006C00 78 STOS DWORD PTR ES:[EDI] 7701CFB7 006C00
7701CFBB 002D 00250030 ADD BYTE PTR DS:[EDI],A 7701CFBB 002D 0
7701CFC1 003400 X,3000250 ADD BYTE PTR DS:[EDI+C00] 7701CFC1 003400
7701CFC4 78 00 JS SHORT ntdd11 7701CFC4 78 00
7701CFC6 2D 00250030 SUB EAX,80000000 7701CFC6 2D 002
AND EAX,80000000
ADD EAX,80000000
ADD BYTE PTR DS:[EAX+EAX]
ADD BYTE PTR DS:[30002500]
ADD BYTE PTR DS:[EAX+EAX]
Address Hex dump
00408000 40 10 40 00 49 10 40 00 00 00 0020 00250030
00408008 52 10 40 00 5B 10 40 00 00 00 003400
```

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.



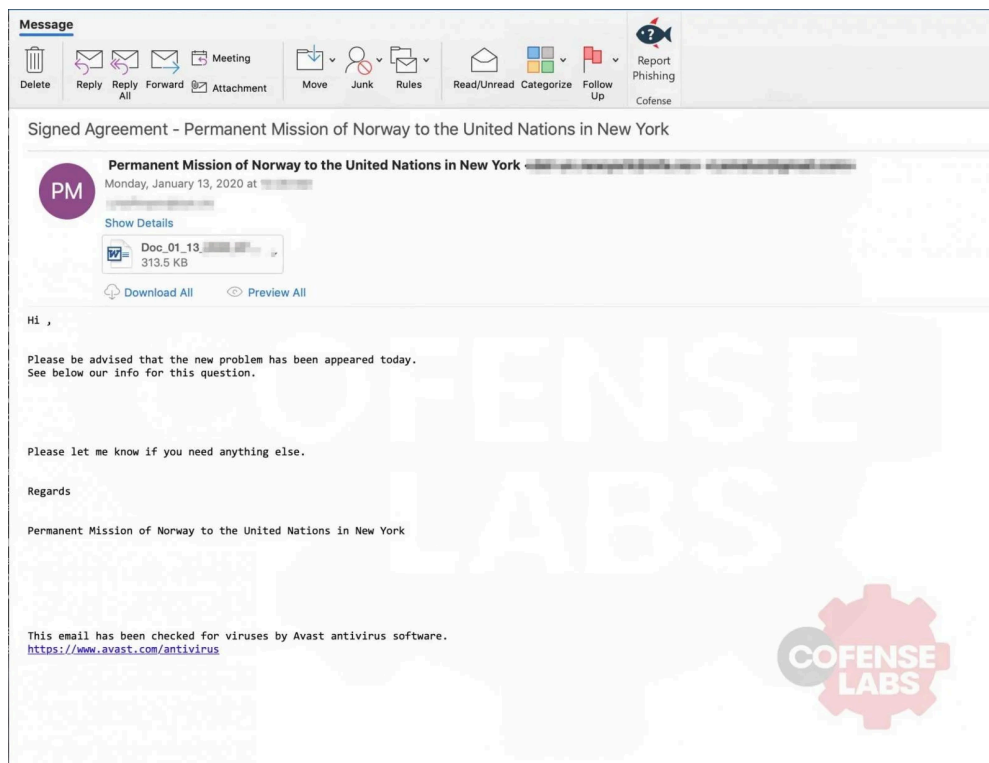
Visit Advertiser website [GO TO PAGE](#)

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.

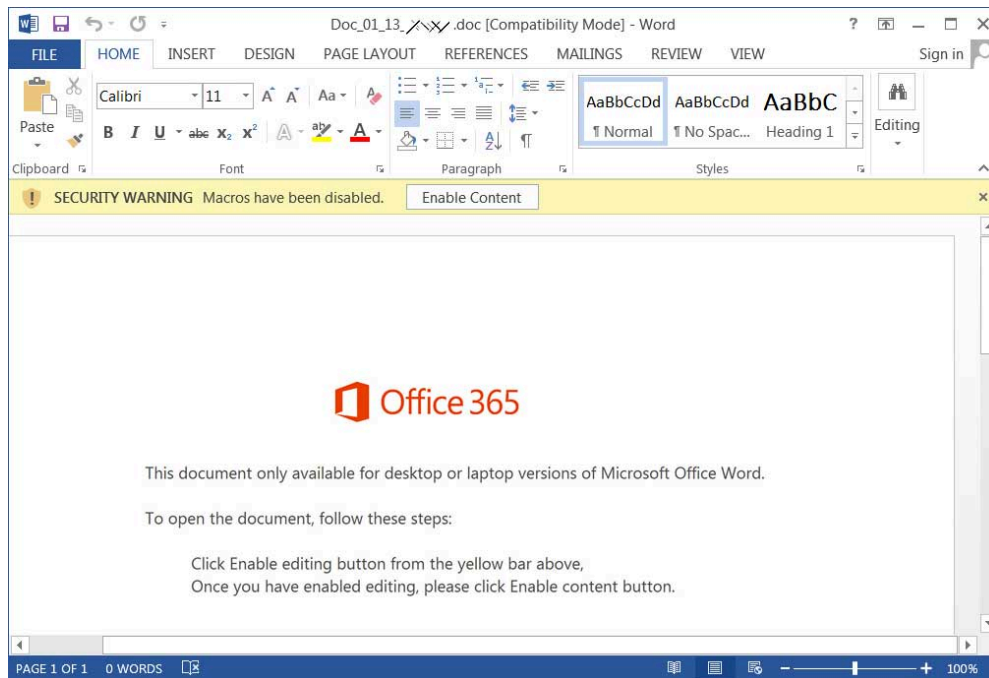
Regards

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.

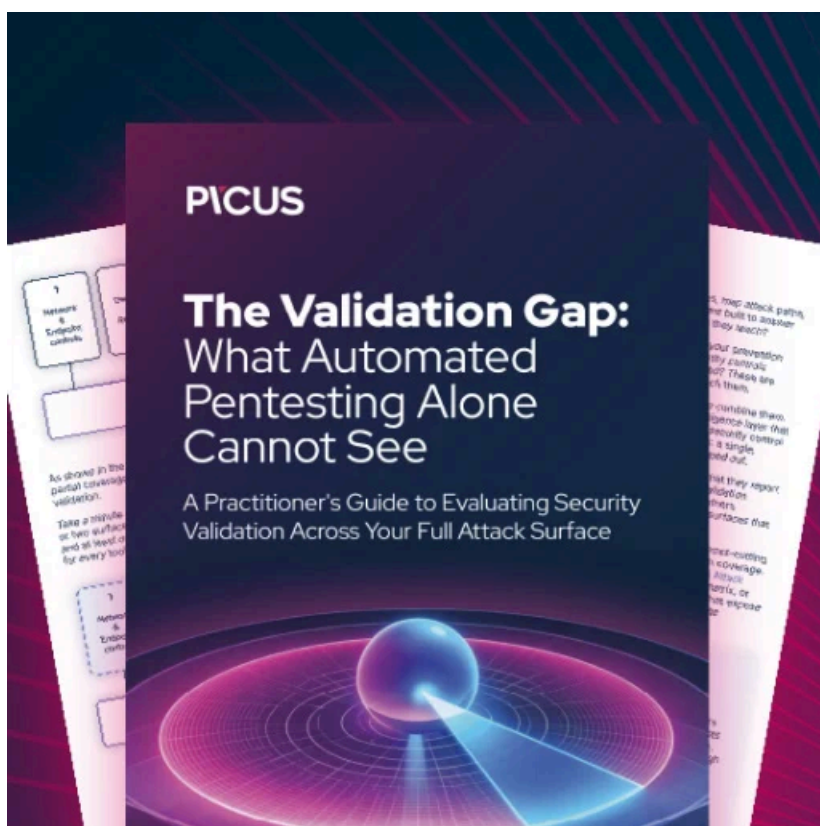
This is particularly worrisome for a UN network as ransomware operators are known to steal data before encrypting files, which could expose extremely sensitive diplomatic or government information.

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.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/united-nations-targeted-with-emotet-malware-phishing-attack/>