The Many Faces of Emotet

spamauditor.org/2020/10/the-many-faces-of-emotet/

By Thomas

October 19, 2020

You've probably heard the recent news of Microsoft's attempt to take down the Trickbot botnet. An interesting correlation with this event (though perhaps not directly related..) is the sudden uptick of Emotet email spam shortly after the Microsoft news hit. Emotet has the functionality to drop other strains of malware on machines that it compromises, and lately Trickbot has been one of the main ones dropped by Emotet. Perhaps these actors are flexing that Microsoft's attempts did nothing; or perhaps they fear this is only the beginning of botnet take downs and are increasing their efforts before they are fully taken down.

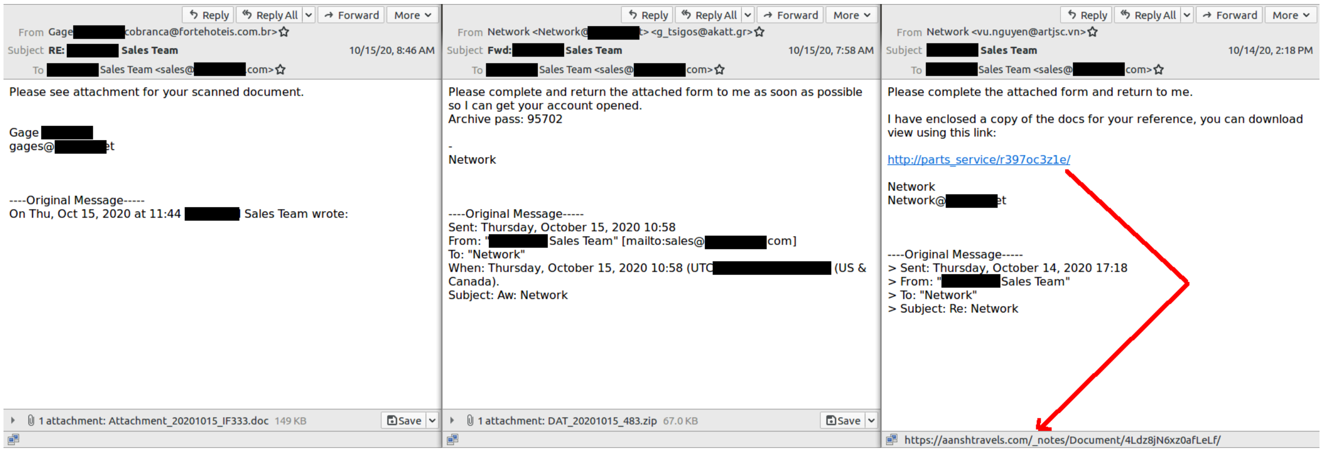
A recent bleeping computer article mentions a new malicious document template that is pretending to be a 'Windows Update'. It uses this to try to trick people into essentially 'enabling macros', which allows the successful execution of the Emotet malware.

However, it is odd that this is the approach in helping people avoid infection. You **should not** be getting to the point where you download a suspicious attachment, execute it, and see the fake Windows Update document asking you to Enable Editing/Enable Content. Although there are many different iterations of Emotet, there does appear to be a set of characteristics that all Emotet spam share to some degree. This article will be going over the most recent email spam templates we've seen from Emotet so that you can identify the spam without downloading and executing a malware file.

Emotet Spam Templates

We've broken down the latest Emotet spam campaign into pieces that anyone can understand and identify. A few months back we wrote a similar article on how to spot Emotet; this article will have more relevant information on current Emotet trends. Although Emotet has been shown to consistently change email templates, usually it is only enough to bypass spam filters and will still retain a familiar Emotet 'feel'. Emotet spam will not always contain all the characteristics which we will describe below, but we can be sure at least a subset will be present.

1. Emotet's Payload is either an Attachment or Link



From Gage [redacted]cobranca@fortehoteis.com.br>
Subject **RE: [redacted] Sales Team** 10/15/20, 8:46 AM
To [redacted] Sales Team <sales@[redacted].com>

Please see attachment for your scanned document.

Gage [redacted]
gages@[redacted]t

----Original Message-----
On Thu, Oct 15, 2020 at 11:44 [redacted] Sales Team wrote:

1 attachment: Attachment_20201015_IF333.doc 149 KB

From Network <Network@[redacted]t> <g_tsigos@akatt.gr>
Subject **Fwd: [redacted] Sales Team** 10/15/20, 7:58 AM
To [redacted] Sales Team <sales@[redacted]com>

Please complete and return the attached form to me as soon as possible
so I can get your account opened.
Archive pass: 95702

-
Network

----Original Message-----
Sent: Thursday, October 15, 2020 10:58
From: "[redacted] Sales Team" [mailto:sales@[redacted]com]
To: "Network"
When: Thursday, October 15, 2020 10:58 (UTC[redacted] (US &
Canada).
Subject: Aw: Network

1 attachment: DAT_20201015_483.zip 67.0 KB

From Network <vu.nguyen@artjsc.vn>
Subject [redacted] **Sales Team** 10/14/20, 2:18 PM
To [redacted] Sales Team <sales@[redacted]com>

Please complete the attached form and return to me.

I have enclosed a copy of the docs for your reference, you can download
view using this link:

http://parts_service/r397oc3z1e/

Network
Network@[redacted]t

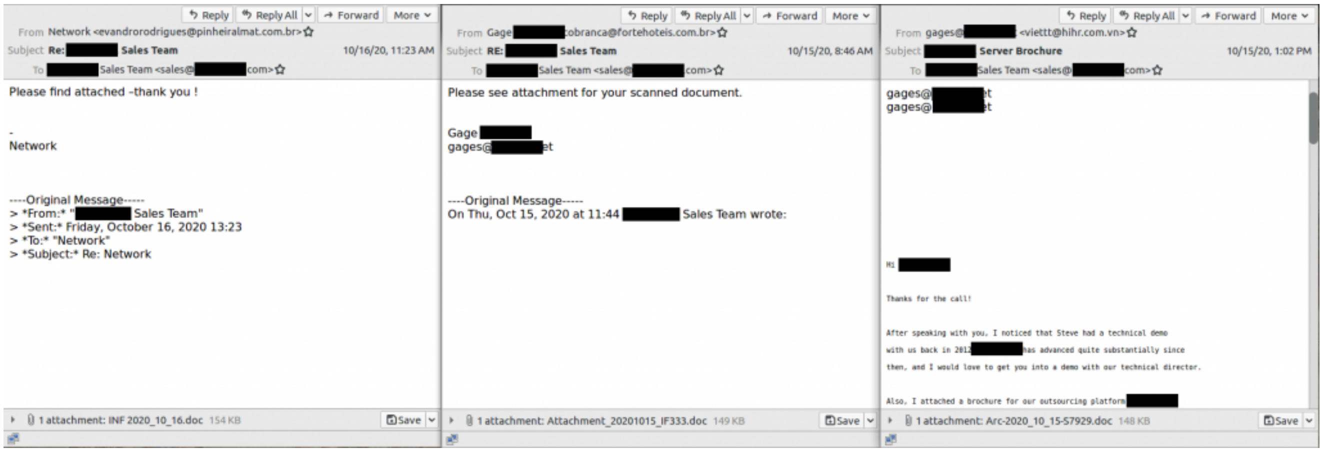
----Original Message-----
> Sent: Thursday, October 14, 2020 17:18
> From: "[redacted] Sales Team"
> To: "Network"
> Subject: Re: Network

https://aanshtravels.com/_notes/Document/4Ldz8jN6xz0afLeLf/

The redacted sections are mostly going to be domain of the recipient, or a 'spoofed' sender. Emotet loves to make you think the email is from somebody you know, or that knows you.

Fairly straightforward, the two ways the malware file will reach your computer will be via attachment or link. The .doc attachment is likely to be identified and blocked by common email antivirus scanners. The password protected zip file is the actors' method of evading these antivirus scans. With regards to links, in the current campaign we are noticing that the 'real' URL when you hover over the link is different than what the link represents. This 'fake' link method is commonly used by spammers to trick people into believing they are clicking a familiar link. Always check where the link goes, either by hovering over it or right clicking and copying the link's location to paste somewhere (but not into your browser!).

2. Emotet may Pretend to be part of an Existing Thread



From Network <evandrorodrigues@pinheiralmat.com.br>
Subject **Re: [redacted] Sales Team** 10/16/20, 11:23 AM
To [redacted] Sales Team <sales@[redacted]com>

Please find attached -thank you !

-
Network

----Original Message-----
> *From:* "[redacted] Sales Team"
> *Sent:* Friday, October 16, 2020 13:23
> *To:* "Network"
> *Subject:* Re: Network

1 attachment: INF 2020_10_16.doc 154 KB

From Gage [redacted]cobranca@fortehoteis.com.br>
Subject **RE: [redacted] Sales Team** 10/15/20, 8:46 AM
To [redacted] Sales Team <sales@[redacted]com>

Please see attachment for your scanned document.

Gage [redacted]
gages@[redacted]t

----Original Message-----
On Thu, Oct 15, 2020 at 11:44 [redacted] Sales Team wrote:

1 attachment: Attachment_20201015_IF333.doc 149 KB

From gages@[redacted] <viettt@hihr.com.vn>
Subject [redacted] **Server Brochure** 10/15/20, 1:02 PM
To [redacted] Sales Team <sales@[redacted]com>

gages@[redacted]t
gages@[redacted]t

Hi [redacted]

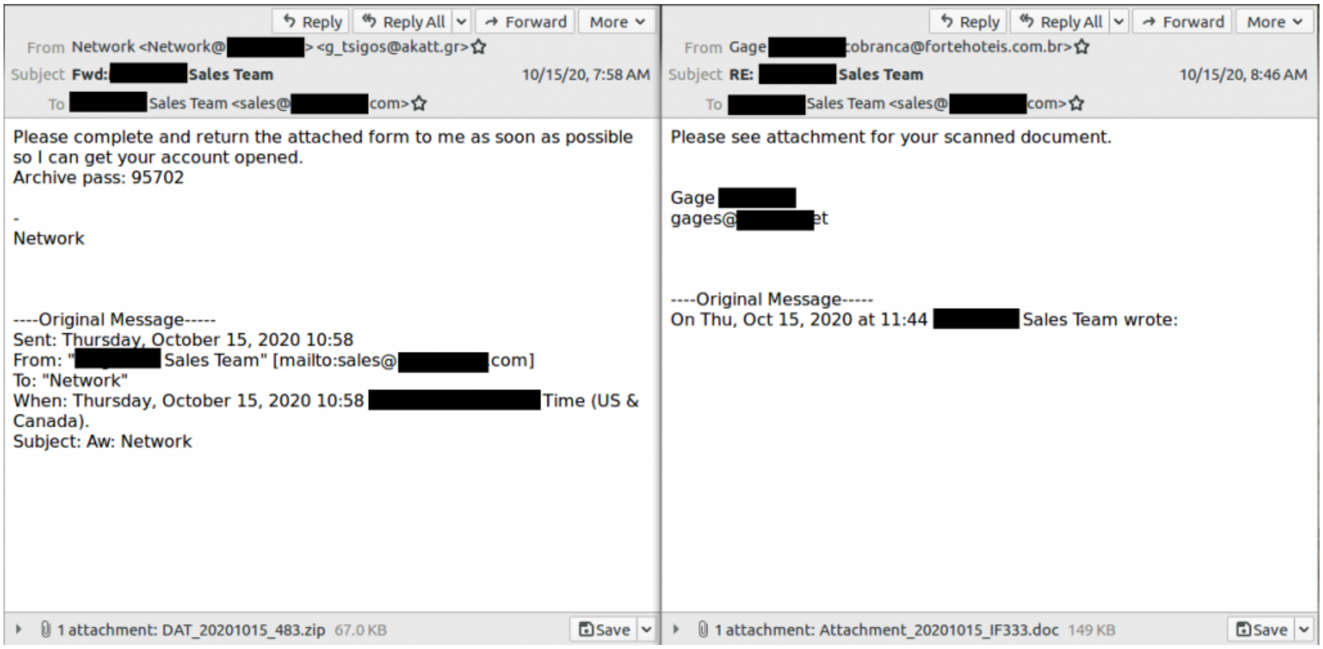
Thanks for the call!

After speaking with you, I noticed that Steve had a technical demo
with us back in 2012[redacted]has advanced quite substantially since
then, and I would love to get you into a demo with our technical director.

Also, I attached a brochure for our outsourcing platform[redacted]

1 attachment: Arc-2020_10_15-57929.doc 148 KB

Emotet spam may pretend to be part of an already existing conversation with you. You might recognize the '—-Original Message—-' line of the email, as it is a common method for Emotet to add this section. Emotet may also just copy and paste a real email reply chain that you might have had with someone in the past (third example in the above picture).



From Network <Network@[redacted]> <g_tsigos@akatt.gr>
Subject Fwd: [redacted] Sales Team 10/15/20, 7:58 AM
To [redacted] Sales Team <sales@[redacted] com>

Please complete and return the attached form to me as soon as possible so I can get your account opened.
Archive pass: 95702

-
Network

----Original Message-----
Sent: Thursday, October 15, 2020 10:58
From: "[redacted] Sales Team" [mailto:sales@[redacted] com]
To: "Network"
When: Thursday, October 15, 2020 10:58 [redacted] Time (US & Canada).
Subject: Aw: Network

1 attachment: DAT_20201015_483.zip 67.0 KB

From Gage [redacted] cobranca@fortehoteis.com.br>
Subject RE: [redacted] Sales Team 10/15/20, 8:46 AM
To [redacted] Sales Team <sales@[redacted] com>

Please see attachment for your scanned document.

Gage [redacted]
gages@[redacted] et

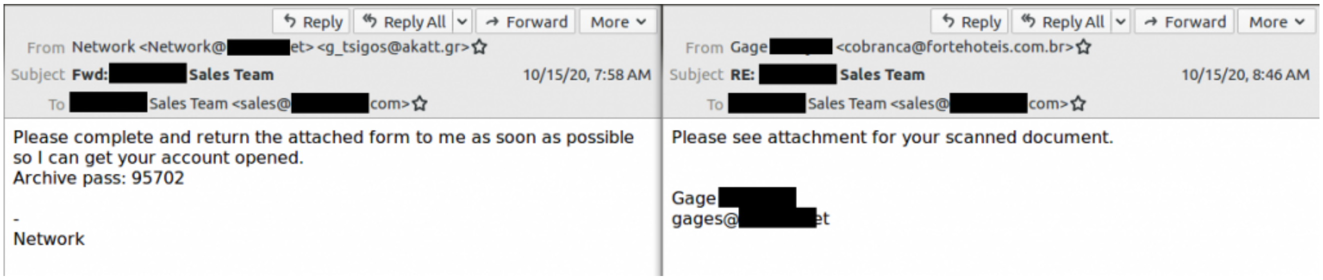
----Original Message-----
On Thu, Oct 15, 2020 at 11:44 [redacted] Sales Team wrote:

1 attachment: Attachment_20201015_IF333.doc 149 KB

Emotet also likes to create a fake ‘Reply’ or ‘Forward’ message by adding that to the beginning of the Subject line. If you have more expertise with email headers, you’ll be able to see why these are not genuine Reply or Forward email chains.

The Emotet malware has many capabilities, and one of them is data exfiltration. When Emotet compromises a computer, it has been seen to steal data such as your email address and name, your email contact list, and emails in your ‘Sent’ folder. With this data, these actors will eventually send spam (using a different compromised machine) with your name in the ‘From’, delivering malware to people on your contact list. This leads to our next point…

3. Emotet may send an Email where the From:Name appears to be Someone you know



From Network <Network@[redacted] et> <g_tsigos@akatt.gr>
Subject Fwd: [redacted] Sales Team 10/15/20, 7:58 AM
To [redacted] Sales Team <sales@[redacted] com>

Please complete and return the attached form to me as soon as possible so I can get your account opened.
Archive pass: 95702

-
Network

From Gage [redacted] <cobranca@fortehoteis.com.br>
Subject RE: [redacted] Sales Team 10/15/20, 8:46 AM
To [redacted] Sales Team <sales@[redacted] com>

Please see attachment for your scanned document.

Gage [redacted]
gages@[redacted] et

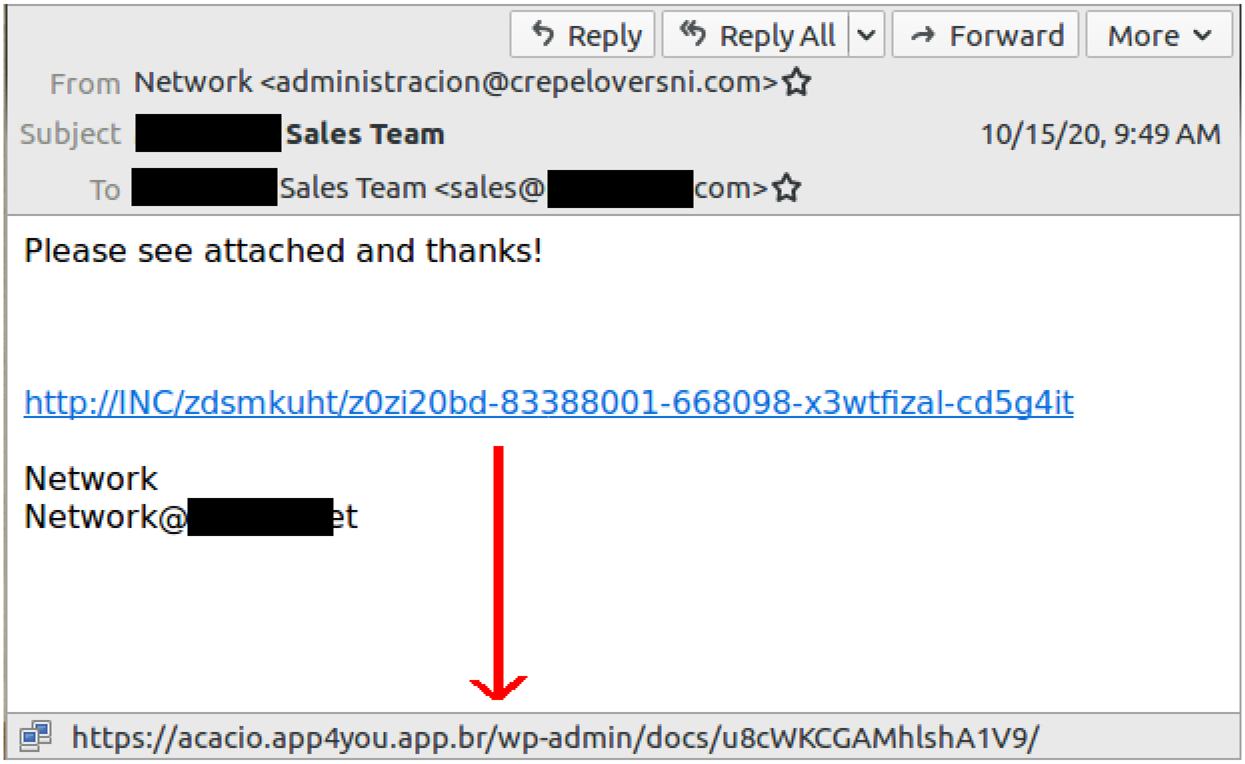
Emotet will sometimes ‘spoof’ the ‘From name’ (the name of the sender in the From line, not to be confused with the ‘domain’ or ’email address’ portion of the From line). Typically the name that is spoofed will be the name of someone whose machine was previously infected with the Emotet malware. It is likely that you will recognize this name, or have engaged in email communication with this person some time in the past. The first example of the above picture shows that sometimes the whole email address will be in the ‘From name’ (disguised as the address by putting brackets <> around it). Many mobile applications for email will only show you the ‘From name’ portion, hiding the actual email address. This method can potentially trick people into thinking they have received an email from someone they know, when in reality the actual sender is a different email address. It is a big red flag if you see two <email1@address><email2@address> in the From line of your email.

4. The latest Trend is that the Subject will contain the Recipient’s Domain

This particular trend will very likely change if it hasn’t already. We have seen a variety of different subject patterns such as Coronavirus News or Fake Invoices. The latest wave of Emotet spam has the ‘To name’ portion copied into the Subject line.

Concluding Remarks

A typical Emotet spam message will always have either an attachment or link. Afterwards, it will have some combination of the characteristics described in this article. However, be warned that there will be some cases with very little identifying characteristics, as seen below.



From Network <administracion@crepeloversni.com>

Subject [redacted] Sales Team 10/15/20, 9:49 AM

To [redacted] Sales Team <sales@[redacted]com>

Please see attached and thanks!

http://INC/zdsmkuht/z0zi20bd-83388001-668098-x3wtfizal-cd5g4it

Network
Network@[redacted]et

https://acacio.app4you.app.br/wp-admin/docs/u8cWKCGAMhlshA1V9/

Remain vigilant, and keep up to date with the latest Emotet trends in order to avoid getting compromised!