Case Study: Emotet Thread Hijacking, an Email Attack Technique

unit42.paloaltonetworks.com/emotet-thread-hijacking/

Brad Duncan September 23, 2020

By Brad Duncan

September 23, 2020 at 6:00 AM

Category: Malware, Unit 42

Tags: botnet, cyber crime, Emotet, MealyBug, TA542

This post is also available in: 日本語 (Japanese)

Executive Summary

Malicious spam (malspam) pushing Emotet malware is the most common email-based threat, far surpassing other malware families, with only a few other threats coming close.

In recent weeks, we have seen significantly more Emotet malspam using a technique called "thread hijacking" that utilizes legitimate messages stolen from infected computers' email clients. This malspam spoofs a legitimate user and impersonates a reply to the stolen email. Thread hijacked malspam is sent to addresses from the original message.

This technique is much more effective than less sophisticated methods, which many people have now learned to spot. The approach is more successful at convincing potential victims to click on an attached file, or to click on a link to download a malicious Word document with macros designed to infect a user with Emotet.

Here, we review a case study of Emotet's thread hijacking process so we can better recognize and understand this technique.

Palo Alto Networks customers are protected from this threat because our Threat Prevention security subscription detects and prevents these types of Emotet infections. AutoFocus users can track Emotet activity using the Emotet tag.

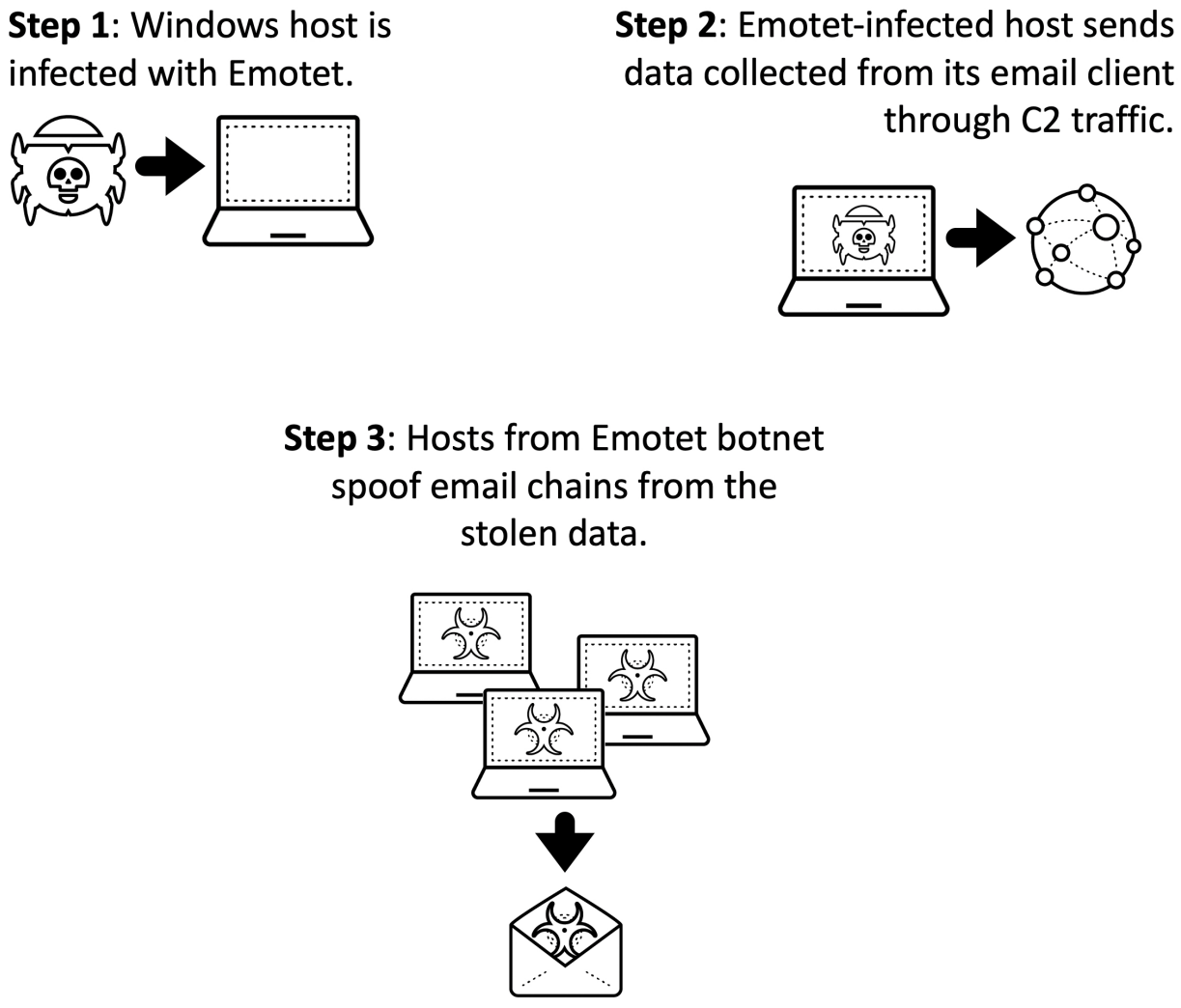

Figure 1. Visual representation of Emotet's thread hijacking process.

Case Study Timeline

To illustrate Emotet's thread hijacking process, our case study focuses on an infection from Sept. 3, 2020. In this example, Emotet hijacks the most recent email in an Outlook inbox from an infected host.

The timeline is:

- 15:35 UTC – Legitimate message received by email client on host.
- 16:31 UTC – Host infected with Emotet.
- 16:34 UTC – Legitimate message collected from infected host is sent through Emotet command and control (C2) traffic.
- 18:22 UTC – Emotet botnet sends spoofed email using legitimate message from the infected host.

This process took one hour and 51 minutes to progress from the infection to the arrival of a thread-hijacked email.

Legitimate Email From the Infected Host

In our example, a vulnerable Windows 10 host used Microsoft Outlook as its email client. Outlook was synchronized to a Microsoft account at k*********.r*******@outlook.com (we have redacted information from the email addresses for this case study). The most recent message in the infected host's email client is shown in Figure 2, and we have loaded a redacted copy of the legitimate email to GitHub.

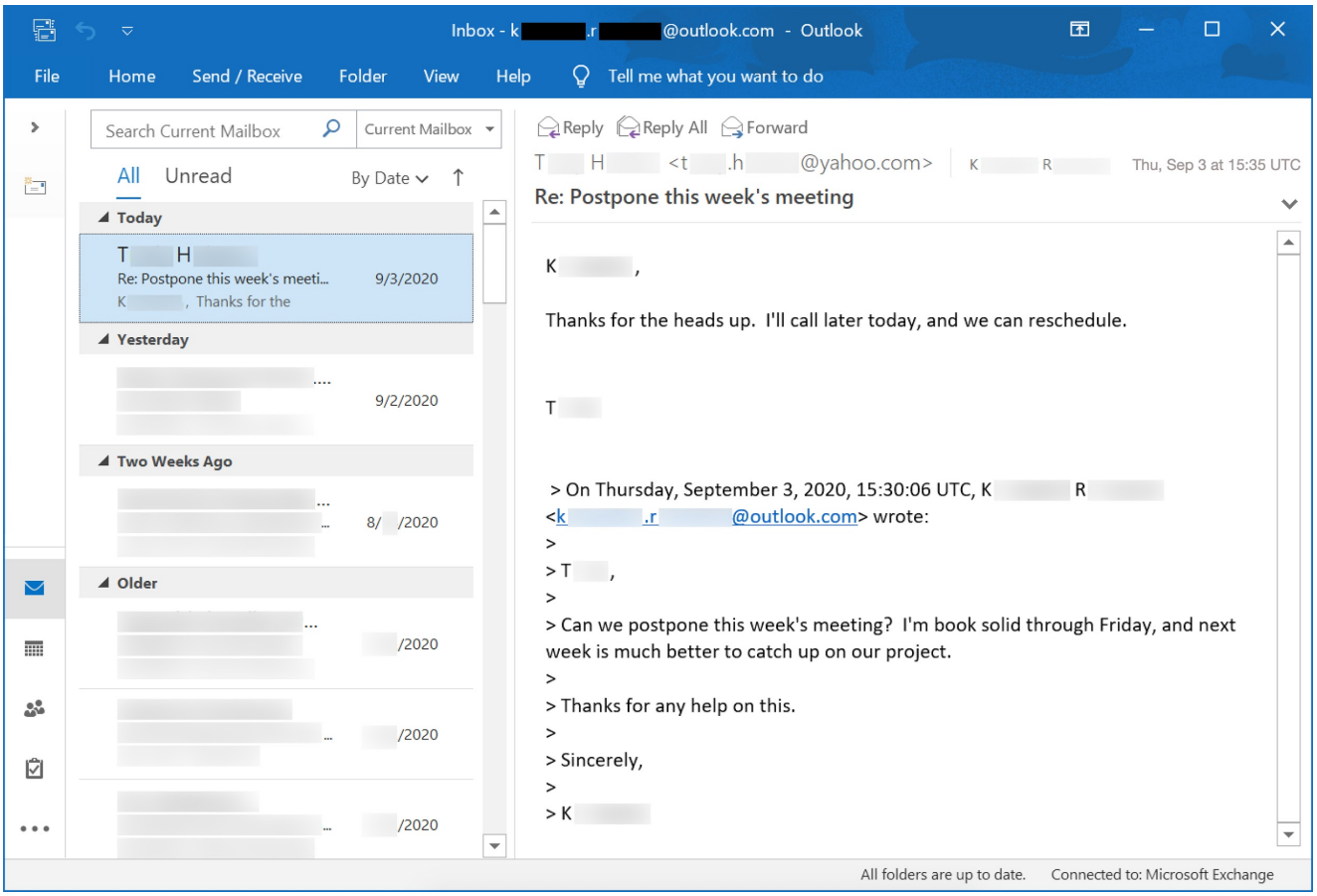

Figure 2. Most recent email from an infected host's Outlook client.

As we see in Figure 2, the most recent email was received at 15:35 UTC, approximately one hour before the host was infected with Emotet. This email is a response from t****.h******@yahoo.com to a previous message from k*********.r*******@outlook.com.

Data Exfiltration Through C2 Traffic

Emotet uses HTTP POST requests over C2 traffic to send data collected from the infected host. This data is encoded or otherwise encrypted before it is sent over HTTP.

Most of these POST requests contain only a small amount of encoded data from the infected host, often much less than 1,000 bytes. These requests contain an extra 4 kB of data for padding and form header data. Figure 3 shows a typical example of Emotet C2 traffic from our case study.

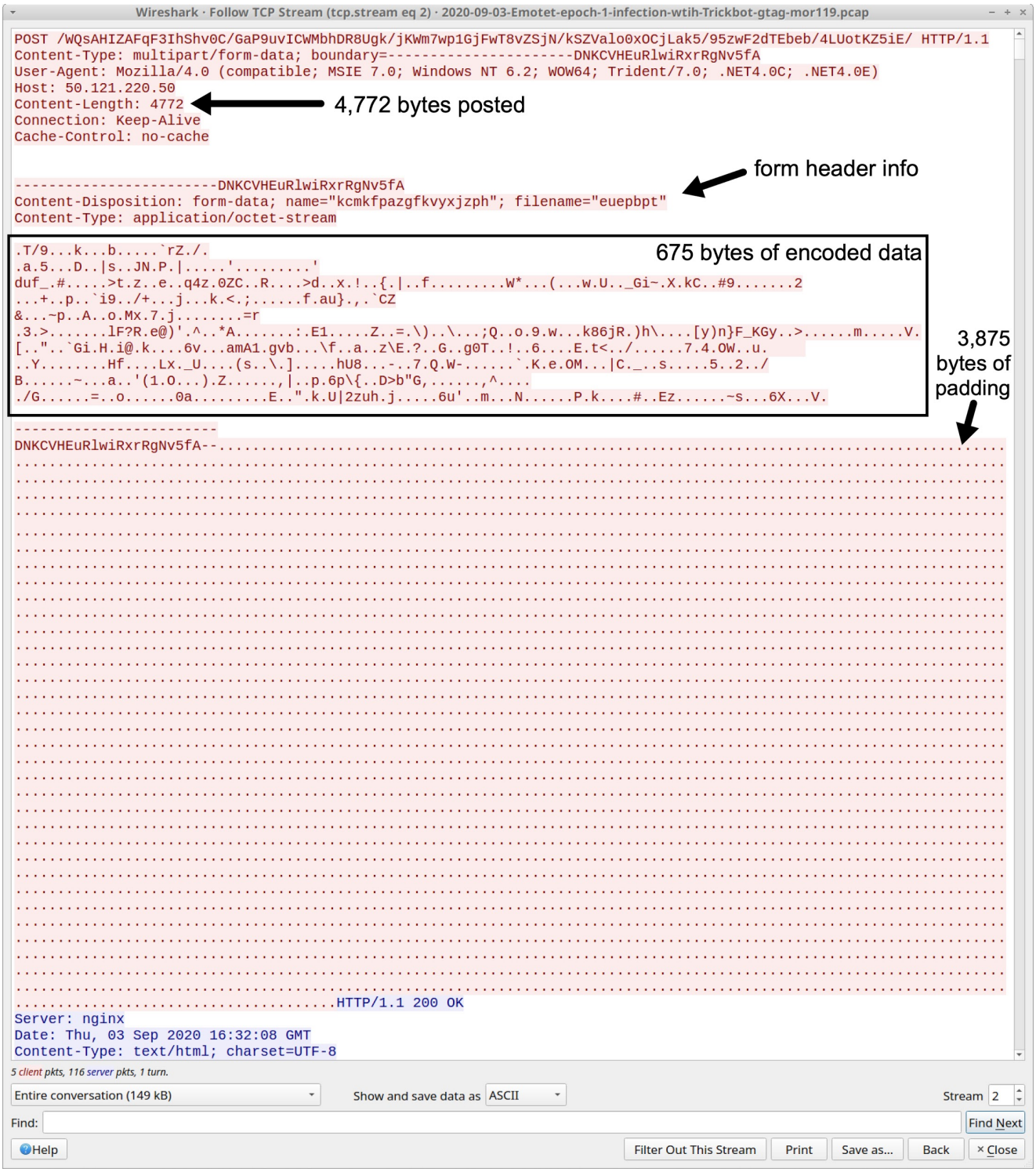

Figure 3. Example of HTTP POST data from Emotet C2 traffic in our case study.

Since the amount of encoded data is so small, it does not contain any email chain data collected from the infected user's email client. However, at 16:34 UTC, we find 13.9 kB of encoded data sent over Emotet HTTP C2 traffic as shown in Figure 4.

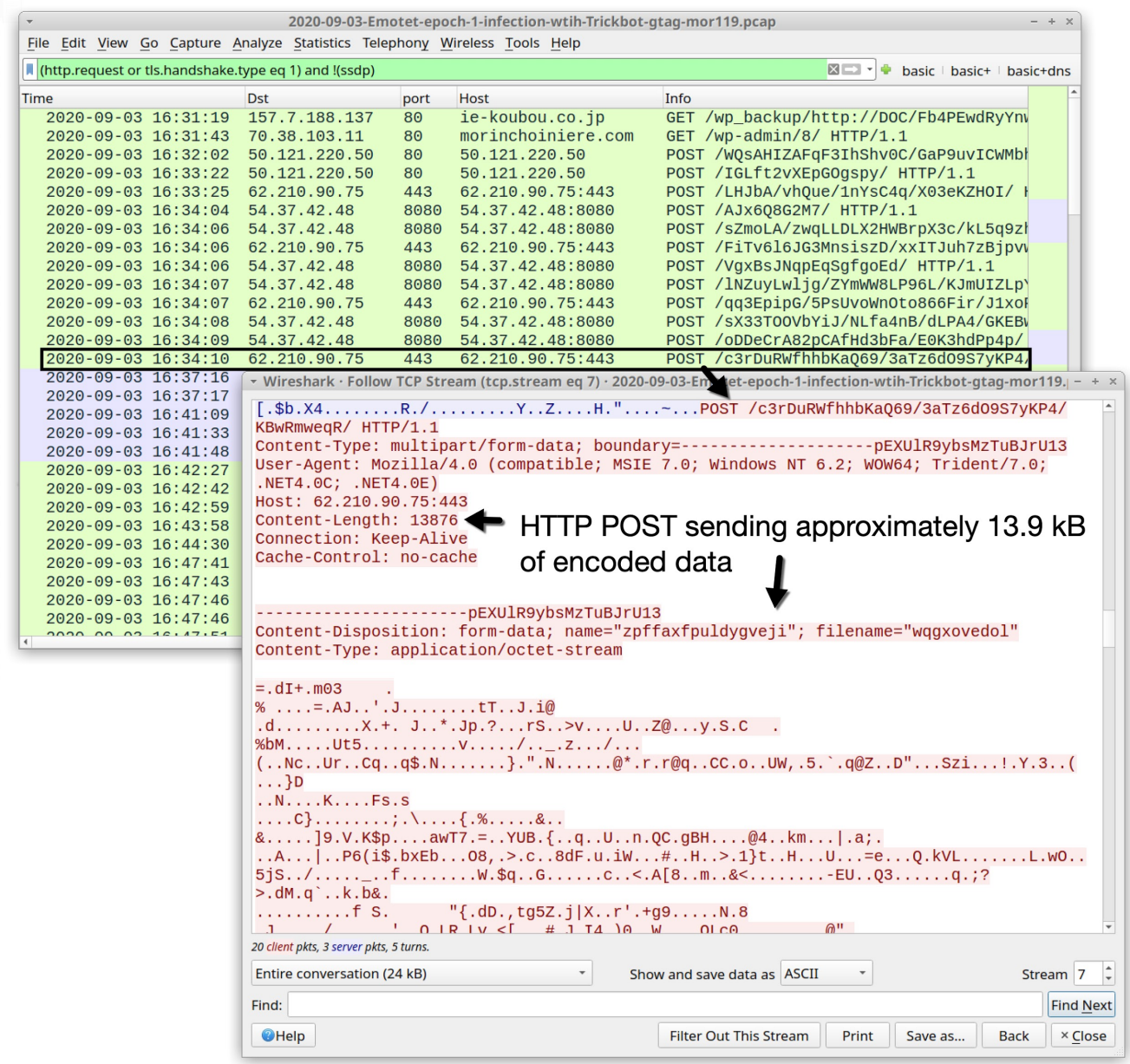

Figure 4. Approximately 13.9 kB of encoded data in Emotet C2 traffic at 16:34 UTC.
This amount is large enough to contain email chain data collected from the infected Windows host. It is the only significant amount of data sent in HTTP POST requests from the Emotet-infected host before we find the thread-hijacked email at 18:22 UTC.

Spoofed Message From Hijacked Email

At 18:22 UTC, a spoofed email was received by t****.h******@yahoo.com, the Yahoo account that had sent the most recent message in correspondence to the infected host. It contains an attached Word document with macros for Emotet. This message is shown in Figure 5, and we have loaded a copy of the spoofed email to GitHub.

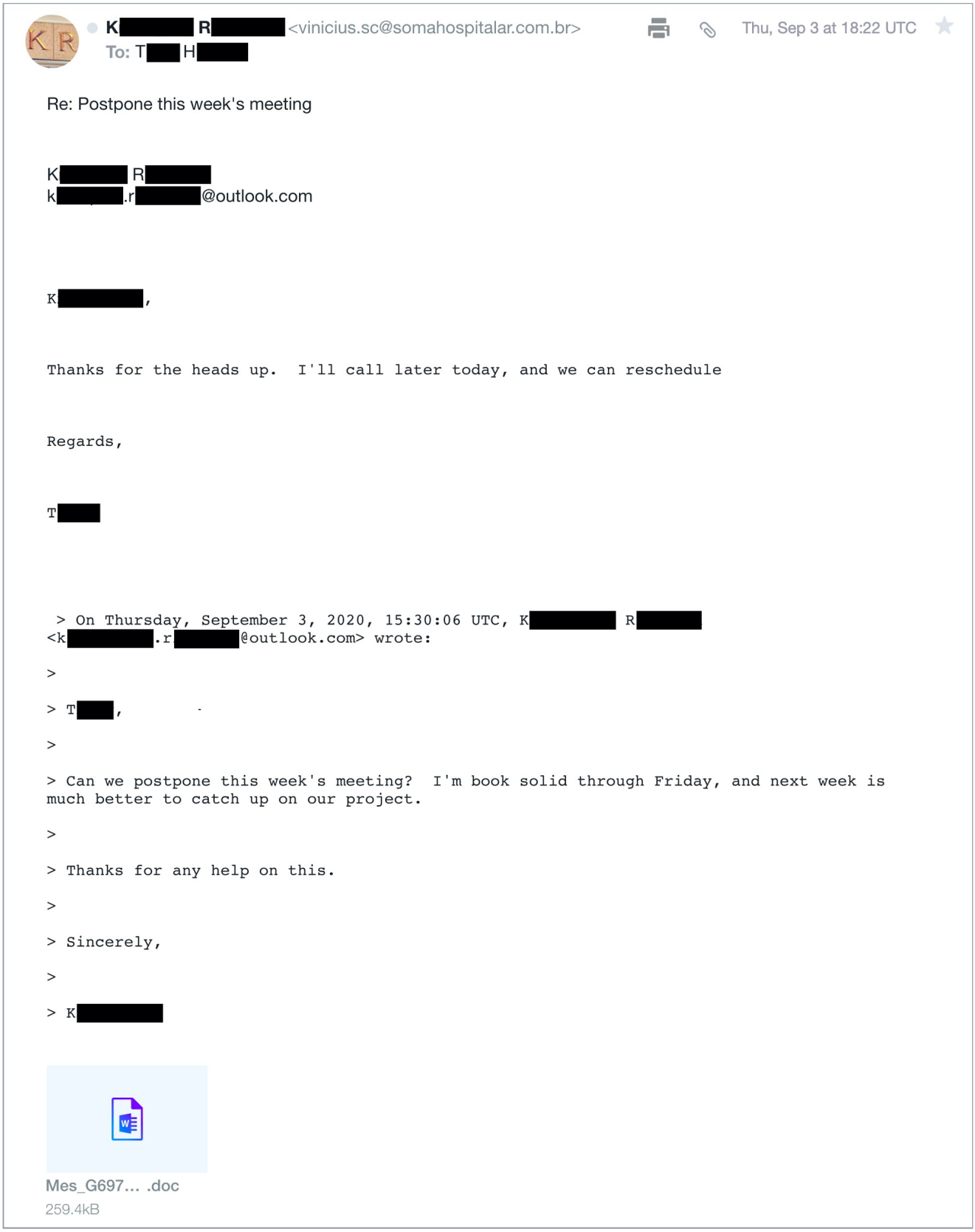

Figure 5. Hijacked email sent from the Emotet botnet.
The message is a reply to t****.h******@yahoo.com that spoofs k*********.r*******@outlook.com from the infected host.

These thread-hijacked messages either have an attached file, or they have a link to download a malicious Word document with macros designed to infect a vulnerable host with Emotet.

Emotet's thread-hijacked message from this case study spoofed the name in the sending address line from the infected host. Headers from the spoofed message indicate the actual sender may have been from a botnet host in Brazil, or a Brazil-based host may have been used to relay the message. Botnet hosts from all over the world are used to send these thread-hijacked messages from Emotet infections.

```
Return-Path: <vinicius.sc@somahospitalar.com.br>
Received: from 191.252.199.165 (EHLO mail199165.hm1831.locaweb.com.br)
 by 10.197.33.12 with SMTPs; Thu, 3 Sep 2020 18:22:33 +0000
X-Originating-Ip: [191.252.199.165]
Received-SPF: pass (domain of somahospitalar.com.br designates 191.252.199.165 as permitted
sender)
Authentication-Results: atlas321.free.mail.bf1.yahoo.com;
 dkim=unknown;
 spf=pass smtp.mailfrom=somahospitalar.com.br;
 dmarc=unknown
X-Apparently-To: t****.h******@yahoo.com; Thu, 3 Sep 2020 18:22:33 +0000
Received: from mcbain0004.email.locaweb.com.br (189.126.112.85) by
mail199145.hm1831.locaweb.com.br id ha4q682n8lgj for <t****.h******@yahoo.com>; Thu, 3 Sep 2020
15:22:11 -0300 (envelope-from <vinicius.sc@somahospitalar.com.br>)
X-Original-To: <t****.h******@yahoo.com>
Received: from LEONARD0039.mail.collab.local (martin0001.email.locaweb.com.br [189.126.112.73])
        by mcbain0004.email.locaweb.com.br (Postfix) with ESMTP id 7D02D180FD3
        for <t****.h******@yahoo.com>; Thu,  3 Sep 2020 15:22:11 -0300 (-03)
Received: from [200.87.242.147] (200.87.242.147) by
 LEONARD0039.mail.collab.local (10.30.188.44) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256) id
 15.1.2044.4; Thu, 3 Sep 2020 15:22:35 -0300
Date: Thu, 3 Sep 2020 14:22:10 -0400
Locaweb_Exchange: Yes
From: K********* R******* <vinicius.sc@somahospitalar.com.br>
To: T**** H****** <t****.h******@yahoo.com>
Subject: Re: Re: Postpone this week's meeting
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="--272164461781354078254733154144247O"
Message-ID:
        <8cadda8f-2f82-407d-9688-a3a2533458b4@LEONARD0039.mail.collab.local>
X-Originating-IP: [200.87.242.147]
X-ClientProxiedBy: PENNY0001.mail.collab.local (10.30.190.2) To
 LEONARD0039.mail.collab.local (10.30.188.44)
X-AuthUser: vinicius.sc@somahospitalar.com.br
Content-Length: 360155
```

Figure 6. Header lines from hijacked message sent to t****.h******@yahoo.com.

These spoofed messages tend to be the most recent emails from a victim's email client because those are the most likely to fool someone.

Of note, we cannot always assume the spoofed sending address is from an infected victim. If the original message from an infected victim has multiple recipients, a hijacked email could spoof one of the other recipients.

Conclusion

We've stored an example of the legitimate email that was hijacked in this case study.

We've also stored an example of the spoofed messages sent from the Emotet botnet.

The pcap of infection traffic from this case study is also available.

This case study shows an example of Emotet thread hijacking so we can better understand how Emotet malware utilizes this technique. Emotet is a very active threat that constantly updates its malware in an attempt to evade detection. This vector of infection can reach a great deal of potential victims.

However, organizations with effective spam filtering that follow best security practices have a much lower risk from this infection vector. Palo Alto Networks customers are further protected from this threat, because our Threat Prevention security subscription detects and prevents these types of Emotet infections. AutoFocus users can track Emotet activity using the Emotet tag.