

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

By Arnold Osipov

Archived: 2026-04-05 13:09:41 UTC

Introduction

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.

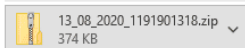
This particular QakBot campaign also includes two new techniques: a bypass of the content disarm and reconstruction (CDR) technology through zipping the Word document, and a bypass of child-parent pattern detection because Visual Basic is executed using Explorer.

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*.



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.

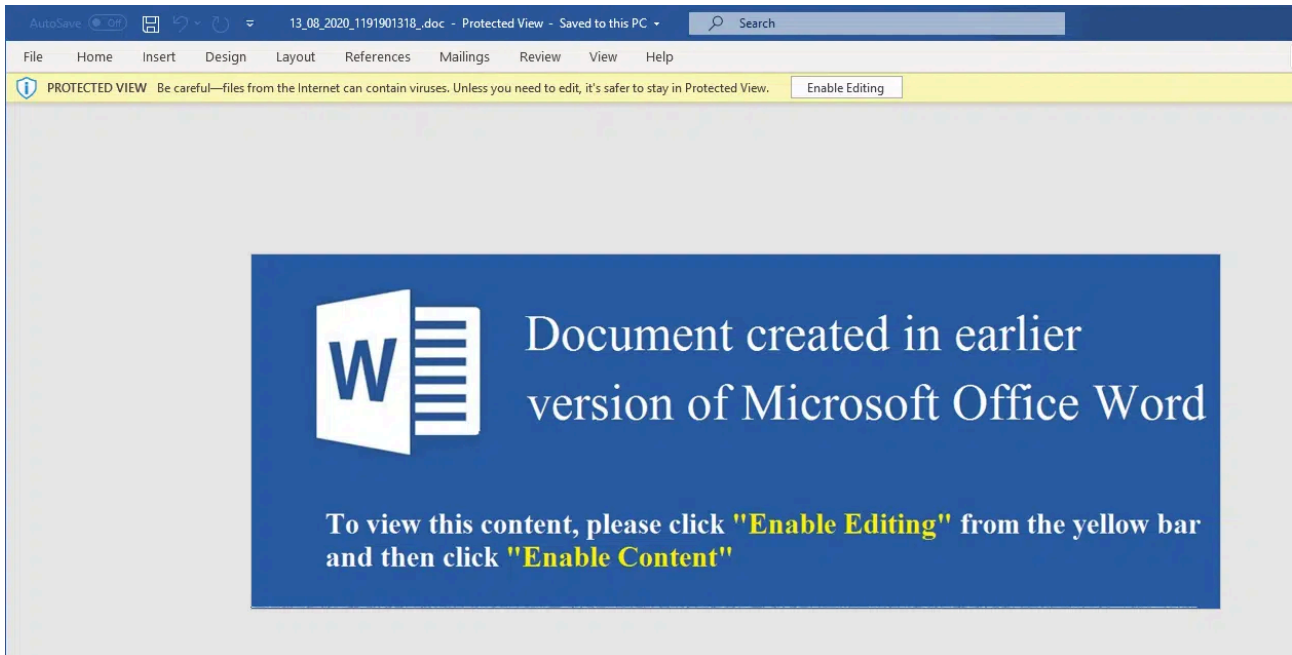


Figure 2: The maldoc asks for the target to enable editing and to enable content

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.

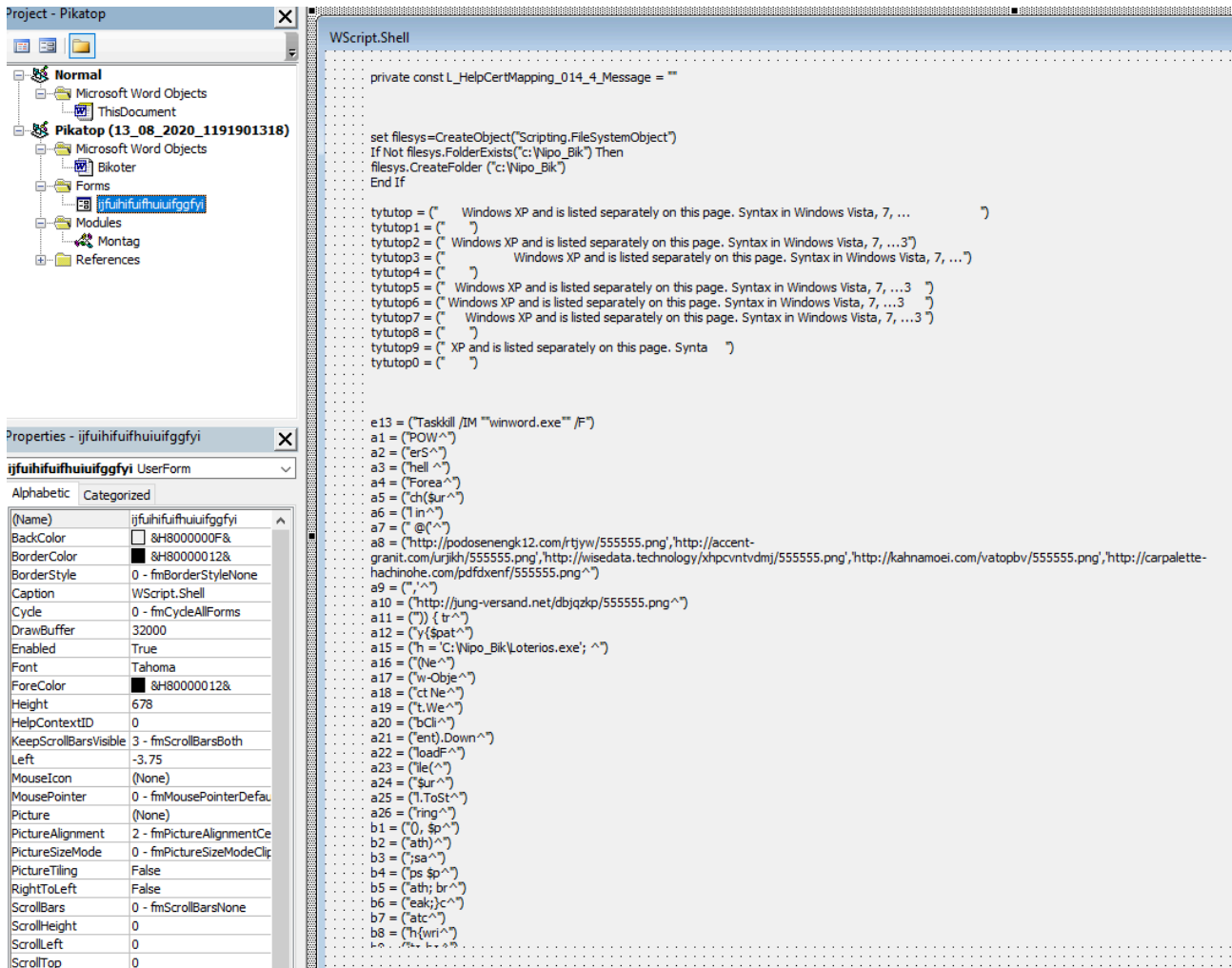


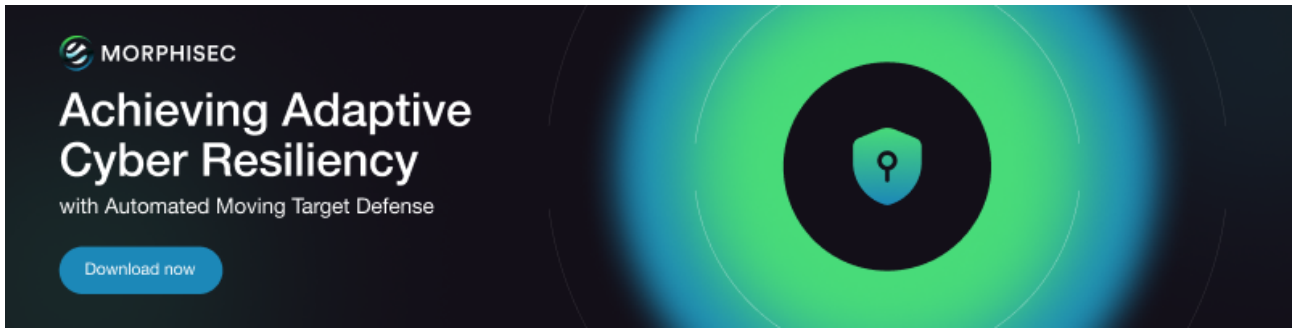
Figure 4: WScript.Shell

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. Morphisec's [Automated Moving Target Defense](#) technology 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):

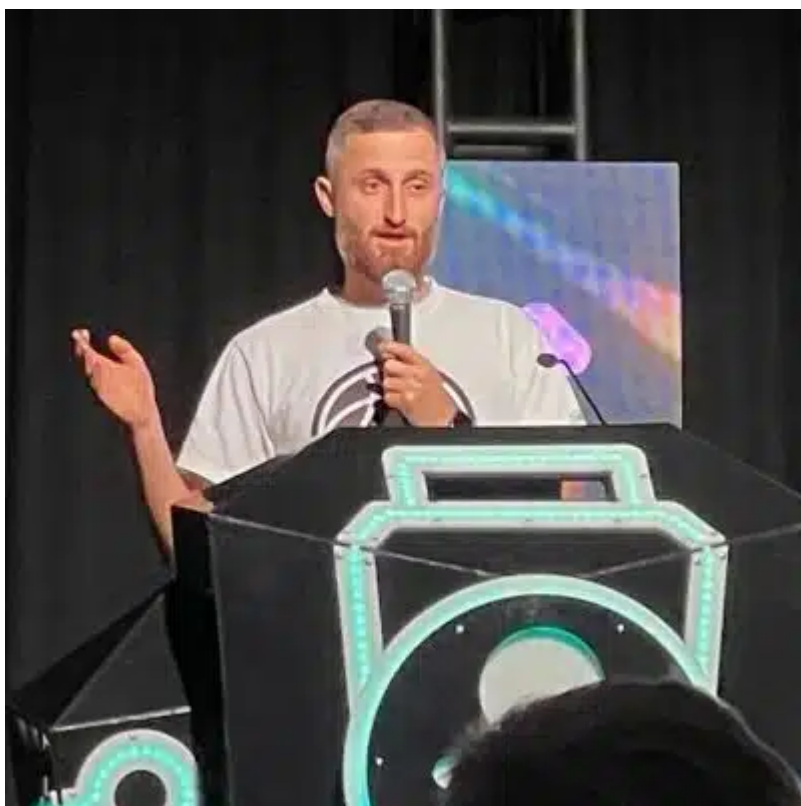
- 791179b20d936cf76d885d1949d4a50a295b4918
- e36af99c29a474f82cd57f2736b9d1b5ecadfffd
- b841a34ec95bd1c3d1afe6d578aade9439f3c38
- e7480e6adb6af1c992bc91605e4bba682d76c43d
- 952917654b5c0328a31c3bbd8c7bf7a70a4a82e7
- 58b023e339a9557adbdbf0de63c0584500438b9b
- 147101a88cc1fe91bac9161425986a1c1e15bc16

URLs:

- hxxp://akindustrieschair.com/smuvtnrgvmd/55555.png
- hxxp://nashsbornik.com/rqzvoxtjyhwh/55555.png
- hxxp://maplewoodstore.com/rmwclxnbeput/55555.png
- hxxp://akersblog.top/kipql/55555.png
- hxxp://all-instal.eu/mgpui/55555.png
- hxxp://ankaramekanlari.net/vmnzwr/55555.png
- hxxp://optovik.store/bkatah/55555.png
- hxxp://store.anniebags.com/qyvbyjaiu/55555.png
- hxxp://atsepetine.com/evuyrurweyib/55555.png
- hxxp://duvarsaatcisi.com/gbmac/55555.png
- hxxp://rijschoolfastandserious.nl/rprmlow/11111.png
- hxxp://nanfeiqiaowang.com/tsxwe/11111.png

- <http://forum.insteon.com/suowb/111111.png>
- <http://webtest.pp.ua/yksrpucvx/111111.png>
- <http://quoraforum.com/btmlxjxmyxb/111111.png>
- <http://quickinsolutions.com/wfqggeott/111111.png>
- <http://bronco.is/pdniovzkgwwt/111111.png>
- <http://studiomascellaro.it/wnzzsbzbd/111111.png>
- <http://craniotylla.ch/vzufnt/111111.png>
- <http://marineworks.eu/dwaunrsamlbq/111111.png>

About the author



Arnold Osipov

Malware Researcher

Arnold Osipov is a Malware Researcher at Morphisec, who has spoken at BlackHat and and been recognized by Microsoft Security for his contributions to malware research related to Microsoft Office. Prior to his arrival at Morphisec 6 years ago, Arnold was a Malware Analyst at Check Point.

Source: <https://blog.morphisec.com/qakbot-qbot-maldoc-two-new-techniques>