A New DatopLoader Delivers QakBot Trojan

blog.minerva-labs.com/a-new-datoploader-delivers-qakbot-trojan

- Tweet
-

A new phishing campaign delivers a Qakbot (also known as Qbot or Quakbot), using DatopLoader(aka Squirrelwaffle).

DatopLoader(aka Squirrelwaffle) compromises victims via a malspam campaign and provides threat actors with the initial foothold into systems and victims' network environments. This can then be used to facilitate further compromises or additional malware infections, which depends on how adversaries wish to monetize their access.

Yesterday (November 8, 2021), we spotted a malicious excel file trying to execute three different files using regsvr32.exe:

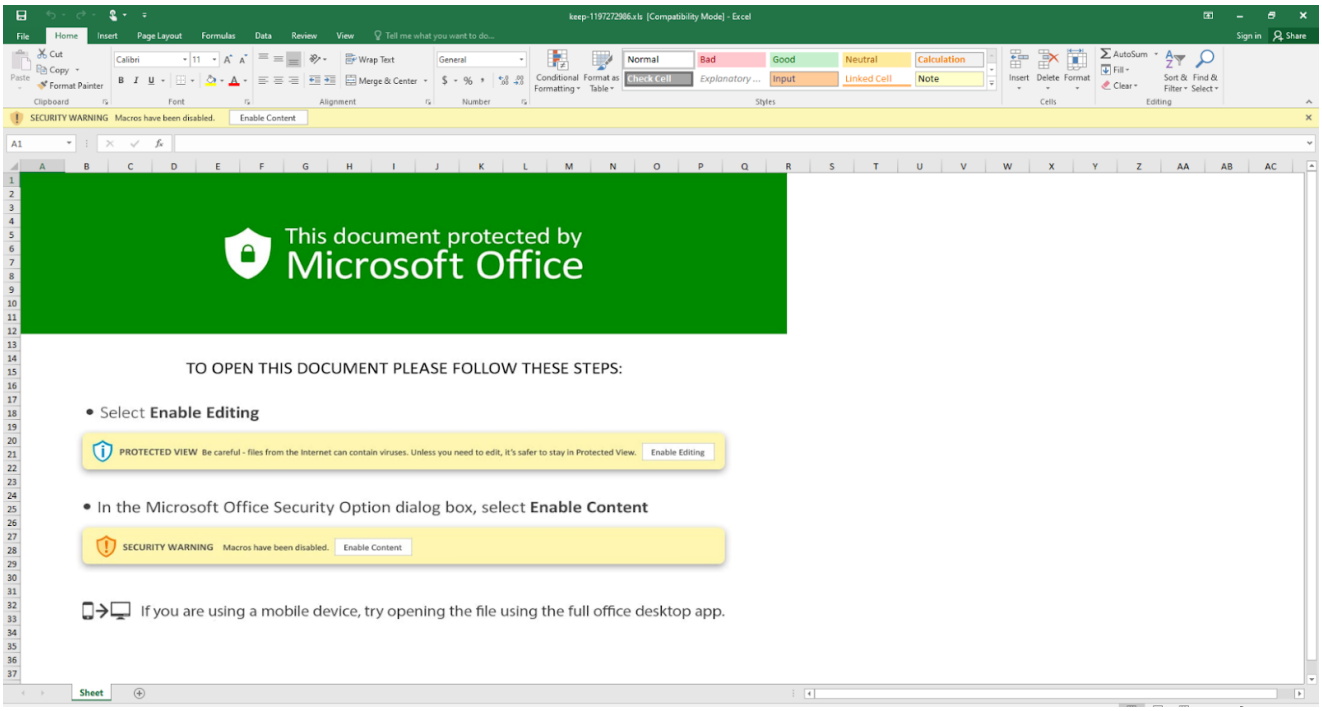
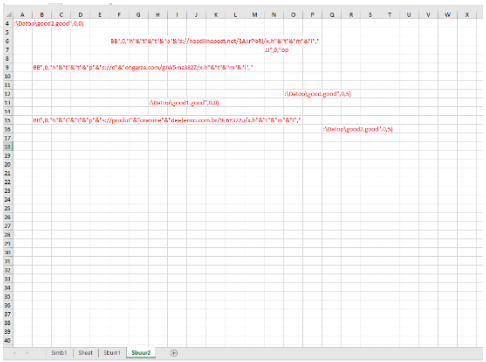
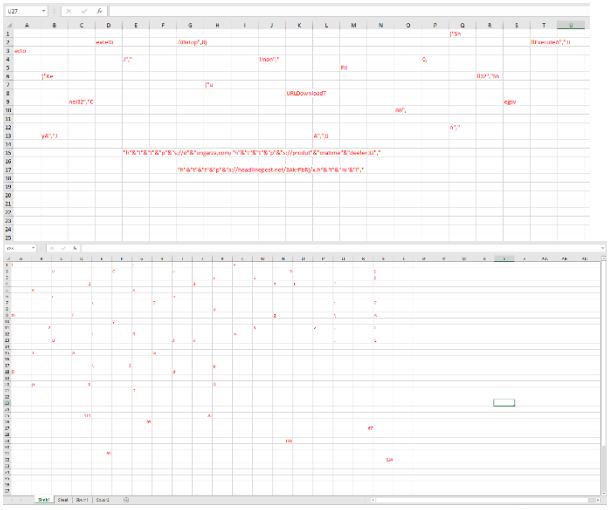


Figure 1 Malicious Excel File

At first glance, this excel file contains one sheet which guides the user to enable the macro, ultimately leading to a network connection and eventual delivery of QakBot. Uncharacteristically, this sheet does not contain the usual culprits of a malicious file i.e. Excel Macro 4, sheet password protection, etc. This makes us suspicious. We enabled a Developer Tab in excel and checked this file's VBA project.

We found three more sheets that were hidden, and switched them to visible mode. All three sheets contained Excel Macro 4; one of the sheets contained letters, numbers, and symbols, and two others seemed to be responsible for creating a new folder using kerner32.dll!CreateDirectoryA, downloading three files from three different domains, saving those files on a local disk in a create folder , and executing each one of them using regsvr32.exe:





- The folder created was named “Datop” under a C:\.
- The downloaded files were named C:\Datop\good.good, C:\Datop\good1.good and C:\Datop\good2.good.

All three downloaded files were found to be Qakbot banking trojans’ DLLs. Qakbot, also known as Pinkslipbot, Qbot, and Quakbot. This is a notorious Banking Trojan designed to steal account credentials and online banking session information, leading to account takeover fraud.

This Squirrelwaffle sample employs the same delivery scheme as the one that was posted by Malware Traffic earlier this month.

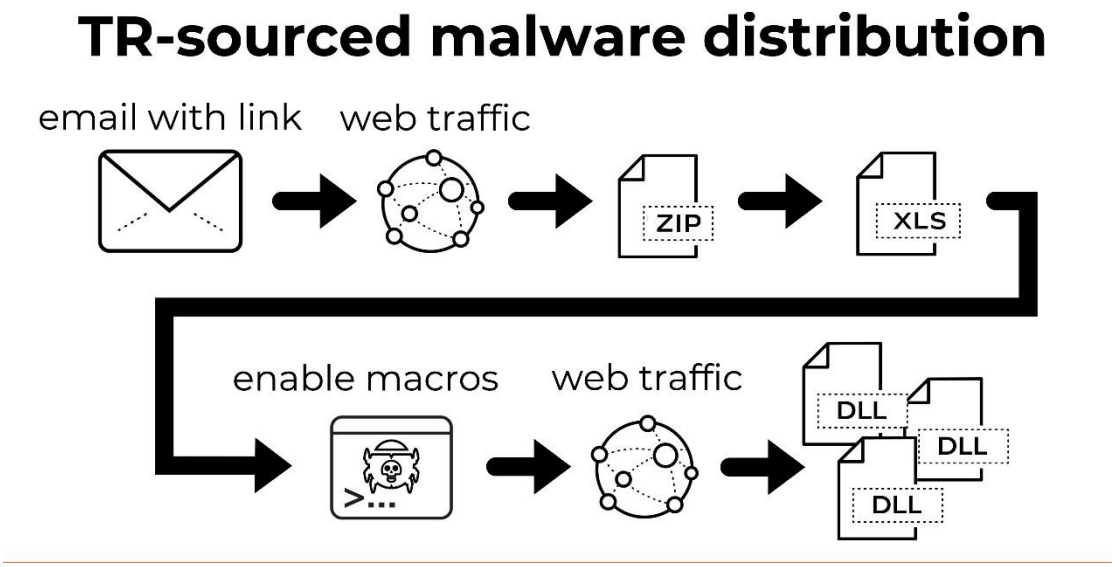
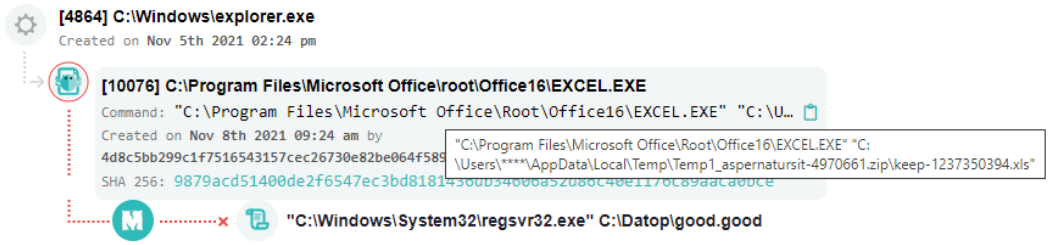


Figure 2 Squirrelwaffle delivery scheme by Malware Traffic

Minerva Lab’s Malicious Document Protection module prevents the execution of Squirrelwaffle-like malware, safeguarding the organization from a mass infection:



IOC's

Domains:

- https://dongarza[.]com/gJW5ma382Z/x.html
- https://headlinepost[.]net/3AkrPbRj/x.html
- https://produtoratimedeelenco[.]com.br/9E6Y322u/x.html

Hashes:

- good.good - 9E27F618EC40BEDBAFBA4FECC1EE84A8 - QakBot
- good1.good - D5A5FB1FBDFEF257653D08A65AC7730A - QakBot
- good2.good - 8EC26FF6330BF890190944DE65BD2B6B - QakBot

Resources

- https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html
- https://blog.cyberint.com/qakbot-banking-trojan

Talk To Minerva Labs