Insights Into an Excel 4.0 Macro Attack using Qakbot Malware

perception-point.io/insights-into-an-excel-4-0-macro-attack-using-qakbot-malware

June 15, 2021

Overview.

In this article, we will present an extensive email security attack that uses Excel 4.0 macros (XLM) to deliver Qakbot malware. Qakbot is a modular information stealer whose original purpose was primarily as a banking Trojan but currently serves as a loader for other crimeware.

In this campaign, the attacker conceals the malicious payload by embedding it deeply with other pieces of content. The attacker sends a malicious email containing a URL, which retrieves a zip file with the target's name as the file name. This zip archive contains a malicious Excel document (xls) that, when opened, runs an Excel 4.0 macro code that downloads and executes a malicious DLL/Qakbot malware to the user's machine.

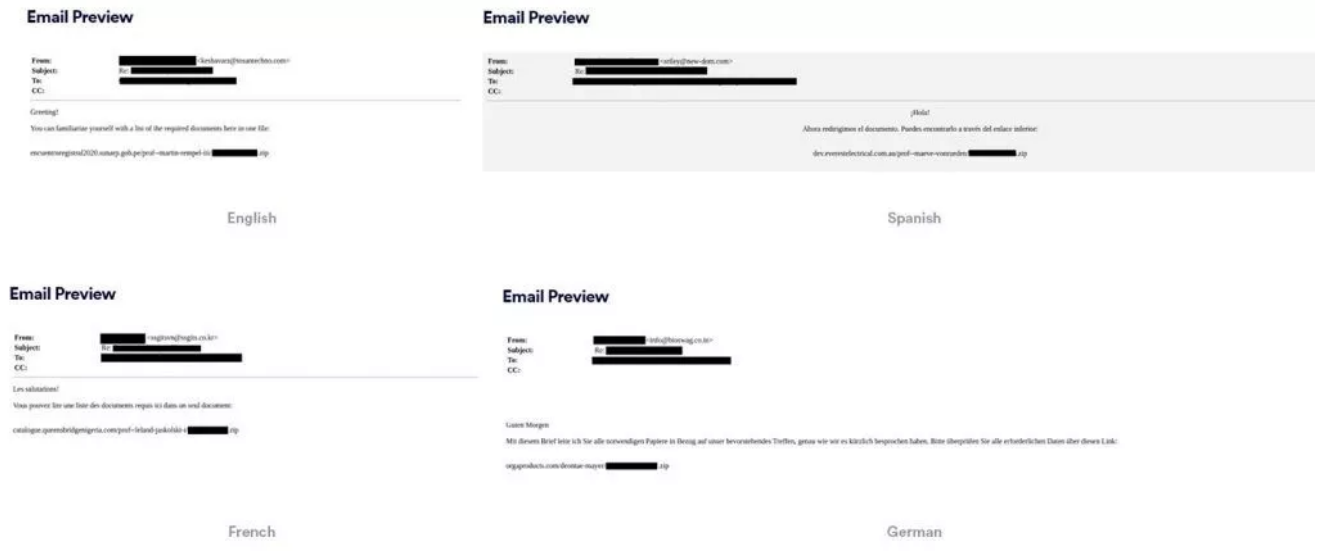
Campaign Details.

The attacker impersonates a person the user knows in an attempt to gain trust and deceive him. He sends an email in the native language of the user, with a URL ending with the user's name + .zip extension. In order to make the email look more authentic, the attacker may add **real email conversations between the user and the person impersonated by the attacker**.

The link is non-clickable, which means the user has to copy and paste it into his browser. This is an evasion technique used against email security solutions.

An example of the attack email concealing the malicious content

The emails have been sent in many different languages, which indicates a widespread attack to different geolocations.



Once the user browses to the link, a zip file with the user's name is generated and downloaded.

How is the zip name generated?

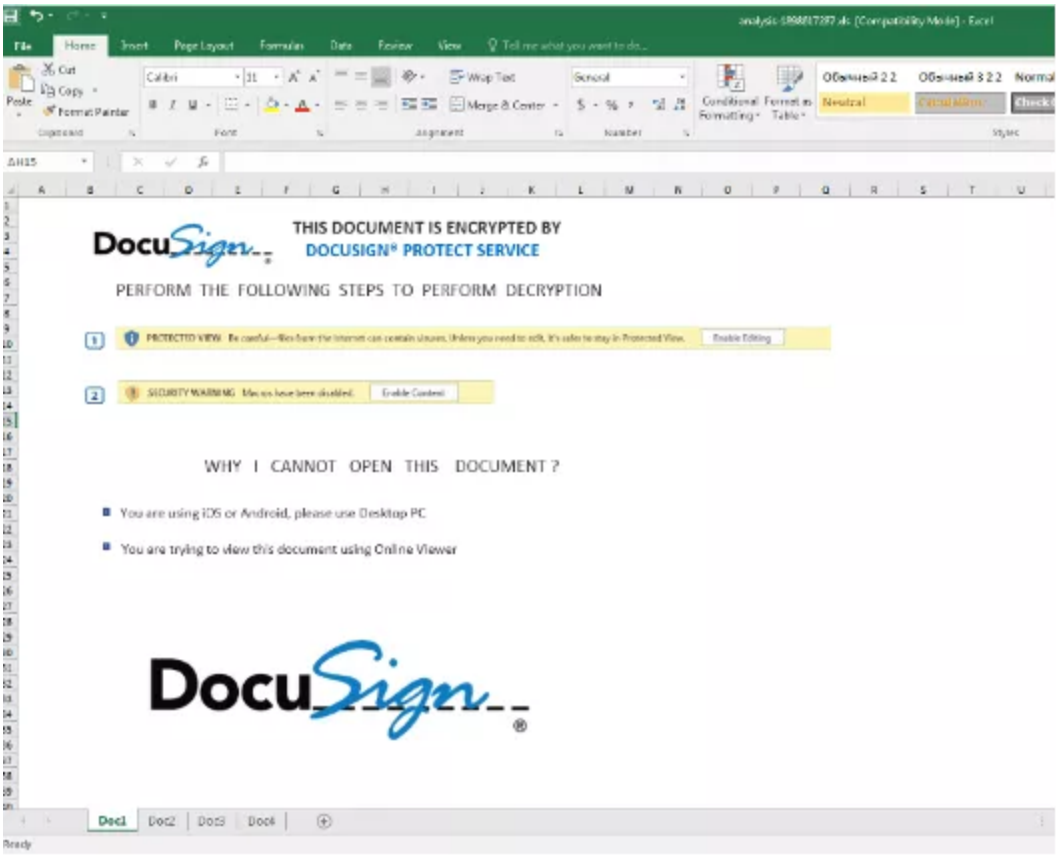
First, let's take the following URL as an example:

`http[:]//microlinsmmn[.]carajasnutricaoanimal[.]com[.]br/mr--simeon-labadie/dan.zip`

After browsing to this link, we get redirected to:

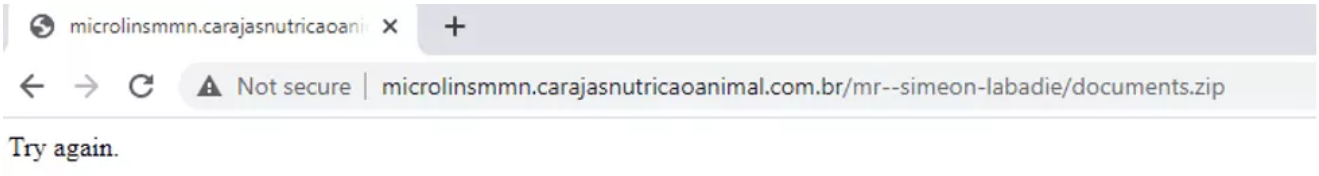
http[:]//microlinsmmn[.]carajasnutricaoanimal[.]com[.]br/mr–simeon-labadie/**documents**.zip

And then a zip file is downloaded automatically with the name 'dan.zip'. The malicious excel, containing hidden XLM code, is found inside the zip file.



Campaign DevSecOps.

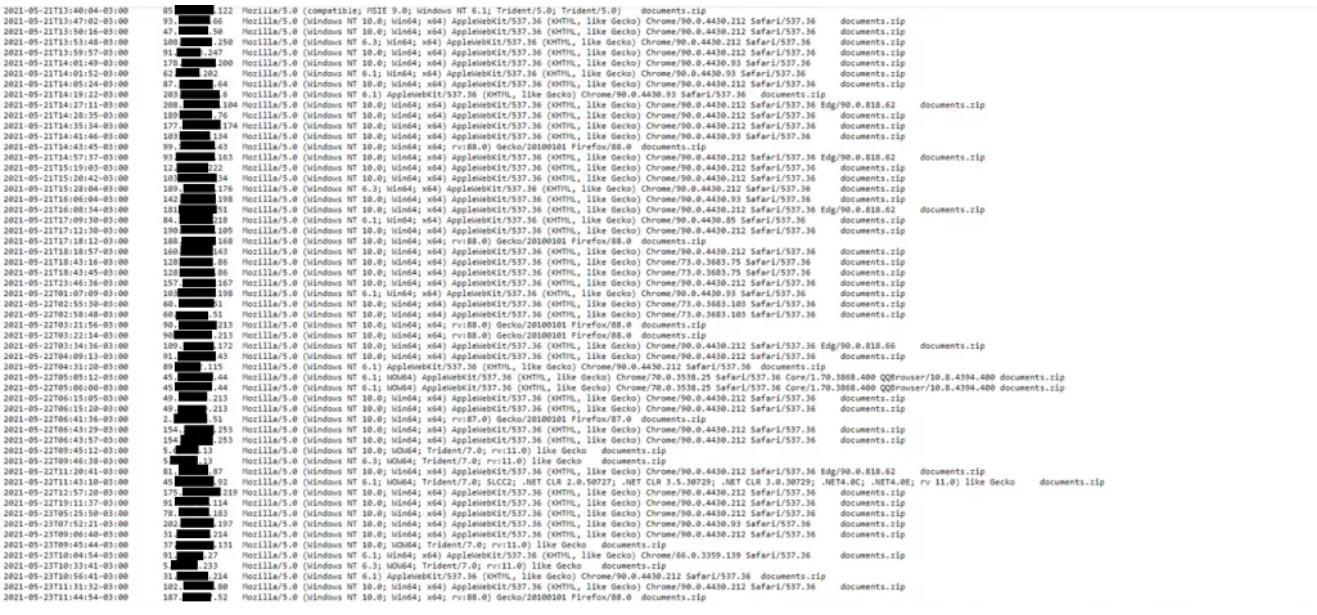
If the same user will try to download the file again, they will receive the following error:



This happens because the server stores all the IP addresses that already accessed the link, and prevents more than one download per IP which is an evasion technique from the attacker.

However, while investigating the URL, it was discovered that the malicious server was accessible without any authentication.

The server log files contains all of the infected computers' IP addresses.



The Malware.

We downloaded more than 30 samples of malicious zip files from one of the malicious URLs and have found that the hashes were different for each file. When comparing between the files, we saw that the differences were minimal.

Changing the hash of each individual file is a technique used by the attacker to evade signature/ioc based detection.

The embedded Excel 4.0 macro code itself is similar to previous attacks we have previously reported – it downloads and executes a malicious DLL. This time, the DLL payload is the Qakbot Trojan, also known as QBOT.

The malware uses a process injection method known as process hollowing, thereby injecting itself into explorer.exe process, where it creates a scheduled task in order to achieve persistence, and later connects to a C&C server.

Perception Point Approach.

This attack was detected using the multiple protection layers in the Perception Point platform.

- The Recursive Unpacker, an anti-evasion layer, instantaneously extracted all files
- Static engines detected the utilization of malicious Excel 4.0 macros
- The HAP engine, a dynamic engine that combines CPU-level data with advanced software algorithms, identified the malicious behavior of the spreadsheet and its content.

In addition, the platform searches for and scrapes non-clickable links which enables the detection of the URLs in the scanned emails.

Recommendations.

- Educate your employees about email security and on the risk of browsing to unknown URLs and downloading files from unknown sources.
- Always check the authenticity of the sender by checking if the display name and the email address match.
- Use an advanced email security solution with dynamic scanning and anti-evasion mechanisms to reduce the risks of cyber-attacks.

IOCs.

List of initial zip download URLs:

- http[:]//luno-offer-rewards[.]greekspeek[.]com/minerva-heathcote/documents[.]zip
- http[:]//forum[.]ennov8[.]com[.]ng/mr–torrey-satterfield/documents[.]zip
- http[:]//rrestetica[.]com/ffJWg/documents[.]zip
- http[:]//microlinsmmn[.]carajasnutricaoanimal[.]com[.]br/mr–simeon-labadie/documents[.]zip
- http[:]//shopifytest[.]recyclemymachine[.]com/mrs–hermina-welch-phd/documents[.]zip
- http[:]//backend[.]southernbellatl[.]co/prof–flossie-kuhn-jr-/documents[.]zip
- http[:]//appsolzone[.]com/chadrick-marvin/documents[.]zip

- http[:]//ulumequran[.]com/kasey-botsford/documents[.]zip
- http[:]//orgaproducts[.]com/deontae-mayer/documents[.]zip
- http[:]//stage1[.]artisanenterprisellc[.]com/dr–era-skiles/documents[.]zip
- http[:]//portal2[.]aladhwa-sch[.]com/nestor-dare/documents[.]zip
- http[:]//covid19[.]iqwasithealth[.]com/jillian-ratke-iii/documents[.]zip
- http[:]//catalogue[.]queensbridgenigeria[.]com/prof–leland-jaskolski-i/documents[.]zip
- http[:]//pavanalakecamping[.]com/mrs–jessika-sporer/documents[.]zip
- http[:]//bengheng-engrg[.]com/carmelo-metz-iii/documents[.]zip
- http[:]//seremanis[.]com/gregg-beier/documents[.]zip
- http[:]//inmobaperu[.]com/letitia-wintheiser/documents[.]zip
- http[:]//ayurskinclinic[.]com/elroy-emard/documents[.]zip
- http[:]//controlling2014[.]erp-corp[.]com/arvid-abbott/documents[.]zip
- http[:]//najihojeily[.]com/mr–kale-ebert-i/documents[.]zip
- http[:]//radiocakrabandung[.]com/prof–tremaine-gerlach-v/documents[.]zip
- http[:]//offlinesharks[.]com/prof–clark-hessel-md/documents[.]zip
- http[:]//connectavet[.]com/efren-crooks-iii/documents[.]zip
- http[:]//infotrekkingnepal[.]com/dr–dahlia-wisoky-phd/documents[.]zip
- http[:]//lookatmemarketing[.]com/EVzBd/documents[.]zip
- http[:]//calvano[.]com/prof–emil-rolfson/documents[.]zip
- http[:]//allyoulovetrading[.]com/emmanuelle-zemlak/documents[.]zip
- http[:]//viewmediads[.]com/dr–lucie-little/documents[.]zip
- http[:]//integrityadvisory[.]in/dedrick-osinski/documents[.]zip
- http[:]//enaruci[.]qwerty[.]ba/prof–dan-denesik-iii/documents[.]zip
- http[:]//slsviews[.]magicways[.]in/mrs–margie-morissette/documents[.]zip
- http[:]//leonandsigourney[.]com/phoebe-wisozk/documents[.]zip
- http[:]//marketbling[.]com/daphne-hamill-phd/documents[.]zip
- http[:]//cac-itc[.]com/lola-wehner/documents[.]zip
- http[:]//germiterra[.]com/hanna-kuphal/documents[.]zip
- http[:]//tracking-centre-redelivery[.]idealnepaltours[.]com/lelia-jones-i/documents[.]zip

List of DLL payload download URLs:

- https[:]//dharamdiwan[.]in/njipkUcz/ork[.]html
- https[:]//lenoirramosjr[.]com/7r9JyFLo/ork[.]html
- https[:]//dev[.]favterest[.]com/VBPFHU4UdmdT/filter[.]html
- https[:]//ethioshare[.]com/q22UgZzM3PV7/filter[.]html
- https[:]//nws[.]visionconsulting[.]ro/N1G1KCXA/dot[.]html
- https[:]//royalpalm[.]sparkblue[.]lk/vCNhYrq3Yg8/dot[.]html
- https[:]//arpanetwifi[.]com/6PJHScezZV/lora[.]html
- https[:]//victoriaholidays[.]co[.]in/JRO9RjMm/lora[.]html

List of malicious DLL hashes (SHA256):

- e6c043cd93e28feb16362ebb329f26f5c323f5c2389ad1bcec55fe033533dbf0

- dbdccafd2ef3a6eeb6b11c684698df279ba843e5a23fae8d92dd2317cc6db3ee
- c2535e800d505cb51e9c3e161e958162ede306a15d30f9316a31e16159187ac3
- c110315c3b81bb6027c78dff280e5f1b2d3cd8a8dcf2ce0724941a8a40abf1ad

List of C&C Servers:

- 24.95.61.62:443
- 24.229.150.54:995
- 45.77.117.108:8443
- 76.94.200.148:995
- 106.250.150.98:443
- 184.185.103.157
- 187.250.238.164:995
- 195.6.1.154:2222