

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.

From: [redacted] [mailto:raymond.mayer@laptop-parts.ir]
Sent: Wednesday, May 19, 2021 4:09 PM
To: [redacted]
Subject: Re: [redacted]

Good afternoon

With this letter I send you all the papers relating to our coming appointment, right as we discussed not long ago. Please take a look at Ð"ll necessary information via the next link:

salonkita.com/kcJ [redacted].zip

On Tue, 18 May 2021 at 13:24 [redacted] wrote:

[redacted]

From: [redacted]
Sent: Tuesday, May 18, 2021 12:02 PM
To: [redacted]
Subject: Re: [redacted]

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.

Email Preview

From: [redacted] [mailto:info@new-dnt.com]
Subject: [redacted]
To: [redacted]
CC: [redacted]

Greeting!

You can familiarize yourself with a list of the required documents here on our file:

recorrenregimnD2010enayr.gpb.pqjof-marte-veogel-ii [redacted].zip

English

Email Preview

From: [redacted] [mailto:info@new-dnt.com]
Subject: [redacted]
To: [redacted]
CC: [redacted]

¡Hola!

Ahora redigamos el documento. Puedes encontrarlo a través del enlace adjunto:

recorrenregimnD2010enayr.gpb.pqjof-marte-veogel-ii [redacted].zip

Spanish

Email Preview

From: [redacted] [mailto:regimn@regimn.com]
Subject: [redacted]
To: [redacted]
CC: [redacted]

Les salutations!

Vous pouvez lire une liste des documents requis ici dans un seul document:

recorrenregimnD2010enayr.gpb.pqjof-marte-veogel-ii [redacted].zip

French

Email Preview

From: [redacted] [mailto:info@new-dnt.com]
Subject: [redacted]
To: [redacted]
CC: [redacted]

Guten Morgen!

Mit diesem Brief sende ich für alle notwendigen Papiere in Bezug auf unser bevorstehendes Treffen, genau wie wir es kürzlich besprochen haben. Bitte überprüfen Sie alle erforderlichen Daten über dieses Link:

recorrenregimnD2010enayr.gpb.pqjof-marte-veogel-ii [redacted].zip

German

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?

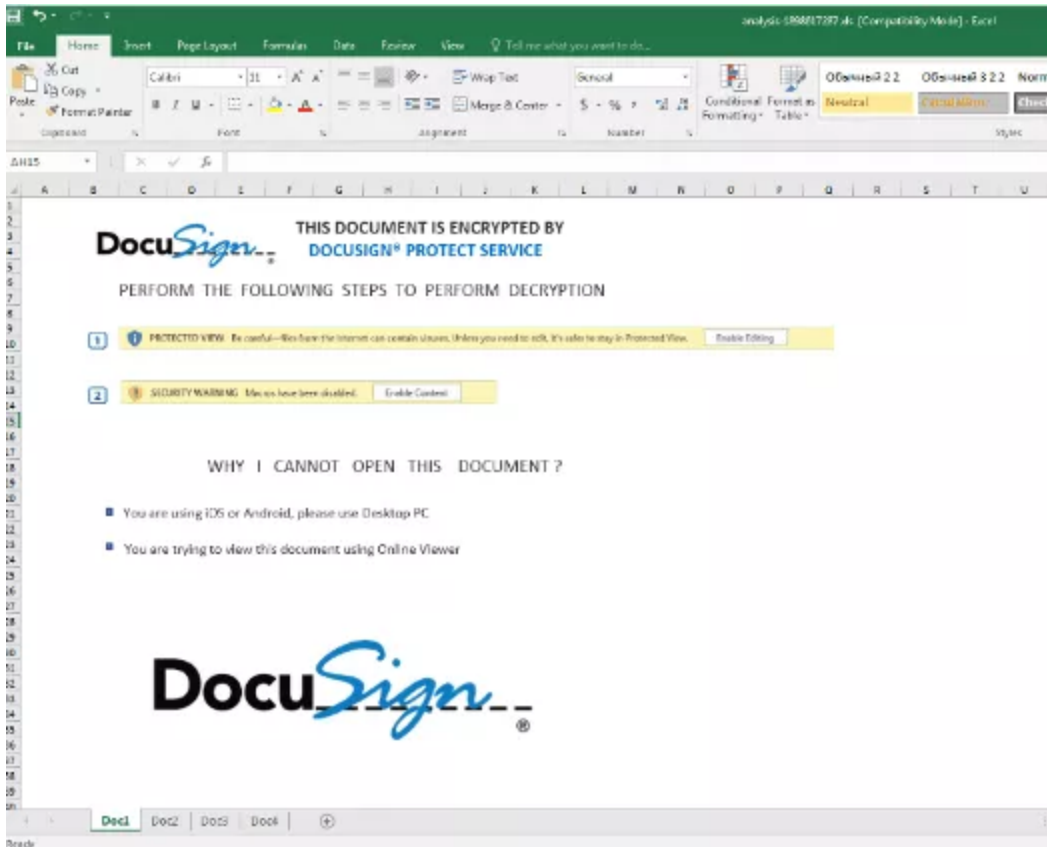
First, let's take the following URL as an example:

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

After browsing to this link, we get redirected to:

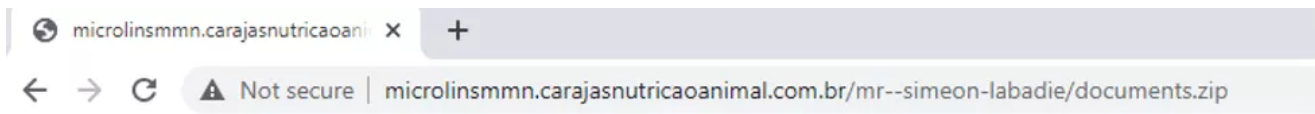
`http[:]//microlinsmmn[.]carajasnutricaoanimal[.]com[.]br/mr--simeon-labadie/documents.zip`

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.

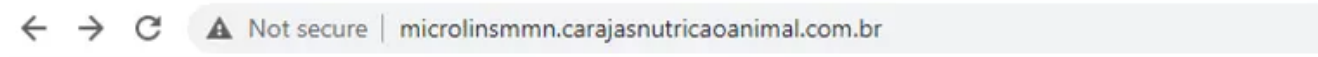
If the same user will try to download the file again, they will receive the following error:



Try again.

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.



Index of /

Name	Last modified	Size	Description
big_stat.txt	2021-05-23 11:44	37K	
dnsck.php	2021-05-21 04:59	5.1K	
expect.php	2020-12-04 19:25	18K	
license.php	2021-05-12 15:40	83K	
mr-simeon-labadie/	2021-05-12 15:40	-	
task.php	2020-09-18 02:44	21K	
try_big_stat.txt	2021-05-23 13:11	79K	

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

```
2021-05-21T13:40:04-03:00 85 122 Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; Trident/5.0) documents.zip
2021-05-21T13:47:02-03:00 93 66 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T13:50:16-03:00 47 50 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T13:53:48-03:00 100 190 Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T13:59:57-03:00 91 127 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T14:01:49-03:00 174 100 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36 documents.zip
2021-05-21T14:01:52-03:00 62 102 Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36 documents.zip
2021-05-21T14:05:24-03:00 87 64 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T14:10:22-03:00 203 6 Mozilla/5.0 (Windows NT 6.1; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36 documents.zip
2021-05-21T14:17:11-03:00 208 70 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 Edg/90.0.818.62 documents.zip
2021-05-21T14:20:35-03:00 109 70 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T14:30:34-03:00 177 174 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T14:41:46-03:00 183 134 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36 documents.zip
2021-05-21T14:43:45-03:00 99 63 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0 documents.zip
2021-05-21T14:57:37-03:00 91 163 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 Edg/90.0.818.62 documents.zip
2021-05-21T15:19:03-03:00 12 122 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T15:20:42-03:00 104 164 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T15:20:04-03:00 189 176 Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T16:00:04-03:00 142 198 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36 documents.zip
2021-05-21T16:00:34-03:00 181 84 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 Edg/90.0.818.62 documents.zip
2021-05-21T17:09:30-03:00 84 118 Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.05 Safari/537.36 documents.zip
2021-05-21T17:12:30-03:00 190 105 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T17:18:12-03:00 208 168 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0 documents.zip
2021-05-21T18:10:57-03:00 160 163 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-21T18:43:16-03:00 128 86 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.75 Safari/537.36 documents.zip
2021-05-21T18:43:45-03:00 128 86 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.75 Safari/537.36 documents.zip
2021-05-21T23:46:36-03:00 157 167 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T01:07:09-03:00 209 198 Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36 documents.zip
2021-05-22T02:50:30-03:00 60 94 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36 documents.zip
2021-05-22T02:53:48-03:00 60 51 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36 documents.zip
2021-05-22T03:21:56-03:00 80 113 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0 documents.zip
2021-05-22T03:22:14-03:00 80 113 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T03:34:36-03:00 109 172 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 Edg/90.0.818.66 documents.zip
2021-05-22T04:09:13-03:00 91 84 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T04:31:20-03:00 80 115 Mozilla/5.0 (Windows NT 6.1; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T05:05:12-03:00 45 64 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.25 Safari/537.36 Core/1.70.3868.400 QQBrowser/10.0.4394.400 documents.zip
2021-05-22T05:06:00-03:00 45 64 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.25 Safari/537.36 Core/1.70.3868.400 QQBrowser/10.0.4394.400 documents.zip
2021-05-22T05:15:05-03:00 40 113 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T06:15:20-03:00 49 213 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T06:43:36-03:00 49 51 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T06:43:39-03:00 154 253 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T06:43:57-03:00 154 253 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T09:45:12-03:00 5 19 Mozilla/5.0 (Windows NT 10.0; Win64; Trident/7.0; rv:11.0) like Gecko documents.zip
2021-05-22T09:46:38-03:00 5 19 Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko documents.zip
2021-05-22T11:20:41-03:00 81 87 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 Edg/90.0.818.62 documents.zip
2021-05-22T11:43:10-03:00 45 93 Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E; rv:11.0) like Gecko documents.zip
2021-05-22T12:57:20-03:00 170 219 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T13:11:37-03:00 91 114 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T05:25:50-03:00 76 183 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T07:52:21-03:00 202 197 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36 documents.zip
2021-05-22T09:00:40-03:00 31 234 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T09:45:44-03:00 37 191 Mozilla/5.0 (Windows NT 10.0; Win64; Trident/7.0; rv:11.0) like Gecko documents.zip
2021-05-22T10:04:54-03:00 91 37 Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36 documents.zip
2021-05-22T10:33:41-03:00 11 233 Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko documents.zip
2021-05-22T10:50:41-03:00 31 234 Mozilla/5.0 (Windows NT 6.1; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T11:33:32-03:00 102 80 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 documents.zip
2021-05-22T11:44:54-03:00 187 52 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0 documents.zip
```

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

- [http://ulumequran\[.\]com/kasey-botsford/documents\[.\]zip](http://ulumequran[.]com/kasey-botsford/documents[.]zip)
- [http://orgaproducts\[.\]com/deontae-mayer/documents\[.\]zip](http://orgaproducts[.]com/deontae-mayer/documents[.]zip)
- [http://stage1\[.\]artisanenterprisellc\[.\]com/dr-era-skiles/documents\[.\]zip](http://stage1[.]artisanenterprisellc[.]com/dr-era-skiles/documents[.]zip)
- [http://portal2\[.\]aladhwa-sch\[.\]com/nestor-dare/documents\[.\]zip](http://portal2[.]aladhwa-sch[.]com/nestor-dare/documents[.]zip)
- [http://covid19\[.\]iqwasithealth\[.\]com/jillian-ratke-iii/documents\[.\]zip](http://covid19[.]iqwasithealth[.]com/jillian-ratke-iii/documents[.]zip)
- [http://catalogue\[.\]queensbridgenigeria\[.\]com/prof-leland-jaskolski-i/documents\[.\]zip](http://catalogue[.]queensbridgenigeria[.]com/prof-leland-jaskolski-i/documents[.]zip)
- [http://pavalalakecamping\[.\]com/mrs-jessika-sporer/documents\[.\]zip](http://pavalalakecamping[.]com/mrs-jessika-sporer/documents[.]zip)
- [http://bengheng-engrg\[.\]com/carmelo-metz-iii/documents\[.\]zip](http://bengheng-engrg[.]com/carmelo-metz-iii/documents[.]zip)
- [http://seremanis\[.\]com/gregg-beier/documents\[.\]zip](http://seremanis[.]com/gregg-beier/documents[.]zip)
- [http://inmobaperu\[.\]com/letitia-wintheiser/documents\[.\]zip](http://inmobaperu[.]com/letitia-wintheiser/documents[.]zip)
- [http://ayurskinclinic\[.\]com/elroy-emard/documents\[.\]zip](http://ayurskinclinic[.]com/elroy-emard/documents[.]zip)
- [http://controlling2014\[.\]erp-corp\[.\]com/arvid-abbott/documents\[.\]zip](http://controlling2014[.]erp-corp[.]com/arvid-abbott/documents[.]zip)
- [http://najihojaily\[.\]com/mr-kale-ebert-i/documents\[.\]zip](http://najihojaily[.]com/mr-kale-ebert-i/documents[.]zip)
- [http://radiocakrabung\[.\]com/prof-tremaine-gerlach-v/documents\[.\]zip](http://radiocakrabung[.]com/prof-tremaine-gerlach-v/documents[.]zip)
- [http://offlinesharks\[.\]com/prof-clark-hessel-md/documents\[.\]zip](http://offlinesharks[.]com/prof-clark-hessel-md/documents[.]zip)
- [http://connectavet\[.\]com/efren-crooks-iii/documents\[.\]zip](http://connectavet[.]com/efren-crooks-iii/documents[.]zip)
- [http://infotrekkingnepal\[.\]com/dr-dahlia-wisoky-phd/documents\[.\]zip](http://infotrekkingnepal[.]com/dr-dahlia-wisoky-phd/documents[.]zip)
- [http://lookatmemarketing\[.\]com/EVzBd/documents\[.\]zip](http://lookatmemarketing[.]com/EVzBd/documents[.]zip)
- [http://calvano\[.\]com/prof-emil-rolfson/documents\[.\]zip](http://calvano[.]com/prof-emil-rolfson/documents[.]zip)
- [http://allyoulovetrading\[.\]com/emmanuelle-zemlak/documents\[.\]zip](http://allyoulovetrading[.]com/emmanuelle-zemlak/documents[.]zip)
- [http://viewmediads\[.\]com/dr-lucie-little/documents\[.\]zip](http://viewmediads[.]com/dr-lucie-little/documents[.]zip)
- [http://integrityadvisory\[.\]in/dedrick-osinski/documents\[.\]zip](http://integrityadvisory[.]in/dedrick-osinski/documents[.]zip)
- [http://enaruci\[.\]qwerty\[.\]ba/prof-dan-denesik-iii/documents\[.\]zip](http://enaruci[.]qwerty[.]ba/prof-dan-denesik-iii/documents[.]zip)
- [http://slsvIEWS\[.\]magicways\[.\]in/mrs-margie-morissette/documents\[.\]zip](http://slsvIEWS[.]magicways[.]in/mrs-margie-morissette/documents[.]zip)
- [http://leonandsigourney\[.\]com/phoebe-wisozk/documents\[.\]zip](http://leonandsigourney[.]com/phoebe-wisozk/documents[.]zip)
- [http://marketbling\[.\]com/daphne-hamill-phd/documents\[.\]zip](http://marketbling[.]com/daphne-hamill-phd/documents[.]zip)
- [http://cac-itc\[.\]com/lola-wehner/documents\[.\]zip](http://cac-itc[.]com/lola-wehner/documents[.]zip)
- [http://germiterra\[.\]com/hanna-kuphal/documents\[.\]zip](http://germiterra[.]com/hanna-kuphal/documents[.]zip)
- [http://tracking-centre-redelivery\[.\]idealnepaltours\[.\]com/lelia-jones-i/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://dharamdiwan[.]in/njipkUcz/ork[.]html)
- [https://lenoirramosjr\[.\]com/7r9JyFLo/ork\[.\]html](https://lenoirramosjr[.]com/7r9JyFLo/ork[.]html)
- [https://dev\[.\]favterest\[.\]com/VBPFHU4UdmdT/filter\[.\]html](https://dev[.]favterest[.]com/VBPFHU4UdmdT/filter[.]html)
- [https://ethioshare\[.\]com/q22UgZzM3PV7/filter\[.\]html](https://ethioshare[.]com/q22UgZzM3PV7/filter[.]html)
- [https://nws\[.\]visionconsulting\[.\]ro/N1G1KCXA/dot\[.\]html](https://nws[.]visionconsulting[.]ro/N1G1KCXA/dot[.]html)
- [https://royalpalms\[.\]sparkblue\[.\]lk/vCNhYrq3Yg8/dot\[.\]html](https://royalpalms[.]sparkblue[.]lk/vCNhYrq3Yg8/dot[.]html)
- [https://arpanetwif\[.\]com/6PJHScezZV/lora\[.\]html](https://arpanetwif[.]com/6PJHScezZV/lora[.]html)
- [https://victoriaholidays\[.\]co\[.\]in/JRO9RjMm/lora\[.\]html](https://victoriaholidays[.]co[.]in/JRO9RjMm/lora[.]html)

List of malicious DLL hashes (SHA256):

- e6c043cd93e28feb16362ebb329f26f5c323f5c2389ad1bcec55fe033533dbf0

- dbdcca2ef3a6eeb6b11c684698df279ba843e5a23fae8d92dd2317cc6db3ee
- 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