Zeus Delivered by DELoader to Defraud Customers of Canadian Banks

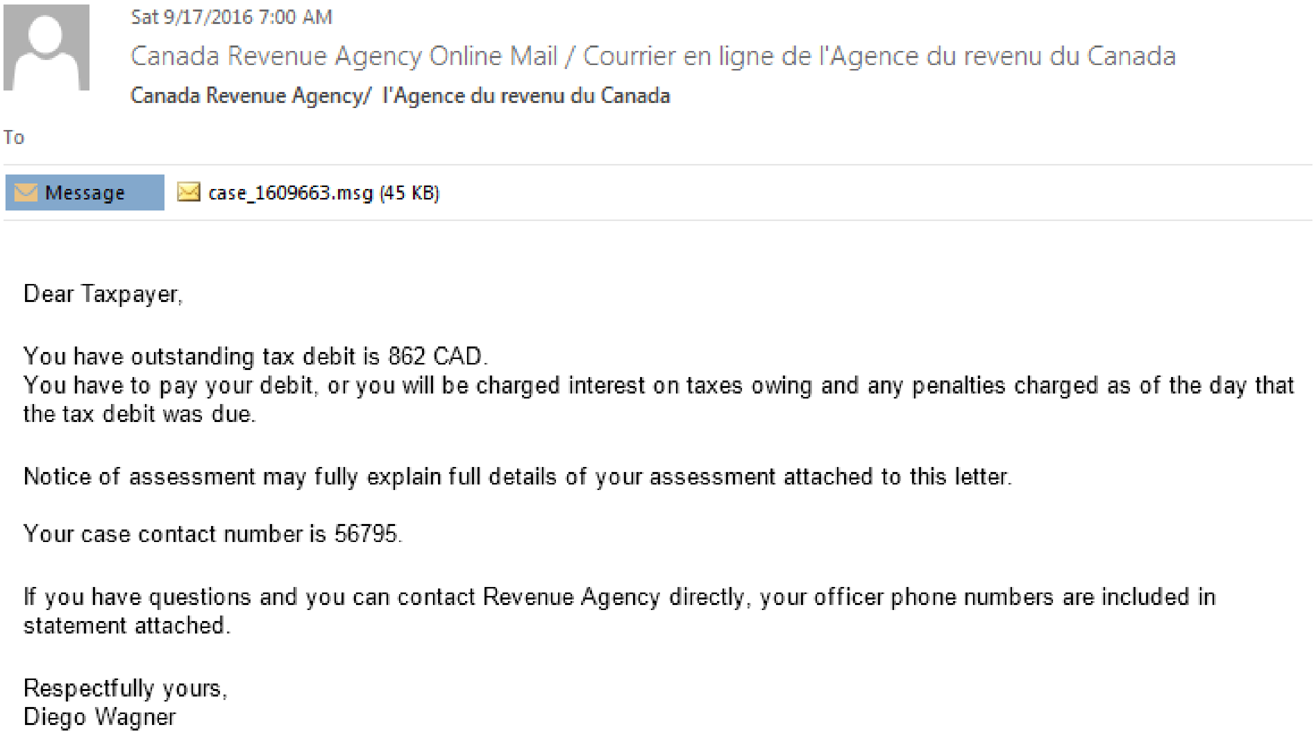
forcepoint.com/blog/security-labs/zeus-delivered-deloader-defraud-customers-canadian-banks

September 22, 2016

Throughout September 2016 we have observed an actor sending malware to Canadian nationals by e-mail. Upon investigation we have determined the malware payload to be DELoader, which downloads a Zeus variant banking trojan upon execution.

E-mail Lures

The e-mails typically pretend to be from the Canada Revenue Agency (CRA) claiming that the individual has a tax payment outstanding.



Sat 9/17/2016 7:00 AM

Canada Revenue Agency Online Mail / Courrier en ligne de l'Agence du revenu du Canada

Canada Revenue Agency/ l'Agence du revenu du Canada

To

Dear Taxpayer,

You have outstanding tax debit is 862 CAD.
You have to pay your debit, or you will be charged interest on taxes owing and any penalties charged as of the day that the tax debit was due.

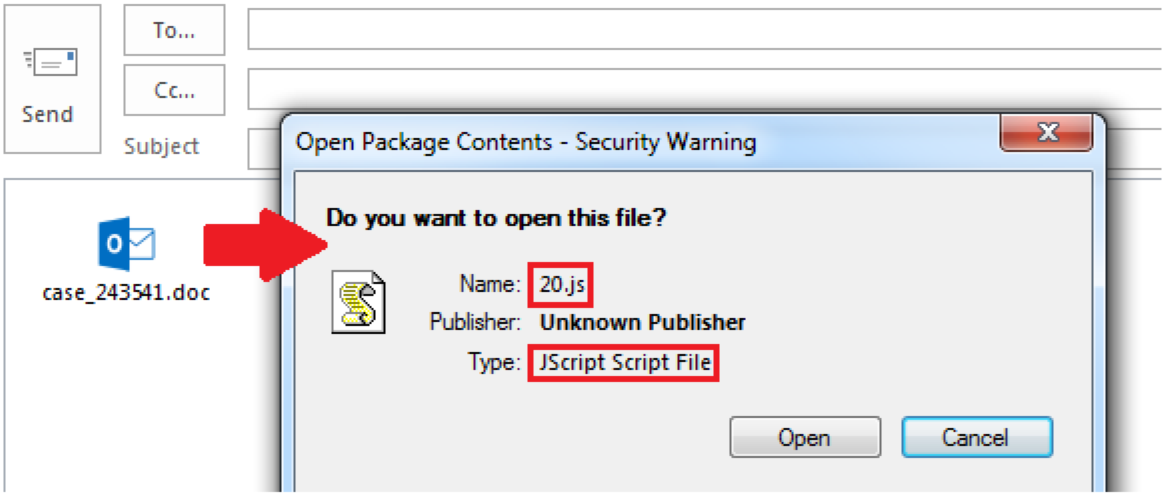
Notice of assessment may fully explain full details of your assessment attached to this letter.

Your case contact number is 56795.

If you have questions and you can contact Revenue Agency directly, your officer phone numbers are included in statement attached.

Respectfully yours,
Diego Wagner

The e-mails contain an MSG attachment with an embedded OLE object. This is not a technique we see very often and is challenging for security products to detect due to the complicated MSG format. When the user opens the MSG attachment they are faced with the following content:



Do you want to open this file?

Name: 20.js
Publisher: Unknown Publisher
Type: JScript Script File

The embedded object name *"case_243541.doc"* here is actually a spoofed object name. Double clicking on this fake document will prompt the user as to whether they wish to run a JScript file. If execution is allowed then the JScript file will begin to download and execute malware from the following URL:

```
hxxp://tradestlo.top/poll.hls
```

Malware Payload (DELoader)

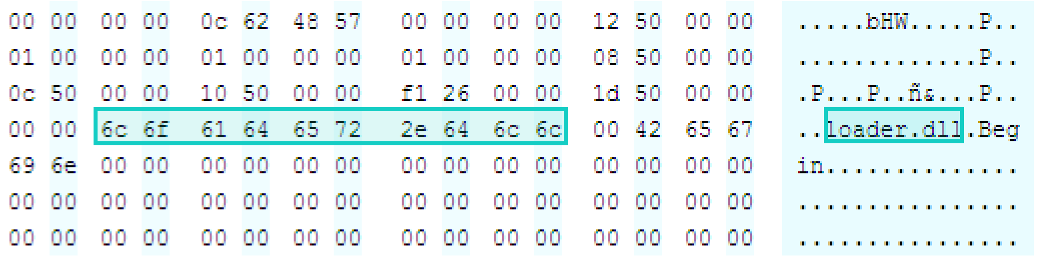
The malware downloaded by the malicious JScript files is a trojan downloader known as DELoader (aka Terdot). This malware has previously been used to target German nationals. In the sample we analysed (SHA1 *5bfb7cbc0c79e1ce7fd4861193bd38ceeb4c8c2d*) DELoader downloaded and executed a Zeus banking trojan variant from one the following URLs:

```
hxxps://aspecto.top/dpr.bin
hxxps://prisectos.top/dpr.bin
```

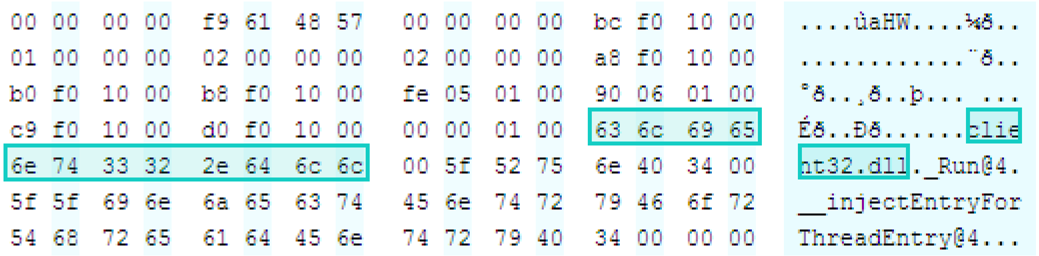
Contrary to previous research we do not believe DELoader to be a generic malware downloader. DELoader seems to be solely used to distribute a specific variant of the Zeus banking trojan. We unpacked the embedded DELoader DLL (SHA1 *cad1715f0ffd32092001a14c5f8de6990c379867*) and compared it with the Zeus variant it downloaded (SHA1 *e57362eaa240da948980c4c6133d63c2a4c07b31*). As a result we noticed the following connections:

- Both use the same domains *aspecto[.]top* and *prisectos[.]top*
- Both contain the string *"shared_%s"*
- Both were compiled using Microsoft Visual Studio 2012
- Both were compiled within 20 seconds of each other according to the PE headers
- DELoader is hard-coded with an export to call in the Zeus DLL

DELoader appears to be compiled under the name *"loader.dll"* and the Zeus variant appears to be compiled under the name *"client32.dll"*.



```
00 00 00 00  0c 62 48 57  00 00 00 00  12 50 00 00  .....bHW.....P..
01 00 00 00  01 00 00 00  01 00 00 00  08 50 00 00  .............P..
0c 50 00 00  10 50 00 00  f1 26 00 00  1d 50 00 00  .P...P..ñ&...P..
00 00 6c 6f  61 64 65 72  2e 64 6c 6c  00 42 65 67  ..loader.dll.Beg
69 6e 00 00  00 00 00 00  00 00 00 00  00 00 00 00  in..............
00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
```



```
00 00 00 00  f9 61 48 57  00 00 00 00  bc f0 10 00  ....ùaHW....¼ð..
01 00 00 00  02 00 00 00  02 00 00 00  a8 f0 10 00  ............¨ð..
b0 f0 10 00  b8 f0 10 00  fe 05 01 00  90 06 01 00  °ð..¸ð..þ... ...
c9 f0 10 00  d0 f0 10 00  00 00 01 00  63 6c 69 65  Éð..Ðð......clie
6e 74 33 32  2e 64 6c 6c  00 5f 52 75  6e 40 34 00  nt32.dll._Run@4.
5f 5f 69 6e  6a 65 63 74  45 6e 74 72  79 46 6f 72  __injectEntryFor
54 68 72 65  61 64 45 6e  74 72 79 40  34 00 00 00  ThreadEntry@4...
```

Malware Payload (Zeus Variant)

Zeus (aka ZBot) is an infamous banking trojan capable of intercepting and modifying online banking traffic in order to perform fraudulent transactions. It does this by injecting itself into web browsers that are running on the machine. It is also capable of stealing other credentials from the machine, enabling remote desktop access, and acting as a proxy server for an attacker.

In the sample we analysed the malware downloaded its main configuration file from one of the following URLs:

```
hxxps://aspecto.top/dsr.bin
hxxps://prisectos.top/dsr.bin
```

We were able to decrypt the configuration to reveal its version number, command-and-control (C&C) and a list of banking websites to steal and modify traffic from.

```
VERSION
        1.5.5.0

COMMAND AND CONTROL URL
        hxxps://namoterno.top/promo.php

ALTERNATIVE CONFIG URL
        hxxps://alecofrinse3.com/aqs.bin
        hxxps://bielakee.xyz/cr2.bin
        hxxps://lwowenase.top/core.bin

...
```

The list of banking websites were mainly Canadian banks, with some US and Australian banks also targeted.

Protection Statement

Forcepoint™ customers are protected against this threat via TRITON® ACE at the following stages of attack:

- Stage 2 (Lure) - Malicious e-mails associated with this attack are identified and blocked.
- Stage 5 (Dropper File) - DELoader is prevented from being downloaded by the malicious JScript file.
- Stage 6 (Call Home) - Attempts by the Zeus variant to call home are identified and blocked.

Summary

The actor behind DELoader has started targeting Canadian nationals with a variant of the Zeus banking trojan. The DELoader malware itself appears to have been designed specifically for use with this Zeus variant. The Zeus code base continues to be a popular choice for malware developers looking to create a quick and easy banking trojan. It is important to be careful when opening e-mail attachments and to verify that the sender is who they say they are.

The Canada Revenue Agency website has additional information for recognising and protecting against fraud.

Blog contributors: Nick Griffin, Ran Mosessco

Indicators of Compromise

JScript Downloader (SHA1)

```
f4a4a2207c8c1135a7bdf819d95e9ee22d34d733
```

DELoader (SHA1)

```
5bfb7cbc0c79e1ce7fd4861193bd38ceeb4c8c2d
```

DELoader Unpacked DLL (SHA1)

```
cad1715f0ffd32092001a14c5f8de6990c379867
```

Zeus Variant (SHA1)

```
e57362eaa240da948980c4c6133d63c2a4c07b31
```

DELoader Payload URL

```
hxxp://tradestlo.top/poll.hls
```

Zeus Variant Payload URL

```
hxxps://aspecto.top/dpr.bin
hxxps://prisectos.top/dpr.bin
```

Zeus Variant Config URLs

```
hxxps://aspecto.top/dsr.bin
hxxps://prisectos.top/dsr.bin
hxxps://alecofrinse3.com/aqs.bin
hxxps://bielakee.xyz/cr2.bin
hxxps://lwowenase.top/core.bin
```

Zeus Variant C&C

```
hxxps://namoterno.top/promo.php
```

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Our solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

Learn more about Forcepoint