[An analysis of JB's Anti-GRC worm]

last updated: 10.Sept.2001

Obscure [obscure@eyeonsecurity.net]

EyeonSecurity
http://eyeonsecurity.net/

[Introduction]

Lost are the days where the simple rule "DON'T ACCEPT FILES FROM IRC" kept all IRC worms away from your pc. It seems that now script kiddies are reading BugTraq, checking SecurityFocus.com and the rest of the security sites. Finally we have silent delivery of a worm, without any user interaction, other then simply following a link to a malicious HTML page.

This particular worm, other than simply infecting the victims, will also attack the (in)famous "Security" website of Steve Gibson, GRC.COM by launching several DDOS attacks also described in this paper. My personal opinion is that this could be an attempt by the worm creator to get some publicity.

[How to get infected]

Getting infected is simple:
A user on IRC messages you and tells you to follow a link. By simply double clicking on the URL in mIRC, Internet Explorer will come up, download the page and execute the script.

This particular worm will display the following messages to try get you infected:

- Welcome to <channelname> Please visit our webpage at http://www.geocities.com/dalnetgirlspics and let me know what you think to it
- I am an exhibitionist and have just bought a new WebCam. My live Cam feed is at http://www.geocities.com/youngdalnetsluts You can see me squeezing my sweet firm
- Free child porn & pretty sweet lolitas http://www.geocities.com/acefreeporn You will be guaranteed to cum in your pants when you see this collection
- :) Want FREE stuff ? http://www.geocities.com/bestfreestuff2000 FREE PORN, FREE WAREZ, Free XXX Passes, UTILS, SHELLS, MP3s & Shitloads More. Dont Miss Out Go Now
- Hey <yournickname> I saw you join <channelname> and you attempted to send me the links.vbs virus. Go here and get a free virus cleaner and come back to IRC when you are properly cleaned up. thanx http://www.geocities.com/freeantivirus2001
- I dont accept Viruses <yournickname> Please stop autosending when you join <channelname> Please go here for instructions on how to remove it. http://www.geocities.com/freeantivirus2001

As you can see, some of the messages look like someone is trying to help you out. Others are simply porn or Warez adverts, which seem to work very well on the IRC community. One can imagine the astonishment of finding a 14 year old girl advertising child porn …

[The issue here is...]

So how does one get infected if he does not even run an executable file? The person who created this particular worm, seems aware of the vulnerabilities associated with Internet Explorer and ActiveX. When a victim who follows the URL from IRC accesses the page with an un-patched Internet Explorer, the browser immediately runs a VB (visual basic) script, which does a couple of things described later on, to the victim computer.

The vulnerability exploited here was first described by Guninsky[1] and made available through script kiddie tools.

Microsoft issued a patch, which fixes the problem, so that this worm would not execute automatically.[2]

However many users do not patch their browsers, and this vulnerability will probably effect a good number of users, making this worm very effective until the sites hosting the malicious html pages are shut down. Even then, people who are infected will still have the worm active, taking down the web sites will only stop further spreading.

[Origin]

This worm seems to originate from KarmaHotel IRC worm, which also makes use of the same vulnerability described before. While the infection procedure is almost exactly the same, the resulting payload code is totally new. There are also suspicions that this particular worm originated from DALnet rather than undernet because of the website names and the long nickname "gribblegrobble". This is also similar to KarmaHotel, which also started on DALnet.

[What the worm does]

The worm is initially installed by an html document. What this html page does is simply exploit the vulnerability found by Georgi Guninski to create a file called JB.VBS on the C:\ and execute it. From here on, things start happening :)

C:\JB.VBS :

1. creates C:\lipreffs.vbs. This file is run everytime windows starts. It basically runs a continuous attack on grc.com and does other routine stuff
2. runs ping flood against grc.com. This is one DDOS attack this worm does on Steve's website.
3. Runs C:\lipreffs.vbs. Will add an entry to run this script everytime windows starts.
4. Search for mirc.ini. This means that it is able to search for the mirc folder.
5. Creates script.ini in the mirc folder. This file is described later on.
6. Writes to mirc.ini to point to script.ini

---

[1] http://www.guninski.com/javaea.html
[2] http://www.microsoft.com/technet/support/kb.asp?ID=275609

7. deletes jb.vbs. Simply cleans up C:\ of files the worm does not need anymore.

Script.ini :

This file is found in the mIRC folder.

upon joining :
1. checks if the user is on #nohack or #virus free. If that is the case it leaves the channel.

Simply a procedure to try keep victims from removing the worm.

2. randomly sends a message to advertise the infective html page.

This is the way the worm propagates

upon connecting to server:
1. sends gribblegrobble a message "GRC loves me man"

Just informs this user, probably the creator of the worm, that another victim has joined his army.

upon starting:
1. updates C:\lipreffs.vbs and adds new entry to ping flood grc.com

2. adds entry to start lipreffs.vbs upon startup.

3. Randomly connencts to grc.com website and does an HTTP request to certain pages.

4. Sends UDP packets to grc.com from source port 53 to destination port 80 with offensive data :)

As you can see, this worm's payload is to attack GRC.com mainly using PING.exe available with all Microsoft Windows boxes, to flood the host. Apart from that, it also uses 2 other techniques, basically:

a. Generating multiple HTTP requests.

b. Sending UDP packets. This is a very similar attack to the ICMP flood.

To launch these two types of attacks, the worm creator makes use of Socket support in mIRC.

[How to remove the worm]

Ok this is the important part for those infected. Please note that i cannot be held responsible in the case that anything wrong happens with your computer. I do not claim

that this is the correct way to clean the worm.It is advised that only advanced users follow this procedure.

To remove the worm :

1. Delete C:\lipreffs.vbs. This is done by double clicking on "My computer", selecting C: drive, and locating the file lipreffs.vbs. Once there, right click on the file and select delete.
2. Delete mirc.ini and script.ini. These files are located in your mIRC folder, typically C:\mIRC. Be sure to close mIRC before doing this.
3. Delete the registry entry for lipreffs.vbs. This is done by starting regedit: Click on start, then on run and type regedit. Once there navigate to the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\jb and delete the key.

[Conclusion]

This particular worm is built on a previously also relatively successful older worm. This means that the worm creator does not have to worry on how to make the users run the file. However it still inherits the same problems to spread, which basically is the need to use hardcoded links. Of course the infectious pages can be put down, stopping further spreading of the worm, making it a very short term problem.

Apart from this, the idea to attack GRC.com is a bit similar to the previous CODE-RED worm payload. However we see that the person creating this particular worm went further to make use of different types of connections to attack different resources and services. Considering the possibility of further infection and spreading of this worm, this could easily create an effective automated DDoS attack on the target server.

So the lesson of the day is: never have an unpatched Internet Explorer .. it could ruin your day.
Maybe we could add that following links from strangers can be harmful nowadays. Anyways, you can check out the source of the worm your self by clicking on download below. All files are renamed to txt or ini to prevent any possible infection.

[Acknowledge]

I acknowledge `eZ of #nohack / undernet for giving me information on KarmaHotel and his useful comments on this article.

[References]

Security issues :
http://www.guninski.com/javaea.html
http://www.securityfocus.com/bid/1754

Microsoft Patch
http://www.microsoft.com/technet/support/kb.asp?ID=275609

Microsoft FAQ
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq00-075.asp

[See for yourself]

htmlpage.txt contains the actual HTML source of the pages created by the worm maker.
jb.txt contains the source of jb.vbs created by by html page.
script.ini is the mIRC script created by jb.vbs.

Download Files: http://eyeonsecurity.net/download/anti-grc.zip