

Re: Inger's spam email claims

Source: <http://sci.tech--archive.net/Archive/sci.archaeology/2005-10/msg00512.html>

- *From:* Philip Deitiker <Donevenask@xxxxxxxxxxxxxxxx>
 - *Date:* Sun, 30 Oct 2005 16:09:38 GMT
-

In sci.archaeology message
news:r6i9m1s7da230mlau2a03vd4lr636fgla@xxxxxxx by Doug Weller
<dweller@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> . . . :

>>You know damned well how a worm is
>>propagated and to put Inger's name in the
>>topic line is ridicoulus.
>
> You still don't get the point.
>
> Inger claims that her ISPs can trace the source of spam mail to
> individuals. Ok, this isn't spam in one sense, but I challenge
> you to trace the source. I've been arguing that it isn't as easy
> as Inger claims, and that she may be maligning people because
> she and her perhaps less-than savvy ISP techs believe the
> headers.
>
> Is that clear?
>
> Doug

You can't trace worms. Worms start at one point and they expand by hopping from vulnerable computer to vulnerable computer, like this.

Suppose I'm a worm and I have just found a vulnerable share on computer X. I then loadmyself into therun portion of the system registry.

The next time the computer comes on I then activate 1 or 2 progrmans. The first program is a sniffer. here is how it works. It takes your IP which is four components IP1.Ip2.IP3.Ip4 in the IP4 segments (because it knows IP1-3 exist, is simply rolls from 1 to 254. Then It queries whether common shares are open like 'windows','temp','share'. It can then upload a program and remotely activate the program, or insert commands in the system registry, or get environment information, like an active email address, etc. If it does not find any vulnerable information it goest to the next level IP3 and begins varying IP3 while rolling IP4. Until it finds an open computer. Once its found an open computer it can activate several commands, most can do limited damage before a reboot. After

Re: Inger's spam email claims

the first reboot they can launch a SMTP email server which then carries the virus by email. It can launch a more effective burrowing program. It can generate its payload on the computer.

Now let us suppose your computer has been taken over by an emailing worm, how would you know. If you had an antivirus program it might give the following message 'blah,blah,blah has attempted to send email directly from this computer' and you would see about 1000 of these messages appear over about a minutes time, depending how many mbx type files it could find with active email addresses. [Your defense at this point is to push the 'off button' on the ATX power supply and hold it till the system goes dead, reboot in safe mode, and do a manual scan of the hard drive, virus lookup, manual virus removal from the registry and run files, system patched, etc].

Because worms propogate from vulnerable machine to vulnerable machines, and because machines become vulnerable within hours of the last microsoft vulnerability patch release, and because most people do not patch these vulnerability within hours after the patch release, it is virtually impossible to predict the path that a worm propogates. Security analyst often rely on incidence information, however all the worm has to do is vary the IP1 segment at random interval relative to IP3 and IP4 and pretty soon its gon from Ireland to Australia, no problem.

How hard is it to write a worm program. If you understand the object code for the MS operating system and the code changes that occur with patches you could deduce where the vulnerability exists in the system. Most of these worm generators know the greatest potential vulnerabilities exist in the new powerful featur of windows XP and windows 2000 pro, and so they are looking for a route from the vulnerability to those features. Programing can be done in C++ and converted to assembly code. Creating an SMTP server is about as easy as can be, since SMTP is about as old as the dinosaurs and has been hacked by 5 year olds using cell phones.

The real question in avoiding these attacks is not how good the hackers are, but how secure your system and your SMTP mail server is. Most good mailservers can now detect and eliminate threats. The ISP services, particularly on T1, DSL, Cable connections can leave ports open that increase vulnerability. The computer builder may have created shares so that he can install software after installation but forgot to remove the shares. Of course you can install the most recent updates, but be aware that at least on 2 occasions, microsofts updates have increased vulnerabilities, so keeping up to date on security bullitens is essential.

I use pre 2000 OS at home over a modem, and I never have been attacked. The reason is that MS is not doing any security patches on older OS, hackers assume that 8 year old OS are no longer 'important' and that it is simply to difficult to worm across modem lines because they are closed 99% of the time, the system on the other end is

Re: Inger's spam email claims

always morphing, and you can't very well distribute 1000 emails a minute over a 5 kB per second connection. However I have been suspicious of attacks twice. The moment I have a suspicion I turn the computer off, take the drives out. Take them to a machine with the most recent viral updates, and scan the drives. Once this task is complete I look for other possible causes.

More importantly now a days is spywear, there is the microsoft antispywear program, the adware program. In addition some programs like real player like to sniff machines and download advertisements. They can be removed from autorun and the advertisement features turned off. In new machines it might not make a difference, however in older machines it can really slow things down.

Any startup run program can be found in the system registry under various microsoft/windows/...../run subdirectories.

All_Users, HKEY_Current_user, HKEY_Local_Machine etc.

Can be removed in safe mode. This applies to worm payloads, spywear, etc.

The other security problem is autolaunching emails. Most emails now a days are imbedded with information and links, SMTP servers cannot be absolutely up to date. The email reader program often launches these embedded images and links automatically. In our group I had turned this service off in eudora to prevent dissemination of pornographic and other 'offensive' material. The institution however is forcing us to migrate to microsoft outlook, and of course everyone knows about microsofts vulnerability. So now everyone is having to suffer through pornographic pictures in email again. Personally I requested a change of address, since worms have distributed address names across the wide expanses of the internet. Institution doesn't want to do this, therefore my work email account has been rendered virtually useless and I don't use it. (I have an active email account of 17 years in age). The email account I use at home is under parental control, I'm the parent and only emails from people on a very, very short list can send me mail, 4 other accounts are temporary and generally I will give someone a temporary address and if the account gets swamped, I destroy it and create a new account. Generally one should not keep a email address for more than 2 years and should have parallel independent accounts for continuity.

I should repeat, however, that Inger's Security issues have no business in a science.archaeology group. When she brings these things up you should ignore her.

.

Re: Inger's spam email claims

- *Follow-Ups:*
 - ◆ *Re: Inger's spam email claims*
 - ◇ *From:* David Johnson

- *References:*
 - ◆ *Inger's spam email claims*
 - ◇ *From:* Doug Weller
 - ◆ *Re: Inger's spam email claims*
 - ◇ *From:* JerryT
 - ◆ *Re: Inger's spam email claims*
 - ◇ *From:* Doug Weller
 - ◆ *Re: Inger's spam email claims*
 - ◇ *From:* JerryT
 - ◆ *Re: Inger's spam email claims*
 - ◇ *From:* Doug Weller

- Prev by Date: *Re: Libels*
- Next by Date: *Re: Libels*
- Previous by thread: *Re: Inger's spam email claims*
- Next by thread: *Re: Inger's spam email claims*
- Index(es):
 - ◆ *Date*
 - ◆ *Thread*