Subject: Rootkits and Renguard
Posted by YSLMuffins on Wed, 09 Nov 2005 05:50:50 GMT
View Forum Message <> Reply to Message

Slashdot and The Register.

According to this, an exposé by sysinternals about an evil Sony DRM technique has resulted not only in a backlash against Sony BMG, but also allowed World of Warcraft cheaters to defeat The Warden, Blizzard's Renguard.

I'm just wondering if this is something to be concerned about--not just with Renegade and Renguard, but in general.  What's the likelihood of a new hoard of viruses that exploit this code? They would be virtually undetectable, from what I've read about rootkits.

Right now, Sony has released a "patch" to allow this rootkit to be detectable, but they are offering no uninstall unless you e-mail Sony directly...

Subject: Re: Rootkits and Renguard
Posted by Blazer on Wed, 09 Nov 2005 08:36:10 GMT
View Forum Message <> Reply to Message

All rootkits are essentially the same in that they are trojans that open backdoors and also do their best to hide themselves. Probably the best way to detect a trojan is running some sort of firewall software that pops up when an application tries to access the internet. These sorts of firewalls are a real pain when you first set them up, as you get frustrated having to allow normal system access like "svchost" and the random "rundll32". After a week or so of letting the firewall learn what should be allowed to connect though, it's great for catching trojans that a virus scanner would miss.

Subject: Re: Rootkits and Renguard
Posted by JPNOD on Wed, 09 Nov 2005 14:22:27 GMT
View Forum Message <> Reply to Message

Yep...

And I would like to add, people running Windows Firewalls and thinking they are safe, well guess what your not. It does not check outgoing c0nn, so run a real firewall.
Or let's say you download a program there might be a botnet in it, not being detected by a virusscanner.. WIndows firewall will just let it trough.
Windows Firewall, does block most worms/trojans. but incomming obviously. (think of msblaster at that time).
Running a Hardware firewall ( like a router is a plus), but a software firewall is needed.

Subject: Re: Rootkits and Renguard
Posted by Olaf van der Spek on Wed, 09 Nov 2005 14:27:19 GMT
View Forum Message <> Reply to Message

Blazer wrote on Wed, 09 November 2005 03:36All rootkits are essentially the same in that they are trojans that open backdoors and also do their best to hide themselves. Probably the best way to detect a trojan is running some sort of firewall software that pops up when an application tries to access the internet. These sorts of firewalls are a real pain when you first set them up, as you get frustrated having to allow normal system access like "svchost" and the random "rundll32". After a week or so of letting the firewall learn what should be allowed to connect though, it's great for catching trojans that a virus scanner would miss.
Any anti-virus/firewall that runs on the same OS as the rootkit can not be trusted.

Subject: Re: Rootkits and Renguard
Posted by Blazer on Wed, 09 Nov 2005 19:52:42 GMT
View Forum Message <> Reply to Message

JPNOD wrote on Wed, 09 November 2005 09:22Yep...

And I would like to add, people running Windows Firewalls and thinking they are safe, well guess what your not. It does not check outgoing c0nn, so run a real firewall.
Or let's say you download a program there might be a botnet in it, not being detected by a virusscanner.. WIndows firewall will just let it trough.
Windows Firewall, does block most worms/trojans. but incomming obviously. (think of msblaster at that time).
Running a Hardware firewall ( like a router is a plus), but a software firewall is needed.

This is absolutely false. Most windows firewalls explicitly check outgoing connections, and this is the best way to detect trojans and the like. As I explained, ANY program which initiates any network connection (TCP or UDP) causes a popup and tells you which application is doing it and if you should temporarily or permanately allow it.

This sort of firewall is how I discovered the "FlyingBuzz Trojan" years ago (it was a trojan that stole your renegade serial number and posted it to FlyingBuzz's website).

As for "real firewalls" being hardware-based, that is also not entirely true. Most routers, including the cisco router I have in my home network just have "ACL's" (Access Lists), that restrict access by IP subnets.

Also, a certain large ISP that I used to work for did extensive testing and found that a software firewall (OpenBSD + IPF), far outperformed all of the tested hardware-based products

That being said, again I want to stress that using a windows firewall more than likely DOES check outgoing connections, at least I have not used one that does not, including Kerio, Norton, ZoneAlarm, BlackIce, etc.

Subject: Re: Rootkits and Renguard
Posted by Blazer on Wed, 09 Nov 2005 19:58:19 GMT
View Forum Message <> Reply to Message

Olaf van der Spek wrote on Wed, 09 November 2005 09:27Any anti-virus/firewall that runs on the same OS as the rootkit can not be trusted.

I would rather have local anti-virus and firewalls, than to trust one central firewall/antivirus, which, once compromised, exposes your entire LAN.

There is no foolproof firewall, the best thing one can do is to be aware of your network connections and OS activity. Even if you had a central firewall that blocked outgoing connections from your PC, it still has to let *something* through, or you wouldn't be able to check email, log into IRC, etc. So then all the attacker has to do is trick you into downloading a rootkit/trojan that sends data out through ports you have permitted, and/or use various methods like arp poisoning.

In short, the only completely secure PC is one that is not connected to the internet in any way, has no USB, floppy, or CDROM drives, and locked behind a cage so there is no physical access.

---

Subject: Re: Rootkits and Renguard
Posted by JPNOD on Wed, 09 Nov 2005 20:21:47 GMT
View Forum Message <> Reply to Message

[quote title=Blazer wrote on Wed, 09 November 2005 14:52]JPNOD wrote on Wed, 09 November 2005 09:22Yep...

And I would like to add, people running Windows Firewalls and thinking they are safe, well guess what your not. It does not check outgoing c0nn, so run a real firewall.
Or let's say you download a program there might be a botnet in it, not being detected by a virusscanner.. WIndows firewall will just let it trough.
Windows Firewall, does block most worms/trojans. but incomming obviously. (think of msblaster at that time).
Running a Hardware firewall ( like a router is a plus), but a software firewall is needed.

This is absolutely false. Most windows firewalls explicitly check outgoing connections, and this is the best way to detect trojans and the like. As I explained, ANY program which initiates any network connection (TCP or UDP) causes a popup and tells you which application is doing it and if you should temporarily or permanately allow it.

Uhhh, With Windows Firewalls I actually just meant the Windows Built in Firewall which comes with SP2, and was already in but with less options and which is also built in Windows Server 2003.

For example, run brenbot, and it windows firewall wont notice it going out. Use zonealarm, or sygate and it will see it straight away. I do agree on that a pc connected to the Internet is nowhere near 100% safe, but if you don't have anything important on it or whatsover. It is really not worth bypassing all this??

http://www.techimo.com/photo/data/500/12firewall.jpg

Subject: Re: Rootkits and Renguard
Posted by Olaf van der Spek on Wed, 09 Nov 2005 20:35:15 GMT
View Forum Message <> Reply to Message

Blazer wrote on Wed, 09 November 2005 14:58Olaf van der Spek wrote on Wed, 09 November 2005 09:27Any anti-virus/firewall that runs on the same OS as the rootkit can not be trusted.

I would rather have local anti-virus and firewalls, than to trust one central firewall/antivirus, which, once compromised, exposes your entire LAN.

I didn't say I prefered hardware firewalls. My points is that once a trojan is on your system, it's already too late.

Subject: Re: Rootkits and Renguard
Posted by Blazer on Wed, 09 Nov 2005 23:41:56 GMT
View Forum Message <> Reply to Message

JPNOD wrote on Wed, 09 November 2005 15:21
Uhhh, With Windows Firewalls I actually just meant the Windows Built in Firewall which comes with SP2, and was already in but with less options and which is also built in Windows Server 2003.

Thanks for clarifying...I agree, the windows (builtin) firewall sucks. But then again, at least they are trying. I imagine they didn't want the support nightmare of old ladies calling up saying "muh online bridge card came wont connect to thar intarweb".

Subject: Re: Rootkits and Renguard
Posted by Blazer on Wed, 09 Nov 2005 23:46:52 GMT
View Forum Message <> Reply to Message

Olaf van der Spek wrote on Wed, 09 November 2005 15:35I didn't say I prefered hardware firewalls. My points is that once a trojan is on your system, it's already too late.

Not always...if you have a decent firewall like the ones I noted, you can catch them trying to make outbound internet access. There have been cases of trojans though that were coded to specifically disable the users virus scanner and/or firewall as one of their first malicious actions. Fortunately since trojans are by design relatively small, they usually aren't complex enough to know how to disable all of the virus scanners or firewalls one might be using.

Pretty much all one can do is to, along with just using common sense as to what one is downloading and installing, is to have an up to date virus scanner and also a firewall that monitors outgoing connections.  Even if you detect a trojan, once it's installed, they can be a real pain to erradicate, or even worse, it may just sit there, being silently blocked by your firewall, but using up your valuable system resources.

Subject: Re: Rootkits and Renguard
Posted by YSLMuffins on Fri, 11 Nov 2005 21:51:00 GMT
View Forum Message <> Reply to Message

The question remains, though--why would Sony BMG put a rootkit on one of their audio CDs?

Subject: Re: Rootkits and Renguard
Posted by Blazer on Fri, 11 Nov 2005 22:09:35 GMT
View Forum Message <> Reply to Message

It's not a "rootkit" in the malicious sense. Their copy protection code includes code that hides the copy protection files. So, trojan writers take advantage of this and code their trojans to have the same file names/extensions/etc as the protected sony files, thus hiding them from virus scanners.

Sony has since released a patch which makes the files visible to the OS.

Subject: Re: Rootkits and Renguard
Posted by YSLMuffins on Fri, 11 Nov 2005 22:17:14 GMT
View Forum Message <> Reply to Message

It's too bad that it's something that installs automatically without any type of consent or notice. Sony isn't doing much else to help uninstall this rootkit, though.

Subject: Re: Rootkits and Renguard
Posted by light on Fri, 11 Nov 2005 22:18:18 GMT
View Forum Message <> Reply to Message

the term root-kit is going to be mis-used so many times.

A rootkit is a set of software tools frequently used by a third-party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system for purposes

unbeknownst to the user.
http://en.wikipedia.org/wiki/Rootkit

And here is the section on Copy-Protection:

Rootkits as copy protection

There are reports as of November 1, 2005 that Sony is using a form of copy protection, or digital rights management, on its CDs called "XCP-Aurora" (a version of Extended Copy Protection from First 4 Internet) which constitutes a rootkit, surreptitiously installing itself in a cloaked manner on the user's computer and resisting attempts to detect, disable, or remove it. Much speculation is taking place on blogs and elsewhere about whether Sony might be civilly or criminally liable for such actions under various anti-computer-hacking and anti-malware legislation. Ironically, there is also speculation to the effect that the bloggers who point out what Sony CDs do, with technical details, may also be committing a civil or criminal offense under anti-circumvention provisions of laws such as the Digital Millennium Copyright Act in the United States. [3] [4]

On November 2, 2005, Sony released a patch to remove this rootkit, while continuing to maintain that it is not malicious and does not pose a security risk. But the patch itself has come under fire as well. First, it requires ActiveX controls to install, and therefore is only available to users of Microsoft's Internet Explorer. Second, the update is more than 3.5 megabytes in size, and appears to contain new versions of almost all the files included in the initial installation of the entire DRM system, and some new files as well. It appears that the patch is adding things to the system, and once again, not informing the user of exactly what is being done.[5][6]

Informed opinions differ on the security implication of this Sony 'XCP-Aurora' technology as there is evidence that the software has caused Blue screen (BSoD) errors on Windows systems while in normal use. In addition the software has been criticized as poorly implemented and the file hiding scheme could be used to hide arbitrary files on a PC simply by prefixing the filename with $sys$.

Further commentary, including security implications, can also be found on the Security Now! #12 podcast with Steve Gibson and Leo Laporte, entitled "Sony's 'Rootkit Technology' DRM (copy protection gone bad)."

A class-action lawsuit has been filed on behalf of California consumers who may have been harmed by anti-piracy software installed by some Sony music CDs. A second, nationwide class-action lawsuit is expected to be filed against Sony in a New York court on Wednesday seeking relief for all U.S. consumers who have purchased any of the 20 music CDs in question.[7]

On November 9, 2005, security companies Sophos and Symantec announced that they had discovered viruses which were exploiting the Sony rootkit in order to gain access to affected systems.[8]. These viruses are appearing primarily on the form of emails with attachments. ZoneAlarm users were protected by the an "os firewall" in their paid products.

As of November 10, 2005, World of Warcraft hackers have confirmed that the hiding capabilities of Sony BMG's content protection software can make tools made for cheating in the online world impossible to detect. The software - deemed a "rootkit" by many security experts - is shipped with tens of thousands of the record company's music titles. Furthermore, experts at SophosLabs™, Sophos's global network of virus and spam analysis centres, have detected a new Trojan horse that exploits the controversial Sony DRM (Digital Rights Management) copy protection included on some of the music giant's CDs.[9][10][11][12]

Again from: http://en.wikipedia.org/wiki/Rootkit

I love WikiPedia