Subject: your product steals my information
Posted by fredcow9 on Wed, 15 Jun 2011 21:41:49 GMT
View Forum Message <> Reply to Message

your program is malicious as detected by my antivirus, thanks for making it impossible for me to play on noobstories now.

Subject: Re: your product steals my information
Posted by Omar007 on Wed, 15 Jun 2011 21:55:43 GMT
View Forum Message <> Reply to Message

If you got RenGuard from here, it's not malicious.
It does get false-positives on some scanners afaik.

Aside from that, you shouldn't use RenGuard anymore imo. It's outdated anyway.

Subject: Re: your product steals my information
Posted by sla.ro(master) on Mon, 04 Jul 2011 21:09:07 GMT
View Forum Message <> Reply to Message

Omar007 wrote on Thu, 16 June 2011 00:55If you got RenGuard from here, it's not malicious.
It does get false-positives on some scanners afaik.

Aside from that, you shouldn't use RenGuard anymore imo. It's outdated anyway.

some communities like n00bstories can force you to use RenGuard and yes, is outdated.

Subject: Re: your product steals my information
Posted by reborn on Fri, 15 Jul 2011 14:44:02 GMT
View Forum Message <> Reply to Message

Omar007 wrote on Wed, 15 June 2011 17:55
it's not malicious

How can you be sure?

Subject: Re: your product steals my information
Posted by Omar007 on Fri, 15 Jul 2011 16:23:40 GMT
View Forum Message <> Reply to Message

It gives on 2 out of 43 AV programs a message. And not even a message that says it is. Just 'Suspicious' or 'Looks Like'.

I'd say it's not malicious, just false positives.

Attached is a Virus Total printout. If you don't even trust the printout, you can always submit it yourself

File Attachments
1) VirusTotal - Free Online Virus, Malware and URL Scanner.pdf, downloaded 1121 times

Subject: Re: your product steals my information
Posted by reborn on Fri, 15 Jul 2011 20:49:02 GMT
View Forum Message <> Reply to Message

The program connects to v00d00.org to download the renguard master server list. It does this by downloading index.bin, which is processed by the client.

Who maintains the file hosted on v00d00.org? Why does it connect to v00d00's site, and not BHS's?

Would it be possible for the index.bin file to contain additional instructions to be processed by the client?

Try to visit v00d00.org in your browser... Likely just some asshat reported the site, or some dousche messed with it, but still...

I am not convinced that it's entirely harmless, but that's just me.

Subject: Re: your product steals my information
Posted by Omar007 on Fri, 15 Jul 2011 22:53:12 GMT
View Forum Message <> Reply to Message

v00d00.org does not exist. It can't find the address 0o

Subject: Re: your product steals my information
Posted by danpaul88 on Wed, 20 Jul 2011 13:25:01 GMT
View Forum Message <> Reply to Message

Actually as I recall the reason for the false positives is because its packaged using the same utility as a lot of malware is packaged with, hence some virus scanners just blindly assume its probably malware itself.

The packaging is also the reason it doesn't work on 64bit operating systems.

reborn;
I believe there are several URLs to download index.bin from (BRenBot certainly knows of more than one) to provide redundancy and, to some extent, load balancing. It *should* randomly choose from the available URLs, so you may find it connects to a different URL each time it is loaded.

Subject: Re: your product steals my information
Posted by iRANian on Wed, 20 Jul 2011 23:33:58 GMT
View Forum Message <> Reply to Message

danpaul88 wrote on Wed, 20 July 2011 06:25Actually as I recall the reason for the false positives is because its packaged using the same utility as a lot of malware is packaged with

lol
