Subject: RG Connects to Malicious IP

Posted by twig123 on Wed, 02 Sep 2009 21:21:00 GMT

View Forum Message <> Reply to Message

Guys,

I have Malwarebytes anti-malware software installed on my system... Every time I start RG I get a warning that access to a malicious IP has been blocked (IP: 213.131.252.251).

What is this IP and why does RG keep trying to communicate with it?

~Dave

## File Attachments

1) RG - Infected IP.JPG, downloaded 860 times



Subject: Re: RG Connects to Malicious IP

Posted by dr3w2 on Thu, 03 Sep 2009 00:12:26 GMT

View Forum Message <> Reply to Message

http://www.ip-adress.com/whois/213.131.252.251

Thats definitely not a crimson renguard server. I'd find out what other applications you have running tbh

Subject: Re: RG Connects to Malicious IP

Posted by dr3w2 on Thu, 03 Sep 2009 00:14:16 GMT

View Forum Message <> Reply to Message

http://www.malwaredomainlist.com/mdl.php?inactive=&sort=Date&search=&colsearch=All&ascordesc=ASC&quantity=100&page=98

^ do a ctrl-f on that IP.

You got infected yo

Subject: Re: RG Connects to Malicious IP

Posted by twig123 on Thu, 03 Sep 2009 14:49:34 GMT

View Forum Message <> Reply to Message

Guys, my system is clean...

This is sourcing from game.exe (RG) trying to communicate with this IP.

Subject: Re: RG Connects to Malicious IP

Posted by Carrierll on Thu, 03 Sep 2009 16:30:01 GMT

View Forum Message <> Reply to Message

Yeah, then the Malware is simply in that EXE, along with several other EXEs on your system.

You should scan your entire system with your installed antivirus, as well as Windows Defender. If you do not have an antivirus installed, AVG antivirus has a free edition.

Subject: Re: RG Connects to Malicious IP

Posted by twig123 on Thu, 03 Sep 2009 19:37:19 GMT

View Forum Message <> Reply to Message

I don't know how to make this more clear...

"my system is clean"

Subject: Re: RG Connects to Malicious IP

Posted by Carrierll on Thu, 03 Sep 2009 21:10:31 GMT

View Forum Message <> Reply to Message

Ok, we'll make this clear:

"We don't think that is the case." Please post SS of scan results to prove your point.

Subject: Re: RG Connects to Malicious IP

Posted by twig123 on Fri, 04 Sep 2009 00:53:31 GMT

View Forum Message <> Reply to Message

Haha! BHS pwnd...

RenGuard\_Setup\_1.0323.exe - 2/41 Detections

https://www.virustotal.com/analisis/a1443e1ca1647f9be21ae62f0547a48238101ca73617

ad86f6806c9a2ed2ad17-1252025106

and

game.exe - 3/41 Detections

https://www.virustotal.com/analisis/bb9ac3edb3977d7a74b33fbc232fdbd5d5f09c59f809 9a3d7bc77bb530e9f739-1252024999

(Check the MD5 Hashes, this was downloaded fresh and directly sent to VirusTotal)

## File Attachments

1) No Infections.JPG, downloaded 736 times



Subject: Re: RG Connects to Malicious IP

Posted by Goztow on Fri, 04 Sep 2009 09:57:11 GMT

View Forum Message <> Reply to Message

Renguard uses some protection measures to protect itself from reverse engineering that some

viruses also use.

Subject: Re: RG Connects to Malicious IP

Posted by Carrierll on Fri, 04 Sep 2009 11:54:49 GMT

View Forum Message <> Reply to Message

Goztow wrote on Fri, 04 September 2009 10:57Renguard uses some protection measures to protect itself from reverse engineering that some viruses also use.

I'll bet this is a repeat of the issue with Norton. Some virus used SVKP.sys to runtime-pack itself, and the virus connected to that IP, so MalwareBytes just assumes anything with SVKP is that virus, and blocks the connection "attempt" (As RG will NOT connect to that IP).

Ok - just add game.exe to your safe list.

Subject: Re: RG Connects to Malicious IP

Posted by SSnipe on Sat, 05 Sep 2009 22:42:29 GMT

View Forum Message <> Reply to Message

I have like 6 anti virus and some pick something up the others dont, so you still could be

Subject: Re: RG Connects to Malicious IP

Posted by raven on Mon, 07 Sep 2009 09:46:57 GMT

View Forum Message <> Reply to Message

SSnipe wrote on Sat, 05 September 2009 17:42I have like 6 anti virus

That's a bad idea.

Subject: Re: RG Connects to Malicious IP

Posted by Carrierll on Mon, 07 Sep 2009 09:54:37 GMT

View Forum Message <> Reply to Message

All of those are "Heuristic" (guess-work) or "Suspect" (looks like) results. I'll tell you why: some git made a virus that used SVKP(.sys) to protect itself, and some (very) lazy anti-virus makers added anything using SVKP(.sys) to the blacklist.

The file is safe.

Subject: Re: RG Connects to Malicious IP
Posted by twig123 on Tue, 08 Sep 2009 21:12:18 GMT
View Forum Message <> Reply to Message

trying to get another SS for you guys...