

Forum:[Hack Forums](#)

Thread: [How can I use Comodo Firewall to monitor malicious outgoing/incoming connections?](#)

Turtle™ - February 28, 2017, 3:47 am

I have recently installed Comodo Firewall as a means of monitoring my outgoing and incoming connections. Aside from the "smart settings" that I could probably just roll with, are there any key "signatures" or "hints" that I could use to identify a connection as being malicious.

For example, if I were to close all web browsers and programs, and look at the list of outgoing/incoming connections, what sort of things should I look out for that might indicate a RAT or keylogger? The information that I'm given for each connection is as follows:

Name of executable file that makes the connection?: (Ex. svchost.exe)

Protocol: (Ex. TCP or UDP OUT)

Source: (Ex. 192.168.1.50:12345)

Destination: (Ex. 104.178.389.209)

Bytes In: (Ex. 66B)

Bytes Out: (Ex. 66B)

I feel like the information itself is quite self-explanatory, but I'm just wondering what people would consider "alarm bells" when looking at this sort of information (aside from an obvious "virus.exe" file name).

Hackoo - February 28, 2017, 8:21 am

Hi ?

Download [ZHPCleaner](#) :Perform a scan.

Clean and Repair.

Post the clean report.

You can also use this tool called : [Emsisoft Emergency Kit](#) and perform a full scan to clean your PC
[Video: https://www.youtube.com/watch?v=7EjCN_jjmk8]

Turtle™ - February 28, 2017, 9:28 pm

(Feb 28, 2017 09:21 AM)Hackoo Wrote: [\[CITE\]](#) Hi ?

Download [ZHPCleaner](#) :Perform a scan.

Clean and Repair.

Post the clean report.

You can also use this tool called : [Emsisoft Emergency Kit](#) and perform a full scan to clean your PC
[Video: https://www.youtube.com/watch?v=7EjCN_jimk8]

While I appreciate your suggestions, they in no way addressed my questions.

Cecilia - March 1, 2017, 2:56 am

Unusual port connections are one for RAT's, rather than Keyloggers (generally http/smtp). RAT's normally have a full-time connection (unless the server goes down, or offline).

Most RAT's around here use TCP, but I bet there's still some old ones that use UDP.

Ports above the specified reserved range could indicate something strange. Common default RAT ports would be something to look at too.

I bet you there's already some network analysis done on common RAT's, like identifying common start packets and such.

Most are encrypted communication though... not sure if identifiable still. Probably a pattern somewhere?

Keyloggers generally just send data at periods of time, you could perhaps look for SMTP port connections from processes like svchost or other 'system' ones if you're worried.

RunPE's can be very easily detected through comparisons of disk header vs memory header (but even then can be spoofed with hooks and such).

Botnet C&C connections are different though, often 443, or 80. Not sure what you can do about that (aside from long posted payloads and weird urls?).

I've never used Comodo Firewall so I can't be of help with 'identification' with it.

Aura - March 1, 2017, 2:54 pm

(Feb 28, 2017 10:28 PM)Turtle™ Wrote: [\[CITE\]](#) While I appreciate your suggestions, they in no way addressed my questions.

Ignore him. Another try hard in the WHH section.