Collection

Users can Collect posts into a printable, sortable format. Collections are a good way to organize posts for quick reading. A Collection must be created to tag posts. More Help

Print Preview | Filter

Sort by Thread Order Order ▼ Descending

Select: All None

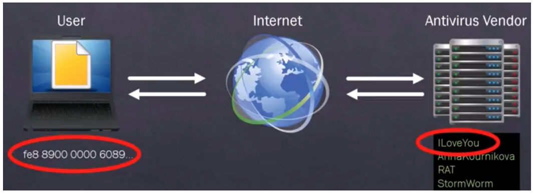
Mark

□

Thread: How Does Antivirus Software **Posted Date:** December 1, 2017 5:10 PM
Post: How Does Antivirus Software **Status:** Published
Author: MOHAMMAD HAZAZI

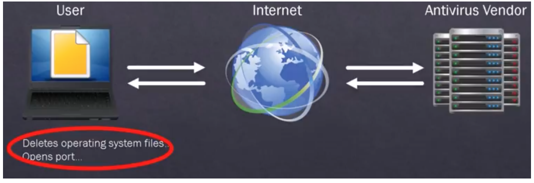
Greeting All,
Have you ever wondered how some Antivirus application catch some kind of viruses while others cant! In below I will try to brief you on the behind seen process.

Signature-based virus recognition



- Any created viruses will have signutre (hash file).
- Cybersecurity community, company, and expert revels this kind of signature, by cooperating to analyze the virus once it's released to find their hashes.
- These hashes are stored in databases which get updated regularly.
- So if you get any virus, your Antivirus App compare the hash code of that file (the content in binary or hex) with its database, if any partial match has found, this file will be quarantined or deleted.
- It is really important to have your antivirus database up to date. FYI , (updates = signatures)

Behavior(Anomaly)-based virus recognition



- Any created viruses shall do specific action or process or behavior (delete files, opens port, delete OS files)
- So if you get any infected attachment file, instead of checking the file hash, the Antivirus App inspect the file and see what does that file do! and compare the behavior to a list of known malicious behaviors
- If that infected attachment starts to delete some files, opens a port, or delete a system file, it will be flagged out and quarantined or deleted.

Thanks for Reading

Mark as Unread

Select: All None

Mark

Forum Statistics

HAZAZI MOHAMMAD (1)

GRADE 3.00 /3
11/26/17 3:40 PM

COMMENTS

← OK