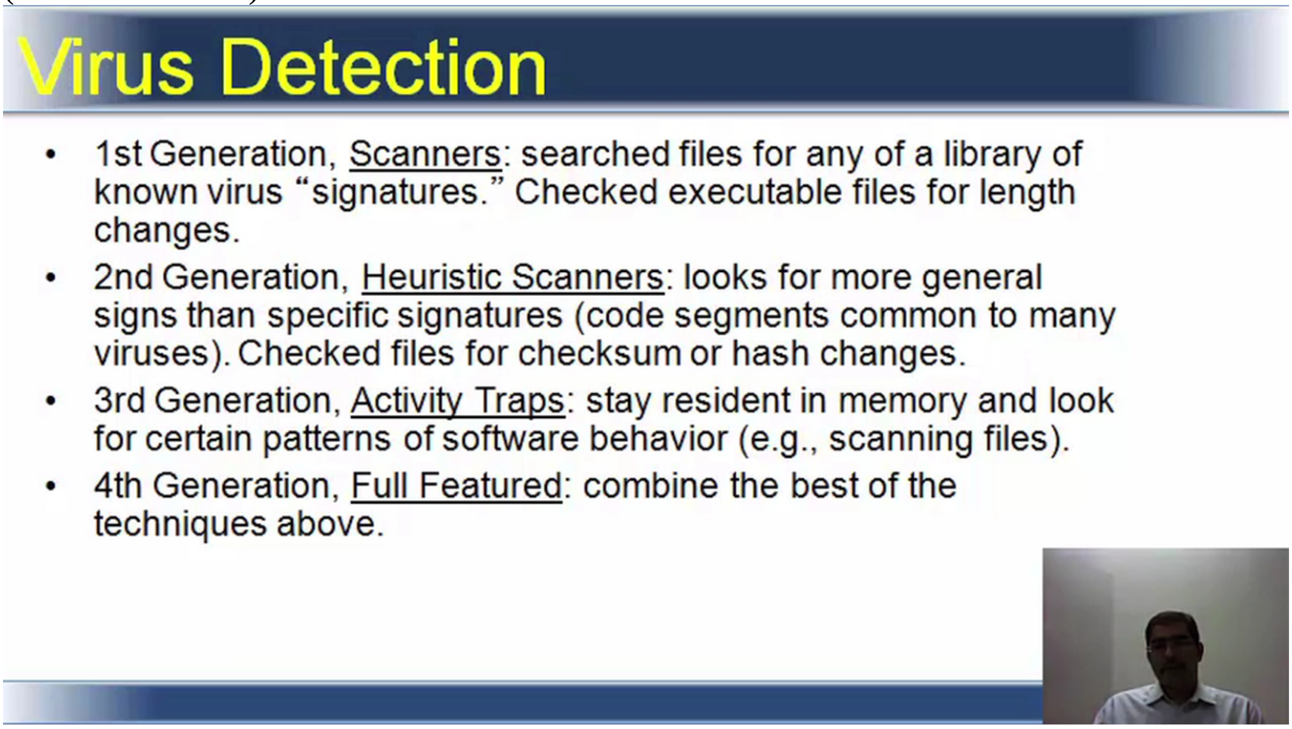
Introduction to Information Security -I
Prof V.Kamakoti
Department of Computer Science and Engineering
Dilip Iyer
Deccan Infotech
Indian Institute of Technology, Madras
Lecture - 35

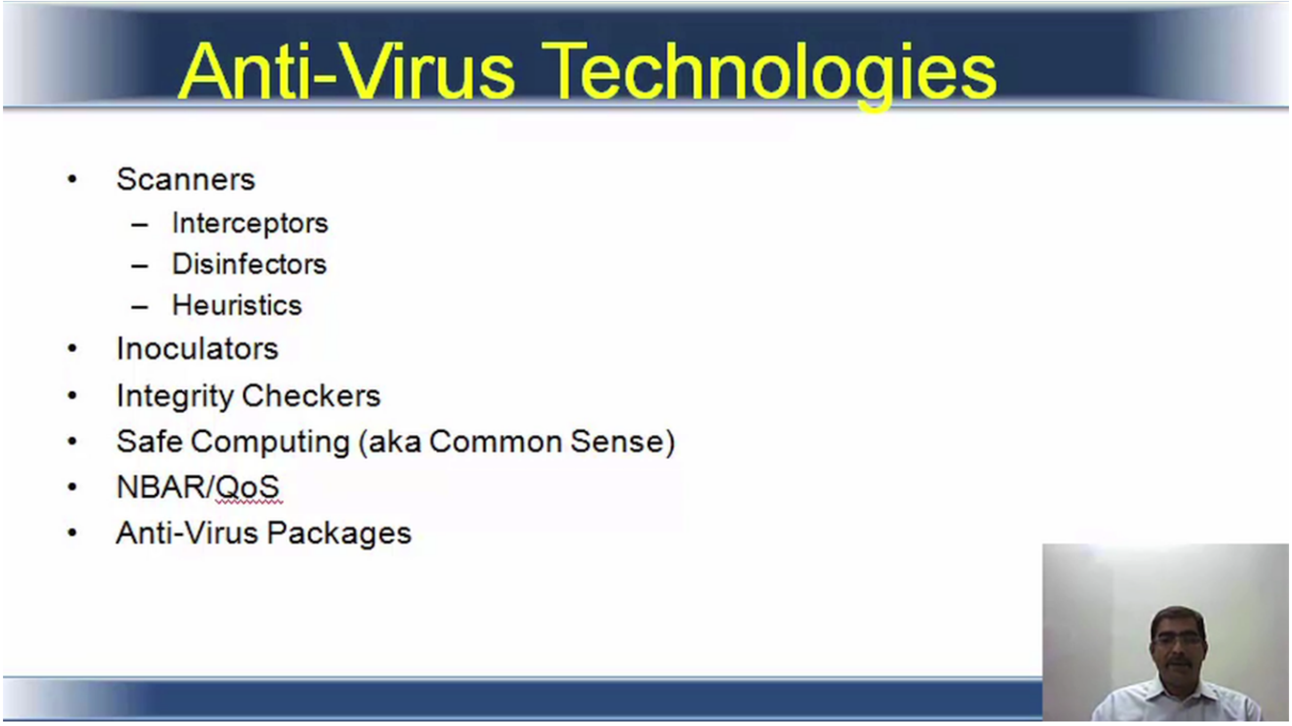
(Refer Time: 00:10)



Virus Detection

- 1st Generation, Scanners: searched files for any of a library of known virus "signatures." Checked executable files for length changes.
- 2nd Generation, Heuristic Scanners: looks for more general signs than specific signatures (code segments common to many viruses). Checked files for checksum or hash changes.
- 3rd Generation, Activity Traps: stay resident in memory and look for certain patterns of software behavior (e.g., scanning files).
- 4th Generation, Full Featured: combine the best of the techniques above.

Then came the fourth generations scanners. They are full featured; they combined the best of all the techniques that we have discussed. Lets take a look at the technologies for antivirus.
(Refer Time 00:22)

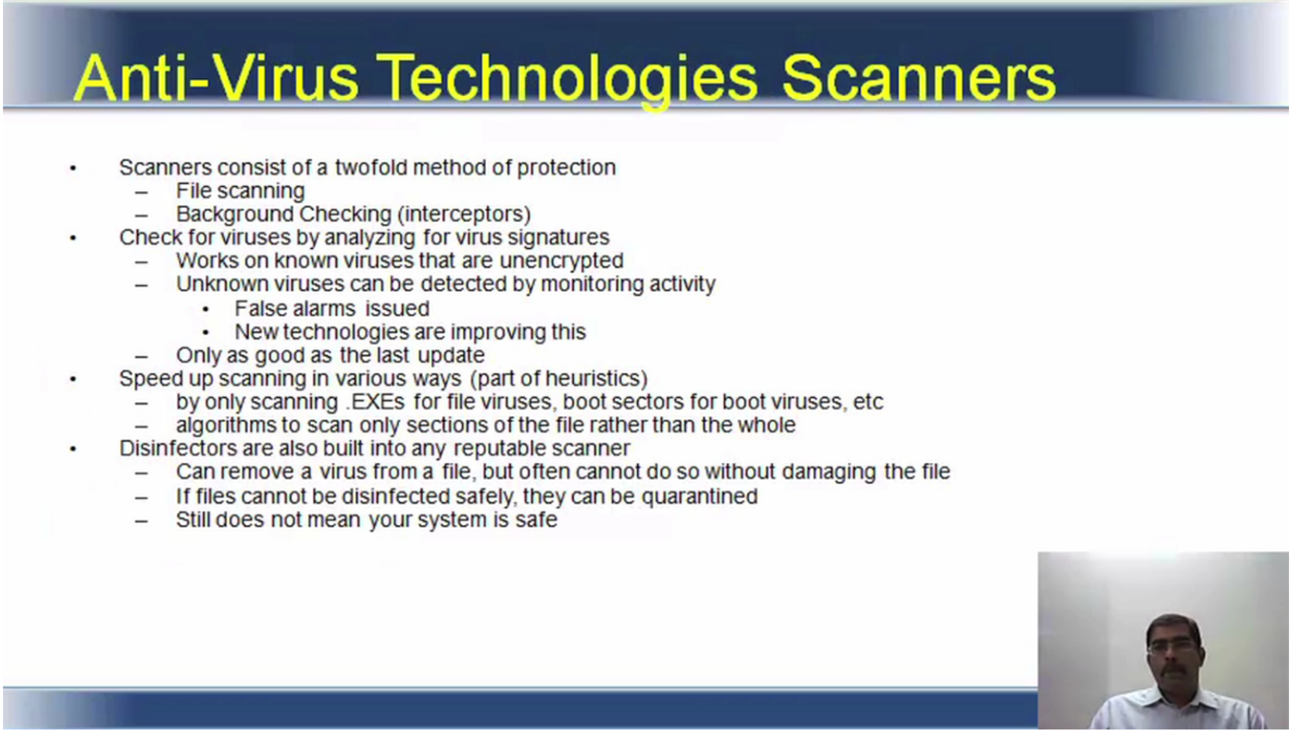


Anti-Virus Technologies

- Scanners
  - Interceptors
  - Disinfectors
  - Heuristics
- Inoculators
- Integrity Checkers
- Safe Computing (aka Common Sense)
- NBAR/QoS
- Anti-Virus Packages

There are scanners; under scanners you have interceptors, you have disinfectors, you have heuristic scanners, then you have inoculators, integrity checkers like file integrity checkers, safe computing or practice common sense, NBAR or quality of service, antivirus packages. Now NBAR is network based application recognition; an, example of detection as the nimda virus are detected using the NBAR or QOS method.

(Refer Time 01:02)



Anti-Virus Technologies Scanners

- Scanners consist of a twofold method of protection
  - File scanning
  - Background Checking (interceptors)
- Check for viruses by analyzing for virus signatures
  - Works on known viruses that are unencrypted
  - Unknown viruses can be detected by monitoring activity
    - False alarms issued
    - New technologies are improving this
  - Only as good as the last update
- Speed up scanning in various ways (part of heuristics)
  - by only scanning .EXEs for file viruses, boot sectors for boot viruses, etc
  - algorithms to scan only sections of the file rather than the whole
- Disinfectors are also built into any reputable scanner
  - Can remove a virus from a file, but often cannot do so without damaging the file
  - If files cannot be disinfected safely, they can be quarantined
  - Still does not mean your system is safe

The scanners basically have a method of two fold protection; one is it scans the files, second background checking that's also called interceptors

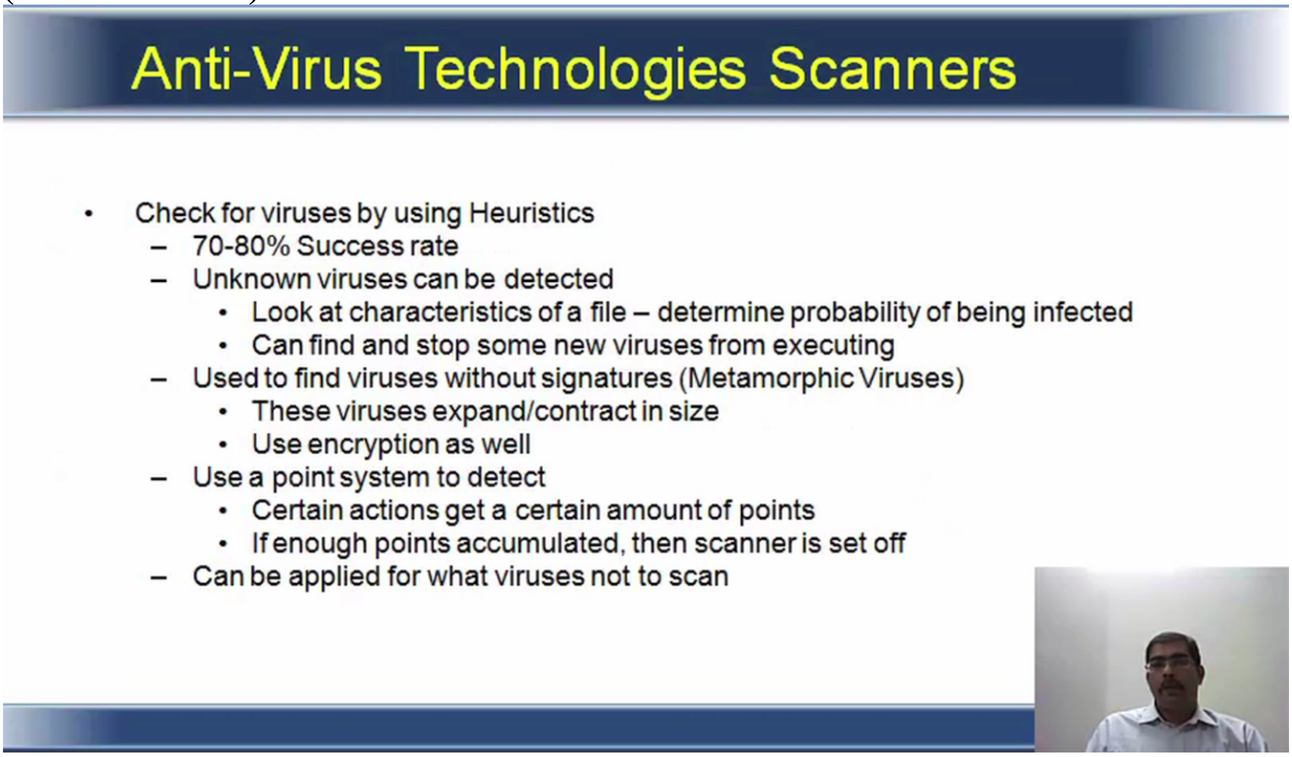
It checks for viruses by analyzing the virus signatures. It works on known viruses that are unencrypted so that's the key point. So anything you encrypt and if there is a virus it will not detect.

Unknown viruses can be detected by monitoring activity; so if you see a sudden surge or sudden usage or for memory, very high memory when you go into that and check then you will know that there is a virus. But the problem is false alarms will be issued, there may genuinely be an application which is consuming a lot of memory. But the new technologies that are coming in are improving this but then your antivirus software is only as good as your last update.) So generally when we go for an audit we ask them when was the or when you verify when will antivirus signatures are last updated

you have varying effects or varying results during the audit. In some is up-to-date on some computers or on some computer it has not been updated for a year. So your latest signatures will not be detected virus signatures will not be detected; so, it becomes a problem; that system which is not updated may in fact go on and infect other systems which are not updated with the latest survivng databases. Then the technologies cannot also speed up by scanning in various way, like it's a part of by heuristic process. It can actually select only the exe's for file viruses, boot sectors or boot viruses, etcetera. So you can have a such criteria or a pattern for which you can speed up the process of antivirus scaning. And then the algorithms are built into scan only the sections of a file rather than the while file.

The disinfectors can also be built into reputable scanners, they are actually built in to reputable scanners. It can remove a virus from a file but it may not be able to do so without damaging the file. If the files cannot be disinfected when they can be quarantined. This is the separate area which the antivirus software marks or holds where the probability of infecting other files are more, so it keeps it in a quarantined area. But that still does not mean that your system is safe.

(Refer Time: 03:58)



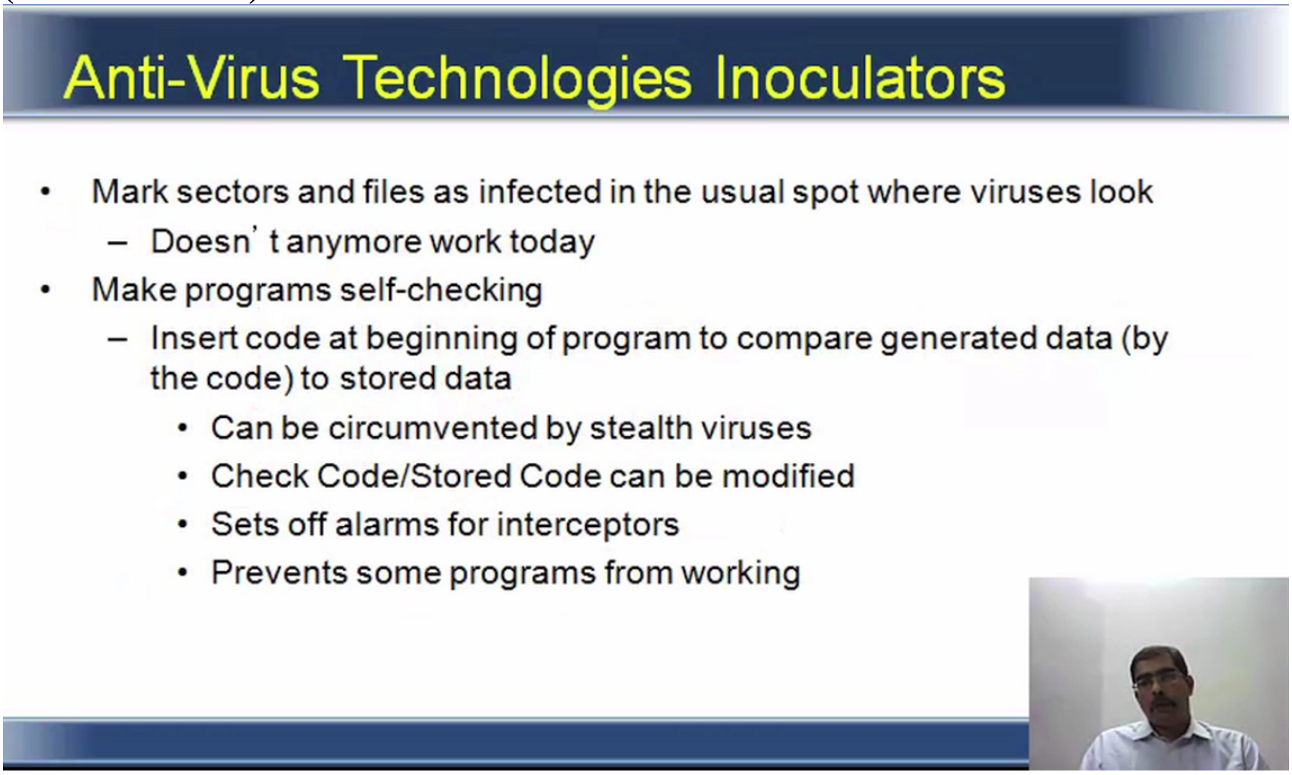
Anti-Virus Technologies Scanners

- Check for viruses by using Heuristics
  - 70-80% Success rate
  - Unknown viruses can be detected
    - Look at characteristics of a file – determine probability of being infected
    - Can find and stop some new viruses from executing
  - Used to find viruses without signatures (Metamorphic Viruses)
    - These viruses expand/contract in size
    - Use encryption as well
  - Use a point system to detect
    - Certain actions get a certain amount of points
    - If enough points accumulated, then scanner is set off
  - Can be applied for what viruses not to scan

The scanners check for viruses by using heuristics there is a seventy-eighty percent success rate.

Unknown viruses can also be detected; meaning it looks for the characteristics of a file and it determines a probability of it being infected. It can find and stop some new viruses from executing. And the heuristics scanners are also used to find viruses without signatures, metamorphic viruses. These viruses expand and contract in size so it is difficult to actually find out whether it is a virus or not. It may use encryption as well so when it uses encryption again the rate of detection is low. It uses a point system to detect that means certain actions get a certain number of points if enough points are accumulated then the scanner is set off it can be applied for what viruses not to scan; so the scanners can be configured to; "ok don't scan the system for this virus", that can be done.

(Refer Time: 05:02)

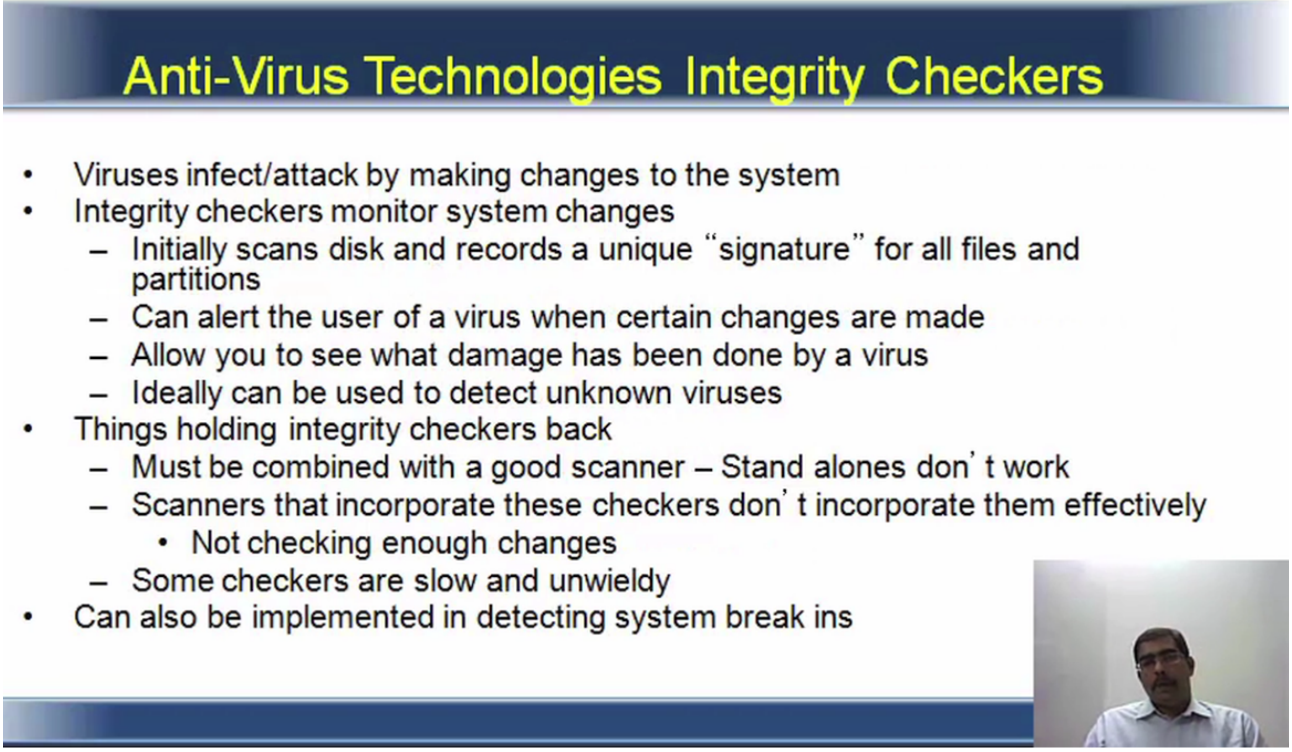


Anti-Virus Technologies Inoculators

- Mark sectors and files as infected in the usual spot where viruses look
  - Doesn't anymore work today
- Make programs self-checking
  - Insert code at beginning of program to compare generated data (by the code) to stored data
    - Can be circumvented by stealth viruses
    - Check Code/Stored Code can be modified
    - Sets off alarms for interceptors
    - Prevents some programs from working

Now you have yet another fancy name, inoculators. What it does is it marks the sectors and files as ins infected in the usual spot wherever viruses look, so it doesn't look in that spot anymore. And it doesn't work in today's environment it makes programs self checking; that means it inserts a code at the beginning of a program to compare the generated data to store data, that is before image and after image. It can be circumvented by stealth viruses, that's one of the blunt move, check code or stored code can be modified, it sets off alarm for the interceptors and it also prevents some program from working; these are the down falls of the inoculators.

(Refer 05:55)



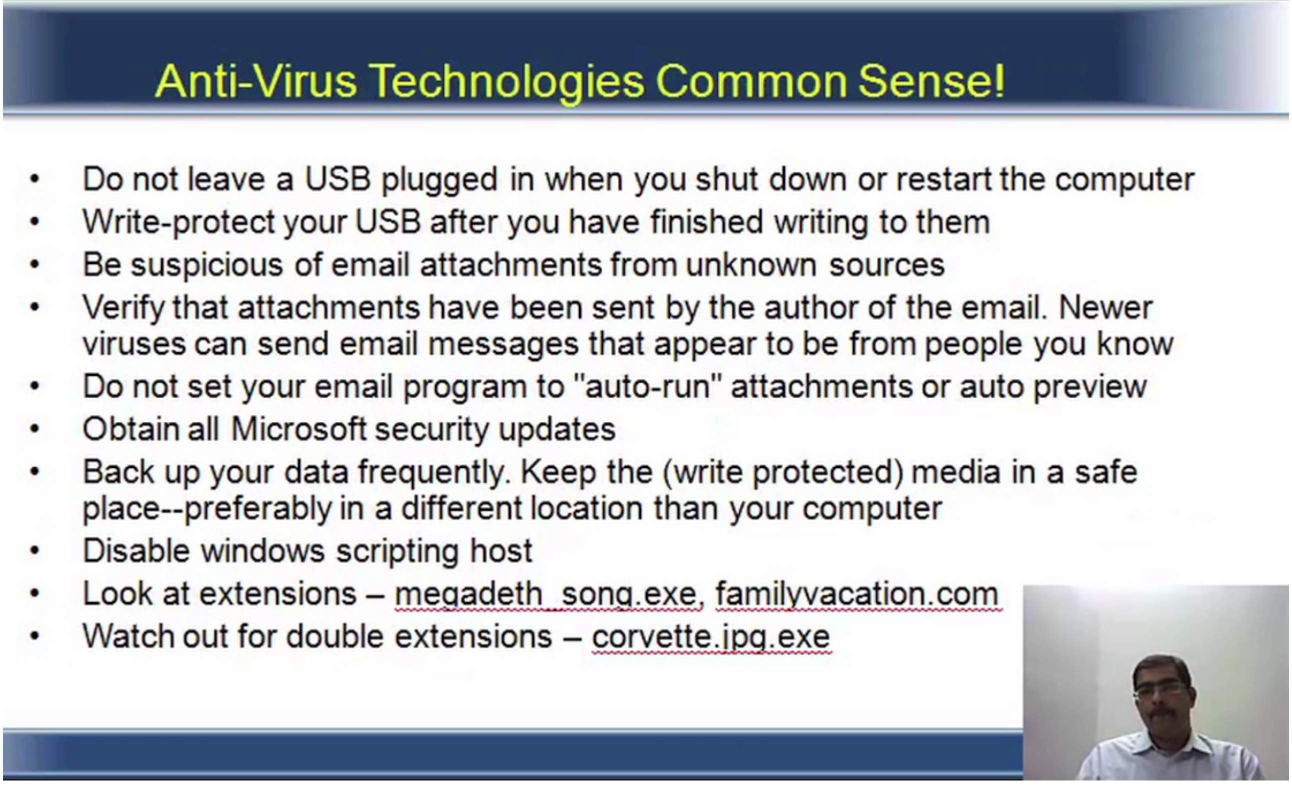
Anti-Virus Technologies Integrity Checkers

- Viruses infect/attack by making changes to the system
- Integrity checkers monitor system changes
  - Initially scans disk and records a unique "signature" for all files and partitions
  - Can alert the user of a virus when certain changes are made
  - Allow you to see what damage has been done by a virus
  - Ideally can be used to detect unknown viruses
- Things holding integrity checkers back
  - Must be combined with a good scanner – Stand alones don't work
  - Scanners that incorporate these checkers don't incorporate them effectively
    - Not checking enough changes
  - Some checkers are slow and unwieldy
- Can also be implemented in detecting system break ins

Then the intergrity checkers; now the viruses infect or attack by making changes to the system we know that we have learnt it by now.

Integrity checkers monitor system changes. It initially scans a disk and record a unique signature for all files and partitions it can also alert the user of a virus when certain changes are made, it allows you to see what damage has been done by the virus, it can also be used to detect unknown viruses. But what are the things that are holding the integrity checkers back; it must be combined with the good scanner, so stand alone intergrity checkers may not work. Scanners that incorporate these intergrity checkers don't incorporate them effectively that means it is not checking enough changes.

Some checkers are slow and unwieldy, difficult to handle uses a of lot of memory. It can also be implemented in detecting system break ins.
(Refer Time: 07:05)



Anti-Virus Technologies Common Sense!

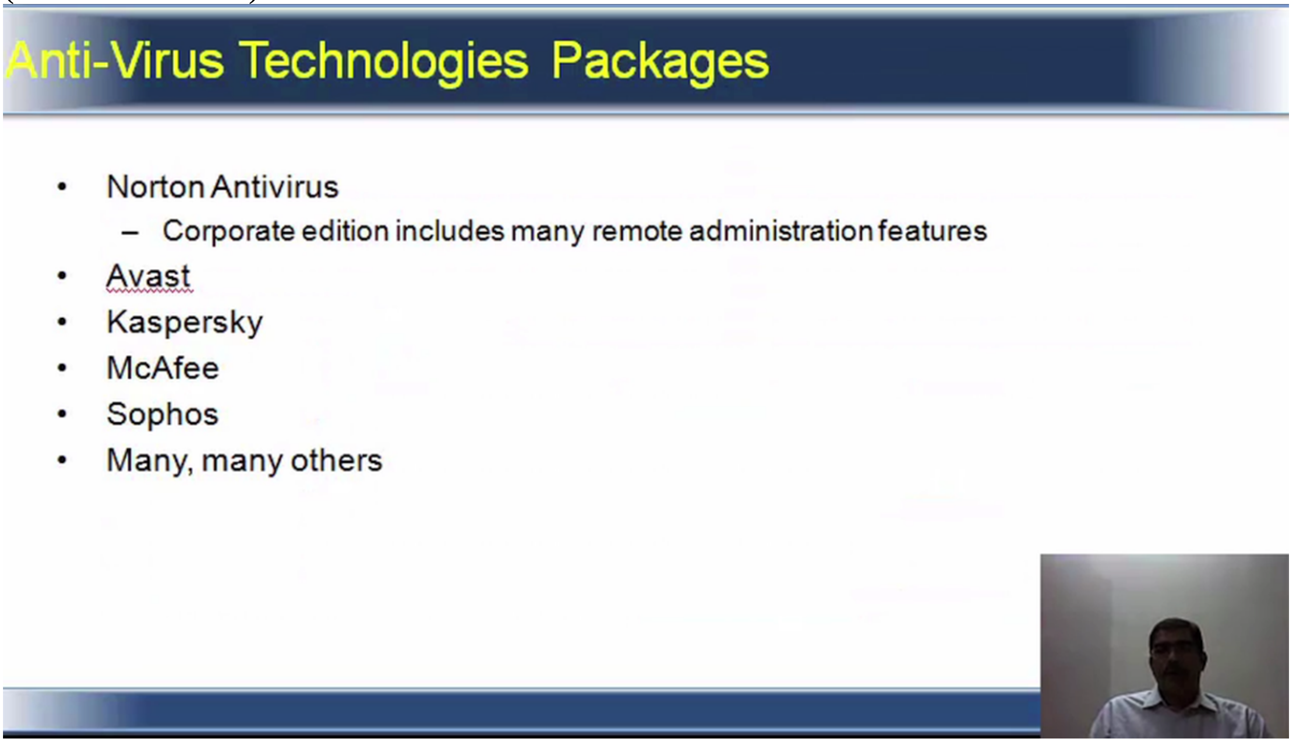
- Do not leave a USB plugged in when you shut down or restart the computer
- Write-protect your USB after you have finished writing to them
- Be suspicious of email attachments from unknown sources
- Verify that attachments have been sent by the author of the email. Newer viruses can send email messages that appear to be from people you know
- Do not set your email program to "auto-run" attachments or auto preview
- Obtain all Microsoft security updates
- Back up your data frequently. Keep the (write protected) media in a safe place--preferably in a different location than your computer
- Disable windows scripting host
- Look at extensions – megadeth_song.exe, familyvacation.com
- Watch out for double extensions – corvette.jpg.exe

This is the human element of it. The basic thing is that every computer user should do. Do not leave a USB plugged in when you shut down or restart the computer, if your USB flash disc is a write protect use it and be suspicious of email attachment from unknown sources don't double click it don't open it if you don't know the sender delete it verify that the attachments have been sent by the author of the email; newer viruses that is the one that are the prevalent now can send email messages that appear to be from people you know but actually are not and do not set your email program to auto run attachments or auto preview and the most important thing is obtain all microsoft security updates.

Backup your data frequently, there is a very famous saying by Simom L Garfinkel in his unix book one who does not archive is condemned rewrite so take the backups of the system, your files regularly otherwise you will have to re do the whole process again. Disable windows scripting, look at extensions; now if you look at this example megadeth underscore song dot e x e, it's a song its not a exe so you will come to know that there is a problem, it should be dot mp3 or dot mov or dot a v i, family vaction dot com i mean you have to look at the extensions very very diligently to see if there is a possibility of a virus and then look out for double extensions a dot j p g and a dot e x e together this is just an example it could be a combination of any two files that just a issue, this double extension thing actually works even though it's a very, its sound very stupid, the windows itself will hide the extension of known types. So it will appear as having only a single extension where you have a dot text dot j p g it may display, in windows will display only dot j p g.

Iit will not display the dot text dot j p g, so that actually works for the virus.

(Refer Time: 09:42)

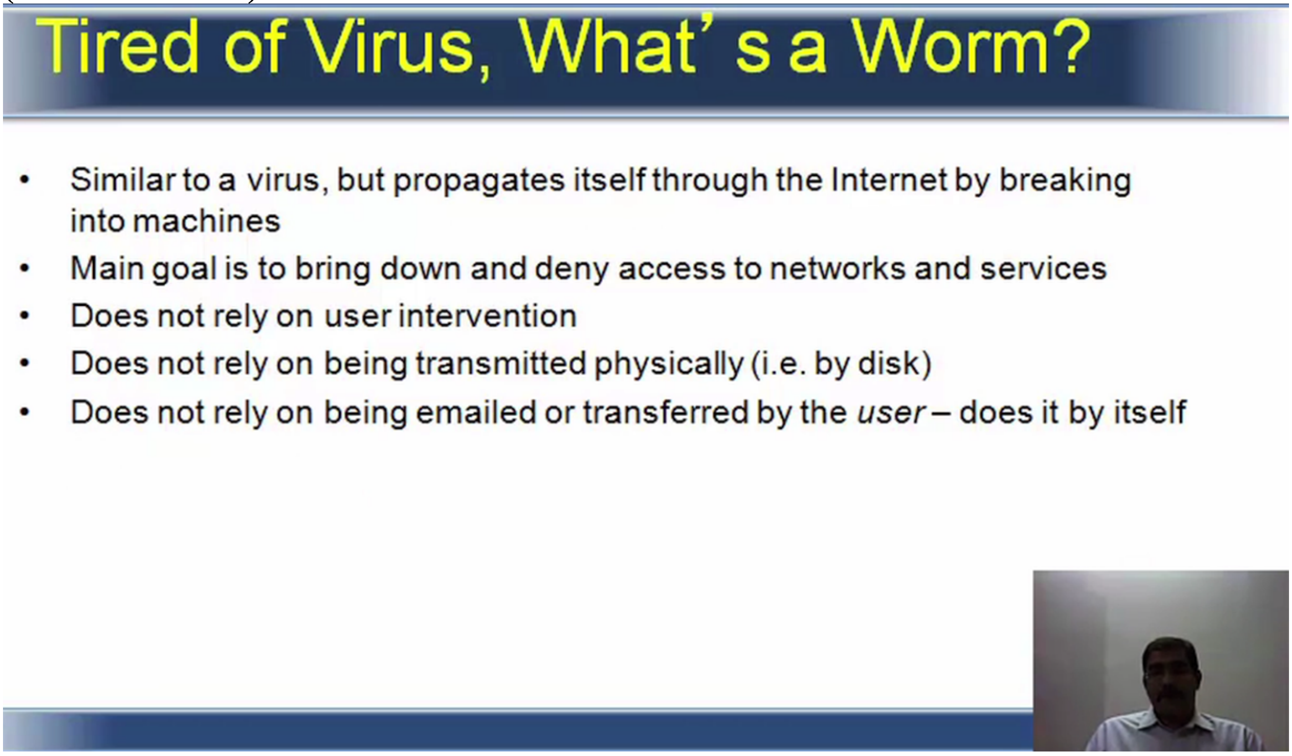


Anti-Virus Technologies Packages

- Norton Antivirus
  - Corporate edition includes many remote administration features
- Avast
- Kaspersky
- McAfee
- Sophos
- Many, many others

Some of the popular packages; there are so many there is no allegiance to any of these companies but the some of the popular one have been listed here; norton is one, avast is a free one, kaspersky, mcafee, sophos. There are several others I mean you can think of so many antivirus; in india itself there was something called caseware computing so there are several antivirus technology packages available.

(Refer Time: 10:11)



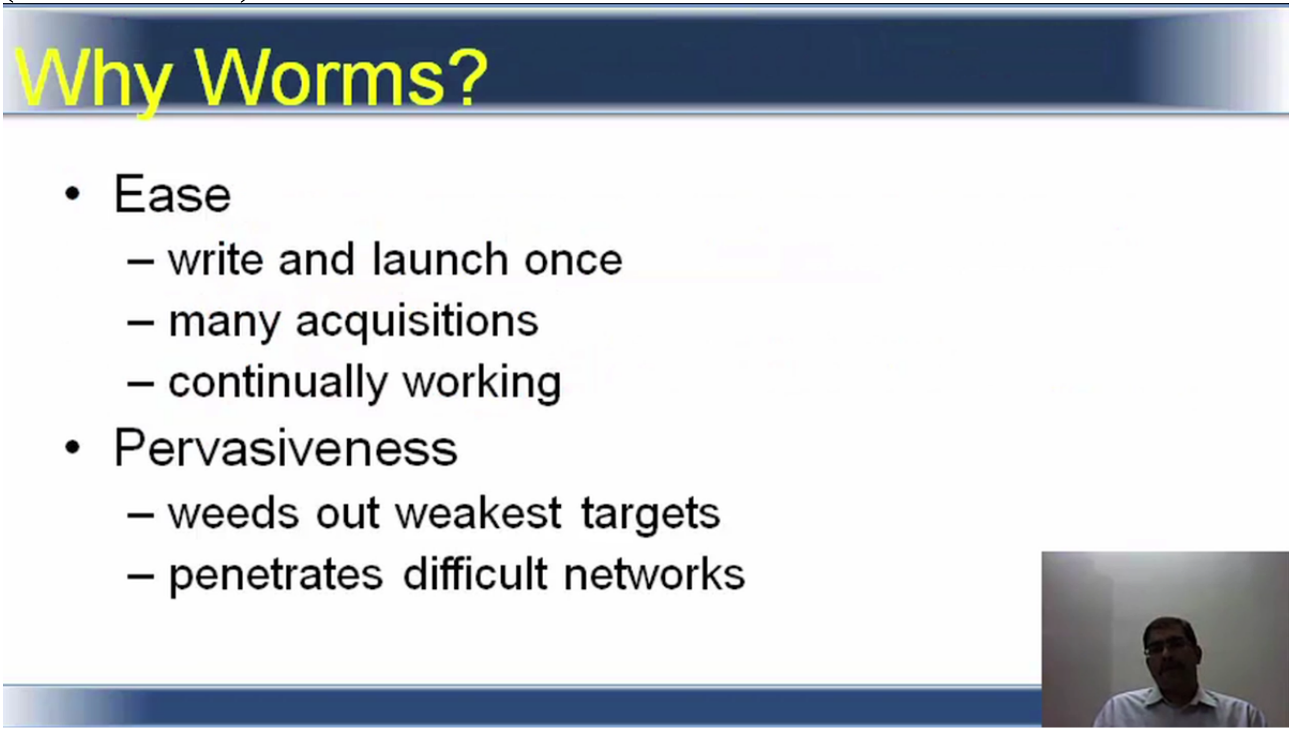
Tired of Virus, What’ s a Worm?

- Similar to a virus, but propagates itself through the Internet by breaking into machines
- Main goal is to bring down and deny access to networks and services
- Does not rely on user intervention
- Does not rely on being transmitted physically (i.e. by disk)
- Does not rely on being emailed or transferred by the *user* – does it by itself

I myself have become tired by talking about virus. Lets go and see whats a worm. Worm is similar to a virus but propagates itself through the internet by breaking into machines.

What are the main goal, it is to bring down and deny access to the networks and services, it does not rely on user intervention and it does not rely on being transmitted physically that is by a disk and it does not rely on being emailed or transferred by the user it does it by itself.

(Refer Time 10:46)

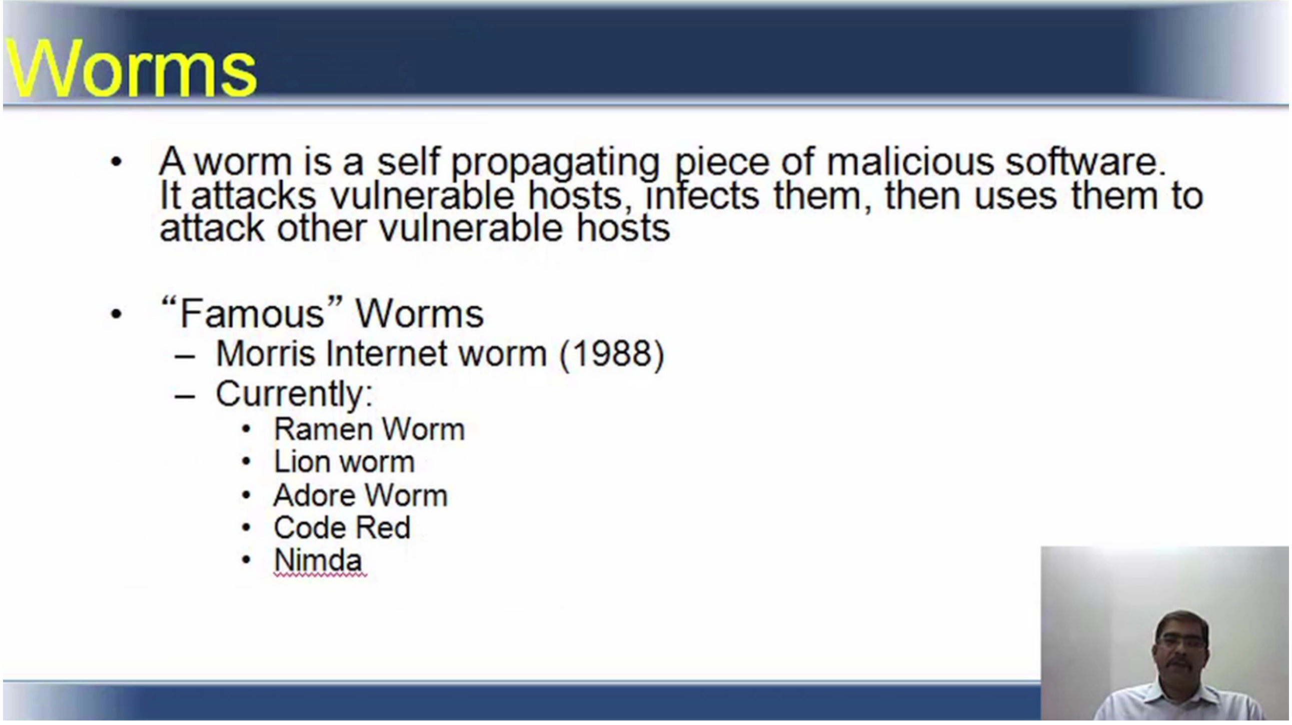


Why Worms?

- Ease
  - write and launch once
  - many acquisitions
  - continually working
- Pervasiveness
  - weeds out weakest targets
  - penetrates difficult networks

But when you have viruses why do you need worms because of ease to write it and launch it once, then the worm takes care of it then you have many acquisitions and it continuously works; then the pervasiveness it weeds out the weakest targets, it penetrates difficult networks.

(Refer Time: 11:13)



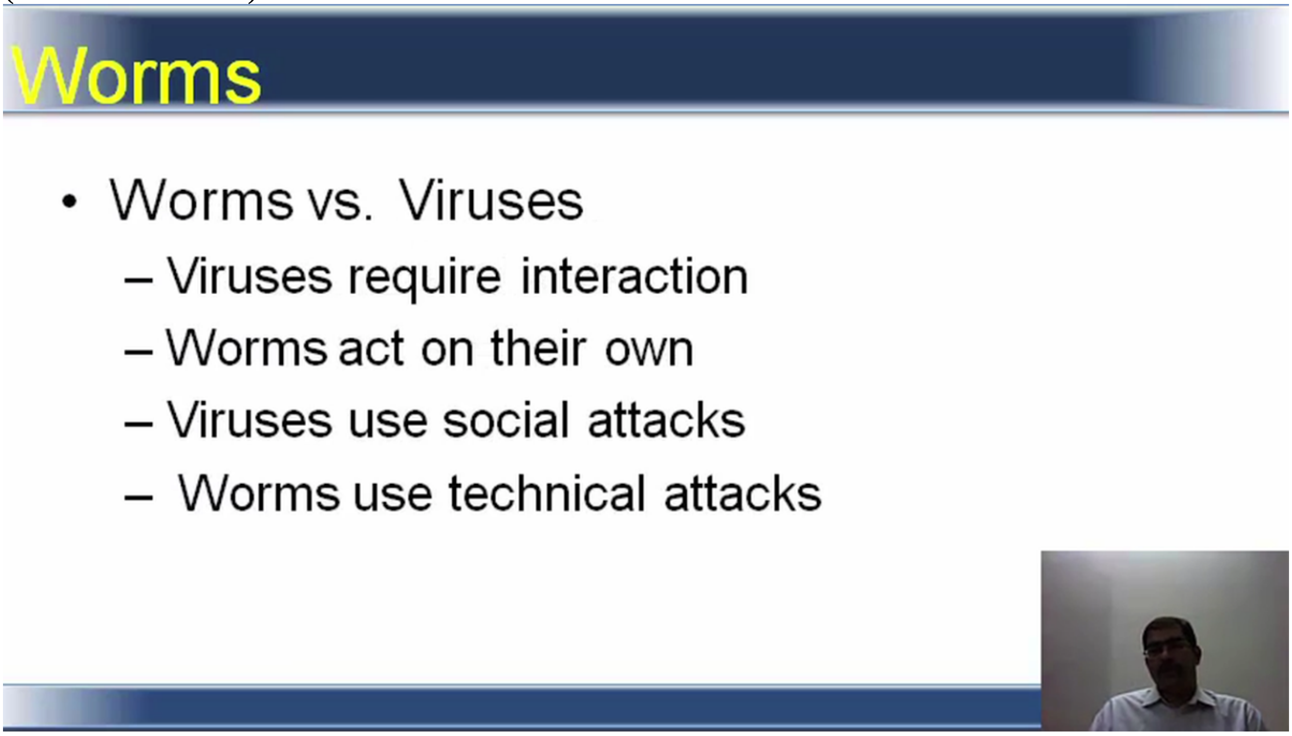
Worms

- A worm is a self propagating piece of malicious software. It attacks vulnerable hosts, infects them, then uses them to attack other vulnerable hosts
- “Famous” Worms
  - Morris Internet worm (1988)
  - Currently:
    - Ramen Worm
    - Lion worm
    - Adore Worm
    - Code Red
    - Nimda

So now if you look at the definition it is a self propagating piece of malicious software, it attacks vulnerable hosts, infects them then uses them to attack other vulnerable hosts. Some of the famous worms were the morris worm of nineteen eighty eight, the ramen worm, the lion worm, adore worm, code red, of late it is the nimda.

But then who writes these worms, hackers write it to penetrate networks, crackers do it, researchers do it then there are a specific brand of people called virus writers, their job is to write the virus they can be use by both the antivirus companies or by malicious people or with the intention of destruction they can be motivated.

(Refer Time: 12:11)

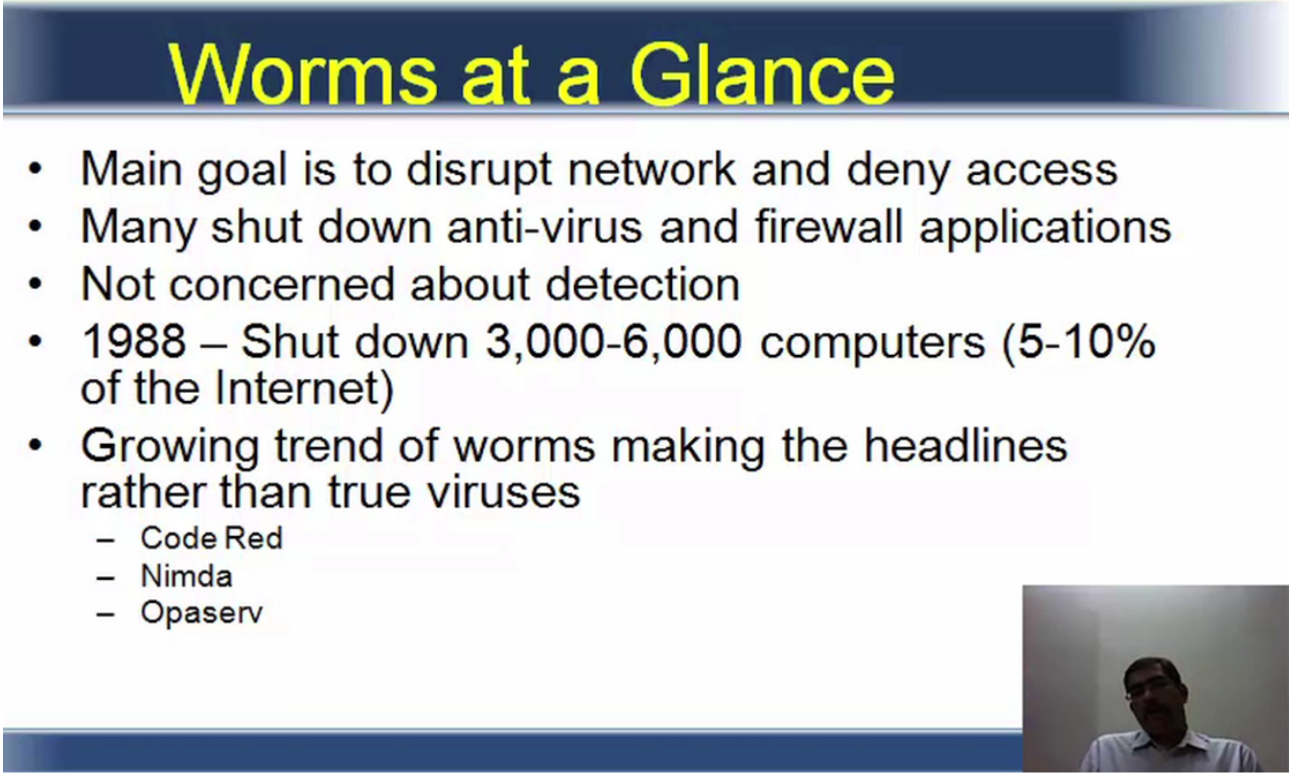


Worms

- Worms vs. Viruses
  - Viruses require interaction
  - Worms act on their own
  - Viruses use social attacks
  - Worms use technical attacks

But when you look at viruses versus worms, the basic differences viruses require interaction that means it needs a carrier it needs some action on the part of the user to propagate but the worms act out on their own. Viruses use social attacks, worms use technical attacks so there is a big different between virs and worms.

(Refer Time: 12:39)

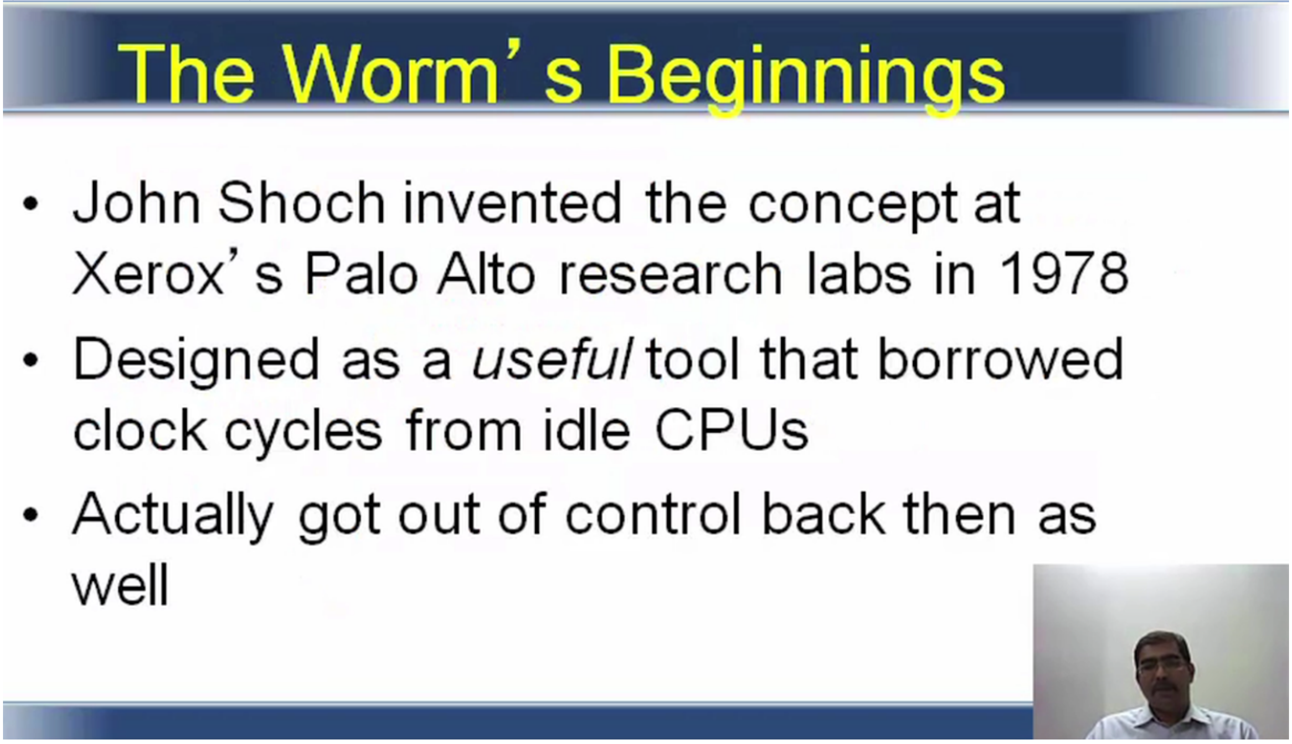


Worms at a Glance

- Main goal is to disrupt network and deny access
- Many shut down anti-virus and firewall applications
- Not concerned about detection
- 1988 – Shut down 3,000-6,000 computers (5-10% of the Internet)
- Growing trend of worms making the headlines rather than true viruses
  - Code Red
  - Nimda
  - Opaserv

The main goal of the worm is todisrupt the network and deny access; many shut down antivirus and firewall applications.

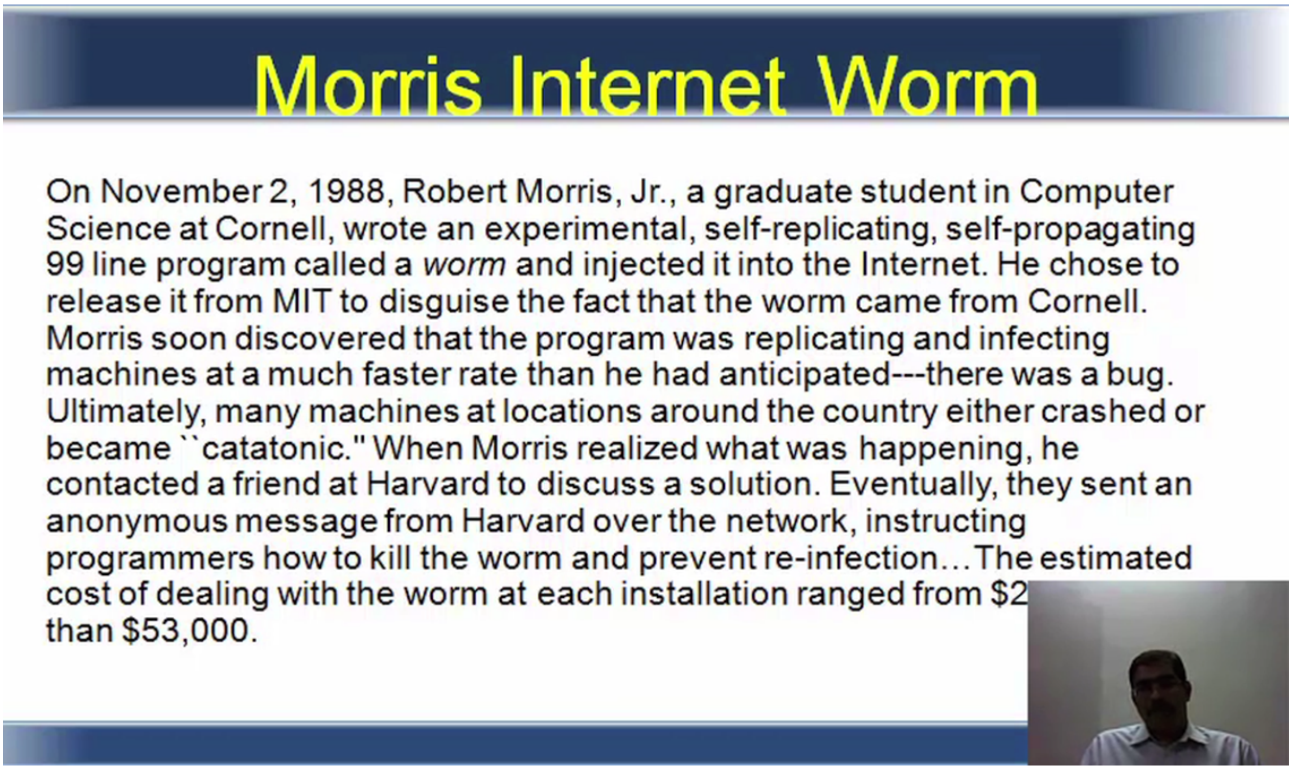
So the worm has a capability to shut down your antivirus program or your firewall applications. Its not concerned about detection in nineteen eighty eight, the worm shut down three thousand to six thousand computers so at that time it was five to ten percent of the internet. And growing trends of the worms making the headlines or rather than true viruses now you read code red was famous nimda was famous opaserv was famous. You have to think of worms like this. It's got wide spread geographic in infection rather than a system infection. The virus has got a wide spread system infection this is got a wide spread geographical infection. So it finds a potential target. replicates itself transfers itself, executes; so worms are much more dangerous than virus.
(Refer Time: 13:42)



The Worm's Beginnings

- John Shoch invented the concept at Xerox's Palo Alto research labs in 1978
- Designed as a *useful* tool that borrowed clock cycles from idle CPUs
- Actually got out of control back then as well

What are the worms' beginnings, when did it start? It started in nineteen seventy eight and john shoch invented the concept at xerox's palo alto research labs it was designed as a useful tool that borrowed clock cycles from idle CPU's and an it actually got of out of control even then. M
(Refer Time: 14:06)



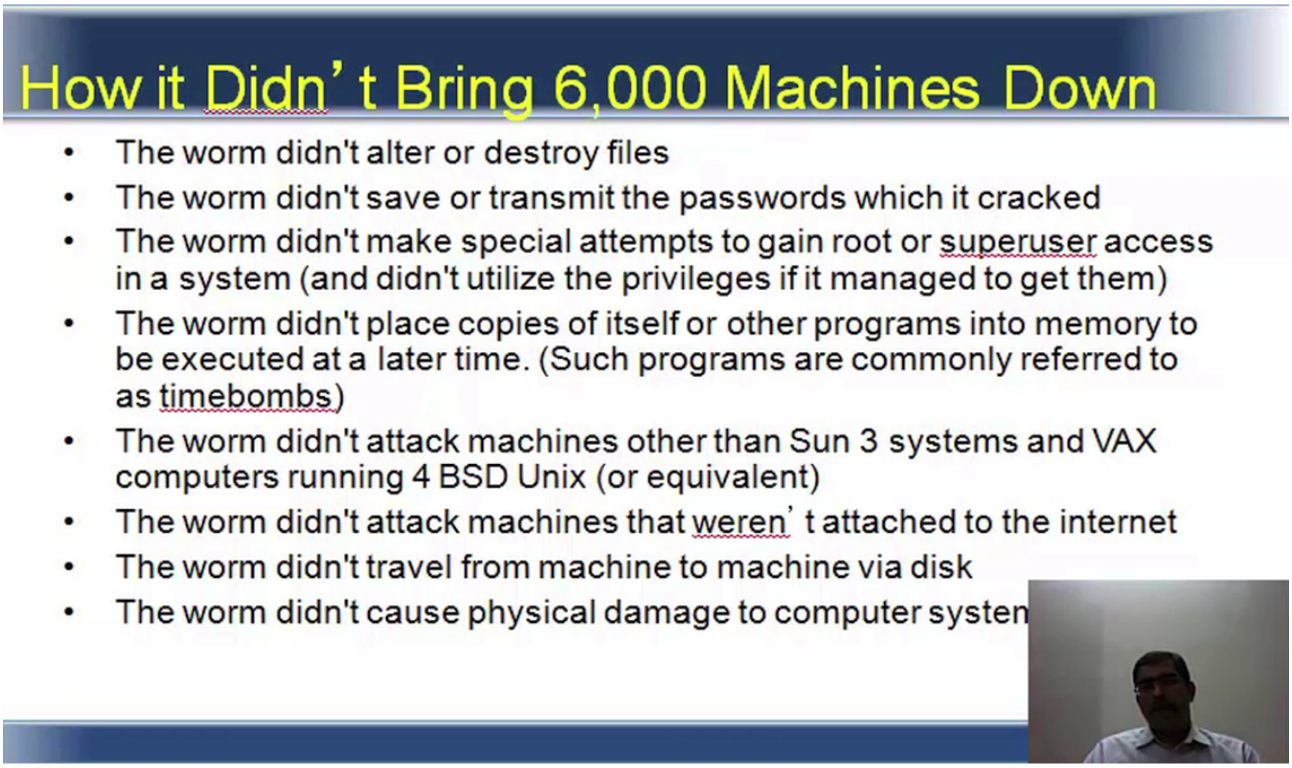
Morris Internet Worm

On November 2, 1988, Robert Morris, Jr., a graduate student in Computer Science at Cornell, wrote an experimental, self-replicating, self-propagating 99 line program called a *worm* and injected it into the Internet. He chose to release it from MIT to disguise the fact that the worm came from Cornell. Morris soon discovered that the program was replicating and infecting machines at a much faster rate than he had anticipated---there was a bug. Ultimately, many machines at locations around the country either crashed or became ``catatonic." When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent re-infection…The estimated cost of dealing with the worm at each installation ranged from $2
than $53,000.

Morris was a very famous internet worm there is a article on that, its replicated here, “On november second nineteen eighty eight robert morris junior, a graduate student in computer science at Cornell wrote an experimental self replicating self propagating ninety nine line program called a worm and injected it into the internet he chose to release it from MIT to disguise the fact that the worm came from Cornell. that was smart move. Morris soon discovered that the program was replicating and infecting machines at a much faster rate than he had anticipated there was a bug so that's why this happened very fast ultimately many machines at the locations around the country either crashed or became catatonic when morris realized what was happening he contacted a friend at harvard to discuss the solution

eventually they sent an anonymous message from harvard over the network instructing programs on how to kill the worm and to prevent re infection the estimated cost of dealing with the worm at each installation ranged from two hundred dollars to more than fifty three thousand dollars so the damage was quite high; in eighty eight two hundred dollars was big, fifty three thousand dollars even bigger.

(Refer Time: 15:35)



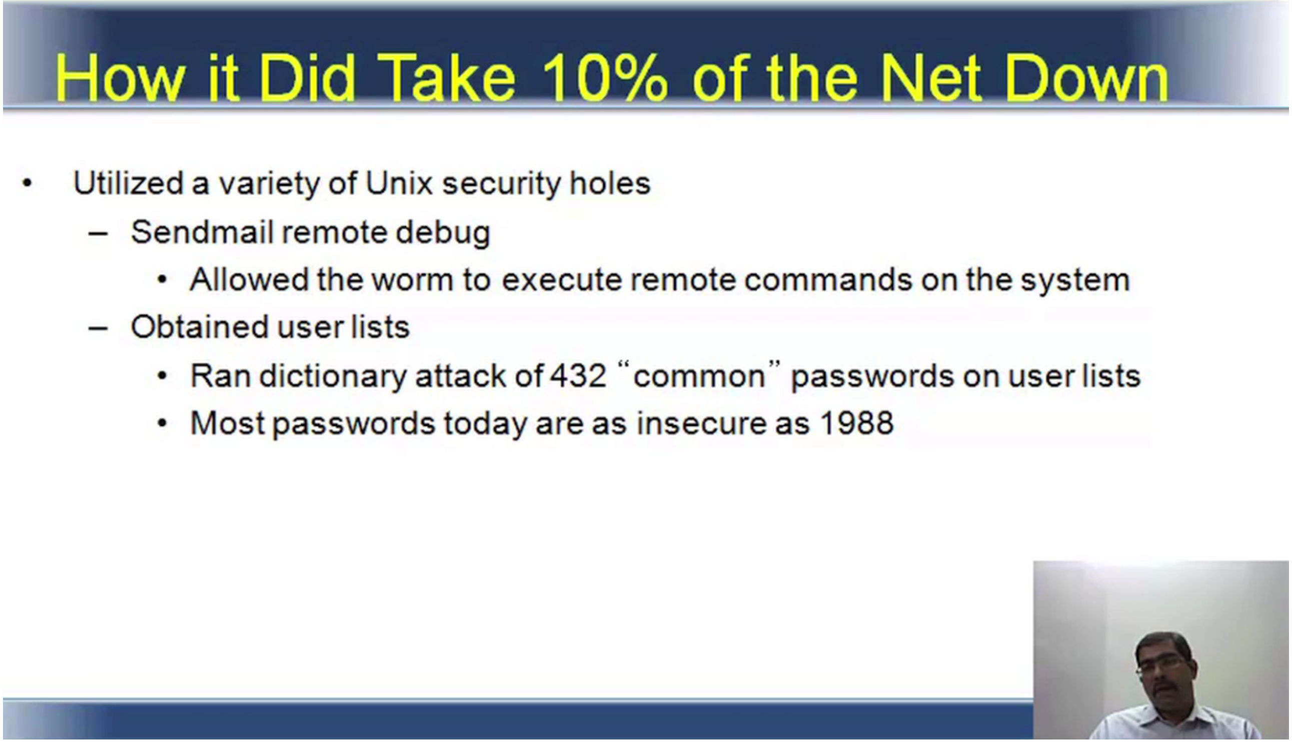
How it Didn’t Bring 6,000 Machines Down

- The worm didn't alter or destroy files
- The worm didn't save or transmit the passwords which it cracked
- The worm didn't make special attempts to gain root or superuser access in a system (and didn't utilize the privileges if it managed to get them)
- The worm didn't place copies of itself or other programs into memory to be executed at a later time. (Such programs are commonly referred to as timebombs)
- The worm didn't attack machines other than Sun 3 systems and VAX computers running 4 BSD Unix (or equivalent)
- The worm didn't attack machines that weren’t attached to the internet
- The worm didn't travel from machine to machine via disk
- The worm didn't cause physical damage to computer systen

How it did not bring six thousand machines down? This particular worm did not alter or destroy the files and it didn't save or transmit the password which it tracked, the worm didn't make special attempts to gain root or super user access in to a system, it didn't place copies of itself or other programs into memory to be executed at a later time,

so say again it didn't to a time bomb like function, it didn't attack machines other than Sun three systems and VAX computers running four BSD unix or equivalent. So it has again focused on a small range of OSs, the worm didn't attack machines that were'nt attached to the internet and it didn't travel from machine to machine via a disk it didn't cause physical damage to the computer system.

(Refer Time: 16:33)



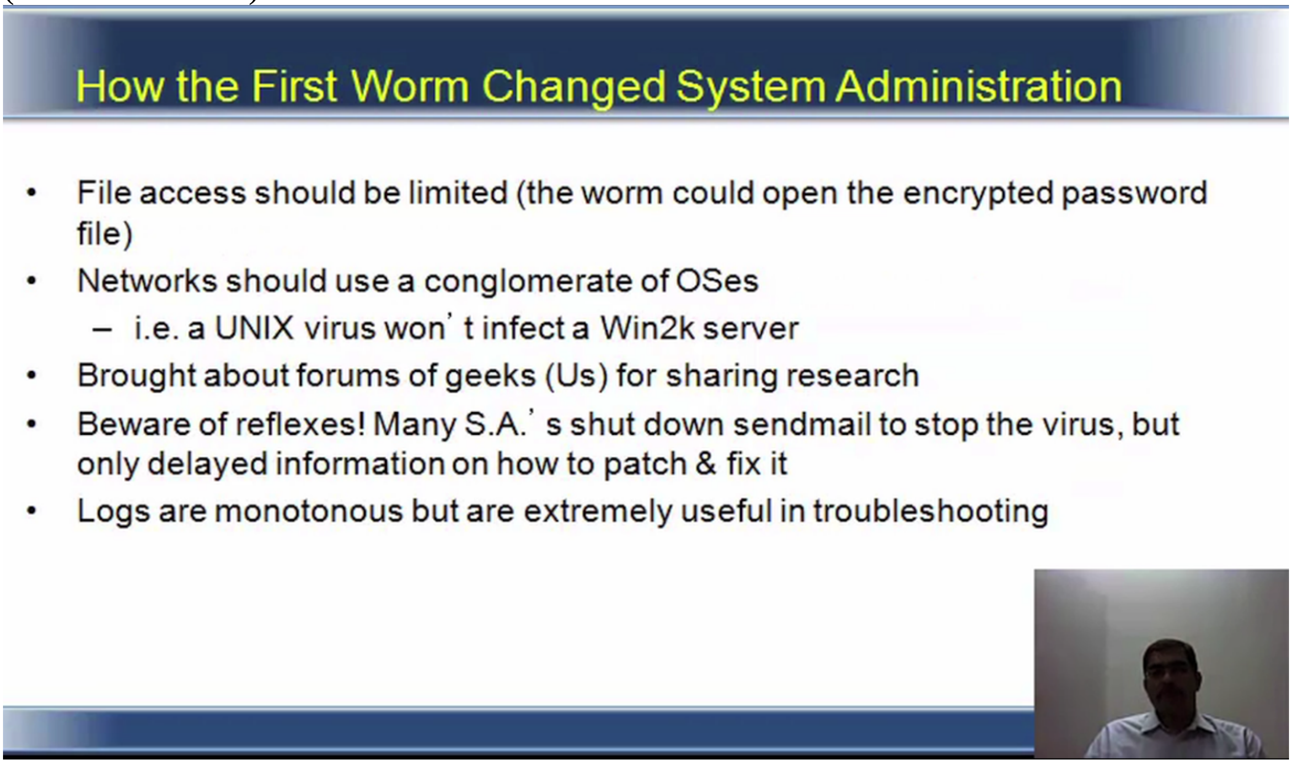
How it Did Take 10% of the Net Down

- Utilized a variety of Unix security holes
  - Sendmail remote debug
    - Allowed the worm to execute remote commands on the system
  - Obtained user lists
    - Ran dictionary attack of 432 “common” passwords on user lists
    - Most passwords today are as insecure as 1988

But then it took on ten percent of the internet how did it take it down? it utilized a variety of unix security holds at that time a sent mail remote debug was a issue, it allowed to worm to execute remote commands on the system.

The send mail remote debug vulnerabililty allowed the worm to execute remote commands on the system. It obtained user lists, it ran a dictionary attack of four thirty two common passwords on user lists and even in nineteen eighty eight the passwords then were as insecure as the password were we used today.

(Refer Time: 17:20)



How the First Worm Changed System Administration

- File access should be limited (the worm could open the encrypted password file)
- Networks should use a conglomerate of OSes
  - i.e. a UNIX virus won’ t infect a Win2k server
- Brought about forums of geeks (Us) for sharing research
- Beware of reflexes! Many S.A.’ s shut down sendmail to stop the virus, but only delayed information on how to patch & fix it
- Logs are monotonous but are extremely useful in troubleshooting

How the first worm changed the system administration, file access should be limited thats worm could open the encrypted password file, network should use a conglomerate of OSs that is a unix virus will not affect a windows two thousand server or a windows two thousand eight server or a two thousand twelve server; it brought about forums of geeks for sharing research and then beware of reflexes, many system administrators shut down the sent mail to stop the viruses but only delayed information on how to patch it and fix it, so just by pulling out the internet they didn't actually prevent the attack, they just delayed the attack from at logs are monotonous but are extremely useful in trouble shooting.

So as auditors or as security professional we also we always tell the customers to have proper log management system to monitor the logs but then the logs provide us a lot of information about how a network performance what the issues are on specific devices, what actually is happening in the applications or on the network, its very helpful in trouble shooting problems.

(Refer Time: 18:46)

The first worms were actually designed and released in the eighties worms were non destructive and generally were released to perform helpful network tasks. If we take an example vampire worm, it remains idle during the day at night it would use the spare CPU cycles to perform complex tasks that required extra computing power.

Sometimes it could also be that these worms were used as the automatic schedule light house operations for taking the system backups when the CPU cycles are idle; so at night time generally when the processing is not done much these worms used to run and create a backup and keep it.

(Refer Time: 19:36)