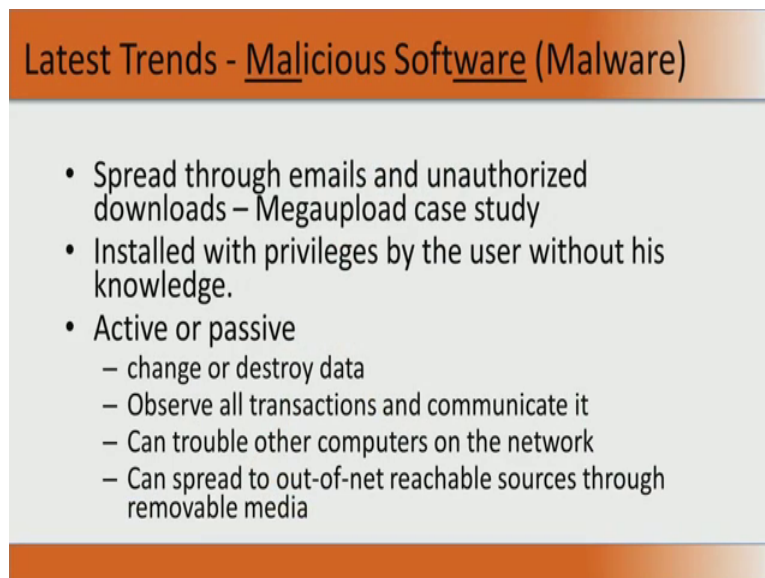


**Introduction to Information Security**  
**Prof. V. Kamakoti**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Madras**

**Lecture - 19**

The next we will see is about malicious software or malware. This is another latest trend of attacking your system.

(Refer Slide Time: 01:31)



Latest Trends - Malicious Software (Malware)

- Spread through emails and unauthorized downloads – Megaupload case study
- Installed with privileges by the user without his knowledge.
- Active or passive
  - change or destroy data
  - Observe all transactions and communicate it
  - Can trouble other computers on the network
  - Can spread to out-of-net reachable sources through removable media

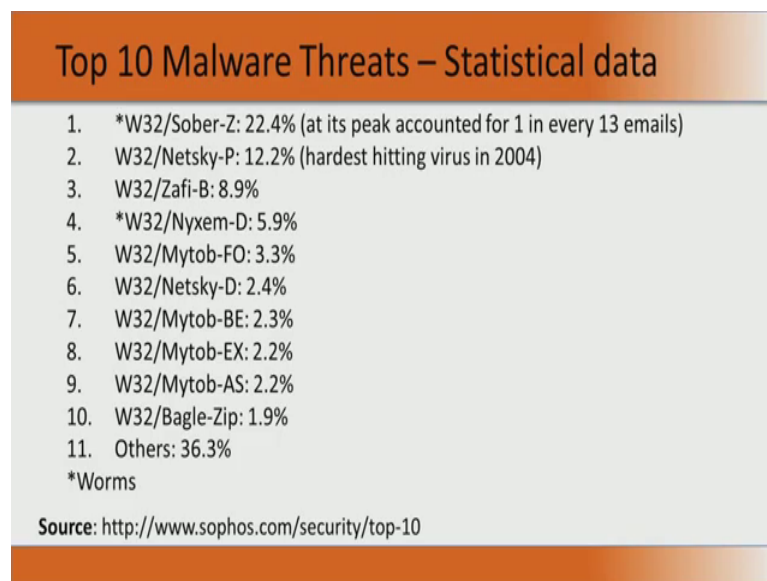
Now, we saw in module 1 that one way that malware, this malicious software can spread is through emails and also through unauthorized downloads. We had a mega upload case study if you remember in the module 1 and what happens is that through these emails and through these unauthorized downloads, the malware actually sticks to these files and emails and the moment you go and click or open these files or the attachments in these emails, the software gets installed. It actually gets installed with the privileges of the user. If you have click it, it actually gets your privilege and after getting installed in your system without your knowledge, what can this do? It can go and change or destroy the data in your system in that case it is an active software, or it can just observe all the transactions that you do and communicate it without your knowledge. That case it is a passive attack on your system and it can also create some random packets and keep pumping into the network creating trouble for the other computers in proximity.

The other interesting virus that you had seen is that this could keep quiet and whenever there is some removable storage like you have USB pen drive comes without this virus,

it can just basically replicate itself into that USB and that when the USB goes to some other place within the network, it can go and infect that system and when the USB from that system has come and insert back into the system, then some data of that system can come here and get transferred.

So, if you have an office where you are made a complete distinction, there are systems which use the computers and there are some systems which are not connected to the internet, there are systems which are connected to the internet, then it is very valid request that somebody wants to say read a paper, a research paper and so, they go and download it from the internet, put it in USB drive and come to the other office, insert it and start reading. Along with that USB, in that USB drive it may not be just the paper that is transferred, but can also be a malware. So, the malware enters from office room A which is connected to the internet to room B, which is not connected to the internet. Now, here the malware can collect some information and some day this USB goes back to room A, then it can transfer it back to the internet. So, it can come here and it can move from room A, to room B and it can start creating issues at room B. So, this is how your malware can even reach out of net reachable, out of net reachable resources. Even the network internet cannot reach there, but your malware can still reach and this is basically possible because we have removable media. That is why many organization USBs are disabled.

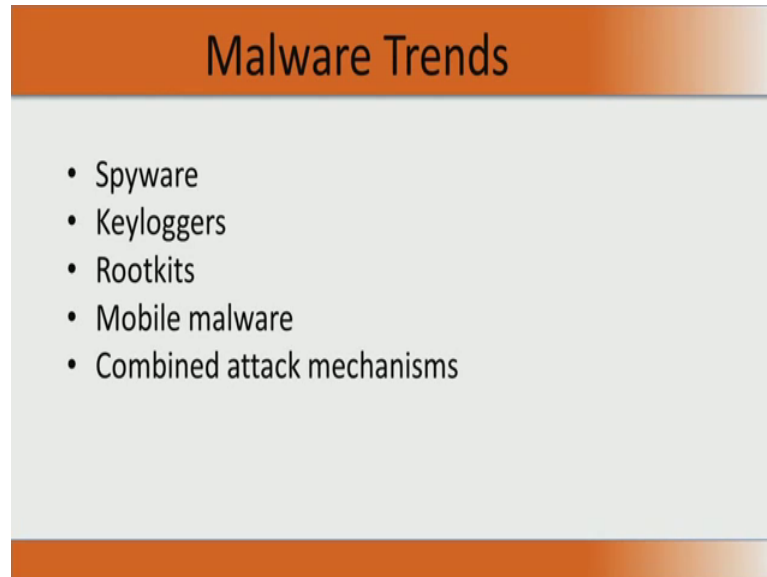
(Refer Slide Time: 03:58)



Now, these are 10 top malware threats. So, statistical data we got from sophos.com in which I did mention the sober actually was the software which gave a wrong email and

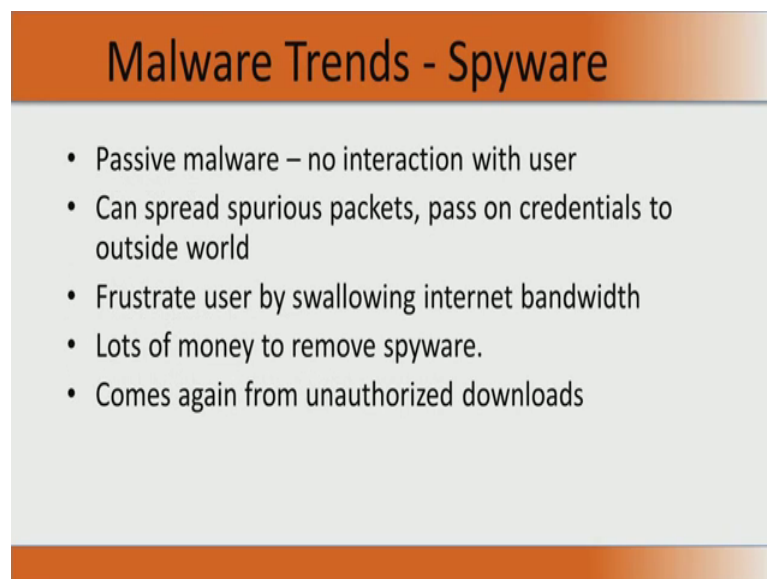
intimated people by using some big words, so that you say you have gone into illegal accounts, all these things and it was basically getting back the credentials of these users.

(Refer Slide Time: 04:36)



Now, we will see what are the ways by which, what are the different types of malware? It could be Spyware, Keyloggers, Rootkits, mobile malware and a combination of these. We will go and quickly see about Spyware, Keyloggers, Rootkits, mobile malware in this talk.

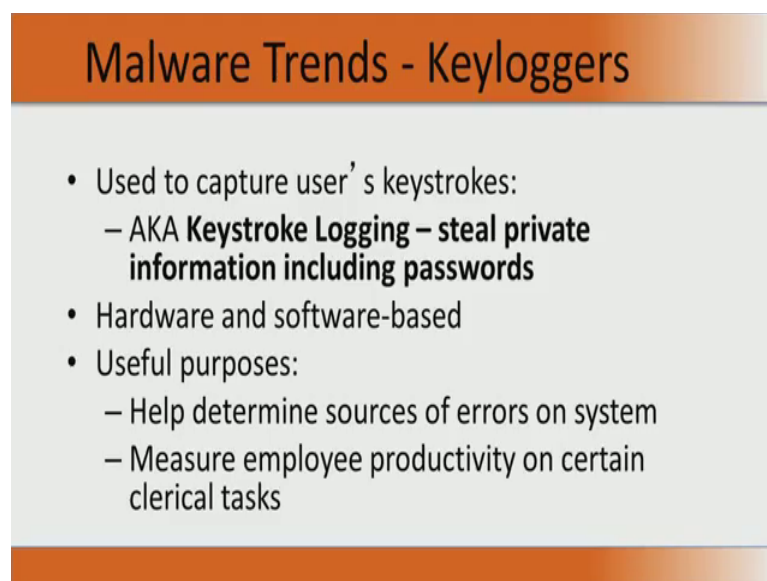
(Refer Slide Time: 04:57)



So, what is a spyware? It is actually a passive malware. It does not show. It is sort of lot of having lot of stealth. It just stays in your system; it does not interact with the user. So,

from the user's perspective, it is very stale. It does not even realise that there is a passive malware running, but what can this malware do. It can start spreading spurious packets on the network, choking the network, making an availability issue; it can pass on credential show outside world. Actually it can frustrate the user by swallowing his complete internet bandwidth. Note that if you want to remove the spyware, lots of money are needed to remove spyware and this spyware like any other malware can also come from the unauthorized downloads like the mega upload case study that we saw in the previous module.

(Refer Slide Time: 05:59)



**Malware Trends - Keyloggers**

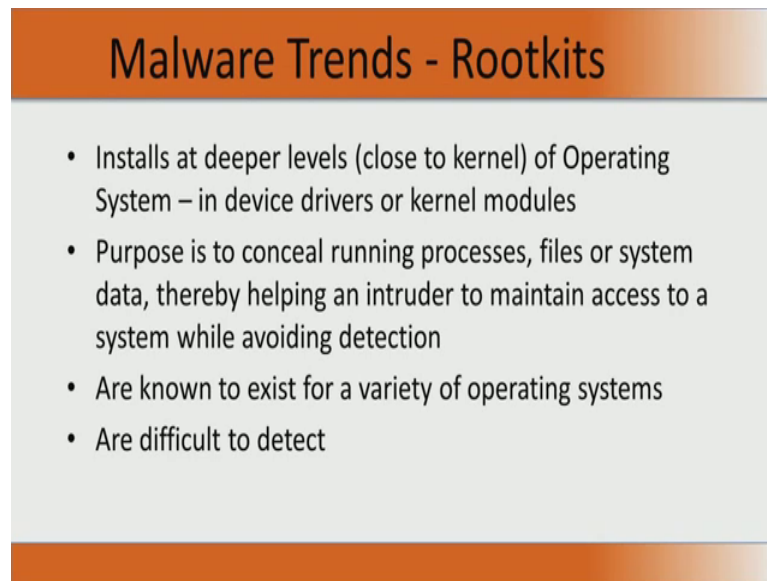
- Used to capture user's keystrokes:
  - AKA **Keystroke Logging – steal private information including passwords**
- Hardware and software-based
- Useful purposes:
  - Help determine sources of errors on system
  - Measure employee productivity on certain clerical tasks

The next type of malware is a Keylogger. It is also known as keystroke logging. So, it can be both hardware and software. We saw an example of hardware in module 1, but it can also be software. What it does? It records all the keystrokes done by the user because when you type in the key, it goes to a driver, a keyboard driver and then basically go to the memory. So, this keylogger will basically target that driver and it will get all the information. So, it can be hardware or software. We are now talking about software and the software basically gets all the keystrokes of a given user and these keystrokes may include your login and password.

So, this can essentially lead to an identity theft, but note that these keyloggers, why at all you need keyloggers if they are going to be an identity theft, they are going to be against security. Why at all you need a key logger? The reason for having a keylogger is, it will help determine source of error on systems. It also measure employee productivity on certain clerical tasks. So, keystroke logger if a employee does not hit one key stroke for

say half an hour, then you will at least know that he has not been working with the system for half an hour, maybe is doing something else constructive, but at least you have a log of this. So, there are users of keyloggers and that is why keyloggers are still in place, but that the negative side of keyloggers is that it will steal, it can basically steal private information including password.

(Refer Slide Time: 07:54)

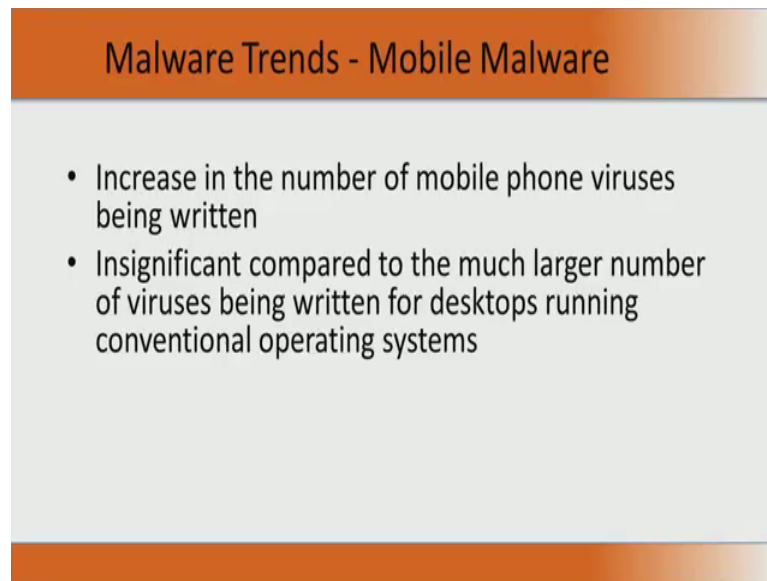


### Malware Trends - Rootkits

- Installs at deeper levels (close to kernel) of Operating System – in device drivers or kernel modules
- Purpose is to conceal running processes, files or system data, thereby helping an intruder to maintain access to a system while avoiding detection
- Are known to exist for a variety of operating systems
- Are difficult to detect

The other type of malware is called a Rootkit. A rootkit is much inside very close to the kernel, unlike the other malware that we have been talking of. It is into deeper levels of the kernel, are very close to the kernel of the operating system. What will rootkit do? The rootkit is essentially to conceal the running process, file or system data, thereby helping an intruder to maintain access to their system while avoiding detection. So, the rootkit essentially promotes stealth and these types of Rootkits are known to exist for a variety of operating systems, and they are very difficult to detect. Now, things like high assurance boot which we will be discussing in the next level 2 course in great detail, these types of high assurance boot, tamper etc can basically go and prevent a rootkit from entering a system. Nevertheless these Rootkits are very difficult to detect.

(Refer Slide Time: 09:15)



The slide features a title bar at the top with a gradient from dark orange to light orange, containing the text 'Malware Trends - Mobile Malware'. Below the title bar is a light gray rectangular area containing two bullet points. At the bottom of the slide is another gradient bar, matching the top one.

### Malware Trends - Mobile Malware

- Increase in the number of mobile phone viruses being written
- Insignificant compared to the much larger number of viruses being written for desktops running conventional operating systems

With lot more mobile phone in place, lot more mobile phone viruses are being written, but however if you look at a desktop, the percentage of the total number of vulnerabilities in a desktop running a conventional operating system to the total thing vary to a total number of desktops running. That is very high. So, if you look at mobile malware, if you compare mobile malware to PC malware, this ratio that is total number of systems running with a virus to the total number of systems in the network, so that ratio is very small when you look at mobile malware because there are so many malware phones available in the market whereas, there are much lesser PC's in the system. Nevertheless malware should take care of mobile malware because all the electronic commerce does happen through the mobile malware mobile systems.

(Refer Slide Time: 10:29)



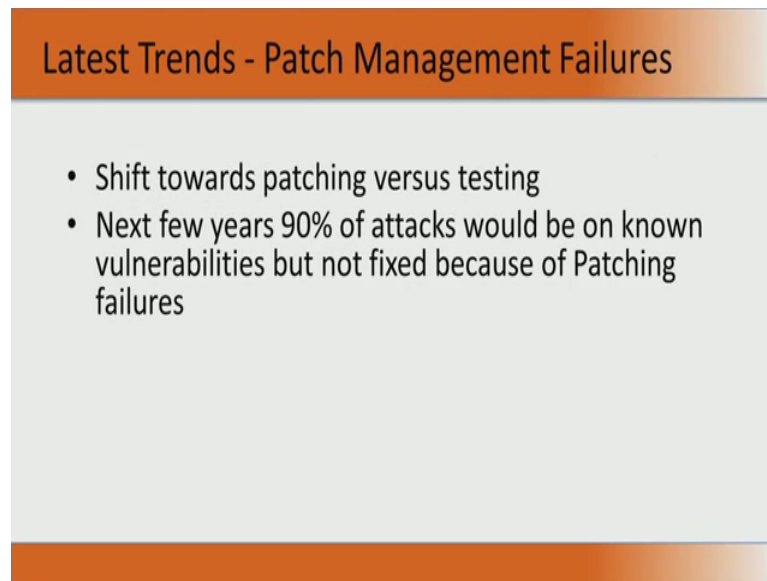
Malware Trends - Combined Attack Mechanisms

- Speed at which malware can spread combined with a lethal payload
- SPAM with spoofed Web sites
- Trojans installing bot software
- Trojans installing backdoors

L

So, today a combination of this for example, I have a malware which is spreading, it is sort of a bot we have seen earlier. It will just be spreading in the internet, but it has a very lethal payload, a very complex program and if it gets installed, all your confidentiality, integrity and availability can go for a toss. Similarly one can spam with already spoofed websites. A Trojan can be there which will keep installing what software which can actually clog your network by creating lot of packets. You could have Trojans that are installing backdoors like example I mentioned in module 1, where there was a very popular data base and it was installed across the world, but if you actually give the user name as politically and password as correct, then you get root access permission to any installation of this database. That is one very important backdoor. Trojans can start creating such type of backdoors.

(Refer Slide Time: 11:54)



The slide features a title bar at the top with a gradient from orange to white, containing the text "Latest Trends - Patch Management Failures". Below the title bar is a light gray rectangular area containing two bullet points. At the bottom of the slide is another gradient bar, matching the top one.

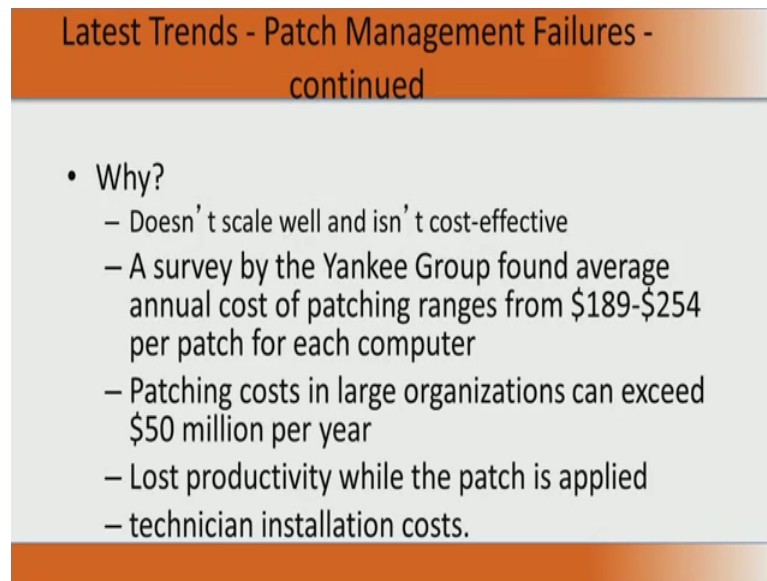
### Latest Trends - Patch Management Failures

- Shift towards patching versus testing
- Next few years 90% of attacks would be on known vulnerabilities but not fixed because of Patching failures

Now, the next very important issue is the patch management. I buy a system and there are certain vulnerabilities. Now, the company ask you to upgrade, update it. Very few actually do that update, right. So, what happens is the vulnerability still exists. So, if you look at in detail, what could happen in the next few years is that 90 percent of the attacks would be on known vulnerabilities for which fixes exist. That is the way to solve the vulnerability, way to avoid or prevent or protect asset from this vulnerability. Those processes exists, but the thing is those patches exists, but those patches are not actually applied on your system. So, over the next few years, 90 percent of attacks would be like this. It will be on known vulnerabilities which has fix, but that fix has not happen because of certain patching failures. We will look at patching failures in more detail as we go through this module.



(Refer Slide Time: 13:24)



Latest Trends - Patch Management Failures - continued

- Why?
  - Doesn't scale well and isn't cost-effective
  - A survey by the Yankee Group found average annual cost of patching ranges from \$189-\$254 per patch for each computer
  - Patching costs in large organizations can exceed \$50 million per year
  - Lost productivity while the patch is applied
  - technician installation costs.

Why does patch management does not happen? First thing is it does not scale well and the second thing is it is not cost effective. For example, there is maintenance money that we need to pay to a software company on a consistent basis for them to release the patches. So, many of the organizations do not pay this annual maintenance contract and on annual basis, they do not do that and that is the reason why many companies have systems in which these patches are not actually loaded, and because of that the security concerns continue to exist. So, a survey by the Yankee group found that on an average 189 to 254 dollars are spent per computer per patch.

So, if you want to patch all the computers in large organization, it can cross dollar 50 million per year because these are licences and floating licenses and other thing is while applying the patch, productivity goes very low. I have seen certain rural branches of a bank working. Morning when they switch on the system and they want to do antivirus update from the data centre, the entire system clogs and sometimes the entire network also fails. So, essentially what happens is till the antivirus is updated, nothing happens and everybody waits for the antivirus to get updated, so that the bandwidth become much free, a little more free for them to carry on the activity.

So, because of application of patch, the productivity is lost and another thing of course, the cost is that a technician installation cost which is quiet heavy. We do not have trained people to come and do this. So, the technicians are very costly. It is very difficult to get a very good technician who has a full understanding of information security that is unfortunately that is what we are in today. So, to get a technician of that calibre and look

at the installation is going to be a next challenge in patch management.

(Refer Slide Time: 16:05)

### A statistics in 2007

	XP	Vista	XP+Vista	MAC OSX
Total Extremely Critical	3	1	4	0
Total Highly Critical	19	12	23	234
Total Moderately Critical	2	1	3	2
Total Less Critical	3	1	4	7
Total Flaws	34	20	44	243
Average Flaws per month	2.83	1.67	3.67	20.25

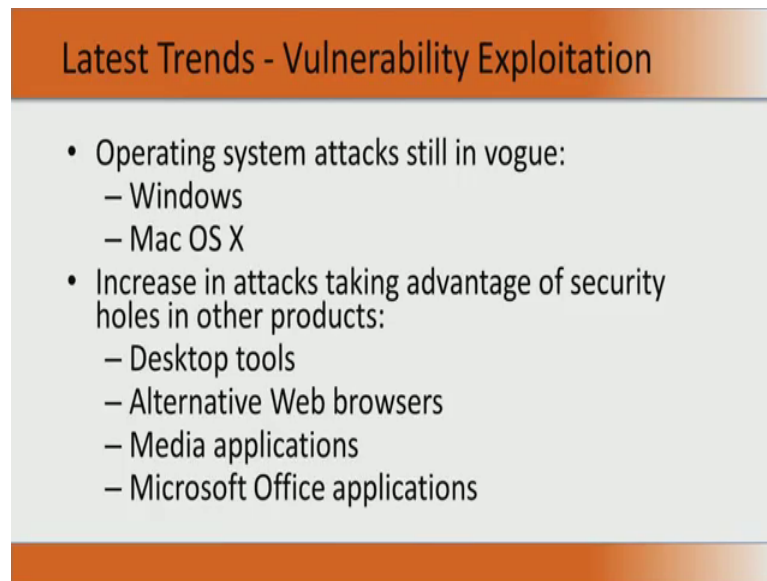
Src: <http://www.zdnet.com/article/mac-versus-windows-vulnerability-stats-for-2007/>

Now, why patches are important? Now, look at this particular survey given in the URL that I have put there. Now, this was done in 2007 and there is a statistics of the different operating systems and how much vulnerabilities of different kinds that they had. For example, if you look at XP, there are three extremely critical vulnerabilities, for the Windows XP in 2007 there were 19 highly critical to moderately critical, 3 less critical and 34 are the total flaws. So, the average flaw per month was 2.83, for Vista it was 1.67, for Xp plus vista it was 3.67. Please note that in the second column, totally high, total highly critical XP had 19 vulnerability, Vista has 12 vulnerabilities, XP plus Vista had only 23 because the vulnerability still where shared.

So, some of those 12 vulnerabilities in Vista was common to some vulnerabilities in XP. So, this also states that when people start releasing new software, it is not guaranteed that all the bugs of the previous software are fixed. Even all the known bugs of the previous software are fixed because it may take much more time and much more understanding for industry to fix those vulnerabilities.

So, here is an example which shows there is statistics done in 2007 and it basically indicates that we need to put patches in, we have to be very rigorous in applying the patches, so that the vulnerabilities get removed. If you have not done a patch from 2007 and say if you are a Mac OS X user, then you have at least 243 vulnerabilities in your PC which is sort of very tricky.

(Refer Slide Time: 18:27)



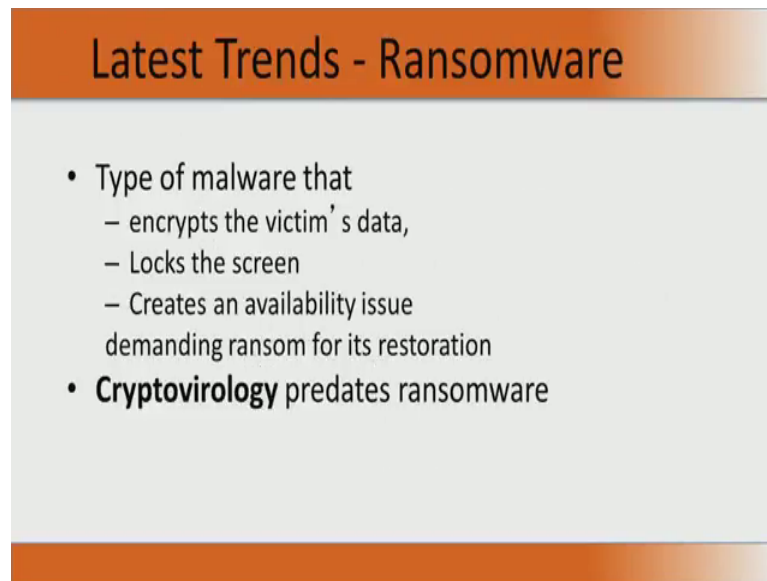
The slide features a title bar at the top with a gradient from orange to white, containing the text "Latest Trends - Vulnerability Exploitation". Below the title bar is a light gray rectangular area containing a bulleted list. The list has two main items, each with sub-items. The first item is "Operating system attacks still in vogue:" followed by "– Windows" and "– Mac OS X". The second item is "Increase in attacks taking advantage of security holes in other products:" followed by "– Desktop tools", "– Alternative Web browsers", "– Media applications", and "– Microsoft Office applications". At the bottom of the slide is a solid orange horizontal bar.

### Latest Trends - Vulnerability Exploitation

- Operating system attacks still in vogue:
  - Windows
  - Mac OS X
- Increase in attacks taking advantage of security holes in other products:
  - Desktop tools
  - Alternative Web browsers
  - Media applications
  - Microsoft Office applications

So, because of this vulnerability exploitation, operating systems are under consistent attack. Operating systems, conventional operating systems like even windows and Mac OS X are under consistent threat or constant rate of being attacked. How does the attack come in? The attack comes in through different desktop tools which are not connected with the operating system, people download. The attacks also come through alternative web browsers, attacks also comes through media applications and Microsoft office applications for example. So, since many of these are not updated against vulnerabilities from the date of the installation, so the hacker could actually exploit the vulnerabilities, known vulnerabilities today, their fixes are known, but they are not applied, but the hacker can basically use these to get access into the system and essentially create a vulnerability exploitation.

(Refer Slide Time: 19:45)

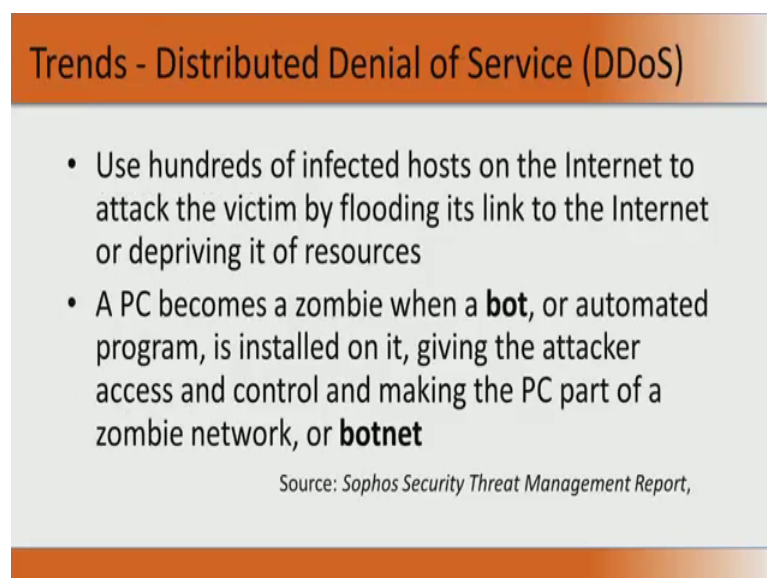


## Latest Trends - Ransomware

- Type of malware that
  - encrypts the victim's data,
  - Locks the screen
  - Creates an availability issue demanding ransom for its restoration
- **Cryptovirology** predates ransomware

There is also a very interesting trend called Ransomware. What happens is the malware in your system will go and encrypt the victim's data. It will go and encrypt your data, you are the victim and then, it will also go and/or lock the screen. This will create an availability issue. You cannot login, you cannot find anything and then, it actually starts demanding ransom for its installation. So, this is actually sometimes this is actually called as cryptovirology and in modern term, it is called a Ransomware.

(Refer Slide Time: 20:27)



## Trends - Distributed Denial of Service (DDoS)

- Use hundreds of infected hosts on the Internet to attack the victim by flooding its link to the Internet or depriving it of resources
- A PC becomes a zombie when a **bot**, or automated program, is installed on it, giving the attacker access and control and making the PC part of a zombie network, or **botnet**

Source: Sophos Security Threat Management Report,

So, in the next session we will start talking about distributed denial of service.