Introduction to Information Security

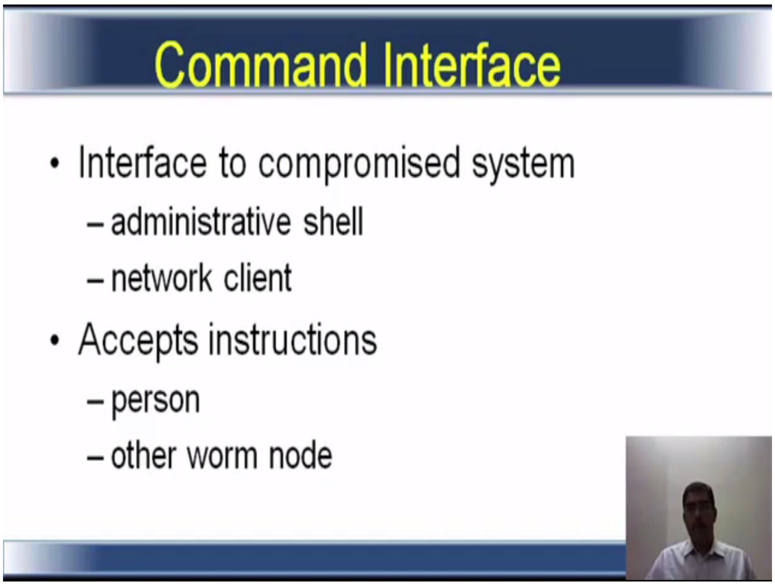
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture – 36
Command Interface

(Refer Time Slide: 00:10)

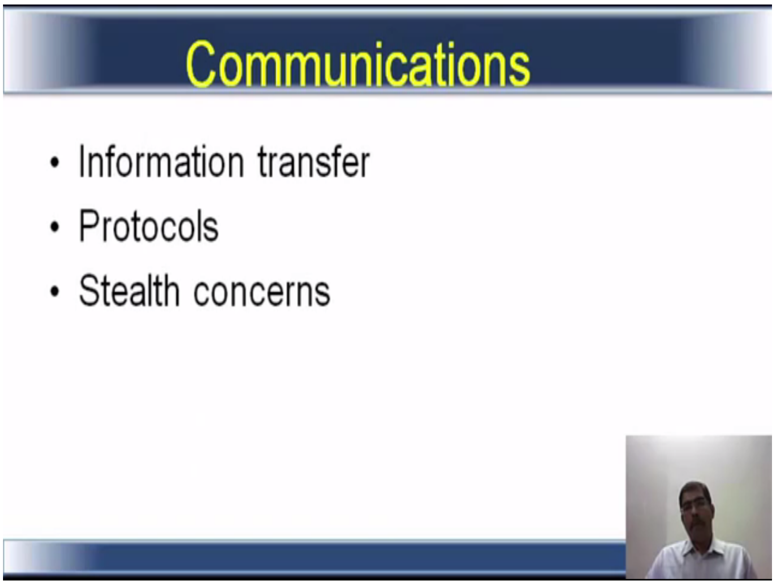


Command Interface

- Interface to compromised system
  - administrative shell
  - network client
- Accepts instructions
  - person
  - other worm node

Now what are command interface of a worm. It is going to be administrative, or it can have, or it can be a network client. It accepts instructions, either from a person or from another worm node.

(Refer Time Slide: 00:25)

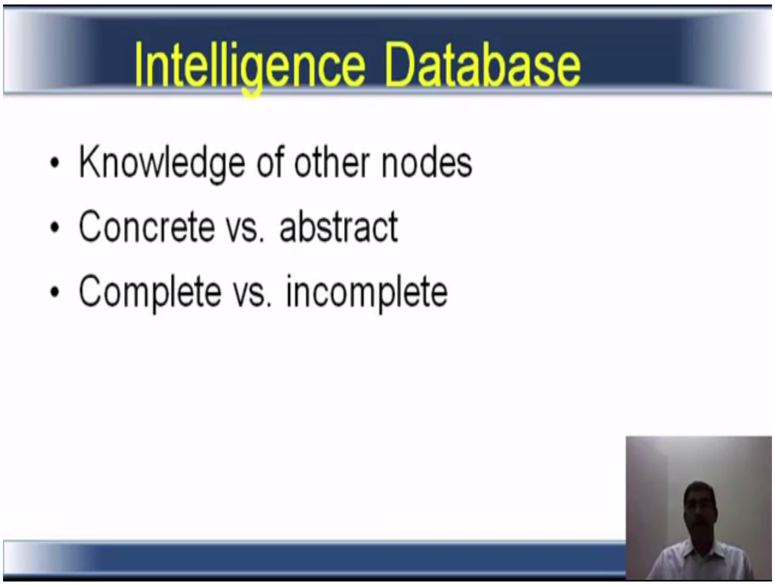


Communications

- Information transfer
- Protocols
- Stealth concerns

How do we communicate? Information transfer, protocols, stealth concerns are there for worms.

(Refer Time Slide: 00:35)

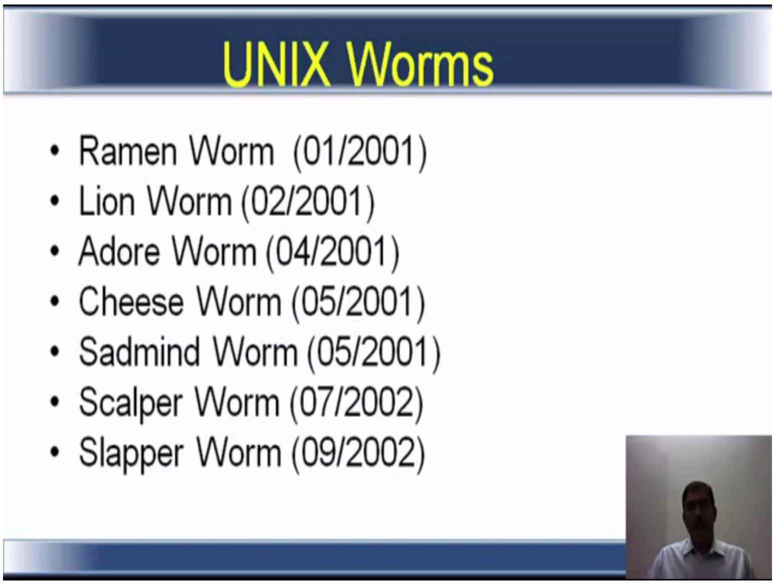


Intelligence Database

- Knowledge of other nodes
- Concrete vs. abstract
- Complete vs. incomplete

The intelligence database, knowledge of other nodes, concrete versus abstract, complete versus incomplete. So, it has an intelligent database which can differentiate between this and propagate.

(Refer Time Slide: 00:52)

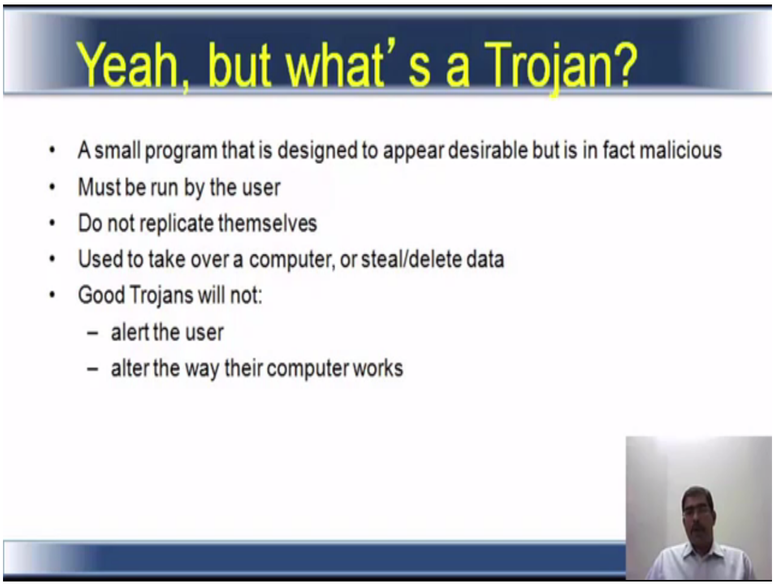


UNIX Worms

- Ramen Worm (01/2001)
- Lion Worm (02/2001)
- Adore Worm (04/2001)
- Cheese Worm (05/2001)
- Sadmind Worm (05/2001)
- Scalper Worm (07/2002)
- Slapper Worm (09/2002)

Some of the famous Unix worms are going detailed here. The quite old but, slapper worm was very famous, ramen was famous, cheese worm was famous, and lion worm was famous. If you need to know what exactly these worms did, just google it, you will get detailed case study on how each of the worm infected the systems, how they brought down the system, and how they were detected.

(Refer Time Slide: 01:30)



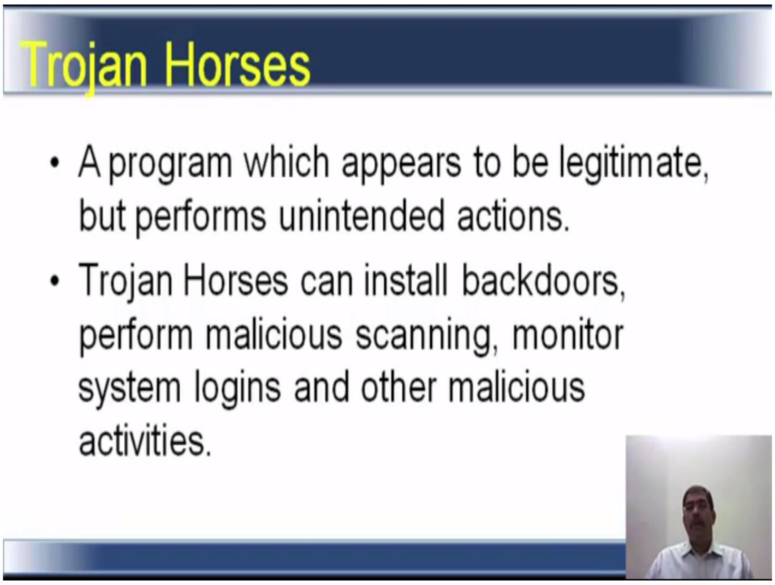
Yeah, but what’s a Trojan?

- A small program that is designed to appear desirable but is in fact malicious
- Must be run by the user
- Do not replicate themselves
- Used to take over a computer, or steal/delete data
- Good Trojans will not:
  - alert the user
  - alter the way their computer works

Enough with worms, now let us talk about what is a Trojan. It is small program that is designed to appear desirable, but is in fact malicious. It must be run by the user. It does not duplicate itself, it is used to take over computer, or steal, or delete data. Good trojans will not alert the user, alter the way their computer works. If you seen or heard of something in, the actual meaning of trojan came from an old saying, be aware of the Greeks bearing straight gifts.

Now, there was a women trojan horse with hundreds of solders inside, and they use the trojan, or they use the trojan to gift it to the enemy. And then once they were inside the boundary walls of the enemy camp, hundreds of soldiers came out of the trojan box and attack them. Similarly, a trojan if you want to define it, it is unauthorized program within an authorized program, which executes whenever the authorized program executes.

(Refer Time Slide: 02:51)

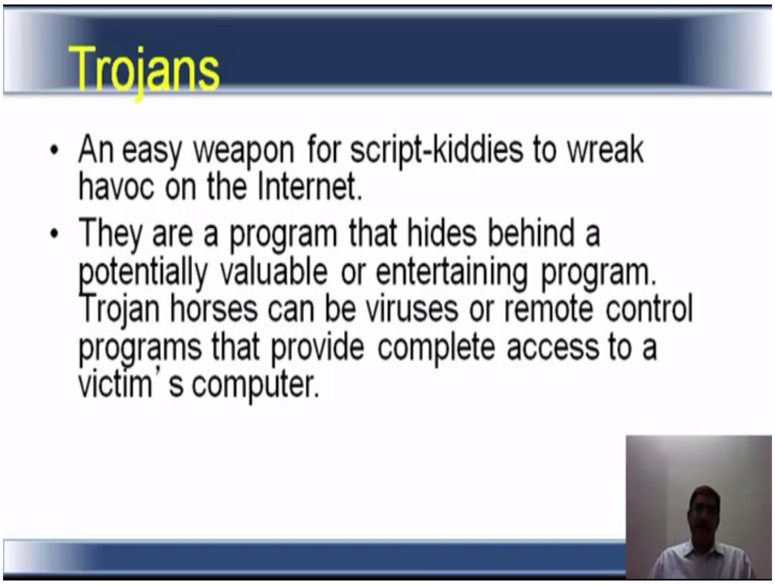


Trojan Horses

- A program which appears to be legitimate, but performs unintended actions.
- Trojan Horses can install backdoors, perform malicious scanning, monitor system logins and other malicious activities.

In a little more simpler term, it is a program which appears to be legitimate, but performs unintended actions. Trojan horses can install backdoors, it can perform malicious scanning, it can monitor system logins, and also do other malicious activities.

(Refer Time Slide: 03:13)

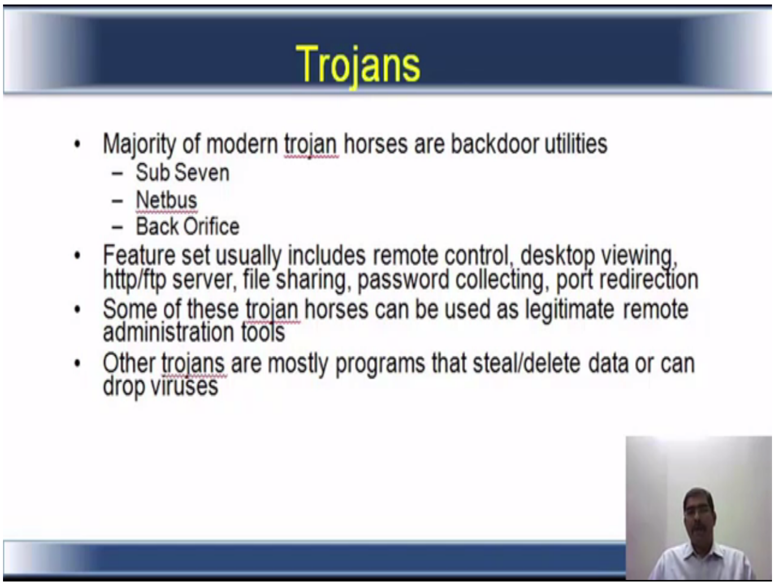


Trojans

- An easy weapon for script-kiddies to wreak havoc on the Internet.
- They are a program that hides behind a potentially valuable or entertaining program. Trojan horses can be viruses or remote control programs that provide complete access to a victim' s computer.

Now, because easy weapon for script kiddies to wreak havoc on the internet. Script kiddies was actually a term found by a sophisticated hackers, or the more immature hackers, but equally as dangerous. And, trojans are a program that hides behind a potentially valuable or entertaining program. Trojan horses can be viruses, or remote control programs that provide complete access, to a victim's computer. So, like I said before, it is a unauthorized program, or a malicious program that reside within the authorize program or the legitimate program, and runs whenever the legitimate program runs.

(Refer Time Slide: 04:08)



Trojans

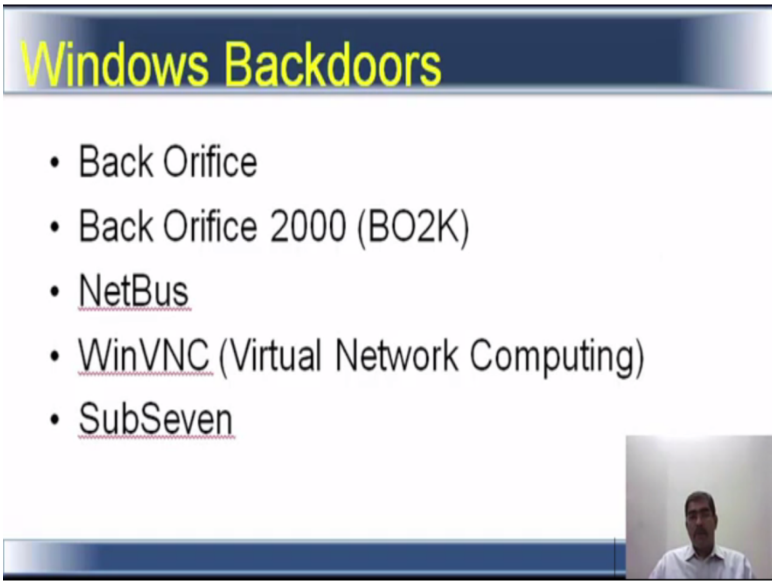
- Majority of modern trojan horses are backdoor utilities
  - Sub Seven
  - Netbus
  - Back Orifice
- Feature set usually includes remote control, desktop viewing, http/ftp server, file sharing, password collecting, port redirection
- Some of these trojan horses can be used as legitimate remote administration tools
- Other trojans are mostly programs that steal/delete data or can drop viruses

But, majority of the trojan horses, the modern ones are backdoor utilities, sub seven is one, Netbus is the another, back orifice is the third, so there are several trojan horses available.

Now, what do this feature, what are the features of this trojans which are back door utilities, they basically include remote controlling, desktop viewing, http or ftp server, file sharing, password collecting, port redirection, basically the functions that a back door utility program can do are these.

Some of the trojans, can be used as legitimate remote administration tools. Other trojans are mostly programs that steal data, or delete data, or even can drop a virus. The best trojan is the one, that you do not know is the trojan. In Unix , if we take for example, there is something called port redirection, hackers use your connection to attack, and then you get blamed. That is an example of a good trojan, or trojan with good trojan properties.

(Refer Slide Time: 05:33)

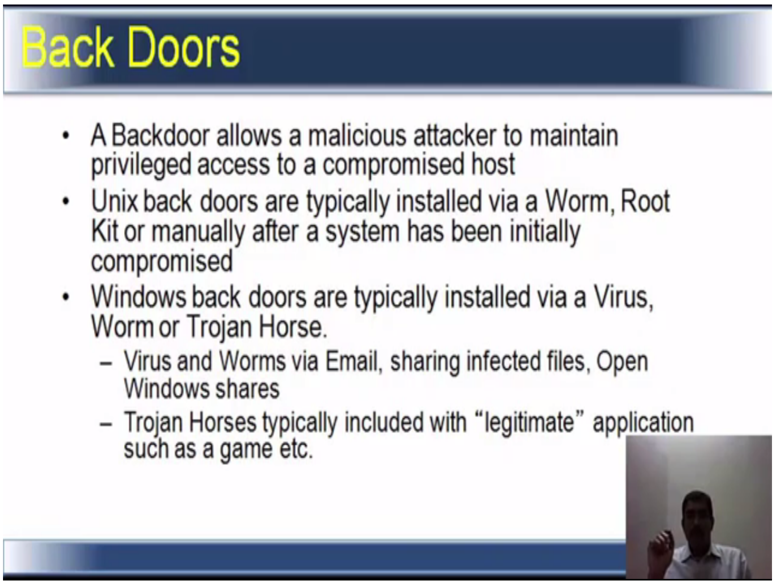


Windows Backdoors

- Back Orifice
- Back Orifice 2000 (BO2K)
- NetBus
- WinVNC (Virtual Network Computing)
- SubSeven

Then there are windows backdoors, back orifice, back orifice 2000 or some other, Netbus, windows VNC virtual network computing, subseven. These are all some example of the windows back doors.

(Refer Time Slide: 05:45)



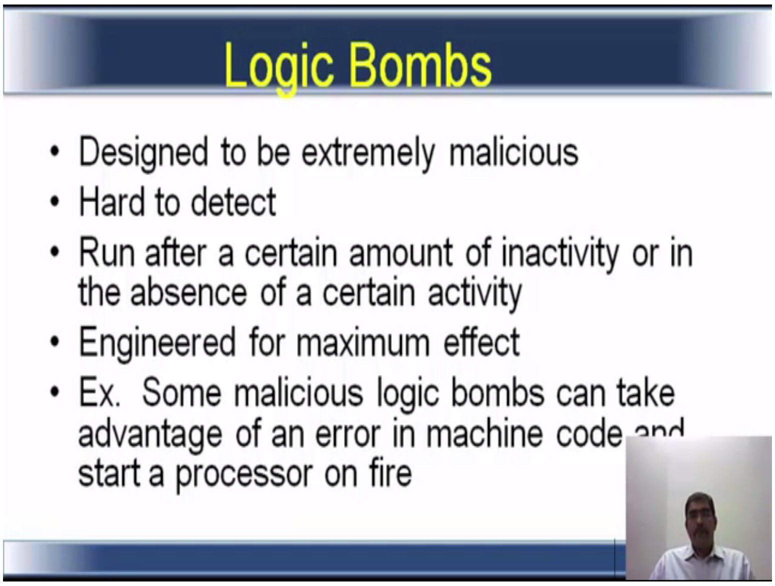
Back Doors

- A Backdoor allows a malicious attacker to maintain privileged access to a compromised host
- Unix back doors are typically installed via a Worm, Root Kit or manually after a system has been initially compromised
- Windows back doors are typically installed via a Virus, Worm or Trojan Horse.
  - Virus and Worms via Email, sharing infected files, Open Windows shares
  - Trojan Horses typically included with "legitimate" application such as a game etc.

What does the back door do, a back door allows the malicious attacker, to maintain privileged access to a compromised host, or compromised system. Unix back doors are typically installed via a worm root kit, or manually after a system has been initially compromised. Windows back doors are typically installed via a virus, worm, or a trojan horse.

Virus and worms via email example of that. Sharing infected files, opening windows shares, trojan horses typically included with legitimate application, such as a game that you download from the net, cab have a trojan within that.

(Refer Time Slide: 06:33)



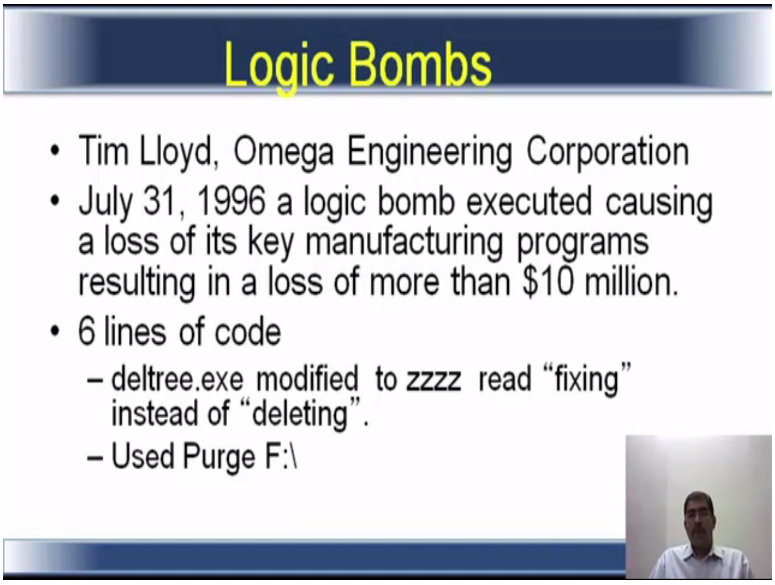
Logic Bombs

- Designed to be extremely malicious
- Hard to detect
- Run after a certain amount of inactivity or in the absence of a certain activity
- Engineered for maximum effect
- Ex. Some malicious logic bombs can take advantage of an error in machine code and start a processor on fire

Then, we see what logic bombs are, we already explained what logic bomb is, it is designed to be extremely malicious, it is very hard to detect, it runs after a certain amount of inactivity, or in the absence of a certain activity. That in the example that I explained earlier, if my name does not appeared in the payroll in the seven of the next month, then star dot star. So, that is an example of that.

It is engineered for maximum effect where all the data is wiped out. Now, as an examples some malicious logic bombs can take advantage of an error in machine code, and start a processor on file. Basically, it updates processor with so many requests, and so many cycles that the processor seizes to function.

(Refer Time Slide: 07:23)

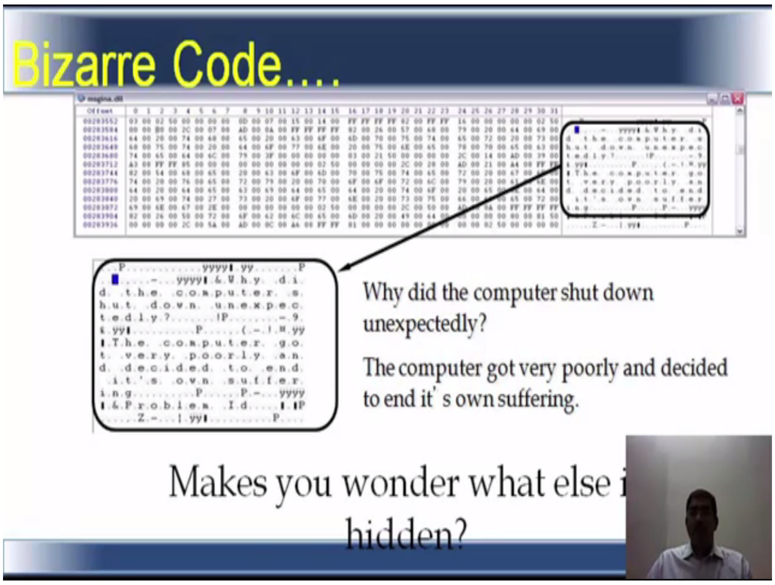


Logic Bombs

- Tim Lloyd, Omega Engineering Corporation
- July 31, 1996 a logic bomb executed causing a loss of its key manufacturing programs resulting in a loss of more than $10 million.
- 6 lines of code
  - deltree.exe modified to zzzz read “fixing” instead of “deleting”.
  - Used Purge F:\

Tim Lloyd of omega engineering corporation, on July 31, 1996, a logic bomb executed causing a loss of its key manufacturing programs, resulting in a loss of more than 10 million euro dolor. There are six lines of code, deltree.exe modified to 4z read fixing instead of deleting, and used purge f colon, so everything was deleted.

(Refer Time Slide: 07:59)



Bizarre Code....

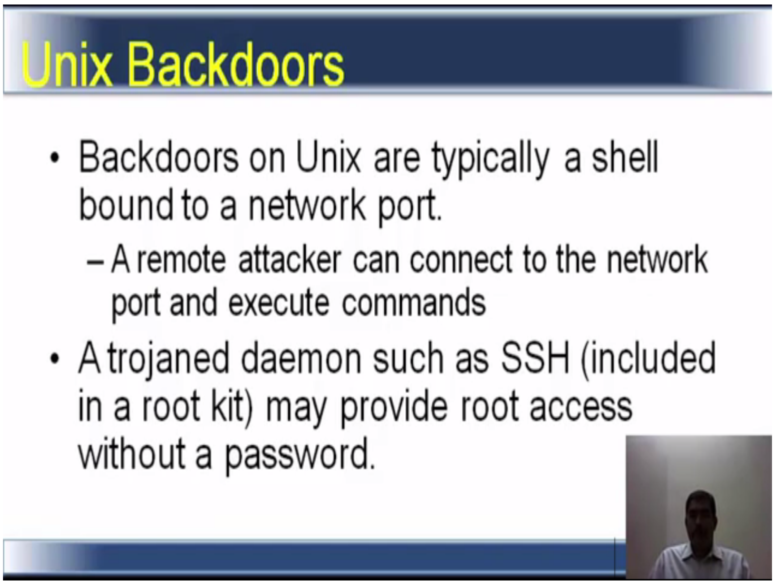
Why did the computer shut down unexpectedly?

The computer got very poorly and decided to end it' s own suffering.

Makes you wonder what else i hidden?

If we do an analysis of the coding, we find the wizard coding. Why did the computer shut down unexpectedly, the computer got very poor and decided to end it is own suffering. So, the computer decided to suicide. Makes you wonder what else is in it. So, casual analysis of the core is required, to find out if there is a logic bomb in it or hidden or written.

(Refer Time Slide: 08:27)

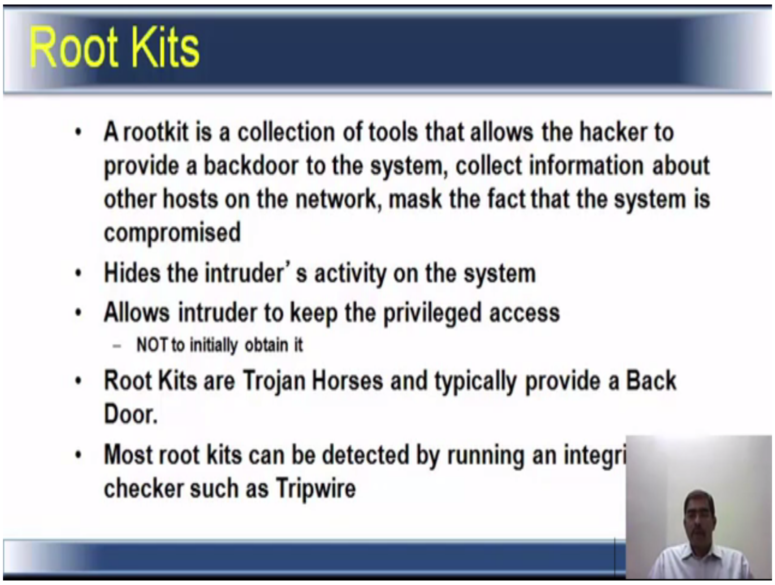


Unix Backdoors

- Backdoors on Unix are typically a shell bound to a network port.
  - A remote attacker can connect to the network port and execute commands
- A trojaned daemon such as SSH (included in a root kit) may provide root access without a password.

Even in Unix, backdoors are typically a shell bound to a network port. A remote attacker can connect, to the network port and execute commands. A trojaned daemon such as an ssh, that is your secured shell used to connect to the server from a remote place, may provide root access without a password. So, the backdoors in Unix, a cause trojaned daemon such as ssh, it provide the root access without a password.

(Refer Time Slide: 09:00)

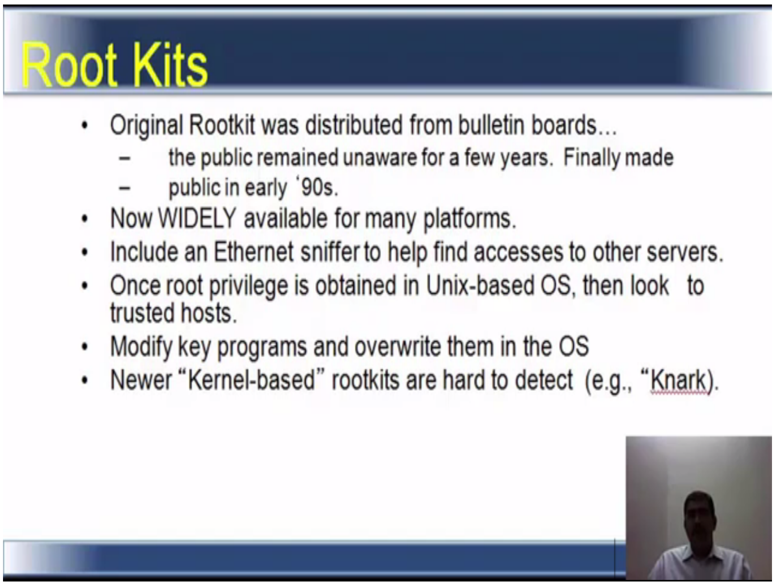


Root Kits

- A rootkit is a collection of tools that allows the hacker to provide a backdoor to the system, collect information about other hosts on the network, mask the fact that the system is compromised
- Hides the intruder' s activity on the system
- Allows intruder to keep the privileged access
  - NOT to initially obtain it
- Root Kits are Trojan Horses and typically provide a Back Door.
- Most root kits can be detected by running an integri checker such as Tripwire

A rootkit is a collection of tools, which allows the hacker to provide a backdoor to the system, collect information about other hosts on the network, or hide the fact that system is compromised. It hides the intruder's activity on the system. It allows the intruder, to keep the privileged access, not to initially obtain it, but to keep it. Root kits are trojan horses, and typically provide a back door. Most root kits can be detected, by running an integrity checker example of an integrity checker, is tripwire.

(Refer Time Slide: 09:38)

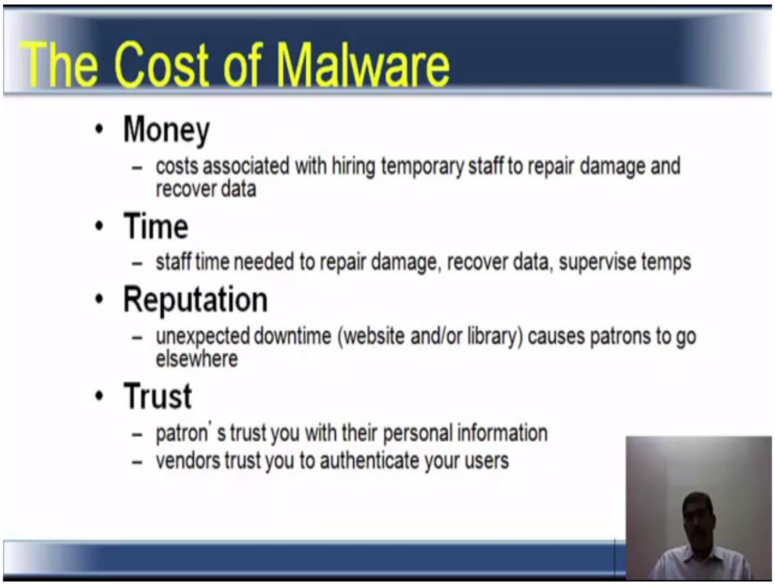


Root Kits

- Original Rootkit was distributed from bulletin boards…
  - the public remained unaware for a few years. Finally made
  - public in early '90s.
- Now WIDELY available for many platforms.
- Include an Ethernet sniffer to help find accesses to other servers.
- Once root privilege is obtained in Unix-based OS, then look to trusted hosts.
- Modify key programs and overwrite them in the OS
- Newer "Kernel-based" rootkits are hard to detect (e.g., "Knark).

Original rootkit, was distributed from bulletin boards the public remained unaware for a many years. Finally, it was made public in early nineties. Now, it is widely available for many platforms. It includes an ethernet sniffer, to help find accesses to other servers. Once the super user, or root privilege is obtained in Unix based os, then it looks to trusted hosts, it can modify key programs and overwrite them in the operating systems. The newer kernel based root kits are very hard, to detect example knark.

(Refer Time Slide: 10:18)



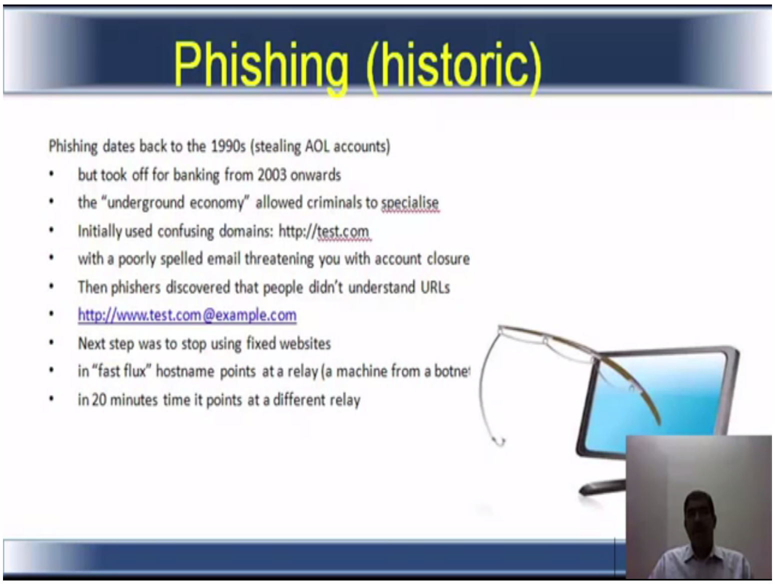
The Cost of Malware

- Money
  - costs associated with hiring temporary staff to repair damage and recover data
- Time
  - staff time needed to repair damage, recover data, supervise temps
- Reputation
  - unexpected downtime (website and/or library) causes patrons to go elsewhere
- Trust
  - patron' s trust you with their personal information
  - vendors trust you to authenticate your users

The cost of malware, it is not only that money that spent on hiring staff, to repair damage and recover data but, there is also time invested, again staff require time to repair the damage, to recover the data, to supervise the temps if they are outsourced. Then there is a question of reputational risk, unexpected downtime. Even if it is a website, and or a library where the files are stored, it causes customers to go elsewhere, because inside it is not up.

Then there is a question of trust, the customer trust you with their personal information, vendors trust you to authenticate your resource . If that does not happen, all of your server is down, then its huge cost to bear.

(Refer Time Slide: 11:14)



Phishing (historic)

Phishing dates back to the 1990s (stealing AOL accounts)

- but took off for banking from 2003 onwards
- the "underground economy" allowed criminals to specialise
- Initially used confusing domains: http://test.com
- with a poorly spelled email threatening you with account closure
- Then phishers discovered that people didn't understand URLs
- http://www.test.com@example.com
- Next step was to stop using fixed websites
- in "fast flux" hostname points at a relay (a machine from a botne
- in 20 minutes time it points at a different relay

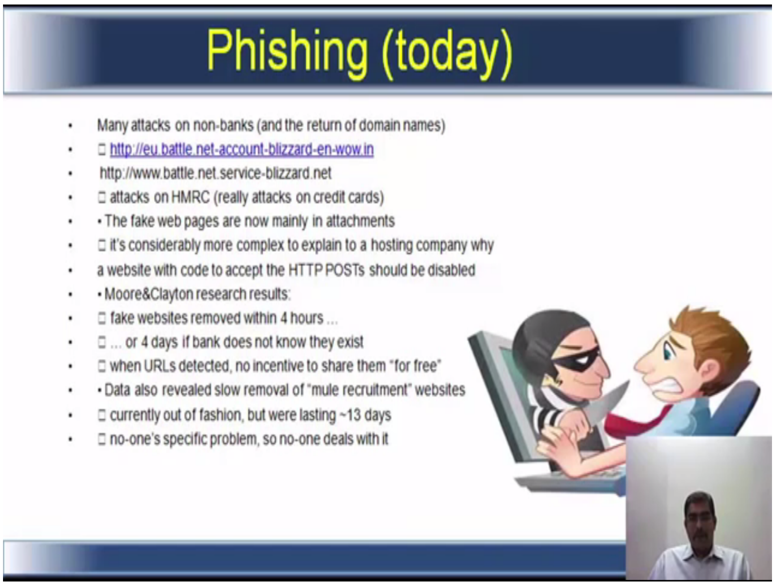
Let us take a look at phishing. Let us go back to, how phishing started, it dates back to nineties because use for stealing America Online accounts. But, it took off for banking from 2003 onwards with an advent of internet technologies coming in, with banks going online for transactions, the customer going online to do transactions on the banking sector. The underground economy allowed criminals to specialize in vision, from initially used confusing domains, example http test.com.

Sounds little legitimate but actually not. Phishing also is propagated with poorly spelled email, threatening you account closure. Now, in this record, there was an incident in financial institute, where the customer was called by some malicious person, and told to give his give his password for internet banking account, claiming that he was some regulatory authority.

Customer did not give the credentials, but then the next morning, he received an email that your account was suspended, or account was closed, because of his not providing the password. Then he actually went to the bank, and asked manager what happened to this, they found that an amount was withdrawn from his account. So, a lot of phishing activity was run. Even though we did not verbally give his username or password,

the hackers managed to exploit his system using browser page malware and started transacting with his, or impersonating him. Then if you go on, the phishers discovered that the people did not understand urls, for example, http www .test.com and example.com. So, then next step was to stop using fixed websites, in fast flux hostname, points at a relay a machine from a botnet in 20 minutes time it points at a different relay. So, it is not a static site, its dynamically changing site every 20 minutes. So, it becomes difficult to identify.

(Refer Time Slide: 13:50)



Phishing (today)

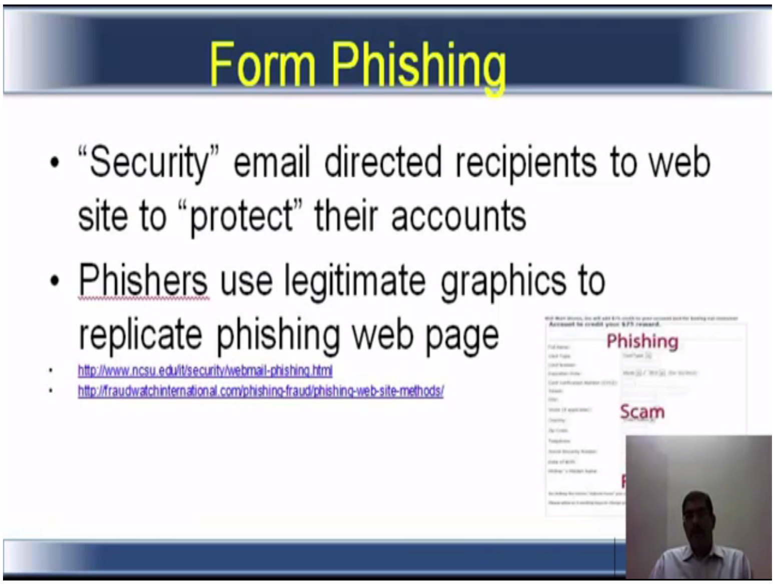
- Many attacks on non-banks (and the return of domain names)
- □ http://eu.battle.net-account-blizzard-en-wow.in
- http://www.battle.net.service-blizzard.net
- □ attacks on HMRC (really attacks on credit cards)
- • The fake web pages are now mainly in attachments
- □ it's considerably more complex to explain to a hosting company why
- a website with code to accept the HTTP POSTs should be disabled
- • Moore&Clayton research results:
- □ fake websites removed within 4 hours ...
- □ ... or 4 days if bank does not know they exist
- □ when URLs detected, no incentive to share them "for free"
- • Data also revealed slow removal of "mule recruitment" websites
- □ currently out of fashion, but were lasting ~13 days
- □ no-one's specific problem, so no-one deals with it

Today phishing is a much more sophisticate, many attacks on non banks also, and the return of domain names, an example is given there, eu.battle.net-account-bizzard-en-wow.in. The HMRC really attacks from credit cards, the fake pages are now mainly in attachments not as a mail body itself. It is considerably more complex to explain a hosting company, why a website with the code to accept the http posts should be disabled.

Generally since, it is a hosting company it is very difficult to explain to them, because they are serving millions of customers thousands of customers. It is very complex to explain to the host company, why a website with code to accept the http posts should be disabled, and there is a research by Moore and Clayton that is fake websites removed within 4 hours, or 4 days if bank does not know they exist.

When urls were detected, no incentive to share them for free, data also revealed slow removal of recruitment websites. Currently out of fashion, but were lasting for at least 13 days. No one's specific problem, so no one deals with it.

(Refer Time Slide: 15:28)



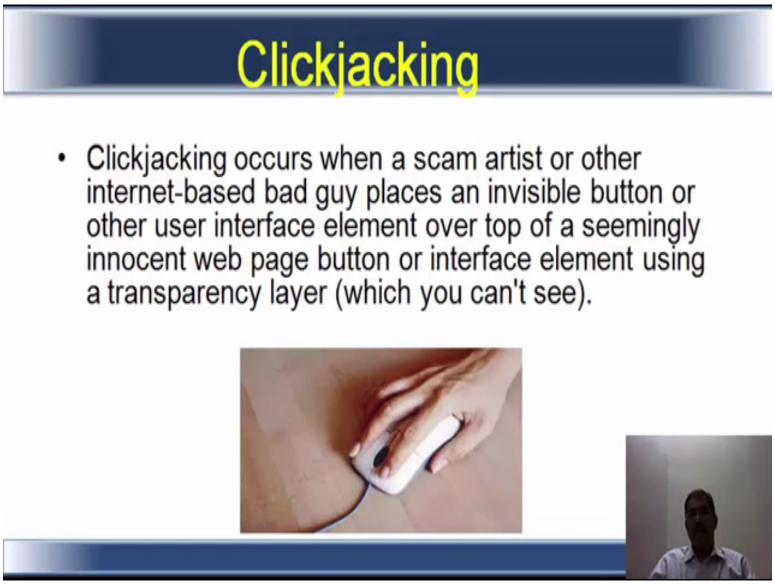
Form Phishing

- “Security” email directed recipients to web site to “protect” their accounts
- Phishers use legitimate graphics to replicate phishing web page
- http://www.ncsu.edu/it/security/webmail-phishing.html
- http://fraudwatchinternational.com/phishing-fraud/phishing-web-site-methods/

A variation of using, it is common reason. It is the security email directed recipients to website to protect their accounts. Suddenly you will receive a message, from a bank stating that, go to the website change your credentials immediately. That is a form of form phishing. And phishers use legitimate graphics, to replicate phishing web page. So, when you look at the mail body, it looks exactly same as though it is originated from the bank.

If it is xyz bank, then logo of the xyz bank, the color combination, the font everything will be the same. But, actually it is a kind of form phishing. The banks generally do not ask information about your personal information, about the net and or through phone. So, the form phishing takes advantage of fact you cannot fool all users, but you can fool some users.

(Refer Time Slide: 16:32)

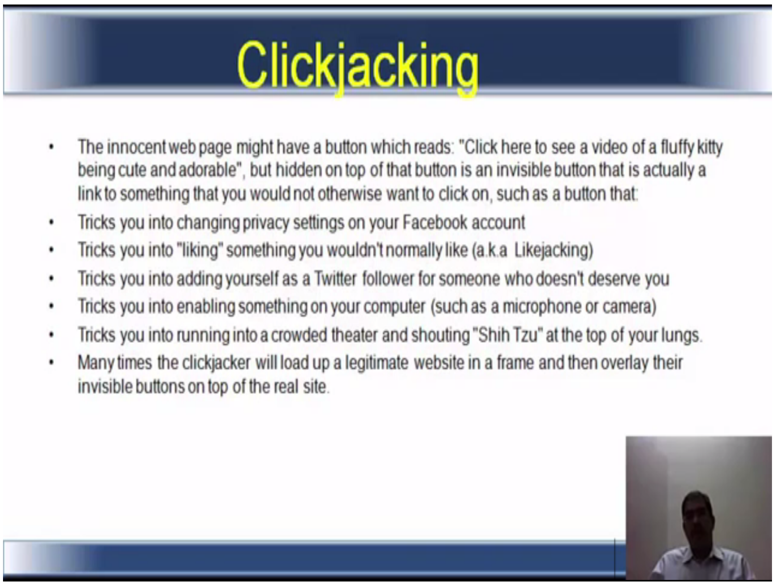


Clickjacking

- Clickjacking occurs when a scam artist or other internet-based bad guy places an invisible button or other user interface element over top of a seemingly innocent web page button or interface element using a transparency layer (which you can't see).

Then there is clickjacking. It happens from scam artist, or other internet based bad guy places an invisible button, or other user interface element over top of a seemingly innocent web page button using transparency layer.

(Refer Time Slide: 16:52)



Clickjacking

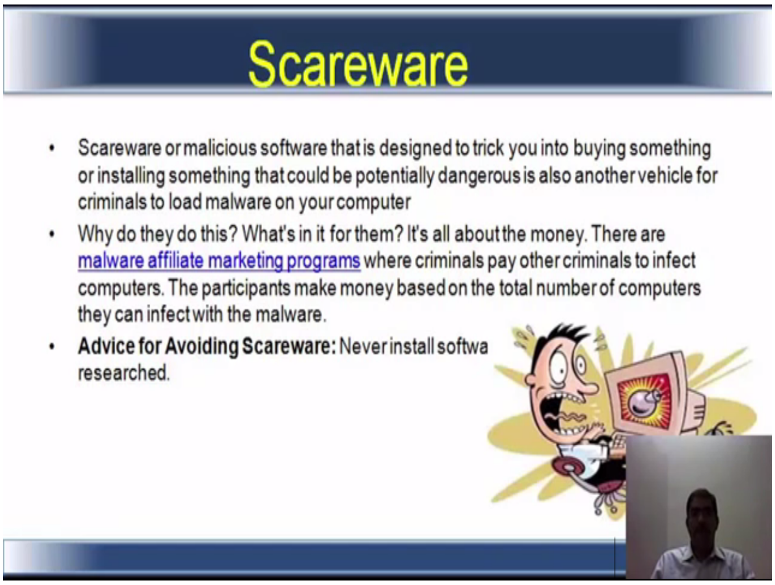
- The innocent web page might have a button which reads: "Click here to see a video of a fluffy kitty being cute and adorable", but hidden on top of that button is an invisible button that is actually a link to something that you would not otherwise want to click on, such as a button that:
- Tricks you into changing privacy settings on your Facebook account
- Tricks you into "liking" something you wouldn't normally like (a.k.a Likejacking)
- Tricks you into adding yourself as a Twitter follower for someone who doesn't deserve you
- Tricks you into enabling something on your computer (such as a microphone or camera)
- Tricks you into running into a crowded theater and shouting "Shih Tzu" at the top of your lungs.
- Many times the clickjacker will load up a legitimate website in a frame and then overlay their invisible buttons on top of the real site.

As a user, cannot be able to see that. The innocent web page might have a button which reads something like, click here to see a video of fluffy kitty being cute, and adorable. But, hidden on top of that button is an invisible button, which is actually a link to something, which you would not otherwise want to click on. Such as button, that tricks you into changing privacy settings on your facebook account, and tricks you into liking something you normally would not like which also known as likejacking.

It tricks you adding yourself as a twitter follower for someone, who does not deserve you. It tricks you into enabling something on your computer, such as microphone or camera. It tricks you into running into a crowd theater, and shouting shih tzu at the top of your lungs. Many times, the clickjacker will load up a legitimate website in a frame, and then overlay their invisible buttons, on top of the real site.

Basically the cure for clickjacking is, you have to update the browser to the latest version, use all your plugins such as adobe plugin, flash plugin could be updated. There are also softwares which is free, which can help you detect that in.

(Refer Time Slide: 18:15)



Scareware

- Scareware or malicious software that is designed to trick you into buying something or installing something that could be potentially dangerous is also another vehicle for criminals to load malware on your computer
- Why do they do this? What's in it for them? It's all about the money. There are malware affiliate marketing programs where criminals pay other criminals to infect computers. The participants make money based on the total number of computers they can infect with the malware.
- **Advice for Avoiding Scareware:** Never install softwa researched.

Again let something called scareware, we have looked at phishing, we have looked at clickjacking, we have looked at malware, and we have looked at virus. Now, there is something called as scareware. Scareware is designed to trick you into buying something, or installing something, that could be potentially dangerous. This is also another medium for criminals to load malware on your computer.

Why do they do this, what is in it for them, it is all about money, there are malware affiliate marketing programs, where criminals pay other criminals to infect computers. The participants make money based on, the total number of computers they can infect with the malware. In simple terms, how do you avoid scareware, never install software that have been researched.

(Refer Time Slide: 19:09)

Tapping Your Cell Phone

- http://www.wthr.com/Global/story.asp?s=9346833

http://www.buzzle.com/articles/cell-phone-tappin

There also method, tap your cell phone, a link is given on, how it has been done. You can go to your link, and learn about how the cell phone was tapped. Now, we can come to the conclusion of this particular aspect, where as we have seen what a virus is, what a worm is, what a parasitic virus is, what a bacteria is, what a trojan horse is, what are the internet or what are the anti virus scanning technologies, innoculators, integrity checkers. Then we have seen different forms of attacks such as clickjacking, scareware, phishing, form phishing, now we will end this particular session.