CSCD 303
Essential Computer Security
Fall 2017

Lecture 8 - Malware

Reading: Chapter 6

Overview

- Learning Objectives
  - Define malware, viruses, worms and trojans
  - Learn how you become infected at the OS level
  - Learn where these programs hide and how they hide

Take a Short Quiz

- You will take a short quiz on malware and then throughout the lecture fill in the answers.
- Turn in the answers with your name at the end of the lecture ...

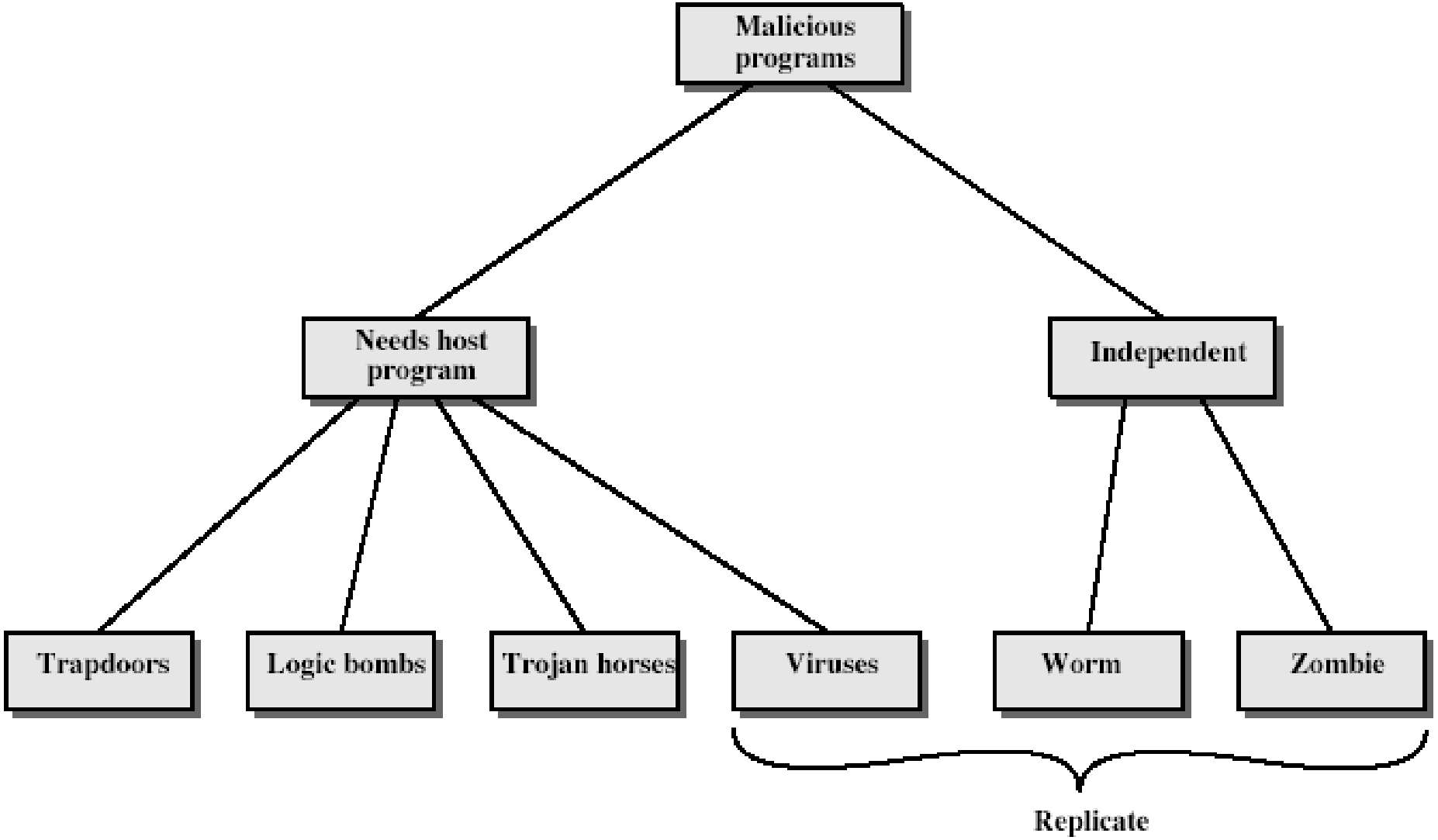
Malware

- What is Malware? How would you define it?
  - "Malware" is short for "malicious software" - computer programs designed to infiltrate and damage computers without users consent
  - "Malware" is a general term covering different types of threats to your computer safety
  - Viruses, spyware, worms, trojans, rootkits and so on

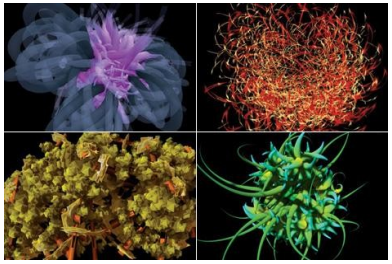
Malware Categories

- What are some common categories of malware?
  - Viruses
  - Worms
  - Trojan Horses and Rootkits
  - Spyware/Adware (covered later)
  - Keyloggers

Malicious Software

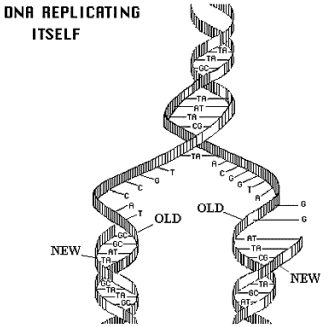


Computer Virus



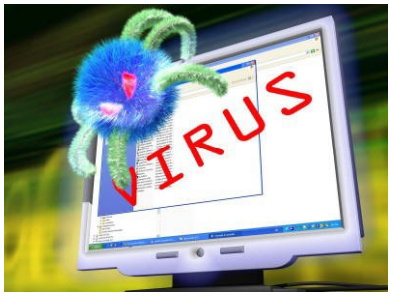
- Computer viruses are called viruses because they have similar traits to biological viruses
  - A computer virus passes from computer to computer like a biological virus passes from person to person – germs, sneezing
  - Can also be passed from file to file on same computer

Computer Virus



- A biological virus is not living
  - It's a fragment of DNA inside a protective jacket
  - Unlike a cell, a virus has no way to do anything or to reproduce by itself -- it is not alive!
- Computer viruses also can not reproduce by themselves

Virus



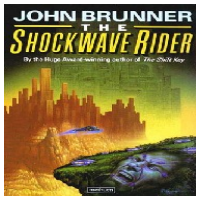
- Definition
  - Key attributes, **self replicates** and i**njects itself into existing code or file**

    http://www.thefreedictionary.com/computer+virus

  - Computer program designed to replicate itself by copying itself to other programs stored in a computer

    ... benign or negative, could cause a program to operate incorrectly or corrupt a computer's memory

Worm



- Definition
  - Self replicates, doesn't rely on infecting existing programs
  - Spreads via a network
  - Some definitions don't distinguish between viruses and worms
- Science Fiction
  - John Brunner – 1975 – Shockwave Rider
    http://en.wikipedia.org/wiki/The_Shockwave_Rider
    - Hero uses computer hacking skills to escape pursuit in a dystopian future, and defined "worm" to describe a program that propagates itself through a computer network
- Experimental
  - Xerox PARC – first, experimented with worms – 1980 – used worms to do administration tasks

Trojan Horse

- Definition
  - A destructive program that masquerades as a benign application
    - Users think they are getting a useful piece of software
    - Unlike viruses, Trojan horses do not replicate themselves ...

Example: Trojan horse

- Supposed to rid computer of viruses
- Instead introduces viruses onto your computer like **Antivirus 2009** ... Look at this one later

Spyware/Adware

- Definition
- Malware installed on computers
  - Collects information about users without their knowledge
  - Spyware hidden from users, secretly installed on user's personal computer
    - Comment
      - Yet, keyloggers as a form of spyware can legally be installed by owner of shared, corporate, or public computer on purpose in order to secretly monitor their users

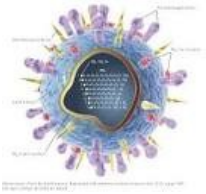
Keylogger

- Definition
  - Keylogger, sometimes called keystroke logger, key logger is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard
  - A keylogger program does not require physical access to user's computer
    - It can be downloaded on purpose by someone who wants to monitor activity on particular computer or it can be downloaded unwittingly as spyware

http://www.securelist.com/en/analysis/204791931/Keyloggers_How_they_work_and_how_to_detect_them_Part_1#what

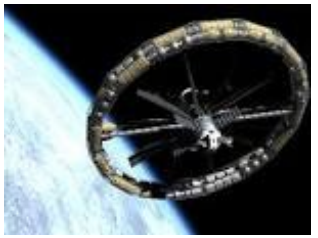
Types of Viruses and Infection Process

Virii – How Do they Spread?



- How do you get infected with a virus?
- Can propagate within a single computer or travel between computers
  - DVD's, USB Drives
  - Today's viruses also take advantage of network services
    - World Wide Web,
    - E-mail,
    - Instant Messaging, IRC, and file sharing systems
  - Next slide has example ...

Virus Spread to Space Station



- NASA confirmed that computer virus sneaked aboard International Space Station – Aug. 2008
  - "worm type" virus was found on laptop computers that astronauts use to send and receive email
  - Computers not linked to any space station's control systems or Internet

http://www.hungry-hackers.com/2008/08/computer-virus-goes-into-orbit.html

Virus Infection

- Three parts
  - **Infection mechanism** – How it spreads
  - **Trigger** – Decide whether to deliver payload
  - **Payload** – What virus does beside spread
    - May involve damage or not

Psuedo Code

```
def virus ()
    infect ()
    if trigger () is true;
        payload ()
```

Structure of A Virus

```
Virus() {
  infectExecutable();
  if (triggered()) {
     doDamage();
  }
  jump to main of infected program;
}

void infectExecutable() {
  file = choose an uninfected executable file;
  prepend V to file;
}

void doDamage() { delete all files C: drive }
int triggered()
 { return (some test? 1 : 0); }
```

Virus Targets

- Boot Sector - (Included for History)
  - Not too common anymore
  - Infects by copying itself to boot block
  - Each time the system is booted, virus loads

  - Few systems boot to floppy anymore
  - OS's prevent writing to disk's boot sector
  - BIOS have boot block protection

File Infector's

- Infects executable files
- Often becomes memory resident when infected file is run
- Binary executables are the most common

- Question: How is the virus executed when the file is run?

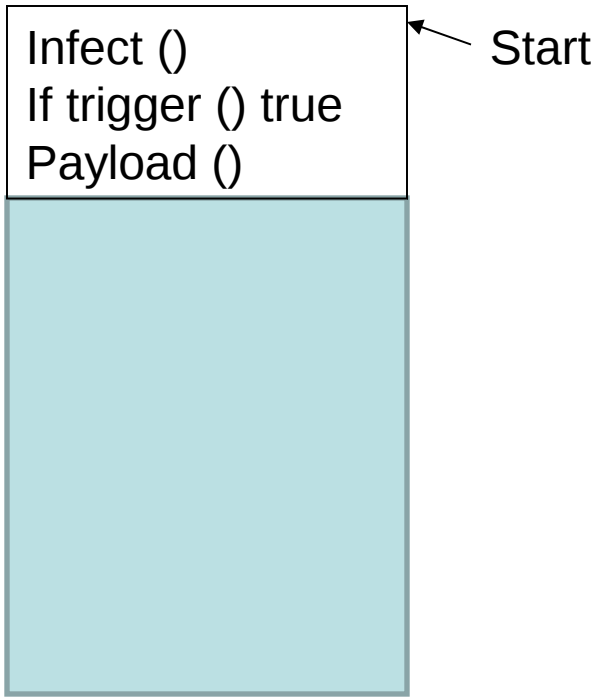
- Different techniques ...

File Infectors

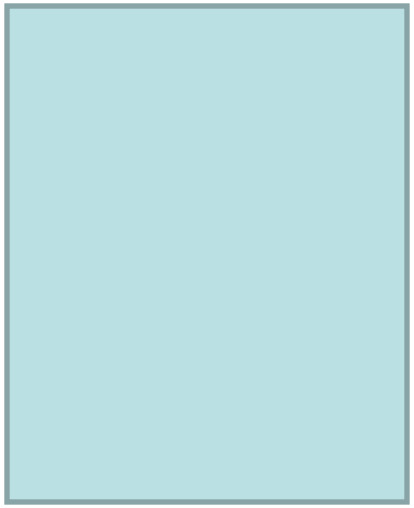
- At the beginning - prepending
  - Simple executables - .COM files
  - Entire file loaded into memory, virus code is placed at the beginning of the file
  - Then the file is run and virus gets executed first
- At the end of the file - appending
  - Appended to end of file
  - File header specifies start of code
  - Change start location to first run virus code, then run executable file

Prepending File Virus

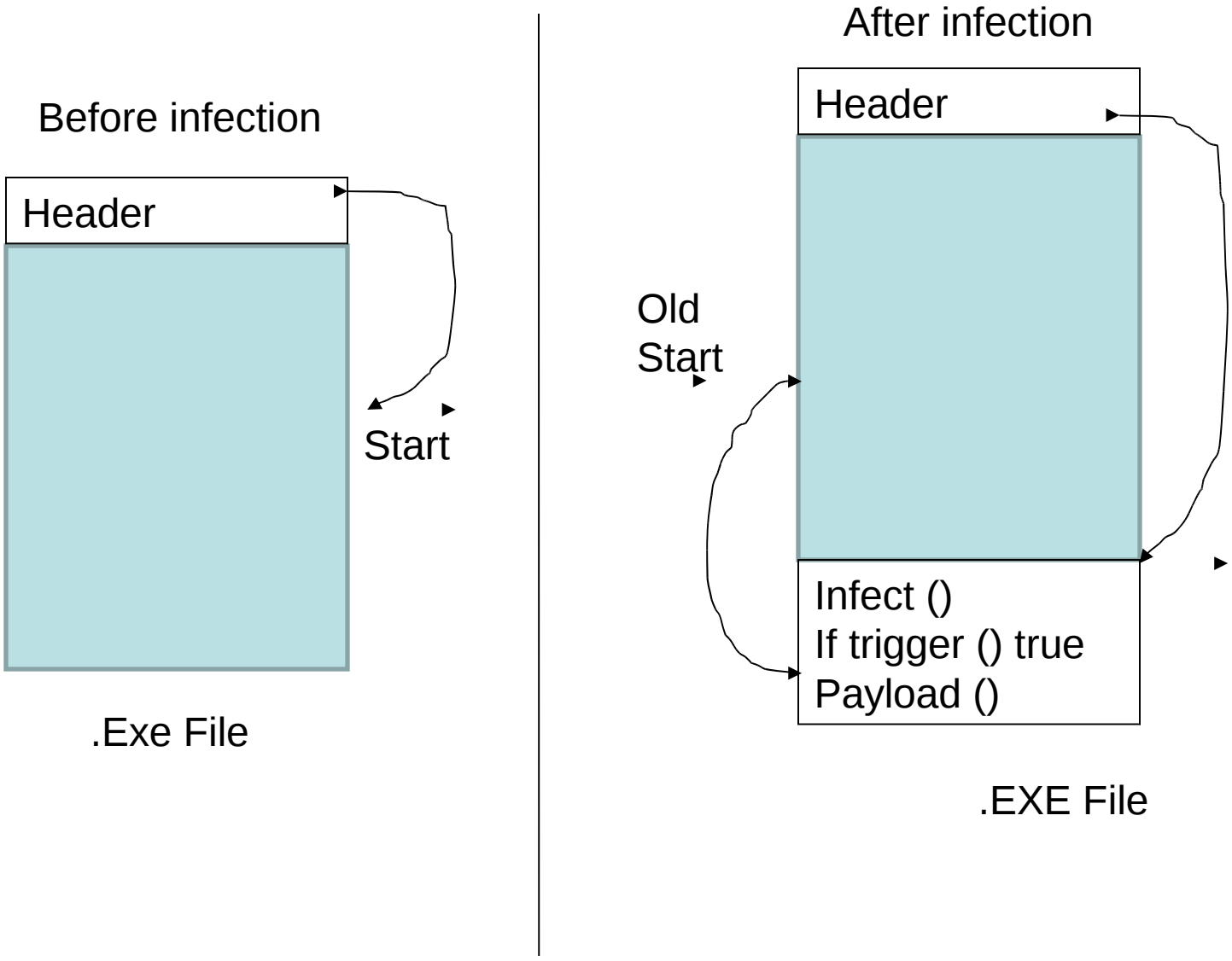
After infection



Before infection

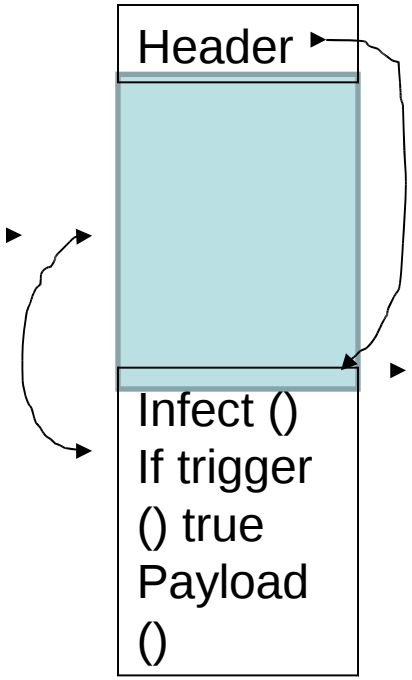


Appending File Virus



Appending Virus.. more

- How to infect a file (appending)
  1. Open Un-infected file
  2. Get Start code offset
  3. Calculate offset to end of file
     Save original start code offset
     Overwrite original start code offset with calculated offset to end of file
  4. Append viral code to end of file
  5. Add jump instruction (jmp) back to original offset



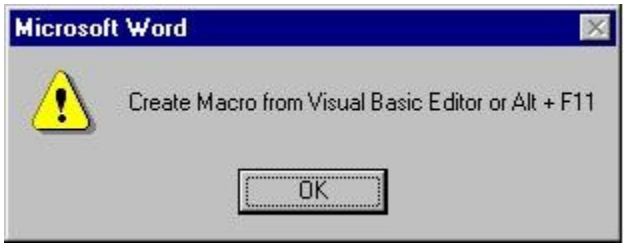
| Header|text|code offsett|| File Code

| Header|text|viral offset||File Code| |Viral Code|jmp code offset|

Perl Example

- Have code and show an example of a file infector ... does not try to hide itself

Data File Infections



Macro Virus

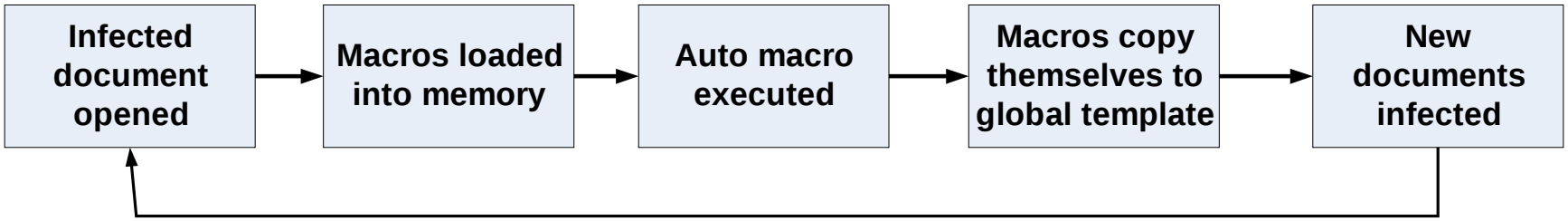
- Word docs allow small pieces of code, macros to be embedded in data file
  - When data file is loaded, macros can be automatically run
  - Word has a global set of macros, easily infected by single document
  - After infection, every document edited is infected by viral macros

Melissa Macro Virus

- Word macro virus delivered through e-mail in an attached Word document
  - Delivered through email
    - Can propagate itself by sending e-mail with the infected document to a number of recipients
    - Virus reads list of members from each Outlook Address Book and sends an e-mail message to first 50 recipients, user clicks on document to infect

How macro virus works

- Every word document is based on a template
- When an existing or new document is opened, the template settings are applied first
- A global template: NORMAL.DOT



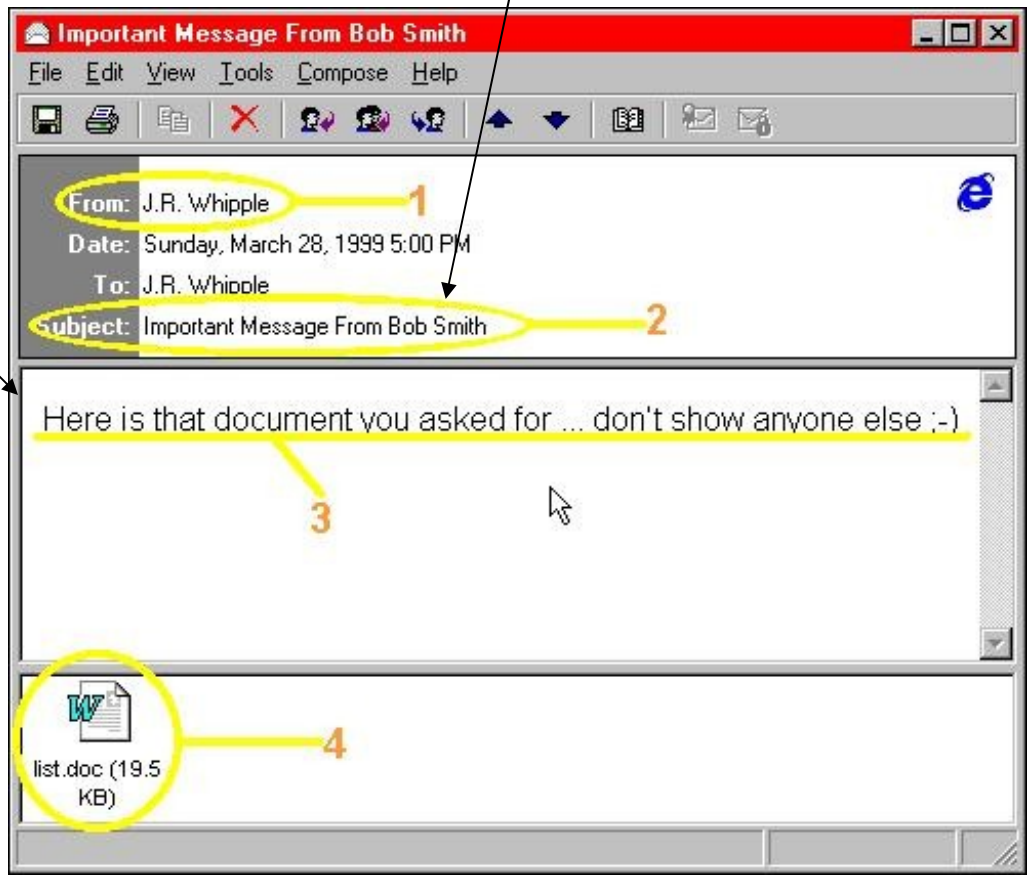
Melissa Virus

E-mail message may have subject line

"Important Message From UserName" in message body,

and

"Here is that document you asked for ... don't show anyone else ;-)“



Melissa Virus

- CERT® Advisory CA-1999-04. March 26, 1999
- Infected more than **one million personal computers** in North America. Caused more than **$80 million in damag**e
-
  - David L. Smith, 31, of Aberdeen Township, NJ, Pleads Guilty
    He was arrested on April 1, 1999
  - **Melissa author jailed for 20 months and imposed a $5,000** fine May 2, 2002

Symptoms of Viruses

- Your computer displays a vulgar, embarrassing or annoying message
- Your computer develops unusual visual or sound effects
- You have difficulty saving files: files mysteriously disappear
- Your computer reboots suddenly
- Your computer works very slowly
- Your executable files unaccountably increase in size
- Your computer starts sending out lots of e-mail messages on its own

Worms

Xerox PARC Experiments

- “Worm" programs Experiment in distributed computations
  - Programs that span machine boundaries and also replicate themselves in idle machines
  - A "worm" is composed of multiple "segments," each running on a different machine
  - Underlying worm maintenance mechanisms are responsible for maintaining wormfinding free machines when needed and replicating program for each additional segment

    http://www.cs.berkeley.edu/~prabal/resources/osprelim/SH82.pdf

How Worms Spread?

- Copy itself directly across the network
- Read your address book
  - Emails itself to everyone in your address book
  - How easy is it to do this?
  - Microsoft outlook – trivial
    < 5 lines of code to send out an email
  - Can cause outlook to send emails without user awareness
  - Reason why were so many worms for Outlook

Blaster Worm

- Aug. 2003
  - W32.Blaster.Worm propagated by exploiting Microsoft Windows DCOM RPC Interface

    Buffer Overrun Vulnerability
    - DCOM RPC allows programs on one computer to access services on another computer
    - **Program** could send a malformed RPC message to the running RPC process
    - Similar to the Server Message block problem
  - User didn't have to be involved with this at all!

Blaster Worm

- Result, critical memory overwritten, allowed remote system to gain shell on TCP port 4444 with System privileges
  - Shell used to invoke 'tftp.exe' to transfer the worm's main executable, 'msblast.exe', from host that compromised the system
  - The worm created registry entry so that it is launched every time Windows started:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update = msblast.exe

Blaster

- The worm caused system to reboot in order to launch 'msblast.exe' immediately

You could get this if your computer was infected or from another computer who was trying to infect your computer!

Blaster

The worm contains two messages hidden in strings.

First:

I just want to say LOVE YOU SAN!!

why worm is sometimes called Lovesan worm

Second:

billy gates why do you make this possible ? Stop making money and fix your software!!

message to Bill Gates, target of the worm

Trojans

- Trojan Horses
  - What are they ...
  - Difference with viruses
  - Example

Trojan Horse

- A Trojan horse looks like useful program but actually contains secret code that can destroy data or install spyware
  - Often referred to as virus, but unlike a true computer virus it does not replicate itself
  - Designed to gain access to your system and wreak havoc
  - Like the mythical Greek soldiers.

Trojan Infection

- How do you get infected with a Trojan?
  - In executable files, you download a “viewer” and it comes with an embedded Trojan
  - Email attachments with links that send you to malicious sites
  - Embedded Trojan within image files

Trojan Purpose and Behavior

- What is their purpose?
  - Anything from your keystrokes being logged and sent to someone, your passwords or Credit Card details transmitted to third parties,
  - Or, allowing someone to remotely control your machine across the Internet
  - Trojans are mostly written by professionals
    - Either extract money directly from end users or use zombie machines to earn money in other ways
    - Creating and selling spam
    - Organizing DoS attacks, with aim being blackmail

Trojan Behavior

1. Files opening on their own
2. Slow computer problems exist
3. You are directed to websites that you did not ask for
4. Your default homepage gets hijacked replaced with off-color sites … PornOurUs.com
5. Pop-ups and autoload toolbars are automatically placed on your PC
6. Cursor leaves a trail
7. Buttons such as the Windows start button are invisible
8. Your computer shuts down on its own, or reboots at will
9. Alt + Control + Delete is not responding
10. Your web surfing is incredibly slow

Trojans vs. Viruses

- What is the difference?
  - Trojans don't have main purpose of replicating themselves
  - Do not operate in stealth mode
  - Purpose is often money oriented
- Sometimes, threat is “blended”
  - Trojan can install a virus as part of its load

Example Trojan

- Win32/Vundo is a **multiple-component family** of programs that deliver 'out of context' pop-up advertisements
- They may also download and execute arbitrary files
- Very complete description of Vundu, Microsoft link below

  http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Win32%2fVundo

Plus, a good summary

http://en.wikipedia.org/wiki/Vundo

Example Trojan

- Vundo infection is caused by
  - Opening an e-mail attachment carrying the trojan, or
  - Browser exploits, including vulnerabilities in popular browser plug-ins, such as Java
- Vundo is often distributed as several DLL files and installed on an affected machine as Browser Helper Object (BHO) without user's consent
- Vundo may use **dropper/downloader** component that may be detected as one of following:

  TrojanDropper:Win32/Vundo.A

  TrojanDropper:Win32/Vundo.B

  TrojanDownloader:Win32/Vundo
- A dropper program is designed to install another program such as trojan or virus
- Designed to hide from anti-malware programs

Trojan Components

- dll files – Dynamic Link Libraries
  - Dynamic linking loads at runtime
  - Instead of linking them in at compile time
  - Subroutines remain as separate files on disk
- BHO – Browser Helper Object
  - A Browser Helper Object (BHO) is a DLL module designed as a plugin for Microsoft's Internet Explorer web browser to provide added functionality

Example Trojan

Vundo may make several registry modifications in order to load itself when Windows starts, for example:

Adds value: <trojan filename>

With data: <trojan path and filename.dll>

Two subkeys:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ……

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce …..

Example Trojan

- In order to protect itself from being deleted by anti-virus software, Trojan **may** monitor and possibly modify following registry entry to rename its file when the system restarts:

  HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations

Vundo may also inject its code into the following processes if they are found to be running on the affected machine:

Ad-aware.exe
Wrsssdk.exe
Hijackthis.exe

These are common protection, diagnostic programs

Example Trojan

- In particular, Vundo has been observed displaying pop-ups that promote the following rogue anti-spyware sites

  “antivirussecuritypro.com"

  “drivecleaner.com"

  "systemdoctor.com"

  "winantivirus.com"

  . . .

Also supposed to be the trojan currently distributing Antivirus 2009 and 2010

Example Trojan Behavior

- Sends Information to Remote Server
- Vundo may gather and send following information from affected machine to a remote server:

  Outlook Express Accounts

  Information from Software\Microsoft\Internet Account Manager\Accounts

  Pop3 and SMTP user names

  Registered owner

Example Trojan

Vundo was undetected by most antivirus packages … in 2008

- Inserts registry entries to suppress Windows warnings about disabling of firewall, antivirus, and Automatic Updates service
- Disables Automatic Updates service and quickly re-disables it if manually reenabled
- Attacks Malware Bytes' Anti-Malware, Spybot Search & Destroy, Lavasoft Ad-Aware, HijackThis, and other malware removal tools
- Not detectable by Vundofix ...

One of the better fixit articles:
http://www.bleepingcomputer.com/virus-removal/remove-vundo-virtumonde

Characteristics of Modern Trojans

1. Trojan distributed as a .dll
   - Why was this done?
   - To avoid detection by anti-virus who looks for running processes
   - These are library files stored on the disk

Characteristics of Modern Trojans

2. Used file hiding techniques so couldn't even see the .dll files

- How do they do this?
  - Intercept all calls to Windows Find File APIs, used by file system utilities, including Explorer and command prompt
  - When an application needs directory listing that would return results of files associated with malware, it intercepts and modifies output to remove entries ... more like a rootkit!

Characteristics of Modern Trojans

3. Modifies registry to allow auto start each time Windows starts
4. Disables firewall, auto-update security features
5. Disables or interferes with added anti-virus software

   Adware, Hijackthis, SypbotSearchandDestroy etc.
6. Opens connections to server

   Sends potentially sensitive information out
7. Keeps re-infecting and hijacking machine

Another Trojan CryptoLocker

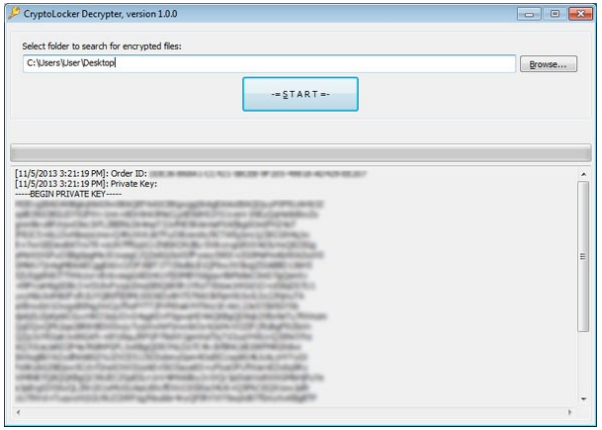
- CryptoLocker September 2013

  Ransomware program that was released September 2013, targets all versions of Windows including Windows XP, Windows Vista, Windows 7, and Windows 8

  Encrypts certain files using mixture of RSA & AES encryption

  CryptoLocker payment program that prompts you to send a ransom of either $100 or $300 to decrypt files ... also displays timer stating that you have 72 hours, or 4 days, to pay ransom or it will delete your encryption key and you will not have any way to decrypt your files.
  http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

Another Trojan CryptoLocker



- This infection is spread through emails sent to company email addresses that pretend to be customer support related issues from Fedex, UPS, DHS, etc.

- These emails contain zip attachments that when opened would infect the computer
- Zip files contain executables that are disguised as PDF files as they have a PDF icon and are typically named something like FORM_101513.exe or FORM_101513.pdf.exe

- Since Microsoft does not show extensions by default, they look like normal PDF files and people open them

RansomeWare WannaCry

- On May 12th 2017, a massive ransomware attack occurred across a wide range of sectors, including
- Health care, government, telecommunications and gas

- To date, WannaCry has spread to over 300,000 systems in over 150 countries

- The countries that appear to be the most affected are Russia and China, probably because of high percentage of legacy software

RansomeWare WannaCry

- WannaCry is a type of ransomware, or extortive malware, that encrypts files, disks and locks computers. The malware demands a ransom of ~$300-600 to be paid to one of three bitcoin accounts within three days in return for decrypting the files.

- WannaCry spreads via SMB, the Server Message Block protocol operating over ports 445 and 139, typically used by Windows machines to communicate with file systems over a network

- Microsoft fixed the vulnerability in the SMB and sent out a patch but not all systems were patched

Charactertistics of Modern Trojans

- If you fight with an infection for a while and still can't get it off your computer, what's your next step?
  - Reformat disk
  - Re-install Operating System
- This is not a failure
- You should do this anyway, every so often
- Cleans up disk and things run faster!
- Will cover this more in separate lecture ...

Summary of Risks

- Malware beginnings
  - Virus vs. Worm
  - Not that much difference
  - Both self-replicate, worm spreads via network
  - Others much more nasty
  - Trojans - professional touch
  - Really hose your system if infected!

Virus Resources

- Number of sites with virus information

Virus Bulletin
http://www.virusbtn.com/index

Viruses in the Wild
http:// www.wildlist.org

Virus and Worm Timeline
http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms

Virus Resources

- Number of sites with virus information

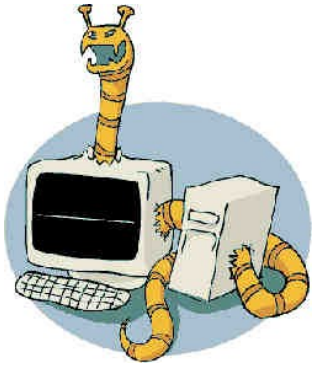
Virus and Other Malware Removal Help

http://www.bleepingcomputer.com/

Avoid Getting Infected - Advice

http://www.wikihow.com/Avoid-Getting-a-Computer-Virus-or-Worm-on-Your-Windows-PC

Malware Resources



- Wikipedia

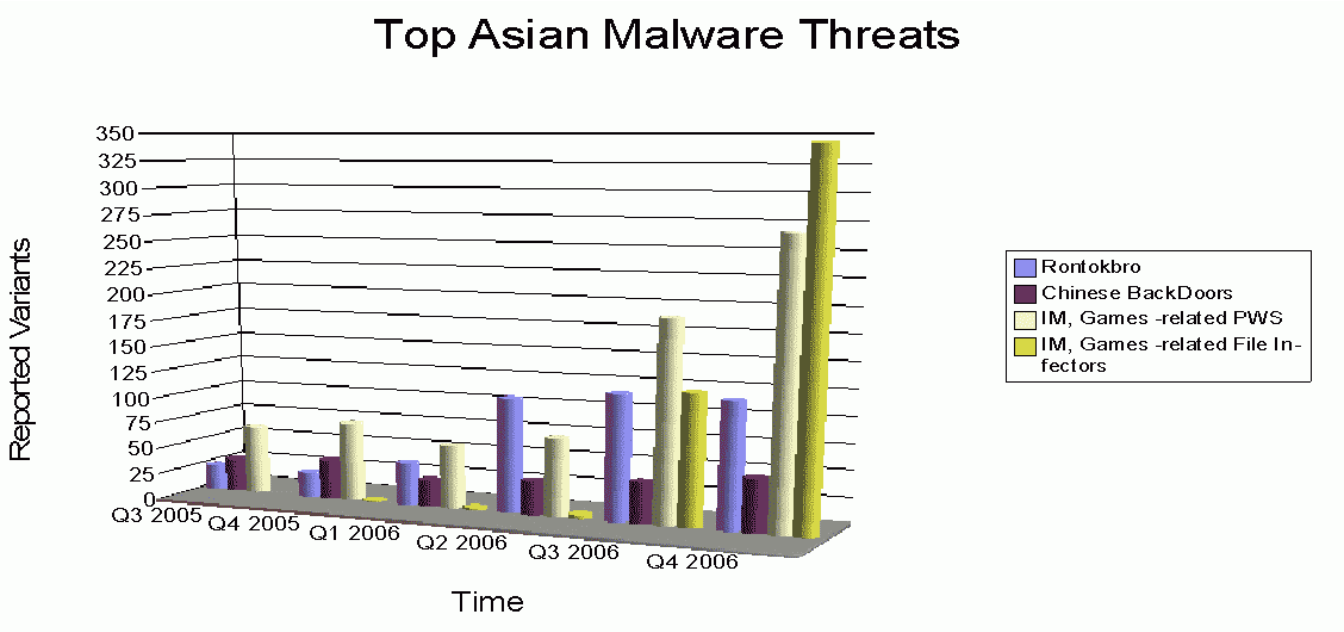
  http://en.wikipedia.org/wiki/Computer_worm
- Security Focus Interview

  http://www.securityfocus.com/columnists/347
- ESET.com Site of Resources

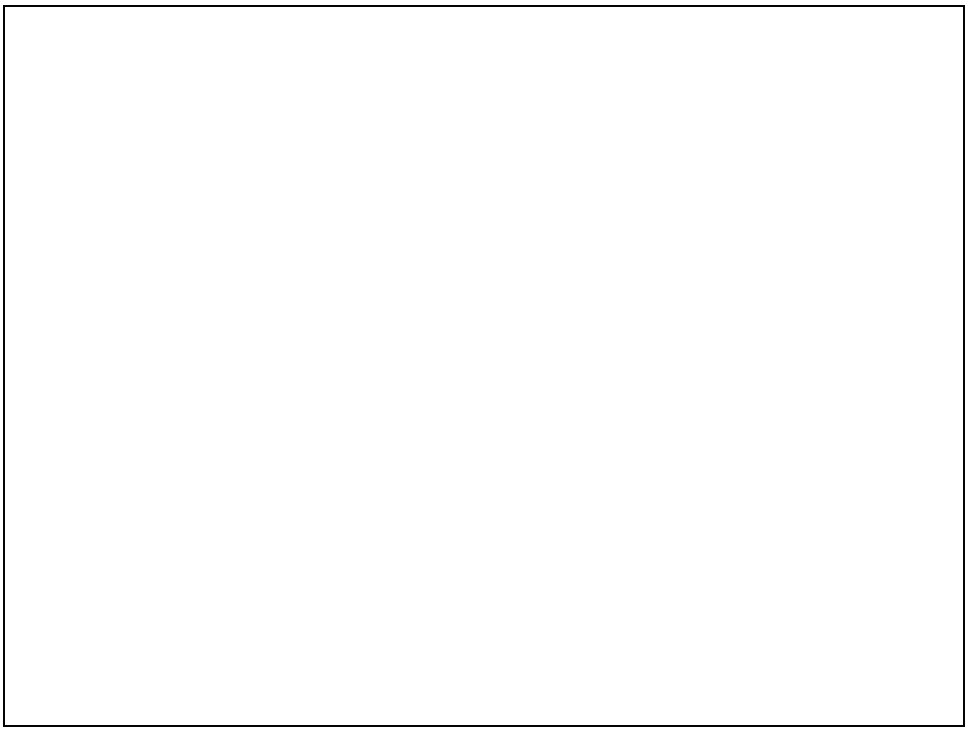
  http://www.eset.com/us/threat-center/
- PCHell - Both virus, malware and worm resources

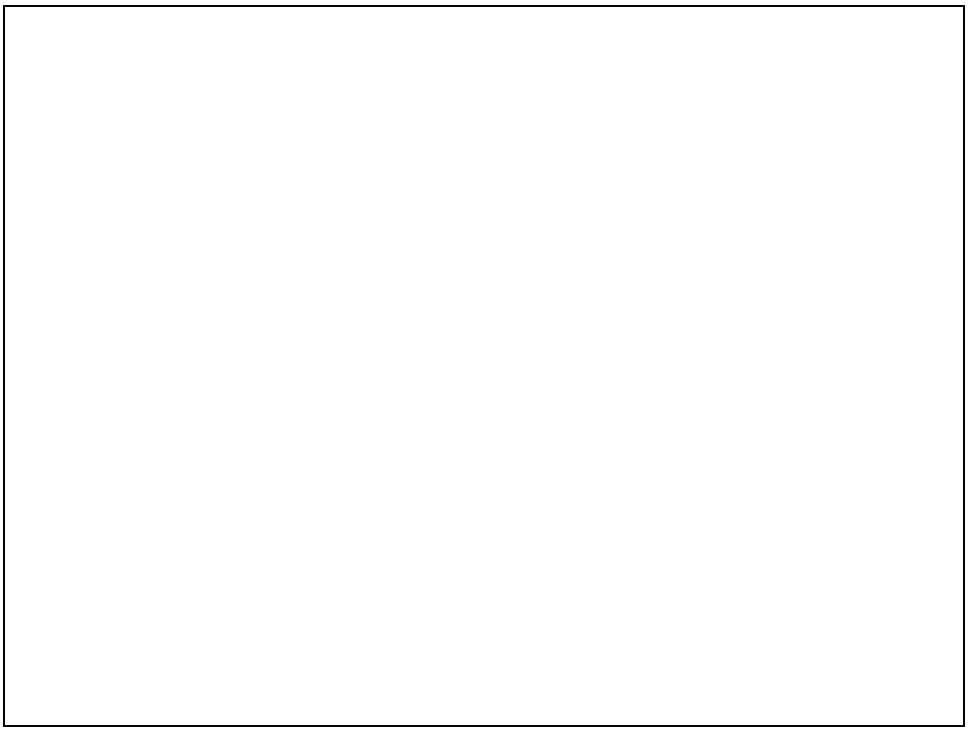
  http://www.pchell.com/

The End



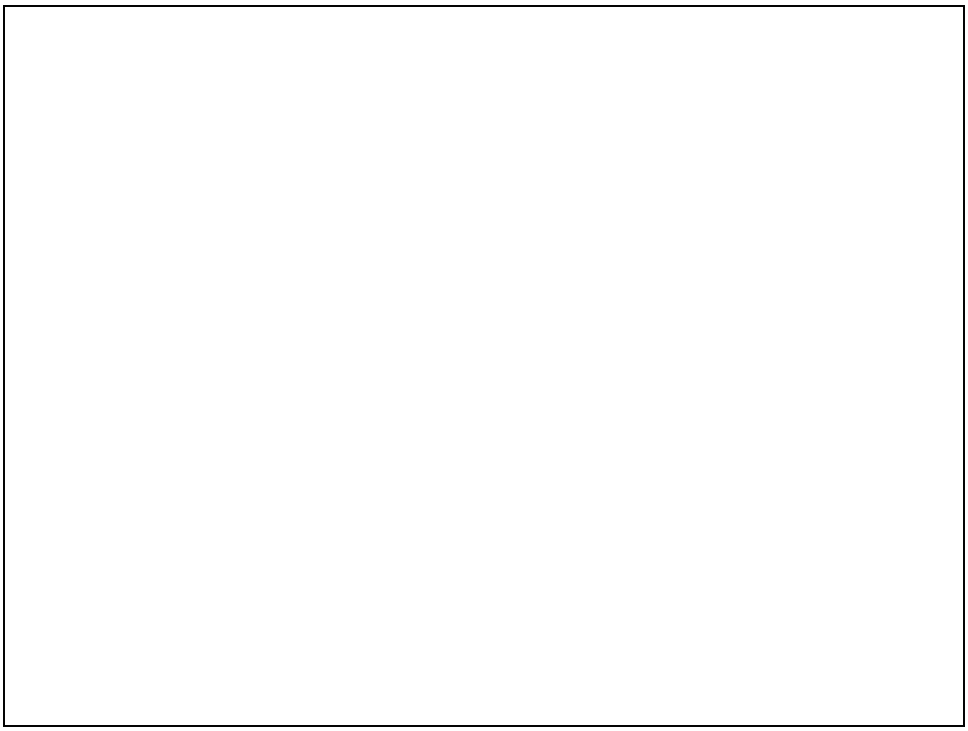
Next Time … More malware and Defenses

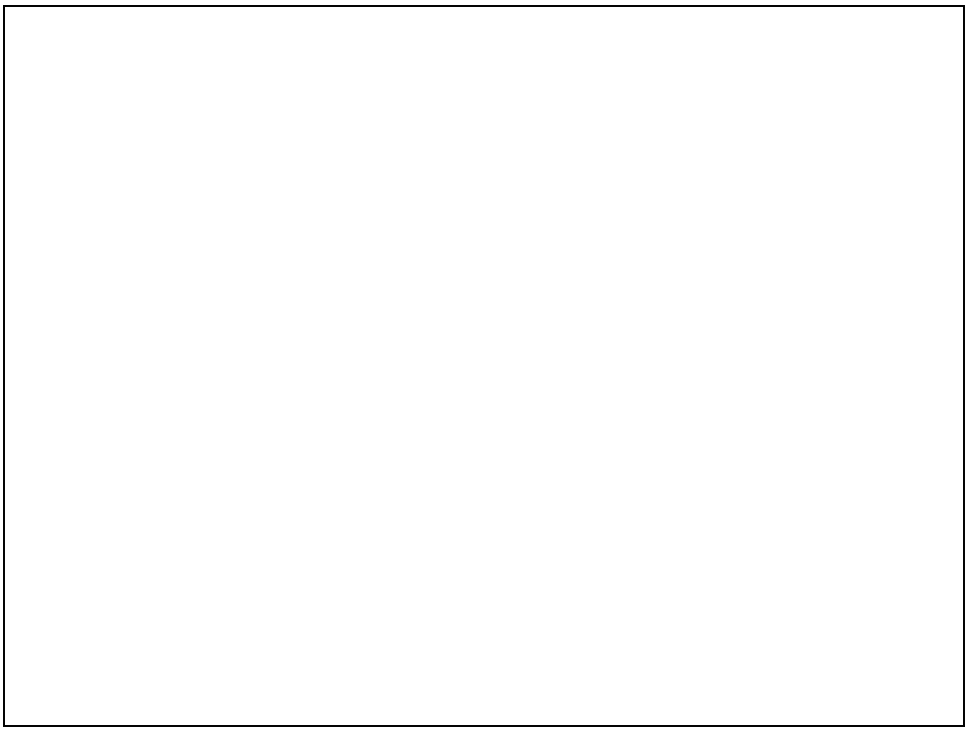


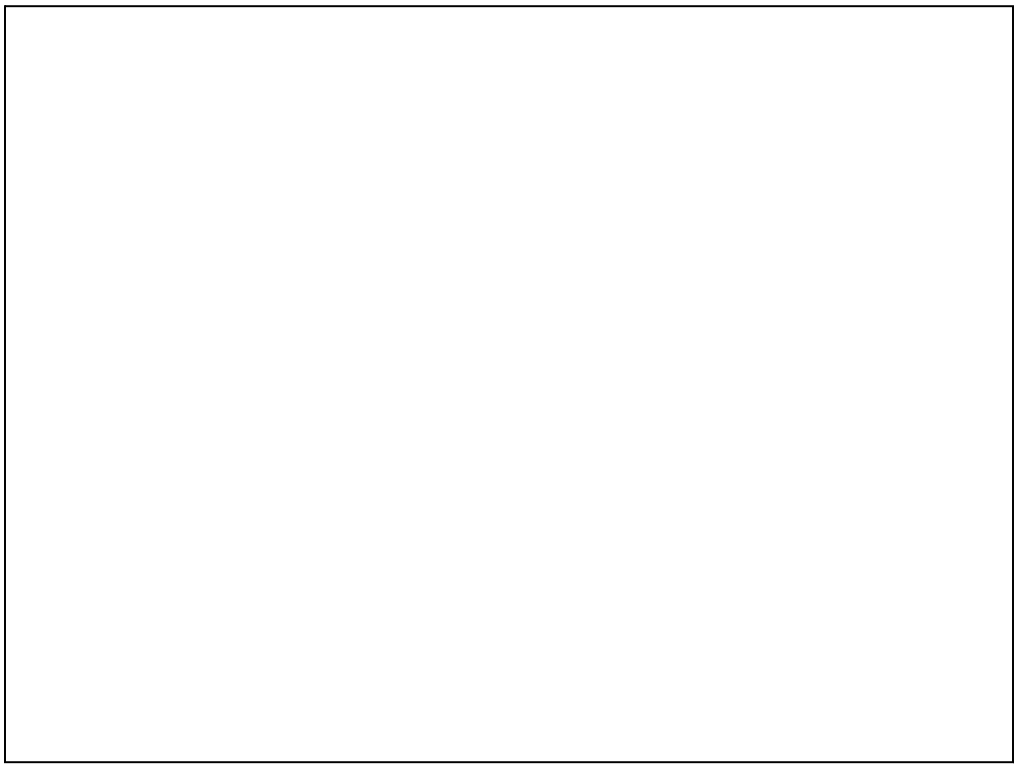


Take a Short Quiz

- You will take a short quiz on malware and then throughout the lecture fill in the answers.
- Turn in the answers with your name at the end of the lecture ...



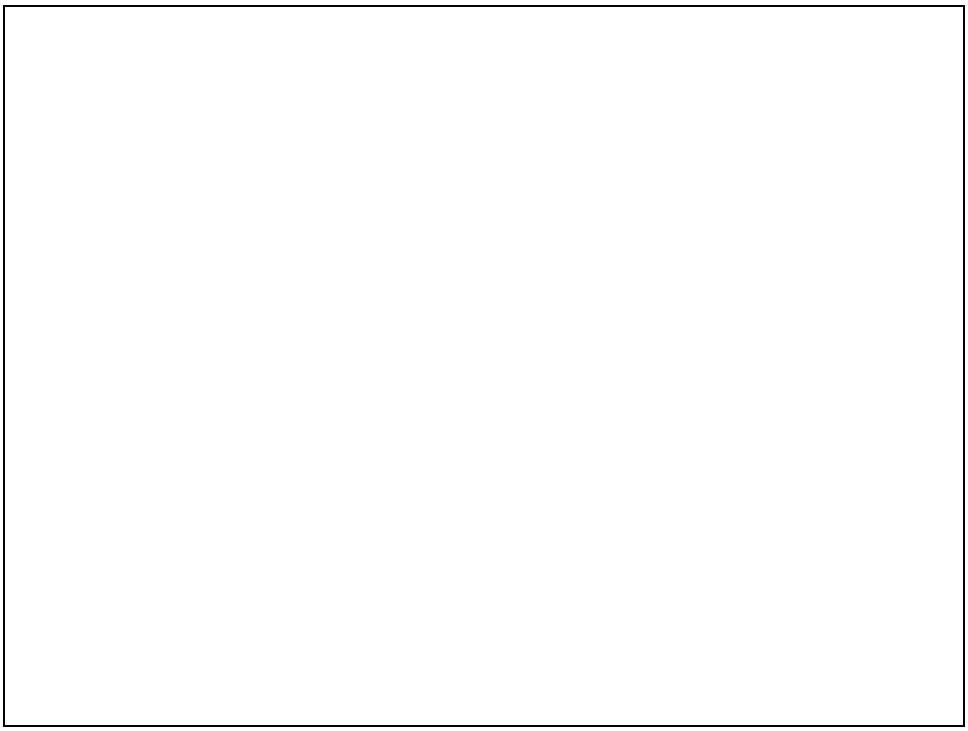


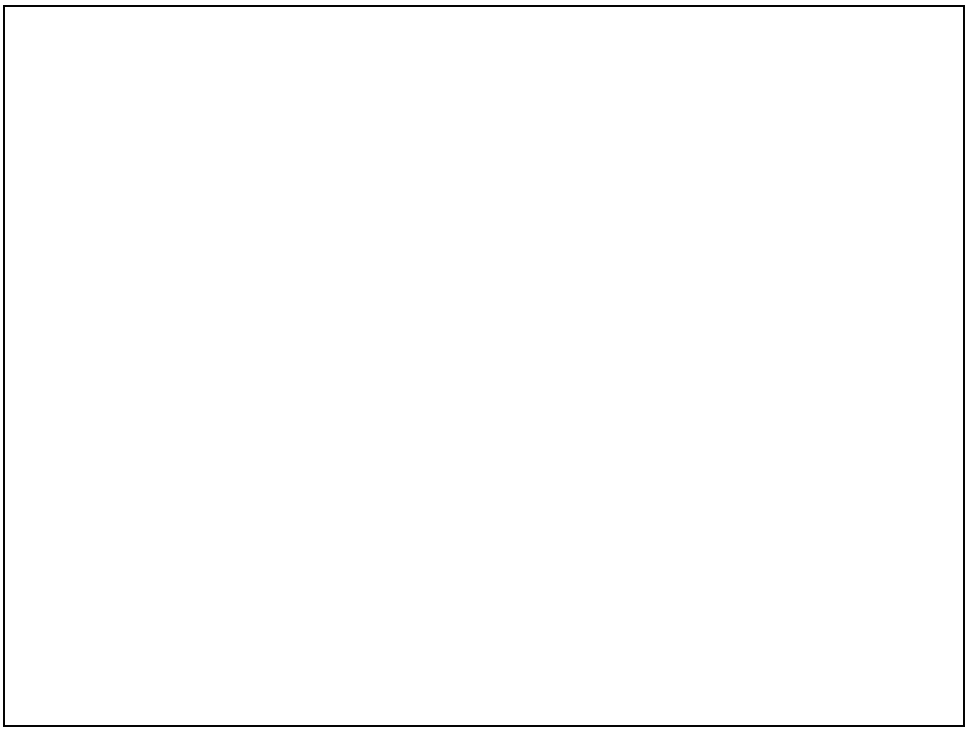


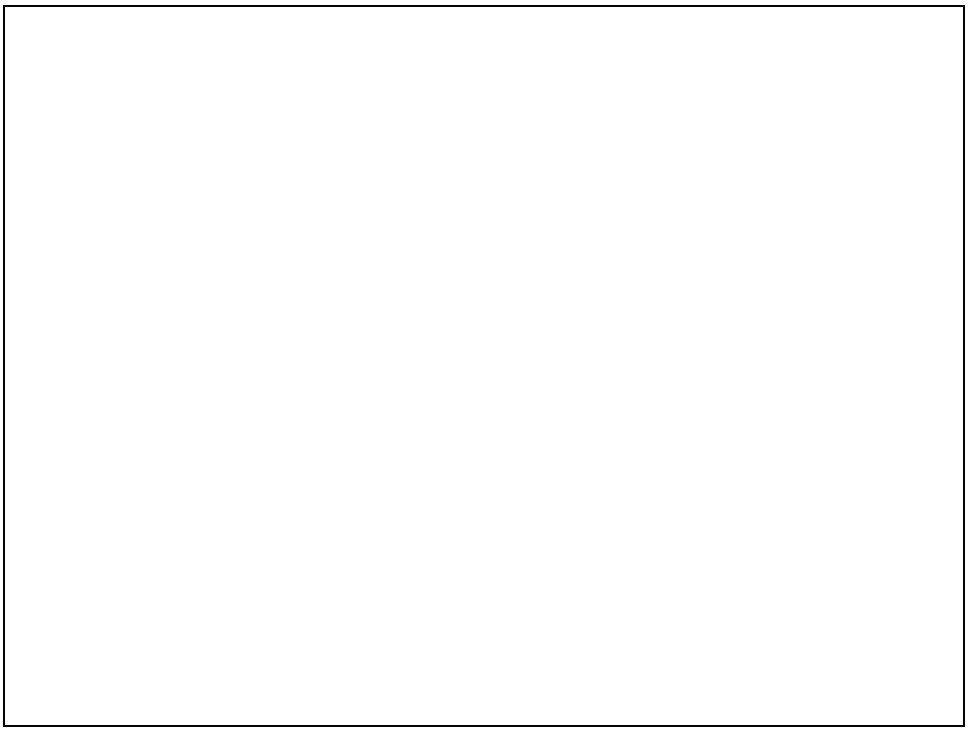
Stallings Fig 19-1.

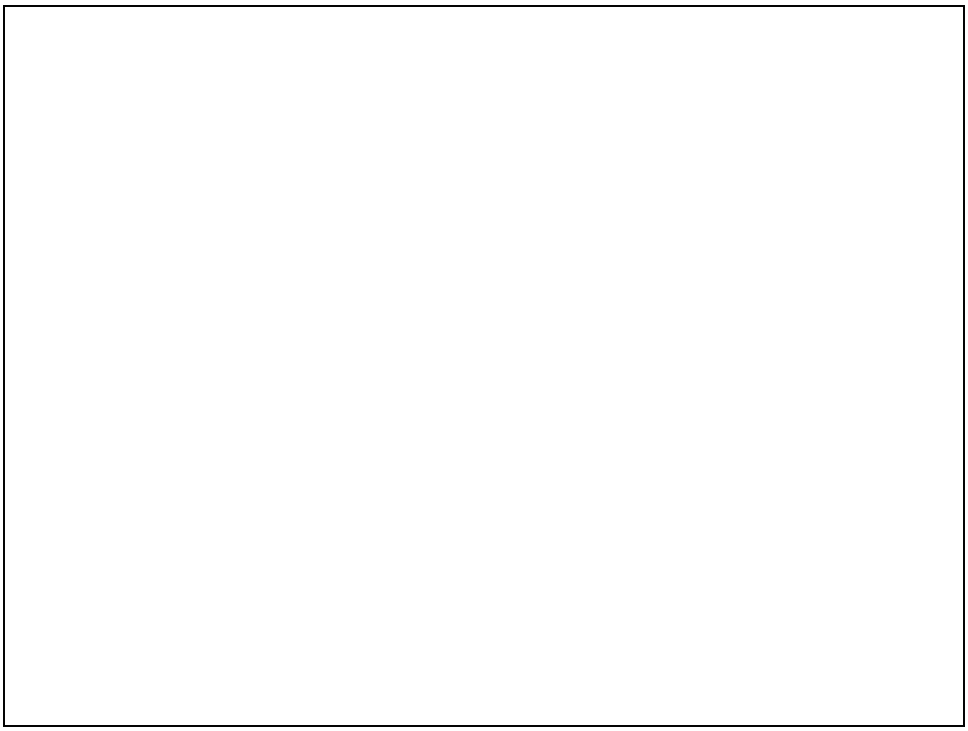
Taxonomy can be divided into two categories: those that need a host program, and those that are independent;

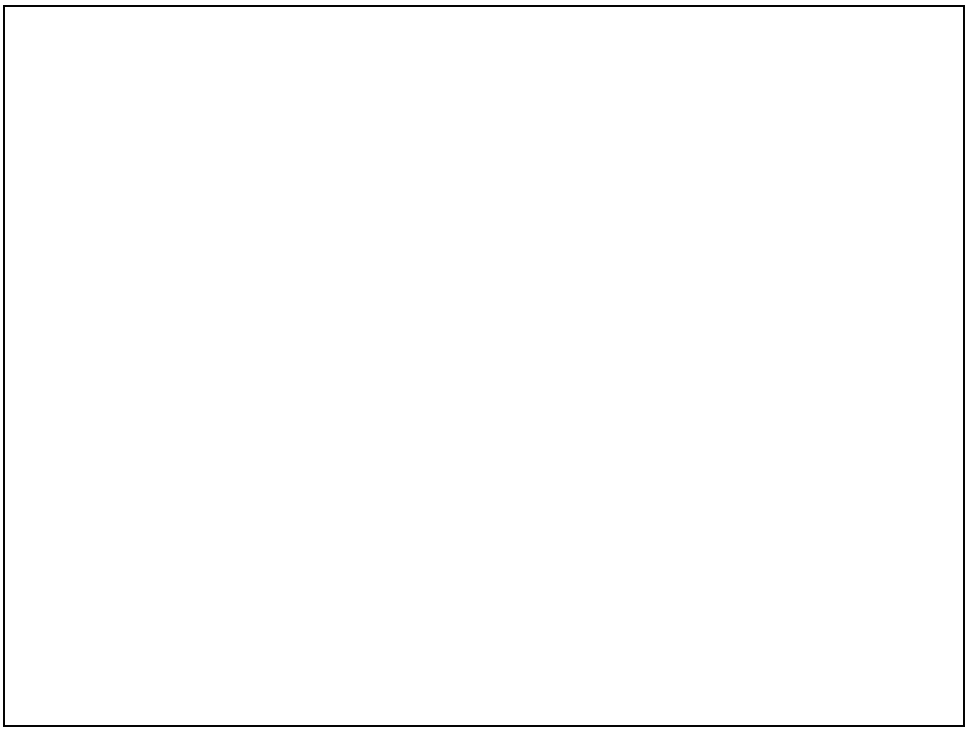
can also differentiate between those software threats that do not replicate and those that do.

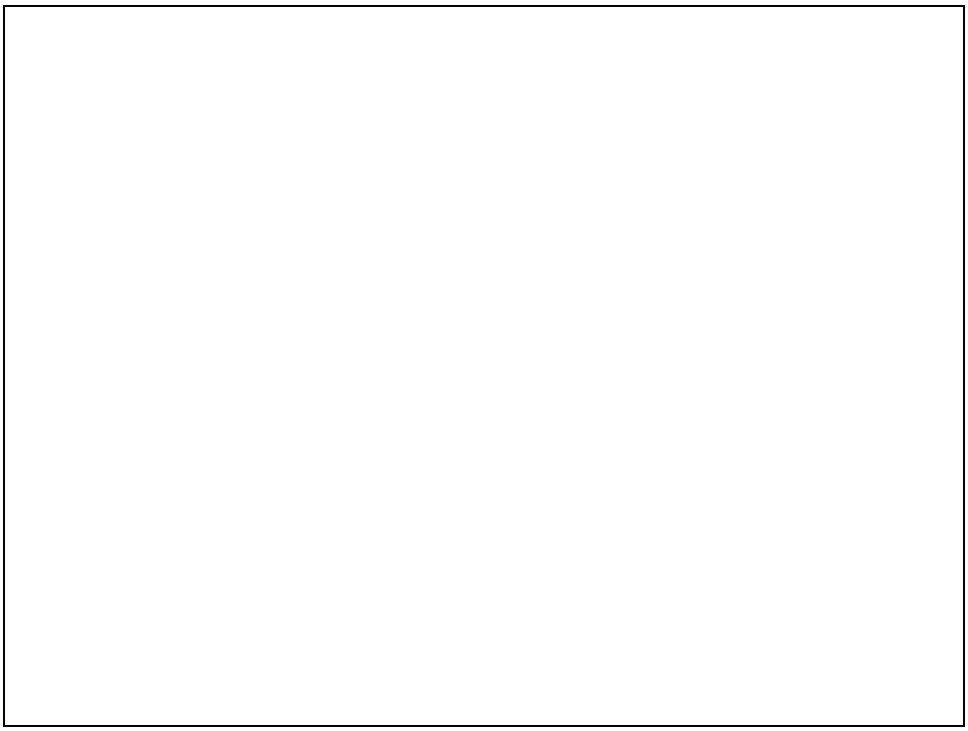








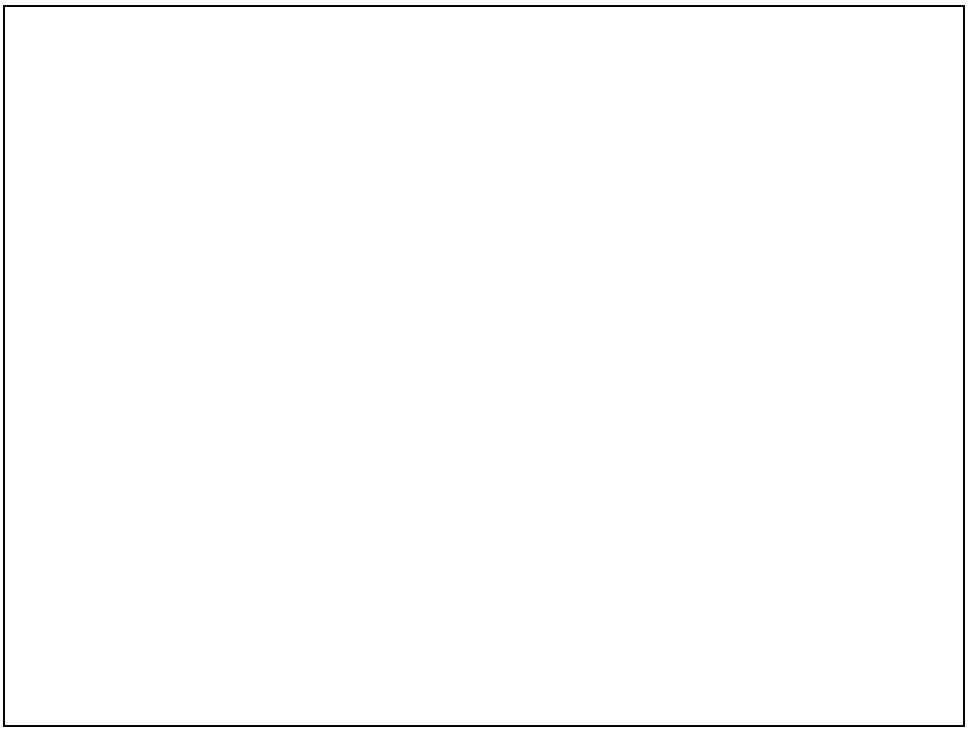


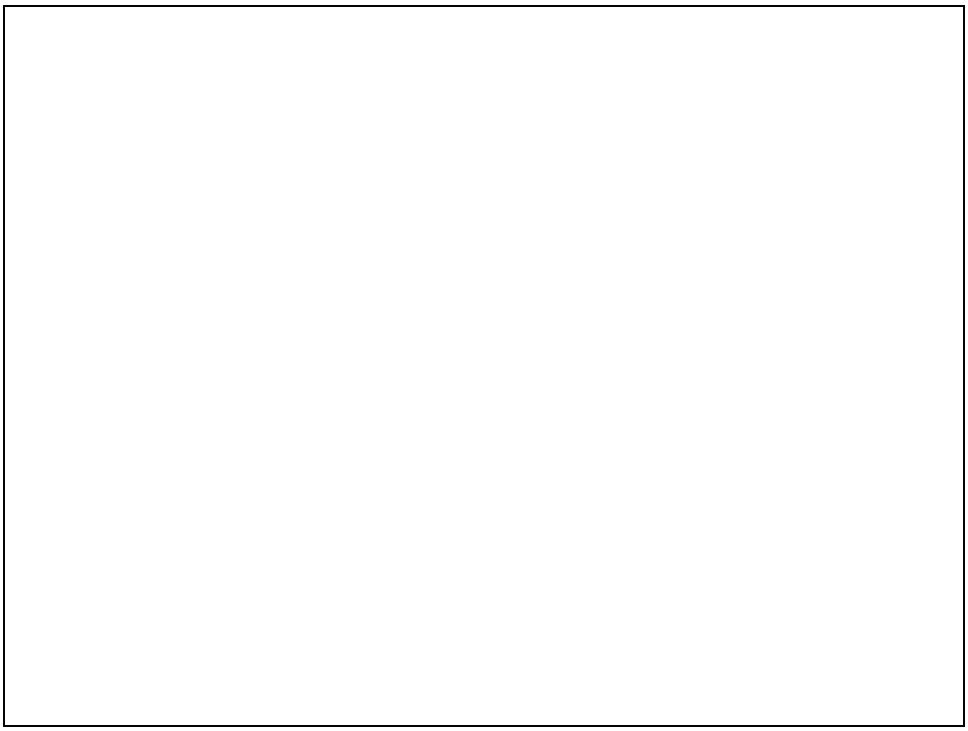


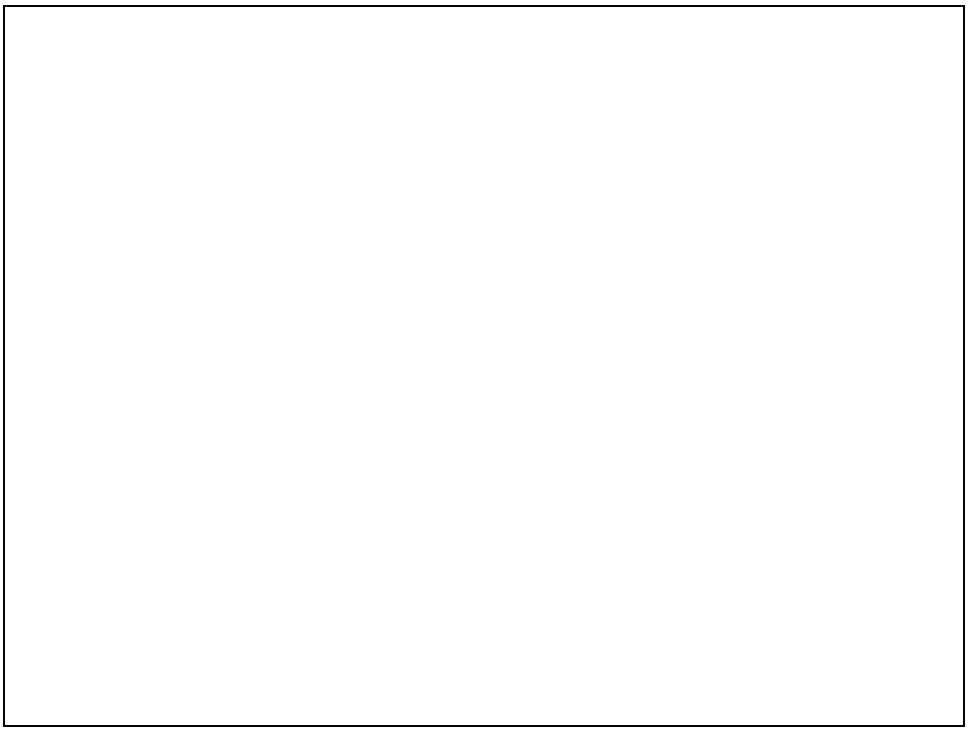
Keylogger

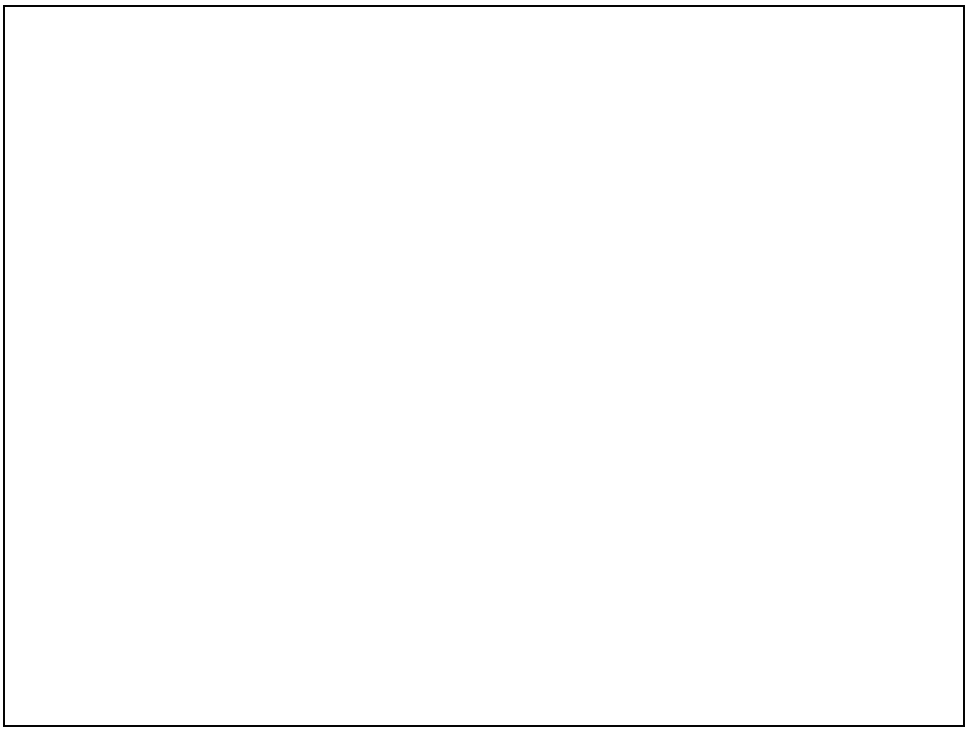
- Definition
  - Keylogger, sometimes called keystroke logger, key logger is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard
  - A keylogger program does not require physical access to user's computer
    - It can be downloaded on purpose by someone who wants to monitor activity on particular computer or it can be downloaded unwittingly as spyware

http://www.securelist.com/en/analysis/204791931/Keyloggers_How_they_work_and_how_to_detect_them_Part_1#what



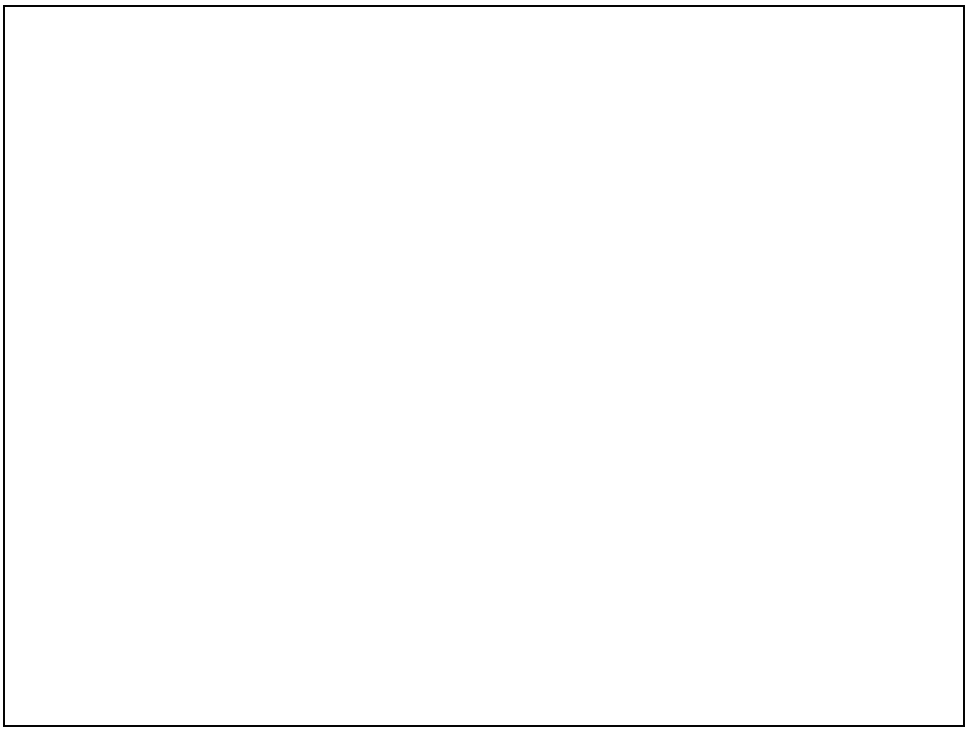


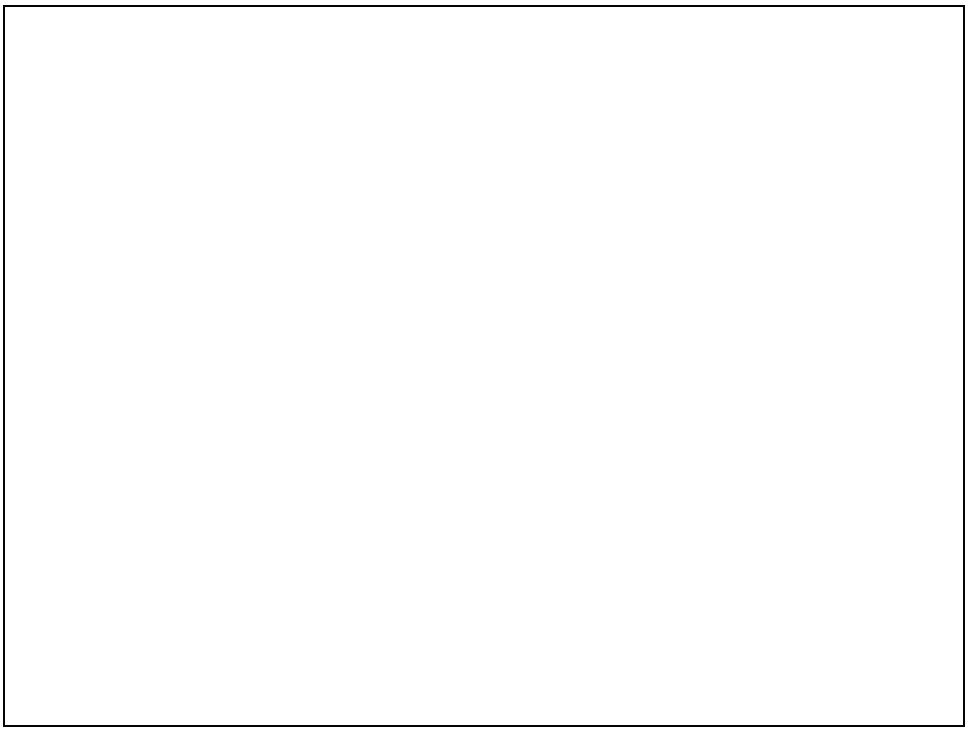


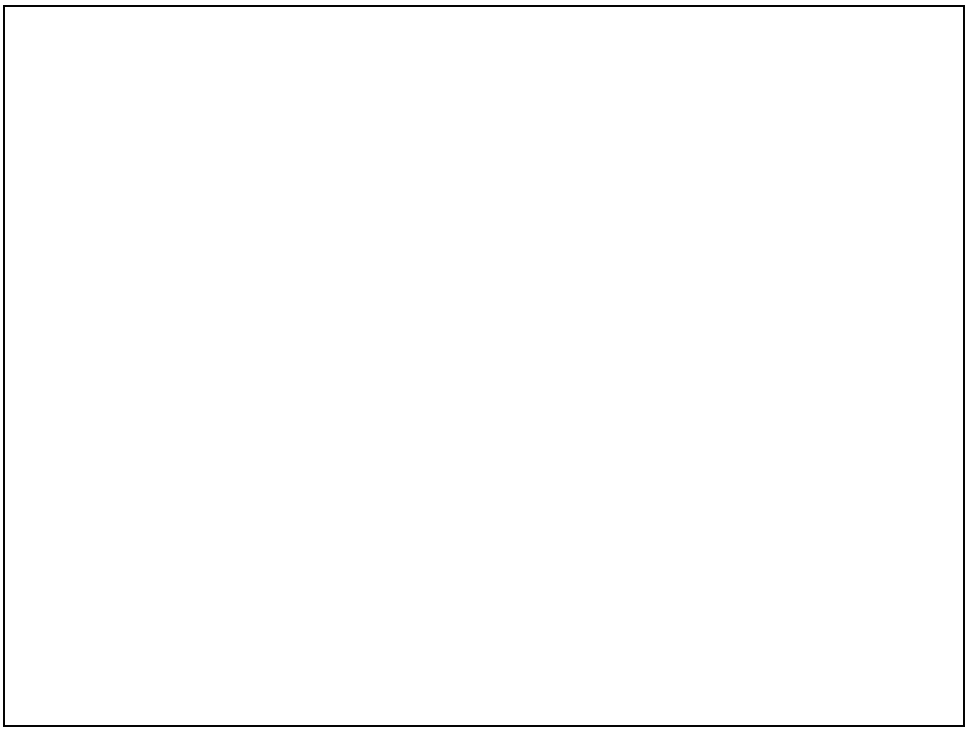


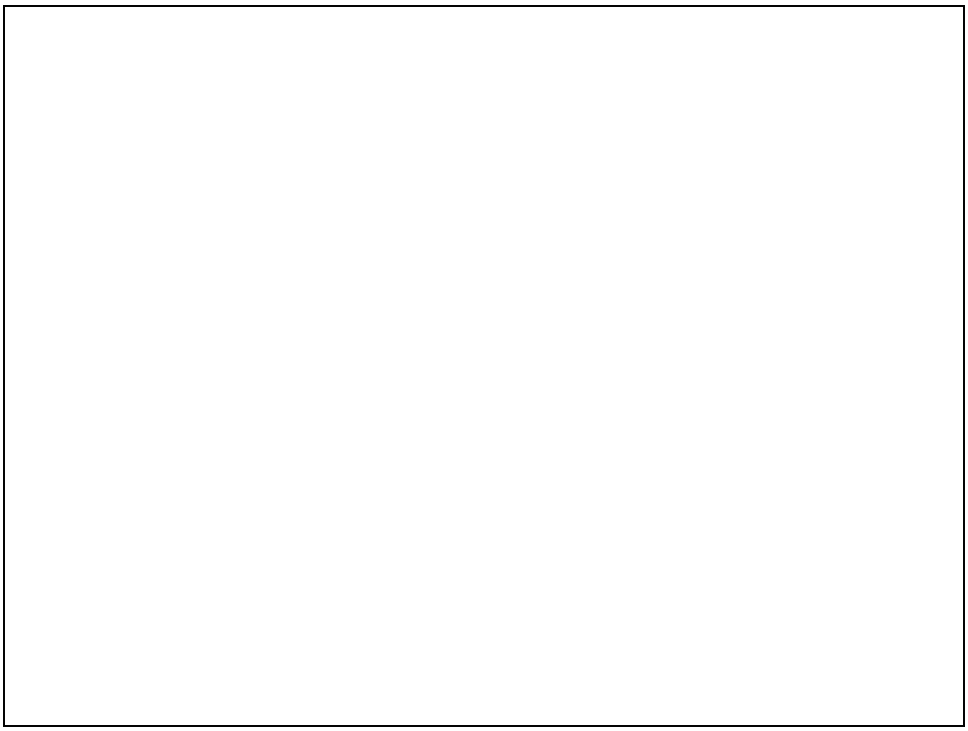
Structure of A Virus

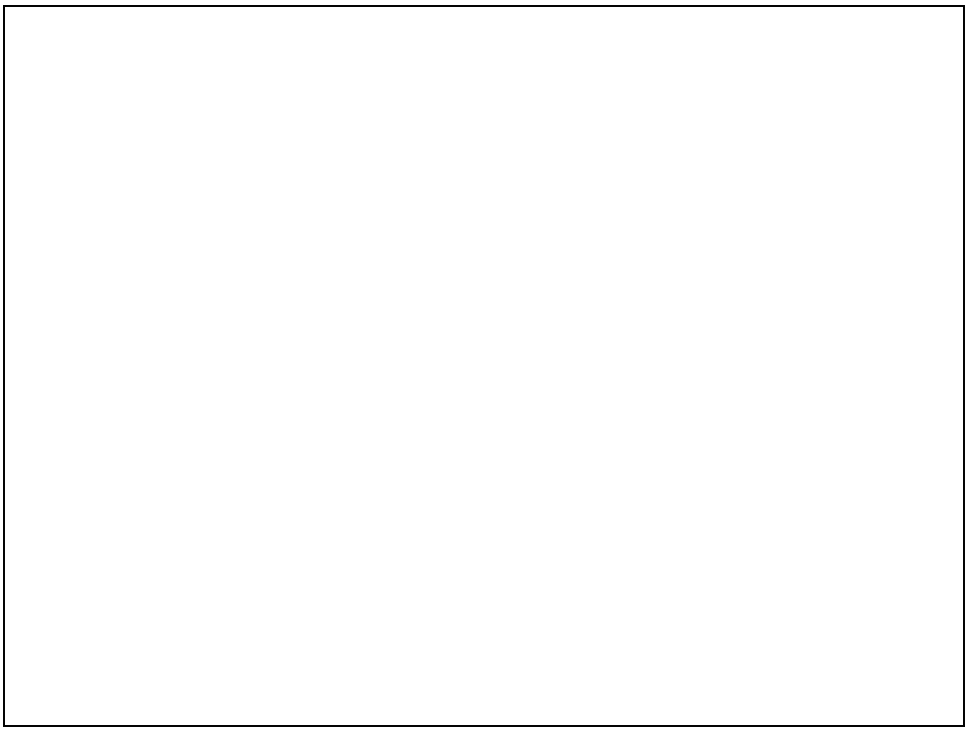
```
Virus() {
  infectExecutable();
  if (triggered()) {
     doDamage();
  }
  jump to main of infected program;
}

void infectExecutable() {
  file = choose an uninfected executable file;
  prepend V to file;
}

void doDamage() { delete all files C: drive }
int triggered()
 { return (some test? 1 : 0); }
```

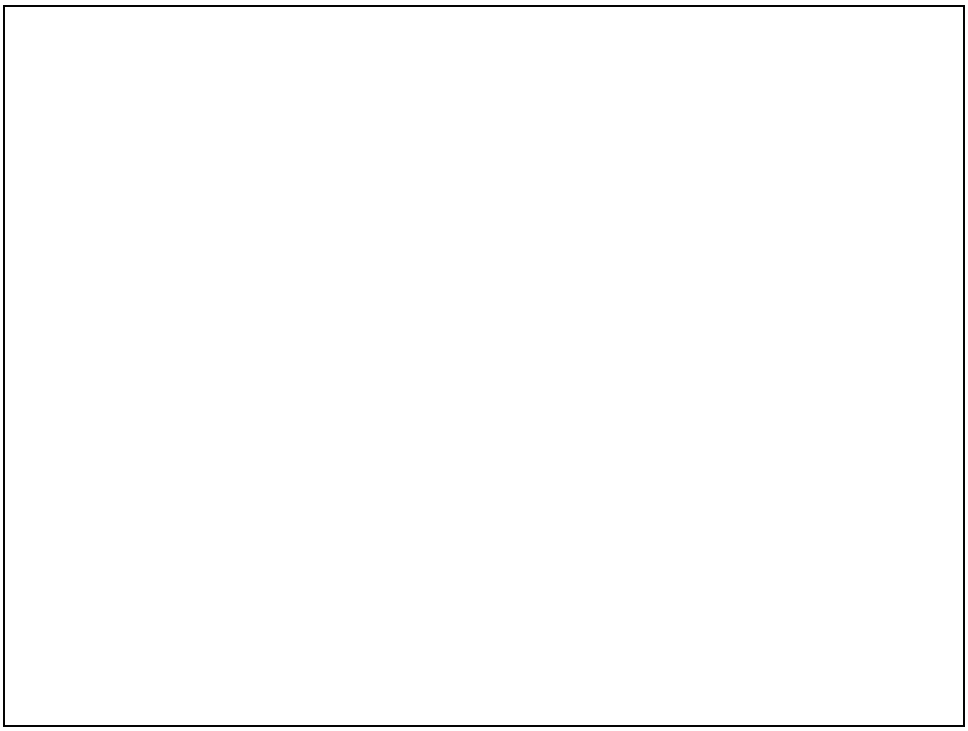


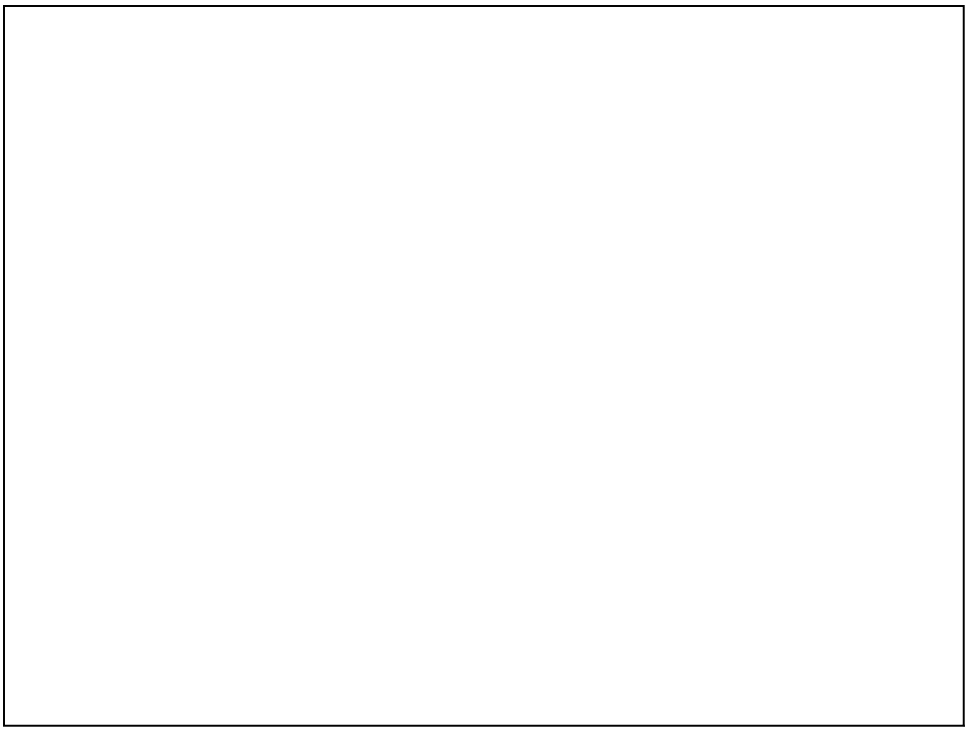


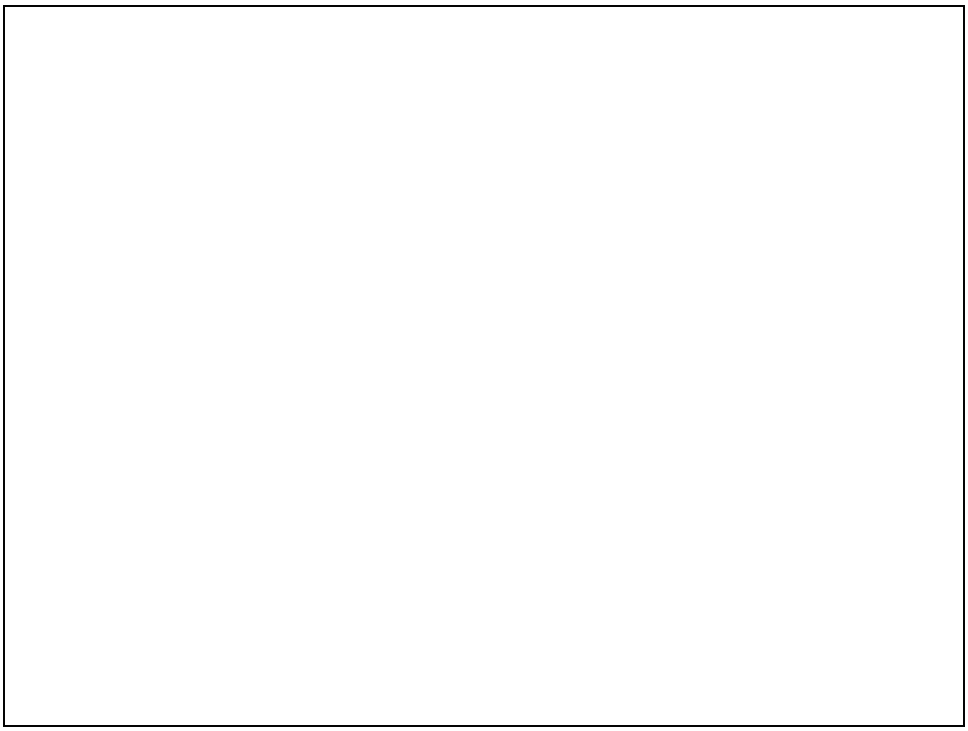


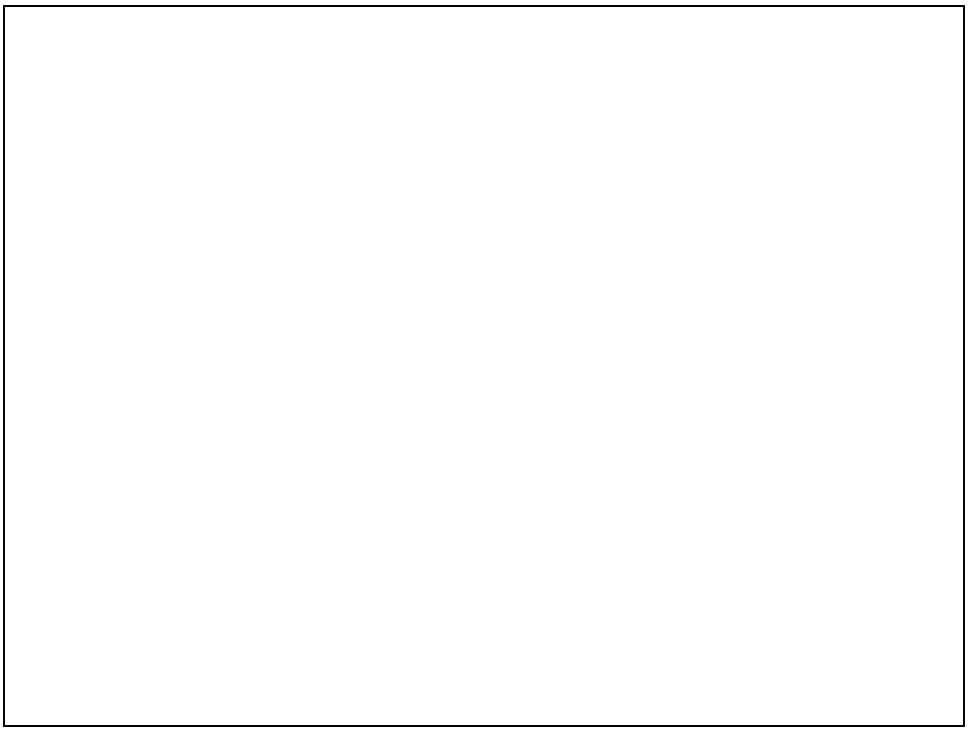






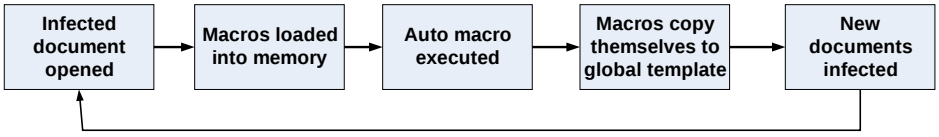


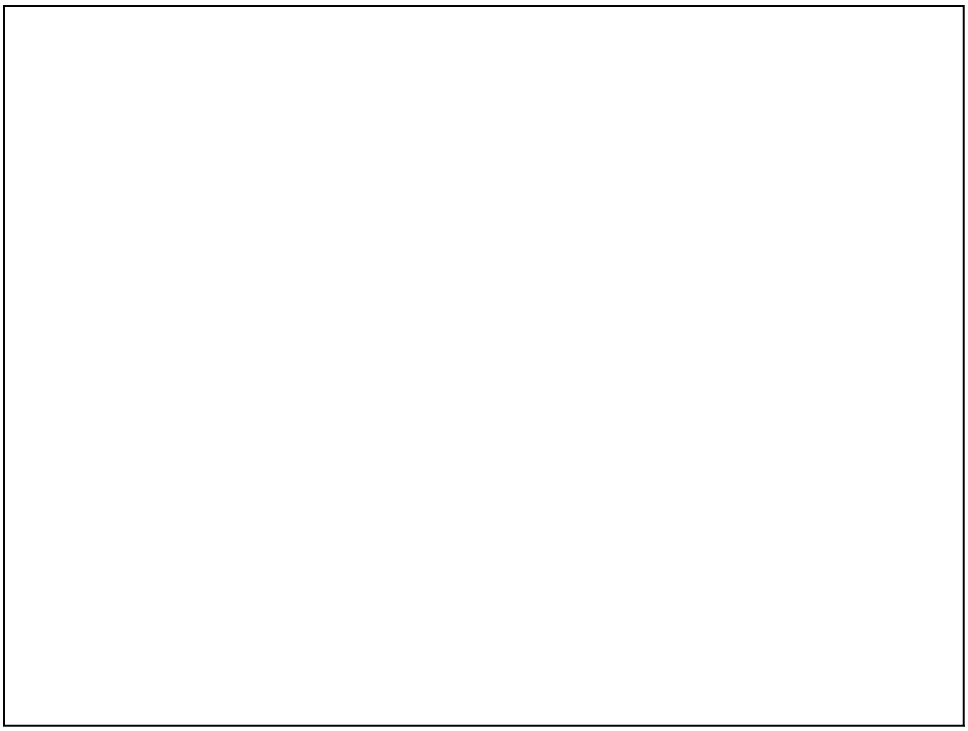


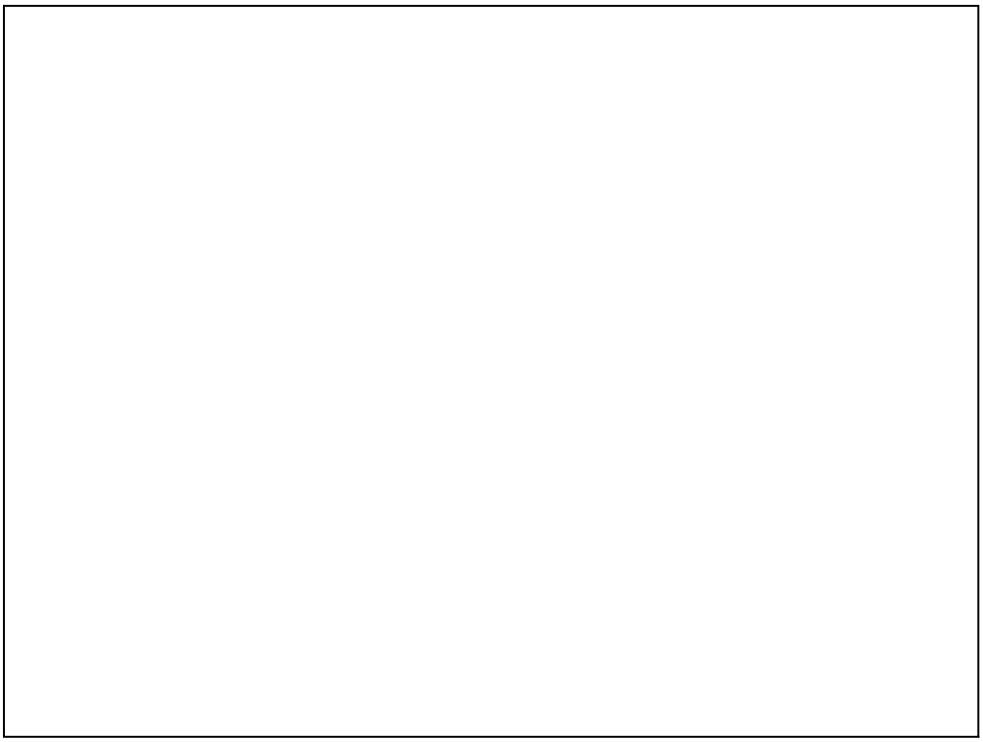


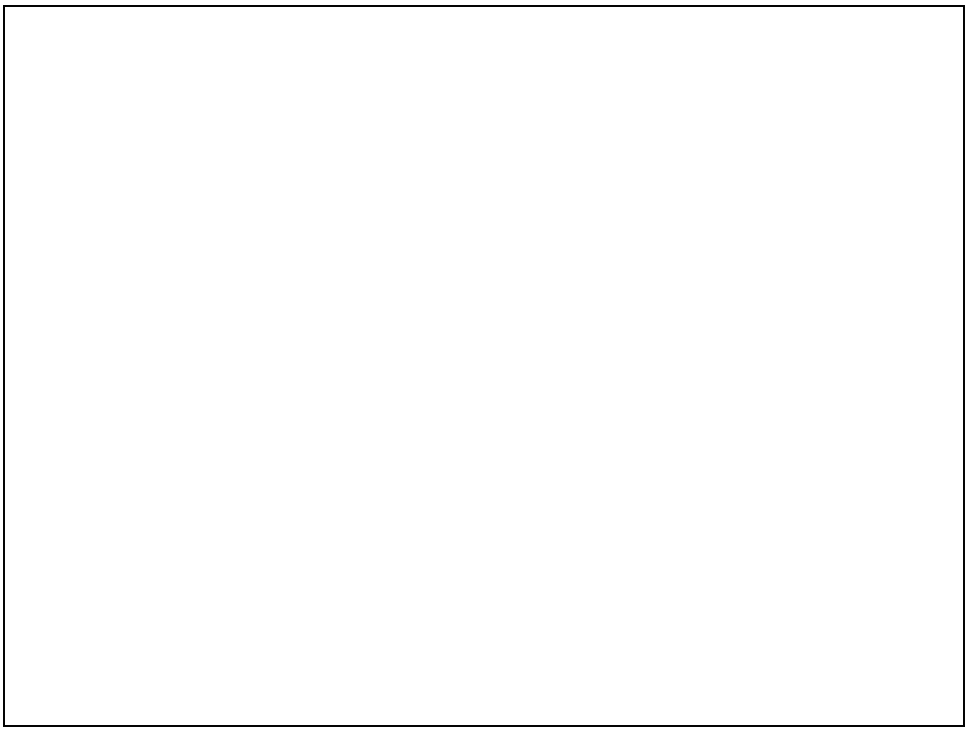
How macro virus works

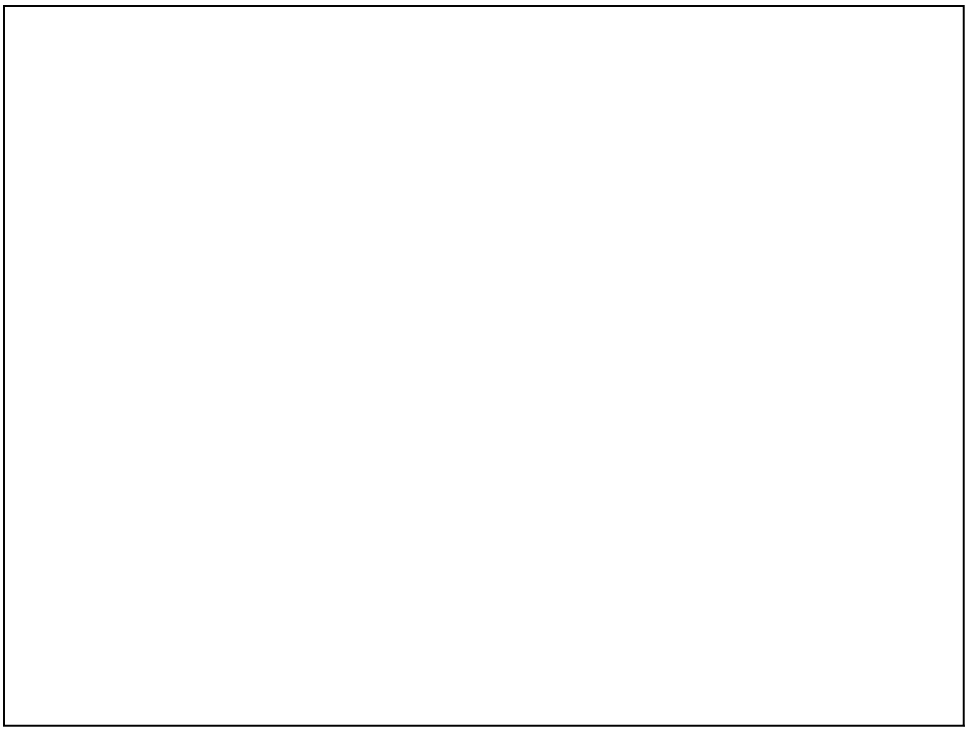
- Every word document is based on a template
- When an existing or new document is opened, the template settings are applied first
- A global template: NORMAL.DOT

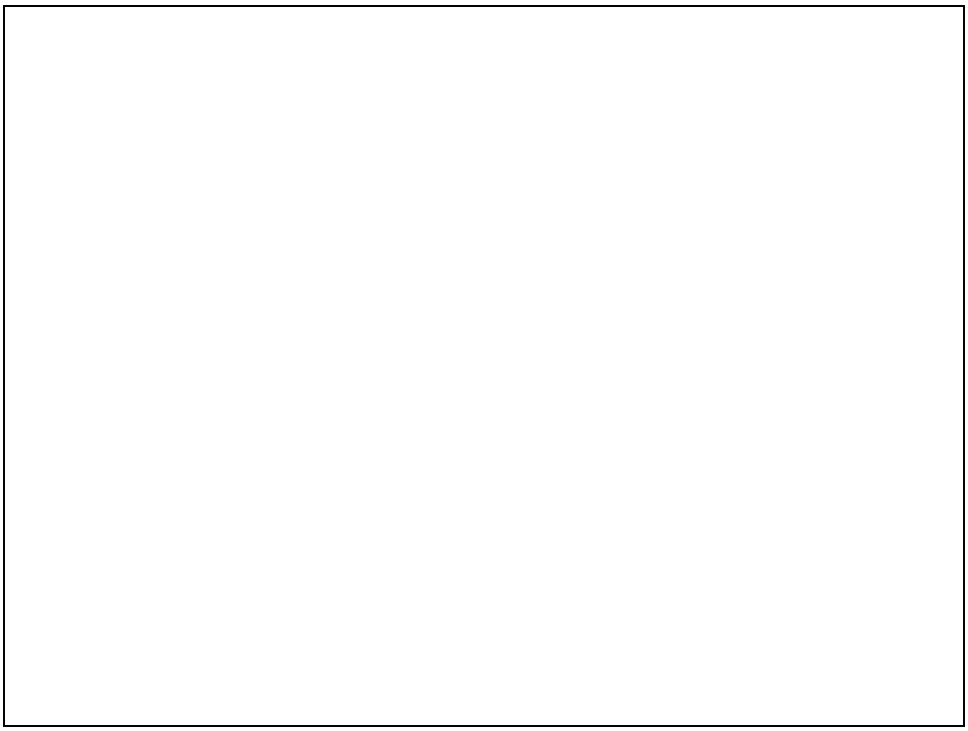


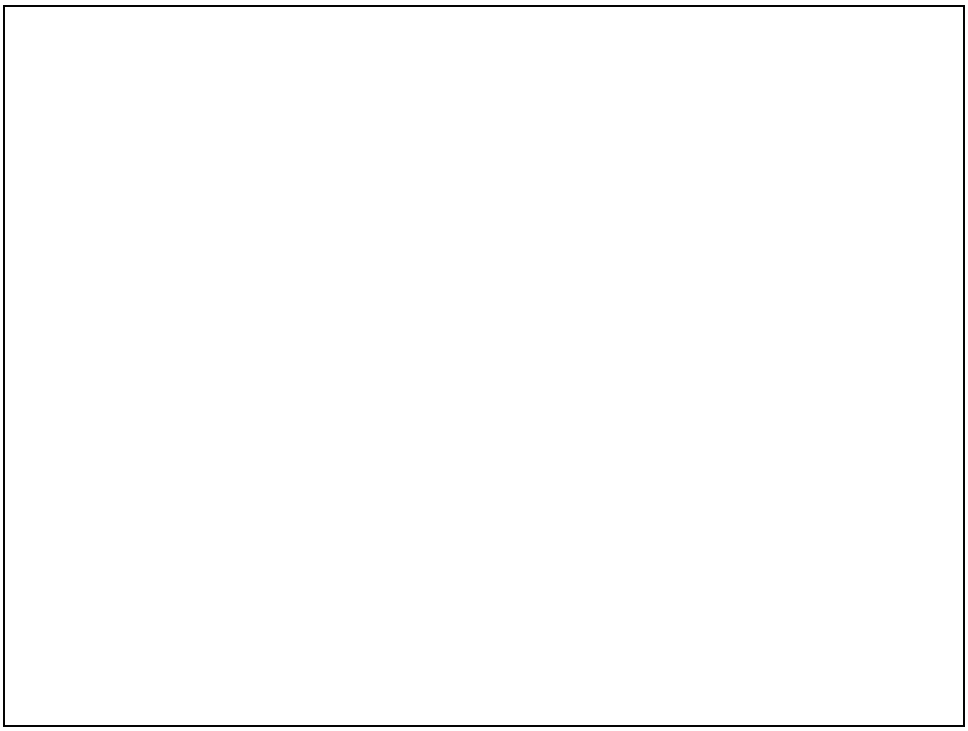


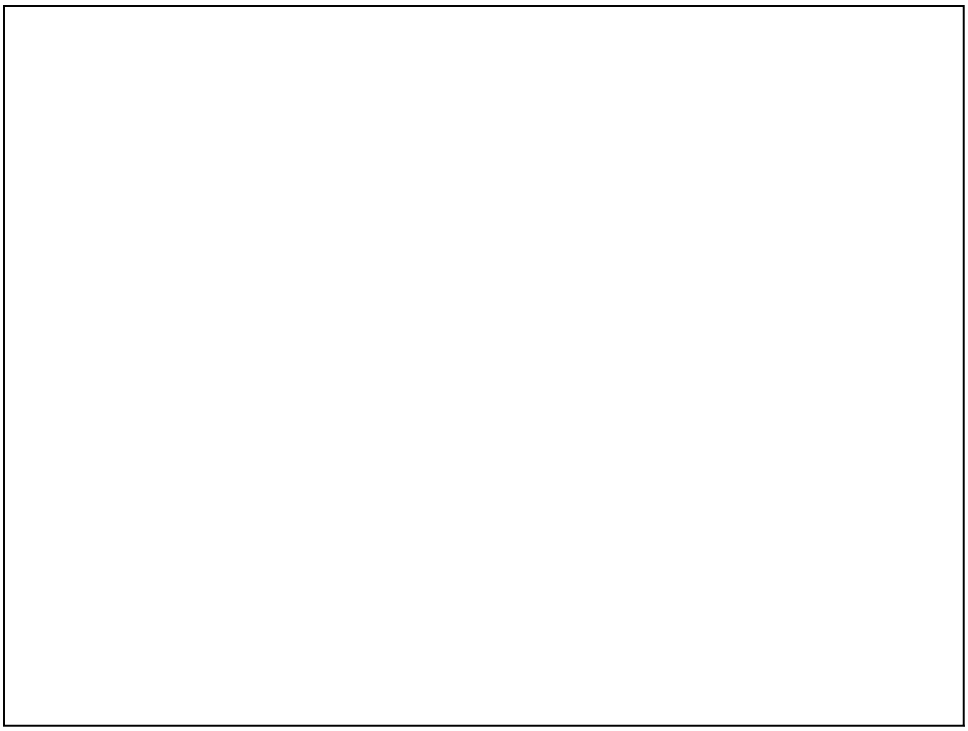


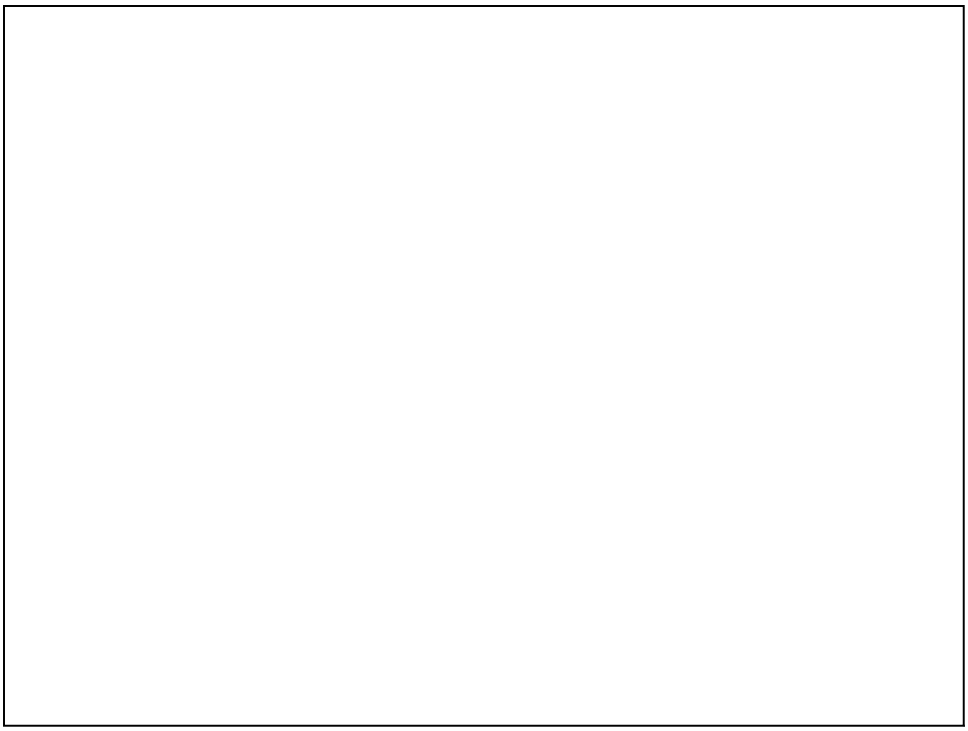


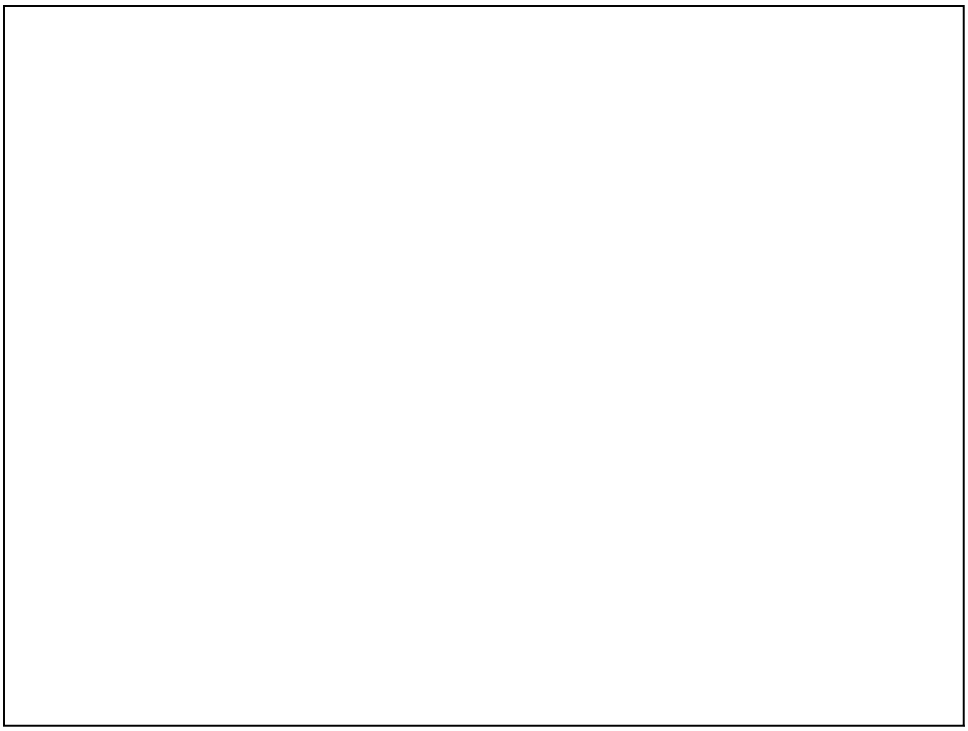


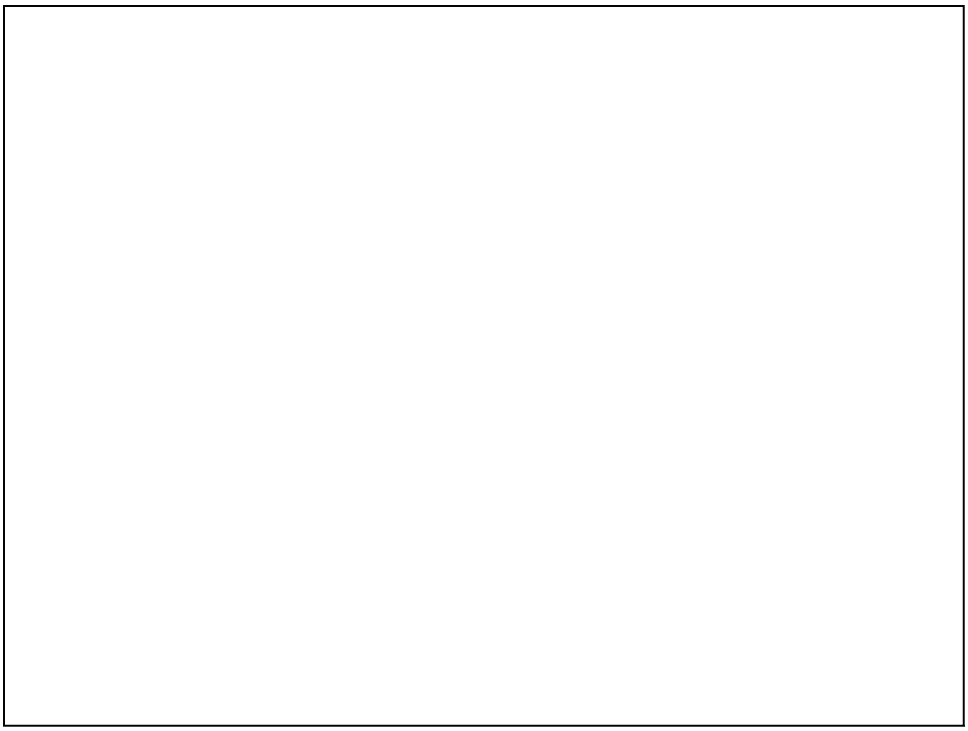


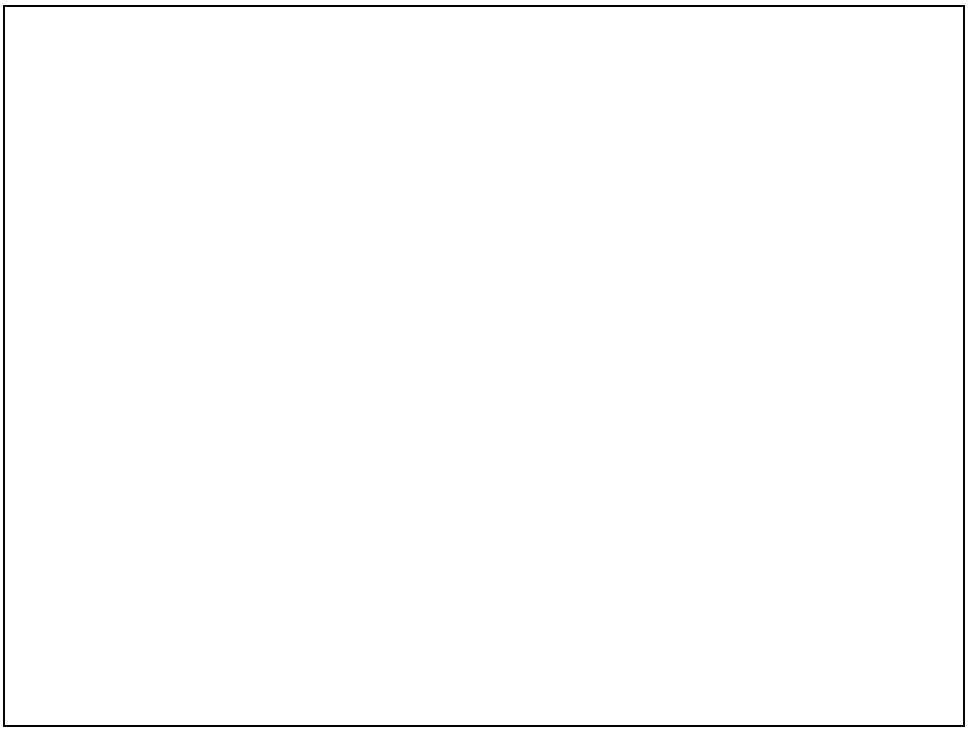


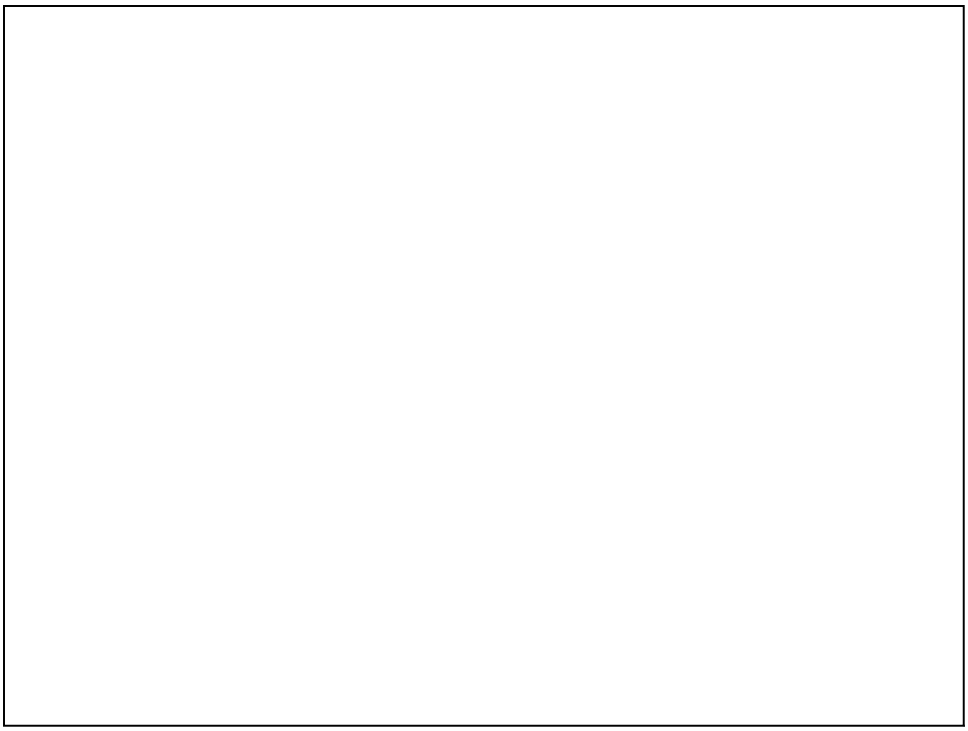


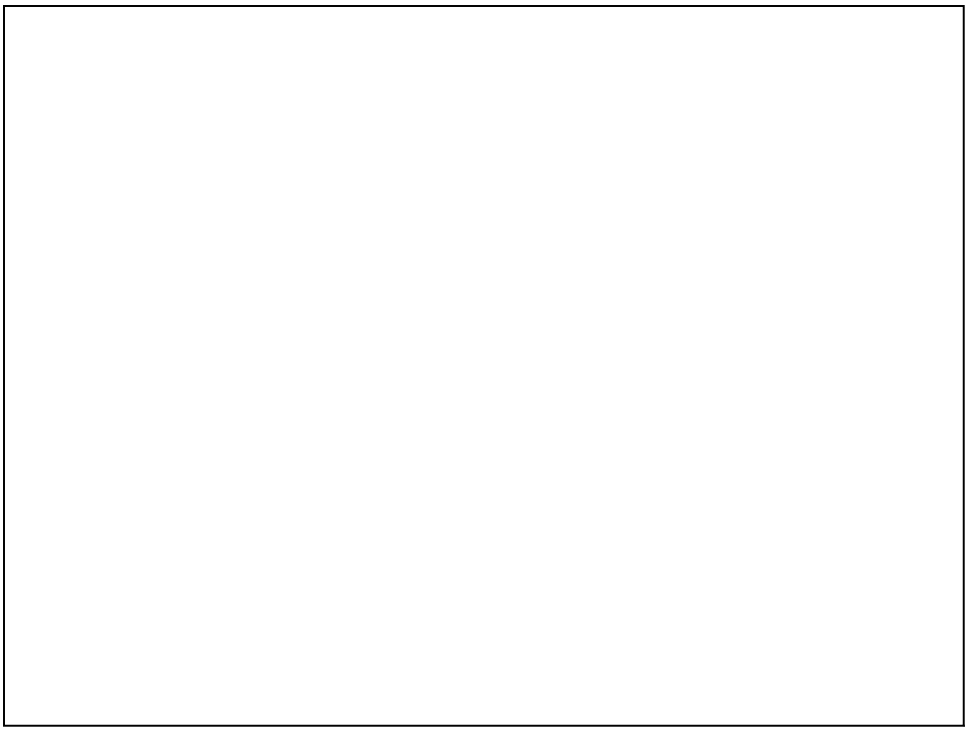


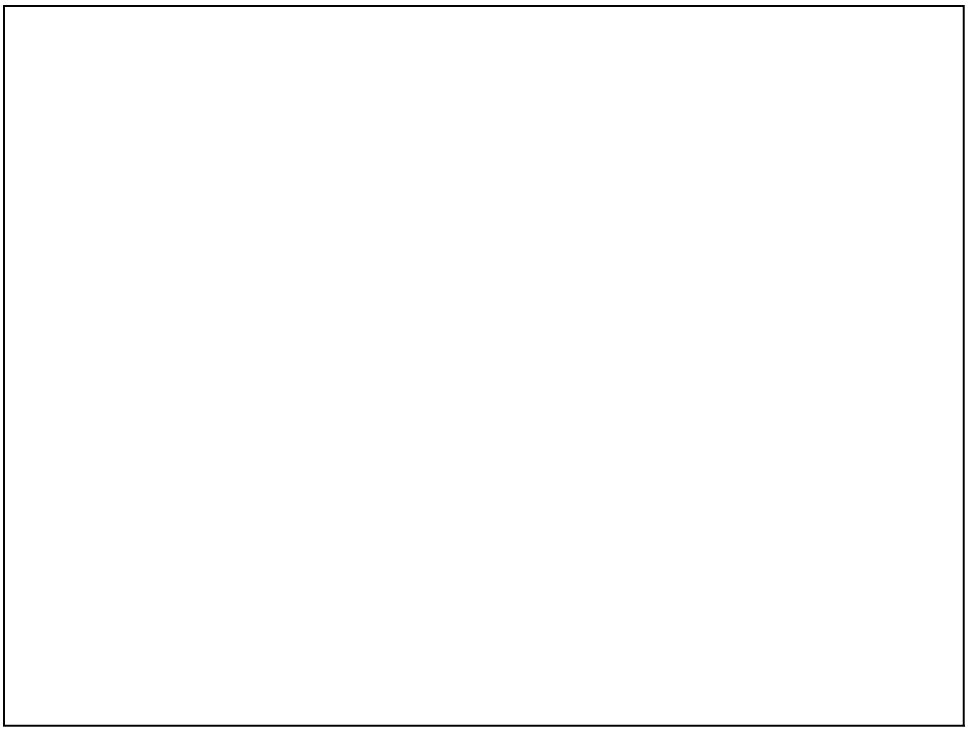


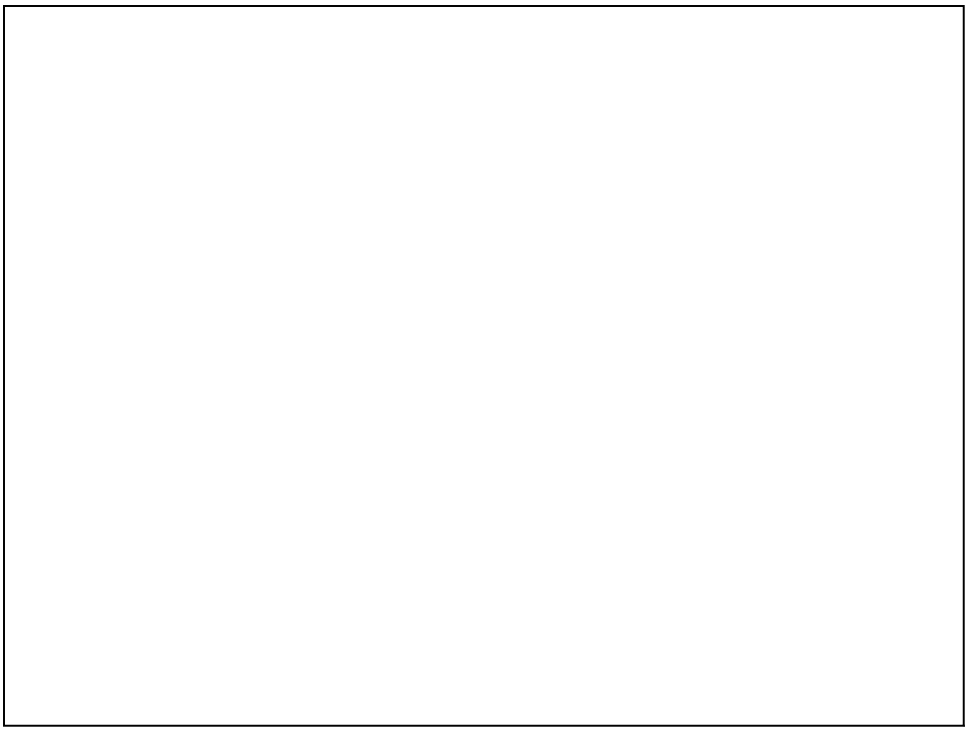


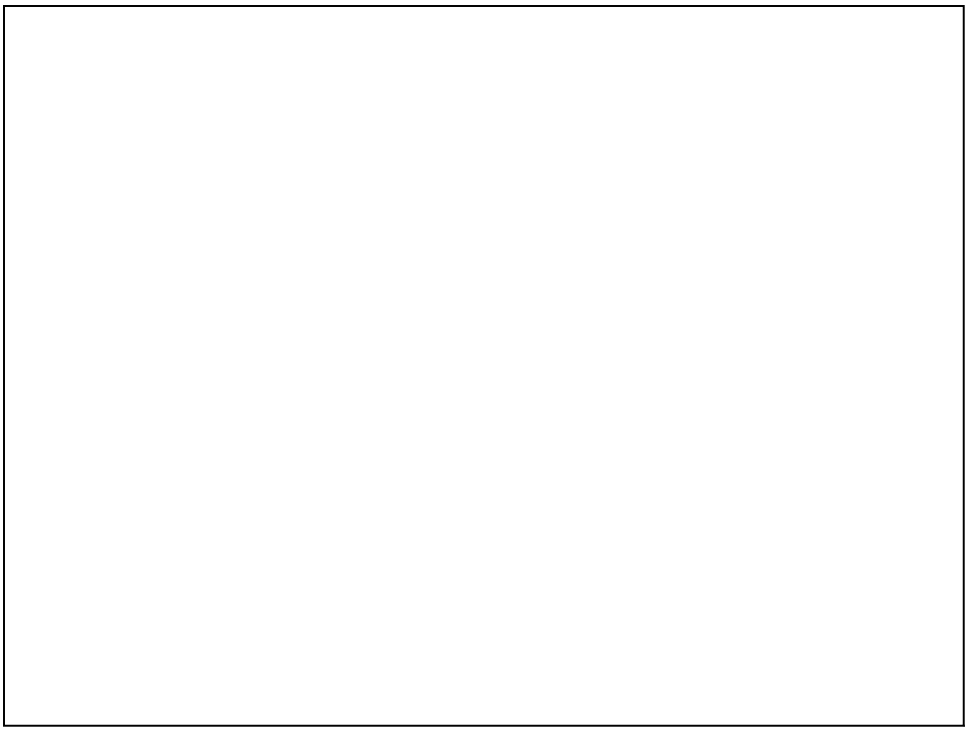


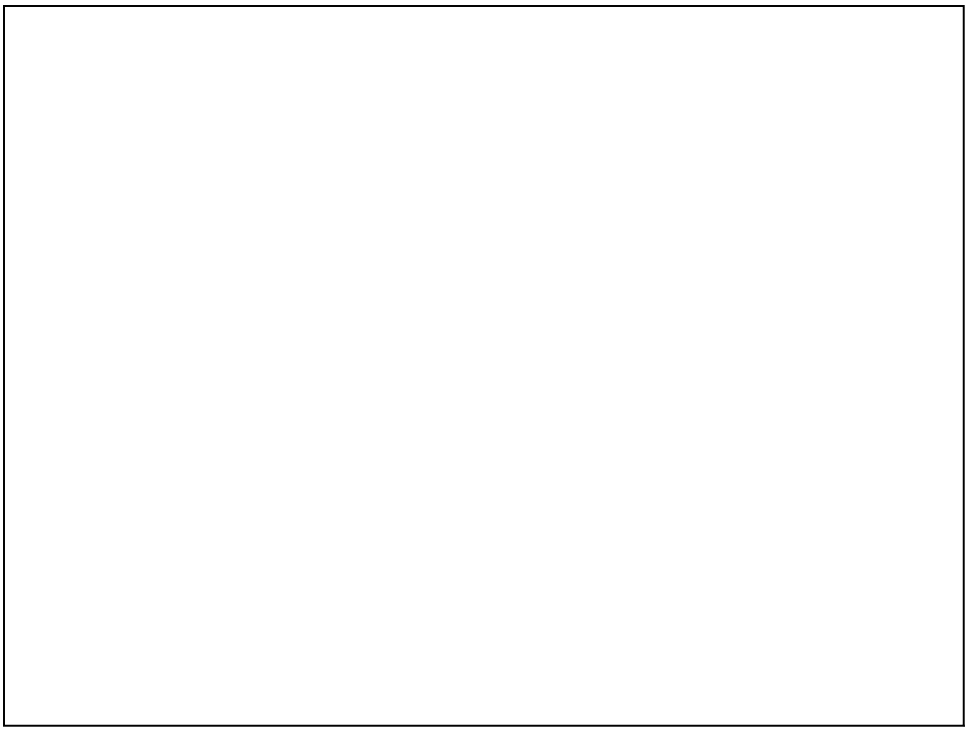


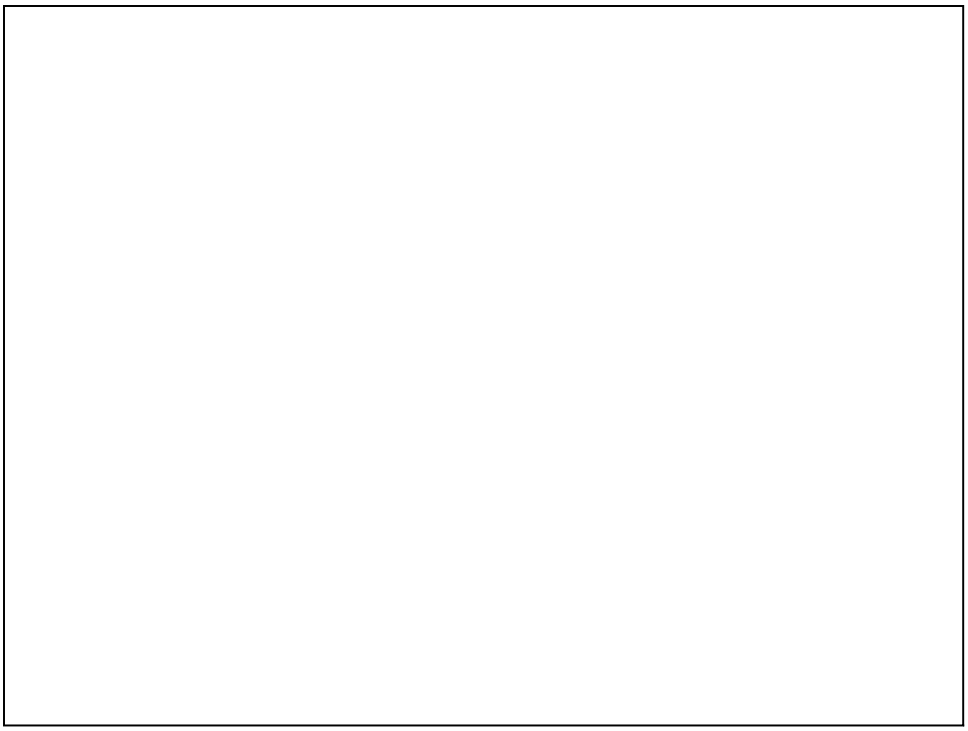


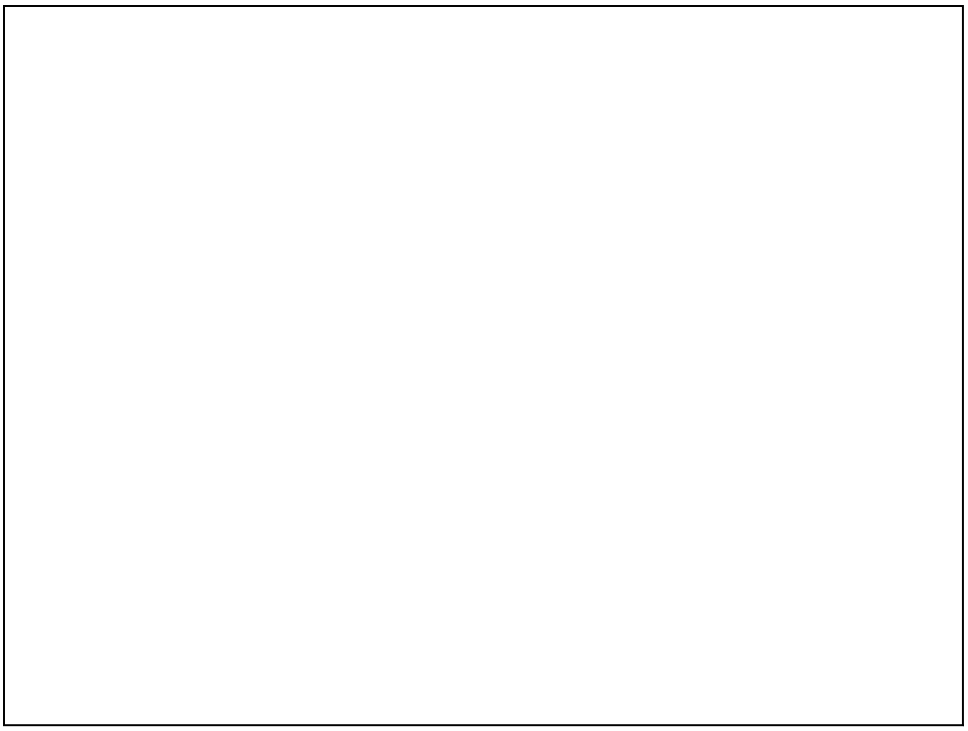


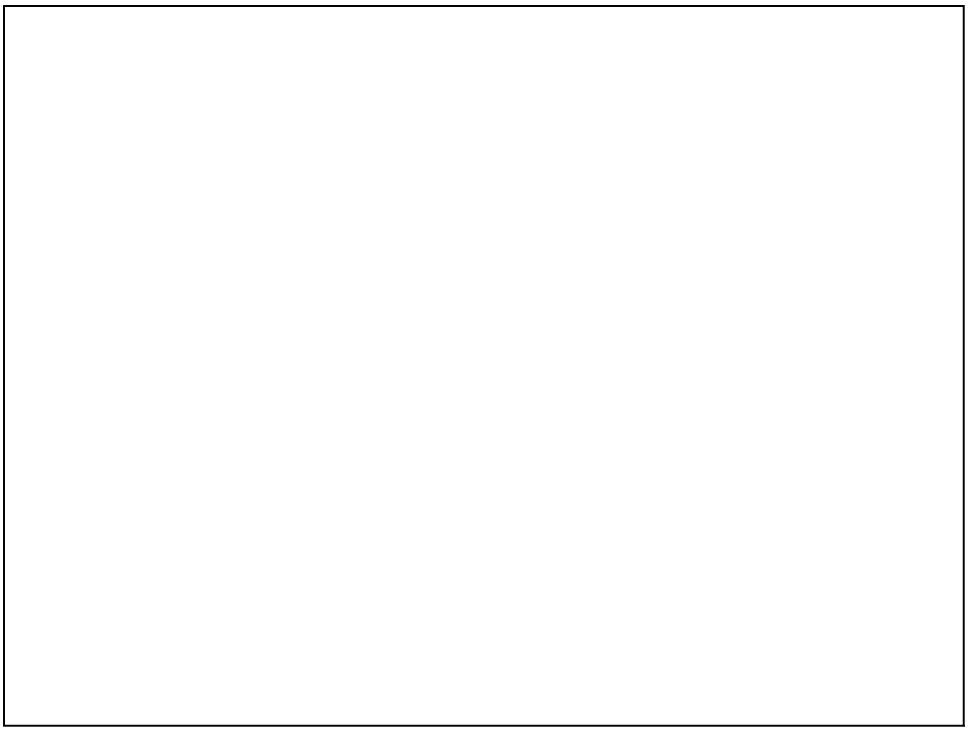


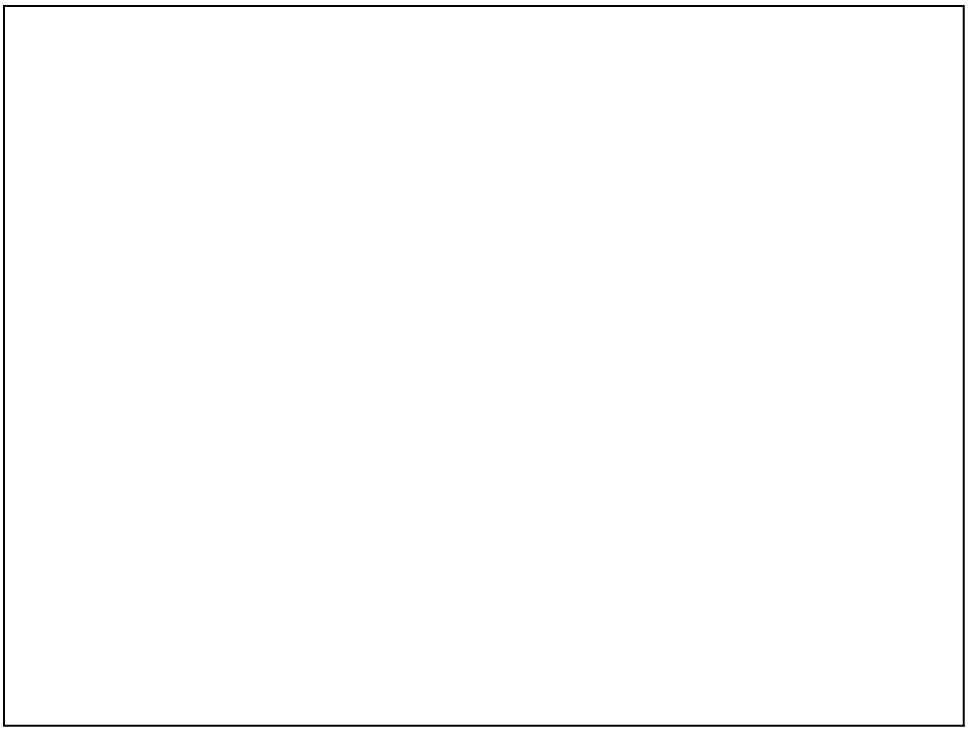


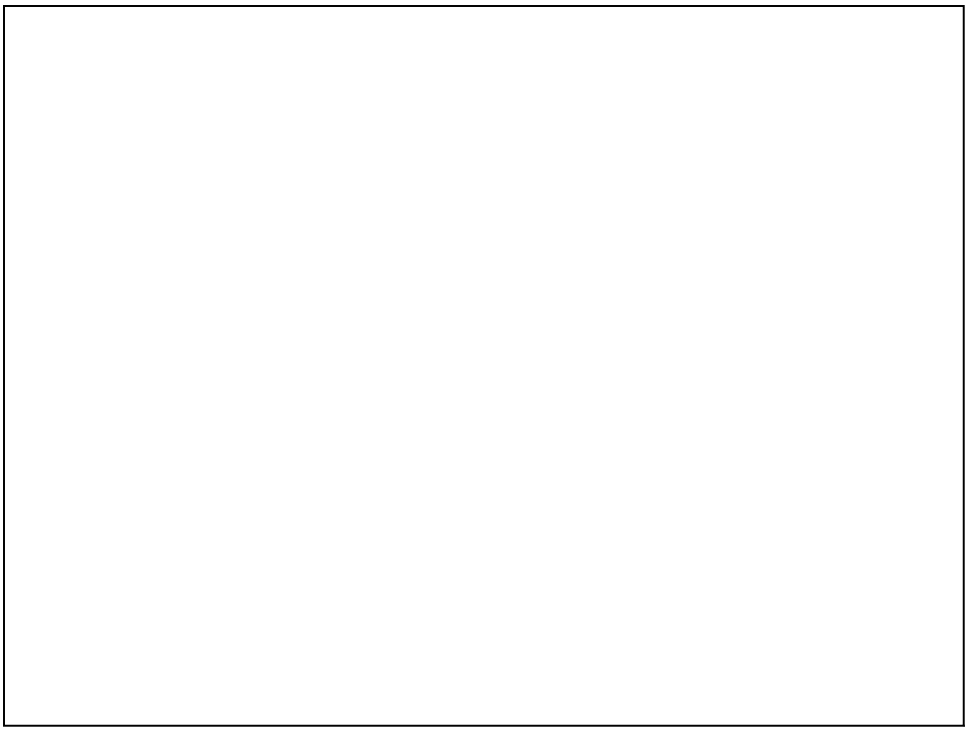


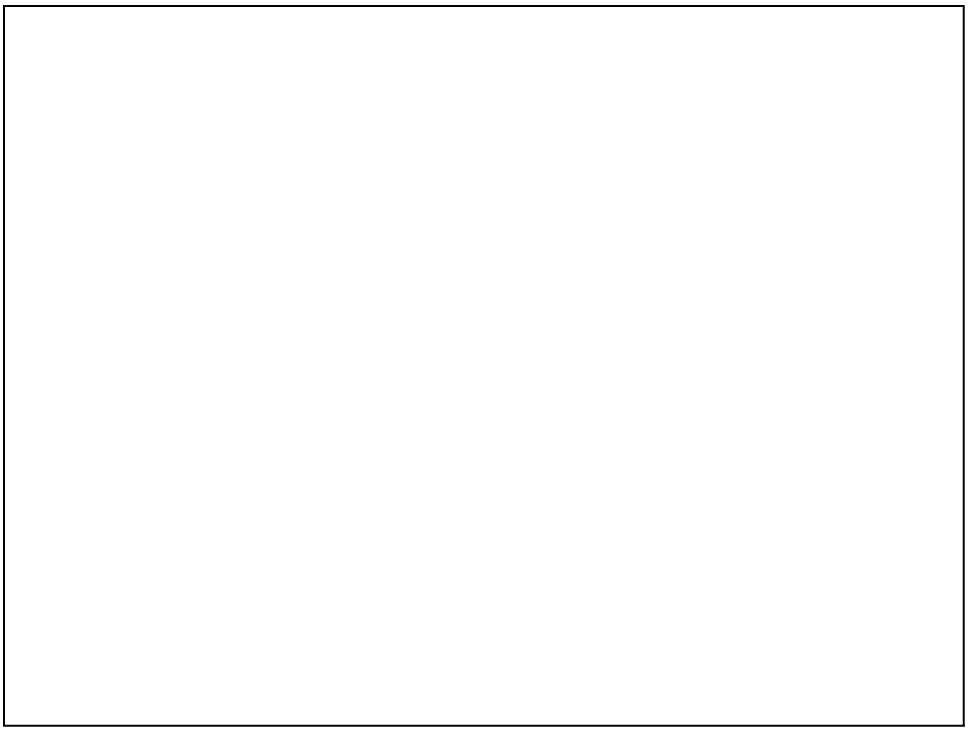


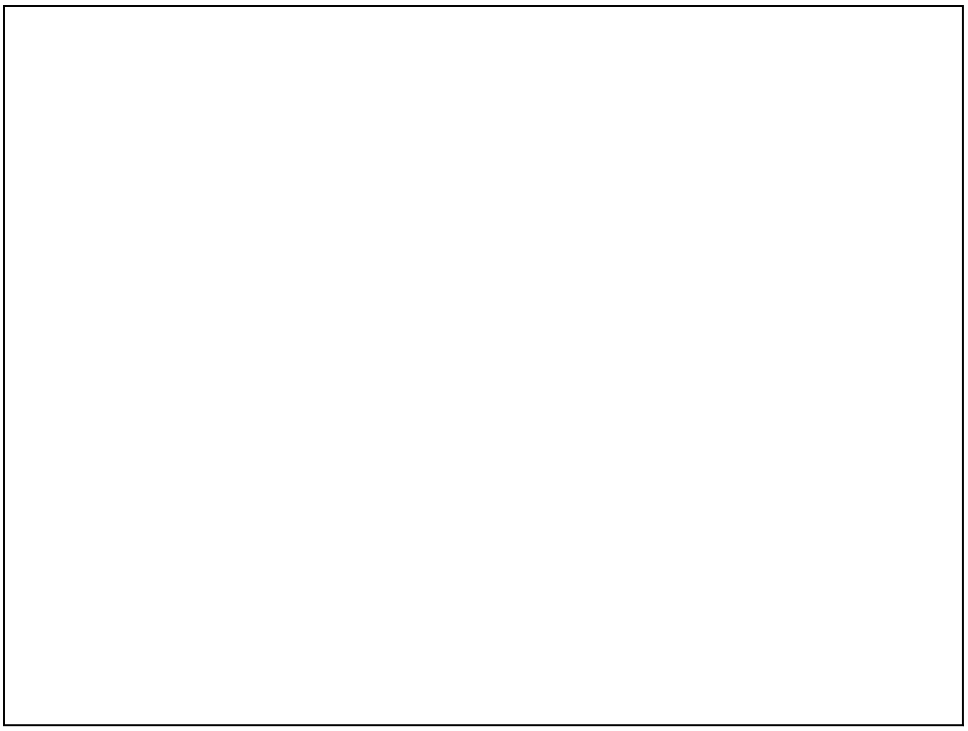


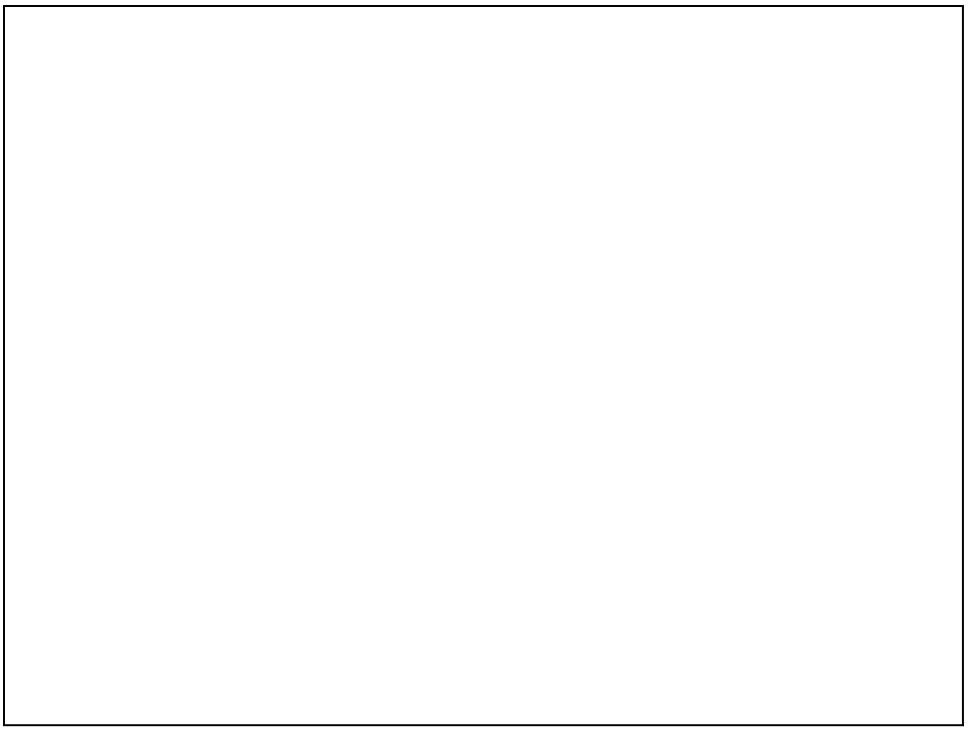


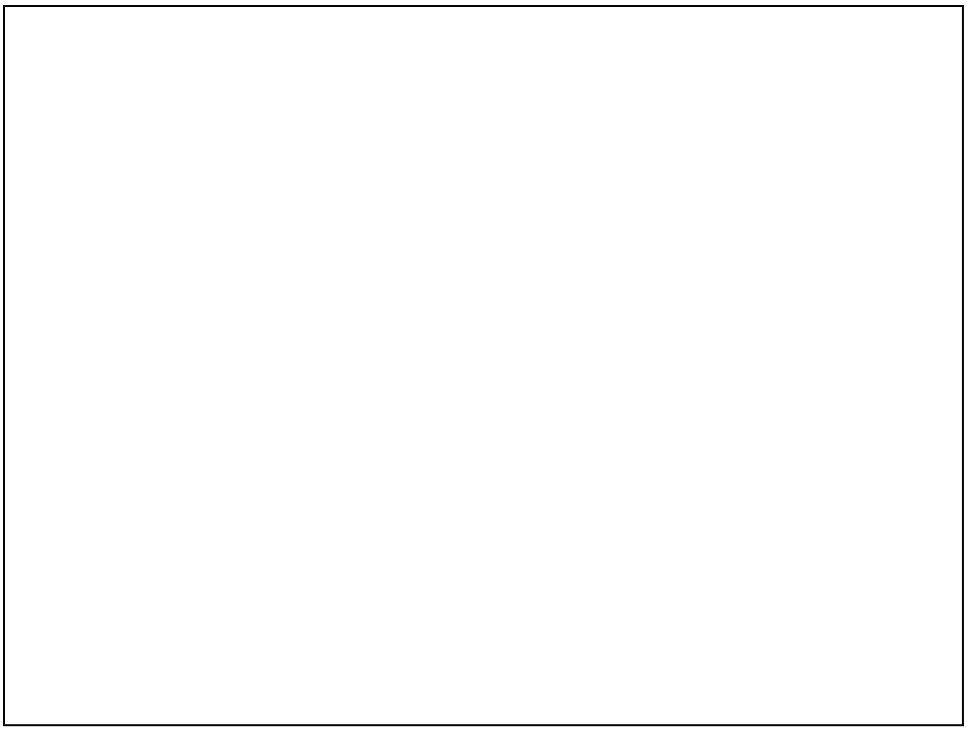


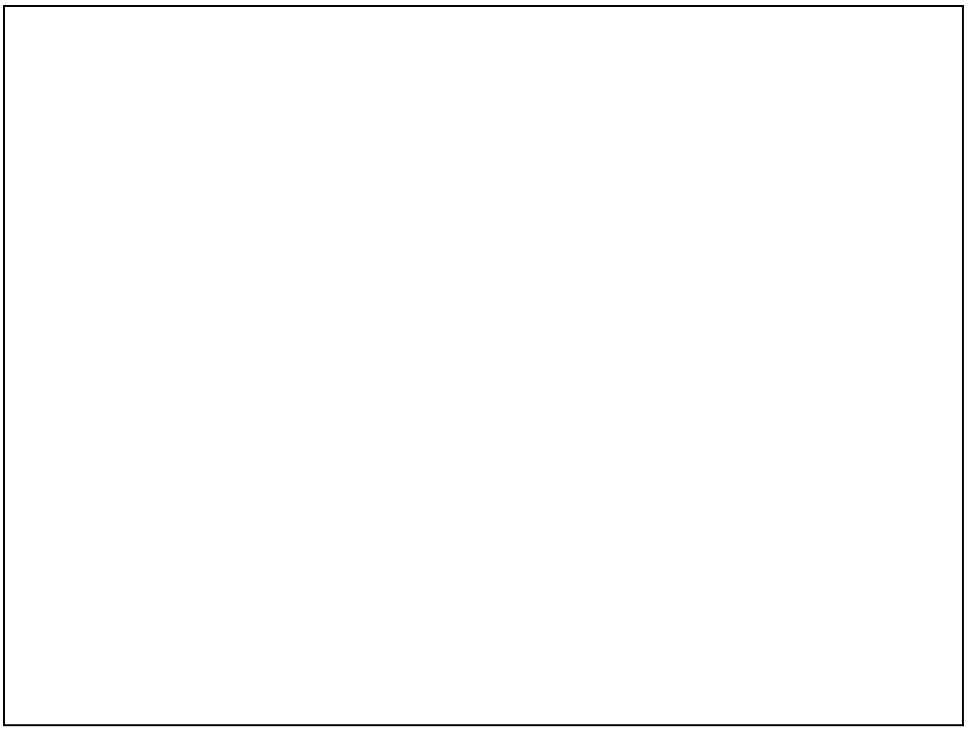












Another Trojan CryptoLocker

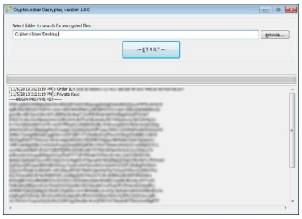
- CryptoLocker September 2013

  Ransomware program that was released September 2013, targets all versions of Windows including Windows XP, Windows Vista, Windows 7, and Windows 8

  Encrypts certain files using mixture of RSA & AES encryption

  CryptoLocker payment program that prompts you to send a ransom of either $100 or $300 to decrypt files ... also displays timer stating that you have 72 hours, or 4 days, to pay ransom or it will delete your encryption key and you will not have any way to decrypt your files.
  http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

Another Trojan CryptoLocker



- This infection is spread through emails sent to company email addresses that pretend to be customer support related issues from Fedex, UPS, DHS, etc.

- These emails contain zip attachments that when opened would infect the computer
- Zip files contain executables that are disguised as PDF files as they have a PDF icon and are typically named something like FORM_101513.exe or FORM_101513.pdf.exe

- Since Microsoft does not show extensions by default, they look like normal PDF files and people open them

RansomeWare WannaCry

- On May 12th 2017, a massive ransomware attack occurred across a wide range of sectors, including
- Health care, government, telecommunications and gas

- To date, WannaCry has spread to over 300,000 systems in over 150 countries

- The countries that appear to be the most affected are Russia and China, probably because of high percentage of legacy software

RansomeWare WannaCry

- WannaCry is a type of ransomware, or extortive malware, that encrypts files, disks and locks computers. The malware demands a ransom of ~$300-600 to be paid to one of three bitcoin accounts within three days in return for decrypting the files.

- WannaCry spreads via SMB, the Server Message Block protocol operating over ports 445 and 139, typically used by Windows machines to communicate with file systems over a network

- Microsoft fixed the vulnerability in the SMB and sent out a patch but not all systems were patched