

# Understanding Malware

An Overview of Malicious SW/Data  
CSC300H Spring 2009

John DiMarco [jdd@cs.toronto.edu](mailto:jdd@cs.toronto.edu)  
<http://www.cs.toronto.edu/~jdd>

## What is Malware?

- **Malware** – prefix “mal” means “bad”, “evil”, “wrong”
  - Malice – evil intent
  - Malevolence – wishing evil on another
  - Malfeasance – wrongdoing
  - Malediction – a curse
- **Malware** – root “ware” same as:
  - software
  - hardware
- **Malware** is software, hardware or data created with evil intent, e.g. with intent to harm or commit wrong.

## Motives for Malware

- Extortion: “Give me money or I’ll take down your very important computers.”
- Theft: “What a nice list of credit card numbers; I’m going shopping!”
- Commerce: “Hmm, that address book is full of valid email addresses, let’s sell them some Viagra!”
- Terrorism: “The imperialist west will weep when we shut down their precious internet!”
- Mischief: “I’m a K001 H@KR D00D!”

## What Can Malware Hope to Achieve?

- **Financial Gain \$\$\$**
- **Access to computer resources**
  - CPU, memory, storage, network connectivity
- **Access to data**
  - Financial information (e.g. credit card numbers)
  - Personal information (e.g. address books)
- **Access to other computers**
- **Confusion, damage, destruction**

## High Stakes

- Networked computer systems are being used for increasingly important things:
  - “...computers aren’t just tools of the bank. Increasingly, they *are* the bank” – Toronto Star, Monday July 19, 2004, p.D1
  - “Why do I rob banks? Because that’s where the money is.” – attributed to Willie Sutton

## Malware is Easier Than Ever

- Microsoft Windows PC monoculture.
- Enormous interconnected international internet: as of 2009, over 600M machines, nearly 26B indexed web pages and about 1.6B people.
- Cellphones increasingly powerful/connected computers.
- Modern software development
  - Hectic pace/time to market, reusable/extensible code.
- **Active content**: mixing code and data

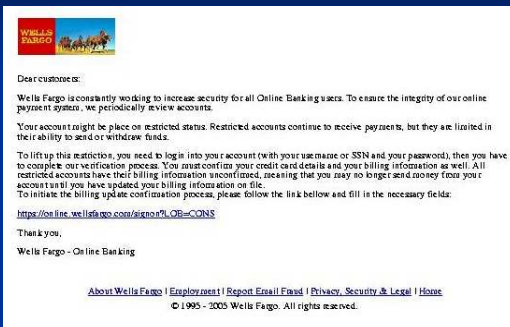
## Malware Goals

- Malware tries to make people and/or their computers do what criminals want them to do.
  - Try to convince people to:
    - Send money, buy a product.
    - Provide confidential information.
    - Provide access to their computer.
  - Access a computer (e.g. PC or smartphone/PDA) in a way that causes it to:
    - Provide access to its data and resources

## Fooling People

- Use a powerful emotion
  - Greed
    - "Nigerian" fraud
    - Most SPAM (e.g. Stock spam)
  - Fear
    - Most phishing
    - E.g. 2005 Chinese SMS scam

## Phishing



Dear customer:

Wells Fargo is constantly working to increase security for all Online Banking users. To ensure the integrity of our online payment system, we periodically review accounts.

Your account might be placed on restricted status. Restricted accounts continue to receive payments, but they are limited in their ability to send or withdraw funds.

To lift up this restriction, you need to log in into your account (with your username or SSN and your password), then you have to complete our verification process. You must confirm your credit card details and your billing information as well. All restricted accounts have their billing information unconfirmed, meaning that you may no longer send money from your account until you have updated your billing information on file.

To initiate the billing update confirmation process, please follow the link below and fill in the necessary fields:

<https://online.wellsfargo.com/signon?LOB=CONS>

Thank you,

Wells Fargo - Online Banking

[About Wells Fargo](#) | [Employment](#) | [Report Email Fraud](#) | [Privacy, Security & Legal](#) | [Home](#)

© 1995 - 2005 Wells Fargo. All rights reserved.

## Invoking Fear

- The motivation
  - Wells Fargo is continually working to increase security... Your account might be ... [put] on restricted status. Restricted accounts... are limited in their ability to send or withdraw funds....
- The hook
  - To lift... this restriction, you need to login to your account... and... complete our verification process.

## The Fraud

- Apparent URL (text highlighted as a URL)
  - <https://online.wellsfargo.com/signon?LOB=CONS>
- Real URL (actual URL the link points to)
  - <http://www.q8555.com/root.php/cgi-pin/wells/wellsfargo-update-information/trust-update-paymnet-account-wells-info/wells%20fargo-account-update-naw-lls/lls-naw-update-wells-info>
- Points to replica of the Wells Fargo web page.
- Criminals hope victims will be so overcome by fear that they will not suspect they are being fooled.

## Defence vs. Fooling People

- Education: do not be naïve!
  - Banks, financial institutions, or other sites **do not** normally send you email asking you to validate your information.
  - Be suspicious of urgent appeals invoking strong emotion.
  - Go directly to the proper institutional site or use the phone number from your bank statements. **Do not use a link or phone number provided by the original message.**
- Spam filters can often catch phishing emails.
- Turn on anti-phishing features of your browser.
- Keep your browser, operating system and antivirus software up to date.

## Fooling Computers

- Exploit a bug
  - E.g. Buffer overflow
    - provide unexpected input that causes program to run arbitrary command specified by attacker.
- Use a stolen credential
  - Fool a computer into thinking that the criminal is an authorized user.

## Buffer Overflow Bug

```
#include <stdio.h>
struct wk {
    char msg[12];
    char cmd[80];
} work;
main(){
    strcpy(work.cmd, "date");    /* Set the command */
    gets(work.msg);             /* Get message to use. */
    printf("%s:\n", work.msg);  /* Output that message */
    system(work.cmd);           /* Run the command */
}
```

## Normal Run

- Input
 

"The Date is"
- Output
 

The Date is:  
Sat Mar 21 13:45:41 EDT 2009

## Exploit Run

- Input
 

" uptime" (12 spaces)
- Output
 

uptime:  
13:50:49 up 3:12, 8 users, load average: 0.0, 0.0, 0.0
- Why? No bounds checking on input, extra data overflows into command field.

## Defending Against Bugs

- Good coding practice.
  - Write the software properly in the first place (bounds checking).
  - Use error-resistant development tools/languages.
  - QA: e.g. fuzzing
- Prompt Security patching
  - E.g. Windows update, up2date, apt-get update

## Stolen Credentials

- Identify "friend" from "foe"
  - Gardening: flowers vs. weeds
  - Warfare: friend vs. foe
  - Herding: sheep vs. wolf
  - Sports: teammate vs. opponent
- Computers: "friend" distinguished from "foe" usually based on *knowledge of information*
- Fraud possible when foe knows information used to identify friend (e.g. stolen credential)

## Defence vs. Stolen Credentials

- Good Security design
  - Multi-factor authentication
  - Two-way authentication
  - Least privilege
- Protection of security credentials
  - Encryption
  - End-point protection
- Tradeoff: security vs. usability

## Networking

- Most machines are now both clients and servers.
  - Peer-to-peer services (net-meeting, various file transfer)
  - Windows sharing and other peer-to-peer file services.
  - Remote access to local printers.
  - Protocols that require connecting back to the client.
  - "Active Content"
- Almost every machine is a server and a client in some way.
- Practically everything is networked. Wireless networking exploding. Portable devices (e.g. cell phones) are small computers.
- Almost everyone is on the network (including millions of potential bad guys!)

## Bluetooth Networking

- Bluetooth on smartphones, PDAs
  - Bluespam: 2005 spam sent by bluetooth to discoverable phones in movie theatres
  - Bluejacking: unsolicited messages for fun to discoverable phones: [www.bluejackq.com](http://www.bluejackq.com)
  - Car Whisperer: Eavesdropping on a bluetooth headset via bluetooth
  - Bluesnarfing: quietly stealing data from smartphone.

## Active Content

- Data that can contain executable scripts can be *very cool*.
- It's hard to make *Active Content* secure.
- The Web is making *Active Content* more important than ever.
- Web *Active Content* consists of data coupled with automatically downloadable programs that execute in your web browser (Java applets, Javascript, Jscript, ActiveX)

## Securing Active Content

- Sandbox: restrict what it can do (like a cage).
  - Unsigned Java applets, javascript/jscript
  - Problem: cages only work when they don't have weaknesses the beast can use to escape.
- Digital Signatures: show who it's from.
  - Signed Java applets
  - ActiveX
  - "Who is it from?" isn't the same question as "What does it do?"
  - "Try it and see" might be too late.

## Defending against Malware

- Several "lines of defence"
  1. **Prevention:** keep Malware off your machine.
  2. **Limit Damage:** keep Malware that gets onto your machine from doing damage.
  3. **Defence:** use antivirus software and keep it up to date.
  4. **Cleanup:** have a reasonable plan to recover from malware.

## Prevention

- Understand enough about computer security mechanisms to use them effectively.
- Keep your passwords secure.
- Keep your system patched and up-to-date.
- Use Firewalls (e.g. built-in)
- SPAM/Phishing: don't propagate your email address. Don't "opt-out" or reply to any SPAM. Use filters.
- Don't necessarily believe persuasive emails asking you to read attachments or visit links.
- Bluetooth: do not make device "discoverable".

## Keep your Systems Patched

- Windows users should regularly run Windows Update (requires Internet Explorer) at <http://windowsupdate.microsoft.com>
- Mac users should run Software Update: <http://www.apple.com/macosex/upgrade/softwareupdates.html>
- Different Linux and BSD distributions have different automatic update mechanisms. Find yours and use it!
- Update your smartphone software.

## Enjoying Active Content Safely

- Surf carefully! Avoid disreputable sites. Turn off Java/Javascript/Jscript/ActiveX for risky sites.
- Keep your browser and OS patches up to date.
- Use a separate (e.g. virtual) computer.
- Don't give unauthorized active content permission to run (not even once!) unless you are certain you know and trust its origin.
- Don't browse the web with Windows 95/98/ME or MacOS 9.x or earlier. Browse only as an unprivileged user on Windows 2000/XP/2003/Vista/7, Linux, MacOS X.
- Consider using less vulnerable web browsers and mail readers for Windows as your default.
- Use the firefox "noscript" add-on for web browsing.

## Firewalls

- A Firewall is a piece of network software or hardware that selectively blocks or permits network traffic based on rules.
- Use built-in Windows XP, MacOS X, BSD and Linux firewalls. Other Windows versions can use free ZoneAlarm from <http://www.zonelabs.com>
- Get a home router with personal firewall for your home internet connection. Turn off uPNP.
- Configure the firewall as tightly as possible, blocking anything you don't need.

## Limit Damage

- Use a modern operating system (e.g. UNIX/NT/MacOSX) that supports per-user authentication.
- Smartphone: Symbian v3 has better security.
- Never do anything as administrator (root) that does not strictly require administrator privileges.
  - Don't browse the web as administrator.
  - Don't read email as administrator.
- Tighten the default security settings on your operating system.

## Tighten Default Security on Your System

- Principle of "least privilege": turn off and/or block all services and features you don't need. E.g. bluetooth.
- Windows, Linux etc. can be configured to be more secure than the default.
  - NSA Information Assurance guides <http://www.nsa.gov/ia/guidance>
  - Windows information at <http://www.microsoft.com/security>
  - MacOS guidelines at <http://www.apple.com/support/security>
  - FreeBSD guidelines at [http://www.freebsd.org/doc/en\\_US.ISO8859-1/books/handbook/security.html](http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/security.html)

## Defense

Use Anti-virus software.

- Includes anti-spyware software!
- Keep virus definitions up-to-date (use the update features of the various packages)
- Use anti-virus software in "resident" mode (runs on your computer and watches for virus activity, like an "auto-immune" system)
- Use SPAM filters.
- Use browser anti-phishing

## Clean-up

- Known malware may have a cleanup utility available from a vendor (e.g. Microsoft) or an anti-virus company.
- But malware, once in, can do pretty much *anything* to your computer:
  - You can't trust what your system utilities tell you.
  - You can't necessarily assume any of your data or software is intact.
- Last line of defense: **backups**. Reinstall your operating system, with patches, and recover your data from backups. Choose a backup from a time before the malware hit, else you will reinstall the malware.

## Software Malware Classified by Propagation

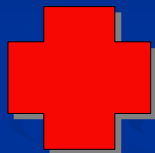
- A piece of malware that silently piggybacks on legitimate software or data, waiting for it to be used is called a **Virus**
- A piece of malware that propagates on its own over a network is called a **Worm**
- A piece of malware that tries to fool a person into running it is called a **Trojan**

## Propagation and Payload

- Malware has both a way to **propagate** and a **payload**.
  - **Propagation**: the part of the piece of malware that is designed to help the malware penetrate computer security and spread from computer to computer.
  - **Payload**: what the malware does with your computer once it's on.
- Some Malware has no payload.

## Virus

- Attaches itself to some legitimate data or software.
- When data or software is used, virus is activated along with the software or data.
- When activated, virus propagates itself to other data and software.



## How does a Virus Propagate?

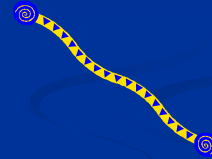
- Looks around for data/software it can write to.
- Attaches itself to beginning or end of data or software, or inserts itself inside.
- Inserts itself into the execution mechanism of the data or software and waits.
  - For data (e.g. MS Word, Excel), adds self as macro.
  - For software, modifies the binary.

## Example: Chernoby/ CIH

- First seen June 1998 in Taiwan: Windows
- Infected Windows .EXE files. 1k in size.
- Widespread through pirated executables.
- Stayed in memory once running, infected any .EXE used. Clever techniques used to avoid changing the size of executables.
- Payload: April 26<sup>th</sup> (some variants the 26<sup>th</sup> of each month), it overwrote most of the hard drive and attempted to overwrite the motherboard BIOS.

## Worm

- Propagates on its own, over a network, from computer to computer.
- When it copies itself onto a computer, it uses that computer to propagate itself to other computers it can access over the network.



## How does a Worm Propagate?

- Looks around for computers on a network
  - Random IP addresses
  - Computers known by the local computer
- Uses or subverts a network service to copy itself
  - Programmed to exploit security flaws in network services.
  - May use network services legitimately to propagate between computers that trust each other (e.g. file sharing).
  - May propagate via email, using any email reader flaws it knows about.
  - May have a list of common known passwords (e.g. default passwords).

## Example: Conficker/ Downadap

- October 2008: Windows
- Exploits RPC buffer overflow in Windows Server Service.
- Dictionary attack on Administrator accounts.
- Uses Windows scheduling to run itself.
- Uses uPNP to circumvent home firewalls.
- Copy to flash memory/remote drives, add to autoplay.
- Payload: used to create a massive botnet, with its own peer-to-peer updating mechanism. Runs a web server on a random port.
- Estimates as high as 15M infected machines by end of January 2009

## Trojan (Horse)

- Name is from Homer's Illiad
- Pretends to be something important, useful, or fun.
- Tries to fool user into running or installing it.



## How does a Trojan propagate?

- Relies on actions by users.
- Uses (sometimes clever) techniques to fool users into running it.
  - "I'm from Microsoft: you need to install this critical patch to protect your system."
  - "Here's a neat game or demo to try."
  - "I'm from your bank: your financial information needs updating, run this software to do so."
- Sometimes fools users into propagating it to other users.

## Example: ecure

- June 2004
- Tries to convince people to download it from a web page and run it. Windows only.
- Payload: Modifies IE home page, puts in a false IP address in the local host file for a large number of sites (making them unbrowsable), shuts down antivirus software running on the machine.

## Virus/ Worm/ Trojans

- Almost all Malware is one of the three, or a combination of two or more.
- Combination Malware could propagate as a virus and a worm, and also email itself as a trojan to unsuspecting users.
- Keys to recognition:
  - Virus: attached to legitimate software or data, activates and copies itself only when software or data is used.
  - Worm: propagates on its own over the network.
  - Trojan: fools people into running it.

## Example: Nimda

- September 18, 2001 – Windows
- Worm:
  - Exploited bug in Microsoft IIS web server.
  - Sent email exploiting automatic flaw in Microsoft Outlook
- Virus:
  - Secretly attached self to web, exploited flaw in IE when browsed.
  - Added itself to .exe, .html and .asp programs on network shares.
- Trojan:
  - Email message tried to convince recipient to run attachment readme.exe (the malware)
- Payload:
  - nimda creates an admin "guest" user
  - shares the "C" drive to the whole world

## Malware Classified by Payload

- Malware can also be classified by what it does once it gets onto your computer (payload).
- Payload can be anything, so only a few common payloads are used for classification.
  - Usually defined by what it does to circumvent your computer's security.

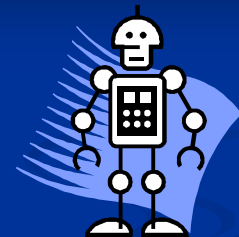
## Backdoors

- Malware opens up a secret way to run commands on your computer (usually over a network) without knowing your password.
- It's like a burglar leaving a basement window unlocked so he can come back later.
- Some worms check for and use backdoors left by other malware.



## Botnet

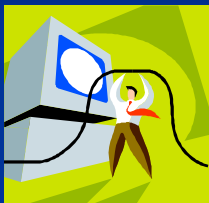
- Malware adds your computer to a giant malware-controlled group of machines
- Malware authors can run anything they want on these machines at any time.





## Sniffers

- Sniffers secretly listen on the machine's network port to capture any passwords that might be going by on the network.
- Network switches can be fooled into show other machines' traffic to the sniffer (e.g. arp cache poisoning).
- Collected passwords can be used by an attacker later to authenticate legitimately to a machine.



## Keyloggers

- A keylogger is malware that records everything you type.
- Attackers are usually most interested in passwords.
- Hardware keyloggers exist: they hook up between the keyboard and the computer.
  - Attacker sneaks it into place, waits, detaches it later and reads the data.



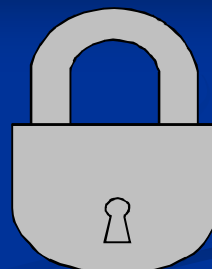
## RootKit

- A Rootkit is a collection of tools for getting Administrator/root access on a machine, and for hiding evidence of malware from the user and/or the system administrator.
- System tools and logs are often modified so that they seem to be working, but they don't reveal the malware running on the machine.
- Anti-malware software disabled, cleanup hindered.



## Encryption Cracker

- A password or encryption cracker tries to break encryption by brute force.
- A dictionary of guesses is used, or random ones are generated, and it tries them one by one to see if they can decrypt the targeted item.
- A worm can get access to millions of machines on the internet, each of which can try different guesses, so brute force decryption can sometimes be feasible.



## Denial of Service

- Denial of Service malware may try to make your computer stop working.
- Denial of Service malware may use your computer to attack another computer on the network, to try to make it stop working.
  - Example: overload a targeted web site (e.g. an antivirus vendor, or e.g. the microsoft update site) with false requests.



## Ransomware

- Special localized form of Denial of Service: encrypts your data, asks for money for the decryption key.
- Rare: risks to the criminal in being caught, e.g. when collecting the funds.
- First widely published example: "AIDS information" floppy, Dec 1989. Criminal captured.
- June 2008: gpcode.ak encrypts hard drive with 1024-bit RSA key, demands purchase of decryptor software.



## Spyware

- Spyware is malware that secretly collects information about your activities (e.g. web sites you browse) and send that information to a third party.
- Some spyware is semi-legitimate: it installs as part of free packages (and there is sometimes small print in software user agreements that says you agree to it)



## Dialers

- Dialers use your modem to call a special phone number without your permission.
- Usually the phone number is a pay-by-the-minute number.
- Your phone bill may contain an expensive surprise.



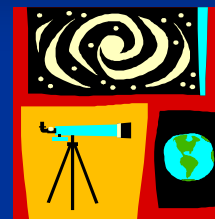
## (Browser) Hijackers

- Hijacker malware rewrites your web browser bookmarks, home page and other data to force you to go to their sites.
- Some forms of this malware are *active content* web pages that try to keep you from leaving a site.



## Port Scanner

- A port scanner is (often legitimate) software that looks for network services running on remote machines on the network.
- Port scanners are sometimes included in a malware payload so that malware (especially worms that know how to exploit a vulnerable network service) can look for other machines running a vulnerable version of that service.
- Stealthy versions exist that try to avoid alerting the remote machine that it is being scanned.



## Malware (PC/ Server) end 2008

- Malware of all types rife in Windows, increasingly commonplace on Macs, Linux
- Trends
  - Flash drive propagation (autorun/autoplay)
  - Targetted attacks using bug-exploiting attachments
  - Massive bot-nets (e.g. Conficker/downadup)

## Smartphone Malware end 2008

- Symbian (Nokia)
  - 12+ extant malware, some active; bluetooth and MMS propagation.
- Windows Mobile (many vendors)
  - A few examples, some active.
- PalmOS
  - A few old (2000) examples.
- iPhone
  - One known trojan
- Blackberry
  - Proof-of-concept but no known exploits.
- Google Android
  - No malware yet.

## Future

- Smartphone problem only beginning
- Criminal subculture preventing massive exploitation (e.g. nimda) lest best flaws be patched aggressively. Growth in "targetted" vs. "blanket" attacks in hopes of patch delays.
- Malware increasingly non-destructive. More money in long-term compromise.