Malware = Malicious Software

Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim.

Quoted from Guide to Malware Incident Prevention and Handling, NIST Tech Report 2005
Terminology

• Virus
• Worm
• Trojan
• Rootkit
• Spyware
• Bots
• Backdoor
• Adware
• Ransomware
• Etc.
Virus

The term is invented by *Fred Cohen* in 1984

Virus

A program that can *infect other programs* by modifying them to include a, possibly evolved, version of itself

Virus Structure

Malicious

Original

infectOtherFiles();
if trigger-cond then action();
else ()
goto Original;
A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.

- Wikipedia
Morris Worm

Exploited a buffer overflow vulnerability in fingerd

```c
int main(int argc, char* argv[]) {
    char line[512];
    /* omitted ... */
    gets(line); /* Buffer Overflow! */
    /* omitted ... */
}
```

This single line allowed the Morris Worm to infect 10% of the Internet computers in 1988
Nov. 2, 1988

The first computer worm (called Morris Worm) was born.

Robert Tappan Morris
Creator of the worm
Cornell graduate
Tenured professor at MIT now
Worm Propagation Model

\[ \frac{dT(t)}{dt} = \beta I(t) S(t) \]

Where

• \( I(t) \) is a number of individuals infected as of time \( t \)
• \( S(t) \) is a number of susceptible individuals at time \( t \)
• \( \beta \) is the contact rate (pairwise rate of infection)
• \( N \) is the size of the population, i.e., \( N = I(t) + S(t) \)
Worm Propagation Model (cont’d)

Image taken from The Monitoring and Early Detection of Internet Worms, *IEEE/ACM Transactions on Networking, 2005*
Trojan (Trojan Horse)
Trojan (Trojan Horse)

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes it.

- Computer Security - Principles and Practice, Stallings
How Trojans Spread?

• Social engineering
  - E-mail, social network, phishing, etc.

• Drive-by download
Spam E-Mail

• Advertisements (including money mule jobs)

• Trojan horse can be attached
Phishing

• Disguising as a trustworthy entity, and obtain private info

• Fishing ~ Phishing
  – Both use a bait to catch a victim 😊
Dear iTunes Customer!

Your iTunes account has been frozen because we are unable to validate your account information. Once you have updated your account records, we will try again to validate your information and your account suspension will be lifted. This will help protect your account in the future. This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

Get Started

If you need help left by clicking the Help link located in the upper right-hand corner of any Apple page.

Sincerely,

Apple Inc

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131.
From: "Bank of America" customerservice@bankofamerica.com
To: “Jane Smith” jane-smith12@gmail.com
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Required

Dear Customer,

At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, sign up now. New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department
Spear Phishing

Phishing attempts directed at specific individuals.

- Wikipedia
From: UDEL HR <hrmoployee payroll@udel.edu>
Date: August 13, 2015 at 12:48:29 PM EDT
To: <removed>
Subject: Your August 2015 Paycheck

Hello,

We assessed the 2015 payment structure as provided for under the terms of employment and discovered that you are due for a salary raise starting August 2015.

Your salary raise documents are enclosed below:

Access the documents here

Faithfully

Human Resources

University of Delaware
Confirm account ownership

Google ArAutoBot <acccgmaiiautobot@gmail.com> 6:38 AM (24 minutes ago)

to me

Hello Hatechnion,

It's been a while since you last changed your password.

Please confirm account ownership by clicking on this link:

https://www.google.com/ConfirmAccount?Email=hatechnion@gmail.com

Thanks,

The Google Team.
Kevin Lucas <ke3luc@gmail.com>
to me

Dear Sang Kil Cha

I am Kevin Lucas a solicitor at law and a personal attorney to late client that shared same last name with you, and he's work with an oil company (company name with held) here in West Africa, Precisely Nigeria. My late client his wife and only son dead in a auto crash, date I have made several attempt to locate any of his relative, all effort to know avail I found in his dairy your name and email so i decided to write you if you can help locate any of this relatives.

Awaiting to hear from you.

Kevin Lucas Jr
Watering Hole Attacks

1. Attacker profiles victims and the kind of websites they go to.

2. Attacker then tests these websites for vulnerabilities.

3. When the attacker finds a website that he can compromise, he injects JavaScript or HTML, redirecting the victim to a separate site that hosts the exploit code for the chosen vulnerability.

4. The compromised website is now “waiting” to infect the profiled victim with a zero-day exploit, just like a lion waiting at a watering hole.
Watering Hole
Bot (Zombie)

A program activated on an infected machine that is activated to launch attacks on other machines.

*Botnet* is the collection of bots.

- Computer Security - Principles and Practice, Stallings
Command and Control (C&C) Server

- Use existing protocols such as IRC and HTTP
  - E.g., each bot connects to an IRC server, and join a specific channel

- Use custom protocols
  - E.g., qbot

Each bot needs to know a specific IP address (or a channel name) of the C&C server
DNS-based C&C Server

• Use a custom domain name generation algorithm

• Each bot randomly generates a series of domain names to be used

• C&C server can be reached unless the generation algorithm is revealed by a defender
P2P-based Botnets

Each bot is a command distribution server as well as a client.

• How about bots that are behind firewall?

• When a bot wants to join a botnet, it needs to know the IP of at least one node in the botnet that can take incoming connections
  – Bootstrapping

• Peer poisoning possible!
  – Having a fake node that provides fake list of IPs
Spyware

Software that collects information from a computer and transmits it to another system.

- Monitoring keystrokes (keylogger)
- Monitoring screen/camera data
- Monitoring network traffic
Rootkit

A collection of utilities that enable access to a compromised machine. A rootkit often masks its existence and other malware.

• Example
  – `ps` command does not show the rootkit process
  – `ls` command does not show malicious files
Logic Bomb

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

- Wikipedia
Sony BMG Copy Protection Rootkit

Over 22 million CDs (2005-2007) included malware
• A rootkit that hides the existence of the malware
• A logic bomb that interferes CD copying
Dropper / Downloader

A program that installs other malware on a target machine.

• The malware code can be contained within the *dropper*
• Or can be downloaded by the *downloader*
Backdoor

Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.

- Computer Security - Principles and Practice, Stallings
Adware

Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.

- Computer Security - Principles and Practice, Stallings
Benign vs. Malicious Adware

The image shows a software interface with a file named "BAND-IP-SETUP.exe" and a file size of 3,669 MB. The interface includes options to download or cancel the download. The advertisement promotes a game called "MVP" from Naver Games, offering a prize of 5,000,000 won for downloading the game and watching a video. The download progress is shown as 0% complete.
Benign vs. Malicious Adware
Ransomware

• Cryptovirus (Cryptoviral extortion attack)
  - Cryptovirology: Extortion-Based Security Threats and Countermeasures, *Oakland 1996*

• Cryptography also has negative usage!
Cryptoviral Extortion

1. Attacker generates a key pair and places the corresponding public key in the malware
2. Malware generates a random symmetric key and encrypts the victim’s data with it
3. Malware uses the public key to encrypt the symmetric key, and “securely” delete the original symmetric key.
4. Show the victim a message with the encrypted symmetric key how to pay the ransom
5. When the payment received, the attacker deciphers the key and send to the victim
Example: CryptoLocker
How to Defend against Cryptovirus?

- Typical anti-malware can help
- Access control to cryptographic tools (APIs)
- Theoretical fault-tolerant model
  - How to Withstand Mobile Virus Attacks, *PDOS 1991*
APT (Advanced Persistent Threat)

Not a new type of malware, but combination of intrusion techniques

• Advanced: advanced intrusion technologies and malware
• Persistent: progressively and stealthily attack the target until the target is compromised over an extended period

• Example: Aurora, Stuxnet
The Arms Race (or Weapons Race)

Attacker vs. Defender