Malware

Malware

- Spam
- Phishing
- Trojan Horse
- Rootkit
- Worms
- Denial of Service Attacks
- Botnets
- Cyber Crime Organisations

Spam

Spam

- Use of electronic messaging systems (often email) to send unsolicited bulk messages indiscriminately.
- Don’t give your email address away.
- Don’t put it on Web sites. (They are trawled for email addresses).

Other types of Spam

- Instant messaging
- Newsgroups
- Web Search Engine Spam
- Blog Spam
- Mobile Phone
- Online game messaging

Blog Spam

- Automatically posting random comments or promoting commercial services to blogs, wikis, guestbooks, or other publicly accessible online discussion boards.

Spam Detection - Integrity Analysis

- Examines the structure of a message looking for
  - Invalid headers
  - Suspicious time stamps
  - Invalid time zones
  - Text patterns indicative of spam, such as opening text in upper case

Spam Detection – Heuristic Analysis

- Examines the message using heuristics (rules of thumb)
  - "Free offer"
  - "Act now to save"
- An overall measure is determined and if above a certain score, the message is marked as spam.
- Often use Baysian classification.

BlackLists and WhiteLists

- Block messages from previously identified spam sources.

Phishing

Phishing

- Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
- Often done by email

Phishing

- User often asked to enter sensitive information in a form and submit it.
- Often the fake web site is made to look like the real one.

Example

- Email
- Download a form and update details
- The form downloads images etc. from the actual (banks) website, so its looks authentic.
- The form submission is to the attackers server obviously.
- After form submission, there is a redirect to the bank's web site.

Spear Phishing

- Directed Phishing attack.
- That is, the bogus email is only sent to customers of the faked bank.

Trojan Horse

Trojan Horse

- Software that appears to be legit before install or run.
- But steals information or harms the system.
- [Possibly in addition to the expected function.]
- The term is derived from the Trojan Horse story in Greek mythology.

Example

- A program that pretends to be virus removal software but actually installs viruses.

Possible Functions

- Use of the machine as part of a botnet.
- Data theft (passwords, credit card information)
- Installation of software, including third-party malware
- Downloading or uploading of files on the user's computer
- Modification or deletion of files

Possible Functions

- Keystroke logging
- Crashing the computer
- Anonymizing internet viewing
  - Security faults in browsers allowing the host to be used as an anonymizer proxy.

Rootkits

Rootkits

- Has privileged access to a computer.
- Hides its presence from administrators.
- Difficult to find as it has control of the software utilities that are used to try and find it.

Sony BMG copy protection rootkit scandal

- "In 2005, Sony BMG published CDs with copy protection and digital rights management software called Extended Copy Protection, created by software company First 4 Internet.
- The software included a music player but silently installed a rootkit which limited the user's ability to access the CD."

Greek wiretapping case 2004–2005

- Involved the illegal tapping of more than 100 mobile phones on the Vodafone Greece network belonging mostly to members of the Greek government and top-ranking civil servants.
- The intruders installed a rootkit that a telephone exchange.

Greek wiretapping case 2004–2005

- Patched the memory of the exchange while it was running.
- Enabled wiretapping.
- Disabled audit logs.
- Patched the commands that list active processes and active data blocks.
- Modify the data block checksum verification command.

Greek wiretapping case 2004–2005

- The Rootkit was discovered when a faulty update was installed, messages were undelivered, and a fault report generated.
- The perpetrators were never found.

Worm

Worm

- Self-replicating malware, which uses the network to send copies of itself to other nodes.
- Tend to harm the network.

Denial of Service

Denial Of Service Attacks

- Saturate the target machine with HTTP requests so that it can't respond to legitimate traffic
- Or responds so slowly as to be rendered effectively unavailable.

DOS Attacks

- Betting organisations have been attacked coming up to a big pay day.
- Usual motive for the attacker is extortion, i.e. the attacked pays to get the web site back up and running.

DDOS

- Denial of Service attacks from different hosts.
- Often using botnets.

BotNets

Resources

- Attack of the Bots
  - http://www.wired.com/wired/archive/14.11/botnet_pr.html
- Know Your Enemy : Tracking Botnets
  - http://old.honeynet.org/papers/bots/

BotNets

- Bots – tools for taking control of computers.
- BotNet - a collection of computers compromised by bots
- Botnet Herder - manages and controls the botnet.
- The botnet herder may not be the person who created the botnet originally. Botnets are traded and stolen.

Uses of Botnets

- Conducting distributed denial of service (DDoS) attacks
- Distributing spam
- Launching phishing attacks
- Conducting click fraud
- Google AdSense abuse

Uses of Botnets

- Sniffing Traffic
  - Stealing personal information
  - Stealing other botnets
- Distributing new malware.
- Installing Advertisement Addons and Browser Helper Objects (BHOs)
- Manipulating online polls/games

Spam

- Maybe 70% of spam sent by botnets!

Click Fraud

- Rent a Botnet.
- Install a specialized click-fraud tool.
- Replay HTTP GET requests often without even using the Web browser.
- Google settled in a click fraud case for $90m.

Stealing Personal Information

- Monitor key strokes to collect passwords.

Bot Building Blocks

- Often use IRC (Internet Relay Chat) for communication between bots and herders.
- Bots duplicate and spread using identified vulnerabilities in network stacks.
- Use HTTP and FTP to download other programs, and upload information.

Defense

- Shutdown the C&C (command and control) server.
- Some bots don't have a centralized C&C center.
- They use a peer to peer model.

Cybercrime Organizations

Russian Business Network (RBN)

- A cybercrime organization.
- Specializing in and in some cases monopolizing personal identity theft for resale.
- Offers web host to all sorts of illegal/semi-legal activities.
- Such as downloading fake anti-spyware software.

MPack

- PHP based malware kit.

- MPack is sold as commercial software (costing $500 to $1,000 US), and is provided by its developers with technical support and regular updates of the software vulnerabilities it exploits.

Storm Botnet

- A Botnet linked by the Storm worm.
- Estimates range from ¼ million to 50 million PC effected.
- So called because of the (initially) "storm" related subject lines in emails.
  - "230 dead as storm batters Europe"