IT2775 Operations Security

Malware Defence and Management

NANYANG POLYTECHNIC

Objectives

- Need for Malware Defence
- Key Concept for Malware Defence
- Malware Management
  1. Detection
  2. Prioritisation
  3. Containment
  4. Eradication
  5. Recovery

malware

/ˈmalwɛː/

noun

software which is specifically designed to disrupt, damage, or gain authorized access to a computer system.

Need for Malware Defence

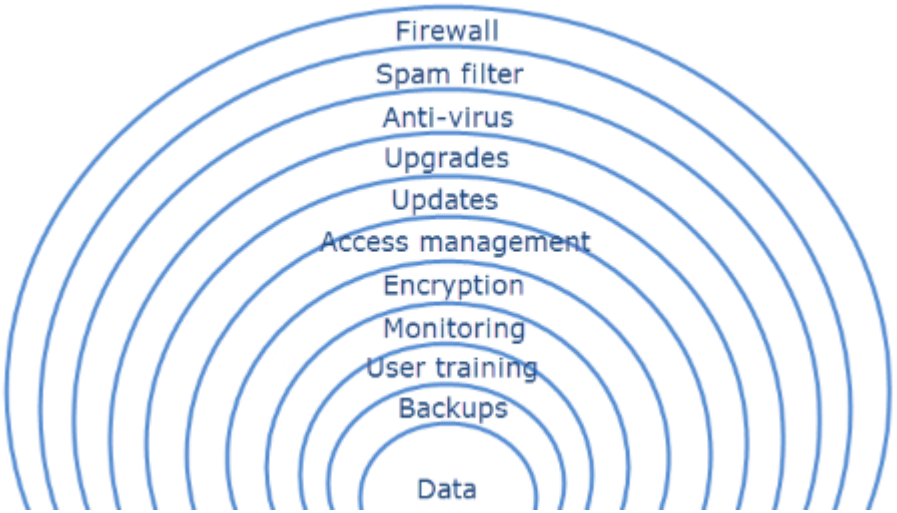
- Prevalence of malware and malware incidents highlights the need for proper malware defence and management.
- Difficulties of malware defence and management lie in the following:
  - Difficult to identify existence of malware
  - Largely non-physical, difficult to response
  - Types of malware is dynamic, dependent on malware creators' creativity.

Malware Defence (Key Concept)

- Need to utilize risk management techniques to build an effective malware defence mechanism within the organization boundaries.
- Defence-in-depth is a very relevant concept in malware defence.
  - Not one single technology is able to sufficiently prevent malware.
  - Malware changes with time, exhibiting different behaviours.

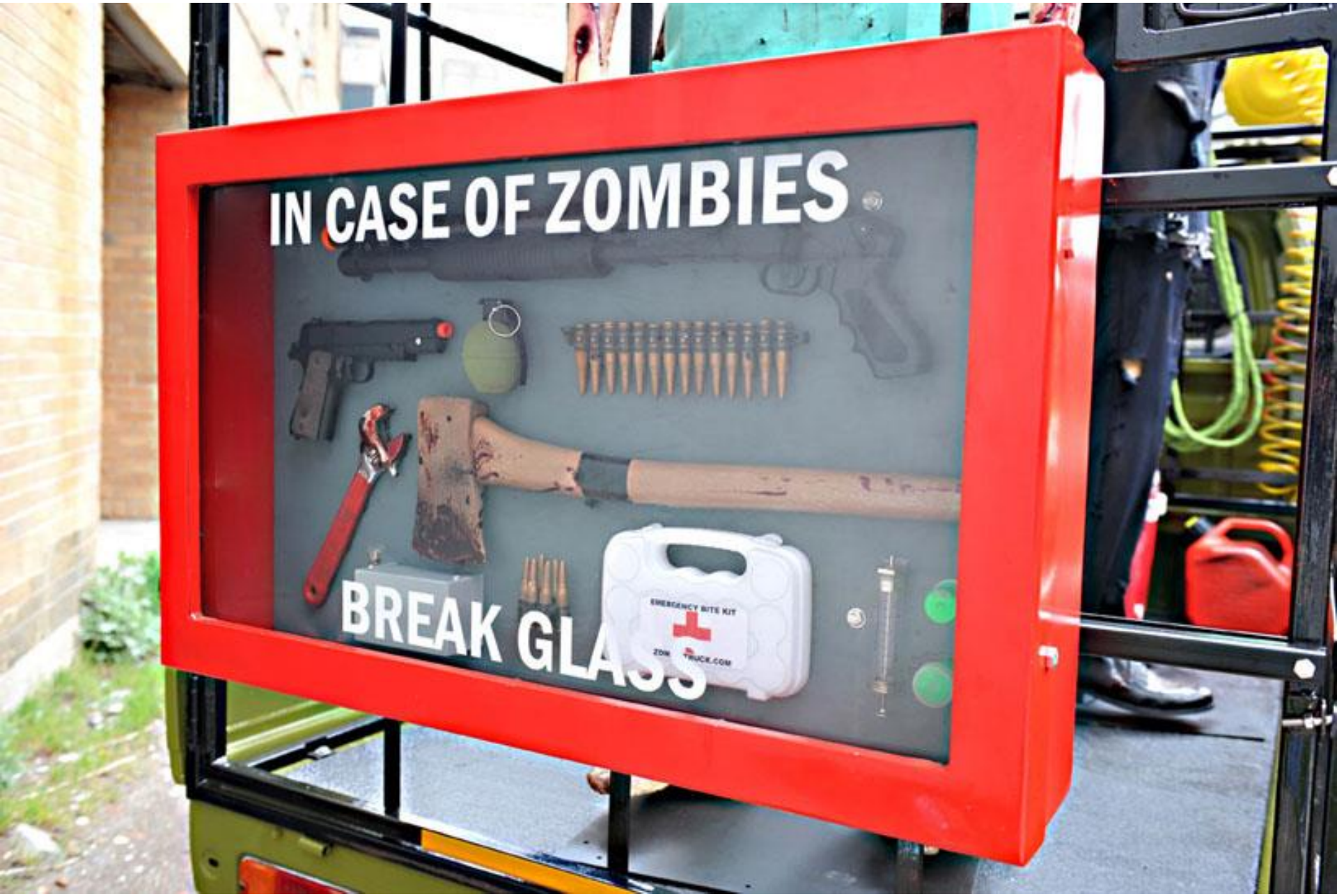
Malware Defence

- Utilising multiple and different layers, to manage the risk level of malware infiltrating the organization's networks.
  - Need to implement different protections at various layers within the infrastructure.
  - Not advisable to duplicate same layer (e.g., having more than 1 firewalls), which is not cost effective.



Malware Management

- Need to prepare for malware incidents even after implementing various preventive controls.
- Key is to ensure required resources are available.
  - Personnel need to have relevant malware skills, e.g.:
    - Infection methods, Detection tools, Broad understanding of IT, Programming etc.
  - Ensure resources are themselves not affected by regular malware infiltration techniques.
    - Preferably through hardware controls, rather than software. Why?


IN CASE OF ZOMBIES
BREAK GLASS
EMERGENCY BITE KIT

Malware Management

1. Detection
2. Prioritisation
3. Containment
4. Eradication
5. Recovery

1. Detection

- Early detection is important
  - Minimize spread of infection.
- Signs of malware presence:
  - Precursors (Signs that malware may attack in the near future)
    - Includes malware advisories or security tool alerts
  - Indication (Signs that malware incident may have occurred or is in the midst of occurring)
    - Includes ‘common’ signs like web server crashes, slow response time from systems, systems rebooting, large number of bounced/suspicious emails
    - Problem is that most indications may have implications other than malware.

1. Detection

- Identify characteristics of malware
  - Incident handlers should obtain information from malware detection tools such as anti-virus programs, IDS, etc.
  - Additional sources include :
    - Firewall and router logs
    - Log files from email servers
    - Packet capture files from sniffers, network traffic recording tools
  - Have access to antivirus tool vendors, local CERT website (https://www.us-cert.gov/ncas/alerts)
    - Obtain info on malware characteristics

2. Prioritisation

- Once malware has been identified, first step is to prioritize incident response, as
  - Some malware is capable of spreading itself, both internally and externally
- Level of response depend on :
  - How the malware entered the organization
  - Type of malware (trojan, worm…)
  - In which network is it infecting
  - Level of impact if incident is not contained

3. Containment

- Need to contain malware to
  - Prevent further infection (if possible)
  - Reduce further damage done to infected systems
- 4 ways to contain malware
  1) Through users
  2) Through automated detection
  3) Through loss of service
  4) Through loss of connectivity

3. Containment

A. Containment through users

- Some malware require users to help eradicate it on their desktops.
- Take care of users who are not around or desktops in common area or not in use.
- Instructions to eradicate malware must be easily understandable.
- Take care of remote sites, especially if program needs to be executed by users to remove malware.

3. Containment

B. Containment through automated detection

- Most malware detection tools already have services that can contain malware.
- When tools cannot identify or handle malware, manual methods to be executed by users have to be relied upon.
- Ineffective against **zero-day** malware attacks where patches are not available.
- Other tools include
  - Email filtering
  - Network-based IPS

3. Containment

C. Containment through loss of service

- Fast spreading malware require termination of services, such as email or web server
- If service is critical to business functions, consider using other alternative services temporarily

D. Containment through loss of connectivity

- Restrict network connectivity can be effective if knowledge on malware characteristics is available.
- Normally used to contain malware

4. Eradication

- Identify infected hosts
  - Forensic identification
    - Use of evidence of recent infections
    - Uses logs of applications, or security tools
    - Used when infection has been removed
  - Active identification
    - Use tools to identify current infection
  - Manual identification
    - Have users or administrators identify the existence of malware manually, such as checking registry, presence/absence of critical files.

4. Eradication

- Eradication of infection
  - Includes BOTH removal of infection and, if possible, ensuring that future infection is impossible by installing appropriate patches.
  - Sometimes, eradication efforts may be done in conjunction with containment efforts.
  - Requires different actions depending on type of damage and nature of the equipment (e.g. server or router)
  - Incident handlers should be aware that infections may come in again later.

5. Recovery

- Recovery of infected systems
  - Systems with damaged data/applications need to be recovered to their original state.
  - Effective recovery needs an updated inventory of software and the expertise to carry it out.
  - Commonly included in maintenance contracts

New Tactic for Fighting Malware

AT MOST BUSINESSES, protecting PCs from malware means installing software patches and rebooting. But when you're patching thousands of systems, the disruptions in productivity can be lengthy. At the recent DEMO conference, security software firm Determina unveiled software for fighting malware before rebooting, to hold the digital fort until a convenient patch time arises.

Rather than patching vulnerable programs on disks, which would necessitate a reboot, Determina's LiveShield technology, based on MIT research, inserts replacement code for programs running in memory as soon as IT staffers become aware of vulnerabilities.—*SR*

Conclusion

- Malware defence and management are critical functions in today's Internet-enabled organization.
- Yet, organizations cannot stop using the Internet due to various risks posed by malware.
- It is important for the organization to effectively manage malware should it infiltrate the company's IT infrastructure.

Summary

- Need for Malware Defence
- Key Concept for Malware Defence
- Malware Management
  1. Detection
  2. Prioritisation
  3. Containment
  4. Eradication
  5. Recovery

References: Tools & Resources

Malware Incident Handler Communications and Facilities
Contact information (e.g., phone numbers, e-mail addresses) for team members and others within and outside the organization (primary and backup contacts), such as antivirus vendors and other incident response teams
On-call information for other teams within the organization, including escalation information
Pagers or cell phones to be carried by team members for off-hour support, onsite communications
Alternate Internet access method for finding information on new threats, downloading patches and updates, and reaching other Internet-based resources when Internet access is lost during a severe malware incident
War room for central communication and coordination; if a permanent war room is not necessary, the team should create a procedure for procuring a temporary war room when needed

References: Tools and Resources

Malware Incident Analysis Hardware and Software
Laptops, which provide easily portable workstations for activities such as analyzing data and sniffing packets
Spare workstations, servers, and networking equipment, which may be used for trying out malware in an isolated environment; if the team cannot justify the expense of additional equipment, perhaps equipment in an existing test lab could be used, or a virtual lab could be established using OS emulation software
Blank media, such as floppy diskettes and CDs, for storing and transporting malware samples and other files as needed
Packet sniffers and protocol analyzers to capture and analyze network traffic that may contain malware activity
Floppies and CDs with up-to-date trusted versions of programs to be used to examine systems for signs of malware infection (e.g., antivirus software, spyware detection and removal utilities)

References: Tools and Resources

Malware Incident Analysis Resources
Port lists, including commonly used ports and known Trojan horse and backdoor ports
Documentation for OSs, applications, protocols, and antivirus and intrusion detection signatures
Network diagrams and lists of critical assets, such as Web, e-mail, and File Transfer Protocol (FTP) servers
Baselines of expected network, system and application activity
Malware Incident Mitigation Software
Media, including OS boot disks and CDs, OS media, and application media
Security patches from OS and application vendors
Backup images of OS, applications, and data stored on secondary media