CIT 270: SYSTEMS SECURITY I

CHAPTER 2: MALWARE AND SOCIAL ENGINEERING ATTACKS

BYU IDAHO

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

INTRODUCTION

Most successful computer attacks fall into one of two categories:

1. Malicious software programs created by a threat actor used to infiltrate a victim's computer without their knowledge.

2. Tricking users into performing a compromising action or providing sensitive information; defeating security through a person is the most *cost* effective approach to hacking.

ATTACKS USING MALWARE

Malware: malicious software that enters a computer system without the owner's knowledge or consent and performs an unwanted or harmful action.

Computer Contaminant is the legal term used instead of malware by law enforcement and lawyers to be as encompassing and precise as possible.

Malware or Computer Contaminant are general words that could refer to any variety of damaging or annoying software.

ATTACKS USING MALWARE

Malware is often classified by the primary trait that the malware possesses:

- circulation
- infection
- concealment
- payload capabilities

ATTACKS USING MALWARE

Malware is often classified by the primary trait that the malware possesses:

- circulation
- infection
- concealment
- payload capabilities

Malware that spreads rapidly to other systems to impact a large amount of users. Spread through the network, by USB, or as attachments:

- viruses
- worms

ATTACKS USING MALWARE

Malware is often classified by the primary trait that the malware possesses:

- circulation
- infection
- concealment
- payload capabilities

Malware that *infects* by embedding itself into a system. It may attach itself to another process or be stand-alone. The malware may run once, on some kind of schedule, or infinitely.

ATTACKS USING MALWARE

Malware is often classified by the primary trait that the malware possesses:

- circulation
- infection
- concealment
- payload capabilities

Malware that avoids detection by concealing its presence from software scanners. This malware can change itself, embed within existing programs, or modify the underlying OS.

ATTACKS USING MALWARE

Malware is often classified by the primary trait that the malware possesses:

- circulation
- infection
- concealment
- payload capabilities

Malware that has a specific nefarious capability; steals passwords, deletes programs, modify security settings, use the computer to launch other attacks, and so on.

ATTACKS USING MALWARE: VIRUSES

Almost all viruses infect by inserting themselves into a computer file:

- executable files
- data files

Program Virus: any virus that infect executable files.

Macro Virus: a virus that has a series of instructions that can be grouped together as a single command.

ATTACKS USING MALWARE: INFECTIONS

Each time a virus infected file runs two things commonly happen:

1. unloads it's payload to perform a malicious action.
2. reproduces itself into another file on the same computer.

Well there are different types (classifications) of viruses there is also different types of infections these viruses cause.

ATTACKS USING MALWARE: INFECTIONS

Appender Infection: attaches or appends inself to the end of the infected file then uses an inserted jump instruction that points to the end of the file.

Swiss Cheese Infection: uses encrypted virus code that is decoded only after several jump instructions where the virus is decoded more and more at each jump.

Mutation infections are a type of virus that can mutate or change itself over time:

- oligomorphic viruses change their internal code to one of a set number of predetermined configurations.
- metamorphic viruses can actually rewrite their own code and appears different each time it's executed.

ATTACKS USING MALWARE: INFECTIONS

Trojan: an executable program that masquerades as performing a benign activity but is also doing something malicious.

Remote Access Trojan (RAT): has the basic functionality of a trojan but also gives a threat actor unauthorized remote access to a victim's computer.

Ransomware: prevents a device from properly functioning until a fee is paid.

Crypto-malware: ransomware that first encrypts the devices data; today this includes data on the network and any connected devices.

ATTACKS USING MALWARE: INFECTIONS

Rootkit: hides its presence or the presence of other malware by accessing lower layers of the operating system.

Spyware: tracking software that secretly monitors users by collecting information; from programs to personal information.

Keylogger: silently captures and stores each keystroke that a user types; there are hardware and software versions.

Adware: delivers advertising content in an unexpected or unwanted manner.

ATTACKS USING MALWARE: INFECTIONS

Logic Bomb: lies dormant until a specific logical event triggers it.

Backdoor: gives access to a computer, program, or service that circumvents any normal security protections.

Bot (zombine): allows computer to be placed under the remote control of threat actors; often works in the background well users still use the machine.

Bot Net: a network of infected computers controlled as a group by a threat actor.

SOCIAL ENGINEERING ATTACKS

Social Engineering is a means of gathering information for an attack by relying on the weakness of individuals. No technical tools or skills are needed.

Social Engineering has two approaches:

1. psychological
2. physical procedures

SOCIAL ENGINEERING ATTACKS: PSYCHOLOGICAL

Impersonation: masquerade as a real or fictitious character and then play out the role on a victim.

Many social engineering attacks rely on person-to-person contact so attackers use a variety of techniques to gain trust:

- provide a reason
- project confidence
- evasion and diversion
- humor, make them laugh

SOCIAL ENGINEERING ATTACKS: PSYCHOLOGICAL

Principle	Description	Example
Authority	Directed by someone impersonating an authority figure.	I'm the CEO calling.
Intimidation	To frighten and coerce by threat.	I will call your supervisor!
Consensus	Influenced by what others do.	You colleague was willing to help!
Scarcity	Something in short supply.	I can't waste my time here.
Urgency	Immediate action is needed.	My meeting starts in 5 minutes!
Familiarity	Victim is well-known and liked.	I remember reading a good review about you.
Trust	Confidence.	You know who I am.

SOCIAL ENGINEERING ATTACKS: PSYCHOLOGICAL

Phishing: email or web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick users into sending private information.

Vishing: (voice phishing) an attacker calls a victim with a prerecorded message with a call back number. The call back number is also automated to record personal details.

Whaling: a targeted phishing attack that aims for *big fish*.

Spear phishing: targets a specific user.

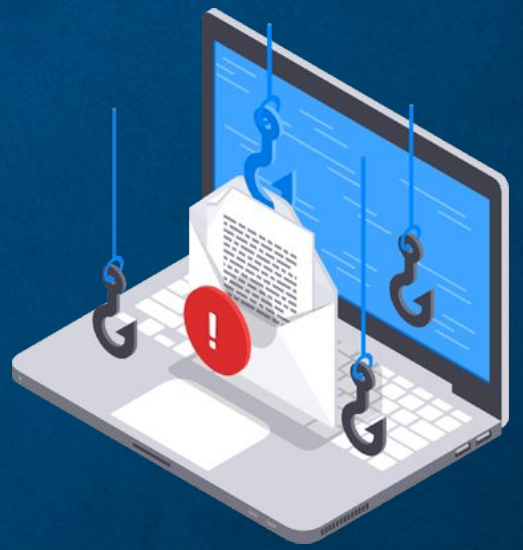

Image: avast.com

SOCIAL ENGINEERING ATTACKS: PSYCHOLOGICAL

Watering Hole Attack: a targeted attack that goes after a specific group, such as major executives in a company. The goal is to infect a common website or recourse this group uses.

Spam: any unsolicited email that is sent to a large number of recipients. By volume it once accounted for 92% of all spent emails. As of 2018 that number has dropped to 61% because of aggressive efforts to combat spam.

Hoax: a false warning often contained in an email message claiming to be coming from the IT department.

SOCIAL ENGINEERING ATTACKS: PHYSICAL

Dumpster diving involves digging through trash to find information that can be useful in an attack.

Google dorking is a technological approach to dumpster diving. Using internet searches attackers will try to uncover information that will help with an attack.

Tailgating: following behind an authorized person who then unknowingly lets you into a building; piggybacking is when the person lets you.

Shoulder Surfing: any setting in which a user casually observes someone entering secret information such as a door keypad.

SUMMARY

Malware is usually used to help threat actors get to their end goal. What threat actors aim to get from their attacks may differ:

Circulation	Infection	Concealment	Payload Capabilities
Viruses	Trojans	Trojans	Spyware
Worms	Ransomware	Rootkits	Adware
	Crypto-malware	Backdoors	

Social Engineering is usually used to help threat actors better use malware to get to their end goal. Sometime Social Engineering attacks are all that are needed to reach a particular threat actors goal.

REFERENCES

Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.). Boston, MA: Cengage.

Phishing Graphic [PNG]. Avast, Sep. 2019, https://www.avast.com/c-phishing.