

CEG 3400

Introduction to CyberSecurity

Malware & Social Engineering

Today's Objective(s)

- Define Malware
- Overview various types of malware
- Explain social engineering attacks

Disclaimer:

- Slide contents are from numerous sources:
 - *Security+ Guide to Network Security Fundamentals, 5th Edition*, by Mark Ciampa
 - Other WSU CyberSecurity Lectures
 - CERT-UK, *An introduction to malware*, 2014
 - National computer emergency response team in the UK
 - Formed in March 2014 as part of UK National CyberSecurity Strategy
 - McAfee Labs Threat Report 2015
 - CS 426 Lectures, Purdue University - http://www.cs.purdue.edu/homes/ninghui/courses/426_Fall10/handouts/426_Fall10_lect11.pdf
 - Wikipedia
 - Other as indicated on slides

Malware – What Is It?



Malware

- Malware → **Malicious Software**: a general term used to refer to a variety of forms of hostile or intrusive software
 - *Computer Contaminant* – “legalese” name used in some state legal codes
 - Enters a computer system without the owner’s knowledge or consent
 - Uses a threat vector to deliver a malicious “payload” that performs a harmful function once it is invoked
- What is the important difference between Malware & other defective software (aka software bugs)? **INTENT!**
- Wide range of names and terms associated with malware – easy to get confused
 - Adware, Backdoor, Bot/Botnet, Dialer, Exploit, Keylogger, Logic Bomb, Malicious BHO, Ransomware, Rootkit, Spyware, Trojan, Virus, Worm, Zombie, ...

Professional Malware

- Growth in professional cybercrime and online fraud has led to demand for professionally developed malware
- New malware is often a custom-designed variations of known exploits, so the malware designer can sell different “products” to his/her customers.
- Like every product, professional malware is subject to the laws of supply and demand.
- Recent studies put the price of a Remote Access Trojan (RAT) at \$1500 for lifetime license and a zero-day exploit at \$80,000 - \$300,000.

Nairaland Forum


Welcome, Guest: [Join Nairaland](#) / [Login](#) / [Trending](#) / [Recent](#) / [New](#)
Stats: 1,666,526 members, 3,125,870 topics. Date: Wednesday, 05 October 2016 at 04:15 PM

Buy Your Botnet Keylogger Fully FUD At A Discounted Price - Computer Market - Nairaland

[Nairaland Forum](#) / [Science/Technology](#) / [Computers](#) / [Computer Market](#) / [Buy Your Botnet Keylogger Fully FUD At A Discounted Price](#)
(269 Views)

[Buy Your FUD VIRUS And Toolz](#) / [Selling Shells/cpanels/rdp/mailers/scampage/leads/overstock/botnet RAT TUTORIALS](#) / [Download Facebook Hacking Keylogger](#) (1) (2) (3) (4)

How To
PLACE TARGETED ADS
on Nairaland



How To
PLACE TARGETED ADS
on Nairaland

(0) (Reply)

[Buy Your Botnet Keylogger Fully FUD At A Discounted Price](#) by [chike00](#): 12:16pm On May 19, 2015

I sell 100%fud keylogger and RAT @ a discount of \$60. If it's gets detected will re-FUD it ASAP. No free please as it takes money to make it. Citadel botnet is d best no doubt.

[Re: Buy Your Botnet Keylogger Fully FUD At A Discounted Price](#) by [chike00](#): 12:17pm On May 19, 2015

Discount last till last day of this month

[Re: Buy Your Botnet Keylogger Fully FUD At A Discounted Price](#) by [samjohn362\(m\)](#): 2:04pm On Jun 04, 2015

To make over #200,000 every single month from de comfort of ur home visit www.incomestreambiz.com/optin.html or watsapp me 08157522433

<http://www.nairaland.com/2323642/buy-botnet-keylogger-fully-fud>

“Common” Types of Malware



Keyloggers



Malware



Watering Holes



Worm



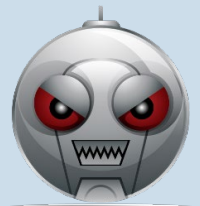
Trojan Horse



Ransomware



Rootkit



Bot



Mobile Malware



Virus



Phishing



Ransomware

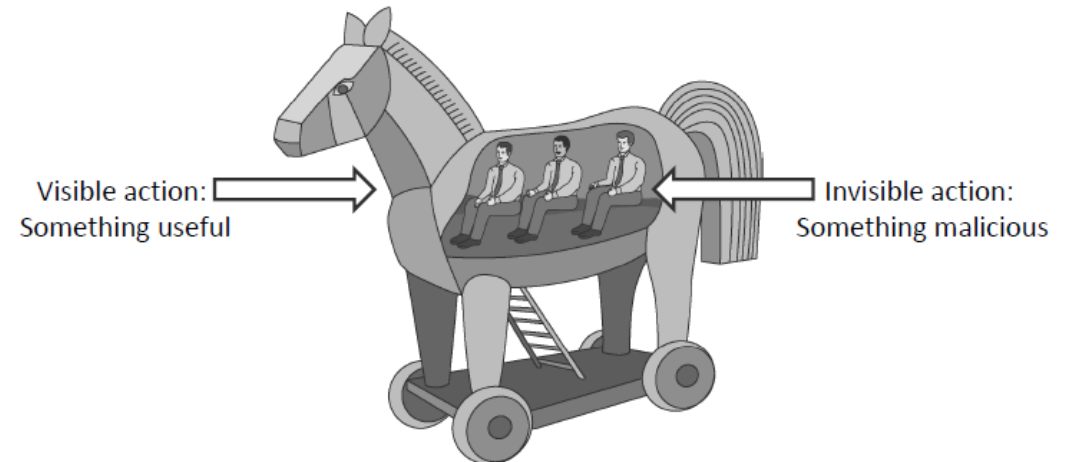
- Ransomware – essentially holds a computer system captive while demanding a ransom
 - Encrypts files on system's harddrive (cryptoviral extortion)
 - Locks the system and displays messages intended to coheres user into paying fee
- **CryptoLocker**, a version of ransomware that first appeared in September 2013
 - It has infected about 25 million systems across the globe
 - Appears to spread through emails that lure victims into opening them
- A new generation of ransomware known as **PowerLocker** -- aka Prison Locker -- is designed to lock PCs using uncrackable crypto – Information Week, 7 Jan 2014
 - PowerLocker's developer said that his malware
 - used the Blowfish symmetric-key block cipher to encrypt all personal data stored on a PC
 - then encrypted those ciphers using 2048-bit RSA encryption





Trojan Horse

- A **Trojan horse (or Trojan)** is a malware program that appears to perform some useful task, but which also does something with negative consequences (e.g., launches a keylogger).
- Trojan horses can be installed as part of the payload of other malware but are often installed by a user or administrator, either deliberately or accidentally.
- Trojans don't replicate and don't infect other files (like viruses & worms do)
- Early Trojans focused on DDOS – now focus is providing backdoor entry to systems
- **Remote Access Trojan (RAT)** – controls a system through a remote network connection
 - Often times delivered as payload of traditional trojan horse
 - Tries to hide its operation





Rootkit

- Stealth is the primary focus of a rootkit
- A rootkit modifies the operating system to hide its existence while gaining remote access or control
 - E.g., modifies file system exploration utilities - install hacked binaries for system programs such as netstat, ps, ls, du, login
 - Hard to detect using software that relies on the OS itself
 - Focuses heavily on gaining root / administrator privileges
 - Can then modify/alter security software so can't be detected/found
 - Provides escalated/admin/root privileges to remote users
- Once embedded in a computer, activates each time system boots up
 - Activated before the system OS has completely booted up
- Can intercept data from terminals, network connections and keyboards
- Stealth is the primary focus of a rootkit

Can't detect attacker's processes, files or network connections by running standard UNIX commands!



Virus

- A **computer virus** is computer code that can replicate itself by modifying other files or programs to insert code that is capable of further replication (“attaches itself to an executable file”)
 - Two distinguishing properties: replication & human assistance
 - Infection Vectors
 - Boot Sector - Loaded when the system is booted
 - Executable – ****most common** - Remains inactive on host system. Doesn’t spread until activated when an executable file is activated
 - Macro files - Triggered when a document is loaded
 - Mutation Techniques
 - Real Permutation Engine/RPME, ADMutate, etc.
 - Large arsenal of obfuscation techniques
 - Instructions reordered, branch conditions reversed, different register names, different subroutine order
 - Jumps and NOPs inserted in random places
 - Garbage opcodes inserted in unreachable code areas
 - Instruction sequences replaced with other instructions that have the same effect, but different opcodes
- Mutate `SUB EAX, EAX` into `XOR EAX, EAX` or `MOV EBP, ESP` into `PUSH ESP; POP EBP`

Remember: the goal is to change enough so “have no real signature” → signature based IDS/IPS can’t detect them



Worm

- A **computer worm** is a malware program that spreads copies of itself without the need to inject itself in other programs, and usually without human interaction
- Thus, computer worms are not considered computer viruses
- In most cases, a computer worm will carry a malicious payload, such as deleting files or installing a backdoor
- Runs independently - does not require a host program
- Propagates a fully working version of itself to other machines
- Carries a payload performing hidden tasks - DDoS attacks, backdoors,

VIP: VIRUS – replicates but requires human assistance ... WORM – replicates and does not require human assistance (can be viewed as autonomous / autonomic software)

Worms - Early History

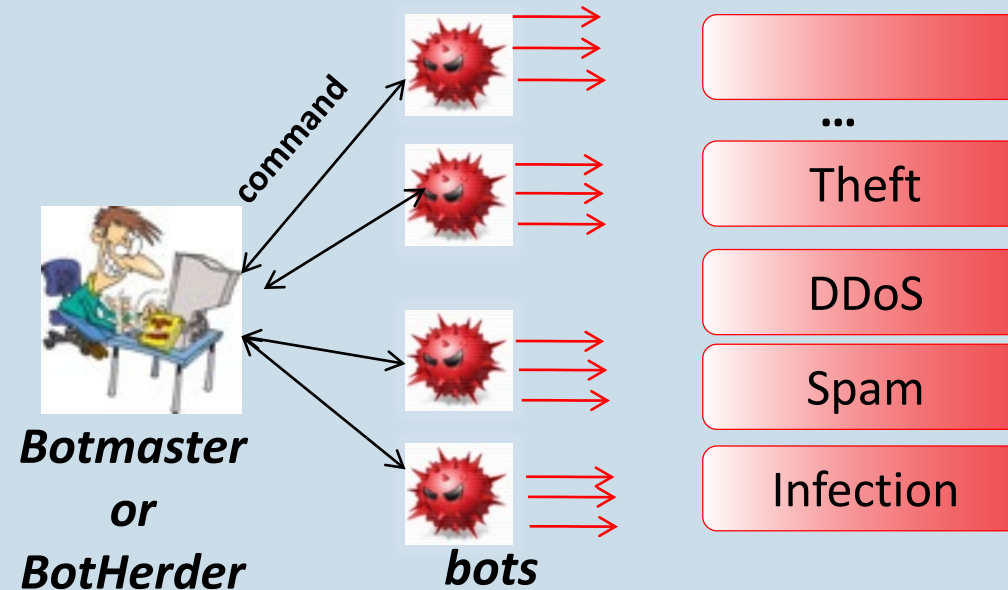
- The first internet worm was the **Morris Worm**
 - Written by Cornell student Robert Tappan Morris
 - Released on November 2, 1988
 - A 99-line program
 - 6000 computers in just few hours
 - Paralyzed the whole Internet at that time
 - Was not really “malicious” (propagate without touching the data)
- The positive impacts
 - Raised attentions to cyber-security
 - Computer Emergency Response Team (CERT) was created
- Worms that affected operation of entire Internet
 - Morris Worm (1988)
 - Code Red (2001)
 - Nimda (2001)
 - Blaster (2003)
 - SQL Slammer (2003)





Bots & Botnets

- Bot – software program created to **automatically** perform specific operations
 - Some bots are benign (used in video games, internet auctions, online contests, etc.)
 - Many bots used today are malicious
 - Note – textbook refers to bots as Zombies
- A botnet is a collection of ***bot-compromised hosts (bots)*** that are coordinated via ***a command and control (C&C) channel*** by an attacker to commit a variety of attacks





Phishing / Spear Phishing

- Phishing - uses social engineering techniques to fraudulently acquire personal information
 - Masquerades as a trustworthy person or business in an apparently official electronic communication
 - Emails or instant messages claiming to originate from banks, online payment processors or IT admins
 - Risk has grown exponentially following the advent of social media
 - Fake website which almost identically mirrors the appearance and operation of the legitimate domain
- Spear phishing - represents a more sophisticated form of traditional phishing attacks
 - Select groups or individuals are targeted
 - Intent is to harvest very specific information or infect very specific entities with malware
 - Bad actors craft emails that appear to be from a legitimate source
- Phishing Variations
 - Whaling - going after the “big fish”
 - Targeting wealthy individuals
 - Vishing (voice phishing)
 - Attacker calls victim with recorded “bank” message with callback number
 - Victim calls attacker’s number and enters private information



Given the importance of the user in this form of malware attack, attempts to deal with the growing number of reported phishing incidents are focused on improving user training and public awareness



Keylogger

- Keyloggers – used to intercept passwords & other confidential info entered via keyboard
 - Present no threat to the system itself
 - Accomplish task via video surveillance, hardware bugs, malicious code that swaps out keyboard driver(s), intercept kernel functions, etc.
- **Heartbleed** – new threat capitalizing on Heartbleed fear
 - Users receive email – you were infected by heartbleed – install the attached file
 - File was encrypted zip file – once extracted users ran *heartbleedbugremovaltool.exe*
 - Keylogger was installed – recorded keystrokes, took screenshots → sent to free hosted email provider



Watering Holes

- Watering Holes - not a form of malware in their own right
 - Watering holes or 'strategic web compromises' are an increasingly common means of introducing malware onto a victim's system
 - Goal is not to disseminate malware to as many systems as possible
 - Goal is to run exploits on trusted sites that are likely to be visited by the attacker's target victims
 - Relying on websites that are known and trusted makes watering holes an extremely efficient attack vector,
 - Common exploits include SQL injection, malicious iFrames or cross-site scripting code
- **The VOHO Campaign – 2012**
 - Focused on US financial and high tech
 - Malicious JavaScript inserted in websites
 - Arriving at site caused installation of gh0st RAT – Remote Access Trojan
 - 32,000 individual hosts across 4000 organizations



Mobile Malware

- Mobile Malware not new
- Worms first attacked Symbian Series 60 mobile phones as far back as 2004
- Recent rapid expansion in number, variety and sophistication
- One of the most common mobile malware variants are SMS-senders, such as Andr/AdSMS
- Malicious application disguises as pirated app
 - Hidden module which will start sending SMS messages to premium rate numbers
- Individuals don't check mobile bills, takes time for any changes to be noticed

Some of Other Malware “Notable Mentions”

- **“Zero” Day** – an unknown security vulnerability
 - One the good guys have not discovered and/or have not had time to patch
 - “good guys” share information about new exploits / vulnerabilities
 - Sometimes privately with just owners and sometimes world wide
 - Fixes are developed and distributed
 - When “bad guys” discover new exploit / vulnerability a potential Zero Day exploit exists
 - The “game” is to track how long a Zero Day remains a Zero Day (stays undetected by “good guys”)

Impossible to defend against these – can’t defend against something you don’t know about

Some of Other Malware “Notable Mentions”

- **Covert Channel** – sends & receives information between machines
 - Doesn't alert any firewalls and/or IDS's on the network
 - Sends traffic through ports that most firewalls will permit through
 - Bypass an IDS by appearing to be an innocuous packet
 - Conceals malicious code in one of the several control fields in the TCP and IP headers.

TCP Packet

Bit Offset	0-3	4-7	8-15	16-18	19-31
0	Source Port			Destination Port	
32	Sequence Number				
64	Acknowledgment Number				
96	Offset	Reserved	Flags	Window Size	
128	Checksum			Urgent Pointer	
160	Options				
>= 160	Payload				

IP Packet

0	4	8	16	19	31
Version	HL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time To Live		Protocol	Header Checksum		
Source IP Address					
Destination IP Address					
Options				Padding	

Social Engineering

“The Art of Human Hacking”

What is Social Engineering

1. At its core it is manipulating a person into knowingly or unknowingly giving up information; essentially 'hacking' into a person to steal valuable information.
 - Psychological manipulation
 - Trickery or Deception for the purpose of information gathering
2. It is a way for criminals to gain access to information systems. The purpose of social engineering is usually to secretly install spyware, other malicious software or to trick persons into handing over passwords and/or other sensitive financial or personal information
3. Social engineering is one of the most effective routes to stealing confidential data from organizations, according to Siemens Enterprise Communications, based in Germany. In a recent Siemens test, 85 percent of office workers were duped by engineering.

“Most employees are utterly unaware that they are being manipulated,” says Colin Greenlees, security and counter-fraud consultant at Siemens.

A Quote from Kevin Mitnick:

“You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain vulnerable to old-fashioned manipulation.”

Real Examples

- **Security Pacific National Bank**
 - Stanley Mark Rifkin managed to steal \$10,200,000 in a single social engineering attack (1978)
- **RSA**
 - Infected Excel attachment, over \$100 million of damage
- **Well Fargo Bank**
 - “Catholic Healthcare” phone call, \$2.1 million vanished
- **Vodafone Help Desk**
 - Malware and fraud call, end user lost everything

What Are They Looking For

- Obtaining simple information such as your pet's name, where you're from, the places you've visited; information that you'd give out freely to your friends.
- Think of yourself as a walking computer, full of valuable information about yourself. You've got a name, address, and valuables. Now categorize those items like a business does. Personally identifiable data, financial information, cardholder data, health insurance data, credit reporting data, and so on...
- Take a close look at some of the 'secure' sites you log into. Some have a 'secret question' you have to answer, if you cannot remember your username or password. The questions seem pretty tough for an outsider looking into trying to hack into your account.
 - What's the name of your first pet?
 - What is your maiden name?
 - When was your mother/father born?
 - Where were you born?

Do these sound familiar?

Tactics

- Pretexting & fake scenarios
- Phishing/Spear Phishing
- Fake Websites
- Fake Pop-up
- Impersonation on help desk calls
- Physical access (such as tailgating)
- Shoulder surfing
- Dumpster diving
- Stealing important documents
- Fake software
- Trojans

REMEMBER: Social Engineering = The Art of Human Hacking

Protecting Yourself

- A security aware culture can help employees identify and repel social engineering attacks
 - Recognize inappropriate requests for information
 - Take ownership for corporate security
 - Understand risk and impact of security breeches
 - Social engineering attacks are personal
 - Password management
 - Two factor authentication
 - Physical security
 - Understand what information you are putting on the Web for targeting at social network sites
- Network defenses to repel virus
 - Virus protection (McAfee, Norton, Symantec, etc...)
 - Email attachment scanning
 - Firewalls, etc...
- Organizations must decide what information is sensitive
- Security must be periodically tested
- Contact your security office immediately if you have any concerns at work

Responding

- You've been attacked: now what?
- Have a place to report incidents
- People need to take responsibility
- Conduct audits
- What damage has been done? What damage can still be done?
- Has a crime actually taken place?

Summary

- Malware is malicious software that enters a computer system without the owner's knowledge or consent
 - Malware that spreads include computer viruses, worms, and Trojans
- Spyware is software that secretly spies on users by collecting information without their consent
 - Type of spyware include keylogger, adware and ransomware
- One of the most popular payloads of malware today carried out by Trojans, worms, and viruses is software that will allow the infected computer to be placed under the remote control of an attacker (infected computer is known as a bot or zombie)
- Social engineering is a means of gathering information for an attack by “hacking into” individuals
 - Types of social engineering approaches include phishing, dumpster diving, and tailgating
 - REMEMBER – social engineering is much more than just various flavors of phishing
- Protecting against social engineering is the same as protecting against other “hacking” exploits and attacks

Class Exercise – Phishing Tests

- This is a table group exercise.
- Hook 1 laptop at each table to projection system
- Look at your table's projection and work as a team to accomplish the following:
 - All other table members collaborate and discuss
 - Document reasoning for each answer (on the white board if possible)
- Exercise #1 - <https://www.sonicwall.com/en-us/phishing-iq-test>
- Exercise #2 - <https://www.opendns.com/phishing-quiz/>