CRAVING αLPHA

Since 2018

CYBERSECURITY AWARENESS

Importance of Cybersecurity

The internet allows an attacker to work from anywhere on the planet.

CRAVING αLPHA
Since 2018

Importance of Cybersecurity

The internet allows an attacker to work from anywhere on the planet.

Risks caused by poor security knowledge and practice:

- IdentityTheft
- MonetaryTheft
- LegalRamifications(foryourselfandyourorganization)
- Sanctions or termination if policies are not followed

CRAVING αLPHA
Since 2018

Security is Safety

Security: We must protect our computers and data in the same way that we secure the doors to our homes.

CRAVING αLPHA
Since 2018

Security is Safety

Security: We must protect our computers and data in the same way that we secure the doors to our homes.

Safety: We must behave in ways that protect us against risks and threats that come with technology.

Leading Threats

Viruses

Worms

- Trojan Horses
- Logic Bombs
- Rootkits

Social Engineering

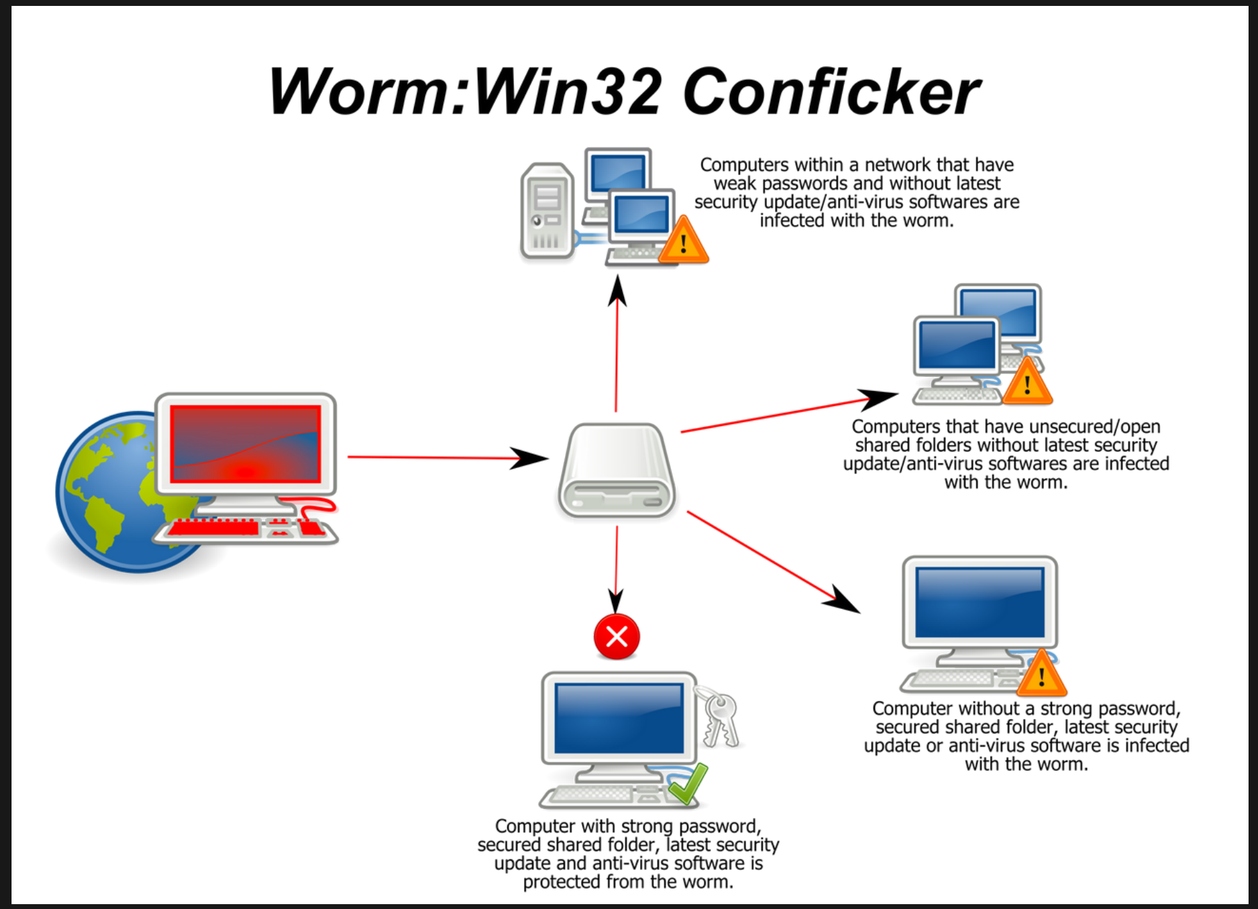
Botnets/ Zombies

Viruses

- A virus attaches itself to a program, file, or disk
- When the program is executed, the virus activates and replicates itself
- The virus may be benign or malignant but executes its payload at some point (often upon contact)
    - Viruses can cause computer crashes and loss of data

Worms

Independent program that replicates itself and sends copies from computer to computer across network connections



Logic Bomb

- **Malware logic executes upon certain conditions. The program is often used for otherwise legitimate reasons, ex-**
  - Software which malfunctions if maintenance fee is not paid
  - Employee triggers a database erase when he is fired

Trojan Horse

- **Masquerades as a benign program while quietly destroying data or damaging your system, example:**
  - *Download a game*: It may be fun but contains hidden code that gathers personal information without your knowledge.

Social Engineering

Manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems

Phishing

Counterfeit Email

A seemingly trustworthy entity asks for sensitive information such as PAN, Adhaar, credit card numbers, login IDs or passwords via e-mail

Pharming

Counterfeit Web Pages

The link provided in the e-mail leads to a counterfeit webpage which collects important information and submits it to the owner

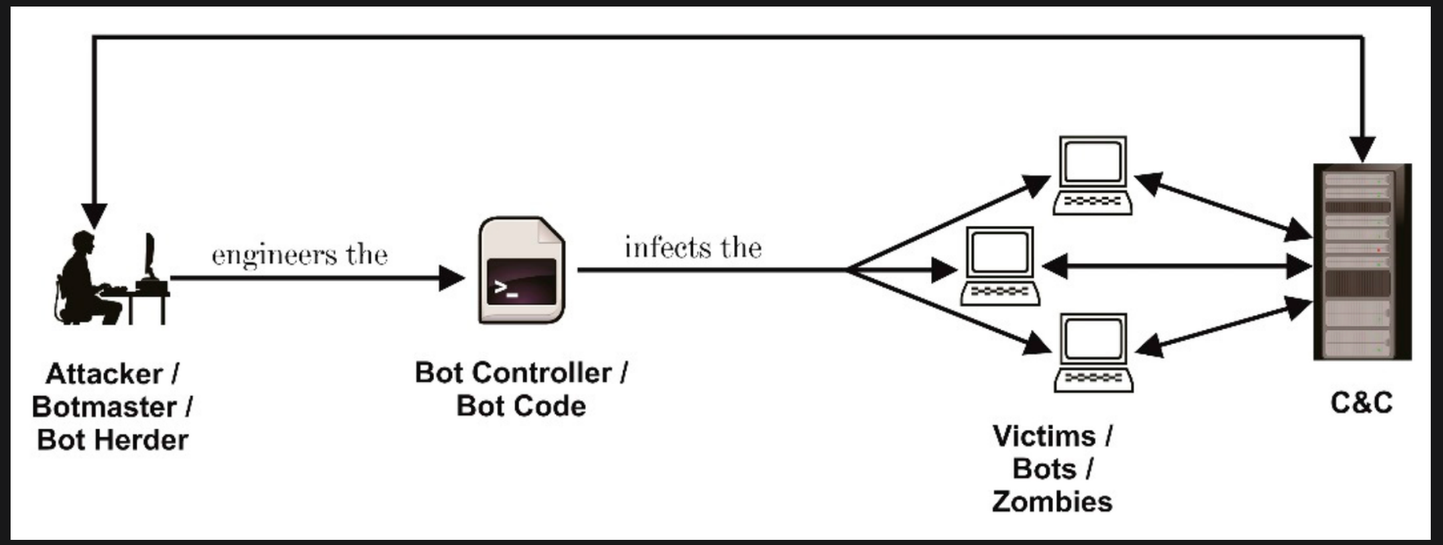
- The counterfeit web page looks like the real thing
- Extracts account information

CRAVING αLPHA
Since 2018

Botnet

A botnet is a number of compromised computers used to create and send spam or viruses or flood a network with messages as a denial of service attack

- The compromised computers are called zombies



Man in the middle

An attacker pretends to be your final destination on the network. When a person tries to connect to a specific destination, an attacker can mislead him to a different service and pretend to be that network access point or server

Rootkit

Upon penetrating a computer, a hacker may install a collection of programs, called a rootkit

- May enable:
  - Easy access for the hacker (and others)into the enterprise
  - Keystroke logger
- Eliminates evidence of break-in
- Modifies the operating system

Identifying Security Compromises

Symptoms

Malware Detection

- Spyware symptoms

Best Practices

- Anti- virus & spyware
- Host based firewalls
- Protect your OS
- Use Strong Passwords
- Avoid Social engineering
- Secure business transactions
- Backup important information
- Cyber Incident Reporting

Symptoms

- Antivirus software detects a problem
- Disk space disappears unexpectedly
- Pop-ups suddenly appear, sometimes selling security software
- Files or transactions appear that should not be there
- Unusual messages, sounds, or displays on your monitor
- The computer spontaneously shuts down or reboots
- Often unrecognized or ignored problems

Stolen laptop: 1 stolen every 53 seconds; 97% never recovered.

Symptoms | Spyware

CRAVING αLPHA
Since 2018

- Changes to your browser homepage/start page
- Ending up on a strange site when conducting a search
- System-based firewall is turned off automatically
- Lots of network activity while not particularly active
- Frequent firewall alerts about unknown programs when trying to access the Internet.
- Poor system performance

First ever used in 1995. Originally term denoted software used for espionage

Best Practices | Anti-Virus & Anti- Spyware

CRAVING αLPHA
Since 2018

- Anti-virus software detects certain types of malware and can destroy it before any damage is done
- Install and maintain anti-virus and anti-spyware software
- Be sure to keep anti-virus software updated
- Many free and commercial options exist
- Contact your Technology Support Professional for assistance

ILOVEYOU virus spread to over 45mn computers

Best Practices | Host-based Firewall

- A firewall acts as a barrier between your computer/private network and the internet
- Hackers may use the internet to find, use, and install applications on your computer which a firewall prevents

Best Practices | Protect your Operating System

- Microsoft regularly issues patches or updates to solve security problems in their software. If these are not applied, it leaves your computer vulnerable to hackers.
- The Windows Update feature built into Windows can be set up to automatically download and install updates.
- Avoid logging in as administrator
- Apple provides regular updates to its operating system and software applications

Best Practices | Use strong passwords

- USG standards:
  - Be at least ten characters in length
  - Must contain characters from at least two of the following four types of characters:
    - English upper or lower case (A-Z)
    - Numbers (0-9)
    - Non-alphanumeric special characters ($, !, %, ^, …)
- Must not contain easily accessible or guessable personal information about the user or user's family, such as birthdays, children's names, addresses, etc

Best Practices | Avoid Social Engineering & Malicious Software

- Do not open email attachments unless you are expecting the email with the attachment and you trust the sender
- Do not click on links in emails unless you are absolutely sure of their validity
- Only visit and/or download software from web pages you trust

Best Practices | Secure Business Transactions

- Always use secure browser to do online activities.
- Frequently delete temp files, cookies, history, saved passwords etc.

Best Practices | Backup important information

- No security measure is 100% reliable
- Even the best hardware fails.
- What information is important to you?
- Is your backup:
  - Recent? Off-site & Secure?
  - Process Documented? Encrypted? Tested?

Fraud

- Organizations lose 5-6% of revenue annually due to internal fraud = $652 Billion in U.S. (2006)
- Average scheme lasts 18 months, costs $159,000
- 25% costs exceed $1M
- Smaller companies suffer greater average dollar losses than large companies

CRAVING αLPHA

Since 2018

Thank You !

Phone
+91 983 616 0204

Email
prosper@cravingalpha.com

Online
www.cravingalpha.com