

# Introduction to Cyber Security

- T. Pushpalatha
- Dr. Yogesh Kumar Sharma
- M. Krishna
- Dr. S. Nagaprasad




**Cyber Crimes  
&  
Security**



Published by: **Book Bazooka Publication, India**

Website: [www.bookbazooka.com](http://www.bookbazooka.com)

Email Address: [info@bookbazooka.com](mailto:info@bookbazooka.com)

 BookBazookaOfficial

 BookBazooka

 BookBazooka

 BookBazooka

 BookBazooka

 BookBazooka

ISBN: 978-93-86895-92-9

Price: ₹**190.00** (Asian Continent), **US \$3.00** (Rest out of world)

Authors: T. Pushpalatha, Dr. Yogesh Kumar Sharma, M. Krishna, Dr. S. Nagaprasad

Publication Year: - July '20

© All Rights including Copyrights reserved with the Author.

This hardcopy edition is printed in India and is authorised for sale only in India, Bangladesh, Bhutan, Pakistan, Nepal, Sri Lanka and the Maldives.

All rights reserved. No part of this book may be reproduced or utilised in any form or by any electronic, mechanical or means, now known or hereafter invented, including photocopying and recording, or in any information storage and retrieval system without permission in writing from the publisher or author.

## **About Authors**



### **T. Pushpalatha**

**T. Pushpalatha** is a Assistant Professor of Computer Applications Department (M.C.A.) in St. Ann's College for Women, Mehadipatnam, Hyderabad. She is Pursuing her Ph.D from JJT University Rajasthan.



### **Dr. Yogesh Kumar Sharma**

Dr. Yogesh Kumar Sharma, Presently working as a Associate Professor (HOD / Research Coordinator) Department of Computer Science Engineering and IT at "Shri Jagdish prasad Jhabarmal Tibrewala University", Chudela, Jhunjhunu (Rajasthan). He completed his B.Sc with Computer Application in the year of 2002 awarded from S.M.L. (P.G.) College, Jhunjhunu, University of Rajasthan, M.C.A from Modi Institute of Management and Technology, Kota, University of Kota in the year 2005, Ph.D. in Faculty of Computer Science, from "Shri Jagdish prasad Jhabarmal Tibrewala University", Jhunjhunu (Rajasthan) in the year 2014. His research areas Data Communication & Networking, Operating System, Computer Organization and Architecture, Data Mining, Image processing, Cloud Computing, Software Engineering etc. In his research life he Published 75 Papers in National and International journals, 25 National and International conferences, 03 workshops. Under his guidance 05 research scholars awarded Ph.D. Presently 08 research scholars working under his guidance. He invited as a Guest Lecturer

for Students in M.Sc. I.T. (Master Program in Information Technology) on the behalf of National University of Science and Technology, Muscat, Oman, Nov. 2019. He is Paper Setter, Answer Sheet Evaluator (Copy Checker) and Practical Examiner in University of Rajasthan, Jaipur, Pandit Deendayal Upadhyay University (Shekhawati University), Sikar, Maharaja Ganga Singh University, Bikaner, University of Kota, Kota, Board of Secondary Education Rajasthan, Ajmer. Ph.D. He is Evaluator and Ph.D. Final Viva-Voce Examiner in OPJS University, NIMS University, Mewar University. Published 2 patents on Title: Parallel Processing System to Reduce Complexity in Data-Mining of Industrial & Social Big-Data. And Title: Computer Implemented Method for Detecting Downlink Control Channel in Long Term Evolution Wireless Communication. He is a member of IAENG, IACSIT, CSTA and UACEE.



### **M. Krishna**

**M. Krishna** is a Faculty of Computer Science and Applications Department of Computers in Tara Government College, Sangareddy, and Telangana State. Presently working as Faculty in Department of Computer Science & Applications at Tara Government College, Sangareddy from the Academic Year 2005-till date. Worked as a CCE-JKC Trainer in Computer Skills to Government Degree and Junior Colleges Principals, Lecturers for the academic years 2008-09 & 2009-10. Worked as Part-Time Lecturer in Computer Science at Ellenki Degree College, Sangareddy for the Academic Year 2006-07. Worked as Senior Teacher in Mathematics at Government High School, Sangareddy for the Academic year 2004-05. Worked as Vidya Volunteer in Mathematics at Government High School, Chitkul for the Academic year 2003-04.



### **Dr. S. Nagaprasad**

**Dr. S. Nagaprasad** working as a Faculty in Computer science and Applications, Dept. of Computer Science and Applications, Tara Government College, Sangareddy, Telangana state. He completed his B.C.A. in the year of 1998-2001 awarded from Osmania university, M.Sc (I.T.) in the year of 2001-2003 awarded from Sikkim Manipal University, Sikkim, his research work completed from Ph.D in Computer Science and Engineering, from Acharya Nagarjuna University, Sep-2015. His research areas data mining, networking, image processing, machine learning etc. In his research life he present completed 30 international journals in his research area, 15 National and International conferences, for his research interest he attended 10 workshops. He worked as a faculty in Computer Science at S.K.N.R. Government Arts and Science College, Jagtial Telangana state for 10 years, and he worked as faculty in Computer Science at S.R.R. Government Arts and Science College, Karimnagar Telangana state for 05 years. Presently he is Guiding 5 Ph.D. scholars in Computer Science and Engineering “Shri. Jagdishprasad Jhabarmal Tibrewala University”, Jhunjhunu (Rajasthan).





# INDEX

<b>Introduction to Cyber Crime</b>	1-6
<ul style="list-style-type: none"><li>• Classification of Cyber Crimes</li><li>• Reasons for Commission of Cyber Crimes</li></ul>	
<b>Malware &amp; Its Type</b>	7-25
<i>Page1-34</i>	
<ul style="list-style-type: none"><li>• Adware</li><li>• Bot</li><li>• Bug</li><li>• Ransomware</li><li>• Rootkit</li><li>• Spyware</li><li>• Browser Hijacking Software</li><li>• Virus</li><li>• Worms</li><li>• Torjan Horse</li><li>• Scareware</li><li>• Malware Symptoms</li><li>• Spam</li><li>• Malware Prevention and Removal</li></ul>	
<b>Kinds of Cyber Crime</b>	26-109
<ul style="list-style-type: none"><li>• Cyber Stalking</li><li>• Child Pornography</li><li>• Forgery and Counterfeiting</li><li>• Software Piracy &amp; Crime Related to IPRs</li><li>• Cyber Terrorism</li><li>• Phishing</li></ul>	

- Spamming
- Cross Site Scripting
- Cyber Squatting
- Logic Bombs
- Web Jacking
- Internet time Thefts
- Denial of Service Attack
- Salami Attack
- Data Diddling
- Email Spoofing
- Identity Theft
- Scamming
- Computer Viruses
- DDos Attack
- Botnets
- Social Engineering
- Malvertising
- Cyber stalking
- Cyber Bullying
- Online Harassment
- Online Scams
- SQL Injections
- Cross-Site Scripting
- Virus Dissemination
- Logic Bombs

Chapter 1

# Introduction

## Classification of Cyber Crimes

Any organisation or person facing the cyber attack may be performing internally or externally. Cyber crime could be mainly categorised into two types of cyber crimes:

1. Insider Attack
2. External Attack

### Insider Attack:

In Insider Attack when any person attack on network or company computer system or any person's personal computer network having authorised system access known insider attack. Usually this kind of activity done by hackers who get access information by hacking computer system. When Insider cyber attack happen could be any, it could be greed or revenge. In Insider attack It's easy for insider to do cyber attack because attacker aware about architecture of security system, process and policies. While having insider information it's easy for attacker to steel sensitive and confidential information.

Paytm Extortion Case<sup>1</sup> is best example of insider attack; How Vijay Shekhar Sharma was blackmailed by his personal secretary.

---

<sup>1</sup> Paytm extortion case: How Vijay Shekhar Sharma was blackmailed by his personal secretary.

<https://www.businesstoday.in/current/corporate/how-paytm-vijay-shekhar-sharma-was-blackmailed-by-his-personal-secretary/story/286217.html>

## **External Attack:**

As its name when any external organisation or entity hired to attack on any network known as External Attack. Motive of this kind of attack to damage reputation of targeted organisation or steal information.

For example whenever there is tension in India and Pakistan, hacker of both countries attack on other's government department website not for data or information just only damage reputation.

For cyber criminals with low-risk with low investment business with good returns. For example, if we talk about credit card frauds in India. Hackers get your credit card from a low secured online shopping website where you give your credit card details to place an order. Hackers get information and use your card for online shopping and also sell credit card details in bulk.

Currently there are several news that one sms received on mobile having link to complete KYC of bank account or link PAN card with your Adhar Card when user click on that link his bank balance empty.

Some Cyber Criminals offers cyber attack on-request service. The individual, association or a nation may contact these digital lawbreakers for hacking an association to access some important and confidential information, or do massive DOS attack on their rivals.

On interest of the client the programmers formally known as hackers write codes to create computer virus, malware according to requirements of client. An association affected by a cyber attack, faces reputation loss and also faces money loss, and the contender association will defiantly profit by it.

## **Reasons behind Cyber Crimes**

There are several reasons behind cyber crimes, few are:

- I. **Money:** People motivated to commit cyber crimes are to make easy and quick money.
- II. **Revenge:** Someone says, "Every thing is fare in LOVE and WAR" basically it's not LOVE and WAR it's just "Revenge" when someone try to take his/her revenge with other person or organisation by damaging reputation. It's also known as Cyber Terrorism.
- III. **Fun:** When any amateur person just wants to test latest tool or do cyber crime just for fun.
- IV. **Recognition:** To feel pride when someone hack the highly secured computer networks like any government, security or defense network sites.
- V. **Cyber Espionage:** Government also involved in this activity when they want to keep eye on any

other nation or person or network, reason could be socially economically or politically motivated.

## **How to report a credit or debit card, net banking fraud**

**Do not ignore!**

**What to do in case of fraud:** at the time when you realize that a suspicious transaction has been done on your credit or debit card, inform the bank immediately and block your card Also lodge a complaint with your bank.

**How to file a complaint:** If you a fraud related ATM transaction, Internet banking or any other online transaction. You need to file written complaint and for that make sure that you have following documents:

- Bank Statement with suspicious transactions
- Copy of SMSs of transaction/transactions
- Your ID & Address proof as you given in bank
- Lodge complaint in nearest police station

There are also many apps on internet, in case of fraud done through any mobile app in addition with above mention documents also take a screenshot of that app.

**Where to file the complaint:** A cyber law expert advocate Puneet Bhasin says, "An FIR has to be filed in



the local police station only. In case police refuses to file an FIR, the court can be approached under section 156(3) of the Cr PC".

**Delhi:** <http://205.147.111.155:84/>

**Noida:** <http://www.cccinoida.org/registration>

**Indore:** <http://www.indorepolice.org/cyber-crime.php>

**Vishakhapatnam:**

<http://vizagcitypolice.gov.in/CyberCrimes.html>

**Mumbai:** Email: [cp.thane.online@mahapolice.gov.in](mailto:cp.thane.online@mahapolice.gov.in)

**Who will pay your money:** RBI says, "Customer is not required to pay if the breach has been reported within 03 days of the fraudulent transaction." But if you not reported within 03 days but reported within 07 days then according to RBI notification "the customer liability shall be determined as per the bank's Board approved policy,"

# Malware & It's Type

1. Adware
2. Bot
3. Bug
4. Ransomware
5. Root kit
6. Spyware
7. Browser Hijacking Software
8. Virus
9. Worms
10. Scareware
11. Malware Symptoms
12. Spam
13. Malware Prevention and Removal

## Adware:

Usually Adware used to describe a form of malicious software (malware) which is responsible to show unwanted online advertisements on users computer screen. Sometimes these advertisements appear on computer screen in form of pop-up messages or sometimes "enclosable window" which can't close easily.

There are two ways by which any adware can install on your computer:

Download any pirated, freeware software from internet and install it on your computer. This happens because the author of that freeware or pirated software signed up with adware vendor for revenue generation. Why? Because this is simple way for showing ads on computers just installing a system application on your computer.



*Fig: Adware Full screen popup message*

Second Method is little clever way, suppose you visited a website, maybe it's trusted or may be not and its infected by adware, after few seconds while be on website you will be redirect to another url which will show more popup ads on your computer screen through your web browser.

## Bot

Bot Malware used to take control over a computer completely. Commonly Bot Malware used to infect large number of computers by producing bot network or **botnet**. It a **Self-Propagating** malware which is capable in infecting its host computer or server and back to central server or servers.

Ministry of Electronics and Information Technology Government of India started **Cyber Swachhta Kendra (साइबर स्वच्छता केंद्र)** Botnet Cleaning and Malware Analysis Centre.

Visit : <https://www.cyberswachhtakendra.gov.in/>

Welcome to **Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra)**

The "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. The "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre) is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber eco system in the country. This centre operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies. This website provides information and tools to users to secure their systems/devices. This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.

Stop Neglecting security warnings. Protect before you connect.

Passwords are key to your personal information, make habit of using strong passwords and change them regularly.

The "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections.

## Ransomware

As suggests by name, demands a ransom from you to fix things back on track on your computer which was infected by this malware.

The main issue with ransomware malware spread extremely fast across networks, organizations, and countries, encrypt all files in network or system and make them inaccessible. For demanding payment in

crypto currency a ransom note pops up for decrypting the files.

The encrypted files could eventually get destroyed if the ransom is not paid and hence ransomware should be seen as one of the most devastating forms of malware.

Mostly ransomware spread through social engineering are they are Trojans. In some cases, after paying ransom hackers refuse to decrypt files.

## **Types of Ransomware**

- 1. Crypto Ransomware:** Encrypts important or valuable files on a computer that user cannot access them.
- 2. Locker Ransomware:** It does not encrypt the files it locks the victim's device, preventing them from using it and demand ransom to unlock.

## **10 Ransomware Examples**

**1. Locky:** First Release in 2016 attack by an organized group of hackers ability to encrypt over 160 file types by tricking victims to install it via fake emails with infected attachments also called phishing form of social engineering.

**2. WannaCry:** WannaCry ransomware allegedly created by the United States National Security Agency

and leaked by the Shadow Brokers group that spread across 150 countries in 2017 and affected 230,000 computers globally. WannaCry Ransomware hit one third hospitals in the United Kingdom costing the NHS an estimated £92 million. For demanding ransom hackers used Bitcoin crypto currency.

**3. Bad Rabbit:** Its 2017 attack spread using drive-by attack method where insecure website used for attack. During Bad Rabbit ransomware attack user visit a website not knowing that they have been compromised by hacker. In this attack user's computer infected when they click on "install" something that is actually malware which is known as malware dropper.

Usually Bad Rabbit ransomware malware used a fake request to install Adobe Flash player to display website features as malware dropper.

**4. Ryuk:** Spreded in 2018 Ryuk disabled the Windows OS System Restore option, make it impossible to restore encrypted files and network drives without backup. Reports estimated funds raised from the attack over US \$6,40,000.

**5. Trolldesh:** Spred in 2015 through spam email with infected attachments or links. This malware communicate directly with victims over email for ransoms. Ever hackers negotiated discounts for victims.

**6. Jigsaw:** started in 2016 got its name Jigsaw as it featured an image of the puppet from the Saw film franchise. Jigsaw deleted more of the victim's files every hour that the ransom demand was left unpaid.

**7. CryptoLocker:** Spread in 2007 through infected email attachments. Once it finds important and valuable files in your computer encrypt and hold to ransom.

**8. Petya:** Attacked in 2016. this ransomware encrypts the victim's entire hard drive rather than encrypting specific files. This ransomware does this by encrypting MFT (master file table) making it impossible to access file on the disk.

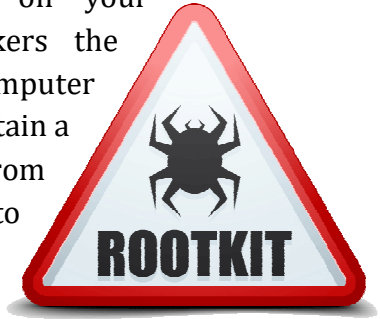
**9. GoldenEye:** This basically resurgence of Petya ransomware led to a global ransomware attack that happened in 2017. Dubbed WannaCry's 'deadly sibling', GoldenEye hit over 2,000 targets, including prominent oil producers in Russia and several banks.

**10. GandCrab:** GandCrab is a rather unsavory ransomware attack that threatened to reveal victim's porn watching habits. Claiming to have hijacked webcam of users computer, hackers demanded a ransom or otherwise GandCrab cybercriminals would make the embarrassing footage public.



# RootKit

Rootkit can remain hidden on your computer. Rootkits give hackers the ability to take access of your computer remotely. This malware can contain a number of tools, ranging from programs that allow hackers to steal your passwords and remote access which make easy to get your credit card information, internet banking login details, your email and important online account login details.



Rootkit are especially hard to detect Sometimes the only way to completely eliminate a well-hidden rootkit is to erase your computer's operating system and rebuild from scratch.

## Type of RootKit

**1. Firmware or Hardware Rootkit:** Rootkit malware could infect your computer's BIOS or hard drive. Even it can infect your router. Usually Hackers use these rootkits to intercept data written on the disk.

**2. Bootloader rootkit:** Bootloader is an important tool for your computer. Bootloader loads your computer's OS (operating system) when you turn on your computer machine. It attacks on bootloader system, replacing your computer's legitimate bootloader with a

hacked one which means that this rootkit is activated even before your computer's OS turns on.

**3. Memory rootkit:** Memory rootkit hides in computer's Random Access Memory (RAM). Memory rootkits will carry out harmful activities in the background. The good news about this memory rootkit which have a short lifespan. This rootkit only live in computer's Random Access Momory (RAM) and will disappear once you reboot your computer system.

**4. Application rootkit:** It replaces standard files with rootkit files in your computer system. Application rootkit might also change the way standard applications work. This application rootkits might also infect programs such as Ms-Word, Paint, WordPad or Notepad. Each and every time when you run these programs or any program which is infected by application rootkit, you will give access of your computer to hackers. It's difficult to detect application rootkit because infected programs will still run normally on your system.

**5. Kernel mode rootkits:** Kernel mode rootkits targets the core operating system of your computer. Hackers / Cybercriminals can use these to change how your operating system functions. Hackers just need to add their own code to it. This makes easy to get access of your computer to steal your personal information.

## Spyware:

It's software that aims to gather information without their knowledge about a person or organisation and send information to another person or organisation without the consumer's consent.



It takes control over a device sends confidential and valuable information to another person or organisation without the consumer's knowledge.

There are 3 types of spyware and each uses unique tricks

**Adware.** Adware spyware basically for track your web browser tracks your browser's history and downloads. Adware will display advertisements for the same or related products or services which you are looking or searching or you made purchase that product earlier. Its used for marketing purpose to increase sales by displaying ads of different products or services by tracking your online activity.

**Trojan.** This spyware used to get credit card information and adhar card information. This spyware controlled by third parties. It may appear to be Flash or Java player update upon download.

**System Monitors.** System Monitors can capture everything which displays on your computer screen. System Monitors can records all keystrokes, webpages

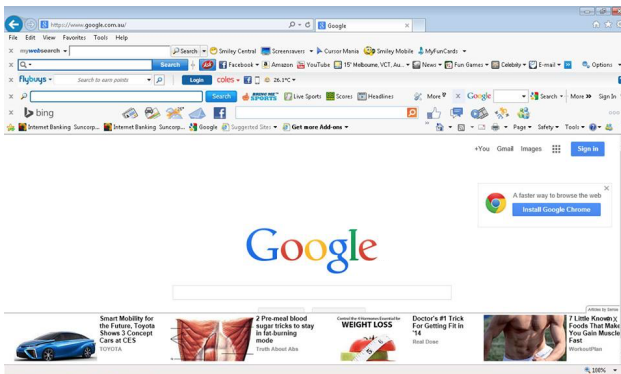
which you visited, chat room dialogs, email everything which shows on your computer screen. Its also known as **Keylogger**.

## How to recognize spyware on your device

- Device is crashes or slow crashes unexpectedly.
- Device is running out of hard drive space without installing other heavy softwares or applications.
- Get pop-ups when you are offline or online.

## Browser Hijacking

Browser hijacking is a method to change the web browser setting without a user's permission form of unwanted software. It's motive to inject unwanted advertising into the user's browser. This may replace the existing error page, error page, or search engine with its own.



In above screenshot you can see that in default microsoft operating system web browser internet explorer there are few unwanted advertisement which is displaying by third party softwares.

### **Signs of your Browser is Hijacked:**

- Searches that are redirected to another different websites
- Multiple pop-up advertisement alerts at same time
- Web pages with Slow-loading
- Multiple toolbars on a web browser which is not installed by user

### **Virus**

A malicious code designed to spread from host to host by itself without the user's knowledge to perform malicious actions called computer virus. It imposes harm to a computer by destroying computer data, corrupting system files. The reason for designing a computer virus is to attack vulnerable systems to steal confidential information and gain admin control.



Different types of computer virus

- Boot sector virus
- Web scripting virus
- Web scripting virus

- Resident virus
- Direct action virus
- Polymorphic virus
- File infector virus
- Multipartite virus
- Macro virus

<https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html>

## **Worms**

A type of malware that spreads copies of itself from computer to another computer. It can replicate itself without any human interaction and it doesn't need attach itself with any software program in order to cause damage.

### **How Worms works on Computer System**

Worms can be transmitted through software program vulnerabilities in computer system. Or computer worms ought to arrive as attachments in junk/spam mail emails or IMs (immediate messages). After opening automatically download the pc malicious program or these documents should provide a hyperlink to a malicious internet site. The malicious program silently goes to work and infects the device without the user's knowledge Once it's installed.

Worms can delete and regulate documents, and they are able to even inject additional malicious software program onto a personal computer. Sometimes a personal computer malicious program's motive is most effective to depleting gadget resources by making copies of itself over — , such as difficult bandwidth or power space by using overloading a shared network. In addition to wreaking havoc on a laptop's resources, worms also can thief data, deploy a backdoor, and allow a hacker to benefit manage over a laptop and its system settings.

## Features<sup>2</sup>

- 1. Contagiousness-** Computer worms are more infectious than traditional viruses. They not only infect local computers, but also all servers and clients on the network based on the local computer. Worms can easily spread through shared folders, e-mails, malicious web pages, and servers with a large number of vulnerabilities in the network.
- 2. Exploit attacks-** Because a worm is not limited by the host program, worms can take advantage of various operating system vulnerabilities to carry

---

<sup>2</sup> [https://en.wikipedia.org/wiki/Computer\\_worm](https://en.wikipedia.org/wiki/Computer_worm)

out active attacks. For example, the "Nimda"<sup>3</sup> virus exploits vulnerabilities to attack.

- 3. Independence-** Worms Computer viruses generally require a host program. Worms virus writes its own code into the host program. The written virus program is executed first, causing infection and damage when virus runs. A worm does not need a host program, as it is an independent program or code chunk. Therefore, it is not restricted by the host program, but can run independently and actively carry out attacks.
- 4. Complexity-** Some worms are combined with web page scripts, and are hidden in HTML pages using VBScript, ActiveX and other technologies. When a user accesses a webpage containing a virus, the virus automatically resides in memory and waits to be triggered. There are also some worms that are combined with backdoor programs or Trojan horses, such as "Code Red".<sup>4</sup>

---

<sup>3</sup> <https://en.wikipedia.org/wiki/Nimda>

<sup>4</sup> [https://en.wikipedia.org/wiki/Code\\_Red\\_\(computer\\_worm\)](https://en.wikipedia.org/wiki/Code_Red_(computer_worm))



## Scareware-

Scareware is a form of malware which uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software. Scareware is part of a class of malicious software that includes rogue security software, ransomware and other scam software that tricks users into believing their computer is infected with a virus, then suggests that they download and pay for fake antivirus software to remove it. Usually the virus is fictional and the software is non-functional or malware itself. According to the Anti-Phishing Working Group, the number of scareware packages in circulation rose from 2,850 to 9,287 in the second half of 2008. In the first half of 2009, the APWG identified a 585% increase in scareware programs.



The "scareware" label can also apply to any application or virus which pranks users with intent to cause anxiety or panic.<sup>5</sup>

## **Legal Action**

<sup>6</sup>In 2005, Microsoft and Washington state successfully sued Secure Computer (makers of Spyware Cleaner) for \$1 million over charges of using scareware pop-ups. Washington's attorney general has also brought lawsuits against Securelink Networks, High Falls Media, and the makers of Quick Shield.

In October 2008, Microsoft and the Washington attorney general filed a lawsuit against two Texas firms, Branch Software and Alpha Red, producers of the Registry Cleaner XP scareware. The lawsuit alleges that the company sent incessant pop-ups resembling system warnings to consumers' personal computers stating "CRITICAL ERROR MESSAGE! - REGISTRY DAMAGED AND CORRUPTED", before instructing users to visit a web site to download Registry Cleaner XP at a cost of \$39.95.

On December 2, 2008, the U.S. Federal Trade Commission ("FTC") filed a Complaint in federal court against Innovative Marketing, Inc., ByteHosting Internet

---

<sup>5</sup> <https://en.wikipedia.org/wiki/Scareware>

<sup>6</sup> <https://en.wikipedia.org/wiki/Scareware>

Services, LLC, as well as individuals Sam Jain, Daniel Sundin, James Reno, Marc D'Souza, and Kristy Ross. The Complaint also listed Maurice D'Souza as a Relief Defendant, alleged that he held proceeds of wrongful conduct but not accusing him of violating any law. The FTC alleged that the other Defendants violated the FTC Act by deceptively marketing software, including WinFixer, WinAntivirus, DriveCleaner, ErrorSafe, and XP Antivirus. According to the complaint, the Defendants falsely represented that scans of a consumer's computer showed that it had been compromised or infected and then offered to sell software to fix the alleged problems.

## **Email Spam**

Email spam, also referred to as junk email, is unsolicited messages sent in bulk by email (spamming).

The name comes from Spam luncheon meat by way of a Monty Python sketch in which Spam is ubiquitous, unavoidable, and repetitive. Email spam has steadily grown since the early 1990s, and by 2014 was estimated to account for around 90% of total email traffic.



Since the expense of the spam is borne mostly by the recipient, it is effectively postage due advertising. This makes it an excellent example of a negative externality.

The legal definition and status of spam varies from one jurisdiction to another, but nowhere have laws and lawsuits been particularly successful in stemming spam.

Most email spam messages are commercial in nature. Whether commercial or not, many are not only annoying, but also dangerous because they may contain links that lead to phishing web sites or sites that are hosting malware - or include malware as file attachments.

Spammers collect email addresses from chat rooms, websites, customer lists, newsgroups, and viruses that harvest users' address books. These collected email addresses are sometimes also sold to other spammers.

# Kinds of Cyber Crime

## Cyber Stalking

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass.

Cyberstalking is often accompanied by realtime or offline stalking. In many jurisdictions, such as California, both are criminal offenses. Both are motivated by a desire to control, intimidate or influence a victim. A stalker may be an online stranger or a person whom the target knows. They may be anonymous and solicit involvement of other people online who do not even know the target.

Cyberstalking is a criminal offense under various state anti-stalking, slander and harassment laws. A conviction can result in a restraining order, probation, or criminal penalties against the assailant, including jail.

Cyberstalking is a technologically-based "attack" on one person who has been targeted specifically for that attack for reasons of anger, revenge or control. Cyberstalking can take many forms, including:

1. harassment, embarrassment and humiliation of the victim
2. emptying bank accounts or other economic control such as ruining the victim's credit score.
3. harassing family, friends and employers to isolate the victim
4. scare tactics to instill fear and more

## **Identification and detection**

When identifying cyberstalking "in the field," and particularly when considering whether to report it to any kind of legal authority, the following features or combination of features can be considered to characterize a true stalking situation: malice, premeditation, repetition, distress, obsession, vendetta, no legitimate purpose, personally directed, disregarded warnings to stop, harassment and threats.

A number of key factors have been identified in cyberstalking:

- False accusations: Many cyberstalkers try to damage the reputation of their victim and turn other people against them. They post false information about them on websites. They may set up their own websites, blogs or user pages for this

purpose. They post allegations about the victim to newsgroups, chat rooms, or other sites that allow public contributions such as Wikipedia or Amazon.com.

- Attempts to gather information about the victim: Cyberstalkers may approach their victim's friends, family and work colleagues to obtain personal information. They may advertise for information on the Internet, or hire a private detective.
- Monitoring their target's online activities and attempting to trace their IP address in an effort to gather more information about their victims.
- Encouraging others to harass the victim: Many cyberstalkers try to involve third parties in the harassment. They may claim the victim has harmed the stalker or his/her family in some way, or may post the victim's name and telephone number in order to encourage others to join the pursuit.
- False victimization: The cyberstalker will claim that the victim is harassing him or her. Bocij writes that this phenomenon has been noted in a number of well-known cases.
- Attacks on data and equipment: They may try to damage the victim's computer by sending viruses.
- Ordering goods and services: They order items or subscribe to magazines in the victim's name. These often involve subscriptions to pornography or ordering sex toys then having them delivered to the victim's workplace.



- Arranging to meet: Young people face a particularly high risk of having cyberstalkers try to set up meetings between them.
- The posting of defamatory or derogatory statements: Using web pages and message boards to incite some response or reaction from their victim.

## **Types of Cyber Stalking**

### **Stalking by Strangers<sup>7</sup>**

According to Joey Rushing, a District Attorney of Franklin County, Alabama, there is no single definition of a cyberstalker - they can be either strangers to the victim or have a former/present relationship. "[Cyberstalkers] come in all shapes, sizes, ages and backgrounds. They patrol Web sites looking for an opportunity to take advantage of people."

### **Gender-Based Stalking**

Harassment and stalking because of gender online, also known as online gender-based violence, is common, and can include rape threats and other threats of violence, as well as the posting of the victim's personal information. It is blamed for limiting victims' activities online or driving them offline entirely, thereby impeding their participation in online life and

---

<sup>7</sup> <https://en.wikipedia.org/wiki/Cyberstalking>

undermining their autonomy, dignity, identity, and opportunities.

## **Of Intimate Partners**

Cyberstalking of intimate partners is the online harassment of a current or former romantic partner. It is a form of domestic violence, and experts say its purpose is to control the victim in order to encourage social isolation and create dependency. Harassers may send repeated insulting or threatening e-mails to their victims, monitor or disrupt their victims' e-mail use, and use the victim's account to send e-mails to others posing as the victim or to purchase goods or services the victim does not want. They may also use the Internet to research and compile personal information about the victim, to use in order to harass him or her.

## **Of Celebrities and Public Persons**

Profiling of stalkers shows that almost always they stalk someone they know or, via delusion, think they know, as is the case with stalkers of celebrities or public persons in which the stalkers feel they know the celebrity even though the celebrity does not know them. As part of the risk they take for being in the public eye, celebrities and public figures are often

targets of lies or made-up stories in tabloids as well as by stalkers, some even seeming to be fans.

In one noted case in 2011, actress Patricia Arquette quit Facebook after alleged cyberstalking. In her last post, Arquette explained that her security warned her Facebook friends to never accept friend requests from people they do not actually know. Arquette stressed that just because people seemed to be fans did not mean they were safe. The media issued a statement that Arquette planned to communicate with fans exclusively through her Twitter account in the future.

### **By anonymous Online Mobs**

Web 2.0 technologies have enabled online groups of anonymous people to self-organize to target individuals with online defamation, threats of violence and technology-based attacks. These include publishing lies and doctored photographs, threats of rape and other violence, posting sensitive personal information about victims, e-mailing damaging statements about victims to their employers, and manipulating search engines to make damaging material about the victim more prominent. Victims frequently respond by adopting pseudonyms or going offline entirely.

Experts attribute the destructive nature of anonymous online mobs to group dynamics, saying that groups with

homogeneous views tend to become more extreme. As members reinforce each others' beliefs, they fail to see themselves as individuals and lose a sense of personal responsibility for their destructive acts. In doing so they dehumanize their victims, becoming more aggressive when they believe they are supported by authority figures. Internet service providers and website owners are sometimes blamed for not speaking out against this type of harassment.

A notable example of online mob harassment was the experience of American software developer and blogger Kathy Sierra. In 2007 a group of anonymous individuals attacked Sierra, threatening her with rape and strangulation, publishing her home address and Social Security number, and posting doctored photographs of her. Frightened, Sierra cancelled her speaking engagements and shut down her blog, writing "I will never feel the same. I will never be the same."

### **Corporate Cyberstalking**

Corporate cyberstalking is when a company harasses an individual online, or an individual or group of individuals harasses an organization. Motives for corporate cyberstalking are ideological, or include a desire for financial gain or revenge.

## **Child Pornography**

Child pornography<sup>8</sup> is a form of pornography showing children which is against the law in many countries as well as in India. Child pornography is most often made by taking pictures or videos, or more rarely sound recordings, of children who are wearing less clothing than usual, wearing no clothing, or having sex. Child pornography is sometimes called "child sexual abuse images" because it is images (pictures) of a child who is being sexually abused. Child pornography can also be drawn, written, or created by a computer. In that case, it is called "simulated child pornography" or "virtual child pornography": the child in the pornography is simulated or virtual, meaning the child is not real.

## **Software Piracy or Copyright Infringement**

Software Piracy or Copyright Infringement<sup>9</sup> (colloquially referred to as piracy) is the use of works protected by copyright law without permission for a usage where such permission is required, thereby infringing certain exclusive rights granted to the copyright holder, such as the right to reproduce,

---

<sup>8</sup> [https://en.wikipedia.org/wiki/Legality\\_of\\_child\\_pornography](https://en.wikipedia.org/wiki/Legality_of_child_pornography)

<sup>9</sup> [https://en.wikipedia.org/wiki/Copyright\\_infringement](https://en.wikipedia.org/wiki/Copyright_infringement)

distribute, display or perform the protected work, or to make derivative works. The copyright holder is typically the work's creator, or a publisher or other business to whom copyright has been assigned. Copyright holders routinely invoke legal and technological measures to prevent and penalize copyright infringement.

Copyright infringement disputes are usually resolved through direct negotiation, a notice and take down process, or litigation in civil court. Egregious or large-scale commercial infringement, especially when it involves counterfeiting, is sometimes prosecuted via the criminal justice system. Shifting public expectations, advances in digital technology, and the increasing reach of the Internet have led to such widespread, anonymous infringement that copyright-dependent industries now focus less on pursuing individuals who seek and share copyright-protected content online[citation needed], and more on expanding copyright law to recognize and penalize, as indirect infringers, the service providers and software distributors who are said to facilitate and encourage individual acts of infringement by others.

Estimates of the actual economic impact of copyright infringement vary widely and depend on many factors. Nevertheless, copyright holders, industry representatives, and legislators have long characterized copyright infringement as piracy or theft – language

which some U.S. courts now regard as pejorative or otherwise contentious.

## **Terminology**

### **"Piracy"**

Pirated edition of German philosopher Alfred Schmidt (Amsterdam, ca. 1970)

The term "piracy" has been used to refer to the unauthorized copying, distribution and selling of works in copyright.[8] The practice of labelling the infringement of exclusive rights in creative works as "piracy" predates statutory copyright law. Prior to the Statute of Anne in 1710, the Stationers' Company of London in 1557 received a Royal Charter giving the company a monopoly on publication and tasking it with enforcing the charter. Article 61 of the 1994 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) requires criminal procedures and penalties in cases of "willful trademark counterfeiting or copyright piracy on a commercial scale." Piracy traditionally refers to acts of copyright infringement intentionally committed for financial gain, though more recently, copyright holders have described online copyright infringement, particularly in relation to peer-to-peer file sharing networks, as "piracy".

Richard Stallman and the GNU Project have criticized the use of the word "piracy" in these situations, saying that publishers use the word to refer to "copying they don't approve of" and that "they [publishers] imply that it is ethically equivalent to attacking ships on the high seas, kidnapping and murdering the people on them."

## **"Theft"**

Copyright holders frequently refer to copyright infringement as theft, "although such misuse has been rejected by legislatures and courts". In copyright law, infringement does not refer to theft of physical objects that take away the owner's possession, but an instance where a person exercises one of the exclusive rights of the copyright holder without authorization. Courts have distinguished between copyright infringement and theft.[13] For instance, the United States Supreme Court held in *Dowling v. United States* (1985) that bootleg phonorecords did not constitute stolen property. Instead,

## **"Freebooting"**

The term "freebooting" has been used to describe the unauthorized copying of online media, particularly videos, onto websites such as Facebook, YouTube or



Twitter. The word itself had already been in use since the 16th century, referring to pirates, and meant "looting" or "plundering". This form of the word – a portmanteau of "freeloading" and "bootlegging" – was suggested by YouTuber and podcaster Brady Haran in the podcast Hello Internet. Haran advocated the term in an attempt to find a phrase more emotive than "copyright infringement", yet more appropriate than "theft".

## Cyberterrorism

Cyberterrorism<sup>10</sup> is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

---

<sup>10</sup>

<https://en.wikipedia.org/wiki/Cyberterrorism#:~:text=The%20FBI%2C%20another%20United%20States,subnational%20groups%20or%20clandestine%20agents>".

Cyberterrorism is a controversial term. Some authors opt for a very narrow definition, relating to deployment by known terrorist organizations of disruption attacks against information systems for the primary purpose of creating alarm, panic, or physical disruption. Other authors prefer a broader definition, which includes cybercrime. Participating in a cyberattack affects the terror threat perception, even if it isn't done with a violent approach. By some definitions, it might be difficult to distinguish which instances of online activities are cyberterrorism or cybercrime.

Cyberterrorism can be also defined as the intentional use of computers, networks, and public internet to cause destruction and harm for personal objectives. Experienced cyberterrorists, who are very skilled in terms of hacking can cause massive damage to government systems, hospital records, and national security programs, which might leave a country, community or organization in turmoil and in fear of further attacks. The objectives of such terrorists may be political or ideological since this can be considered a form of terror.

There is much concern from government and media sources about potential damage that could be caused by cyberterrorism, and this has prompted efforts by government agencies such as the Federal Bureau of Investigations (FBI) and the Central

Intelligence Agency (CIA) to put an end to cyber attacks and cyberterrorism.

There have been several major and minor instances of cyberterrorism. Al-Qaeda utilized the internet to communicate with supporters and even to recruit new members.[5] Estonia, a Baltic country which is constantly evolving in terms of technology, became a battleground for cyberterror in April, 2007 after disputes regarding the removal of a WWII soviet statue located in Estonia's capital Tallinn.

## **Defining Cyberterrorism**

The use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terroristic threats made via electronic communication.

## Types of Cyberterror Capability

In 1999 the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California defined three levels of cyberterror capability:

- **Simple-Unstructured:** the capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target-analysis, command-and-control, or learning capability.
- **Advanced-Structured:** the capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking-tools. The organization possesses an elementary target-analysis, command-and-control, and learning capability.
- **Complex-Coordinated:** the capability for a coordinated attack capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target-analysis, command-and-control, and organization learning-capability.

## **Phishing**

Phishing<sup>11</sup> is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or IT administrators.

Attempts to deal with phishing incidents include legislation, user training, public awareness, and technical security measures (the latter being due to phishing attacks frequently exploiting weaknesses in current web security).

The word itself is a neologism created as a homophone of fishing.

---

<sup>11</sup> <https://en.wikipedia.org/wiki/Phishing>

## **Types of Phishing**

### **Spear phishing**

Phishing attempts directed at specific individuals or companies is known as spear phishing.[8] In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their target to increase their probability of success.

The first study of social phishing, a type of spear-phishing attack that leverages friendship information from social networks, yielded over 70% success rate in experiments.

Threat Group-4127 (Fancy Bear) used spear phishing tactics to target email accounts linked to Hillary Clinton's 2016 presidential campaign. They attacked more than 1,800 Google accounts and implemented the accounts-google.com domain to threaten targeted users.

### **Whaling**

The term whaling refers to spear phishing attacks directed specifically at senior executives and other high-profile targets. In these cases, the content will be crafted to target an upper manager and the person's role in the company. The content of a whaling attack email may be an executive issue such as a subpoena or customer complaint.

## **Catphishing/Catfishing**

Catphishing (spelled with a “ph”) is a type of online deception that involves getting to know someone closely in order to gain access to information and/or resources, usually in the control of the mark, or to otherwise get control over the conduct of the target.

Catfishing (spelled with an “f”), a similar but distinct concept, involves a person creating a social network presence as a sock puppet or fictional person in order to finagle someone into a (usually) romantic relationship. This usually begins online, with the hope or promise of it progressing to real-life romance. This is never the object of the perpetrator; in general, he is seeking access to the mark's money or resources, or to receive gifts or other consideration from the victim. Occasionally, it may be a form of self-serving attention-getting.[18]

## **Clone phishing**

Clone phishing is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original. Typically this requires either the sender or recipient to

have been previously hacked for the malicious third party to obtain the legitimate email.

### **Link Manipulation**

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers. In the following example URL, <http://www.yourbank.example.com/>, it appears as though the URL will take you to the example section of the yourbank website; actually this URL points to the "yourbank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link (the text between the <A> tags) suggest a reliable destination, when the link actually goes to the phishers' site. Many desktop email clients and web browsers will show a link's target URL in the status bar while hovering the mouse over it. This behavior, however, may in some circumstances be overridden by the phisher. Equivalent mobile apps generally do not have this preview feature.

Internationalized domain names (IDN) can be exploited via IDN spoofing or homoglyph attacks, to create web addresses visually identical to a legitimate site, that lead instead to malicious version. Phishers have taken advantage of a similar risk, using open URL redirectors on the websites of trusted organizations to disguise



malicious URLs with a trusted domain. Even digital certificates do not solve this problem because it is quite possible for a phisher to purchase a valid certificate and subsequently change content to spoof a genuine website, or, to host the phish site without SSL at all.

### **Filter Evasion**

Phishers have sometimes used images instead of text to make it harder for anti-phishing filters to detect the text commonly used in phishing emails. In response, more sophisticated anti-phishing filters are able to recover hidden text in images using OCR (optical character recognition).

### **Website forgery**

Some phishing scams use JavaScript commands in order to alter the address bar of the website they lead to. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL.

An attacker can also potentially use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to

spot without specialist knowledge. Such a flaw was used in 2006 against PayPal.

To avoid anti-phishing techniques that scan websites for phishing-related text, phishers sometimes use Flash-based websites (a technique known as phlashing). These look much like the real website, but hide the text in a multimedia object.

### **Covert Redirect**

Covert redirect is a subtle method to perform phishing attacks that makes links appear legitimate, but actually redirect a victim to an attacker's website. The flaw is usually masqueraded under a log-in popup based on an affected site's domain. It can affect OAuth 2.0 and OpenID based on well-known exploit parameters as well. This often makes use of open redirect and XSS vulnerabilities in the third-party application websites. Users may also be redirected to phishing websites covertly through malicious browser extensions.

Normal phishing attempts can be easy to spot because the malicious page's URL will usually be different from the real site link. For covert redirect, an attacker could use a real website instead by corrupting the site with a malicious login popup dialogue box. This makes covert redirect different from others.

For example, suppose a victim clicks a malicious phishing link beginning with Facebook. A popup window from Facebook will ask whether the victim would like to authorize the app. If the victim chooses to

authorize the app, a "token" will be sent to the attacker and the victim's personal sensitive information could be exposed. These information may include the email address, birth date, contacts, and work history. In case the "token" has greater privilege, the attacker could obtain more sensitive information including the mailbox, online presence, and friends list. Worse still, the attacker may possibly control and operate the user's account. Even if the victim does not choose to authorize the app, he or she will still get redirected to a website controlled by the attacker. This could potentially further compromise the victim.

This vulnerability was discovered by Wang Jing, a Mathematics Ph.D. student at School of Physical and Mathematical Sciences in Nanyang Technological University in Singapore. Covert redirect is a notable security flaw, though it is not a threat to the Internet worth significant attention.

## **Social Engineering**

Users can be encouraged to click on various kinds of unexpected content for a variety of technical and social reasons. For example, a malicious attachment might masquerade as a benign linked Google Doc.

Alternatively users might be outraged by a fake news story, click a link and become infected.

## **Voice Phishing**

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

## **Hacking**

Hacking is method where a hacker is any skilled computer expert who uses their technical knowledge to overcome a problem. While "hacker" can refer to any skilled computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems.

## **Spamming**

Spamming is the use of messaging systems to send an unsolicited message (spam) to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, or for any prohibited purpose (especially the fraudulent purpose of phishing). While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam,

Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social spam, spam mobile apps, television advertising and file sharing spam. It is named after Spam, a luncheon meat, by way of a Monty Python sketch about a restaurant that has Spam in almost every dish and where vikings annoyingly sing "Spam" over and over again.

Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, servers, infrastructures, IP ranges, and domain names, and it is difficult to hold senders accountable for their mass mailings. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the volume. Spamming has been the subject of legislation in many jurisdictions

## **Types of Spam**

### **Email Spam**

Email spam, also known as unsolicited bulk email (UBE), or junk mail, is the practice of sending unwanted email messages, frequently with commercial content, in large quantities. Spam in email started to become a problem when the Internet was opened for commercial use in the mid-1990s. It grew exponentially over the

following years, and by 2007 it constituted about 80% to 85% of all e-mail, by a conservative estimate. Pressure to make email spam illegal has resulted in legislation in some jurisdictions, but less so in others. The efforts taken by governing bodies, security systems and email service providers seem to be helping to reduce the volume of email spam. According to "2014 Internet Security Threat Report, Volume 19" published by Symantec Corporation, spam volume dropped to 66% of all email traffic.

An industry of email address harvesting is dedicated to collecting email addresses and selling compiled databases. Some of these address-harvesting approaches rely on users not reading the fine print of agreements, resulting in their agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spam such as that generated by the social networking site Quechup.

### **Instant Messaging**

Instant messaging spam makes use of instant messaging systems. Although less prevalent than its e-mail counterpart, according to a report from Ferris Research, 500 million spam IMs were sent in 2003, twice the level of 2002.

### **Newsgroup and Forum**

Newsgroup spam is a type of spam where the targets are Usenet newsgroups. Spamming of Usenet

newsgroups actually pre-dates e-mail spam. Usenet convention defines spamming as excessive multiple posting, that is, the repeated posting of a message (or substantially similar messages). The prevalence of Usenet spam led to the development of the Breidbart Index as an objective measure of a message's "spamminess".

Forum spam is the creation of advertising messages on Internet forums. It is generally done by automated spambots. Most forum spam consists of links to external sites, with the dual goals of increasing search engine visibility in highly competitive areas such as weight loss, pharmaceuticals, gambling, pornography, real estate or loans, and generating more traffic for these commercial websites. Some of these links contain code to track the spambot's identity; if a sale goes through, the spammer behind the spambot earns a commission.

### **Mobile Phone**

Mobile phone spam is directed at the text messaging service of a mobile phone. This can be especially irritating to customers not only for the inconvenience, but also because of the fee they may be charged per text message received in some markets. To comply with CAN-SPAM regulations in the US, SMS messages now must provide options of HELP and STOP, the latter to end communication with the advertiser via SMS altogether.

Despite the high number of phone users, there has not been so much phone spam, because there is a charge for sending SMS. Recently, there are also observations of mobile phone spam delivered via browser push notifications. These can be a result of allowing websites which are malicious or delivering malicious ads to send a user notifications.

### **Social Networking Spam**

Facebook and Twitter are not immune to messages containing spam links. Spammers hack into accounts and send false links under the guise of a user's trusted contacts such as friends and family. As for Twitter, spammers gain credibility by following verified accounts such as that of Lady Gaga; when that account owner follows the spammer back, it legitimizes the spammer. Twitter has studied what interest structures allow their users to receive interesting tweets and avoid spam, despite the site using the broadcast model, in which all tweets from a user are broadcast to all followers of the user. Spammers, out of malicious intent, post either unwanted (or irrelevant) information or spread misinformation on social media platforms.

### **Social Spam**

Spreading beyond the centrally managed social networking platforms, user-generated content increasingly appears on business, government, and nonprofit websites worldwide. Fake accounts and



comments planted by computers programmed to issue social spam can infiltrate these websites.

### **Blog and Guestbook**

Blog spam is spamming on weblogs. In 2003, this type of spam took advantage of the open nature of comments in the blogging software Movable Type by repeatedly placing comments to various blog posts that provided nothing more than a link to the spammer's commercial web site. Similar attacks are often performed against wikis and guestbooks, both of which accept user contributions. Another possible form of spam in blogs is the spamming of a certain tag on websites such as Tumblr.

### **Spam Targeting Video Sharing Sites**

In actual video spam, the uploaded movie is given a name and description with a popular figure or event that is likely to draw attention, or within the video a certain image is timed to come up as the video's thumbnail image to mislead the viewer, such as a still image from a feature film, purporting to be a part-by-part piece of a movie being pirated, e.g. Big Buck Bunny Full Movie Online - Part 1/10 HD, a link to a supposed keygen, trainer, ISO file for a video game, or something similar. The actual content of the video ends up being totally unrelated, a Rickroll, offensive, or simply on-screen text of a link to the site being promoted.[31] In some cases, the link in question may lead to an online

survey site, a password-protected archive file with instructions leading to the aforementioned survey (though the survey, and the archive file itself, is worthless and doesn't contain the file in question at all), or in extreme cases, malware.[32] Others may upload videos presented in an infomercial-like format selling their product which feature actors and paid testimonials, though the promoted product or service is of dubious quality and would likely not pass the scrutiny of a standards and practices department at a television station or cable network.

### **VoIP Spam**

VoIP spam is VoIP (Voice over Internet Protocol) spam, usually using SIP (Session Initiation Protocol). This is nearly identical to telemarketing calls over traditional phone lines. When the user chooses to receive the spam call, a pre-recorded spam message or advertisement is usually played back. This is generally easier for the spammer as VoIP services are cheap and easy to anonymize over the Internet, and there are many options for sending mass number of calls from a single location. Accounts or IP addresses being used for VoIP spam can usually be identified by a large number of outgoing calls, low call completion and short call length.

### **Academic Search**

Academic search engines enable researchers to find academic literature and are used to obtain citation data

for calculating performance metrics such as the H-index and impact factor. Researchers from the University of California, Berkeley and OvGU demonstrated that most (web-based) academic search engines, especially Google Scholar are not capable of identifying spam attacks. The researchers manipulated the citation counts of articles, and managed to make Google Scholar index complete fake articles, some containing advertising.

### **Mobile Apps**

Spamming in mobile app stores include

- I. apps that were automatically generated and as a result do not have any specific functionality or a meaningful description;
- II. multiple instances of the same app being published to obtain increased visibility in the app market; and
- III. apps that make excessive use of unrelated keywords to attract users through unintended searches.

### **Cross-Site Scripting**

Cross-site scripting<sup>12</sup> (XSS) is a type of computer security vulnerability typically found in web

---

<sup>12</sup> [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)

applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec up until 2007. In 2017, XSS attacks were still considered a major threat vector. XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

## **Types of Cross Site Scripting**

### **Non-Persistent (reflected)**

The non-persistent (or reflected) cross-site scripting vulnerability is by far the most basic type of web vulnerability. These holes show up when the data provided by a web client, most commonly in HTTP query parameters (e.g. HTML form submission), is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the content.

Because HTML documents have a flat, serial structure that mixes control statements, formatting, and the

actual content, any non-validated user-supplied data included in the resulting page without proper HTML encoding, may lead to markup injection. A classic example of a potential vector is a site search engine: if one searches for a string, the search string will typically be redisplayed verbatim on the result page to indicate what was searched for. If this response does not properly escape or reject HTML control characters, a cross-site scripting flaw will ensue.

A reflected attack is typically delivered via email or a neutral web site. The bait is an innocent-looking URL, pointing to a trusted site but containing the XSS vector. If the trusted site is vulnerable to the vector, clicking the link can cause the victim's browser to execute the injected script.

### **Persistent (or stored)**

A persistent cross-zone scripting vulnerability coupled with a computer worm allowed execution of arbitrary code and listing of file system contents via a QuickTime movie on MySpace.

The persistent (or stored) XSS vulnerability is a more devastating variant of a cross-site scripting flaw: it occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users in the course of

regular browsing, without proper HTML escaping. A classic example of this is with online message boards where users are allowed to post HTML formatted messages for other users to read.

For example, suppose there is a dating website where members scan the profiles of other members to see if they look interesting. For privacy reasons, this site hides everybody's real name and email. These are kept secret on the server. The only time a member's real name and email are in the browser is when the member is signed in, and they can't see anyone else's.

Suppose that Mallory, an attacker, joins the site and wants to figure out the real names of the people she sees on the site. To do so, she writes a script designed to run from other users' browsers when they visit her profile. The script then sends a quick message to her own server, which collects this information.

To do this, for the question "Describe your Ideal First Date", Mallory gives a short answer (to appear normal) but the text at the end of her answer is her script to steal names and emails. If the script is enclosed inside a `<script>` element, it won't be shown on the screen. Then suppose that Bob, a member of the dating site, reaches Mallory's profile, which has her answer to the First Date question. Her script is run automatically by the browser and steals a copy of Bob's real name and email directly from his own machine.

Persistent XSS vulnerabilities can be more significant than other types because an attacker's malicious script is rendered automatically, without the need to individually target victims or lure them to a third-party website. Particularly in the case of social networking sites, the code would be further designed to self-propagate across accounts, creating a type of client-side worm.

The methods of injection can vary a great deal; in some cases, the attacker may not even need to directly interact with the web functionality itself to exploit such a hole. Any data received by the web application (via email, system logs, IM etc.) that can be controlled by an attacker could become an injection vector.

### **Server-Side versus DOM-based Vulnerabilities**

Before the bug was resolved, Bugzilla error pages were open to DOM-based XSS attacks in which arbitrary HTML and scripts could be injected using forced error messages.

Historically XSS vulnerabilities were first found in applications that performed all data processing on the server side. User input (including an XSS vector) would be sent to the server, and then sent back to the user as a web page. The need for an improved user experience resulted in popularity of applications that had a majority of the presentation logic (maybe written in

JavaScript) working on the client-side that pulled data, on-demand, from the server using AJAX.

As the JavaScript code was also processing user input and rendering it in the web page content, a new subclass of reflected XSS attacks started to appear that was called DOM-based cross-site scripting. In a DOM-based XSS attack, the malicious data does not touch the web server. Rather, it is being reflected by the JavaScript code, fully on the client side.

An example of a DOM-based XSS vulnerability is the bug found in 2011 in a number of jQuery plugins. Prevention strategies for DOM-based XSS attacks include very similar measures to traditional XSS prevention strategies but implemented in JavaScript code and contained in web pages (i.e. input validation and escaping). Some JavaScript frameworks have built-in countermeasures against this and other types of attack — for example Angular.js.

## **Self-XSS**

Self-XSS is a form of XSS vulnerability which relies on Social Engineering in order to trick the victim into executing malicious JavaScript code into their browser. Although it is technically not a true XSS vulnerability due to the fact it relies on socially engineering a user into executing code rather than a flaw in the affected



website allowing an attacker to do so, it still poses the same risks as a regular XSS vulnerability if properly executed.

## **Mutated XSS (mXSS)**

Mutated XSS happens when the attacker injects something that is seemingly safe, but rewritten and modified by the browser, while parsing the markup. This makes it extremely hard to detect or sanitize within the websites application logic. An example is rebalancing unclosed quotation marks or even adding quotation marks to unquoted parameters on parameters to CSS font-family.

## **Cybersquatting**

Cybersquatting<sup>13</sup> (also known as domain squatting), according to the United States federal law known as the Anti cybersquatting Consumer Protection Act, is registering, trafficking in, or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else. The cybersquatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price.

---

<sup>13</sup> <https://en.wikipedia.org/wiki/Cybersquatting>

The term is derived from "squatting", which is the act of occupying an abandoned or unoccupied space or building that the squatter does not own, rent, or otherwise have permission to use.

## **Legal resolution**

Some countries have specific laws against cybersquatting beyond the normal rules of trademark law. The United States, for example, has the U.S. Anticybersquatting Consumer Protection Act (ACPA) of 1999. This expansion of the Lanham (Trademark) Act (15 U.S.C.) is intended to provide protection against cybersquatting for individuals as well as owners of distinctive trademarked names. However, some notable personalities, including rock star Bruce Springsteen and actor Kevin Spacey, failed to obtain control of their names on the internet.

Jurisdiction is an issue, as shown in the case involving Kevin Spacey, in which Judge Gary A. Feess, of the United States District Court of the Central District of California, ruled that the actor would have to file a complaint in a Canadian court, where the current owner of kevinspacey.com resided. Spacey later won the domain through the Forum (alternative dispute resolution) f.k.a National Arbitration Forum.

## **Logic Bomb**

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company.

Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fools' Day. Trojans and other computer viruses that activate on certain dates are often called "time bombs".

To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs.

## Successful Logic Bombs

- In June 2006 Roger Duronio, a system administrator for UBS, was charged with using a logic bomb to damage the company's computer network, and with securities fraud for his failed plan to drive down the company's stock with activation of the logic bomb. Duronio was later convicted and sentenced to 8 years and 1 month in prison, as well as a \$3.1 million restitution to UBS.
- On 20 March 2013, in an attack launched against South Korea, a logic bomb struck machines and "wiped the hard drives and master boot records of at least three banks and two media companies simultaneously." Symantec reported that the malware also contained a component that was capable of wiping Linux machines.
- On 19 July 2019, David Tinley, a contract employee, pleaded guilty for programming logic bombs within the software he created for Siemens Corporation. The software was intentionally made to malfunction after a certain amount of time, requiring the company to hire him to fix it for a fee. The logic bombs went undetected for two years, but was then discovered while he was out of town and had to hand over the administrative password to his software.

## Attempted Logic Bombs

- In February 2000, Tony Xiaotong, indicted before a grand jury, was accused of planting a logic bomb during his employment as a programmer and securities trader at Deutsche Morgan Grenfell. The bomb, planted in 1996, had a trigger date of 20 July 2000, but was discovered by other programmers in the company. Removing and cleaning up after the bomb allegedly took several months.
- On 2 October 2003 Yung-Hsun Lin, also known as Andy Lin, changed code on a server at Medco Health Solutions Inc.'s Fair Lawn, New Jersey headquarters, where he was employed as a Unix administrator, creating a logic bomb set to go off on his birthday in 2004. It failed to work due to a programming error, so Lin corrected the error and reset it to go off on his next birthday, but it was discovered and disabled by a Medco computer systems administrator a few months before the trigger date. Lin pleaded guilty and was sentenced to 30 months in jail in a federal prison in addition to \$81,200 in restitution. The charges held a maximum sentence of 10 years and a fine of US\$250,000.
- On 29 October 2008 a logic bomb was discovered at American mortgage giant Fannie Mae. The bomb was planted by Rajendrasinh Babubhai Makwana, an IT contractor who worked at Fannie Mae's Urbana, Maryland facility. The bomb was set to activate on 31 January 2009 and could have wiped all of Fannie Mae's 4000 servers. Makwana had been terminated around

1:00pm on 24 October 2008 and managed to plant the bomb before his network access was revoked. Makwana was indicted in a Maryland court on 27 January 2009 for unauthorized computer access, convicted on 4 October 2010, and sentenced to 41 months in prison on 17 December 2010.

- In October 2009, Douglas Duchak was terminated from his job as data analyst at the Colorado Springs Operations Center (CSOC) of the U.S. Transportation Security Administration. Surveillance cameras captured images of Duchak entering the facility after hours and loading a logic bomb onto a CSOC server that stored data from the U.S. Marshals. In January 2011, Duchak was sentenced to two years in prison, \$60,587 in fines, and three years on probation.[18] At his sentencing, Duchak tearfully apologized as his lawyer noted that at the time of the incident, Duchak's wife was pregnant with their second child. The judge at the sentencing mentioned that this logic bomb planting "incident was an anomaly in an otherwise untarnished work history."

## **Denial-of-Service Attack**

In computing, a denial-of-service attack<sup>14</sup> (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely

---

<sup>14</sup> [https://en.wikipedia.org/wiki/Denial-of-service\\_attack](https://en.wikipedia.org/wiki/Denial-of-service_attack)

disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, thus disrupting trade. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail and activism can motivate these attacks.

## **Types of Denial-of-Service Attack**

### **Distributed DoS**

A distributed denial-of-service (DDoS) is a large-scale DoS attack where the perpetrator uses more than one unique IP address or machines, often from thousands of hosts infected with malware.] A distributed denial of service attack typically involves more than around 3–5

nodes on different networks; fewer nodes may qualify as a DoS attack but is not a DDoS attack. Since the incoming traffic flooding the victim originates from different sources, it may be impossible to stop the attack simply by using ingress filtering. It also makes it difficult to distinguish legitimate user traffic from attack traffic when spread across multiple points of origin. As an alternative or augmentation of a DDoS, attacks may involve forging of IP sender addresses (IP address spoofing) further complicating identifying and defeating the attack.

The scale of DDoS attacks has continued to rise over recent years, by 2016 exceeding a terabit per second. Some common examples of DDoS attacks are UDP flooding, SYN flooding and DNS amplification.

## **Application Layer Attacks**

An application layer DDoS attack (sometimes referred to as layer 7 DDoS attack) is a form of DDoS attack where attackers target application-layer processes. The attack over-exercises specific functions or features of a website with the intention to disable those functions or features. This application-layer attack is different from an entire network attack, and is often used against financial institutions to distract IT and security personnel from security breaches. In 2013, application-



layer DDoS attacks represented 20% of all DDoS attacks. According to research by Akamai Technologies, there have been "51 percent more application layer attacks" from Q4 2013 to Q4 2014 and "16 percent more" from Q3 2014 over Q4 2014. In November 2017; Junade Ali, a Computer Scientist at Cloudflare noted that whilst network-level attacks continue to be of high capacity, they are occurring less frequently. Ali further notes that although network-level attacks are becoming less frequent, data from Cloudflare demonstrates that application-layer attacks are still showing no sign of slowing down.

## **Application layer**

The OSI model (ISO/IEC 7498-1) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO). The model groups similar communication functions into one of seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the communications path needed by applications above it,

while it calls the next lower layer to send and receive packets that traverse that path.

In the OSI model, the definition of its application layer is narrower in scope than is often implemented. The OSI model defines the application layer as being the user interface. The OSI application layer is responsible for displaying data and images to the user in a human-recognizable format and to interface with the presentation layer below it. In an implementation, the application and presentation layers are frequently combined.

## **Method of Attack**

An application layer DDoS attack is done mainly for specific targeted purposes, including disrupting transactions and access to databases. It requires fewer resources than network layer attacks but often accompanies them. An attack may be disguised to look like legitimate traffic, except it targets specific application packets or functions. The attack on the application layer can disrupt services such as the retrieval of information or search functions on a website. It is very common for attackers to use pre-built applications and open-source projects to run the attack.

## **Advanced persistent DoS**

An advanced persistent DoS (APDoS) is associated with an advanced persistent threat and requires specialised DDoS mitigation. These attacks can persist for weeks; the longest continuous period noted so far lasted 38 days. This attack involved approximately 50+ petabits (50,000+ terabits) of malicious traffic.

Attackers in this scenario may tactically switch between several targets to create a diversion to evade defensive DDoS countermeasures but all the while eventually concentrating the main thrust of the attack onto a single victim. In this scenario, attackers with continuous access to several very powerful network resources are capable of sustaining a prolonged campaign generating enormous levels of un-amplified DDoS traffic.

APDoS attacks are characterised by:

- Advanced reconnaissance (pre-attack OSINT and extensive decoyed scanning crafted to evade detection over long periods)
- Tactical execution (attack with both primary and secondary victims but focus is on primary)
- Explicit motivation (a calculated end game/goal target)

- Large computing capacity (access to substantial computer power and network bandwidth)
- Simultaneous multi-threaded OSI layer attacks (sophisticated tools operating at layers 3 through 7)
- Persistence over extended periods (combining all the above into a concerted, well managed attack across a range of targets).

## **Denial-of-Service as a Service**

Some vendors provide so-called "booter" or "stresser" services, which have simple web-based front ends, and accept payment over the web. Marketed and promoted as stress-testing tools, they can be used to perform unauthorized denial-of-service attacks, and allow technically unsophisticated attackers access to sophisticated attack tools. Usually powered by a botnet, the traffic produced by a consumer stresser can range anywhere from 5-50 Gbit/s, which can, in most cases, deny the average home user internet access.

## **Attack Techniques**

A wide array of tools and techniques are used to launch DoS-attacks.

The simplest DoS attack relies primarily on brute force, flooding the target with an overwhelming flux of packets, oversaturating its connection bandwidth or depleting the target's system resources. Bandwidth-saturating floods rely on the attacker's ability to generate the overwhelming flux of packets. A common way of achieving this today is via distributed denial-of-service, employing a botnet.

## **Attack tools**

In cases such as MyDoom and Slowloris the tools are embedded in malware and launch their attacks without the knowledge of the system owner. Stacheldraht is a classic example of a DDoS tool. It uses a layered structure where the attacker uses a client program to connect to handlers which are compromised systems that issue commands to the zombie agents which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.

In other cases a machine may become part of a DDoS attack with the owner's consent, for example, in Operation Payback organized by the group Anonymous. The Low Orbit Ion Cannon has typically been used in this way. Along with High Orbit Ion Cannon a wide variety of DDoS tools are available today, including paid and free versions, with different features available. There is an underground market for these in hacker related forums and IRC channels.

## **Application-layer Attacks**

Application-layer attacks employ DoS-causing exploits and can cause server-running software to fill the disk space or consume all available memory or CPU time. Attacks may use specific packet types or connection requests to saturate finite resources by, for example, occupying the maximum number of open connections or filling the victim's disk space with logs. An attacker with shell-level access to a victim's computer may slow it until it is unusable or crash it by using a fork bomb. Another kind of application-level DoS attack is XDoS (or XML DoS) which can be controlled by modern web application firewalls (WAFs).

Another target of DDoS attacks may be to produce added costs for the application operator, when the latter uses resources based on cloud computing. In this

case normally application-used resources are tied to a needed quality of service (QoS) level (e.g. responses should be less than 200 ms) and this rule is usually linked to automated software (e.g. Amazon CloudWatch[32]) to raise more virtual resources from the provider in order to meet the defined QoS levels for the increased requests. The main incentive behind such attacks may be to drive the application owner to raise the elasticity levels in order to handle the increased application traffic, in order to cause financial losses or force them to become less competitive.

A banana attack is another particular type of DoS. It involves redirecting outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with the sent packets. A LAND attack is of this type.

## **Degradation-Of-Service Attacks**

Pulsing zombies are compromised computers that are directed to launch intermittent and short-lived floodings of victim websites with the intent of merely slowing it rather than crashing it. This type of attack, referred to as degradation-of-service, can be more difficult to detect and can disrupt and hamper connection to websites for prolonged periods of time, potentially causing more overall disruption than a

denial-of-service attack. Exposure of degradation-of-service attacks is complicated further by the matter of discerning whether the server is really being attacked or is experiencing higher than normal legitimate traffic loads.

## **Denial-of-service Level II**

The goal of DoS L2 (possibly DDoS) attack is to cause a launching of a defense mechanism which blocks the network segment from which the attack originated. In case of distributed attack or IP header modification (that depends on the kind of security behavior) it will fully block the attacked network from the Internet, but without system crash.

## **Distributed DoS attack**

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.[12] Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic. A botnet is a network of zombie computers programmed to receive commands without the owners' knowledge.[36] When a server is overloaded with connections, new connections



can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This, after all, will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

A system may also be compromised with a trojan, allowing the attacker to download a zombie agent, or the trojan may contain one. Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web. Stacheldraht is a classic example of a DDoS tool. It uses a layered structure where the

attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents. In some cases a machine may become part of a DDoS attack with the owner's consent, for example, in Operation Payback, organized by the group Anonymous. These attacks can use different types of internet packets such as: TCP, UDP, ICMP etc.

These collections of systems compromisers are known as botnets / rootservers. DDoS tools like Stacheldraht still use classic DoS attack methods centered on IP spoofing and amplification like smurf attacks and fraggle attacks (these are also known as bandwidth consumption attacks). SYN floods (also known as resource starvation attacks) may also be used. Newer tools can use DNS servers for DoS purposes. Unlike MyDoom's DDoS mechanism, botnets can be turned against any IP address. Script kiddies use them to deny the availability of well known websites to legitimate users. More sophisticated attackers use DDoS tools for the purposes of extortion – even against their business rivals.

Simple attacks such as SYN floods may appear with a wide range of source IP addresses, giving the appearance of a well distributed DoS. These flood attacks do not require completion of the TCP three way handshake and attempt to exhaust the destination SYN queue or the server bandwidth. Because the source IP addresses can be trivially spoofed, an attack could come from a limited set of sources, or may even originate from a single host. Stack enhancements such as syn cookies may be effective mitigation against SYN queue flooding, however complete bandwidth exhaustion may require involvement.

If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a denial-of-service attack. On the other hand, if an attacker uses many systems to simultaneously launch attacks against a remote host, this would be classified as a DDoS attack.

It has been reported that there are new attacks from internet of things (IoT) devices which have been involved in denial of service attacks. In one noted attack that was made peaked at around 20,000 requests per second which came from around 900 CCTV cameras.

UK's GCHQ has tools built for DDoS, named PREDATORS FACE and ROLLING THUNDER.

## **Salami Attack**

In information security, a salami attack is a series of minor attacks those together results in a larger attack. Computers are ideally suited to automating this type of attack.

## **Data Diddling**

Data diddling is a type of cybercrime in which data is altered as it is entered into a computer system, most often by a data entry clerk or a computer virus. Computerized processing of the altered data results in a fraudulent benefit. In some cases, the altered data is changed back after processing to conceal the activity. The results can be huge. They might include adjusting financial figures up or down marginally, or it could be more complex and make an entire system unusable.

## Email Spoofing

Email spoofing<sup>15</sup> is the creation of email messages with a forged sender address.

The core email protocols do not have any mechanism for authentication, making it common for spam and phishing emails to use such spoofing to mislead or even prank the recipient about the origin of the message.

### Technical details

- **MAIL FROM:** - generally presented to the recipient as the Return-path: header but not normally visible to the end user, and by default no checks are done that the sending system is authorized to send on behalf of that address.
- **RCPT TO:** - specifies which email address the email is delivered to, is not normally visible to the end user but may be present in the headers as part of the "Received:" header.

Together these are sometimes referred to as the "envelope" addressing, by analogy with a traditional paper envelope, and unless the receiving mail server signals that it has problems with either of these items,

---

<sup>15</sup> [https://en.wikipedia.org/wiki/Email\\_spoofing](https://en.wikipedia.org/wiki/Email_spoofing)

the sending system sends the "DATA" command, and typically sends several header items, including:

- **From:** Ore Q Jo <oreqjo@example.com> - the address visible to the recipient; but again, by default no checks are done that the sending system is authorized to send on behalf of that address.
- **Reply-to:** Ore Jo <Ore.Jo@hello.me> - similarly not checked

and sometimes:

- **Sender:** alex John <alex.john@demo.com> - also not checked

The result is that the email recipient sees the email as having come from the address in the From: header; they may sometimes be able to find the MAIL FROM address; and if they reply to the email it will go to either the address presented in the From: or Reply-to: header - but none of these addresses are typically reliable, so automated bounce messages may generate backscatter.

Although email spoofing is effective in forging the email address, the IP address of the computer sending the mail can generally be identified from the "Received:" lines in the email header. In malicious cases however, this is likely to be the computer of an innocent third

party infected by malware that is sending the email without the owner's knowledge.

## **Malicious use of Spoofing**

Phishing and business email compromise scams generally involve an element of email spoofing.

Email spoofing has been responsible for public incidents with serious business and financial consequences, such as an October 2013 email to a news agency, spoofed to look like it was from the Swedish company Fingerprint Cards, saying that Samsung offered to purchase the company. The news spread and the stock exchange rate surged by 50%.

Malware such as Klez and Sober and many more modern examples often search for email addresses within the computer they have infected, and use those addresses both as targets for email, but also to create credible forged From fields in the emails that they send, so that these emails are more likely to be opened. For example:

1. Alice is sent an infected email which she opens, running the worm code.
2. The worm code searches Alice's email address book and finds the addresses of Bob and Charlie.

3. From Alice's computer, the worm sends an infected email to Bob, but forged to appear to have been sent by Charlie.

In this case, even if Bob's system detects the incoming mail as containing malware, he sees the source as being Charlie, even though it really came from Alice's computer; meanwhile Alice may remain unaware that her computer has been infected.

## **Legitimate Use**

In the early Internet, "legitimately spoofed" email was common. For example, a visiting user might use the local organization's SMTP server to send email from the user's foreign address. Since most servers were configured as "open relays", this was a common practice. As spam email became an annoying problem, these sorts of "legitimate" uses fell out of favor.

When multiple software systems communicate with each other via email, spoofing may be required in order to facilitate such communication. In any scenario where an email address is set up to automatically forward incoming emails to a system which only accepts emails from the email forwarder, spoofing is required in order to facilitate this behavior. This is common between ticketing systems which communicate with other ticketing systems.



## **The effect on Mailservers**

Traditionally, mail servers could accept a mail item, then later send a Non-Delivery Report or "bounce" message if it couldn't be delivered or had been quarantined for any reason. These would be sent to the "MAIL FROM:" aka "Return Path" address. With the massive rise in forged addresses, Best Practice is now to not generate NDRs for detected spam, viruses etc. but to reject the email during the SMTP transaction. When mail administrators fail to take this approach, their systems are guilty of sending "backscatter" emails to innocent parties - in itself a form of spam - or being used to perform "Joe job" attacks.

## **Identity Theft**

Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, especially if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to

commit fraud or other crimes. The term identity theft was coined in 1964. Since that time, the definition of identity theft has been statutorily proscribed throughout both the U.K. and the United States as the theft of personally identifiable information, generally including a person's name, date of birth, social security number, driver's license number, bank account or credit card numbers, PIN numbers, electronic signatures, fingerprints, passwords, or any other information that can be used to access a person's financial resources

Determining the link between data breaches and identity theft is challenging, primarily because identity theft victims often do not know how their personal information was obtained, and identity theft is not always detectable by the individual victims, according to a report done for the FTC. Identity fraud is often but not necessarily the consequence of identity theft. Someone can steal or misappropriate personal information without then committing identity theft using the information about every person, such as when a major data breach occurs. A US Government Accountability Office study determined that "most breaches have not resulted in detected incidents of identity theft". The report also warned that "the full extent is unknown". A later unpublished study by Carnegie Mellon University noted that "Most often, the

causes of identity theft is not known", but reported that someone else concluded that "the probability of becoming a victim to identity theft as a result of a data breach is ... around only 2%". More recently, an association of consumer data companies noted that one of the largest data breaches ever, accounting for over four million records, resulted in only about 1,800 instances of identity theft, according to the company whose systems were breached.

An October 2010 article entitled "Cyber Crime Made Easy" explained the level to which hackers are using malicious software. As Gunter Ollmann, Chief Technology Officer of security at Microsoft, said, "Interested in credit card theft? There's an app for that." This statement summed up the ease with which these hackers are accessing all kinds of information online. The new program for infecting users' computers was called Zeus; and the program is so hacker-friendly that even an inexperienced hacker can operate it. Although the hacking program is easy to use, that fact does not diminish the devastating effects that Zeus (or other software like Zeus) can do to a computer and the user. For example, the article stated that programs like Zeus can steal credit card information, important documents, and even documents necessary for homeland security. If the hacker were to gain this information, it would mean identity theft or even a

possible terrorist attack. The ITAC says that about 15 million Americans had their identity stolen in 2012.

## **Types**

Sources such as the Non-profit Identity Theft Resource Center sub-divide identity theft into five categories:

- Criminal identity theft (posing as another person when apprehended for a crime)
- Financial identity theft (using another's identity to obtain credit, goods and services)
- Identity cloning (using another's information to assume his or her identity in daily life)
- Medical identity theft (using another's identity to obtain medical care or drugs)
- Child identity theft.

Identity theft may be used to facilitate or fund other crimes including Illegal immigration, terrorism, phishing and espionage. There are cases of identity cloning to attack payment systems, including online credit card processing and medical insurance.

## **Identity Cloning and Concealment**

In this situation the identity thief impersonates someone else in order to conceal their own true identity. Examples are illegal immigrants hiding their illegal status, people hiding from creditors or other individuals, and those who simply want to become "anonymous" for personal reasons. Another example is posers, a label given to people who use someone else's photos and information on social networking sites. Posers mostly create believable stories involving friends of the real person they are imitating. Unlike identity theft used to obtain credit which usually comes to light when the debts mount, concealment may continue indefinitely without being detected, particularly if the identity thief is able to obtain false credentials in order to pass various authentication tests in everyday life.

### **Criminal identity theft**

When a criminal fraudulently identifies themselves to police as another individual at the point of arrest, it is sometimes referred to as "Criminal Identity Theft." In some cases, criminals have previously obtained state-issued identity documents using credentials stolen from others, or have simply presented a fake ID. Provided the subterfuge works, charges may be placed under the

victim's name, letting the criminal off the hook. Victims might only learn of such incidents by chance, for example by receiving a court summons, discovering their drivers licenses are suspended when stopped for minor traffic violations, or through background checks performed for employment purposes.

It can be difficult for the victim of a criminal identity theft to clear their record. The steps required to clear the victim's incorrect criminal record depend in which jurisdiction the crime occurred and whether the true identity of the criminal can be determined. The victim might need to locate the original arresting officers and prove their own identity by some reliable means such as fingerprinting or DNA testing, and may need to go to a court hearing to be cleared of the charges. Obtaining an expungement of court records may also be required. Authorities might permanently maintain the victim's name as an alias for the criminal's true identity in their criminal records databases. One problem that victims of criminal identity theft may encounter is that various data aggregators might still have the incorrect criminal records in their databases even after court and police records are corrected. Thus it is possible that a future background check will return the incorrect criminal records. This is just one example of the kinds of impact that may continue to affect the victims of identity theft for some months or even years

after the crime, aside from the psychological trauma that being 'cloned' typically engenders.

## **Synthetic Identity Theft**

A variation of identity theft which has recently become more common is synthetic identity theft, in which identities are completely or partially fabricated. The most common technique involves combining a real social security number with a name and birth date other than the ones associated with the number. Some thieves use social security numbers belonging to people who have been incarcerated for a long period of time, but many begin with a child's social security number that was issued after the year that would make that individual at least 18 years old. Synthetic identity theft is more difficult to track as it doesn't show on either person's credit report directly but may appear as an entirely new file in the credit bureau or as a subfile on one of the victim's credit reports. Synthetic identity theft primarily harms the creditors who unwittingly grant the fraudsters credit. Individual victims can be affected if their names become confused with the synthetic identities, or if negative information in their subfiles impacts their credit ratings.

## **Medical Identity Theft**

Privacy researcher Pam Dixon, the founder of the World Privacy Forum, coined the term medical identity theft and released the first major report about this issue in 2006. In the report, she defined the crime for the first time and made the plight of victims public. The report's definition of the crime is that medical identity theft occurs when someone seeks medical care under the identity of another person. Insurance theft is also very common, if a thief has your insurance information and or your insurance card, they can seek medical attention posing as yourself. In addition to risks of financial harm common to all forms of identity theft, the thief's medical history may be added to the victim's medical records. Inaccurate information in the victim's records is difficult to correct and may affect future insurability or cause doctors relying on the misinformation to deliver inappropriate care. After the publication of the report, which contained a recommendation that consumers receive notifications of medical data breach incidents, California passed a law requiring this, and then finally HIPAA was expanded to also require medical breach notification when breaches affect 500 or more people. Data collected and stored by hospitals and other organizations such as medical aid schemes is up to 10 times more valuable to cybercriminals than credit card information.



## **Child Identity Theft**

Child identity theft occurs when a minor's identity is used by another person for the impostor's personal gain. The impostor can be a family member, a friend, or even a stranger who targets children. The Social Security numbers of children are valued because they do not have any information associated with them. Thieves can establish lines of credit, obtain driver's licenses, or even buy a house using a child's identity. This fraud can go undetected for years, as most children do not discover the problem until years later. Child identity theft is fairly common, and studies have shown that the problem is growing. The largest study on child identity theft, as reported by Richard Power of the Carnegie Mellon Cylab with data supplied by AllClear ID, found that of 40,000 children, 10.2% were victims of identity theft.

The Federal Trade Commission (FTC) estimates that about nine million people will be victims of identity theft in the United States per year. It was also estimated that in 2008 630,000 people under the age of 19 were victims of theft. This then gave them a debt of about \$12,799 which was not theirs.

Not only are children in general big targets of identity theft but children who are in foster care are even bigger targets. This is because they are most likely moved around quite frequently and their SSN is being shared

with multiple people and agencies. Foster children are even more victims of identity theft within their own family and other relatives. Young people in foster care who are victims of this crime are usually left alone to struggle and figure out how to fix their newly formed bad credit.

### **Financial Identity Theft**

The most common type is financial identity theft, where someone wants to gain economical benefits in someone else's name. This includes getting credits, loans, goods and services, claiming to be someone else.

### **Tax Identity Theft**

One of the major identity theft categories is tax identity theft. The most common method is to use a person's authentic name, address, and Social Security Number to file a tax return with false information, and have the resulting refund direct-deposited into a bank account controlled by the thief. The thief in this case can also try to get a job and then their employer will report the income of the real taxpayer, this then results in the taxpayer getting in trouble with the IRS.

The 14039 Form to the IRS is a form that will help one fight against a theft like tax theft. This form will put the

IRS on alert and someone who believed they have been a victim of tax related theft will be given an Identity Protection Personal Identification Number (IP PIN), which is a 6 digit code used in replace of a SSN for filing tax returns.

## **Techniques for Obtaining and Exploiting Personal Information**

- Rummaging through rubbish for personal information (dumpster diving)
- Retrieving personal data from redundant IT equipment and storage media including PCs, servers, PDAs, mobile phones, USB memory sticks and hard drives that have been disposed of carelessly at public dump sites, given away or sold on without having been properly sanitized
- Using public records about individual citizens, published in official registers such as electoral rolls[25]
- Stealing bank or credit cards, identification cards, passports, authentication tokens ... typically by pickpocketing, housebreaking or mail theft
- Common-knowledge questioning schemes that offer account verification, such as "What's your mother's maiden name?", "what was your first car model?", or "What was your first pet's name?".

- Skimming information from bank or credit cards using compromised or hand-held card readers, and creating clone cards
- Using 'contactless' credit card readers to acquire data wirelessly from RFID-enabled passports
- Shoulder-Surfing, involves an individual who discreetly watches or hears others providing valuable personal information. This is particularly done in crowded places because it is relatively easy to observe someone as they fill out forms, enter PIN numbers on ATMs or even type passwords on smartphones.
- Stealing personal information from computers using breaches in browser security or malware such as Trojan horse keystroke logging programs or other forms of spyware
- Hacking computer networks, systems and databases to obtain personal data, often in large quantities
- Exploiting breaches that result in the publication or more limited disclosure of personal information such as names, addresses, Social Security number or credit card numbers
- Advertising bogus job offers in order to accumulate resumes and applications typically disclosing applicants' names, home and email addresses,

telephone numbers and sometimes their banking details

- Exploiting insider access and abusing the rights of privileged IT users to access personal data on their employers' systems
- Infiltrating organizations that store and process large amounts or particularly valuable personal information
- Impersonating trusted organizations in emails, SMS text messages, phone calls or other forms of communication in order to dupe victims into disclosing their personal information or login credentials, typically on a fake corporate website or data collection form (phishing)
- Brute-force attacking weak passwords and using inspired guesswork to compromise weak password reset questions
- Obtaining castings of fingers for falsifying fingerprint identification.
- Browsing social networking websites for personal details published by users, often using this information to appear more credible in subsequent social engineering activities

- Diverting victims' email or post in order to obtain personal information and credentials such as credit cards, billing and bank/credit card statements, or to delay the discovery of new accounts and credit agreements opened by the identity thieves in the victims' names
- Using false pretenses to trick individuals, customer service representatives and help desk workers into disclosing personal information and login details or changing user passwords/access rights (pretexting)
- Stealing cheques (checks) to acquire banking information, including account numbers and bank codes
- Guessing Social Security numbers by using information found on Internet social networks such as Facebook and MySpace
- Low security/privacy protection on photos that are easily clickable and downloaded on social networking sites.
- Befriending strangers on social networks and taking advantage of their trust until private information is given.

## Indicators

The majority of identity theft victims do not realize that they are a victim until it has negatively impacted their lives. Many people do not find out that their identities have been stolen until they are contacted by financial institutions or discover suspicious activities on their bank accounts. According to an article by Herb Weisbaum, everyone in the US should assume that their personal information has been compromised at one point. It is therefore of great importance to watch out for warning signs that your identity has been compromised. The following are eleven indicators that someone else might be using your identity.

1. Credit or debit card charges for goods or services you are not aware of, including unauthorized withdrawals from your account.
2. Receiving calls from credit or debit card fraud control department warning of possible suspicious activity on your credit card account.
3. Receiving credit cards that you did not apply for
4. Receiving information that a credit scoring investigation was done. They are often done when a loan or phone subscription was applied for.
5. Checks bouncing for lack of enough money in your account to cover the amount. This might be as a

result of unauthorized withdrawals from your account

6. Identity theft criminals may commit crimes with your personal information. You may not realize this until you see the police on your door arresting you for crimes that you did not commit
7. Sudden changes to your credit score may indicate that someone else is using your credit cards
8. Bills for services like gas, water, electricity not arriving in time. This can be an indication that your mail was stolen or redirected
9. Not Being approved for loans because your credit report indicates that you are not credit worthy
10. Receiving notification from your post office informing you that your mails are being forwarded to another unknown address
11. Your yearly tax returns indicating that you have earned more than you have actually earned. This might indicate that someone is using your national identification number e.g. SSN to report their earnings to the tax authorities.



## **Individual Identity Protection**

The acquisition of personal identifiers is made possible through serious breaches of privacy. For consumers, this is usually a result of them naively providing their personal information or login credentials to the identity thieves (e.g., in a phishing attack) but identity-related documents such as credit cards, bank statements, utility bills, checkbooks etc. may also be physically stolen from vehicles, homes, offices, and not the least letterboxes, or directly from victims by pickpockets and bag snatchers. Guardianship of personal identifiers by consumers is the most common intervention strategy recommended by the US Federal Trade Commission, Canadian Phone Busters and most sites that address identity theft. Such organizations offer recommendations on how individuals can prevent their information falling into the wrong hands.

Identity theft can be partially mitigated by not identifying oneself unnecessarily (a form of information security control known as risk avoidance). This implies that organizations, IT systems and procedures should not demand excessive amounts of personal information or credentials for identification and authentication. Requiring, storing and processing personal identifiers (such as Social Security number, national identification number, driver's license number, credit card number, etc.) increases the risks of identity theft unless this

valuable personal information is adequately secured at all times. Committing personal identifiers to memory is a sound practice that can reduce the risks of a would-be identity thief from obtaining these records. To help in remembering numbers such as social security numbers and credit card numbers, it is helpful to consider using mnemonic techniques or memory aids such as the mnemonic Major System.

Identity thieves sometimes impersonate dead people, using personal information obtained from death notices, gravestones and other sources to exploit delays between the death and the closure of the person's accounts, the inattentiveness of grieving families and weaknesses in the processes for credit-checking. Such crimes may continue for some time until the deceased's families or the authorities notice and react to anomalies.

In recent years, commercial identity theft protection/insurance services have become available in many countries. These services purport to help protect the individual from identity theft or help detect that identity theft has occurred in exchange for a monthly or annual membership fee or premium. The services typically work either by setting fraud alerts on the individual's credit files with the three major credit bureaus or by setting up credit report monitoring with the credit bureaus. While identity theft

protection/insurance services have been heavily marketed, their value has been called into question.

## **Malvertising**

Malvertising (a portmanteau of "malicious advertising") is the use of online advertising to spread malware. It typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages. Online advertisements provide a solid platform for spreading malware because significant effort is put into them in order to attract users and sell or advertise the product. Because advertising content can be inserted into high-profile and reputable websites, malvertising provides malefactors an opportunity to push their attacks to web users who might not otherwise see the ads, due to firewalls, more safety precautions, or the like. Malvertising is "attractive to attackers because they 'can be easily spread across a large number of legitimate websites without directly compromising those websites'."

Malvertising is a fairly new concept for spreading malware and can be extremely hard to combat because it can quietly work its way into a webpage or advertisement on a webpage and spread unknowingly: "The interesting thing about infections delivered

through malvertising is that it does not require any user action (like clicking) to compromise the system and it does not exploit any vulnerabilities on the website or the server it is hosted from... infections delivered through malvertising silently travel through Web page advertisements." It is able to expose millions of users to malware, even the most cautious, and is growing rapidly: "In 2012, it was estimated nearly 10 billion ad impressions were compromised by malvertising." Attackers have a very wide reach and are able to deliver these attacks easily through advertisement networks. Companies and websites have had difficulty diminishing the number of malvertising attacks, which "suggests that this attack vector isn't likely to disappear soon."

## **Types and Modes**

By visiting websites that are affected by malvertising, users are at risk of infection. There are many different methods used for injecting malicious advertisements or programs into webpages:

- Pop-up ads for deceptive downloads, such as fake anti-virus programs that install malicious software on the computer
- In-text or in-content advertising

- Drive-by downloads
- Web widgets in which redirection can be co-opted into redirecting to a malicious site
- Hidden iframes that spread malware into websites
- Content delivery networks exploited to share malware
- Malicious banners on websites
- Third-party advertisements on webpages
- Third-party applications, such as forums, help desks, and customer relationship management and content management systems .

## SQL Injection

SQL injection<sup>16</sup> is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an

---

<sup>16</sup>

[https://en.wikipedia.org/wiki/SQL\\_injection#:~:text=SQL%20injection%20is%20a%20code,database%20contents%20to%20the%20attacker](https://en.wikipedia.org/wiki/SQL_injection#:~:text=SQL%20injection%20is%20a%20code,database%20contents%20to%20the%20attacker)

application}}s software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

In a 2012 study, it was observed that the average web application received 4 attack campaigns per month, and retailers received twice as many attacks as other industries.

## **Form**

SQL injection (SQLI) was considered one of the top 10 web application vulnerabilities of 2007 and 2010 by the Open Web Application Security Project. In 2013, SQLI was rated the number one attack on the OWASP top ten. There are four main sub-classes of SQL injection:

- Classic SQLI
- Blind or Inference SQL injection

- Database management system-specific SQLI
- Compounded SQLI
  - SQL injection + insufficient authentication
  - SQL injection + DDoS attacks
  - SQL injection + DNS hijacking
  - SQL injection + XSS

The Storm Worm is one representation of Compounded SQLI.

This classification represents the state of SQLI, respecting its evolution until 2010—further refinement is underway.

## Reference:

1. The Economics Times:

<https://economictimes.indiatimes.com/industry/banking/finance/banking/how-to-report-a-net-banking-debit-or-credit-card-fraud/where-to-file-the-complaint/slideshow/67073231.cms>

2. Cyber Swachhta Kendra (साइबर स्वच्छता केंद्र)

<https://www.cyberswachhtakendra.gov.in/index.html>

3. 10 Ransomware Example:

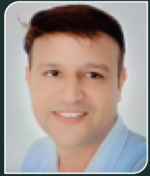
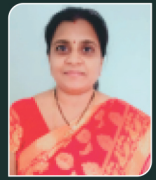
<https://www.kaspersky.co.in/resource-center/threats/ransomware-examples>

4. RootKit Malware

<https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html>



**T. Pushpalatha** is a Assistant Professor of Computer Applications Department (M.C.A.) in St. Ann's College for Women, Mehadipatnam, Hyderabad. She is Pursuing her Ph.D from JJT University Rajasthan.



**Dr. Yogesh Kumar Sharma**, Presently working as a Associate Professor (HOD / Research Coordinator) Department of Computer Science Engineering and IT at "Shri Jagdish prasad Jhabarmal Tibrewala University", Chudela, Jhunjhunu (Rajasthan). He completed his B.Sc with Computer Application in the year of 2002 awarded from S.M.L. (P.G.) College, Jhunjhunu, University of Rajasthan, M.C.A from Modi Institute of Management and Technology, Kota, University of Kota in the year 2005, Ph.D. in Faculty of Computer Science, from "Shri Jagdish prasad Jhabarmal Tibrewala University", Jhunjhunu (Rajasthan) in the year 2014.

**M. Krishna** is a Faculty of Computer Science and Applications Department of Computers in Tara Government College, Sangareddy, and Telangana State. Presently working as Faculty in Department of Computer Science & Applications at Tara Government College, Sangareddy from the Academic Year 2005-till date. Worked as a CCE-JKC Trainer in Computer Skills to Government Degree and Junior Colleges Principals, Lecturers for the academic years 2008-09 & 2009-10. Worked as Part-Time Lecturer in Computer Science at Ellenki Degree College, Sangareddy for the Academic Year 2006-07. Worked as Senior Teacher in Mathematics at Government High School, Sangareddy for the Academic year 2004-05. Worked as Vidya Volunteer in Mathematics at Government High School, Chitkul for the Academic year 2003-04.



**Dr. S. Nagaprasad** working as a Faculty in Computer science and Applications, Dept. of Computer Science and Applications, Tara Government College, Sangareddy, Telangana state. He completed his B.C.A. in the year of 1998-2001 awarded from Osmania university, M.Sc (I.T) in the year of 2001-2003 awarded from Sikkim Manipal University, Sikkim, his research work completed from Ph.D in Computer Science and Engineering, from Acharya Nagarjuna University, Sep-2015. His research areas data mining, networking, image processing, machine learning etc. In his research life he present completed 30 international journals in his research area, 15 National and International conferences, for his research interest he attended 10 workshops. He worked as a faculty in Computer Science at S.K.N.R. Government Arts and Science College, Jagtial Telangana state for 10 years.

 **Bazooka**.com  
www.bookbazooka.com

₹190

ISBN:978-93-86895-92-9



9 1789386 895929 1