**Malware Design Case Studies**

| **Type of malware** | **Description** |
| --- | --- |
| **Virus** | Code with malicious behavior. Copies itself to other programs. |
| **Trojan Horse** | Code that contains unexpected, undocumented malicious features. Often hidden within a useful or legitimate looking program. |
| **Worm** | Code that copies itself through a network. Usually degrades performance. |
| **Rabbit** | Code that replicates itself without limit to exhaust resources. |
| **Logic bomb** | Code that triggers an action when a certain condition is met. |
| **Time bomb** | Code that triggers an action at a certain date. |
| **Spyware** | Code that intercepts communications or steals data from a user. |
| **Bot** | Program controlled remotely by a master “herder.” |
| **Rootkit** | A program or entire computer unknowingly under control of a remote master program. |
| **Hijack** | Code that changes settings in a browser to allow access to website or redirect browsers to specific sites. |
| **Resident virus** | Code that bypasses normal authentication methods. |
| **Adware** | Code that causes advertisements to appear on the user’s computer. |
| **Ransomware** | Code that disables a computer system and requires payment to the perpetrator in order to be reversed. |
| **Keylogger** | Code to record keystrokes. |
| **Malware** | Malicious code written in a scripting language for application commands. |
| **Grayware** | Unwanted software that is installed as a default option during a legitimate installation process of another program. |
| **Botnet** | Group of computers used to perform a coordinated attack on a targeted resource. Often results in a denial of service event. |
| **Boot sector infection** | Code embedded in the startup process of an operating system that often redistributes its code on each restart. |
| **Cavity virus** | Code that can modify itself in order to make it less visible to antivirus software. |
| **Zero Day Exploit** | Vulnerability of a program that has not yet been discovered by the maker. |
| **Payload** | Code within a malware package that accomplishes the goal of the attacker. |
| **Backdoor** | A program that remains resident in the RAM of a computer and is frequently used by the operating system. |
| **Kernel Process** | A program that has access to the core operations of an operating system, which typically requires special credential rights above that of a user process. |
| **Heuristics** | The study of the behavior of a program such as observing the fact that a program modifies its own code or changes other files or other actions that are common to viruses. |
| **Macro virus** | Virus that can utilize empty or unused spaces within a host file to store itself. This prevents the file from changing size. |
| **Cyclic redundancy check** | A process to compare the initial values of a set of data (or program file) to current values to ensure that the file has not been modified. |
|  |  |

White hat hackers, also called ethical hackers, are trained in ethical hacking and use hacking skills to find security holes in programs, devices, and networks. Despite the fact that white hat hackers are on the good side, it's not uncommon for them to start out as black hats. The overall goal of black and white hats is to find loopholes in a system. Black hats exploit loopholes to monetize, while ethical hackers protect owners from exploitation.

The bible says: "seest thou a man diligent or skillful in his business or profess-ion, he will serve before kings and he will not be found in the midst of mean men," - Proverbs 22:29. Using your talents for God can help you find purposeful work and share God's love. It is true that white-hat hackers are capable of doing a great deal of damage, but their just cause is what allows them to act as an angel of Internet security and to share God's love.

One way a white-hat hacker mitigated criminal behavior was when Charlie Miller started penetrating automotive security systems. Using his hacking skills, he had complete control over multiple cars, including breaks, steering wheels, radio, etc. This led to a recall of 1.4 million vehicles, because it was an obvious safety concern that wasn't addressed. Ideally, the exploit would have been discovered before the rollout of over a million vehicles, but better late than never, I suppose! It is safe to say that this white hat hacker saved many lives by preventing the theft of whole vehicles via remote control.

**Virus Hall of Shame**

Complete this section using complete sentences and fully-developed ideas.

|  | **Year(s)** | **What type of virus was this?** | **Notorious for?** | **Exploited what vulnerability?** | **Remedy** |
| --- | --- | --- | --- | --- | --- |
| **Creeper** | 1971 | Worm | First computer worm! Showed that a self-replicating computer program can spread. | The Advanced Research Projects Agency Network (ARPANET) | First antivirus!  “Reaper” program was created to delete it. |
| **Melissa** | 1999 | Macro Virus | Targeting Microsoft word and outlook-based systems. | Hijacked user's Word programs and Outlook email to send emails to the first 50 people on their list. | FBI issued warnings about the virus and how to avoid it. Enhancements made to online security |
| **ILOVEYOU** | 2000 | Worm  Rabbit (?) | Overwriting system and personal files. Endlessly reproducing. | Systemic weaknesses in the design of Microsoft Outlook and Microsoft Windows | Enacting new laws & taking down server. |
| **Chernobyl** | 1998 | Worm | Recognized as the first virus known to have the power to damage computer hardware. | It spread via a portable .exe file. It splits its code up and inserts it into gaps, so no file size increase is caused. | Only affects outdated equipment. Creator released an anti-virus for it. |
| **Code Red** | 2001 | Worm | This was the first successful enterprise network attack with mixed threats. | It attacked computers running Microsoft's IIS web server. | Worm stopped infections by itself |
| **WannaCry** | 2017 | Ransomware Worm | Encrypts files, makes access impossible, and demands a bitcoin ransom for the infected files. | SMB implementation flaw in Microsoft Windows. | Marcus Hutchins registered a web domain found in the malware's code. |
| **Conficker** | 2008 | Worm | Access by remote computers is enabled by disabling many security features. | Targets a vulnerability (MS08-067) in Windows operating systems. | Microsoft released virus removal guide, as well as applying a patch to prevent the virus. |
| **Samy** | 2005 | Worm | MySpace virus that changed user’s profiles to display “Samy is my hero” and send a friend request to Samy. | An XSS vulnerability in MySpace was exploited | Taken down by Author, and restrictions were added to MySpace |
| **Slammer** | 2003 | Worm | Caused a denial of service on some Internet hosts and dramatically slowed general Internet traffic. | Buffer overflow vulnerability was exploited | A patch had been available from Microsoft for six months prior to the worm's launch |
| **NIMDA** | 2001 | Worm | Surpassing the economic damage caused by previous outbreak. Used five different infection vectors! | By slowing traffic or denying services, it caused chaos rather than destroying files or harming computer security. | Either deleting the entire folder and emptying the recycle bin, or disabling the download of files |
| **Storm Worm** | 2007 | Trojan Horse | Email about recent weather disaster | Merged into a botnet one the executable was activated | No remedy/ wiping entire harddrive |
| **Stuxnet** | 2005-2010 | Dropper  Worm | Causing damage to Iranian nuclear facilities | An executable worm. An executable linkfile. A rootkit to hide the evidence. | Call customer support who suggests to update windows for security vulnerabilities |
| **Elk Cloner** | 1982 | Boot sector virus | Being on apple II operating system specifically! | Infected all floppy disk after the 50th launch of a game | Do not use floppy disks, or only boot up the game 49 times |
| **Chameleon** | 1991 | File | the entire virus is encrypted with many individual bytes having their own levels of encryption on top of that | Infected all .com in current dirrectory | Run antivirus software, wipe hard drive and operating system |
| **Mebroot** | 2007-2008 | Trojan Horse | Stealth Techniques to get access to computers | Invade deep into the operating system and intercept reads and writes, bypassing some safeguards | Using antivirus software, wiping or repairing the hard drive, master boot record, and operating system |
| **Cryptolocker** | 2013-2014 | Trojan Horse | Locked up files to be unlocked with bitcoin | A message is sent by email when a file with a difficult encryption code is activated | Safe internet access. Botnet distributing the virus was stopped by the FBI. |
| **Jerusalem** | 1987 | Logic Bomb DOS Virus  Resident Virus | Memory resident and then infects every executable file run, except for COMMAND.COM | Hooks into interrupt processing and other low-level DOS services | DOS interrupts are no longer used, so Jerusalem and its variants have become obsolete |
|  |  |  |  |  |  |