Malware Removal

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com

https://www.facebook.com/tutorialspointindia

https://twitter.com/tutorialspoint

About the Tutorial

A malware can cause harm to a system or a network directly, or subvert them to be used by others, rather than as intended by their owners. It is a combination of two words: **Mal** meaning **Bad** and **Ware** meaning **Software**.

In this tutorial, we will discuss various precautionary ways and the tools that can be used to protect our systems and networks from harmful Malware.

Audience

This tutorial has been prepared mainly for those professionals who are within the IT industry, working as IT specialists, System administrators, and Security administrators.

Prerequisites

It is an elementary tutorial and you can easily understand the concepts explained here with a basic knowledge of how a company or an organization deals with its Computer and Network Security. However, it will help if you have some prior exposure on how to carry out computer updates regularly, setting up firewalls, antiviruses, etc.

Copyright and Disclaimer

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at contact@tutorialspoint.com

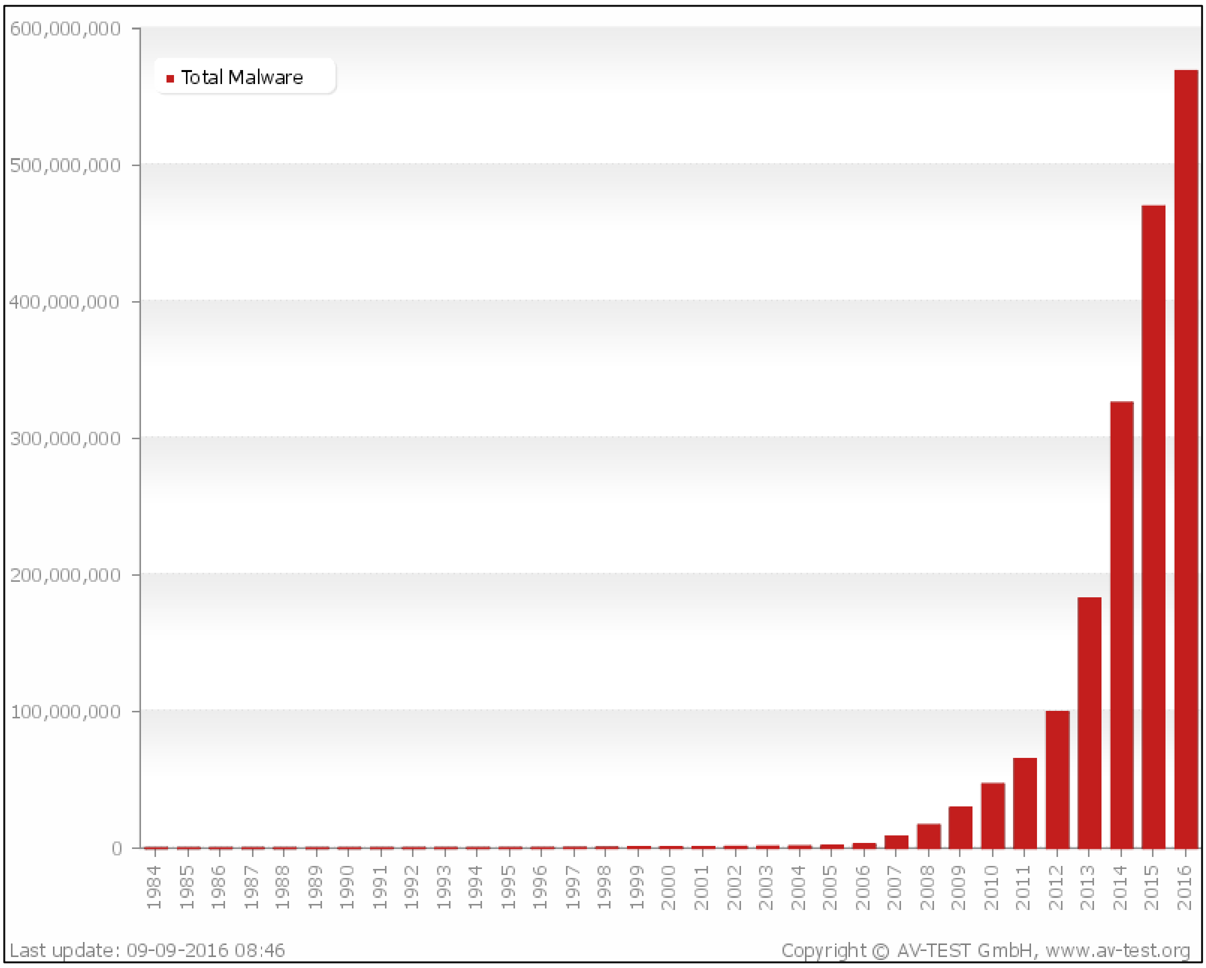
Table of Contents

1. Malware – Overview

In the recent years, we have heard of many people and big corporates losing their precious data or being in a situation where their systems are hacked. These unwanted activities are being caused, in most of the cases, using a piece of software inserted into a network system, server or a personal computer. This piece of software is known as a **malware**.

A malware can cause harm to a system or a network directly, or subvert them to be used by others, rather than as intended by their owners. It is a combination of two words: **Mal** meaning **Bad** and **Ware** meaning **Software**.

Based on www.av-test.org, the statistics are growing tremendously. Please look at the following graph to understand the growth of Malware.



As you can see, there were more than 600,000,000 malwares detected in 2016 alone. Based on **securelist.com**, the countries that have infected computers compared to the cleaner ones are:

- **Maximum risk (over 60%)**: 22 countries, including Kyrgyzstan (60.77%), Afghanistan (60.54%).

- **High risk (41-60%):** 98 countries including India (59.7%), Egypt (57.3%), Belarus (56.7%), Turkey (56.2%), Brazil (53.9%), China (53.4%), UAE (52.7%), Serbia (50.1%), Bulgaria (47.7%), Argentina (47.4%), Israel (47.3%), Latvia (45.9%), Spain (44.6%), Poland (44.3%), Germany (44%), Greece (42.8%), France (42.6%), Korea (41.7%), Austria (41.7%).

- **Moderate local infection rate (21-40.99%):** 45 countries including Romania (40%), Italy (39.3%), Canada (39.2%), Australia (38.5%), Hungary (38.2%), Switzerland (37.2%), USA (36.7%), UK (34.7%), Ireland (32.7%), Netherlands (32.1%), Czech Republic (31.5%), Singapore (31.4%), Norway (30.5%), Finland (27.4%), Sweden (27.4%), Denmark (25.8%), Japan (25.6%).

Malware can be designed from the hackers for different purposes like destroying data, sending the data automatically to some other place, altering the data or can keep monitoring it until the specified time-period. Disable security measures, damage the information system, or otherwise affect the data and system integrity.

They also come in different types and forms, which we will discuss in detail in the upcoming chapters of this tutorial.

2. Malware – How It Works

To understand how malware works, we should first see the anatomy of a malware attack, which is separated in five steps as shown below:

- Entry point
- Distribution
- Exploit
- Infection
- Execution

Let us understand the above-mentioned points in detail.

Entry Point

A malware can enter into the system in many ways:

- The user visits his favorite website that has been infected recently. This can be an entry point for a malware.

- If a user clicks on a URL that has come in an email, it will hijack that browser.

- Malware can also enter through any infected external media such as a USB or an external hard drive.

Distribution

The malware initiates a process that redirects the traffic to an exploit server which checks the OS and applications such as the browser, Java, Flash player, etc.

Exploit

In this phase, the **exploit** will try to execute based on the OS and will find a way to escalate the privilege.

Infection

Now, the exploit that was successfully installed will upload a payload to maintain access and to manage the victim like remote access, file upload/download, etc.

Execution

In this phase, the hacker who manages the Malware will start to steal your data, encrypt your files, etc.

3. Malware – Types

Malwares are diverse; they come from different functions and behave differently under various situations. Some of the most infamous and dangerous types of malwares are given below:

- Virus
- Adware
- Spyware
- Trojan
- Rootkits
- Botnets
- Ransom Ware

Let us understand each of these in detail.

Virus

Virus is a malware program that acts in an interesting way. This program executes or replicates itself by putting-in some copies of itself in other computer programs, boot sector, data files, hard disk, etc. When the replication process is done, then the areas that are affected are said to be the infected ones.

Viruses are built to perform some of the most harmful activities on the hosts when they are infected. They can steal the CPU time or even the space in the hard disk. They can also corrupt the data and can put some funny messages on the screen of the system.

Adware

This software is mainly the advertising supporting software. A package that comes automatically with the advertisements inside. Hence, it can generate some good income for the owner.

Spyware

Spyware is a software that is mainly used for the gathering of information about some organization or a person. That information is gathered without anyone getting to know that the information is being fathered from his or her system.

Trojan

Trojan is a non-self-replicating type of malware. It contains some malicious code, which carries out some actions that are determined by the nature of that specific Trojan. This happens upon the execution only. The result of the action is normally the data loss and it can also harm the system in many ways.

Rootkits

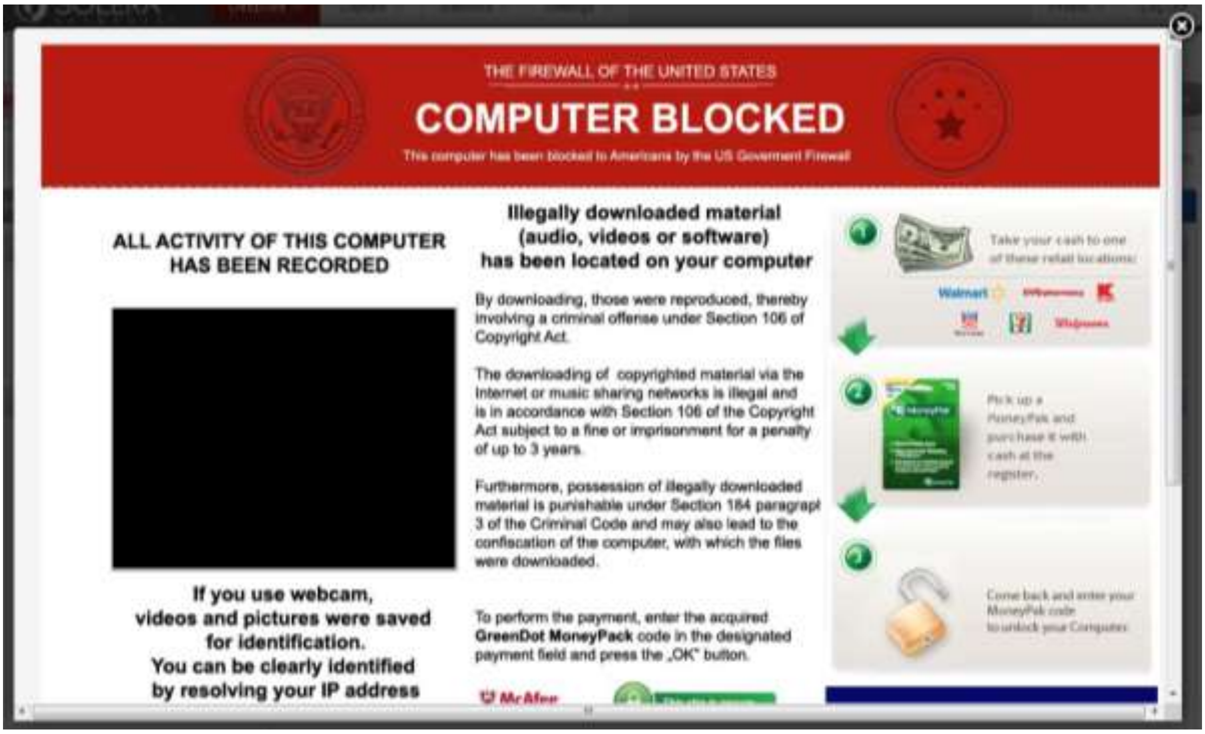
Rootkits are the stealth type of malware. They are designed in some special way that they can actually hide themselves very well and it is quite difficult to detect them in a system. The normal methods of detection do not work on them.

Botnets

Botnet is a software installed on a computer that is connected through the internet and it can help one communicate with the other same type of programs, so that some actions can be performed. They can be same as keeping control of some IRC, which are Internet Related Charts. In addition, it can be utilized for sending out some spam emails or to participate in some distribution of denial of services attacks.

Ransom Ware

Ransom ware is a software that encrypts files, which are on the hard drives. Some of them can even end up with simply showing some message about payment of money to the person, who has implemented this program.



THE FIREWALL OF THE UNITED STATES

COMPUTER BLOCKED

This computer has been blocked to Americans by the US Goverment Firewall

ALL ACTIVITY OF THIS COMPUTER HAS BEEN RECORDED

If you use webcam, videos and pictures were saved for identification. You can be clearly identified by resolving your IP address

Illegally downloaded material (audio, videos or software) has been located on your computer

By downloading, those were reproduced, thereby involving a criminal offense under Section 106 of Copyright Act.

The downloading of copyrighted material via the Internet or music sharing networks is illegal and is in accordance with Section 106 of the Copyright Act subject to a fine or imprisonment for a penalty of up to 3 years.

Furthermore, possession of illegally downloaded material is punishable under Section 184 paragrapl 3 of the Criminal Code and may also lead to the confiscation of the computer, with which the files were downloaded.

To perform the payment, enter the acquired **GreenDot MoneyPack** code in the designated payment field and press the „OK" button.

1 Take your cash to one of these retail locations:

2 Pick up a MoneyPak and purchase it with cash at the register.

3 Come back and enter your MoneyPak code to unlock your Computer.

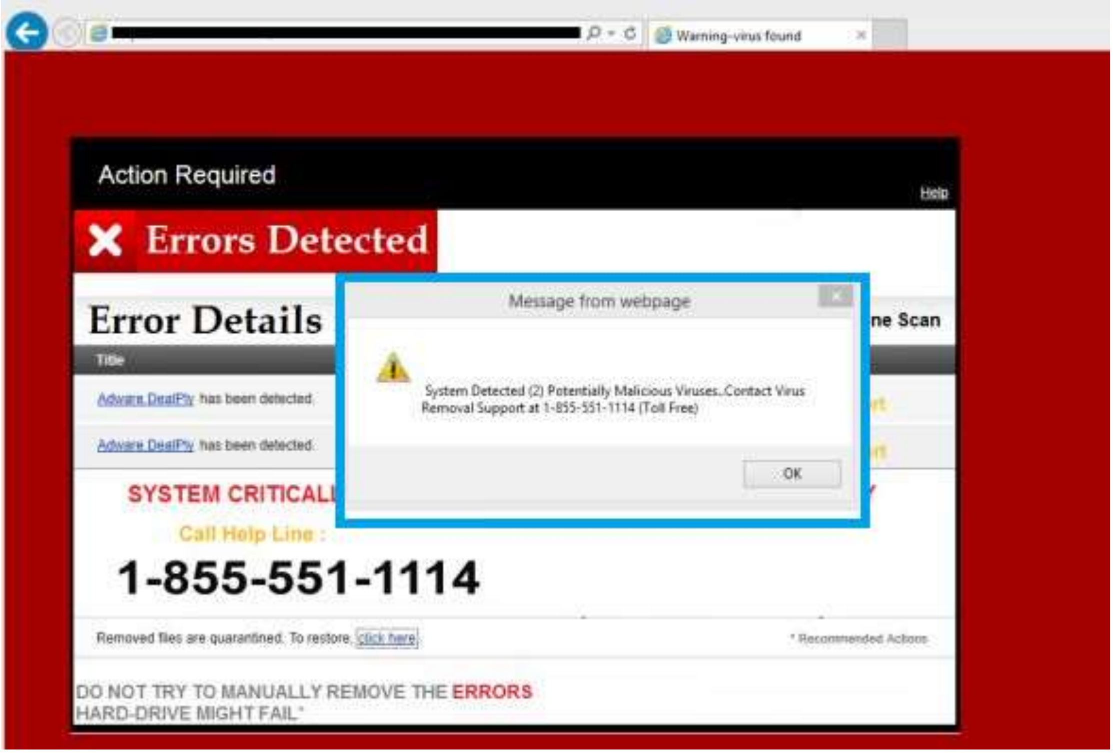
4. Malware – Detection Techniques

Generally, if a computer is infected there are some symptoms, which even simpler users can notice.

Common Malware Detection Techniques

Some of the most commonly used Malware Detection Techniques are listed as follows.

- Your computer shows a pop-up and error message.



[redacted]

Action Required

Errors Detected

Error Details

Adware DealPly has been detected.

Adware DealPly has been detected.

SYSTEM CRITICALL

Call Help Line :

1-855-551-1114

Removed files are quarantined. To restore, click here

* Recommended Actions

DO NOT TRY TO MANUALLY REMOVE THE ERRORS
HARD-DRIVE MIGHT FAIL*

ne Scan

Message from webpage

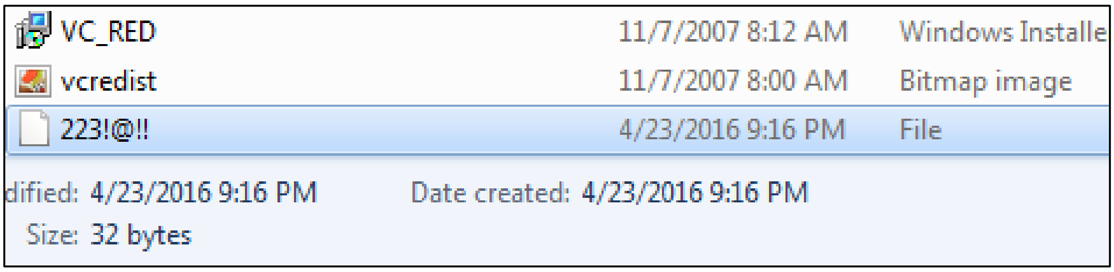
System Detected (2) Potentially Malicious Viruses..Contact Virus Removal Support at 1-855-551-1114 (Toll Free)

- Your computer freezes frequently and you are unable to work on it.

- The computer slows down when a program or process starts. This can be noticed in the task manager that the process of the software has started, but it has not opened yet for working.

- Third parties complain that they are receiving invitation in social media or via emails from you.

- File extensions changes appear or files are added to your system without your consent.



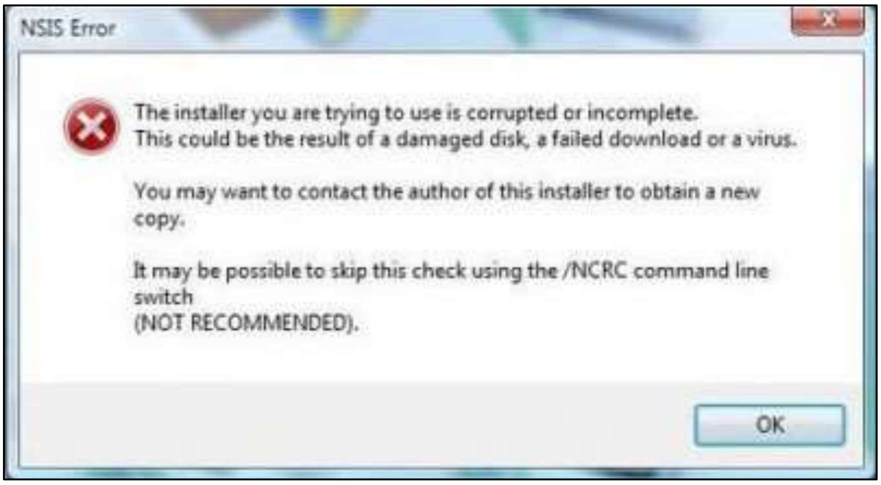
VC_RED	11/7/2007 8:12 AM	Windows Installe
vcredist	11/7/2007 8:00 AM	Bitmap image
223!@!!	4/23/2016 9:16 PM	File

dified: 4/23/2016 9:16 PM Date created: 4/23/2016 9:16 PM

Size: 32 bytes

- Internet explorer freezes too often even though your internet speed is very good.
- Your hard disk is accessed most of the time, which you can see from the blinking LED light of your computer.

- OS files are corrupted or missing.



NSIS Error

The installer you are trying to use is corrupted or incomplete.
This could be the result of a damaged disk, a failed download or a virus.

You may want to contact the author of this installer to obtain a new copy.

It may be possible to skip this check using the /NCRC command line switch
(NOT RECOMMENDED).