CS-MINOR-SEP

Name – Anjali Kumari

Email- anjalirajwar101@gmail.com

Collage Name – BIT Sindri

Domain – Cyber Security

Project Name : Cyber Security Minor Project

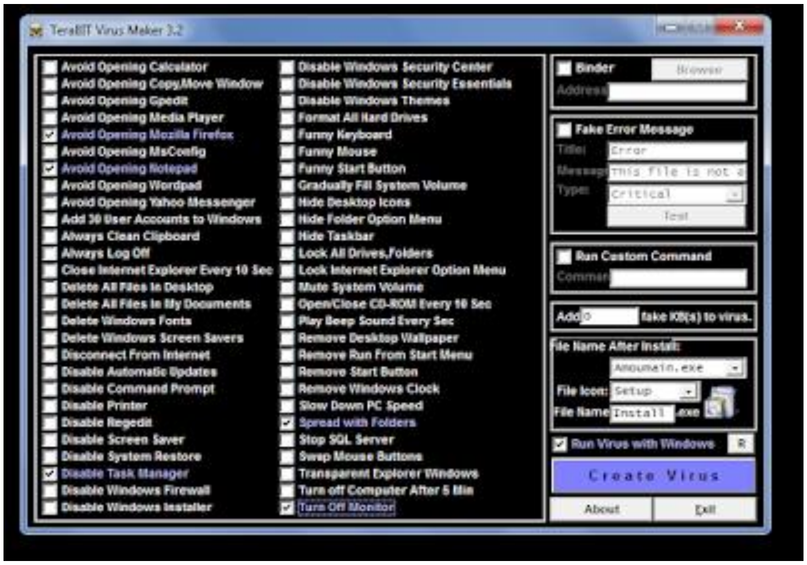
3. Use Tetrabit virus maker Tool (Download from Internet) to create a virus and inject in to Virtual system and perform destruction program as per your wish and write a document along with screenshots and suggest the preventive measures to avoid this malware affect Hacker Machine : Windows 7 / Windows 10 Victim machine : Windows XP / Windows 7

Download the application must first Terabit Virus Maker then install. Download here !

Check the action on the part of the virus. For example, here I just menceklis some action, namely:

- **Avoid Opening Mozilla Firefox**

- Avoid Opening Notepad
- Disable Task Manager
- Spread with Folders
- Turn off Monitor
- And others simply choose according to your liking



TeraBIT Virus Maker 3.2

□ Avoid Opening Calculator
□ Avoid Opening Copy,Move Window
□ Avoid Opening Gpedit
□ Avoid Opening Media Player
☑ Avoid Opening Mozilla Firefox
□ Avoid Opening MsConfig
☑ Avoid Opening Notepad
□ Avoid Opening Wordpad
□ Avoid Opening Yahoo Messenger
□ Add 30 User Accounts to Windows
□ Always Clean Clipboard
□ Always Log Off
□ Close Internet Explorer Every 10 Sec
□ Delete All Files In Desktop
□ Delete All Files In My Documents
□ Delete Windows Fonts
□ Delete Windows Screen Savers
□ Disconnect From Internet
□ Disable Automatic Updates
□ Disable Command Prompt
□ Disable Printer
□ Disable Regedit
□ Disable Screen Saver
□ Disable System Restore
☑ Disable Task Manager
□ Disable Windows Firewall
□ Disable Windows Installer

□ Disable Windows Security Center
□ Disable Windows Security Essentials
□ Disable Windows Themes
□ Format All Hard Drives
□ Funny Keyboard
□ Funny Mouse
□ Funny Start Button
□ Gradually Fill System Volume
□ Hide Desktop Icons
□ Hide Folder Option Menu
□ Hide Taskbar
□ Lock All Drives,Folders
□ Lock Internet Explorer Option Menu
□ Mute System Volume
□ Open/Close CD-ROM Every 10 Sec
□ Play Beep Sound Every Sec
□ Remove Desktop Wallpaper
□ Remove Run From Start Menu
□ Remove Start Button
□ Remove Windows Clock
□ Slow Down PC Speed
☑ Spread with Folders
□ Stop SQL Server
□ Swap Mouse Buttons
□ Transparent Explorer Windows
□ Turn off Computer After 5 Min
☑ Turn Off Monitor

□ Binder
Address:

□ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

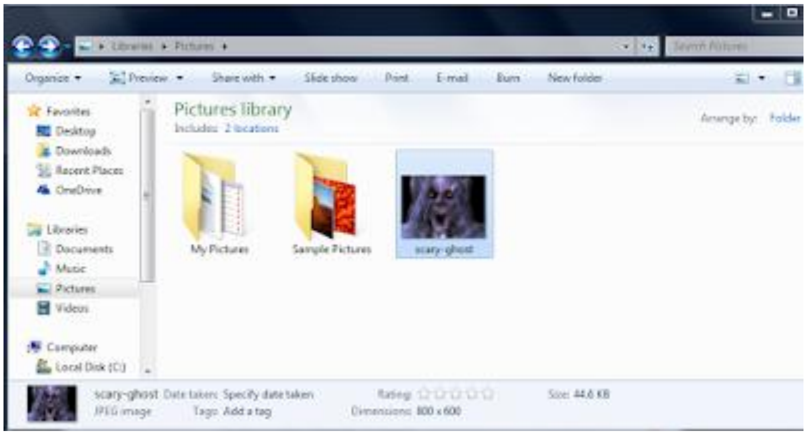
□ Run Custom Command
Command:

Add 0 fake KB(s) to virus.

File Name After Install: Amoumain.exe
File Icon: Setup
File Name: Install .exe

☑ Run Virus with Windows

If so now please click Browser to find the file that will be inserted.
As an example I will insert the picture below.



scary-ghost Date taken: Specify date taken Rating: ☆☆☆☆☆ Size: 44.6 KB
JPEG image Tags: Add a tag Dimensions: 800 x 600

Thus, if the virus is executed it will open the following images.
Then in the Fake Error Message please create headings and text messages that you want on the Message box.
In the File Name After Install please specify a file of the virus. Here I chose to Microsoft Word icon.

And I gave the name Secret in the File Name box
Then click the Create button Virus
Determine where you want to place the virus file and click OK

Virus file created successfully.

Since my last select Microsoft Word icon, the virus also shaped exactly like a Microsoft Word file and absolutely not suspicious.

If the virus is executed, it will immediately open an image that we had a paste.

Then will appear and a message was created.
Furthermore, the virus will infect the victim's computer according to the action that you created earlier.
Congratulations !! you successfully create a virus.

How to prevent malware

1. **Keep your computer and software updated :-** Microsoft and Apple often release updates for their operating systems, and it's a good idea to install these updates when they become available for your Windows and Mac computers.

2. **Use a non-administrator account whenever possible :-** Most operating systems allow you to create multiple user accounts on your computer, so that different users can have different settings. These user accounts can also be set up to have different security settings.

3. **Think twice before clicking links or downloading anything:-** In the real world, most people would probably be a little suspicious about stepping into a shady-looking building with a sign that says "Free computers!" in flashing lights. On the web, you should adopt a similar level of caution when entering unfamiliar websites that claim to offer free things.

4. **Be careful about opening email attachments or images:-** If a random person sends you a box of chocolates in the mail, would you open it and scarf it down without any hesitation? Probably not. Similarly, you should be wary if a random person sends you a suspicious email containing attachments or images. Sometimes, those emails might just be spam, but other times, those emails might secretly contain harmful malware.

5. **Don't trust pop-up windows that ask you to download software :-** When surfing the web, you might come across sites that show pop-up windows, making you believe your computer has been infected and asking you to download some software in order to protect yourself.

6. **Limit your file-sharing:-** Some sites and applications allow you to easily share files with other users. Many of these sites and applications offer little protection against malware. If you exchange or download files using these file-sharing methods, be on the lookout for malware.

7. **Use antivirus software :-** If you need to download something, you should use an antivirus program to scan that download for malware before opening it. Antivirus software also allows you to scan your entire computer for malware. It's a good idea to run regular scans of your computer to catch malware early and prevent it from spreading.

Thank You…