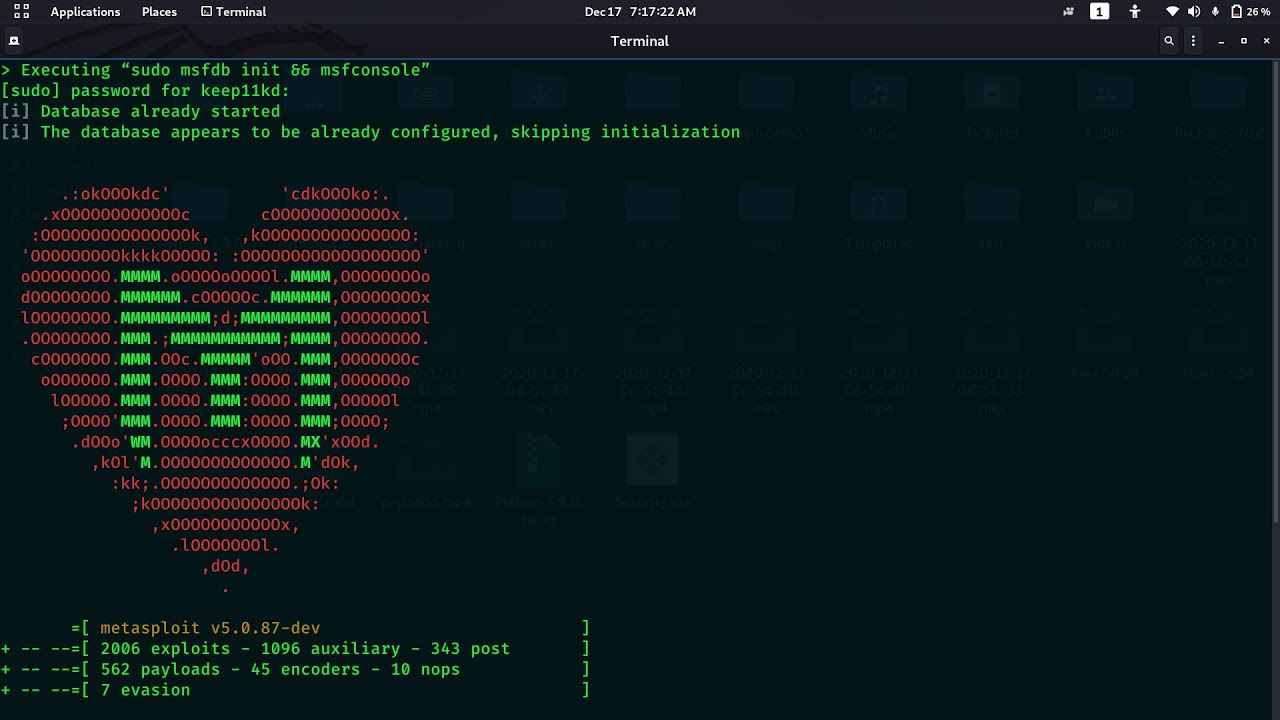
**Game Of Payloads**

Hey techies , our todays title is payloads not that PUBG’s payload gaming mode . It is a real life cyber game with same level of destructions and this is well said by **JOHN MARIOTTI** in his quote given below : -

“**We worried for decades about WMDs – Weapons of mass destruction. Now it is time to worry about a new kind of WMDs – Weapons of mass disruption” .** It is like a game of “hide and seek”, if you hide it successfully then definitely you will win the game. The payload can be anything from a simple virus to a more complex piece of malware such as rootkit. This malware is usually spread via email attachments , websites , software applications , and other means of electronic distribution.

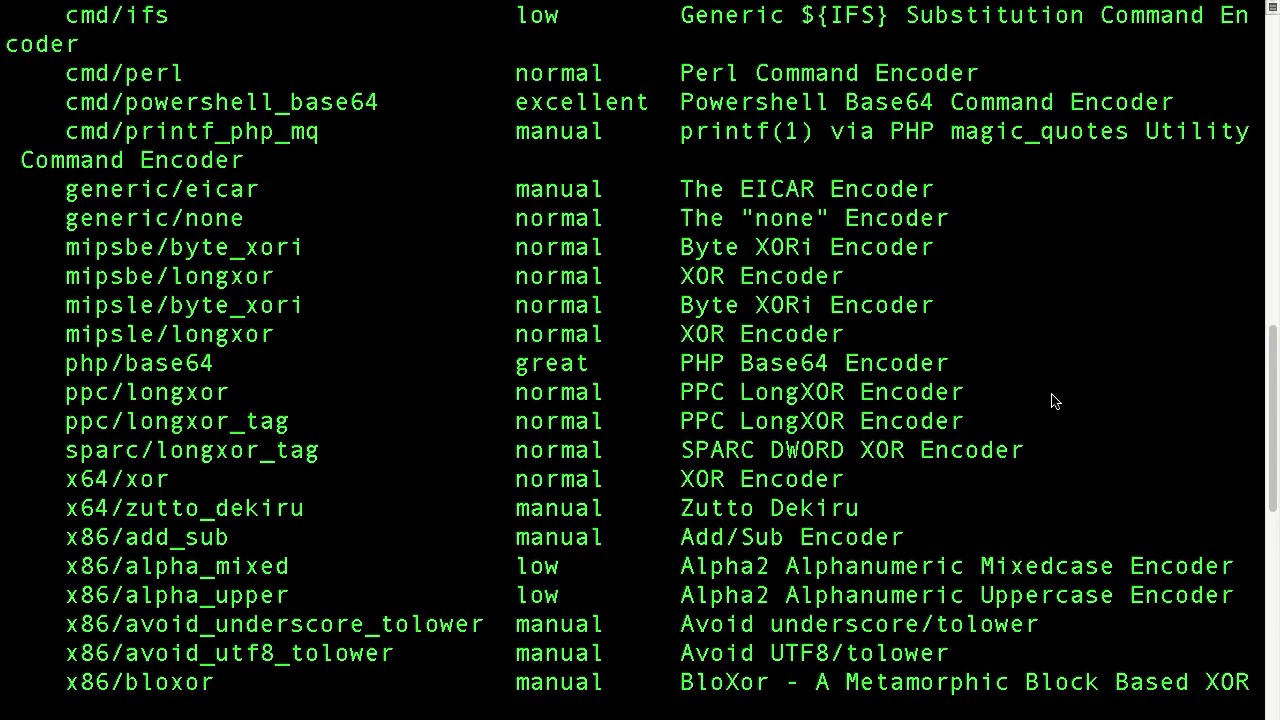


**Let’s Know the Payload :**

Payloads are the components of a malware program which is typically some form of malicious code that perform malicious actions on a victim’s system. These actions can include deleting files, stealing data, or installing additional malware. It is designed to perform a specific function or set of functions. It is typically installed by a virus or worm and is executed when the system is booted up. It may be installed as part of a larger piece of software, or it may be installed separately.

**Working of the Payload :**

Once it installed in system , it direct connects the target system with the source system and makes the target system vulnerable or easily exploitable. Now , attacker can easily access any data from compromised system and also use that system to perform many cyber attacks such as DoS (Denial-of-service) , Man in the middle , etc.

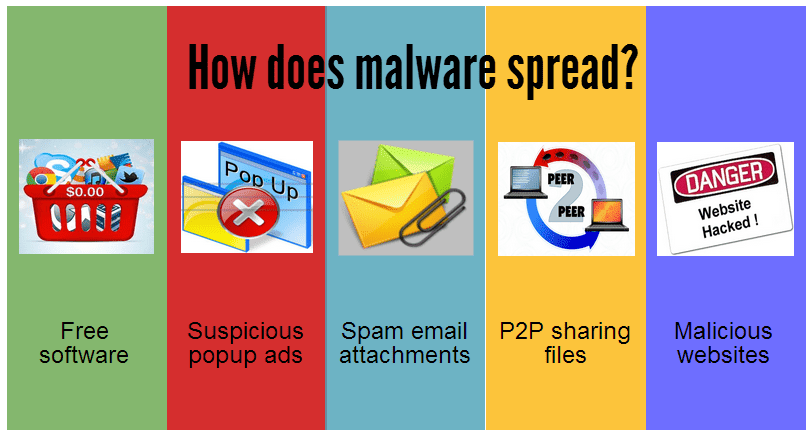


The payload is a .NET assembly compiled for any CPU. It is a simple C# console application that executes the following tasks:

* Disable Windows Defender
* Copies itself to hidden directory in the user’s home directory
* Spawns a CMD process and runs a .vbs script
* In the CMD process , it waits for a process to end then delete .vbs script and C# console application
* In the CMD process , it executes a PowerShell script that downloads and executes a payload from a remote server

**How it unfurls :**

There are many ways that payload malware can spread. One common way is for the malware to be embedded in a piece of software that is downloaded from the internet. Once the software is installed, the malware is executed and can then begin to spread to other computers on the network. Another common method is for the malware to be emailed to unsuspecting users. When the email is opened, the attachment is executed and the malware can begin to spread.



<https://1.bp.blogspot.com>

**Demolition by Payloads :**

In recent years, payload malware has become increasingly prevalent. This type of malware is designed to remain dormant on a system until it is triggered by a specific event or condition. Once activated, payload malware can cause a wide range of damage, from deleting files to encrypting data. Payload malware is often used in targeted attacks, where the attackers have specific goals in mind. This type of malware can be very difficult to detect and remove, as it is designed to avoid detection by security tools.

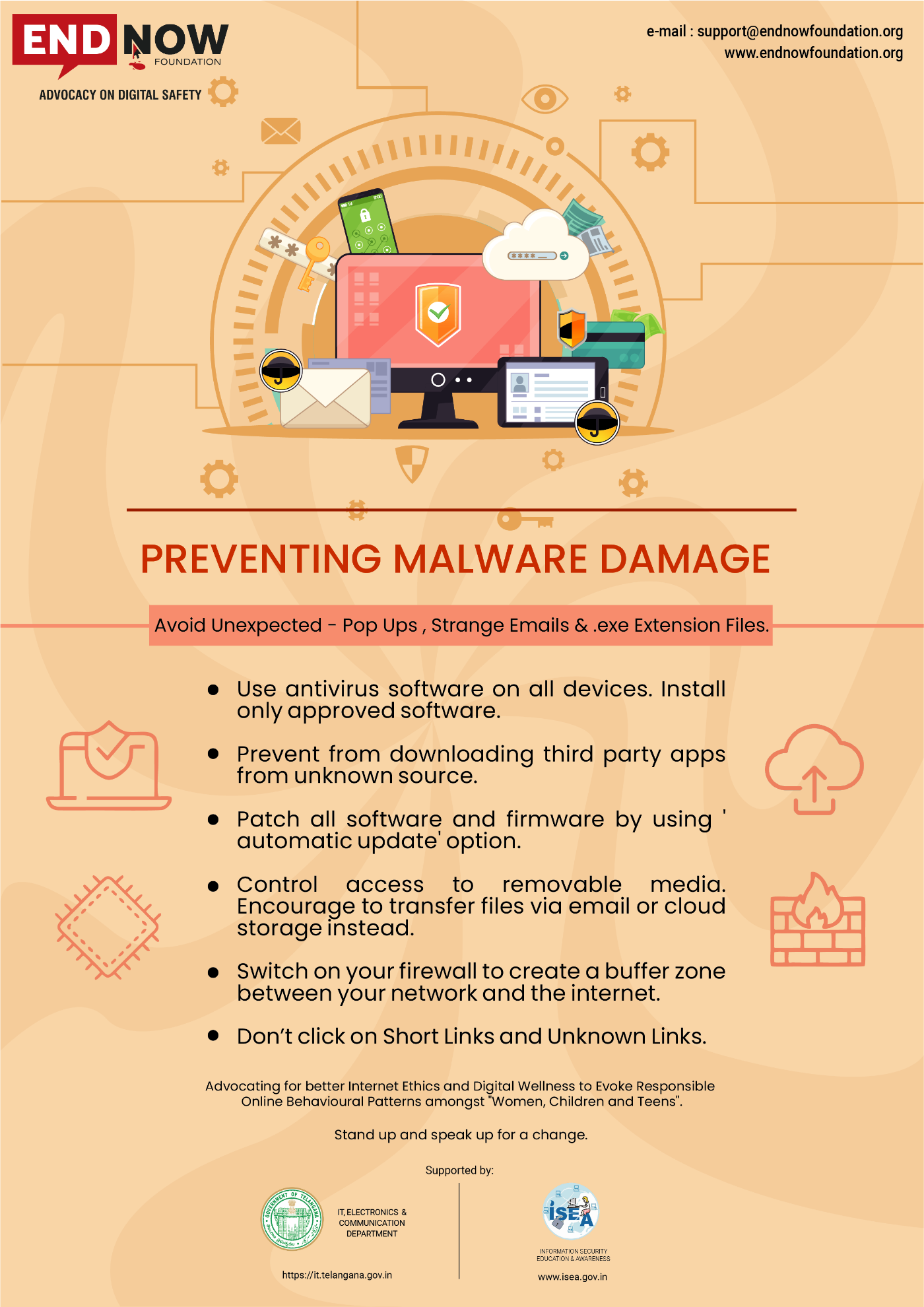


<https://sectigostore.com>

One of the most common payload malwares is the WannaCry ransomware , which made headlines in 2017 after it infected over 200,000 computers in 150 countries and caused billions of dollars in damages. WannaCry spread via email attachments and exploit kits , and once it gains access to system , it encrypts all of the user’s file and demands a ransom be paid in order to decrypt them. Other notable payload malwares include Stuxnet , which was used to sabotage Iran’s nuclear program , and NotPetya , which caused over $10 billion in damages after it crippled Ukraine’s infrastructure.

**Safety Measures:**

The capability of payloads is defined by level of encryption and encoding used in it because of that reason sometimes system security panel doesn’t recognize any malware or malfunctioning in the system. For different type of Operating Systems different types of payloads are used by the attacker.



<https://www.endnowfoundation.org>

In case of payload malware, it is common for attackers to upload malicious code to the server and run it from the browser. One way to prevent this is to remove the .php extension from all files that do not need to be executed by the server.

However, this method has one big disadvantage. Normally, all files with the .php extension are executed by the server, so the attacker can upload a malicious file with the .php extension, and the server will execute the code. The attacker can then use the same code to call the file without the .php extension, and the server will execute the malicious code.

**How to Remove the .php Extension?**

In order to remove the .php extension, you need to edit the .htaccess file on your server and add the following lines of code:

**Options +FollowSymLinks RewriteEngine On RewriteCond %{REQUEST\_FILENAME} !-d RewriteCond %{REQUEST\_FILENAME}\.php -f RewriteRule ^(.\*)$ $1.php [NC,L]**

This code tells the server to remove the .php extension from all files that do not need to be executed by the server.

**About Me :**

Hey guyz , myself Deepak Verma , 2nd year UG student at IIIT-Allahabad and member of Cyber Security Wing at GeekHaven , IIIT-A. If you want more cyber security stuffs then just stay tuned with me . You can reach me here [LinkedIn](https://www.linkedin.com/in/deepak-verma-a7bb54234/) . Thanks everyone who gave your’s precious time to read this blog .