

Forum:[Hack Forums](#)

Thread: [./Dark Legion/Blocking Malicious Entities with HOSTS File](#)

Dread.Reaper - March 31, 2023, 9:55 am

@Genuine@

The Windows HOSTS file is a local plain-text file that maps domain names to IP addresses. When a user types a domain name into their web browser or other network application, the HOSTS file is checked first to see if there is a corresponding IP address associated with that domain. If there is, the application will use that IP address to connect to the domain.

By editing the HOSTS file, users can add entries to block access to specific IP addresses or domain names. This can be useful for blocking access to known malicious websites or blocking ads and other unwanted content.

To block a malicious entity using the HOSTS file, a user can add an entry for the domain name associated with the malicious entity and map it to the IP address of their local machine or to an IP address that doesn't exist. This effectively prevents any connections to that domain name or IP address from being established, effectively blocking the malicious entity.

For example, if a user wants to block access to a malicious website called "example.com", they could add an entry to their HOSTS file that looks like this:

```
127.0.0.1 example.com
```

This maps the domain name "example.com" to the loopback IP address, which is the IP address used to refer to the local machine. When the user attempts to connect to "example.com", their application will attempt to connect to the loopback address instead, effectively blocking access to the malicious website.

Using the HOSTS file to block malicious entities can be a useful additional layer of security, but it's important to note that it's not a substitute for other security measures such as antivirus software or firewalls. Additionally, the HOSTS file can become large and difficult to manage if too many entries are added, so it's important to keep it well-organized and up-to-date.

Attached is my personal HOSTS file used. ?