This article will discuss the Silkroad Edx Loader 6.30 and what it does. In short the Silkroad Edx Loader is a software that executes encoded DLL files from a given directory with Microsoft's Internet Explorer, Firefox, or Google Chrome browser in order to run malicious-looking JavaScript on infected machines. The most important part of this software's functionality is to load a remote DLL file by exploiting a Windows vulnerability in IE6 and newer browsers. This remote DLL is an obfuscated shellcode which can be used to download additional malware or exfiltrate data from vulnerable systems by sending it back to the attacker's computer. Silkroad Edx Loader was developed by Grupochek, a cybercriminal group that is well known for their blackhat software and the theft of data from internal corporate networks. It was released in 2012 and is used widely (about 12,000 computers were infected by this piece of malware). This operating system infection technique uses social engineering to trick internet users into clicking on malicious links or visiting compromised websites. The attackers delivering the malicious code behind Silkroad Edx Loader use "drive-by" malware attacks to gain unauthorized access to computers without user interaction. For example, the attacker could have modified a legitimate search engine's homepage so that it contains malicious code to download the infected shellcode. The file is then downloaded by the legitimate IE browser, which then executes it. Any web browser that runs on Windows XP or Vista are vulnerable to this type of attack. If any application that uses Windows' built-in IE rendering engine is installed on a machine, it is likely to be compromised as well because the weaponized DLL file used to infect the system will be run in memory by the client browser itself if it is signed by Microsoft, and not by an external program. The vulnerability exploited by this program is CVE-2012-4788, which Microsoft addressed on May 8, 2012. It is critical to install the update for this vulnerability as soon as possible if you are using Internet Explorer. When the DLL file downloads the malicious JavaScript code it will then run on the victim's machine. This will either be a variant of the infamous Blackhole Exploit Kit or some other type of malware that targets various vulnerabilities on Windows systems. The instructions below are for users who have already been infected with Silkroad Edx Loader, and want to remove it from their machines. To remove the malware, follow the steps below. This process will erase all data on the computer, including personal files that have been copied onto it. It is important to also backup any files that are of importance before proceeding with the steps below. 1.] If you have installed IE on your system, go to Control Panel | Programs | Turn Windows Features On or Off. 2.] Open Internet Explorer and select Manage Add-ons from the Tools menu at the top of the browser window. 3.] Locate and disable plugins for Silkroad Edx Loader DLL file ("Silkroad_EDX_Loader_6.30").

688eeb4e9f3225