

USB Switchblade - Take passwords and take names

₪0.0267

[add to cart](#) | [bookmark](#) | [discuss 0](#) | [report](#)

Item info:	
seller	DrawkwarD 0.0
ships from	undeclared
ships to	Worldwide
category	Media

Description

USB Switchblade is the outcome of community project to merge various tools and techniques that take advantage of various Microsoft Windows security vulnerabilities, the majority of which are related to USB ports.

The primary purpose of this tool is to silently recover information from Windows systems, such as password hashes, LSA secrets, IP information as well as browser history and autofill information as well as create a backdoor to the target system for later access. The tool through community development ended up creating a Frankenstein application that exposed some very serious security vulnerabilities in Windows, particularly with regards to removable media devices.

The tool takes advantage of a security hole in U3 drives that allows the creation of a virtual CD-ROM drive, which allows the Windows autorun feature to work (unless disabled on the target system). Even if autorun or a U3 drive is not used, the application can still be started by executing a single script on the drive.

The most damaging feature of this tool is the ability to extract the passwords hashes from the target system and load them onto the drive for later cracking through the use of Rainbow tables. The weakness of Windows LM hashes is fairly well known. With this application installed on a U3 drive it would only take a few seconds for someone with malicious intent to plug in the drive to an open USB port on a system and walk away with the passwords for that system.

The application also finds browser history (for both IE and Firefox) including autofill information (exposing website passwords etc), as well as AIM and MSN Messenger passwords. It will also reveal product keys for some applications (mostly Microsoft applications).

The tool will also create a ghost admin account, which can function as a back door to the system if it is not behind a firewall.

The tool has evolved in the last month or so to include multiple version including a way to circumvent anti-virus protection that would usually detect some of the malicious executables. Additional files were also added to check the vulnerabilities listing all security and patches installed to the target system, as well as another which will start a VNC service silently in the background.

Reviews:

sort by: 

GOVERNMENT
EXHIBIT
916 T
14 Cr. 68 (KBF)