Ethical Hacking and Countermeasures

Version 6

Module XLI

Hacking USB Devices

CEH™ Certified Ethical Hacker News

'Silly' worm targets USB sticks

Malware uses old-fashioned propagation technique

Iain Thomson, vnunet.com 04 May 2007

Experts are warning of a new worm which spreads via USB keys in a reversion to the earliest methods of virus distribution.

SillyFD-AA installs itself onto systems and puts a message in Internet Explorer reading 'Hacked by 1BYTE'. It also installs an autorun.inf on any removable drives, such as USB sticks or floppy discs.

"USB keys are becoming so cheap that marketing people are prepared to use them as 'throwaways' with the aim of securing sales leads," said Graham Cluley, senior technology consultant for Sophos.

"Computer owners should tread very carefully when plugging an unknown device into their PC, however, as it could have malicious code planted on it.

"With a significant rise in financially motivated malware it could be an obvious backdoor into a company for criminals bent on targeting a specific business with malicious code."

Once the drive is connected to another computer the worm automatically installs itself on the new computer and repeats the exercise in an attempt to spread further. Users are advised to turn off the Autorun feature in Windows.

The technique mimics the very earliest methods of virus propagation when viruses were spread solely via floppy discs.

Virus protection then was easy; users simply had to cover the indented tab on a 5.25in floppy with sticky tape, the so called 'virus condom'.

Permalink to this story

www.vnunet.com/2189228

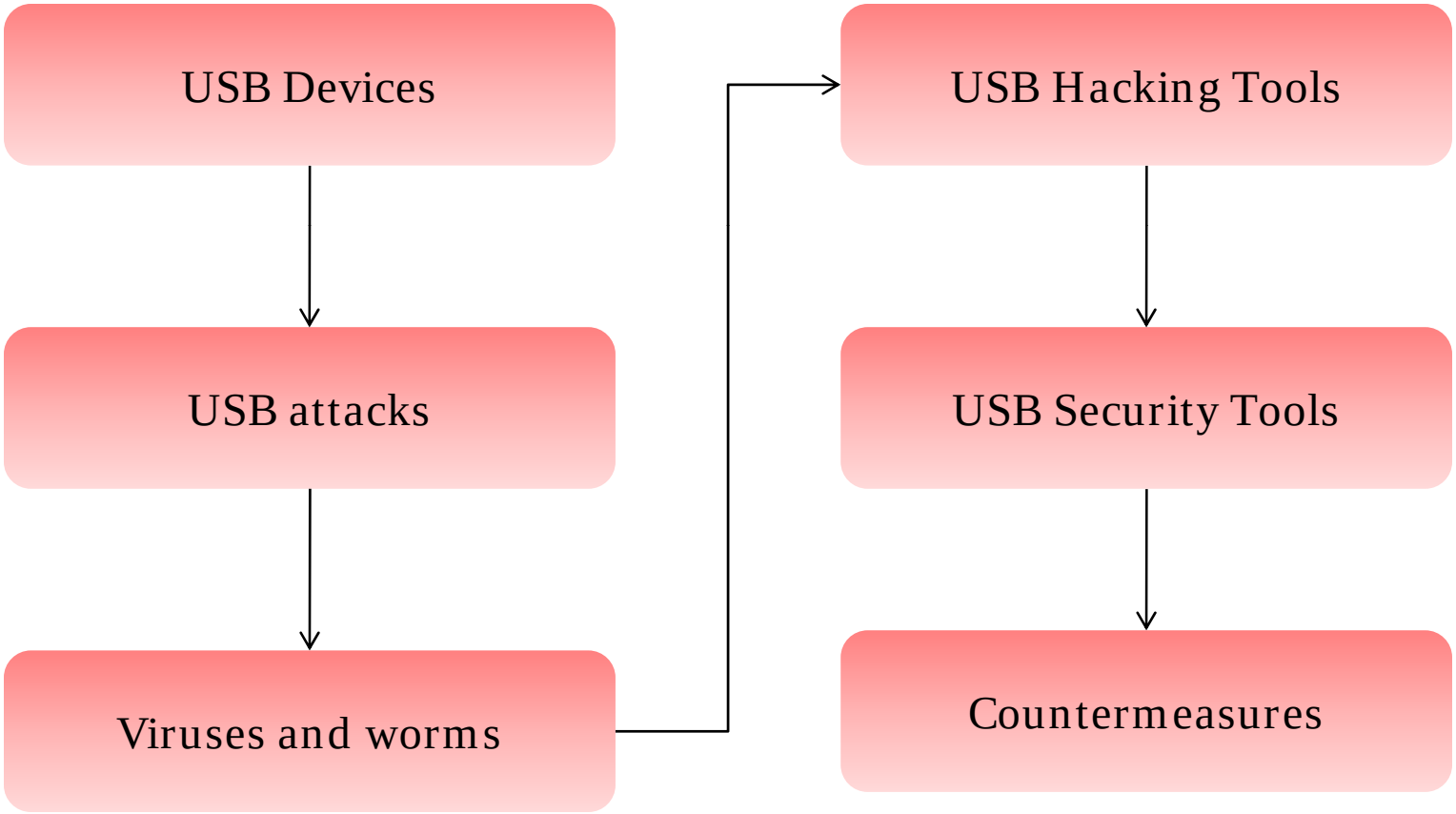
Source: *http://www.vnunet.com/*

Module Objective

This module will familiarize you with:

- USB Devices
- USB attacks
- Viruses and worms
- USB Hacking Tools
- USB Security Tools
- Countermeasures

Module Flow



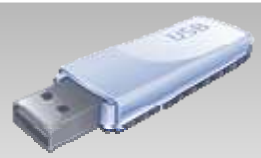
Introduction to USB Devices

Universal Serial Bus (USB) is a serial bus standard to interface devices

It is pluggable, allowing device to be connected or removed while computer is running

A pen drive is a compact, removable storage device just like a floppy disk or a CD

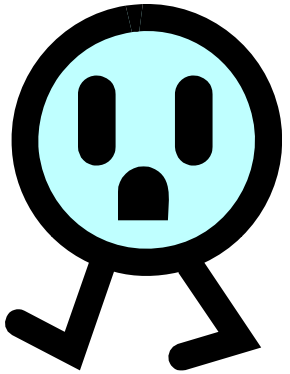
A pen drive can be plugged into the USB port



USB Attacks

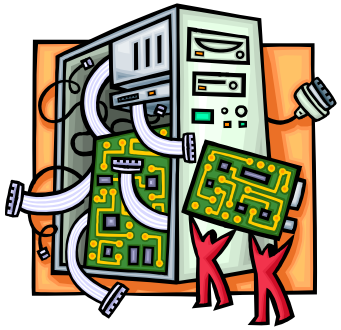
Electrical Attack

Electrical attacks mounted against the USB keys require physical access to the device circuit boards



Primary goal is to access private data, which is supposed to be protected by legitimate user's PIN number or password without detection by the legitimate user

A design flaw common to the USB keys is the improper storage of password values, which can allow the extraction of all data, including private information



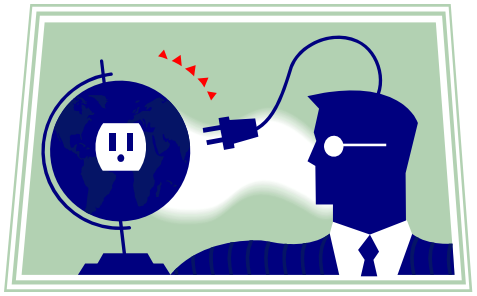
Changing the password value which is stored in an EEPROM allows access to the device and extract all private information

Software Attack

Attacker examines the communication channels between the USB device and host computer

It analyzes and determines the possibility to brute-force a password which will give access to the USB key device

By sending incorrect and known erroneous USB packets to the USB key, USB may leak information such as the contents of protected memory areas



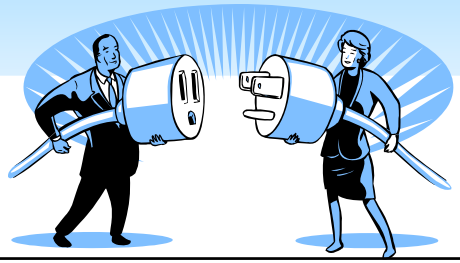
USB Attack on Windows

Buffer-overflow vulnerabilities in USB device allow an attacker to bypass the Windows security and gain administrative privileges of the host machine

Attacker having idea about the vulnerability in a USB device driver can program one USB device, known as portable memory stick, to pose as the kind of device that uses the vulnerable driver

Attacker then plugs the device into the host system and triggers the exploit when the host system loads the flawed driver

This allows an attacker to take control of host computer



Viruses And Worms

Virus: W32/Madang-Fam

W32/Madang-Fam is a family of viruses for the Windows platform, which spreads via Removable storage devices

It attempts to infect files with an EXE or SCR extension on all drives and on connected network shares

It contains the code to download and execute code from one or more remote websites

It may attempt to run the files <System>\setupx.exe and <System>\Updatex.exe

It attempts to inject itself into the Kernel or into another process that is already running

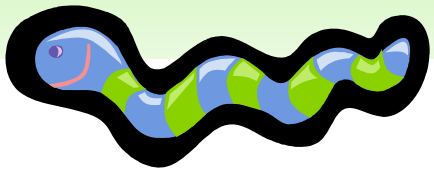
Worm: W32/Hasnot-A

W32/Hasnot-A is a worm and companion virus for the Windows platform, which spreads via Removable storage devices

W32/Hasnot-A will hide files and folders, appending the original file or folder name to a copy of itself

Once installed, W32/Hasnot-A spreads through network shares and removable storage devices, including USB keys

File <Root>\autorun.inf is designed to start the worm once the drive is mounted



W32/Fujacks-AK

W32/Fujacks-AK spreads to other network computers through available network shares and removable storage devices

It copies itself with the filenames GameSetup.exe and setup.exe correspondingly

It also creates the file autorun.inf to insure that the file setup.exe is executed

It has the functionality to access the Internet and communicate with a remote server via HTTP

It attempts to periodically copy itself to removable drives, including floppy drives and USB keys

W32/Fujacks-E

W32/Fujacks-E is a prepending virus and worm with backdoor functionality for the Windows platform

It spreads in network computers through available network shares and removable storage devices with the filenames GameSetup.exe and setup.exe correspondingly

It runs continuously in the background, providing a backdoor server which allows a remote intruder to gain access and control over the computer

It has the functionality to access the Internet and communicate with a remote server via HTTP and it may change HTML files

W32/Dzan-C

W32/Dzan-C is a virus for the Windows platform that also spreads via removable storage devices

It runs continuously in the background, providing a backdoor server which allows a remote intruder to gain access and control over the computer

It adds its 66048 Bytes of code at the end of the original file, so whenever the file is executed, the virus is also executed

W32/SillyFD-AA

W32/SillyFD-AA is a worm for the Windows platform

Once installed, W32/SillyFD-AA spreads through removable storage devices, including floppy drives and USB keys

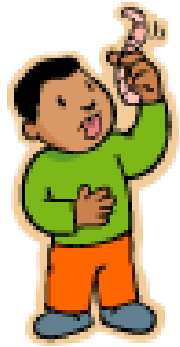
This worm attempts to create a hidden file Autorun.inf on the removable drive and copies itself to the removable drive with the hidden filename <Root>\handydriver.exe

W32/SillyFDC-BK

W32/SillyFDC-BK is a worm for the Windows platform

W32/SillyFDC-BK spreads via removable shared drives by copying itself to <Root>\krage.exe and creating the file <Root>\autorun.inf

File <Root>\autorun.inf is designed to run the worm when the removable drive is connected to an uninfected computer



W32/LiarVB-A

W32/LiarVB-A is a worm for the Windows platform

Once installed, W32/LiarVB-A spreads through network shares and removable storage devices, including floppy drives and USB keys

W32/LiarVB-A copies itself to the root folder of the drive and adds an autorun.inf file

W32/LiarVB-A leaves an html file on the infected system with a message about AIDS

W32/Hairy-A

W32/Hairy-A is a worm for the Windows platform

W32/Hairy-A will attempt to copy itself and create autorun.inf to removable drives

W32/Hairy-A changes settings for Microsoft Internet Explorer by modifying values

W32/QQRob-ADN

W32/QQRob-ADN is a worm for the Windows platform

W32/QQRob-ADN spreads by copying itself to removable storage devices

W32/QQRob-ADN copies itself to removable storage devices as the hidden file oso.exe and creates a hidden autorun.inf to launch oso.exe automatically when the device is plugged in

W32/QQRob-ADN attempts to block access to security-related sites by modifying the HOSTS file

W32/VBAut-B

W32/VBAut-B has functionality to spread via removable storage devices and Instant Messaging protocols and to download, install, and run new software

This worm attempts to copy itself with the filename boot.exe to the available removable storage device creating Autorun.inf to ensure that the copy of the worm is executed once device is accessed

HTTP W32.Drom

HTTP W32.Drom is a worm for the Windows platform

W32.Drom is a worm that downloads and executes malicious files on the compromised computer and spreads through removable storage devices

Hacking Tools

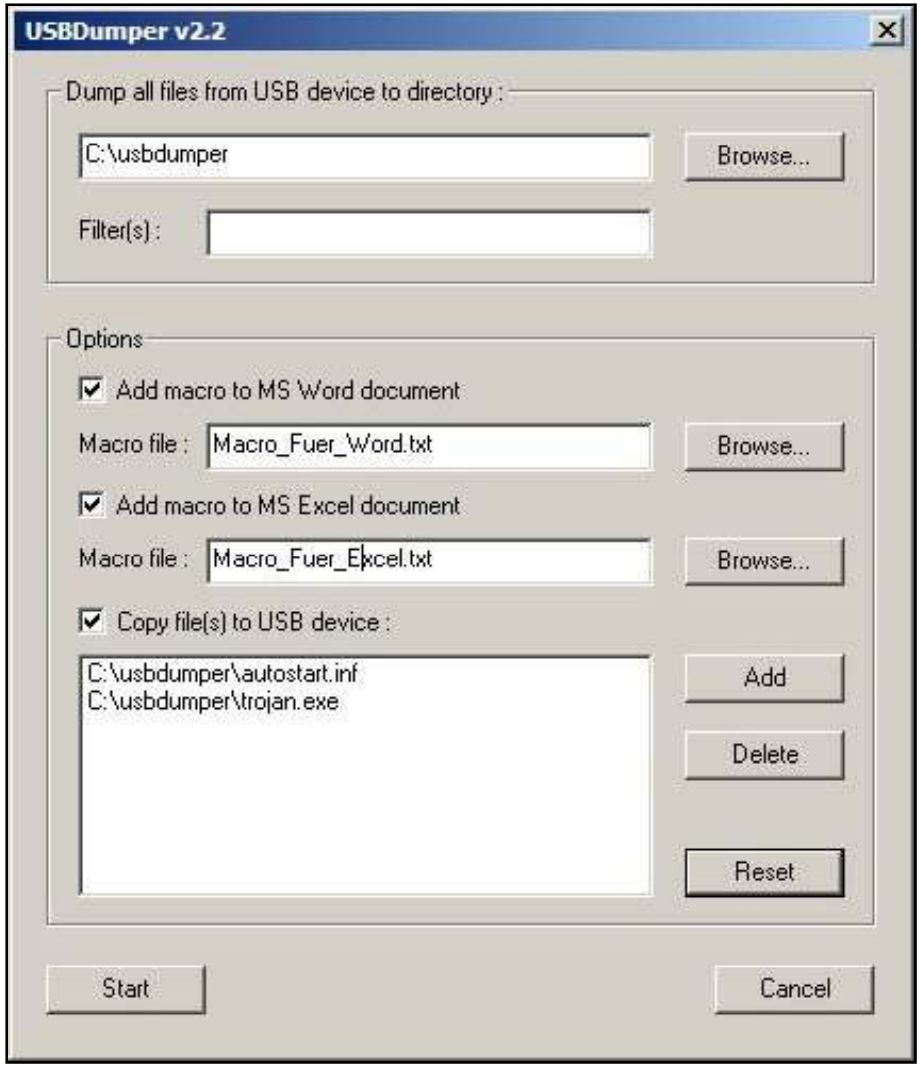
USB Dumper

USB Dumper is an application that when installed on a system runs a background process which copies files from any USB flash drive installed to it silently

Simplicity of this application is what makes it quite dangerous, it needs a user to double click the executable

Once this is done, application runs in the background and any USB drive that is connected will automatically have its contents downloaded to the system

USB Dumper: Screenshot



USB Switchblade

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

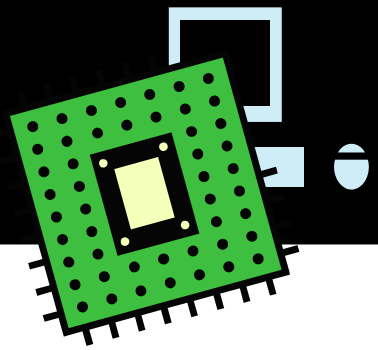
Purpose of this tool is to:

- Silently recover information from Windows systems, such as password hashes, LSA secrets, IP information, browser history, and auto fill information
- Create a backdoor to the target system for later access

It takes advantage of a security hole in U3 drives that allows the creation of a virtual CD-ROM drive, which allows the Windows auto run feature to work

If auto run or a U3 drive is not used, the application can still be started by executing a single script on the drive

USB Hacksaw



USB Hacksaw is an application created as a proof of concept developed by Hak5 and as an extension to the USB Switchblade

USB Hacksaw uses a modified version of USB Dumper that once installed on a system will run a process in the background whenever that computer starts, waiting for a USB thumb drive to be installed

Once a USB thumb drive is inserted into a system its contents is automatically sent via an encrypted SMTP connection to a remote email account which is configured

USB Security Tools

MyUSBonly

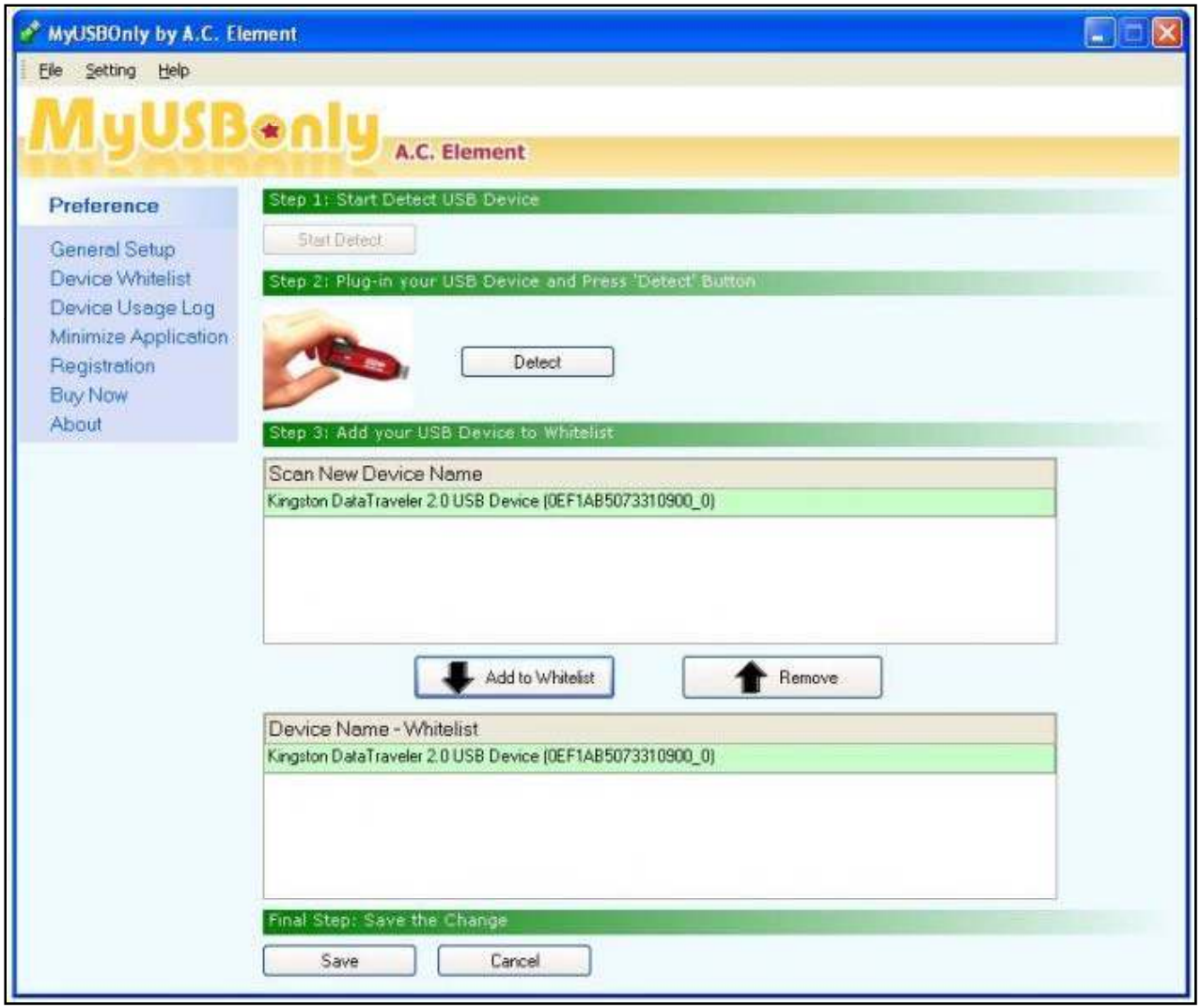
Prevents data theft by blocking all but your trusted USB storage devices

Stops files from walking away on thumb drives, mp3 players, flash cards, and portable USB hard drives

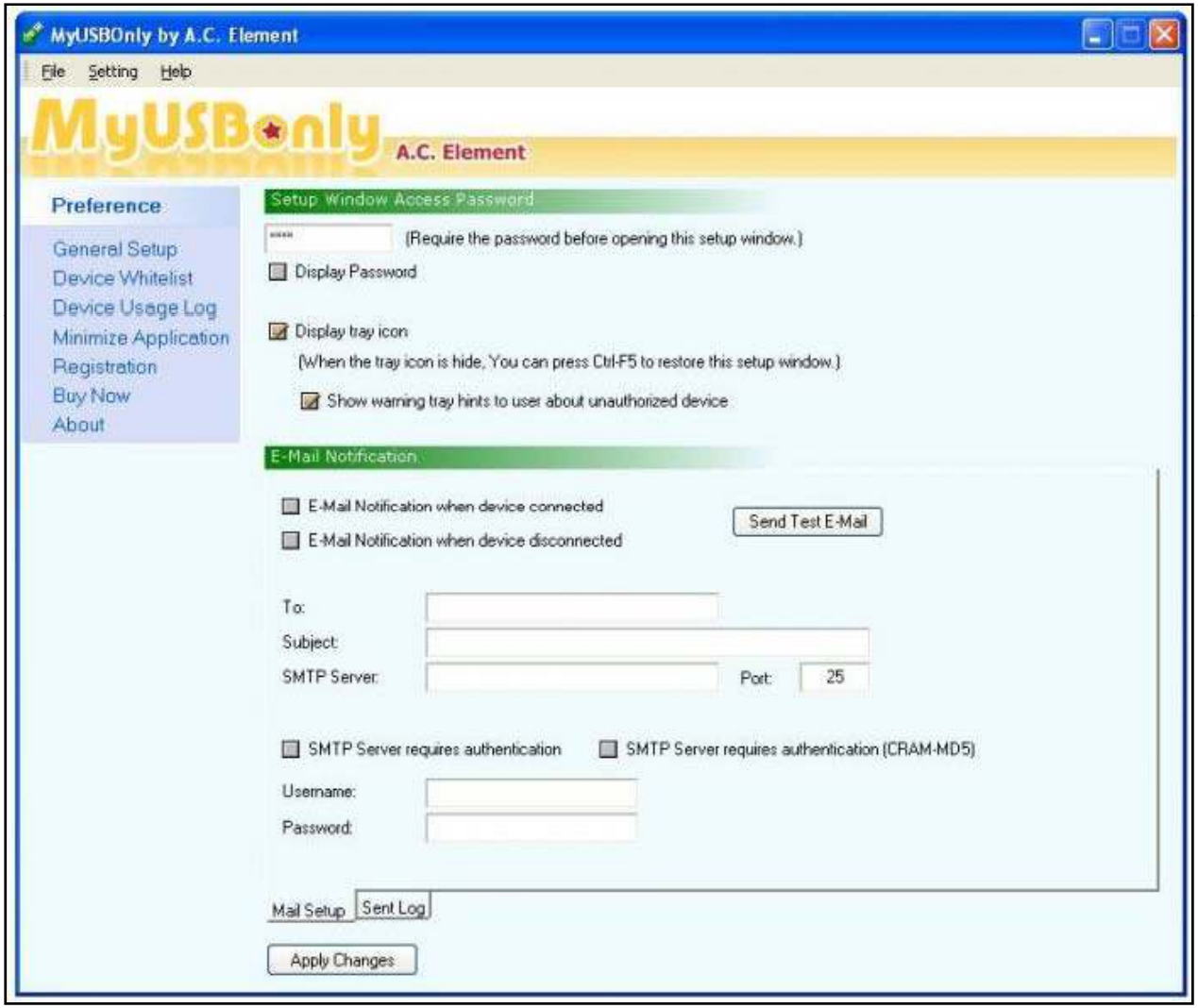
Secretly logs all USB connect and disconnect activity

Gives an email notification message when an unauthorized USB storage device is connected to your PC

MyUSBonly: Screenshot 1



MyUSBonly: Screenshot 2



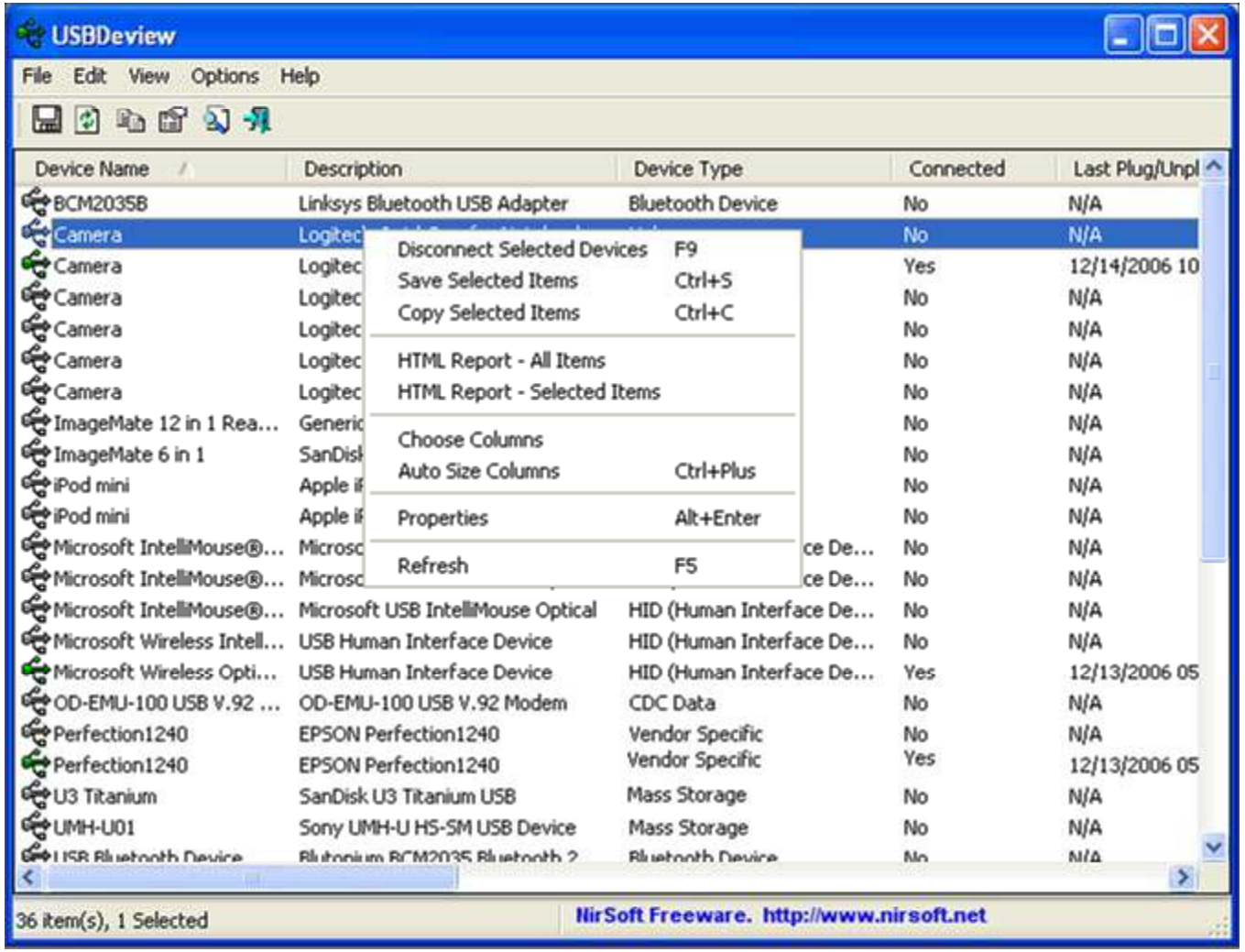
USBDeview

USBDeview is a small utility that lists all USB devices that are currently connected to your PC or have been connected to it in the past

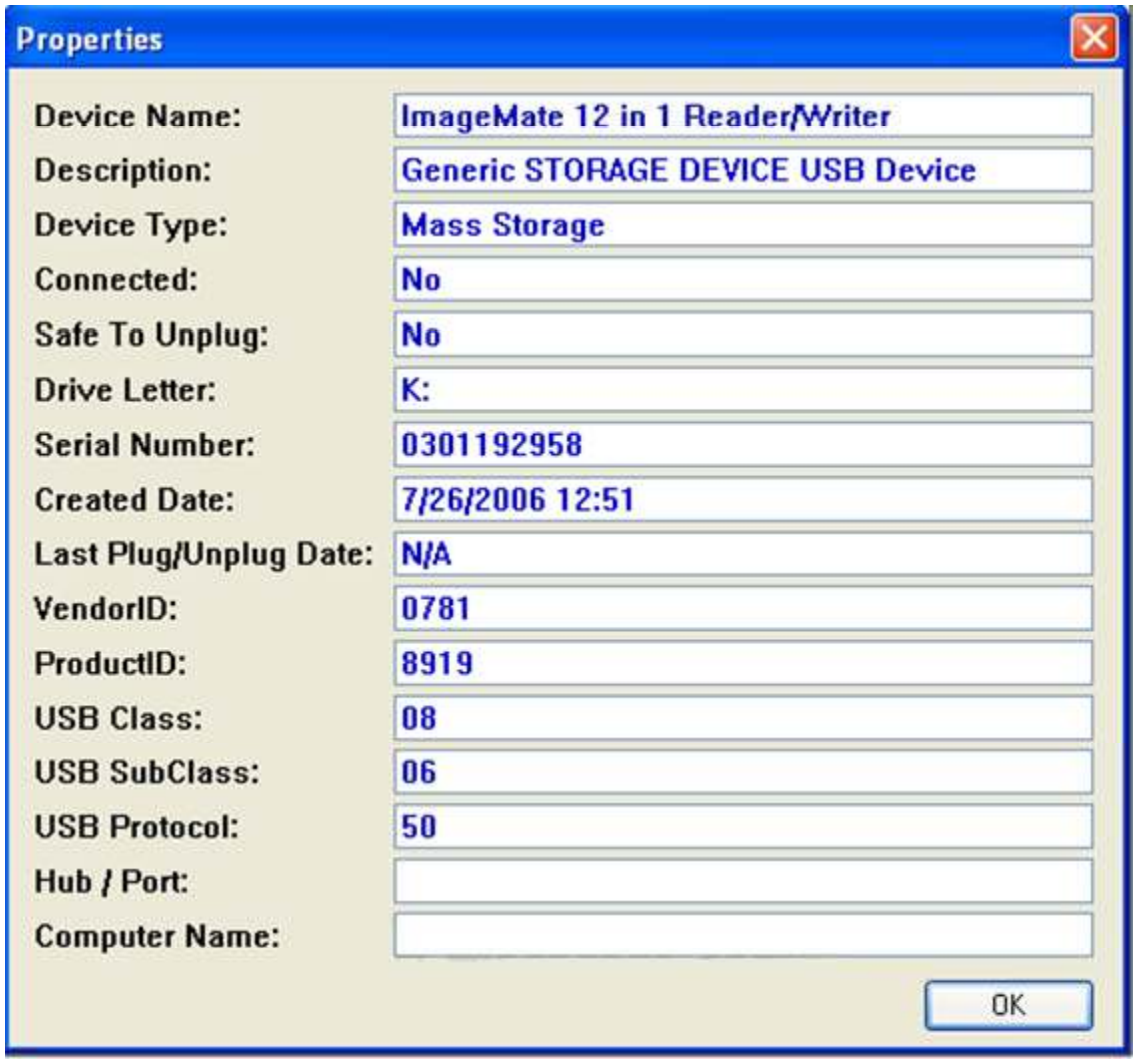
Along with the device name and description, it displays the serial number, date the device was added and last connected, VendorID, and other information

USBDeview can also be used to gather USB devices from a remote computer via command line

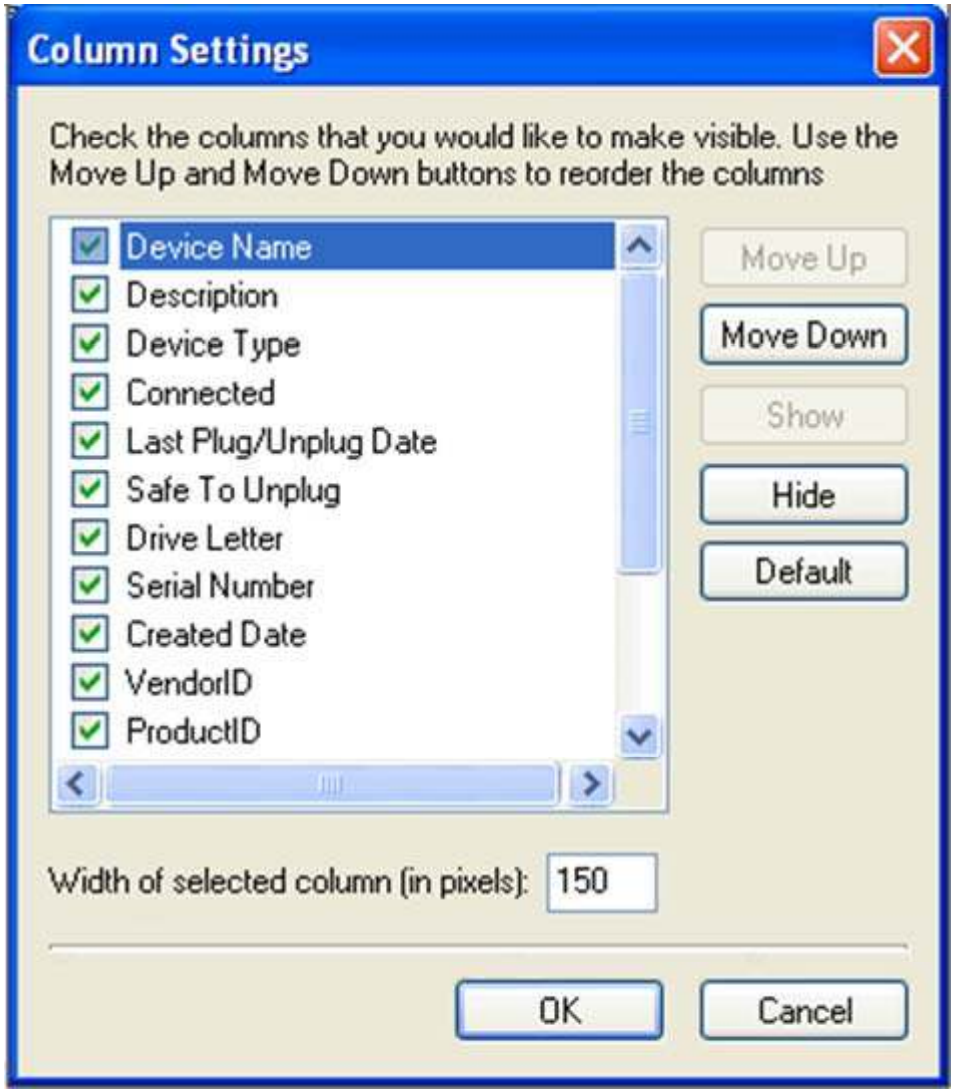
USBDeview: Screenshot 1



USBDeview: Screenshot 2



USBDeview: Screenshot 3



USB Blocker

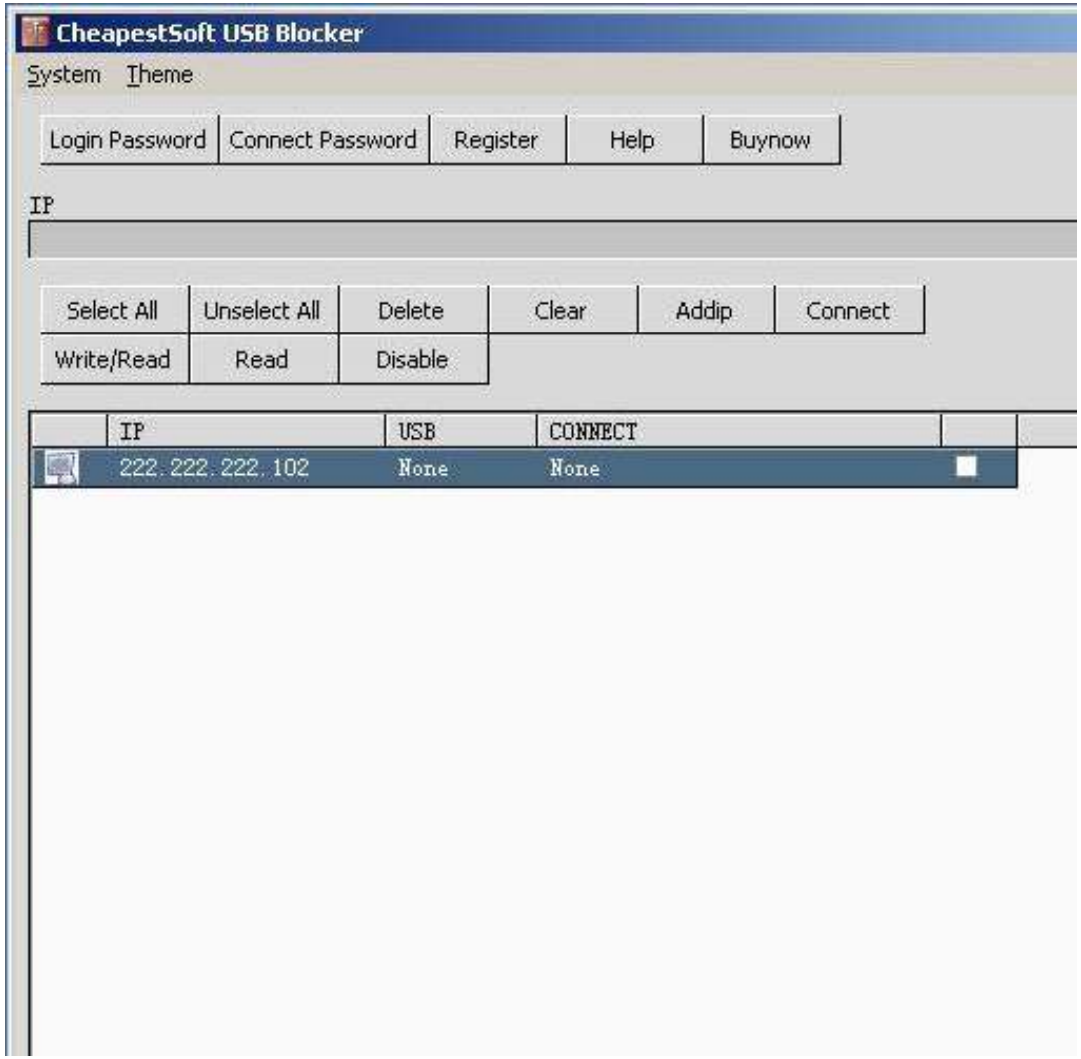
USB Blocker enforces centralized access control to prevent unauthorized use of removable media that connects to computer USB ports

Hardens endpoint security

Enables regulatory compliance, such as SOX, GLBA, and HIPAA

Seamlessly integrates with Active Directory

USB Blocker: Screenshot



USB CopyNotify

USB CopyNotify is a software utility that notifies when a USB Stick is being used on any of the PCs on the network

As soon as someone uses removable media such as a USB drive or an iPod, the sophisticated detection system of the software notifies the same

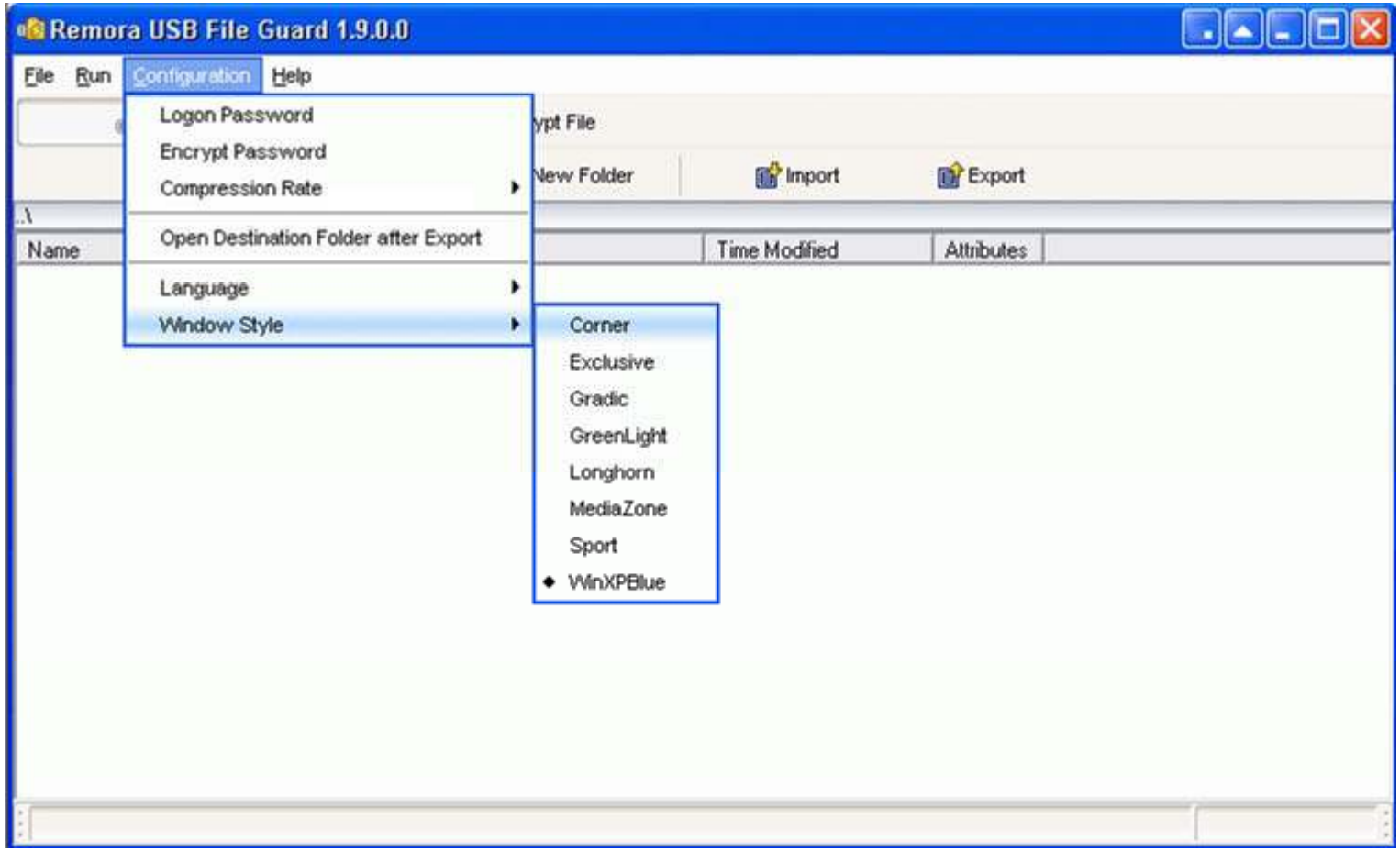
Remora USB File Guard

Remora USB File Guard is designed to do file encryption and compression in USB storage devices

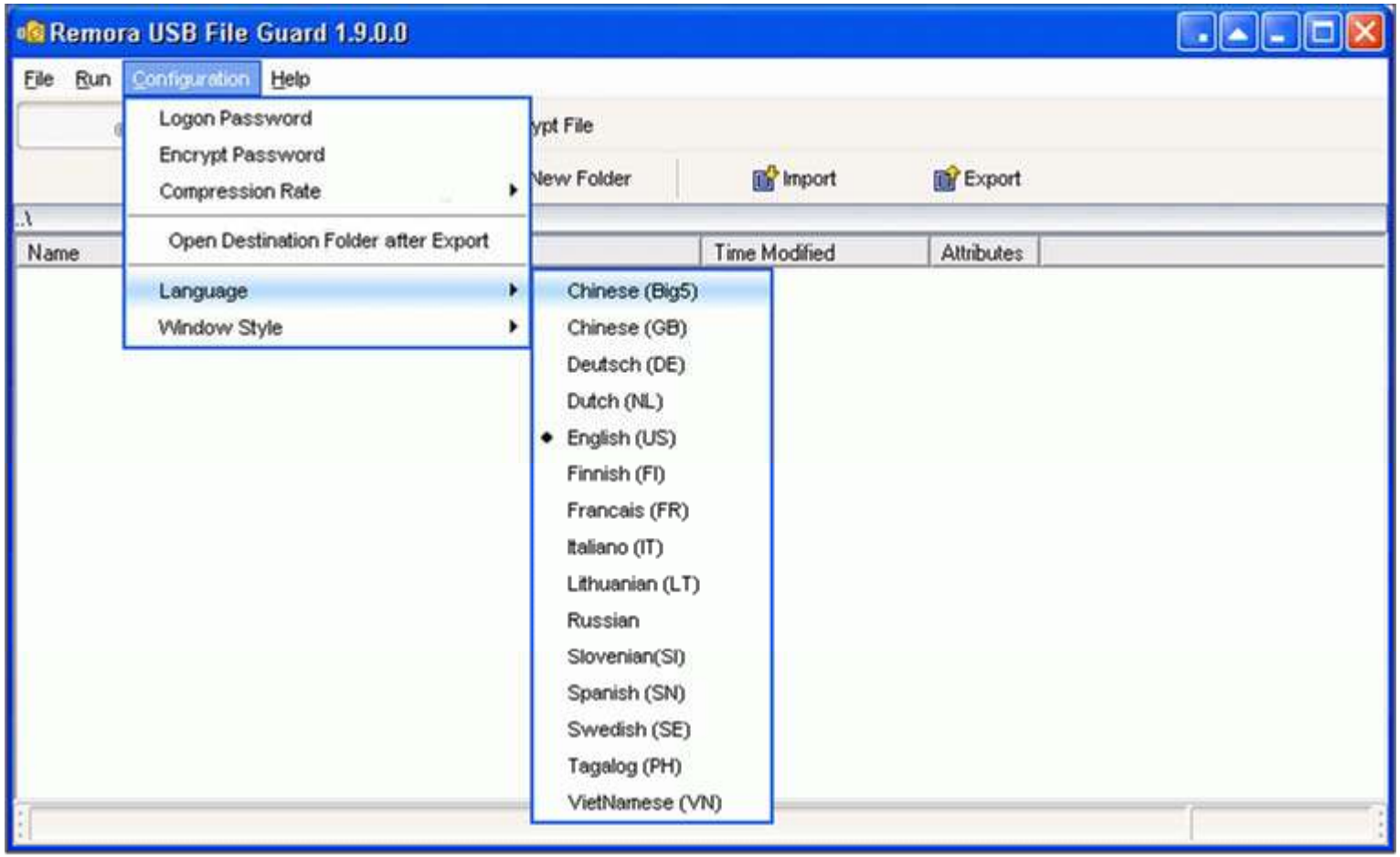
It can secure all files and store them in USB disk anytime and anywhere

Fast encryption and compression using strong 128 bits encryption technique, and at least a 50% compression rate to double storage capacity

Remora USB File Guard: Screenshot 1



Remora USB File Guard: Screenshot 2



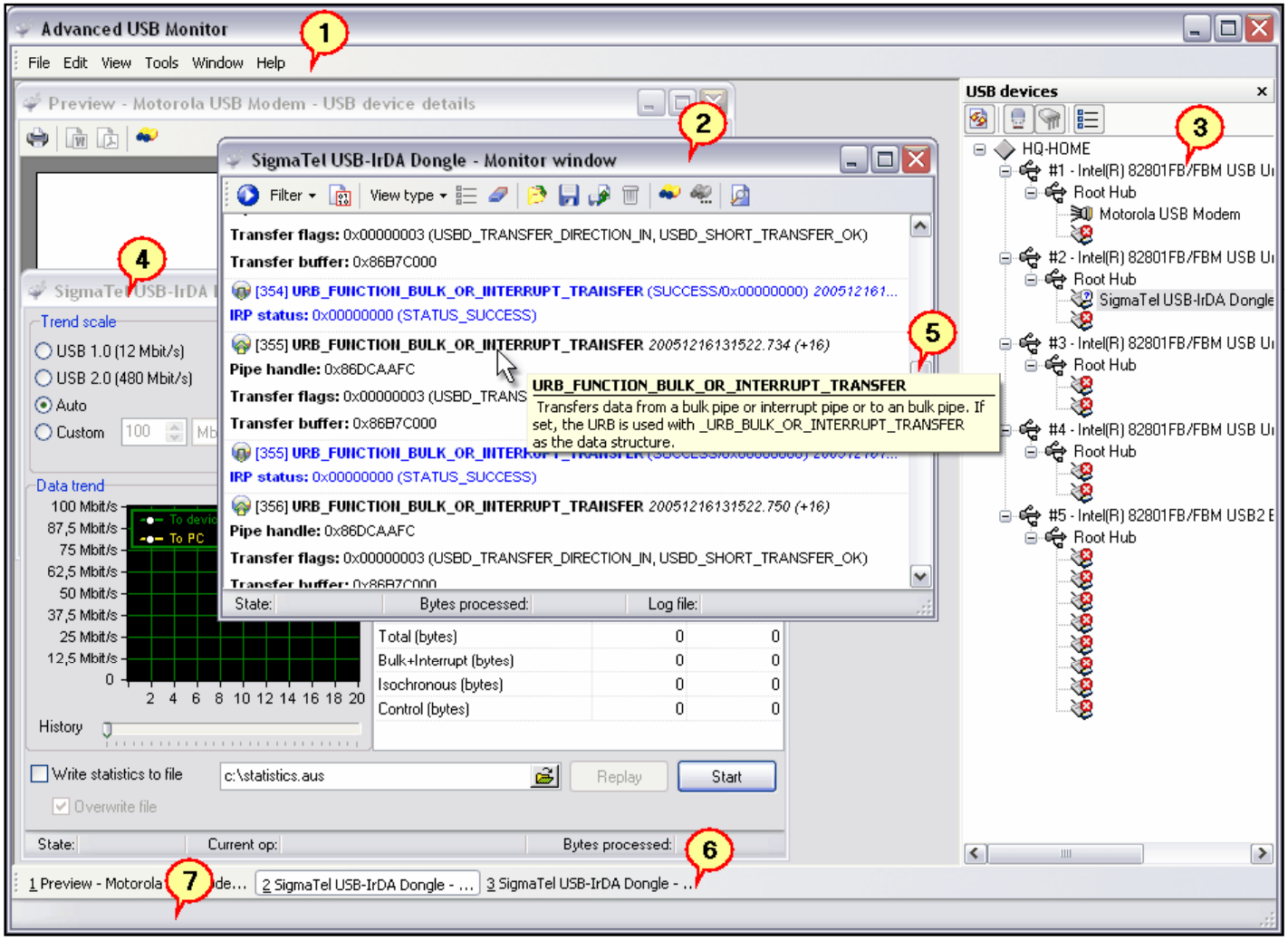
Advanced USB Port Monitor

Advanced USB Port Monitor is USB Bus, USB Device, and Protocol Analyzer

Advanced USB Port Monitor packs the robust functionality to capture, view, and process USB traffic

It offers sophisticated viewing and intelligent searching to accurately and efficiently debug and test High (480Mbps), Full (12Mbps), and Low (1.5Mbps) speed USB devices and software

Advanced USB Port Monitor: Screenshot



Folder Password Expert USB

Folder Password Expert USB is a security software designed to protect folders against unauthorized access to their contents

Install Folder Password Expert USB right on flash, USB external, or removable drive

No need to install the program on each computer

Folder Password Expert USB: Screenshot

USBlyzer

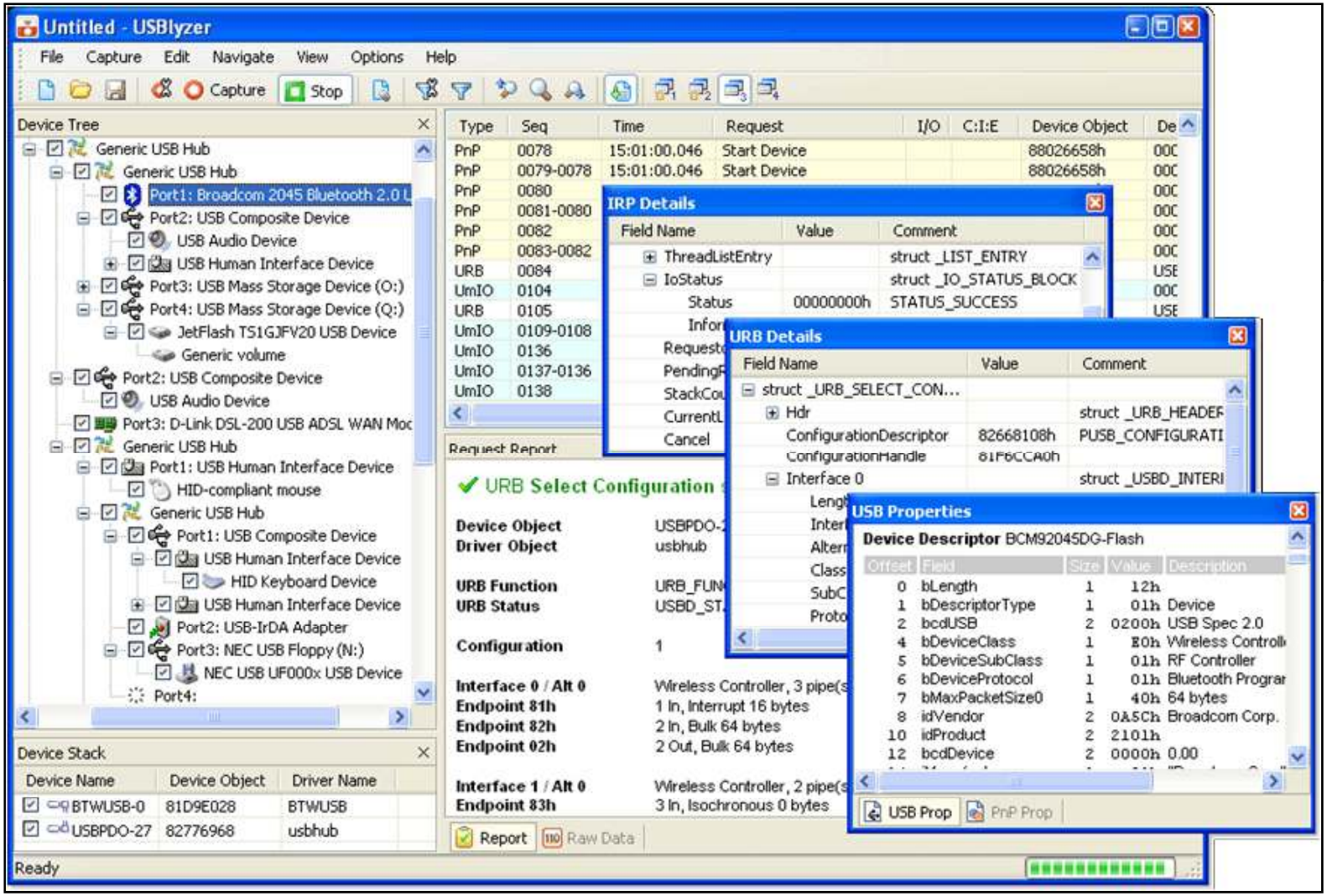
USBlyzer is an USB protocol analyzer for Windows

It provides a view for analyzing USB Host Controllers, USB Hubs, and USB Devices activity

USBlyzer can view detailed information about all USB devices and their child components

USBlyzer allows to capture, decode, and display important information going through USB device stack

USBlyzer: Screenshot



USB PC Lock Pro

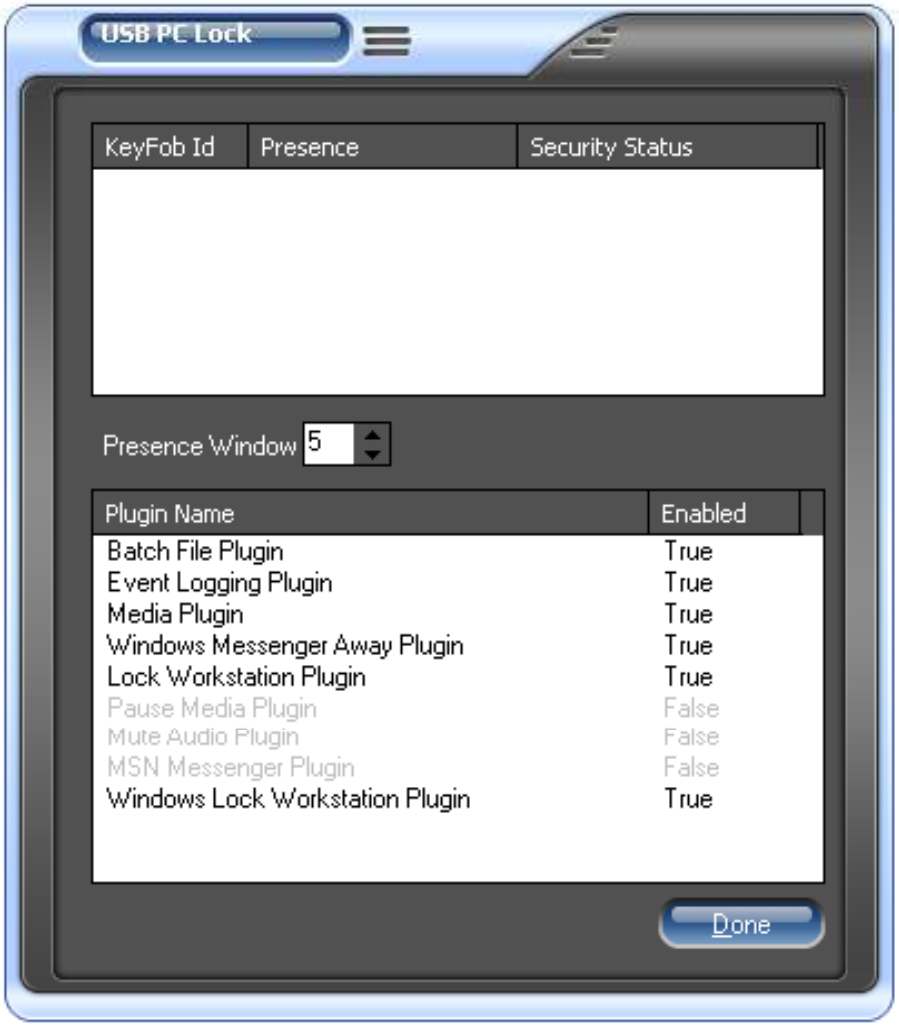
It turns any USB Flash Drive into a key that prevents unauthorized people from using computer

USB PC Lock will automatically lock your computer and perform other actions when you step away from it

Features:

- Locks workstation when you step away
- Locks MSN Messenger
- Stops streaming media traffic
- Mutes audio
- Starts or stops event logger

USB PC Lock Pro: Screenshot



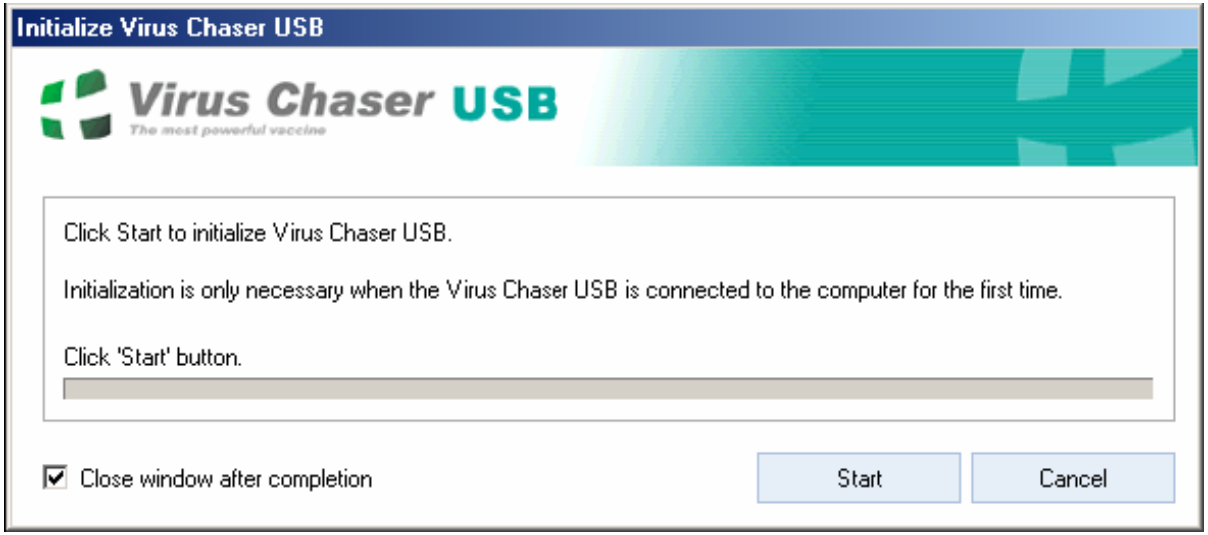
Virus Chaser USB

Virus Chaser USB supports Anti-Virus Vaccine software based on USB Flash Drive

It can scan, cure, delete, or monitor for virus infections of your computer

Features:

- Virus Scanning
- System Monitoring



Countermeasures

Conformal Coatings, such as epoxy, help protect critical components from probing and tampering

All functionality not used or needed in the production unit should be completely removed from the firmware

Scan the removable storage media by certain antivirus software whenever it is plugged into a computer

Disable autorun

Disable USB ports and CD-ROM's use on Windows using Group Policy

Summary

- USB (Universal Serial Bus) acts as an interface and add on device
- Primary goal was to attempt to access private data, which is supposed to be protected by legitimate user's PIN number or password without detection by the legitimate user
- Once the modified buffer is programmed back into the Serial, EEPROM attacker can login using the default PIN and make use of the legitimate user's credentials
- USB Dumper is an application up that when installed on a system will run a background process that will copy files from any USB flash drive installed to it silently
- USB Blocker enforces centralized access control to prevent unauthorized use of removable media that connects to computer USB ports

"I'm looking for some foreign language software that will teach me how to speak Encryption."

"Information security is a big deal at my office so sometimes we have to communicate in code. We have 37 different symbols for the word 'jerk'."