USB Malware Detection by Utilizing USB Usage Patterns

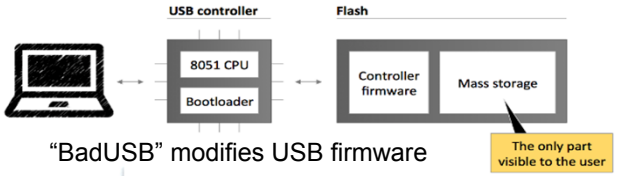
Hessam Mohammadmoradi and Omprakash Gnawali
Networked Systems Laboratory, Computer Science Department
University of Houston

Overview

- ✓ There are many devices which use USB port for communication and this popularity seems very interesting to hackers.
- ✓ Most of protection products need detailed specification of malware to be able to detect it.
- ✓ We analyze how students use USB devices in a school environment.
- ✓ We proposed effective approach to detect malware infected devices (90% accuracy) utilizing collected usage data.

"BadUSB"

- ✓ "BadUSB" is one of the most recent USB Malwares
- ✓ There is no effective solution against "BadUSB"
- ✓ Our approach can detect infected USB devices .



"BadUSB" modifies USB firmware

In Our Research

- ✓ We analyze how USB devices are used in an operational academic lab.
- ✓ Our results provide general insight about USB device's popularity and usage pattern.
- ✓ We analyzed USB malware behavior (propagation speed, final infected set) using on our collected data.
- ✓ We extracted reliable facts about USB devices that can be utilized by other researchers

Dataset

Collected Attributes

- ✓ Device Type: Based on USB class code there are different device types such as Mass Storage and Human Interface Devices.
- ✓ Serial Number
- ✓ Last Plug/UnPlug Time
- ✓ VendorID/ProductID
- ✓ USBClass/SubClass/Protocol
- ✓ IP and MAC Addresses
- ✓ UserID

Data Collection Process

- ✓ Lightweight Java Application
- ✓ Fetch Windows registry file (Windows keeps track of devices connected to USB ports in registry file)
- ✓ Extract information regarding devices connected to USB port
- ✓ Send information to central database over the Internet

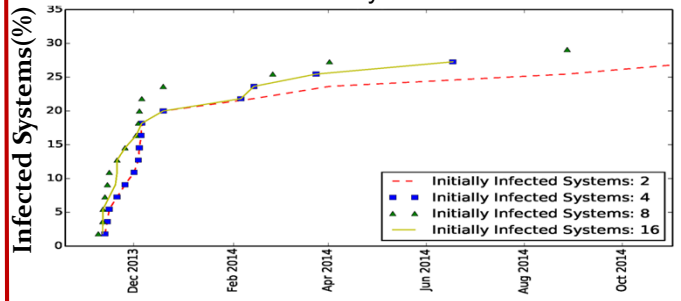
Summary of Dataset

- ✓ We monitored **57** desktop computers located in **2** academic labs
- ✓ Host operating systems were **Windows 7 & 8**
- ✓ Sampling rate was **1** sample per minute
- ✓ Monitoring process started by **November 2013** and ended by **December 2014**

Insights

Initial Infected Set Analysis

- ✓ Malware propagation speed considering different number of initial infected systems



- ✓ Early Propagation Stages: Propagation speed is independent of initial infected nodes
- ✓ Later Propagation Stages: Initial number of infected nodes increases speed of propagation and size of final infected set

"BadUSB" Detection

- ✓ Use collected properties as feature list
- ✓ Apply machine learning to classify USB devices
- ✓ Detect abnormal instances

USB Identification using Neural Networks

- ✓ **90.99** % Correctly Classified USBs
- ✓ **0.003** Mean Absolute Error
- ✓ **8122** Total Number of Instances

Outdated Drivers

- ✓ **75** % of Desktops with Windows 8 and **25**% of Windows 7 use **outdated** drivers

We would like to thank Tom Cumpain for logistics support.