

You Can do **THAT** With a **USB?** **USB Drive Hacking**

Al Maslowski-Yerges
Security Practice Manager
ayerges@novacoast.com

Who is Novacoast?

USB/Removable Media Types

A tool for the Diabolical.

USB “Switchblade” with U3 -
Setup/Configuration

The Attack

The Results

Methods for Protection

Protection with Endpoint Security solutions

Novacoast is an IT professional services and product development company. We offer organizations our technological experience so they can make informed decisions and avoid costly IT mistakes.

We combine our customers' expertise with our technical knowledge to rapidly deploy fixed cost solutions customized for their environment.



- Systems integrity
 - Security, identity management
- Data center solutions
 - Availability
- Productivity solutions
 - Resource management, training
- Product development
 - Voice RD, CASTOR, ZORRO
- Product fulfillment
 - Software acquisition

- **Some tools and programs used in this session may cause damage to computer systems. Test ONLY in lab environments and ALWAYS obtain written permission. Novacoast and it's employees are not responsible for any damage caused to computer systems nor for any loss or exposure of data as a result of any use of these tools or the information shared in this presentation.**

- The “Universal” in USB
- Typical types and functions

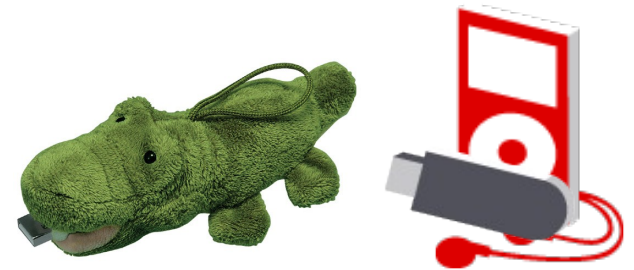


■ Ubiquitous

- Ports on every PC
- Sold in huge capacities almost everywhere

■ Easily hidden

- USB sushi anyone?
- Just my iPod



■ Steal Data

- Corporate secrets
- Passwords
- The bidding starts at \$2000.00 for “Mr. Smith”
- Account numbers

■ Gain Unauthorized Access

- Set up back-doors
- Steal/crack passwords



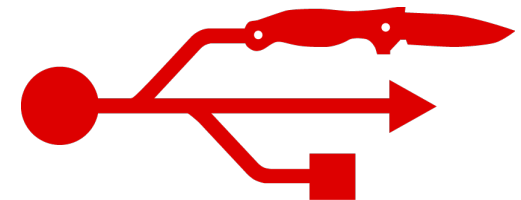
On to the Actual Tools

■ Collaborative Open Source

- The goal is to silently recover information from a target Windows 2000 or higher computer

■ Architectures/Methods used

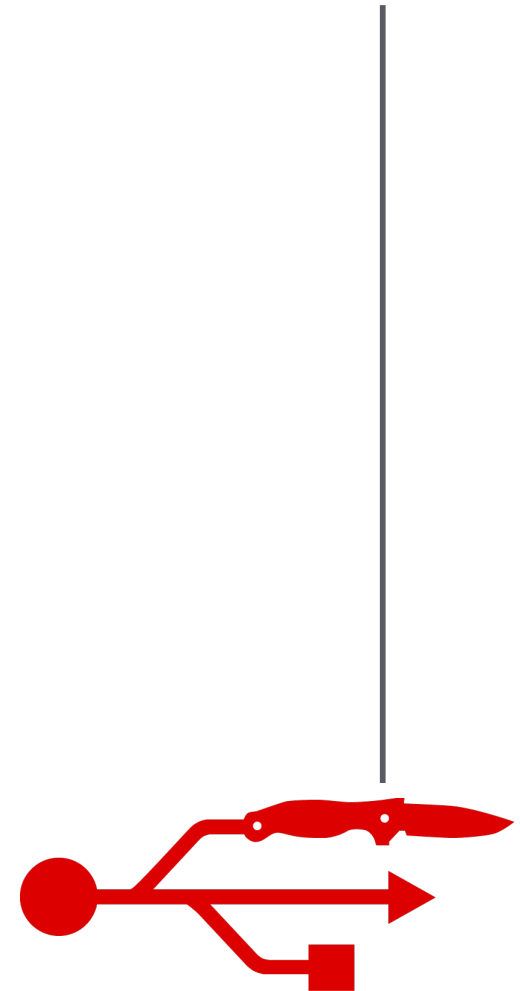
- Need autorun or social engineering
- Utilize classic hacker tools
- Avoid detection by AV etc...



USB “Switchblade”

■ U3 Method – most stealthy

- <http://www.u3.com>
- Virtual CD drive and storage



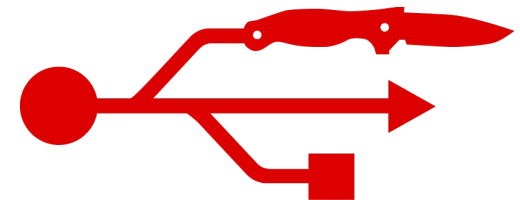
USB “Switchblade”



O-ISC '07
Ohio Information Security Conference

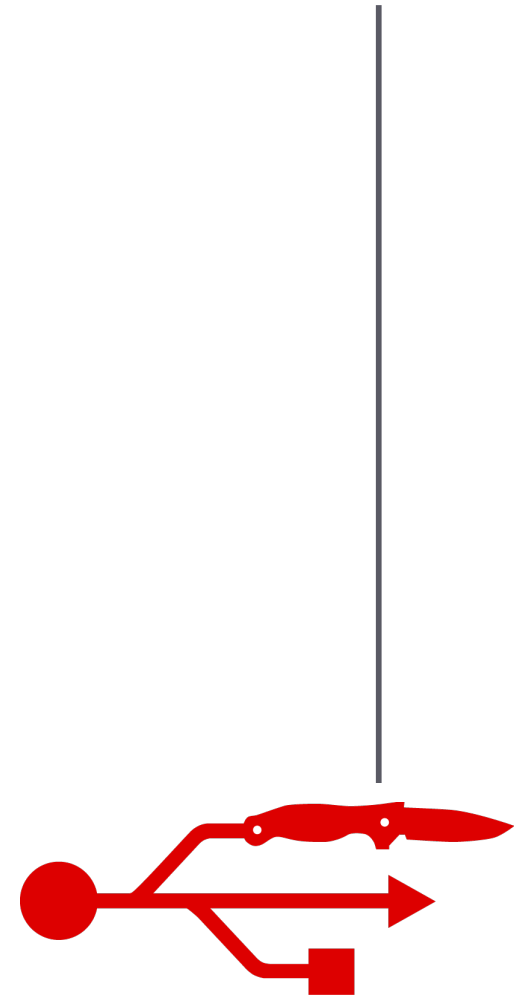
■ Making a “Switchblade”

- Obtain drive
 - SanDisk (<http://www.sandisk.com/>), Memorex (<http://www.memorex.com>)
- Download new ISO (CD image)
 - <http://www.hak5.org/releases/2x02/switchblade/>



USB “Switchblade”

- Replace standard U3 auto-run
- Edit scripts
- Recompile tools
- Duplicate
- Distribute



The Attack

■ Entice use

- “Lost” thumb drive
- Simulate “promotional video”
- Put in inter-office mail

■ Compromised at first insertion

- Passwords securely mailed to anonymous account
- AV processes killed
- Software license keys
- Remote control software
- Back-door
- and more ...





Demo of a USB Switchblade

The Result

- Remote compromise
- Internal Network Architecture
- Passwords
- Remote control
- Encrypted data channel

- POLP
- Egress Filtering
- Protection of critical binaries
- Lock down of USB ports

■ But what about...

- The boss' PC
- Keyboards, mice, printers
- Legitimate use of iPods, etc...



■ Endpoint Security Protection

- Intelligently block/monitor access according to policy and need

- Two products we like and deploy
 - Symantec Sygate Enterprise Protection
 - Secure Wave's Sanctuary
 - Others are entering this market as well



Summary

- Dangers
- Review switchblade attack
- Methods of protection
 - Defense-in-depth
- End-point protection from vendors



Questions & Answers