Bring Your Own Dilemma: OEM Laptops and Windows 10 Issues

Mark Loveless

Introduction

- Sr Security Researcher @ Duo Security
- aka Simple Nomad from the Interwebz
- Not selling a book or consulting services
- Known as a “soft sell” talk

DUO SECURITY

Platforms Examined

- Three inexpensive laptops from Best Buy
- One inexpensive laptop via mail order in Canada
- Three inexpensive laptops from London
- All running Windows 8.1 or 10

DUO SECURITY

Attack Scenario - Public Wifi

- Employee accesses work resources from personal laptop
- Coffee shop or hotel near important conference or business headquarters
- Airplane wifi in/out of large business center (NYC, DC, etc)

DUO SECURITY

Methodology Used

- Network-centric discovery, use a sniffer as primary tool
- Note use of networking protocols, including insecure configurations
- Note privacy issues
- Document oddities such as strange server connections
- What is done correctly?

DUO SECURITY

Boring Stuff - What is Done Right

- Tries to patch itself out of the box
- OEM bloatware has updaters, so in theory they can patch
- Most privacy-related data appears to be encrypted during network transmission

DUO SECURITY

Hijackable/Leaky/ Predictable Protocols

- Link-local in general
- WPAD
- LLMNR
- Smart Multi-Homed Name Resolution
- Teredo tunneling
- ISATAP

DUO SECURITY

Fingerprinting

- Open ports
- OS and laptop brand identification via Microsoft and OEM vendor server access
- No OEM laptop user surfing, idle machine gives it up

DUO SECURITY

Determining Patch Levels

- Windows Update is in plaintext
- All data is signed, but determining patch level is possible

DUO SECURITY

OEM-Specific Issues

- The eDellRoot issue (google "duo edellroot")
- OEM bloatware does a lot of plaintext traffic
  - Unsigned manifests and binary updates
- Numerous security issues found in updaters alone (co-workers found numerous CVE-able issues)

DUO SECURITY

Tags aka Web Bugs

- What tags are
- Used by Microsoft for ads in tiles
- Used by McAfee to gather platform data via forged Refered-By headers
- All tags done without user surfing, just idle machines

DUO SECURITY

Privacy Issues

- Lots of privacy-related traffic back to Microsoft servers, some traffic occurs even if all privacy settings are off
- After a Cumulative Update in Nov 2015, some privacy settings reverted back to "on"
- Signing up for live.com account results in HUGE amounts of traffic back to Microsoft servers
- All OEM vendors gathered data
- Data gathering starts from first boot before desktop is reached

DUO SECURITY

Mitigation

- Delete McAfee and use Windows Defender (nearly as good, perfect for home users)
- Tweaks to firewall
- Turn shitty protocols off
- Turn bothersome privacy settings off
- Involves registry tweaks because GUIs don't solve everything

DUO SECURITY

Proof

- Fire up a sniffer…

DUO SECURITY

Questions

- duo.sc/BringYourOwnDilemma
- mloveless@duo.com
- @simplenomad

DUO SECURITY