We have you by the gadgets

Hitting your OS below the belt
Legal Notice

Our opinion is our own. It **DOES NOT IN ANY WAY** represent the view of our employers.
whoami - Toby
whoami - Mickey
Agenda

• Who we are
• What are Gadgets
  o A little bit of history
  o Why this matters
  o How to develop gadgets
  o Gadget security model
• What's wrong with them
• Attack Surface
• Problems found
• Demos
• What do you do about it?
Thank you:
Itzik Kotler, FX, Ian Amit, Jayson Street, SophSec, Wim Remes, Aviv Raff, Gal Diskin
#include <full_list.h>
What are Gadgets

• Little applications that run on your Windows desktop
• For instance:
A little bit of history

- **Windows XP** - Concept first introduced as "Active Desktop"
  - Allowed you to put updating content on your desktop.
- **Vista** - Sidebar introduced, first mention of "gadgets"
  - Gadgets ran in the sidebar "container" couldn't be placed randomly on the desktop
- **Windows 7** - significant changes
  - Improvements in management:
    - Gadgets now can be anywhere on the desktop
    - All gadgets run in a single process
  - Addition of the enterprise security features
  - Also - New stuff to help in development
Why this still matters

- Gadget use is in decline
- But! This style of app development is taking off
  - Container-based apps for smartphones that allow you to do all your dev in HTML, XML, Javascript, etc…
Windows Vista Sidebar
Windows 7 Gadgets
Creating Gadgets

• Just a zip file
Creating Gadgets

• Usually just a web app
  o html
  o css
  o javascript
  o gadget specific manifest file

• Can also be WPF or Silverlight
Gadget Security Model

MSFT provides a detailed explanation
  - (see references)

• Code signing is possible but not required
• Prompt for install similar to standard applications:
Gadget Security Model

• Most similar to HTA - HTML Applications
• Basically run in "Local Machine Zone" with some differences:
  o Can instantiate any installed ActiveX object
  o UAC
    ▪ Runs as standard user even if the user is part of the admin group
    ▪ Can't raise UAC prompts BUT! apps launched by a gadget can
• Parental Controls apply
Gadget Security Model

- Some enterprise controls available
  - Turn off Windows Sidebar.
  - This policy allows administrators to completely disable the Windows Sidebar.
  - Disable unpacking and installation of gadgets that are not digitally signed.
    - Only affects gadgets that are downloaded and installed by double-clicking on the gadget package. All previously installed gadgets, as well as those installed manually, will still function.
  - Turn off user-installed gadgets.
  - Override the "Get more gadgets online" link.
Attack Surface

• Attacking **with** gadgets
• Attacking gadgets
Attacking **with** gadgets

- Delivery:
  - Install this gadget? Sure!
- Sidebar gadgets aren't perceived as being dangerous software or even software at all.
Attacking **with** gadgets

- So I installed your gadget, so what?
- I can't do much, just this:
  - Execute code
    - Game over
- Also:
  - Open URLs
  - Create files with arbitrary content
  - Read files
  - Make your computer speak
Attacking **with** gadgets

- Demo time
Attacking Gadgets

• Gadgets are code. Therefore gadgets are vulnerable

• Step 1 - Search for gadgets
• Step 2 - Analyze
• Step 3 - ...
• Step 4 - Profit (and share the findings)
Attacking Gadgets

- LOTS of malware claiming to be gadgets
- Minimal use of SSL
- Lots of ad server connections (no ads displayed)
  - And domain parking sites
- A couple primary producers, shared code between gadgets
  - If you find something in one, it's probably in the others
Attacking Gadgets

• Poor security practices, easy targets
  o Multiple ways to inject code
  o Default Permissions is "full"

• Traffic sniffing

• Easy to spot
  o (x64)
Attacking Gadgets – Traffic Sniffing

- SSL is haaaaaard
- All downloaded gadgets pulled most of their content w/o SSL
- Including updated gadget code in some cases
Attacking Gadgets - MitM

- There are not many gadgets out there, capturing their requests is simple. (AirPwn)
- Using a custom simple proxy to automate injection.
- Demo
Attacking Gadgets – Code Injection

• Any web scripting language
  o Or powershell

• Demo
What to do about it?

• Code is code
  o Remember not to take candy from strangers
• Write applications properly
• Microsoft’s solution
Microsoft Solution

• Security Advisory 2719662
  • “Microsoft is aware of vulnerabilities in insecure Gadgets affecting the Windows Sidebar on supported versions of Windows Vista and Windows 7”

• Fix It Solution
  • Engineering solution that removes the attack vector.

• Moving away from the Windows Sidebar and towards the Windows Store.
  • Deprecated the Windows Gadget Gallery
  • Updated developer documentation
Prior Work

Standing on the shoulders of giants

• CVEs
  o CVE 2007-3032
  o CVE 2007-3033
  o CVE 2007-3891

• Presentations
  o The Inherent Insecurity of Widgets and Gadgets - Aviv Raff, Ian Amit
  o Jinx - Malware 2.0 - Itzik Kotler, Jonathan Rom
References

- Gadget Security Model

- Writing Secure Gadgets