Mobile Device Security and Ethical Hacking

Mobile Application Penetration Testing

Windows Phone 8

Wouter Veugelen

Mobile Application Security

- Background
  - Mobile operating systems
  - Microsoft operating systems
    - Windows 8, Windows RT, Windows Phone
- Windows Phone 8
  - Application Penetration Testing
    - XAP file format, sideloading, decompiling, configuring a web application proxy
  - Mobile Device Security Testing
    - Jailbreaking, File system analysis, network vulnerability assessment
- Future work
- Resources and further references

Background

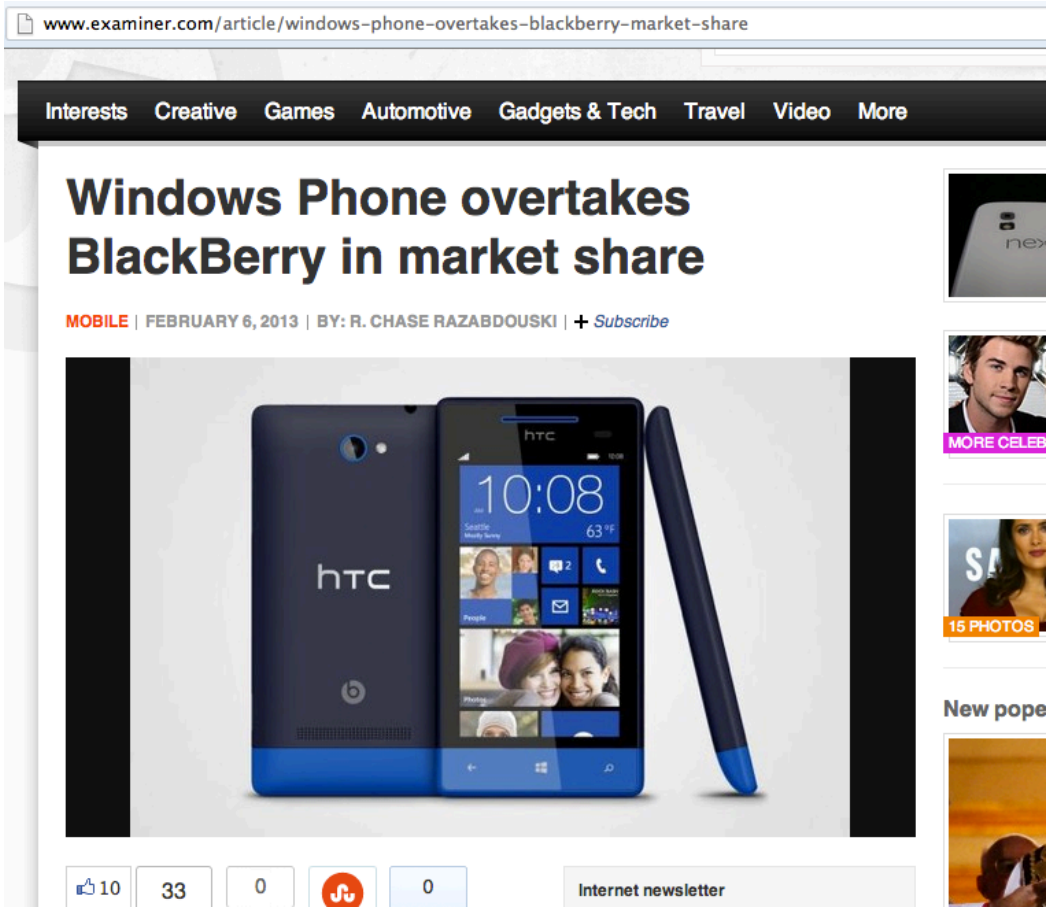
Mobile operating systems

Top Smartphone Operating Systems, Forecast Market Share and CAGR, 2012–2016

Smartphone OS	2012 Market Share	2016 Market Share	CAGR 2012 - 2016 (%)
Android	68.3%	63.8%	16.3%
iOS	18.8%	19.1%	18.8%
BlackBerry OS	4.7%	4.1%	14.6%
Windows Phone	2.6%	11.4%	71.3%
Linux	2.0%	1.5%	10.5%
Others	3.6%	0.1%	-100.0%
Total	**100.0%**	**100.0%**	**18.3%**

Source: IDC Worldwide Mobile Phone Tracker, December 3, 2012

Mobile operating systems



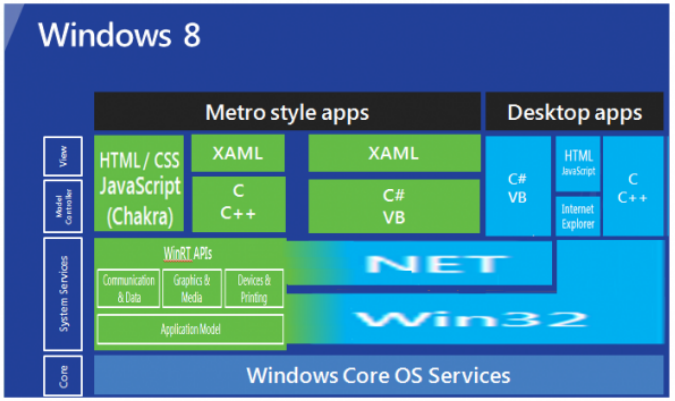
Microsoft's current OS portfolio

- Windows 8
- Windows RT
- Windows Phone 8

	Hardware Architecture	Applications Architecture	OS Kernel
Windows 8	x86/x64	Win32/WinRT	Windows NT
Windows RT	ARM	WinRT	Windows NT
Windows Phone 7	ARM	Silverlight / XNA	Windows CE
Windows Phone 8	ARM	Windows Phone RT	Windows NT

Windows 8

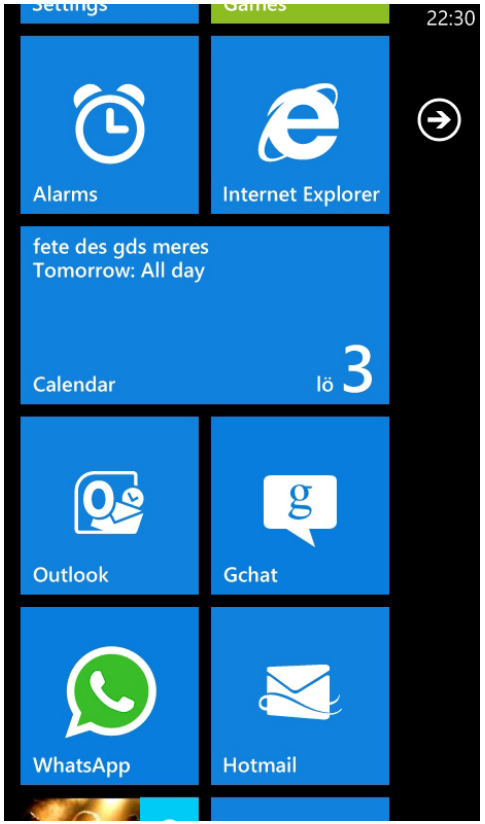
- x86/x64 CPU compatible hardware hardware
- Win32 and WinRT application architecture
- Key OS security features:
  - ASLR (Address Space Layout Randomization)
  - DEP (Data Execution Prevention)
  - SMEP (Supervisor Mode Execution Protection)
  - Secure boot (UEF)
  - ELAM (Early Launch Anti-Malware)
  - Bitlocker
  - Application sandboxing
  - …



Windows Phone

- 'Rebranded' Windows Mobile:
  - Up to v6.x: Windows Mobile
  - V7.x+: Windows Phone
- ARM hardware architecture (similar to iOS, Blackberry OS and Android)
- Windows Phone Runtime application architecture (not identical to WinRT)
- Windows Phone 7: Windows CE kernel
- Windows Phone 8: Windows NT kernel

Windows Phone 7



- Windows CE kernel based
- First mobile MS OS with 'Metro' interface
- No device encryption
- Only Microsoft and Marketplace apps have digital signatures
- Apps require either a Silverlight or XNA runtime; Susceptible to reverse-engineering and manipulation
- Marketspace for Homebrew: DevStore8

Windows Phone 8

- NT Kernel based
  - NTFS support
  - Device encryption (BitLocker)
  - Sandboxed apps
  - SafeBoot: Secure EUFI Boot (Unified Extensible Firmware Interface). UEFI = Successor to the legacy BIOS firmware interface
    - Makes it difficult for software without correct digital signature to be loaded on your Windows Phone
    - TPM 2.0 standard, requires unique keys to be burned into the chip during production
  - All Windows Phone 8 binaries must have digital signatures by Mircrosoft to run

Windows Phone: Application Penetration Testing

Prerequisites

- When using a physical phone: unlocked phone is required
- Application logic and server side can be tested with an intercepting proxy (e.g. Burp) without unlocked phone, but local storage and local application configuration settings cannot.
- Unlocking phone:
  - Using a developer account and developer unlock: 99$/year. Developer can install up to 10 sideloaded applications
  - Students: can install up to 3 sideloaded apps
  - Register a company trusted certificate for enterprise app stores: $399 / year

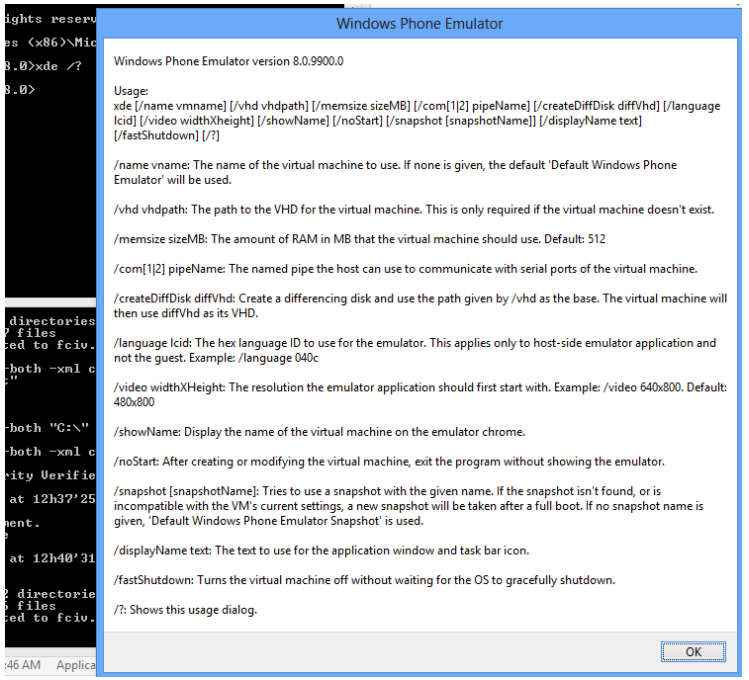
Prerequisites

- Windows Phone SDK install:

http://dev.windowsphone.com/

- Emulator is installed as part of SDK. Emulator is installed at the following location:

C:\program files (x86)\
Microsoft XDE\8.0\XDE.exe



- Visual Studio Express 2012 (free) or Visual Studio 2012

Prerequisites

- Windows Phone Power Tools - http://wptools.codeplex.com/
- ILSpy - http://ilspy.net/
- Tangerine - https://github.com/andreycha/tangerine

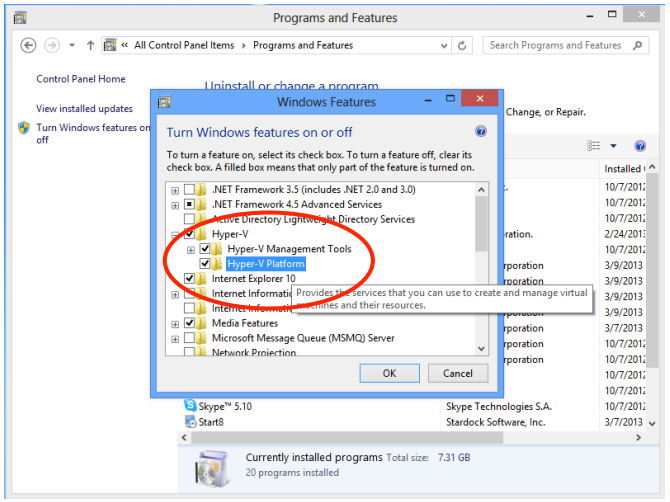
Commercial alternatives:

  - XAML Spy - http://xamlspy.com/
  - .NET Reflector - http://www.reflector.net/

Prerequisites

- Windows Phone 8 emulators are Hyper-V virtual machines having their own IP address.
- When using an emulator for testing, system with ore i3, i5 or i7 or equivalent AMD processor supporting newer hardware virtualization features is required.

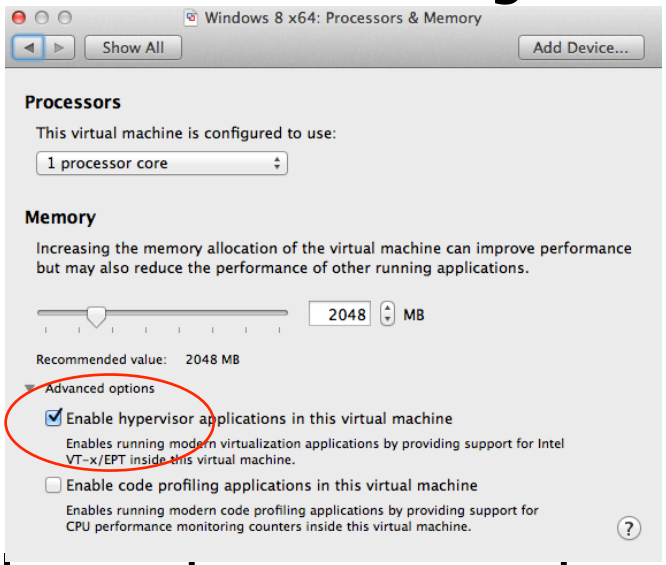
Check that Hyper-V is enabled in Windows:

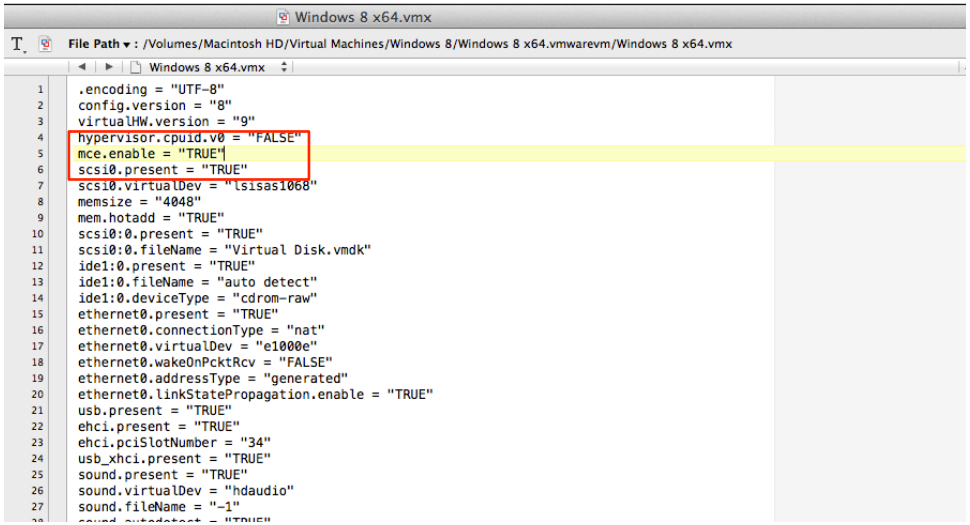


Prerequisites

When using vmware:

- enable the VT-x/EPT hypervisor option
- Add the following line to your vmx file, if not already there

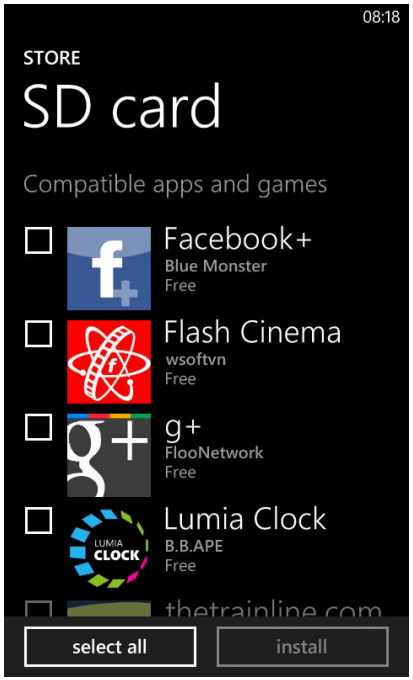




Also make sure your hypervisor settings in your BIOS are enabled.

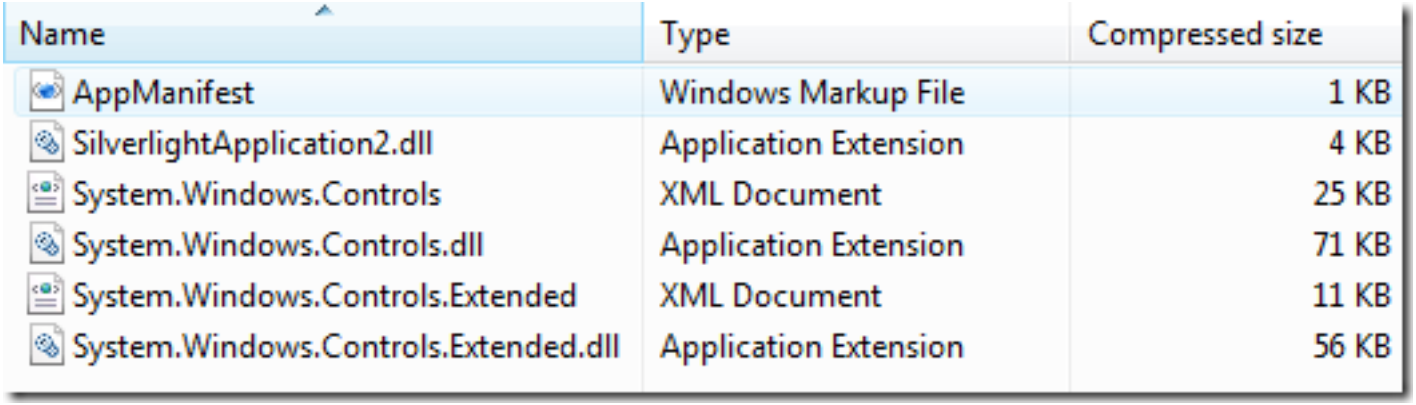
Sideloading apps

- Sideloading: installing applications on your device without using the official Marketplace directly
- Windows Phone 8 only allows apps downloaded through the Windows Phone Store by default
- XAP applications can be download from the store or provided by the developer and sideloaded via MicroSD storage card
- Limitation:
  - Only apps signed with trusted certificates will run (on unlocked phones)
  - Phone will validate that the app on the storage card is the latest release



Windows Phone: XAP files

- ZIP file formatted packages (similar to Android APK)
  - AppManifest.xaml file: defines the assemblies that get deployed in the client application. Updated when compiling your application
  - DLLs required
- MIME type: application/x-silverlight-app



Name	Type	Compressed size
AppManifest	Windows Markup File	1 KB
SilverlightApplication2.dll	Application Extension	4 KB
System.Windows.Controls	XML Document	25 KB
System.Windows.Controls.dll	Application Extension	71 KB
System.Windows.Controls.Extended	XML Document	11 KB
System.Windows.Controls.Extended.dll	Application Extension	56 KB

Windows Phone: XAP files

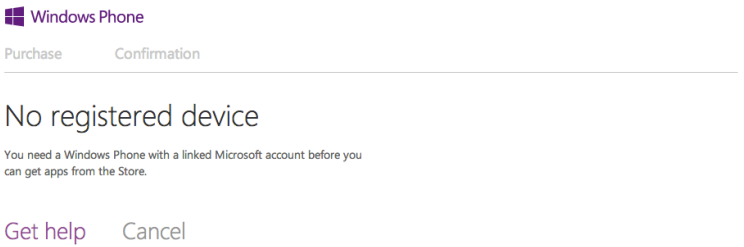
- XAP Files from app store: PlayReady DRM encrypted

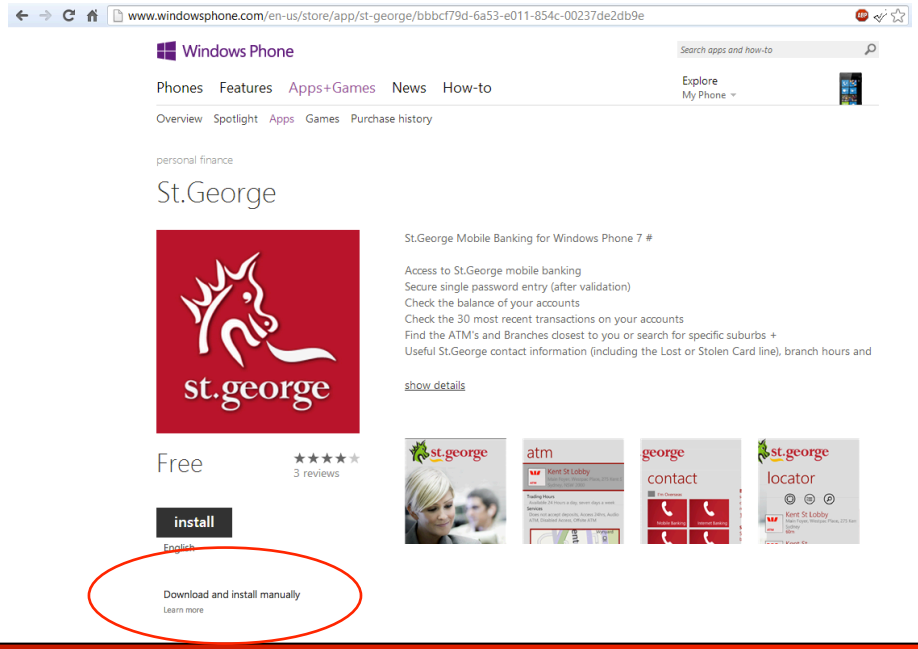
```
PlayReady DRM header:
<WRMHEADER xmlns="http://schemas.microsoft.com/DRM/2007/03/PlayReadyHeader"
version="4.0.0.0">

<DATA><PROTECTINFO><KEYLEN>16</KEYLEN><ALGID>AESCTR</ALGID></
PROTECTINFO><KID>w3i0edJP7EOqQ6aQzdAoSQ==</KID><LA_URL>http://microsoft.com/</
LA_URL><CUSTOMATTRIBUTES xmlns=""><S>9FcV5qmfIsMc+X2MVmX3Hw==</S><KGV>0</
KGV></CUSTOMATTRIBUTES><CHECKSUM>Hu3+fizBvKU=</CHECKSUM></DATA>

</WRMHEADER>
```

- DRM is added by the marketplace in real time, based on the LiveID cookie value
- Encrypted XAP files do not run in emulator!

Windows Phone: XAP files

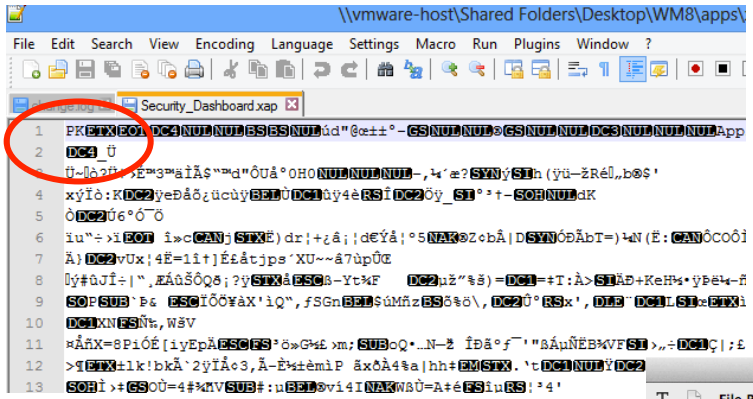
- XAP application binaries can be downloaded from Windows Phone Store from a computer
- Windows Live account required with Windows Mobile linked device





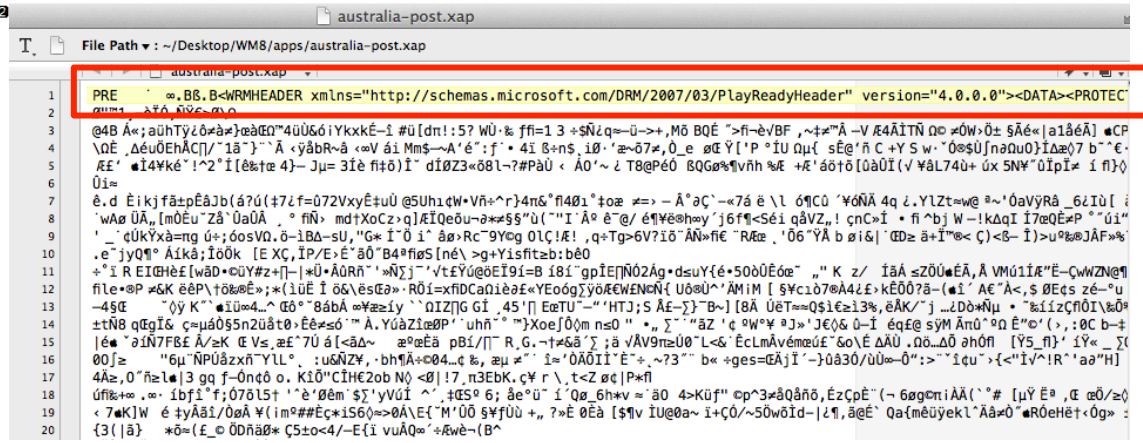
Windows Phone: XAP files

- How to recognise difference?



Not encrypted: PK (ZIP) header

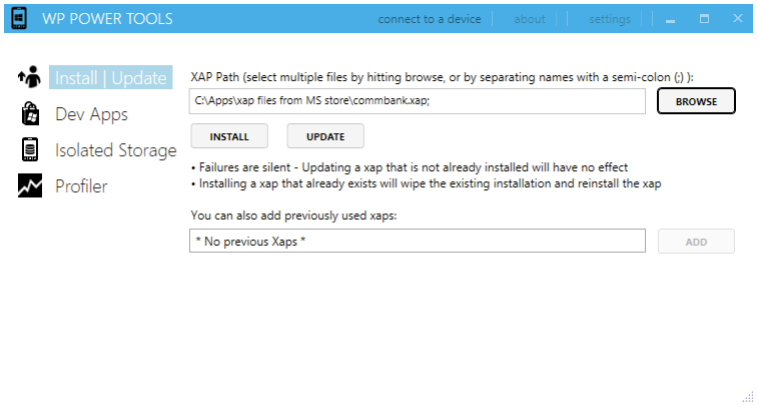
Encrypted: PlayDRM header

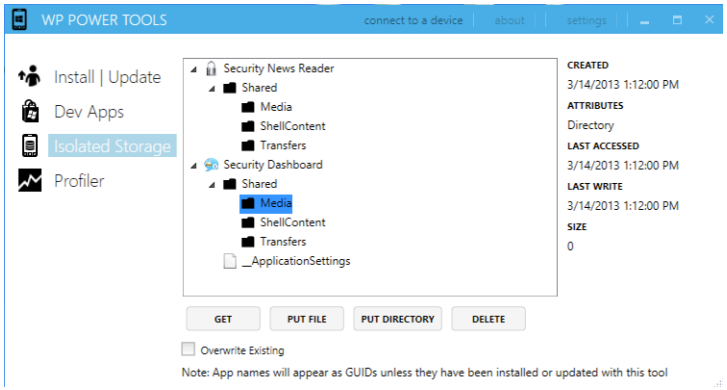


Windows Phone Power Tools

Great tool that can be used to:

- Deploy XAP files
- Inspect device storage on a physical device or on an emulator



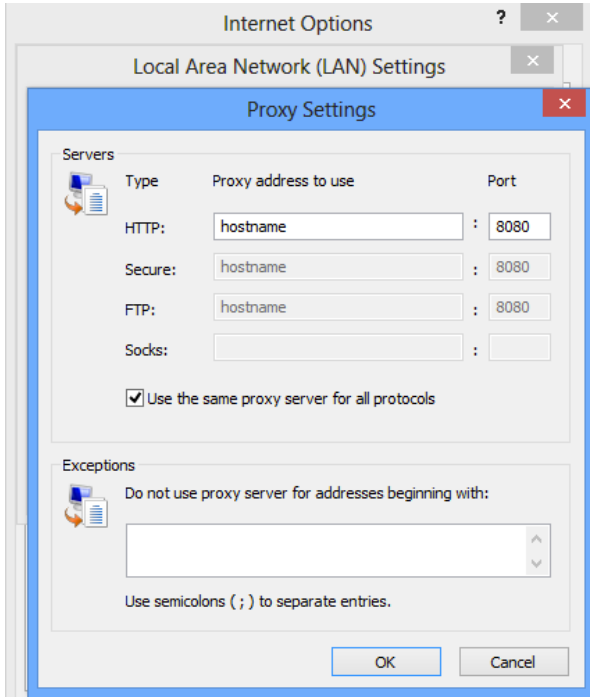


Setting up your proxy server

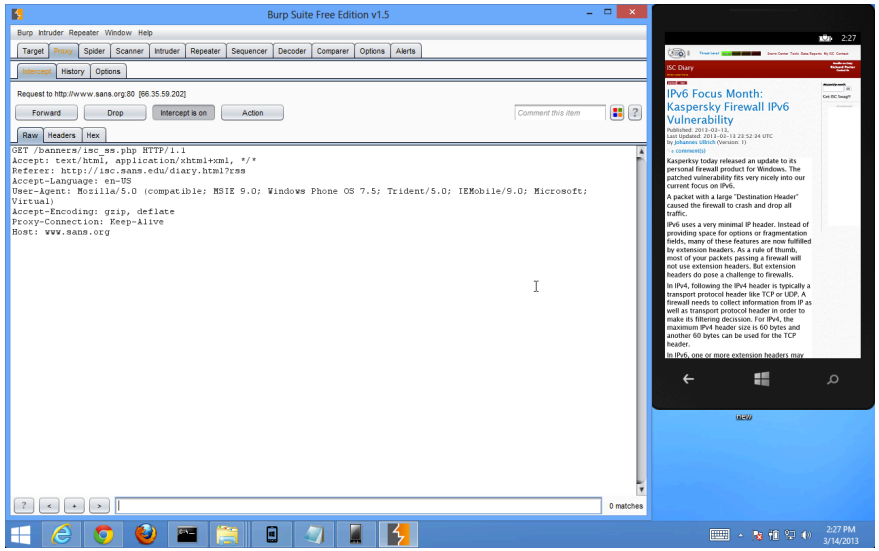
- Windows Phone 8 emulators are Hyper-V virtual machines having their own IP address.
- Network traffic needs to route from the Hyper-V virtual machines through the Hyper-V host (i.e. our test machine)
- As a result, we need to:
  - Make sure your proxy software is configured to **not** only listen on the local interface
  - Configure your IE proxy settings to proxy through your **HOSTNAME**, not 127.0.0.1 or LOCALHOST!

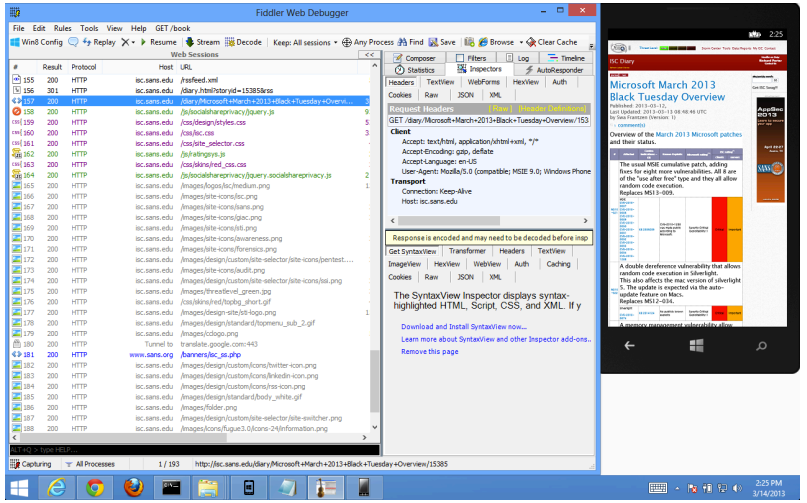
Setting up your proxy server

- Change the proxy settings in Internet Explorer to your system HOSTNAME
- Restart your emulator (Each time you change your proxy settings you will need to restart the emulator)



Demo

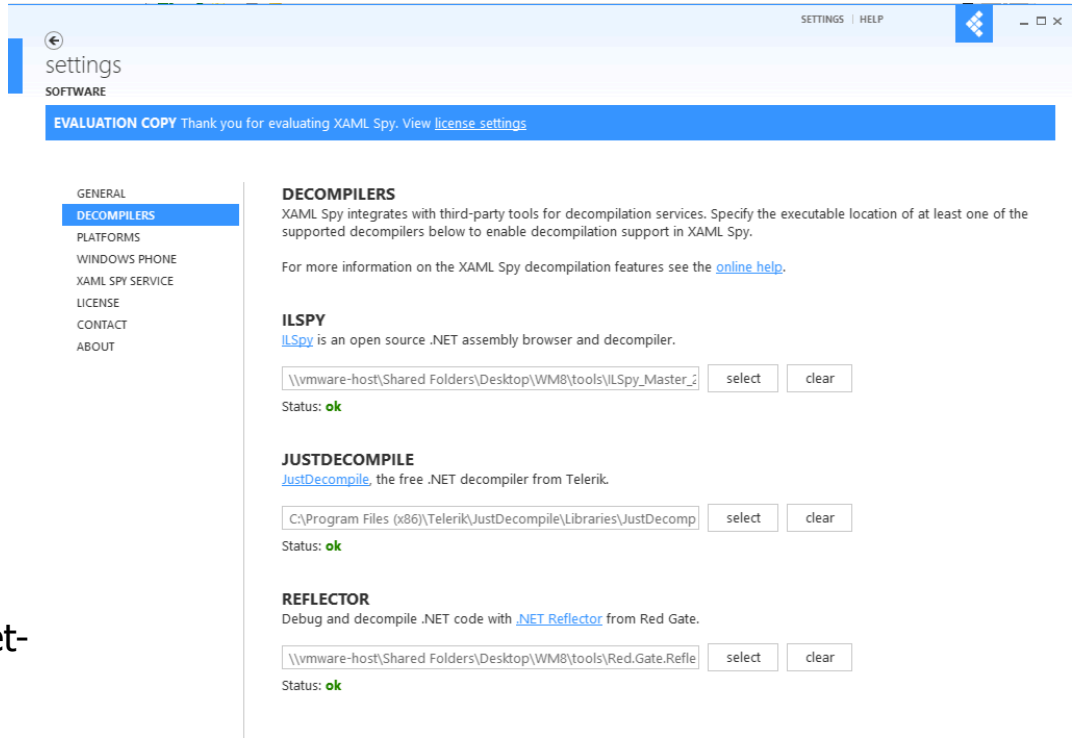

Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept History Options
Request to http://www.sans.org:80 [66.35.59.202]
Forward Drop Intercept is on Action
Raw Headers Hex
GET /banners/isc_ss.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://isc.sans.edu/diary.html?rss
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0; Microsoft; Virtual)
Accept-Encoding: gzip, deflate
Proxy-Connection: Keep-Alive
Host: www.sans.org
0 matches
IPv6 Focus Month: Kaspersky Firewall IPv6 Vulnerability


Fiddler Web Debugger
File Edit Rules Tools View Help GET /book
Web Sessions
The SyntaxView Inspector displays syntax-highlighted HTML, Script, CSS, and XML. If y
Microsoft March 2013 Black Tuesday Overview

Decompiling applications: XAML Spy

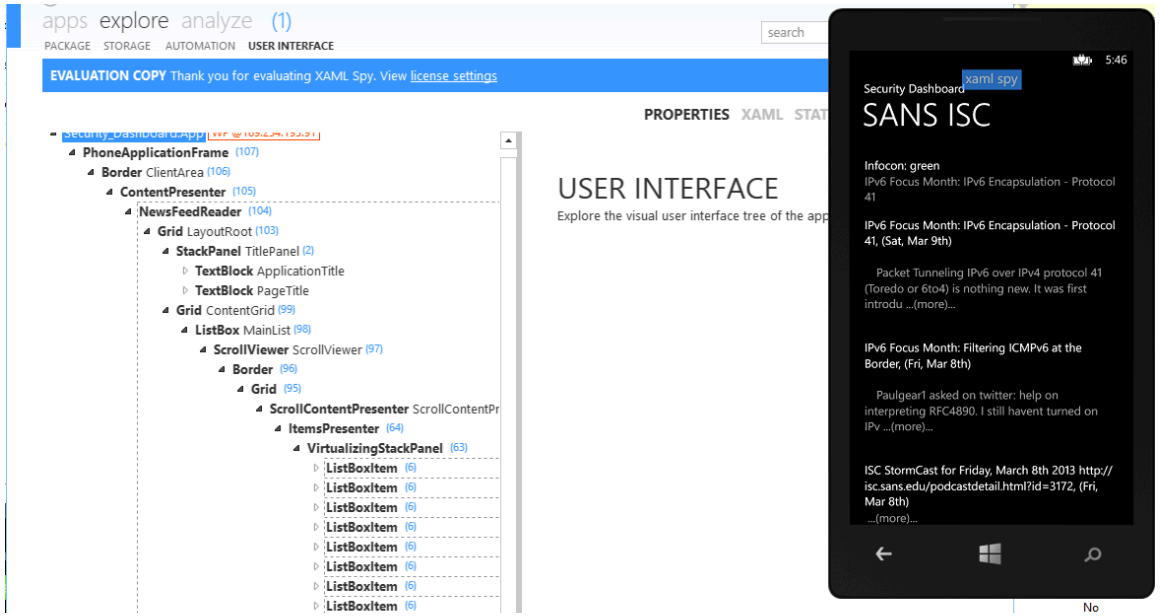
XAML Spy ($79, free trial). Prerequisites are 1 of the following:

- ILSPY
- JustDecompile
- Reflector



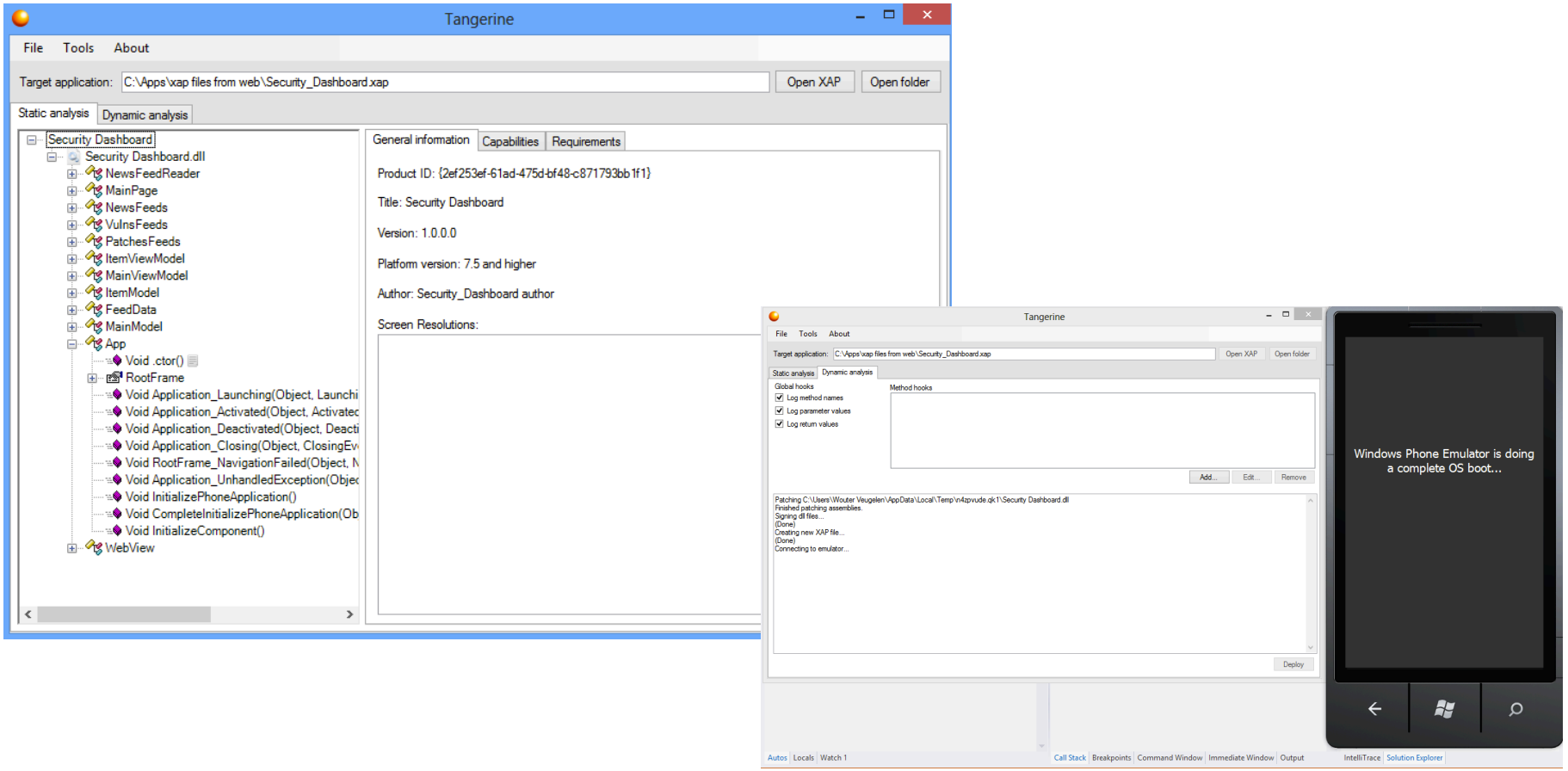
- ILSPY (free): http://ilspy.net/
- JustDecompile (free): http://www.telerik.com/products/decompiler.aspx
- Reflector ($95, free trial) http://www.red-gate.com/products/dotnet-development/reflector/

Decompile XAP files: XAML Spy (Commercial)



Limitations: only works for non DRM protected XAP files (i.e. apps **not** from Microsoft store)

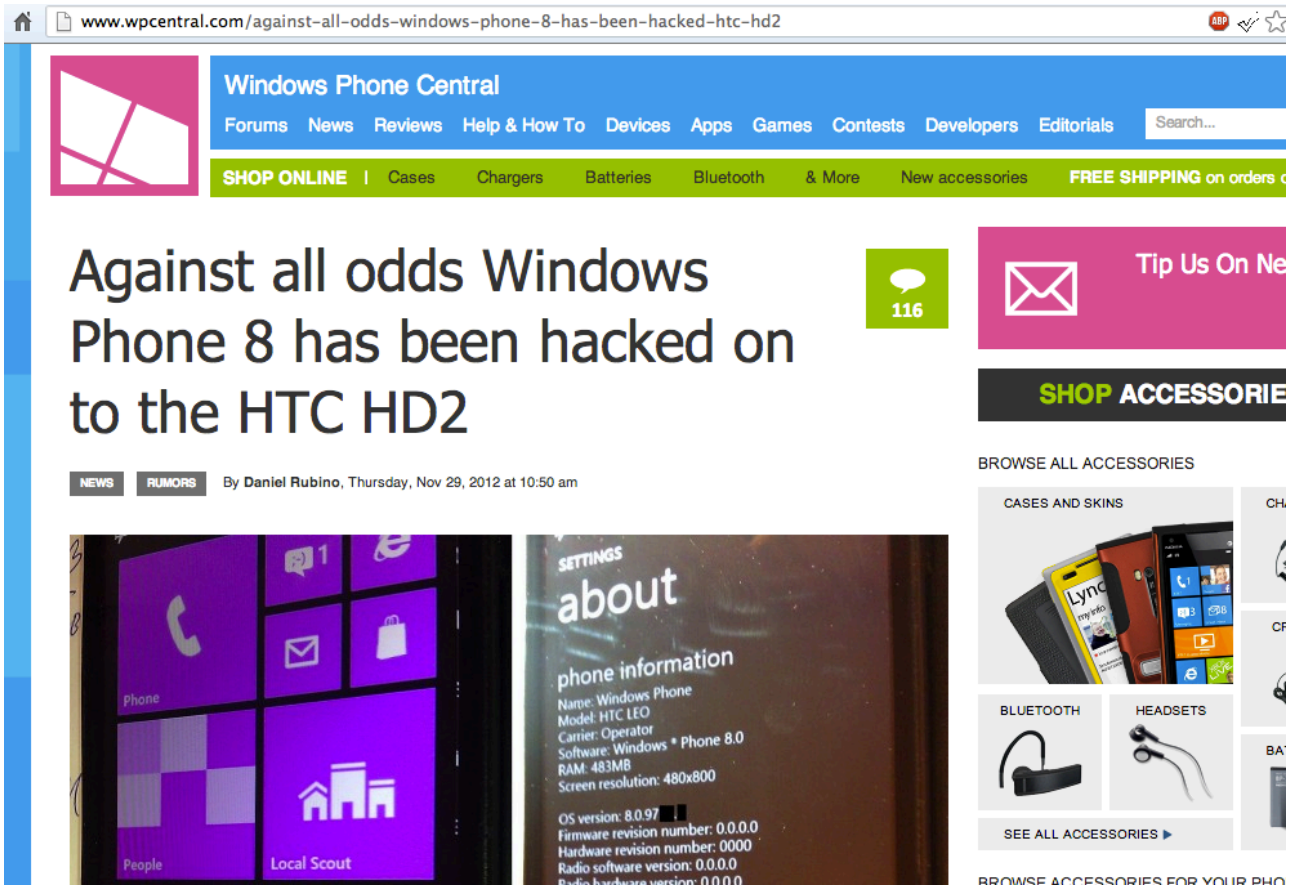
Decompile XAP files: Tangerine (Free)



Windows Phone:
Mobile Device Security Testing

Windows Phone 8

Windows Phone 8



Jailbreaking

- Windows Phone 8 is a closed operating system.
- During a mobile device security test we need to conduct activities such as inspecting the file system, data storage, memory, and transfer files which is all prevented out of the box.
- It is possible to test the application with a web application proxy without jailbreaking

Jailbreaking methods?

- Escalate privileges:
  - Drive by Download IE 10 exploit
  - Exploit trusted OEM app on phone
- Enable support for running untrusted code
  - SecureBoot bypass: Secure the boot process prevents the loading of drivers or OS loaders that are not signed with an acceptable digital signature
  - Disable application code signing
  - Add private Enterprise App Store certificate
- …

Drive by Download

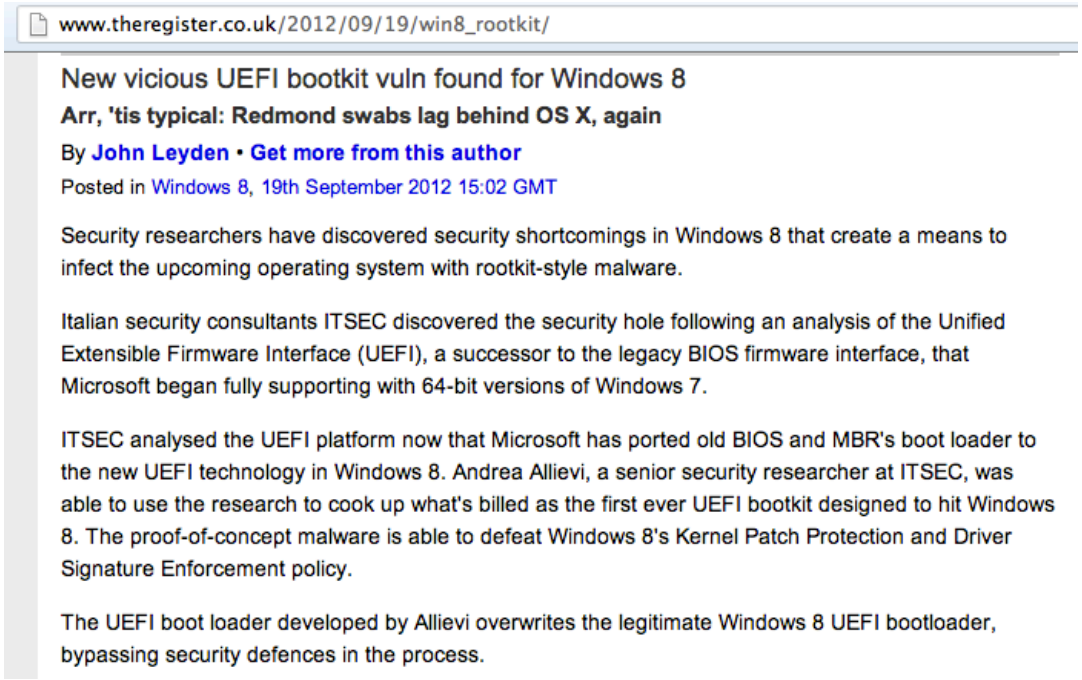
- pwn2own March 2012
  - Internet Explorer 10: owned
  - Windows RT + IE10: owned

Windows Phone 8 uses….

IE10!

SecureBoot bypass: Windows 8

Successful attack on Windows 8 (September 2012)



www.theregister.co.uk/2012/09/19/win8_rootkit/

New vicious UEFI bootkit vuln found for Windows 8

Arr, 'tis typical: Redmond swabs lag behind OS X, again

By **John Leyden** • **Get more from this author**

Posted in Windows 8, 19th September 2012 15:02 GMT

Security researchers have discovered security shortcomings in Windows 8 that create a means to infect the upcoming operating system with rootkit-style malware.

Italian security consultants ITSEC discovered the security hole following an analysis of the Unified Extensible Firmware Interface (UEFI), a successor to the legacy BIOS firmware interface, that Microsoft began fully supporting with 64-bit versions of Windows 7.

ITSEC analysed the UEFI platform now that Microsoft has ported old BIOS and MBR's boot loader to the new UEFI technology in Windows 8. Andrea Allievi, a senior security researcher at ITSEC, was able to use the research to cook up what's billed as the first ever UEFI bootkit designed to hit Windows 8. The proof-of-concept malware is able to defeat Windows 8's Kernel Patch Protection and Driver Signature Enforcement policy.

The UEFI boot loader developed by Allievi overwrites the legitimate Windows 8 UEFI bootloader, bypassing security defences in the process.

http://www.saferbytes.it/2012/09/18/uefi-technology-say-hello-to-the-windows-8-bootkit/

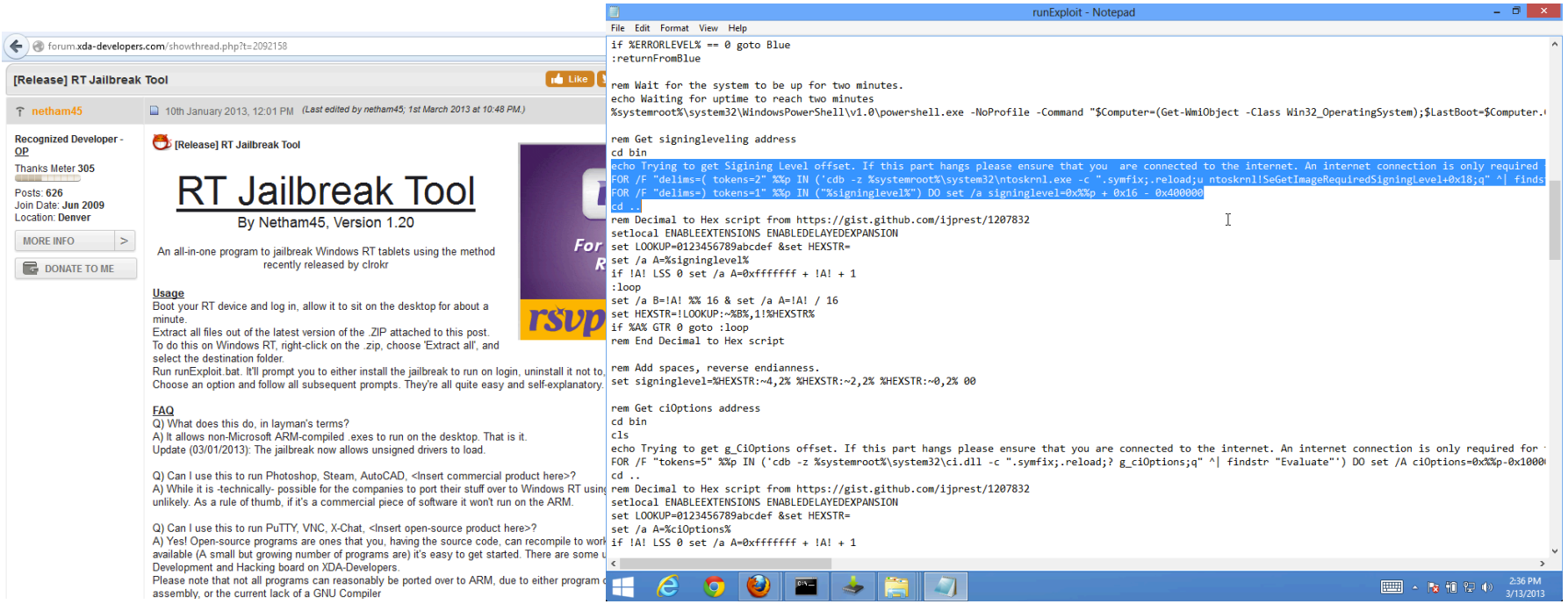
Disable application code signing

- Vulnerability in the Windows kernel that has existed for a long time — since before Microsoft ported Windows from x86 to ARM
- Windows kernel on your computer is configured to only execute files that meet a certain level of authentication:
  - Unsigned (0), Authenticode (4), Microsoft (8), and Windows (12).
- Windows 8: default value is Unsigned
- Windows RT: default, hard-coded setting is Microsoft (8); i.e. only apps signed by Microsoft, or parts of Windows itself, can be executed.'"

Disable application code signing: Windows RT

... and successfully replicated on Windows RT

- Proof of concept: January 2013
- Jailbreak script released: February 2013

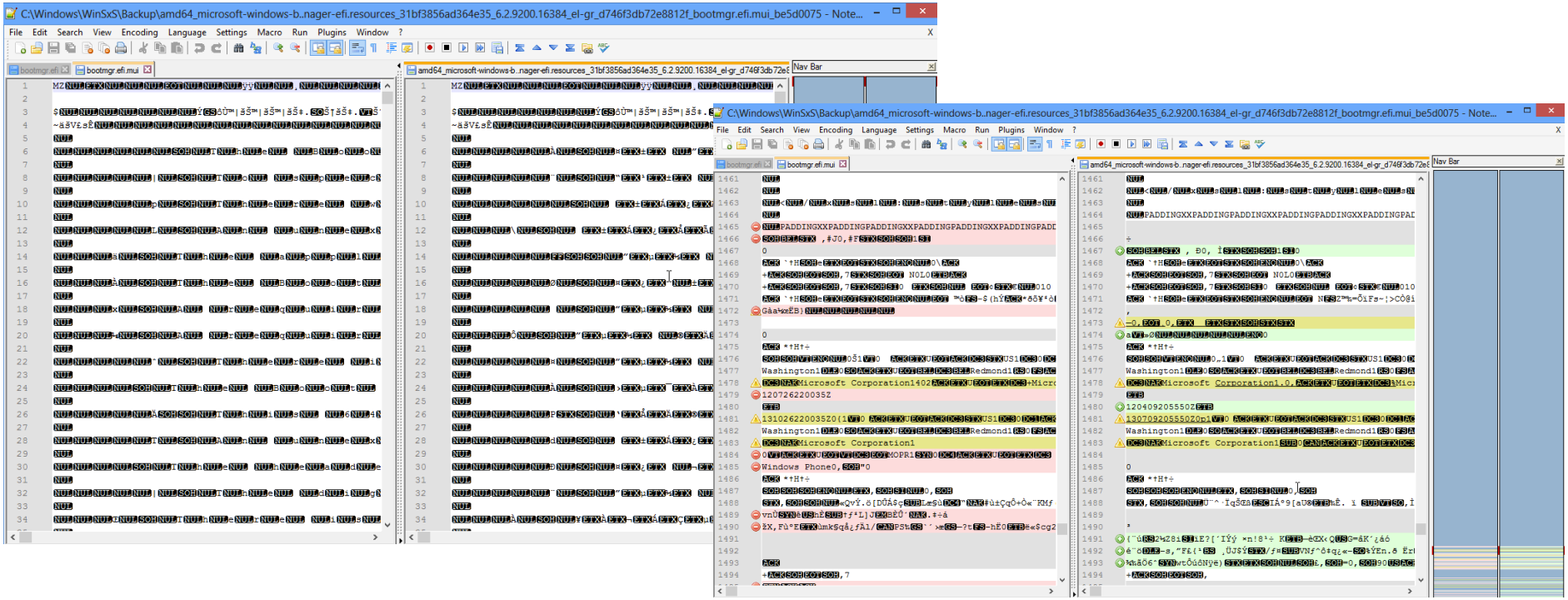


SecureBoot bypass: Windows Phone

- How about replicating the Windows RT jailbreak on Windows Phone?
- This has not been done yet

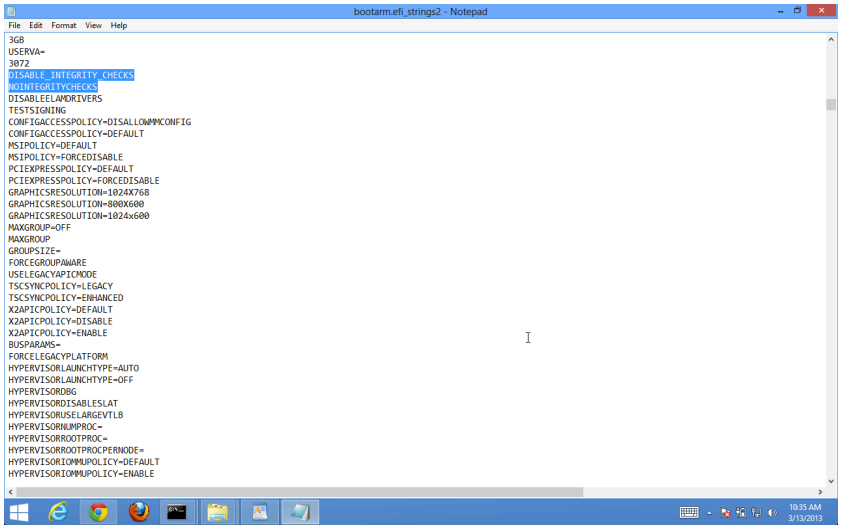
SecureBoot bypass: Windows Phone

- Quick analysis performed: bootloaders look very, very similar (Windows 8 vs. Windows Phone 8)



SecureBoot bypass: Windows Phone

- Looking at the Windows Phone 8 bootloader with strings.exe, the same configuration parameters that were exploited in the WinRT jailbreak can be found

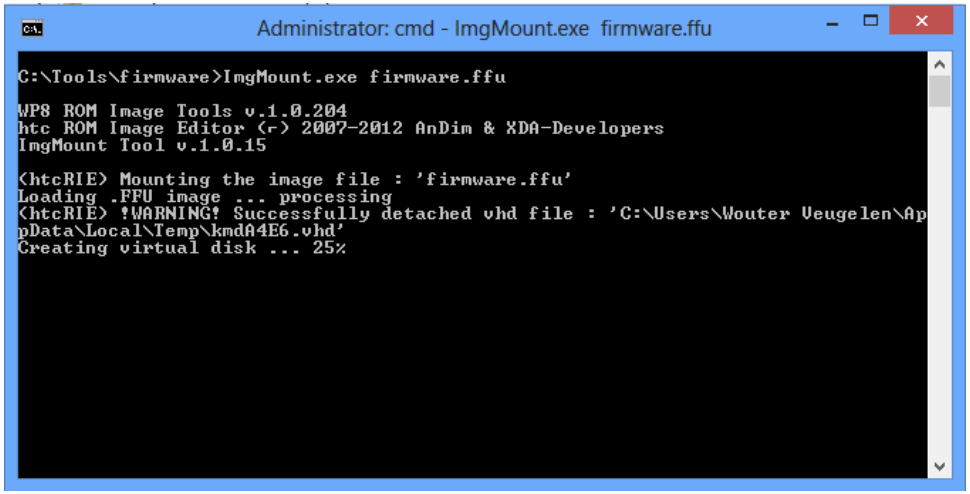


File system analysis

- No file system access without jailbreak :(
- How can we gain an understanding of the Windows Phone 8 file system architecture and configuration?
  - Analyse Windows Phone 8 firmware files

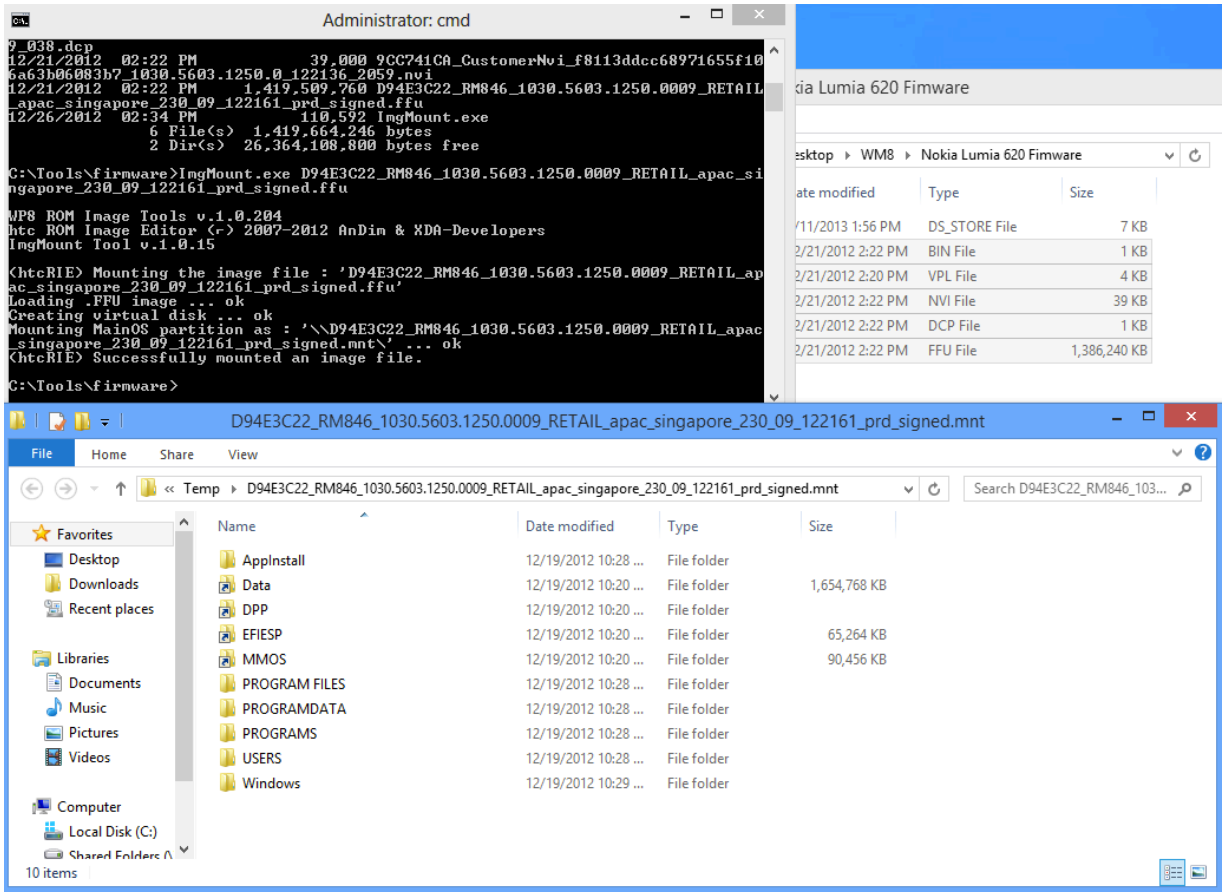
File system analysis

- Windows Phone is a closed OS: It is not possible to browse the file system on a Windows Phone device.



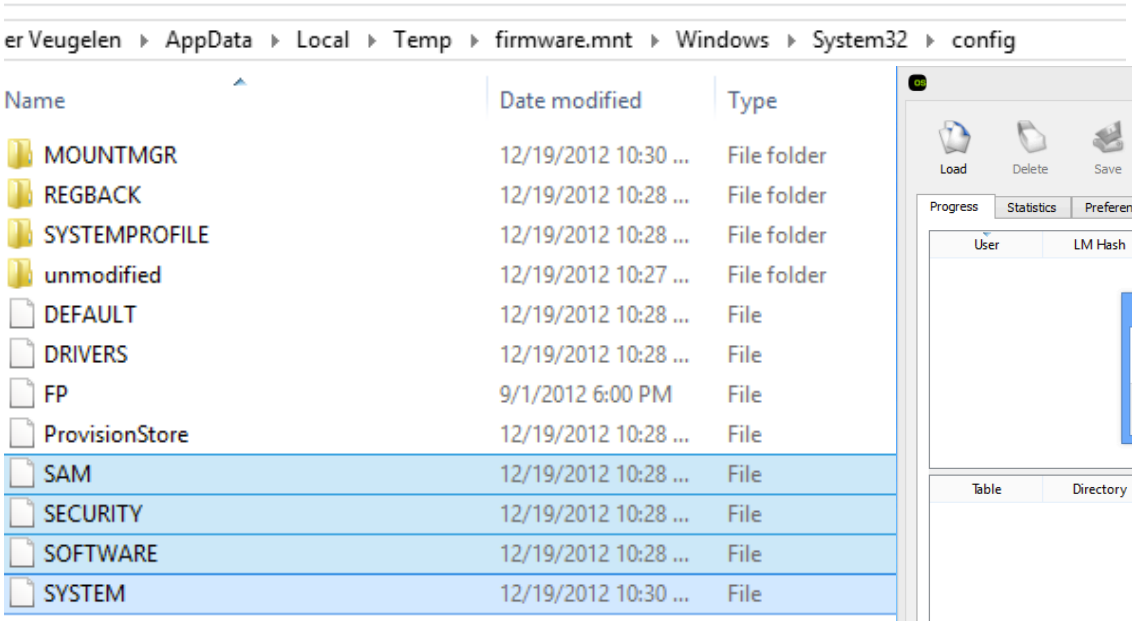
- Software required: ImgMount.exe
  http://forum.xda-developers.com/showthread.php?p=36014289

File system analysis

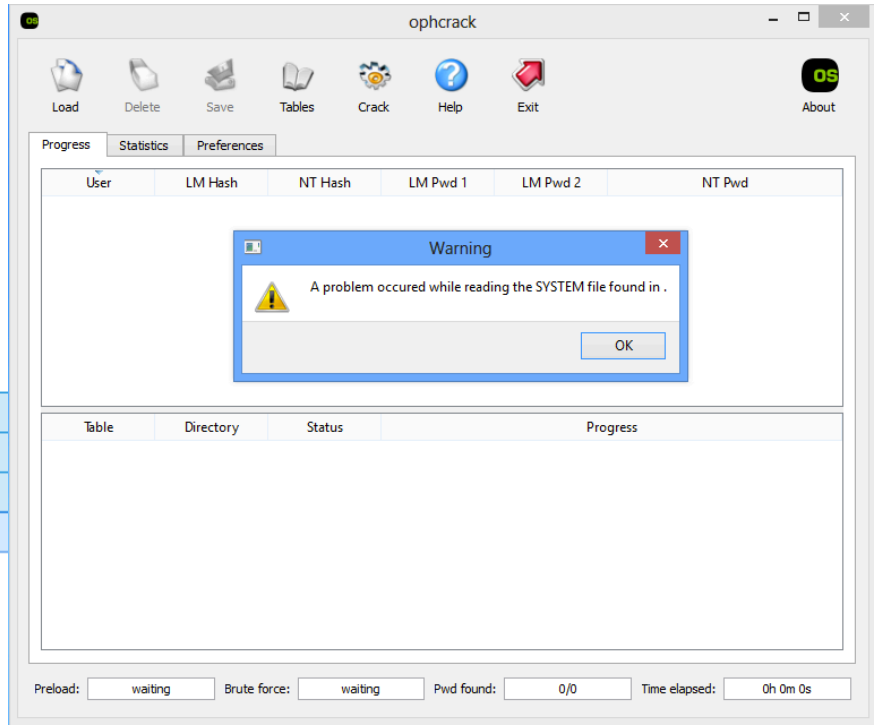


SAM files

SAM files

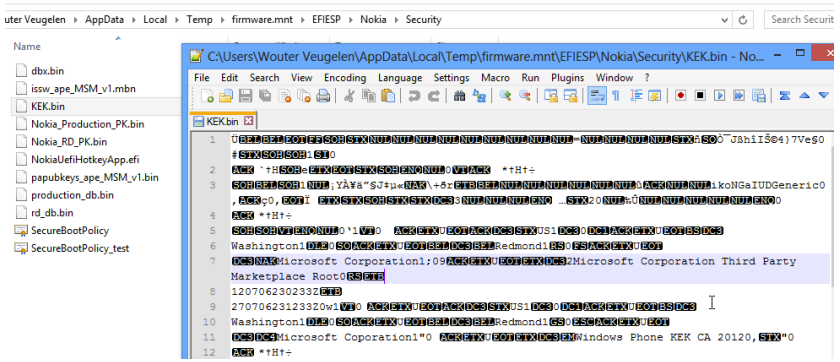


Bad luck...



Certificates

Applications – signing CA's



Microsoft Root Certificate Authority 2010

28 CC 3A 25 BF BA 44 AC 44 9A 9B 58 6B 43 39 AA

Microsoft Corporation Third Party Marketplace Root

33 95 9C 19 50 48 71 91 42 38 DF 73 D3 B4 9A 3D

Microsoft Windows Phone Production PCA 2012

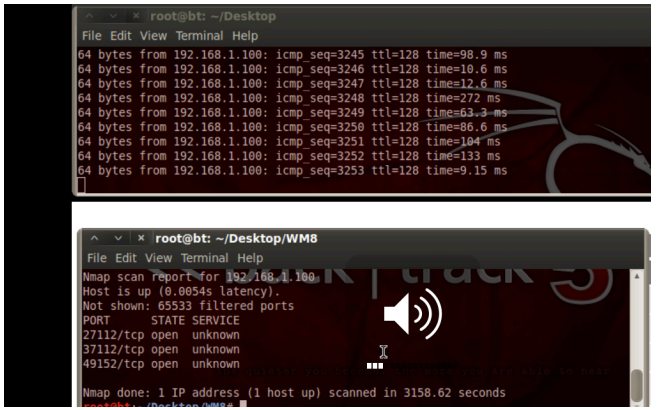
33 00 00 00 0b fc f9 8e 58 4c 15 50 bf 00 00 00 00 00 0b

Microsoft Time-Stamp PCA 2010

?61 09 81 2a 00 00 00 00 00 02

Portscan results - TCP

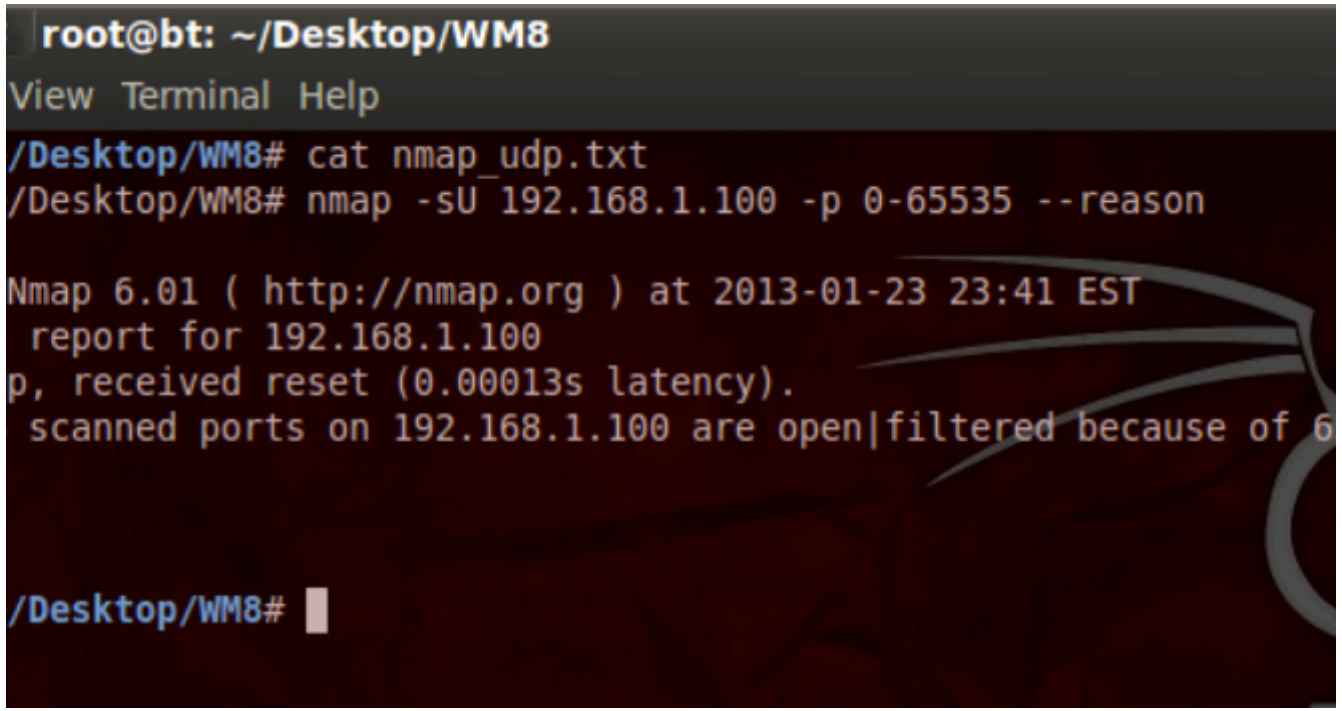
- Open ports:
  - 27112/tcp open unknown
  - 37112/tcp open unknown
  - 49152/tcp open unknown
- Port 27112 fingerprint:




```
SF-Port27112-TCP:V=6.01%I=7%D=1/23%Time=50FFD97B%P=x86_64-unknown-linux-gn
SF:u%r(GetRequest,70,"HTTP/1\.1\x20404\x20File\x20Not\x20Found\r\nContent-
SF:Length:\x200\r\nServer:\x20NWP-HTTPAPI/2\.0\r\nDate:\x20Sat,\x2009\x20M
SF:ar\x202013\x2002:46:31\x20GMT\r\n\r\n")%r(HTTPOptions,70,"HTTP/1\.1\x20
SF:404\x20File\x20Not\x20Found\r\nContent-Length:\x200\r\nServer:\x20NWP-H
SF:TTPAPI/2\.0\r\nDate:\x20Sat,\x2009\x20Mar\x202013\x2002:46:31\x20GMT\r\
SF:n\r\n")%r(RTSPRequest,70,"HTTP/1\.1\x20404\x20File\x20Not\x20Found\r\nC
SF:ontent-Length:\x200\r\nServer:\x20NWP-HTTPAPI/2\.0\r\nDate:\x20Sat,\x20
SF:09\x20Mar\x202013\x2002:46:31\x20GMT\r\n\r\n")%r(FourOhFourRequest,70,"
SF:HTTP/1\.1\x20404\x20File\x20Not\x20Found\r\nContent-Length:\x200\r\nSer
SF:ver:\x20NWP-HTTPAPI/2\.0\r\nDate:\x20Sat,\x2009\x20Mar\x202013\x2002:46
SF::31\x20GMT\r\n\r\n")%r(SIPOptions,70,"HTTP/1\.1\x20404\x20File\x20Not\x
SF:20Found\r\nContent-Length:\x200\r\nServer:\x20NWP-HTTPAPI/2\.0\r\nDate:
SF:\x20Sat,\x2009\x20Mar\x202013\x2002:46:31\x20GMT\r\n\r\n");
```

Microsoft Lyc?

Portscan results - UDP



Future work

- Write Windows Phone 8 application that:
  - Hooks into a remote debugger
  - Search for the code signing parameters
  - Change the code signing parameters in memory (Similar to Windows RT jailbreak)
- Identify vulnerabilities trusted OEM app on phone
- Research manual unlocks of Windows Phone 8
  - Capture, analyse and replay device unlock communications (IP over USB) between host and Windows Phone

Resources and further references

- SANS SEC575 Mobile Device Security and Ethical Hacking
  - SANS Canberra 2013
  - Jul 1, 2013 - Jul 13, 2013

- XDA-developers – Windows Phone 8 Development and Hacking forum