

### Compass Security [The ICT-Security Experts]

Windows Phone

Windows Phone 8.1 [Beer Talk – Berlin – 2015/07/21]

Stephan Sekula

Compass Security Deutschland GmbH Tauentzienstr. 18 De-10789 Berlin Tel. +49 30 21 00 253-0 Fax +49 30 21 00 253-69 team@csnc.de www.csnc.de

### May I introduce myself?



### Stephan Sekula

- ✤ With Compass since August 2013
- Career: Studied Computer Science, worked in research, now gathering practical experience
- ✤ <u>Expertise</u>
  - ✤ War Dialing
  - Social Engineering basics (from Psychology minor)

### Hobbies

- Cooking & baking
- Bicycling
- Climbing
- IT-Security



## Agenda



### Introduction

### Windows Aspects

- Windows Environment
- ✤ Attack Surface
- ✤ Breaking Out

### Mobile Aspects

Sandboxing & Encryption

### Findings

- ✤ MDM Integration
- ✤ Wi-Fi Sense
- Low Level Storage API

### Conclusion



### Microsoft

- ✤ Major player in home computing, servers, software, and entertainment
- ✤ Still very new to the mobile sector
- But attempting to catch up with the acquisition of Nokia
- Still understands / answers companies' needs best

Main focus of analysis

Windows Phone platform itself

### Let's get started



ð ð

### Let's start

We're here to help. In just a handful of steps, your phone will be ready to go.

Connecting to a network

Choosing phone settings

Setting up a Microsoft account

Activate your phone

previous

next



### Introduction

### Windows Aspects

- Windows Environment
- ✦ Attack Surface
- **Breaking Out**

### **Mobile Aspects**

Sandboxing & Encryption

### Findings

- ✤ MDM Integration
- Wi-Fi Sense
- Low Level Storage API +

### Conclusion



### Crash dumps are always useful and a good start...

ALLUSERSPROFILE=C:\Data\ProgramData APPDATA=C:\Data\Users\DefApps\AppData\Roaming CommonProgramFiles=C:\Program Files\Common Files COMPUTERNAME=Windows Phone ComSpec=C:\windows\system32\cmd.exe FP\_NO\_HOST\_CHECK=NO LOCALAPPDATA=C:\Data\Users\DefApps\APPDATA\Local\Packages\8dd8d60d-8b28-4e52-b113c2aac34b9ac3\_yhxz8gp8y0q0t\AC NUMBER\_OF\_PROCESSORS=4 OS=Windows\_NT Path=C:\windows\system32;C:\windows;C:\Programs\CommonFiles\System;C:\wtt;C:\data\test\bin; PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC PROCESSOR\_ARCHITECTURE=ARM

ProgramData=C:\Data\ProgramData ProgramFiles=C:\Program Files PUBLIC=C:\Data\Users\Public SystemDrive=C: SystemRoot=C:\windows TEMP=C:\Data\Users\DefApps\APPDATA\Local\Packages\8dd8d60d-8b28-4e52-b113c2aac34b9ac3\_yhxz8gp8y0q0t\AC\Temp TMP=C:\Data\Users\DefApps\APPDATA\Local\Packages\8dd8d60d-8b28-4e52-b113c2aac34b9ac3\_yhxz8gp8y0q0t\AC\Temp USERDOMAIN=Windows Phone USERNAME=DefApps USERPROFILE=C:\Data\Users\DefApps windir=C:\windows



### (Ab)Use of Windows Utilities and Features

Is it possible to gather information or perform undesired actions using built-in features?

### **Application Attack Surface**

✦ Can apps such as Internet Explorer be used to run unwanted code?

### Development and APIs

✦ Can APIs be leveraged to execute malicious code?



### A Windows desktop is user (and attacker) friendly

- ✤ Lots of information (event logs, detailed error messages, ...)
- Lots of settings to influence (control panel, file & registry access, ...)
- Built-in programs and features (notepad, sticky keys for accessibility, ...)
- Various ways to execute code (bat, vbs, WMI, PowerShell, compilers, ...)

### Windows Phone exposes

- ✤ Very little information or settings are available
- No interesting default apps
- No possibility to "run" stuff
- No sticky keys
- ✤ It is impossible to e.g. get the UEFI settings details of the phone...

**CEPASS** SECURITY

### Internet Explorer is the most interesting app on the phone User influence / interaction

- ✤ High privileges on the phone
- ✤ Increased attack surface

### Failed abuse scenarios

- Run VBScript within the browser
- ✤ Browse the local file system using <u>file:///</u>
- ✤ SMB connect-back from the phone to the attacker
- ✤ No way to download and execute e.g. .bat, .exe, or .vbs files
- ✤ Link files (.lnk) are not executed, either

We can't download this file, because Windows Phone doesn't support this file type.

### Can't complete

ok

Can't open file lnk\_DriveC.lnk. Error code: -2147024809. You can mention this code when providing feedback.

Compass Security Deutschland GmbH

www.csnc.de



### If no app provides the desired feature, develop your own!

# The C++ and.NET APIs are trimmed down & restricted, preventing breaking out / unwanted actions

### Failed abuse scenarios

- ✤ Controlling processes or threats to fork new content within an application
- Running arbitrary commands using Shell.Execute
- Accessing WMI (Windows Management Instrumentation) to gather information and execute arbitrary commands
- Running PowerShell for the same reasons

### **Open Questions**



### Of course, not all options have been explored so far, e.g.

- ✤ Is arbitrary execution of commands possible, via e.g. Lambda expressions?
- Can the restricted APIs be abused?
   (e.g. attempt to load an assembly not present within the Windows Phone SDK)
- In-depth audit of the Protected Data / Vault feature
- Study of the AppContainer and SIDs separation
- Understand the steps involved in the application signing process (and their capabilities restrictions)
- Subversion of accorded capabilities

   (capabilities seem to be labels assigned to a given process).
- Content of C:\WTT
- Corruption via the video driver e.g. within the browser (WebGL)



### So from a Windows perspective, there is not much attack surface

### Some information leaks from application crash dumps, e.g.

- User executing the app / App Container context
- List of defined drives:

  - ✤ D:\ (probably SD card)
  - ✤ U:\ (probably a mapping to C:\data\.
  - ✤ PATH variable contains unknown folder C:\WTT\.
  - Data seems shared via C:\Data\Share
  - C:\windows\system32\cmd.exe does not exist



### Introduction

### Windows Aspects

- Windows Environment
- ✦ Attack Surface
- **Breaking Out**

### **Mobile Aspects**

✦ Sandboxing & Encryption

### Findings

- ✤ MDM Integration
- Wi-Fi Sense
- Low Level Storage API +

### Conclusion



### Sandboxing

- Attack surface reduction (Least Privilege Principle)
- User consent and control (Capabilities)
- Isolation (AppContainer, dedicated SIDs)

### Malware Resistance

- ✤ UEFI, Trusted / Secure Boot
- System and app integrity (code signing)
- Windows Phone Store (automated malware scan)

### **Exploit Mitigation**

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)

### Encryption

BitLocker (AES-128, TPM)

### Sandboxing



### AppContainer

- + Isolation
- Credentials
- ✦ Roaming
- ✤ Data access
- ✦ Sharing data
- Encrypting data

### Capabilities

### **Restricted APIs**

✦ Isolated storage

### File System Overview



### Data Access

## Locations where apps can access data



http://channel9.msdn.com/Series/Building-Apps-for-Windows-Phone-8-1/09

CCA PASS SECURITY



#### Example:

var vault = new PasswordVault();
PasswordCredential cred = new PasswordCredential("account", username, password);
vault.Add(cred);

### Roaming

Sharing data e.g. credentials across devices



## Roaming

### Credentials roam across trusted devices



### Sharing Data



### Sharing data between apps works using:

• URI association, where the registered app obtains the data stored in the URI



• File association, where the registered app obtains the file content

| urce   | File association  |              | target       |
|--------|---|--------------|--------------|
|        | <pre>Windows.System.Launcher.LaunchFileAsync(     myStorageFile);</pre> | Data in File |              |
| S # 4- | -   |              | <b>* * *</b> |

• Share contract, allowing custom DataPackages to be shared

| share source | Share contract   |  | File, text, HTML,      | Share                     |
|--------------|--|--|------------------------|---------------------------|
|              | Windows.ApplicationModel.DataTransfer.<br>DataTransferManager.ShowShareUI(); | Annual     Annual     Annual     Annual     Annual     Annual     Annual     Annual     Annual | data in<br>DataPackage | UI                        |
| 2 <b>2</b> 4 | <  | 4 <b>1</b> +   |                        | $(a^{*} - b^{*}) = b^{*}$ |



### Disk Encryption using BitLocker is disabled by default

- ✤ End-user cannot enable or disable encryption
- Can only be activated through ActiveSync or MDM policy

### Applications can use DPAPI to protect confidential data

- DPAPI (Data Protection API) generates and stores a cryptographic key by using the user and device credentials
- Every app gets its own encryption key, which is created upon the app's first launch
- Keys are persistent across app updates

https://msdn.microsoft.com/en-us/windows/apps/hh487164.aspx

## Capabilities



### Software capabilities

- ✦ Capability elements are entries in the app manifest file
- User is notified upon installation of an app which capabilities are required
- + E.g. location services

### Hardware requirements

- ✤ Optional entry in the app manifest file
- Specifies hardware required for running the app
- E.g. Near Field Communication (NFC)

### Functional capabilities

- ✤ Optional entry in the app manifest file
- Indicates that an app requires a hardware capability of the phone which is present, but not automatically granted
- E.g. higher memory limits (in Windows Phone 8.0 only)

### Software Capabilities



11:39

### Capabilities listed in the app manifest

- Displayed to the user upon installation
- Some capabilities are prominently displayed (e.g., location services)

### Allow access to location?

Skype Skype

5) 6 C

Skype needs to know your location to work correctly. If you don't want to allow access to your location, tap Cancel and the app won't be installed.

Each time Skype requests your location, Microsoft will collect information about your location to provide and improve the location services. The information is not used to identify or contact you.

Read Privacy Statement online



### Setting capabilities using Microsoft Visual Studio 2013 Express:

| Application            | Visual Assets               | Requirements   | Capabilities            | Declarations                 | Content URIs          | Packaging |  |  |  |  |  |  |
|------------------------|-----------------------------|--|-------------------------|------------------------------|-----------------------|-----------|--|--|--|--|--|--|
| Use this page to speci | fy system features or devic | es that your app can use.  |                         |                              |                       |           |  |  |  |  |  |  |
| Capabilities:          |                             | Description:   |                         |                              |                       |           |  |  |  |  |  |  |
| Appointments           |                             | Provides access to the   | user's appointment stor | e. This gives read access to | appointments obtained | from the  |  |  |  |  |  |  |
| Contacts               |                             | available. With this capability your app can create new calendars and write appointment store, and mark those as |                         |                              |                       |           |  |  |  |  |  |  |
| Enterprise Auther      | ntication                   | creates.   |                         |                              |                       |           |  |  |  |  |  |  |
| 📃 Internet (Client &   | l Server)                   | More information   |                         |                              |                       |           |  |  |  |  |  |  |
| Location               |                             |  |                         |                              |                       |           |  |  |  |  |  |  |
| Microphone             |                             |  |                         |                              |                       |           |  |  |  |  |  |  |
| Music Library          |                             |  |                         |                              |                       |           |  |  |  |  |  |  |
| Pictures Library       |                             |  |                         |                              |                       |           |  |  |  |  |  |  |
| Proximity              |                             |  |                         |                              |                       |           |  |  |  |  |  |  |
| Removable Stora        | ge                          |  |                         |                              |                       |           |  |  |  |  |  |  |
| Shared User Certi      | ficates                     |  |                         |                              |                       |           |  |  |  |  |  |  |
| Videos Library         |                             |  |                         |                              |                       |           |  |  |  |  |  |  |
| Webcam                 |                             |  |                         |                              |                       |           |  |  |  |  |  |  |

Note: When testing apps using the Windows Phone emulator the capabilities are granted automatically, even when not included in the app manifest

### **Capabilities Overview**



#### **Appointments**

#### Libraries

Allows an app to access the calendar and Allows an app to access all photos, appointment info. music, and videos on your phone.

#### Camera

Allows an app to access the built-in camera.

#### Compass

Allows an app to access the built-in compass, if available.

#### Contacts

Allows an app to access the contact info. Allows access to the Bluetooth, Wi-Fi,

#### Data services

Your phone's cellular data or Wi-Fi connection.

#### Gyroscope

Allows an app to access the built-in gyroscope, if available.

#### Location services

The approximate location.

#### Microphone

Allows an app to record audio and to use Allows an app to access the ringtones. Speech features.

#### Movement sensor

Allows an app to access the motion sensor.

#### Proximity

and near field communication (NFC) capabilities.

#### **Owner** identity

An anonymous identifier that allows an app to distinguish one person from another, but provides no personal info.

#### Phone identity

A unique device identifier that allows an app to distinguish one phone from another.

#### Push notification service

Notifications that an app automatically sends to your phone.

#### Ringtones

SD card

Allows an app access to the SD card.

Speech recognition

Allows an app to access Speech features.

#### Wallet

Allows an app to access items in your Wallet or to make payments.

#### Web browser

Allows an app to access the web browser.

#### Xbox

Allows an app to access the Xbox service or your account info.



### Capabilities – WhatsApp

social

# WhatsApp



Free

\* \* \* \* \* \* 29190 reviews

By installing you agree to the Terms of Use and other terms

#### App requires

appointments contacts phone identity owner identity video and still capture location services maps music library photos library media playback microphone data services phone dialer push notification service movement and directional sensor VOIP calling web browser component HD720P (720x1280) WVGA (480x800) WXGA (768x1280) appointments Proximity SD card internet connection videos library photo, music, and video libraries camera





### Locations all apps can access:

- Application install directory (read only)
- Application data locations (local, roaming and temporary directories are created upon app installation)
- Removable devices (SD card; access is limited to specific file types)
- User's Downloads folder

### Locations requiring additional capabilities in the app manifest:

- Libraries (Documents, Music, Pictures, Videos)
- Removable devices (SD card)
- Homegroup libraries
- Media server devices (DLNA)
- Universal Naming Convention (UNC) folders



## Windows Aspects

- Windows Environment
- ✦ Attack Surface
- ✤ Breaking Out

### Mobile Aspects

Sandboxing & Encryption

### Findings

- ✤ MDM Integration
- ✤ Wi-Fi Sense
- ✤ Low Level Storage API

### Conclusion

### **MDM** Integration



### Push communication

- ✤ To distribute policies and configuration standards
- Periodically contacts the MDM server to:
  - ✤ Download configurations, apps, updates
  - Upload asset information



Microsoft: Windows Phone 8.1 Mobile Device Management Overview



### **Device Configuration Management**

- Configuration policies
- Access management
- Storage management
- Wi-Fi network / VPN / certificate management
- Email account / message management

### App Management

- Windows Phone Store apps
- Side loaded apps
- Allow / deny apps

### **Remote Inventory**

Remote inventory / assistance (lock / PIN reset)

### **Device Retirement**



Password policy

| Policies that MDM and EAS support   | Policies that only MDM supports                  |
|-------------------------------------|--|
| Simple password                     | Disable cellular data roaming                    |
| Alphanumeric password               | Disable Location                                 |
| Minimum password length             | Disable NFC                                      |
| Minimum password complex characters | Disable Microsoft Account                        |
| Password expiration                 | Disable roaming between Windows devices          |
| Password history                    | Disable custom email accounts                    |
| Device wipe threshold               | Disable screen capture                           |
| Inactivity timeout                  | Disable copy & paste functionality               |
| Device encryption                   | Disable share and save as                        |
| Disable removable storage card      | App Allow/Deny list                              |
| Disable Camera                      | Disable Microsoft Store                          |
| Disable Bluetooth                   | Disable development unlock (side loading)        |
| Disable Wi-Fi                       | Disable Internet Explorer                        |
| Disable Sync via USB                | Disable Internet Sharing over Wi-Fi              |
|                                     | Disable Wi-Fi Off loading                        |
|                                     | Disable Manual Configuration of Wi-Fi Profiles   |
|                                     | Disable Wi-Fi Hotspot reporting                  |
|                                     | Disable VPN when Roaming over Cellular           |
|                                     | Disable VPN over Cellular                        |
|                                     | Disable mdm un-enrollment and soft factory reset |
|                                     | Disable Wi-Fi credential sharing                 |
|                                     | Lock screen notification controls                |
|                                     | Disable telemetry data submission                |

Microsoft: Windows Phone 8.1 Mobile Device Management Overview

www.csnc.de

### Wi-Fi Sense



### Automatically establishes Wi-Fi connections

- Based on crowdsourcing (Wi-Fi networks other Windows Phone users have connected to)
- Automatically accepts the Wi-Fi's Terms of Use
- Automatically provides additional information required to connect (email address, phone number, etc.)
- Automatically shares Wi-Fi credentials with:
  - ✤ Facebook friends
  - Outlook.com contacts
  - ✤ Skype contacts

### How to prevent users from sharing credentials:

- ✤ Add \_optout to the Wi-Fi's SSID
- Problem: Google's \_nomap suffix

https://www.windowsphone.com/en-us/how-to/wp8/connectivity/wi-fi-sense-faq

### Low-Level Storage API



### Win32 storage APIs supported on Windows Phone 8

Windows Phone 8 supports the following Win32 storage APIs for working with the local folder. For the full list of supported Win32 APIs, see Supported Win32 APIs for Windows Phone 8.

- CopyFile2
- CreateDirectoryW
- CreateFile2
- DeleteFileW
- FindClose
- FindFirstFileExW
- FindNextFileW
- FlushFileBuffers

Local folder only?

### Demo





.....



Device has to be registered / developer unlocked to deploy apps locally (side loading)

Our test app can now access files / pipes etc. outside of the "official" folders

The app can also access documents stored by another app when knowing the path

Does not work anymore if app is signed and distributed via Windows Phone Store

We managed to brick our test phone and had to perform a full reset...

### **Open Research**

Analysis of extracted information



### Extracted ~10,000 operating system files

|                      | · · · · · · · · · · · · · · · · · · · |                 | 1.22                           | 2 1 22           |     | 2 |
|----------------------|---------------------------------------|-----------------|--------------------------------|------------------|-----|---|
| -) -> -> T           | ▶ Windows ▶ system32                  |                 | V C                            | Search system32  |     | Q |
| vame *               | Date modified                         | n.              | Windows Properti               | es 💽             | ¢   |   |
| 📙 ADVANCEDINSTALLERS | 09.06.2015 10:02                      |                 | land land                      |                  | -14 |   |
| 📙 af-za              | 09.06.2015 11:09                      | General Shar    | ing Security Customise         |                  | 8   |   |
| 📙 ar-sa              | 09.06.2015 11:09                      |                 | AND STREET                     |                  |     |   |
| 📙 az-latn-az         | 09.06.2015 11:09                      | 1               | Windows                        |                  |     |   |
| 📙 backgrounds        | 09.06.2015 11:09                      | 1               | 19 <u>2</u> 01202020           |                  |     |   |
| be-by                | 09.06.2015 11:09                      | Type:           | File folder                    |                  |     |   |
| 📙 bg-bg              | 09.06.2015 11:09                      | Location:       | C:\Users\root\Desktop\From     | SD card          |     |   |
| 📙 воот               | 09.06.2015 11:09                      | Size:           | 880 MB (923'152'325 bytes)     |                  |     |   |
| 📙 ca-es              | 09.06.2015 11:09                      | Size on disk:   | 895 MB (939'417'600 bytes)     |                  |     |   |
| CATROOT              | 09.06.2015 11:09                      | OLD ON GIOL     |                                |                  |     |   |
| 📙 CodeIntegrity      | 09.06.2015 11:11                      | Contains:       | 9 944 Files, 256 Folders       |                  |     |   |
| 📙 Comms              | 09.06.2015 11:09                      | Created         | Today 9 Juni 2015 2 hours      |                  |     |   |
| 📙 config             | 09.06.2015 10:02                      | Cleated.        | 100dy, 3. Juni 2013, 3 hours - |                  |     |   |
| cs-cz                | 09.06.2015 11:09                      | Attributes:     | Bead-only (Only applies to     | files in folder) |     |   |
| 📙 da-dk              | 09.06.2015 11:09                      | 1.1.2.000.00000 |                                | Advanced         |     |   |
| 📙 de-de              | 09.06.2015 11:09                      |                 |                                | Advanced         |     |   |
| DRIVERS              | 09.06.2015 11:10                      |                 |                                |                  |     |   |
| 📙 el-gr              | 09.06.2015 11:11                      |                 |                                |                  |     |   |
| en-gb                | 09.06.2015 11:10                      |                 |                                |                  |     |   |
| 📕 en-in              | 09.06.2015 11:10                      | 5               |                                |                  |     |   |
| EN-US                | 09.06.2015 11:10                      |                 | OK Ca                          | ncel Apply       |     |   |
| es-es                | 09.06.2015 11:10                      |                 |                                | . 4990           |     |   |
| 📙 es-mx              | 09.06.2015 11:10                      | File folder     |                                |                  |     |   |

### Open Research

Analysis of extracted information



### Some documents seem to be encrypted ...

| HAD. |           | Н       | хD        | - [C:      | :\Us     | ers\  | roo | t\D      | eskt | op\   | Fror     | n Sl | D ca | ard\ | Win  | dov | vs\Pa | Packages\RegistryFiles\Microsoft.Comms.rga] -   | □ ×   |
|------|-----------|---------|-----------|------------|----------|-------|-----|----------|------|-------|----------|------|------|------|------|-----|-------|---|-------|
| i Fi | File Edit | Searc   | h V       | iew        | Ana      | lysis | Ext | tras     | Win  | dow   | ?        |      |      |      |      |     |       |   | _ 8 × |
|      | ) 👌 🕶 🗐   | Same    |           | + +        | 16       |       | ¥   | AN       | SI   |       | ¥        | he   | x    |      | /    |     |       |   |       |
|      | 05145-44  |         | FD        | 1 64       | MD       | c l   | FØ  | SEC1     |      |       | F        |      |      |      | PEC  | FØ  | CV/C  | STEM REC I Missesoft Ann Distform and Missesoft Co  |       |
|      | OEMSettin | igs.reg | <u>A0</u> | JЗА        | uvi.ru   |       | 80  | SECU     | וואי | r.REG |          | 9.30 |      |      | .REG | 80  | 313   | STEWINEG MICrosoft AppPlatform.rga  |       |
|      | Offset(h) | 00      | 01        | 02         | 03       | 04    | 05  | 06       | 07   | 08    | 09       | 0A   | 0B   | 0C   | 0D   | 0E  | OF    |   | ^     |
|      | 00000000  | 1F      | 8B        | 08         | 00       | 00    | 00  | 00       | 00   | 04    | 0B       | C5   | 56   | 6B   | 6B   | 13  | 41    | .<ÅVkk.A  |       |
|      | 00000010  | 14      | ЗD        | 9F         | 05       | FF    | 43  | E9       | 27   | 85    | 22       | 3E   | 36   | BB   | 6A   | FO  | 43    | .=Ÿ.ÿCé'">6»jðC   |       |
|      | 00000020  | 9A      | D4        | B6         | 68       | 62    | 30  | 55       | 11   | 23    | 65       | 49   | AЗ   | 86   | DA   | 4D  | C8    | šÔ¶hb0U.#eI£†ÚMÈ  |       |
|      | 00000030  | A6      | OF        | FF         | BC       | 7A    | 66  | B6       | 9B   | 7B    | C6       | EC   | 88   | 62   | 41   | 96  | 36    | ¦.ÿ₩zf¶>{Æì^bA-6  |       |
|      | 00000040  | 33      | 73        | 1F         | 73       | CE    | 9D  | 3B       | 73   | EF    | 8F       | EF   | EF   | 30   | 43   | 81  | 13    | 3s.sÎ.;sï.ïïOC  |       |
|      | 00000050  | CC      | 71        | 89         | 12       | 5B    | 78  | 8D       | 29   | 3E    | 73       | AD   | C4   | A0   | 4B   | 7C  | E3    | Ìq‰.[x.)>s.Ä.K ã  |       |
|      | 00000060  | CA      | 1E        | <b>A</b> 5 | 33       | CE    | E6  | 9C       | 6F   | E1    | 2D       | E5   | 4B   | 4A   | 67   | 9C  | 17    | Ê.¥3Îæœoá-åKJgœ.  |       |
|      | 00000070  | 9C      | B7        | 70         | OF       | F7    | F9  | DD       | C6   | 2D    | 7C       | C0   | 01   | 5E   | 50   | FF  | ЗD    | œ·p.÷ùÝÆ−∣Å.^Pÿ=  |       |
|      | 00000080  | 8E      | F1        | 12         | AF       | DO    | 45  | 87       | BF   | C7    | E8       | F3   | Β7   | 4B   | D9   | 21  | 06    | Źñ. ĐE‡¿Çèó KÚ!.  |       |
|      | 00000090  | 94      | 8E        | 31         | A2       | ED    | 27  | 7A       | BC   | 44    | 4E       | 5F   | 53   | AE   | F4   | E9  | 6F    | "Z1¢í'z≒DN_S®ôéo  |       |
|      | 0A000000  | C2      | F1        | 9C         | 9E       | 2B    | D9  | 18       | BF   | 22    | 1B       | ΕO   | 88   | 9A   | 5D   | 9C  | 53    | Añœž+U.¿".à^š]œS  |       |
|      | 000000B0  | CF      | 59        | 15         | F4       | 10    | A2  | 71       | 9E   | 2F    | E8       | E7   | CO   | FB   | 59   | E1  | A3    | IY.ô.¢qž/èçAûYá£  |       |
|      | 00000000  | 47      | D5        | A6         | 56       | 8E    | AF  | B4       | 9B   | E2    | 29       | ED   | E7   | 38   | E3   | 57  | A2    | GO¦VZ ´→ä)iç8ä₩¢  |       |
|      | 00000D0   | C7      | 3D        | 9D         | 9F       | 09    | FD  | 74       | F8   | BF    | 44       | 18   | 43   | AE   | 9D   | 11  | E7    | Ç=.Y.ýtø¿D.C®ç  |       |
|      | 000000E0  | 09      | AE        | 88         | 29       | E7    | CC  | ED       | D2   | C6    | 18       | 4A   | 10   | EF   | 1E   | D7  | 56    | .00°)ÇI10ALJ.1.×V   |       |
|      | 00000020  | FC OC   | 1B        | 19         | D9       | 85    | 4/  | 30       | 15   | 12    | 82       | 63   | 17   | 33   | 17   | AS  | E9    | u.u∪  |       |
|      | 00000100  | 00      | 72        |            | ED<br>D2 | 70    | 10  | 1A<br>66 | 51   | 50    | AS<br>EA | 70   | 20   | E 9  | 25   | 70  | 49    | tovipotq;a.ti   |       |
|      | 00000110  | 30      | /J<br>1 ह | 87         | 93       | 63    | DA  | 26       | C7   | 03    | 53       | 01   | 67   | 74   | C4   | BD  | 73    | / .fclísří álatike  |       |
|      | 00000120  | 50      | 96        | 58         | 78       | 10    | OF  | 79       | 25   | 37    | 14       | 70   | 53   | FΔ   | CF   | 60  | 9B    | $\hat{\Pi} = X \mathbf{y}$ , $\nabla \mathbf{y} \geq \nabla \mathbf{y} \in \mathbf{A}^{2S}$ |       |
|      | 00000140  | 71      | 1E        | 4 A        | 54       | 42    | 66  | 25       | E5   | CF    | FO       | 85   | FB   | 5D   | E1   | OE  | 32    | α.JTBf%åÏð ûlá.2  |       |
|      | 00000150  | DC      | 65        | 04         | 13       | 30    | C2  | 8E       | 3F   | F3    | 10       | Δ4   | 78   | 2E   | E3   | 5E  | E3    | Üe<ÂŽ?ó.∦x.ã^ã  |       |
|      | 00000160  | 38      | 13        | FD         | 84       | D6    | 66  | FB       | 64   | 3D    | CE       | FO   | 70   | 3D   | 4E   | 99  | 53    | 8.ý"Öfûd=Îðp=N™S  |       |
|      | 00000170  | A6      | 63        | 7B         | 65       | 62    | 9B  | EO       | 41   | 44    | C7       | F4   | 5D   | 56   | D6   | 7E  | 5A    | c{eb>àADCô]VÖ~Z   |       |
|      | 00000180  | 32      | 4E        | 61         | FB       | A6    | 3C  | D1       | 5A   | 27    | 09       | D6   | 0D   | E7   | D8   | 67  | 51    | 2Naû¦<ÑZ'.Ö.çØgQ  | ~     |
| Off  | fset: 0   |         | В         | lock:      | 0-9      |       |     |          |      |       |          | Le   | ngth | : A  |      |     |       | Overwrite   |       |

www.csnc.de

### Open Research

Analysis of extracted information



### While others are not ...

| 🎍 l 🗋 🚇 🜩 l                         | Manifests   | - 🗆 🗡     |  |  |  |  |  |  |  |
|-------------------------------------|---|-----------|--|--|--|--|--|--|--|
| File Home Share View                |   | ~ Ø       |  |  |  |  |  |  |  |
| ( → ↑ ) + From SD card +            | Windows > system32 > Manifests v C Search Mar   | nifests 🔎 |  |  |  |  |  |  |  |
| Name                                | AccountsManagerPackMan.xml - Notepad  | - 0 ×     |  |  |  |  |  |  |  |
| AboutPackMan.xml                    | File Edit Format View Help  |           |  |  |  |  |  |  |  |
| AccessibilityPackMan.xml            | xml version="1.0" encoding="utf-8"?   | ~         |  |  |  |  |  |  |  |
| AccessoriesPackMan.xml              | AccessoriesPackMan.xml  |           |  |  |  |  |  |  |  |
| AccountsManagerPackMan.xml          | Copyright (c) Microsoft Corporation. All rights reserved.   |           |  |  |  |  |  |  |  |
| ActionUriHostManifest.xml           | >   |           |  |  |  |  |  |  |  |
| AdvertisingIdPackMan.xml            | <pre></pre>   |           |  |  |  |  |  |  |  |
| AgeOutPackMan.xml                   | Title=" $\Delta c_{count}$ SettingsRes dll _24001"  |           |  |  |  |  |  |  |  |
| AlarmsPackMan.xml                   | Version="1.0"   |           |  |  |  |  |  |  |  |
| APMUXPackMan.xml                    | Genre=""  |           |  |  |  |  |  |  |  |
| AppCornerPackMan.xml                | CornerPackMan.xml ProductID="{5B04B775-356B-4AA0-AAF8-6491FFEA5616}"  |           |  |  |  |  |  |  |  |
| AppResolverUI.xml                   | DisplayOnAppList="false"  |           |  |  |  |  |  |  |  |
| ARLensManifest.xml                  | SingleInstanceHost="true">  |           |  |  |  |  |  |  |  |
| AuthHostMsa.xml                     | <pre><iconpath xmins="">res://UIXMODIleAssets{Screenkesolution}:allapp.email<br/></iconpath></pre>  | .png      |  |  |  |  |  |  |  |
| AuthHostWabA.xml                    | <pre><!--/mageParams--></pre>   | ageracity |  |  |  |  |  |  |  |
| AuthHostWabB.xml                    | <tasks xmlns=""></tasks>  |           |  |  |  |  |  |  |  |
| AuthHostWabC.xml                    | <pre><defaulttask <="" activationpolicy="Replace" name="_default" pre=""></defaulttask></pre>   |           |  |  |  |  |  |  |  |
| AuthHostWabEnterprise.xml           | NavigationPage="res://AccountSettings!AccountsPage.uix#AccountsPage   | "/>       |  |  |  |  |  |  |  |
| AuthHostWabSSO.xml                  | <extendedtask activationpolicy="Replace" name="USW"></extendedtask>   |           |  |  |  |  |  |  |  |
| AuthHostWabSSOEnterprise.xml        | <pre><extendedtask activationpolicy="Replace" name="CreateAccount"></extendedtask> <extendedtask activationpolicy="Replace" name="ShowSettings"></extendedtask></pre> |           |  |  |  |  |  |  |  |
| BatteryUXPackMan.xml                |   |           |  |  |  |  |  |  |  |
| BingConfigurationManifest.xml       | <tokens xmlns=""></tokens>  |           |  |  |  |  |  |  |  |
| BingSuggestsHighlightsManifest.xml  | <primarytoken <="" td="" tokenid="Default"><td></td></primarytoken>   |           |  |  |  |  |  |  |  |
| □ D:==:)A/=1!=====:D==:I:A A======1 |   | *         |  |  |  |  |  |  |  |
| 122 items 1 item selected 1.37 KB   | <   | >         |  |  |  |  |  |  |  |



### Introduction

### Windows Aspects

- Windows Environment
- ✦ Attack Surface
- **Breaking Out**

### **Mobile Aspects**

Sandboxing & Encryption

### Findings

- ✤ MDM Integration
- Wi-Fi Sense
- Low Level Storage API +

### Conclusion



### Windows Phone 8.1

- ✤ Is more similar to iOS and Android than to a Windows desktop
- ✤ Is based on secure and proven good security technologies
- ✤ Is a first step into a more mature Windows 10 ecosystem
- ✤ Is as business ready as your current MDM solution is

## Open discussion







### © Compass Security Deutschland GmbH

Thank you!

www.csnc.de

Thank you for

your attention!



### Contact

#### **Compass Security Deutschland GmbH**

Tauentzienstr. 18 10789 Berlin Germany

team@csnc.de | www.csnc.de | +49 30 21 00 253-0

Secure File Exchange: www.filebox-solution.com

# PGP-Fingerprint:

