



ERNW
providing security.



Bundesamt
für Sicherheit in der
Informationstechnik

The Anatomy of Windows Telemetry

Dominik Phillips, Aleksandar Milenkoski, Maximilian Winkler

Agenda

Introduction

Analysis

- Architecture of Windows Telemetry

- Data sources

- Network interface

- Disabling and reducing Windows Telemetry

- Final remarks

Introduction

The German Federal Office for Information Security

Bundesamt für Sicherheit in der Informationstechnik (BSI)

The national cyber security authority in Germany

Mission: Improve IT security for the government, industry, and citizens

Staff (2018): 940



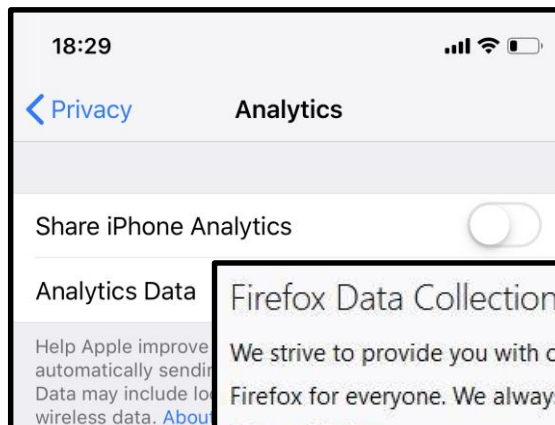
Telemetry

Telemetry is everywhere

Is the trend really your friend?

The positives:

- (Device) health monitoring
- Threat analysis
- Industry automation
- ...



Firefox Data Collection and Use

We strive to provide you with choices and collect only what we need Firefox for everyone. We always ask permission before receiving pe

Privacy Notice

☒ Allow Firefox to send technical and interaction data to Mozilla

Diagnostics & feedback

Diagnostic data

Choose how much data you send to Microsoft. Select [Learn more](#) for info on this setting, how Windows Defender SmartScreen works, and the related data transfers and uses.

- ☒ Basic: Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic

Telemetry (cont.)

The negatives:

- My data may be shared with someone I don't know/trust
- My behavior is being tracked and this information can be misused
- Sensitive or confidential information of my organization may leak
- Sensitive data on my system may leak
- . . .

Telemetry (cont.)

Why is telemetry relevant to the BSI?

Confidentiality

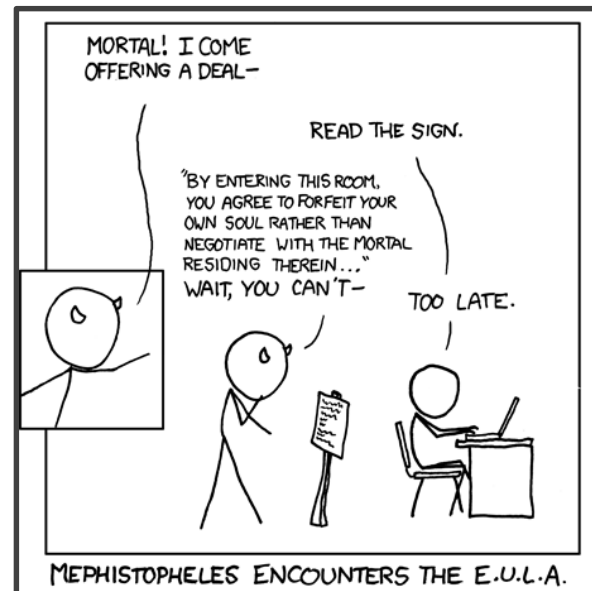
Data transmissions

Integrity

Remote access

User control

Who controls telemetry behavior?



©xkcd

Telemetry (cont.)

Why is Windows 10 Telemetry especially relevant to the BSI?

Popularity and timeliness

Windows (desktop) has 90% market share
End of support for Windows 7 in less than one year

Windows 10
Build 1607, 64-bit
Long Term Service Branch

Relevance

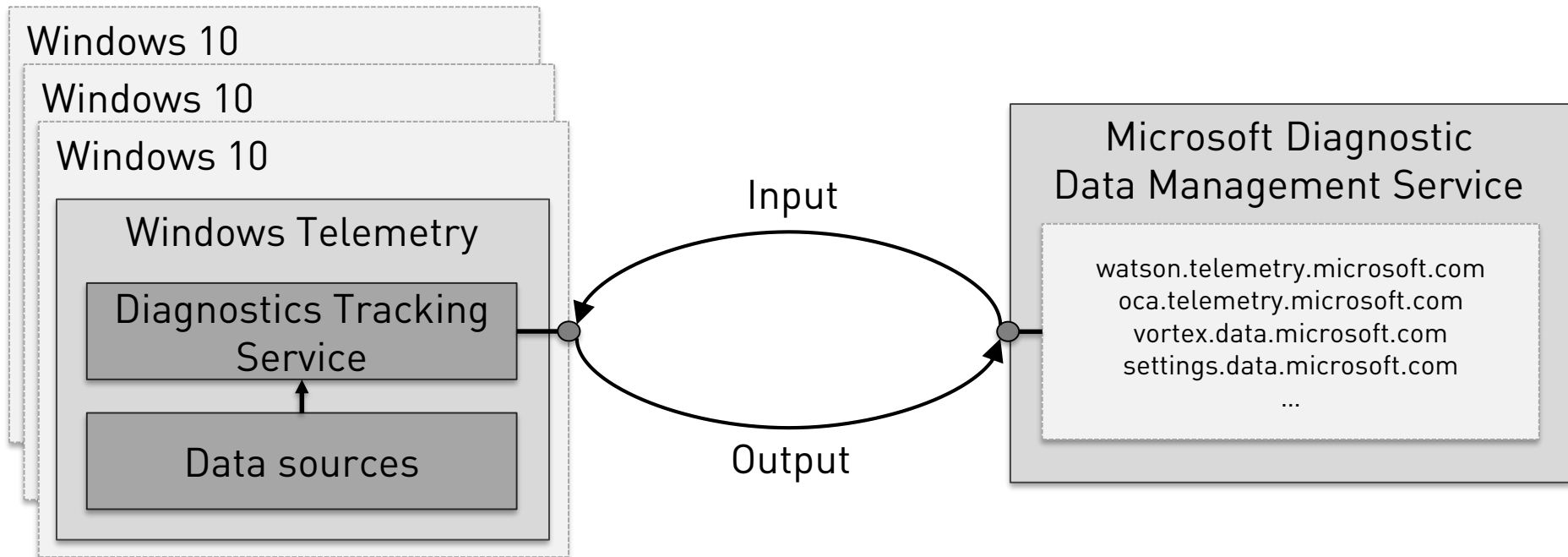
Windows 10 is set to be the OS for the new federal government client



Analysis



Windows Telemetry: Architecture



Diagnostics Tracking Service

Official name: Connected User Experiences and Telemetry

Hosted in svchost.exe: diagtrack.dll, service group: utcsvc

Tasks:

- Data collection and storage
- Network interface to the Microsoft Diagnostic Data Management Service
 - Bi-directional
 - Input: Control of service behavior
 - Output: Data distribution

Data sources

Primary data source: Event tracing for Windows (ETW)

- Data is logged during
 - system boot and shut-down
 - system run-time

Secondary data source

- Executables and API functions

Primary data source: Event Tracing for Windows (ETW)

ETW components

- Data collection points
 - Software entities
- Data management units
 - System entities for receiving and storing data
- Data storage
 - Software-entity (real-time feed) or file
- Controller
 - Maps data collection points to data management units

ETW: Data collection points

Direct data logging

- Instrumentation

Indirect data logging

- Usage of instrumented Windows facilities
 - Example: The Windows API, syscalls

```
EventRegister( ProviderId, [...], RegHandle );  
  
EnableTraceEx( ProviderId, [...] );  
  
EventWriteEx( RegHandle, [...] );
```

Windows is heavily instrumented

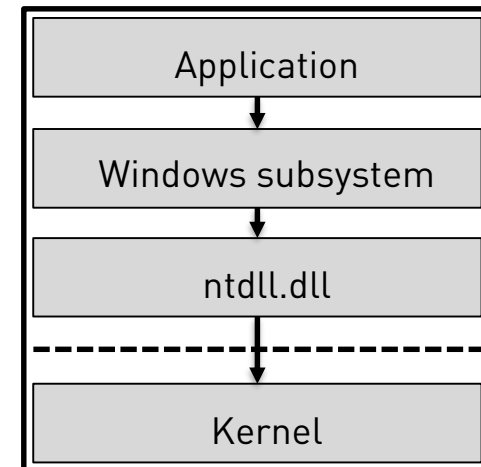
ETW: Data collection points

Direct data logging

- Instrumentation

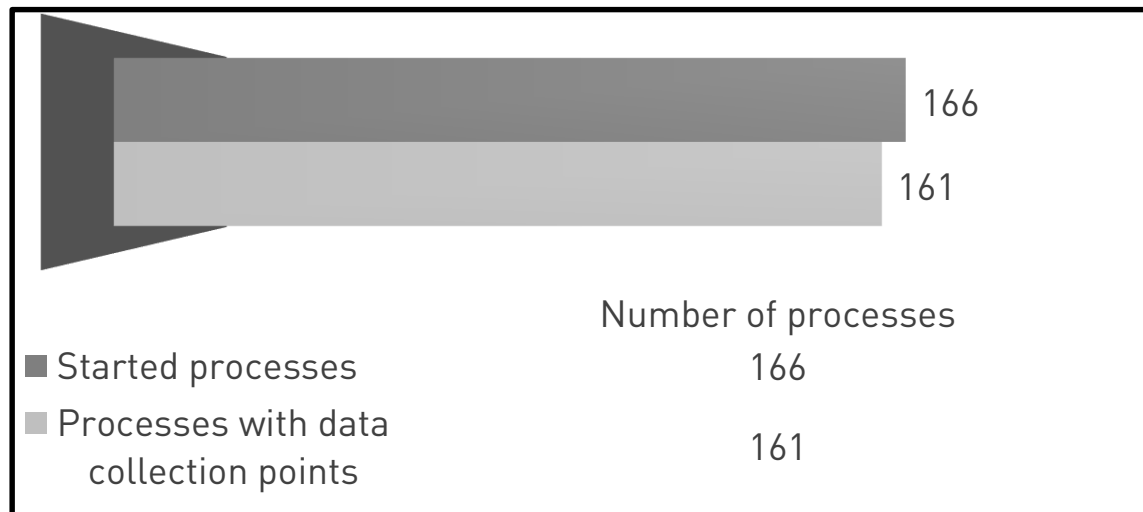
Indirect data logging

- Usage of instrumented Windows facilities
 - Example: The Windows API, syscalls

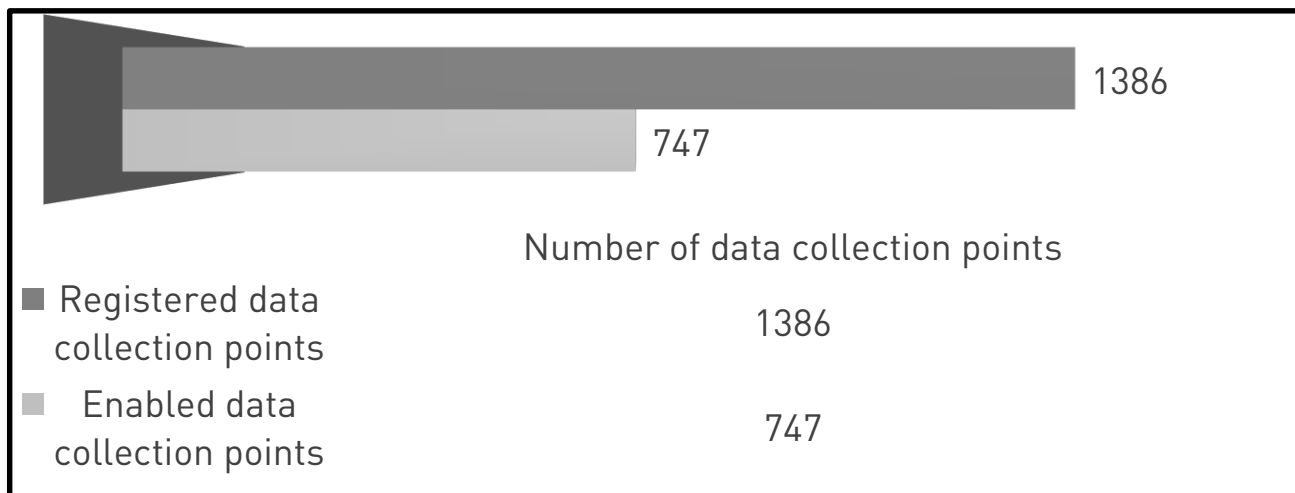


Windows is heavily instrumented

Data collection points: System integration



Data collection points: System integration



Data collection points: Data content

Developers decide what data is logged

Data is structured into event records

Event record

Record metadata

Timestamp
Event name
Process name
...

Record data

Strings
Byte arrays
Memory addresses
...

Data collection points: Data content (cont.)

Fid_URB_TransferData								ASCII
0	0	0	0	64	0	...	==>	1
0	0	0	0	128	0	...	==>	2
0	0	0	0	0	1	...	==>	3
0	0	0	0	0	2	...	==>	4
0	16	0	0	0	0	...	==>	a
0	32	0	0	0	0	...	==>	b
0	64	0	0	0	0	...	==>	c
0	128	0	0	0	0	...	==>	d

MessageNumber	Timestamp ▲	TimeElapsed	Module	Summary	Fid_URB_TransferData
759	2018-10-22T16:57:46.8098402	64,5271016	UsbSpec	Interrupt In Transfer	[0,0,0,0,64,0,0,0,0,0,0,0,0,0,0]
769	2018-10-22T16:58:51.3370071	9,0408098	UsbSpec	Interrupt In Transfer	[0,0,0,0,128,0,0,0,0,0,0,0,0,0,0]
777	2018-10-22T16:59:00.3778461	5,6351083	UsbSpec	Interrupt In Transfer	[0,0,0,0,0,1,0,0,0,0,0,0,0,0,0]
785	2018-10-22T16:59:06.0130207	6,0978893	UsbSpec	Interrupt In Transfer	[0,0,0,0,0,2,0,0,0,0,0,0,0,0,0]
793	2018-10-22T16:59:12.1109876	5,3458850	UsbSpec	Interrupt In Transfer	[0,16,0,0,0,0,0,0,0,0,0,0,0,0,0]
801	2018-10-22T16:59:17.4569184	6,0849504	UsbSpec	Interrupt In Transfer	[0,32,0,0,0,0,0,0,0,0,0,0,0,0,0]
809	2018-10-22T16:59:23.5419386	7,9648304	UsbSpec	Interrupt In Transfer	[0,64,0,0,0,0,0,0,0,0,0,0,0,0,0]
817	2018-10-22T16:59:31.5068067	7,0771646	UsbSpec	Interrupt In Transfer	[0,128,0,0,0,0,0,0,0,0,0,0,0,0,0]

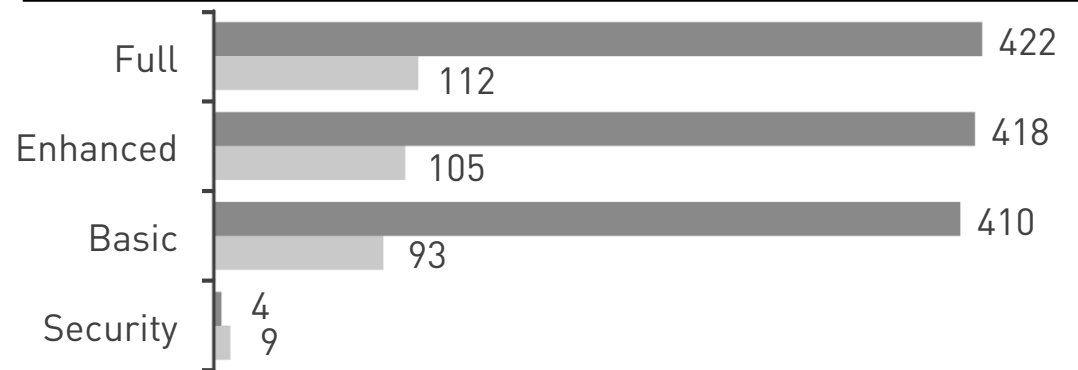
Secondary data source: Executables and API functions

```
Microsoft::Diagnostics::CGetProcessDumpAction::DumpProcess( [...] )  
{  
    [...]  
    if ( Wow64Process ) {  
        [...]  
        CreateProcessW(  
            [...],  
            "%windir%\\SysWow64\\dtdump.exe [...]",  
            [...]  
        );  
        [...]  
    }  
    [...]  
}
```

```
Microsoft::Diagnostics::CGetProcessDumpAction::DumpProcess( [...] )  
{  
    [...]  
    if ( NotWow64Process ) {  
        [...]  
        hModule = LoadLibraryExW(L"dbghelp.dll", [...]);  
        [...]  
        fProc = GetProcAddress(hModule, "MiniDumpWriteDump");  
        [...]  
    }  
    [...]  
}
```


Primary data source: Data collection management

Telemetry levels: Groups of data collection points



	Security	Basic	Enhanced	Full
■ Data collection points (at run-time)	4	410	418	422
■ Data collection points (at boot)	9	93	105	112

Primary data source: Data collection management (cont.)

Configuration file for managing data collection points

- %ProgramData%\Microsoft\Diagnosis\DownloadedSettings\utc.app.json
- Mapping between levels and data collection points
- Controlled by Microsoft

```
{
  "queryUrl": "/settings/v3.0/utc/app",
  "settings": {
    [...]
    "UTC:::VORTEXENDPOINT.WINDOWSTELEMETRY.UK": "https://v10.vortex-win.data.microsoft.com/collect/v1|https://vortex-win.data.microsoft.com",
    [...]
    "UTC:::GROUPDEFINITION.OFFICE": "8DBEEE55-EAB8-41BE-988E-B1FAE0397155",
    [...]
    "UTC:::ONESETTINGSVERSION": "3",
    [...]
    "UTC:::PROVIDERDEFINITION.KERNELPROCESS": "2839ff94-8f12-4e1b-82e3-af7af77a450f",
    [...]
  }
}
```

Secondary data source: Data collection management

Execution controlled by Microsoft

- %ProgramData%\Microsoft\Diagnosis\DownloadedScenarios\WINDOWS.DIAGNOSTICS.xml
- Execution logic of Microsoft unknown
 - Execution may be triggered based on data from the primary data source

```
[...]
<action actionname="H_WpSystem_ACLS" ignorefailure="1">
  <runexewithargsaction>
    <exename>%windir%\system32\icacls.exe</exename>
    <commandline>H:\WpSystem</commandline>
    <maximumruntime>60000</maximumruntime>
  </runexewithargsaction>
</action>
[...]
```

Data sources and the Diagnostics Tracking Service

Data collected during system boot and shut-down

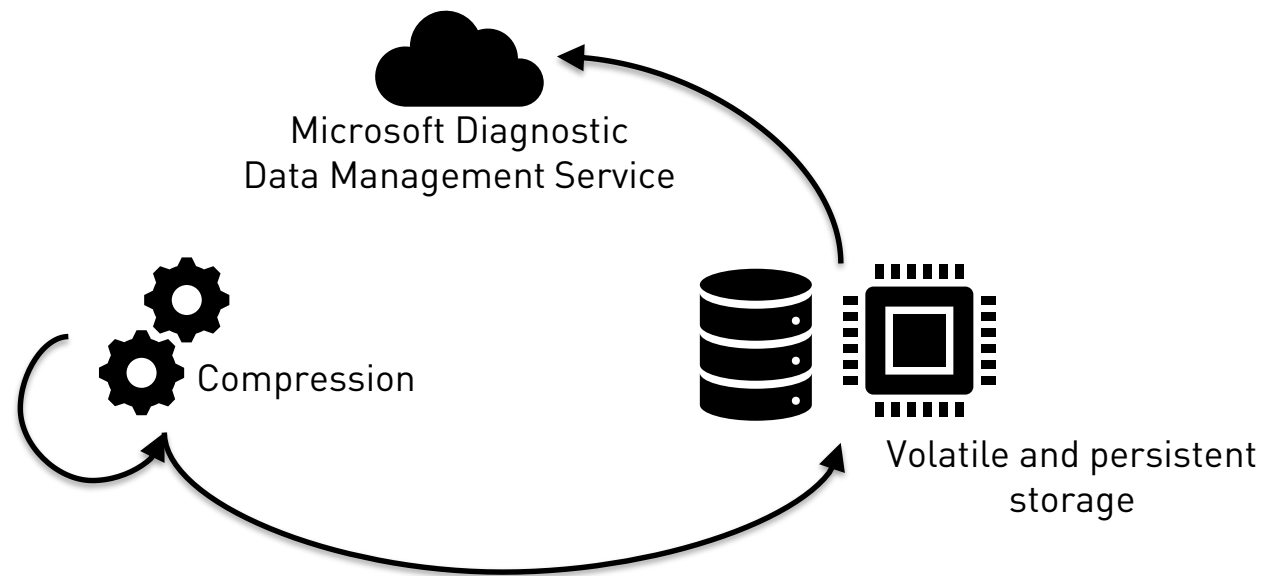
- % ProgramData%\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-Diagtrack-Listener.etl
- % ProgramData%\Microsoft \Diagnosis\ETLLogs\ShutdownLogger\AutoLogger-Diagtrack-Listener.etl
- Read and deleted at each system boot

Data collected during system run-time

- Delivered directly to the Diagnostics Tracking Service

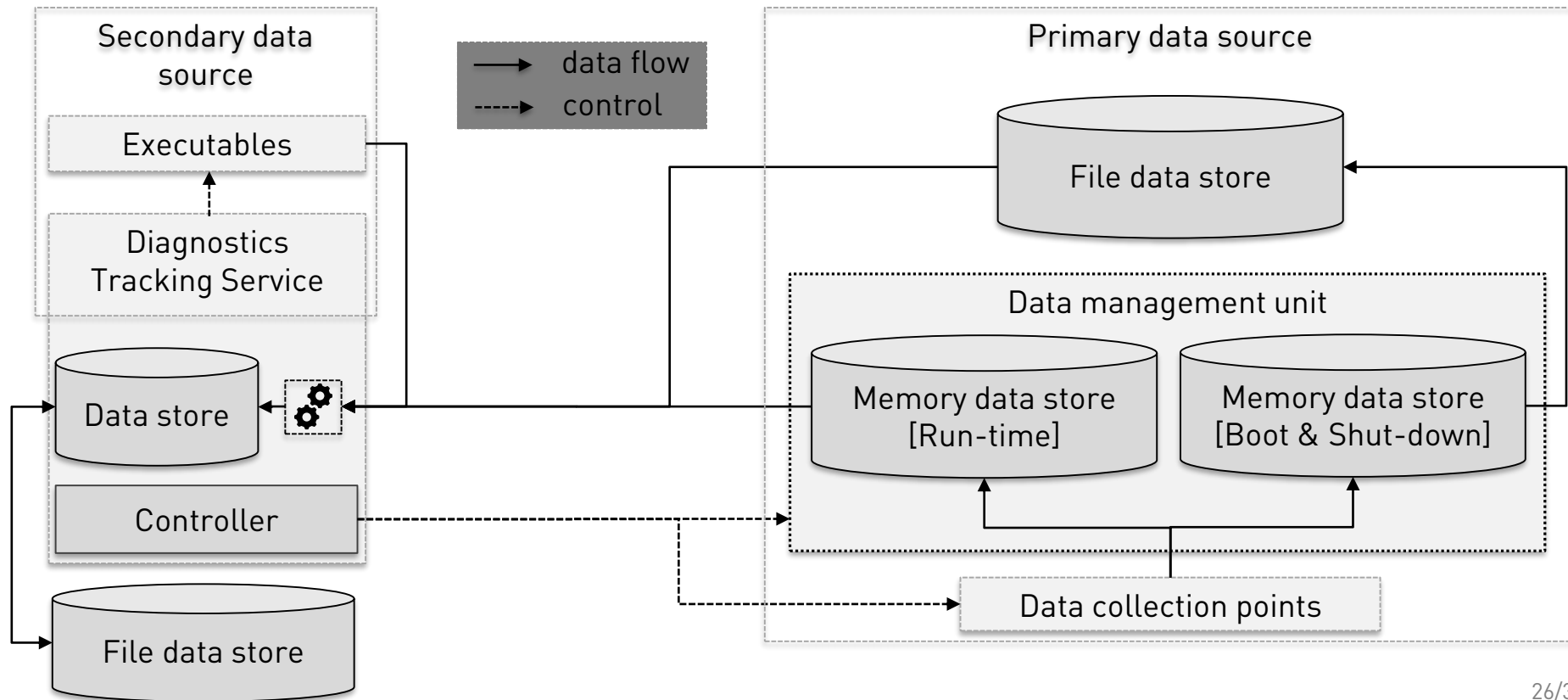
Data sources and the Diagnostics Tracking Service (cont.)

The Diagnostics Tracking Service processes collected data



```
    "loc": {  
      "timeZone": "+01:00"  
    },  
    "data": {  
      [...]  
      "SignatureParameter01": "appcrash.exe",  
      "SignatureParameter02": "0.0.0.0",  
      "SignatureParameter03": "5be95e52",  
      "SignatureParameter04": "appcrash.exe",  
      "SignatureParameter05": "0.0.0.0",  
      "SignatureParameter06": "5be95e52",  
      "SignatureParameter07": "00001015",  
      "SignatureParameter08": "c0000409",  
      "SignatureParameter09": "00000015",  
      [...]  
    }  
  }
```

Data sources and the Diagnostics Tracking Service



Diagnostics Tracking Service: Network interface

TLS-protected network interface

- HTTP messages (JSON)
- Client-triggered communication
 - Data upload – output: Data distribution
 - Data download – input: Control of service behavior

```

0000 7b 22 71 75 65 72 79 55 72 6c 22 3a 22 2f 73 65 {"queryUrl":"/se
0010 74 74 69 6e 67 73 2f 76 33 2e 30 2f 75 74 63 2f ttings/v3.0/utc/
0020 61 70 70 22 2c 22 73 65 74 74 69 6e 67 73 22 3a app","settings":
0030 7b 22 55 54 43 3a 3a 3a 45 4e 44 50 4f 49 4e 54 {"UTC::ENDPOINT
0040 2e 54 45 4c 45 4d 45 54 52 59 2e 41 53 4d 2d 57 .TELEMETRY.ASM-W
0050 49 4e 44 4f 57 53 53 51 22 3a 22 74 65 6c 65 6d INDOSSQ":"telem
[...]
ced0 46 49 43 41 54 49 4f 4e 52 45 47 49 53 54 52 41 FICATIONREGISTRA
cee0 54 49 4f 4e 55 52 49 22 3a 22 68 74 74 70 73 3a TIONURI":"https:
cef0 2f 2f 73 65 74 74 69 6e 67 73 2d 77 69 6e 2e 64 //settings-win.d
cf00 61 74 61 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f ata.microsoft.co
cf10 6d 2f 72 65 67 69 73 74 65 72 63 68 61 6e 6e 65 m/registerchanne
cf20 6c 2f 76 31 2e 30 2f 22 7d 7d l/v1.0/"}
    
```

Diagnostics Tracking Service: Network interface (cont.)

Implementation based on the WinHTTP API

- CheckCertForMicrosoftRoot
- SendRequestWithRetry

```
[...]
hSession = WinHttpOpen(L"MSDW", [...]);
*(_QWORD *)hInternet = hSession;
[...]

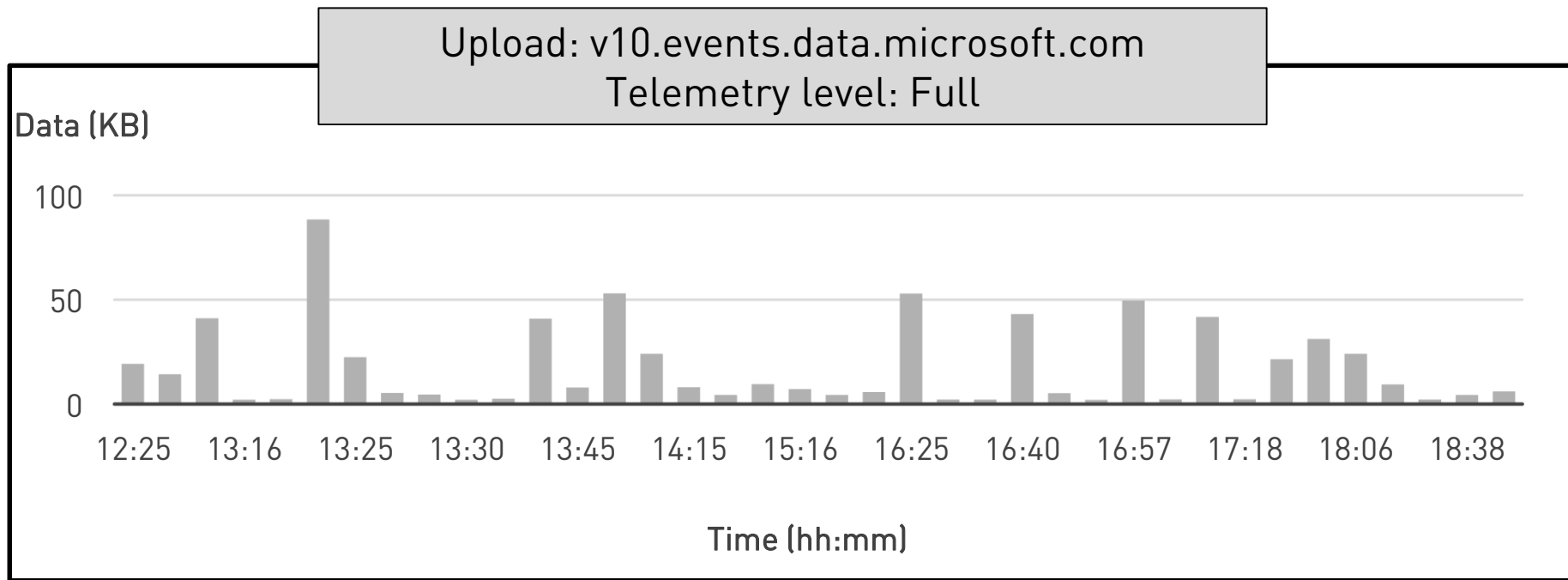
hConnect = WinHttpConnect(hSession, pServerName, nServerPort, [...]);
*((_QWORD *)hInternet + 1) = hConnect;
[...]

hRequest = WinHttpOpenRequest(hConnect, pVerb, pObjectName, [...]);
*((_QWORD *)hInternet + 2) = hRequest;
[...]

returnCode = CHttpRequest::SendRequestWithRetry(hInternet, [...]);
[...]

if ( returnCode >= 0 )
{
    if ( !(FlagsBitMask & 0x40) )
    {
        goto LABEL_113;
    }
    [...]
    returnCode = CHttpRequest::CheckCertForMicrosoftRoot(hRequest);
    [...]
}
```

Diagnostics Tracking Service: Network interface (cont.)



Diagnostics Tracking Service: Network interface (cont.)

Download: settings-win.data.microsoft.com
Telemetry level: Full

Data (KB)

40

20

0

12:26 12:56 13:26 13:57 14:42 14:57 15:27 15:57 16:27 16:57 17:27 17:42 18:27 18:57

Time (hh:mm)

Diagnostics Tracking Service: Network interface (cont.)

Hostname	Direction	Location
geo.settings-win.data.microsoft.com db5-eap.settings-win.data.microsoft.com settings-win.data.microsoft.com ...	Download	Ireland, Dublin
db5.vortex.data.microsoft.com v10-win.vortex.data.microsoft.com ...	Upload	Ireland, Dublin
us.vortex-win.data.microsoft.com	Upload	Virginia (US), Boston
eu.vortex-win.data.microsoft.com	Upload	Netherlands, Amsterdam
vortex-win-sandbox.data.microsoft.com	Upload	California (US), Los Angeles
alpha.telemetry.microsoft.com	Upload	California (US), Los Angeles
oca.telemetry.microsoft.com	Upload	Wyoming (US), Cheyenne

Disabling and reducing Windows Telemetry

Deactivation of data
collection points

Restriction of network
communication

Service deactivation

Isolation of Windows 10

Configuring a less intensive Telemetry level
Removing or deactivating software

Blocking communication with the
Microsoft Diagnostic Data Management Service

Deactivating the Diagnostics Tracking Service

Isolating from the Internet

Disabling and reducing Windows Telemetry (cont.)

	Data transfer	Sustainability	Maintenance
Deactivation of data collection points	Reduced	Non-sustainable	High
Restriction of network communication	Disabled or reduced	Non-sustainable	Moderate
Service deactivation	Disabled	(Non-)sustainable	Low
Isolation of Windows 10	Disabled	Sustainable	Low

Final remarks

Final remarks: Windows Telemetry

Potentially any data may be extracted via data collection points

Confidentiality?

Highly dynamic behavior, controlled by Microsoft

User control? Giving up sovereignty?

Remotely triggered execution of executables and functions

Integrity?

No „zero exhaust“ setting

Transparency

- Some information about transmitted data
- No information about the Microsoft Diagnostic Data Management Service

Final remarks: Windows Telemetry

Potentially any data may be extracted via data collection points

Confidentiality?

Highly dynamic behavior, controlled by Microsoft

User control? Giving up sovereignty?

Remotely triggered execution of executables and functions

Integrity?

The federal government client is planned to be isolated from the Internet

No „zero exhaust“ setting

Transparency

- Some information about transmitted data
- No information about the Microsoft Diagnostic Data Management Service

Final remarks: Windows Telemetry (cont.)

Let's be fair

- Microsoft improved transparency
 - Public documentation of collected data
 - Diagnostic Data Viewer
- Concerns apply to all telemetry implementations – not only that by Microsoft

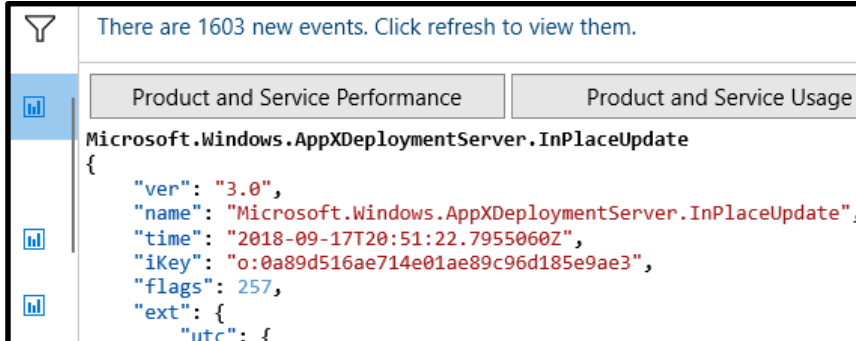
Account trace logging provider events

Microsoft.Windows.Mitigation.AccountTraceLoggingProvider.General

This event provides information about application properties to indicate the successful execution.

The following fields are available:

- AppMode Indicates the mode the app is being currently run around privileges.
- ExitCode Indicates the exit code of the app.
- Help Indicates if the app needs to be launched in the help mode.



There are 1603 new events. [Click refresh to view them.](#)

Product and Service Performance | Product and Service Usage

Microsoft.Windows.AppXDeploymentServer.InPlaceUpdate

```
{
  "ver": "3.0",
  "name": "Microsoft.Windows.AppXDeploymentServer.InPlaceUpdate",
  "time": "2018-09-17T20:51:22.7955060Z",
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "flags": 257,
  "ext": {
    "utc": {
```

Final remarks: Telemetry

The BSI rates telemetry as a potential risk for confidentiality and integrity

Disable telemetry if you don't need it

Vendors should provide a „zero exhaust“ setting

Future work

Frequent updates

- Establishment of a continuous analysis approach

Data richness

- Data visualization
- Data systematization
- Data interpretation

Secondary data source

- Analysis of capabilities
- Systematization of capabilities
- Analysis of execution conditions



Future study

Windows 10
Build 1809, 64-bit
Long Term Servicing Channel

```
Microsoft::Diagnostics::CGetKernelDumpAction::Execute( [...] )  
{  
    [...]  
    std::basic_string<[...]>(  
        [...],  
        L"Live kernel dumps are not currently available. This is a placeholder. Enjoy...");  
    [...]  
}
```

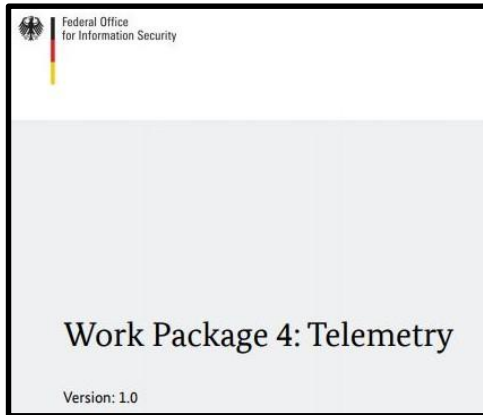
Thank you for your attention!

Questions?

Publications

<https://tinyurl.com/wtelem1>

<https://tinyurl.com/wtelem2>



Contact

Dominik Phillips

✉ dphillips@ernw.de

🐦 @0xpeanuts

Aleksandar Milenkoski

✉ amilenkoski@ernw.de

🐦 @milenkowski

Maximilian Winkler

✉ bsi@bsi.bund.de
