Bavarian Data Protection
Authority for the Private Sector

Windows 10 Investigation Report

Findings regarding Windows 10 Enterprise Version for data controllers in the private sector (September '17)

Introduction

This report contains information about our approach and current findings concerning the Microsoft Windows 10 Enterprise investigation. We, the Bavarian DPA for the private sector, decided to clarify the question, if the operating system Windows 10 can be used for data controllers in the private sector in a compliant form concerning data protection regulations.

For this purpose, we prepared a laboratory set-up for a technical analysis in our authority, which enables us to analyze data flows of any Operating System (OS) or device within our own test set-up in Ansbach, Germany. The aim of our investigation was to determine whether data flows of the operating system Windows 10 can be disabled by specific privacy settings and system configurations. As versions such as Home and Pro do not offer enough options to regulate outgoing information traffic, we decided to focus on the Enterprise Version of Windows 10. In our opinion, data controllers require transparency and control over the processing of personal data that is initiated also through the OS itself – otherwise serious violations against European data protection law threaten.

We are aware of the fact that already many different ways exist to limit or even prevent such data transmission, e.g. via the Windows Group Policies, the User Interface (UI), the MDM Policy, the Registry, the Windows Firewall or even the Command Line of the OS. In this investigation we tried to restrict the relevant data flows preferentially through changes in the Windows Group Policies.

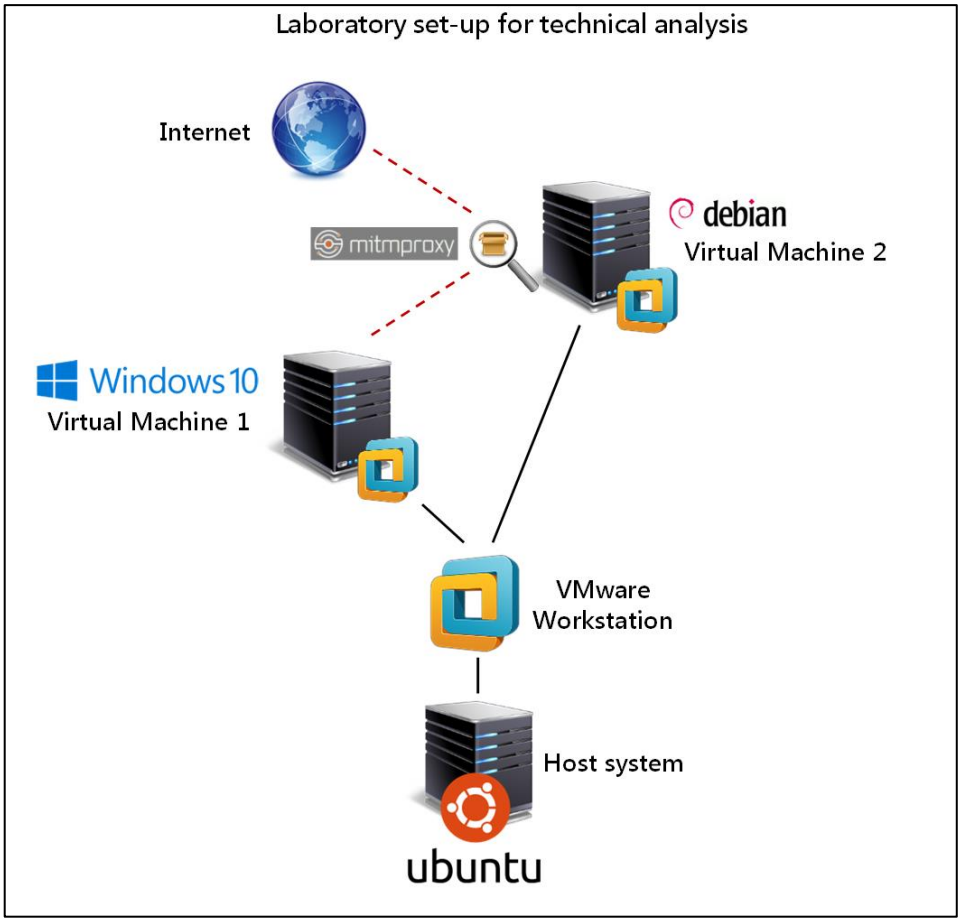
In our approach, a new installation of a Windows 10 Enterprise system was examined for its communication behavior in predefined use cases in short time intervals. Thus no monitoring took place over a longer period of time.

After completion of our first investigation in March 2017, a comprehensive update of Windows 10 was offered by Microsoft – the so-called "Creators Update". According to Microsoft, it has a positive effect on the possibilities for the Privacy Settings. For this reason, we decided to repeat the investigation with this newer version to the same extent and summarize our findings in a combined report.

I. Preparation and set-up

For Investigation in March 2017:

- Installation of Windows 10 Enterprise Evaluation – Version 1607 **Build 14393** (German Version) as Virtual Machine (Virtual Machine 1) in VMware Workstation Version 12 Pro (Version 12.1.1) on Host System Ubuntu
- Running Virtual Machine 1 and installing all available OS updates
- Installation of a further Virtual Machine with Debian 8.x 64bit and the tool mitmproxy (Virtual Machine 2) to analyze data traffic of Virtual Machine 1 inside of the laboratory set-up
- Installation of the mitmproxy-CA-certificate (SSL) in Virtual Machine 1 (to get an insight into encrypted TLS-connections)
- Saving a snapshot of Virtual Machine 1 as a rollback-point



For Investigation in May 2017:

- Installation of Windows 10 Enterprise Evaluation – Version 1703 **Build 15063 (Creators Update)** (English Version) as Virtual Machine (Virtual Machine 1) in VMware Workstation Version 12 Pro (Version 12.1.1) on Host System Ubuntu
- Remaining set-up as before

II. Investigation March 2017: Win10 Enterprise Version Build 14393

1. Scenario 1:
Disable data flows after OS start

The settings which we have chosen to prevent OS initiated data flows are listed below. Only the settings are listed that differ from the default configuration after first OS installation. The policies can be found in "*Computer Configuration\Administrative Templates*".

1.1 Settings

#	Directory	Name	Policy Setting Name	Setting
1	Windows Components	Application Compatibility appcompat.admx	Turn off Inventory Collector	enabled
2	Windows Components	Application Compatibility appcompat.admx	Turn off Application Telemetry	enabled
3	Windows Components	Application Compatibility appcompat.admx	Turn off Steps Recorder	enabled
4	System	User Profiles userprofiles.admx	System\User Profiles	enabled
5	Windows Components	App Package Deployment appxpackagemanager.admx	Allow a Windows app to share application data between users	disabled
6	Windows Components	Cloud Content cloudcontent.admx	Do not show Windows tips	enabled
7	Windows Components	Cloud Content cloudcontent.admx	Turn off Microsoft consumer experiences	enabled
8	Windows Components	Data Collection and Preview Builds datacollection.admx	Allow Telemetry	enabled: 0 (Security)
9	Windows Components	Data Collection and Preview Builds datacollection.admx	Do not show feedback notifications	enabled
10	Windows Components	Data Collection and Preview Builds datacollection.admx	Disable pre-release features or settings	enabled
11	Windows Components	Sync your settings settingsync.admx	Do not sync	enabled
12	Windows Components	Sync your settings settingsync.admx	Do not sync app settings	enabled
13	Windows Components	Sync your settings settingsync.admx	Do not sync Apps	enabled
14	Windows Components	Sync your settings settingsync.admx	Do not sync browser settings	enabled
15	Windows Components	Sync your settings settingsync.admx	Do not sync desktop personalization	enabled
16	Windows Components	Sync your settings settingsync.admx	Do not sync on metered connections	enabled
17	Windows Components	Sync your settings settingsync.admx	Do not sync passwords	enabled
18	Windows Com-	Sync your settings	Do not sync personalize	enabled

	ponents	settingsync.admx		
19	Windows Components	Sync your settings settingsync.admx	Do not sync start settings	enabled
20	Windows Components	Sync your settings settingsync.admx	Do not sync other Windows settings	enabled
21	Windows Components	Windows Defender Antivirus windowsdefender.admx	Turn off Windows Defender Antivirus	enabled
22	Windows Components	Endpoint Protection > Reporting windowsdefender.admx	Configure Watson events	disabled
23	Windows Components	Endpoint Protection > Real-time Protection windowsdefender.admx	Turn off real-time protection	enabled
24	Windows Components	Endpoint Protection > Real-time Protection windowsdefender.admx	Turn on behavior monitoring	disabled
25	Windows Components	Endpoint Protection > MAPS windowsdefender.admx	Send file samples when further analysis is required	enabled: (0x2) Never send
26	System	Internet Communication Management > Internet Communication settings icm.admx	Turn off Windows Error Reporting	enabled
27	System	Internet Communication Management > Internet Communication settings icm.admx	Turn off access to the Store	enabled
28	Windows Components	OneDrive skydrive.admx	Prevent the usage of OneDrive for file storage	enabled
29	Windows Components	Location and Sensors sensors.admx	Turn off location	enabled
30	Windows Components	Location and Sensors > Windows Location Provider locationprovideradm.admx	Turn off Windows Location Provider	enabled
31	Windows Components	Game Explorer gameexplorer.admx	Turn off game updates	enabled
32	Windows Components	Store windowsstore.admx	Disable all apps from Windows Store	enabled
33	Windows Components	Store windowsstore.admx	Turn off the Store application	enabled
34	Windows Components	Store windowsstore.admx	Turn off Automatic Download and Install of updates	enabled
35	Windows Components	Search search.admx	Allow Cortana	disabled
36	Windows Components	Search search.admx	Allow search and Cortana to use location	disabled
37	Windows Components	Search search.admx	Do not allow web search	enabled
38	Windows Components	Search search.admx	Don't search the web or display web results in Search	enabled
39	Windows Com-	Search	Set what information is shared in Search	enabled:

	ponents	search.admx		Anonymous info
40	Windows Components	Search search.admx	Allow indexing of encrypted files	disabled
41	Windows Components	Search search.admx	Allow Cortana above lock screen	disabled
42	Windows Components	Windows Update windowsupdate.admx	Configure Automatic Updates	enabled: 2 - Notify before downloading and installing any update
43	Windows Components	Windows Error Reporting errorreporting.admx	Automatically send memory dumps for OS-generated error reports	disabled
44	Windows Components	Windows Error Reporting > Consent errorreporting.admx	Configure Default consent	enabled: Always ask before sending data

1.2 Actions

- Restart of Virtual Machine 1 (Windows 10 Enterprise Version)
- Start monitoring through Virtual Machine 2 (mitmproxy)
- Open Windows Start Menu in Virtual Machine 1 (Click on Windows Start Button)
- Use search function and search exemplary for two keywords “gpedit” and “test”
- Stop Virtual Machine 1 (Windows 10 Enterprise Version)
- Stop monitoring through Virtual Machine 2 (mitmproxy)

1.3 Detected data flows

The results of the mitmproxy-analysis, i.e. the registered requests, are listed below.

#	IP	Domain *[+DNS Lookup]*	Request
1	104.98.143.57	**sway-cdn.com** *[a104-98-143-57.deploy.static .akamaitechnologies.com]*	/api/1.0/getTileUpdate(de-DE)
2	104.98.143.57	**sway-cdn.com** *[a104-98-143-57.deploy.static .akamaitechnologies.com]*	/api/1.0/getTileUpdate(de-DE)
3	23.201.167.27	**tile-service.weather.microsoft.com** *[a23-201-167-27.deploy.static .akamaitechnologies.com]*	/de-DE/livetile/preinstall?region=DE&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold
4	184.25.245.193	**cdn.content.prod.cms.msn.com** *[a184-25-245-193.deploy.static .akamaitechnologies.com]*	/singletile/summary/alias/experiencebyname/today?market=de-DE&tenant=amp&vertical=news
5	131.253.61.100	**login.live.com** *[-]*	/RST2.srf
6	104.104.201.9	**cdn.onenote.net** *[a104-104-201-9.deploy.static .akamaitechnologies.com]*	/livetile/?Language=de-DE
7	92.123.195.108	**img-s-msn-com.akamaized.net** *[a92-123-195-108.deploy .akamaitechnologies.com]*	/tenant/amp/entityid/AAnFiuZ.img?w=100&h=100&m=6&tilesize=medium&x=478&y=561&ms-scale=100&ms-contrast=standard

8	92.123.195.108	**img-s-msn-com.akamaized.net** *[a92-123-195-108.deploy .akamaitechnologies.com]*	/tenant/amp/entityid/AAnFiuZ.img?w=100&h=100&m=6&tilesize=medium&x=478&y=561&ms-scale=100&ms-contrast=standard
9	104.104.201.97	**geover-prod.do.dsp.mp.microsoft.com** *[a104-104-201-97.deploy.static .akamaitechnologies.com]*	/geoversion/?doClientVersion=10.0.14393.594&profile=16
10	64.4.54.116	**geo-prod.do.dsp.mp.microsoft.com** *[-]*	/geo/?doClientVersion=10.0.14393.594&profile=16
11	23.9.128.119	**kv401-prod.do.dsp.mp.microsoft.com** *[a23-9-128-119.deploy.static .akamaitechnologies.com]*	/all/?doClientVersion=10.0.14393.594&countryCode=DE&profile=16
12	104.68.216.8	**sway-cdn.com** *[a104-68-216-8.deploy.static .akamaitechnologies.com]*	/api/1.0/getTileUpdate(de-DE)
13	23.40.1.157	**tile-service.weather.microsoft.com** *[a23-40-1-157.deploy.static .akamaitechnologies.com]*	/de-DE/livetile/preinstall?region=DE&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold
14	104.92.107.200	**cdn.content.prod.cms.msn.com** *[a104-92-107-200.deploy.static .akamaitechnologies.com]*	/singletile/summary/alias/experiencebyname/today?market=de-DE&tenant=amp&vertical=news
15	104.104.201.9	**cdn.onenote.net** *[a104-104-201-9.deploy.static .akamaitechnologies.com]*	/livetile/?Language=de-DE
16	104.68.216.8	**sway-cdn.com** *[a104-68-216-8.deploy.stati c.akamaitechnologies.com]*	/api/1.0/getTileUpdate(de-DE)
17	207.46.194.33	**arc.msn.com** *[msnbot-207-46-194-33.search.msn.com]*	/v3/Delivery/Events/Impression
18	207.46.194.14	**g.live.com** *[msnbot-207-46-194-14.search.msn.com]*	/1rewlive5skydrive/ODSUProduction
19	104.92.88.173	**oneclient.sfx.ms** *[a104-92-88-173.deploy.static .akamaitechnologies.com]*	/Win/Prod/17.3.6743.1212/update100.xml
20	207.46.194.14	**g.live.com** *[msnbot-207-46-194-14.search.msn.com]*	/1rewlive5skydrive/ODSUProduction
21	104.92.88.173	**oneclient.sfx.ms** *[a104-92-88-173.deploy.static .akamaitechnologies.com]*	/Win/Prod/17.3.6743.1212/update100.xml
22	40.127.129.109	**mobile.pipe.aria.microsoft.com** *[-]*	/Collector/3.0/
23	40.127.129.109	**mobile.pipe.aria.microsoft.com** *[-]*	/Collector/3.0/
24	40.127.129.109	**mobile.pipe.aria.microsoft.com** *[-]*	/Collector/3.0/

1.4 Review

Our settings in the Windows Group Policy did not prevent all data transmission of the Windows 10 Enterprise Version. After starting the OS, using the Windows Start Menu, and searching for two keywords, several requests by the OS were registered. We noticed that most of these requests were initiated by the Windows Start Menu configuration (e.g. tiles for Sway, Live, OneNote, and Weather), so we decided to eliminate these data transmission behavior in the next use case.

2. Scenario 2:
Disable data flows after usage of Windows Start Menu

2.1 Settings (in addition to the previous settings)

Further setting in the Policy in *Computer Configuration\Administrative Templates*:

Directory	Name	Policy Setting Name	Setting
Start Menu and Taskbar startmenu.admx	-	Start Layout	enabled: Layout file in C:\temp\StartLayout.xml

The start menu has been modified by us with a new StartLayout.xml-file so that no more "live tiles" were integrated. All apps included by default were removed in this file - completely. However, we also deactivated the tile notifications in the user configuration of the Windows Group Policy in *User\Administrative Templates*:

Directory	Name	Policy Setting Name	Setting
Start Menu and Taskbar	Notifications wpn.admx	Turn off tile notifications	enabled

2.2 Actions

- Restart of Virtual Machine 1 (Windows 10 Enterprise Version)
- Start monitoring through Virtual Machine 2 (mitmproxy)
- Open Windows Start Menu in Virtual Machine 1 (Click on Windows Start Button)
- Use search function and search exemplary for two keywords "gpedit" and "test"
- Open Microsoft Edge without entering a URL
- Open Windows File Explorer and unzip a zip-file
- Stop Virtual Machine 1 (Windows 10 Enterprise Version)
- Stop monitoring through Virtual Machine 2 (mitmproxy)

2.3 Detected data flows

#	IP	Domain *[+DNS Lookup]*	Request
1	204.79.197.203	**www.msn.com** *[a-0003.a-msedge.net]*	/spartan/dhp?locale=de-DE&market=DE&enableregulatorypsm=0
2	92.123.195.105	**static-spartan-neu-s-msn-**	/spartan/de-de/_sc/css/e6001bca-

		com.akamaized.net *[a92-123-195-105.deploy .akamaitechnologies.com]*	f7f02e9e/direction=ltr.locales=de-de.themes=start.dpi=resolution1x/4d-67fcea-68ddb2ab/51-e8ede3-a7f23727/c9-41b710-6f437223/dc-3ca27f-fd6c119a/ed-2be182-9cb72fd7/44-2e8c9f-a2b67bb1/97-8e4310-93ac2788/ef-f70743-68ddb2ab/a7-5134f8-dbc6220a/b9-c39e45-1e7f64cd/63-1b5078-4a73e1fe?ver=2.0.6267.39773&fdhead=muidflt14cf
3	207.46.194.10	**c.msn.com** *[msnbot-207-46-194-10.search .msn.com]*	/c.gif?udc=true&rid=07366c10c44443848473fc20c4ad778e&rnd=1488383823270&rf=&tp=https%3A%2F%2Fwww.msn.com%2Fspartan%2Fdhp%3Flocale%3Dde-DE%26market%3DDE%26enableregulatorypsm%3D0%26ocid%3Dspartandhp&scr=1440x900&di=108&lng=de-de&cv.product=spartan&pn=dhp&activityId=07366c10c44443848473fc20c4ad778e&d.dgk=tmx.pc.edge.spartan.serviceui&d.imd=0&st.dpt=dhp&st.sdpt=&subcvs=homepage
4	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?evt=impr&js=1&rid=07366c10c44443848473fc20c4ad778e&cts=1488383823271&clid=3CC1108501826E2A2A8D1AB300E46F9D&rf=&cu=https%3A%2F%2Fwww.msn.com%2Fspartan%2Fdhp%3Flocale%3Dde-DE%26market%3DDE%26enableregulatorypsm%3D0%26ocid%3Dspartandhp&scr=1440x900&bh=782&bw=1290&dv.Title1=Start&viewType=size4column&prs=%7B%22srch3P%22%3Afalse%7D&scp=&di=108&mkt=de-de&pn=dhp&su=https%253A%252F%252Fwww.msn.com%252Fspartan%252Fdhp%253Flocale%253Dde-DE%2526market%253DDE%2526enableregulatorypsm%253D0%2526ocid%253Dspartandhp&pid=Spartan_DHP&cv.product=spartan&flightid=muidflt14cf%2Cmuidflt15cf%2Cmuidflt19cf%2Carooabt%2Cmuidflt258cf%2Cmuidflt261cf%2Cmuidflt312cf&activityId=07366c10c44443848473fc20c4ad778e&cvs=Browser&subcvs=homepage&st.dpt=dhp&st.sdpt=&cv.partner=&cv.publcat=&cv.author=&cv.entityId=&cv.entitySrc=&cv.parentId=&provid=&ar=0&d.dgk=tmx.pc.edge.spartan.serviceui&d.imd=0&tmpl=infopane%3A0%3Bcat%3A0%3BIP%3ACookie%3BRV%3ACookie%3BEP%3A0%3BCI%3A1%3BspartanExternalContentModule%3A1%3Bsuiv%3A8&isStaticPage=False&pgIdx=&pgTot=&pp=False&pb=%7B%7D
5	207.46.194.10	**c.bing.com** *[msnbot-207-46-194-10.search .msn.com]*	/c.gif?Red3=MSNLI_pd&rid=07366c10-c444-4384-8473-fc20c4ad778e&lng=de-de&dgk=tmx.pc.edge.spartan.serviceui&imd=0&pn=spartanstartpage&rf=&tp=https%3A%2F%2Fwww.msn.com%2Fspartan%2Fdhp%3Flocale%3Dde-DE%26market%3DDE%26enableregulatorypsm%3D0
6	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
7	204.79.197.203	**www.msn.com** *[a-0003.a-msedge.net]*	/spartan/dhp/de-de/ecpajax/1.2?appslocale=de-de&externalContentProvider=taboolasponcon&recommendationsRequested=3&infopane Recommendations=1
8	104.40.210.32	**otf.msn.com**	/c.gif?

		[-]	
9	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
10	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
11	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
12	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
13	131.253.61.66	**login.live.com** *[-]*	/login.srf?wa=wsignin1.0&rpsnv=13&checkda=1&ct=1488383822&rver=6.7.6643.0&wp=lbi&wreply=https%3a%2f%2fwww.msn.com%2fspartan%2fde-de%2fsecure%2fsilentpassport%3fsecure%3dtrue&lc=1033&id=1184&mkt=de-de
14	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
15	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
16	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
17	204.79.197.203	**www.msn.com** *[a-0003.a-msedge.net]*	/spartan/de-de/secure/silentpassport?secure=true&lc=1031
18	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
19	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
20	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
21	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?rid=07366c10c44443848473fc20c4ad778e&cts=1488383835260&aop=main%3Esection.apps.postcontent_sec-tion&eventIndex=2&clid=3CC1108501826E2A2A8D1AB300E46F9D&gesture=&viewType=size4column&di=108&mkt=de-de&pn=dhp&su=https%253A%252F%252Fwww.msn.com%252Fspartan%252Fdhp%253Flocale%253Dde-DE%2526market%253DDE%2526enableregulatorypsm%253D0%2526ocid%253Dspartandhp&pid=Spartan_DHP&cv.product=spartan&flightid=muidflt14cf%2Cmuidflt15cf%2Cmuidflt19cf%2Carooabt%2Cmuidflt258cf%2Cmuidflt261cf%2Cmuidflt312cf&activityId=07366c10c44443848473fc20c4ad778e&cvs=Browser&subcvs=homepage&evt=click_nonnav&cm=maincontent%3Emain%3Edelayloadedcontent%3Econtentsection%3Entss&hl=Anpassen&du=&e1=%7B%22i%22%3A32%2C%22p%22%3A31%2C%22n%22%3A%22show_customize%22%2C%22y%22%3A14%2C%22o%22%3A1%7D&l=main%3Esection_header%3Eshow_customize&lo=8%3E1&TTI=13513&pb=
22	172.227.15.146	**api.taboola.com**	/1.2/json/msn-edgedefaulthomepage-germany/recommendations.notify-

		[a172-227-15-146.deploy.static .akamaitechnologies.com]	visible?app.type=desktop&app.apikey=dd914485a5ed62ec1086bc1f372e410b851bc1e0&response.session=v2_49b062d0aeee27426d3bc485ed6a80a2_3CC1108501826E2A2A8D1AB300E46F9D_1488383822_1488383822_CIi3jgYQiadAGKGY29SoKyABKAU&response.id=__feb45b9cabdb01dcfbc622627769471b__4e9179dd922e47b0c2fb63f44909dc8c__~~V1~~6323882792569909201~~AKNK9EkrSd_GpZwURehsIzQ3lJHA37jAQFKuV2sMJMESO_fFkG-bpaW2-qyqBDD692O2HuksVwHJ29qQPrBJZbTufXnPZ2XkSmshp8V2IGE6Fo0nPn6u25OYX283bkoclkRw-hIutQ4jjSBDWOHR-A__text
23	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
24	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
25	104.40.210.32	**otf.msn.com** *[-]*	/c.gif?
26	93.184.221.200	**iecvlist.microsoft.com** *[-]*	/edge/desktop/1432152749/edgecompatviewlist.xml

2.4 Review

In this second use case we noticed that no data transfers were initiated after opening the Windows Start Menu again. Further actions like opening the browser Microsoft Edge (initial use), however, resulted in a large number of data flows. The reason for this was on the one hand the default homepage (MSN) and on the other hand the preset SmartScreen filter. Additionally, we registered that unzipping a standard zip-file in the Windows File Explorer also causes data traffic. As a result of these findings, we decided to deactivate SmartScreen in the next use case and to prevent unnecessary data flows in the browser Microsoft Edge by changing the default start setting.

3. Scenario 3:
Disable further data flows (focus on Smart Screen)

In this use case we disabled the SmartScreen in Microsoft Edge and the Windows File Explorer.

3.1 Settings (in addition to the previous settings)

Settings for SmartScreen have been done in *Computer Configuration\Administrative Templates*:

Directory	Name	Policy Setting Name	Setting
Windows Components	Microsoft Edge microsoftedge.admx	Configure Windows Defender SmartScreen	disabled
Windows Components	File Explorer windowsexplorer.admx	Configure Windows Defender SmartScreen	disabled

3.2 Actions

- Restart of Virtual Machine 1 (Windows 10 Enterprise Version)
- Start monitoring through Virtual Machine 2 (mitmproxy)
- Open Windows Start Menu in Virtual Machine 1 (Click on Windows Start Button)
- Use search function and search exemplary for a keyword "test"
- Open Microsoft Edge without entering a URL
- Open Windows Explorer and unzip a Zip-file
- Open different folders in the Windows Explorer
- Open system settings and change the desktop background image
- Stop Virtual Machine 1 (Windows 10 Enterprise Version)
- Stop monitoring through Virtual Machine 2 (mitmproxy)

3.3 Detected data flows

#	IP	Domain *[+DNS Lookup]*	Request
1	92.123.254.111	**geover-prod.do.dsp.mp.microsoft.com** *[a92-123-254-111.deploy .akamaitechnologies.com]*	/geoversion/?doClientVersion=10.0.14393.594&profile=16
2	40.77.226.220	**geo-prod.do.dsp.mp.microsoft.com** *[-]*	/geo/?doClientVersion=10.0.14393.594&profile=16
3	88.221.136.207	**kv401-prod.do.dsp.mp.microsoft.com** *[a88-221-136-207.deploy .akamaitechnologies.com]*	/all/?doClientVersion=10.0.14393.594&countryCode=DE&profile=16
4	207.46.194.14	**g.bing.com** *[msnbot-207-46-194-14.search.msn.com]*	/meedco/FirstLaunch?pg=PC000P0FR5.0000000INE&placementType=PostOOBE&pid=400014371&cid=730000000002661 62&tid=700010366&reqasid=BCAEA580F0EF42DE8728C388560DA561&region=DE&lang=DE-DE&oem=&devFam=WINDOWS.DESKTOP&ossku=ENTER-PRISEEVAL&cmdVer=10.0.14393.0&mo=&cap=&itemId=9WZDNCRFHVN5&skuId=0010&auid=A4BFDF2E4681E9BA155152BEFC7A49BB&anid=&bSrc=i.t&installKind=Install&ctid=store-curated-postoobe&asid=71fe4510bc9b44bc8b8a9568aa9ad4da&time=20170302T133912Z
5	207.46.194.14	**g.bing.com** *[msnbot-207-46-194-14.search.msn.com]*	/meedco/FirstLaunch?pg=PC000P0FR5.0000000ING&placementType=PostOOBE&pid=400014372&cid=510000000002799 16&tid=700010368&reqasid=3F4789CADDBA4C2AA3261F902580F483&region=DE&lang=DE-DE&oem=&devFam=WINDOWS.DESKTOP&ossku=ENTER-PRISEEVAL&cmdVer=10.0.14393.0&mo=&cap=&itemId=9WZDNCRD2G0J&skuId=0010&auid=A4BFDF2E4681E9BA155152BEFC7A49BB&anid=&bSrc=i.t&installKind=Install&ctid=store-curated-postoobe&asid=39016bcb585a4de696e1b4a600799b58&time=20170302T133849Z

6	207.46.194.14	**g.bing.com** *[msnbot-207-46-194-14.search.msn.com]*	/meedco/FirstLaunch?pg=PC000P0FR5.0000000ING&placementType=PostOOBE&pid=400014372&cid=510000000002799 16&tid=700010368&reqasid=3F4789CADDBA4C2AA3261F902580F483&region=DE&lang=DE-DE&oem=&devFam=WINDOWS.DESKTOP&ossku=ENTER-PRISEEVAL&cmdVer=10.0.14393.0&mo=&cap=&itemId=9WZDNCRDTBJJ&skuId=0010&auid=A4BFDF2E4681E9BA155152BEFC7A49BB&anid=&bSrc=i.t&installKind=Install&ctid=store-curated-postoobe&asid=39016bcb585a4de696e1b4a600799b58&time=20170302T133855Z
7	207.46.194.33	**arc.msn.com** *[msnbot-207-46-194-33.search.msn.com]*	/v3/Delivery/Events/Impression
8	157.56.77.148	**sls.update.microsoft.com** *[-]*	/SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.14393.0/0?CH=956&L=de-DE&P=&PT=0x48&WUA=10.0.14393.594
9	157.56.77.148	**sls.update.microsoft.com** *[-]*	/SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.14393.0/0?CH=956&L=de-DE&P=&PT=0x48&WUA=10.0.14393.594
10	157.56.77.148	**sls.update.microsoft.com** *[-]*	/SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.14393.0/0?CH=956&L=de-DE&P=&PT=0x48&WUA=10.0.14393.594
11	157.56.77.148	**sls.update.microsoft.com** *[-]*	/SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.14393.0/0?CH=956&L=de-DE&P=&PT=0x48&WUA=10.0.14393.594
12	157.56.77.148	**sls.update.microsoft.com** *[-]*	/SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.14393.0/0?CH=956&L=de-DE&P=&PT=0x48&WUA=10.0.14393.594
13	157.56.77.148	**sls.update.microsoft.com** *[-]*	/SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.14393.0/0?CH=956&L=de-DE&P=&PT=0x48&WUA=10.0.14393.594

3.4 Review

By deactivating the SmartScreen filter the data flows could be restricted. However, it was not possible to completely stop the background data flows in this use case. Although the test was limited by time and by scope using the system, sufficient data traffic of the OS has been detected to prove that the OS still sends data requests.

III. Investigation May 2017: Win10 Enterprise Version after Creators Update - Build 15063

1. Scenario 1: Disable data flows after OS start

The settings we have chosen to prevent OS initiated data flows have been the same like in our first investigation in March 2017 for Build 14393. For this reason we just refer to the Windows Group Policy settings which were mentioned before.

1.1 Settings

See above (Settings in Scenario 1 for Investigation March 2017: Win10 Enterprise Version - Build 14393).

1.2 Actions

- Restart of Virtual Machine 1 (Windows 10 Enterprise Version)
- Start monitoring through Virtual Machine 2 (mitmproxy)
- Open Windows Start Menu in Virtual Machine 1 (Click on Windows Start Button)
- Use search function and search exemplary for two keywords “gpedit” and “test”
- Stop Virtual Machine 1 (Windows 10 Enterprise Version)
- Stop monitoring through Virtual Machine 2 (mitmproxy)

1.3 Detected data flows

The results of the mitmproxy-analysis, i.e. the registered requests, are listed below.

#	IP	Domain *[+DNS Lookup]*	Request
1	13.107.4.52	**www.msftconnecttest.com** *[4-c-0003.c-msedge.net]*	/connecttest.txt
2	104.84.217.229	**cdn.content.prod.cms.msn.com** *[e10663.g.akamaiedge.net]*	/singletile/summary/alias/experiencebyname/today?market=de-DE&source=appxmanifest&tenant=amp&vertical=news
3	104.84.154.122	**tile-service.weather.microsoft.com** *[e7070.g.akamaiedge.net]*	/de-DE/livetile/preinstall?region=DE&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold
4	104.104.201.9	**cdn.onenote.net** *[e1553.dspg.akamaiedge.net]*	/livetile/?Language=de-DE
5	204.79.197.200	**www.bing.com** *[-]*	/AS/API/WindowsCortanaPane/V2/Init
6	104.84.217.229	**cdn.content.prod.cms.msn.com** *[e10663.g.akamaiedge.net]*	/singletile/summary/alias/experiencebyname/today?market=de-DE&source=appxmanifest&tenant=amp&vertical=news
7	23.222.39.64	**sway-cdn.com** *[-]*	/api/1.0/getTileUpdate(de-DE)
8	104.84.154.122	**tile-service.weather.microsoft.com**	/de-DE/livetile/preinstall?region=DE&appid=

		[e7070.g.akamaiedge.net]	C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold
9	207.46.194.33	**arc.msn.com** *[arc.msn.com.nsatc.net]*	/v3/Delivery/Events/Impression
10	104.84.167.52	**livetileedge.dsx.mp.microsoft.com** *[e1898.dspg.akamaiedge.net]*	/v8.0/background/pages/livetile?appversion=11703.1001.45.0&market=DE&locale=de-DE&deviceFamily=Windows.Desktop&catalogLocales=en-DE%2Cde-DE%2Cen-GB&musicMarket=
11	2.16.4.208	**img-s-msn-com.akamaized.net** *[a1834.dspg2.akamai.net]*	/tenant/amp/entityid/BBBLhJg.img?w=100&h=100&m=6&tilesize=medium&x=881&y=791&ms-scale=100&ms-contrast=standard
12	23.9.137.220	**blob.weather.microsoft.com** *[e7070.g.akamaiedge.net]*	/static/mws-new/WeatherImages/210x173/3.jpg?a

1.4 Review

Like in the first investigation, our settings in the Windows Group Policy did not prevent all data transmission of the Windows 10 Enterprise Version. After starting the OS, using the Windows Start Menu and searching for two keywords, several requests were registered. We noticed that most of these requests were similar to the results of our first investigation before Creators Update. The requests were mainly initiated by the Windows Start Menu configuration (e.g. tiles for Sway, Live, OneNote, and Weather), so we decided to eliminate these data transmission behavior in the next use case again.

2. Scenario 2:
Disable data flows after usage of Windows Start Menu

2.1 Settings (in addition to the previous settings)

Further setting in the Policy in *Computer Configuration\Administrative Templates*:

Directory	Name	Policy Setting Name	Setting
Start Menu and Taskbar startmenu.admx	-	Start Layout	enabled: Layout file in C:\temp\StartLayout.xml

The start menu has been modified by us with a new StartLayout.xml-file so that no more "live tiles" were integrated. The procedure was identical to the first investigation. We also deactivated the tile notifications in the user configuration of the Windows Group Policy in *User\Administrative Templates*:

Directory	Name	Policy Setting Name	Setting
Start Menu and Taskbar	Notifications wpn.admx	Turn off tile notifications	enabled

2.2 Actions

- Restart of Virtual Machine 1 (Windows 10 Enterprise Version)
- Start monitoring through Virtual Machine 2 (mitmproxy)
- Open Windows Start Menu in Virtual Machine 1 (Click on Windows Start Button)

- Use search function and search exemplary for two keywords “gpedit” and “test”
- Open Microsoft Edge without entering a URL
- Open Windows Explorer and unzip a Zip-file
- Stop Virtual Machine 1 (Windows 10 Enterprise Version)
- Stop monitoring through Virtual Machine 2 (mitmproxy)

2.3 Detected data flows

#	IP	Domain *[+DNS Lookup]*	Request
1	204.79.197.200	**www.bing.com** *[-]*	/AS/API/WindowsCortanaPane/V2/Init
2	204.79.197.203	**www.msn.com** *[a-0003.a-msedge.net]*	/spartan/dhp?locale=en-US&market=DE&enableregulatorypsm=0&enablecpsm=0&ishostisolationenforced=0&targetexperience=enterprise
3	92.123.195.108	**img-s-msn-com.akamaized.net** *[a1834.dspg2.akamai.net]*	/tenant/amp/entityid/AAehLNN.img
4	92.123.195.108	**img-s-msn-com.akamaized.net** *[a1834.dspg2.akamai.net]*	/tenant/amp/entityid/BBtxOyX.img?h=174&w=300&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1031&y=397
5	92.123.195.108	**img-s-msn-com.akamaized.net** *[a1834.dspg2.akamai.net]*	/tenant/amp/entityid/BBBL95p.img?h=174&w=300&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1343&y=293
6	92.123.195.108	**img-s-msn-com.akamaized.net** *[a1834.dspg2.akamai.net]*	/tenant/amp/entityid/BBnGKDa.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
7	92.123.195.108	**img-s-msn-com.akamaized.net** *[a1834.dspg2.akamai.net]*	/tenant/amp/entityid/BBhma8H.img?h=174&w=300&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1530&y=1185
8	92.123.195.108	**img-s-msn-com.akamaized.net** *[a1834.dspg2.akamai.net]*	/tenant/amp/entityid/AAdz7P0.img?h=88&w=88&m=6&q=60&u=t&o=t&l=f&f=png
9	204.79.197.200	**www.bing.com** *[-]*	/manifest/IEOneBox_V2.appcache?setlang=en-US
10	204.79.197.200	**www.bing.com** *[-]*	/AS/IEOneBox/xls.aspx
11	204.79.197.203	**www.msn.com** *[a-0003.a-msedge.net]*	/spartan/dhp/en-us/ecpajax/1.2?appslocale=en-us&externalContentProvider=taboolasponcon&recommendationsRequested=3&infopaneRecommendations=1
12	104.73.138.159	**sb.scorecardresearch.com** *[e1879.e7.akamaiedge.net]*	/b?c1=2&c2=3000001&rn=1496316671076&c7=https%3A%2F%2Fwww.msn.com%2Fspartan%2Fdhp%3Flocale%3Den-US%26market%3DDE%26enableregulatorypsm%3D0%26enablecpsm%3D0%26ishostisolationenforced%3D0%26targetexperience%3Denterprise%26ocid%3Dspartandhp&c8=Start&c9=
13	204.79.197.203	**www.msn.com** *[a-0003.a-msedge.net]*	/spartan/dhp/en-us/ecpajax/1.0?appslocale=en-us&externalContentProvider=emspromo&recommendationsRequested=2
14	204.79.197.200	**c.bing.com** *[a-0001.a-msedge.net]*	/c.gif?Red3=MSNLI_pd&rid=3eee3ca5-188c-4596-bce3-bc1c143dbd8f&lng=en-

			us&dgk=tmx.pc.edge.spartan.serviceui&imd=0&pn=spartan-startpage&rf=&tp=https%3A%2F%2Fwww.msn.com%2Fspartan%2Fdhp%3Flocale%3Den-US%26market%3DDE%26enableregulatorypsm%3D0%26enablecpsm%3D0%26ishostisolationenforced%3D0%26targetexperience%3Denterprise
15	40.127.142.76	**otf.msn.com** *[iceotf-prdo-fe-westeurope.cloudapp.net]*	/c.gif?
16	104.92.91.124	**sci2-1.am.microsoft.com** *[e13082.dspg.akamaiedge.net]]*	/433730151296701052/media2.png
17	40.127.142.76	**otf.msn.com** *[iceotf-prdo-fe-westeurope.cloudapp.net]*	/c.gif?
18	93.184.221.200	**iecvlist.microsoft.com** *[cs9.wpc.v0cdn.net]*	/edge/desktop/1475001623/edgecompatviewlist.xml

2.4 Review

In this second use case we noticed that no data transfers were initiated after opening the Windows Start Menu. Further actions like opening the browser Microsoft Edge (initial use), however, resulted in a large number of data flows. The reason for this was the default homepage (MSN) as well as the preset Smart-Screen filter. As a result of these findings, we decided to deactivate SmartScreen in the next use case and to prevent unnecessary data flows in the browser Microsoft Edge by changing the default start setting.

3. Scenario 3:
Disable further data flows (focus on Smart Screen)

In this use case we disabled the SmartScreen in Microsoft Edge and the Windows File Explorer.

3.1 Settings (in addition to the previous settings)

Settings for SmartScreen have been done in *Computer Configuration\Administrative Templates*:

Directory	Name	Policy Setting Name	Setting
Windows Components	Microsoft Edge microsoftedge.admx	Configure Windows Defender SmartScreen	disabled
Windows Components	File Explorer windowsexplorer.admx	Configure Windows Defender SmartScreen	disabled

3.2 Actions

- Restart of Virtual Machine 1 (Windows 10 Enterprise Version)
- Start monitoring through Virtual Machine 2 (mitmproxy)
- Open Windows Start Menu in Virtual Machine 1 (Click on Windows Start Button)
- Use search function and search exemplary for a keyword “test”
- Open Microsoft Edge without entering a URL
- Open Windows Explorer and unzip a Zip-file

- Open different folders in the Windows Explorer
- Open system settings and change the desktop background image
- Stop Virtual Machine 1 (Windows 10 Enterprise Version)
- Stop monitoring through Virtual Machine 2 (mitmproxy)

3.3 Detected data flows

#	IP	Domain *[+DNS Lookup]*	Request
1	204.79.197.200	**www.bing.com** *[-]*	/manifest/threshold.appcache
2	204.79.197.200	**ww.bing.com** *[-]*	/AS/API/WindowsCortanaPane/V2/Init
3	191.232.80.62	**fe2.update.microsoft.com** *[fe2.update.microsoft.com.nsatc.net]*	/v6/ClientWebService/client.asmx
4	64.4.54.18	**fe3.delivery.mp.microsoft.com** *[fe3.delivery.dsp.mp.microsoft.com.nsatc.net]*	/ClientWebService/client.asmx

3.4 Review

By deactivating the SmartScreen filter the data flows could be further restricted. However, it was not possible to completely stop the background data flows in this use case. Although the test was limited by time and by scope using the system, sufficient data traffic of the OS has been detected to prove that the OS still sends data requests.

IV. Conclusion

As we detected, only special versions of Windows 10 seem to be appropriate for data controllers in the private sector in Europe, because the level of security and privacy options differ in the versions. Therefore, we focused in our investigation on the version that offers the highest level of setting options – Windows 10 Enterprise.

The result of this investigation is that via Windows Group Policy settings most data traffic can be stopped. With Windows 10 Enterprise, especially Version 1703 Build 15063, many problematic functions regarding data protection regulations can be disabled (e.g. App Store, Smart Screen Filter, OneDrive, and Cortana). However, parts of the Windows Updates and some Telemetry and Security functions still could not be deactivated by us in this investigation via Windows Group Policies. As there are a thousand of possible settings in the Windows Group Policies, we cannot rule out that we have overlooked further helpful settings to limit data traffic of the OS or that there may be easy ways to restrict the traffic via other settings (for example in the Registry or the UI) . Nevertheless, this investigation was very useful for us to record that there can be ways to restrict the data transmission behavior of Windows 10. On the basis of this examination, we believe that it may well be possible that European data controllers can use Windows 10 in compliance with data protection. But for us, not all relevant points have been clarified through this examination.

We are also aware of the Group Policy Settings Reference for Windows 10 Version 1703 that was officially published by Microsoft on 5/22/2017 under https://docs.microsoft.com/en-us/windows/configuration/manage-connections-from-windows-operating-system-components-to-microsoft-services. We consider this transparent presentation as very helpful support for data controllers and the right step in terms of transparency. However, there is still no extensive guidance on how Windows 10 can be used in full compliance with European data protection law.