

**dn**

*Systems*

# **(technische) Analyse Microsoft Office 365 & W10 Telemetry und Datenschutz**

**Lukas Grunwald**

**mbuf focus day IT-Security, Mannheim**

**2019.07.23**

# Who am I

- Lukas Grunwald
  - Security Consulting since 1998
  - Founder DN-Systems Enterprise Internet Sol. GmbH
  - Speaker at BlackHat, DefCon, PoC, Coinsec ...
  - Writes for Heise
    - [https://www.heise.de/suche/?q=%22Lukas+Grunwald%22&search\\_submit.x=0&search\\_submit.y=0&rm=search&sort\\_by=date](https://www.heise.de/suche/?q=%22Lukas+Grunwald%22&search_submit.x=0&search_submit.y=0&rm=search&sort_by=date)
- DN-Systems
  - Operates own Security Lab
  - Integral Security (not only ICT)
  - Malware and APT Analysis
  - Investigation / Digital Forensics
  - Consulting IT-Companies on global scale

# Agenda

- 
- Back at the Blackhat 2008
  - Lab setup and components
  - Direction User to Microsoft
  - Direction Microsoft to User
  - Office 2013/2016/365
  - Possible improvements
-

# Microsoft Software Updates

- Work presented 2008 at Blackhat
  - Demonstration of Infection Proxys
  - Unsecure Software Updates
  - Vulnerabilities used by FinFisher and Leonardo
    - Government SpySoftware by Gamma Intl. and Hacking Team
- Microsoft fixed the vulnerabilities rapidly and quickly
  - Worked with Blackhat on site Security Team
- But .. in 2015 came
  - Windows 10

## Software update cures it all (excerpt 2008)

- Vendors publish security patches via Software Updates
- Adobe plans to install / update software for the Acrobat Reader autonomously
  - No user control any more
  - Background process while user is online
- Apple updates Safari and iTunes with Apple Update
- Microsoft updates in Background
  - (XP, Vista, W7, Server)
- How trusted are these update mechanisms?

# Update via Internet (excerpt 2008)

1. DNS Resolve of update cluster / hosts
2. Connect to the update server
3. Get a index of actual version
4. Calculate the needed patches / updates
5. Download the patch / updates
6. Install them on the target system

# Attacks to updates (excerpt 2008)

- DNS Spoofing to redirect to a infection server
- Transparent infection Proxy
  - Can be sit on the wire, or as Trojan on the system
  - Drive-By-Exploits
  - Fake-Downloads from 3rd Party Download Sites
    - Google Search poisoning

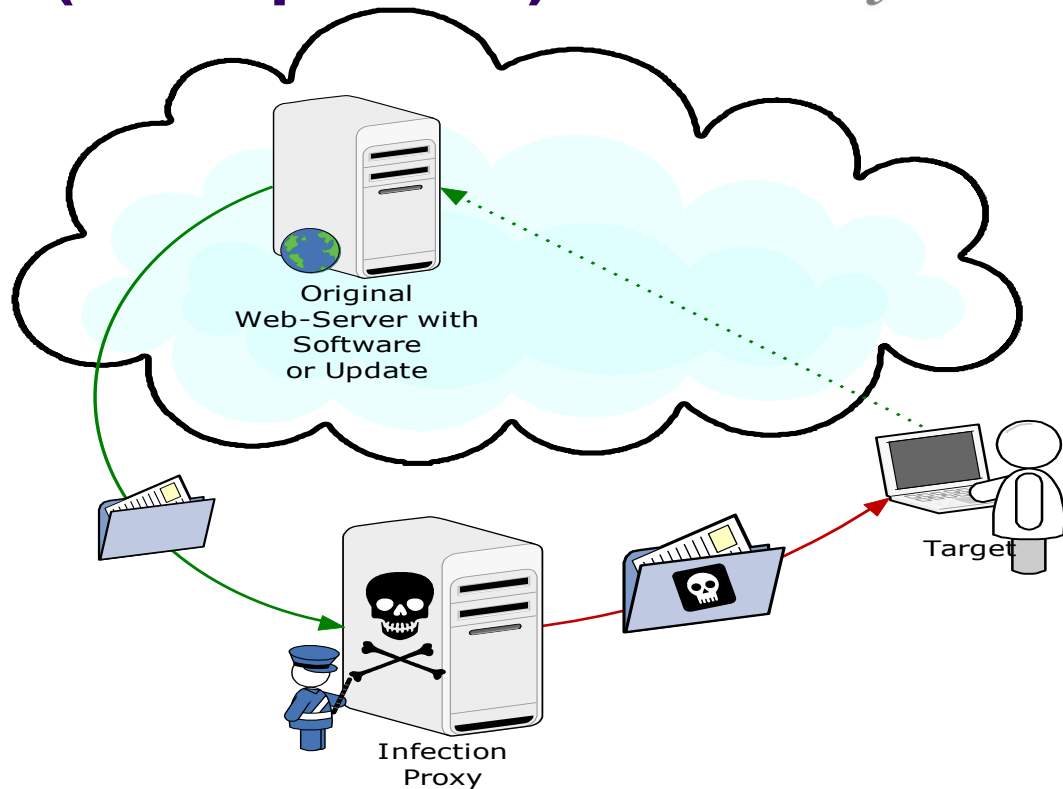
## Motivation for Poisoning (excerpt 2008)

- Lawful Interception / Offensive Forensic
- Criminal Intention
  - Attack Home Banking
  - Zombie infection to get a Bot-Net Node
  - Referrer Poisoning go get sales margin
- Private Investigation
- Corporate Intelligence



# Poisoned Downloads (excerpt 2008)

- Million of Firefox downloads on the first release day
- Take advantage of Internet software updates
- Support from software industry will make it easy
- Possible with every software download / upload



## Microsoft Update (excerpt 2008)

- Update is using CRL correct
  - Lost certificate is not fatal
  - Software segments are signed
  - Update uses HTTP (not HTTPS)
  - **Microsoft Update V6 is secure (XP, Vista, W7)**
- **Fixed by Microsoft 2 weeks after the BlackHat talk**

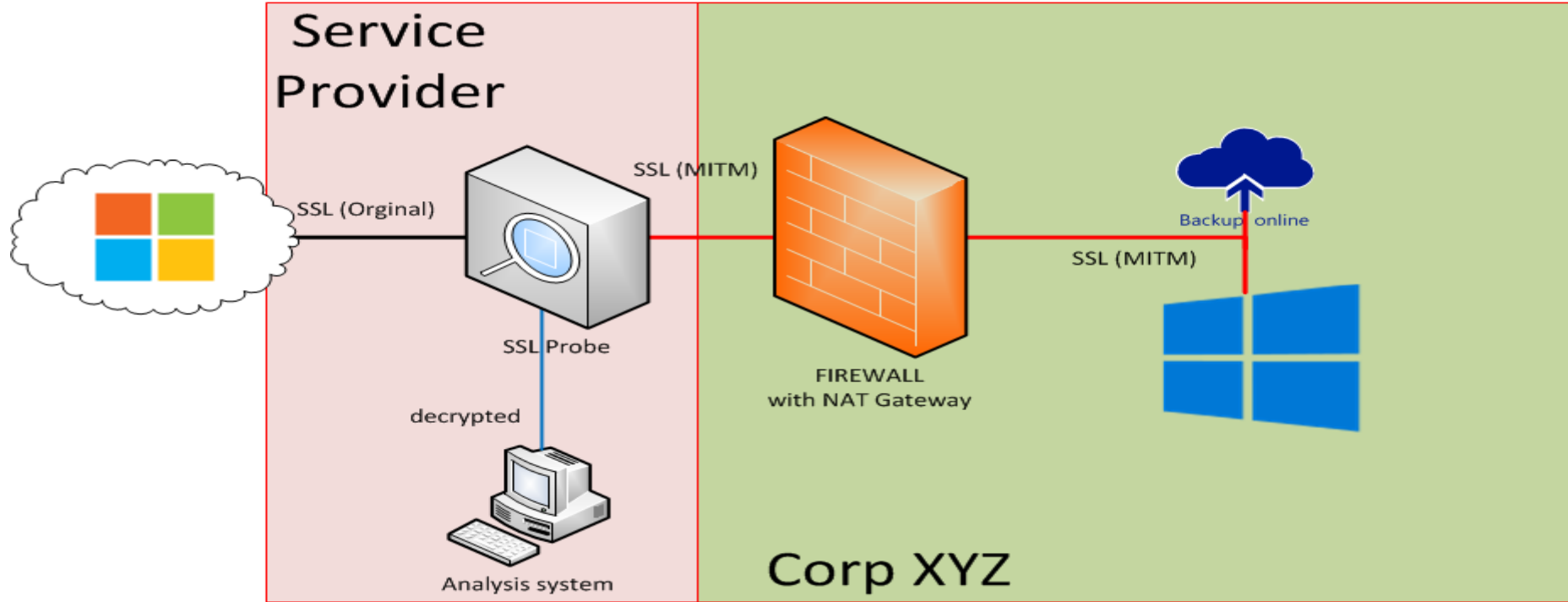
- 
- Back at the Blackhat 2008
  - Lab setup and components
  - Direction User to Microsoft
  - Direction Microsoft to User
  - Office 2013/2016/365
  - Possible improvements
-

# Let's check Windows 10 (back to the future 2015)

- Windows 10 is cloud centric
- Telemetry is send periodically
- Cortana sends huge amount of personal data e.g.:  
Voice, Search, Handwriting
- WLAN-Keys, UserIDs, passwords, Edge Data etc are stored in cloud as well
- BitLocker Keys and Office 360 data are stored in the Microsoft cloud

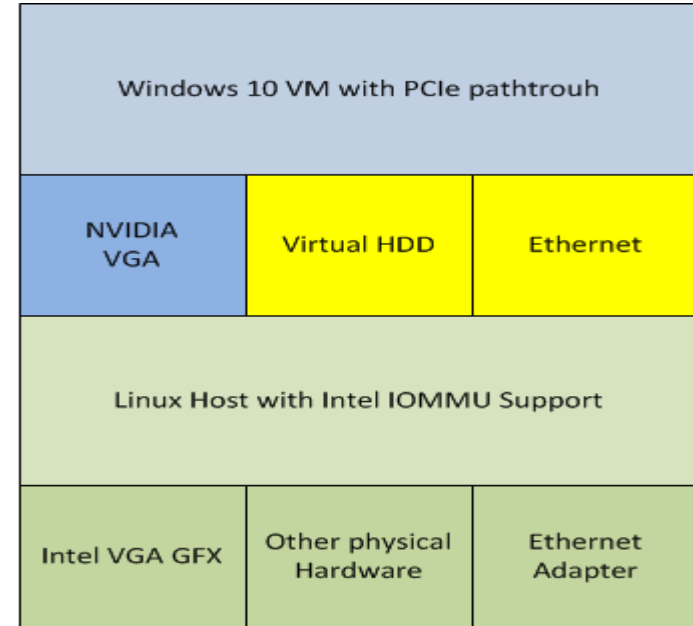


# Test setup for interception



# One Machine implementation

- Not all hardware components are virtualized
- On Linux-Host are based:
  - Infection Proxy
  - Man in the Middle (SSL Proxy)
  - Analysis Tools
- Setup explained in the iX article in detail



# Ups they did it again ...

- The bug from 2008 is back
- Windows Update (and the store) is secure, but the rest is total interceptable

```
[...]  
X-MSEdge-ExternalExpType: JointCoord  
X-MSEdge-ExternalExp: d-thshld39,d-thshldspcl40,d-thshld42  
Content-type: text/xml  
X-Search-SafeSearch: Moderate  
X-Device-SKU: To be filled by O.E.M.  
X-Device-MachineId: {7A00EF93-FD60-45AA-ACB0-06629146C562}  
X-BM-Market: DE  
X-BM-DateFormat: M/d/yyyy  
X-Device-OSSKU: 48  
X-Device-NetworkType: ethernet  
X-BM-DTZ: 120  
X-DeviceID: 0100040C0900369F  
X-BM-DeviceScale: 100  
X-Device-Manufacturer: Gigabyte Technology Co., Ltd.  
X-BM-Theme: fffffff;004275  
X-BM-DeviceDimensionsLogical: 344x520  
X-BM-DeviceDimensions: 344x520  
[...]
```



## Windows Update

We couldn't get online to download your updates. We'll try again later, or you can check now. If it still doesn't work, make sure you're connected to the Internet.

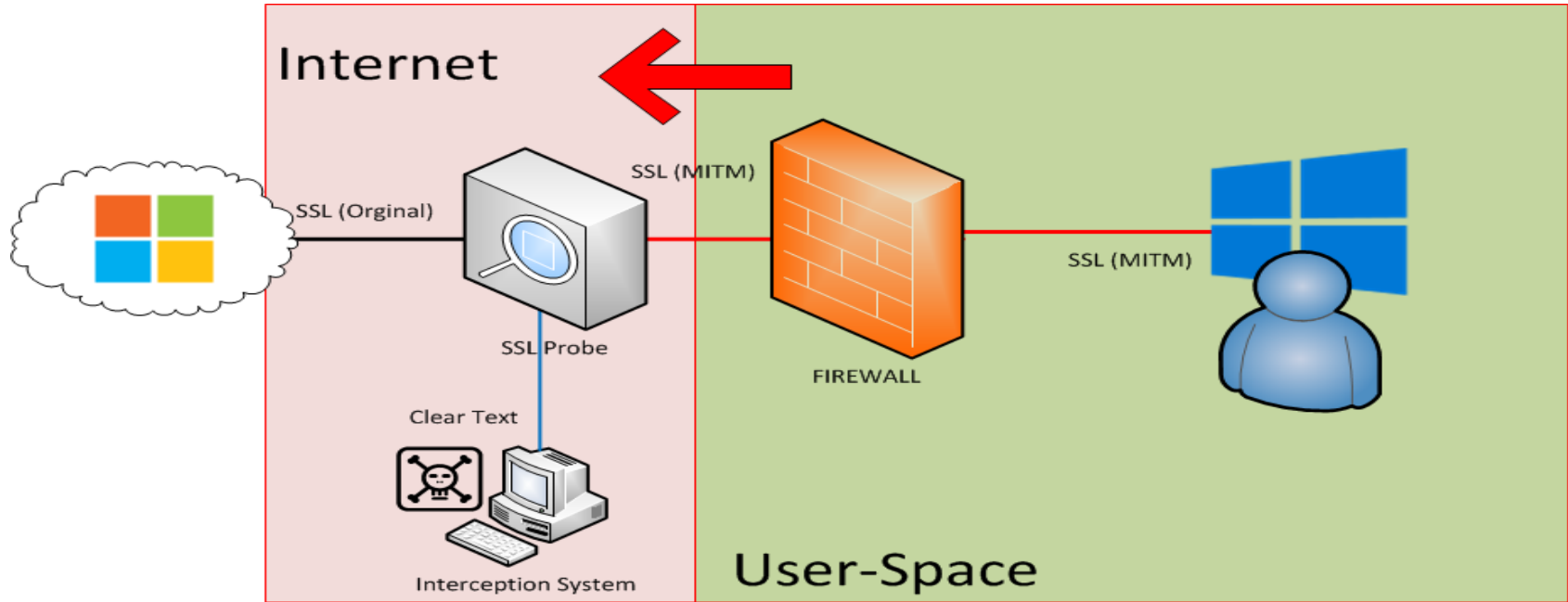
Retry

[Advanced options](#)

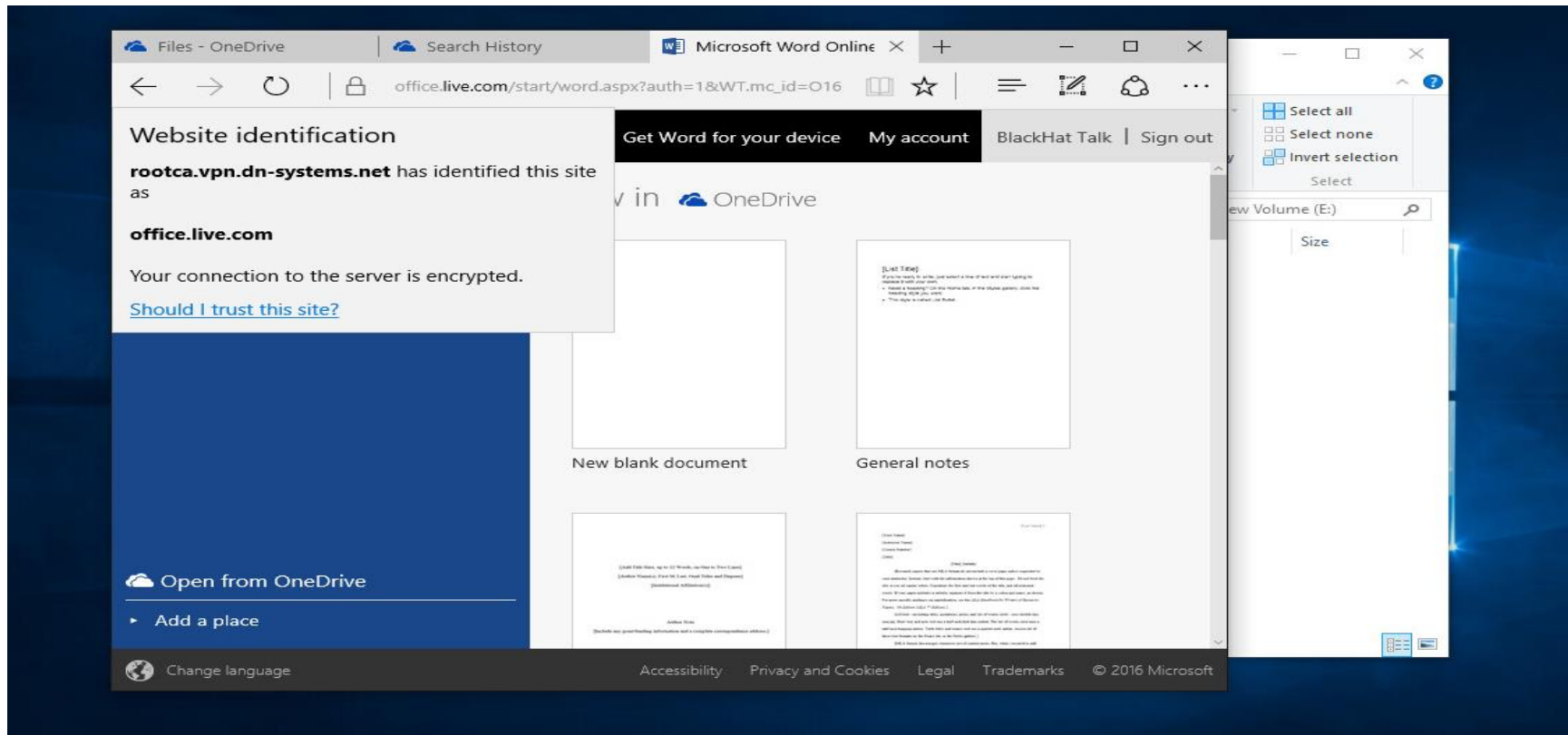
- 
- Back at the Blackhat 2008
  - Lab setup and components
  - Direction User to Microsoft
  - Direction Microsoft to User
  - Office 2013/2016/365
  - Possible improvements
-



# Direction – User to Microsoft (Cloud)



# SSL in the Middle attack



# Smart-Screen send URL to Microsoft



- EDGE Browser sending URLs to MS

```
POST /urs.asmx?MSURS-Client-Key=5178pvN3uGdwzGWbvvu6Nw%3d%3d&MSURS-MAC=q0Asz9t12ok%3d HTTP/1.1
Accept: text/*
Content-Type: text/xml; charset=utf-8
User-Agent: VCSoapClient
Host: urs.microsoft.com
Content-Length: 571
Cache-Control: no-cache
<RepLookup v="5"><G>379BDC39-D58D-44AA-986B-FD2CBFFA75A6</G><O>80E6C742-3F85-4A5C-9405-
0930AB345910</O><D>10.0.8110.6</D><C>11.00.10240.16384</C><OS>10.0.10240.0.0</OS><I>9.11.10240
.16384</I><L>de-
DE</L><RU>aHR0cDovL3d3dy5oZWlzM5kZS8=</RU><RI>0.0.0.0</RI><R><Rq><URL>aHR0cDovL3d3dy5oZWlzM5kZS8
kZS8=</URL><O>PRE</O><T>TOP</T><HIP>2a00:1450:4005:0800:0000:0000:0000:100b</HIP></Rq><Rq><URL
>aHR0cDovL1syYTAwOjE0NTA6NDAwNTowODAwOjAwMDA6MDAwMDowMDAwOjEwMGJdLw==</URL><O>PRE</O><T>IP</T>
<HIP>[2a00:1450:4005:0800:0000:0000:0000:100b]</HIP></Rq></R><WA/><PRT>219</PRT></RepLookup>
```

```
aHR0cDovL1syYTAwOjE0NTA6NDAwNTowODAwOjAwMDA6MDAwMDowMDAwOjEwMGJdL
w==http://\[2a00:1450:4005:0800:0000:0000:0000:100b\]
aHR0cDovL3d3dy5oZWlzM5kZS8= http://www.heise.de/
```

# Local command are visible to Microsoft as well

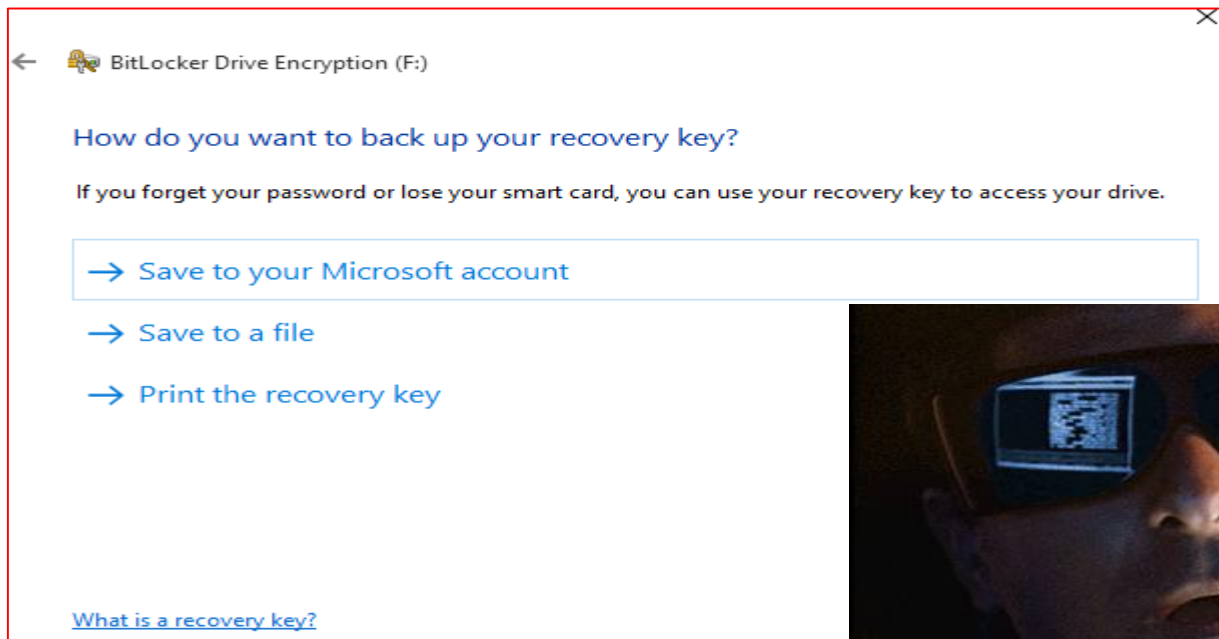


- Cortana is sending local system commands to Microsoft as well

```
", "K":1001, "Q":"cmd", "Val":"CG", "Ho":2, "Gr":3, "HC":1, "DeviceSignals":{"Rank":0, "PHits":null, "Id":"C:\\\\WINDOWS\\\\system32\\\\cmd.exe", "DName":"cmd"}}}], {"T":"D.LocalApps", "AppNS":"SmartSearch", "Service":"AutoSuggest", "Scenario":"LocalApps", "SC":1, "DS":[{"T":"D.Url", "Tx":"Command Prompt", "K":1002, "Q":"Command Prompt", "Val":"PP", "Ho":2, "Gr":0, "DeviceSignals":{"Rank":990, "PHits":{"0":"System.FileName", "1":"System.ParsingName"}, "Id":"{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\\\cmd.exe", "DName":"Command Prompt", "LAD":"2015-07-31T11:28:57.852Z", "AppLnch":7, "Args":0, "MDN":0}, "RankerSignals":{"rankingScore":7.170697083715229, "featureStore":{"0":0.18786, "1":1, "2":7, "3":0.00257, "5":"0.001", "6":131218.02, "7":990, "8":1, "
```

# Backup to skydrive ?

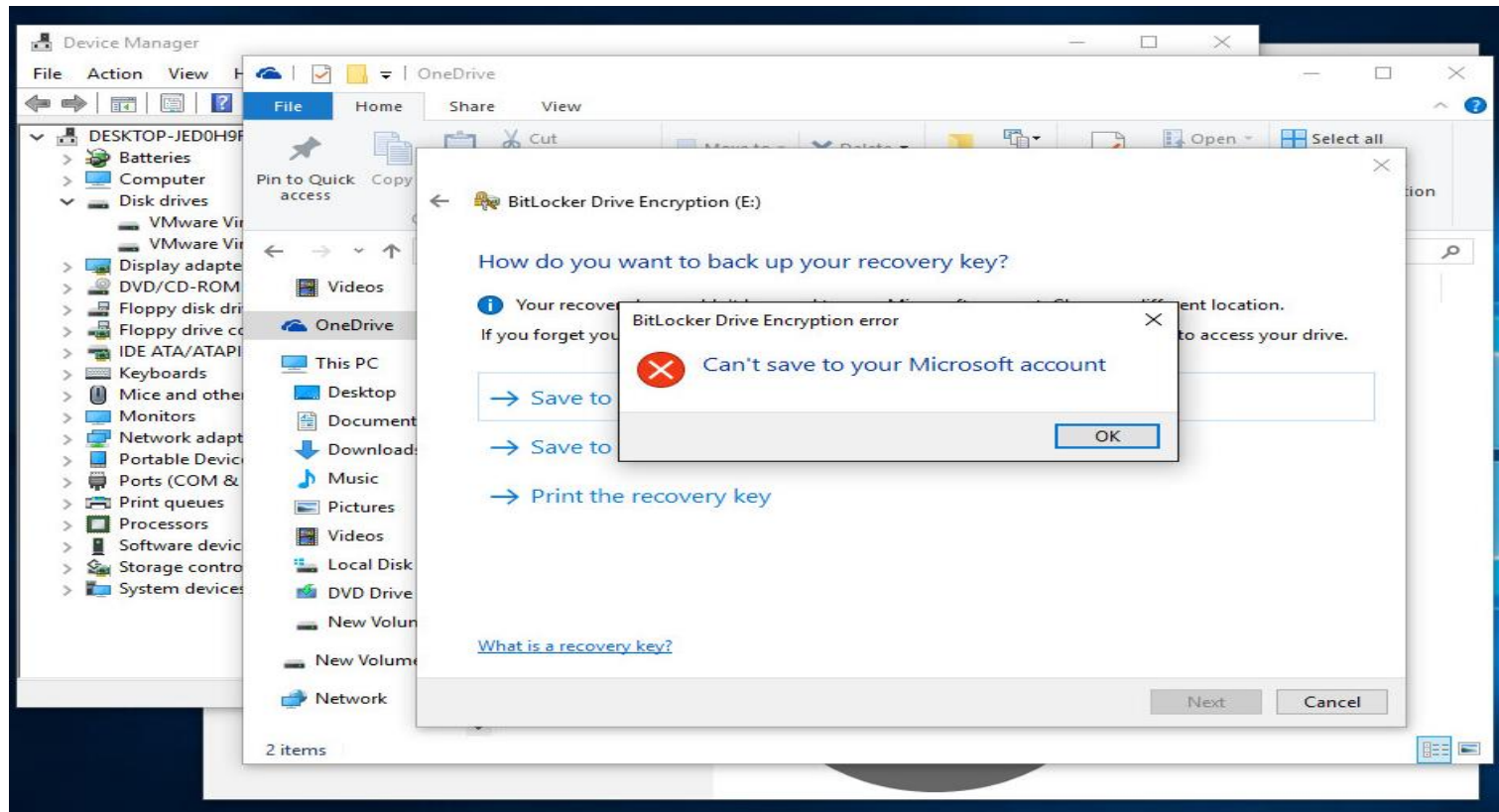
- Windows 10 allows you to backup recovery key to Microsoft, but you never know what happens on the way there and in the cloud



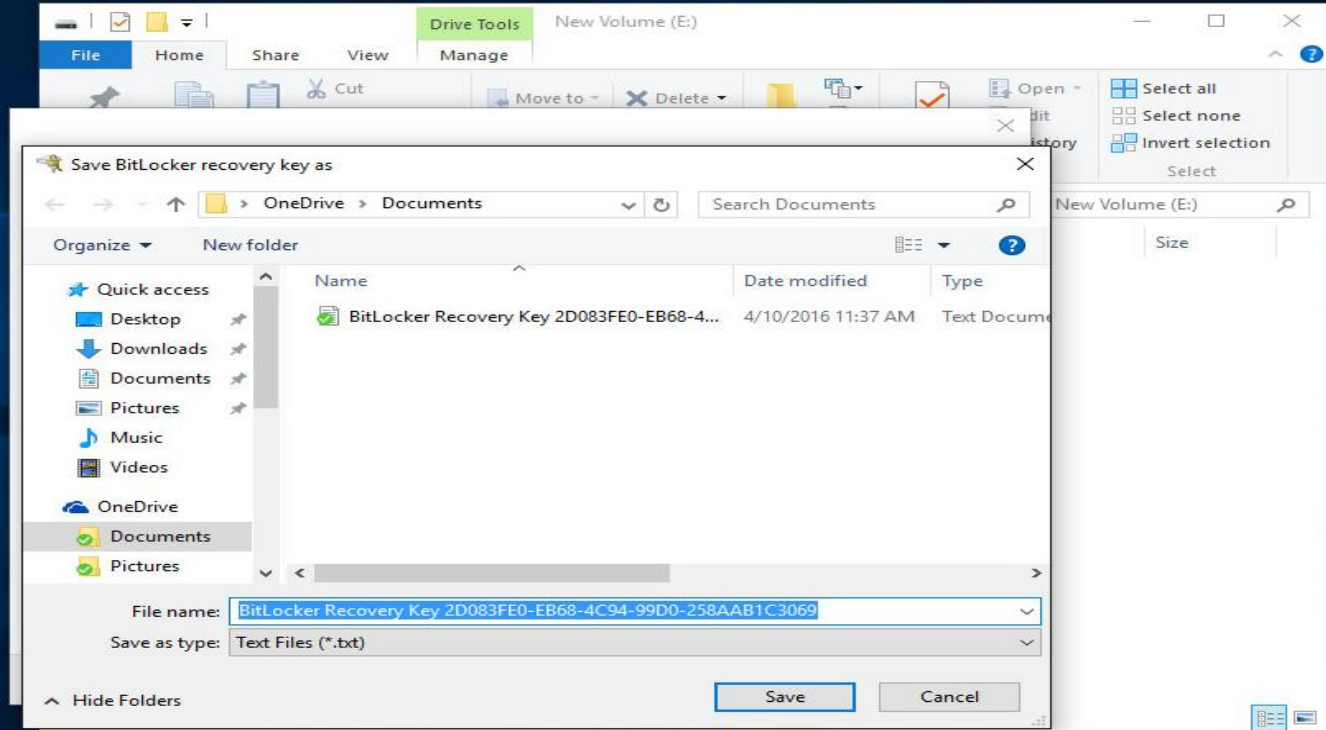
# Even Bitlocker Key is ^h^h was send

```
User-Agent: Microsoft SkyDriveSync 17.3.5907.0716 ship; Windows NT 10.0 (10240)
X-TransactionId: Plat.17.3.5907.0716.357c54f5-4c12-4b9f-a5ba-4a09a8adbb09
X-RequestStats: did=fe86480b-79e4-6cd3-1401-214f65e1f20d
Wlc-Version: 23
Host: act-3-blu.mesh.com
HTTP/1.1 200 OK
Cache-Control: no-store,no-cache
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: application/octet-stream;v0
Last-Modified: Sun, 02 Aug 2015 17:35:12 GMT
ETag: 0
Date: Sun, 02 Aug 2015 17:35:19 GMT
act-3-blu.mesh.comd
4S7ZFSJDEZMZ5YKVWT7UJVUJTQe
-urn:uuid:c992bfe4-2623-9e59-e155-b4ff44d6899c
```

# No warning about wrong certificate, but it stopped working



# But it can still be saved to OneDrive



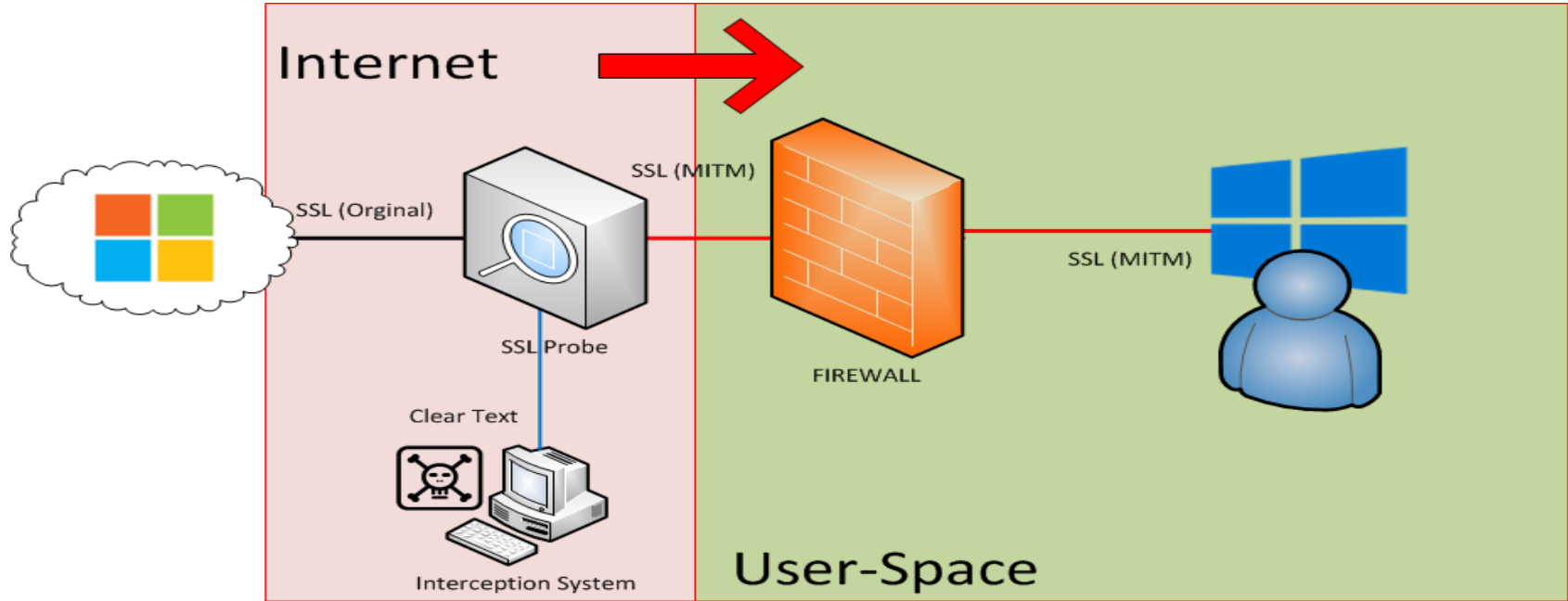


# Create a Microsoft Login User

```
- <s:Envelope>
- <s:Header>
- <wsa:Action s:mustUnderstand="1">
  http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue
</wsa:Action>
<wsa:To s:mustUnderstand="1">https://login.live.com:443/RST2.srf</wsa:To>
<wsa:MessageID>1460307907</wsa:MessageID>
- <ps:AuthInfo Id="PPAuthInfo">
  <ps:HostingApp>{DF60E2DF-88AD-4526-AE21-83D130EF0F68}</ps:HostingApp>
  <ps:BinaryVersion>12</ps:BinaryVersion>
  <ps:UTVersion>1</ps:UTVersion>
  <ps:InlineUX>TokenBroker</ps:InlineUX>
  <ps:IsAdmin>1</ps:IsAdmin>
- <ps:InlineFT>
  DUMCDUTICD0bYjKJfMBOZa*14QFiYOTSGMKR4e6278i0XtrukpflhYCglhvmJTzwViSYMXCwsaP7F9CQ09nwS5zJv*UsUVo*U
</ps:InlineFT>
<ps:Cookies/>
<ps:RequestParams>AQAAAAIAAABsYwQAAAAxMDMz</ps:RequestParams>
<ps:WindowsClientString>GYiC9MzxVTvX57n8/RSuuc87wOt4Pb8tPe5T+Zs8ZeE=</ps:WindowsClientString>
</ps:AuthInfo>
- <wsse:Security>
- <wsse:UsernameToken wsu:Id="user">
  <wsse:Username>bh16talk@outlook.com</wsse:Username>
  <wsse:Password>LVPassword</wsse:Password>
  <wsse:LoginOption>16908291</wsse:LoginOption>
</wsse:UsernameToken>
```


- 
- Back at the Blackhat 2008
  - Lab setup and components
  - Direction User to Microsoft
  - Direction Microsoft to User
  - Office 2013/2016/365
  - Possible improvements
-

# Direction – Microsoft (Cloud) to User



# Microsoft sends strange data to the user system

- Within the interception, data send to Cortana could be intercepted as well ...
- For a full list see appendix - some highlight here ...



```
[..]
{"are you afraid of clowns" : {"LL" : [{"are you afraid of clowns?",2,0.72775}],["are you afraid of clowns?",2,0.72775]}, "TSK" : [], "SUP" : []}}
{"are you better than siri" : {"LL" : [{"are you better than siri?",2,0.282}],["are you better than siri?",2,0.282]}, "TSK" : [], "SUP" : []}}
[..]
{"daemon tools" : {"LL" : [{"daemon tools lite",0,0.17548},["daemon tools",11,0.05972],["http://www.daemon-
tools.cc",11,0.30059],["searchmystuff",101,0.31453]], "TSK" : [2017], "SUP" : []}}
[..]
{"do you have nightmares" : {"LL" : [{"do you have nightmares?",2,0.20188}],["do you have nightmares?",2,0.75405]}, "TSK" : [], "SUP" : []}}
{"do you know siri" : {"LL" : [{"do you know siri?",2,0.31014}],["do you know siri?",2,0.51049]}, "TSK" : [], "SUP" : []}}
{"do you know siri?" : {"LL" : [{"do you know siri?",2,0.81344}], "TSK" : [], "SUP" : []}}
{"do you like dogs" : {"LL" : [{"do you like dogs?",2,0.58014}],["do you like dogs?",2,0.28826]}, "TSK" : [], "SUP" : []}}
{"do you like me" : {"LL" : [{"do you like me?",2,0.29925}],["do you like me?",2,0.57161]}, "TSK" : [], "SUP" : []}}
{"do you like me?" : {"LL" : [{"do you like me?",2,0.88864}], "TSK" : [], "SUP" : []}}
{"do you like siri" : {"LL" : [{"do you like siri?",2,0.18319}],["do you like siri?",2,0.3669],["searchtheweb",100,0.34127]}, "TSK" : [], "SUP" :
[]}}
{"do you love me" : {"LL" : [{"do you love me?",2,0.31556}],["do you love me?",2,0.52486]}, "TSK" : [], "SUP" : []}}
{"do you love me?" : {"LL" : [{"do you love me?",2,0.82589]}, "TSK" : [], "SUP" : []}}
[..]
{"good night" : {"LL" : [{"good night",2,0.8072}], "TSK" : [], "SUP" : []}}
[..]
{"i love you cortana" : {"LL" : [{"i love you cortana",11,0.05048}],["i love you cortana",2,0.79747]}, "TSK" : [], "SUP" : []}}
```


# Microsoft sends strange data to the user system

```
{ "pirat" : { "LL" : [ ["pirate bay",11,0.19389],["pirate bay torrent",11,0.05449],["eve pirate's little helper",0,0.07809],["thepiratebay.se",11,0.05304],["play pirate101",0,0.17275]], "TSK": [671], "SUP": [] }  
{ "pirate" : { "LL" : [ ["pirate bay",11,0.18019],["eve pirate's little helper",0,0.07426],["play pirate101",0,0.16775],["pirate bay torrent",11,0.054],["thepiratebay.se",11,0.05644]], "TSK": [671], "SUP": [] }  
{ "pirate bay" : { "LL" : [ ["http://thepiratebay.se",11,0.21317],["pirate bay",11,0.38584],["https://www.thepiratebay.se",11,0.16775]], "TSK": [671], "SUP": [] }  
{ "piratebay" : { "LL" : [ ["thepiratebay.se",11,0.19765],["searchtheweb",100,0.57437],["pirate bay",11,0.05367]], "TSK": [671], "SUP": [] }  
[...]  
{ "sex" : { "LL" : [ ["searchtheweb",100,0.73567],["searchmystuff",101,0.16243]], "TSK": [], "SUP": [] }  
{ "sex videos" : { "LL" : [ ["searchtheweb",100,0.98422]], "TSK": [], "SUP": [] }  
{ "sexy" : { "LL" : [ ["searchtheweb",100,0.43236],["sexy_sex",10,0.05022],["sexy?",10,0.06043],["sexy girls hd",10,0.06255]], "TSK": [], "SUP": [] }  
[...]  
{ "what are you afraid of" : { "LL" : [ ["what are you afraid of?",2,0.22708],["what are you afraid of",2,0.71611]], "TSK": [], "SUP": [] }  
[...]  
{ "what is the meaning of life" : { "LL" : [ ["what is the meaning of life",11,0.15217],["what is the meaning of life",2,0.51097],["what is the meaning of life?",2,0.21781]], "TSK": [], "SUP": [] }  
{ "what is the meaning of life?" : { "LL" : [ ["what is the meaning of life",11,0.13429],["what is the meaning of life?",2,0.73849]], "TSK": [], "SUP": [] }  
[...]  
{ "you porn" : { "LL" : [ ["searchtheweb",100,0.98472]], "TSK": [], "SUP": [] }  
{ "you suck" : { "LL" : [ ["searchmystuff",101,0.05741],["searchtheweb",100,0.93633]], "TSK": [], "SUP": [] }  
{ "you t" : { "LL" : [ ["http://www.youtube.com",11,0.47237],["youtube music",11,0.05229],["youtube",11,0.20698]], "TSK": [], "SUP": [] }  
{ "you tu" : { "LL" : [ ["youtube",11,0.1877],["youtube music",11,0.05039],["http://www.youtube.com",11,0.48963]], "TSK": [], "SUP": [] }  
{ "you tub" : { "LL" : [ ["http://www.youtube.com",11,0.50179],["youtube",11,0.17374]], "TSK": [], "SUP": [] }  
{ "you tube" : { "LL" : [ ["http://www.youtube.com",11,0.50929],["youtube",11,0.16674]], "TSK": [], "SUP": [] }  
{ "you tube " : { "LL" : [ ["youtube music",11,0.10496],["youtube downloader",11,0.0892],["youtube videos",11,0.06908],["searchtheweb",100,0.58987]], "TSK": [], "SUP": [] }  
{ "you tube.com" : { "LL" : [ ["searchtheweb",100,0.82069]], "TSK": [], "SUP": [] }
```



# Strange Telemetry data

- Microsoft sends Software-strings
  - Any idea for this ?



```
{ "709" : [ "C:\\Tor Browser\\Browser\\firefox.exe", "1" ] }  
[...]  
{ "3262" : [ "{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\GNU\\GnuPG\\gpa.exe", "1" ] }  
{ "3263" : [ "{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\GNU\\GnuPG\\kleopatra.exe", "1" ] }  
[...]  
{ "4013" : [ "{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\PGP Corporation\\PGP  
Desktop\\PGPdesk.exe", "1" ] }  
[...]  
  
{ "4761" : [ "{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\aMule\\amule.exe", "1" ] }  
[...]  
{ "4779" : [ "{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\eMuleTorrent\\eMuleTorrent.exe", "1" ] }  
{ "4780" : [ "{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\eMule\\emule.exe", "1" ] }
```

- Why is Microsoft interested in installed encryption or privacy software ?

7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E = C:\ProgramFilesX86

- 
- Back at the Blackhat 2008
  - Lab setup and components
  - Direction User to Microsoft
  - Direction Microsoft to User
  - Office 2013/2016/365
  - Possible improvements
-

# Office is worse (Office 2013/ Office 2016)



- Office sends every configuration and interaction to Microsoft
  - Access, Excel, OneNote, PowerPoint, Project, Publisher, Visio and Word
    - Telemetry sends Hardware, Software (Office Clicks and Use, complete user data and use data, etc ...)
  - File name, File format (extension), Size, Author, Location, Title, Office Version,
- All send to a US Datacenter



# Office collection example Word



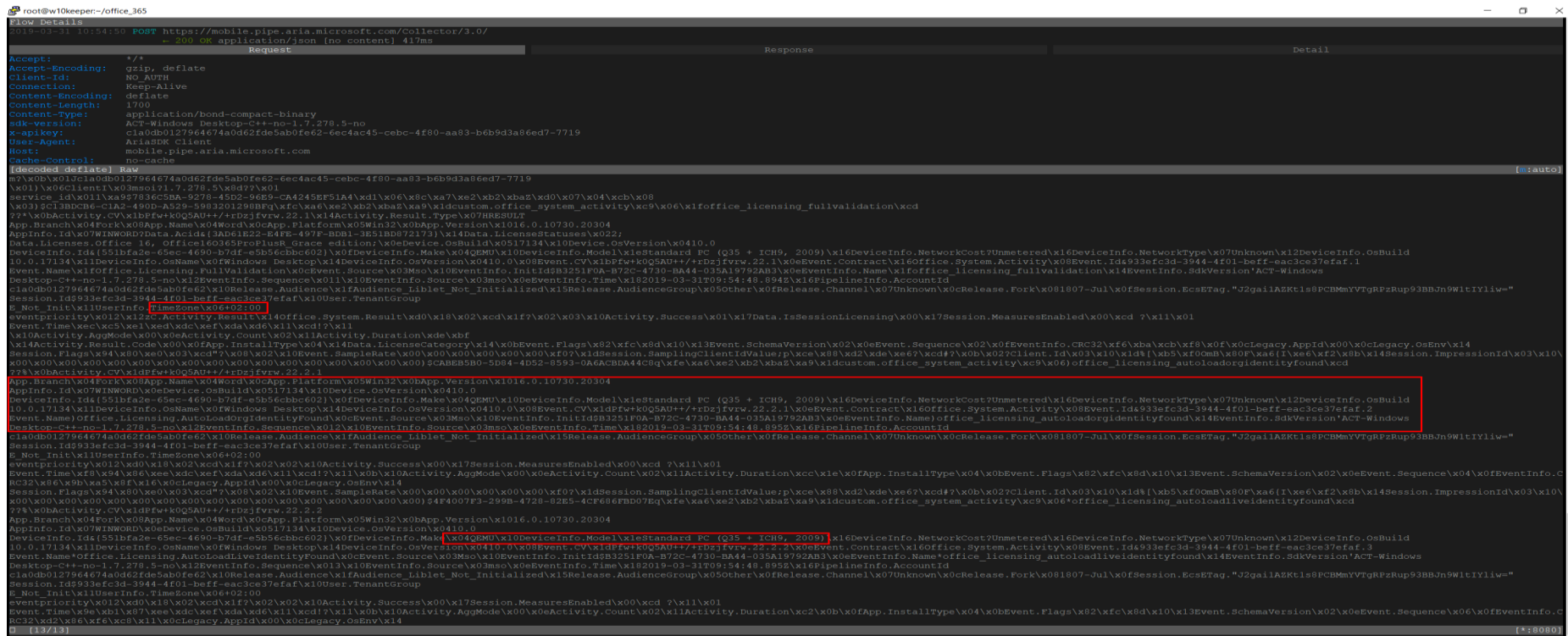
```
User-Agent: Microsoft Office/16.0 (Windows NT 10.0; Microsoft Word 16.0.6701; Pro)
X-IDCRL_ACCEPTED: t
X-Office-Version: 16.0.6701
X-Office-Application: 0
X-Office-Platform: Win32
X-Office-SqmUserId: {35BEEC9A-0FA6-41A0-B05E-4656C64464EC}
X-Office-LastUpdate: 2016-08-22T20:32:43Z
X-Office-SusClientId: 82e544ce-1a72-4842-ab5f-2506eef2c8fe
Host: officeclient.microsoft.com
GET /ab?&clientid=%7b35BEEC9A-0FA6-41A0-B05E-4656C64464EC%7d HTTP/1.1
Connection: Keep-Alive
User-Agent: Microsoft Office 2014
X-MSEdge-AppID: word
X-OCAS-Platform: win32
X-OCAS-IsEnterprise: 1
X-OCAS-Build: 16.0.6741
X-OCAS-IsSubscription: 0
X-MSEdge-IG: 8899FE7B-24AD-4A3A-ABD4-83F4CBC6FB2D
Host: ocos-office365-s2s.msedge.net
VGET /ab?&clientid=%7b35BEEC9A-0FA6-41A0-B05E-4656C64464EC%7d HTTP/1.1

Host: nexus.officeapps.live.com
Production_CBB Production NoNL::NoFlights Z97X-SLI+
Gigabyte Technology Co., Ltd.K
winword.exe en-US 10.0 78cf6450d9d71352_LiveId winword.exe 10.0 78cf6450d9d71352_LiveId
x64E To be filled by O.E.M. To be filled by O.E.M. 02025-010-47974016B7f 02025-010-47974016B7+ To be filled by O.E.M.
Z97X-SLI Gigabyte Technology Co., Ltd.f
```

# Office collection example Excel



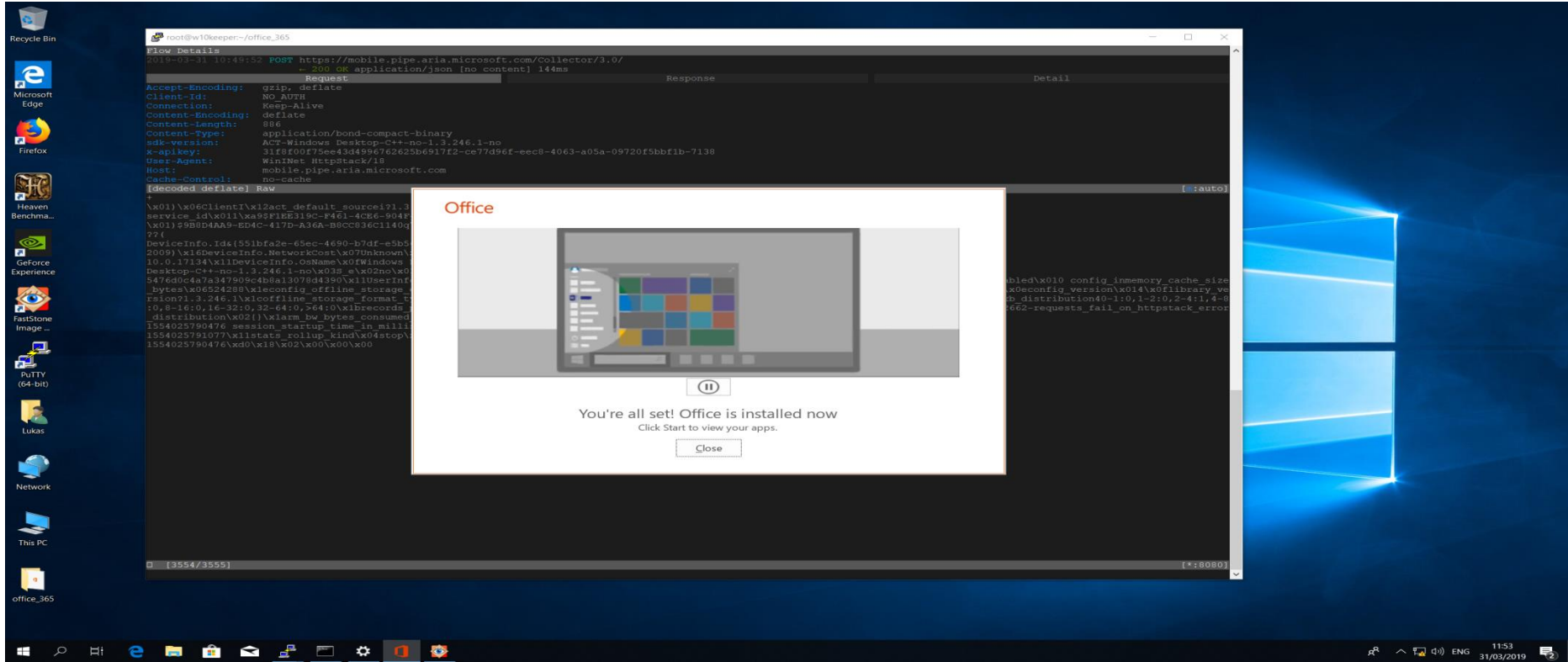
```
XLDesktop Command Execution:119
XLDesktop Command Execution:119d
FileIO::CMsoOLDocBase::Lockd
)FileIO::CMsoOLDocBase::HrReadWriteLockCmd
4PlacesPickerFeatureServiceList::GetAppSaveAsFindFiled =<E@
3PlacesPickerFeatureServiceList::FGetDefaultFilePathd DocToIdentityMapping::Initd
3MsoDocs.DesktopBackstage.Navigation.ReadLocalFolderd 8MsoDocs.DesktopBackstage.Navigation.UpdateNavContentListd /{Tb0
1MsoDocs.DesktopBackstage.Navigation.SaveFileCached
2MsoDocs.DesktopBackstage.Navigation.ReadThisPCRootd
+FileIO::CMsoOLDocBaseImpIOLDoc2::BeginCmdExd
&Excel.DesktopBackstage.SaveAs.SaveFile FileIO::CMsoOLDocBase::LockdG
%Excel.DesktopBackstage.SaveAs.LoadCFD+FileIO::CMsoOLDocBaseImpIOLDoc2::BeginCmdExd
%Excel.DesktopBackstage.SaveAs.LoadCFD&Excel.DesktopBackstage.SaveAs.LoadCFDd&Excel.DesktopBackstage.SaveAs.SaveFile
,FileIO::CMsoOLDocBaseImpIOLDoc2::RecordEventd&Excel.DesktopBackstage.SaveAs.SaveFile
+FileIO::CMsoOLDocBaseImpIOLDoc2::BeginCmdExd+FileIO::CMsoOLDocBaseImpIOLDoc2::BeginCmdEx
FileIO::CMsoOLDocBase::Lockd&Excel.DesktopBackstage.SaveAs.SaveFile
)FileIO::CMsoOLDocBase::HrReadWriteLockCmdrr q?
&Excel.DesktopBackstage.SaveAs.SaveFileMso.OpenXml.OpenPackageda2U0*
&Excel.DesktopBackstage.SaveAs.SaveFileXLShared ISAVE::HrSaved
XLDesktop Manual Save%FileIO::CMsoOLDocFile::HrDownloadTempdb2U0*
XLDesktop Manual SaveMso.OpenXml.OpenPackaged
XLDesktop Manual SaveXLDesktop Manual Saved
&Excel.DesktopBackstage.SaveAs.SaveFile
FileIO::CMsoOLDocFile::Saved
,FileIO::CMsoOLDocBaseImpIOLDoc2::RecordEvent
)FileIO::CMsoOLDocBase::HrReadWriteLockCmd
,FileIO::CMsoOLDocBaseImpIOLDoc2::RecordEvent
,FileIO::CMsoOLDocBaseImpIOLDoc2::RecordEventd
,FileIO::CMsoOLDocBaseImpIOLDoc2::RecordEvent
1MsoDocs.DesktopBackstage.Navigation.LoadFileCachee
,DocToIdentityMapping::TryIdentityParentMatche
'DocToIdentityMapping::GetIdentityForVUrl
'DocToIdentityMapping::GetIdentityForUrle
1MsoDocs.DesktopBackstage.Navigation.SaveFileCachee
```



# Time of use / time of display

- Without the user consent, the Office 365 installer is transferring telemetry data to the US without getting the user consent first before doing it
- Telemetry data is not complaint in ANY case with the DGSVO
- No „opt-out“ or better optional „opt-in“ is offered

# Time of use / time of display



# Office 365 installer



- Installer works through the man in the middle proxy
- Why so many wildcard certificates ?
  - One lost certificate and the whole Office 365 installation base is doomed !

```
Flow Details
2019-03-31 10:25:38 GET https://fp.msedge.net/conf/v1/asgw/fpconfig.min.json HTTP/2.0
    ↳ 200 application/json 2k 167ms
Request Response Detail
Server Connection:
  Address      fp.msedge.net:443
  Resolved Address 204.79.197.222:443
  HTTP Version  HTTP/2.0
  ALPN         h2
Server Certificate:
  Type      RSA, 2048 bits
  SHA1 digest FA:81:E0:D1:B5:51:62:0C:6F:DC:CA:EF:7E:BF:06:44:0D:CD:0A:97
  Valid to   2020-12-13 22:54:06
  Valid from 2018-12-13 22:54:06
  Serial     490617672716690239293469482390990250196582841
  Subject    CN *.msedge.net
  Issuer     C US
             ST Washington
             L Redmond
             O Microsoft Corporation
             OU Microsoft IT
             CN Microsoft IT TLS CA 4
  Alt names  *.msedge.net, *.a-msedge.net, a-msedge.net, b-msedge.net, *.b-msedge.net, c-msedge.net, *.c-msedge.net, dc-msedge.net, *.dc-msedge.net, *.lbas.msedge.net,
             *.test.msedge.net, *.azp.footprintdns.com, *.footprintdns.com, *.clo.footprintdns.com, *.any.footprintdns.com, *.nrb.footprintdns.com, *.perf.msedge.net,
             *.fp.measure.office.com
Client Connection:
  Address      ::ffff:192.168.0.33:50019
  HTTP Version HTTP/2.0
  TLS Version  TLSv1.2
  Server Name Indication fp.msedge.net
  Cipher Name  ECDHE-RSA-AES128-GCM-SHA256
  ALPN         h2
Timing:
  Client conn. established 2019-03-31 10:25:37.942
  Server conn. initiated   2019-03-31 10:25:37.953
  Server conn. TCP handshake 2019-03-31 10:25:38.044
  Server conn. TLS handshake 2019-03-31 10:25:38.100
  Client conn. TLS handshake 2019-03-31 10:25:38.114
  First request byte       2019-03-31 10:25:38.119
  Request complete         2019-03-31 10:25:38.226
  First response byte      2019-03-31 10:25:38.282
  Response complete        2019-03-31 10:25:38.287
```

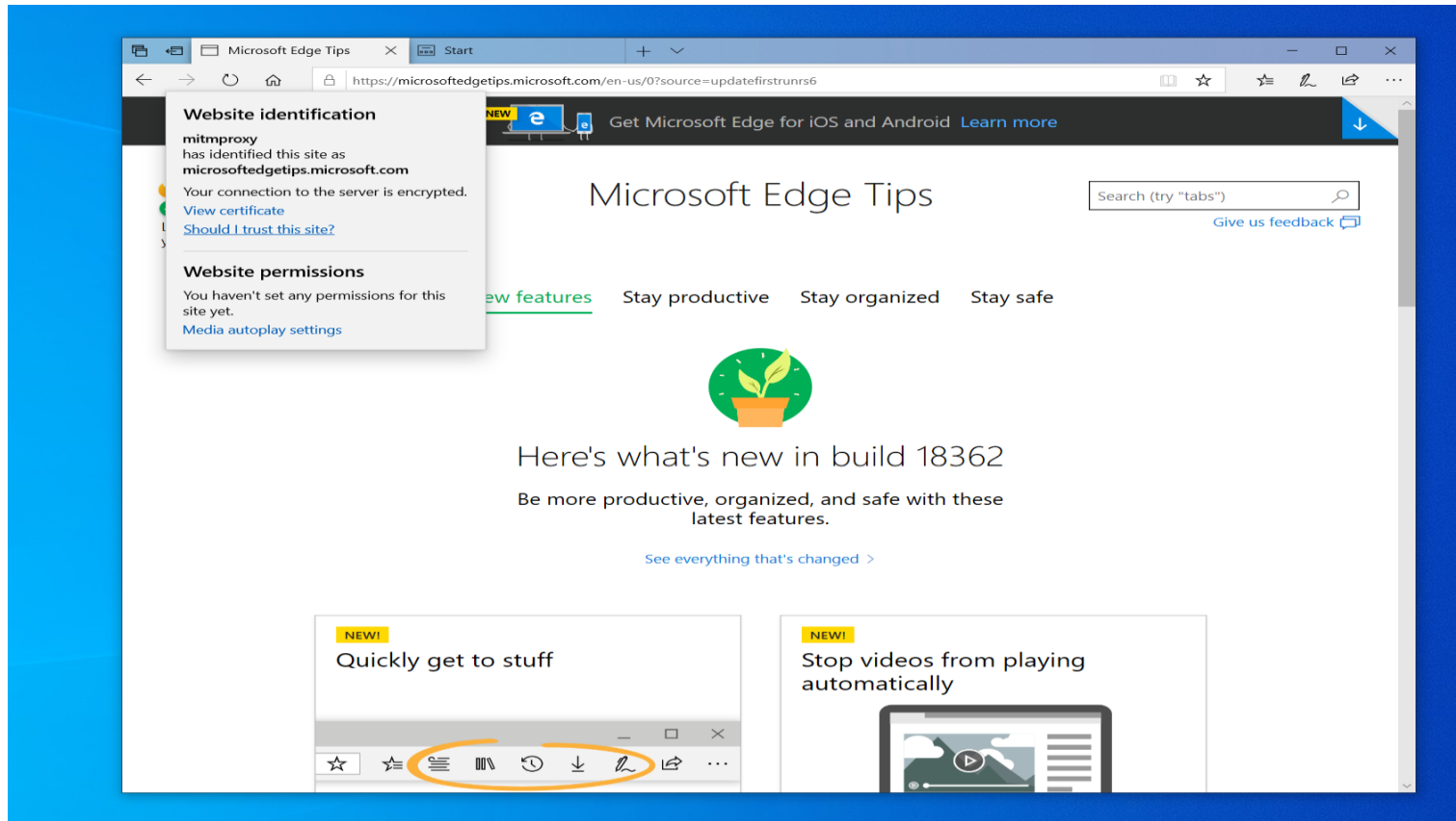
**dn**  
*Systems*

- [illegible]

- 
- Back at the Blackhat 2008
  - Lab setup and components
  - Direction User to Microsoft
  - Direction Microsoft to User
  - Office 365 & Bonus W10 1903
  - Possible improvements
-




# Windows 1903 in details



# Windows 1903 and Office 365

dn  
Systems



The screenshot shows a Windows 1903 desktop environment. In the center, there is a window titled "Office" with a close button (X). Inside the window, there are icons for Office applications: Outlook, Word, Excel, PowerPoint, OneDrive, and Skype. Below the icons, there is a message in German: "Bleiben Sie bitte online, während Office heruntergeladen wird." (Please stay online while Office is being downloaded). Below the message, there is a progress bar and the text "Wir sind gleich fertig." (We are almost done).

On the right side of the screenshot, there is a network traffic capture window showing a list of network packets. The packets are captured on the interface "eth0" and show a series of HTTP requests and responses between the client and the Office 365 servers. The packets are numbered 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000.

- Click-to-Run via Interception Proxy

# Windows 1903 Telemetry

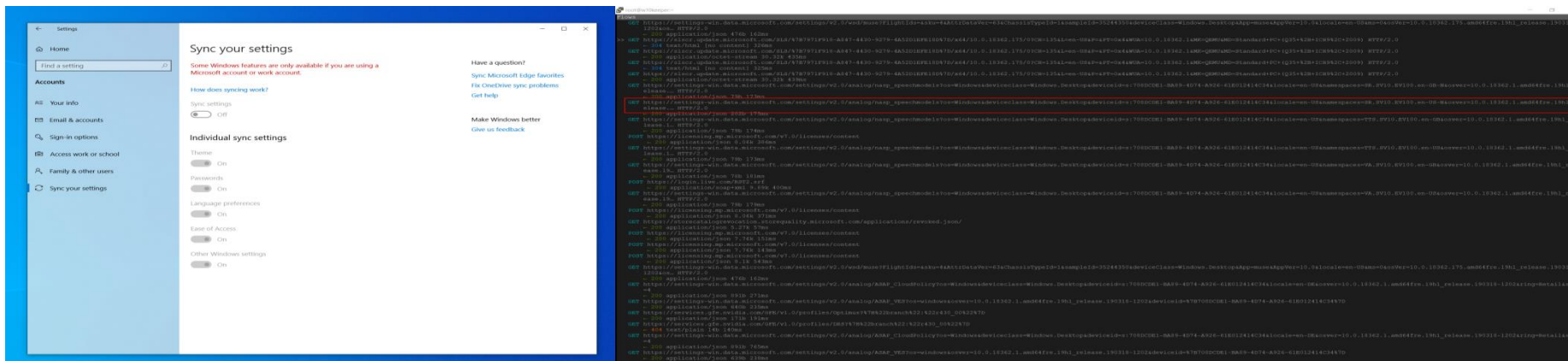


- Telemetry seems to be certificate pinned

```
:ffff:192.168.0.33:50680: Certificate verification error for watson.telemetry.microsoft.com: unable to get local issuer certificate (errno: 20, depth: 1)
:ffff:192.168.0.33:50680: Ignoring server verification error, continuing with connection
:ffff:192.168.0.33:50680: TcpDisconnect("(32, 'EPIPE')"),
192.168.0.33:50680: clientdisconnect
192.168.0.33:50681: clientconnect
:ffff:192.168.0.33:50681: Certificate verification error for watson.telemetry.microsoft.com: unable to get local issuer certificate (errno: 20, depth: 1)
:ffff:192.168.0.33:50681: Ignoring server verification error, continuing with connection
:ffff:192.168.0.33:50681: TcpDisconnect("(32, 'EPIPE')"),
192.168.0.33:50681: clientdisconnect
192.168.0.33:50682: clientconnect
:ffff:192.168.0.33:50682: Certificate verification error for watson.telemetry.microsoft.com: unable to get local issuer certificate (errno: 20, depth: 1)
:ffff:192.168.0.33:50682: Ignoring server verification error, continuing with connection
:ffff:192.168.0.33:50682: TcpDisconnect("(104, 'ECONNRESET')"),
192.168.0.33:50682: clientdisconnect
192.168.0.33:50683: clientconnect
:ffff:192.168.0.33:50683: Certificate verification error for watson.telemetry.microsoft.com: unable to get local issuer certificate (errno: 20, depth: 1)
:ffff:192.168.0.33:50683: Ignoring server verification error, continuing with connection
192.168.0.33:50683: clientdisconnect
192.168.0.33:50684: clientconnect
:ffff:192.168.0.33:50684: Certificate verification error for watson.telemetry.microsoft.com: unable to get local issuer certificate (errno: 20, depth: 1)
:ffff:192.168.0.33:50684: Ignoring server verification error, continuing with connection
192.168.0.33:50684: clientdisconnect
192.168.0.33:50685: clientconnect
:ffff:192.168.0.33:50685: Certificate verification error for watson.telemetry.microsoft.com: unable to get local issuer certificate (errno: 20, depth: 1)
:ffff:192.168.0.33:50685: Ignoring server verification error, continuing with connection
:ffff:192.168.0.33:50685: TcpDisconnect("(32, 'EPIPE')"),
192.168.0.33:50685: clientdisconnect
192.168.0.33:50686: clientconnect
:ffff:192.168.0.33:50686: Certificate verification error for watson.telemetry.microsoft.com: unable to get local issuer certificate (errno: 20, depth: 1)
:ffff:192.168.0.33:50686: Ignoring server verification error, continuing with connection
:ffff:192.168.0.33:50686: TcpDisconnect("(32, 'EPIPE')"),
192.168.0.33:50686: clientdisconnect
192.168.0.33:50687: clientconnect
:ffff:192.168.0.33:50687: Certificate verification error for watson.telemetry.microsoft.com: unable to get local issuer certificate (errno: 20, depth: 1)
:ffff:192.168.0.33:50687: Ignoring server verification error, continuing with connection
:ffff:192.168.0.33:50687: TcpDisconnect("(32, 'EPIPE')"),
192.168.0.33:50687: clientdisconnect
```

**dn**  
*Systems*

- Why is W10-1903 connecting to setting sync ?



- 
- Back at the Blackhat 2008
  - Lab setup and components
  - Direction User to Microsoft
  - Direction Microsoft to User
  - Office 2013/2016/365
  - Possible improvements

# Suggested improvements

- Offer MSI and make „Click-to-Run“ optional, it´s a high risk in environment and unsecure
- Cloud offering optional (Store, OneDrive, Cortana, ..)
- Comply with EU-GDPR

# Questions ?



# Thank You

**dn**  
*Systems*

**dn**  
*Systems*

**DN-Systems GmbH**  
**Hornemannstr. 12/13**  
**31137 Hildesheim, Germany**  
**Phone: +49-5121-28989-0**  
**Mail: [info@dn-systems.de](mailto:info@dn-systems.de)**