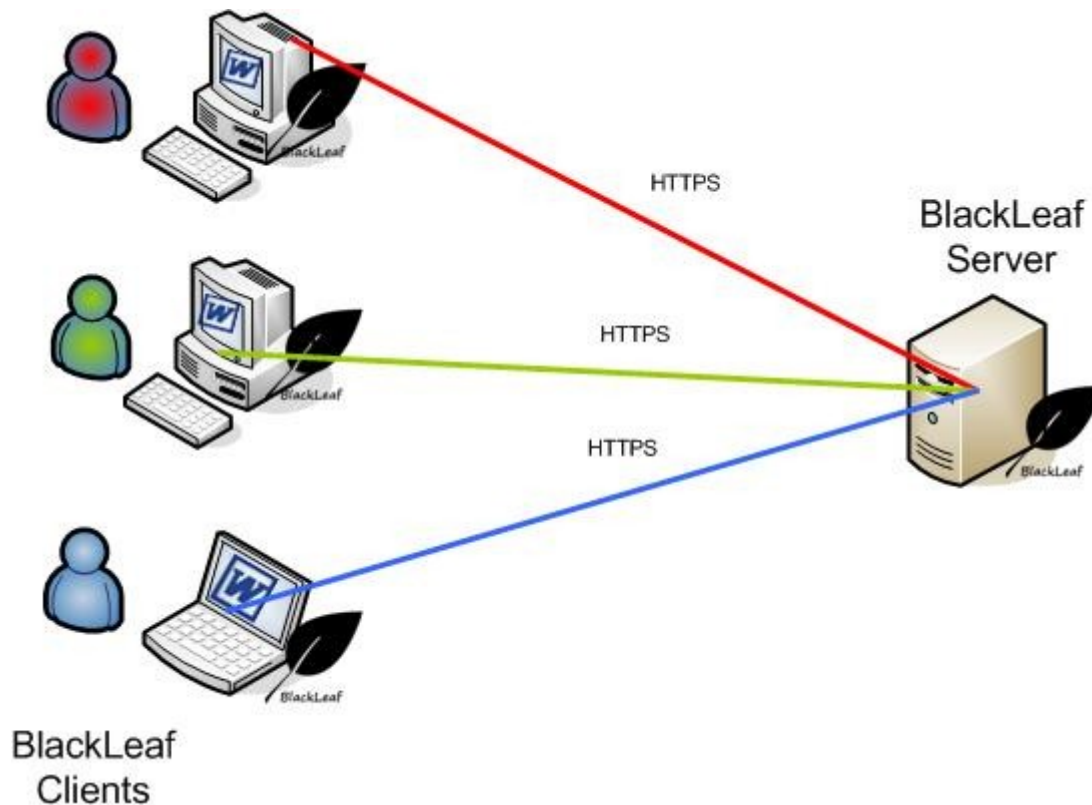




- **Word Spying Software**
- Developed by Ruben Santamarta, Wintercore.

BlackLeaf is a framework that allows to capture every document opened in Microsoft Word. It is intended for pentesting and monitoring purposes.

BlackLeaf is developed following a client/server architecture.



- **BlackLeaf clients**

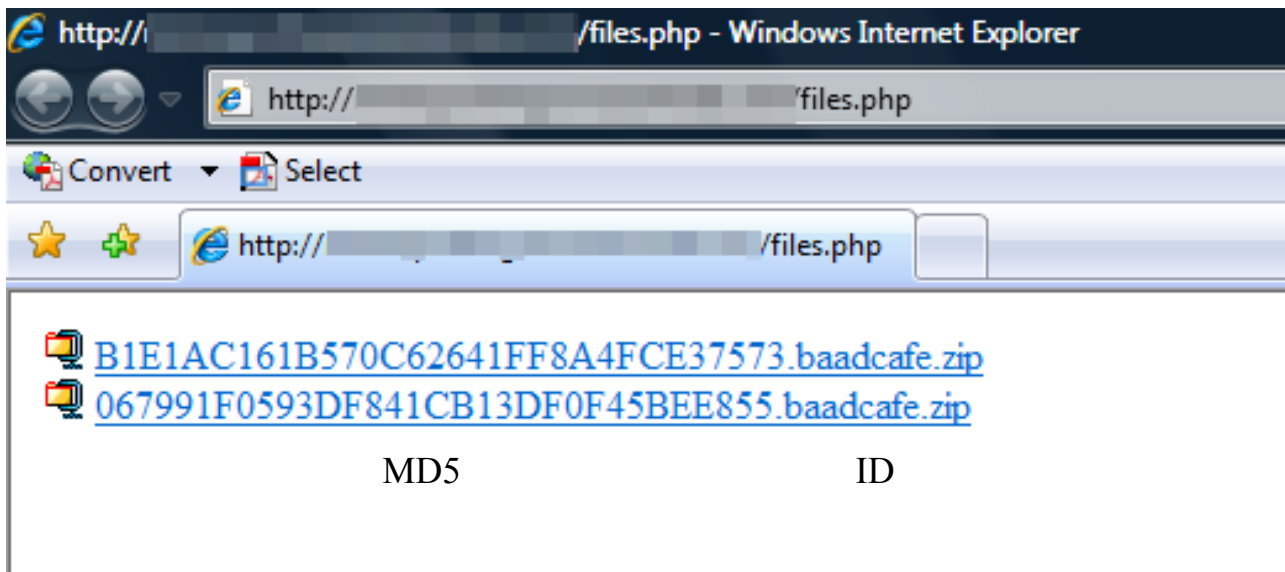
The client must be installed on the target's computer. The program to do so is included within the framework, it silently drops, runs and configures all the needed components without user interaction ( requires admin privileges).

- **BlackLeaf Server**

The server components are PHP script files that must be uploaded to a web hosting. Even free hosting accounts can albergate these files.

Once the client is installed on the target's machine, it interacts with Word in a manner that allows that every document opened in it will be uploaded to a remote server of your choosing. Even the password protected documents will be uploaded and unprotected.

The documents are zipped and uploaded to the remote server, being identified by their MD5 and a configurable 32-bit identification number in order to distinguish the source.



BlackLeaf client uses HTTPS to securely upload the documents. A valid certificate is not needed, self-signed certificates do the work, although your hosting server should accept HTTPS requests.

- Works on Word XP, 2003 and 2007.
- Works on 2000, XP, 2003, 2008, Vista, Windows 7.
- You just need a web hosting where the files will be uploaded.
- Bypasses Word's password protection. You receive the document unprotected.
- Bypasses Kaspersky IS 2009, Symantec Norton 360 2.0 and McAfee IS 2009 among others...
- Files are identified by a customizable identification number to distinguish their source.
- Obtains the exact location from where the document was opened.
- Point-and-click configuration

Video:

<http://blackleaf.reversemode.com/demo.avi>

contact (at) reversemode (dot) com [email concealed]

[www.reversemode.com](http://www.reversemode.com)

[www.wintercore.com](http://www.wintercore.com)