ACCESSING THE DOCUMENT OBJECT


```
STDMETHODIMP Invoke( DISPID dispidMember, REFIID riid, LCID lcid, WORD wFlags, DISPPARAMS*
pDispParams, VARIANT* pvarResult, EXCEPINFO*  pExcepInfo,  UINT* puArgErr )
{
        CComPtr<IDispatch> spDisp;
        if ( dispidMember == DISPID_DOCUMENTCOMPLETE ) {
                m_spWebBrowser2 = pDispParams->rgvarg[1].pdispVal;
                CComPtr<IDispatch> pDisp;
                HRESULT hr = m_spWebBrowser2->get_Document( &pDisp );
                if ( FAILED( hr ) ) break;
                CComQIPtr<IHTMLDocument2, &IID_IHTMLDocument2> spHTML;
                spHTML = pDisp;
                if ( spHTML ) {
                        // Get the BODY object
                        CComPtr<IHTMLElement> m_pBody;
                        hr = spHTML->get_body( &m_pBody );
                        // Get the HTML text
                        BSTR bstrHTMLText;
                        hr = m_pBody->get_outerHTML( &bstrHTMLText );
                        // Get the URL
                        CComBSTR url;
                        m_spWebBrowser2->get_LocationURL( &url );
                }
        }
        return S_OK;
}
```

AGENDA

- Overview of the attack
- Demos
- General analysis
- Technical analysis
- **How to defend?**
- Conclusion
- Questions and Answers

CONCLUSION

- Attack can be selective, personalized
  - => The malicious can connect to an external website and download specific information

- You should not trust what you see (especially if this is not your computer)

- Use BHOWatcher to regurarly check the BHO installed on your computer