Hack any website

Defcon 11 – 2003 Edition - Alexis Park, Las Vegas, USA
Grégoire Gentil
CEO and CTO of Twingo Systems

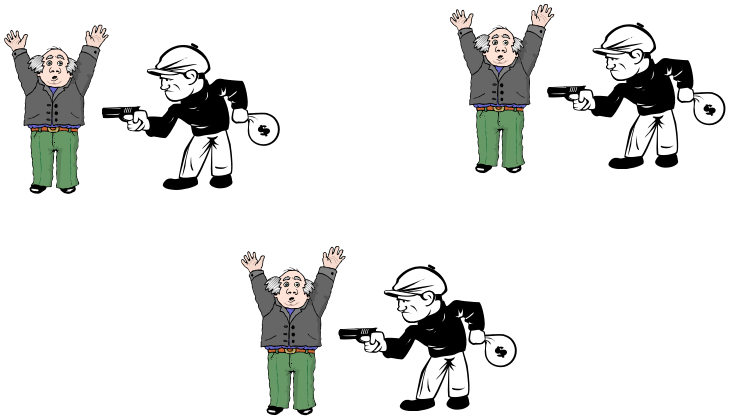
AGENDA

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

WHAT CAN YOU DO WHEN YOU WANT TO STEAL MONEY?

• You can either attack the bank…

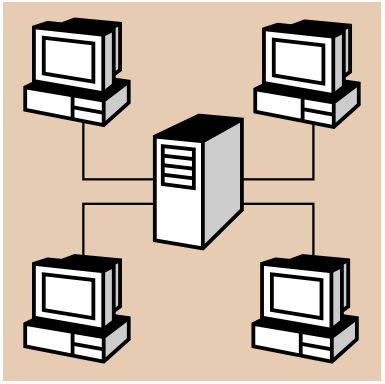
• Or you can attack all the customers of the bank



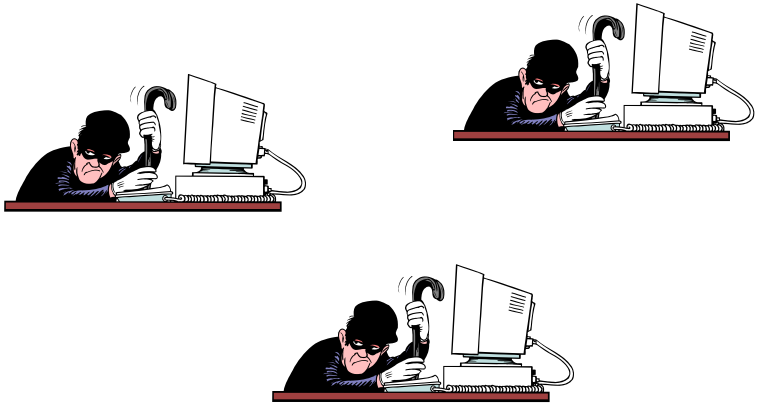
• But be careful, security can be tough

WHAT CAN YOU DO WHEN YOU WANT TO HACK A WEBSITE?

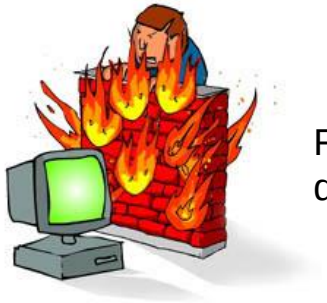
- You can either attack the server…



- Or you can attack all the clients



- But be careful, security can be tough



Firewall, intrusion detection, anti-virus, …

- This is what I will teach you today

AGENDA

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

DEMOS

- Demo 1: Dynamic modification of the content of a webpage

  ⇒ Modify the homepage of a media website

- Demo 2: Dynamic modification of the javascript of a webpage

  ⇒ Modify the features of the list view of a webmail

AGENDA

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

SCOPE OF THE SECURITY VULNERABILITY

• Requires Internet explorer 4.0 and Windows 95 or later

⇒ Google Zeitgeist (http://www.google.com/press/zeitgeist.html) shows that more than 90% of the Google requests come from Windows – Internet Explorer

• Requires DLL registration

⇒ An executable must be run once with “Power user” privileges

⇒ Many privilege escalation and code execution from a webpage without user intervention have been discovered

• As you will see through this presentation, the attack is extremely generic and can lead to a lot of malicious scenarii.

ADVANTAGES OF THE ATTACK

• No modification on the targeted server is required

• The attack uses a feature developped by Internet Explorer!!!

⇒ Microsoft provides and supports all the required tools

• The installed DLL cannot be detected by anti-virus. This is a standard DLL with no specific signature or whatsoever

• You can “personalize” the attack for all the clients

• You can attack only one client

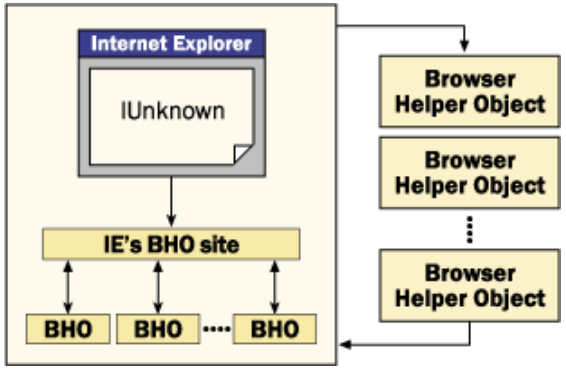
AGENDA

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

INTRODUCING BROWSER HELPER OBJECTS

• Implemented as COM in-process DLL and loaded by Internet Explorer.

• The browser initializes the object and asks it for a certain interface. If that interface is found, Internet Explorer uses the methods provided to pass its **IUnknown** pointer down to the helper object



• Implemented also in Explorer

• See Dino Esposito article “Browser Helper Objects: The Browser the Way You Want It” in MSDN

ACCESSING THE INTERFACE OF THE BROWSER

- The IObjectWithSite Interface: HRESULT SetSite(IUnknown* pUnkSite)

  ⇒ Receives the IUnknown pointer of the browser. The typical implementation will simply store such a pointer for further use

```
HRESULT SetSite( IUnknown* pUnkSite )
{
	if ( pUnkSite != NULL ) {
		m_spWebBrowser2 = pUnkSite;
		if ( m_spWebBrowser2 ) {
			// Connect to the browser in order to handle events
			if ( ! ManageConnection( Advise ) )
				MessageBox( NULL, "Error", "Error", MB_ICONERROR );
		}
	}
	return S_OK;
}
```

GETTING THE BROWSER EVENTS

- The IConnectionPoint interface: HRESULT Connect(void)

  ⇒ To intercept the events fired by the browser, the BHO needs to connect to it via an IConnectionPoint interface and pass the IDispatch table of the functions that will handle the various events

```
HRESULT Connect( void )
{
	HRESULT hr;
	CComPtr<IConnectionPoint> spCP;
	// Receives the connection point for WebBrowser events
	hr = m_spCPC->FindConnectionPoint( DIID_DWebBrowserEvents2, &spCP );
	if ( FAILED( hr ) )
		return hr;

	// Pass our event handlers to the container. Each time an event occurs
	// the container will invoke the functions of the IDispatch interface we implemented
	hr = spCP->Advise( reinterpret_cast<IDispatch*>(this), &m_dwCookie );
	return hr;
}
```

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;
}
```

REGISTRING AND INSTALLING THE COMPONENT

• Register the DLL (regsvr32.exe myBHO.dll for instance) and create a key in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows\CurrentVersion\Explorer\Browser Helper Objects with the GUID of the component

⇒ The next instance of Internet Explorer will automatically load the BHO

AGENDA

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

SOME POSSIBLE DEFENSES

- Disable all or selected BHOs installed on the client

  ⇒ Simply Enumerate the BHOs from the registry and analyze the DLL information (see code on the DefCon CD)

```
HKEY hkey;
TCHAR szPath = “SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Browser Helper Objects”;
If ( RegOpenKey( HKEY_LOCAL_MACHINE, szPath, &hkey ) == ERROR_SUCCESS ) {
        TCHAR szGUID[255];
        LONG ret = RegEnumKey( HKEY_LOCAL_MACHINE, 0, szGUID, 255 );
        Int i = 0;
        while ( ( ret != ERROR_NO_MORE_ITEMS ) && ( ret == ERROR_SUCCESS ) ) {
                // You have the BHO GUID in szGUID
                ret = RegEnumKey ( HKEY_LOCAL_MACHINE, i, szGUID, 255 );
                i++;
        }
}
```

- Main drawback: Pretty painful as BHOs can be sometimes useful

  ⇒ Acrobat plug-in is a BHO, Google toolbar uses BHO, …

SOME POSSIBLE OTHER DEFENSES

- Microsoft could improve BHO support in coming releases of Internet Explorer

  ⇒ Create a tag <disableBHO> to disable all BHOs for a given web page

  ⇒ Implement an authentication system to disable only non approved BHOs (implementation of a tag <disableNonApprovedBHO>)

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

CONTACT INFORMATION

- Main contact: Gregoire Gentil
  CEO and CTO of Twingo Systems
  gregoire@twingosystems.com

- Company: Twingo Systems, Inc.
  Provides security tool to secure the untrusted computer

AGENDA

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

QUESTIONS AND ANSWERS

- If you have any question, it is the moment to ask…