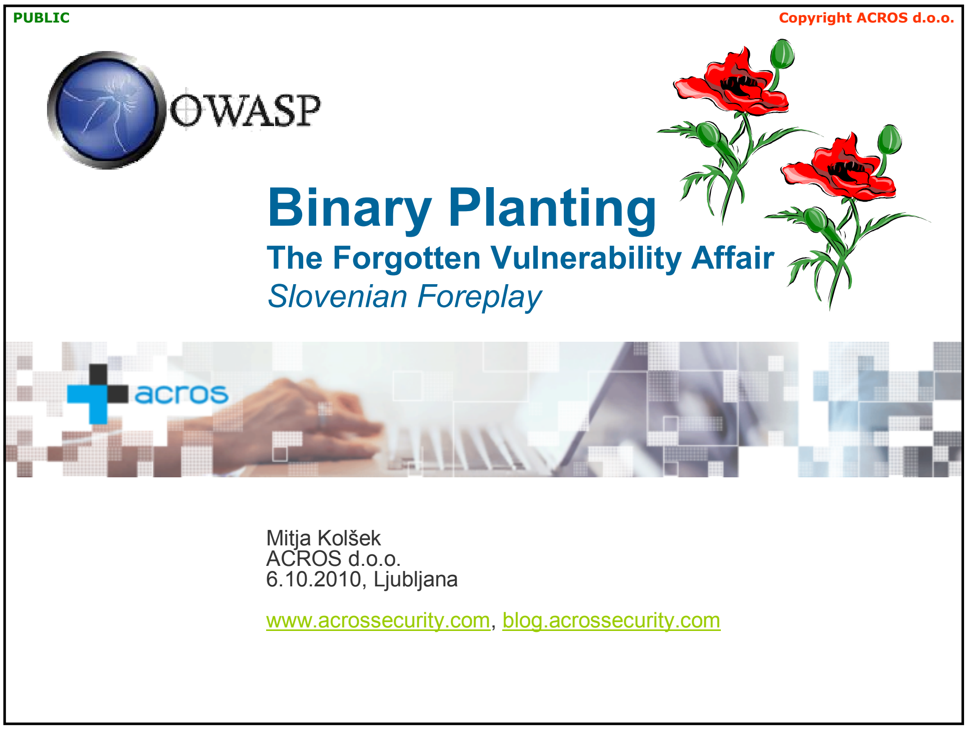


Binary Planting

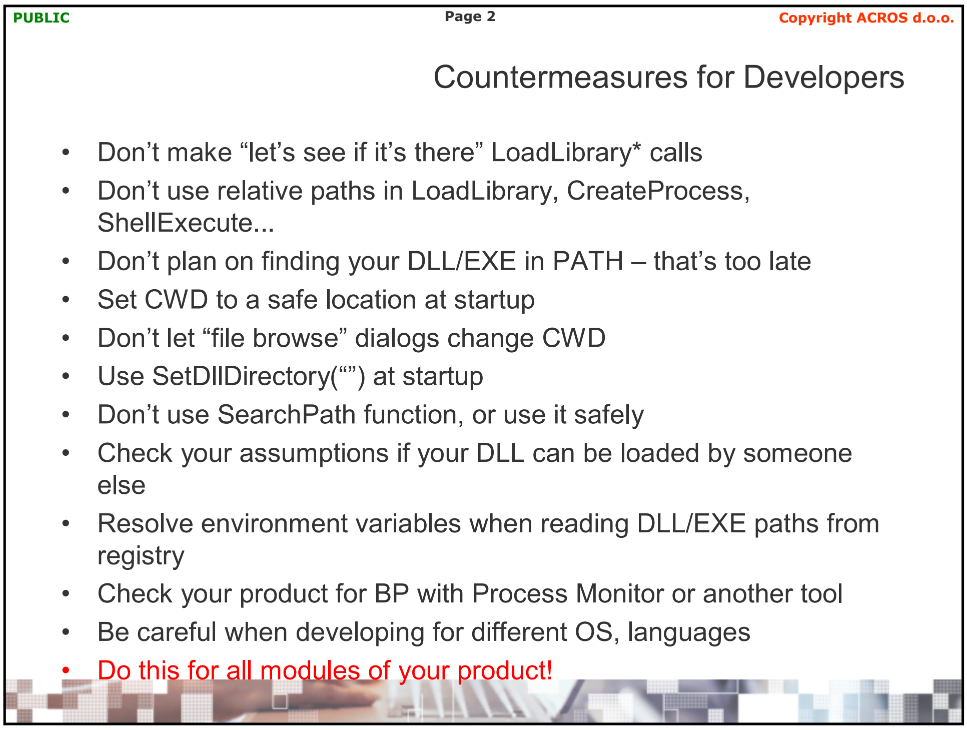
The Forgotten Vulnerability Affair

Slovenian Foreplay

OWASP
acros

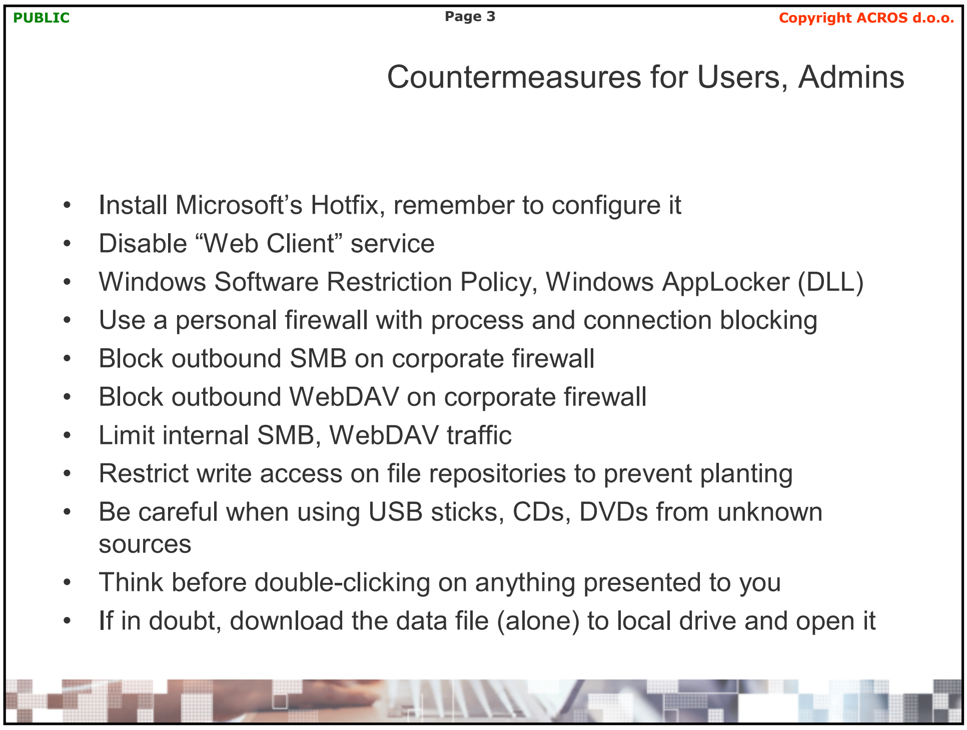
Mitja Kolšek
ACROS d.o.o.
6.10.2010, Ljubljana

www.acrossecurity.com, blog.acrossecurity.com



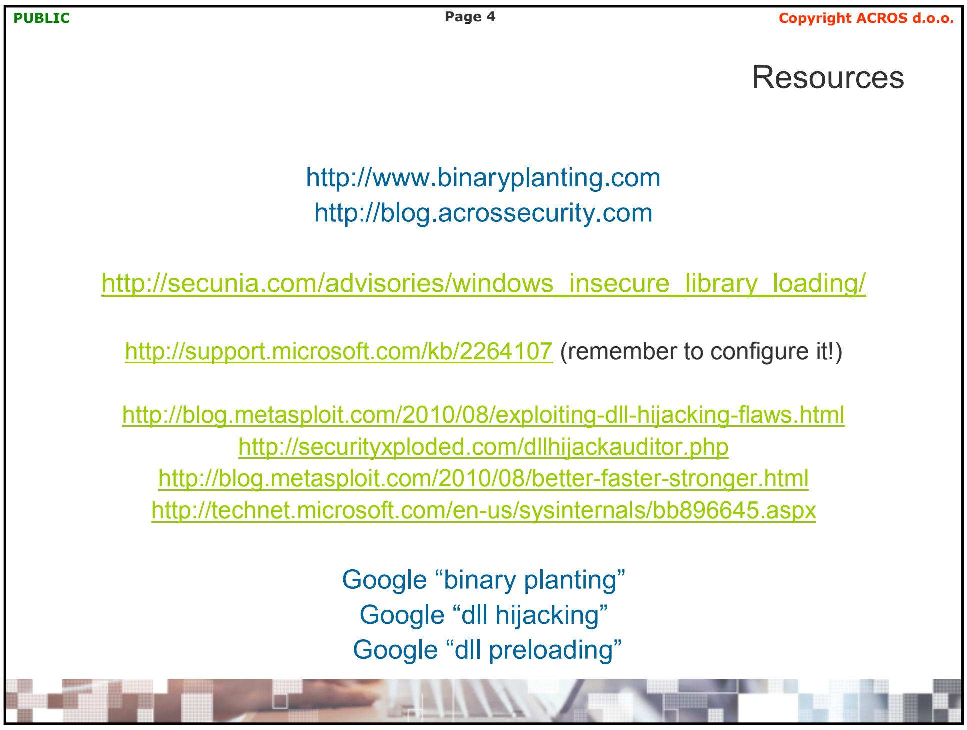
Countermeasures for Developers

- Don’t make “let’s see if it’s there” LoadLibrary* calls
- Don’t use relative paths in LoadLibrary, CreateProcess, ShellExecute...
- Don’t plan on finding your DLL/EXE in PATH – that’s too late
- Set CWD to a safe location at startup
- Don’t let “file browse” dialogs change CWD
- Use SetDllDirectory(“”) at startup
- Don’t use SearchPath function, or use it safely
- Check your assumptions if your DLL can be loaded by someone else
- Resolve environment variables when reading DLL/EXE paths from registry
- Check your product for BP with Process Monitor or another tool
- Be careful when developing for different OS, languages
- Do this for all modules of your product!



Countermeasures for Users, Admins

- Install Microsoft's Hotfix, remember to configure it
- Disable "Web Client" service
- Windows Software Restriction Policy, Windows AppLocker (DLL)
- Use a personal firewall with process and connection blocking
- Block outbound SMB on corporate firewall
- Block outbound WebDAV on corporate firewall
- Limit internal SMB, WebDAV traffic
- Restrict write access on file repositories to prevent planting
- Be careful when using USB sticks, CDs, DVDs from unknown sources
- Think before double-clicking on anything presented to you
- If in doubt, download the data file (alone) to local drive and open it



Resources

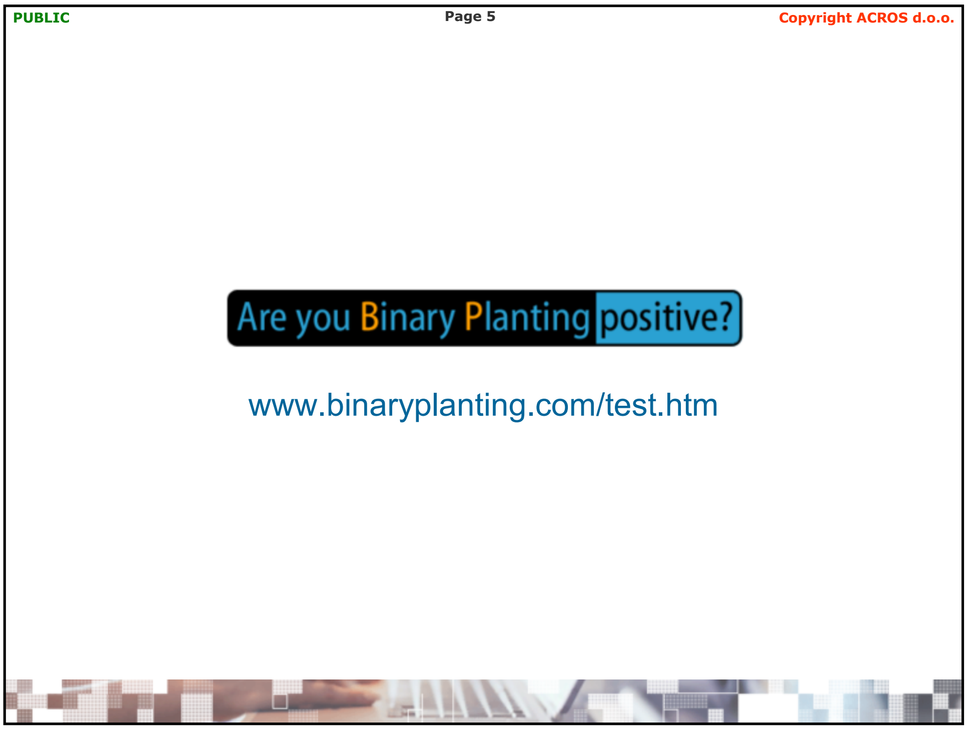
http://www.binaryplanting.com
http://blog.acrossecurity.com

http://secunia.com/advisories/windows_insecure_library_loading/

http://support.microsoft.com/kb/2264107 (remember to configure it!)

http://blog.metasploit.com/2010/08/exploiting-dll-hijacking-flaws.html
http://securityxploded.com/dllhijackauditor.php
http://blog.metasploit.com/2010/08/better-faster-stronger.html
http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx

Google "binary planting"
Google "dll hijacking"
Google "dll preloading"



Are you Binary Planting positive?

www.binaryplanting.com/test.htm