



DLL Search Order Hijacking

(... or how I got calc.exe to cut ahead of the line)

James Russell



But first...

What is a “DLL”?





Simply put:

A DLL (or **D**ynamic **L**ink **L**ibrary) is a file containing executable code which can be used by multiple applications

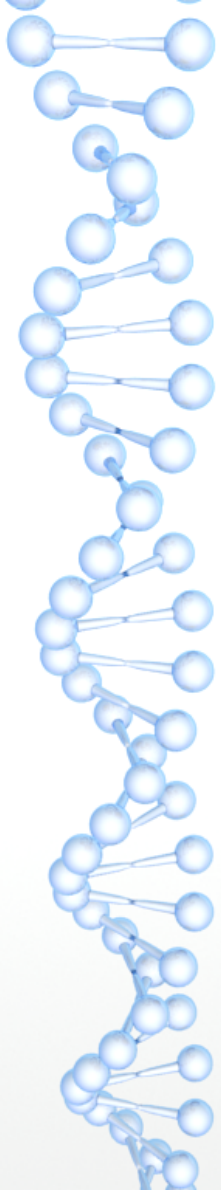


So why use a DLL?

- DLLs assist in making applications more modular
- Allows for easier application updating
- Quicker load time

With that being said, MS won't be giving up on DLLs anytime soon...

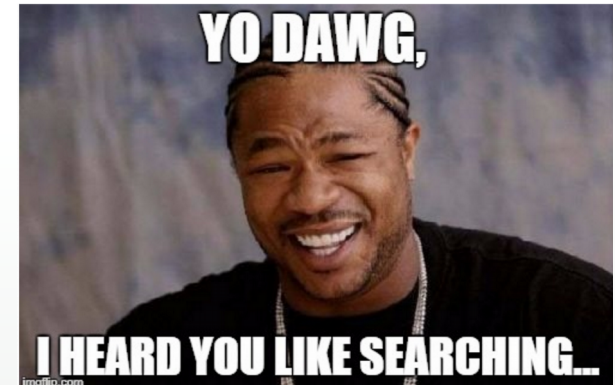


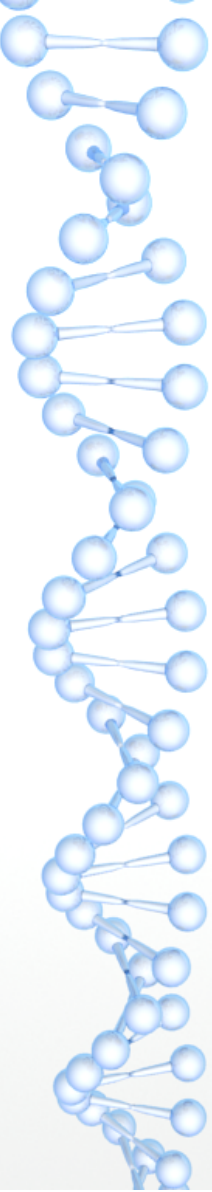


So how does an application
reference a DLL?

Assuming “Safe DLL search mode” is enabled (by default it is)

- If it's currently loaded in memory
- The “Known DLLs” registry key *
- The directory where the application was launched in
- The system directory (C:\Windows\System32)
- The 16-bit system directory (C:\Windows\System)
- The Windows directory (C:\Windows)
- The current directory
- Directories defined in the PATH variables

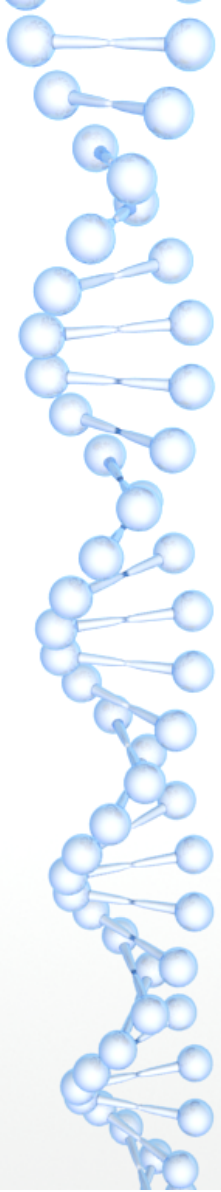




Q. So what's up with this "Known DLL" registry key and why is it important?

A. These are the most commonly called upon DLLs (in System32) that could possibly be used by other applications.

Think Speeeeeeeddd



Great, so what?



DLL Hijacking

When a benign DLL for a known program is replaced for a malicious one. The program launches, the malicious DLL gets called upon and the evil payload (or evil command) is executed.

DLL Search Order Hijacking

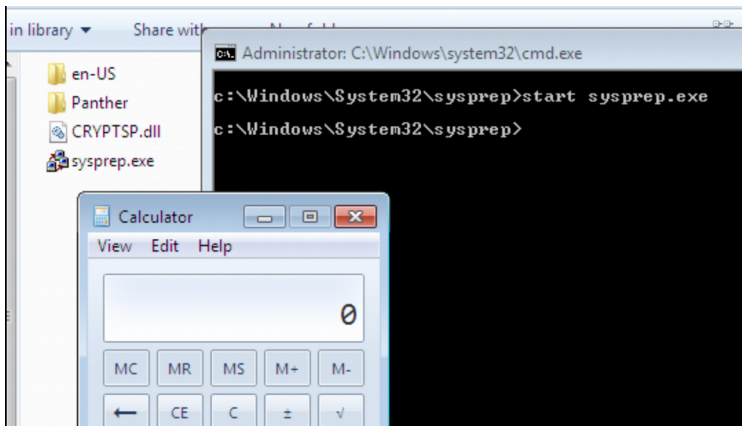
Same as before, but this time you are specifically taking advantage of **where in the search order** the DLL is located.



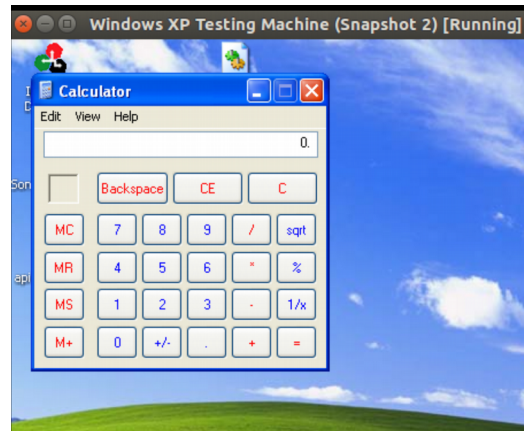
So why would a Red Team be interested in it?



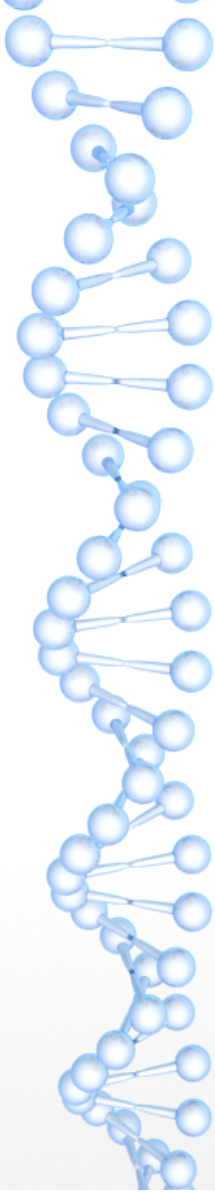
```
root@Nightcrawler:~# msfvenom -p windows/exec CMD=calc.exe -f dll > calc.dll
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 193 bytes
Final size of dll file: 5120 bytes
```



Win7 – Search Order Hijack
renamed the evil DLL to “CRYPTSP.dll” and
moved it into the directory of the .exe
(needed by sysprep.exe)



WinXP – hijack of ntshrui.dll,
Causing persistent calc.exe popups
at startup (needed by explorer.exe)
no other interaction required





Where else has DLL Hijacking been used lately?

- Youndoo.com Browser Hijacker

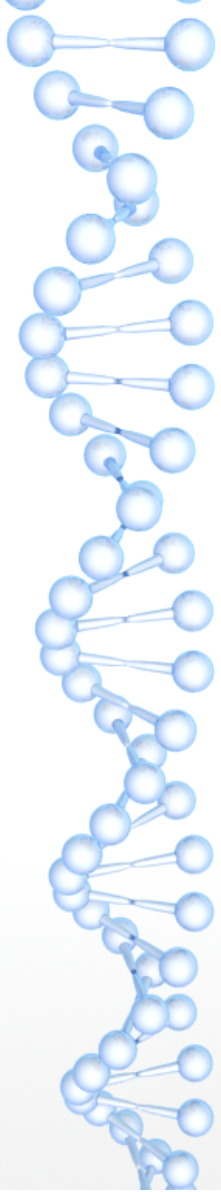
Forced Chrome and Firefox to display Youndoo.com as the homepage by replacing **wtsapi32.dll**, a DLL used by both browsers.

(<https://www.bleepingcomputer.com/news/security/youndoo-adware-hijacks-browser-homepage-using-dll-hijacking/>)

- CIA “Fine Dining” Project

Involved 23 applications vulnerable to DLL Hijacking for the purpose acting as decoys for other tools simultaneously running in the background.

(<https://news.sophos.com/en-us/2017/03/10/qa-wikileaks-the-cia-fine-dining-and-dll-hijacks/>)



Questions?