Windows Live Response using WMIC

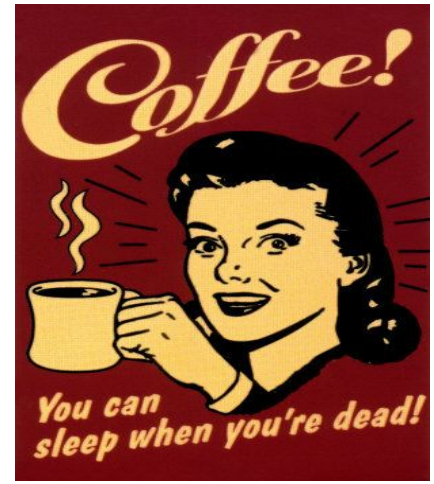
Justin Hall

Why do
live response?

Maybe we haven't confirmed compromise yet...

Maybe the killer IS STILL IN THE HOUSE!!1!1!!!one

Windows Sysinternals



F-Response

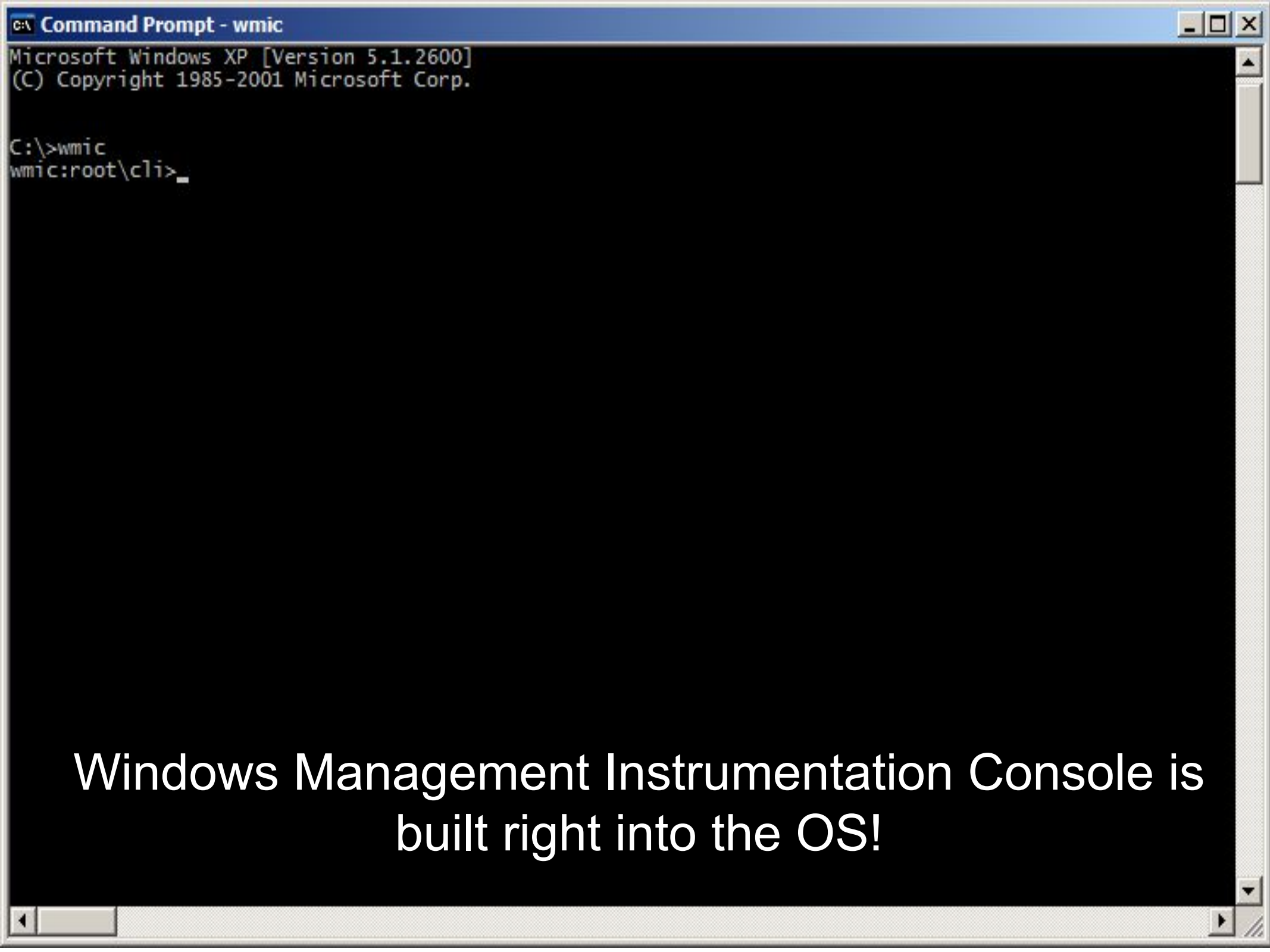
Lots of LR tools exist today.
Well, maybe not lots.
But enough.

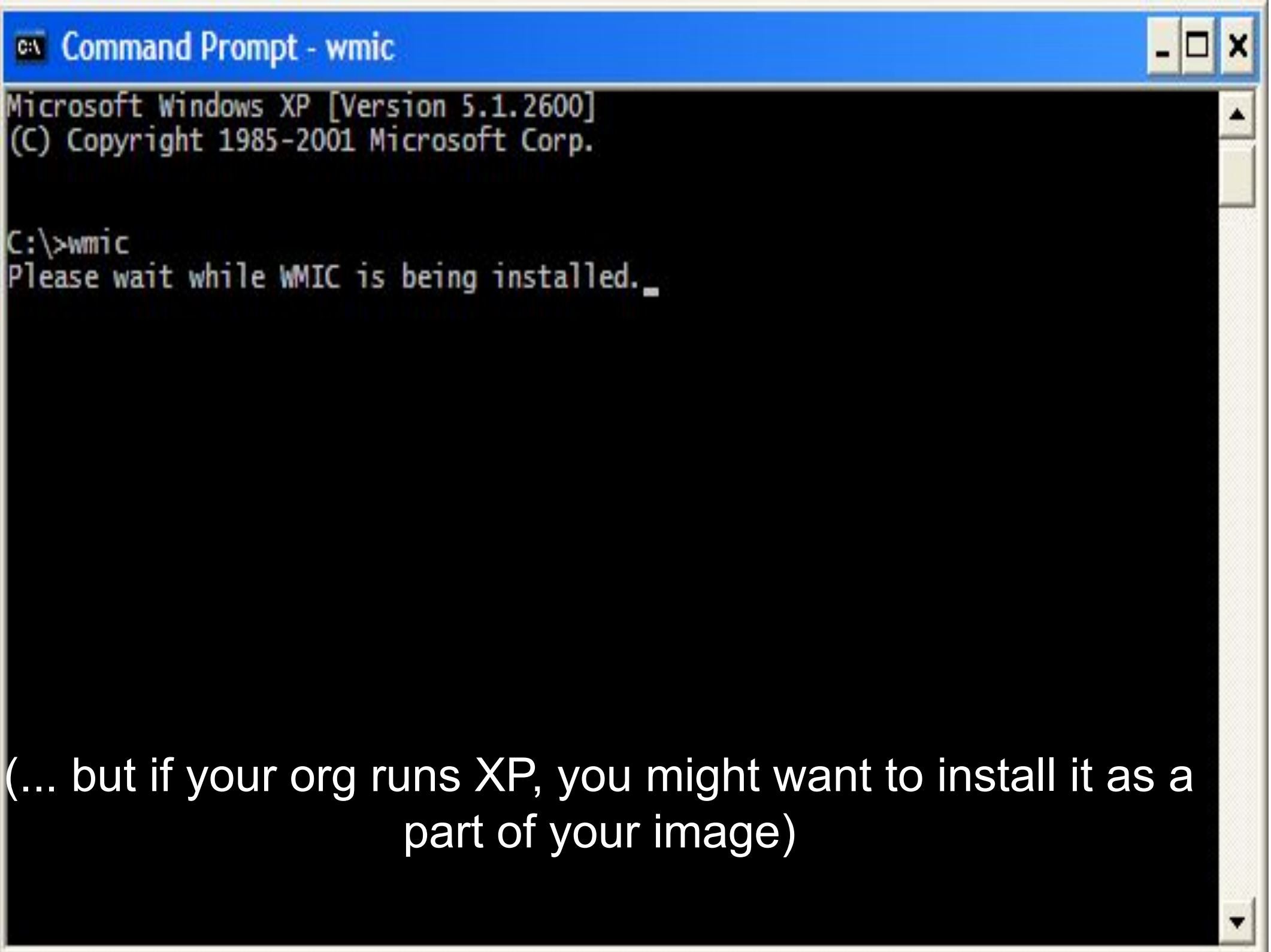

But what if we don't want to "contaminate the scene of the crime"?

arp table
autorun entries
current logon sessions
current network connections
directory listing of mounted filesystems
dump of registry
event logs
image of memory
image of pagefile
list of drivers loaded by OS
list of files in prefetch
list of mapped network drives / shares / RPC objects
list of running processes
list of scheduled tasks
list of services
list of system objects
list of user profiles
logged in user
network configuration
open handles by running processes
ports opened by running processes
remotely opened files on system
system's audit policies
Windows install/system information

When we LR a host, we grab lots of data from it, using a few dozen CLI utilities...

That's a lot of garbage to drop into its memory.


Command Prompt - wmic
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>wmic
wmic:root\cli>
Windows Management Instrumentation Console is built right into the OS!



(... but if your org runs XP, you might want to install it as a part of your image)

Think of WMIC as a swiss army knife to access Windows configuration information.

... A swiss army knife you can use remotely!

WMIC syntax (and some examples)

wmic /<switches> <alias> <where clause> <verb> <qualifier>

switches: /user:DOMAIN\user - specify credentials to use
/node:10.0.0.1 - specify a remote host to hit

alias: what piece of Windows you want to pull information about. ex: LOGON, NIC, QFE, REGISTRY, SERVICE

where clause: narrow your query, i.e. WHERE HOTFIXID=KB956844 or WHERE (MESSAGE LIKE "%FOO%")

verb: what do you want WMIC to do? i.e. LIST, CALL
note: GET or LIST are almost exclusively used when performing live response

qualifier: how much data do you want? i.e. LIST FULL, BRIEF or a field name, i.e. GET COMMANDLINE

Trick out the results:

Specify **/output:<filename>** to dump results to a file. Also specify a **/format:** to tailor formatting. Your options:

CSV:

```
Node,Description,ExecutablePath,ParentProcessId,ProcessId
XPSP2VM,smss.exe,C:\WINDOWS\System32\smss.exe,4,380
XPSP2VM,csrss.exe,C:\WINDOWS\system32\csrss.exe,380,592
XPSP2VM,winlogon.exe,C:\WINDOWS\system32\winlogon.exe,380,616
XPSP2VM,services.exe,C:\WINDOWS\system32\services.exe,616,660
XPSP2VM,lsass.exe,C:\WINDOWS\system32\lsass.exe,616,672
```

HTABLE:

22 Instances of Win32_Process

Node	Description	ExecutablePath	ParentProcessId	ProcessId
XPSP2VM	System Idle Process		0	0
XPSP2VM	System		0	4
XPSP2VM	smss.exe	C:\WINDOWS\System32\smss.exe	4	380
XPSP2VM	csrss.exe	C:\WINDOWS\system32\csrss.exe	380	592
XPSP2VM	winlogon.exe	C:\WINDOWS\system32\winlogon.exe	380	616
XPSP2VM	services.exe	C:\WINDOWS\system32\services.exe	616	660
XPSP2VM	lsass.exe	C:\WINDOWS\system32\lsass.exe	616	672
XPSP2VM	VBoxService.exe	C:\WINDOWS\system32\VBoxService.exe	660	824
XPSP2VM	svchost.exe	C:\WINDOWS\system32\svchost.exe	660	836

LIST:

```
Description=cmd.exe
ExecutablePath=C:\WINDOWS\system32\cmd.exe
ParentProcessId=1484
ProcessId=208


Description=IEXPLORE.EXE
ExecutablePath=C:\Program Files\Internet Explorer\iexplore.exe
ParentProcessId=1484
ProcessId=232


Description=wuauclt.exe
ExecutablePath=C:\WINDOWS\system32\wuauclt.exe
ParentProcessId=1004
ProcessId=524
```

CSV
HFORM
HMOF
HTABLE
HXML
LIST
RAWXML
TABLE
VALUE
htable-sortby
htable-sortby.xsl
texttablewsys
texttablewsys.xsl
wmiclimofformat
wmiclimofformat.xsl
wmiclitableformat
wmiclitableformat.xsl
wmiclitableformatnosys
wmiclitableformatnosys.xsl
wmiclivalueformat
wmiclivalueformat.xsl

A wild script appears!  WMIC_LR

Grab **http://jdeezy.org/wmic_lr.zip**
MD5 51C964B6E34BCD99D853715604D6B568

Contains two scripts: **wmic_lr_local.cmd** - run on target system, gather text files with results, analyze

wmic_lr_remote.cmd - run with privileged account (or modify to use /USER and /PASSWORD switches)

- one command line argument: target hostname or IP
  - i.e. wmic_remote_cmd 192.168.1.101
- make sure you can reach RPC services on the remote host
- text files with results are dumped in working directory

Scripts released under Creative Commons ShareAlike license - feel free to redistribute, modify, etc. See scripts for details.

WMIC notes

DO NOT TRY TO LIST ALL EVENT LOGS, (i.e. 'ntevent list brief') - **IT'LL BLOW UP**. Same with the 'fsdir' alias.

The "**JOB**" alias will only show scheduled tasks created with Windows' "**AT**" command - not "SCHTASKS"

Try /node:"@hosts.txt" to specify multiple remote hosts

LR'ing Windows 2003 Server? Install the WMI Windows Installer Provider (Add/Remove Programs -> Windows Components -> Management and Monitoring tools) or you'll get Invalid Class errors

References

Command Line Kung Fu blog: http://commandlinekungfu.com
Microsoft's WMIC on XP manual: http://bit.ly/wmic-xp

Questions?

Justin Hall
justin.hall@cbts.cinbell.com