



SilentBreak
S E C U R I T Y

Getting Windows to Play with Itself

A Hacker's Guide to Windows API Abuse

Brady Bloxham

Founder/Principal Security Consultant

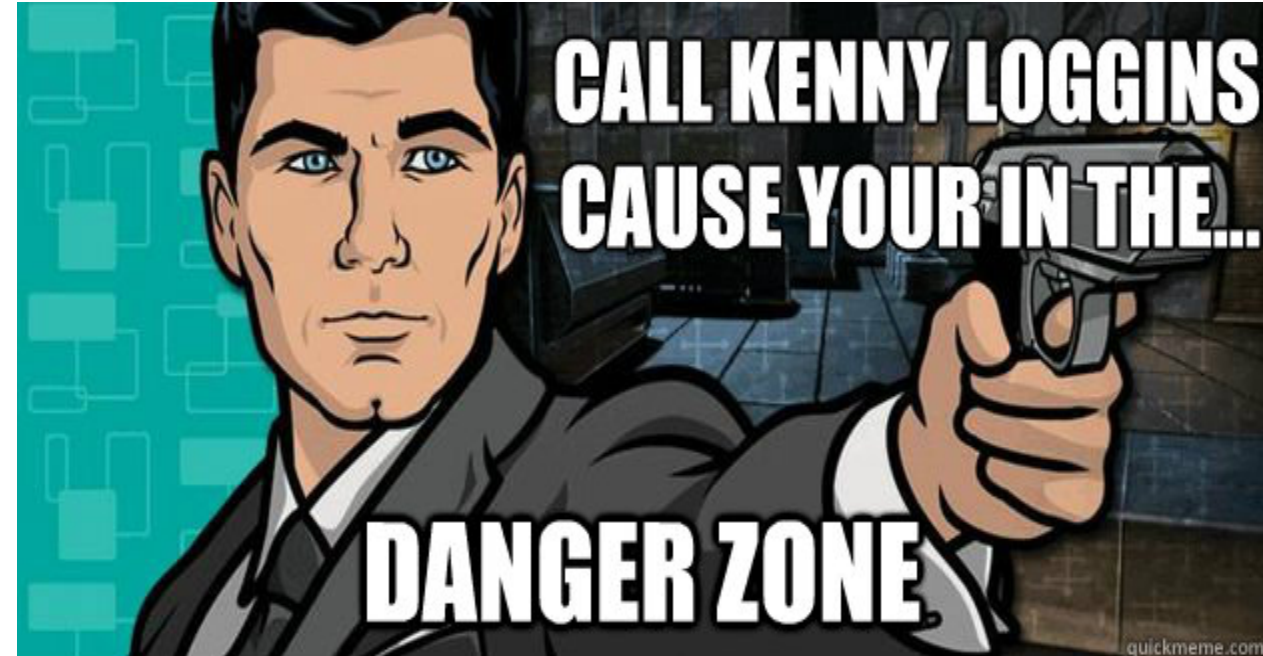
@silentbreaksec

<http://www.silentbreaksecurity.com>

<http://www.blacksquirrel.io>

Background

- Shorten the gap between penetration test and actual attack
- Few covert persistence tools
- Reduce reliance on Metasploit



Got a lot to cover

- DLL Injection
- Persistence
- Throwback
- Lots of demos along the way



DLL Injection

- Traditional methods
 - CreateRemoteThread()
 - NtCreateThreadEx()
 - RtlCreateUserThread()
 - NtQueueApcThread ()
 - Can blue screen certain OSes
 - Code Cave
 - Suspend process
 - Inject code
 - Change EIP to location of injected code
 - Resume process
 - Difficult on x64



AddMonitor()

- +
 - Injects into spoolsv.exe
 - Doesn't require matching architecture
 - Easy to use
- -
 - Dll must be on disk
 - Requires administrator privs

The **AddMonitor** function installs a local port monitor and links the configuration, data, and monitor files.

Syntax

C++

```
BOOL AddMonitor(  
    _In_ LPTSTR pName,  
    _In_ DWORD Level,  
    _In_ LPBYTE pMonitors  
);
```

Dll Injection Demo



Persistence

- Lots of persistence in Windows
 - Service
 - Run keys
 - Schtasks
 - ...
- And lots still to find...
- Lots of techniques
 - Process monitor
 - Hook LoadLibrary()



vmtoolsd.exe	2884	CreateFile	C:\Windows\System32\wbem\fastprox.dll	SUCCESS	Desired Access: Read Attributes, Disposition
vmtoolsd.exe	2884	QueryBasicInformationFile	C:\Windows\System32\wbem\fastprox.dll	SUCCESS	CreationTime: 7/13/2009 5:47:53 PM, LastA
vmtoolsd.exe	2884	CloseFile	C:\Windows\System32\wbem\fastprox.dll	SUCCESS	
vmtoolsd.exe	2884	CreateFile	C:\Windows\System32\wbem\fastprox.dll	SUCCESS	Desired Access: Read Data/List Directory, B
vmtoolsd.exe	2884	CreateFileMapping	C:\Windows\System32\wbem\fastprox.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageP
vmtoolsd.exe	2884	CreateFileMapping	C:\Windows\System32\wbem\fastprox.dll	SUCCESS	SyncType: SyncTypeOther
vmtoolsd.exe	2884	Load Image	C:\Windows\System32\wbem\fastprox.dll	SUCCESS	Image Base: 0x7ef9ca0000, Image Size: 0x
vmtoolsd.exe	2884	CloseFile	C:\Windows\System32\wbem\fastprox.dll	SUCCESS	
vmtoolsd.exe	2884	CreateFile	C:\Windows\System32\wbem\NTDSAPI.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition
vmtoolsd.exe	2884	CreateFile	C:\Windows\System32\ntdsapi.dll	SUCCESS	Desired Access: Read Attributes, Disposition
vmtoolsd.exe	2884	QueryBasicInformationFile	C:\Windows\System32\ntdsapi.dll	SUCCESS	CreationTime: 7/13/2009 5:54:08 PM, LastA
vmtoolsd.exe	2884	CloseFile	C:\Windows\System32\ntdsapi.dll	SUCCESS	
vmtoolsd.exe	2884	CreateFile	C:\Windows\System32\ntdsapi.dll	SUCCESS	Desired Access: Read Data/List Directory, B
vmtoolsd.exe	2884	CreateFileMapping	C:\Windows\System32\ntdsapi.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageP
vmtoolsd.exe	2884	CreateFileMapping	C:\Windows\System32\ntdsapi.dll	SUCCESS	SyncType: SyncTypeOther
vmtoolsd.exe	2884	Load Image	C:\Windows\System32\ntdsapi.dll	SUCCESS	Image Base: 0x7ef7770000, Image Size: 0x
vmtoolsd.exe	2884	CloseFile	C:\Windows\System32\ntdsapi.dll	SUCCESS	
vmtoolsd.exe	2884	CreateFile	C:\Windows\System32\comsvcs.dll	SUCCESS	Desired Access: Read Attributes, Disposition
vmtoolsd.exe	2884	QueryBasicInformationFile	C:\Windows\System32\comsvcs.dll	SUCCESS	CreationTime: 7/13/2009 6:01:16 PM, LastA
vmtoolsd.exe	2884	CloseFile	C:\Windows\System32\comsvcs.dll	SUCCESS	

Persistence

- 1st Technique
 - Requires VM
 - Just drop a dll
 - c:\windows\
 - Note: Dll must be real ntdsapi.dll

- 2nd Technique
 - VMware patch
 - Requires VM
 - Just drop a dll to disk
 - c:\windows\system32\wbem\tpgenlic.dll
 - c:\windows\system32\wbem\thinmon.dll

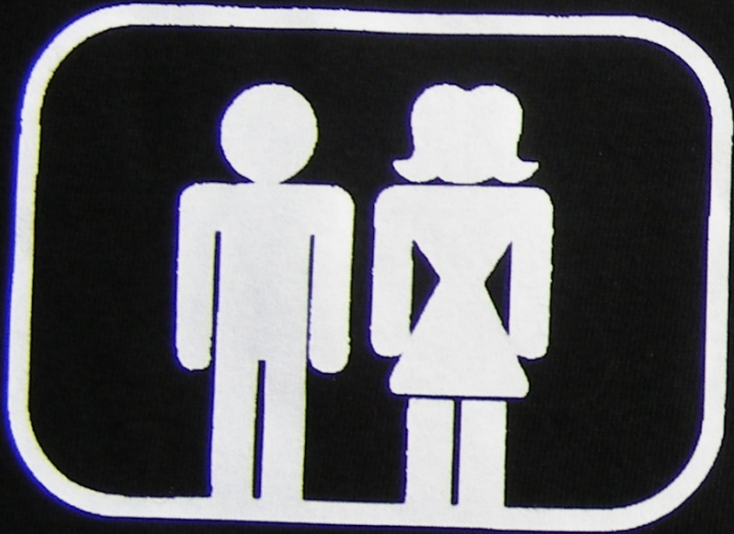


Windows

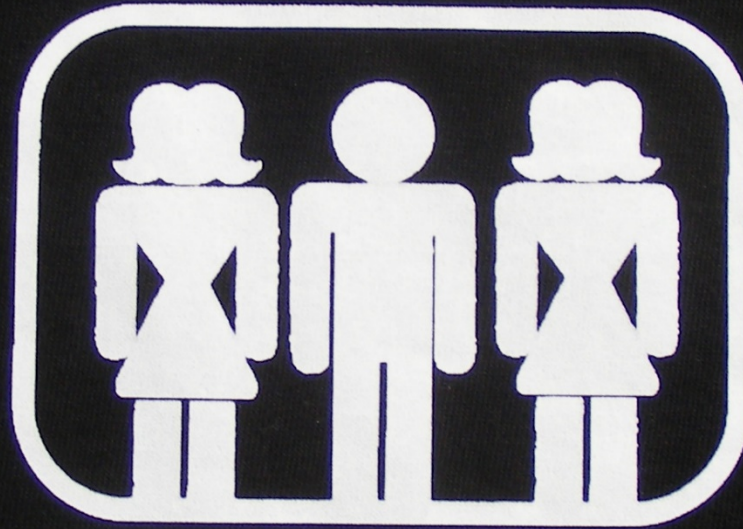
**HE ACTUALLY
WANTS TO STOP**

OR IS TURNED ON BY MY PERSISTENCE

quickmeme.com



GOOD



BETTER



BEST

Persistence Demo



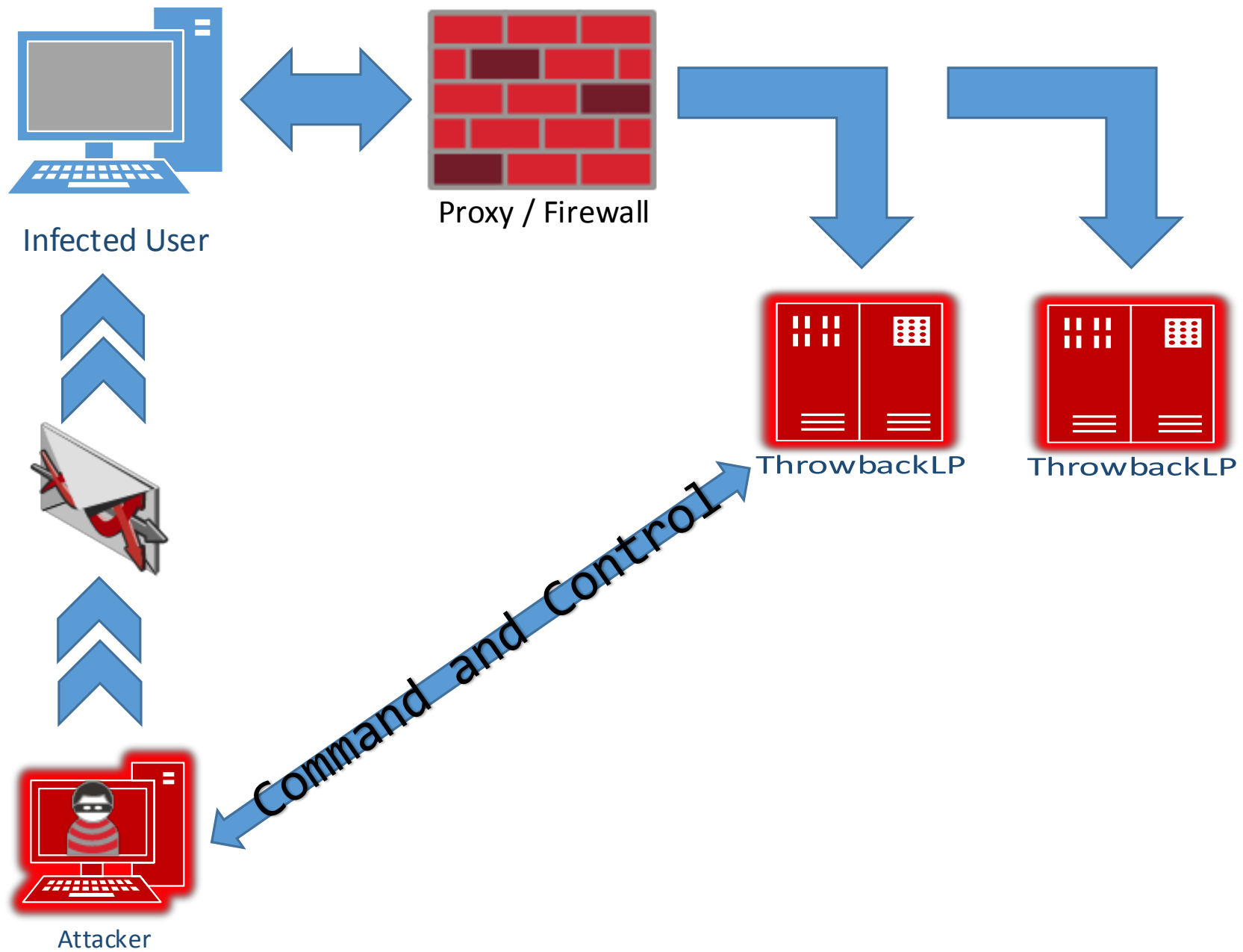
Windows API HTTP Cheatsheet

- WinHTTP
 - Intended for services
 - Does not pull user proxy settings
 - Supports impersonation
- WinINET
 - More robust in proxy environment
 - Variety of flags that enable/disable functionality automatically
 - Prompts user for password if authentication is required
 - Uses IE settings

What is Throwback?

- C++ HTTP/S beaoning backdoor
- PHP control panel w/ MySQL backend
- Built for stealth
- Persistence built-in
 - Dll
 - Exe





Throwback Features

- Robust proxy detection
- Distributed LPs
- Uses MSGRPC to generate MSF payloads
- RC4 encrypted comms
- Implements reflective dll injection
- String encryption











Action Command Arguments

Select one...

Submit

Current time is Aug 5, 2014 4:54 pm.

Status	Version	IP Address	Target Name	Callback Period	Last Callback	Actions
 	2.50	192.168.20.183	IETEMPLATE	1 minutes	Aug 5, 2014 4:04 pm	History Radar
 	2.50	192.168.20.1	IE11TEMPLATE	1 minutes	Aug 4, 2014 10:35 pm	History Radar
 	2.16	192.168.20.1	IE10TEMPLATE	1 minutes	Aug 2, 2014 12:28 am	History Radar
 	2.16	192.168.20.112	IE9TEMPLATE	10 minutes	Aug 1, 2014 5:55 pm	History Radar

Throwback Demo



Going Forward...

- Community based project!!!
- Create modules
 - Keylogger, Mimikatz, Hashdump, etc.
 - Various transport methods
- Additional persistence techniques
- Modification of comms

~~The End~~ Shameless Plug

- Interested in writing custom malware/backdoors?
 - Dark Side Ops: Custom Penetration Testing
 - Blackhat Europe and East Coast Trainings
- Pen test networks from your browser
 - <https://www.blacksquirrel.io>
- Silent Break Security
 - Blackbox/Red Team Pen Testing
 - brady@silentbreaksecurity.com
 - @silentbreaksec
 - <https://github.com/silentbreaksec>

