Process Monitor - Sysinternals; www.sysinternals.com File Edit Event Filter Tools Options Help Time Process Name Operation Path Result 2948 Process Start putty.exe SUCCESS 4:14:1... 2948 CThread Create 4.14.1 Dutty exe SUCCESS

2948 QueryNameInfo...C:\Windows

2948 CloseFile

2948 RegOpenKey

2948 RegQueryValue

2948 RegQueryValue

2948 ReaCloseKev

2948 ct Load Image

2948 RegOpenKey

2948 RegOpenKey

2948 RegCloseKey

2948 RegOpenKey

2948 RegOpenKey

2948 RegOpenKey

2948 RegSetInfoKev

2948 RegQueryValue

4:14:1... putty.exe

4:14:1... Pputty.exe

4:14:1... Putty.exe

4:14:1... Putty.exe

4:14:1... putty.exe

4:14:1... 🗗 putty.exe

4:14:1... Putty.exe

4:14:1... Putty.exe

4:14:1... Putty.exe

4:14:1... Poutty.exe

4:14:1... Putty.exe

4:14:1... Poutty.exe

4:14:1... Putty.exe

4:14:1... putty.exe

4:14:1... putty.exe

	putty.exe	2948	Thread Create		SUCCESS	Thread ID: 3820
:14:1	putty.exe	2948	Ç [©] Load Image	C:\Users\vboxuser\Desktop\putty.exe	SUCCESS	Image Base: 0x400
:14:1	putty.exe	2948	Ç [©] Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fff
:14:1	putty.exe	2948	Ç [©] Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x76e
:14:1	putty.exe	2948	 ■ RegOpenKey	HKLM\System\CurrentControlSet\Contr	REPARSE	Desired Access: Q
:14:1	putty.exe	2948	■ RegOpenKey	HKLM\System\CurrentControlSet\Contr	SUCCESS	Desired Access: Q
	(m)				NAME WATERWAY	

		2948	III RegOpenKey	HKLM\System\CurrentControlSet\Contr REPARSE	Desire
14:1	putty.exe	2948	RegOpenKey	HKLM\System\CurrentControlSet\Contr SUCCESS	Desire
14:1	putty.exe	2948	RegQueryValue	HKLM\System\CurrentControlSet\Contr NAME NOT	FOUND Length
14:1	putty.exe	2948	RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
14:1	putty.exe	2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desire

	Control Control				
		2948	 ■ RegOpenKey	HKLM\System\CurrentControlSet\Contr SUCCESS	Desired
4:1	putty.exe	2948	RegQueryValue	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND	Length:
4:1	putty.exe	2948	RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
4:1	putty.exe	2948	⊯ RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired

14:1	<u>re</u> puπy.exe	2548	m RegOpenkey	HKLIVI \System \currentcontrolSet \contr SUCCESS	Desirea
14:1	putty.exe	2948	RegQueryValue	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND	Length:
14:1	putty.exe	2948	RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
14:1	putty.exe	2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired
14:1	putty.exe	2948	RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND	Desired
14:1	putty.exe	2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired

		2948	RegOpenKey	HKLM\System\CurrentControlSet\Contr SUCCESS	Desired Access: Q
		2948	RegQueryValue	HKLM\System\CurrentControlSet\Contr NAME NOT FOUI	ND Length: 80
		2948	RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
		2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired Access: Q
14:1	putty.exe	2948	RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT FOUl	ND Desired Access: Q
1/1-1	contty eve	20/10	PagOpanKay	HKLM\CVCTEM\CurrentControlSet\ConREPARCE	Desired Access: O

	E Party . arra				
4:1	putty.exe	2948	RegQueryValue	HKLM\System\CurrentControlSet\Contr NAME NOT FOU	JND Length:
4:1	putty.exe	2948	RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
4:1	putty.exe	2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired
4:1	putty.exe	2948	RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT FOU	JND Desired
4:1	putty.exe	2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired

	putty.onc	2010		riegoperitoy	The System Control Con	Desired
4:1	putty.exe	2948	H	RegQueryValue	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND I	Length:
4:1	putty.exe	2948	H	RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
4:1	putty.exe	2948	H	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE [Desired
		2948	H	RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND [Desired
4:1	putty.exe	2948		RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE [Desired

	<u>r</u> eputty.exe	2948		HKLM\System\CurrentControlSet\Contr NAME_NOT	FOUND Length: 80
		2948	RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
4:14:1	putty.exe	2948	II RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired Access: Q
4:14:1	putty.exe	2948	RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT	FOUND Desired Access: Q
4:14:1	putty.exe	2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired Access: Q
4-14-1	and the eve	20/10	III [®] PagOpanKay	HKLM\System\CurrentControlSat\Contr SHCCESS	Desired Access: O

4:14:1		2948	RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
		2948	⊯ RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired Access: Q
		2948	II RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND	Desired Access: Q
		2948	II RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired Access: Q
		2948	∰ RegOpenKey	HKLM\System\CurrentControlSet\Contr SUCCESS	Desired Access: Q
4:14:1	putty.exe	2948	RegQueryValue	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND	Length: 24

4:14:1	putty.exe	2948	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con	.REPARSE	Desired Access: Q.
4:14:1	putty.exe	2948	■ RegOpenKey	HKLM\System\CurrentControlSet\Contr	SUCCESS	Desired Access: Q.
4:14:1	putty.exe	2948	RegQueryValue	HKLM\System\CurrentControlSet\Contr	NAME NOT FOUND	Length: 24
4:14:1	putty.exe	2948	RegCloseKey	HKLM\System\CurrentControlSet\Contr	SUCCESS	
4-14-1	danutty eve	29/12	Creste File	C:\Windowe	SUCCESS	Desired Access: E

4:14:1	putty.exe	2948	RegQueryValue	HKLM\System\CurrentControlSet\Contr	NAME NOT FOUN	D Length: 24
				HKLM\System\CurrentControlSet\Contr		-
		2948	CreateFile	C:\Windows	SUCCESS	Desired Access: E
4:14:1	putty.exe	2948	Calculation Logical Logica	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7fff

HKLM\Software\Microsoft\Wow64\x86 SUCCESS

HKLM\SOFTWARE\Microsoft\Wow64\...SUCCESS

HKLM\SOFTWARE\Microsoft\Wow64\...SUCCESS

HKLM\Svstem\CurrentControlSet\Contr... REPARSE

HKLM\Svstem\CurrentControlSet\Contr... SUCCESS

HKLM\Svstem\CurrentControlSet\Contr... SUCCESS

HKLM\Svstem\CurrentControlSet\Contr... SUCCESS

HKLM\SYSTEM\CurrentControlSet\Con...REPARSE

HKLM\SYSTEM\CurrentControlSet\Con...REPARSE

C:\Windows\Svstem32\wow64cpu.dll

4:1	putty.exe	2948	⊈ Load Image	C:\Windows\System32\wow64.dll	SUCCESS	lmage Ba
4:1	putty.exe	2948	\$\$Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	lmage Ba
4:1	putty.exe	2948	🦐 CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT	FOUND Desired A
	(a)	00.40		0.110	01100500	

4:14:1 putty.exe	2948 CLoad Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x /fff
4:14:1 Putty.exe	2948 🛱 Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fff
4:14:1 🗗 putty.exe	2948 🧱 Create File	C:\Windows\System32\wow64log.dll	NAME NOT FOU	JND Desired Access: R

4:14:1	<u>re</u> puπy.exe	2548	© Load Image	C:\vvindows\5ystem32\wow64.dil	SUCCESS	image Base: ux /πr
4:14:1	putty.exe	2948	ç [©] Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fff
4:14:1	putty.exe	2948	🦮 Create File	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R
4:14:1	putty.exe	2948	🦮 Create File	C:\Windows	SUCCESS	Desired Access: R

C:\Windows



SUCCESS

SUCCESS

SUCCESS

HKLM\SOFTWARE\Microsoft\Wow64\...NAME NOT FOUND Length: 520

HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 80

HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Desired Access: Q...

Detail

Parent PID: 3420. ...

Name: \Windows

Desired Access: R...

Type: REG SZ, Le...

Image Base: 0x76e...

Desired Access: Q....

Desired Access: Q....

KeySetInformation...

Desired Access: Q...

Desired Access: Q...