



| Time ...  | Process Name | PID  | Operation        | Path                                   | Result         | Detail                |
|-----------|--------------|------|------------------|--|----------------|-----------------------|
| 4:14:1... | putty.exe    | 2948 | Process Start    |  | SUCCESS        | Parent PID: 3420, ... |
| 4:14:1... | putty.exe    | 2948 | Thread Create    |  | SUCCESS        | Thread ID: 3820       |
| 4:14:1... | putty.exe    | 2948 | Load Image       | C:\Users\vbouser\Desktop\putty.exe     | SUCCESS        | Image Base: 0x400...  |
| 4:14:1... | putty.exe    | 2948 | Load Image       | C:\Windows\System32\ntdll.dll          | SUCCESS        | Image Base: 0x7fff... |
| 4:14:1... | putty.exe    | 2948 | Load Image       | C:\Windows\SysWOW64\ntdll.dll          | SUCCESS        | Image Base: 0x76e...  |
| 4:14:1... | putty.exe    | 2948 | RegOpenKey       | HKLM\System\CurrentControlSet\Contr... | 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: 80            |
| 4:14:1... | putty.exe    | 2948 | RegCloseKey      | HKLM\System\CurrentControlSet\Contr... | SUCCESS        |                       |
| 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... | NAME NOT FOUND | Desired Access: Q...  |
| 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... | putty.exe    | 2948 | CreateFile       | C:\Windows                             | SUCCESS        | Desired Access: E...  |
| 4:14:1... | putty.exe    | 2948 | Load Image       | C:\Windows\System32\wow64.dll          | SUCCESS        | Image Base: 0x7fff... |
| 4:14:1... | putty.exe    | 2948 | Load Image       | C:\Windows\System32\wow64win.dll       | SUCCESS        | Image Base: 0x7fff... |
| 4:14:1... | putty.exe    | 2948 | CreateFile       | C:\Windows\System32\wow64log.dll       | NAME NOT FOUND | Desired Access: R...  |
| 4:14:1... | putty.exe    | 2948 | CreateFile       | C:\Windows                             | SUCCESS        | Desired Access: R...  |
| 4:14:1... | putty.exe    | 2948 | QueryNameInfo... | C:\Windows                             | SUCCESS        | Name: \Windows        |
| 4:14:1... | putty.exe    | 2948 | CloseFile        | C:\Windows                             | SUCCESS        |                       |
| 4:14:1... | putty.exe    | 2948 | RegOpenKey       | HKLM\Software\Microsoft\Wow64\x86      | SUCCESS        | Desired Access: R...  |
| 4:14:1... | putty.exe    | 2948 | RegQueryValue    | HKLM\SOFTWARE\Microsoft\Wow64\...      | NAME NOT FOUND | Length: 520           |
| 4:14:1... | putty.exe    | 2948 | RegQueryValue    | HKLM\SOFTWARE\Microsoft\Wow64\...      | SUCCESS        | Type: REG_SZ, Le...   |
| 4:14:1... | putty.exe    | 2948 | RegCloseKey      | HKLM\SOFTWARE\Microsoft\Wow64\...      | SUCCESS        |                       |
| 4:14:1... | putty.exe    | 2948 | Load Image       | C:\Windows\System32\wow64cpu.dll       | SUCCESS        | Image Base: 0x76e...  |
| 4:14:1... | putty.exe    | 2948 | RegOpenKey       | HKLM\System\CurrentControlSet\Contr... | 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 | RegSetInfoKey    | HKLM\System\CurrentControlSet\Contr... | SUCCESS        | KeySetInformation...  |
| 4:14:1... | putty.exe    | 2948 | RegQueryValue    | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Length: 80            |
| 4:14:1... | putty.exe    | 2948 | RegCloseKey      | HKLM\System\CurrentControlSet\Contr... | SUCCESS        |                       |
| 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... | NAME NOT FOUND | Desired Access: Q...  |
| 4:14:1... | putty.exe    | 2948 | RegOpenKey       | HKLM\SYSTEM\CurrentControlSet\Con...   | REPARSE        | Desired Access: Q...  |