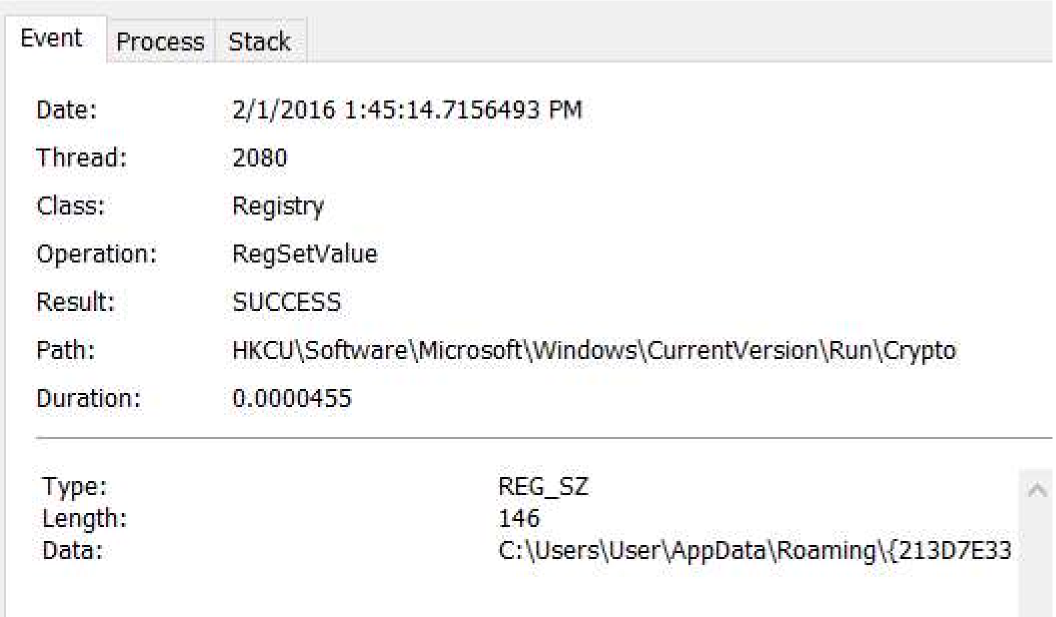
1. bash.exe 3196



Date: 2/1/2016 1:45:14.7156493 PM

Thread: 2080

Class: Registry

Operation: RegSetValue

Result: SUCCESS

Path: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Crypto

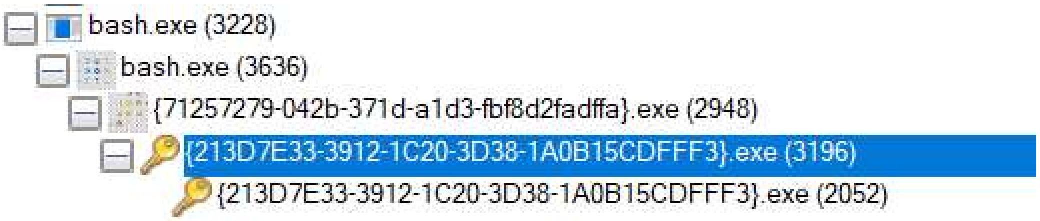
Duration: 0.0000455

Type: REG_SZ

Length: 146

Data: C:\Users\User\AppData\Roaming\{213D7E33

2. bash 3228 started it.



```
bash.exe (3228)
  bash.exe (3636)
    {71257279-042b-371d-a1d3-fbf8d2fadffa}.exe (2948)
      {213D7E33-3912-1C20-3D38-1A0B15CDFFF3}.exe (3196)
        {213D7E33-3912-1C20-3D38-1A0B15CDFFF3}.exe (2052)
```

3.

Process 3228 opens a file called bash.exe. It then It then opens reg key and performs some querys. It then opens some reg keys. 3228 then closes bash.exe.

Process 3636 then loads an image. And then reads several files. It also queries those files. It then opens some registry keys, and reads some dll files. It also starts some processes.

The above two processes are likely legit.

Process 3196 is started by a process started by3636. It edits a registry key.

4.

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker

This makes it so that anytime the user is logged in the program will run.