```
rule NotPetya_Ransomware_Jun17 {
   meta:
      description = "Detects new NotPetya Ransomware variant from June 2017"
      author = "Florian Roth"
      reference = "https://goo.gl/h6iaGj"
      date = "2017-06-27"
      hash1 = "027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745"
      hash2 = "45ef8d53a5a2011e615f60b058768c44c74e5190fefd790ca95cf035d9e1d5e0"
      hash3 = "64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1"
   strings:
      $x1 = "Ooops, your important files are encrypted." fullword wide ascii
      $x2 = "process call create \"C:\\Windows\\System32\\rundll32.exe \\\"C:\\Windows\\%s\\\" 
#1 " fullword wide
      $x3 = "-d C:\\Windows\\System32\\rundll32.exe \"C:\\Windows\\%s\",#1 " fullword wide
      $x4 = "Send your Bitcoin wallet ID and personal installation key to e-mail " fullword wide
      $x5 = "fsutil usn deletejournal /D %c:" fullword wide
      $x6 = "wevtutil cl Setup & wevtutil cl System" ascii
      /* ,#1 ..... rundll32.exe */
      $x7 = { 2C 00 23 00 31 00 20 00 00 00 00 00 00 00 00 00 72 00 75 00 6E
         00 64 00 6C 00 6C 00 33 00 32 00 2E 00 65 00 78 00 65 00 }

      $s1 = "%s /node:\"%ws\" /user:\"%ws\" /password:\"%ws\" " fullword wide
      $s4 = "\\\\.\\pipe\\%ws" fullword wide
      $s5 = "schtasks %ws/Create /SC once /TN \"\" /TR \"%ws\" /ST %02d:%02d" fullword wide
      $s6 = "u%s \\\\%s -accepteula -s " fullword wide
      $s7 = "dllhost.dat" fullword wide
   condition:
      uint16(0) == 0x5a4d and filesize < 1000KB and ( 1 of ($x*) or 3 of them )
}
```