Sign in

Neo23x0 / signature-base Public

Notifications Fork 603 Star 2.5k

Code Issues 11 Pull requests 4 Actions Projects Security Insights

signature-base / yara / gen_susp_lnk_files.yar

63 lines (60 loc) · 2.11 KB

Code Blame Raw

```

rule SUSP_LNK_lnkfileoverRFC {
   meta:
      description = "detect APT lnk files that run double extraction and launch routines with autor
      author = "@Grotezinfosec, modified by Florian Roth"
      date = "2018-09-18"
   strings:
      $command = "C:\\Windows\\System32\\cmd.exe" fullword ascii //cmd is precursor to findstr
      $command2 =  {2F 00 63 00 20 00 66 00 69 00 6E 00 64 00 73 00 74 00 72} //findstr in hex
      $base64 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAD" ascii //some base64 filler, needed to wo
      $cert = " -decode " ascii //base64 decoder
   condition:
      uint16(0) == 0x004c and uint32(4) == 0x00021401 and
      filesize > 15KB and (
         2 of them
      )
}

rule SUSP_LNK_SuspiciousCommands {
   meta:
      description = "Detects LNK file with suspicious content"
      author = "Florian Roth"
      date = "2018-09-18"
      score = 60
   strings:
      $s1 = " -decode " ascii wide
      $s2 = " -enc " ascii wide
      $s3 = " -w hidden " ascii wide
      $s4 = " -ep bypass " ascii wide
      $s5 = " -noni " ascii nocase wide
      /* $s6 = " bypass " ascii wide */
      $s7 = " -noprofile " ascii wide
      $s8 = ".DownloadString(" ascii wide
      $s9 = ".DownloadFile(" ascii wide
      $s10 = "IEX(" ascii wide
      $s11 = "iex(" ascii wide
      $s12 = "WScript.shell" ascii wide fullword nocase
      $s13 = " -nop " ascii wide
      $s14 = "&tasklist>"
      $s15 = "setlocal EnableExtensions DisableDelayedExpansion"
      $s16 = "echo^ set^"
      $s17 = "del /f /q "
      $s18 = " echo | start "
      $s19 = "&& echo "
      $s20 = "&&set "
      $s21 = "%&&@echo off "
   condition:
      uint16(0) == 0x004c and 1 of them
}

rule SUSP_DOC_LNK_in_ZIP {
   meta:
      description = "Detects suspicious .doc.lnk file in ZIP archive"
      author = "Florian Roth"
      reference = "https://twitter.com/RedDrip7/status/1145877272945025029"
      date = "2019-07-02"
      score = 50
      hash1 = "7ea4f77cac557044e72a8e280372a2abe072f2ad98b5a4fbed4e2229e780173a"
   strings:
      $s1 = ".doc.lnk" fullword ascii
   condition:
      uint16(0) == 0x4b50 and 1 of them
}
```