Gian Piero Siroli e' un fisico che lavora nel dominio sub-nucleare della fisica delle particelle elementari, la maggior parte della sua attivita' di ricerca ha luogo presso il CERN di Ginevra, ed in particolare si occupa degli aspetti informatici e delle infrastrutture di calcolo utilizzate in Fisica delle Alte Energie, nel cui contesto ha rappresentato l'Istituto Nazionale di Fisica Nucleare in commissioni e gruppi di lavoro internazionali. Nel passato GPS ha partecipato alle fasi iniziali dello sviluppo del World Wide Web avvenuto al CERN; attualmente e' il Computer Security Officer della collaborazione internazionale CMS, sempre al CERN.

Oltre ad altre attivita' didattiche nel settore della Fisica, GPS si occupa da piu' di 20 anni anche di cyber-security ed in particolare di aspetti riguardanti problematiche di guerra informatica (cyber/info-war), in un contesto ampiamente interdisciplinare.
Dal 1999 al 2008 ha insegnato un corso su "Tecnologie dell'informazione e sicurezza internazionale" presso il Dipartimento di Informatica dell'Universita' di Pisa; dal 2001 al 2009 ha insegnato un corso di "Laboratorio di reti di calcolatori", con particolare riferimento alla sicurezza di computer e reti, presso il Dipartimento di Fisica dell'Universita' di Bologna. Attualmente insegna un corso su "Cybersecurity e cybercrime" al corso di laurea magistrale in Relazioni Internazionali del Dipartimento di Scienze Politiche dell'Universita' di Bologna, e' membro del comitato scientifico del centro Dipartimentale per Computational Social Science e del comitato scientifico di IRIAD Review dell'Archivio Disarmo.
Su argomenti connessi a queste attivita', inclusi la digitalizzazione del campo di battaglia, l'uso della Artificial Intelligence nelle armi autonome, le Information Operations di manipolazione dei contenuti in rete per scopi di disinformazione, la cyber-intelligence e le dinamiche internazionali e ONU nel campo cibernetico, GPS ha tenuto e continua a tenere lezioni, seminari e conferenze, ha scritto vari articoli su riviste del settore, di divulgazione e contributi specifici su libri, in Italia ed all'estero, ed ha preso parte ad iniziative radio-televisive.

Tra numerose altre attivita', GPS e' stato coautore di un rapporto su "Protezione delle infrastrutture critiche informatizzate" del relativo gruppo di lavoro della Presidenza del Consiglio dei Ministri pubblicato nel 2004, ha tenuto lezioni presso il "Master in Relazioni Internazionali" dell'Universita' di Bologna, all'Academic Training Programme del CERN, e seminari all'Istituto Alti Studi della Difesa e presso il Quartier Generale I Brigata Aerea Operazioni Speciali.
Gian Piero Siroli ha partecipato a riunioni e conferenze organizzate dal United Nations Institute for Disarmament Affaris (UNIDIR) presso la sede ONU di Ginevra ed e' coinvolto nelle attivita' del Pugwash Conferences on Science and World Affairs, fondato dal A.Einstein e B.Russel nel 1955 ed insignito del Premio Nobel per la Pace nel 1995, nel cui contesto coordina le iniziative nel dominio della cybersecurity.
GPS e' disponibile a tenere lezioni, seminari e conferenze, ed e' aperto ad iniziative e collaborazioni su questi temi, sia a carattere di ricerca che divulgativo, soprattutto in contesti multidisciplinari.

```
10002033 mov     edi, ecx
10002035 call    esi ; GetTickCount
10002037 lea     ecx, ds:0[eax*8]
1000203E sub     ecx, eax
10002040 add     ecx, edi
10002042 push    ecx
10002043 push    offset aShell32_dll_as ; "SHELL32.DLL.ASLR."
10002048 lea     edx, [esp+224h+strFileName]
1000204C push    offset aS08x     ; "%s%08x"
10002051 push    edx              ; LPWSTR
10002052 call    ds:wsprintfW
10002058 mov     eax, [esp+22Ch+arg_4]
1000205F mov     ecx, [esp+22Ch+var_20C]
10002063 mov     edx, [esp+22Ch+hObject]
10002067 push    eax              ; int
10002068 push    ecx              ; int
10002069 push    edx              ; int
1000206A lea     eax, [esp+238h+strFileName]
1000206E push    eax              ; lpString2
1000206F call    sub_100034D2
10002074 mov     ecx, [esp+23Ch+hObject]
10002078 push    ecx              ; lpAddress
10002079 mov     esi, eax
1000207B call    sub_1000368F
10002080 add     esp, 24h
10002083 xor     eax, eax
10002085 pop     edi
10002086 test    esi, esi
```

) 00001423 10002023: CraftFile+53

```
v1 = GetModuleHandleA("kernel32.dll");
if ( v1
  && (v3 = GetModuleHandleA("ntdll.dll"),
      v4 = (int)GetModuleExport(v1, "VirtualAlloc"),
      (a1->Api.VirtualAlloc = v4) != 0)
  && (v5 = (int)GetModuleExport(v1, "Sleep"), (a1->Api.Sleep = v5) != 0)
  && (v6 = (int)GetModuleExport(v1, "VirtualFree"), (a1->Api.VirtualFree = v6) != 0)
  && (v7 = (int)GetModuleExport(v1, "VirtualProtect"), (a1->Api.VirtualProtect = v7) != 0)
  && (v8 = (int)GetModuleExport(v1, "LoadLibraryA"), (a1->Api.LoadLibraryA = v8) != 0)
  && (v9 = (int)GetModuleExport(v1, "GetProcAddress"), (a1->Api.GetProcAddress = v9) != 0)
  && (v10 = (int)GetModuleExport(v1, "GetModuleHandleA"), (a1->Api.GetModuleHandleA = v10) != 0)
  && (v11 = (int)GetModuleExport(v3, "memcpy"), (a1->Api.memcpy = v11) != 0)
  && (v12 = (int)GetModuleExport(v3, "memset"), (a1->Api.memset = v12) != 0)
  && (v13 = (int)GetModuleExport(v1, "FreeLibrary"), (a1->Api.FreeLibrary = v13) != 0)
  && (v14 = (int)GetModuleExport(v1, "OpenMutexW"), (a1->Api.OpenMutexW = v14) != 0)
  && (v15 = (int)GetModuleExport(v1, "CreateFileMappingW"), (a1->Api.CreateFileMappingW = v15) != 0)
  && (v16 = (int)GetModuleExport(v1, "MapViewOfFile"), (a1->Api.MapViewOfFile = v16) != 0)
  && (v17 = (int)GetModuleExport(v1, "UnmapViewOfFile"), (a1->Api.UnmapViewOfFile = v17) != 0)
  && (v18 = (int)GetModuleExport(v1, "CreateMutexW"), (a1->Api.CreateMutexW = v18) != 0)
  && (v19 = (int)GetModuleExport(v1, "WaitForSingleObject"), (a1->Api.WaitForSingleObject = v19) != 0)
  && (v20 = (int)GetModuleExport(v1, "CloseHandle"), (a1->Api.CloseHandle = v20) != 0)
  && (v21 = (int)GetModuleExport(v3, "NtQueryInformationProcess"), (a1->Api.NtQueryInformationProcess = v21) != 0)
  && (v22 = (int)GetModuleExport(v1, "GetLastError"), (a1->Api.GetLastError = v22) != 0)
  && (v23 = (int)GetModuleExport(v1, "ReleaseMutex"), (a1->Api.ReleaseMutex = v23) != 0)
  && (v24 = (int)GetModuleExport(v1, "OpenFileMappingW"), (a1->Api.OpenFileMappingW = v24) != 0)
  && (v25 = (int)GetModuleExport(v1, "LoadLibraryW"), (a1->Api.LoadLibraryW = v25) != 0)
  && (v26 = (int)GetModuleExport(v1, "CreateFileW"), (a1->Api.CreateFileW = v26) != 0) )
{
  v27 = (int)GetModuleExport(v1, "LocalFree");
  a1->Api.LocalFree = v27;
  result = v27 != 0;
}
```

```
jnieto@behindthefirewalls:/home/volatility-2.1$ python2 vol.py -f stuxnet.vmem pslist
Volatile Systems Volatility Framework 2.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ------ ------ ------ -------- ------ ------ -------------------
0x823c8830 System                    4      0     59      403 ------      0
0x820df020 smss.exe                376      4      3       19 ------      0 2010-10-29 17:08:53
0x821a2da0 csrss.exe               600    376     11      395      0      0 2010-10-29 17:08:54
0x81da5650 winlogon.exe            624    376     19      570      0      0 2010-10-29 17:08:54
0x82073020 services.exe            668    624     21      431      0      0 2010-10-29 17:08:54
0x81e70020 lsass.exe               680    624     19      342      0      0 2010-10-29 17:08:54
0x823315d8 vmacthlp.exe            844    668      1       25      0      0 2010-10-29 17:08:55
0x81db8da0 svchost.exe             856    668     17      193      0      0 2010-10-29 17:08:55
0x81e61da0 svchost.exe             940    668     13      312      0      0 2010-10-29 17:08:55
0x822843e8 svchost.exe            1032    668     61     1169      0      0 2010-10-29 17:08:55
0x81e18b28 svchost.exe            1080    668      5       80      0      0 2010-10-29 17:08:55
0x81ff7020 svchost.exe            1200    668     14      197      0      0 2010-10-29 17:08:55
0x81fee8b0 spoolsv.exe            1412    668     10      118      0      0 2010-10-29 17:08:56
0x81e0eda0 jqs.exe                1580    668      5      148      0      0 2010-10-29 17:09:05
0x81fe52d0 vmtoolsd.exe           1664    668      5      284      0      0 2010-10-29 17:09:05
0x821a0568 VMUpgradeHelper        1816    668      3       96      0      0 2010-10-29 17:09:08
0x8205ada0 alg.exe                 188    668      6      107      0      0 2010-10-29 17:09:09
0x820ec7e8 explorer.exe           1196   1728     16      582      0      0 2010-10-29 17:11:49
0x820ecc10 wscntfy.exe            2040   1032      1       28      0      0 2010-10-29 17:11:49
0x81e86978 TSVNCache.exe           324   1196      7       54      0      0 2010-10-29 17:11:49
0x81fc5da0 VMwareTray.exe         1912   1196      1       50      0      0 2010-10-29 17:11:50
0x81e6b660 VMwareUser.exe         1356   1196      9      251      0      0 2010-10-29 17:11:50
0x8210d478 jusched.exe            1712   1196      1       26      0      0 2010-10-29 17:11:50
0x82279998 imapi.exe               756    668      4      116      0      0 2010-10-29 17:11:54
0x822b9a10 wuauclt.exe             976   1032      3      133      0      0 2010-10-29 17:12:03
0x81c543a0 Procmon.exe             660   1196     13      189      0      0 2011-06-03 04:25:56
0x81fa5390 wmiprvse.exe           1872    856      5      134      0      0 2011-06-03 04:25:58
0x81c498c8 lsass.exe               868    668      2       23      0      0 2011-06-03 04:26:55
0x81c47c00 lsass.exe              1928    668      4       65      0      0 2011-06-03 04:26:55
0x81c0cda0 cmd.exe                 968   1664      0 --------      0      0 2011-06-03 04:31:35
0x81f14938 ipconfig.exe            304    968      0 --------      0      0 2011-06-03 04:31:35
```