APT3 Uncovered:
The code evolution of Pirpi

Your functions are showing (and leaving a trail)

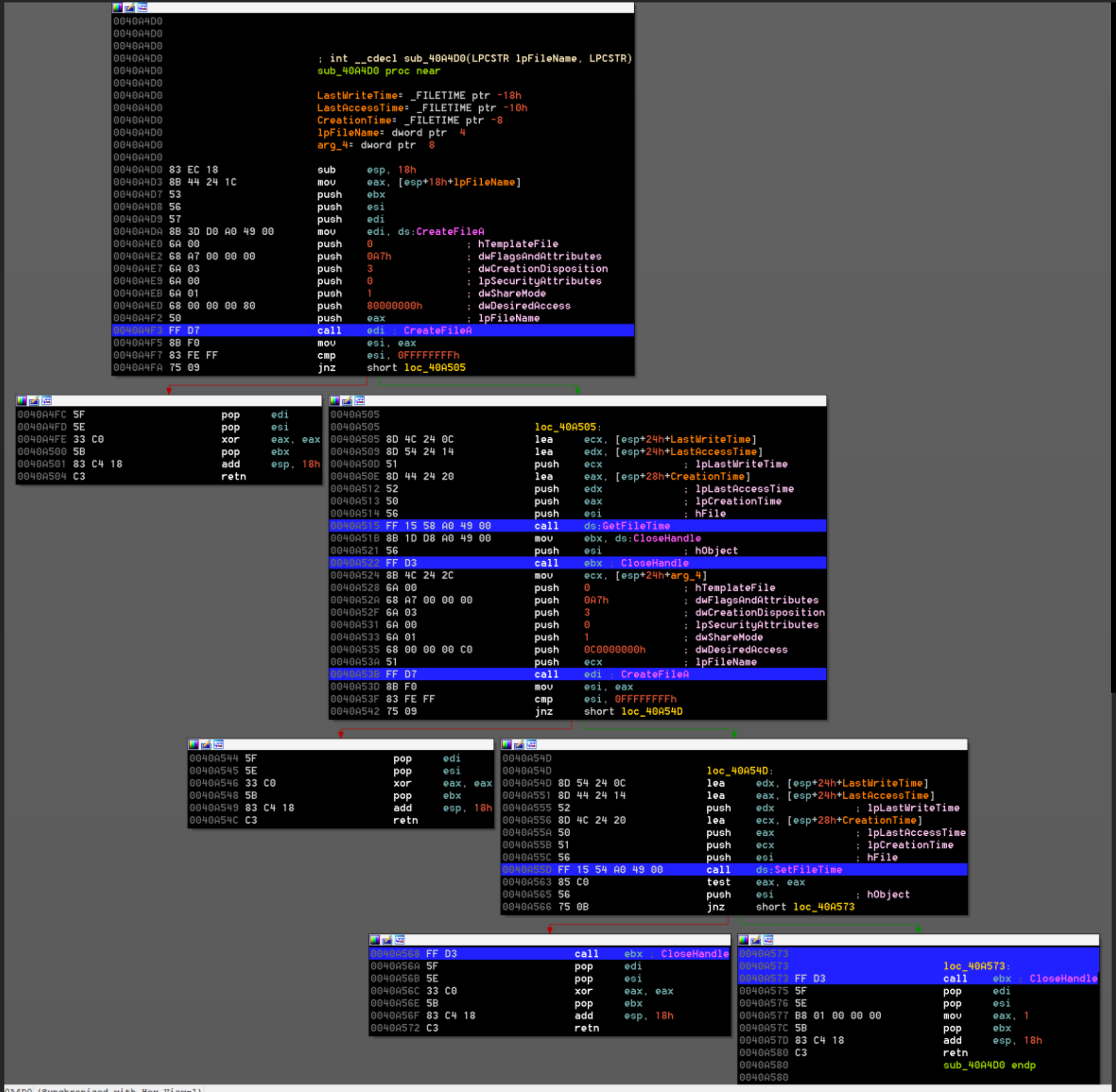
Micah Yates - @m1k4chu

Palo Alto Networks

Your functions are showing

- Persistent Code Reuse
- Finding The Trail
- Pirpi.201x vs Operation Clandestine DoubleTap
- Just give me all the Pirpi you have
- EXEProxy

Persistent Code Reuse: function_1



```
0040A4D0
0040A4D0
0040A4D0
0040A4D0                   ; int __cdecl sub_40A4D0(LPCSTR lpFileName, LPCSTR)
0040A4D0                   sub_40A4D0 proc near
0040A4D0
0040A4D0                   LastWriteTime= _FILETIME ptr -18h
0040A4D0                   LastAccessTime= _FILETIME ptr -10h
0040A4D0                   CreationTime= _FILETIME ptr -8
0040A4D0                   lpFileName= dword ptr  4
0040A4D0                   arg_4= dword ptr  8
0040A4D0
0040A4D0 83 EC 18          sub     esp, 18h
0040A4D3 8B 44 24 1C       mov     eax, [esp+18h+lpFileName]
0040A4D7 53                push    ebx
0040A4D8 56                push    esi
0040A4D9 57                push    edi
0040A4DA 8B 3D D0 A0 49 00 mov     edi, ds:CreateFileA
0040A4E0 6A 00             push    0               ; hTemplateFile
0040A4E2 68 A7 00 00 00    push    0A7h            ; dwFlagsAndAttributes
0040A4E7 6A 03             push    3               ; dwCreationDisposition
0040A4E9 6A 00             push    0               ; lpSecurityAttributes
0040A4EB 6A 01             push    1               ; dwShareMode
0040A4ED 68 00 00 00 80    push    80000000h       ; dwDesiredAccess
0040A4F2 50                push    eax             ; lpFileName
0040A4F3 FF D7             call    edi ; CreateFileA
0040A4F5 8B F0             mov     esi, eax
0040A4F7 83 FE FF          cmp     esi, 0FFFFFFFFh
0040A4FA 75 09             jnz     short loc_40A505
```

```
0040A4FC 5F                pop     edi
0040A4FD 5E                pop     esi
0040A4FE 33 C0             xor     eax, eax
0040A500 5B                pop     ebx
0040A501 83 C4 18          add     esp, 18h
0040A504 C3                retn
```

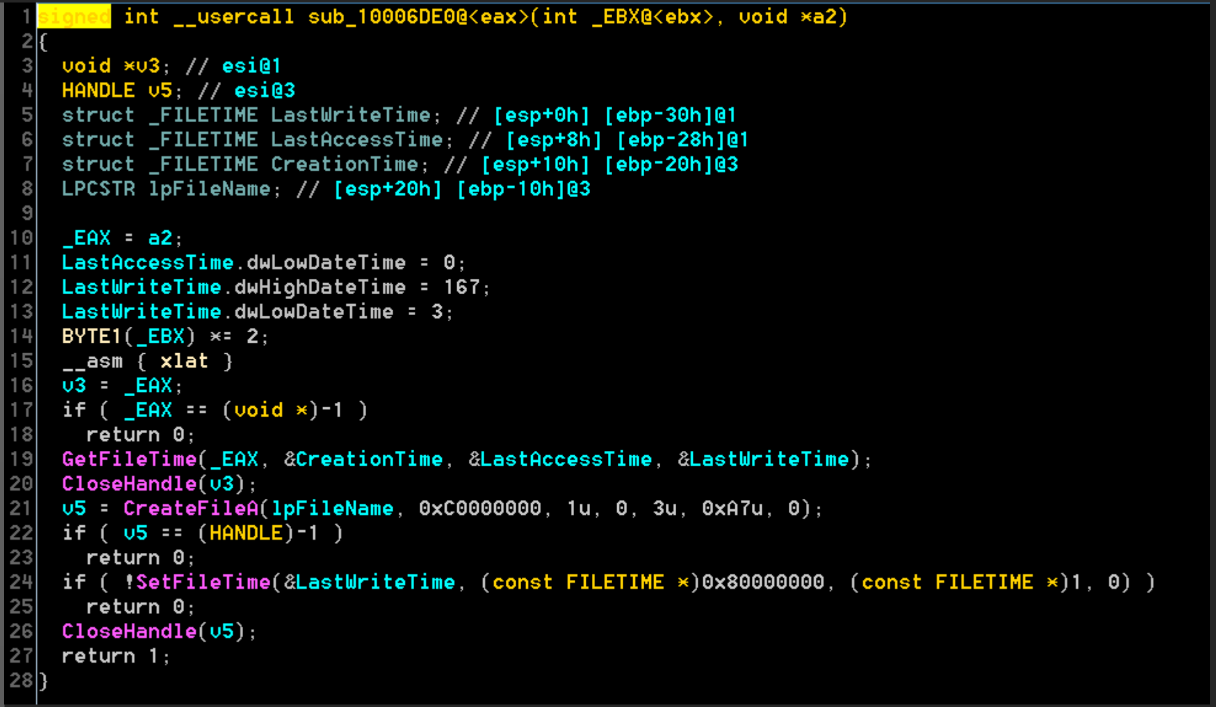
```
0040A505
0040A505                   loc_40A505:
0040A505 8D 4C 24 0C       lea     ecx, [esp+24h+LastWriteTime]
0040A509 8D 54 24 14       lea     edx, [esp+24h+LastAccessTime]
0040A50D 51                push    ecx             ; lpLastWriteTime
0040A50E 8D 44 24 20       lea     eax, [esp+28h+CreationTime]
0040A512 52                push    edx             ; lpLastAccessTime
0040A513 50                push    eax             ; lpCreationTime
0040A514 56                push    esi             ; hFile
0040A515 FF 15 58 A0 49 00 call    ds:GetFileTime
0040A51B 8B 1D D8 A0 49 00 mov     ebx, ds:CloseHandle
0040A521 56                push    esi             ; hObject
0040A522 FF D3             call    ebx ; CloseHandle
0040A524 8B 4C 24 2C       mov     ecx, [esp+24h+arg_4]
0040A528 6A 00             push    0               ; hTemplateFile
0040A52A 68 A7 00 00 00    push    0A7h            ; dwFlagsAndAttributes
0040A52F 6A 03             push    3               ; dwCreationDisposition
0040A531 6A 00             push    0               ; lpSecurityAttributes
0040A533 6A 01             push    1               ; dwShareMode
0040A535 68 00 00 00 C0    push    0C0000000h      ; dwDesiredAccess
0040A53A 51                push    ecx             ; lpFileName
0040A53B FF D7             call    edi ; CreateFileA
0040A53D 8B F0             mov     esi, eax
0040A53F 83 FE FF          cmp     esi, 0FFFFFFFFh
0040A542 75 09             jnz     short loc_40A54D
```

```
0040A544 5F                pop     edi
0040A545 5E                pop     esi
0040A546 33 C0             xor     eax, eax
0040A548 5B                pop     ebx
0040A549 83 C4 18          add     esp, 18h
0040A54C C3                retn
```

```
0040A54D
0040A54D                   loc_40A54D:
0040A54D 8D 54 24 0C       lea     edx, [esp+24h+LastWriteTime]
0040A551 8D 44 24 14       lea     eax, [esp+24h+LastAccessTime]
0040A555 52                push    edx             ; lpLastWriteTime
0040A556 8D 4C 24 20       lea     ecx, [esp+28h+CreationTime]
0040A55A 50                push    eax             ; lpLastAccessTime
0040A55B 51                push    ecx             ; lpCreationTime
0040A55C 56                push    esi             ; hFile
0040A55D FF 15 54 A0 49 00 call    ds:SetFileTime
0040A563 85 C0             test    eax, eax
0040A565 56                push    esi             ; hObject
0040A566 75 0B             jnz     short loc_40A573
```

```
0040A568 FF D3             call    ebx ; CloseHandle
0040A56A 5F                pop     edi
0040A56B 5E                pop     esi
0040A56C 33 C0             xor     eax, eax
0040A56E 5B                pop     ebx
0040A56F 83 C4 18          add     esp, 18h
0040A572 C3                retn
```

```
0040A573
0040A573                   loc_40A573:
0040A573 FF D3             call    ebx ; CloseHandle
0040A575 5F                pop     edi
0040A576 5E                pop     esi
0040A577 B8 01 00 00 00    mov     eax, 1
0040A57C 5B                pop     ebx
0040A57D 83 C4 18          add     esp, 18h
0040A580 C3                retn
0040A580                   sub_40A4D0 endp
0040A580
```



```
signed int __usercall sub_10006DE0@<eax>(int _EBX@<ebx>, void *a2)
{
  void *v3; // esi@1
  HANDLE v5; // esi@3
  struct _FILETIME LastWriteTime; // [esp+0h] [ebp-30h]@1
  struct _FILETIME LastAccessTime; // [esp+8h] [ebp-28h]@1
  struct _FILETIME CreationTime; // [esp+10h] [ebp-20h]@3
  LPCSTR lpFileName; // [esp+20h] [ebp-10h]@3

  _EAX = a2;
  LastAccessTime.dwLowDateTime = 0;
  LastWriteTime.dwHighDateTime = 167;
  LastWriteTime.dwLowDateTime = 3;
  BYTE1(_EBX) *= 2;
  __asm { xlat }
  v3 = _EAX;
  if ( _EAX == (void *)-1 )
    return 0;
  GetFileTime(_EAX, &CreationTime, &LastAccessTime, &LastWriteTime);
  CloseHandle(v3);
  v5 = CreateFileA(lpFileName, 0xC0000000, 1u, 0, 3u, 0xA7u, 0);
  if ( v5 == (HANDLE)-1 )
    return 0;
  if ( !SetFileTime(&LastWriteTime, (const FILETIME *)0x80000000, (const FILETIME *)1, 0) )
    return 0;
  CloseHandle(v5);
  return 1;
}
```

Persistent Code Reuse

- What is Pirpi?
  - Targeted malware delivered via 0-days
    - (CVE-2010-3962)
    - (CVE-2014-1776)
    - (CVE-2014-4113)
    - (CVE-2014-6332)
    - (CVE-2015-3113)
    - (CVE-2015-5119)
  - Appended to a valid gif
  - Obfuscated Command and Control
  - Compromised infrastructure

Finding a Trail

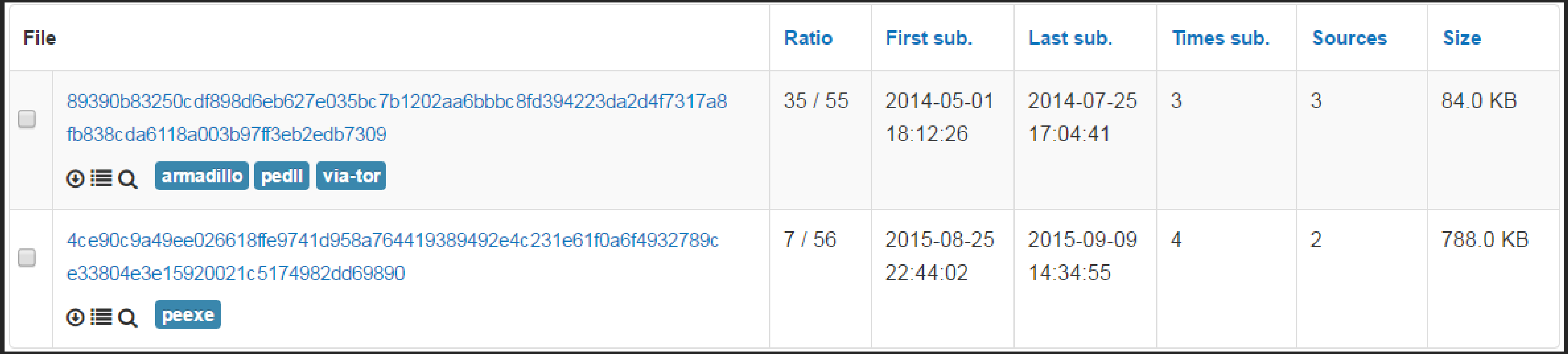
- Why are you doing this?
  - It’s fun
  - You don’t know what you don’t know

- Pick 2 binaries by:
  - Family
  - Compile Times
  - File Size
  - % similarity (ssdeep)

It started out with a diff, how did it end up like this?

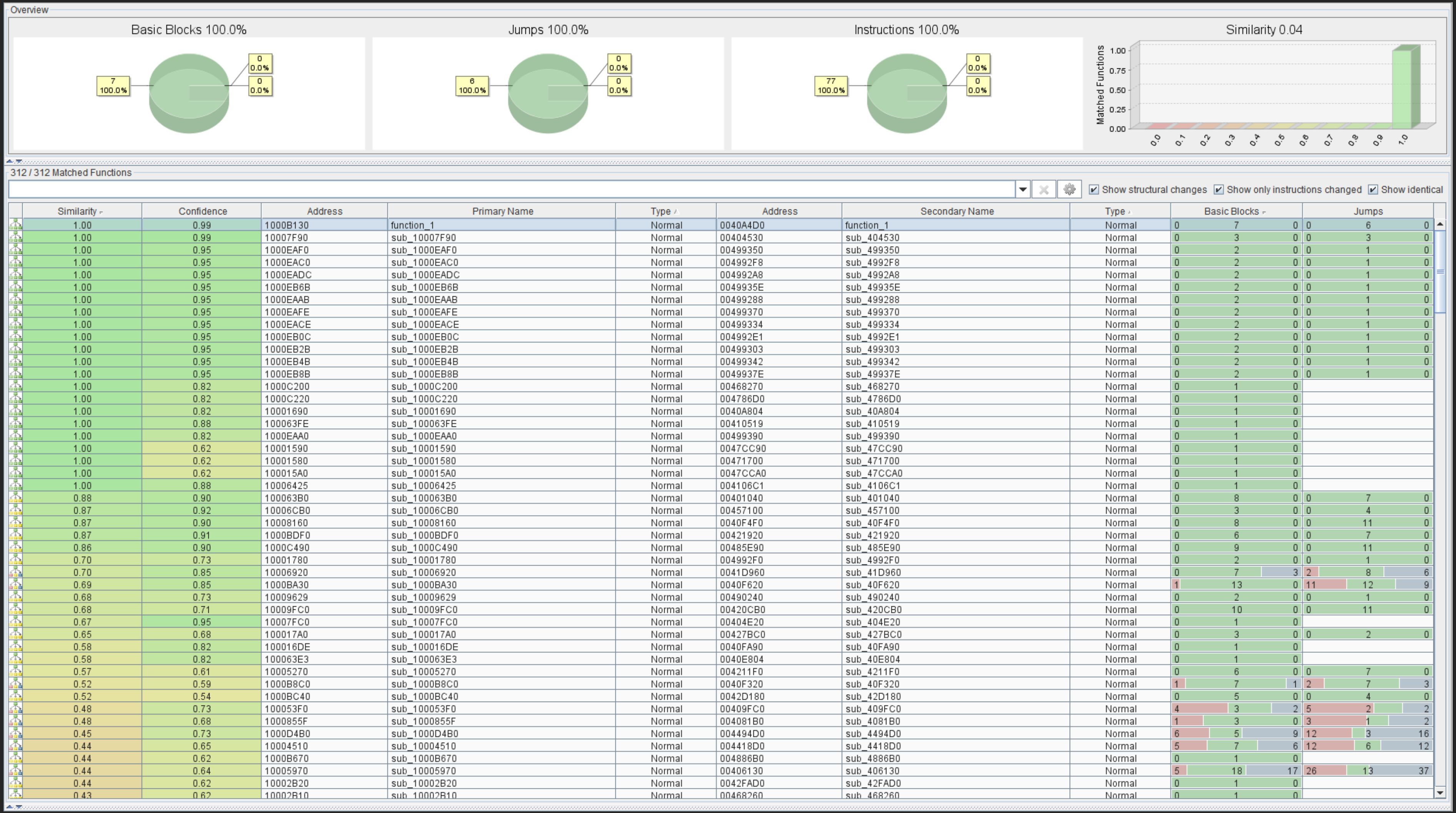
- Inspect Binaries w/ IDA Tools
  - Bindiff – Hex Rays
  - IDAScope – Plohmann/Hanel

- Bindiff two known Pirpi samples
  - fb838cda6118a003b97ff3eb2edb7309
  - e33804e3e15920021c5174982dd69890



File		Ratio	First sub.	Last sub.	Times sub.	Sources	Size
□	89390b83250cdf898d6eb627e035bc7b1202aa6bbbc8fd394223da2d4f7317a8 fb838cda6118a003b97ff3eb2edb7309 armadillo pedll via-tor	35 / 55	2014-05-01 18:12:26	2014-07-25 17:04:41	3	3	84.0 KB
□	4ce90c9a49ee026618ffe9741d958a764419389492e4c231e61f0a6f4932789c e33804e3e15920021c5174982dd69890 peexe	7 / 56	2015-08-25 22:44:02	2015-09-09 14:34:55	4	2	788.0 KB

It was only a diff

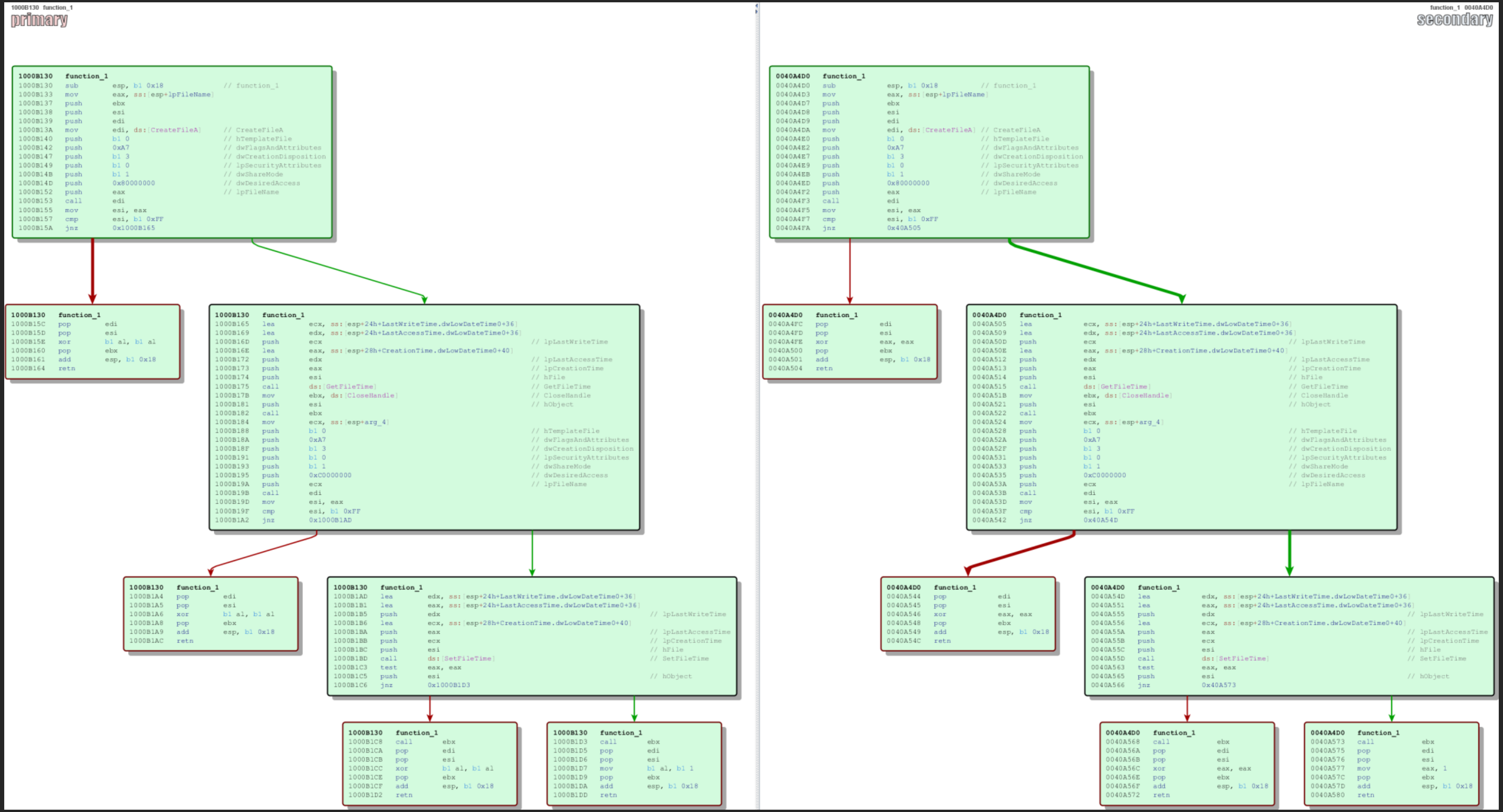


312 / 312 Matched Functions

☑ Show structural changes ☑ Show only instructions changed ☑ Show identical

Similarity	Confidence	Address	Primary Name	Type	Address	Secondary Name	Type	Basic Blocks	Jumps
1.00	0.99	1000B130	function_1	Normal	0040A4D0	function_1	Normal	0 7 0	0 6 0
1.00	0.99	10007F90	sub_10007F90	Normal	00404530	sub_404530	Normal	0 3 0	0 3 0
1.00	0.95	1000EAF0	sub_1000EAF0	Normal	00499350	sub_499350	Normal	0 2 0	0 1 0
1.00	0.95	1000EAC0	sub_1000EAC0	Normal	004992F8	sub_4992F8	Normal	0 2 0	0 1 0
1.00	0.95	1000EADC	sub_1000EADC	Normal	004992A8	sub_4992A8	Normal	0 2 0	0 1 0
1.00	0.95	1000EB6B	sub_1000EB6B	Normal	0049935E	sub_49935E	Normal	0 2 0	0 1 0
1.00	0.95	1000EAAB	sub_1000EAAB	Normal	00499288	sub_499288	Normal	0 2 0	0 1 0
1.00	0.95	1000EAFE	sub_1000EAFE	Normal	00499370	sub_499370	Normal	0 2 0	0 1 0
1.00	0.95	1000EACE	sub_1000EACE	Normal	00499334	sub_499334	Normal	0 2 0	0 1 0
1.00	0.95	1000EB0C	sub_1000EB0C	Normal	004992E1	sub_4992E1	Normal	0 2 0	0 1 0
1.00	0.95	1000EB2B	sub_1000EB2B	Normal	00499303	sub_499303	Normal	0 2 0	0 1 0
1.00	0.95	1000EB4B	sub_1000EB4B	Normal	00499342	sub_499342	Normal	0 2 0	0 1 0
1.00	0.95	1000EB8B	sub_1000EB8B	Normal	0049937E	sub_49937E	Normal	0 2 0	0 1 0
1.00	0.82	1000C200	sub_1000C200	Normal	00468270	sub_468270	Normal	0 1 0	
1.00	0.82	1000C220	sub_1000C220	Normal	004786D0	sub_4786D0	Normal	0 1 0	
1.00	0.82	10001690	sub_10001690	Normal	0040A804	sub_40A804	Normal	0 1 0	
1.00	0.88	100063FE	sub_100063FE	Normal	00410519	sub_410519	Normal	0 1 0	
1.00	0.82	1000EAA0	sub_1000EAA0	Normal	00499390	sub_499390	Normal	0 1 0	
1.00	0.62	10001590	sub_10001590	Normal	0047CC90	sub_47CC90	Normal	0 1 0	
1.00	0.62	10001580	sub_10001580	Normal	00471700	sub_471700	Normal	0 1 0	
1.00	0.62	100015A0	sub_100015A0	Normal	0047CCA0	sub_47CCA0	Normal	0 1 0	
1.00	0.88	10006425	sub_10006425	Normal	004106C1	sub_4106C1	Normal	0 1 0	
0.88	0.90	100063B0	sub_100063B0	Normal	00401040	sub_401040	Normal	0 8 0	0 7 0
0.87	0.92	10006CB0	sub_10006CB0	Normal	00457100	sub_457100	Normal	0 3 0	0 4 0
0.87	0.90	10008160	sub_10008160	Normal	0040F4F0	sub_40F4F0	Normal	0 8 0	0 11 0
0.87	0.91	1000BDF0	sub_1000BDF0	Normal	00421920	sub_421920	Normal	0 6 0	0 7 0
0.86	0.90	1000C490	sub_1000C490	Normal	00485E90	sub_485E90	Normal	0 9 0	0 11 0
0.70	0.73	10001780	sub_10001780	Normal	004992F0	sub_4992F0	Normal	0 2 0	0 1 0
0.70	0.85	10006920	sub_10006920	Normal	0041D960	sub_41D960	Normal	0 7 3	2 8 6
0.69	0.85	1000BA30	sub_1000BA30	Normal	0040F620	sub_40F620	Normal	1 13 0	11 12 9
0.68	0.73	10009629	sub_10009629	Normal	00490240	sub_490240	Normal	0 2 0	0 1 0
0.68	0.71	10009FC0	sub_10009FC0	Normal	00420CB0	sub_420CB0	Normal	0 10 0	0 11 0
0.67	0.95	10007FC0	sub_10007FC0	Normal	00404E20	sub_404E20	Normal	0 1 0	
0.65	0.68	100017A0	sub_100017A0	Normal	00427BC0	sub_427BC0	Normal	0 3 0	0 2 0
0.58	0.82	100016DE	sub_100016DE	Normal	0040FA90	sub_40FA90	Normal	0 1 0	
0.58	0.82	100063E3	sub_100063E3	Normal	0040E804	sub_40E804	Normal	0 1 0	
0.57	0.61	10005270	sub_10005270	Normal	004211F0	sub_4211F0	Normal	0 6 0	0 7 0
0.52	0.59	1000B8C0	sub_1000B8C0	Normal	0040F320	sub_40F320	Normal	1 7 1	2 7 3
0.52	0.54	1000BC40	sub_1000BC40	Normal	0042D180	sub_42D180	Normal	0 5 0	0 4 0
0.48	0.73	100053F0	sub_100053F0	Normal	00409FC0	sub_409FC0	Normal	4 3 2	5 2 2
0.48	0.68	1000855F	sub_1000855F	Normal	004081B0	sub_4081B0	Normal	1 3 0	3 1 2
0.45	0.73	1000D4B0	sub_1000D4B0	Normal	004494D0	sub_4494D0	Normal	6 5 9	12 3 16
0.44	0.65	10004510	sub_10004510	Normal	004418D0	sub_4418D0	Normal	5 7 6	12 6 12
0.44	0.62	1000B670	sub_1000B670	Normal	004886B0	sub_4886B0	Normal	0 1 0	
0.44	0.64	10005970	sub_10005970	Normal	00406130	sub_406130	Normal	5 18 17	26 13 37
0.44	0.62	10002B20	sub_10002B20	Normal	0042FAD0	sub_42FAD0	Normal	0 1 0	
0.43	0.62	10002B10	sub_10002B10	Normal	00468260	sub_468260	Normal	0 1 0	

It was only a diff



1000B130 function_1

primary

```
1000B130   function_1
1000B130   sub        esp, b1 0x18                 // function_1
1000B133   mov        eax, ss:[esp+lpFileName]
1000B137   push       ebx
1000B138   push       esi
1000B139   push       edi
1000B13A   mov        edi, ds:[CreateFileA]        // CreateFileA
1000B140   push       b1 0                         // hTemplateFile
1000B142   push       0xA7                         // dwFlagsAndAttributes
1000B147   push       b1 3                         // dwCreationDisposition
1000B149   push       b1 0                         // lpSecurityAttributes
1000B14B   push       b1 1                         // dwShareMode
1000B14D   push       0x80000000                   // dwDesiredAccess
1000B152   push       eax                          // lpFileName
1000B153   call       edi
1000B155   mov        esi, eax
1000B157   cmp        esi, b1 0xFF
1000B15A   jnz        0x1000B165
```

```
1000B130   function_1
1000B15C   pop        edi
1000B15D   pop        esi
1000B15E   xor        b1 al, b1 al
1000B160   pop        ebx
1000B161   add        esp, b1 0x18
1000B164   retn
```

```
1000B130   function_1
1000B165   lea        ecx, ss:[esp+24h+LastWriteTime.dwLowDateTime0+36]
1000B169   lea        edx, ss:[esp+24h+LastAccessTime.dwLowDateTime0+36]
1000B16D   push       ecx                                                  // lpLastWriteTime
1000B16E   lea        eax, ss:[esp+28h+CreationTime.dwLowDateTime0+40]
1000B172   push       edx                                                  // lpLastAccessTime
1000B173   push       eax                                                  // lpCreationTime
1000B174   push       esi                                                  // hFile
1000B175   call       ds:[GetFileTime]                                     // GetFileTime
1000B17B   mov        ebx, ds:[CloseHandle]                                // CloseHandle
1000B181   push       esi                                                  // hObject
1000B182   call       ebx
1000B184   mov        ecx, ss:[esp+arg_4]
1000B188   push       b1 0                                                 // hTemplateFile
1000B18A   push       0xA7                                                 // dwFlagsAndAttributes
1000B18F   push       b1 3                                                 // dwCreationDisposition
1000B191   push       b1 0                                                 // lpSecurityAttributes
1000B193   push       b1 1                                                 // dwShareMode
1000B195   push       0xC0000000                                           // dwDesiredAccess
1000B19A   push       ecx                                                  // lpFileName
1000B19B   call       edi
1000B19D   mov        esi, eax
1000B19F   cmp        esi, b1 0xFF
1000B1A2   jnz        0x1000B1AD
```

```
1000B130   function_1
1000B1A4   pop        edi
1000B1A5   pop        esi
1000B1A6   xor        b1 al, b1 al
1000B1A8   pop        ebx
1000B1A9   add        esp, b1 0x18
1000B1AC   retn
```

```
1000B130   function_1
1000B1AD   lea        edx, ss:[esp+24h+LastWriteTime.dwLowDateTime0+36]
1000B1B1   lea        eax, ss:[esp+24h+LastAccessTime.dwLowDateTime0+36]
1000B1B5   push       edx                                                  // lpLastWriteTime
1000B1B6   lea        ecx, ss:[esp+28h+CreationTime.dwLowDateTime0+40]
1000B1BA   push       eax                                                  // lpLastAccessTime
1000B1BB   push       ecx                                                  // lpCreationTime
1000B1BC   push       esi                                                  // hFile
1000B1BD   call       ds:[SetFileTime]                                     // SetFileTime
1000B1C3   test       eax, eax
1000B1C5   push       esi                                                  // hObject
1000B1C6   jnz        0x1000B1D3
```

```
1000B130   function_1
1000B1C8   call       ebx
1000B1CA   pop        edi
1000B1CB   pop        esi
1000B1CC   xor        b1 al, b1 al
1000B1CE   pop        ebx
1000B1CF   add        esp, b1 0x18
1000B1D2   retn
```

```
1000B130   function_1
1000B1D3   call       ebx
1000B1D5   pop        edi
1000B1D6   pop        esi
1000B1D7   mov        b1 al, b1 1
1000B1D9   pop        ebx
1000B1DA   add        esp, b1 0x18
1000B1DD   retn
```

function_1 0040A4D0

secondary

```
0040A4D0   function_1
0040A4D0   sub           esp, b1 0x18          // function_1
0040A4D3   mov           eax, ss:[esp+lpFileName]
0040A4D7   push          ebx
0040A4D8   push          esi
0040A4D9   push          edi
0040A4DA   mov           edi, ds:[CreateFileA] // CreateFileA
0040A4E0   push          b1 0                  // hTemplateFile
0040A4E2   push          0xA7                  // dwFlagsAndAttributes
0040A4E7   push          b1 3                  // dwCreationDisposition
0040A4E9   push          b1 0                  // lpSecurityAttributes
0040A4EB   push          b1 1                  // dwShareMode
0040A4ED   push          0x80000000            // dwDesiredAccess
0040A4F2   push          eax                   // lpFileName
0040A4F3   call          edi
0040A4F5   mov           esi, eax
0040A4F7   cmp           esi, b1 0xFF
0040A4FA   jnz           0x40A505
```

```
0040A4D0   function_1
0040A4FC   pop           edi
0040A4FD   pop           esi
0040A4FE   xor           eax, eax
0040A500   pop           ebx
0040A501   add           esp, b1 0x18
0040A504   retn
```

```
0040A4D0   function_1
0040A505   lea           ecx, ss:[esp+24h+LastWriteTime.dwLowDateTime0+36]
0040A509   lea           edx, ss:[esp+24h+LastAccessTime.dwLowDateTime0+36]
0040A50D   push          ecx                                                  // lpLastWriteTime
0040A50E   lea           eax, ss:[esp+28h+CreationTime.dwLowDateTime0+40]
0040A512   push          edx                                                  // lpLastAccessTime
0040A513   push          eax                                                  // lpCreationTime
0040A514   push          esi                                                  // hFile
0040A515   call          ds:[GetFileTime]                                     // GetFileTime
0040A51B   mov           ebx, ds:[CloseHandle]                                // CloseHandle
0040A521   push          esi                                                  // hObject
0040A522   call          ebx
0040A524   mov           ecx, ss:[esp+arg_4]
0040A528   push          b1 0                                                 // hTemplateFile
0040A52A   push          0xA7                                                 // dwFlagsAndAttributes
0040A52F   push          b1 3                                                 // dwCreationDisposition
0040A531   push          b1 0                                                 // lpSecurityAttributes
0040A533   push          b1 1                                                 // dwShareMode
0040A535   push          0xC0000000                                           // dwDesiredAccess
0040A53A   push          ecx                                                  // lpFileName
0040A53B   call          edi
0040A53D   mov           esi, eax
0040A53F   cmp           esi, b1 0xFF
0040A542   jnz           0x40A54D
```

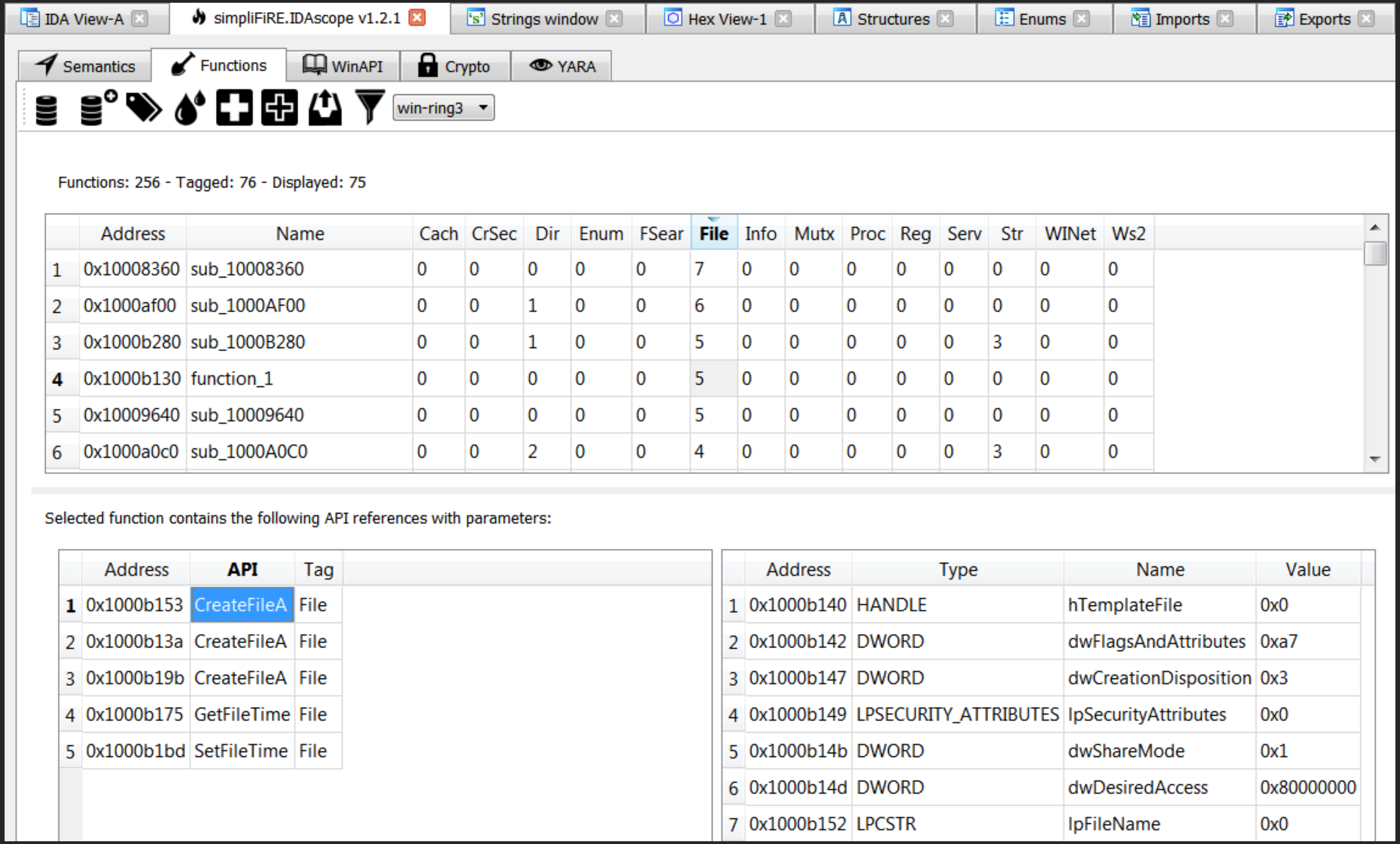
```
0040A4D0   function_1
0040A544   pop           edi
0040A545   pop           esi
0040A546   xor           eax, eax
0040A548   pop           ebx
0040A549   add           esp, b1 0x18
0040A54C   retn
```

```
0040A4D0   function_1
0040A54D   lea           edx, ss:[esp+24h+LastWriteTime.dwLowDateTime0+36]
0040A551   lea           eax, ss:[esp+24h+LastAccessTime.dwLowDateTime0+36]
0040A555   push          edx                                                  // lpLastWriteTime
0040A556   lea           ecx, ss:[esp+28h+CreationTime.dwLowDateTime0+40]
0040A55A   push          eax                                                  // lpLastAccessTime
0040A55B   push          ecx                                                  // lpCreationTime
0040A55C   push          esi                                                  // hFile
0040A55D   call          ds:[SetFileTime]                                     // SetFileTime
0040A563   test          eax, eax
0040A565   push          esi                                                  // hObject
0040A566   jnz           0x40A573
```

```
0040A4D0   function_1
0040A568   call          ebx
0040A56A   pop           edi
0040A56B   pop           esi
0040A56C   xor           eax, eax
0040A56E   pop           ebx
0040A56F   add           esp, b1 0x18
0040A572   retn
```

```
0040A4D0   function_1
0040A573   call          ebx
0040A575   pop           edi
0040A576   pop           esi
0040A577   mov           eax, 1
0040A57C   pop           ebx
0040A57D   add           esp, b1 0x18
0040A580   retn
```

Aside:
Putting the FUN in Function



Functions: 256 - Tagged: 76 - Displayed: 75

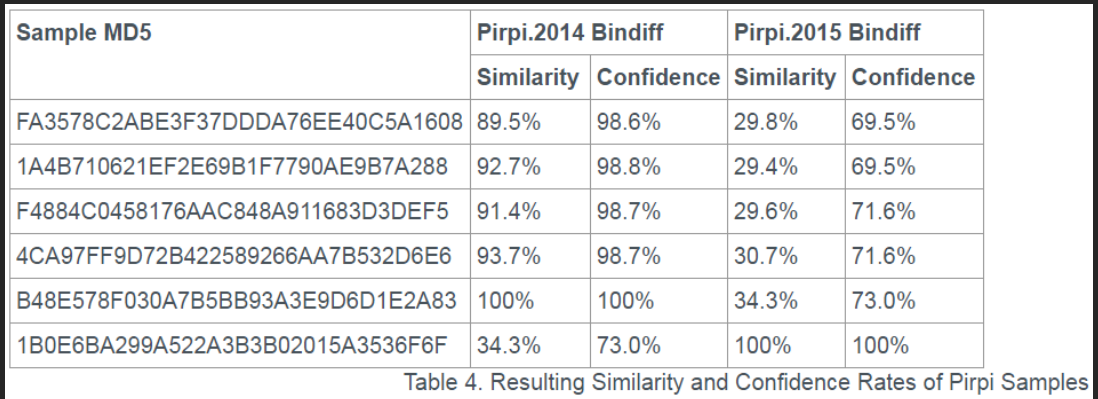
	Address	Name	Cach	CrSec	Dir	Enum	FSear	File	Info	Mutx	Proc	Reg	Serv	Str	WINet	Ws2
1	0x10008360	sub_10008360	0	0	0	0	0	7	0	0	0	0	0	0	0	0
2	0x1000af00	sub_1000AF00	0	0	1	0	0	6	0	0	0	0	0	0	0	0
3	0x1000b280	sub_1000B280	0	0	1	0	0	5	0	0	0	0	0	3	0	0
4	0x1000b130	function_1	0	0	0	0	0	5	0	0	0	0	0	0	0	0
5	0x10009640	sub_10009640	0	0	0	0	0	5	0	0	0	0	0	0	0	0
6	0x1000a0c0	sub_1000A0C0	0	0	2	0	0	4	0	0	0	0	0	3	0	0

Selected function contains the following API references with parameters:

	Address	API	Tag
1	0x1000b153	CreateFileA	File
2	0x1000b13a	CreateFileA	File
3	0x1000b19b	CreateFileA	File
4	0x1000b175	GetFileTime	File
5	0x1000b1bd	SetFileTime	File

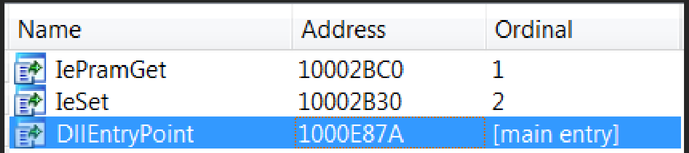
	Address	Type	Name	Value
1	0x1000b140	HANDLE	hTemplateFile	0x0
2	0x1000b142	DWORD	dwFlagsAndAttributes	0xa7
3	0x1000b147	DWORD	dwCreationDisposition	0x3
4	0x1000b149	LPSECURITY_ATTRIBUTES	lpSecurityAttributes	0x0
5	0x1000b14b	DWORD	dwShareMode	0x1
6	0x1000b14d	DWORD	dwDesiredAccess	0x80000000
7	0x1000b152	LPCSTR	lpFileName	0x0

Pirpi.201x vs Operation Clandestine DoubleTap

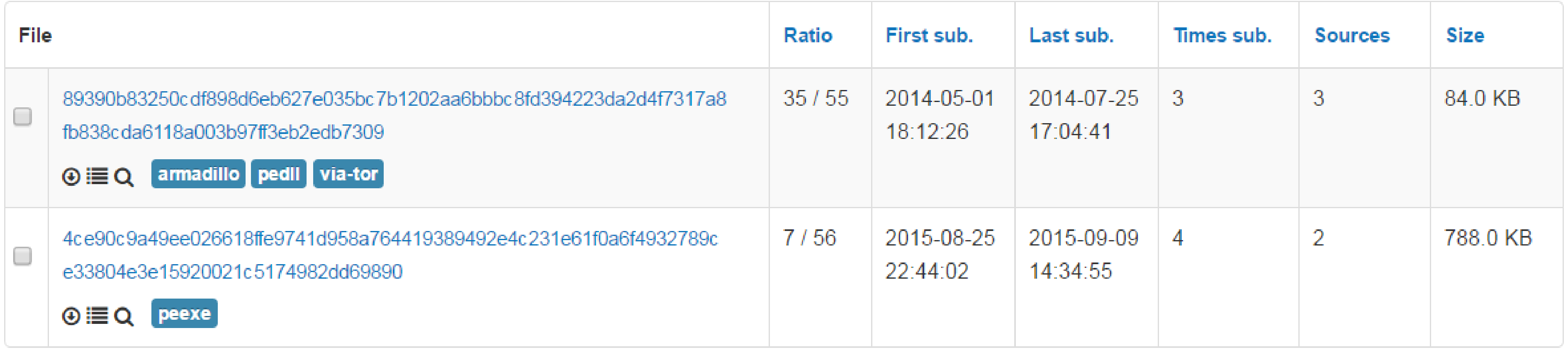


Sample MD5	Pirpi.2014 Bindiff		Pirpi.2015 Bindiff	
	Similarity	Confidence	Similarity	Confidence
FA3578C2ABE3F37DDDA76EE40C5A1608	89.5%	98.6%	29.8%	69.5%
1A4B710621EF2E69B1F7790AE9B7A288	92.7%	98.8%	29.4%	69.5%
F4884C0458176AAC848A911683D3DEF5	91.4%	98.7%	29.6%	71.6%
4CA97FF9D72B422589266AA7B532D6E6	93.7%	98.7%	30.7%	71.6%
B48E578F030A7B5BB93A3E9D6D1E2A83	100%	100%	34.3%	73.0%
1B0E6BA299A522A3B3B02015A3536F6F	34.3%	73.0%	100%	100%

Table 4. Resulting Similarity and Confidence Rates of Pirpi Samples

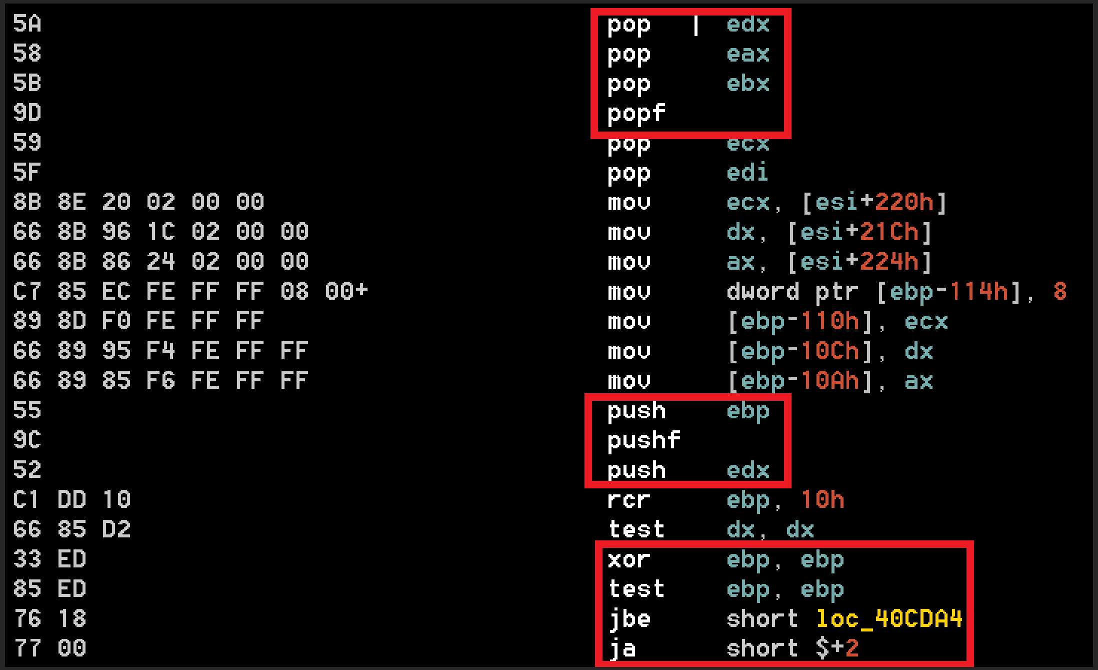


Name	Address	Ordinal
IePramGet	10002BC0	1
IeSet	10002B30	2
DllEntryPoint	1000E87A	[main entry]

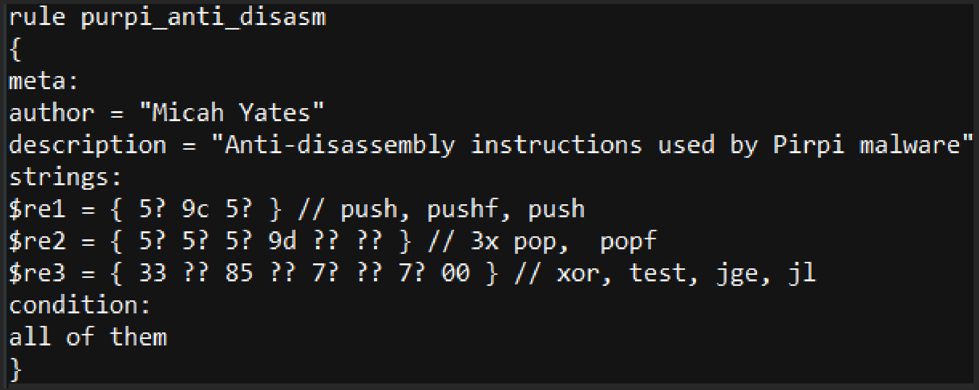


	File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
□	89390b83250cdf898d6eb627e035bc7b1202aa6bbbc8fd394223da2d4f7317a8fb838cda6118a003b97ff3eb2edb7309 armadillo pedll via-tor	35 / 55	2014-05-01 18:12:26	2014-07-25 17:04:41	3	3	84.0 KB
□	4ce90c9a49ee026618ffe9741d958a764419389492e4c231e61f0a6f4932789ce33804e3e15920021c5174982dd69890 peexe	7 / 56	2015-08-25 22:44:02	2015-09-09 14:34:55	4	2	788.0 KB

Pirpi.201x vs Operation Clandestine DoubleTap

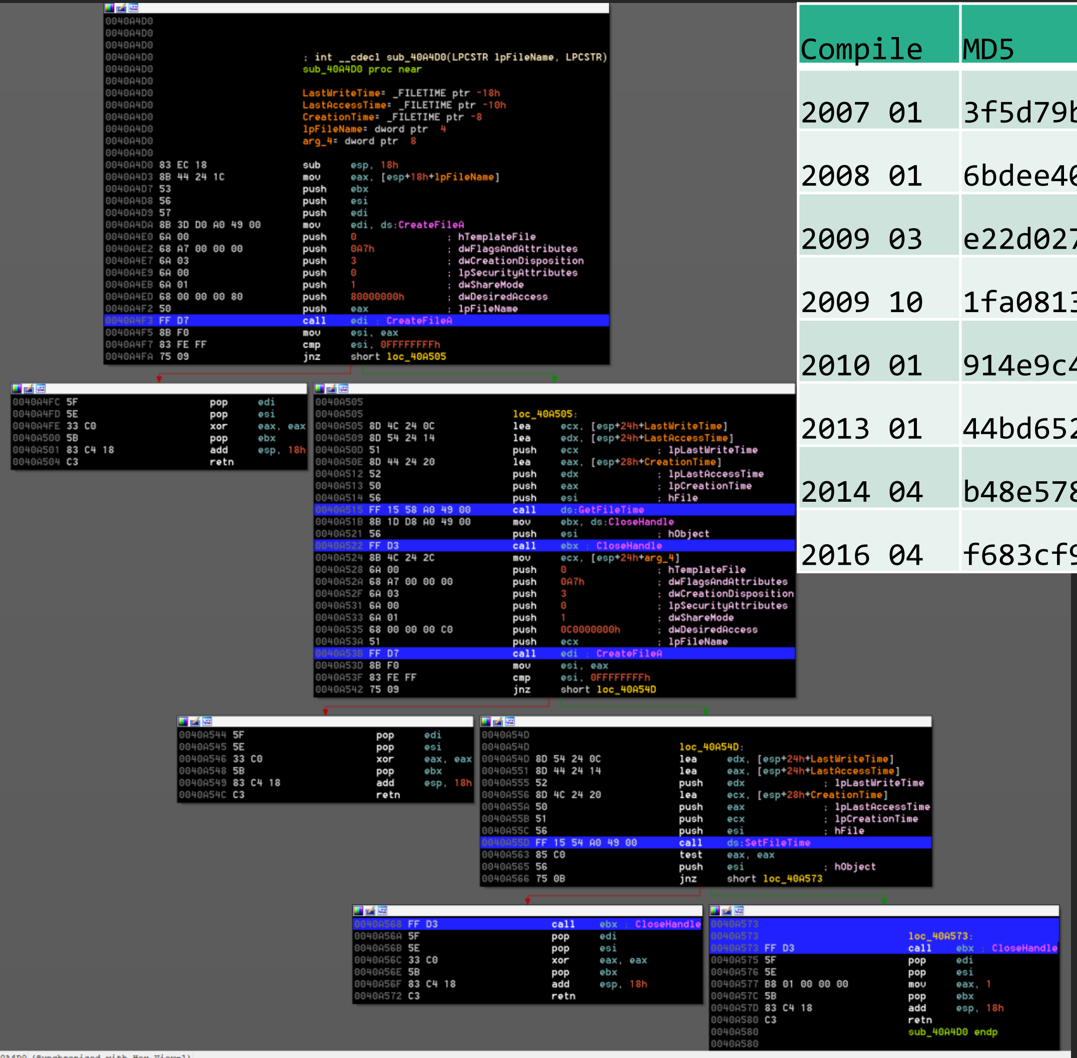


```
5A                        pop     edx
58                        pop     eax
5B                        pop     ebx
9D                        popf
59                        pop     ecx
5F                        pop     edi
8B 8E 20 02 00 00         mov     ecx, [esi+220h]
66 8B 96 1C 02 00 00      mov     dx, [esi+21Ch]
66 8B 86 24 02 00 00      mov     ax, [esi+224h]
C7 85 EC FE FF FF 08 00+  mov     dword ptr [ebp-114h], 8
89 8D F0 FE FF FF         mov     [ebp-110h], ecx
66 89 95 F4 FE FF FF      mov     [ebp-10Ch], dx
66 89 85 F6 FE FF FF      mov     [ebp-10Ah], ax
55                        push    ebp
9C                        pushf
52                        push    edx
C1 DD 10                  rcr     ebp, 10h
66 85 D2                  test    dx, dx
33 ED                     xor     ebp, ebp
85 ED                     test    ebp, ebp
76 18                     jbe     short loc_40CDA4
77 00                     ja      short $+2
```



```
rule purpi_anti_disasm
{
meta:
author = "Micah Yates"
description = "Anti-disassembly instructions used by Pirpi malware"
strings:
$re1 = { 5? 9c 5? } // push, pushf, push
$re2 = { 5? 5? 5? 9d ?? ?? } // 3x pop,  popf
$re3 = { 33 ?? 85 ?? 7? ?? 7? 00 } // xor, test, jge, jl
condition:
all of them
}
```

Just give me all the Pirpi you have: function_1



```
0040A4D0
0040A4D0
0040A4D0
0040A4D0                          ; int __cdecl sub_40A4D0(LPCSTR lpFileName, LPCSTR)
0040A4D0                          sub_40A4D0 proc near
0040A4D0
0040A4D0                          LastWriteTime= _FILETIME ptr -18h
0040A4D0                          LastAccessTime= _FILETIME ptr -10h
0040A4D0                          CreationTime= _FILETIME ptr -8
0040A4D0                          lpFileName= dword ptr  4
0040A4D0                          arg_4= dword ptr  8
0040A4D0
0040A4D0 83 EC 18                 sub     esp, 18h
0040A4D3 8B 44 24 1C              mov     eax, [esp+18h+lpFileName]
0040A4D7 53                       push    ebx
0040A4D8 56                       push    esi
0040A4D9 57                       push    edi
0040A4DA 8B 3D D0 A0 49 00        mov     edi, ds:CreateFileA
0040A4E0 6A 00                    push    0               ; hTemplateFile
0040A4E2 68 A7 00 00 00           push    0A7h            ; dwFlagsAndAttributes
0040A4E7 6A 03                    push    3               ; dwCreationDisposition
0040A4E9 6A 00                    push    0               ; lpSecurityAttributes
0040A4EB 6A 01                    push    1               ; dwShareMode
0040A4ED 68 00 00 00 80           push    80000000h       ; dwDesiredAccess
0040A4F2 50                       push    eax             ; lpFileName
0040A4F3 FF D7                    call    edi ; CreateFileA
0040A4F5 8B F0                    mov     esi, eax
0040A4F7 83 FE FF                 cmp     esi, 0FFFFFFFFh
0040A4FA 75 09                    jnz     short loc_40A505
```

```
0040A4FC 5F                       pop     edi
0040A4FD 5E                       pop     esi
0040A4FE 33 C0                    xor     eax, eax
0040A500 5B                       pop     ebx
0040A501 83 C4 18                 add     esp, 18h
0040A504 C3                       retn
```

```
0040A505
0040A505                          loc_40A505:
0040A505 8D 4C 24 0C              lea     ecx, [esp+24h+LastWriteTime]
0040A509 8D 54 24 14              lea     edx, [esp+24h+LastAccessTime]
0040A50D 51                       push    ecx             ; lpLastWriteTime
0040A50E 8D 44 24 20              lea     eax, [esp+28h+CreationTime]
0040A512 52                       push    edx             ; lpLastAccessTime
0040A513 50                       push    eax             ; lpCreationTime
0040A514 56                       push    esi             ; hFile
0040A515 FF 15 58 A0 49 00        call    ds:GetFileTime
0040A51B 8B 1D D8 A0 49 00        mov     ebx, ds:CloseHandle
0040A521 56                       push    esi             ; hObject
0040A522 FF D3                    call    ebx ; CloseHandle
0040A524 8B 4C 24 2C              mov     ecx, [esp+24h+arg_4]
0040A528 6A 00                    push    0               ; hTemplateFile
0040A52A 68 A7 00 00 00           push    0A7h            ; dwFlagsAndAttributes
0040A52F 6A 03                    push    3               ; dwCreationDisposition
0040A531 6A 00                    push    0               ; lpSecurityAttributes
0040A533 6A 01                    push    1               ; dwShareMode
0040A535 68 00 00 00 C0           push    0C0000000h      ; dwDesiredAccess
0040A53A 51                       push    ecx             ; lpFileName
0040A53B FF D7                    call    edi ; CreateFileA
0040A53D 8B F0                    mov     esi, eax
0040A53F 83 FE FF                 cmp     esi, 0FFFFFFFFh
0040A542 75 09                    jnz     short loc_40A54D
```

```
0040A544 5F                       pop     edi
0040A545 5E                       pop     esi
0040A546 33 C0                    xor     eax, eax
0040A548 5B                       pop     ebx
0040A549 83 C4 18                 add     esp, 18h
0040A54C C3                       retn
```

```
0040A54D
0040A54D                          loc_40A54D:
0040A54D 8D 54 24 0C              lea     edx, [esp+24h+LastWriteTime]
0040A551 8D 44 24 14              lea     eax, [esp+24h+LastAccessTime]
0040A555 52                       push    edx             ; lpLastWriteTime
0040A556 8D 4C 24 20              lea     ecx, [esp+28h+CreationTime]
0040A55A 50                       push    eax             ; lpLastAccessTime
0040A55B 51                       push    ecx             ; lpCreationTime
0040A55C 56                       push    esi             ; hFile
0040A55D FF 15 54 A0 49 00        call    ds:SetFileTime
0040A563 85 C0                    test    eax, eax
0040A565 56                       push    esi             ; hObject
0040A566 75 0B                    jnz     short loc_40A573
```

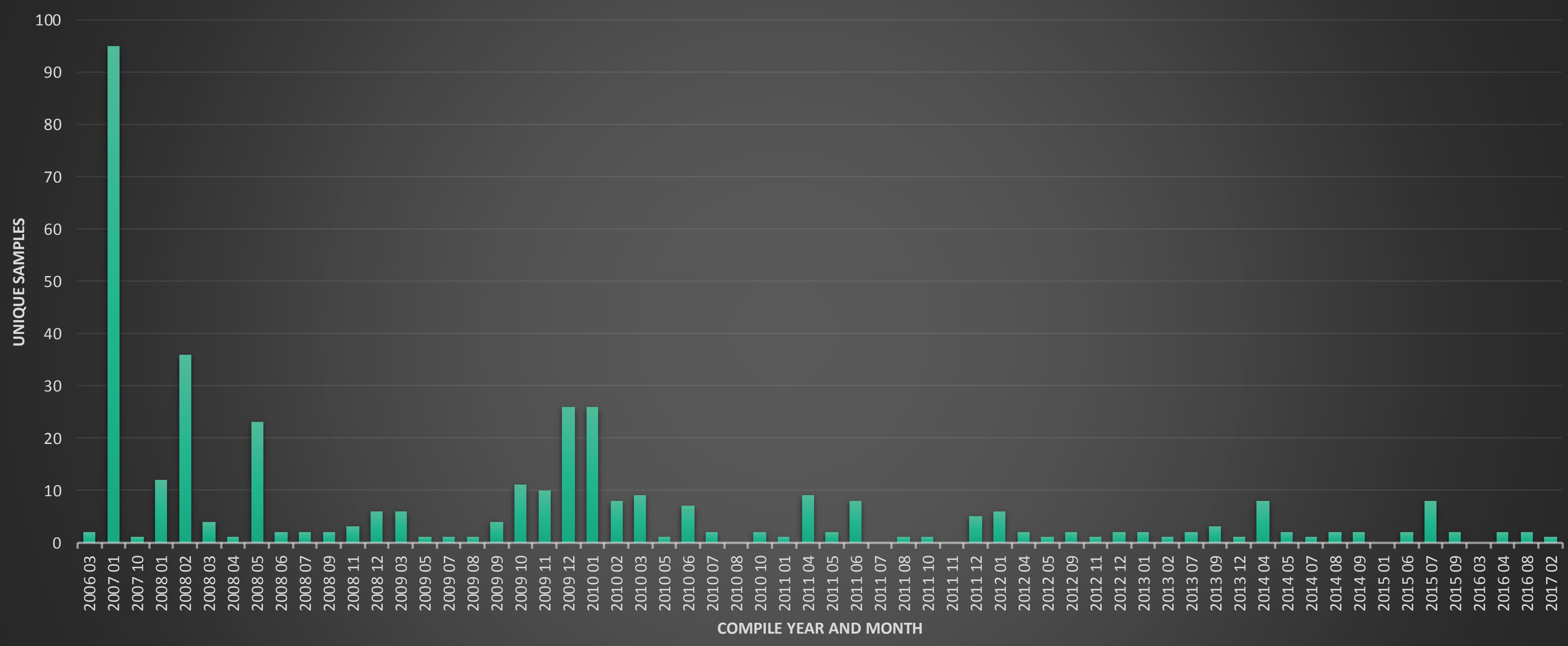
```
0040A568 FF D3                    call    ebx ; CloseHandle
0040A56A 5F                       pop     edi
0040A56B 5E                       pop     esi
0040A56C 33 C0                    xor     eax, eax
0040A56E 5B                       pop     ebx
0040A56F 83 C4 18                 add     esp, 18h
0040A572 C3                       retn
```

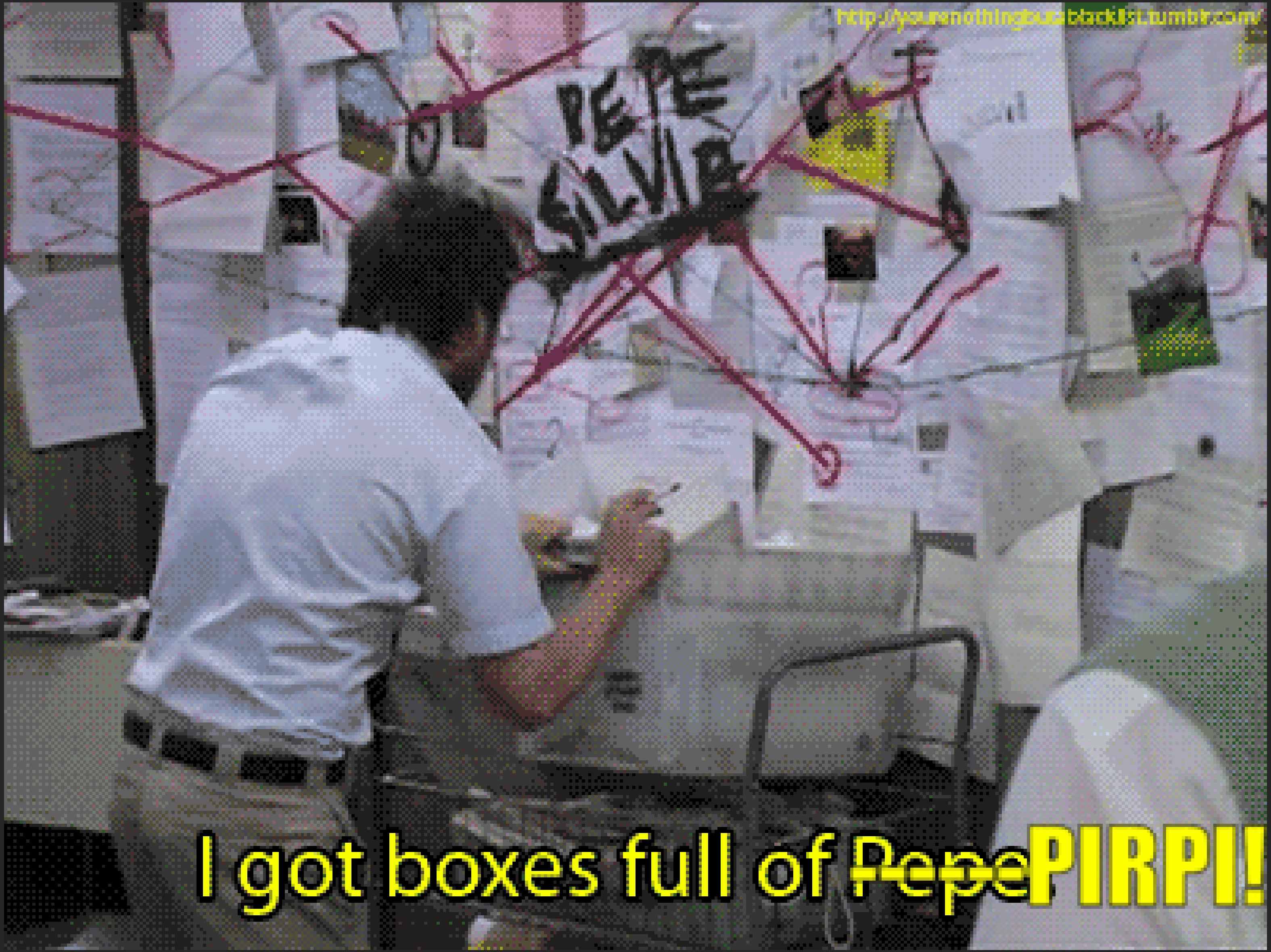
```
0040A573
0040A573                          loc_40A573:
0040A573 FF D3                    call    ebx ; CloseHandle
0040A575 5F                       pop     edi
0040A576 5E                       pop     esi
0040A577 B8 01 00 00 00           mov     eax, 1
0040A57C 5B                       pop     ebx
0040A57D 83 C4 18                 add     esp, 18h
0040A580 C3                       retn
0040A580                          sub_40A4D0 endp
0040A580
```

Compile	MD5	Beacon
2007 01	3f5d79b262472a12e3666118a7cdc2ca	www.msnmessengerupdate.com/index31382/f2ae95b93i97.bmp
2008 01	6bdee405ed857320aa8c822ee5e559f2	www.msnmessengerupdate.com/image19582/7e7e7eb7fi7f.gif
2009 03	e22d02796cfb908aaf48e2e058a0890a	www.office2008updates.com/dream/dream.php?
2009 10	1fa0813be4b9f23613204c94e74efc9d	ini.msnmessengerupdate.net/smart/smartmain.php?
2010 01	914e9c4c54fa210ad6d7ed4f47ec285f	ini.office2005updates.net/smart/smartmain.php?
2013 01	44bd652a09a991100d246d8280cac3ac	218.42.147.106/bussinesses/caetrwet/
2014 04	b48e578f030a7b5bb93a3e9d6d1e2a83	product.sorgerealty.com
2016 04	f683cf9c2a2fdc27abff4897746342c4	ste.mullanclan.com

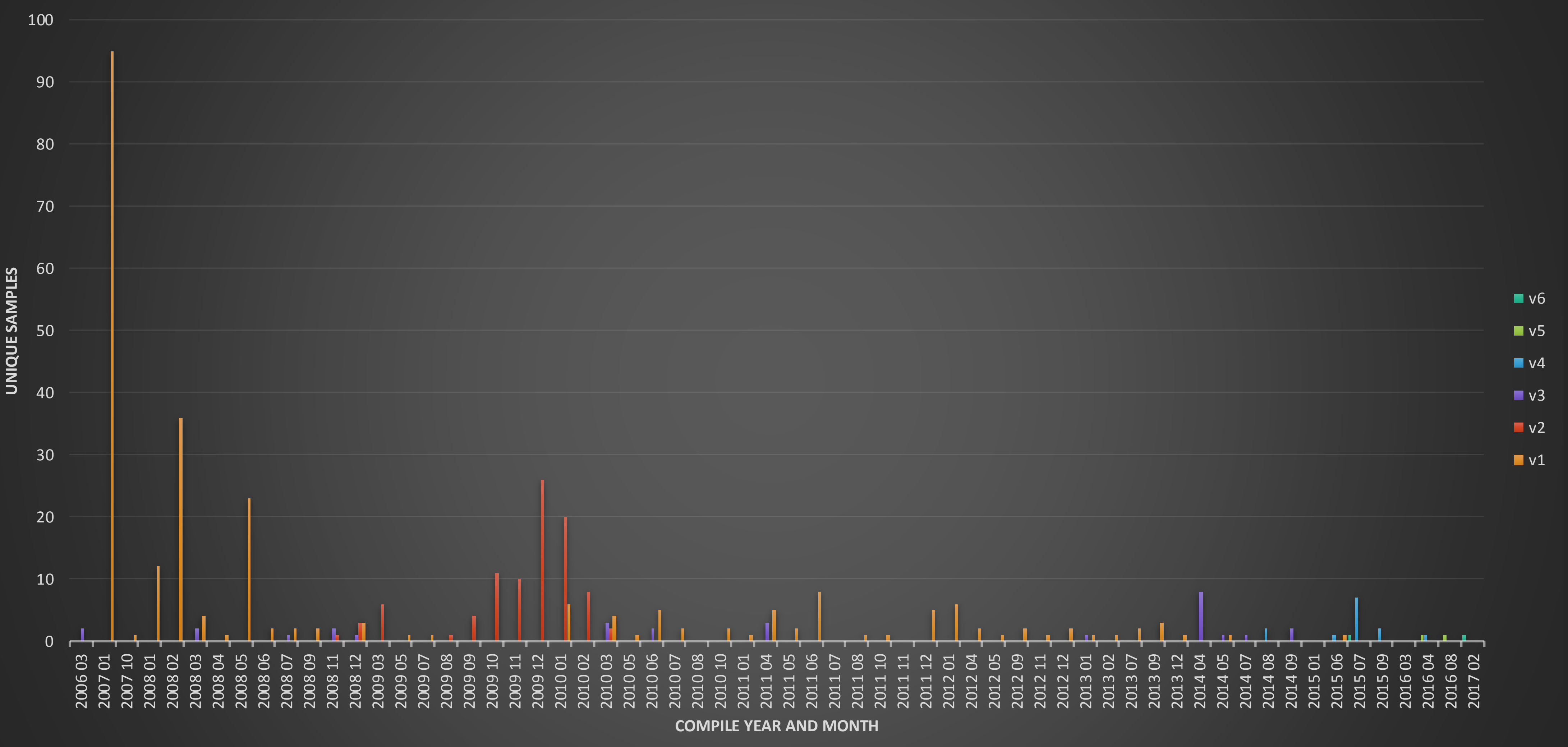
11monitor_MutexTest
MutexTest_IeInBrowser

Just give me all the Pirpi you have: function_1

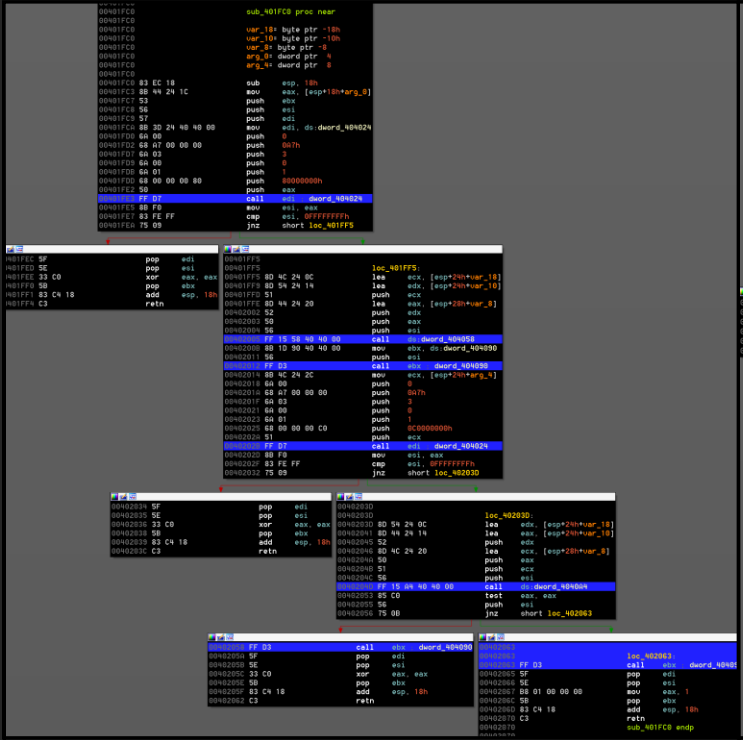


http://yourenothingbutablacklist.tumblr.com/
PEPE SILVIA
I got boxes full of ~~Pepe~~ PIRPI!

function_1 - minor versions



function_1 - minor versions



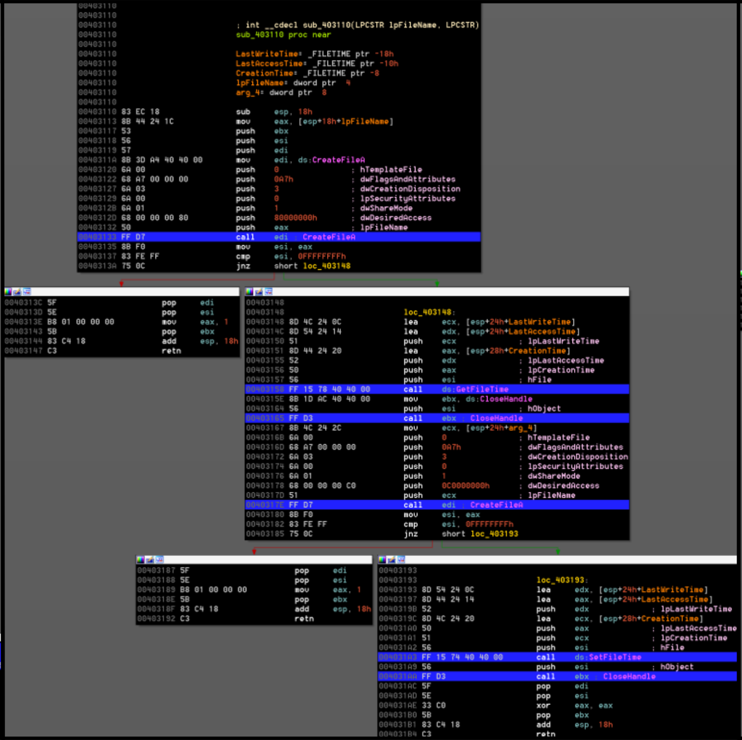
```
00401FC0                                  sub_401FC0 proc near
00401FC0
00401FC0                                  var_18= byte ptr -18h
00401FC0                                  var_10= byte ptr -10h
00401FC0                                  var_8= byte ptr -8
00401FC0                                  arg_0= dword ptr  4
00401FC0                                  arg_4= dword ptr  8
00401FC0
00401FC0 83 EC 18                         sub     esp, 18h
00401FC3 8B 44 24 1C                      mov     eax, [esp+18h+arg_0]
00401FC7 53                               push    ebx
00401FC8 56                               push    esi
00401FC9 57                               push    edi
00401FCA 8B 3D 24 40 40 00                mov     edi, ds:dword_404024
00401FD0 6A 00                            push    0
00401FD2 68 A7 00 00 00                   push    0A7h
00401FD7 6A 03                            push    3
00401FD9 6A 00                            push    0
00401FDB 6A 01                            push    1
00401FDD 68 00 00 00 80                   push    80000000h
00401FE2 50                               push    eax
00401FE3 FF D7                            call    edi ; dword_404024
00401FE5 8B F0                            mov     esi, eax
00401FE7 83 FE FF                         cmp     esi, 0FFFFFFFFh
00401FEA 75 09                            jnz     short loc_401FF5

401FEC 5F                    pop     edi
401FED 5E                    pop     esi
401FEE 33 C0                 xor     eax, eax
401FF0 5B                    pop     ebx
401FF1 83 C4 18              add     esp, 18h
401FF4 C3                    retn

00401FF5
00401FF5                                  loc_401FF5:
00401FF5 8D 4C 24 0C                      lea     ecx, [esp+24h+var_18]
00401FF9 8D 54 24 14                      lea     edx, [esp+24h+var_10]
00401FFD 51                               push    ecx
00401FFE 8D 44 24 20                      lea     eax, [esp+28h+var_8]
00402002 52                               push    edx
00402003 50                               push    eax
00402004 56                               push    esi
00402005 FF 15 58 40 40 00                call    ds:dword_404058
0040200B 8B 1D 90 40 40 00                mov     ebx, ds:dword_404090
00402011 56                               push    esi
00402012 FF D3                            call    ebx ; dword_404090
00402014 8B 4C 24 2C                      mov     ecx, [esp+24h+arg_4]
00402018 6A 00                            push    0
0040201A 68 A7 00 00 00                   push    0A7h
0040201F 6A 03                            push    3
00402021 6A 00                            push    0
00402023 6A 01                            push    1
00402025 68 00 00 00 C0                   push    0C0000000h
0040202A 51                               push    ecx
0040202B FF D7                            call    edi ; dword_404024
0040202D 8B F0                            mov     esi, eax
0040202F 83 FE FF                         cmp     esi, 0FFFFFFFFh
00402032 75 09                            jnz     short loc_40203D

00402034 5F                               pop     edi
00402035 5E                               pop     esi
00402036 33 C0                            xor     eax, eax
00402038 5B                               pop     ebx
00402039 83 C4 18                         add     esp, 18h
0040203C C3                               retn

0040203D
0040203D                                  loc_40203D:
0040203D 8D 54 24 0C                      lea     edx, [esp+24h+var_18]
00402041 8D 44 24 14                      lea     eax, [esp+24h+var_10]
00402045 52                               push    edx
00402046 8D 4C 24 20                      lea     ecx, [esp+28h+var_8]
0040204A 50                               push    eax
0040204B 51                               push    ecx
0040204C 56                               push    esi
0040204D FF 15 A4 40 40 00                call    ds:dword_4040A4
00402053 85 C0                            test    eax, eax
00402055 56                               push    esi
00402056 75 0B                            jnz     short loc_402063

00402058 FF D3                            call    ebx ; dword_404090
0040205A 5F                               pop     edi
0040205B 5E                               pop     esi
0040205C 33 C0                            xor     eax, eax
0040205E 5B                               pop     ebx
0040205F 83 C4 18                         add     esp, 18h
00402062 C3                               retn

00402063
00402063                                  loc_402063:
00402063 FF D3                            call    ebx ; dword_40409
00402065 5F                               pop     edi
00402066 5E                               pop     esi
00402067 B8 01 00 00 00                   mov     eax, 1
0040206C 5B                               pop     ebx
0040206D 83 C4 18                         add     esp, 18h
00402070 C3                               retn
00402070                                  sub_401FC0 endp
```

V1 - 2007

MD5:

98011f5b7b957a142f14cbda57a5ea82

@00401FC0



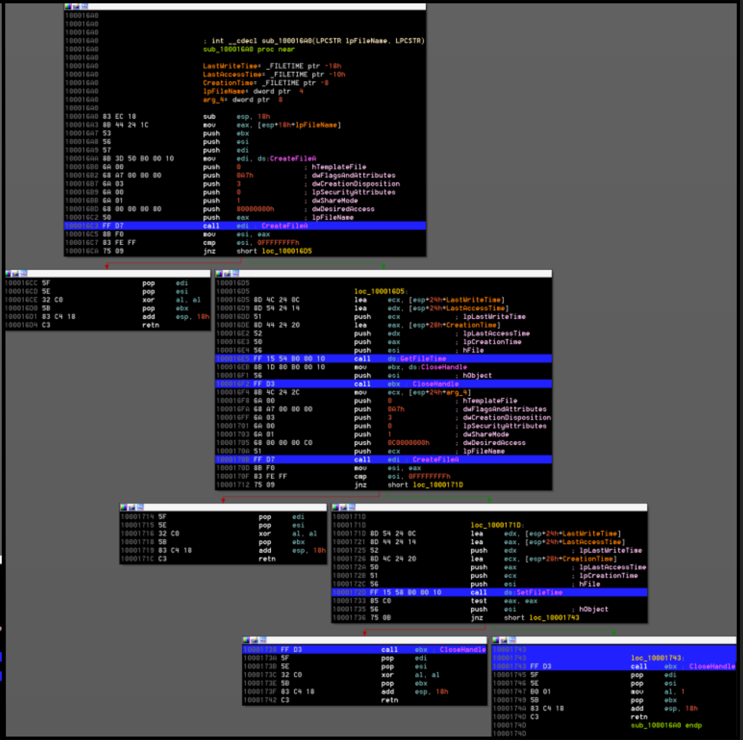
```
00403110
00403110
00403110                                  ; int __cdecl sub_403110(LPCSTR lpFileName, LPCSTR)
00403110                                  sub_403110 proc near
00403110
00403110                                  LastWriteTime= _FILETIME ptr -18h
00403110                                  LastAccessTime= _FILETIME ptr -10h
00403110                                  CreationTime= _FILETIME ptr -8
00403110                                  lpFileName= dword ptr  4
00403110                                  arg_4= dword ptr  8
00403110
00403110 83 EC 18                         sub     esp, 18h
00403113 8B 44 24 1C                      mov     eax, [esp+18h+lpFileName]
00403117 53                               push    ebx
00403118 56                               push    esi
00403119 57                               push    edi
0040311A 8B 3D A4 40 40 00                mov     edi, ds:CreateFileA
00403120 6A 00                            push    0               ; hTemplateFile
00403122 68 A7 00 00 00                   push    0A7h            ; dwFlagsAndAttributes
00403127 6A 03                            push    3               ; dwCreationDisposition
00403129 6A 00                            push    0               ; lpSecurityAttributes
0040312B 6A 01                            push    1               ; dwShareMode
0040312D 68 00 00 00 80                   push    80000000h       ; dwDesiredAccess
00403132 50                               push    eax             ; lpFileName
00403133 FF D7                            call    edi ; CreateFileA
00403135 8B F0                            mov     esi, eax
00403137 83 FE FF                         cmp     esi, 0FFFFFFFFh
0040313A 75 0C                            jnz     short loc_403148

0040313C 5F                               pop     edi
0040313D 5E                               pop     esi
0040313E B8 01 00 00 00                   mov     eax, 1
00403143 5B                               pop     ebx
00403144 83 C4 18                         add     esp, 18h
00403147 C3                               retn

00403148
00403148                                  loc_403148:
00403148 8D 4C 24 0C                      lea     ecx, [esp+24h+LastWriteTime]
0040314C 8D 54 24 14                      lea     edx, [esp+24h+LastAccessTime]
00403150 51                               push    ecx             ; lpLastWriteTime
00403151 8D 44 24 20                      lea     eax, [esp+28h+CreationTime]
00403155 52                               push    edx             ; lpLastAccessTime
00403156 50                               push    eax             ; lpCreationTime
00403157 56                               push    esi             ; hFile
00403158 FF 15 78 40 40 00                call    ds:GetFileTime
0040315E 8B 1D AC 40 40 00                mov     ebx, ds:CloseHandle
00403164 56                               push    esi             ; hObject
00403165 FF D3                            call    ebx ; CloseHandle
00403167 8B 4C 24 2C                      mov     ecx, [esp+24h+arg_4]
0040316B 6A 00                            push    0               ; hTemplateFile
0040316D 68 A7 00 00 00                   push    0A7h            ; dwFlagsAndAttributes
00403172 6A 03                            push    3               ; dwCreationDisposition
00403174 6A 00                            push    0               ; lpSecurityAttributes
00403176 6A 01                            push    1               ; dwShareMode
00403178 68 00 00 00 C0                   push    0C0000000h      ; dwDesiredAccess
0040317D 51                               push    ecx             ; lpFileName
0040317E FF D7                            call    edi ; CreateFileA
00403180 8B F0                            mov     esi, eax
00403182 83 FE FF                         cmp     esi, 0FFFFFFFFh
00403185 75 0C                            jnz     short loc_403193

00403187 5F                               pop     edi
00403188 5E                               pop     esi
00403189 B8 01 00 00 00                   mov     eax, 1
0040318E 5B                               pop     ebx
0040318F 83 C4 18                         add     esp, 18h
00403192 C3                               retn

00403193
00403193                                  loc_403193:
00403193 8D 54 24 0C                      lea     edx, [esp+24h+LastWriteTime]
00403197 8D 44 24 14                      lea     eax, [esp+24h+LastAccessTime]
0040319B 52                               push    edx             ; lpLastWriteTime
0040319C 8D 4C 24 20                      lea     ecx, [esp+28h+CreationTime]
004031A0 50                               push    eax             ; lpLastAccessTime
004031A1 51                               push    ecx             ; lpCreationTime
004031A2 56                               push    esi             ; hFile
004031A3 FF 15 74 40 40 00                call    ds:SetFileTime
004031A9 56                               push    esi             ; hObject
004031AA FF D3                            call    ebx ; CloseHandle
004031AC 5F                               pop     edi
004031AD 5E                               pop     esi
004031AE 33 C0                            xor     eax, eax
004031B0 5B                               pop     ebx
004031B1 83 C4 18                         add     esp, 18h
004031B4 C3                               retn
```

V2 - 2008

MD5:

272cb6c16e083ca143d40c63005753a2

@00403110



```
100016A0
100016A0
100016A0
100016A0                                  ; int __cdecl sub_100016A0(LPCSTR lpFileName, LPCSTR)
100016A0                                  sub_100016A0 proc near
100016A0
100016A0                                  LastWriteTime= _FILETIME ptr -18h
100016A0                                  LastAccessTime= _FILETIME ptr -10h
100016A0                                  CreationTime= _FILETIME ptr -8
100016A0                                  lpFileName= dword ptr  4
100016A0                                  arg_4= dword ptr  8
100016A0
100016A0 83 EC 18                         sub     esp, 18h
100016A3 8B 44 24 1C                      mov     eax, [esp+18h+lpFileName]
100016A7 53                               push    ebx
100016A8 56                               push    esi
100016A9 57                               push    edi
100016AA 8B 3D 50 B0 00 10                mov     edi, ds:CreateFileA
100016B0 6A 00                            push    0               ; hTemplateFile
100016B2 68 A7 00 00 00                   push    0A7h            ; dwFlagsAndAttributes
100016B7 6A 03                            push    3               ; dwCreationDisposition
100016B9 6A 00                            push    0               ; lpSecurityAttributes
100016BB 6A 01                            push    1               ; dwShareMode
100016BD 68 00 00 00 80                   push    80000000h       ; dwDesiredAccess
100016C2 50                               push    eax             ; lpFileName
100016C3 FF D7                            call    edi ; CreateFileA
100016C5 8B F0                            mov     esi, eax
100016C7 83 FE FF                         cmp     esi, 0FFFFFFFFh
100016CA 75 09                            jnz     short loc_100016D5

100016CC 5F                               pop     edi
100016CD 5E                               pop     esi
100016CE 32 C0                            xor     al, al
100016D0 5B                               pop     ebx
100016D1 83 C4 18                         add     esp, 18h
100016D4 C3                               retn

100016D5
100016D5                                  loc_100016D5:
100016D5 8D 4C 24 0C                      lea     ecx, [esp+24h+LastWriteTime]
100016D9 8D 54 24 14                      lea     edx, [esp+24h+LastAccessTime]
100016DD 51                               push    ecx             ; lpLastWriteTime
100016DE 8D 44 24 20                      lea     eax, [esp+28h+CreationTime]
100016E2 52                               push    edx             ; lpLastAccessTime
100016E3 50                               push    eax             ; lpCreationTime
100016E4 56                               push    esi             ; hFile
100016E5 FF 15 54 B0 00 10                call    ds:GetFileTime
100016EB 8B 1D 80 B0 00 10                mov     ebx, ds:CloseHandle
100016F1 56                               push    esi             ; hObject
100016F2 FF D3                            call    ebx ; CloseHandle
100016F4 8B 4C 24 2C                      mov     ecx, [esp+24h+arg_4]
100016F8 6A 00                            push    0               ; hTemplateFile
100016FA 68 A7 00 00 00                   push    0A7h            ; dwFlagsAndAttributes
100016FF 6A 03                            push    3               ; dwCreationDisposition
10001701 6A 00                            push    0               ; lpSecurityAttributes
10001703 6A 01                            push    1               ; dwShareMode
10001705 68 00 00 00 C0                   push    0C0000000h      ; dwDesiredAccess
1000170A 51                               push    ecx             ; lpFileName
1000170B FF D7                            call    edi ; CreateFileA
1000170D 8B F0                            mov     esi, eax
1000170F 83 FE FF                         cmp     esi, 0FFFFFFFFh
10001712 75 09                            jnz     short loc_1000171D

10001714 5F                               pop     edi
10001715 5E                               pop     esi
10001716 32 C0                            xor     al, al
10001718 5B                               pop     ebx
10001719 83 C4 18                         add     esp, 18h
1000171C C3                               retn

1000171D
1000171D                                  loc_1000171D:
1000171D 8D 54 24 0C                      lea     edx, [esp+24h+LastWriteTime]
10001721 8D 44 24 14                      lea     eax, [esp+24h+LastAccessTime]
10001725 52                               push    edx             ; lpLastWriteTime
10001726 8D 4C 24 20                      lea     ecx, [esp+28h+CreationTime]
1000172A 50                               push    eax             ; lpLastAccessTime
1000172B 51                               push    ecx             ; lpCreationTime
1000172C 56                               push    esi             ; hFile
1000172D FF 15 58 B0 00 10                call    ds:SetFileTime
10001733 85 C0                            test    eax, eax
10001735 56                               push    esi             ; hObject
10001736 75 0B                            jnz     short loc_10001743

10001738 FF D3                            call    ebx ; CloseHandle
1000173A 5F                               pop     edi
1000173B 5E                               pop     esi
1000173C 32 C0                            xor     al, al
1000173E 5B                               pop     ebx
1000173F 83 C4 18                         add     esp, 18h
10001742 C3                               retn

10001743
10001743                                  loc_10001743:
10001743 FF D3                            call    ebx ; CloseHandle
10001745 5F                               pop     edi
10001746 5E                               pop     esi
10001747 B0 01                            mov     al, 1
10001749 5B                               pop     ebx
1000174A 83 C4 18                         add     esp, 18h
1000174D C3                               retn
1000174D                                  sub_100016A0 endp
1000174D
```

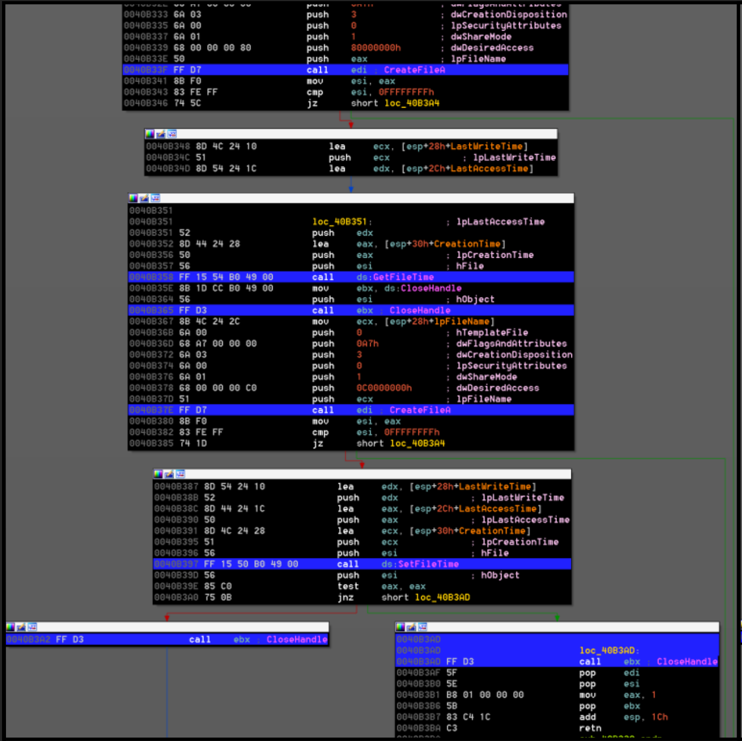
V3 – 2006

MD5:

acd8d34d8360129df1c8d03f253ba747

@100016A0

function_1 - minor versions



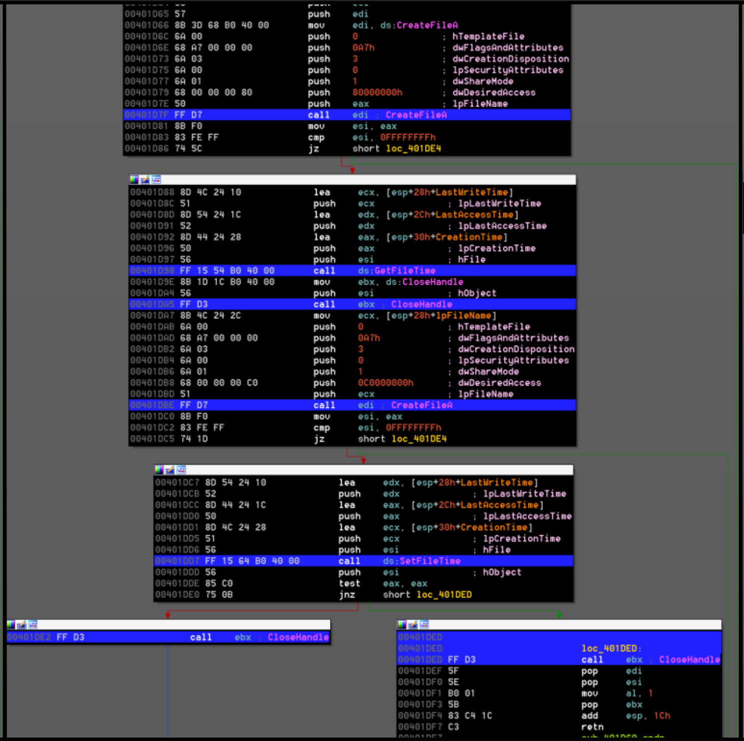
```
0040B333 6A 03             push    3               ; dwCreationDisposition
0040B335 6A 00             push    0               ; lpSecurityAttributes
0040B337 6A 01             push    1               ; dwShareMode
0040B339 68 00 00 00 80    push    80000000h       ; dwDesiredAccess
0040B33E 50                push    eax             ; lpFileName
0040B33F FF D7             call    edi ; CreateFileA
0040B341 8B F0             mov     esi, eax
0040B343 83 FE FF          cmp     esi, 0FFFFFFFFh
0040B346 74 5C             jz      short loc_40B3A4

0040B348 8D 4C 24 10       lea     ecx, [esp+28h+LastWriteTime]
0040B34C 51                push    ecx             ; lpLastWriteTime
0040B34D 8D 54 24 1C       lea     edx, [esp+2Ch+LastAccessTime]

0040B351
0040B351                   loc_40B351:             ; lpLastAccessTime
0040B351 52                push    edx
0040B352 8D 44 24 28       lea     eax, [esp+30h+CreationTime]
0040B356 50                push    eax             ; lpCreationTime
0040B357 56                push    esi             ; hFile
0040B358 FF 15 54 B0 49 00 call    ds:GetFileTime
0040B35E 8B 1D CC B0 49 00 mov     ebx, ds:CloseHandle
0040B364 56                push    esi             ; hObject
0040B365 FF D3             call    ebx ; CloseHandle
0040B367 8B 4C 24 2C       mov     ecx, [esp+28h+lpFileName]
0040B36B 6A 00             push    0               ; hTemplateFile
0040B36D 68 A7 00 00 00    push    0A7h            ; dwFlagsAndAttributes
0040B372 6A 03             push    3               ; dwCreationDisposition
0040B374 6A 00             push    0               ; lpSecurityAttributes
0040B376 6A 01             push    1               ; dwShareMode
0040B378 68 00 00 00 C0    push    0C0000000h      ; dwDesiredAccess
0040B37D 51                push    ecx             ; lpFileName
0040B37E FF D7             call    edi ; CreateFileA
0040B380 8B F0             mov     esi, eax
0040B382 83 FE FF          cmp     esi, 0FFFFFFFFh
0040B385 74 1D             jz      short loc_40B3A4

0040B387 8D 54 24 10       lea     edx, [esp+28h+LastWriteTime]
0040B38B 52                push    edx             ; lpLastWriteTime
0040B38C 8D 44 24 1C       lea     eax, [esp+2Ch+LastAccessTime]
0040B390 50                push    eax             ; lpLastAccessTime
0040B391 8D 4C 24 28       lea     ecx, [esp+30h+CreationTime]
0040B395 51                push    ecx             ; lpCreationTime
0040B396 56                push    esi             ; hFile
0040B397 FF 15 50 B0 49 00 call    ds:SetFileTime
0040B39D 56                push    esi             ; hObject
0040B39E 85 C0             test    eax, eax
0040B3A0 75 0B             jnz     short loc_40B3AD

0040B3A2 FF D3             call    ebx ; CloseHandle

0040B3AD
0040B3AD                   loc_40B3AD:
0040B3AD FF D3             call    ebx ; CloseHandle
0040B3AF 5F                pop     edi
0040B3B0 5E                pop     esi
0040B3B1 B8 01 00 00 00    mov     eax, 1
0040B3B6 5B                pop     ebx
0040B3B7 83 C4 1C          add     esp, 1Ch
0040B3BA C3                retn
```

V4 - 2014

MD5:

c006faaf9ad26a0bd3bbd597947da3e1

@0040B320



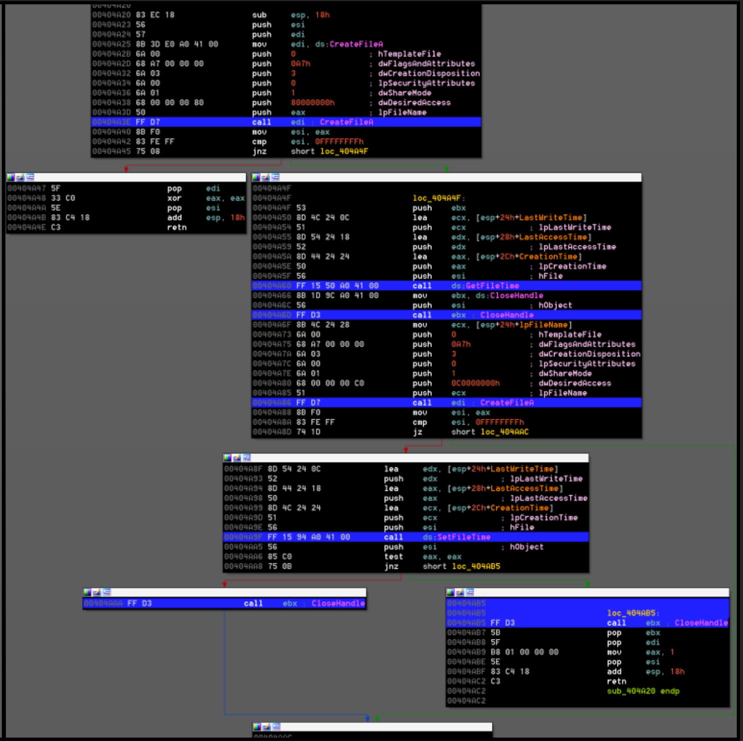
```
00401D65 57                push    edi
00401D66 8B 3D 68 B0 40 00 mov     edi, ds:CreateFileA
00401D6C 6A 00             push    0               ; hTemplateFile
00401D6E 68 A7 00 00 00    push    0A7h            ; dwFlagsAndAttributes
00401D73 6A 03             push    3               ; dwCreationDisposition
00401D75 6A 00             push    0               ; lpSecurityAttributes
00401D77 6A 01             push    1               ; dwShareMode
00401D79 68 00 00 00 80    push    80000000h       ; dwDesiredAccess
00401D7E 50                push    eax             ; lpFileName
00401D7F FF D7             call    edi ; CreateFileA
00401D81 8B F0             mov     esi, eax
00401D83 83 FE FF          cmp     esi, 0FFFFFFFFh
00401D86 74 5C             jz      short loc_401DE4

00401D88 8D 4C 24 10       lea     ecx, [esp+28h+LastWriteTime]
00401D8C 51                push    ecx             ; lpLastWriteTime
00401D8D 8D 54 24 1C       lea     edx, [esp+2Ch+LastAccessTime]
00401D91 52                push    edx             ; lpLastAccessTime
00401D92 8D 44 24 28       lea     eax, [esp+30h+CreationTime]
00401D96 50                push    eax             ; lpCreationTime
00401D97 56                push    esi             ; hFile
00401D98 FF 15 54 B0 40 00 call    ds:GetFileTime
00401D9E 8B 1D 1C B0 40 00 mov     ebx, ds:CloseHandle
00401DA4 56                push    esi             ; hObject
00401DA5 FF D3             call    ebx ; CloseHandle
00401DA7 8B 4C 24 2C       mov     ecx, [esp+28h+lpFileName]
00401DAB 6A 00             push    0               ; hTemplateFile
00401DAD 68 A7 00 00 00    push    0A7h            ; dwFlagsAndAttributes
00401DB2 6A 03             push    3               ; dwCreationDisposition
00401DB4 6A 00             push    0               ; lpSecurityAttributes
00401DB6 6A 01             push    1               ; dwShareMode
00401DB8 68 00 00 00 C0    push    0C0000000h      ; dwDesiredAccess
00401DBD 51                push    ecx             ; lpFileName
00401DBE FF D7             call    edi ; CreateFileA
00401DC0 8B F0             mov     esi, eax
00401DC2 83 FE FF          cmp     esi, 0FFFFFFFFh
00401DC5 74 1D             jz      short loc_401DE4

00401DC7 8D 54 24 10       lea     edx, [esp+28h+LastWriteTime]
00401DCB 52                push    edx             ; lpLastWriteTime
00401DCC 8D 44 24 1C       lea     eax, [esp+2Ch+LastAccessTime]
00401DD0 50                push    eax             ; lpLastAccessTime
00401DD1 8D 4C 24 28       lea     ecx, [esp+30h+CreationTime]
00401DD5 51                push    ecx             ; lpCreationTime
00401DD6 56                push    esi             ; hFile
00401DD7 FF 15 64 B0 40 00 call    ds:SetFileTime
00401DDD 56                push    esi             ; hObject
00401DDE 85 C0             test    eax, eax
00401DE0 75 0B             jnz     short loc_401DED

00401DE2 FF D3             call    ebx ; CloseHandle

00401DED
00401DED                   loc_401DED:
00401DED FF D3             call    ebx ; CloseHandle
00401DEF 5F                pop     edi
00401DF0 5E                pop     esi
00401DF1 B0 01             mov     al, 1
00401DF3 5B                pop     ebx
00401DF4 83 C4 1C          add     esp, 1Ch
00401DF7 C3                retn
```

V5 - 2016

MD5:

f683cf9c2a2fdc27abff4897746342c4

@00401D60



```
00404A20 83 EC 18          sub     esp, 18h
00404A23 56                push    esi
00404A24 57                push    edi
00404A25 8B 3D E0 A0 41 00 mov     edi, ds:CreateFileA
00404A2B 6A 00             push    0               ; hTemplateFile
00404A2D 68 A7 00 00 00    push    0A7h            ; dwFlagsAndAttributes
00404A32 6A 03             push    3               ; dwCreationDisposition
00404A34 6A 00             push    0               ; lpSecurityAttributes
00404A36 6A 01             push    1               ; dwShareMode
00404A38 68 00 00 00 80    push    80000000h       ; dwDesiredAccess
00404A3D 50                push    eax             ; lpFileName
00404A3E FF D7             call    edi ; CreateFileA
00404A40 8B F0             mov     esi, eax
00404A42 83 FE FF          cmp     esi, 0FFFFFFFFh
00404A45 75 08             jnz     short loc_404A4F

00404A47 5F                pop     edi
00404A48 33 C0             xor     eax, eax
00404A4A 5E                pop     esi
00404A4B 83 C4 18          add     esp, 18h
00404A4E C3                retn

00404A4F
00404A4F                   loc_404A4F:
00404A4F 53                push    ebx
00404A50 8D 4C 24 0C       lea     ecx, [esp+24h+LastWriteTime]
00404A54 51                push    ecx             ; lpLastWriteTime
00404A55 8D 54 24 18       lea     edx, [esp+28h+LastAccessTime]
00404A59 52                push    edx             ; lpLastAccessTime
00404A5A 8D 44 24 24       lea     eax, [esp+2Ch+CreationTime]
00404A5E 50                push    eax             ; lpCreationTime
00404A5F 56                push    esi             ; hFile
00404A60 FF 15 50 A0 41 00 call    ds:GetFileTime
00404A66 8B 1D 9C A0 41 00 mov     ebx, ds:CloseHandle
00404A6C 56                push    esi             ; hObject
00404A6D FF D3             call    ebx ; CloseHandle
00404A6F 8B 4C 24 28       mov     ecx, [esp+24h+lpFileName]
00404A73 6A 00             push    0               ; hTemplateFile
00404A75 68 A7 00 00 00    push    0A7h            ; dwFlagsAndAttributes
00404A7A 6A 03             push    3               ; dwCreationDisposition
00404A7C 6A 00             push    0               ; lpSecurityAttributes
00404A7E 6A 01             push    1               ; dwShareMode
00404A80 68 00 00 00 C0    push    0C0000000h      ; dwDesiredAccess
00404A85 51                push    ecx             ; lpFileName
00404A86 FF D7             call    edi ; CreateFileA
00404A88 8B F0             mov     esi, eax
00404A8A 83 FE FF          cmp     esi, 0FFFFFFFFh
00404A8D 74 1D             jz      short loc_404AAC

00404A8F 8D 54 24 0C       lea     edx, [esp+24h+LastWriteTime]
00404A93 52                push    edx             ; lpLastWriteTime
00404A94 8D 44 24 18       lea     eax, [esp+28h+LastAccessTime]
00404A98 50                push    eax             ; lpLastAccessTime
00404A99 8D 4C 24 24       lea     ecx, [esp+2Ch+CreationTime]
00404A9D 51                push    ecx             ; lpCreationTime
00404A9E 56                push    esi             ; hFile
00404A9F FF 15 94 A0 41 00 call    ds:SetFileTime
00404AA5 56                push    esi             ; hObject
00404AA6 85 C0             test    eax, eax
00404AA8 75 0B             jnz     short loc_404AB5

00404AAA FF D3             call    ebx ; CloseHandle

00404AB5
00404AB5                   loc_404AB5:
00404AB5 FF D3             call    ebx ; CloseHandle
00404AB7 5B                pop     ebx
00404AB8 5F                pop     edi
00404AB9 B8 01 00 00 00    mov     eax, 1
00404ABE 5E                pop     esi
00404ABF 83 C4 18          add     esp, 18h
00404AC2 C3                retn
00404AC2                   sub_404A20 endp
00404AC2
```

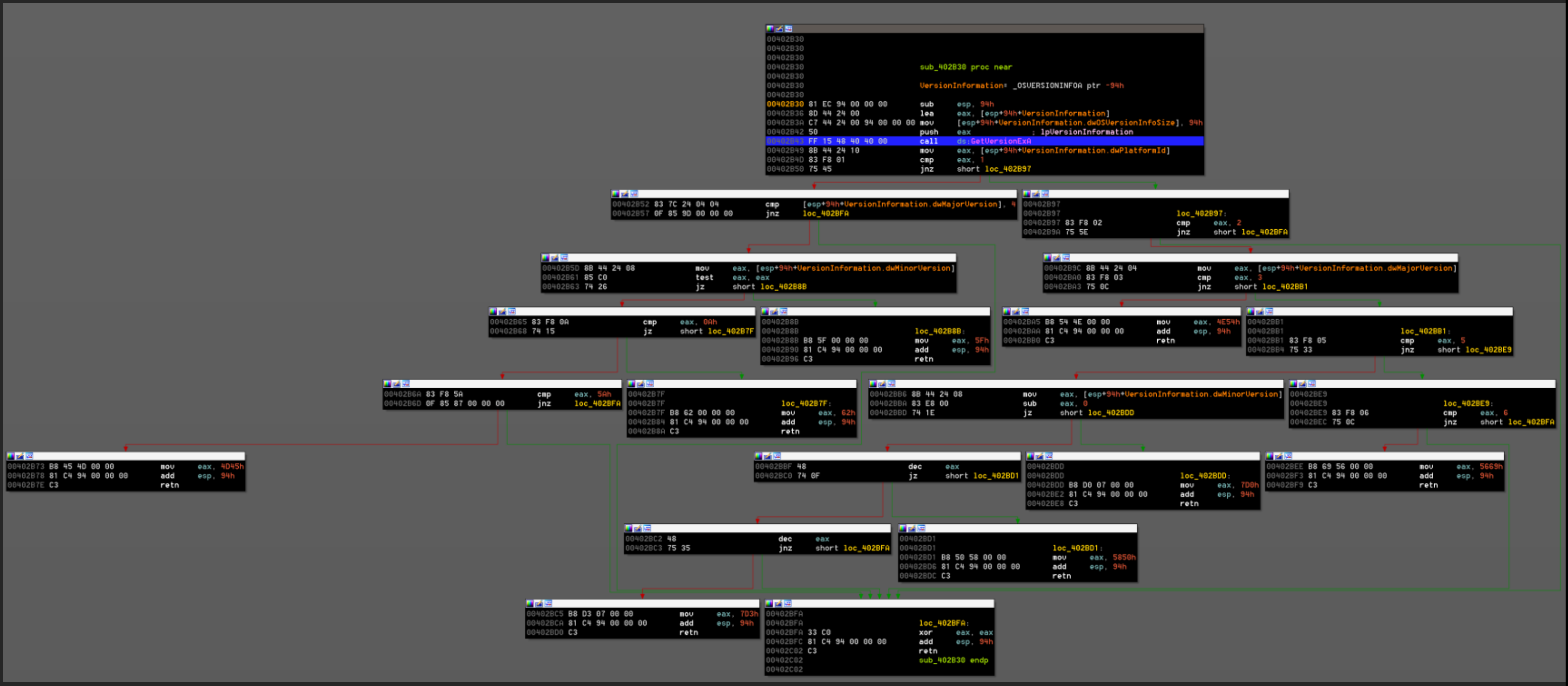
V6 - 2017

MD5:

07b4d539a6333d7896493bafd2738321

@00404A20

function_2



```
00402B30
00402B30
00402B30
00402B30                               sub_402B30 proc near
00402B30
00402B30                               VersionInformation= _OSVERSIONINFOA ptr -94h
00402B30
00402B30 81 EC 94 00 00 00             sub     esp, 94h
00402B36 8D 44 24 00                   lea     eax, [esp+94h+VersionInformation]
00402B3A C7 44 24 00 94 00 00 00       mov     [esp+94h+VersionInformation.dwOSVersionInfoSize], 94h
00402B42 50                            push    eax             ; lpVersionInformation
00402B43 FF 15 48 40 40 00             call    ds:GetVersionExA
00402B49 8B 44 24 10                   mov     eax, [esp+94h+VersionInformation.dwPlatformId]
00402B4D 83 F8 01                      cmp     eax, 1
00402B50 75 45                         jnz     short loc_402B97
```

```
00402B52 83 7C 24 04 04                cmp     [esp+94h+VersionInformation.dwMajorVersion], 4
00402B57 0F 85 9D 00 00 00             jnz     loc_402BFA
```

```
00402B97
00402B97                               loc_402B97:
00402B97 83 F8 02                      cmp     eax, 2
00402B9A 75 5E                         jnz     short loc_402BFA
```

```
00402B5D 8B 44 24 08                   mov     eax, [esp+94h+VersionInformation.dwMinorVersion]
00402B61 85 C0                         test    eax, eax
00402B63 74 26                         jz      short loc_402B8B
```

```
00402B9C 8B 44 24 04                   mov     eax, [esp+94h+VersionInformation.dwMajorVersion]
00402BA0 83 F8 03                      cmp     eax, 3
00402BA3 75 0C                         jnz     short loc_402BB1
```

```
00402B65 83 F8 0A                      cmp     eax, 0Ah
00402B68 74 15                         jz      short loc_402B7F
```

```
00402B8B
00402B8B                               loc_402B8B:
00402B8B B8 5F 00 00 00                mov     eax, 5Fh
00402B90 81 C4 94 00 00 00             add     esp, 94h
00402B96 C3                            retn
```

```
00402BA5 B8 54 4E 00 00                mov     eax, 4E54h
00402BAA 81 C4 94 00 00 00             add     esp, 94h
00402BB0 C3                            retn
```

```
00402BB1
00402BB1                               loc_402BB1:
00402BB1 83 F8 05                      cmp     eax, 5
00402BB4 75 33                         jnz     short loc_402BE9
```

```
00402B6A 83 F8 5A                      cmp     eax, 5Ah
00402B6D 0F 85 87 00 00 00             jnz     loc_402BFA
```

```
00402B7F
00402B7F                               loc_402B7F:
00402B7F B8 62 00 00 00                mov     eax, 62h
00402B84 81 C4 94 00 00 00             add     esp, 94h
00402B8A C3                            retn
```

```
00402BB6 8B 44 24 08                   mov     eax, [esp+94h+VersionInformation.dwMinorVersion]
00402BBA 83 E8 00                      sub     eax, 0
00402BBD 74 1E                         jz      short loc_402BDD
```

```
00402BE9
00402BE9                               loc_402BE9:
00402BE9 83 F8 06                      cmp     eax, 6
00402BEC 75 0C                         jnz     short loc_402BFA
```

```
00402B73 B8 45 4D 00 00                mov     eax, 4D45h
00402B78 81 C4 94 00 00 00             add     esp, 94h
00402B7E C3                            retn
```

```
00402BBF 48                            dec     eax
00402BC0 74 0F                         jz      short loc_402BD1
```

```
00402BDD
00402BDD                               loc_402BDD:
00402BDD B8 D0 07 00 00                mov     eax, 7D0h
00402BE2 81 C4 94 00 00 00             add     esp, 94h
00402BE8 C3                            retn
```

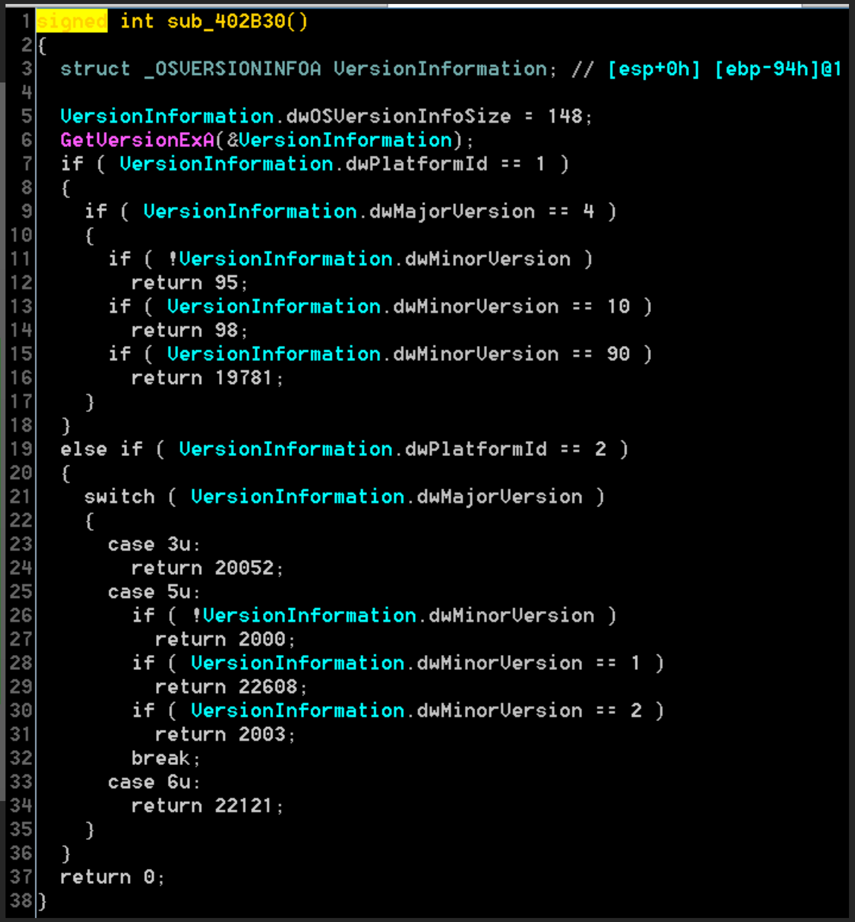
```
00402BEE B8 69 56 00 00                mov     eax, 5669h
00402BF3 81 C4 94 00 00 00             add     esp, 94h
00402BF9 C3                            retn
```

```
00402BC2 48                            dec     eax
00402BC3 75 35                         jnz     short loc_402BFA
```

```
00402BD1
00402BD1                               loc_402BD1:
00402BD1 B8 50 58 00 00                mov     eax, 5850h
00402BD6 81 C4 94 00 00 00             add     esp, 94h
00402BDC C3                            retn
```

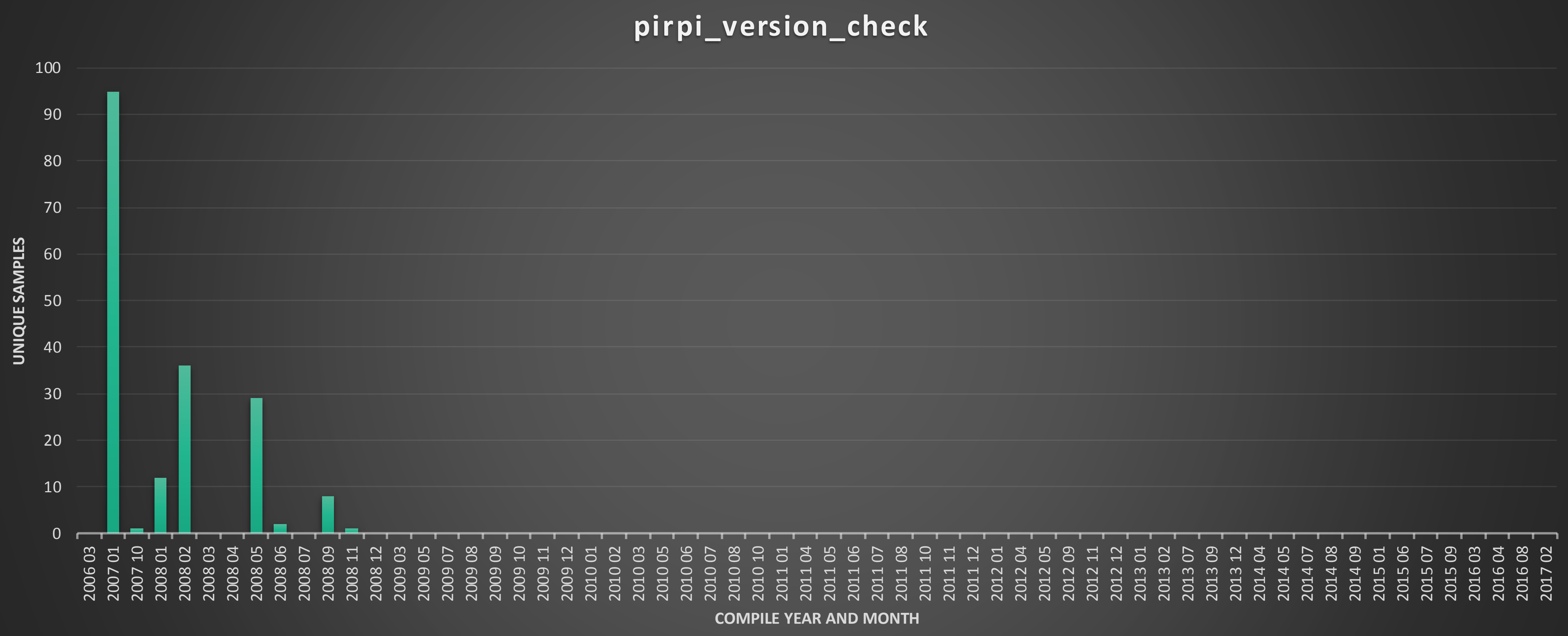
```
00402BC5 B8 D3 07 00 00                mov     eax, 7D3h
00402BCA 81 C4 94 00 00 00             add     esp, 94h
00402BD0 C3                            retn
```

```
00402BFA
00402BFA                               loc_402BFA:
00402BFA 33 C0                         xor     eax, eax
00402BFC 81 C4 94 00 00 00             add     esp, 94h
00402C02 C3                            retn
00402C02                               sub_402B30 endp
00402C02
```

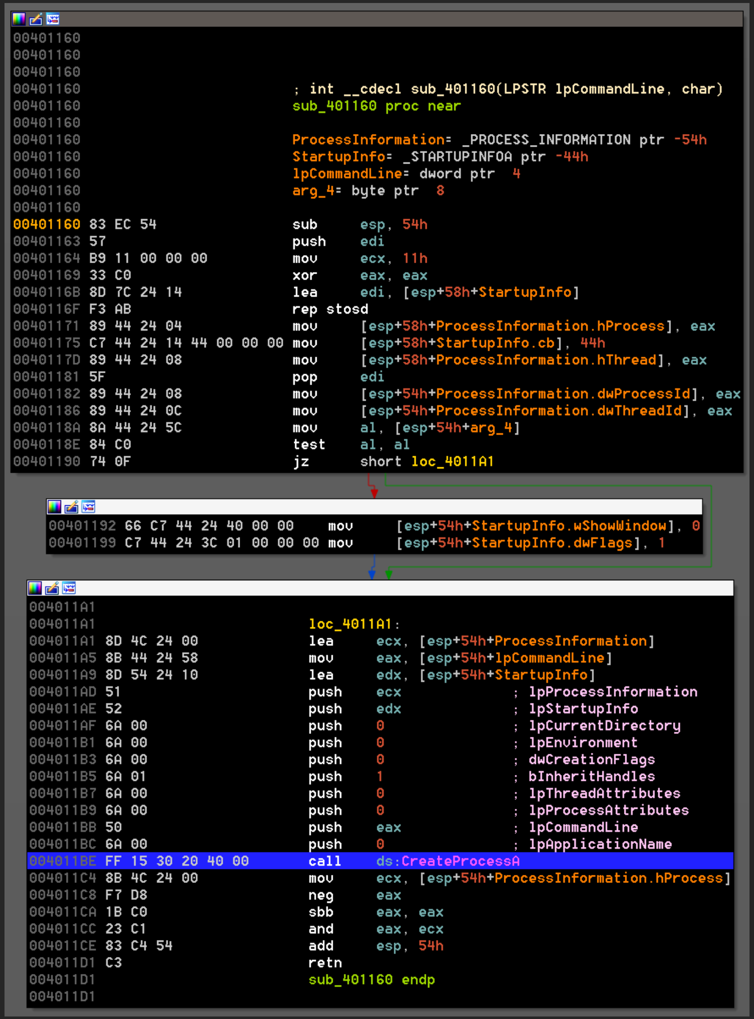


```
signed int sub_402B30()
{
  struct _OSVERSIONINFOA VersionInformation; // [esp+0h] [ebp-94h]@1

  VersionInformation.dwOSVersionInfoSize = 148;
  GetVersionExA(&VersionInformation);
  if ( VersionInformation.dwPlatformId == 1 )
  {
    if ( VersionInformation.dwMajorVersion == 4 )
    {
      if ( !VersionInformation.dwMinorVersion )
        return 95;
      if ( VersionInformation.dwMinorVersion == 10 )
        return 98;
      if ( VersionInformation.dwMinorVersion == 90 )
        return 19781;
    }
  }
  else if ( VersionInformation.dwPlatformId == 2 )
  {
    switch ( VersionInformation.dwMajorVersion )
    {
      case 3u:
        return 20052;
      case 5u:
        if ( !VersionInformation.dwMinorVersion )
          return 2000;
        if ( VersionInformation.dwMinorVersion == 1 )
          return 22608;
        if ( VersionInformation.dwMinorVersion == 2 )
          return 2003;
        break;
      case 6u:
        return 22121;
    }
  }
  return 0;
}
```

function_2


pirpi_version_check
UNIQUE SAMPLES
100
90
80
70
60
50
40
30
20
10
0
2006 03
2007 01
2007 10
2008 01
2008 02
2008 03
2008 04
2008 05
2008 06
2008 07
2008 09
2008 11
2008 12
2009 03
2009 05
2009 07
2009 08
2009 09
2009 10
2009 11
2009 12
2010 01
2010 02
2010 03
2010 05
2010 06
2010 07
2010 08
2010 10
2011 01
2011 04
2011 05
2011 06
2011 07
2011 08
2011 10
2011 11
2011 12
2012 01
2012 04
2012 05
2012 09
2012 11
2012 12
2013 01
2013 02
2013 07
2013 09
2013 12
2014 04
2014 05
2014 07
2014 08
2014 09
2015 01
2015 06
2015 07
2015 09
2016 03
2016 04
2016 08
2017 02
COMPILE YEAR AND MONTH

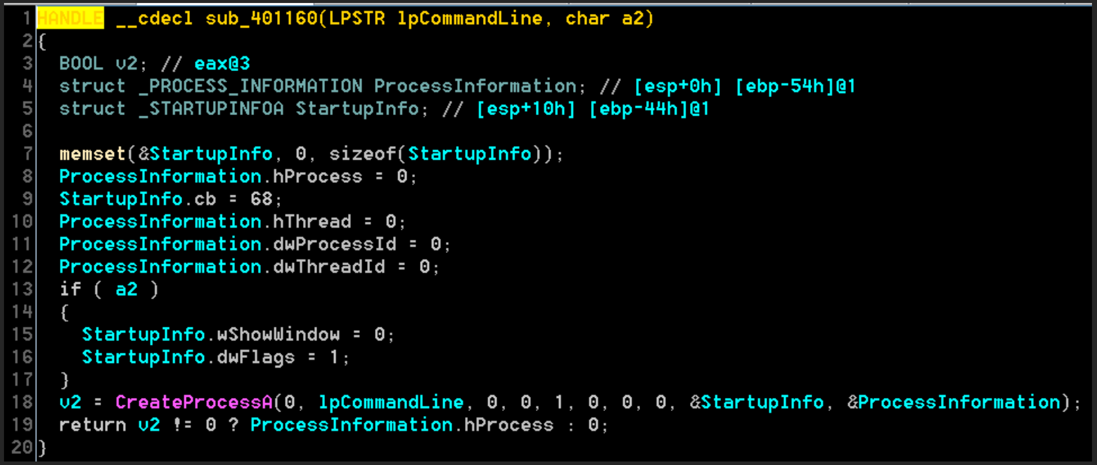
function_3



```
00401160
00401160
00401160
00401160                                 ; int __cdecl sub_401160(LPSTR lpCommandLine, char)
00401160                                 sub_401160 proc near
00401160
00401160                                 ProcessInformation= _PROCESS_INFORMATION ptr -54h
00401160                                 StartupInfo= _STARTUPINFOA ptr -44h
00401160                                 lpCommandLine= dword ptr  4
00401160                                 arg_4= byte ptr  8
00401160
00401160 83 EC 54                        sub     esp, 54h
00401163 57                              push    edi
00401164 B9 11 00 00 00                  mov     ecx, 11h
00401169 33 C0                           xor     eax, eax
0040116B 8D 7C 24 14                     lea     edi, [esp+58h+StartupInfo]
0040116F F3 AB                           rep stosd
00401171 89 44 24 04                     mov     [esp+58h+ProcessInformation.hProcess], eax
00401175 C7 44 24 14 44 00 00 00         mov     [esp+58h+StartupInfo.cb], 44h
0040117D 89 44 24 08                     mov     [esp+58h+ProcessInformation.hThread], eax
00401181 5F                              pop     edi
00401182 89 44 24 08                     mov     [esp+54h+ProcessInformation.dwProcessId], eax
00401186 89 44 24 0C                     mov     [esp+54h+ProcessInformation.dwThreadId], eax
0040118A 8A 44 24 5C                     mov     al, [esp+54h+arg_4]
0040118E 84 C0                           test    al, al
00401190 74 0F                           jz      short loc_4011A1
```

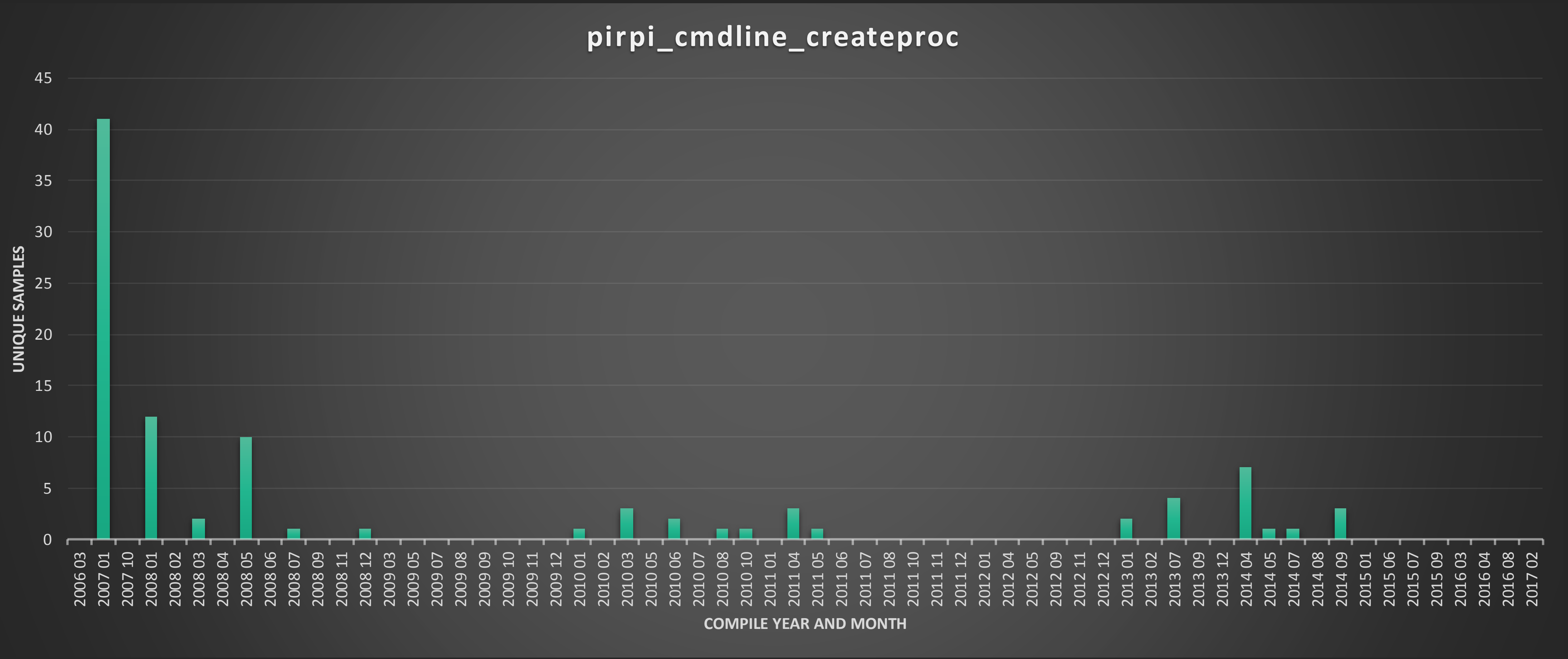
```
00401192 66 C7 44 24 40 00 00    mov     [esp+54h+StartupInfo.wShowWindow], 0
00401199 C7 44 24 3C 01 00 00 00 mov     [esp+54h+StartupInfo.dwFlags], 1
```

```
004011A1
004011A1                                 loc_4011A1:
004011A1 8D 4C 24 00                     lea     ecx, [esp+54h+ProcessInformation]
004011A5 8B 44 24 58                     mov     eax, [esp+54h+lpCommandLine]
004011A9 8D 54 24 10                     lea     edx, [esp+54h+StartupInfo]
004011AD 51                              push    ecx             ; lpProcessInformation
004011AE 52                              push    edx             ; lpStartupInfo
004011AF 6A 00                           push    0               ; lpCurrentDirectory
004011B1 6A 00                           push    0               ; lpEnvironment
004011B3 6A 00                           push    0               ; dwCreationFlags
004011B5 6A 01                           push    1               ; bInheritHandles
004011B7 6A 00                           push    0               ; lpThreadAttributes
004011B9 6A 00                           push    0               ; lpProcessAttributes
004011BB 50                              push    eax             ; lpCommandLine
004011BC 6A 00                           push    0               ; lpApplicationName
004011BE FF 15 30 20 40 00               call    ds:CreateProcessA
004011C4 8B 4C 24 00                     mov     ecx, [esp+54h+ProcessInformation.hProcess]
004011C8 F7 D8                           neg     eax
004011CA 1B C0                           sbb     eax, eax
004011CC 23 C1                           and     eax, ecx
004011CE 83 C4 54                        add     esp, 54h
004011D1 C3                              retn
004011D1                                 sub_401160 endp
004011D1
```

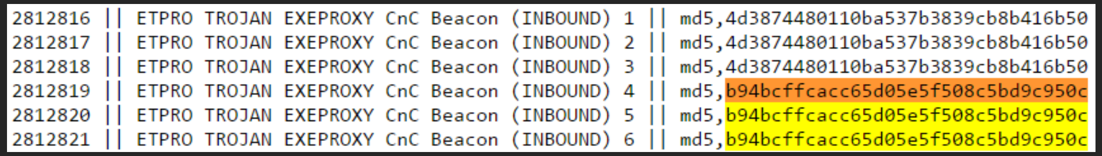


```c
HANDLE __cdecl sub_401160(LPSTR lpCommandLine, char a2)
{
  BOOL v2; // eax@3
  struct _PROCESS_INFORMATION ProcessInformation; // [esp+0h] [ebp-54h]@1
  struct _STARTUPINFOA StartupInfo; // [esp+10h] [ebp-44h]@1

  memset(&StartupInfo, 0, sizeof(StartupInfo));
  ProcessInformation.hProcess = 0;
  StartupInfo.cb = 68;
  ProcessInformation.hThread = 0;
  ProcessInformation.dwProcessId = 0;
  ProcessInformation.dwThreadId = 0;
  if ( a2 )
  {
    StartupInfo.wShowWindow = 0;
    StartupInfo.dwFlags = 1;
  }
  v2 = CreateProcessA(0, lpCommandLine, 0, 0, 1, 0, 0, 0, &StartupInfo, &ProcessInformation);
  return v2 != 0 ? ProcessInformation.hProcess : 0;
}
```

function_3

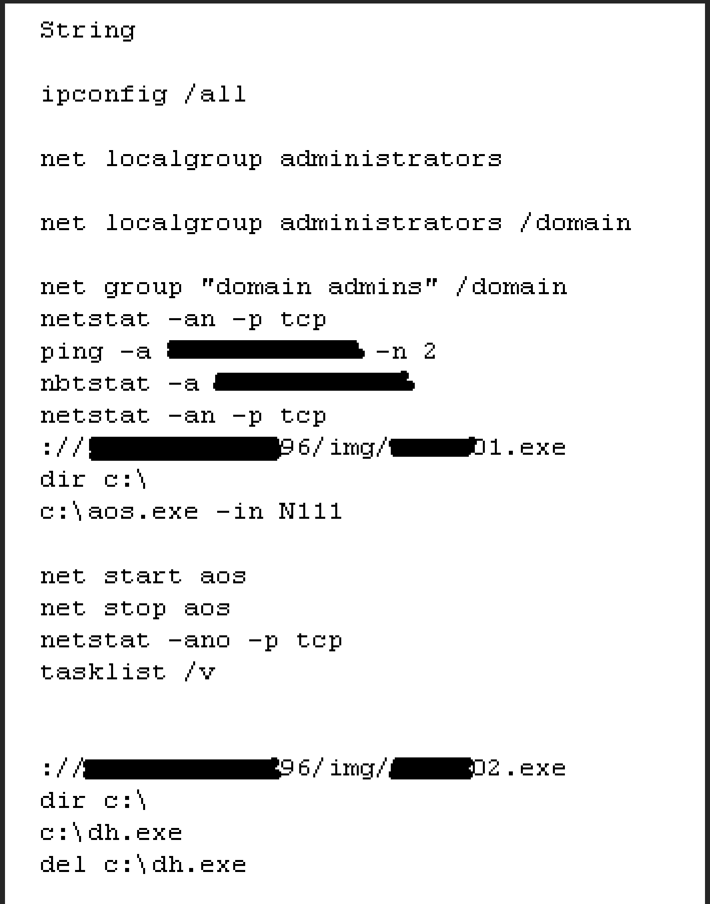

pirpi_cmdline_createproc
UNIQUE SAMPLES
45
40
35
30
25
20
15
10
5
0
2006 03
2007 01
2007 10
2008 01
2008 02
2008 03
2008 04
2008 05
2008 06
2008 07
2008 09
2008 11
2008 12
2009 03
2009 05
2009 07
2009 08
2009 09
2009 10
2009 11
2009 12
2010 01
2010 02
2010 03
2010 05
2010 06
2010 07
2010 08
2010 10
2011 01
2011 04
2011 05
2011 06
2011 07
2011 08
2011 10
2011 11
2011 12
2012 01
2012 04
2012 05
2012 09
2012 11
2012 12
2013 01
2013 02
2013 07
2013 09
2013 12
2014 04
2014 05
2014 07
2014 08
2014 09
2015 01
2015 06
2015 07
2015 09
2016 03
2016 04
2016 08
2017 02
COMPILE YEAR AND MONTH

EXEProxy



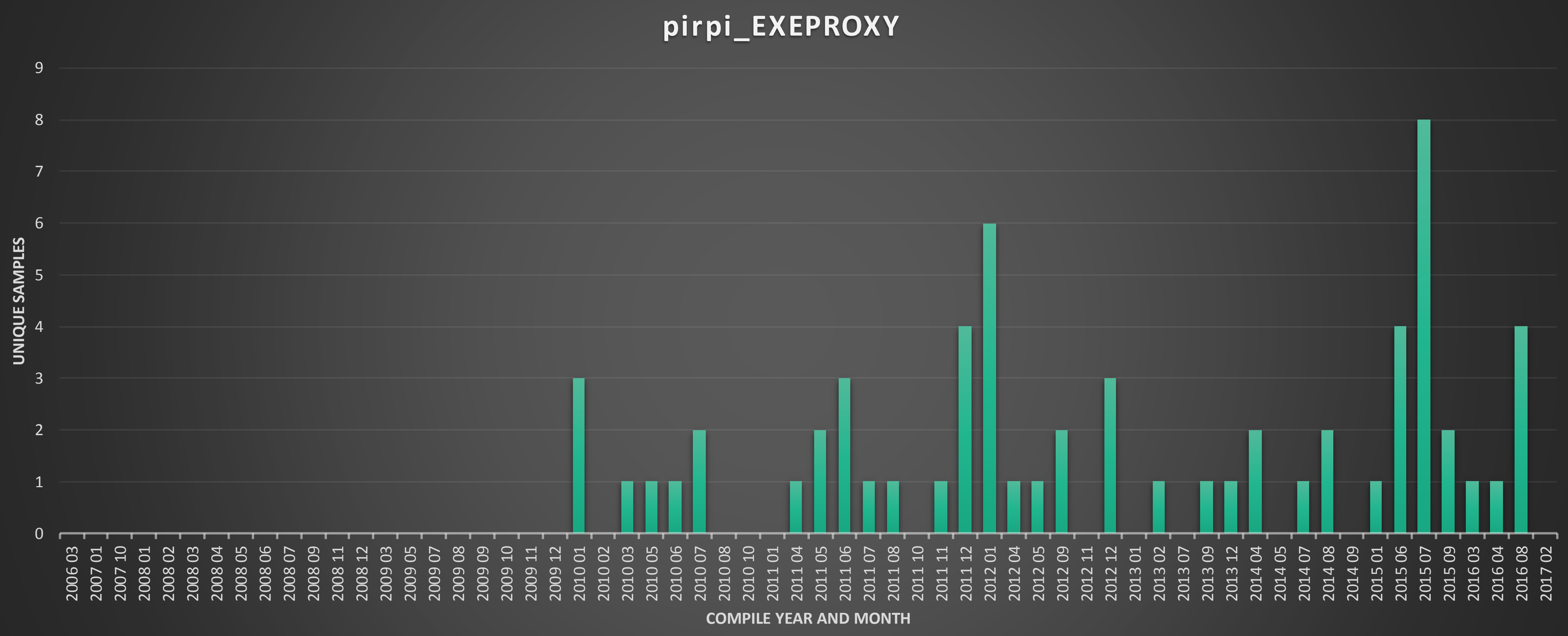
```
2812816 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 1 || md5,4d3874480110ba537b3839cb8b416b50
2812817 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 2 || md5,4d3874480110ba537b3839cb8b416b50
2812818 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 3 || md5,4d3874480110ba537b3839cb8b416b50
2812819 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 4 || md5,b94bcffcacc65d05e5f508c5bd9c950c
2812820 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 5 || md5,b94bcffcacc65d05e5f508c5bd9c950c
2812821 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 6 || md5,b94bcffcacc65d05e5f508c5bd9c950c
```

- b94bcffcacc65d05e5f508c5bd9c950c
- Contains function_1
- Contains Anti-Disasm
- OpenSSL included
- Requires cmd line params to run



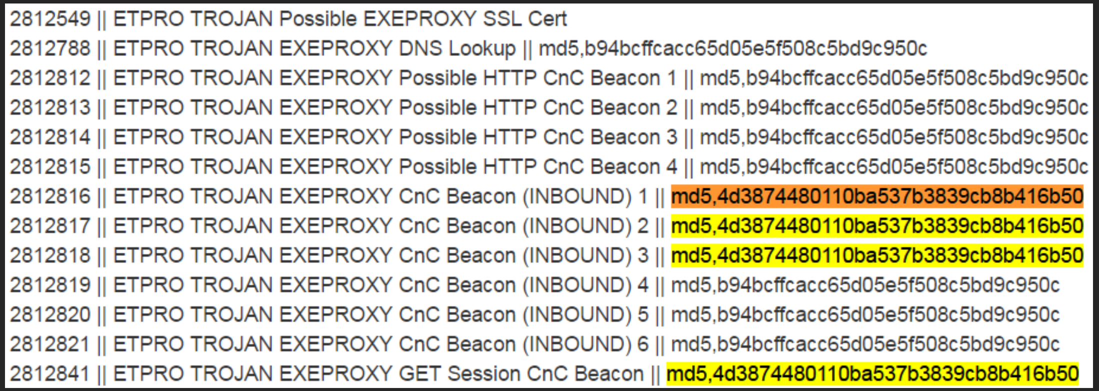
```
String

ipconfig /all

net localgroup administrators

net localgroup administrators /domain

net group "domain admins" /domain
netstat -an -p tcp
ping -a [redacted] -n 2
nbtstat -a [redacted]
netstat -an -p tcp
://[redacted]96/img/[redacted]1.exe
dir c:\
c:\aos.exe -in N111

net start aos
net stop aos
netstat -ano -p tcp
tasklist /v


://[redacted]96/img/[redacted]2.exe
dir c:\
c:\dh.exe
del c:\dh.exe
```

EXEProxy: pirpi_EXEPROXY



EXEProxy 2: Electric Boogaloo

- 4d3874480110ba537b3839cb8b416b50
- Contains function_1
- Server tool
- Requires Cmd Line Params
- No other notable anchor functions

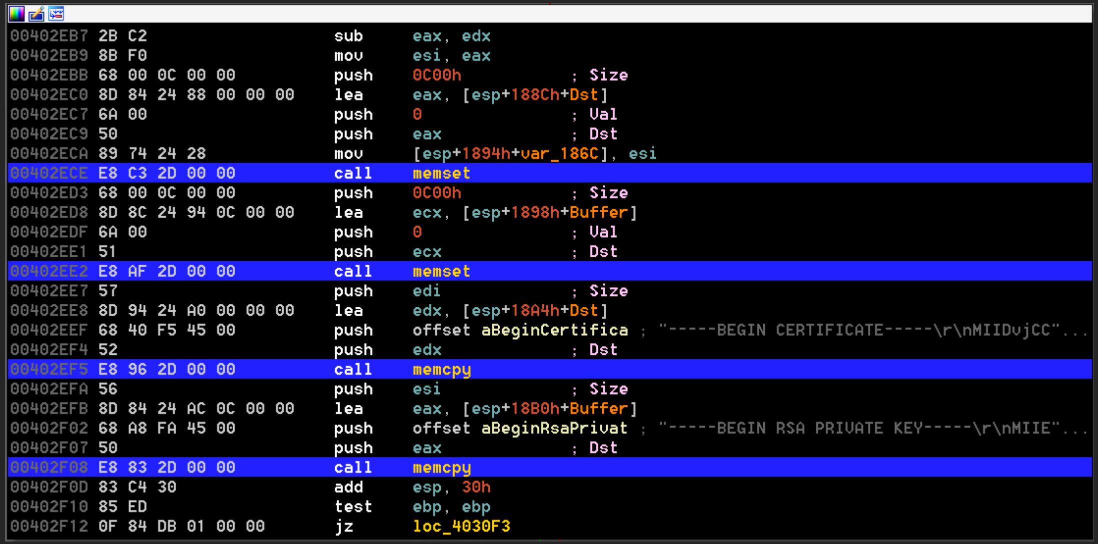


```
2812549 || ETPRO TROJAN Possible EXEPROXY SSL Cert
2812788 || ETPRO TROJAN EXEPROXY DNS Lookup || md5,b94bcffcacc65d05e5f508c5bd9c950c
2812812 || ETPRO TROJAN EXEPROXY Possible HTTP CnC Beacon 1 || md5,b94bcffcacc65d05e5f508c5bd9c950c
2812813 || ETPRO TROJAN EXEPROXY Possible HTTP CnC Beacon 2 || md5,b94bcffcacc65d05e5f508c5bd9c950c
2812814 || ETPRO TROJAN EXEPROXY Possible HTTP CnC Beacon 3 || md5,b94bcffcacc65d05e5f508c5bd9c950c
2812815 || ETPRO TROJAN EXEPROXY Possible HTTP CnC Beacon 4 || md5,b94bcffcacc65d05e5f508c5bd9c950c
2812816 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 1 || md5,4d3874480110ba537b3839cb8b416b50
2812817 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 2 || md5,4d3874480110ba537b3839cb8b416b50
2812818 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 3 || md5,4d3874480110ba537b3839cb8b416b50
2812819 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 4 || md5,b94bcffcacc65d05e5f508c5bd9c950c
2812820 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 5 || md5,b94bcffcacc65d05e5f508c5bd9c950c
2812821 || ETPRO TROJAN EXEPROXY CnC Beacon (INBOUND) 6 || md5,b94bcffcacc65d05e5f508c5bd9c950c
2812841 || ETPRO TROJAN EXEPROXY GET Session CnC Beacon || md5,4d3874480110ba537b3839cb8b416b50
```

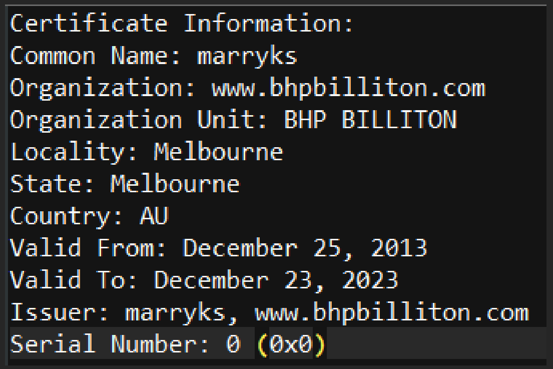
```
">Ltime %2d:%2d:%2d Disconnect >"
"%2d:%2d:%2d >Cback:"
">LTime: %2d:%2d:%2d"
">Cback: %s:%d"
"H:%s "
"Ok. "
"K:%d"
```

EXEProxy 2: Electric Boogaloo

- a85f9b4c33061ee724e59291242b9e86
- OpenSSL Server
- Contains Public/Private Keys



```
00402EB7 2B C2                sub     eax, edx
00402EB9 8B F0                mov     esi, eax
00402EBB 68 00 0C 00 00       push    0C00h               ; Size
00402EC0 8D 84 24 88 00 00 00 lea     eax, [esp+188Ch+Dst]
00402EC7 6A 00                push    0                   ; Val
00402EC9 50                   push    eax                 ; Dst
00402ECA 89 74 24 28          mov     [esp+1894h+var_186C], esi
00402ECE E8 C3 2D 00 00       call    memset
00402ED3 68 00 0C 00 00       push    0C00h               ; Size
00402ED8 8D 8C 24 94 0C 00 00 lea     ecx, [esp+1898h+Buffer]
00402EDF 6A 00                push    0                   ; Val
00402EE1 51                   push    ecx                 ; Dst
00402EE2 E8 AF 2D 00 00       call    memset
00402EE7 57                   push    edi                 ; Size
00402EE8 8D 94 24 A0 00 00 00 lea     edx, [esp+18A4h+Dst]
00402EEF 68 40 F5 45 00       push    offset aBeginCertifica ; "-----BEGIN CERTIFICATE-----\r\nMIIDvjCC"...
00402EF4 52                   push    edx                 ; Dst
00402EF5 E8 96 2D 00 00       call    memcpy
00402EFA 56                   push    esi                 ; Size
00402EFB 8D 84 24 AC 0C 00 00 lea     eax, [esp+18B0h+Buffer]
00402F02 68 A8 FA 45 00       push    offset aBeginRsaPrivat ; "-----BEGIN RSA PRIVATE KEY-----\r\nMIIE"...
00402F07 50                   push    eax                 ; Dst
00402F08 E8 83 2D 00 00       call    memcpy
00402F0D 83 C4 30             add     esp, 30h
00402F10 85 ED                test    ebp, ebp
00402F12 0F 84 DB 01 00 00    jz      loc_4030F3
```



```
Certificate Information:
Common Name: marryks
Organization: www.bhpbilliton.com
Organization Unit: BHP BILLITON
Locality: Melbourne
State: Melbourne
Country: AU
Valid From: December 25, 2013
Valid To: December 23, 2023
Issuer: marryks, www.bhpbilliton.com
Serial Number: 0 (0x0)
```

In Summary:

- Some families never change
- Anchor Functions are Fun!
- Use public info
- Pirpi malware active since at least 2006
- Unintended findings

- Thanks:
  - Richard Wartell – Palo Alto Networks
  - Mike Scott – Palo Alto Networks

- Biblio:
  - MITRE:
    - https://attack.mitre.org/wiki/Software/S0063
  - FireEye:
    - https://www.fireeye.com/blog/threat-research/2010/11/ie-0-day-hupigon-joins-the-party.html
    - https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html
    - https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html
    - https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
  - Symantec:
    - https://www.symantec.com/connect/blogs/new-ie-zero-day-used-targeted-attacks
    - https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
    - http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/Symantec-Buckeye-IOCs.txt
  - EmergingThreats:
    - https://rules.emergingthreats.net/changelogs/suricata-1.3.etpro.2015-09-10T21:29:38.txt
    - (cached by other sites, search for hash 4d3874480110ba537b3839cb8b416b50 and EXEProxy)
  - Palo Alto Networks:
    - https://researchcenter.paloaltonetworks.com/2015/07/apt-group-ups-targets-us-government-with-hacking-team-flash-exploit/
    - https://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/