Stuxnet and Flame – burning ring of fire

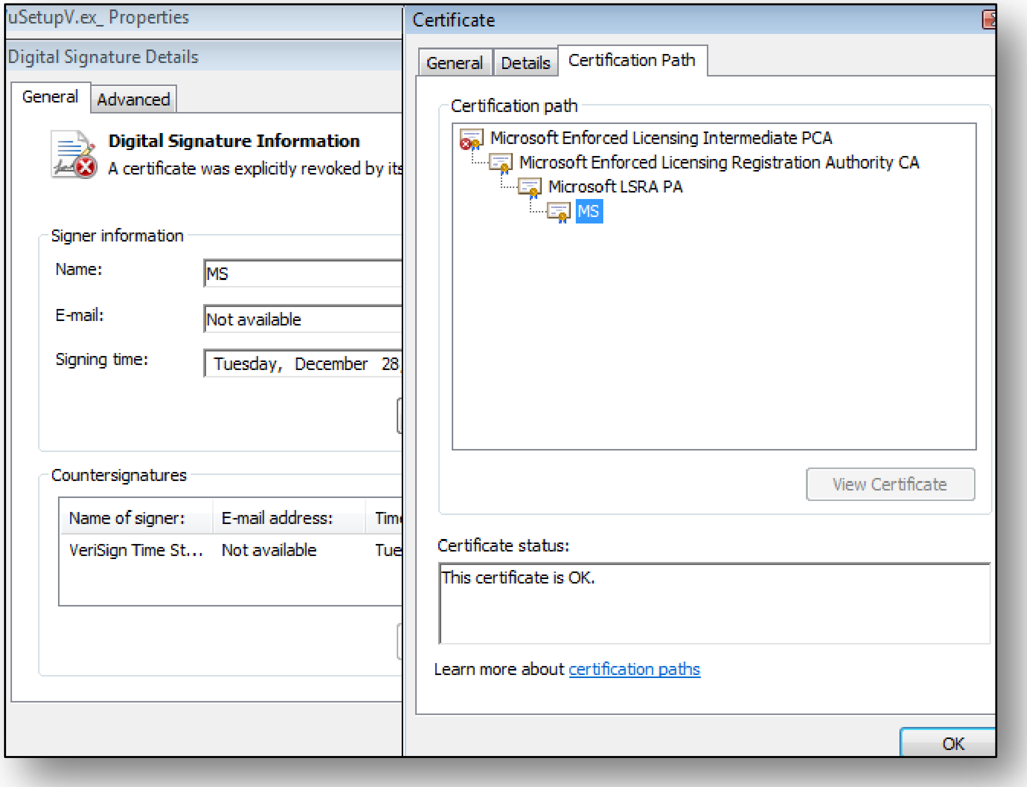
Roel Schouwenberg

Senior Researcher, Global Research & Analysis Team, Kaspersky Lab

Boston, MA, USA

Flame re-cap – MS certificate ‘God-mode’ attack

- **Extremely sophisticated MD5 hash collision attack**
- **True crypto “masters”**



uSetupV.ex_ Properties

Digital Signature Details

Digital Signature Information

A certificate was explicitly revoked by its

Signer information

Name:	MS
E-mail:	Not available
Signing time:	Tuesday, December 28

Countersignatures

Name of signer:	E-mail address:	Tim
VeriSign Time St...	Not available	Tue

Certificate

Certification path

- Microsoft Enforced Licensing Intermediate PCA
  - Microsoft Enforced Licensing Registration Authority CA
    - Microsoft LSRA PA
      - MS

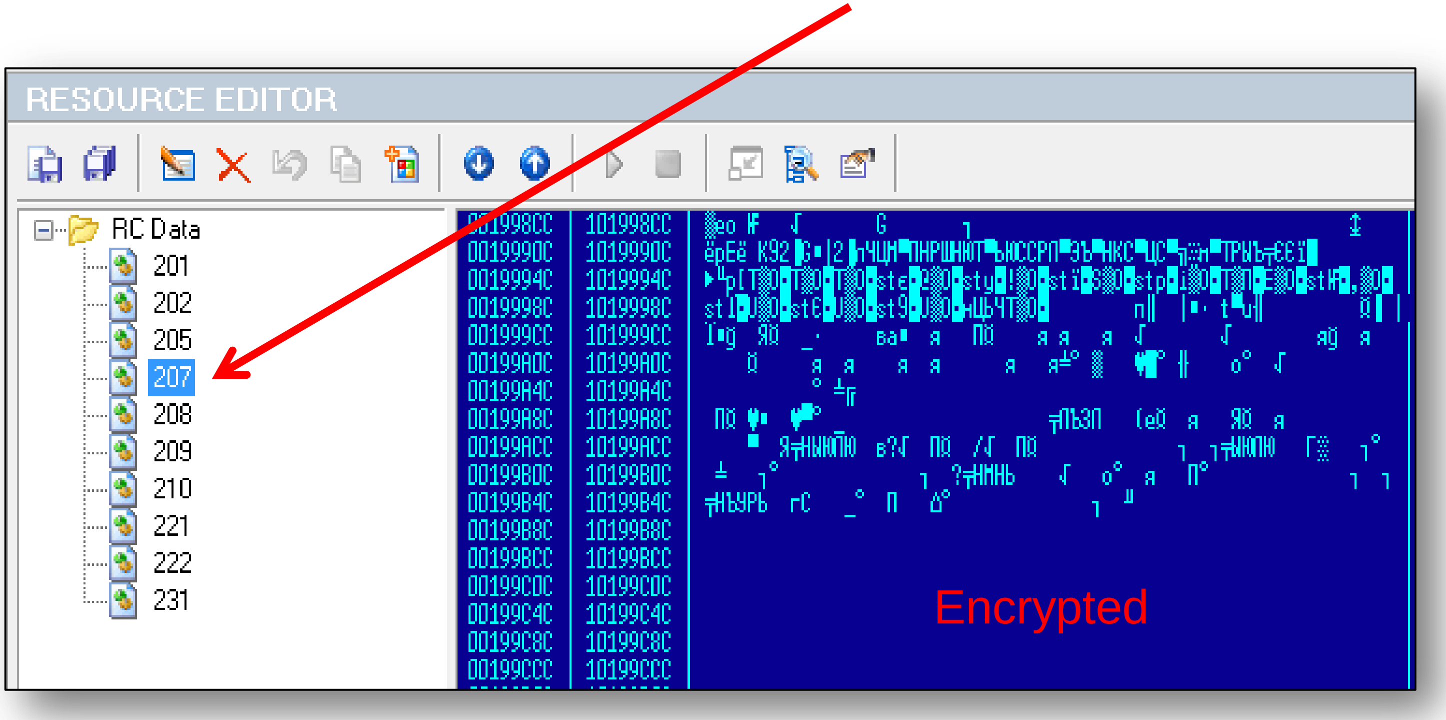
Certificate status:

This certificate is OK.

Learn more about certification paths

A Flame module inside Stuxnet.a

- **Security industry focused analysis on Stuxnet.b/c (from 2010)**
- **Resource 207 can only be found in Stuxnet.a (from 2009)**

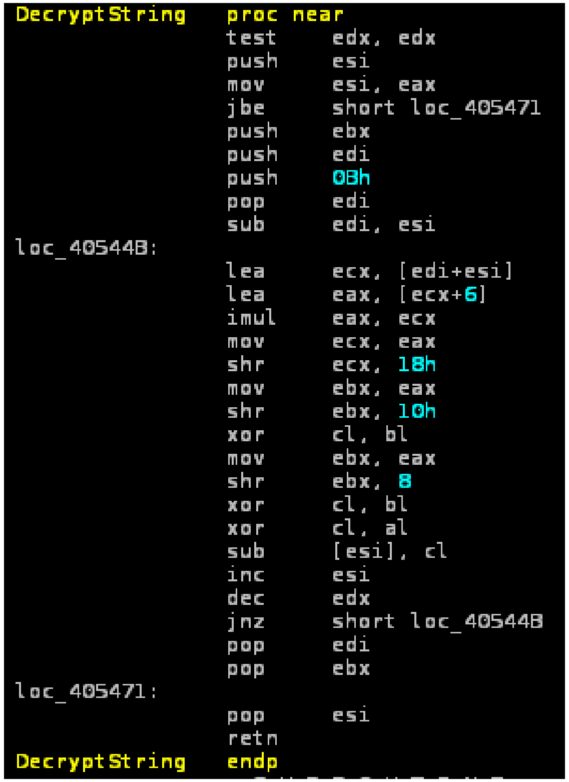


```
001998CC  101998CC
0019990C  1019990C
0019994C  1019994C
0019998C  1019998C
001999CC  101999CC
00199A0C  10199A0C
00199A4C  10199A4C
00199A8C  10199A8C
00199ACC  10199ACC
00199B0C  10199B0C
00199B4C  10199B4C
00199B8C  10199B8C
00199BCC  10199BCC
00199C0C  10199C0C
00199C4C  10199C4C
00199C8C  10199C8C
00199CCC  10199CCC
```

In October 2010, Kaspersky's Autowoodpecker system classified a Flame module as "Stuxnet.s". We manually renamed it to "Tocy".

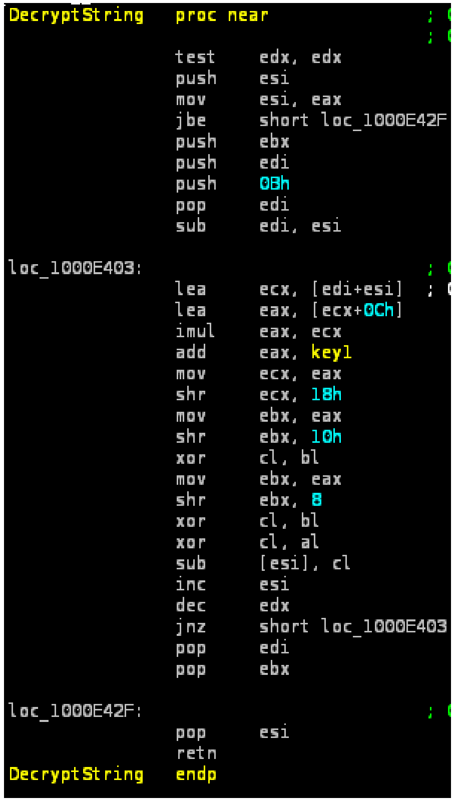
Extreme similarities in the code

- **Source code, rather than compiled binary was shared**
- **DecryptString – Resource 207, mssecmgr.ocx, browse32.ocx**



```
DecryptString   proc near
                test    edx, edx
                push    esi
                mov     esi, eax
                jbe     short loc_405471
                push    ebx
                push    edi
                push    0Bh
                pop     edi
                sub     edi, esi
loc_40544B:
                lea     ecx, [edi+esi]
                lea     eax, [ecx+6]
                imul    eax, ecx
                mov     ecx, eax
                shr     ecx, 18h
                mov     ebx, eax
                shr     ebx, 10h
                xor     cl, bl
                mov     ebx, eax
                shr     ebx, 8
                xor     cl, bl
                xor     cl, al
                sub     [esi], cl
                inc     esi
                dec     edx
                jnz     short loc_40544B
                pop     edi
                pop     ebx
loc_405471:
                pop     esi
                retn
DecryptString   endp
```

Stuxnet.a

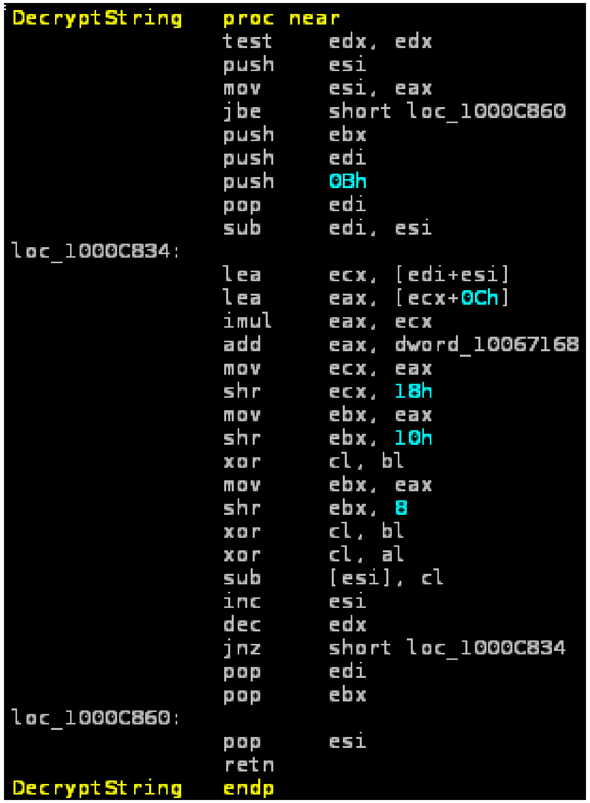


```
DecryptString   proc near                               ;
                                                        ;
                test    edx, edx
                push    esi
                mov     esi, eax
                jbe     short loc_1000E42F
                push    ebx
                push    edi
                push    0Bh
                pop     edi
                sub     edi, esi

loc_1000E403:                                           ;
                lea     ecx, [edi+esi]                  ;
                lea     eax, [ecx+0Ch]
                imul    eax, ecx
                add     eax, key1
                mov     ecx, eax
                shr     ecx, 18h
                mov     ebx, eax
                shr     ebx, 10h
                xor     cl, bl
                mov     ebx, eax
                shr     ebx, 8
                xor     cl, bl
                xor     cl, al
                sub     [esi], cl
                inc     esi
                dec     edx
                jnz     short loc_1000E403
                pop     edi
                pop     ebx

loc_1000E42F:                                           ;
                pop     esi
                retn
DecryptString   endp
```

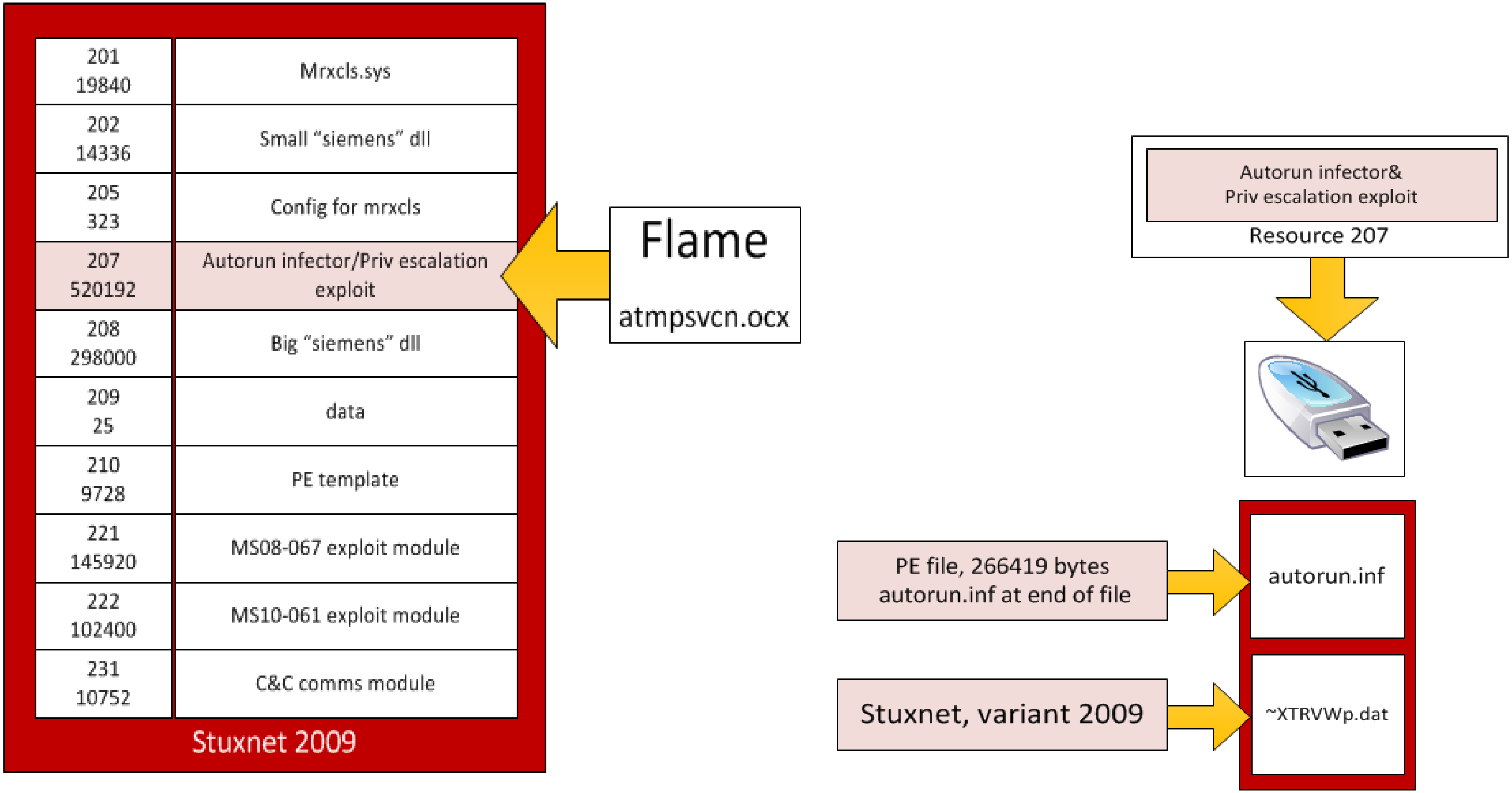
Flame



```
DecryptString   proc near
                test    edx, edx
                push    esi
                mov     esi, eax
                jbe     short loc_1000C860
                push    ebx
                push    edi
                push    0Bh
                pop     edi
                sub     edi, esi
loc_1000C834:
                lea     ecx, [edi+esi]
                lea     eax, [ecx+0Ch]
                imul    eax, ecx
                add     eax, dword_10067168
                mov     ecx, eax
                shr     ecx, 18h
                mov     ebx, eax
                shr     ebx, 10h
                xor     cl, bl
                mov     ebx, eax
                shr     ebx, 8
                xor     cl, bl
                xor     cl, al
                sub     [esi], cl
                inc     esi
                dec     edx
                jnz     short loc_1000C834
                pop     edi
                pop     ebx
loc_1000C860:
                pop     esi
                retn
DecryptString   endp
```

Flame plugin

Stuxnet.a



201 19840	Mrxcls.sys
202 14336	Small “siemens” dll
205 323	Config for mrxcls
207 520192	Autorun infector/Priv escalation exploit
208 298000	Big “siemens” dll
209 25	data
210 9728	PE template
221 145920	MS08-067 exploit module
222 102400	MS10-061 exploit module
231 10752	C&C comms module

Stuxnet 2009

Flame

atmpsvcn.ocx

Autorun infector&
Priv escalation exploit

Resource 207

PE file, 266419 bytes
autorun.inf at end of file

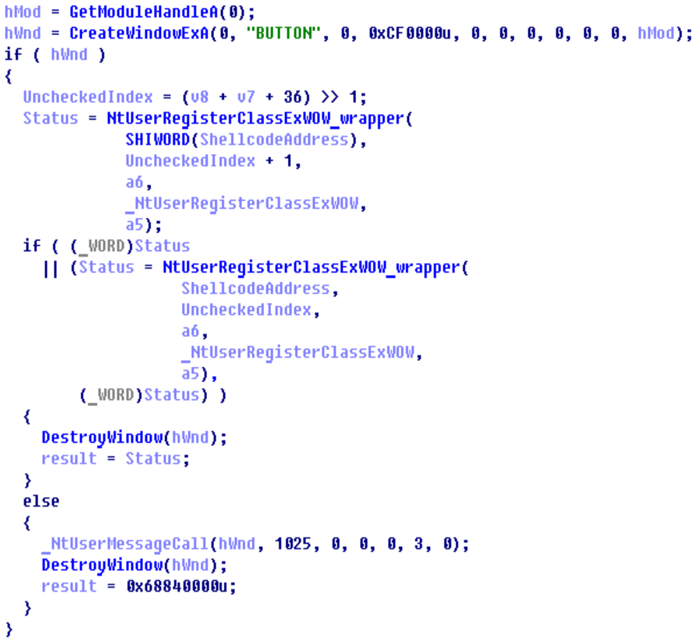
autorun.inf

Stuxnet, variant 2009

~XTRVWp.dat

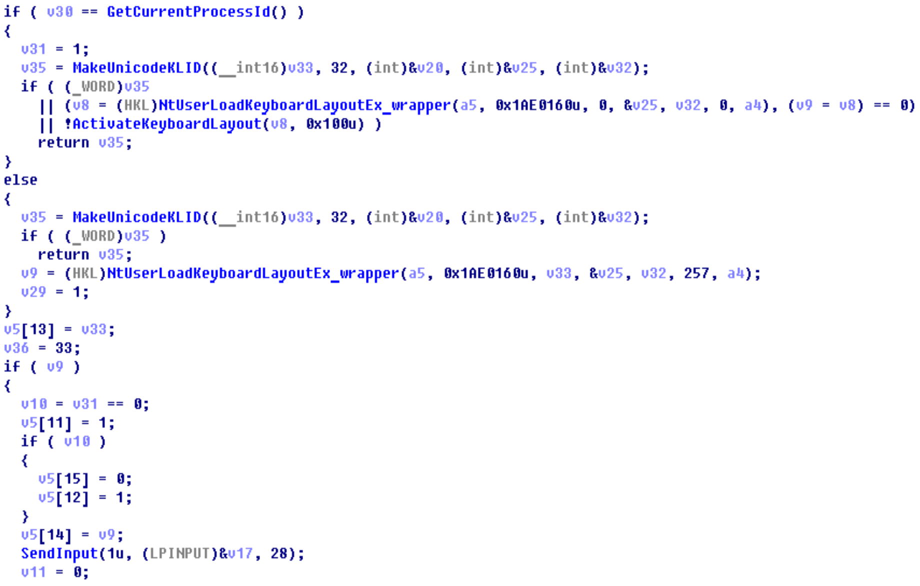
A new old zero-day?

- **Previously unrecognized EoP exploit in Resource 207**
- **Looks like “MS09-025” – we’ve asked MS for confirmation**
- **Same programmer who did MS10-073 exploit (Stuxnet.b)**



```
hMod = GetModuleHandleA(0);
hWnd = CreateWindowExA(0, "BUTTON", 0, 0xCF0000u, 0, 0, 0, 0, 0, 0, hMod);
if ( hWnd )
{
  UncheckedIndex = (v8 + v7 + 36) >> 1;
  Status = NtUserRegisterClassExWOW_wrapper(
             SHIWORD(ShellcodeAddress),
             UncheckedIndex + 1,
             a6,
             _NtUserRegisterClassExWOW,
             a5);
  if ( (_WORD)Status
    || (Status = NtUserRegisterClassExWOW_wrapper(
                   ShellcodeAddress,
                   UncheckedIndex,
                   a6,
                   _NtUserRegisterClassExWOW,
                   a5),
        (_WORD)Status) )
  {
    DestroyWindow(hWnd);
    result = Status;
  }
  else
  {
    _NtUserMessageCall(hWnd, 1025, 0, 0, 0, 3, 0);
    DestroyWindow(hWnd);
    result = 0x68840000u;
  }
}
```

Flame / Stuxnet.a



```
if ( v30 == GetCurrentProcessId() )
{
  v31 = 1;
  v35 = MakeUnicodeKLID((__int16)v33, 32, (int)&v20, (int)&v25, (int)&v32);
  if ( (_WORD)v35
    || (v8 = (HKL)NtUserLoadKeyboardLayoutEx_wrapper(a5, 0x1AE0160u, 0, &v25, v32, 0, a4), (v9 = v8) == 0)
    || !ActivateKeyboardLayout(v8, 0x100u) )
    return v35;
}
else
{
  v35 = MakeUnicodeKLID((__int16)v33, 32, (int)&v20, (int)&v25, (int)&v32);
  if ( (_WORD)v35 )
    return v35;
  v9 = (HKL)NtUserLoadKeyboardLayoutEx_wrapper(a5, 0x1AE0160u, v33, &v25, v32, 257, a4);
  v29 = 1;
}
v5[13] = v33;
v36 = 33;
if ( v9 )
{
  v10 = v31 == 0;
  v5[11] = 1;
  if ( v10 )
  {
    v5[15] = 0;
    v5[12] = 1;
  }
  v5[14] = v9;
  SendInput(1u, (LPINPUT)&v17, 28);
  v11 = 0;
```

Stuxnet.b/c

Summary & Conclusions

- The Flame platform predates Stuxnet (it was “mature” technology in 2009)
- A full Flame module exists in Stuxnet.a as part of “Resource 207”
- Previously undiscovered, patched EoP zero-day inside “Resource 207”
- “Resource 207” was removed from Stuxnet in 2010
- Stuxnet and Flame development separated after 2009, except for the exploits

Thank You