y

证书

证书信息

这个证书的目的如下:

- 确保软件来自软件
- 保护软件在发行后

发布者

不被更改

* 有关详细信息，请参考证

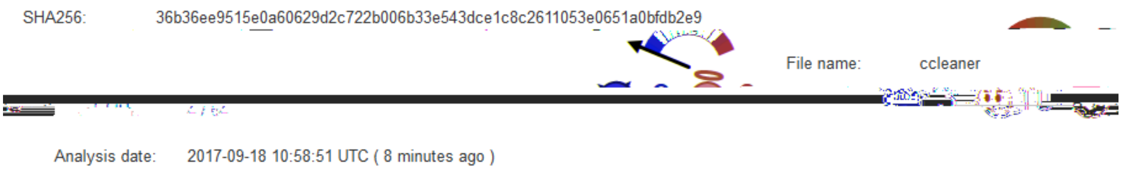
书颁发机构的说明。

颁发给: Pirifo

orm Ltd

颁发者:

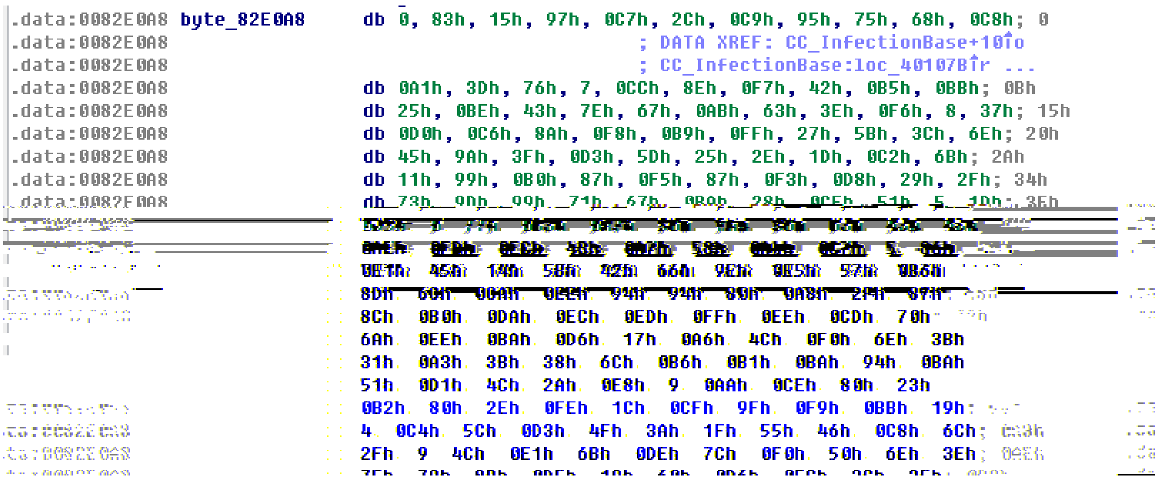
有效期从 2015/8/12 到 2018/10/11



SHA256: 36b36ee9515e0a60629d2c722b006b33e543dce1c8c2611053e0651a0bfdb2e9

File name: ccleaner

Analysis date: 2017-09-18 10:58:51 UTC (8 minutes ago)



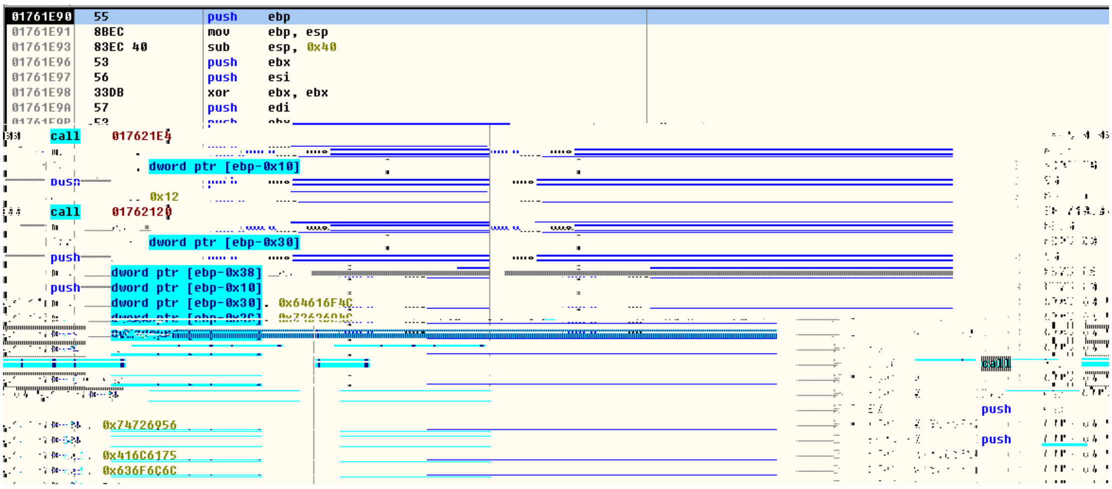
```
.data:0082E0A8 byte_82E0A8     db 0, 83h, 15h, 97h, 0C7h, 2Ch, 0C9h, 95h, 75h, 68h, 0C8h; 0
.data:0082E0A8                                         ; DATA XREF: CC_InfectionBase+10↑o
.data:0082E0A8                                         ; CC_InfectionBase:loc_40107B↑r ...
.data:0082E0A8                 db 0A1h, 3Dh, 76h, 7, 0CCh, 8Eh, 0F7h, 42h, 0B5h, 0BBh; 0Bh
.data:0082E0A8                 db 25h, 0BEh, 43h, 7Eh, 67h, 0ABh, 63h, 3Eh, 0F6h, 8, 37h; 15h
.data:0082E0A8                 db 0D0h, 0C6h, 8Ah, 0F8h, 0B9h, 0FFh, 27h, 5Bh, 3Ch, 6Eh; 20h
.data:0082E0A8                 db 45h, 9Ah, 3Fh, 0D3h, 5Dh, 25h, 2Eh, 1Dh, 0C2h, 6Bh; 2Ah
.data:0082E0A8                 db 11h, 99h, 0B0h, 87h, 0F5h, 87h, 0F3h, 0D8h, 29h, 2Fh; 34h
.data:0082E0A8                 db 73h, 9Dh, 99h, 71h, 67h, 0BAh, 28h, 0CEh, 51h, 5, 1Dh; 3Eh

                                  0E1h, 45h, 14h, 58h, 42h, 66h, 9Eh, 0E5h, 57h, 0B6h
                                  8Dh, 60h, 0DAh, 0EEh, 94h, 94h, 89h, 0A8h, 2Fh, 87h
                                  8Ch, 0B0h, 0DAh, 0ECh, 0EDh, 0FFh, 0EEh, 0CDh, 70h
                                  6Ah, 0EEh, 0BAh, 0D6h, 17h, 0A6h, 4Ch, 0F0h, 6Eh, 3Bh
                                  31h, 0A3h, 3Bh, 38h, 6Ch, 0B6h, 0B1h, 0BAh, 94h, 0BAh
                                  51h, 0D1h, 4Ch, 2Ah, 0E8h, 9, 0AAh, 0CEh, 80h, 23h
                                  0B2h, 80h, 2Eh, 0FEh, 1Ch, 0CFh, 9Fh, 0F9h, 0BBh, 19h;
                                  4, 0C4h, 5Ch, 0D3h, 4Fh, 3Ah, 1Fh, 55h, 46h, 0C8h, 6Ch;
                                  2Fh, 9, 4Ch, 0E1h, 6Bh, 0DEh, 7Ch, 0F0h, 50h, 6Eh, 3Eh;
```

```
.text:00401000 sub_401000      proc near               ; CODE XREF: CC_InfectionBase+16↓p
.text:00401000                                         ; DATA XREF: HEADER:00400164↑o ...
.text:00401000
.text:00401000 arg_0           = dword ptr  8
.text:00401000 arg_4           = dword ptr  0Ch
.text:00401000
.text:00401000                 mov     edi, edi
.text:00401002                 push    ebp
.text:00401003                 mov     ebp, esp
.text:00401005                 push    esi
.text:00401006                 xor     esi, esi
```

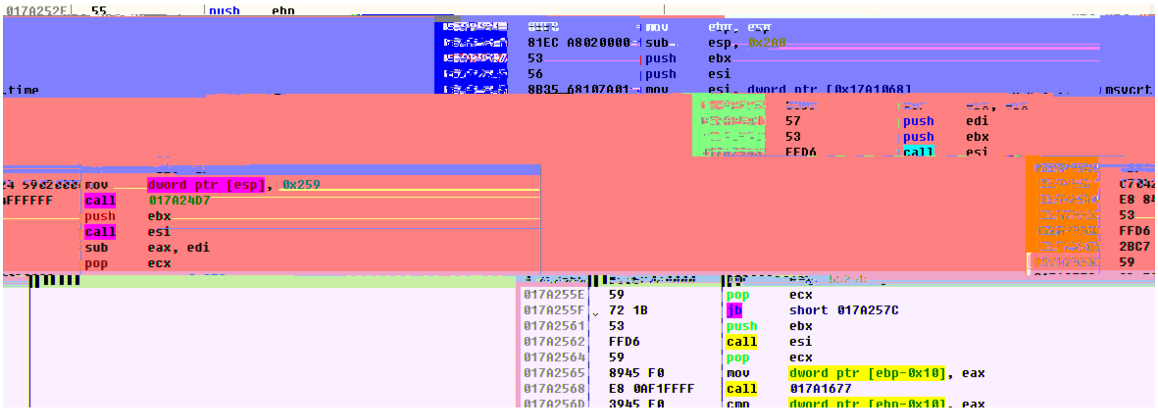
```
                                     ; CODE XREF: sub_401000+27↓j
mov     eax, [ebp+arg_0]
imul    ecx, 47A6547h
mov     dl, cl
```

```
.text:00401029 loc_401029:                             ; CODE XREF: sub_401000+10
.text:00401029                 pop     esi
.text:0040102A                 pop     ebp
.text:0040102B                 retn
.text:0040102B sub_401000      endp
```

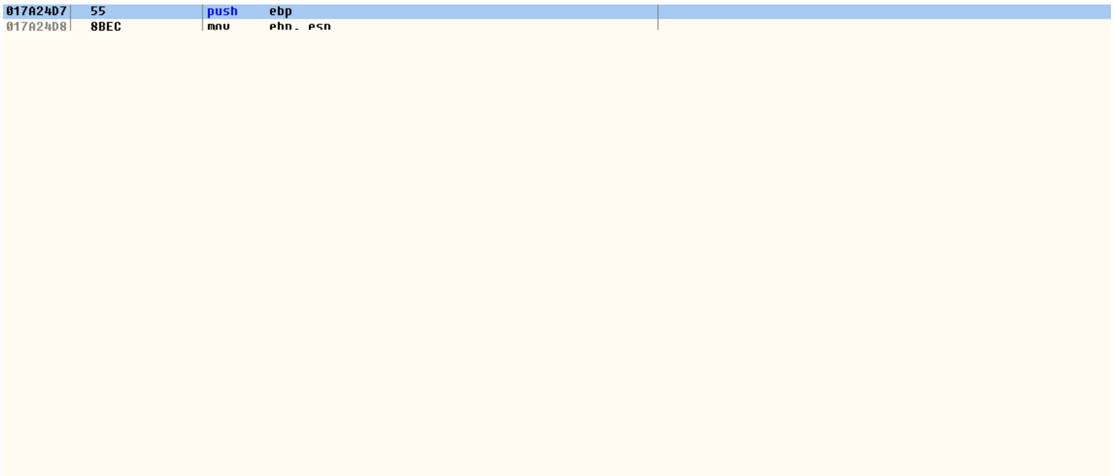


```
01761E90  55         push    ebp
01761E91  8BEC       mov     ebp, esp
01761E93  83EC 40    sub     esp, 0x40
01761E96  53         push    ebx
01761E97  56         push    esi
01761E98  33DB       xor     ebx, ebx
01761E9A  57         push    edi
```

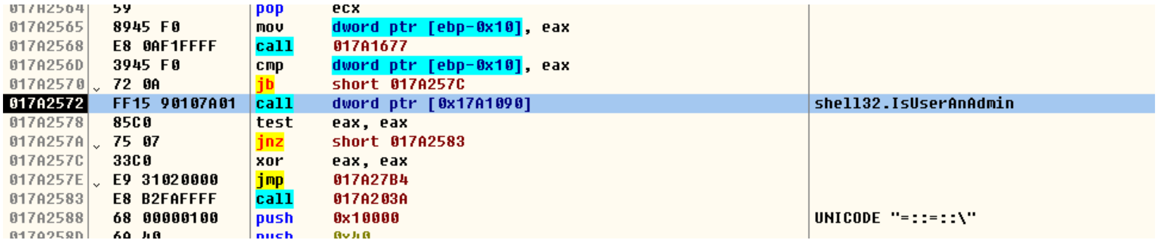
```
call    017621E4
        dword ptr [ebp-0x10]
push
        0x12
call    01762120
        dword ptr [ebp-0x30]
push
        dword ptr [ebp-0x38]
push    dword ptr [ebp-0x10]
        dword ptr [ebp-0x30]  0x64616F4C
        0x74726956
        0x416C6175
        0x636F6C6C
```



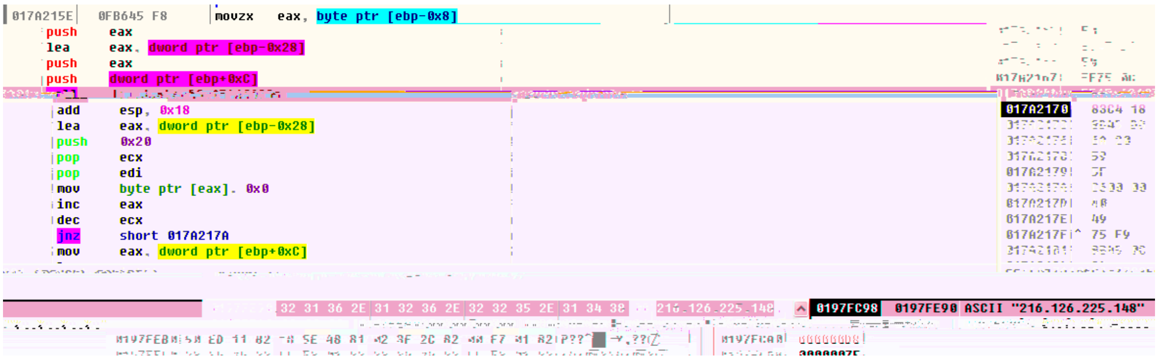
```
017A252E  55             push    ebp
          81EC A8020000  sub     esp, 0x2A8
          53             push    ebx
          56             push    esi
          8B35 68107A01  mov     esi, dword ptr [0x17A1068]        msvcrt.
.time
          57             push    edi
          53             push    ebx
          FFD6           call    esi
          mov     dword ptr [esp], 0x259
FFFFFF    call    017A24D7
          push    ebx
          call    esi
          sub     eax, edi
          pop     ecx
017A255E  59             pop     ecx
017A255F  72 1B          jb      short 017A257C
017A2561  53             push    ebx
017A2562  FFD6           call    esi
017A2564  59             pop     ecx
017A2565  8945 F0        mov     dword ptr [ebp-0x10], eax
017A2568  E8 0AF1FFFF    call    017A1677
017A256D  3945 F0        cmp     dword ptr [ebp-0x10], eax
```



```
017A24D7  55             push    ebp
017A24D8  8BEC           mov     ebp, esp
```



```
017A2564   59             pop     ecx
017A2565   8945 F0        mov     dword ptr [ebp-0x10], eax
017A2568   E8 0AF1FFFF    call    017A1677
017A256D   3945 F0        cmp     dword ptr [ebp-0x10], eax
017A2570 ⌄ 72 0A          jb      short 017A257C
017A2572   FF15 90107A01  call    dword ptr [0x17A1090]          shell32.IsUserAnAdmin
017A2578   85C0           test    eax, eax
017A257A ⌄ 75 07          jnz     short 017A2583
017A257C   33C0           xor     eax, eax
017A257E ⌄ E9 31020000    jmp     017A27B4
017A2583   E8 B2FAFFFF    call    017A203A
017A2588   68 00000100    push    0x10000                        UNICODE "=::=::\"
017A258D   6A 40          push    0x40
```



```
017A215E  0FB645 F8      movzx   eax, byte ptr [ebp-0x8]
          push    eax
          lea     eax, dword ptr [ebp-0x28]
          push    eax
          push    dword ptr [ebp+0xC]
          add     esp, 0x18
          lea     eax, dword ptr [ebp-0x28]
          push    0x20
          pop     ecx
          pop     edi
          mov     byte ptr [eax], 0x0
          inc     eax
          dec     ecx
          jnz     short 017A217A
          mov     eax, dword ptr [ebp+0xC]

017A2170   83C4 18
017A2179   5F
017A217D   40
017A217E   49
017A217F ^ 75 F9

32 31 36 2E 31 32 36 2E 32 32 35 2E 31 34 38  216.126.225.148
0197FC98  0197FE90  ASCII "216.126.225.148"
0197FEB0  5D ED 11 02 E0 5E 40 01 02 3F 2C 02 00 F7 01 02
0197FCA0  00000008
```
