New Apple Mac Trojan Called OSX/Crisis Discovered

By Lysa Myers

Published: 2012-07-25 · Archived: 2026-04-05 13:42:25 UTC

Malware + Recommended

Posted on July 24th, 2012 by 

Intego has discovered a new Trojan called **OSX/Crisis**. This threat is a dropper which creates a backdoor when it's run. It installs silently, without requiring a password, and works only in OSX versions 10.6 and 10.7 – Snow Leopard and Lion. **Update:** This threat may run on Leopard 10.5, but it has a tendency to crash. It does not run on the new Mountain Lion 10.8.

The Trojan preserves itself against reboots (i.e. it establishes persistence), so it will continue to run until it's removed. Depending on whether or not the dropper runs on a user account with Admin permissions, it will install different components. We have not yet seen if or how this threat is installed on a user's system; it may be that an installer component will try to establish Admin permissions.

If the dropper runs on a system with Admin permissions, it will drop a rootkit to hide itself. In either case, it creates a number of files and folders to complete its tasks. It creates 17 files when it's run with Admin permissions, 14 files when it's run without. Many of these are randomly named, but there are some that are consistent.

With or without Admin permissions, this folder is created in the infected user's home directory:

- ~/Library/ScriptingAdditions/appleHID/

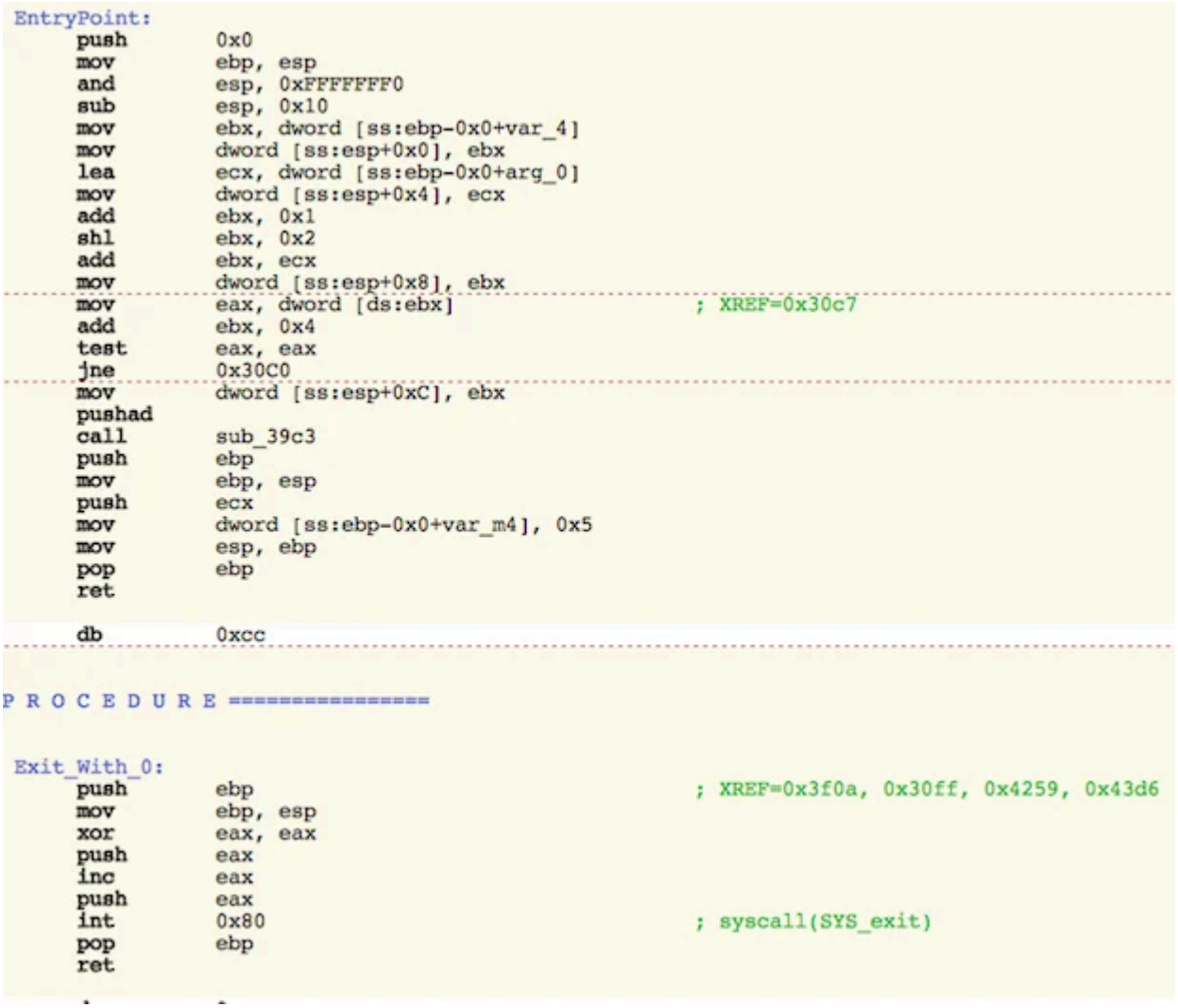
Only with Admin permissions, this folder is created:

- /System/Library/Frameworks/Foundation.framework/XPCServices/

The backdoor component calls home to the IP address 176.58.100[.]37 every 5 minutes, awaiting instructions. The file is created in a way that is intended to make reverse engineering tools more difficult to use when analyzing the file. This sort of anti-analysis technique is common in Windows malware, but is relatively uncommon for OS X malware.

It uses low-level system calls to hide its activities, as shown in the following images:

```
   ; Basic Block Input Regs: eax -  Killed Regs: eax edx esp ebp
OpenAndMapLibSystem106:
     push        ebp                                     ; XREF=0x3ef6
     mov         ebp, esp
     sub         esp, 0x6C
     sub         esp, 0x80
     push        'ib..'                                  ; /usr/lib/libSystem.B.dylib - 10.6
     push        '.dyl'
     push        'em.B'
     push        'Syst'
     push        '/lib'
     push        '/lib'
     push        '/usr'
     mov         edx, esp
     push        0x0
     push        edx
     xor         eax, eax
     mov         al, 0x5
     push        eax
     int         0x80                                    ; syscall(SYS_open)
     mov         dword [ss:ebp-0x6c+var_0], eax
     cmp         dword [ss:ebp-0x6c+var_0], 0xFFFFFFFF
     jne         0x370B
   ; Basic Block Input Regs: eax -  Killed Regs: eax
     xor         eax, eax
     jmp         0x376E
   ; Basic Block Input Regs: ebp -  Killed Regs: eax esp ebp
     lea         eax, dword [ss:ebp-0x6c+var_12]         ; XREF=0x3705
     mov         dword [ss:esp+0x4], eax
     mov         eax, dword [ss:ebp-0x6c+var_0]
     mov         dword [ss:esp], eax
     xor         eax, eax
     mov         al, 189
     push        eax
     int         0x80                                    ; syscall(SYS_fstat)
     mov         dword [ss:ebp-0x6c+var_8], eax
     cmp         dword [ss:ebp-0x6c+var_8], 0x0
     je          0x372C
   ; Basic Block Input Regs: eax -  Killed Regs: eax
     xor         eax, eax
     jmp         0x376E
   ; Basic Block Input Regs: ebp -  Killed Regs: eax esp ebp
     mov         dword [ss:esp+0x18], 0x0                ; XREF=0x3726
     mov         dword [ss:esp+0x14], 0x0
     mov         eax, dword [ss:ebp-0x6c+var_0]
     mov         dword [ss:esp+0x10], eax
     mov         dword [ss:esp+0xC], 0x2
     mov         dword [ss:esp+0x8], 0x1
     mov         eax, dword [ss:ebp-0x6c+var_60]
     mov         dword [ss:esp+0x4], eax
     mov         dword [ss:esp], 0x0
     xor         eax, eax
     mov         al, 197
     push        eax
     int         0x80                                    ; syscall(SYS_mmap)
     mov         dword [ss:ebp-0x6c+var_4], eax
     mov         eax, dword [ss:ebp-0x6c+var_4]
   ; Basic Block Input Regs: ebp -  Killed Regs: esp ebp
     mov         esp, ebp                                ; XREF=0x3709, 0x372a
     pop         ebp
```



```
EntryPoint:
        push    0x0
        mov     ebp, esp
        and     esp, 0xFFFFFFF0
        sub     esp, 0x10
        mov     ebx, dword [ss:ebp-0x0+var_4]
        mov     dword [ss:esp+0x0], ebx
        lea     ecx, dword [ss:ebp-0x0+arg_0]
        mov     dword [ss:esp+0x4], ecx
        add     ebx, 0x1
        shl     ebx, 0x2
        add     ebx, ecx
        mov     dword [ss:esp+0x8], ebx
        mov     eax, dword [ds:ebx]                     ; XREF=0x30c7
        add     ebx, 0x4
        test    eax, eax
        jne     0x30C0
        mov     dword [ss:esp+0xC], ebx
        pushad
        call    sub_39c3
        push    ebp
        mov     ebp, esp
        push    ecx
        mov     dword [ss:ebp-0x0+var_m4], 0x5
        mov     esp, ebp
        pop     ebp
        ret

        db      0xcc

P R O C E D U R E ================

Exit_With_0:
        push    ebp                                     ; XREF=0x3f0a, 0x30ff, 0x4259, 0x43d6
        mov     ebp, esp
        xor     eax, eax
        push    eax
        inc     eax
        push    eax
        int     0x80                                    ; syscall(SYS_exit)
        pop     ebp
        ret
```

Intego found samples of this malware on the VirusTotal website, a site used by security companies to share malware samples. This threat has ~~not yet~~ been found in the wild~~, and so far there is no indication that this Trojan has infected users so right now the threat is considered to be a low risk~~ (note: see updates below). Nonetheless, Intego VirusBarrier X6 detects and removes this malware using today's definitions. It detects the dropper component as **OSX/Crisis**, and the backdoor component as **Backdoor:OSX/Crisis**. It will also block connections with the IP address the backdoor component seeks to connect with.

Intego VirusBarrier X6 users should update as soon as possible to get protection from this threat.

We are still analyzing the threat at this time. We will post a more in-depth analysis as we have more details. **Update:** We have posted a deeper dive into OSX/Crisis, and details about how this OSX/Crisis variant was used in a targeted attack. We have also written several write-ups about later OSX/Crisis variants. You may also be interested in our write-up of OSX/NetWeirdRC (aka NetWire), another commercial macOS remote access tool (RAT). See also our latest malware write-ups.

How can I learn more?

Each week on the **Intego Mac Podcast**, Intego's Mac security experts discuss the latest Apple news, including security and privacy stories, and offer practical advice on getting the most out of your Apple devices. Be sure to **follow the podcast** to make sure you don't miss any episodes.

You can also subscribe to our **e-mail newsletter** and keep an eye here on **The Mac Security Blog** for the latest Apple security and privacy news. And don't forget to follow Intego on your favorite social media channels:

Source: https://www.intego.com/mac-security-blog/new-apple-mac-trojan-called-osxcrisis-discovered-by-intego-virus-team/?