Apple updates XProtect to block 'Windows' malware on a Mac

Apple's XProtect security software has recently been quietly updated to add some signature to help detect Windows PE files as well as Windows executable files that can be run on Mac using Mono .NET framework.

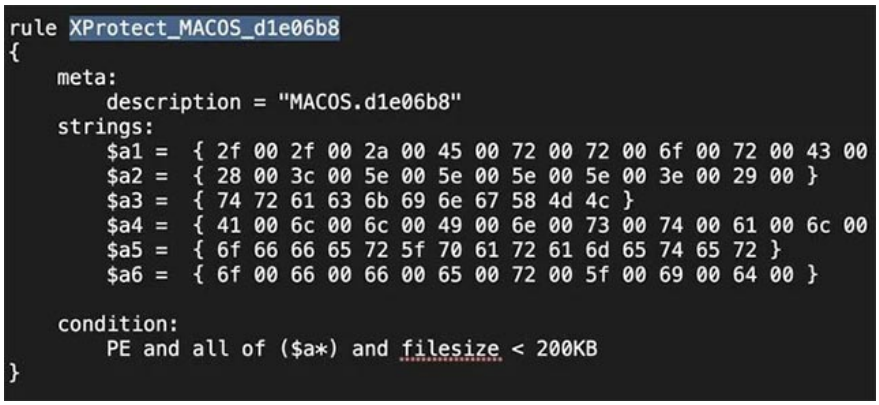
Apple's XProtect security software has recently been quietly updated to add some signature to help detect Windows PE files as well as Windows executable files that can be run on Mac using Mono .NET framework.

If you don't know, XProtect is Apple's built-in antivirus software that acts as a real-time protection shield on a Mac. To protect users from viruses and malicious code, XProtect uses signatures built from many Yara rules aimed at known security threats for Mac users.

1. India's largest IT services company is hit by a hacker '

According to security expert Patrick Wardle, the two new signatures released on April 19, 2019 when used together can help detect ad packages containing Windows executable files running on macOS. .

The two new signatures are called "PE", which helps detect Windows PE files and "MACOS.d1e06b8", and is also used to identify a specially built Windows executable file that can run on Mac, as illustrated below:



```
rule XProtect_MACOS_d1e06b8
{
    meta:
        description = "MACOS.d1e06b8"
    strings:
        $a1 =  { 2f 00 2f 00 2a 00 45 00 72 00 72 00 6f 00 72 00 43 00
        $a2 =  { 28 00 3c 00 5e 00 5e 00 5e 00 5e 00 3e 00 29 00 }
        $a3 =  { 74 72 61 63 6b 69 6e 67 58 4d 4c }
        $a4 =  { 41 00 6c 00 6c 00 49 00 6e 00 73 00 74 00 61 00 6c 00
        $a5 =  { 6f 66 66 65 72 5f 70 61 72 61 6d 65 74 65 72 }
        $a6 =  { 6f 00 66 00 66 00 65 00 72 00 5f 00 69 00 64 00 }

    condition:
        PE and all of ($a*) and filesize < 200KB
}
```

1. Malicious ad campaigns abuse Chrome to steal 500 million iOS user sessions

Basically, XProtect will use the above rule to detect Windows executable files that contain the following strings. Note, the strings below are built based on the rules shown above, so they can also be 'torn' small.

```
// * ErborC
()
trackingXML
AllInstal
offer_parameter
offer_id
```

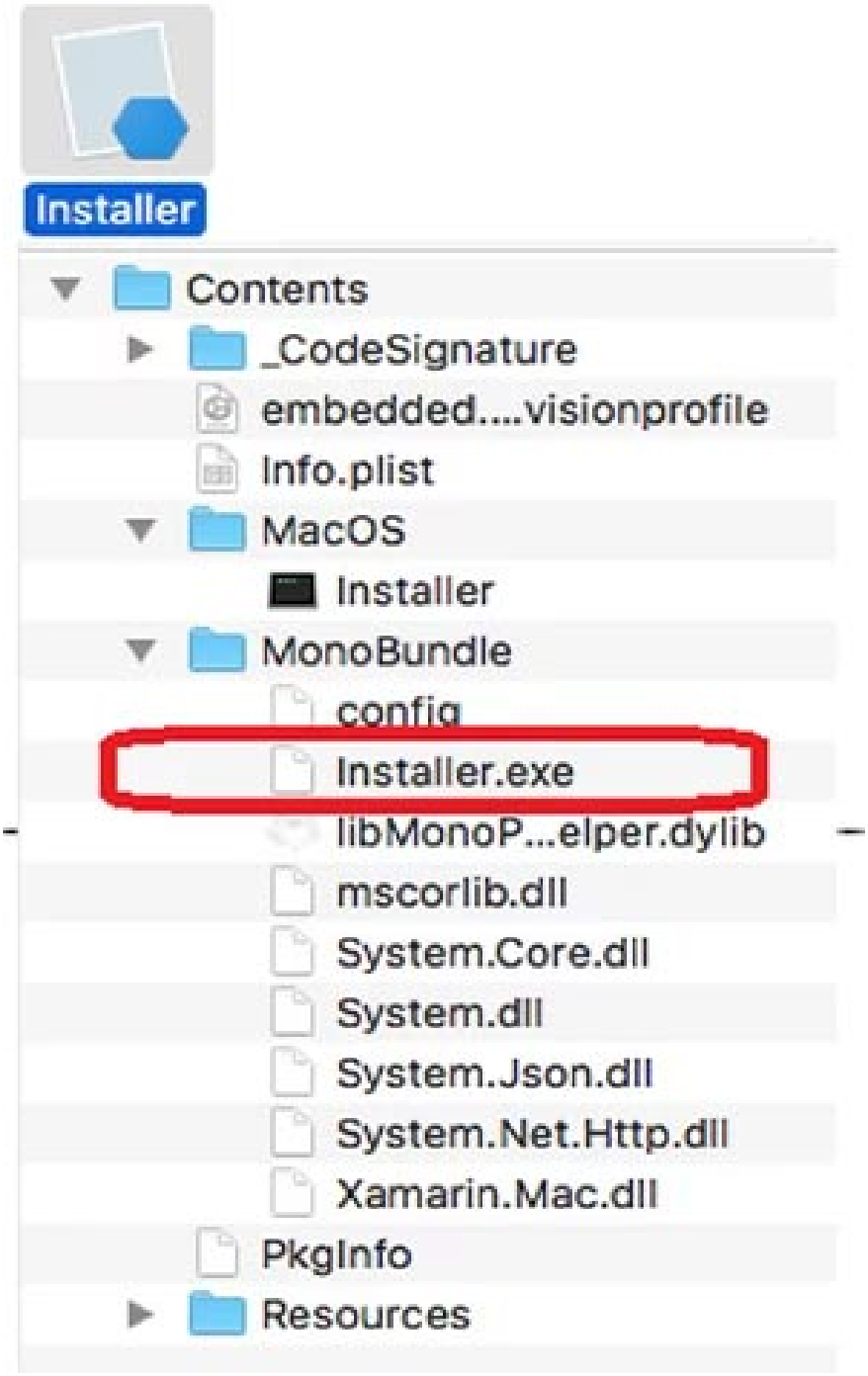
These strings are linked to many ad packages containing modified Windows executable files to run on Mac using Mono C # framework.

Malicious code targeted Mac adware package.

In February, a number of major technology news sites around the world reported cases of malware detected using the Mac installer to launch Windows executable files using Mono. C # framework.

Mono is basically a cross-platform framework, allowing C # programs to run on many popular operating systems today, including Windows, Mac and Linux.

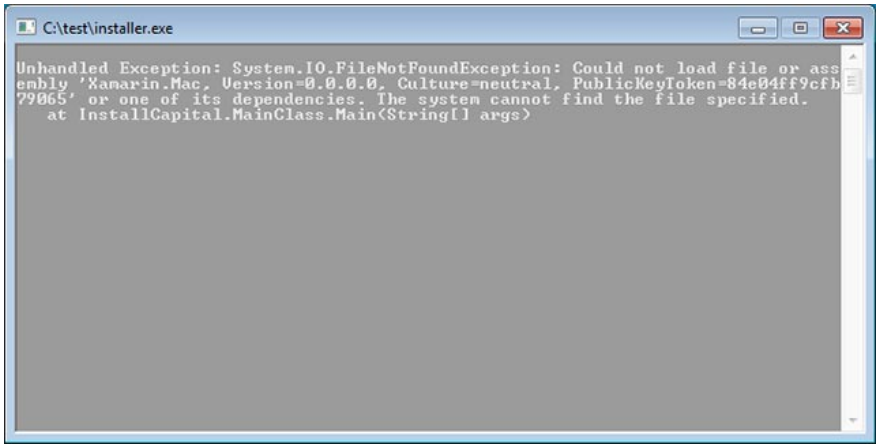
Some of the detected malware samples will extract a Windows executable file named Installer.exe. This file will then use the included Mono Mac libraries to be able to run on this operating system.



1. 25% of "out-of-the-box" phishing emails are the default security of Office 365

After successfully launching, the ad package will silently contact the crook's remote servers to download the 'offers' and install them into the victim's system. These 'offers' can be browser extensions, adware, exploit tools and unwanted password theft.

Although these ad software packages are essentially executable files of Windows, they are actually not able to run on Windows. This is because they are programmed to try to download the Mac Mono framework libraries, while those are completely unavailable in Windows. If you try to run these executable files in Windows, the system will report an error as shown in the illustration below:



1. Detect spyware targeting iOS users

When programming languages ??like C # become cross-platform languages, being able to discover Windows PE files will play a very important role in protecting users from malware, which can be easy. spread to Mac using frameworks like Mono.