THE CONVERSATION
Academic rigour, journalistic flair

# iWorm hack shows Macs are vulnerable too

October 8, 2014 6.18am BST

That's one sad Mac. nickkellet, CC BY

## Author

**Bill Buchanan**

Head, Centre for Distributed Computing, Networks and Security, Edinburgh Napier University

The computer operating systems and applications we use today have often evolved over many years, decades even, and contain tens or hundreds of millions of lines of code. Flaws in that code – and there will always be some – give rise to security problems that, in an internet-connected world, are an increasing problem.

Many are found in code written in the C++ programming language – in Microsoft Windows, in Java, in applications such as Abode Flash or Reader, the Outlook email client, browsers such as Internet Explorer and Firefox, and increasingly Linux and OS X. Any issues found to affect Linux and other

Unix-like operating systems causes problems for Apple because OS X is Unix-like in nature.

Apple's decision to redevelop a new operating system for the Macintosh based on Unix was a momentous one. A family of related operating systems, Unix has evolved since the early 1970s and continues to be used and developed today. Technically OS X is a "Unix-like" operating system called Darwin; Linux is another Unix-like operating system. This decision meant the company could rely on the stability of Unix and focus on the user experience.

Will this decision return to bite Apple, however? The flaws now being discovered in Unix-like operating systems also affect OS X. Many bugs are being found that have gone unnoticed for years – the Heartbleed flaw in OpenSSL for example relates to C++ code written by Eric Young in 1998.

## Lair of the iWorm

Last week, Dr. Web (a Russian security firm) detailed a newly discovered piece of malware for OS X, called Mac.BackDoor.iWorm. This allows hackers to take control of a computer, using it as part of a botnet (a group of perhaps thousands of compromised, remotely-controlled computers) for illegal activity such as spamming or performing Denial of Service (DDoS) attacks, where a website is overloaded with requests and forced offline.

After Dr. Web detected more than 17,000 computers infected with the worm, Apple responded quickly by adding the malware's signature to the Xprotect malware scanner built into OS X. But this will only protect against the worm if it has been updated to include the latest changes.


Detecting the iWorm.

Interestingly iWorm's creators used the popular website Reddit as an attack vector. In a fake Minecraft discussion forum were posted the addresses of the hackers' command and control servers – iWorm would browse Reddit to find these addresses, connect and wait for instructions. Reddit closed the hacker's user accounts and the fake forum, cutting off the iWorm's controllers – for now. The suggestion is that it spread originally through pirated software infected with malicious code downloaded from torrent sites (making it more of a Trojan than a worm).

## Shell Shock

Another recent bug, the Shellshock vulnerability found in the Bash shell program affects practically all Unix-like operating systems (including Linux and OS X) because it's such a common program, included by default in most installations. As Linux is found in many embedded systems – network hardware such as routers and switches, microcontrollers that operate traffic lights, industrial production lines and all sorts of other uses – the number of potentially vulnerable devices is huge.

The bug allows an intruder to remotely run arbitrary commands. The efforts of hackers have been to use Shellshock to control web servers through their CGI function, one of the oldest methods through which a program could communicate with a web server. Today CGI has been largely replaced by PHP and other high-level scripting languages, but many millions of servers retain it for compatibility.

Even by using Shellshock to run commands on remote machines, on a properly security-hardened server the potential for damage is limited, as most of the important operations require higher-level privileges – if correctly configured.

## Buffer overflow attack

Such programming errors show how sloppy software developers have been (and often continue to be), and how long such flaws can hang around – some 23 years for Heartbleed. Many bugs are due to C++ programming errors, causing programs to act incorrectly when the data a program receives is not what it expects. A common way of exploiting this is a buffer overflow.

Programs typically allocate a certain amount of memory (buffer) to variables used by programs to store and pass around data. That data is expected to arrive in a certain format and fit within the memory allocation. If it arrives and is larger than it should be it can overwrite code stored in neighbouring memory areas, causing the program to become erratic, crash, or execute code contained in the data sent that overruns the buffer.

Similar but not quite the same, the Heartbleed flaw lay in a feature of SSL called a "heartbeat", a challenge-response between two computers designed to keep the connection open. The code required the client computer to send a string of characters, and a number totalling the length of that string of characters. The server reads the number and sends back that many characters. The attack worked

because the attacker could, for example, deliberately send only one character but ask for 500; the server responds with a further 499 characters drawn from memory which, on a server running SSL, may well contain sensitive data such as usernames, passwords or even credit card details.

## Moving targets

So after decades of vulnerabilities appearing on Microsoft Windows, now they are beginning to show up in others such as Linux and OS X. Code will always contain errors and oversights and the apparent security of an operating system is as much to do with the extent to which people are interested in finding flaws. With billions of desktop, laptop and mobile devices running some version of Windows, it's a magnet for hackers as much as it is for security experts trying to find those vulnerabilities first.

Personal computers running Linux (less than 2% of all PCs) or OS X (less than 7%) are few in comparison. But two-thirds of the internet's servers are Linux/Unix-based and perhaps this is where those with malicious intent are turning their attention. And if that happens, Mac OS X may well become collateral damage.

While Apple has been fast to release patches, the danger is that users do not install the updates – as is the case with many Windows users, millions of whom run old, out-of-date and vulnerable versions of Windows and other programs. In the future, Apple will need to find its own vulnerabilities, review its own code and not leave it to the security community – which becomes a race between then protectors and the exploiters.

**Apple** **Linux** **UNIX** **Heartbleed** **Mac OS**