1030 - Offensive Malware Analysis: Dissecting OSX/FruitFly via a Custom C&C Server

Friday at 10:30 in 101 Track
20 minutes | Demo, Tool
Patrick Wardle*Chief Security Researcher, Synack / Creator of Objective-See*

Creating a custom command and control (C&C) server for someone else's malware has a myriad of benefits. If you can take over it a domain, you then may able to fully hijack other hackers' infected hosts. A more prosaic benefit is expediting analysis. While hackers and governments may be more interested in the former, malware analysts can benefit from the later

FruitFly, the first OS X/macOS malware of 2017, is a rather intriguing specimen. Selectively targeting biomedical research institutions, it is thought to have flown under the radar for many years. In this talk, we'll focus on the 'B' variant of FruitFly that even now, is only detected by a handful of security products.

We'll begin by analyzing the malware's dropper, an obfuscated perl script. As this language is rather archaic and uncommon in malware droppers, we'll discuss some debugging techniques and fully deconstruct the script.

While this dropper component also communicates with the C&C server and supports some basic commands, it drops a binary payload in order to perform more complex actions. However, instead of fully reversing this piece of the malware, the talk will focus on an initial triage and show how this was sufficient for the creation of a custom C&C server. With such a server, we can easily coerce the malware to reveal it's full capabilities. For example, the malware invokes a handful of low-level mouse & graphics APIs, passing in a variety of dynamic parameters. Instead of spending hours reversing and debugging this complex code, via the C&C server, we can simply send it various commands and observe the effects.

Of course this approach hinges on the ability to closely observe the malware's actions. As such, we'll discuss macOS-specific tools that can monitor various events, and where necessary detail the creation of custom ones (e.g. a 'mouse sniffer' that locally observes and decodes commands sent from the malware to the OS, in order to control the mouse).

While some of this talk is FruitFly and/or macOS specific, conceptually it should broadly apply to analyzing other malware, even on other operating systems :)

Patrick Wardle

Patrick Wardle is the Chief Security Researcher at Synack, and founder of Objective-See. Having worked at NASA and the NSA, and well as presented at many security conferences, he is intimately familiar with aliens, spies, and talking nerdy. Currently, Patrick's focus is on automated vulnerability discovery, and the emerging threats of OS X and mobile malware. In his personal time, Patrick collects macOS malware and writes free macOS security tools.

@patrickwardle, objective-see.com

#defcon25/by_track/101/Friday #defcon25/By_Day/_Friday