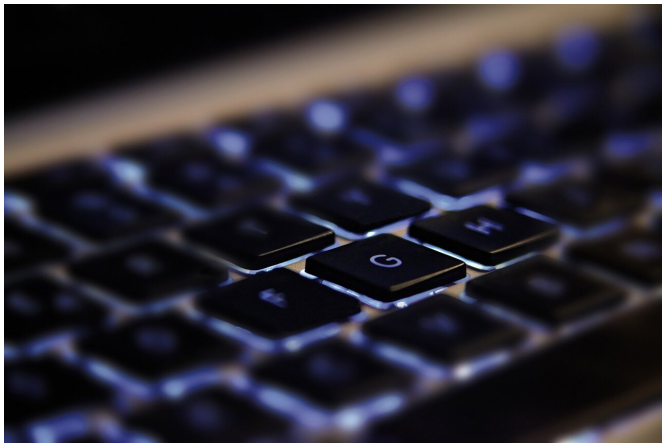
Red Canary researchers find evidence of malware on 30,000 infected Apple computers

22 February 2021, by Bob Yirka



Credit: Pixabay/CC0 Public Domain

A team of researchers at security firm Red Canary has found evidence of a new kind of malware infecting Apple brand computers. They claim on their website that they have found evidence of the malware, which they have named Silver Sparrow, infecting up to 30,000 Mac computers.

Just last week, security researcher Patrick Wardle reported that he had found an instance of malware that was targeting Apple computers running the M1 chipset. In that instance, the malware was an adware-type web browser extension called GoSearch22—in this new finding by Red Canary, the malware runs on the macOS (including M1 chipset machines) using a LaunchAgent to allow it to persist on a host computer.

The team at Red Canary found the malware to be unique in initial testing, mostly in the way it used JavaScript. And thus far, the malware does not appear to do anything once it installs itself on a host machine. This is worrisome, because it suggests that it is waiting for a specific event before going live.

In consulting with another security firm, Malwarebytes, the researchers found evidence of the malware infecting 29,139 Mac computers in multiple countries, mostly in the U.S., Canada, the U.K. and Europe. They also acknowledge that they do not know yet what sort of payload the malware might be set to deliver. But they suggest the malware could present a major security threat to Mac owners—they note that because it has been designed to run on all Mac platforms (including the M1 machines) and because of its far-reaching infection history and high infection rate, it could very well be poised to create problems for people whose machines are already infected and for others yet to come in the future.

They note that it appears likely that the malware could unleash a payload upon receiving a command from whoever wrote the software for it. They also note that the malware has another unique feature—it can erase itself from a host computer, a feature generally only seen in very high-end stealth software. They also note that the malware uses Amazon Web Services as well as the Akamai content delivery network to ensure that it can receive commands from the malware creator.

The team at Red Canary has outlined the known technical details of the malware on their website.

More information:
redcanary.com/blog/clipping-silver-sparrows-wings/