When ok is not ok: Security presenter talks about synthetic clicks

August 17 2018, by Nancy Owano

A warnings bypass in macOS High Sierra made news this week in security land. Think on lines such as security check-ins, where the user is asked to confirm that an app should be granted permission to do things like access contacts or location data, as noted in *9to5Mac*.

The bypass was shown by Patrick Wardle, Digita Security's Chief Research Officer. His research into invisible clicks ("synthetic" clicks) has drawn interest, and he was one of the presenters at the recent DefCon computer security conference in Las Vegas. Synthetic events are when attackers can virtually "click" objects in order to load code without user consent, said *ZDNet*.

Malcolm Owen in *AppleInsider* said software-based clicking of interface objects was a problem, and that the discovery meant synthetic clicks could work in certain circumstances. Here, let Andy Greenberg in *Wired* elucidate what the problem can be over warnings and Wardle's bypass:

The operating system gives users a choice—either allow or deny a program's access to sensitive data or features. That way, the OS sets up a checkpoint, able to halt malware while letting innocent apps through. Along comes Patrick Wardle to explore: "What if a piece of malware can reach out and click on that 'allow' button just as easily as a human."

Mike Mimoso, *Flashpoint*, also commented on Wardle's research, where "a threat actor with access to a compromised computer can interact with the user interface and control the user's mouse clicks—essentially a synthetic click—to bypass security prompts available to the user, enabling access to the keychain, load third-party kernel extensions, or authorize an outgoing network connection."

Wait, what is High Sierra? This is referring to the macOS High Sierra release of macOS, Apple Inc.'s desktop operating system for Macintosh computers.

How serious is this situation?

Paul Ducklin, *Naked Security* said, "it's more a tweak to an anti-security trick that Wardle himself found and reported last year than a brand new attack."

What could an attacker accomplish? *Ars Technica*'s Dan Goodin said, "With the ability to generate synthetic clicks, an attack, for example, could dismiss many of Apple's privacy-related security prompts."

Ben Lovejoy in *9to5Mac* said this is where "rogue code mimics a user clicking a button to grant a permission."

Malcom Owen in *AppleInsider* provided an account of what happened that led to Wardle's discovery. It happened by accident. Wardle discovered it by making a mistake while copying and pasting code for synthetic mouse clicks, as he forgot to change a flag value for an up event. After compiling the code, he discovered it allowed the synthetic click to function.

Naked Security commented on this as a "copy-and-paste programming mistake" and said it ought not to have worked, yet bypassed Apple's security checks. "This is a stark reminder that hackers and cybercrooks can succeed through dogged determination and a whiff of good luck, simply by trying things no one else had thought of before, or things that everyone else assumed would fail."

More information: Fire & Ice: Making and Breaking macOS Firewalls: www.blackhat.com/us-18/briefin … king-macos-firewalls

Citation: When ok is not ok: Security presenter talks about synthetic clicks (2018, August 17) retrieved 25 April 2024 from https://techxplore.com/news/2018-08-synthetic-clicks.html