INVISIBLE MOUSE CLICKS LET HACKERS BURROW DEEP INTO MACOS

JEROME CID/ALAMY

ONE WAY OPERATING system developers try to protect a computers's secrets from probing hackers is with an appeal to the human at the keyboard. By giving the user a choice to “allow” or “deny” a program’s access to sensitive data or features, the operating system can create a checkpoint that halts malware while letting innocent applications through. But former NSA staffer and noted Mac hacker Patrick Wardle has spent the last year exploring a nagging problem: What if a piece of malware can reach out and click on that “allow” button just as easily as a human?

At the DefCon hacker conference Sunday in Las Vegas, Wardle plans to present a devious set of automated attacks he’s pulled off against macOS versions as recent as 2017 release High Sierra, capable of so-called synthetic clicks that allow malware to breeze through the permission prompts meant to block it. The result could be malware that, once it has found a way onto a user's machine, can bypass layers of security to perform tricks like finding the user's location, stealing their contacts or, with his most surprising and critical technique, taking over the deepest core of the operating system, known as the kernel, to fully control the computer.

"The user interface is that single point of failure," says Wardle, who now works as a security researcher for Digita Security. "If you have a way to synthetically interact with these alerts, you have a very powerful and generic way to bypass all these security mechanisms."

Wardle's attacks, to be clear, don't offer a hacker an initial foothold on a computer; they only help a hacker's malware penetrate layers of security on an already infected machine. But Wardle argues they could nonetheless serve as powerful tools for sophisticated attackers trying to silently steal more data from, or gain deeper control of, a machine they’ve already penetrated with a malicious attachment in a phishing email or some other common technique.

Invisible Clicks

MacOS includes a feature that lets some programs, like AppleScript, generate “synthetic clicks"—mouse clicks that are generated by a program rather than a human finger—that allow features like automation and usability tools for the disabled. To keep malware from abusing those programmed clicks, however, it blocks them on some sensitive “allow” prompts.

But Wardle was surprised to discover that macOS fails to protect the prompts for things like extracting the user’s contacts, accessing their calendar, or reading the latitude and longitude of their machine, determined by which Wi-Fi networks it’s connected to. His malicious test code could simply click through prompts as easily as human.

'It's this ridiculous bypass that I found by incorrectly pasting code.'

PATRICK WARDLE, DIGITA SECURITY

Wardle has also experimented with using synthetic clicks for far more serious hacking techniques. He had previously discovered that malware could also use an obscure macOS feature called "mouse keys," which allows the user to manipulate the mouse cursor with the keyboard, to perform synthetic clicks that bypass security prompts. In a talk he gave last March at the SyScan security conference in Singapore, Wardle pointed out that Apple had overlooked the mouse key function, so that it wasn't blocked when it clicked through "allow" prompts on even highly sensitive features like accessing the macOS keychain, which contains users' passwords, and installing kernel extensions that can add code to the most powerful part of a Mac's operating system.

Apple responded by patching Wardle's mouse-key hack. But when he later tried testing ways to get around that patch, he stumbled into an even stranger bug. A synthetic click includes both a "down" command and an "up" command, which correlate to clicking a mouse and then releasing it. But Wardle accidentally copied and pasted the wrong snippet of code, so that it performed two down commands instead. When he ran that code, the operating system mysteriously translated the second "down" into an "up," completing the click. And those "down-down" synthetic clicks, Wardle discovered, aren't actually blocked when used to click on an "allow" prompt for installing a kernel extension.

"It's this ridiculous bypass that I found by incorrectly pasting code," he says. "I tripped over it because I wanted to run out and surf and I was being lazy."

If malware can use that trick to install a kernel extension, it can often exploit that added code to gain full control of a target machine. Kernel extensions—like drivers in Windows—must be signed by a developer for MacOS to install them. But if an existing signed kernel extension has a security flaw, a piece of malware can install that extension and then exploit its flaw to take control of the kernel. Wardle points out that the Slingshot malware Kaspersky revealed last March, which was later revealed to be a hacking tool used by US special forces to track ISIS targets, used this exact technique.

"A lot of advanced malware really tries to get into the kernel. It's like god mode," Wardle says. "If you can infect the kernel, you can see everything, bypass any security mechanism, hide processes, sniff user keystrokes. It's really game over."

Low-Hanging Bugs

Apple didn't respond to WIRED's request for comment on Wardle's findings. Wardle admits that he didn't actually tell Apple the details of his research ahead of his DefCon talk, instead handing them an unpleasant surprise. But he argues that after he alerted the company to his earlier findings before SyScan, Apple shouldn't have left sloppy, exploitable bugs in the same security protections. "I've reported a ton of bugs to them and it doesn't seem like it's inspiring changes," Wardle says. "So let's try something else."

Of course, the pop-up prompts that Wardle's synthetic clicks bypass are still be visible to users, tipping them off to the presence of malware on their computer. But Wardle points out that malware can wait for signs of inactivity, which hint that the user might have walked away from the machine, before triggering and clicking through macOS's prompts. It can even dim the screen during those inactive moments so that those prompts aren't visible at all.

Wardle concedes that his synthetic click attacks don't exactly offer instant access to a Mac's inner sanctum. But in certain hackers' hands, they could be a dangerous tool. And he argues they're part of a repeating pattern of Apple's recent security sloppiness, from a vulnerabilty that allowed anyone to gain privileged access to a Mac simply by typing "root" as their username to a bug in Apple's file system software that revealed users' passwords when someone merely asks for a password hint.
"We're seeing these really low-hanging vulnerabilities that keep popping up," Wardle says. "This bug is so lame in a way, but it's also very powerful. It makes me want to laugh and cry at the same time."