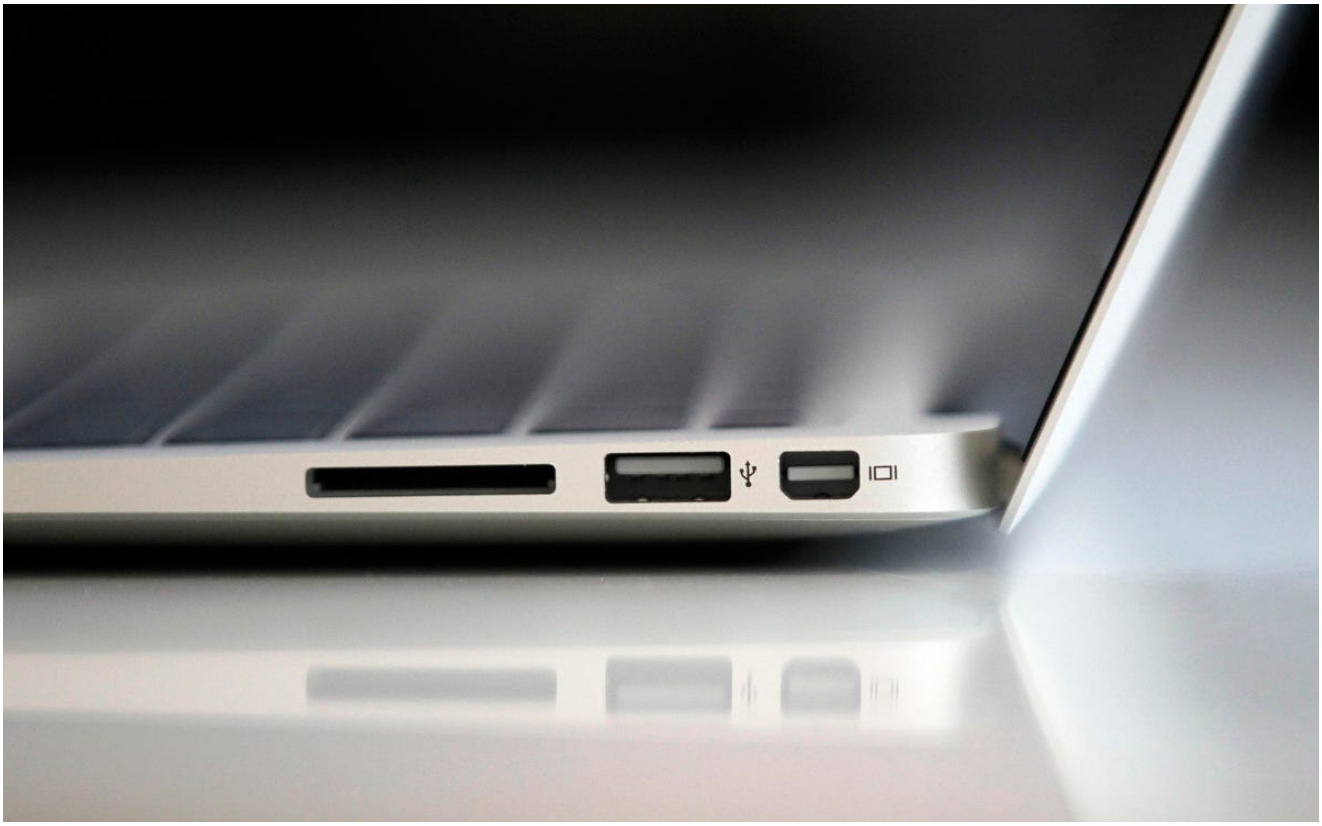
Hackers Are Exposing An Apple Mac Weakness In Middle East Espionage

forbes.com/sites/thomasbrewster/2018/08/30/apple-mac-loophole-breached-in-middle-east-hacks/

Thomas Brewster August 30, 2018



Cybersecurity
Thomas Brewster
Forbes Staff

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Aug 30, 2018,06:00am EDT|

This article is more than 3 years old.

Apple Mac Event

ASSOCIATED PRESS

Apple Macs are rarely the target of digital espionage. But in recent years, a mysterious hacker crew called WindShift has targeted specific individuals working in government departments and critical infrastructure across the Middle East. And they're exploiting weaknesses believed to affect all Apple Mac models.

That's according to United Arab Emirates-based researcher Taha Karim, who said the targets were located in the so-called Gulf Cooperation Council (GCC) region. That encompasses Saudi Arabia, Kuwait, the UAE, Qatar, Bahrain and Oman. The targets were sent spear phishing emails containing a link to a site run by the hackers. Once the target clicked on the link, an attack would launch, the eventual aim of which was to download malware dubbed WindTale and WindTape.

Karim, a researcher at cybersecurity company DarkMatter, said the attackers had found a way to "bypass all native macOS security measures." Once they'd penetrated those defenses, the malware would exfiltrate documents of interest and continuously take screenshots of the victims' desktops. The attacks have been ongoing from 2016, through to today, the researcher added.

Karim declined to say what kinds of critical infrastructure had been targeted and would name neither specific countries nor victims. He's presenting his full findings on Thursday at the Hack In The Box conference in Singapore.

The Mac hack explained

DarkMatter said the hackers' web page would attempt to install a .zip file containing the malware. Once the download was completed, the malware would attempt to launch via what's known as a "custom URL-scheme." That's not as complex as it sounds. Developers can create their own URL scheme so that specific parts of their app will open when a link is opened. For instance, imagine a link that opens a Maps application that takes the user to a specific place and instantly provides directions from their location. That requires a custom URL scheme to be registered on the computer or smartphone first to work as it does.

Here's what happens in the case of the WindShift team's malware: First, a user visits a website that tries to install a .zip file. Inside is the malware. The Apple Safari browser will automatically unzip the file and macOS will automatically register the malware's chosen URL scheme. The same website from which the malware was downloaded will then make a request, via the now-registered custom URL scheme, to launch the malicious software. The attackers are relying on victims to keep the site live once they've installed the .zip file, long enough for the malware to work. The malware is then run by the operating system to handle the custom URL scheme's request. From there, WindTale and WindTape can silently start pilfering documents and taking screenshots.

Looking across major desktop operating systems, the problem may be unique to Apple. This same method wouldn't have worked on Windows, according to Karim, who said Microsoft had added extra protections to prevent such attacks.

There are some barriers the WindShift hackers had to overcome to successfully infect their targets. The latest versions of Safari will show a prompt asking the user to confirm they want to run those custom URL schemes. And if the user clicks allow, there will be another request

from Apple's Gatekeeper security feature, which will again ask the user if they really want to install the files.

Those might seem like decent preventative measures, but as Karim said, the attacker can control much of what's inside the Safari alert to make their malware appear innocuous. Wardle, who tested the attack method for *Forbes,* played around with prompts, so that one asked: "Do you want to allow this page to open Google?" Another replaced "Google" with a smiley face emoji. Karim suggested Mail.app might dupe the average user.

Mac hacker Patrick Wardle replicates an attack that tries to trick users into downloading malware. ... [+] In this demo, the malware's name has been turned into a smiley face.

Patrick Wardle

There's another potentially troublesome aspect to the WindShift hacks. If the attackers or their victims copied the malware so it was shared across a network, all users could have the malicious custom URL scheme automatically added to their Apple Macs. "Attackers could use this simple technique to move laterally inside the network resulting in the infection of a larger number of Mac computers," Karim added.

Karim said he'd contacted Apple. The company told him the issue was closed from its perspective. "But it's unclear whether any specific remediation action was taken," he added.

At the time of publication, Apple hadn't responded to a request for comment.

Follow me on Twitter. Check out my website. Send me a secure tip.

Thomas Brewster