your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

Beware of Buying Used or Jailbroke Cellphones

Sometimes that 'Good Deal' isn't as 'Good' as You Think!

Many people are tired of paying high prices from the big cell phone providers, so they go out and buy a used or new phone that has been 'Jailbreaked' to save money.

It's only been a few weeks since a researcher released an iOS exploit that allowed outsiders to jailbreak an iPhone, and the scammers leverage the tool to try commandeer victims' devices and take over your mobile handset.

Last month, a researcher known as @axi0mx published checkm8, a series of technical instructions that enable users to remove restrictions imposed on their iPhone by Apple or telecommunication companies. Now, after weeks of publicity around checkm8, attackers have launched a malicious website that masquerades as a legitimate page, only to launch a hacking tool that tries to take over an affected device.

Cisco's Talos threat intelligence crew on Tuesday said they found checkrain[.]com, a site meant to look like an off-shoot of checkra1n, a legitimate project that researchers can use to modify their iPhone's processes and jailbreak their device. Instead of allowing that, though, the malicious checkrain site encourages visitors to download an application that clicks on risky advertisements and installs iOS video games. All the while, it looks like the true checkra1n installation process is underway.

"The chain used in this processes through several ad-tracking, verification, geolocation and, finally, campaign delivery," wrote researchers Warren Mercer and Paul Rascagneres.

The fake checkrain page downloads a slot machine game called "POP! Slots," and instructs the user to use the app for seven days to guarantee the jailbreak works.

"This is obviously nonsense—the user will merely provide more interactive sessions throughout the gameplay, which may result in additional revenue for the attack," the Talos blog post goes on.

It's not clear who is behind this effort, or how much money they made from fraudulent clicks But it's become common for scammers to create apps that try to capitalize off another's popularity, only instead of providing what they promised, directing users to a series of landing points that monetize their connection.

The checkm8 maneuver works on devices with Apple chipsets from A5 to A11, which have powered iPhones and iPads since 2011. Apple's newer chip models—A12 and A13—are not affected. It works by exploiting flaws in the bootrom process, allowing users to more control over their device while also removing some of the safeguards meant to keep hackers out. Take heed...a 'Good' deal isn't always 'Good' for you or your privacy!

Read More: https://www.cyberscoop.com/ios-jailbreak-checkm8-app-fraud/

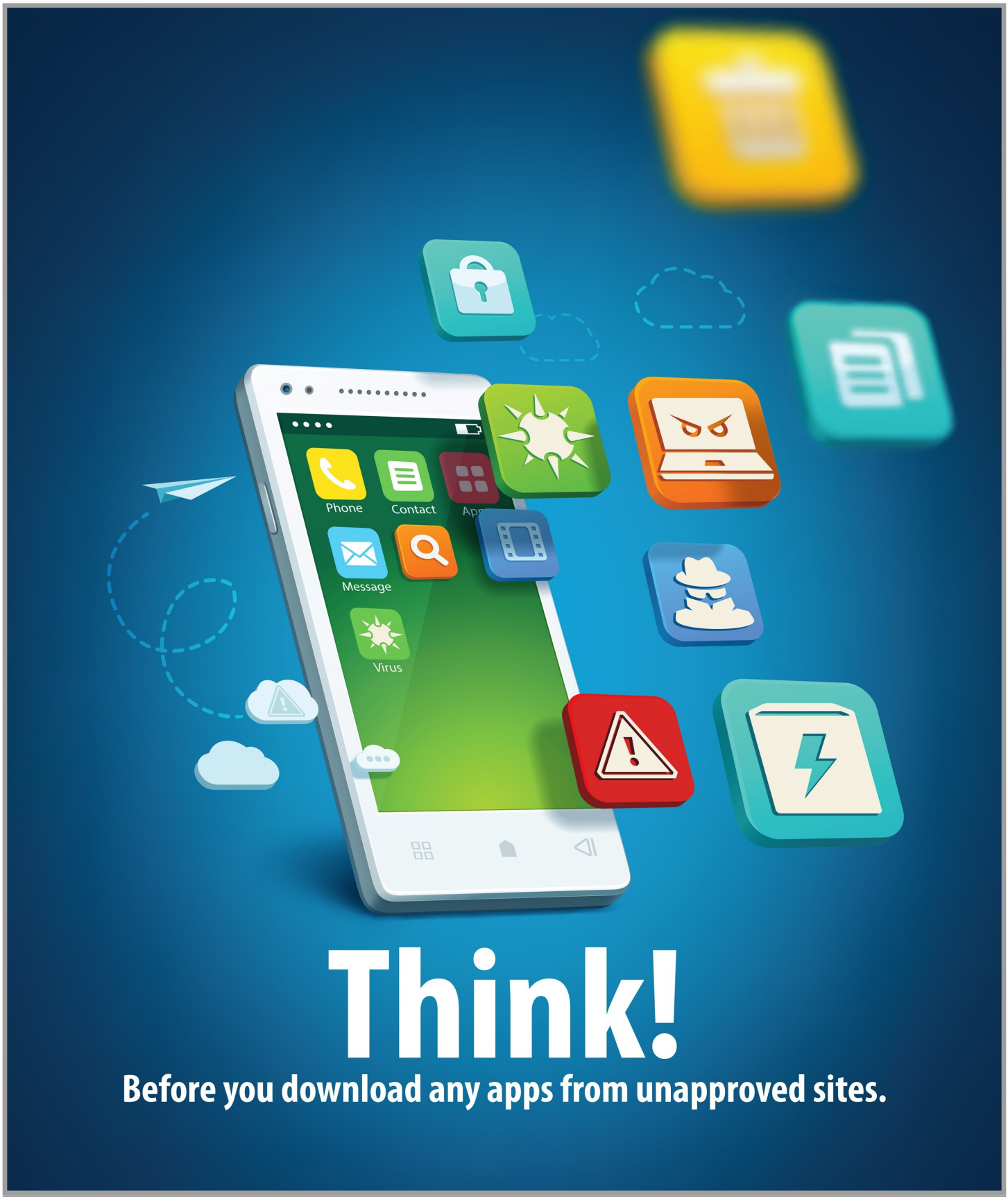
Scammers are using Play Store apps to serve ads that nobody can escape— Cyber Scoop Reports

A sneaky network of more than 100 Android applications is allowing fraudsters to make money by pushing pervasive advertisements to users' devices, according to new cybersecurity findings. The device owners aren't the real victims, even though they're being exploited. The constant stream of ads, some miniscule and others loud and inescapable, are leveraging victims' phones as conduits for scammers to rip off companies' marketing dollars. More than 100 applications with some 4.6 million downloads from the Google Play Store include malicious code that enables the bogus advertising network, according to research published Thursday by the bot detection firm White Ops.

Android subscribers who downloaded these apps, some of which still existed on the Play Store at press time, believed they were installing programs that would predict their fortune, play games, take selfies or remove bugs. But the apps also abused their access to inundate the devices with advertisements that could be tracked but often couldn't be seen. Most of the apps first appeared in the Play Store in mid-September and, while duplicitous apps are all too common, these findings are the latest evidence that ad fraud campaigners are investing in new ways to maintain access on affected devices. "The code has aggressive persistence mechanisms," said Inna Vasilyeva, a threat intelligence analyst at White Ops. "Once we started looking into one application, we could see that it was related to what a lot of other apps were doing." This malicious activity was made possible by two code libraries, which White Ops dubbed Soraka and Sogo. The apps also use AppsFlyer, a framework for mobile attribution and marketing analytics. It's a combination that enables the apps to remove a background notification service meant to prohibit fraud activity when a phone is powered down, and schedule ads to start appearing seconds after those anti-fraud measures are disabled.

The paychecks available to ad fraud scammers are large enough to encourage the research and development of new malware and evasion techniques, which then can be repurposed to carry out more traditional forms of cybercrime. U.S. prosecutors accused one fraud ring of stealing roughly $30 million over a span of years, in part by commandeering a network of 1.7 million hacked computers. In this case, White Ops researchers cited Best Fortune Explorer, an app still lurking on the Play Store at press time, as one of the most nefarious. The game promises to predict user's future, such as when they will meet their true love and if they will be promoted at work. In fact, based on White Ops' code analysis, the app sends a nonstop stream of ads that many of the thousands of negative reviewers compared to a virus. A representative from Google's Play Store acknowledged questions about White Ops' findings to CyberScoop before press time. The app, which has 170,000 downloads, was published on Sept. 9 and shares many characteristics with the larger Soraka network, White Ops determined. Researchers from throughout the security community in recent months have tightened their focus on mobile apps that promise one thing only to do something very different. Google removed more than 100 adware-laced apps from the Play Store in response to findings from Trend Micro, while Wandera also has uncovered gaming apps capable of stealing users' credentials.

Read More: https://www.cyberscoop.com/play-store-adware-white-ops/



Pay attention to what you download. Who is the manufacturer? How many reviews does it have? (few or no reviews is a clear sign to stay away from an app!) What permissions is the app requesting? Although the 'app stores' are the best place to download your apps, they are not always 100% secure. Pay attention each time you download a new app and perform some simple checks to help keep malicious applications off your phone.