The Rise of "Zero-Click" Hacks Provides Cautionary Tale when Using Personal Devices for Business Use

Related Attorneys

Christopher L. Ingram

John L. Landolfi

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 3.8.2022

A new threat, known as "zero-click" hacks, is emerging from well documented state-sponsored spyware schemes. While users have grown accustomed to guarding against phishing attacks, the latest zero-click compromises enable threat actors to gain unauthorized control of smart phones and computers without the user's knowledge – no malicious link or attachment is required. Instead, hackers exploit security flaws in applications and operating systems – such as Apple Inc.'s iOS and Google's Android – to breach a device without any action by the victim. Once in control, hackers can install spyware capable of stealing data, listening to calls, watching through cameras, and tracking the user's location.

For example, a zero-click hack was used to compromise smart phones over the popular communication application WhatsApp. When video calls are normally placed through the application, the recipient's WhatsApp reads metadata in order to display certain call information to the recipient. A previously unknown flaw in the application enabled a threat actor to load malicious code into a video call's metadata such that when the recipient's WhatsApp read an incoming video call's metadata, the malicious code was launched on the recipient's phone. The malicious code could be deployed even if the recipient did not answer the call. Once loaded, the spyware operated in the background of the device, providing the threat actor access the device's information – from text messages to webpages the user opened. Moreover, this spyware was virtually undetectable to the average user. WhatsApp eventually provided a security patch to remediate this vulnerability.

The reality is that businesses are faced with increasing state-sponsored cyber security threats, such as zero-click hacks. Companies can take practical steps to manage these threats. For example, companies may re-evaluate whether personnel should be permitted to use personal devices for work purposes whenever they have access to sensitive or regulated company data, particularly during international travel. Among other things, companies should also take steps to ensure that any device that processes sensitive or regulated data is routinely

updated pursuant to a security patch management policy.

For more information, please contact John Landolfi, Chris Ingram, Jordan Patterson, or your Vorys attorney.