DIGITAL FORENSICS - ARTICLE ON MOBILE DEVICE MALWARE

CNBC.com, Sunday, 9 Mar 2014 | 11:24 AM ET

YOUR APPLICATIONS MIGHT BE SPYING ON YOU, OR WORSE...

http://www.cnbc.com/id/101477801#
Cadie Thompson | @CadieThompson

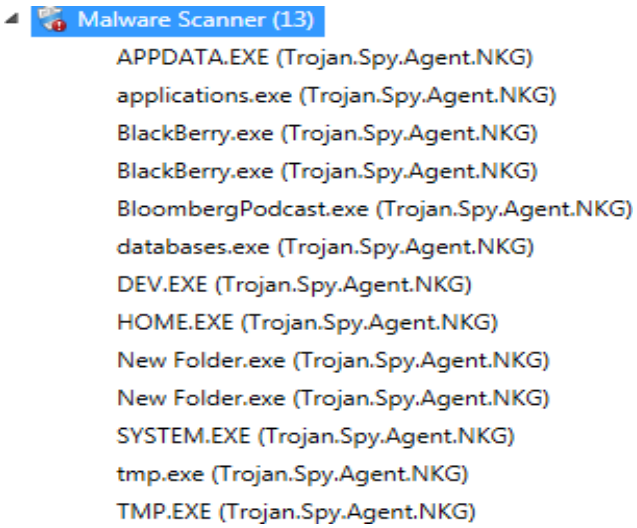
APP PRIVACY CONCERNS: YOUR SMARTPHONE APPLICATIONS MIGHT BE SPYING ON YOU

A growing number of malicious mobile applications are doing everything from tracking people without their permission to completely taking over their security experts said Saturday at South by Southwest Interactive during a mobile security panel.

"We discover a large quantity of malicious applications every day at an alarmingly growing rate," said Grayson Milbourne, a security intelligence director at the mobile security firm Webroot, in an interview with CNBC.

"Last year, we had roughly 250,000 malicious applications in our depository. We have over a million today." Consumers have shifted to mobile, cyber criminals have as well, and are developing applications that can infiltrate a person's phone to collect data to sell on the black market, Milbourne said.

EXAMPLE OF A MOBILE DEVICE RESULT AFTER BEING SCANNED FOR MALWARE



Some malicious applications do this by "rooting" a device, which means the app completely takes over the smartphone's operating system. Usually, when an app wants access to a user's information--like a user's contact list-- it must request permission, but a rooted device gives the app access to everything on a smartphone without the user's knowledge, Milbourne explained.

"That's the trick, you can't tell once a device has been rooted. It will take advantage of an exploit and you will have no idea that has taken place," he said. "They have the ultimate permission."

But a device doesn't need to be rooted to be dangerous. One way applications can take your information is by asking for permission to access a user's data that it doesn't need access to, said Erich Stuntebeck, the director of mobility research at Airwatch, in an interview with CNBC. For example, if a person downloads a flashlight app, it doesn't need permission to access your contacts or microphone. "The scariest thing is applications that request excessive permissions—they appear and originally act completely benign," he said. "You install it and it can access everything. It may not do anything with that access at first. But once you give it those permissions it has access and then there could be an update pushed out in future that could take advantage of those permissions. And your phone can be turned into a full-fledged spy phone."

So even though the hypothetical flashlight app didn't access, say, your microphone at first, it might eventually take advantage of that permission to spy on you later, he explained. "All this data that's on your phone, your contact list, your location, who you are emailing, who you are calling, this is all worth money to folks on some dark corner of the Internet," Stuntebeck said during the panel. There are a few things people can do to help protect their smartphone from becoming a spying device. First, be careful where you download applications, experts said. Don't download applications on third party sites, they cautioned. Also, read the permissions you give an application when you download it and if something looks suspicious, don't download it. People can also buy mobile security software for their phones that will scan applications for suspicious behaviour and will block users from dangerous mobile web browsing.

"It's your data, it's your content, it's your conversations, it's your location, it's your behavior, it's your reputation, it's all these things," said Alan Murray, the senior vice president of product at Apperian, during the panel. "In the 21st century these (smartphones) are our avatars, they represent everything you are."

Our associate company Dynamdre can assist in mobile device investigations to gather information from mobile devices which may contain infected and malicious data. Please visit www.dynamdre.co.za and contact Dynamdre direct for further information and assistance.