GlobalResearch
Center for Research on Globalization

US Government Planting Malicious Software On Your Phone, So It Can Bypass Encryption and "See What You're Doing"

Spy Agencies Are Intentionally Destroying Digital Security. Inventor of Antivirus Sofware:

By Washington's Blog
Global Research, April 15, 2015
Washington's Blog

Region: USA
Theme: Intelligence, Police State & Civil Rights

Top computer and internet experts say that NSA spying breaks the functionality of our computers and of the Internet. It reduces functionality and reduces security by – for example – creating backdoors that malicious hackers can get through.

Remember, American and British spy agencies have *intentionally* weakened security for *many decades*. And it's getting worse and worse. For example, they plan to use automated programs to infect millions of computers.

Smart Phones Vulnerable to Spying

We documented in 2013 that smart phones are very vulnerable to spying:

> The government is spying on you through your phone ... and may even remotely turn on your camera and microphone when your phone is off.
>
> As one example, the NSA has inserted its code into Android's operating system ... buggingthree-quarters of the world's smartphones. Google – or the NSA – can remotely turn on your phone's camera and recorder at any time.
>
> Moreover, Google knows just about every WiFi password in the world ... and so the NSA does as well, since it spies so widely on Google.
>
> But it's not just the Android. In reality, the NSA can spy on just about everyone's smart phone.
>
> Cell towers track where your phone is at any moment, and the major cell carriers, including Verizon and AT&T, responded to at least 1.3 million law enforcement requestsfor cell phone locations and other data in 2011. (And – given that your smartphoneroutinely sends your location information back to Apple or Google – it would be child's play for the government to track your location that way.) Your iPhone, or other brand of smartphone is spying on virtually everything you do (ProPublica notes: "That's No Phone. That's My Tracker"). Remember, that might be happening even when your phone is turned off.
>
> The NSA has gathered all of that cellphone location information.

"Encryption Doesn't Matter In a World Where Anyone Can Plant Software On Your Phone and See What You're Seeing"

John McAfee *invented* commercial antivirus software. He may be a controversial and eccentric figure ... but the man knows his technology.

Earlier this month, McAfee told security expert Paul Asadoorian that encryption is dead. Specifically, he said:

- Every city in the country has 1 to 3 Stingray spy devices ... Bigger cities like New York probably have 200 or 300
- When you buy a Stingray, Harris Corporation makes you sign a contract keeping your Stingray secret (background here and here)
- Stingray pushes automatic "updates" – really malicious software – onto your phone as soon as you come into range
- The software – written by the largest software company in the world – allows people to turn on your phone, microphone and camera, and read everything you do and see everything on your screen
- Encryption doesn't matter in a world where anyone can plant software on your phone and see what you're seeing. Protecting transmission of information from one device to the other doesn't matter anymore ... they can see what you see on your device
- There are many intrusions other than Stingray. For example, everyone has a mobile phone or mobile device which has at least 10 apps which have permission to access camera and microphone
- Bank of America's online banking app requires you to accept microphones and cameras. McAfee called Bank of America and asked why they require microphones and cameras. They replied that – if you emptied all of the money in your account and said "it wasn't me", they could check, and then say:

Well, it certainly looks like you. And it certainly sounds like you.

- In order to do that, B of A's app keeps your microphone and camera on for a half hour *after* you've finished your banking
- In addition, people can call you – and have you call them back – and plant software on your phone when you call them back

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Washington's Blog