

MUST READ Find a zero-day exploit to hack IOS 9 and win a \$1m prize

China spies on airline passengers with IMSI-catchers

September 23, 2015 By [Pierluigi Paganini](#)



The popular expert John McAfee claims passengers with four Chinese airlines are spied with the IMSI-catchers technology by the Government of Beijing.

The former owner of McAfee security firm, John McAfee was always known to have made some controversial comments in the IT industry, but also to have good sources that let him get precious information at first hand. This time in his most recent article, he talks about the ability of the Chinese government to spy on four highly renowned airlines costumers.

John McAfee has never revealed the names of the airlines and never explained how he got this information, but he provided details on the tactic behind the cyber espionage campaign.



First, he got an Android software that had the capability to detect “man in the middle attacks by devices that emulate legitimate cell phone towers, to hundreds of international travelers flying with four highly renowned airlines”.

The software tries to detect anomalies in the [IMSI-catchers](#) (International Mobile Subscriber Identity), something that manufacturers can’t hide.

The next question is, but what is an IMSI-catcher?

“IMSI-catchers are devices that emulate cell phone towers. They trick our smartphones into believing a cell tower suddenly appeared in close range and entices our phones to connect through it.”

If your mobile is caught by any IMSI-catchers, you are in trouble. Once you are connected to the fake cell tower a man-in-the-middle attack is performed, “the IMSI-catcher analyses our configuration and “pushes” the necessary software into our smartphones in order for some third party related to the IMSI catcher to take control.”

If you are interested in more details on this technology give a look to the post [“StingRay Technology: How Government Tracks Cellular Devices”](#) where I provided detailed information on IMSI-catchers and similar devices.

The use of IMSI-catchers is well-known and documented, but it’s alarming that is being used by airlines controlled by the Chinese government.

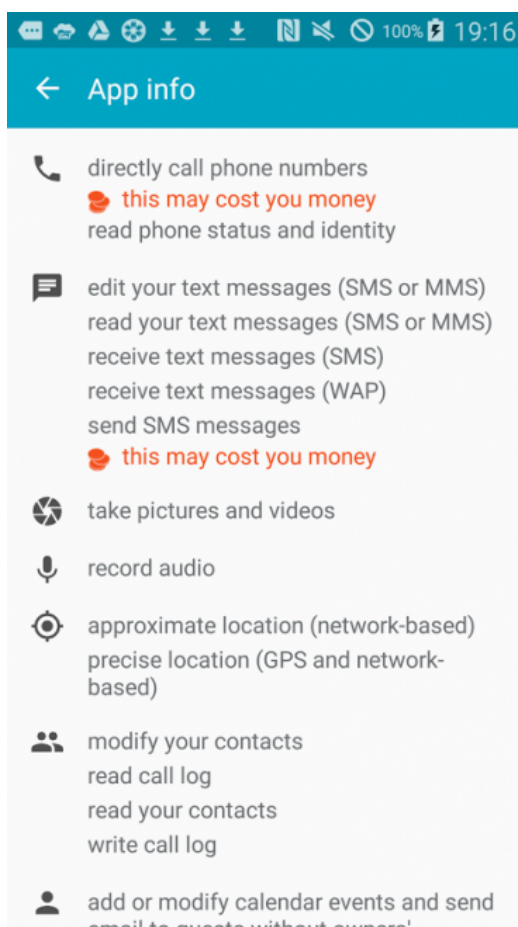
The method used by the airlines to control the passengers is simple as effective as reported by the [International Business Times](#), the airlines use the IMSI-catcher to compromise traveler’s devices when it is attempting to connect to the onboard Internet.

“In every case where an international traveler with these four airlines attempted to connect to the

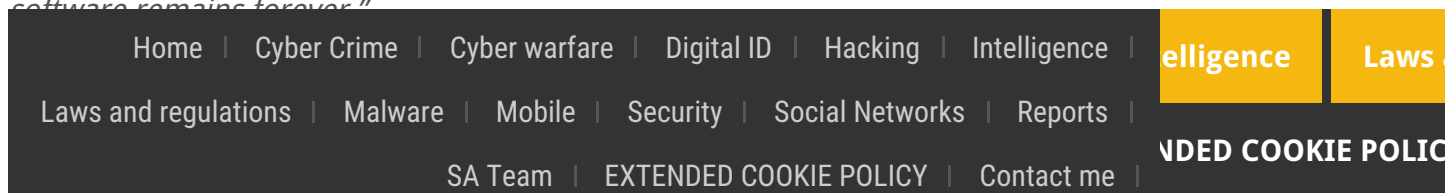
onboard internet, a module was pushed to the connecting smartphone that surreptitiously turned on the 3G or 4G communications (without displaying the corresponding icon). From that point, an onboard IMSI-catcher attempted to connect to the phone. There was a 100% success rate."

After this step, it will be determined if your mobile have already installed an Android APP called "Silent Logging", if not the application will be pushed to your device.

"Silent Logging" has the purpose of spying on you and uses the following permissions:



"After Silent Logging is activated, a spyware app is downloaded to the users' smartphone that utilises the Silent Logging app, unless the phone is "physically wiped" by the manufacturer, this software remains forever."



Once you have this spyware installed your device will available for the government to check on you, reading emails, SMS, recording videos, voice,etc etc, and all is sent to China.

The alleged espionage activity operated by the Chinese Government through the IMSI-catcher technology is alarming, and should be taken seriously.

About the Author Elsieo Pinto

Elsio Pinto (@high54security) is at the moment the Lead McAfee Security Engineer at Swiss Re, but he also as knowledge in the areas of malware research, forensics, ethical hacking. He had previous experiences in major institutions being the European Parliament one of them. He is a security enthusiast and tries his best to pass his knowledge. He also owns his own blog McAfee Security Engineer at Swiss Re, but he also as knowledge in the areas of malware research, forensics, ethical hacking. He had previous experiences in major institutions being the European Parliament one of them. He is a security enthusiast and tries his best to pass his knowledge. He also owns his own blog <http://high54security.blogspot.com/>

Edited by **Pierluigi Paganini**

(**Security Affairs** – IMSI-catchers, cyber espionage)

Share it please ...        

Share this:

 Email  Twitter 111  Print  LinkedIn 159  Facebook 65  More

 [Breaking News](#) [Cyber Crime](#) [Hacking](#) [Intelligence](#) [Laws and regulations](#) [Security](#)

SHARE ON

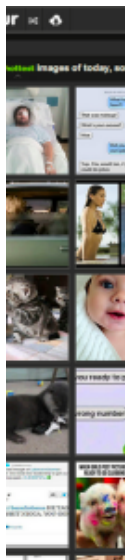


This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish. [Accept](#) [Read More](#)



Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications

MORE S



Targete
8Chan e
Recently
discover
allowed t
into an ir

in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".



PREVIOUS ARTICLE

**Targeted attacks on 4Chan and 8Chan
exploited bot code in Imgur**

NEXT ARTICLE

**National Encryption Policy draft,
everyone is under strict surveillance**



Promote your solution on Security Affairs

Promote your
solutions on
Security
Affairs...
contact us!



Copyright Security Affairs by Pierluigi Paganini - All Right Reserved.