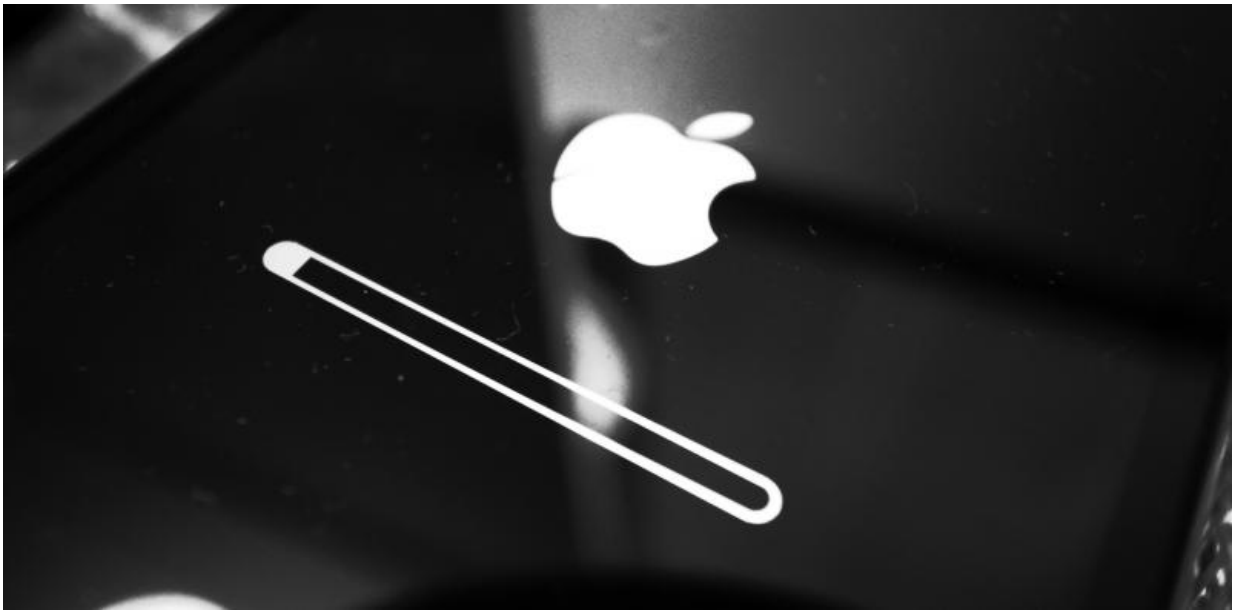
iPhone hack attack shows why we need to rein in the trade in spyware

September 16 2016, by Robert Merkel



Apple didn’t know about the vulnerability until the iPhone hack. Credit: Flickr/Toshiyuki IMAI, CC BY-SA

Downloading security updates for computers and mobile devices is a regular routine for most of us.

But not all such updates are created equal. Apple's recent iOS 9.3.5 update (and a related update to parts of OS X) was one of the more significant in recent memory.

The update fixed three security flaws which, used in combination, could give an attacker full control over an iPhone if the phone's user clicked on a malicious link.

The discovery of these security flaws brought to light a relatively new, low-profile and ethically questionable business: selling potent hacking tools, and information about security flaws that make them effective, to government agencies and private companies around the world.

Zero-day exploits – a hacker's wild card

In the world of information security, a vulnerability is a flaw in an IT system with security implications. A zero-day vulnerability is simply one that is unknown to the developers of an IT system. This means there is no fix available for the it.

An exploit is a computer program that takes advantage of one or more vulnerabilities to make an IT system to do something its administrator didn't intend it to do.

A zero-day exploit is an exploit that uses an zero-day vulnerability. If an zero-day exploit is in the hands of an attacker, there is little a user or system administrator can do to stop them.

Exploits vary greatly in the scope of things they enable an attacker to do to a system. The most potent exploits are "root" exploits, which give an attacker complete control over the system.

Similarly, exploits vary in the ways that they can be delivered. A remote exploit is one that can be transmitted to the target device over a network.

The most insidious remote exploits happen without any user involvement, but even remote exploits that require tricking a user to

click on a link, for instance, are often effective.

Spying on a human rights activist

The vulnerabilities in iOS came to light when an internationally recognised Emirati human rights activist, Ahmed Mansoor, received an odd-looking text message on his iPhone.

Mansoor was sufficiently sceptical to forward the message to security researchers, who investigated the message and discovered the exploit and its origins. Detailed reports are available from the researchers at Citizen Lab and Lookout Security.

The attempted attack against Mansoor's iPhone was extremely potent. It used a combination of three zero-day vulnerabilities that were unknown to Apple and would have given the attackers complete control over his iPhone and the data on it.

It was sent to his phone as a text message. Its one weakness was that it required that Mansoor actually click on the malicious link in that message. It is the first known such attack against the iPhone.

NSO Group, spyware exporters extraordinaire

According to Citizen Lab researchers, the software used to target Mansoor's iPhone was probably the work of NSO Group, an Israel-based company that is reportedly American-owned.

The Citizen Lab report on the Mansoor case says:

The high cost of iPhone zero-days, the apparent use of NSO Group's government-exclusive Pegasus product, and prior known targeting of

Mansoor *by the UAE government provide indicators that point to the UAE government as the likely operator behind the targeting.*

It says the same NSO Group software was also used to target journalists in Mexico, and had also been used in Kenya.

Israeli newspaper YnetNews reports that the Defense Export Controls Agency (DECA) granted the NSO Group a license to sell its espionage program, Pegasus, to a private company in an Arab state, despite some strong objections.

The news report goes on to say that Foreign Ministry officials stress the NSO Group was not involved in any data breach itself.

The spyware bazaar

NSO Group is but one of a number of companies domiciled in wealthy American-allied democracies offering similar hacking tools to government agencies, including undemocratic governments known for systematic human rights violations.

One such company, Italy-based Hacking Team, was itself hacked in 2014. Its customer list was leaked to media outlets, and included the Sudanese and Saudi Arabian governments.

As well as the trade in complete spyware products, another group of companies trade in information about zero-day vulnerabilities. One company, Zerodium, has even posted a "reward list", indicating what it will pay for different zero-day exploits against different software platforms. Apple iOS exploits can fetch up to US$500,000.

Zerodium claims to have purchased a zero-day remote exploit against the iPhone, similar in its effects to the NSO Group hack, in November

2015.

It is unknown whether the vulnerabilities used by the exploit (if it indeed exists) are common to the NSO Group hack, and therefore whether it still works on iOS 9.3.5 and 10.

Zerodium's client list is known only to Zerodium and the governments that permit it to operate. But spyware vendors such as NSO Group need a steady supply of exploits for their tools to remain functional, so they would be plausible customers.

Leaving the rest of us exposed

Police forces and intelligence agencies do have legitimate reasons for wanting to get covert access to IT systems. But the current trade in hacking tools and zero-day vulnerabilities should, in my view, be drastically reined in.

First, Western democracies are far too willing to permit the sale of these tools to undemocratic governments that use them to spy on political opponents.

Second, by stockpiling and exploiting vulnerabilities rather than assisting software developers to fix them, this trade leaves the rest of us unprotected if other parties discover and exploit the same zero-days.

While core government defence and intelligence infrastructure might get its own, secret protection against such attacks, there are a broad range of other targets who are potentially at risk of highly sophisticated attacks, even by state-sponsored hackers, and do not have the benefit of such protection.

Russian state-sponsored hackers, for instance, have been accused of

attacking high-profile non-government organisations, such as the organisational wing of the US Democratic Party, and even the World Anti-Doping Agency (WADA).

The WADA hack was apparently the result of spearphishing and probably did not involve use of a zero-day exploit. But zero-days could easily be used for similar attacks.

'NOBUS' for the NSA, but not for the private sector

The US government's own hacking agency, the National Security Agency, reportedly has a "Nobody But Us" policy that guides a decision whether to reveal vulnerabilities it finds to software developers, or keep them secret for exploitation.

As former NSA director Michael Hayden put it:

If there's a vulnerability here that weakens encryption but you still need four acres of Cray computers in the basement in order to work it you kind of think "NOBUS" and that's a vulnerability we are not ethically or legally compelled to try to patch – it's one that ethically and legally we could try to exploit in order to keep Americans safe from others.

Whether the NSA is actually following the spirit of this stated policy is open to doubt.

But there is no such principle guiding the broader trade in hacking tools between private companies and governments around the world. It appears to be disturbingly close to open slather.

It's time for this to change.

This article was originally published on The Conversation. *Read the*

original article.

Source: The Conversation