MaddyFeed brings you everything you need to know about Pegasus, online privacy attacks and how you can protect your data

Every week, Maddyness curates articles from other outlets on a topic that is driving the headlines. This week, we're talking about the investigation into devices targeted by NSO Group's spyware, Pegasus, why such software needs to be regulated and how you can protect your online data from hackers.

Temps de lecture : minute

---

26 July 2021

An investigation by media organisations and Amnesty International into a huge data leak has revealed that politicians, activists, journalists and lawyers around the world have been targeted or selected using spyware sold by Israeli surveillance company, NSO Group.

Pegasus is a malware that infects android and iOS devices to enable hackers to extract data, access cameras and mics, and track the movements of the smartphone user.

The leak contains a list of over 50,000 phone numbers believed to be held by people of interest to NSO clients. Though the listing of a phone number does not reveal whether a device was compromised by Pegasus software, the project believes this signals a list of potential targets.

In forensic analysis of only a small number of phones appearing in the

data, over half had traces of the spyware. The leaked list includes a number of high-profile figures, including French President Emmanuel Macron and FT Editor, Roula Khalaf. The phone numbers selected spanned more than 45 countries across four continents, with more than 1000 numbers in European Countries.

Analysis of the leaked data by the consortium revealed at least 10 governments believed to be operating the Pegasus spyware including Mexico, Hungary, Saudi Arabia and the UAE.

Read more via *The Guardian*.

What is Pegasus and how does it work?

The software was developed by surveillance company, NSO Group and has been exported to government clients across the globe. The spyware can be used to capture data and communications, track the device and spy on users by accessing and recording calls.

NSO's software was designed to target terrorist and criminal groups but has since been deployed to as a tool to spy on dissidents, critics and reporters, as well as family members of NSO clients. Governments ties up in the allegations include Saudi Arabia, the UAE and Hungary.

The hacking process involves a fabricated link send via email or SMS which, when clicked, will deliver malicious software and compromise the device.

The software can be used to seize full control of the device's operating system, by rooting on Android devices or jailbreaking on iOS devices. Both processes remove the security controls embedded in the device operating system by hacking core elements of the system or changing the configuration. Once a device is unlocked, the hacker can use more

software to access the device’s data and functions. Throughout the entirety of the process, the owner of the device is likely to be completely unaware. Read more via *The Conversation.*

Apple is generally considered secure, but it has a major security problem, according to cybersecurity researcher

Following the data leak and investigation, doubts have been raised about the security provided by iOS devices. Forensic reports carried out by Amnesty International and verified by Citizen Lab found that even iPhones running iOS 14.6, the latest version of software update, were susceptible to hacking.

"All this indicates that NSO Group can break into the latest iPhones,” said Bill Marczak, Senior Research Fellow at Citizen Lab. “Apple has a major blinking red five-alarm-fire problem with iMessage security.”

Using the software, hackers are able to comprise iOS devices even through “zero-click” iMessage texts, meaning the target doesn’t even have to interact with the text to have their data violated.

Ivan Krstić, security-engineering chief at Apple told Insider, "Attacks like the ones described are highly sophisticated, cost millions of dollars to develop, often have a short shelf life, and are used to target specific individuals.”

"While that means they are not a threat to the overwhelming majority of our users, we continue to work tirelessly to defend all our customers, and we are constantly adding new protections for their devices and data."

Read more via *Insider.*

Spyware must be regulated

Amnesty International, alongside Paris-based non-profit, Forbidden Stories and media outlets have conducted a forensic investigation into 37 devices believed to be compromised by NSO's software. NSO has since denied what it said were “false allegations” in the project and has maintained that is does not have access to data accessed by its customers and will “investigate all credible claims of misuse.

But this is not the first time allegations have been made against the software. NSO is already battling a court case of over allegations its software was used to spy on journalists, meanwhile Whatsapp has brought forward allegations that crafted links and messages were sent to 1000 users via their platform.

Tech giants and governments can collaborate to share findings, but there is mounting pressure on Israel to monitor exports of the software, as well as all governments who buy into the software to ensure that fundamental rights to privacy are protected. Read more via *The FT.*

How can you protect your online privacy?

The risk of a breach in privacy is now new, but the threat of online privacy invasions is increasing multi-fold. It’s not just viruses we have to worry about, but spyware, malware and hacker threats. *CNBC* has compiled a list of how you can protect your data online, including investing in security suites, using two factor authentication and strong passwords as well as being alert for scams and third party account access. Read more *here*.

Article by Abby Wallace