Icaramba!
Iphone vulnerabilities compromise personal data

Innovatech

September 13, 2016

Table of contents

An innocuous text

New secrets about torture of Emiratis in state prisons `http://go.osu.edu/not_a_virus`

Icaramba! Iphone vulnerabilities compromise personal data

Initial Attack

An innocuous text

An innocuous text

New secrets about torture of Emiratis in state prisons `http://go.osu.edu/not_a_virus`

An innocuous text was sent to a human rights activist from UAE. Inside there was a link that would remotely jailbreak his Iphone. Since he had already been targeted before, he notified the security firm 'Citizen Lab'

What was vulnerable?

Icaramba! Iphone vulnerabilities compromise personal data

How it worked

What was vulnerable?

What was vulnerable?

The software was evaluated and it was determined that this link would've given access to all data accessible by the phone. It in fact incorporated three unknown vulnerabilities (also known as zero days)

Zero Day exploits

Zero day exploits/vulnerabilities are exploits that are unknown to a product creator, meaning there have been zero days to patch it

Simple explanation is simple

Zero day exploits/vulnerabilities are exploits that are unknown to a product creator, meaning there have been zero days to patch it

Who did it?

- A little-known company called 'NSO Group'
- Based out of Tel-Aviv
- Sells malware to governments

Icaramba! Iphone vulnerabilities compromise personal data

Who did it?

Who did it?

Who did it?

Who did it?

- A little-known company called 'NSO Group'
- Based out of Tel-Aviv
- Sells malware to governments

NSO Group was founded in 2010 and we're quoted as saying "we're a ghost". They give no interviews etc. It was only through tracing the servers it these exploits went through that the malware's codename 'Pegasus' was found. They sell malware to countries that often end up using the malware on journalists and political dissident

Malware for sale

]HackingTeam[

FINFISHER™
EXCELLENCE IN
IT INVESTIGATION

]HackingTeam[

An example of three companies that were/are in this business. Hacking team was based in Italy and had a major blunder when their servers were hacked and documents released

Conclusions

Security should never be assumed as there are always malicious actors and unknown vulnerabilities that present a clear danger to information.

References

Images

- Bart Iphone case-Pinterest
- Diagram of vulnerable data-Motherboard(https://motherboard.vice.com/read/government-hackers-iphone-hacking-jailbreak-nso-group)

Information

- Motherboard, Government Hackers Caught Using Unprecedented iPhone Spy Tool