# ZERO - Click Exploit

*Generally, attackers target victims through some form of social engineering, which requires user interaction like opening a malicious URL or installing a malevolent application. But what if I tell you, now hackers can attack your mobile without any user interaction. It sounds scary, right? Read on for more details…*

## What is a Zero-Click Exploit?

**Zero-click attacks**, *also known as interaction-less or fully remote attacks, bypass the need for social engineering entirely, giving threat actors the ability to take over a smartphone in real-time without any interaction with the target. This invisibility makes zero-click exploits highly coveted by exploit brokers, spyware vendors, and nation-state hackers alike.*

## How does it work?

***Zero-click attacks*** *often target apps that provide messaging or voice calling because these services are designed to receive and parse data from untrusted sources. Attackers generally use specially formed data, such as a hidden text message or image file, to inject code that compromises the device.*

## Case Study:

*According to research released on December 20, 2020, iPhones belonging to as many as 36* Al Jazeera *journalists were silently infected with malware.*

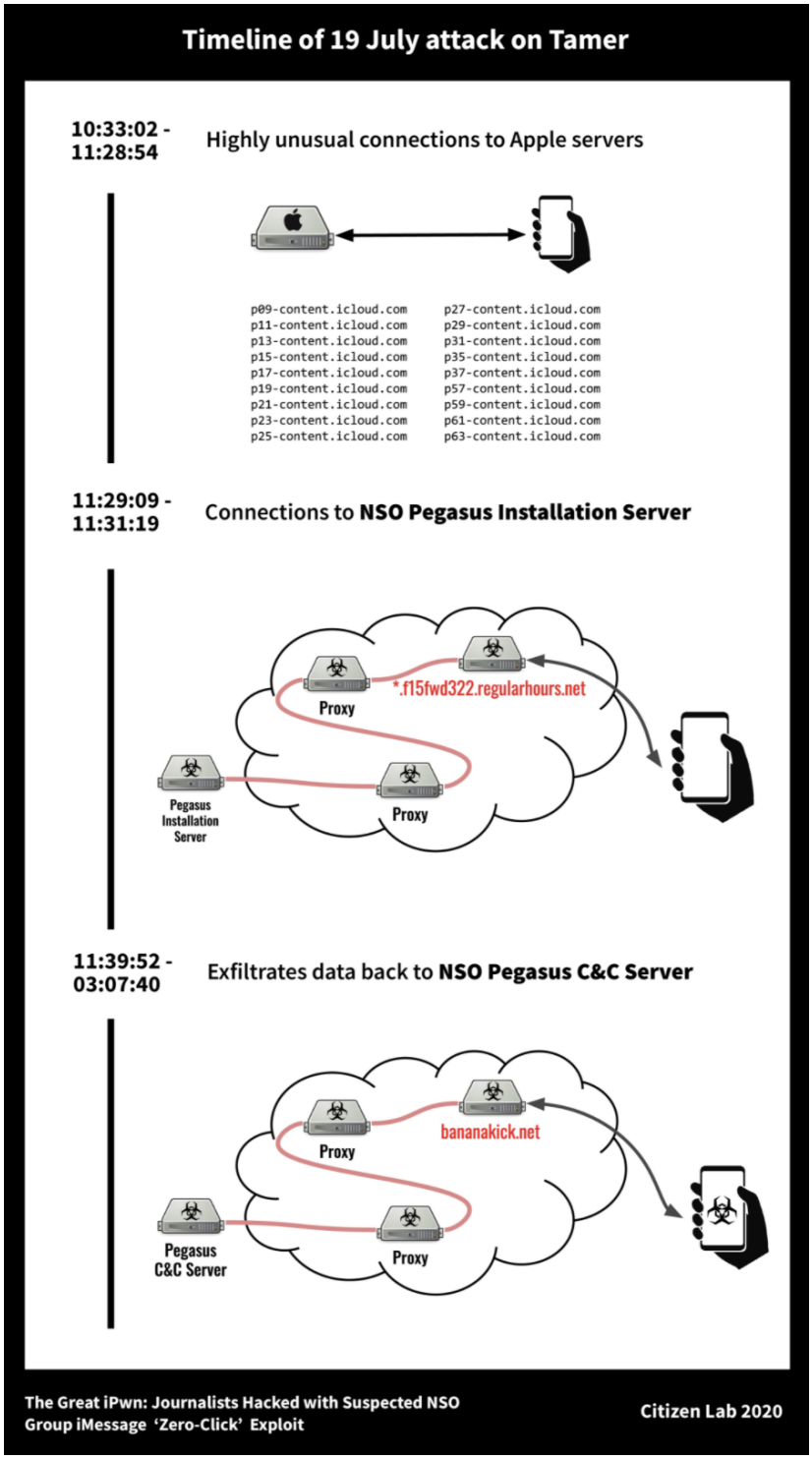
### Key Findings:

- *The phones were compromised using an exploit chain that we call* ***KISMET****, which appears to involve an invisible zero-click exploit in iMessage. In July 2020, KISMET was a zero-day against at least iOS 13.5.1 and could hack Apple's then-latest iPhone 11*

- *Based on logs from compromised phones, we believe that NSO Group customers also successfully deployed KISMET or a related zero-click, zero-day exploit between October and December 2019.*

## How did this happen?

*The first stage appears to have involved an exploit transmitted through Apple's servers. Then, his phone connected to an "Installation server" to download the spyware, and finally sent his personal data back to the spyware operators. And all this happened without his interaction.*



## Is this the first Zero-Click attack?

*Nope, just earlier this month, a Google researcher showed how he could hack into any iPhone within 100 meters thanks to a weakness in the Apple tech that enabled Airdrop and other wireless tools.*

*In 2016, a tool named Karma was used to take advantage of a flaw in the iPhone.*

*In 2019, it was revealed that a vulnerability in WhatsApp was being exploited by attackers to inject spyware onto victim's phones simply by calling them*

## What can we do?

*If you're a smartphone user concerned that you may be the target of a zero-click attack, the frustrating reality is that other than keeping your device's operating system up to date to ensure that any known critical bugs have been patched, there's not a lot that you can do.*
*if you own an Apple iOS device you should immediately update to iOS 14. Click here for instructions.*

Until next time.....

### Resources:

The great iPwn - Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit

An iOS zero-click radio proximity exploit odyssey

Dozens of Al Jazeera journalists allegedly hacked