

How “Pegasus” hacks a smartphone

Pegasus spyware can be deployed onto mobile phones running most versions of iOS and Android, and be used to access data and sensors

ATTACK VECTORS

Pegasus uses **zero-day** vulnerabilities (so-called because software authors have zero days to fix issues, as they are unaware of them) to gain access to restricted areas of operating system

Infection can begin by clicking link sent in message or viewed online

Zero-click attacks can install Pegasus just by placing call to target device, e.g. via **WhatsApp**, even if not answered



Messaging apps



Email



Browser



WhatsApp

CAPABILITIES

Spyware can access and copy or record all areas of phone:



Email



SMS



Microphone



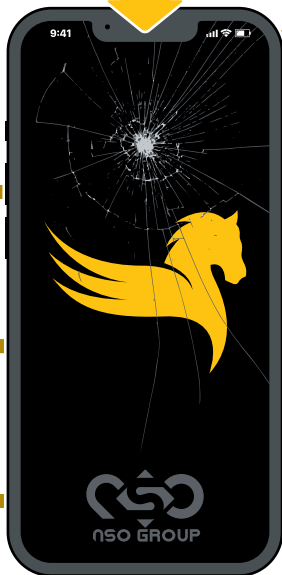
Phone calls



Contacts



Camera



Photos app



Screen shots



Location tracking



Browser history



Calendar



Passwords



Settings



Files

Pegasus – only available to governments – was developed by private Israeli company **NSO Group** to help governments track criminal and terrorist activity. Cost involves setup fee of **\$500,000**, plus **\$650,000** to spy on 10 **iPhones** or **Android** devices, with extra costs for additional targets