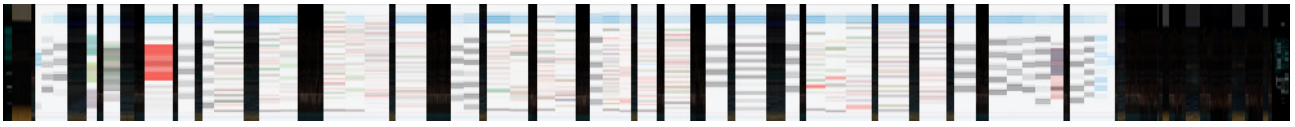
Pegasus internals

Max Bazaliy

Video Player

00:00



00:00 | 29:38

- None
- eng
- fin (translated)

- 2.00x
- 1.50x
- 1.25x
- 1.00x
- 0.75x

Playlists: '33c3' videos starting here / audio / related events

This talk will take an in-depth look at the technical capabilities and vulnerabilities used by Pegasus. We will focus on Pegasus’s features and the exploit chain Pegasus used called Trident. Attendees will learn about Pegasus’s use of 0-days, obfuscation, encryption, function hooking, and its ability to go unnoticed. We will present our detailed technical analysis that covers each payload stage of Pegasus including its exploit chain and the various 0-day vulnerabilities that the toolkit was using to jailbreak a device. After this talk attendees will have learned all of the technical details about Pegasus and Trident and how the vulnerabilities we found were patched.

Download

These files contain multiple languages.

This Talk was translated into multiple languages. The files available for download contain all languages as separate audio-tracks. Most desktop video players allow you to choose between them.

Please look for "audio tracks" in your desktop video player.

Subtitles

Audio

Related

Tags
