



PEGASUS SPYWARE ATTACK

INTRODUCTION

- Pegasus is a highly advanced spyware
- Developed by Israeli cyber-arms firm NSO Group
- Used to secretly monitor smartphones



HOW PEGASUS WORKS [OVERVIEW]

- Exploits zero-day vulnerabilities in mobile OS
- Installed without user interaction (zero-click)
- Full access to device data & sensors



TECHNICAL CAPABILITIES

- Reads messages, emails, call logs
- Activates microphone & camera silently
- Tracks real-time GPS location



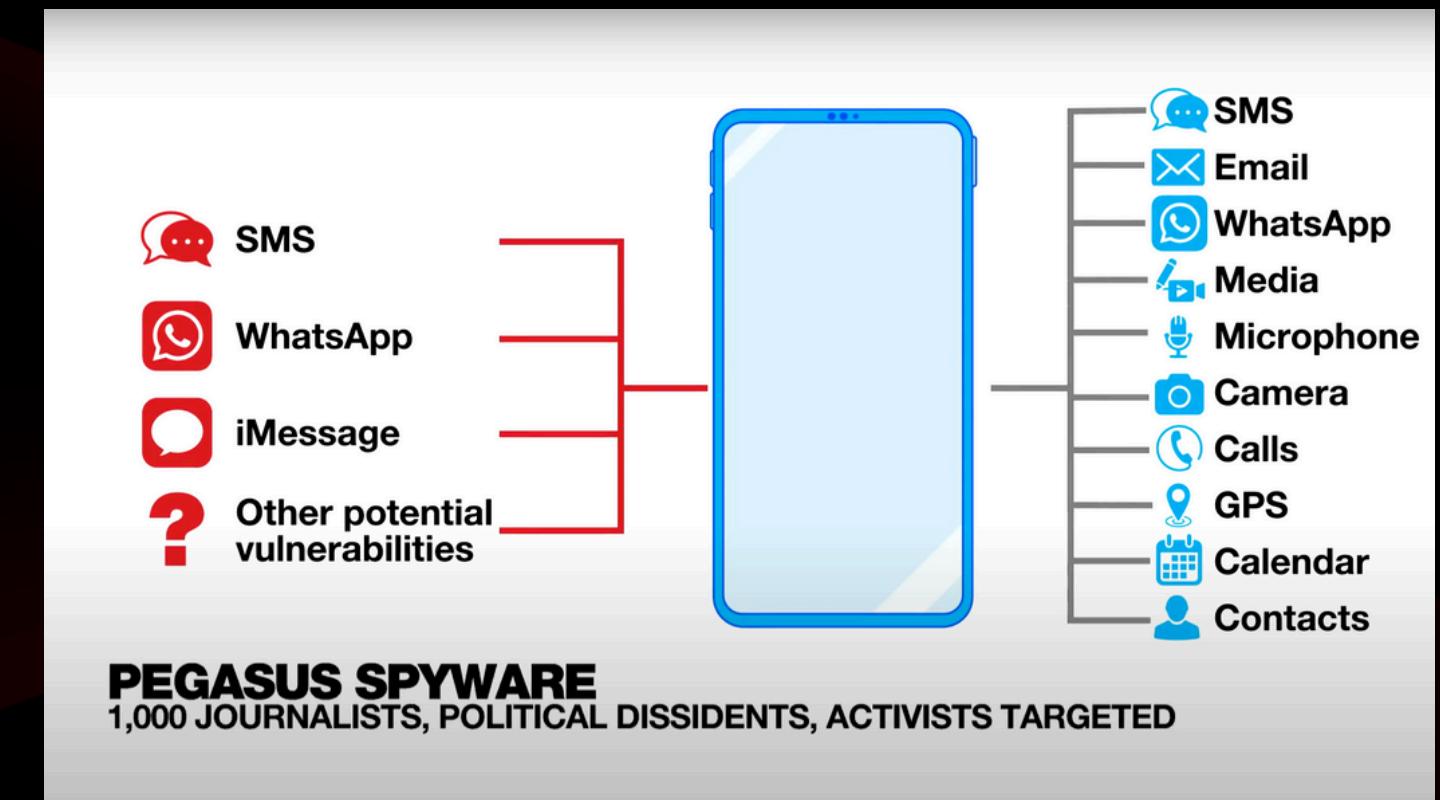
ATTACK VECTORS

- Malicious links (spear phishing in early versions)
- WhatsApp & iMessage zero-click exploits
- Exploiting vulnerabilities in mobile OS (iOS & Android)



Cybersecurity Threats

- Compromises confidentiality of communication
- Enables surveillance on activists, journalists, politicians
- High risk of misuse by authoritarian regimes



CASE STUDIES

- 2016: UAE activist Ahmed Mansoor targeted
- 2019: WhatsApp lawsuit against NSO Group
- 2021: Pegasus Project revealed mass surveillance

CHEAT SECURITY IMPLICATIONS

- Undermines trust in secure communications
- Breaks end-to-end encryption protections
- Raises privacy & human rights concerns



DETECTION CHALLENGES

- Very stealthy – leaves little trace
- Constantly evolves to bypass defenses
- Requires forensic analysis for confirmation



DEFENSE MECHANISMS

- Regular OS updates & patching vulnerabilities
- Security audits & mobile threat detection tools
- Awareness of phishing & suspicious activities



GOVERNMENT & LEGAL RESPONSE

- Lawsuits filed against NSO Group (e.g., WhatsApp, Apple)
- Debate on regulation of spyware industry
- International pressure to restrict misuse



CYBERSECURITY LESSONS

- Zero-day exploits are dangerous & costly
- Security cannot rely only on encryption
- Need for stronger global cyber norms

CONCLUSION

- Pegasus is a powerful cyber weapon
- Raises ethical, legal, and cybersecurity challenges
- Protecting digital privacy is crucial in today's world

THANK YOU