KAEZAL: A Social Engineering Toolkit, initially developed with four key tools, has evolved through further development to include six powerful tools, each enhanced with additional features to simulate a comprehensive range of social engineering attacks. Created by Team KAEZAL, this toolkit serves as both a learning and testing platform, equipping users with a deeper understanding of social engineering tactics and their potential impact on organizational security.

Initially, the toolkit included fundamental tools for phishing, QR code attacks, and URL shortening. Building on this foundation, two additional tools were integrated—geolocation through IP tracking and a backdoor injection feature—while existing tools were refined with enhanced functionality for more sophisticated simulations. Each tool addresses specific security vulnerabilities:

1. **Phishing Tool**: Generates customizable phishing pages to obtain credentials and IP addresses.
2. **Camera Phishing Tool**: Lures users into allowing webcam access, capturing and sending images for analysis.
3. **QR Code Attack Tool**: Converts phishing URLs into QR codes to exploit the rise of QR code scanning.
4. **URL Shortener Tool**: Obscures phishing links, demonstrating the use of shortened URLs in social engineering.
5. **Userfinder Tool**: Pinpoints a target’s location using IP data, highlighting potential privacy risks.
6. **Backdoor Injection Tool**: Embeds backdoors into popular file formats (JPG, PDF, DOCX), functioning as a remote access trojan.

This expanded version of KAEZAL now offers a comprehensive suite that provides valuable insights into the latest techniques used in social engineering, helping cybersecurity professionals and organizations build stronger defenses against these increasingly sophisticated threats.