IKARUS
security software

IKARUS
scan.engine

# Award-winning IKARUS scan.engine, developed in-house

The **IKARUS scan.engine** is one of the world‘s best carrier-grade scan engines for advanced content analysis. Our defense technology against cyber threats and malware of all kinds has been developed in-house and detects, extracts, analyses and eliminates malware, vulnerabilities and exploits in almost all file systems and archives. Integrate the **IKARUS scan.engine** into your existing products or use it to develop your own security products: The possibilities are almost endless.

## Behavioural heuristics and simulation

**IKARUS scan.engine** uses powerful, advanced scanning technologies to analyse all kinds of content - regardless of its appearance, size or file identifier. The first scanning procedure calculates cryptographic hash values, analyses suspicious file elements and searches for signatures and exploits. Known malware is isolated and neutralised immediately. A large portion is subjected to further analyses in a secure environment.

Packed files are unpacked, and all files are extracted. Executables are identified and decrypted, simulations are started in an integrated virtual environment and files are scanned for exploits, scripts, iFrames, Java scripts, ActionScripts, macros and embedded font or PE files. Emails are analysed according to their content, headers and attachments. Scripts, such as HTML, XML, Java script, VBS, MIRC script, Web script, X script, BAT, TXT and binary files, are executed, monitored and checked for jumps and calls.

In a closed virtual environment, the **IKARUS scan.engine** replaces calls from interfaces with its own functions. Behaviour analyses are created, including analysis of API calls, loaded DLLS and files. In addition, opcodes are generated and the memory areas and unpacked codes or files that have been modified by the program are observed and evaluated. In addition, the behaviour of the files after the start of the simulation is observed, as some viruses possess functions that test their environment and recognise simulations: For example, if a file checks and compares error messages for the use of incorrect parameters, searches for specific files in the process environment block or calls APIs to compare register values, you can conclude that there is malware present using a camouflage function.

The IKARUS analysis team is continuously augmenting and supporting the ability of the **IKARUS scan.engine** with manual analyses and reverse engineering. The worldwide threat data provided by the IKARUS SigQA (Signature Quality Assurance Program), combined with the ongoing exchange within the anti-virus industry, also ensure fast and reliable detection performance.

## Product highlights

- Automatic, malware-dependent selection of the testing environment
- Behavioural heuristics
- Generic analysis methods
- High-speed multi-threading
- Platform-independent
- Advanced virtual environment with low resource usage

secure your business

www.IKARUSsecurity.com

**IKARUS Sales Team** | sales@ikarus.at | +43 1 589 95-500
**IKARUS Support Team** | support@ikarus.at | +43 1 589 95-400

www.ikarussecurity.com/ikarus-scanengine