IKARUS
security software

IKARUS
scan.engine

Selbst entwickelte, preisgekrönte IKARUS scan.engine

Die IKARUS scan.engine ist eine der weltweit besten Carrier-grade Scan Engines zur erweiterten Inhaltsanalyse. Die selbst entwickelte Abwehrtechnologie gegen Cyber-Bedrohungen und Malware aller Art findet, extrahiert, analysiert und eliminiert Schädlinge, Schwachstellen und Exploits in nahezu allen Dateisystemen und Archiven. Integrieren Sie die IKARUS scan.engine in Ihre bestehenden Produkte oder nutzen Sie sie zur Entwicklung eigener Security-Produkte: Die Möglichkeiten sind nahezu unbegrenzt.

Verhaltensbasierte Heuristik und Simulation

Die **IKARUS scan.engine** arbeitet mit hochentwickelten, leistungsstarken Scan-Technologien zur Analyse von Inhalten verschiedenster Art – unabhängig von deren Erscheinung, Größe oder Dateikennung. Der erste Scanvorgang berechnet kryptografische Hashwerte, analysiert verdächtige Dateielemente und sucht nach Signaturen und Exploits. Bekannte Schädlinge werden sofort isoliert und unschädlich gemacht. Ein Großteil wird in einer geschützten Umgebung weiteren Analysen unterzogen.
Gepackte Files werden entpackt und alle Dateien extrahiert, ausführbare Dateien identifiziert und entschlüsselt, Simulationen werden in einer integrierten virtuellen Umgebung gestartet und Dateien auf Exploits, Scripte, iFrames, Java Scripte, ActionScripts, Makros und eingebundene Font- oder PE-Dateien untersucht. E-Mails werden anhand ihres Inhaltes, Headers und ihrer Anhänge analysiert. Scripte wie HTML, XML, Java Script, VBS, MIRC Script, Web Script, X Script, BAT, TXT und Binäre Dateien werden auf Jumps und Calls überprüft, ausgeführt und beobachtet.

Aufrufe von Schnittstellen ersetzt die **IKARUS scan.engine** im geschlossenen virtuellen Umfeld mit eigenen Funktionen. Es werden Verhaltensanalysen inkl. Analyse von API Aufrufen, nachgeladenen DLLS und Dateien erstellt, Opcodes erzeugt und die vom Programm veränderten Speicherbereiche und entpackte Codes oder Dateien beobachtet und bewertet. Außerdem wird das Verhalten der Dateien nach Start der Simulation beobachtet, da einige Viren über Funktionen verfügen, um ihr Umfeld zu testen und Simulationen zu erkennen: Ruft eine Datei beispielsweise APIs auf, um Registerwerte zu vergleichen, überprüft und vergleicht Error-Meldungen nach der Nutzung falscher Paramater oder sucht nach bestimmten Files im Process Environment Block, kann man auf Tarnfunktionen eines Schädlings schließen.
Das IKARUS Analyse-Team ergänzt und unterstützt die Leistungsfähigkeit der **IKARUS scan.engine** laufend mit manuellen Analysen und Reverse-Engineering. Auch die weltweiten Bedrohungsdaten aus dem IKARUS SigQA (Signature Quality Assurance Program) und der laufende Austausch innerhalb der Antiviren-Industrie sorgen für schnelle und verlässliche Erkennungsleistung.

Produkt-Highlights

- Malware-abhängige, automatische Auswahl der Test-Umgebung
- Verhaltensbasiert Heuristik
- Generische Analyse-Verfahren
- Multithreading in Höchstgeschwindigkeit
- Plattformunabhängig
- Hochentwickelte virtuelle Umgebung mit geringer Ressourcennutzung

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/at/ikarus-scanengine