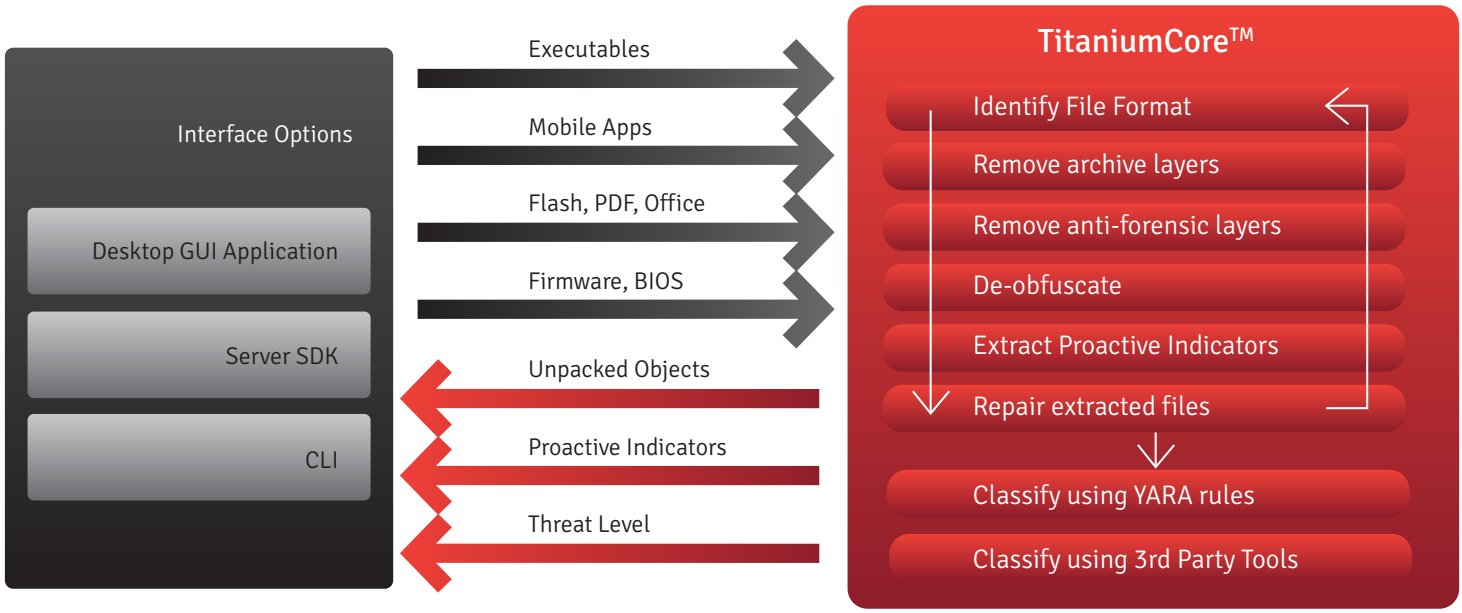
TitaniumCore™ Release 3.1

Threat detection and automated static analysis for files



TitaniumCore™ release 3.1

is the world's fastest and most comprehensive software platform for threat detection and automated static analysis. The platform recursively unpacks internal objects, extracts Proactive Threat Indicators (PTIs) and identifies threat level for a broad array of binary file types, including: Windows, Linux, Mac OS, Android, iOS, firmware, Flash, PDF, and other documents. TitaniumCore performs advanced file inspection to identify threats before they execute. TitaniumCore provides a powerful solution for operations on any scale from a few samples to millions of samples daily.

The TitaniumCore Automated Static Decomposition engine removes all packing, obfuscation and protection from binary files to extract all internal objects and their PTIs. The unpacked objects are fully repaired and available for further analysis using debuggers, decompilers, sandboxes, YARA rules or other 3rd party tools. The PTIs provide critical information, not visible to conventional tools, for determining the intent, threat level and capabilities of a binary file.

The Desktop Edition GUI supports ad hoc analysis of samples. The Server Edition SDK and CLI enable integration with automated workflows or other platforms and extension of file processing procedures. The platform produces detailed XML reports for consumption by back end systems and databases for further analysis.

FEATURES

- Multi-threaded architecture to detect and analyze threats in milliseconds without executing files
- 3500+ file format families identified
- Recursive unpacking of 300+ families of installers, packers and compressors
- 3,000+ internal proactive file threat indicators extracted from PE/Windows, ELF/Linux, Mac OS, iOS, Android, firmware, Flash, and other documents
- Detailed application capability, functional analysis and external usage for Android/DEX, iOS/Mach-O and Windows Phone/.NET applications
- Analyzes and decomposes PCAP objects
- YARA-based rules matched on all decompressed content
- Custom YARA rules and 3rd party modules supported
- Exports all results in CybOX, MAEC, STIX and IOC fomats
- All unpacked PE files repaired for further analysis
- Server CLI and SDK (C, C++, .NET, Python) for integrating with automated workflows or OEM products

USE CASES

Malware Analysis Triage

- TitaniumCore can preprocess hundreds of thousands of files per day and integrate to support automated classification and triage workflows to optimize analyst and asset utilization.
- Samples are unpacked and de-obfuscated to enable further analysis by sandboxes, debuggers and decompilers.
- PTIs provide valuable information not readily available from other tools to accelerate triage and complement other analysis methods.

Incident Response

- TitaniumCore can rapidly scan file shares and system images at the breach site to identify the most suspicious files.
- Automated static analysis of suspicious files extracts PTIs to reveal intent and capabilities.
- Analyst-written custom YARA rules are matched against all decomposed objects (e.g., Adobe Flash).

Software Validation for Code Signing

- TitaniumCore enables analysis of binary files for capabilities and intent without the source code and before digital certificates are applied.
- PTIs expose internal information about every binary including imports, exports, resources, strings and access privileges.

OEM Solutions

- TitaniumCore provides and is being used as a powerful OEM solution for software and hardware vendors to extend their products.

EXAMPLES OF PROACTIVE INDICATORS

- File validation and malformation, protection, crypto and repair data
- Format, file type, architecture, language, icons, strings, graphic resources, compile date and other file internals
- Embedded domains, IP Addresses, IRC handles, spam dictionaries, registry entries and URLs
- Full certificate data chains with detailed X.509 records

(Windows, Java, Apple, Android)

- Executable file formats (PE/ELF/Mach-O/DEX/SWF/PDF)
- Imports, exports, resources, behaviors, classes, properties events and strings before and after decomposition
- Section names, sizes and hashes
- Mobile application capabilities based on embedded functions (iOS, Android & Windows Phone)
- Relative and full install paths with extracted files' relationships
- Standard and fuzzy hashes for all extracted objects

TITANIUM CORE STANDARD EDITIONS

	Desktop	Server
Desktop Application	✓	
Server Application		✓
SDK		✓
Max. Daily Samples	1000	100,000
Users	1	100
Operating Systems	Linux Windows	Linux Windows

TITANIUM CORE ENTERPRISE PLATFORM (TCEP) EDITION

- As with Standard Editions + Titanium Cloud File Reputation Lookup
- See TCEP Data Sheet: http://reversinglabs.com/products.htmlhes for all extracted objects