DATA SHEET

ЯL REVERSINGLABS

ReversingLabs Spectra Analyze

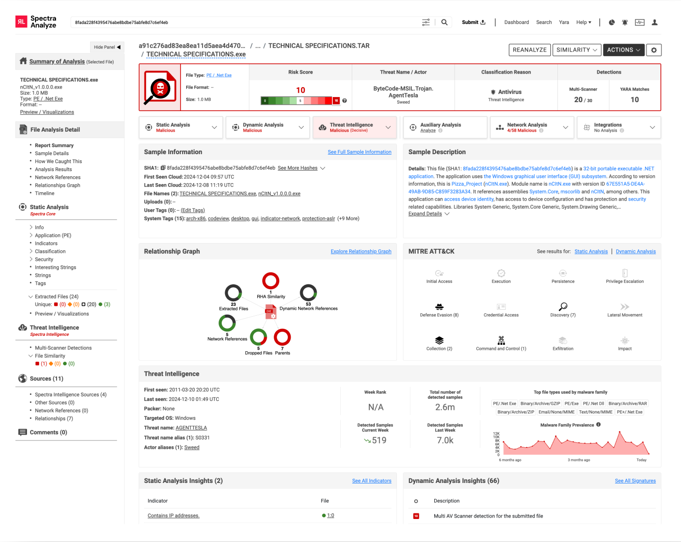
Advanced Malware Analysis and Threat Hunting Workbench

Spectra Analyze empowers the SOC with a malware analysis and threat hunting workbench that delivers the speed, depth, coverage, and accuracy analysts need to speed alert triage, enrich security tools, and accelerate response actions.

Powered by RL's proprietary, AI-driven, complex binary analysis technology and the industry's largest repository of file and network intelligence, Spectra Analyze is a powerful, integrated, out-of-the-box solution that makes malware threat detection, deep analysis, and analyst collaboration more effective and productive.

Spectra Analyze accelerates threat detection and response capabilities for all skill levels throughout the SOC. From L1 analysts doing initial evaluation and triage, to L2 analysts performing deeper malware inspection and investigation, to L3 analysts writing YARA rules and conducting threat hunting, Spectra Analyze provides the tooling and intelligence required to optimize SOC workflows and outpace advanced malware threats.

An Automated Malware Analysis Solution to Drive Efficiency and Efficacy in the SOC.



a91c276ad83ea8ea11d5aea4d470... / ... / TECHNICAL SPECIFICATIONS.TAR / TECHNICAL SPECIFICATIONS.exe

TECHNICAL SPECIFICATIONS.exe
nCltN_v1.0.0.0.exe
Size: 1.0 MB
Type: PE / .Net Exe
Format: --
Preview / Visualizations

File Type: PE / .Net Exe
File Format: --
Size: 1.0 MB

Risk Score	Threat Name / Actor	Classification Reason	Detections	
			Multi-Scanner	YARA Matches
10	ByteCode-MSIL.Trojan.AgentTesla Sweed	Antivirus Threat Intelligence	20 / 30	10

Sample Information

SHA1: 8fada228f4395476abe8bdbe75abfe8d7c6ef4eb See More Hashes
First Seen Cloud: 2024-12-04 09:57 UTC
Last Seen Cloud: 2024-12-08 11:19 UTC
File Names (2): TECHNICAL SPECIFICATIONS.exe, nCltN_v1.0.0.0.exe
Uploads (0): --
User Tags (0): -- (Edit Tags)
System Tags (15): arch-x86, codeview, desktop, gui, indicator-network, protection-aslr (+9 More)

Sample Description

Details: This file (SHA1: 8fada228f4395476abe8bdbe75abfe8d7c6ef4eb) is a 32-bit portable executable .NET application. The application uses the Windows graphical user interface (GUI) subsystem. According to version information, this is Pizza_Project (nCltN.exe). Module name is nCltN.exe with version ID 67E551A5-DE4A-49AB-9D85-C859F3283A34. It references assemblies System.Core, mscorlib and nCltN, among others. This application can access device identity, has access to device configuration and has protection and security related capabilities. Libraries System Generic, System.Core Generic, System.Drawing Generic,...
Expand Details

Threat Intelligence

First seen: 2011-03-20 20:20 UTC
Last seen: 2024-12-10 01:49 UTC
Packer: None
Targeted OS: Windows
Threat name: AGENTTESLA
Threat name alias (1): S0331
Actor aliases (1): Sweed

Week Rank	Total number of detected samples
N/A	2.6m
Detected Samples Current Week	**Detected Samples Last Week**
519	7.0k

Static Analysis Insights (2)

Indicator	File
Contains IP addresses.	● 1:0

Dynamic Analysis Insights (66)

○	Description
10	Multi AV Scanner detection for the submitted file

Figure 1: Intuitive and customizable dashboard, plus robust API, streamlines SOC workflows

Highlights

In-depth, high-speed binary analysis fully dissects complex files in seconds, detecting embedded threats missed by other tools.

Verified threat classifications for reduced false positives, faster alert triage, and more effective response actions.

Broadest coverage in the industry with support for more than 4800 file types and multi-gigabyte file sizes.

Privacy by default including private file analysis and private datastore.

Advanced search functionality enables more than 500 unique search expressions and the ability to create targeted, multi-conditional queries.

Simplified YARA rule development with the ability to easily import, build, test, and deploy rules – all from a single interface.

YARA hunting and retrohunting across local dataset and RL's global threat repository provides powerful malware discovery.

Real-time alerting on changes to malware classification and analysis results to stay ahead of threats, including zero-day attacks.

Intuitive relationship graph to quickly see the bigger picture and intelligently pivot on interconnected malware artifacts.

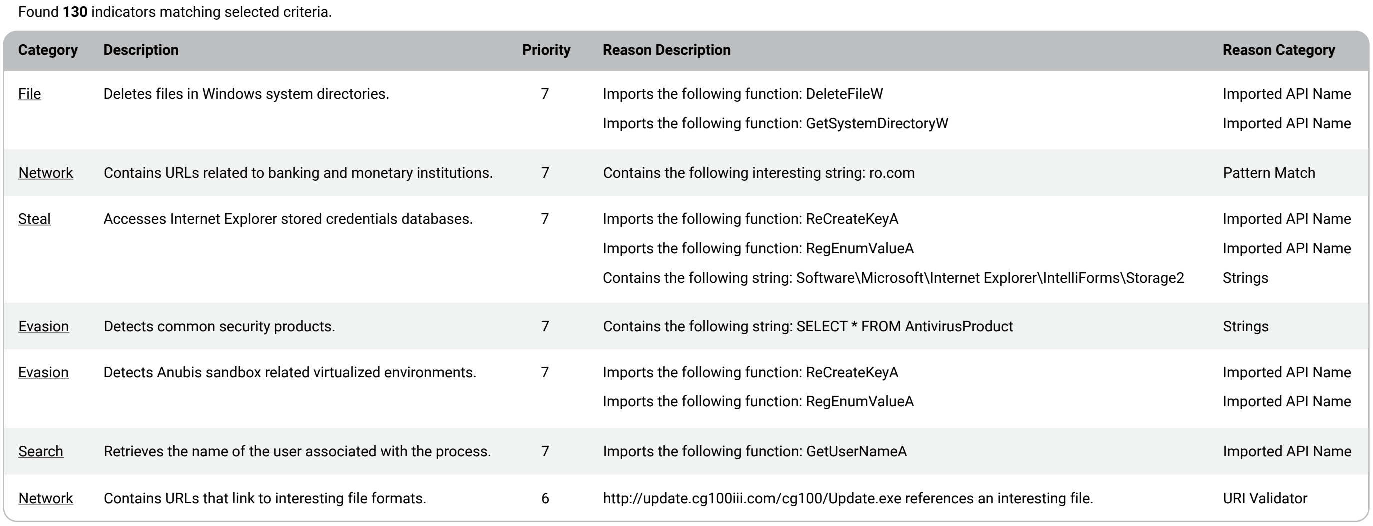
Built-in cloud sandbox, as well as direct integration with third-party sandboxes.

MITRE ATT&CK mapping bridges analysts' language to triage, investigation, and response activities.

Pre-built connectors and REST API to automate analysis workflows with enterprise infrastructure and existing security tools.

Advanced Analysis. Rich Context. Actionable Malware Intelligence.

Security analysts can leverage the power of RL's malware analysis capabilities and context-rich results through an instinctive, easy-to-navigate GUI, as well as a robust REST API. Regardless of how analysts use Spectra Analyze, the result is truly actionable file and network intelligence, backed by verifiable threat verdicts that explain the "why" behind RL's risk score and classification. SOC analysts, incident responders, and threat hunters alike get the intelligence they need to more effectively and efficiently carry out their responsibilities to keep the organization safe from advanced malware and sophisticated cyber attacks.



Found **130** indicators matching selected criteria.

Category	Description	Priority	Reason Description	Reason Category
File	Deletes files in Windows system directories.	7	Imports the following function: DeleteFileW Imports the following function: GetSystemDirectoryW	Imported API Name Imported API Name
Network	Contains URLs related to banking and monetary institutions.	7	Contains the following interesting string: ro.com	Pattern Match
Steal	Accesses Internet Explorer stored credentials databases.	7	Imports the following function: ReCreateKeyA Imports the following function: RegEnumValueA Contains the following string: Software\Microsoft\Internet Explorer\IntelliForms\Storage2	Imported API Name Imported API Name Strings
Evasion	Detects common security products.	7	Contains the following string: SELECT * FROM AntivirusProduct	Strings
Evasion	Detects Anubis sandbox related virtualized environments.	7	Imports the following function: ReCreateKeyA Imports the following function: RegEnumValueA	Imported API Name Imported API Name
Search	Retrieves the name of the user associated with the process.	7	Imports the following function: GetUserNameA	Imported API Name
Network	Contains URLs that link to interesting file formats.	6	http://update.cg100iii.com/cg100/Update.exe references an interesting file.	URI Validator

Figure 2: ReversingLabs Explainable Threat Intelligence with contextual, human-readable descriptions of sample behavior

AI-Driven Complex Binary Analysis: The Power Behind Spectra Analyze

Spectra Analyze is powered by RL's unique binary analysis engine, which can fully deconstruct the internal contents of a file, in milliseconds, to reveal hidden threats with the fastest times in the industry. This proprietary technology recursively unpacks and deobfuscates files, including large, complex files, extracting thousands of indicators and rich metadata, applying global threat context from RL's authoritative database of over 400 billion malware and goodware samples, and delivering a verified threat verdict – all without executing the file. The result is real-time, next-level threat intelligence to prioritize alerts, enrich security tools, drive response actions, and perform advanced threat hunting with context, clarity, accuracy, and speed.

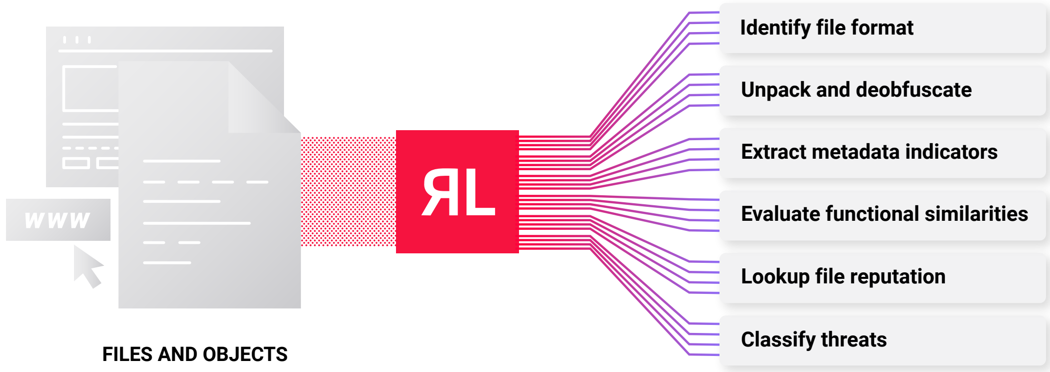


Figure 3: Proprietary, high-speed file deconstruction and threat classification

Spectra Analyze Features

Comprehensive Malware Analysis

- In-depth file and URL analysis with context-rich threat intelligence
- High-speed, fully recursive binary deconstruction in seconds
- Identifies more than 4,800 file types across Windows, MacOS, Linux, iOS, and Android platforms
- Unpacks over 400 formats of archives, installers, packers, and compressors
- Extracts over 20,000 file intent behavior indicators
- Extracts network IOCs from URL, domain, and IP address analysis

Privacy Controls

- Safely and privately analyze files and URLs
- Securely store files and all context in private datastore
- On-premises deployment options available

Advanced Search

- Build more than 500 unique search queries using Boolean operators
- Leverage the autocomplete functionality for faster research
- Use Quick Search feature for advanced capabilities without knowing the syntax
- Perform targeted queries on large sample datasets
- Search by hash, imphash, file name, tags, and more
- Find files based on functional similarity

YARA Hunting

- Leverage RL-supplied or user-defined YARA rules for matching and hunting
- Import, build, test, and deploy YARA rules from a single interface
- Automatically update and sync YARA rulesets from third-party repositories
- Match on thousands of characteristics from all files and objects unpacked and extracted during RL's binary analysis process
- Perform YARA hunting and retro-hunting across local dataset and RL's threat repository, simultaneously

RL Spectra Sandbox / Dynamic Analysis

- Built-in, highly-available, and scalable cloud sandbox, including interactivity capabilities
- Easy-to-understand sandbox analysis results, including quick visibility into all historical reports
- Includes screenshots generated from dynamic detonations of files and URLs
- Default Snort and Sigma rules automatically available without any additional set up
- Download screenshots, PCAP, memory strings, and dropped files from individual analysis

MITRE ATT&CK Mapping

- Provides an understanding of the tactics and techniques used in malware
- Delivers human-readable indicators for each threat to enable analysts to react faster and with more confidence
- Allows security operations teams (SOC) to strengthen defenses and find operational issues in existing controls

API Integrations

- Automate analysis workflows via pre-built connectors, direct integrations, and flexible REST API
- Connect to email sources (IMAP, Microsoft Exchange, SMTP servers) and analyze retrieved emails and attachments
- Connect to cloud storage, including S3 and Azure Data Lake, as well as local network file shares (SMB or NFS)
- Feed orchestration-ready intelligence into SIEM/SOAR, EDR, TIPs, and other security tools

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, RL Spectra Core powers the software supply chain and file security insights, tracking over 422 billion searchable files daily with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

Get Started!

We will show you how to empower your SOC with
RL Spectra Analyze

REQUEST A DEMO

reversinglabs.com

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com