REVERSINGLABS

Automated Analysis of Binary Files

Defending the Digital Supply Chain from the Tactical Edge to the Cloud

Overview

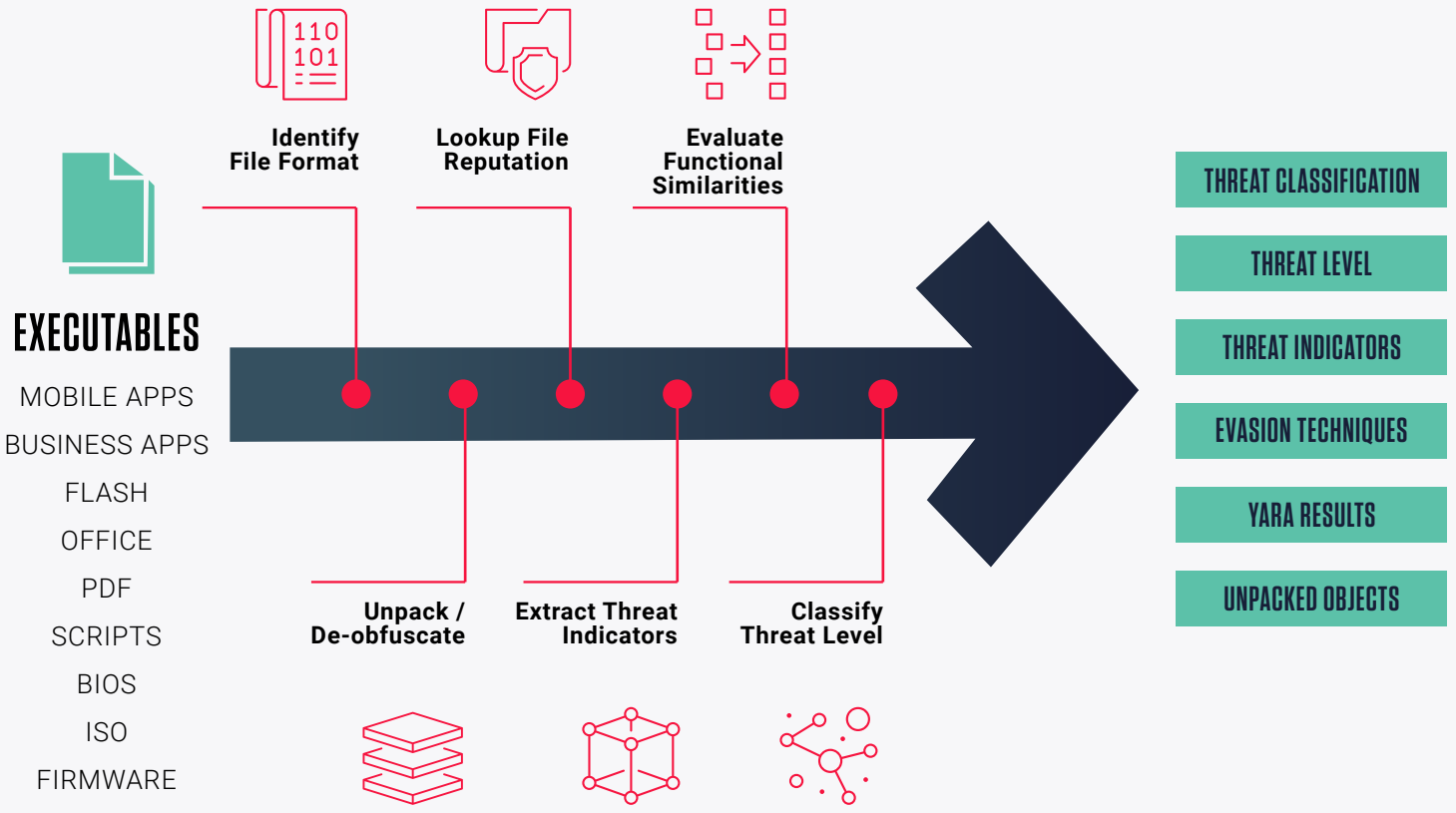
The Federal Government views open source as critical for enhancing our digital services and mission capabilities. The U.S. government and others view open-source software—blocks of code that are publicly accessible for anyone to use—as vital in the development of new services, systems and technologies. The use of open-source code has become ubiquitous in the Federal sector in recent years. Our digital adversaries recognize this and are capitalizing on open source code malware campaigns to wreak havoc on our critical infrastructure.

In 2022, it was reported by Checkmarx that a 1,500% increase in opensource campaigns we created to exploit the open-source repositories. "The threat actors create malicious websites and publish empty packages with links to those malicious websites, taking advantage of open-source
ecosystems' good reputation on search engines." The battle against threat actors poisoning our software supply chain ecosystem continues to be a growing challenge, as attackers constantly adapt and surprise the industry with new and unexpected technics.

ReversingLabs empowers modern software development, security operations center teams and forward operating units to protect and defend our critical infrastructure from sophisticated software supply chain security attacks, malware, ransomware and other threats.

The ReversingLabs reverse engineering platform analyzes any file, binary or object including those that evade traditional security solutions. The platform unifies operators, Dev and SOC teams with transparent and human readable threat analysis, arming developers, DevSecOps, SOC analysts, cyber operators and threat hunters to confidently respond to software tampering and security incidents. Given the pace and complexity of Federal missions and platforms, Reversing Labs solutions seamlessly integrate, rapidly scale, and provide interfaces which allow each side of the interface to independently evolve. Segmented standard interfaces, as well as automation and autonomy, are key elements of any solution.

INSERT TITLE



Vulnerabilities and Exploits Discovery and Analysis

Defensive Cyber Operations Teams need the ability to scan and collect from a variety of sources to identify, analyze, and report events that occur or might occur within the edge network to protect information, information systems, and networks from threats. Reversing Labs provides industry's best capabilities to the warfighter for identifying and remediating malware in over 4,000 types using automation saving 100 of hours in manual analysis work. This capability allows Cyber Protection Leadership to quickly ensure kits and capabilities are always mission ready.

PRODUCT CAPABILITIES

- Analysis Engine performs high-speed, static analysis to unpack files, extract internal indicators and assign a threat level
- Integrated with file reputation services to provide in-depth rich context and threat classification on tens of billions of files across all file types
- Visualization GUI for quickly viewing classification, threat level and understanding functional similarity and metadata indicators

DEPLOYMENT OPTIONS

- Cloud
- On-Premise
- Tactical Edge

USE CASES

Polymorphic Malware/Countering Adversarial Signature Diversity

Enable defenders to recognize polymorphic malware in real-time, at network perimeters or when malware has penetrated perimeter security. New ideas to enhance immediate malware recognition.

Malware Analysis of multi-cloud and hybrid infrastructure cloud analysis (Cloud Deep Scan)

Federal customers are driving to multicloud environments and require a unified toolset to seamlessly scan and operate secure cloud environments. ReversingLabs Cloud Deep Scan is a cloud file share threat intelligence solution that continuously scans Amazon Web Services S3 buckets for threats. This solution provides quality classification for large files (up to 10GB), allowing IT and SOC teams to quickly prioritize malicious files for investigation and remediation. It provides file reputation and threat analysis. ReversingLabs Cloud Deep Scan enables file-based business workflows with easy-to-understand file classification based on one of the largest repositories of known goodware and malware files.

Malware Analysis of Network PCAP files at scale

The Federal government has a need to rapidly scan and discover new or existing networks to discover if malware or exploits exist. Protocol (PCAP) reverse engineering is the process of extracting the application/ network level protocol used by either a client-server or an application. Nowadays this task of Reverse Engineering protocols has become very important for network security. Organizations need to easily reverse engineer PCAP files to learn about and organizations structure, how it passes the data, and then look for exploits in the protocol which generally would attribute to vulnerabilities in the network.

Rapidly Generate Defensive Capabilities

Reversing Labs enables Federal Organizations to rapidly generate defensive capabilities, and rapidly patch newly discovered vulnerabilities, i.e., mechanisms deploy patches reliably in an automated or accelerated way to reduce or even eliminate the need for human operators' intervention.

Modeling & Predictive Analytics

Modeling and Predictive analytics are necessary capabilities which provide the ability to detect highly advanced nation-state cyber implants and supply chain attacks within Federal systems. Modeling helps capture behavioral based observations rated to the cyber vulnerability. Predictive analytics allow users and decision makers to anticipate possible future states, either as a result of taking no action or from pursuing various alternatives. The need for highly tuned cybersecurity sensors, supported by automation and machine-assisted decision making are required for threat correlation, hunting, and response.

Conventional malware products focus on detecting malware while treating unknown files as good, essentially overlooking them. As the amount of malware that evades detection grows, the need to profile, track and correlate undetected files becomes imperative to limit the impact of incidents and breaches. This intelligence data helps close the visibility gap between malware detection and tedious and expensive post-breach reconstruction.

To effectively pull together precise models and predictive analytics organizations rely on authoritative file reputation services to check the reputation of each file against an extensive database of known goodware and malware.

PRODUCT CAPABILITIES

- Increases detection, analysis, and response efficiency by identifying files from queries to an authoritative goodware and malware file reputation database
- Analysis Engine performs high-speed, static analysis to unpack files, extract internal indicators, and assign a threat level
- Integrated with file reputation services to provide in-depth rich context and threat classification on tens of billions of files across all file types
- Visualization GUI for quickly viewing classification, threat level and understanding functional similarity and metadata indicators
- Securely store files with all context in the onboard database for future collaborative search, analysis, hunting and development of local threat intelligence

DEPLOYMENT OPTIONS

- Cloud
- On-Premise
- Tactical Edge

USE CASES

Automated Anomaly Detection

Identify anomalous behavior in the offensive and defensive cyber operating environments. These capabilities help to determine, measure, and characterize, both accurately and efficiently, the baseline state of a network and systematically specify what constitutes deviation from "normal" activity. The ability to recommend actions based on situations that defenders can quickly understand and implement.

Automated Threat Discovery

Automated solutions for the repetitive, data-intensive tasks of detecting indicators of possible compromise, to bring them to the analysts' awareness, and when appropriate, to apply mitigations or countermeasures to compensate for low human response time. Leverage automated solutions for vulnerability discovery in systems, and then integrate stronger defenses into those systems.

Predictive Network Modeling

Identify and characterize adversary behaviors and potential attack vectors to enable both offensive and defensive operations. Automate the modeling of threats using partial knowledge to enable creation of multiple scenarios for operational rehearsals. Generate recommendations or perform evaluations on adversary attack behavior to reduce organizational response times.

Software Supply Chain Security

Risks to the software supply chain have never been greater. The consequences of software supply chain attacks were made well-known thanks to the SolarWinds compromise of December 2020. Since the SolarWinds attack, countless other attacks and proof-of-concepts have arisen stemming from several vulnerable risks. These risks, such as open-source software, software tampering, malicious binaries, and insider developer threats have become a necessity to manage.

We enable Federal stakeholders to collaborate and integrate our analysis tool throughout the entire software development lifecycle. By using ReversingLabs we provide improved prototype frequency, rapid product delivery to our cyber defenders, ultimately a delivering a lower failure rate on tools development. Improved collaboration and secure code between organizational teams and industry enables us to achieve faster prototyping and delivery to our global cyber defenders.

PRODUCT CAPABILITIES

- Close application security testing gaps by complementing your existing tool investments with analysis that detects advanced software supply chain attacks other solutions cannot
- Identify and remediate CI/CD workflow compromises, secrets exposures, malicious open source packages and other threats at any point within your software development lifecycle
- Federal programs can remediate high-risk threats earlier and faster. Security teams are enabled to track improvements and export compliance reports.

DEPLOYMENT OPTIONS

- Cloud
- On-Premise with Internet Access

USE CASES

Discovery of Malicious Intent in Incremental Software Updates

Once third-party software is deployed, every subsequent update and patch can present new risks. With every new patch or software release, ReversingLabs will produce evidence-based reports highlighting any malicious or unintended changes to the software behavior characteristics from version to version.

Software Code Provenance

Federal clients looking for automated ways to detect what is in a code base and where did it come from. To do this Analyst need to understand the provenance of the software. The term "provenance" refers to a place of origin or history of ownership. DoD's implementation of security controls and secure code is rapidly evolving. DoD and Federal application security teams need to ensure code provenance is being detected and analyzed to ensure we have a verifiable attestation of the origin of all code running in production. This provides a root of trust as we move forward in defining and enforcing a collection of policies throughout each stage of the software development process.

TRUSTED BY

U.S. AIR FORCE

REVERSINGLABS

www.reversinglabs.com
Russell Jacobs
russell.jacobs@reversinglabs.com
1-703-403-8843