RevBits®

DATA SHEET

Malware Analysis Service

A Crucial Discipline to Enhance Cybersecurity for Our Customers to Understand the Impact of Malicious Software

Overview

Businesses, especially those with limited security personnel, are struggling to keep up with the alarming rate of cyber threats. The sheer volume of malware attacks is staggering. The relentless surge in cyber threats has forced organizations to rethink their security strategies, leading to a significant shift toward outsourced malware analysis services.

The numbers paint a clear picture: Research from the World Economic Forum's Global Cybersecurity Outlook 2025 states that 66% of organizations anticipate that AI will have the most significant impact on cybersecurity in the coming year. This trend is driven by the increasing complexity of cyberattacks, which require specialized expertise and advanced tools to detect and neutralize threats effectively.

The financial impact of cybercrime is another major factor fueling the demand for malware analysis services. The global cost of cybercrime is expected to reach trillions of dollars. Businesses that fail to invest in proactive security measures risk devastating financial losses, reputational damage, and operational disruptions.

Beyond the financial toll, the nature of malware itself is becoming more sophisticated. Security research from Kaspersky observed an average of 400,000 new malware variants daily. Attackers are constantly refining their techniques, making traditional security measures insufficient. This has led to a surge in demand for expert-driven malware analysis services that can provide deeper insights into emerging threats.

Attackers are constantly refining their techniques, making traditional security measures insufficient.

Research from CONTROL D found fileless attacks are another alarming trend, which rely on scripts or in-memory payloads rather than traditional malware files. These attacks are projected to account for 70% of all serious malware incidents. This shift underscores the need for advanced malware analysis capabilities that can detect and mitigate threats beyond conventional antivirus solutions.

Outsourcing Malware Analysis

Outsourcing malware analysis to a trusted service provider, such as RevBits, allows you to strengthen your cybersecurity defenses while maximizing your available resources. Here's how it can make a difference:

- **Smarter Resource Allocation:** Organizations can focus their budget, personnel, and infrastructure where they matter most, ensuring cybersecurity investments align with business priorities.
- **Maximize Security Investments:** By gathering and deploying indicators of compromise (IoCs) across your security tools, your team can more effectively detect and counter malware threats.
- **Simplify Security Operations:** Having worked with many different businesses, outsourced services have streamlined their processes and accumulated advanced tools that help reduce complexity, improve efficiency, and enhance protection across the cybersecurity ecosystem.

- **Access to Deep Expertise:** Dedicated and highly experienced malware analysts bring specialized knowledge to uncover and assess potential threats, including malicious files, hashes, and URLs, delivering deeper insights that support proactive threat management.

RevBits Malware Analysis Service

RevBits is dedicated to helping you strengthen your security posture and stay ahead of evolving cyber threats while unburdening your internal team. The RevBits Malware Analysis Service (MAS) empowers security teams with deep insights, actionable intelligence, and enhanced defense mechanisms. While malware analysis is crucial for identifying and mitigating threats, many security teams are often constrained by limited time, resources, and specialized expertise. RevBits helps you overcome these critical limitations, offering a powerful service that enables you to stay ahead of malicious campaigns and attacks.

By combining advanced static, dynamic, behavioral, and network analysis techniques, RevBits Malware Analysis Service uncovers hidden threats, correlates attack patterns, and develops proactive defense strategies. With comprehensive intelligence and expert-driven analysis, your security team can respond more effectively, strengthen your security posture, and minimize risks in an increasingly volatile digital environment.

RevBits' dedicated team and platform enable your security team to safely submit suspicious files, URLs, and network activity for detailed examination. The service utilizes:

- **Static Analysis:** Examines file attributes, metadata, and embedded code structures to detect anomalies.
- **Dynamic Analysis:** Executes malware in a controlled environment (sandboxing) to observe its real-time behavior.
- **Memory Analysis:** Investigates volatile memory for indicators of infection or unauthorized activity.
- **Network Analysis:** Monitors communications and interactions with external systems to detect command-and-control (C2) traffic.
- **Behavioral Analysis:** Maps malware execution patterns against known tactics, techniques, and procedures (TTPs) from threat actor groups.

The Four Step Process for Deep Malware Analysis

RevBits approaches malware analysis with a structured, multi-step process that ensures your security team gains a complete understanding of potential threats. Each step is designed to uncover critical insights and provide actionable intelligence.

Step 1 - Static Analysis
Before executing any suspicious files, static analysis examines code structures, file attributes, hashes, and metadata to identify potential risks. This initial step offers quick insights that help security teams assess threats without launching harmful code, reducing the likelihood of accidental system compromise.

Step 2 - Dynamic Analysis
To observe malware behavior in real-time, our system deploys a sandboxed environment where suspected malicious code is safely executed. This allows cybersecurity teams to monitor interactions, detect hidden payloads, and analyze execution patterns without endangering live networks or critical systems.

Step 3 - Code Reversing
For more complex threats, our analysts conduct more in-depth investigations. Reverse engineering is used to deconstruct the malware's inner workings, revealing concealed functionalities, encryption methods, and evasive techniques designed to bypass security measures.

Step 4 - Comprehensive Reporting
Once the analysis is complete, findings are compiled into a detailed report. This includes the malware's capabilities, potential impacts, indicators of compromise (IoCs), recommended mitigation strategies, and a threat mapping aligned with the MITRE ATT&CK framework. These insights empower you to defend against similar threats in the future proactively.

The complete process provides your team with a clear, strategic approach to identifying and neutralizing malware threats before they escalate.

Benefits

Enhance your cybersecurity defenses with a powerful service that combines automation and expert analysis to detect, contain, and prevent malware threats while integrating global intelligence for proactive protection.

- Provides deep insights into malware tactics and techniques.

- Accelerates malware identification and containment efforts.
- Combines automation with expert human review for accuracy.
- Integrates findings with global intelligence sources to detect emerging threats.
- Equips your security team with the knowledge to prevent future attacks.
- Helps meet compliance standards for security and threat management.

Malware Analysis Service Use Cases

Incident Response & Threat Investigation

- An enterprise detects abnormal outbound traffic from multiple endpoints. RevBits MAS identifies the source as malware attempting to communicate with a C2 server, providing actionable insights to block the attack.
- A financial institution experiences a phishing attack that distributes malicious attachments. RevBits MAS extracts indicators of compromise (IoCs), enabling the security team to update firewall rules and block further infiltration..

SOC & Threat Hunting Operations

- An organization suspects advanced persistent threat (APT) activity based on unusual registry modifications. RevBits MAS reveals the malware's persistence mechanisms and provides countermeasures.
- A cybersecurity team investigates anomalous behaviors in endpoint logs. RevBits MAS uncovers an undocumented variant of ransomware, allowing teams to develop proactive defense strategies.

Malware Research & Reverse Engineering

- A healthcare provider identifies new malware strains targeting their systems. The RevBits MAS provides detailed behavioral reports and sandbox execution logs for reverse engineering.
- A research firm analyzes malware samples from underground forums. RevBits MAS extracts the encryption techniques used by threat actors.

Digital Forensics & Compliance

- Forensic investigators and regulatory compliance teams trace cyberattacks and maintain industry-standard compliance by integrating the RevBits MAS into their workflows.
- An e-commerce company investigates data breaches affecting customer credentials. The RevBits MAS correlates malware activities with breach timestamps, aiding forensic teams.
- A government agency requires detailed malware assessments for regulatory documentation. The RevBits MAS generates comprehensive reports that align with cybersecurity compliance frameworks.

Enterprise Security & Risk Management

- A large organization employs RevBits MAS to strengthen its cybersecurity posture and manage cyber risks effectively.
- A retail corporation evaluates third-party applications before deployment. The RevBits MAS scans executables for embedded malicious scripts, ensuring supply chain security.
- An industrial manufacturer detects anomalies in IoT devices. The RevBits MAS identifies malware targeting embedded systems and recommends security measures.

Each of these use cases demonstrates how security teams can leverage the RevBits Malware Analysis Service to enhance their defense capabilities, improve incident response efficiency, and effectively mitigate threats.

Summary

By outsourcing malware analysis, organizations optimize their security investments, streamline operations, and leverage specialized expertise. The RevBits MAS utilizes static, dynamic, memory, network, and behavioral analysis to identify and neutralize malware threats. This service supports multiple cybersecurity applications, including incident response, SOC operations, malware research, digital forensics, and enterprise security risk management.

Through integrating automation and expert analysis, RevBits MAS augments your security team's capabilities to accelerate threat detection, ensure compliance, and proactively defend against evolving cyber threats.

Keep Your Enterprise Protected. Get a Demo or Free Evaluation.
To learn more, visit www.revbits.com

34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248) • www.revbits.com