SecondWrite

The ineffectiveness of signature based defenses has resulted in a wave of security solutions in the category of *automated malware analysis,* wherein a suspicious file observed at the network boundary or an endpoint is automatically submitted to an isolated environment, called a sandbox. A sandbox detonates (executes) this file, analyzes its behavior and classifies the object as malicious or benign. Automated sandboxes suffer from several limitations.

Evasive Malware

Evasive malware successfully bypass other sandboxes through sleeping, logic-bombs, targeted attacks, and zero-day evasions.

Anti-analysis Malware

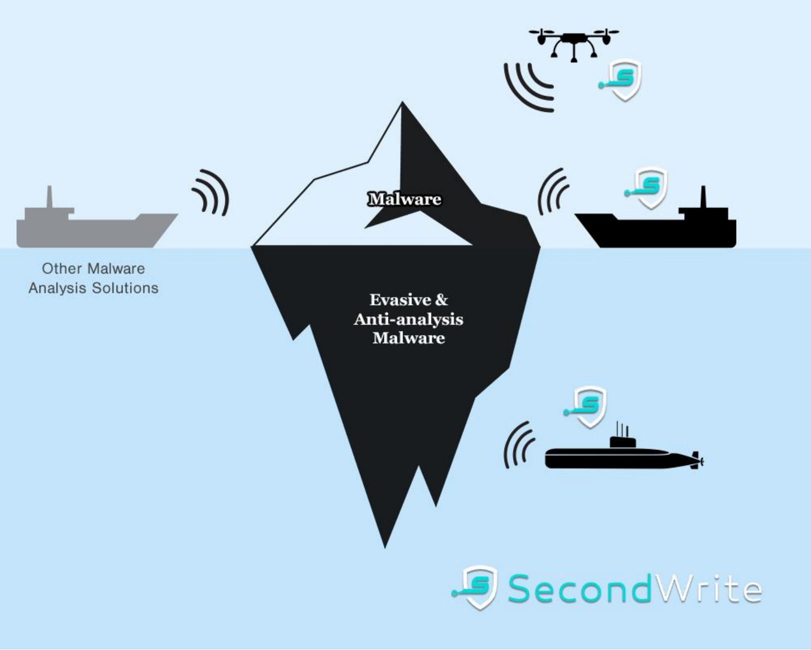
Other sandboxes fail to detect malware hiding from a variety of other tools, such as AV, endpoint and debuggers.

Blind Spots

A typical sandbox only monitors interaction of malware with operating system and lacks deep program introspection.

SECONDWRITE TECHNOLOGY

SecondWrite adds another dimension to malware analysis by including a component on deep program analysis at run time, leveraging our unique binary rewriting technology. This pushes the envelope of malware detection.



KEY ADVANTAGES

- Patent-pending university-developed technology.
- Handles all types of evasion:
  - Zero-day attacks
  - Sleeping
  - Useless Code
  - Logic Bombs
  - Targeted Attacks
- Captures Indicators of Compromise based on internal program properties:
  - Internal Program structure
  - Anti-analysis features
  - Anti-reverse engineering features.
- 95% zero-day detection rate with 1% False positive.

Next Generation Malware Analysis and Detection

SecondWrite

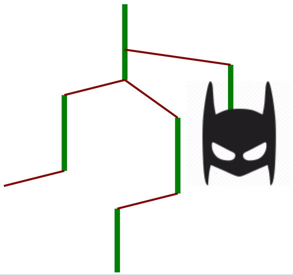
Windows Executables	MS Word (.doc and .docx)
Windows DLLs	MS Powerpoint (.ppt and .pptx)
.NET Executables	MS Excel (.xls and .xlsx)
PDF	HTML & URLs
Archives (.zip, .rar, .7z, .iso, .tar,.gz.,.bz2)	

Files, Attachments, URLs

SecondWrite sandbox accepts files of varied types shown above

Anti-evasive Technology

A patented technology performs complete code exploration forcing malware to be revealed



Program-level Features

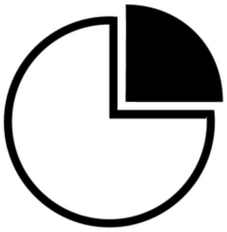
Captures Indicators of compromise such as internal program structure and anti-analysis features.

Easy to use API

Can be easily integrated with malware analysis workflows using programmable APIs

Comprehensive Analysis

Real network traffic,Yara and Suricata rules, detailed process behavior graphs and PCAP files.



Score & Report

Machine learning methods for malware classification. Reports available in JSON or HTML formats.

TRY IT OUT

SecondWrite sandbox is available as a cloud solution with free, basic and enterprise licenses. It is being used by SOCs, malware analysts, Incidence response professionals, network security vendors, endpoint security vendors, threat intelligence products, and MSSPs .

Sign up for your free license at www.secondwrite.com or write to us at info@secondwrite.com