Datasheet

MALWARE ANALYSIS

An enterprise that underwent a targeted attack must mandatorily perform analysis of the malicious code and not just rely on routine antivirus scan as

- There can be unknown malware samples that go undetected
- Knowing the features, capability and configurations of the malware sample helps to assess risk and potential impact
- Identify similar attacks in future via threat intelligence
- Removal of all persistence and artifacts created by the malware

Malware analysis by ActiveBytes experts frees your security team from time-consuming setup, baselining and restoration of the virtual machine environments used in malware analysis. In our sandbox mode analysis, the execution path of particular malware samples is fully contained and visible in the virtual environment. This is secure testing as the malicious program doesn't collaborate with the system. Also, we leverage malware communication protocol characteristics to perform dynamic blocking of data exfiltration attempts across the organization in the form of threat intelligence feeds.

Our malware analysis service includes

- Identify and assess assets and data at risk of exposure to malware
- Complete analysis of features and functionality through Reverse-engineering
- Identifying IOCs that will aid during threat hunting and forensic analysis
- Customized reports detailing the composition and behavior of malware
- Extraction of configuration (if applicable)
- Find whether the malware was customized to perform targeted attack

activebytes innovations

Our malware analysis is a multi-dimensioned approach that includes

- Static Code Analysis
- Windows Emulation
- Behavioral Analysis
- EXE and DLL Support
- YARA Rule Analysis
- Virtual Sandbox support for Office vand PDF files, JAVA, MSI, RTF, ZIP
- Inline, Real-time Blocking
- Full Windows OS Detonation
- File and URL Reputation
- Identifying indicators of compromise and recommending eradication steps
- Customized reports detailing the composition and behavior of malware, detonation

Key Features

- Analysis of suspicious web code, executables and files
- Reports in-depth on system level OS and application changes to file systems, memory and registries
- Sandbox analysis to confirm zero-day exploits
- Streamlined incident response prioritization
- Deep inspection of common web objects, email attachments and files. Malware
- Forensic data block outbound data exfiltration attempts and stop inbound known attacks
- In sandbox mode, the execution path of particular malware samples is fully contained and visible in the virtual environment.
- Threat data from analysis will be processed to threat intelligence

Benefits

- Uncover hidden IOCs which need to be immediately blocked
- Context enrichment during threat hunting
- Detect zero-day attacks
- Deep insight to prevent future attacks

Contact us

contact@active-bytes.com +971 50 513 3973

www.active-bytes.com