Deep Malware Analysis

JOE Sandbox Cloud

☑ Fully Cloud Based, No Installation Effort, Ready to Go

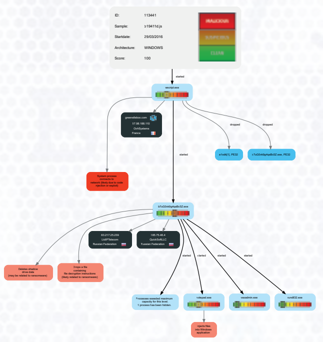
☑ Analysis on Windows, macOS, Linux and Android

☑ Deep Malware Analysis - from API Calls to Single Opcodes

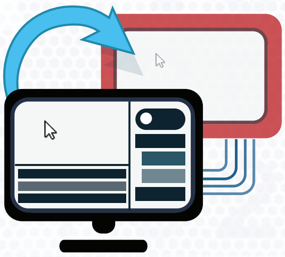
Classification

Ransomware
Evader
Spreading
Exploiter
malicious
suspicious
clean
Phishing
Spyware
Banker
Adware
BUY!
Trojan / Bot

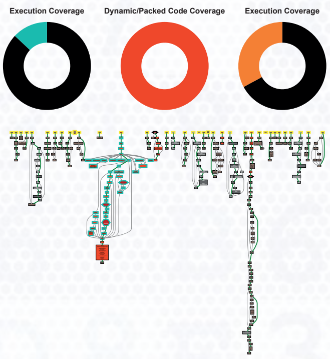
Behavior Graph



Live Interaction



Execution Graph



Highlights

- ☑ Fully Cloud Based, no installation effort, ready to go
- ☑ Deep Malware Analysis, unprecedented depth and detail of analysis
- ☑ Analysis on Windows, macOS, Linux and Android
- ☑ Analysis on virtual machines
- ☑ VBA Instrumentation for deep Macro analysis
- ☑ Hybrid Code Analysis, discovers hidden payloads and evasive behavior
- ☑ Hybrid Decompilation, generates c-code from binary code
- ☑ Execution Graph Analysis, visualizes the program code as a graph
- ☑ Automation Cookbook, fully control the analysis of a malware sample and change the analysis environment
- ☑ Live Interaction: Connect to the analysis machine and manually detonate malware
- ☑ Joe Sandbox Hypervisor PLUGIN uses latest hardware virtualization for deep and stealthy introspection
- ☑ Joe Sandbox ML PLUGIN Machine Learning and AI based malware detection

Key Features

- ☑ Behavior Graphs, visualizes the behavior of the malware in a graph
- ☑ High precision, low FP and FN for detection
- ☑ Reports in multiple formats: HTML, PDF, XML, JSON, MAEC and MISP
- ☑ 2437+ behavior signatures, identifies and classifies key behavior
- ☑ Extensive supplementary analysis data: memory dumps, dropped files, screenshots, unpacked PE files, Yara rules, strings, PCAP, shellcode, decompiled .Net and more
- ☑ IDA integration to load memory dumps
- ☑ Automated user behavior simulation, automatically clicks on buttons and other UI elements
- ☑ HTTPS inspection, analyzes encrypted network traffic
- ☑ Reporting system, notifies users based on detection or other events
- ☑ User management, create and manage users, share reports
- ☑ Fully private, no data and sample sharing

APIs and Integration

- ☑ Full integration via RESTful API to: upload, download, search, filter, alerts etc.
- ☑ Example scripts in Python available
- ☑ Yara editor: scans all downloads, uploads, memory dumps etc.
- ☑ Sigma, Snort and Cookbook editors
- ☑ Virustotal, Metadefender, Bro and Snort
- ☑ Threat Intelligence: Anomali, Misp, TheHive, Splunk, Swimlane, ReliaQuest and many more
- ☑ SOAR Integration: Cortex XSOAR, Splunk, Rapid7, Fortinet, Exabeam, ThreatConnect and many more
- ☑ Enpoint Protection: Microsoft Defender, Crowdstrike, SentinelOne, Kaspersky and many more

Explore Joe Sandbox Cloud

Contact Joe Security to schedule a technical presentation or to receive a free 14-days trial for Joe Sandbox Cloud Pro.

Joe Security LLC
business parc Reinach
Christoph Merian-Ring 11
4153 Reinach
Switzerland

JoeSecurity
www.joesecurity.org

✉ info@joesecurity.org
joe4security.blogspot.ch
twitter.com/joe4security
LinkedIn: Joe Security
Facebook: Joe Security