



Agile Malware Analysis

A unique Approach to fight evasive Cyber Threats!

Joe Security is the first vendor that introduces **Agile Malware Analysis** to the sandbox world. **Agile Malware Analysis** puts the fight against **evasive malware in the hands of security professional's** by providing a flexible, open and transparent analysis system. With the **unmatched flexibility** of the Joe Sandbox platform security professionals get a powerful tool to spot, analyze, detect and mitigate evasive malware.

[Checkout our Technology Whitepaper to learn more about Agile Malware Analysis.](#)

In order to assist security professionals in detecting and mitigating evasive cyber threats, Joe Security has developed a set of **cutting edge technologies** which are deeply integrated into Joe Sandbox:

Hybrid Code Analysis

■ Executed

■ Not executed



```
call eax
mov eax, dword[ebp-20h]
...
cmp eax, esi
jbe 300012h
call edx
```

GlobalMemoryStatus
executed
ExitProcess

```
300012h:
...
lea esi, dword ptr [ebp-420]
push esi
call dword ptr[ebx-55FD]
```

ASCII "C:\Windows\tmp.exe"
CreateFile

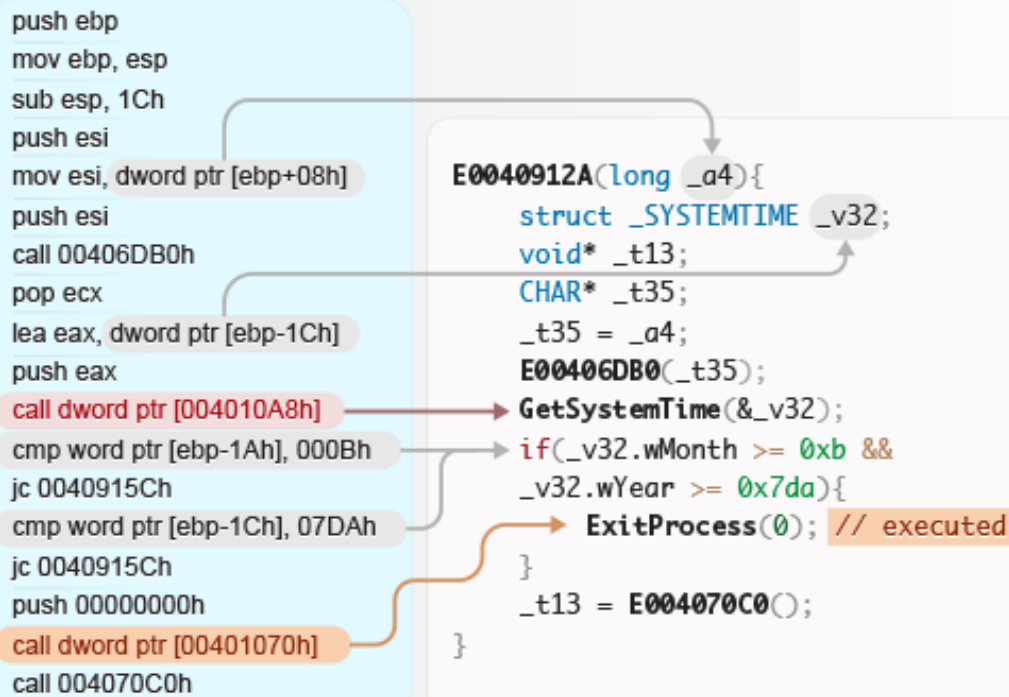
Hybrid Code Analysis

HCA

Hybrid Code Analysis (HCA) combines dynamic and static program analysis while retaining the main benefits of both techniques: context awareness, resilience against code obfuscation such as packing and self-modifying code on the one hand, and code analysis completion on the other hand. It enables to **understand evasions against malware analysis systems** including sleeps, logic bombs and system fingerprinting. Moreover, it allows discovering hidden behavior – dormant functionality which is executed only under rare conditions. Hybrid Code Analysis enables security professionals to understand the **complete malware behavior**, not just the installation.

Checkout [analysis reports](#) of latest malware for **Hybrid Code Analysis** or some of our latest blog posts: [New Sandbox Evasion Tricks](#) spot, [Finding a DGA in less than one Minute](#) and [Joe Sandbox aware Malware? Certainly not! But surely!](#).

Hybrid Decompilation



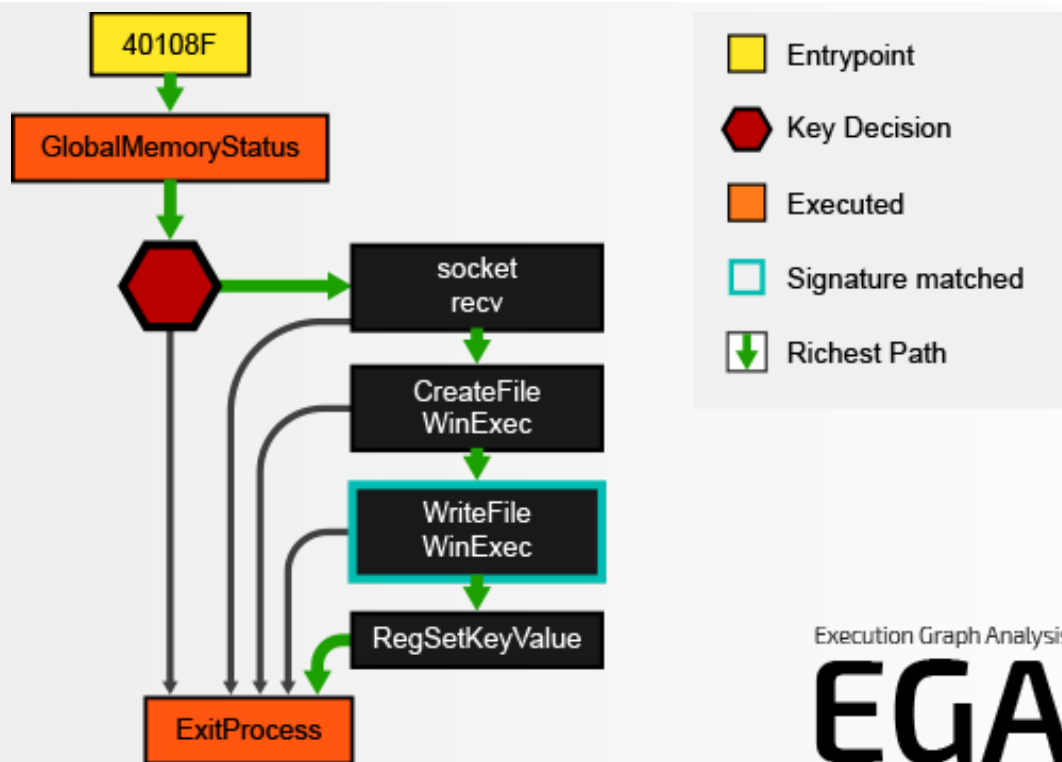
Hybrid Decompilation

HDC

Hybrid Decompilation (HDC) combines static decompilation techniques with knowledge of **dynamic code execution** to generate high level C-code. The automatically generated C-code features high-level control structures (if, do-while loops, switch statements), function parameters and local variables, high-level types (including high-level types for APIs), and function call arguments. Compared to standard decompilation Hybrid Decompilation directly **operates on memory** and **benefits from dynamic data** such as strings, function arguments and execution marks. Due to that HDC generates easy to understand codes which enable security professionals to quickly understand key behavior of evasive threats.

Checkout [codes](#) generated by **Hybrid Decompilation** or some of our latest blog posts: [Pure innovation: Hybrid Decompilation with Joe Sandbox DEC](#).

Execution Graph Analysis



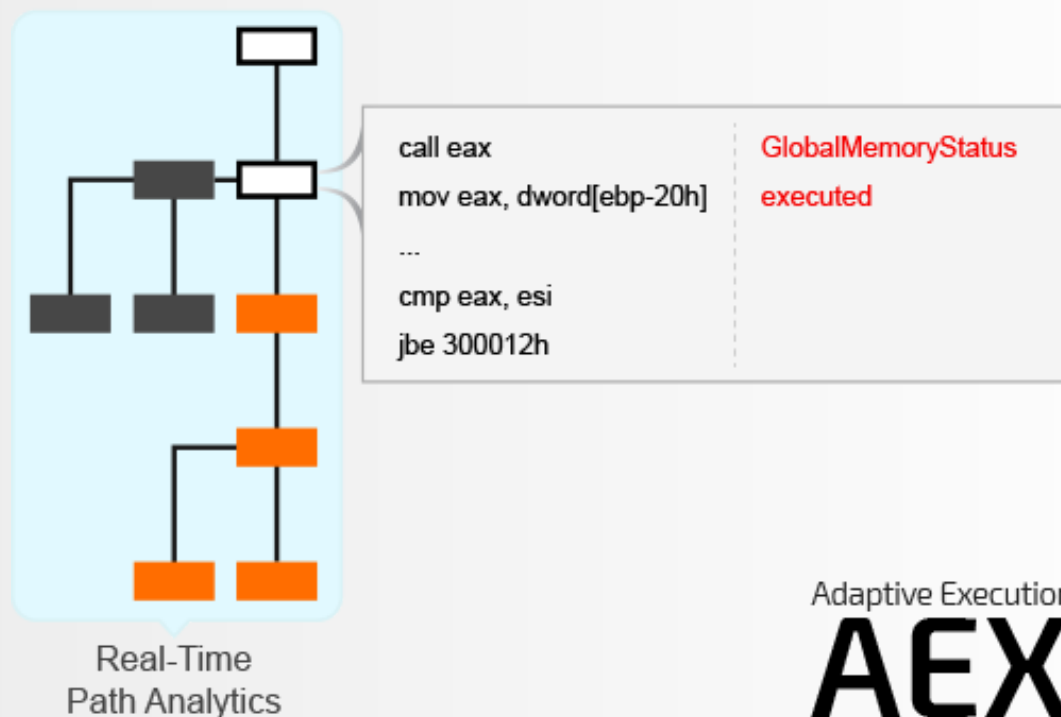
Execution Graph Analysis (EGA) generates highly **condensed control flow graphs**, so called Execution Graphs to visualize codes detected by Hybrid Code Analysis. Execution Graphs highlight the full logical behavior of the malware and include additional runtime information such as execution status, signature matches, key decisions, unpacked code and richest paths. Execution Graph Analysis **detects evasions against malware analysis systems completely automated**, without any human interaction. Furthermore EGA rates the behavior by looking at API chains, execution coverage and loops.

Checkout [analysis reports](#) of latest malware for **Execution Graph Analysis** or some of our latest blog posts: [The Power of Execution Graphs](#).

Adaptive Execution

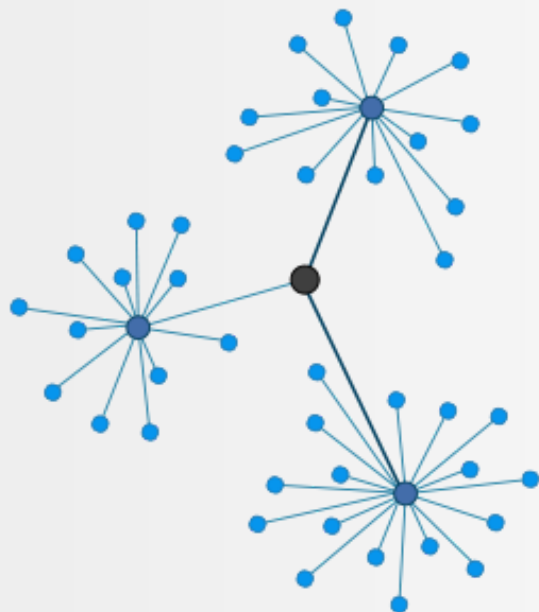
- Evasive Behavior







- Forced Payload Execution



Adaptive Execution (AEX) automatically detects and circumvents **evasive behavior**. To do so, key decisions of the program code are monitored constantly. If a key decision has been found adaptive execution detects if one of branches is pointing to evasive behavior. If so it **forces the execution of the alternative branch**. All this is done in **real time** during execution and completely **stealthy**. Adaptive Execution enables to analyze evasive malware **without fighting the cat and mouse game** of VM, user behavior or sandbox detection.

Extensive Behavior Signature Set



-  Document exploit detected (droppes PE files)
-  Modifies the hosts file
-  Sends SMS secretly using decrypted strings and reflection
-  Found dropped PE file which has not been started or loaded
-  Creates driver files
-  Urls found in memory or binary dat

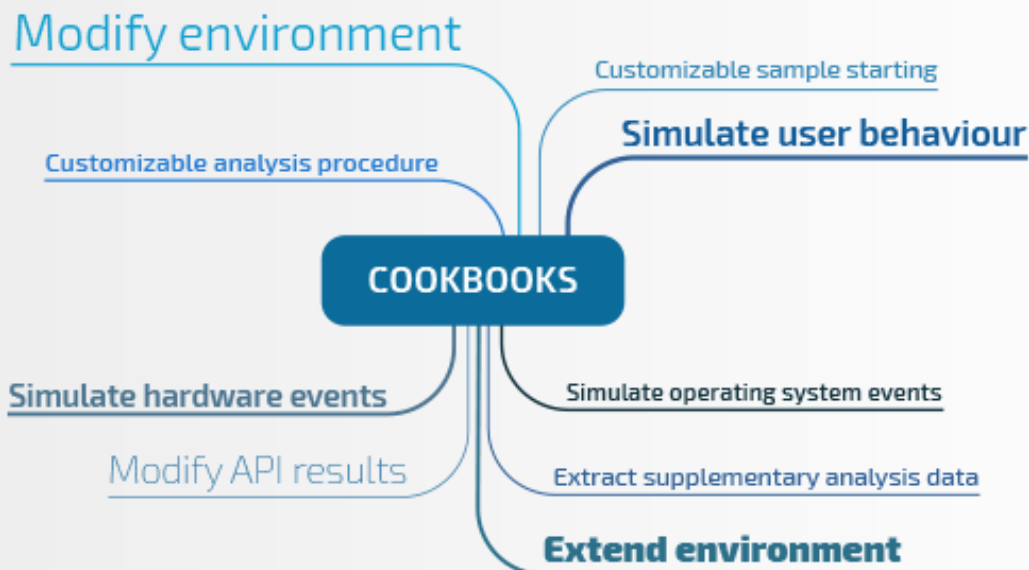
Behavior Signatures

SIG

Joe Security has one of the most extensive generic Behavior Signature set. The set consisting of over **830 signatures** covers multiple platforms including **Windows, Android and Mac OS X**. Behavior Signatures enable detecting, classifying and summarizing malicious behavior, dangerous code and **evasions**. Joe Sandbox applies each signature to an enormous amount of captured data ranging from **operating system to network, browser, memory, file, binary and screen data**.

Checkout [analysis reports](#) of latest malware for behavior signature results.

Cookbooks



Automation Cookbooks

CBK

While **Hybrid Code Analysis** and behavior signatures detect evasive threats, **Cookbooks** enable to easily **influence and change** the malware's behavior automatically. With **Cookbooks** security professionals can change the environment, simulate operating system events or modify the operating system behavior. **Cookbooks** also enable to completely customize the analysis procedure including malware startup, analysis duration and analysis chaining on multiple systems. The **Cookbook** technology makes Joe Sandbox the most flexible and customizable malware analysis system in the industry.

Checkout some of our latest blog posts to see Cookbooks in action: [New Sandbox Evasion Tricks spot](#) and [Joe Sandbox aware Malware? Certainly not! But surely!](#).

Joe Security LLC

business parc Reinach
Christoph Merian-Ring 11
4153 Reinach
Switzerland

[Contact](#)



swiss made
software



Information
Security Society
Switzerland



 Follow @joe4security

[Sitemap](#)

Copyright © 2015 Joe Security LLC