JoeSecurity

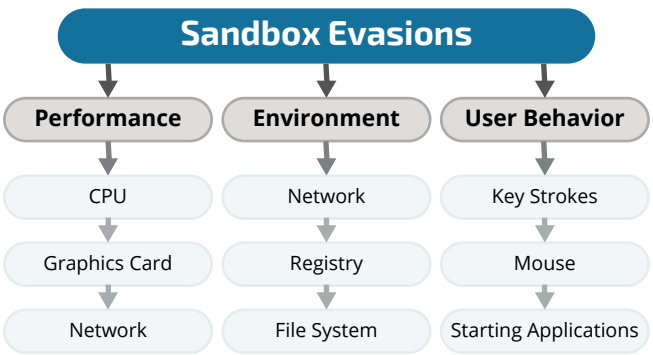
Fighting Evasive Cyber Threats

"Joe Sandbox analyses cyber threats in extreme depth. This enables us to detect and understand cyber threats which evade other malware analysis systems. Thanks to its flexibility of deployment and tuning, we were able to easily integrate Joe Sandbox into our existing malware analysis workflow."

CERT based in Switzerland

Today's evasive cyber threats can easily bypass traditional defences. As a result, enterprises have started to use automated malware analysis systems – so-called sandboxes - as an additional protection layer to proactively detect and block cyber threats. However, in response malware is becoming sandbox aware, bypassing detection and analysis.

Targeted and personalized attacks are very difficult to detect and prevent. To maximise success, malware is specifically crafted to evade any protective measures. This includes sandboxes, which execute code in a safe environment in order to detect malicious behaviour. Sandboxes work well since they cannot easily be defeated by using packing or code obfuscation – the two main techniques used to evade traditional defences such as antivirus software. However malware creators have also found various ways to evade analysis in sandboxes. One of the most common evasions is to check for differences between the sandbox environment and the real target. These differences can be at an environmental, CPU, user behaviour or even performance level. Corresponding checks are added to the malware to terminate, show fake behaviour or kill the machine if a sandbox is detected.



The image on the right shows two examples of evasive code. The first code sample is time aware. The malware only executes if the sandbox time is set to November 2010. Therefore, a sandbox will not detect any malicious behaviour. The second code sample checks for the number of CPU cores on the sandbox. If the sandbox has only one core, the sample goes into an endless sleep loop.

```
E0040912A(long _a4){
    struct _SYSTEMTIME _v32;
    void* _t13;
    CHAR* _t35;
    _t35 = _a4;
    E00406DB0(_t35);
    GetSystemTime(&_v32);
    if(_v32.wMonth >= 0xb &&
    _v32.wYear >= 0x7da){
        ExitProcess(0); // executed
    }
    _t13 = E004070C0();
}
```

Time based Evasive Code

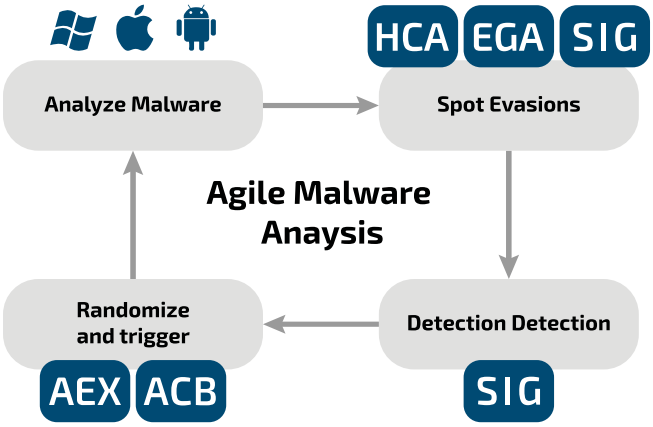
```
E0040924A(){
    int* _v44;
    _v44 =  *[fs:0x30];
    if(*(_v44 + 0x64)) < 2){
        while(1){
          Sleep(0x3e8); // executed
        }
    }
    E00403820();
}
```

Environment based Evasive Code

Agile Malware Analysis

Hybrid Code Analysis **HCA** | Execution Graph Analysis **EGA** | Adaptive Execution **AEX** | Behavior Signatures **SIG** | Analysis Cookbooks **ACB**

Sandbox evasions are very easy to implement but extremely difficult to find and eliminate. Unlike many of our competitors, Joe Security has focused on solving the problem of evasive threats. Joe Security's flagship product, Joe Sandbox Ultimate, includes a set of unique and innovative technologies to fight evasive threats. Joe Security has also developed a new security approach called Agile Malware Analysis to quickly adapt to the latest evasion techniques.



Agile Malware Analysis Process

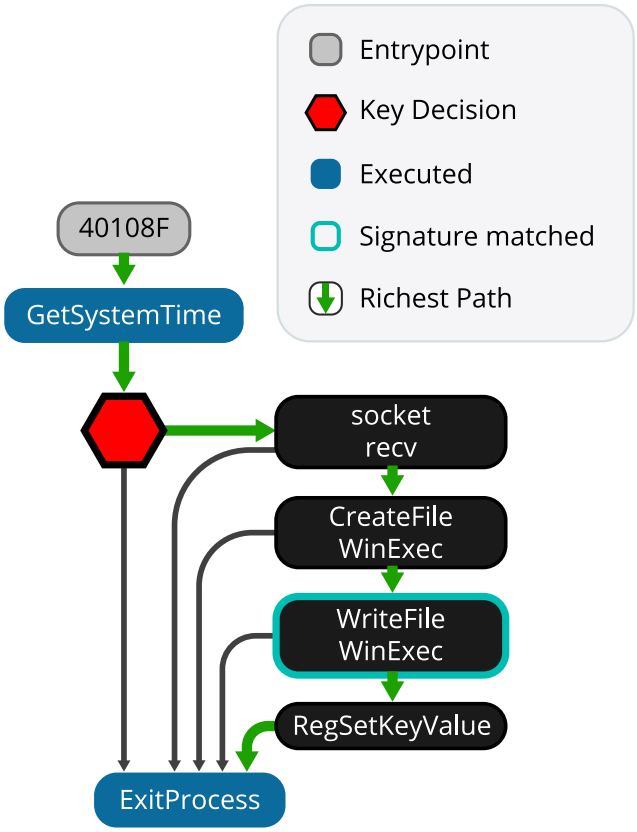
Joe Security is the first vendor to introduce Agile Malware Analysis to the sandbox world. Agile Malware Analysis puts the fight against evasive malware in the hands of security professionals by providing them a tool with the following advantages:

- Fine-grained, in-depth analysis
- Open, transparent and flexible system

Joe Sandbox's in-depth malware analysis engine includes Hybrid Code Analysis (HCA) and Execution Graph Analysis (EGA). Both techniques work on the binary code level and can help spot evasive codes. Once the evasive code has been detected, cyber security professionals can write a behaviour signature in order to detect the evasion in future threats (so-called detection detection). Finally, the evasive behaviour is eliminated via Adaptive Execution or by using the flexibility of Cookbooks, a technology to launch custom elimination code within a sandbox.

Hybrid Code Analysis 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 and code analysis completion. HCA extracts any malicious code, even if it is not executed or hidden. HCA is the base technology for Execution Graph Analysis. **Execution Graph Analysis** generates highly condensed control flow graphs (so-called execution graphs) to visualize codes detected via HCA. Execution graphs highlight the full logical behaviour of the malware and include additional runtime information such as execution status, signature matches, key decisions, unpacked code and richest paths.

Due to their design and format, execution graphs allow easy recognition of attempts to evade malware analysis systems. The complete graph can be rated by using behaviour signatures.



Execution Graph Analysis

Fighting Evasive Cyber Threats

About Joe Security

Joe Security specializes in the development of automated malware analysis systems for malware detection and forensics. Based on the agile malware analysis methodology, we have developed unique and patent-pending technologies to analyse advanced malware, even if the malware tries to evade analysis. These innovative technologies allow malware analysis at previously unavailable depths. Joe Security offers malware analysis systems as a cloud service or on premises of any size for Windows, Android and Mac based operating systems. Joe Security's malware analysis systems are built with openness in mind and are therefore extremely flexible.

With booming markets in Europe and the United States, Joe Security operates worldwide. Our customers include CIRTs and CERTs from small to large corporations which use our products as a daily tool to protect their infrastructure. Antivirus and firewall vendors have seamlessly integrated our products for efficient automated malware detection on a large scale.

Joe Security is renowned for providing excellent technical support with low response times. We listen extremely carefully to customers' requirements. This allows us to develop effective malware analysis systems which are among the best in the world!

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

info@joesecurity.org
www.joesecurity.org