

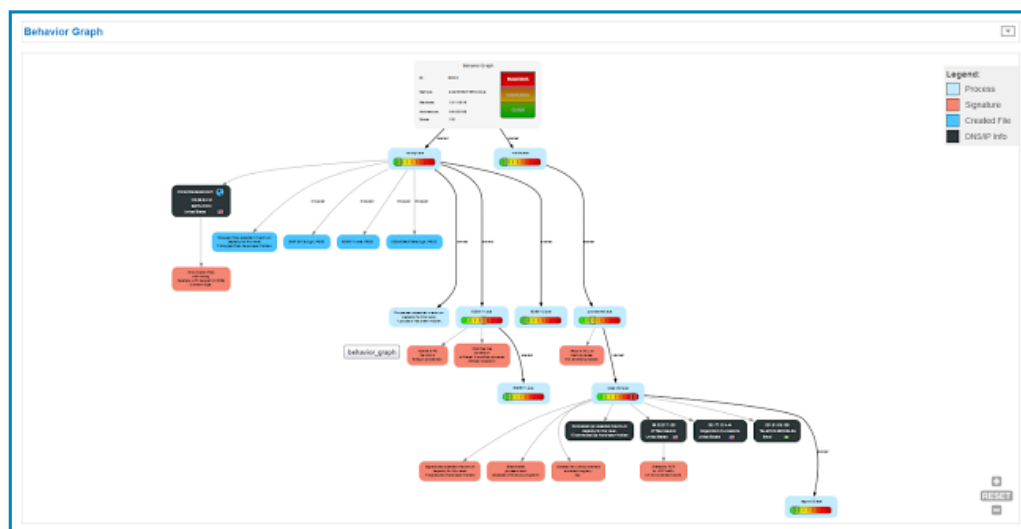
# Automated Malware Analysis

## Introducing Behavior Graphs in Joe Sandbox 13

We are proud to release today **Joe Sandbox 13**! The 13 release includes a couple of very cool new features, including:

- Support for Windows 10
- 70 new behavior signatures
- Analysis advice signatures
- Static unpackers for VBE and SWF
- Live system performance statistics in the web interface
- COM Analysis
- String analysis in compressed files
- Static file analysis for Flash
- Static PE file analysis for dropped / downloaded files
- New tricks to prevent VM-detection
- ASN detection for IPs
- Code obfuscation detection for [Hybrid Code Analysis \(HCA\)](#)
- Behavior graphs
- [Hybrid Decompilation \(HDC\)](#) Plugin
- Big performance improvements

Beside of the Hybrid Decompilation (DEC) Technology we have also developed a new feature called Behavior graphs. Behavior graphs are new graphs which display the behavior of a sample. They show processes, IPs, domains, dropped files as well as behavior signatures in a connected graph. The graph coloring is very simple and intuitive while the format is clean and well structured.



We also invested lot of brain power into shrinking and compressing the graph so that it stays small and clear.

Below you find several behavior graphs with the corresponding Joe Sandbox analysis report:

### Subscribe

[Newsletter](#)

### Analyzers

[Joe Sandbox Cloud](#)

[File Analyzer](#)

[APK Analyzer](#)

[Document Analyzer](#)

[URL Analyzer](#)

### Generators

[Yara Rule Generator](#)

### Links

[Joe Security Products](#)

[Mobile Blog Archive](#)

[Joe Security on Twitter](#)

### Tweets

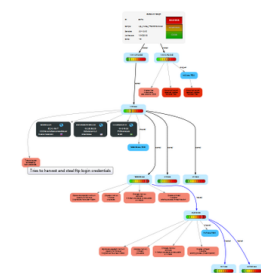
[Follow](#)



**Joe Security LLC** 18h  
@joe4security

Nice Behavior Graph of latest UPS doc dropping Dyre:

[joesecurity.org/reports/lightr...](#)  
#DFIR #MALWARE  
[pic.twitter.com/E0ARNjSNRd](#)



Tweet to @joe4security

### Blog Archive

▼ 2015 (9)

▼ November (1)

[Introducing Behavior Graphs in Joe Sandbox 13](#)

► September (1)

► August (1)

► July (1)

► June (1)

► May (1)

► April (1)

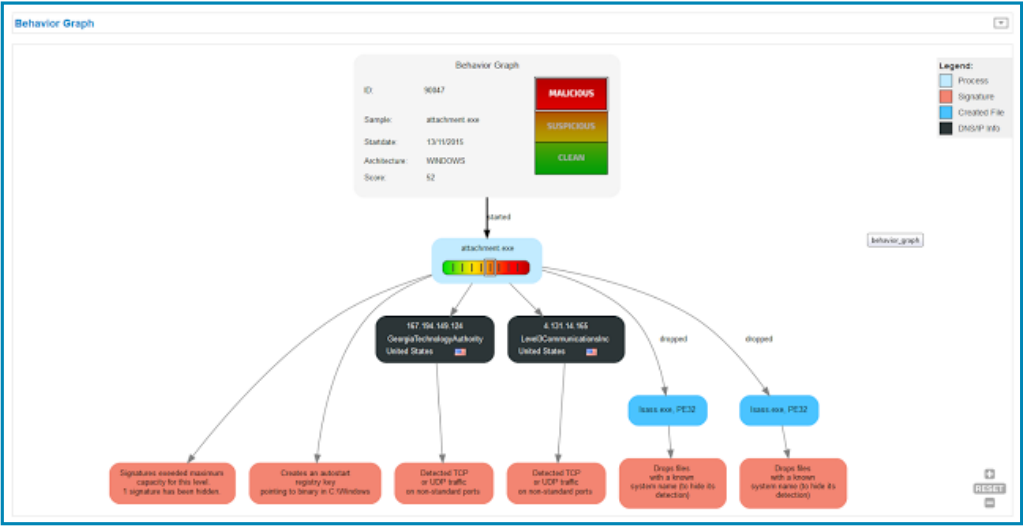
► February (1)

► January (1)

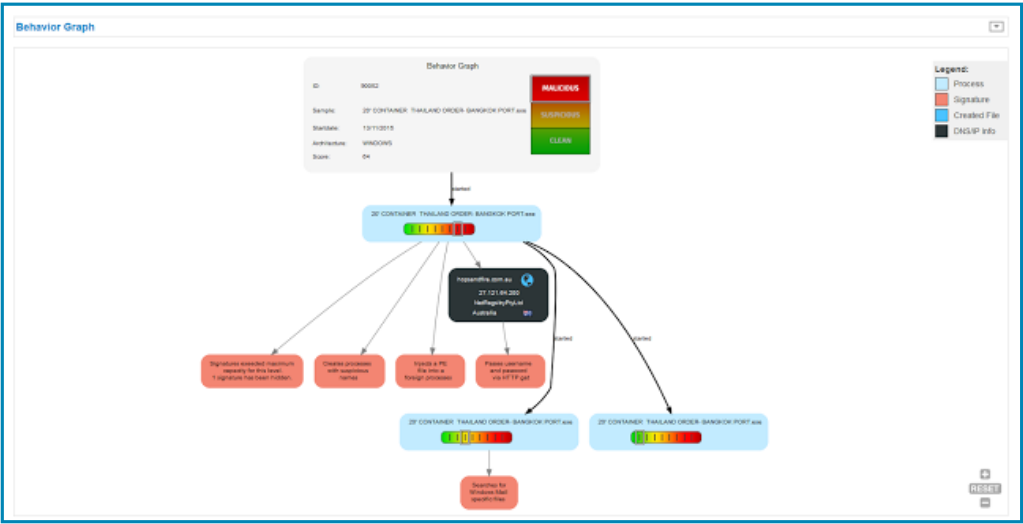
► 2014 (11)

► 2013 (10)

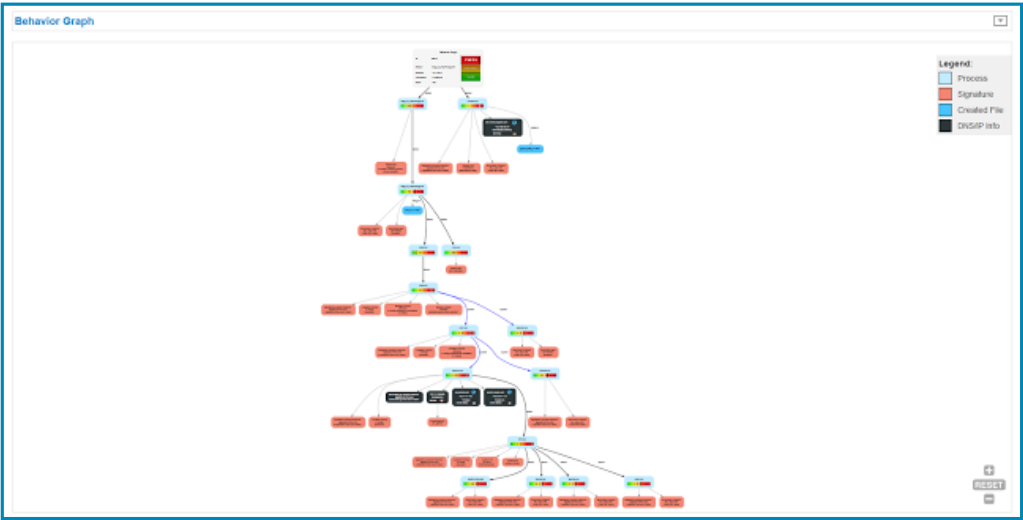
► 2012 (12)



- [Joe Sandbox 13 Analysis for a44d377b7916cd7a08240d1d0fc4ba32](#)



- [Joe Sandbox 13 Analysis for f1af3fc4d59d1245889811b7ed7d2cec](#)



- [Joe Sandbox 13 Analysis for 51365B90CD5E3671852E5C28EAB20A63](#)

Posted by joesecurity  
Monday, November 16, 2015  
10:07 AM

