

JoeSandbox Cloud BASIC



**ID:** 634139

**Sample Name:** pago.exe

**Cookbook:** default.jbs

**Time:** 16:46:01

**Date:** 25/05/2022

**Version:** 34.0.0 Boulder Opal

## Table of Contents

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| Table of Contents                                                                | 2  |
| Windows Analysis Report pago.exe                                                 | 4  |
| Overview                                                                         | 4  |
| General Information                                                              | 4  |
| Detection                                                                        | 4  |
| Signatures                                                                       | 4  |
| Classification                                                                   | 4  |
| Process Tree                                                                     | 4  |
| Malware Configuration                                                            | 4  |
| Threatname: GuLoader                                                             | 4  |
| Yara Signatures                                                                  | 4  |
| Memory Dumps                                                                     | 4  |
| Sigma Signatures                                                                 | 4  |
| Snort Signatures                                                                 | 5  |
| Joe Sandbox Signatures                                                           | 5  |
| AV Detection                                                                     | 5  |
| Networking                                                                       | 5  |
| Data Obfuscation                                                                 | 5  |
| Malware Analysis System Evasion                                                  | 5  |
| Mitre Att&ck Matrix                                                              | 5  |
| Behavior Graph                                                                   | 5  |
| Screenshots                                                                      | 6  |
| Thumbnails                                                                       | 6  |
| Antivirus, Machine Learning and Genetic Malware Detection                        | 7  |
| Initial Sample                                                                   | 7  |
| Dropped Files                                                                    | 7  |
| Unpacked PE Files                                                                | 7  |
| Domains                                                                          | 7  |
| URLs                                                                             | 8  |
| Domains and IPs                                                                  | 8  |
| Contacted Domains                                                                | 8  |
| URLs from Memory and Binaries                                                    | 8  |
| World Map of Contacted IPs                                                       | 8  |
| General Information                                                              | 8  |
| Warnings                                                                         | 9  |
| Simulations                                                                      | 9  |
| Behavior and APIs                                                                | 9  |
| Joe Sandbox View / Context                                                       | 9  |
| IPs                                                                              | 9  |
| Domains                                                                          | 9  |
| ASNs                                                                             | 9  |
| JA3 Fingerprints                                                                 | 9  |
| Dropped Files                                                                    | 9  |
| Created / dropped Files                                                          | 9  |
| C:\Users\user\AppData\Local\Temp\Adventure_15.bmp                                | 9  |
| C:\Users\user\AppData\Local\Temp\BRUGERMSSIGE.dis                                | 10 |
| C:\Users\user\AppData\Local\Temp\Lovprisendes8.omb                               | 10 |
| C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualBasic.dll | 10 |
| C:\Users\user\AppData\Local\Temp\application-exit-symbolic.symbolic.png          | 11 |
| C:\Users\user\AppData\Local\Temp\insaB9F5.tmp\System.dll                         | 11 |
| C:\Users\user\AppData\Local\Temp\process-stop-symbolic.svg                       | 11 |
| Static File Info                                                                 | 12 |
| General                                                                          | 12 |
| File Icon                                                                        | 12 |
| Static PE Info                                                                   | 12 |
| General                                                                          | 12 |
| Authenticode Signature                                                           | 13 |
| Entrypoint Preview                                                               | 13 |
| Rich Headers                                                                     | 14 |
| Data Directories                                                                 | 14 |
| Sections                                                                         | 14 |
| Resources                                                                        | 14 |
| Imports                                                                          | 15 |
| Version Infos                                                                    | 15 |
| Possible Origin                                                                  | 15 |
| Network Behavior                                                                 | 15 |
| Statistics                                                                       | 16 |
| System Behavior                                                                  | 16 |
| Analysis Process: pago.exePID: 5312, Parent PID: 3460                            | 16 |
| General                                                                          | 16 |
| File Activities                                                                  | 16 |
| File Created                                                                     | 16 |
| File Deleted                                                                     | 17 |
| File Written                                                                     | 17 |
| File Read                                                                        | 21 |

|                     |    |
|---------------------|----|
| Registry Activities | 21 |
| Key Created         | 21 |
| Key Value Created   | 21 |
| Disassembly         | 22 |





































