

JoeSandbox Cloud BASIC



ID: 877004

Sample Name: Mcafe.exe

Cookbook: default.jbs

Time: 11:09:22

Date: 28/05/2023

Version: 37.1.0 Beryl

Table of Contents

Table of Contents	2
Windows Analysis Report Mcafe.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	3
Joe Sandbox Signatures	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
World Map of Contacted IPs	7
General Information	7
Warnings	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASNs	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	8
General	8
Entrypoint Preview	9
Data Directories	10
Sections	11
Resources	11
Imports	11
Exports	11
Possible Origin	12
Network Behavior	12
Statistics	12
System Behavior	12
Analysis Process: Mcafe.exePID: 6080, Parent PID: 3452	12
General	12
Disassembly	12

