

JOESandbox Cloud BASIC



ID: 755881

Sample Name: E-DEKONT.exe

Cookbook: default.jbs

Time: 09:09:52

Date: 29/11/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report E-DEKONT.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Memory Dumps	4
Sigma Signatures	4
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	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	7
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
World Map of Contacted IPs	8
General Information	8
Warnings	8
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\nsc1ED3.tmp\System.dll	9
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Internalisere\Brnesangen.End	9
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Slde\memstat.c	10
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Slde\selection-end-symbolic.symbolic.png	10
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\logicalization\libxml2-2.0.typelib	10
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\logicalization\sgelngdernes.Dep74	11
Static File Info	11
General	11
File Icon	11
Static PE Info	12
General	12
Entrypoint Preview	12
Rich Headers	13
Data Directories	13
Sections	13
Resources	14
Imports	14
Possible Origin	15
Network Behavior	15
Statistics	15
System Behavior	15
Analysis Process: E-DEKONT.exePID: 3648, Parent PID: 3324	15
General	15
File Activities	15
File Created	15
File Deleted	18
File Written	18
File Read	20
Registry Activities	20
Key Created	20
Key Value Created	20
Disassembly	21

