

JOeSandbox Cloud BASIC



ID: 560537

Sample Name:

gnAYDP69br2v.vbs

Cookbook: default.jbs

Time: 16:57:03

Date: 26/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report gnAYDP69br2v.vbs	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: Ursnif	3
Yara Overview	3
Memory Dumps	4
Unpacked PEs	4
Sigma Overview	4
Jbx Signature Overview	4
AV Detection	4
Key, Mouse, Clipboard, Microphone and Screen Capturing	4
E-Banking Fraud	4
Data Obfuscation	4
Persistence and Installation Behavior	4
Hooking and other Techniques for Hiding and Protection	4
Malware Analysis System Evasion	5
Anti Debugging	5
HIPS / PFW / Operating System Protection Evasion	5
Stealing of Sensitive Information	5
Remote Access Functionality	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	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\adobe.url	9
C:\Users\user\AppData\Local\Temp\melange.yuv	10
Static File Info	10
General	10
File Icon	10
Network Behavior	10
Statistics	11
Behavior	11
System Behavior	11
Analysis Process: wscript.exePID: 6536, Parent PID: 3440	11
General	11
File Activities	11
File Deleted	11
Analysis Process: WmiPrvSE.exePID: 6620, Parent PID: 792	11
General	11
Analysis Process: rundll32.exePID: 6788, Parent PID: 6620	12
General	12
File Activities	12
File Read	12
Analysis Process: rundll32.exePID: 6772, Parent PID: 6788	12
General	12
Disassembly	13

