JoeSandbox Cloud BASIC

ID: 430987
Sample Name: vbc.exe.vir
Cookbook: default.jbs
Time: 10:11:10
Date: 08/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

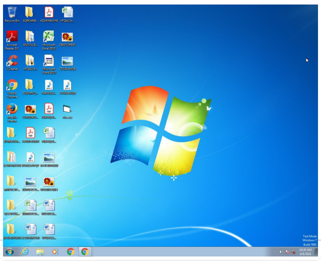
Analysis Report vbc.exe.vir

Overview

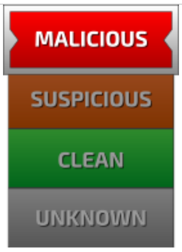
General Information

Sample Name:	vbc.exe.vir (renamed file extension from vir to exe)
Analysis ID:	430987
MD5:	788016c9072423..
SHA1:	040f85b4ef512bb..
SHA256:	df34f3d4030a5ea..
Infos:	

Most interesting Screenshot:



Detection



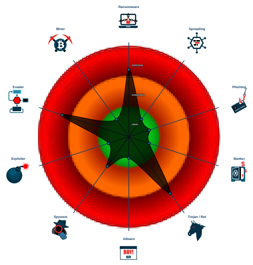
GuLoader

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Allocates memory within range whic…
- Contains functionality for execution …
- Contains functionality to call native f…
- Contains functionality to query CPU …

Classification



Process Tree

- **System is w7x64**
- vbc.exe.exe (PID: 2400 cmdline: 'C:\Users\user\Desktop\vbc.exe.exe' MD5: 788016C9072423914B96F0D15A61812D)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://bara-seck.com/bin_YIuwAXdc211.bin, https://wizumiya.co.jp/html/user_data/"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
vbc.exe.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.2095163938.0000000000401000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000000.00000002.3175874940.0000000000401000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.vbc.exe.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
0.2.vbc.exe.exe.400000.1.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

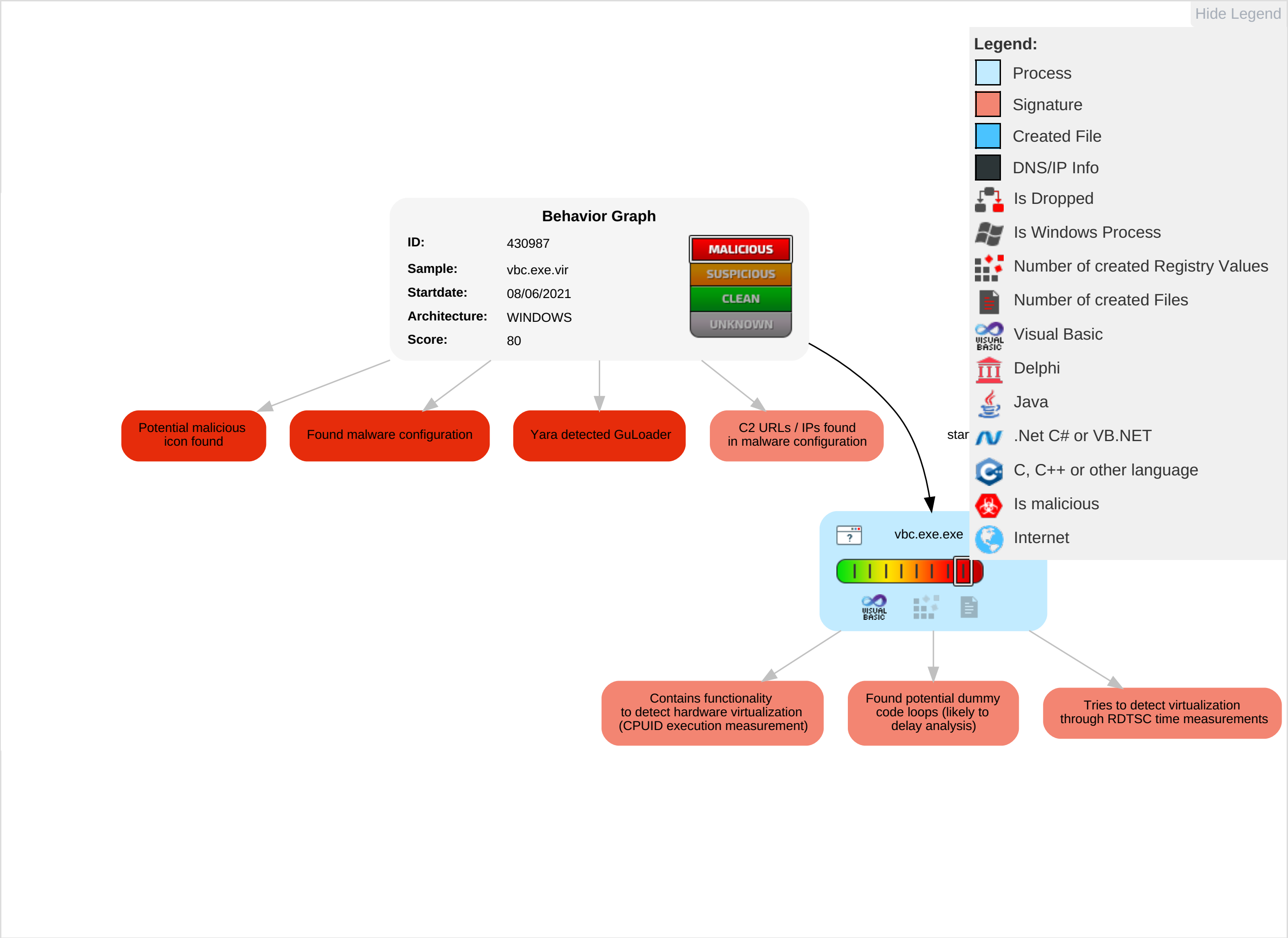
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	R W W A

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



Hide Legend

Behavior Graph

ID: 430987

Sample: vbc.exe.vir

Startdate: 08/06/2021

Architecture: WINDOWS

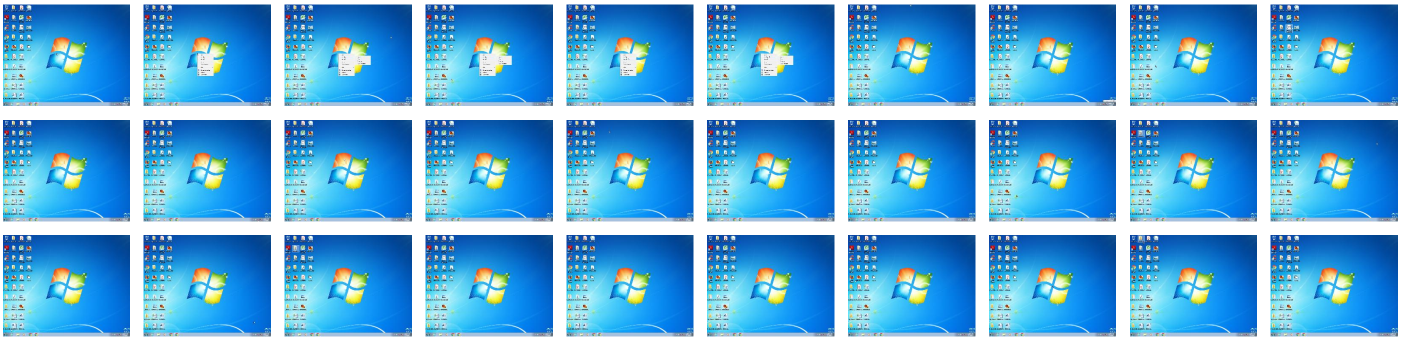
Score: 80

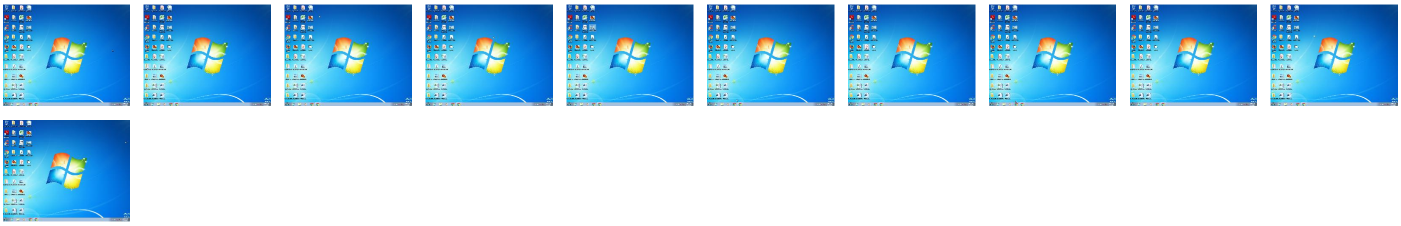
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Potential malicious icon found
Found malware configuration
Yara detected GuLoader
C2 URLs / IPs found in malware configuration
star
vbc.exe.exe
Contains functionality to detect hardware virtualization (CPUID execution measurement)
Found potential dummy code loops (likely to delay analysis)
Tries to detect virtualization through RDTSC time measurements
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

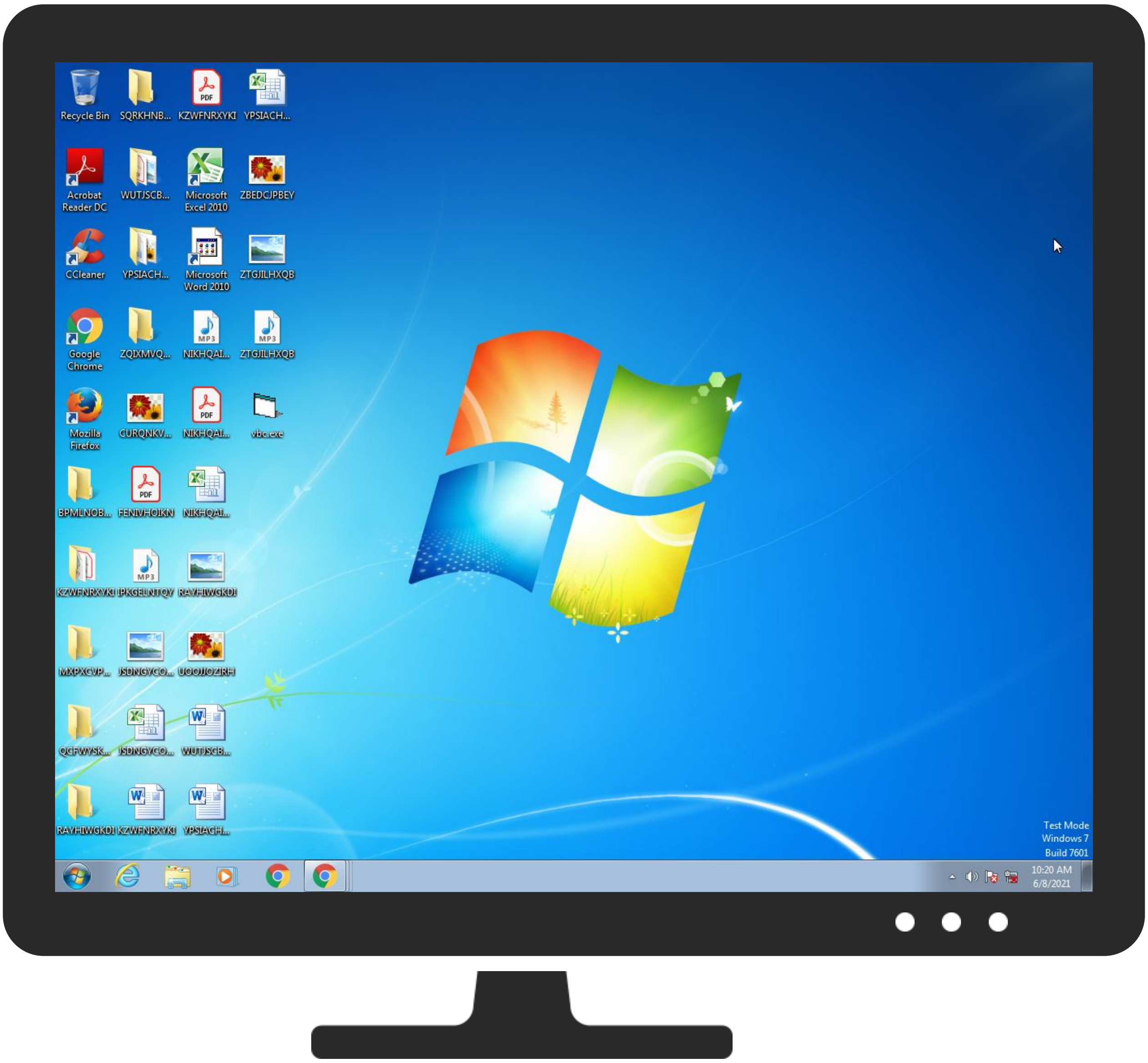
Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bara-seck.com/bin_YIuwAXdc211.bin, https://wizumiya.co.jp/html/user_data/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bara-seck.com/bin_YIuwAXdc211.bin, https://wizumiya.co.jp/html/user_data/	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	430987
Start date:	08.06.2021
Start time:	10:11:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vbc.exe.vir (renamed file extension from vir to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	2
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 15.9% (good quality ratio 5.2%) • Quality average: 18% • Quality standard deviation: 27.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

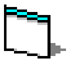
General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.60090149728624
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	vbc.exe.exe
File size:	147456
MD5:	788016c9072423914b96f0d15a61812d
SHA1:	040f85b4ef512bb74990becfa1a5029f92eb65c7
SHA256:	df34f3d4030a5ea484108271f749ca5fbc3af0f415051e98b342a505c88971e4
SHA512:	c9a75e6b54113d3d02c32d314ff76cc82b9bd4b88d07fec6b7636417e49184ebb691ecf63db3aac8dd4a96e49392959638c70ab20412f1c4454ac7963266c2c4
SSDEEP:	3072:JX84PzFh5UOkyp2te2+4lM20JMN0z3wnz:xxFjpYF+4lM20JMN0z3A

General

File Content Preview:	MZ.....................@..!..L.!Th is program cannot be run in DOS mode....$........#...B...B ...B..L^...B...`...B...d...B..Rich.B..........PE..L...x..Q.................0............... ....@................

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401c10
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x51CF9578 [Sun Jun 30 02:18:32 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	9b8686288ab82fdbf8ede30bc55c83b7

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20608	0x21000	False	0.357185132576	data	5.84922850488	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1250	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x970	0x1000	False	0.1728515625	data	2.05495100774	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: vbc.exe.exe PID: 2400 Parent PID: 912

General

Start time:	10:11:44
Start date:	08/06/2021
Path:	C:\Users\user\Desktop\vbc.exe.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\vbc.exe.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	788016C9072423914B96F0D15A61812D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000000.2095163938.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000002.3175874940.0000000000401000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis