

JoeSandbox Cloud BASIC



ID: 755946

Sample Name:

SecuriteInfo.com.Win32.PWSX-
gen.27251.20675.exe

Cookbook: default.jbs

Time: 10:44:30

Date: 29/11/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report SecuriteInfo.com.Win32.PWSX-gen.27251.20675.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: FormBook	4
Yara Signatures	6
Memory Dumps	6
Unpacked PEs	6
Sigma Signatures	7
Snort Signatures	7
Joe Sandbox Signatures	7
AV Detection	7
Networking	7
E-Banking Fraud	7
System Summary	7
Malware Analysis System Evasion	8
HIPS / PFW / Operating System Protection Evasion	8
Stealing of Sensitive Information	8
Remote Access Functionality	8
Mitre Att&ck Matrix	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	10
Domains and IPs	11
Contacted Domains	11
Contacted URLs	12
URLs from Memory and Binaries	12
World Map of Contacted IPs	15
General Information	15
Warnings	16
Simulations	16
Behavior and APIs	16
Joe Sandbox View / Context	16
IPs	16
Domains	16
ASNs	16
JA3 Fingerprints	16
Dropped Files	16
Created / dropped Files	17
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.PWSX-gen.27251.20675.exe.log	17
Static File Info	17
General	17
File Icon	17
Static PE Info	17
General	17
Entrypoint Preview	18
Data Directories	19
Sections	20
Resources	20
Imports	20
Network Behavior	20
Statistics	20
Behavior	20
System Behavior	21
Analysis Process: SecuriteInfo.com.Win32.PWSX-gen.27251.20675.exePID: 5448, Parent PID: 3320	21
General	21
File Activities	21
File Created	21
File Written	22
File Read	22
Analysis Process: SecuriteInfo.com.Win32.PWSX-gen.27251.20675.exePID: 5572, Parent PID: 5448	22
General	22

Disassembly

