

ID: 626308
Sample Name:
SecuriteInfo.com.W32.AIDetectNet.01.21425.740
Cookbook: default.jbs
Time: 20:41:11
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.W32.AIDetectNet.01.21425.740 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 7
Stealing of Sensitive Information 7
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 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 14
General Information 14
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.21425.exe.log 15
Static File Info 15
General 15
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 16
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 19
Network Behavior 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.21425.exePID: 3748, Parent PID: 5704 19
General 19
File Activities 20
File Created 20
File Written 20
File Read 20
Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.21425.exePID: 3620, Parent PID: 3748 21
General 21
File Activities 21
File Read 21

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022