GS Analyzer

Static binary threat analysis

GS Analyzer is a binary threat-assessment upgrade for GateScanner suite.

Executable malicious code within files poses a major challenge for detection and mitigation. The SolarWinds supply chain attack of 2020 saw a major software developer targeted, and malicious code injected into its software updates. As a result, customers inadvertently installed malware onto their systems, providing attackers with backdoors to hundreds of affected networks in government, technology firms, and major entities around the world.

The challenge lies in the fact that the malicious nature of an executables is not evident until it is run, and often - much later than that. The infection of SolarWinds' Orion platform updates had gone undetected for nearly nine months.

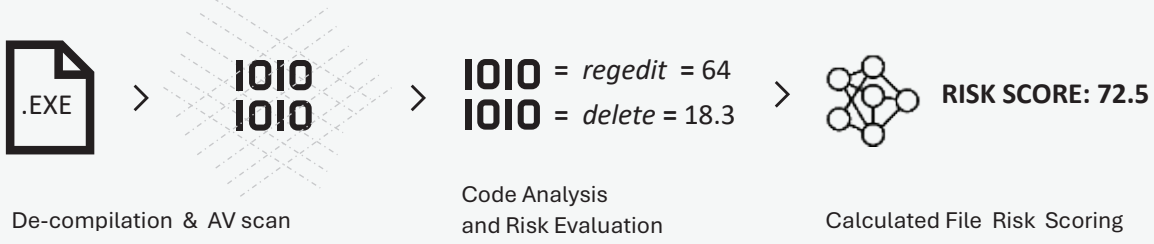
Sandboxing - the standard line of defence against threat in executables, has limitations, being resource-intensive and introducing considerable delay. Furthermore, sophisticated malware can detect sandbox environments and alter its behaviour to evade detection.

An innovative approach is the application of static binary analysis for threat evaluation. The de-compilation of the code (i.e. its reverse engineering) offers a view into the functionality of the execution code - without actually running it.

Execution flow, data structures, and interactions with the operating system and other software components, are all analysed and scored, to quantify the risk they represent. A total risk score for the file is then calculated.

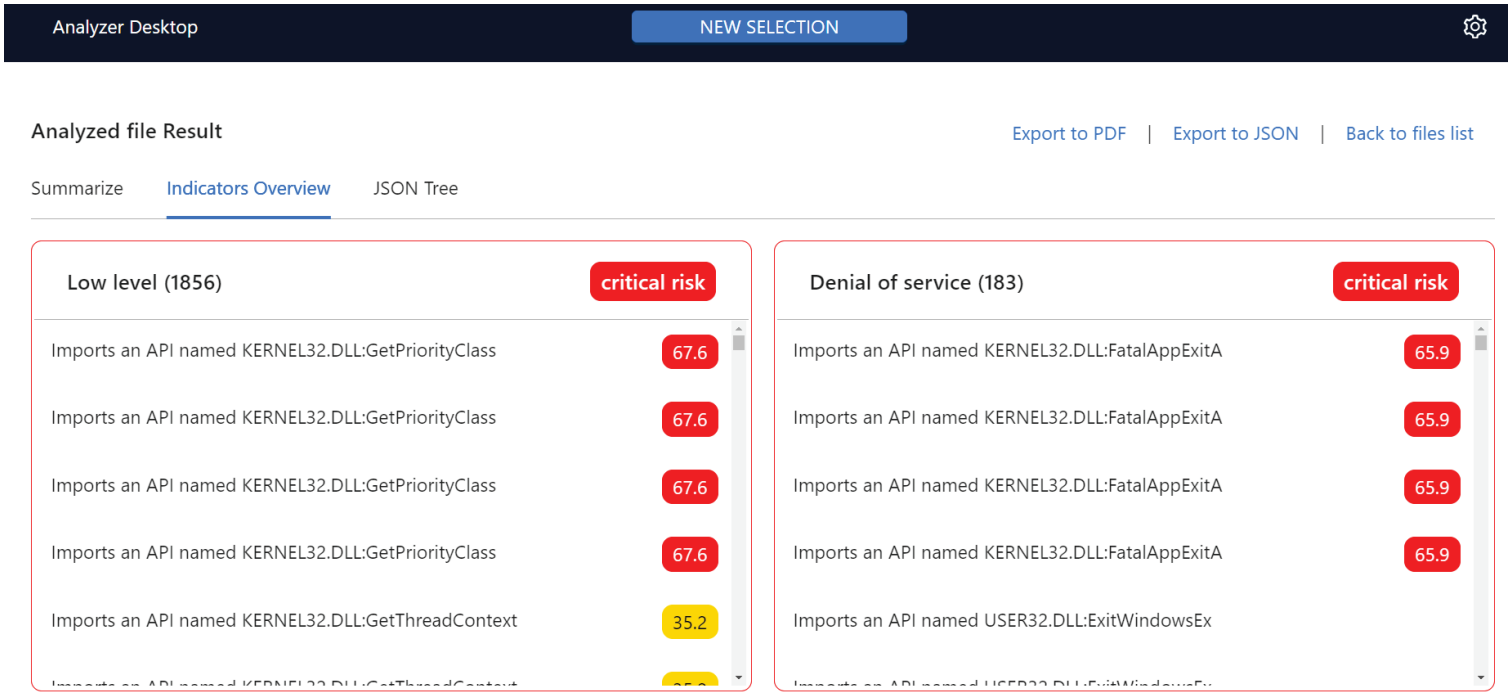
This score can serve as a threshold for automated threat-based filtering of executable content, enabling admins to quickly channel-out high-risk content.

GS Analyser processing stages:



GS Analyzer supports a broad range of file types , including:
EXE, WIN_PE, BASE64, COM, MACHO, SCRIPT, SYS, VHD, VNWR, XML (see reverse side for a full list)

GATESCANNER GS ANALYZER
by Sasa Software



GS Analyzer overview panel showing the risk scoring of decompiled executable content within a file

Supported file types:

ACE | BZ2 | CAB | DMG | GZIP | LZIP | LZMA | RPM | TAR | XZ | 7Z | 8VY2 | 8BY3 | AIF | ALZ | AMI | APP | AR | ARJ | AUTOIT | BASE64 | BAT | BMP | BINXML | BOOT | CDR | CHM | COM | CRX | CRTF | CPIO | DBS | DEX | DFL | DOOM | DUMP | E32 | E64 | EBCDIC | EGG | EMF | ENC | EXE | FAT_MACHO | FDBS | GIF | HA | HDBS | HFS | HLP | HQX | HTA | HQX | INI | INNO | IS | ISO | ICR | INF | IMATE | JET | JAVA | JOB | JEG | LZH | LNX | LINEAR | MACHO | MACBIN | MACHYPER | MACPEF | MACRSRC | MBR | MF | MIME | MSLZ | MSO | NSIS | OBJ | OLE | OLESTREAM | OS2_LE | OS2_LX | PALM | PDF | PIF | PNG | PHP | RAR | REG | RIFF | RISI | RTF | SH | SIM | SIS | SLK | SWF | SCRIPT| SUB | SUHD | SYMBIAN | SYS | SUF | TNEF | TAZ | TELEDISK | TEMP | TEXT | TIFF | UU | UNICODE | UNICODE4 | UNICODE4B | UNICODESB | UTF_8 | VBA | VHD | WASM | VMWR | WIN_64 | WIN_CE | WIN_NE | WIN_PE | WISE | WBT | WMF | WKS | WORD2 | WORD6 | WPD | XLSB | XX | XML | XOR | YNC | ZIP | ZOO