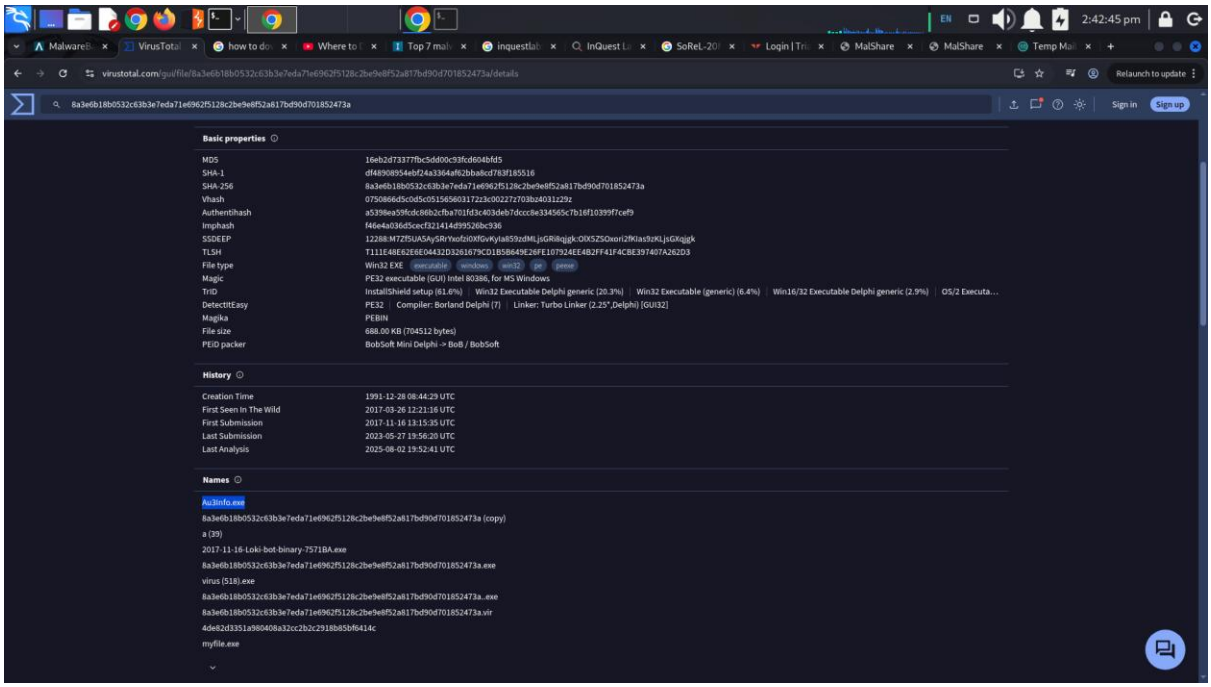
Malware Analysis POC

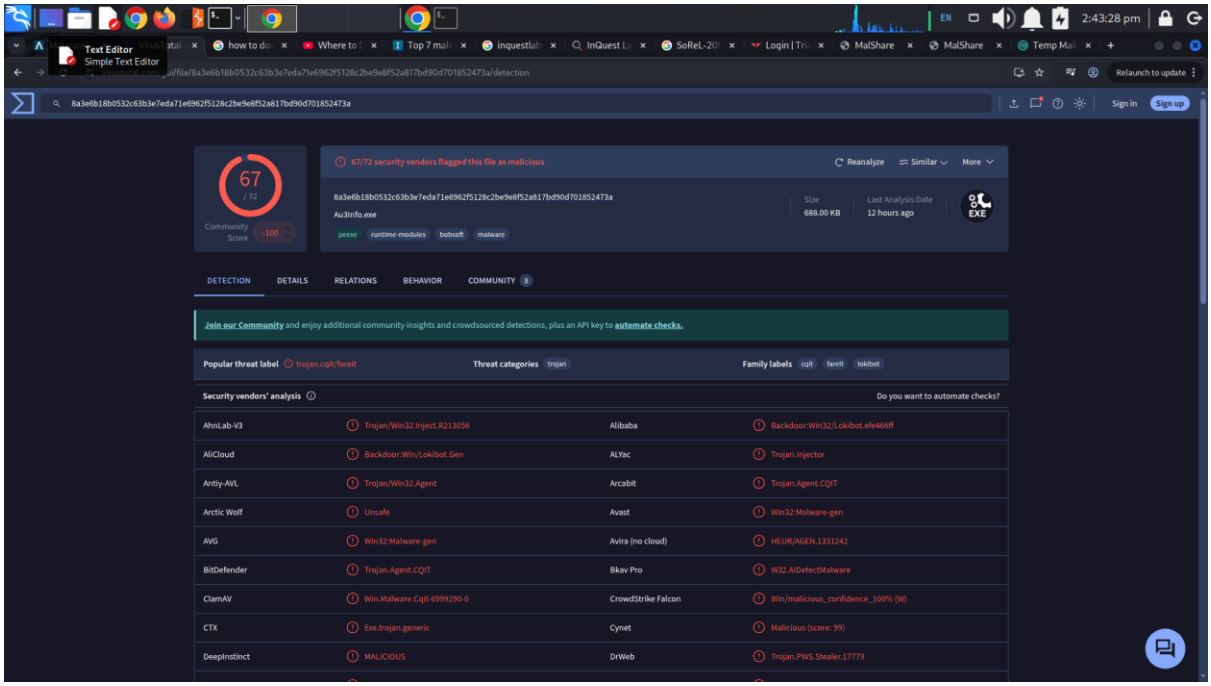
Name: Au3Info.exe

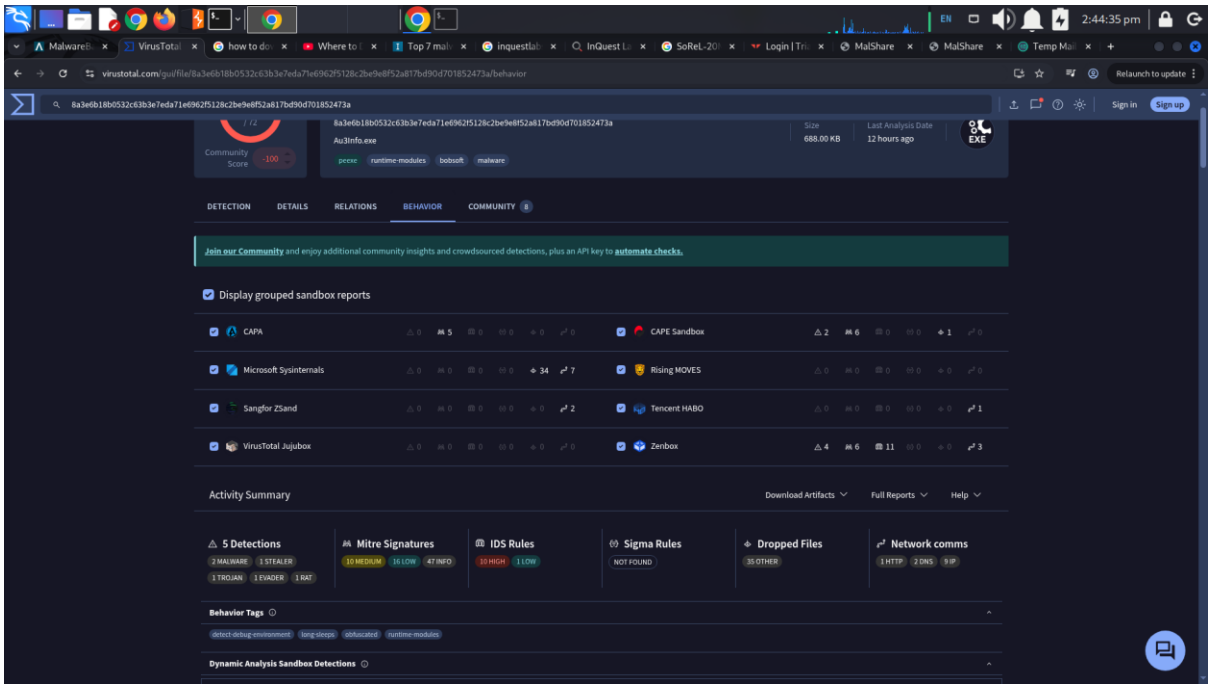
Hashes

1. MD5: 16eb2d73377fbc5dd00c93fcd604bfd5
2. SHA1: df48908954ebf24a3364af62bba8cd783f185516
3. SHA256: 8a3e6b18b0532c63b3e7eda71e6962f5128c2be9e8f52a817bd90d701852473a
4. SSDEEP: 12288:M7Zf5UA5AySRrYxofzi0XfGvKyIa859zdMLjsGRi8qjgk:OlX5ZSOxori2fKIas9zKLjsGXqjgk

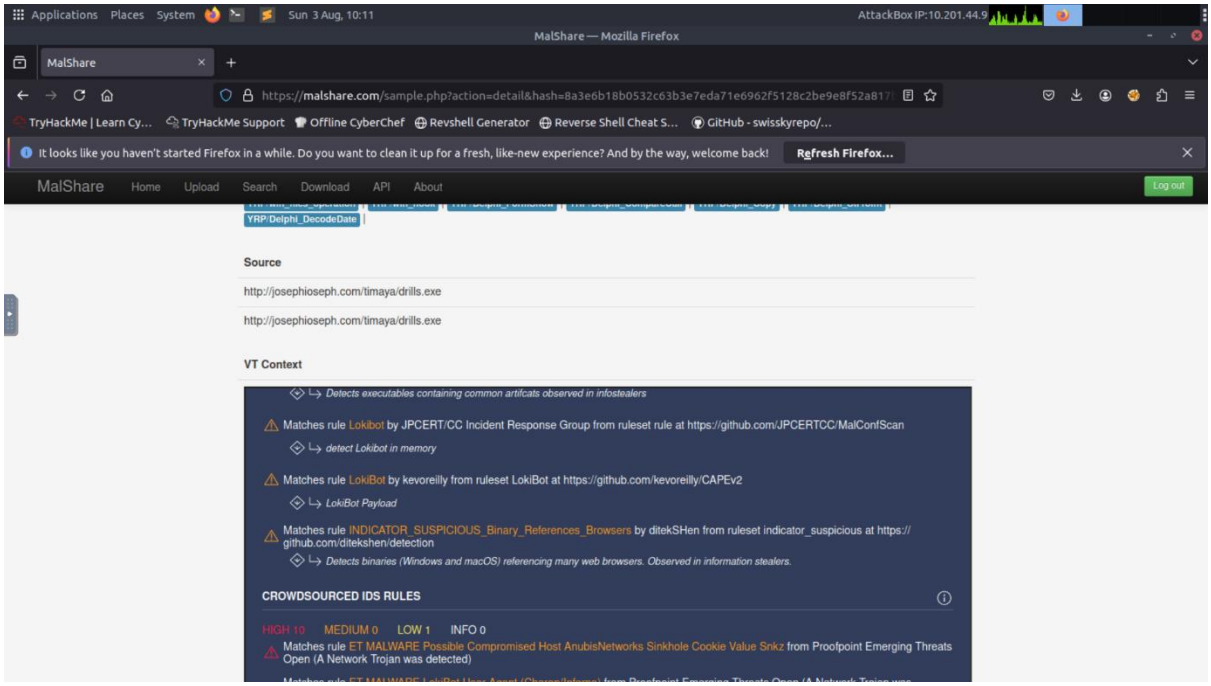
VirusTotal source



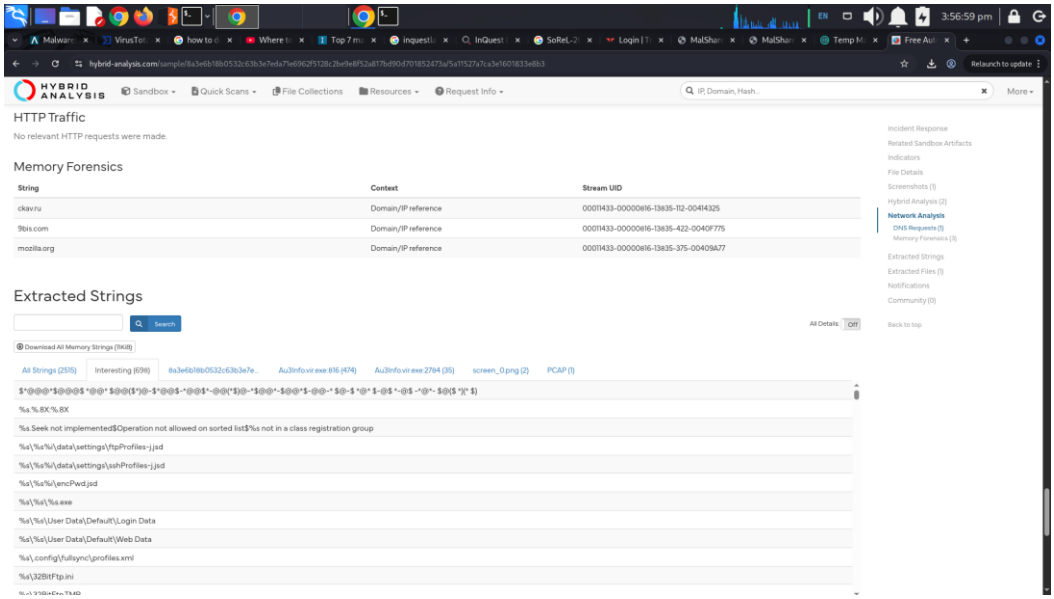

Text Editor
Simple Text Editor
8a3e6b18b0532c63b3e7eda71e6962f5128c2be9e8f52a817bd90d701852473a
67
/ 72
Community Score
-100
67/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
8a3e6b18b0532c63b3e7eda71e6962f5128c2be9e8f52a817bd90d701852473a
Au3Info.exe
peexe
runtime-modules
bobsoft
malware
Size
688.00 KB
Last Analysis Date
12 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 8
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.cqit/fareit
Threat categories trojan
Family labels cqit fareit lokibot
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Trojan/Win32.Inject.R213056
Alibaba Backdoor:Win32/Lokibot.efe466ff
AliCloud Backdoor:Win/Lokibot.Gen
ALYac Trojan.Injector
Antiy-AVL Trojan/Win32.Agent
Arcabit Trojan.Agent.CQIT
Arctic Wolf Unsafe
Avast Win32:Malware-gen
AVG Win32:Malware-gen
Avira (no cloud) HEUR/AGEN.1331242
BitDefender Trojan.Agent.CQIT
Bkav Pro W32.AIDetectMalware
ClamAV Win.Malware.Cqit-6999290-0
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.generic
Cynet Malicious (score: 99)
DeepInstinct MALICIOUS
DrWeb Trojan.PWS.Stealer.17779

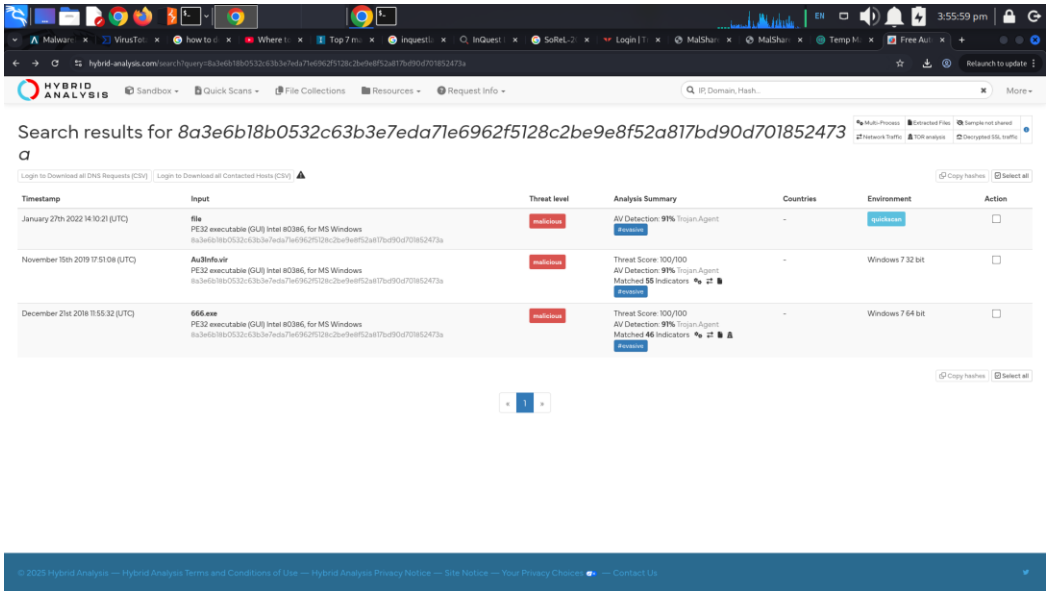

virustotal.com/gui/file/8a3e6b18b0532c63b3e7eda71e6962f5128c2be9e8f52a817bd90d701852473a/behavior
8a3e6b18b0532c63b3e7eda71e6962f5128c2be9e8f52a817bd90d701852473a
Community Score
-100
8a3e6b18b0532c63b3e7eda71e6962f5128c2be9e8f52a817bd90d701852473a
Au3Info.exe
peexe
runtime-modules
bobsoft
malware
Size
688.00 KB
Last Analysis Date
12 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 8
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Display grouped sandbox reports
CAPA
CAPE Sandbox
Microsoft Sysinternals
Rising MOVES
Sangfor ZSand
Tencent HABO
VirusTotal Jujubox
Zenbox
Activity Summary
Download Artifacts
Full Reports
Help
5 Detections
2 MALWARE
1 STEALER
1 TROJAN
1 EVADER
1 RAT
Mitre Signatures
10 MEDIUM
16 LOW
47 INFO
IDS Rules
10 HIGH
1 LOW
Sigma Rules
NOT FOUND
Dropped Files
35 OTHER
Network comms
1 HTTP
2 DNS
9 IP
Behavior Tags
detect-debug-environment
long-sleeps
obfuscated
runtime-modules
Dynamic Analysis Sandbox Detections

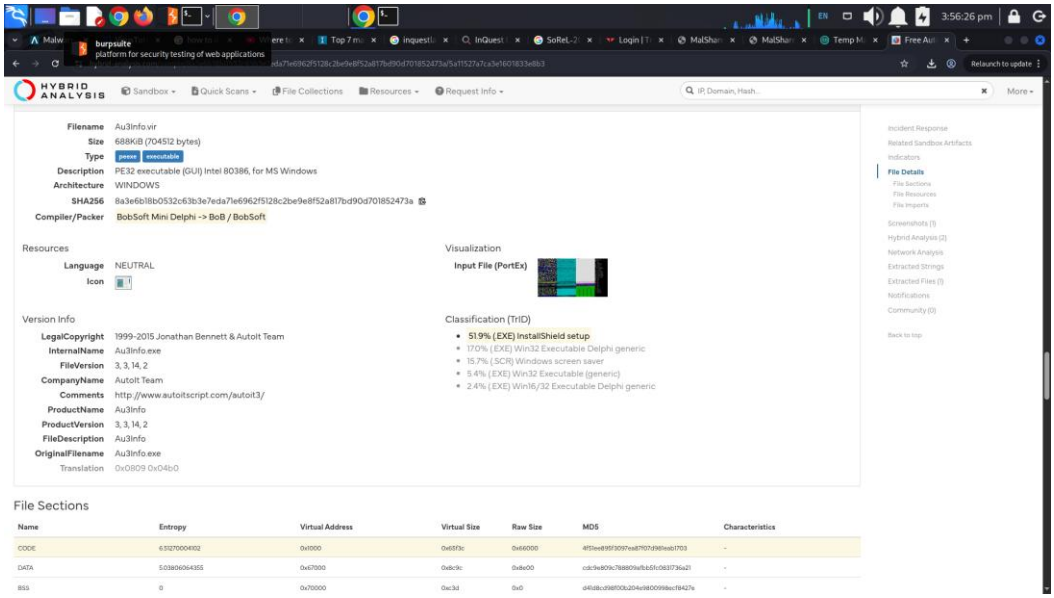
MalShare source



HybridAnalysis:




HYBRID ANALYSIS
Search results for 8a3e6b18b0532c63b3e7eda71e6962f5128c2be9e8f52a817bd90d701852473a
Timestamp
Input
Threat level
Analysis Summary
Countries
Environment
Action
January 27th 2022 14:10:21 (UTC)
file
PE32 executable (GUI) Intel 80386, for MS Windows
malicious
AV Detection: 91% Trojan.Agent
quickscan
November 15th 2019 17:51:08 (UTC)
Au3Info.vir
PE32 executable (GUI) Intel 80386, for MS Windows
malicious
Threat Score: 100/100
AV Detection: 91% Trojan.Agent
Matched 55 Indicators
Windows 7 32 bit
December 21st 2018 11:55:32 (UTC)
666.exe
PE32 executable (GUI) Intel 80386, for MS Windows
malicious
Threat Score: 100/100
AV Detection: 91% Trojan.Agent
Matched 46 Indicators
Windows 7 64 bit


HYBRID ANALYSIS
Filename Au3Info.vir
Size 688KiB (704512 bytes)
Type pexe executable
Description PE32 executable (GUI) Intel 80386, for MS Windows
Architecture WINDOWS
SHA256 8a3e6b18b0532c63b3e7eda71e6962f5128c2be9e8f52a817bd90d701852473a
Compiler/Packer BobSoft Mini Delphi -> BoB / BobSoft
Resources
Language NEUTRAL
Icon
Visualization
Input File (PortEx)
Version Info
LegalCopyright 1999-2015 Jonathan Bennett & AutoIt Team
InternalName Au3Info.exe
FileVersion 3, 3, 14, 2
CompanyName AutoIt Team
Comments http://www.autoitscript.com/autoit3/
ProductName Au3Info
ProductVersion 3, 3, 14, 2
FileDescription Au3Info
OriginalFilename Au3Info.exe
Translation 0x0809 0x04b0
Classification (TrID)
51.9% (.EXE) InstallShield setup
17.0% (.EXE) Win32 Executable Delphi generic
15.7% (.SCR) Windows screen saver
5.4% (.EXE) Win32 Executable (generic)
2.4% (.EXE) Win16/32 Executable Delphi generic
File Sections
Name
Entropy
Virtual Address
Virtual Size
Raw Size
MD5
Characteristics
CODE
DATA
BSS