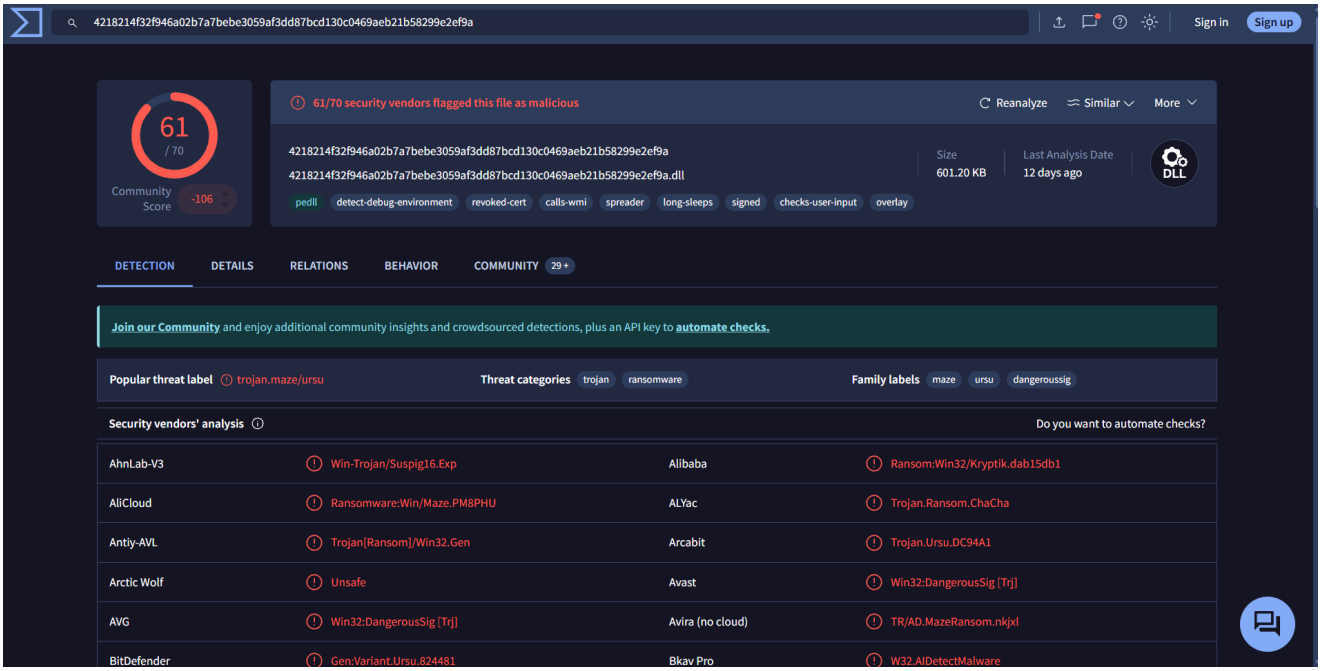
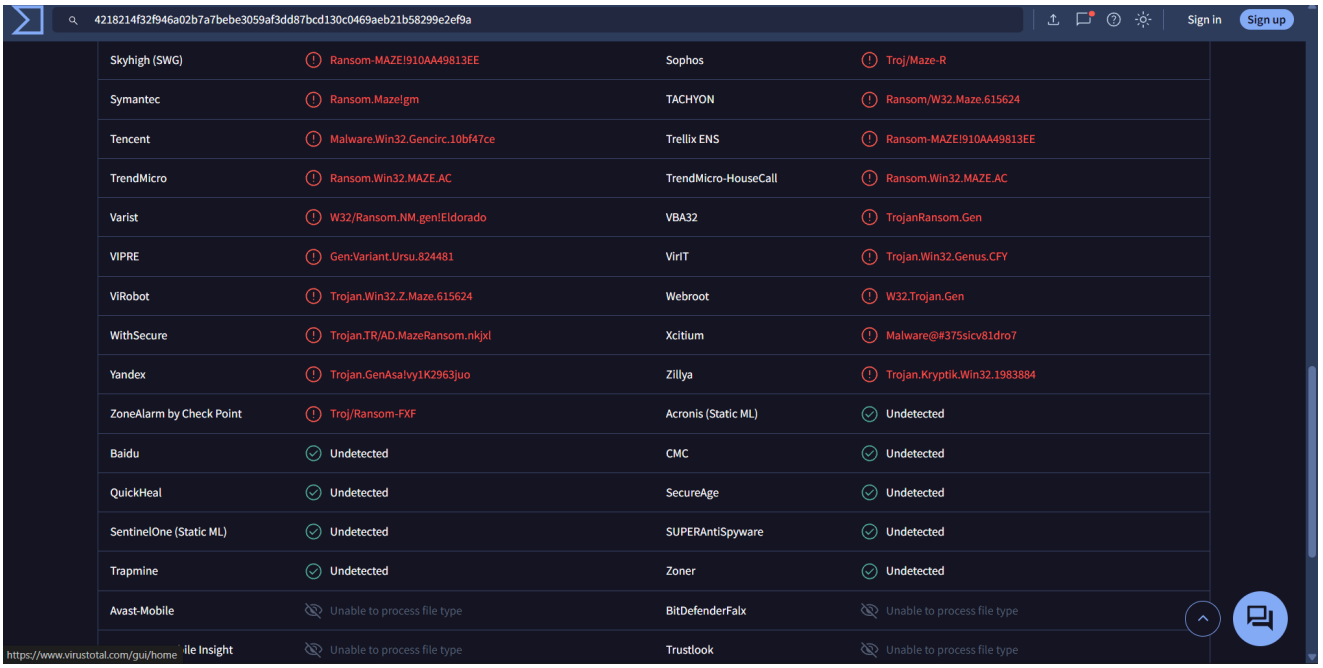
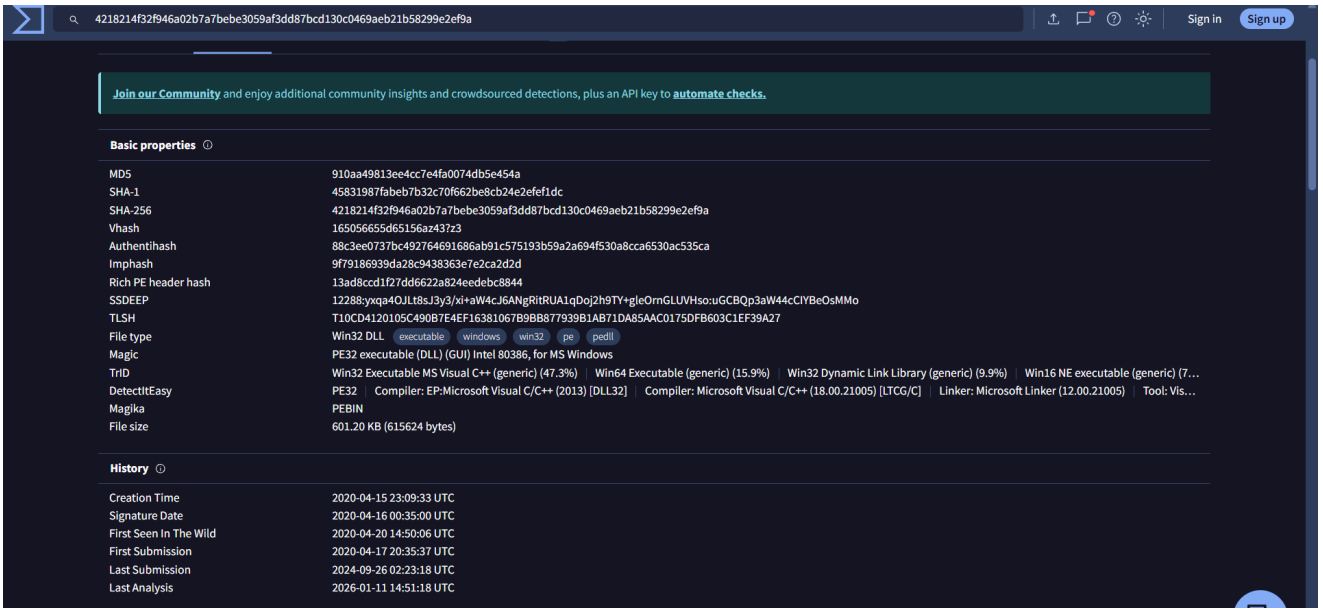
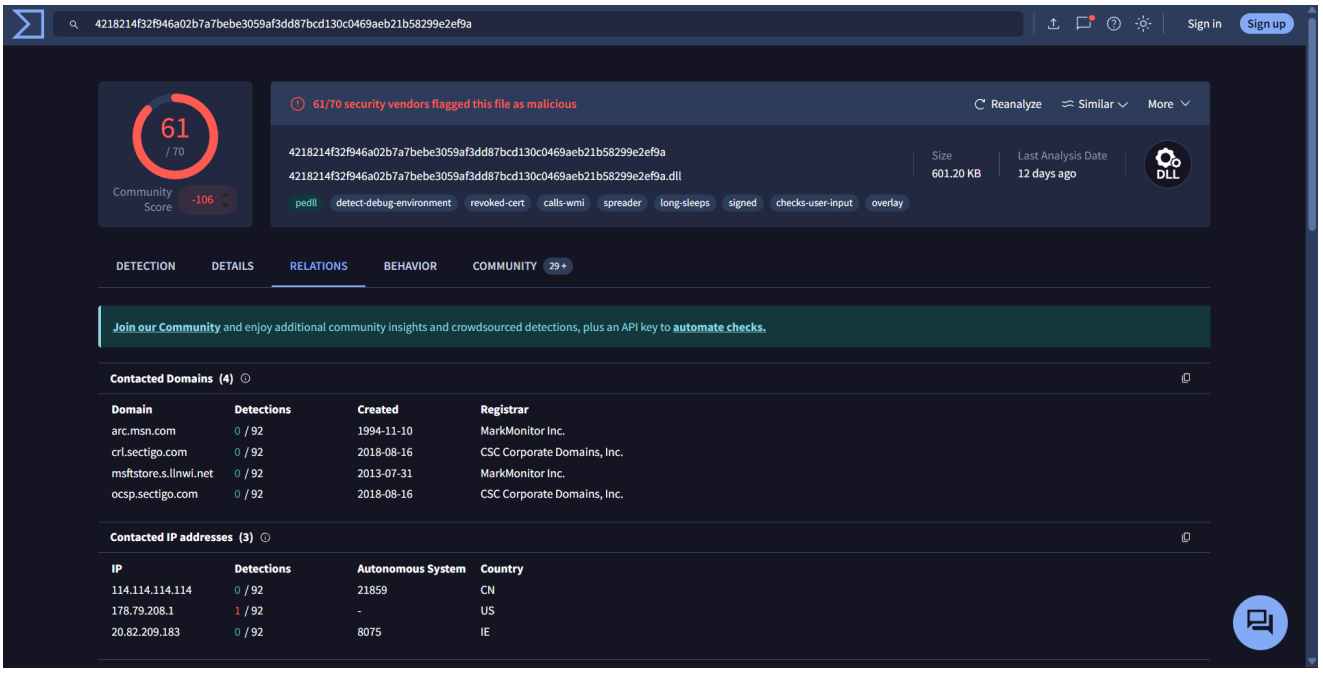
ALL screenshots from virus total

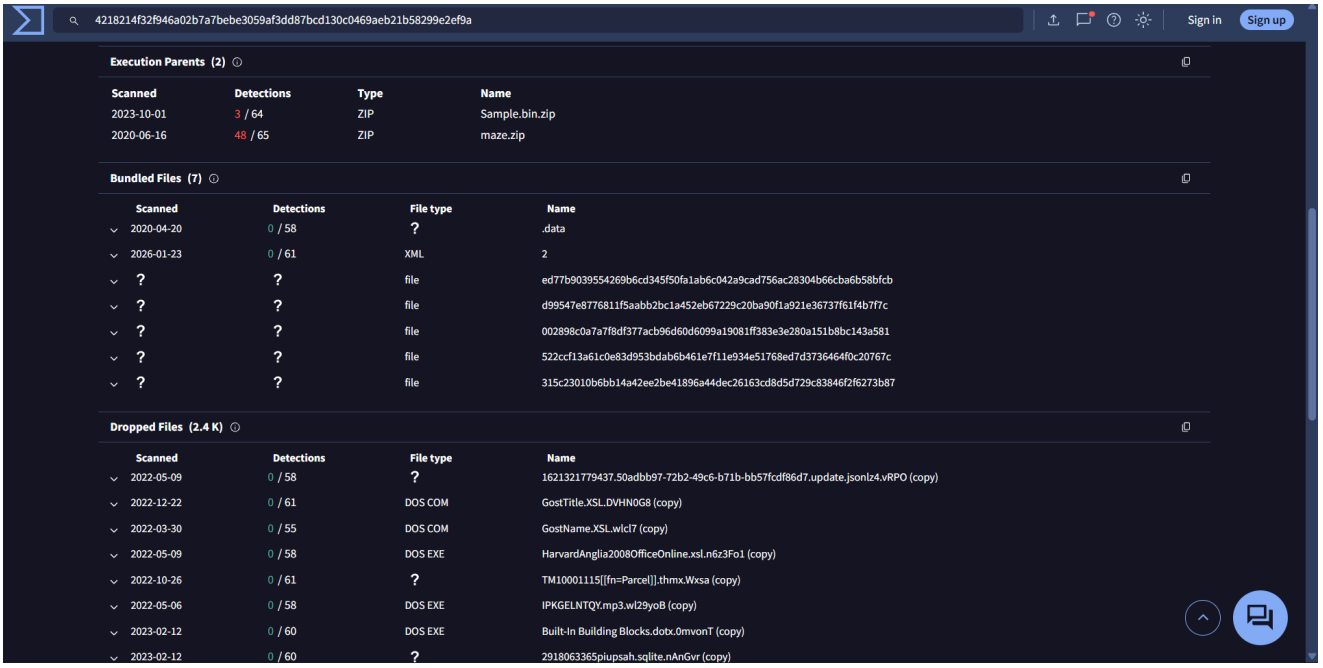


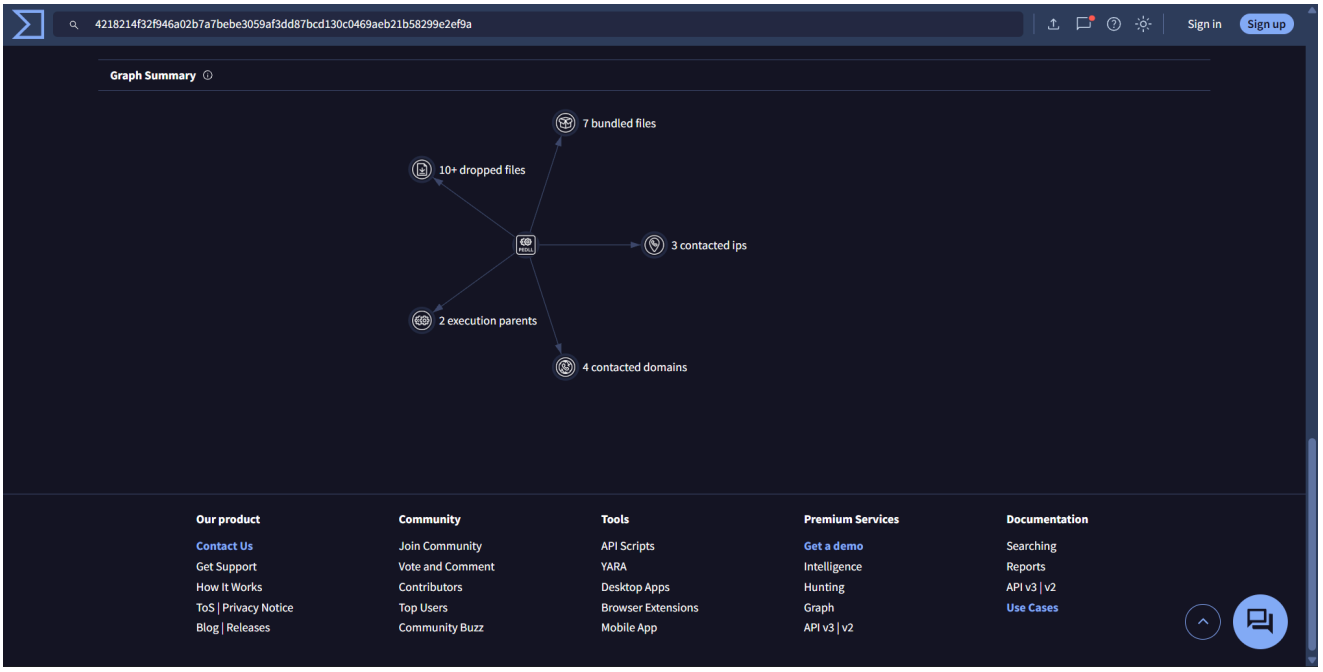

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
Sign in
Sign up
Skyhigh (SWG) Ransom-MAZE!910AA49813EE
Sophos Troj/Maze-R
Symantec Ransom.Maze!gm
TACHYON Ransom/W32.Maze.615624
Tencent Malware.Win32.Gencirc.10bf47ce
Trellix ENS Ransom-MAZE!910AA49813EE
TrendMicro Ransom.Win32.MAZE.AC
TrendMicro-HouseCall Ransom.Win32.MAZE.AC
Varist W32/Ransom.NM.gen!Eldorado
VBA32 TrojanRansom.Gen
VIPRE Gen:Variant.Ursu.824481
VirIT Trojan.Win32.Genus.CFY
ViRobot Trojan.Win32.Z.Maze.615624
Webroot W32.Trojan.Gen
WithSecure Trojan.TR/AD.MazeRansom.nkjxl
Xcitium Malware@#375sicv81dro7
Yandex Trojan.GenAsa!vy1K2963juo
Zillya Trojan.Kryptik.Win32.1983884
ZoneAlarm by Check Point Troj/Ransom-FXF
Acronis (Static ML) Undetected
Baidu Undetected
CMC Undetected
QuickHeal Undetected
SecureAge Undetected
SentinelOne (Static ML) Undetected
SUPERAntiSpyware Undetected
Trapmine Undetected
Zoner Undetected
Avast-Mobile Unable to process file type
BitDefenderFalx Unable to process file type
ile Insight Unable to process file type
Trustlook Unable to process file type
https://www.virustotal.com/gui/home

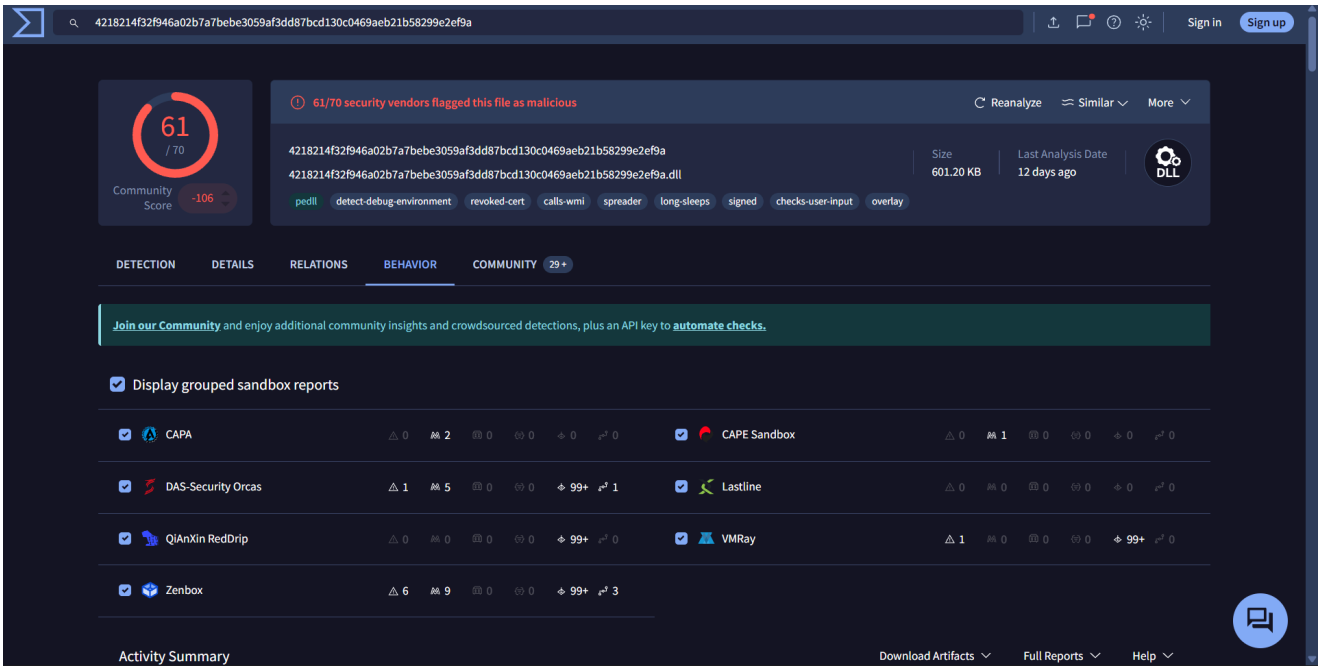

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
Sign in
Sign up
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Basic properties
MD5 910aa49813ee4cc7e4fa0074db5e454a
SHA-1 45831987fabeb7b32c70f662be8cb24e2efef1dc
SHA-256 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
Vhash 165056655d65156az43?z3
Authentihash 88c3ee0737bc492764691686ab91c575193b59a2a694f530a8cca6530ac535ca
Imphash 9f79186939da28c9438363e7e2ca2d2d
Rich PE header hash 13ad8ccd1f27dd6622a824eedebc8844
SSDEEP 12288:yxqa4OJLt8sJ3y3/xi+aW4cJ6ANgRitRUA1qDoj2h9TY+gleOrnGLUVHso:uGCBQp3aW44cCIYBeOsMMo
TLSH T10CD4120105C490B7E4EF16381067B9BB877939B1AB71DA85AAC0175DFB603C1EF39A27
File type Win32 DLL executable windows win32 pe pedll
Magic PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
TrID Win32 Executable MS Visual C++ (generic) (47.3%) | Win64 Executable (generic) (15.9%) | Win32 Dynamic Link Library (generic) (9.9%) | Win16 NE executable (generic) (7…
DetectItEasy PE32 | Compiler: EP:Microsoft Visual C/C++ (2013) [DLL32] | Compiler: Microsoft Visual C/C++ (18.00.21005) [LTCG/C] | Linker: Microsoft Linker (12.00.21005) | Tool: Vis…
Magika PEBIN
File size 601.20 KB (615624 bytes)
History
Creation Time 2020-04-15 23:09:33 UTC
Signature Date 2020-04-16 00:35:00 UTC
First Seen In The Wild 2020-04-20 14:50:06 UTC
First Submission 2020-04-17 20:35:37 UTC
Last Submission 2024-09-26 02:23:18 UTC
Last Analysis 2026-01-11 14:51:18 UTC

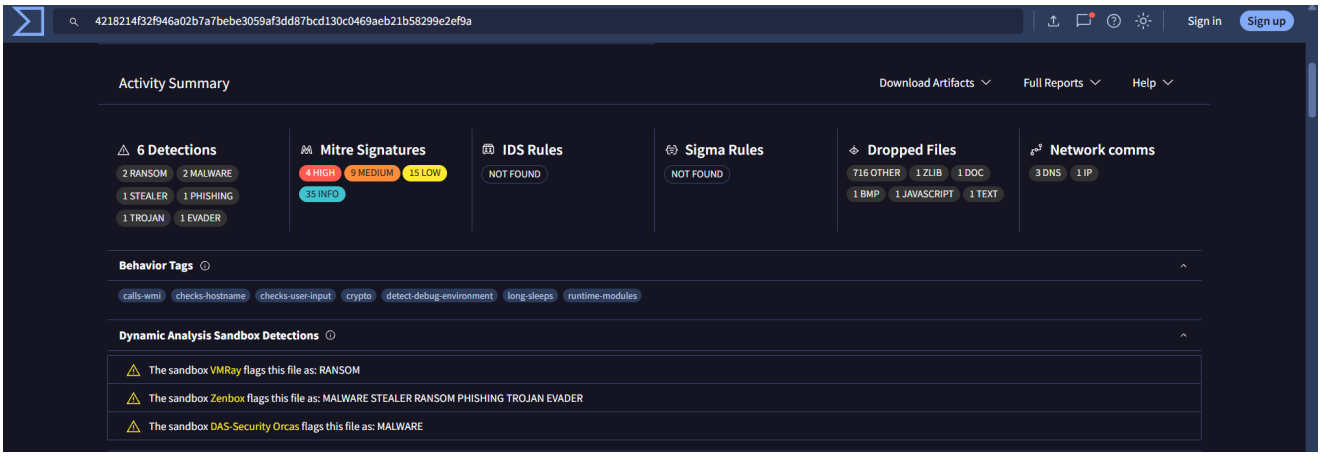

Names
910AA49813EE4CC7E4FA0074DB5E454A
45831987fabeb7b32c70f662be8cb24e2efef1dc
4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a.dll
Sample.bin
partmgr.sys
fHuFFchMCwJfBZjJT1M6XQMyTa.dll
FH0ZyYiNA0sRb17xiHvThS7a11PEjJE.dll
FBq7MScAMO5VUyfPD9SRXJ.dll
u6yZRhGlrHnkymOEDzlAyyAOQt.dll
Ba4NlVJAoEk5yvSdha.dll

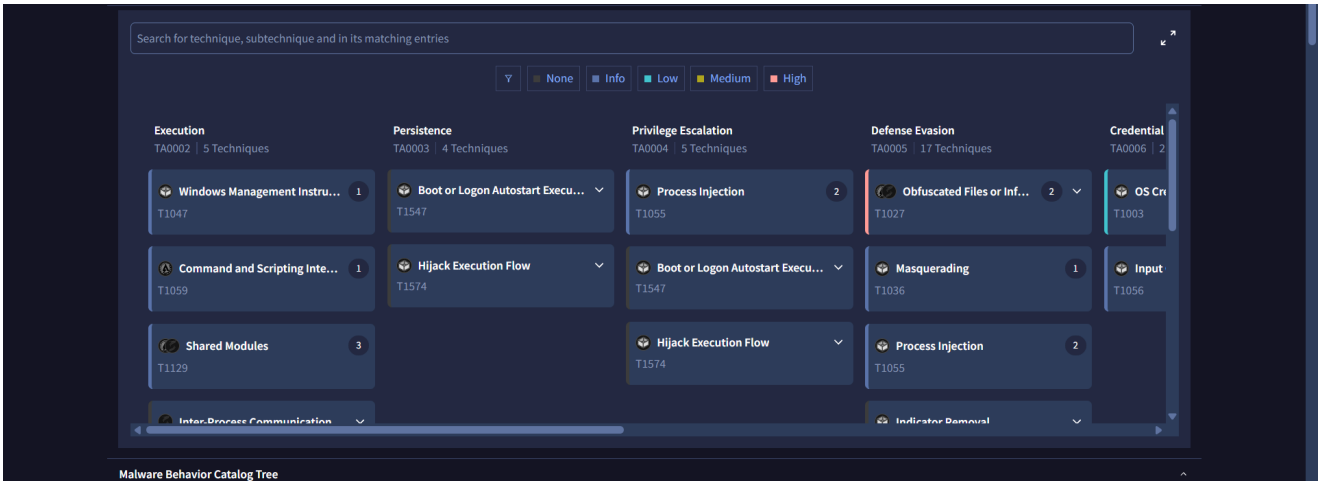


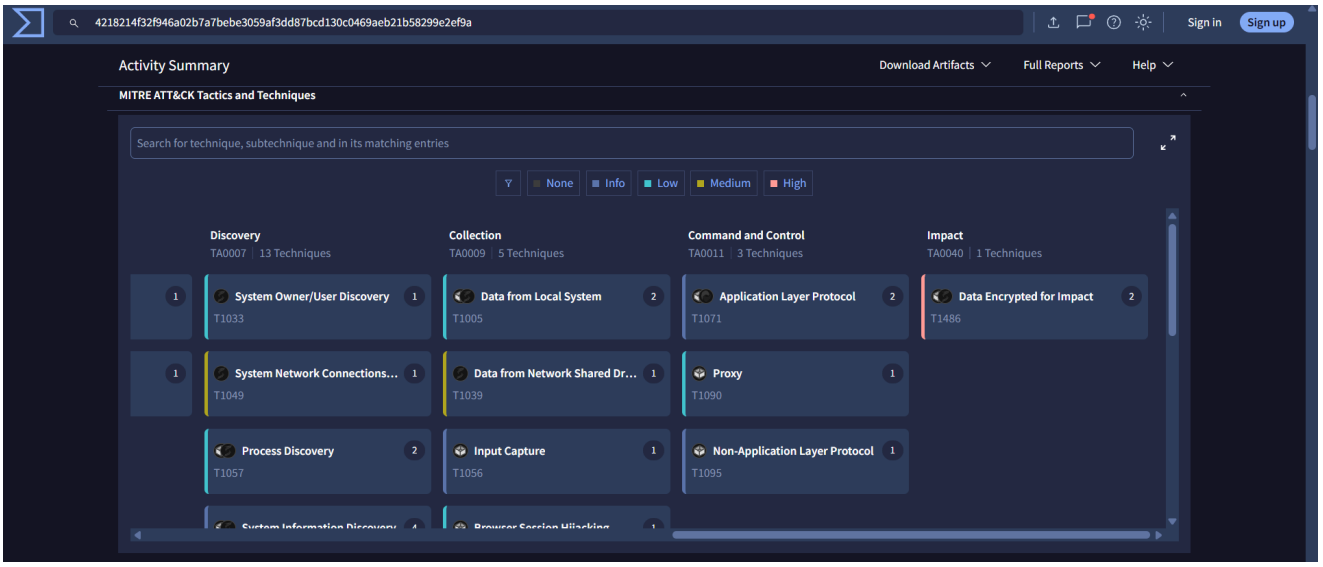


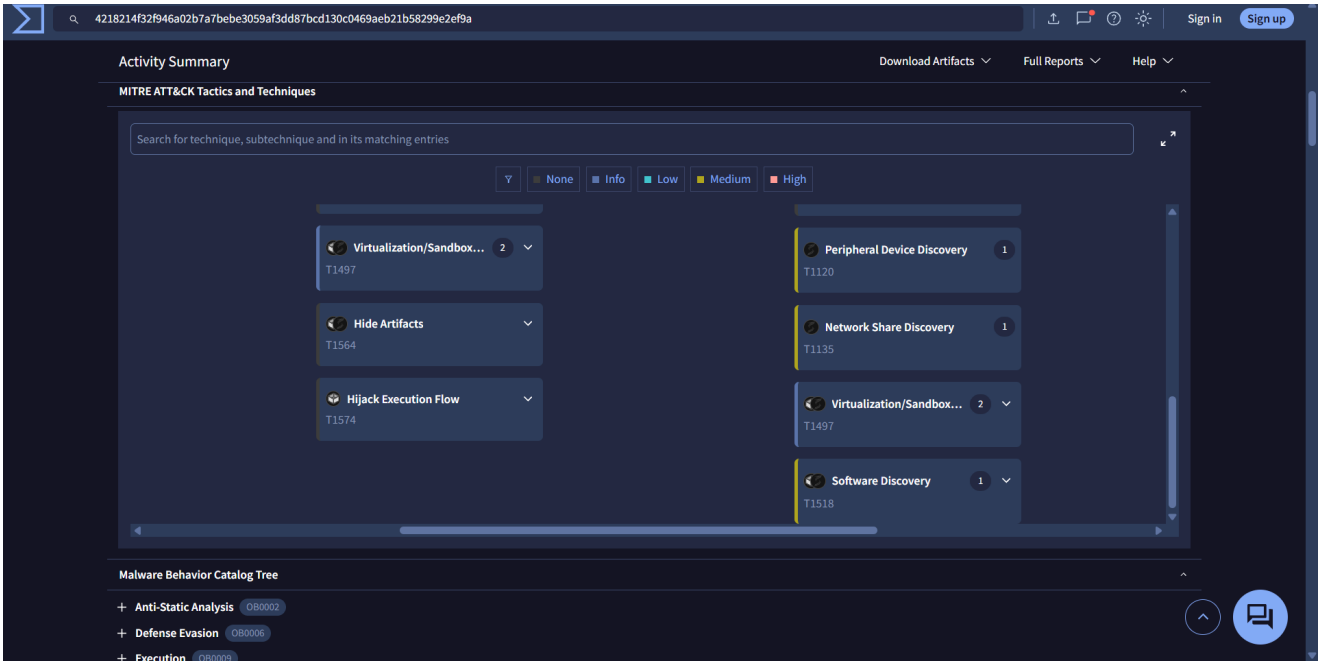



4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
Sign in
Sign up
61
/ 70
Community Score
-106
61/70 security vendors flagged this file as malicious
Reanalyze
Similar
More
4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a.dll
Size
601.20 KB
Last Analysis Date
12 days ago
DLL
pedll
detect-debug-environment
revoked-cert
calls-wmi
spreader
long-sleeps
signed
checks-user-input
overlay
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 29+
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
DAS-Security Orcas
Lastline
QiAnXin RedDrip
VMRay
Zenbox
Activity Summary
Download Artifacts
Full Reports
Help


4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
Sign in
Sign up
Activity Summary
Download Artifacts
Full Reports
Help
6 Detections
2 RANSOM
2 MALWARE
1 STEALER
1 PHISHING
1 TROJAN
1 EVADER
Mitre Signatures
4 HIGH
9 MEDIUM
15 LOW
35 INFO
IDS Rules
NOT FOUND
Sigma Rules
NOT FOUND
Dropped Files
716 OTHER
1 ZLIB
1 DOC
1 BMP
1 JAVASCRIPT
1 TEXT
Network comms
3 DNS
1 IP
Behavior Tags
calls-wmi
checks-hostname
checks-user-input
crypto
detect-debug-environment
long-sleeps
runtime-modules
Dynamic Analysis Sandbox Detections
The sandbox VMRay flags this file as: RANSOM
The sandbox Zenbox flags this file as: MALWARE STEALER RANSOM PHISHING TROJAN EVADER
The sandbox DAS-Security Orcas flags this file as: MALWARE


Search for technique, subtechnique and in its matching entries
None
Info
Low
Medium
High
Execution
TA0002 | 5 Techniques
Persistence
TA0003 | 4 Techniques
Privilege Escalation
TA0004 | 5 Techniques
Defense Evasion
TA0005 | 17 Techniques
Credential
Windows Management Instru...
T1047
Boot or Logon Autostart Execu...
T1547
Process Injection
T1055
Obfuscated Files or Inf...
T1027
OS Cr
T1003
Command and Scripting Inte...
T1059
Hijack Execution Flow
T1574
Boot or Logon Autostart Execu...
T1547
Masquerading
T1036
Input
T1056
Shared Modules
T1129
Hijack Execution Flow
T1574
Process Injection
T1055
Malware Behavior Catalog Tree


4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
Sign in
Sign up
Activity Summary
Download Artifacts
Full Reports
Help
MITRE ATT&CK Tactics and Techniques
Search for technique, subtechnique and in its matching entries
None
Info
Low
Medium
High
Discovery
TA0007 | 13 Techniques
Collection
TA0009 | 5 Techniques
Command and Control
TA0011 | 3 Techniques
Impact
TA0040 | 1 Techniques
System Owner/User Discovery
T1033
Data from Local System
T1005
Application Layer Protocol
T1071
Data Encrypted for Impact
T1486
System Network Connections...
T1049
Data from Network Shared Dr...
T1039
Proxy
T1090
Process Discovery
T1057
Input Capture
T1056
Non-Application Layer Protocol
T1095


4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
Sign in
Sign up
Activity Summary
Download Artifacts
Full Reports
Help
MITRE ATT&CK Tactics and Techniques
Search for technique, subtechnique and in its matching entries
None
Info
Low
Medium
High
Virtualization/Sandbox...
T1497
Hide Artifacts
T1564
Hijack Execution Flow
T1574
Peripheral Device Discovery
T1120
Network Share Discovery
T1135
Virtualization/Sandbox...
T1497
Software Discovery
T1518
Malware Behavior Catalog Tree
Anti-Static Analysis
OB0002
Defense Evasion
OB0006
Execution
OB0009