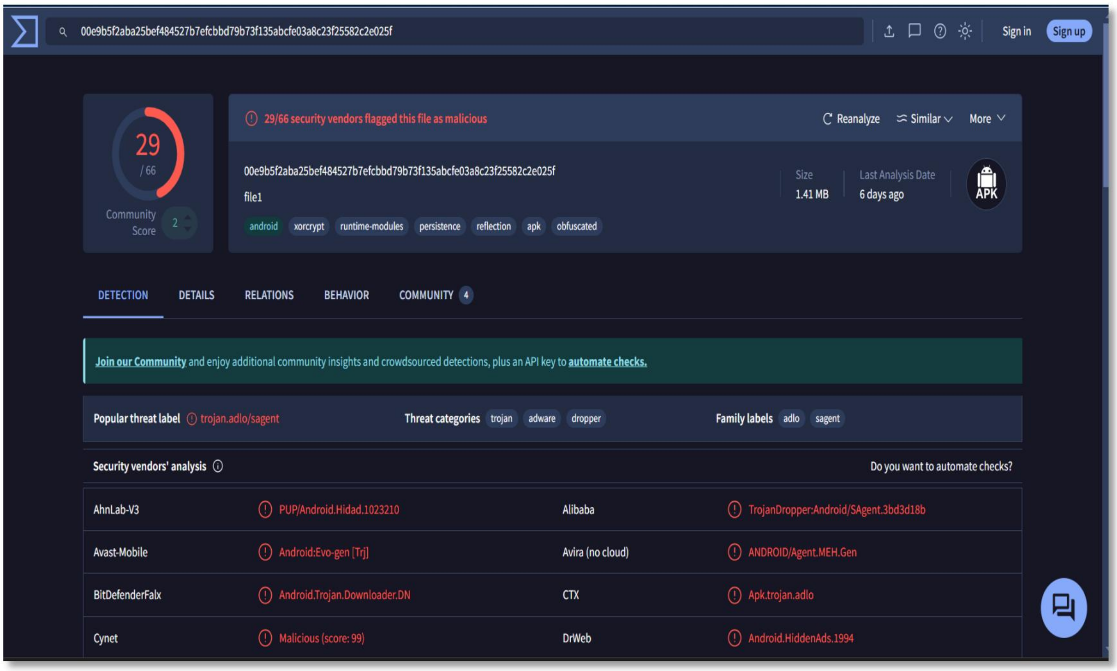
LAB 6

AIM: Analyzing mobile and IoT malware samples using tools like VirusTotal and Yara.

VirusTotal:

SHA-256 (file hash):
00e9b5f2aba25bef484527b7efcbbd79b73f135abcfe03a8c23f25582c2e025f



29/66 security vendors flagged this file as malicious

00e9b5f2aba25bef484527b7efcbbd79b73f135abcfe03a8c23f25582c2e025f

file1

android xorcrypt runtime-modules persistence reflection apk obfuscated

Size 1.41 MB

Last Analysis Date 6 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.adlo/sagent

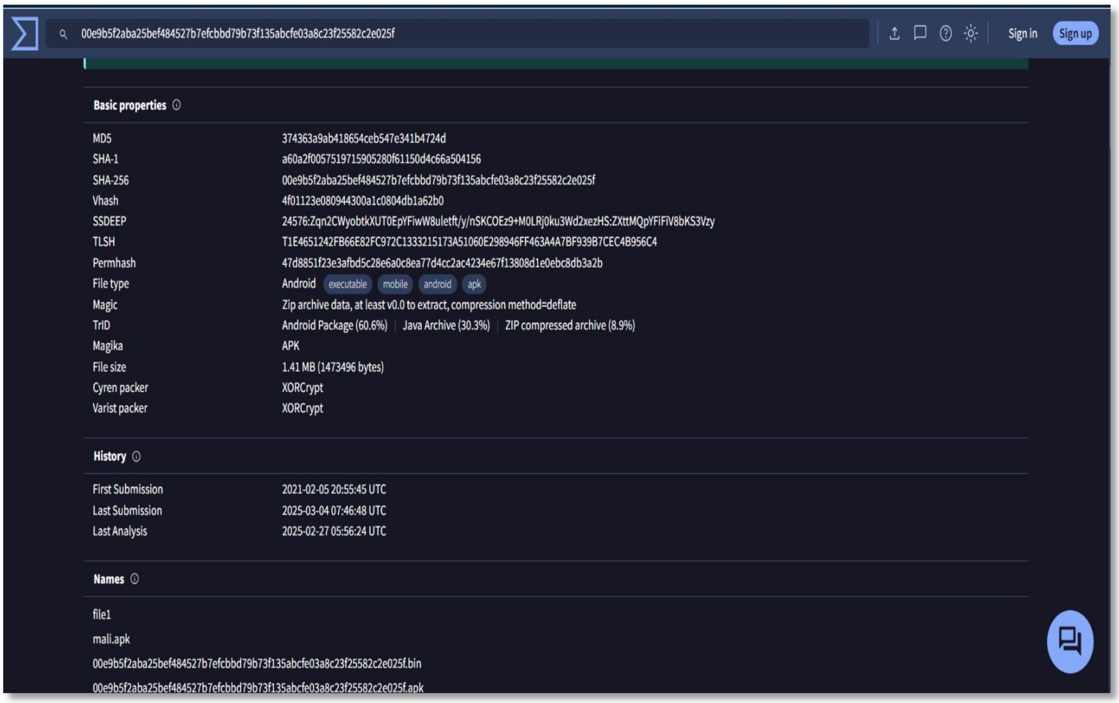
Threat categories trojan adware dropper

Family labels adlo sagent

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	PUP/Android.Hidad.1023210	Alibaba	TrojanDropper:Android/SAgent.3bd3d18b
Avast-Mobile	Android:Evo-gen [Trj]	Avira (no cloud)	ANDROID/Agent.MEH.Gen
BitDefenderFalx	Android.Trojan.Downloader.DN	CTX	Apk.trojan.adlo
Cynet	Malicious (score: 99)	DrWeb	Android.HiddenAds.1994



00e9b5f2aba25bef484527b7efcbbd79b73f135abcfe03a8c23f25582c2e025f
Sign in
Sign up

Basic properties

MD5	374363a9ab418654ceb547e341b4724d
SHA-1	a60a2f0057519715905280f61150d4c66a504156
SHA-256	00e9b5f2aba25bef484527b7efcbbd79b73f135abcfe03a8c23f25582c2e025f
Vhash	4f01123e080944300a1c0804db1a62b0
SSDEEP	24576:Zqn2CWyobtkXUT0EpYFiwW8uletft/y/nSKCOEz9+M0LRj0ku3Wd2xezHS:ZXttMQpYFiFiV8bKS3Vzy
TLSH	T1E4651242FB66E82FC972C1333215173A51060E298946FF463A4A7BF939B7CEC4B956C4
Permhash	47d8851f23e3afbd5c28e6a0c8ea77d4cc2ac4234e67f13808d1e0ebc8db3a2b
File type	Android executable mobile android apk
Magic	Zip archive data, at least v0.0 to extract, compression method=deflate
TrID	Android Package (60.6%) | Java Archive (30.3%) | ZIP compressed archive (8.9%)
Magika	APK
File size	1.41 MB (1473496 bytes)
Cyren packer	XORCrypt
Varist packer	XORCrypt

History

First Submission	2021-02-05 20:55:45 UTC
Last Submission	2025-03-04 07:46:48 UTC
Last Analysis	2025-02-27 05:56:24 UTC

Names

file1

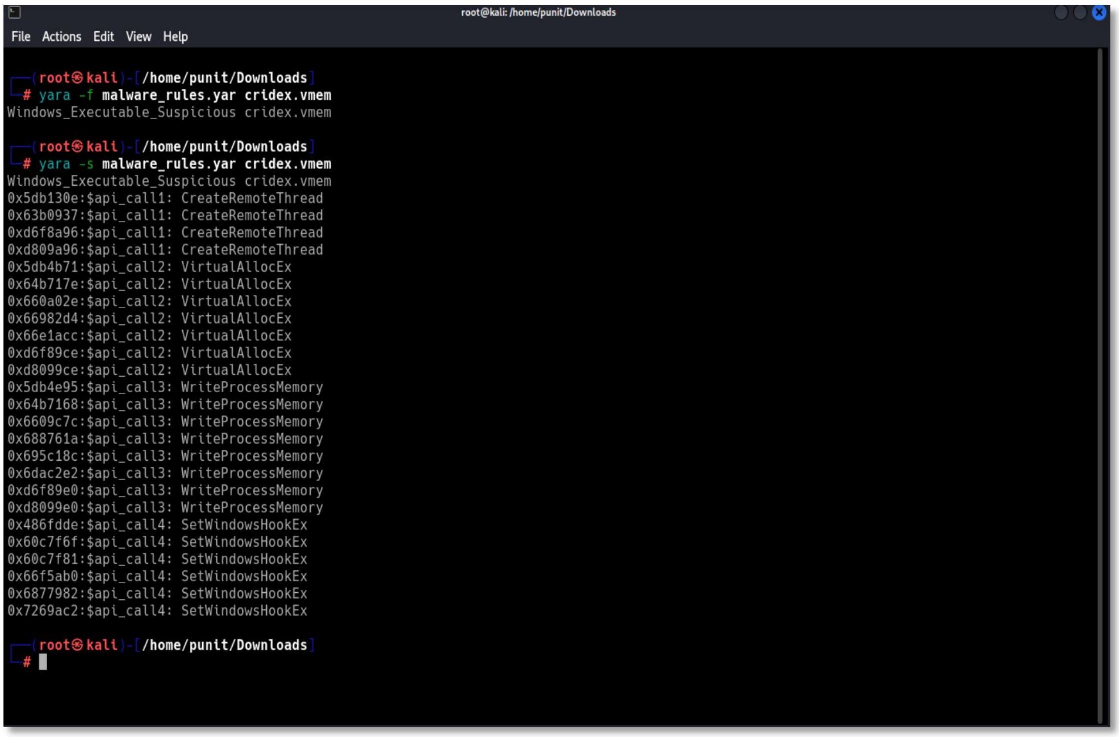
mali.apk

00e9b5f2aba25bef484527b7efcbbd79b73f135abcfe03a8c23f25582c2e025f.bin

00e9b5f2aba25bef484527b7efcbbd79b73f135abcfe03a8c23f25582c2e025f.apk

<u>Yara Tool:</u> Scan Using Custom Rules(malware_rules.yar)

cridex.vmem (Malware Sample):

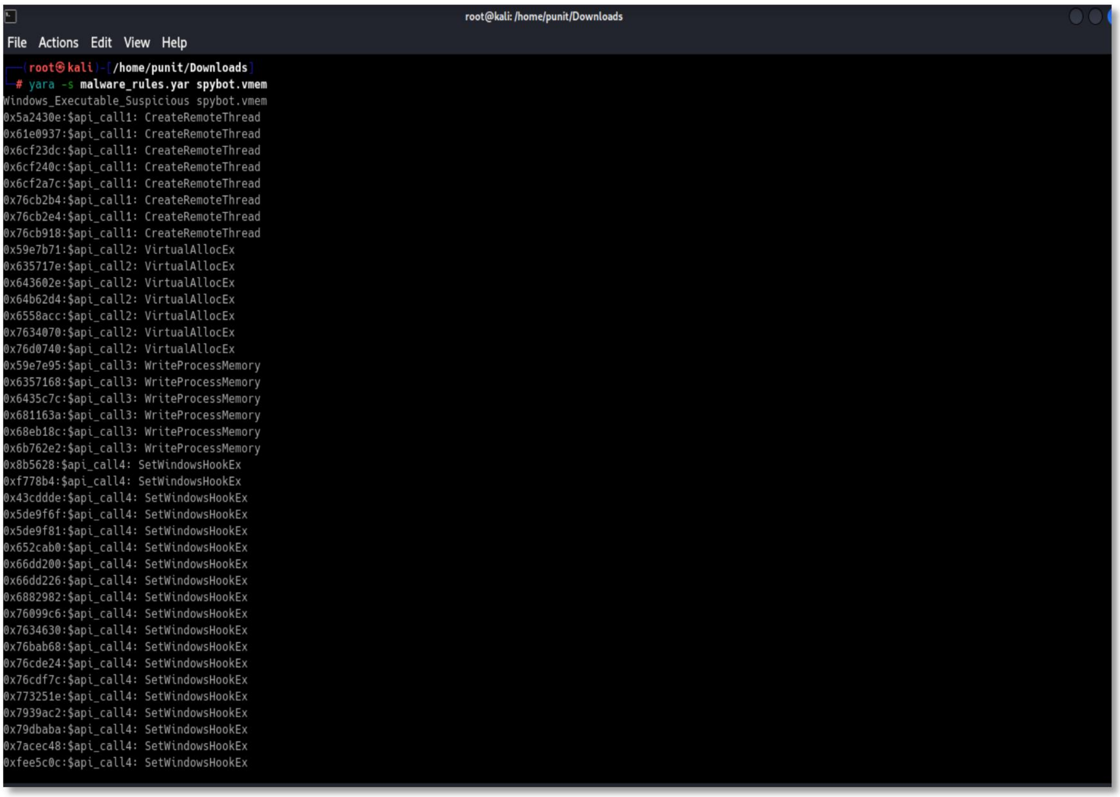


```
┌──(root㉿kali)-[/home/punit/Downloads]
└─# yara -f malware_rules.yar cridex.vmem
Windows_Executable_Suspicious cridex.vmem

┌──(root㉿kali)-[/home/punit/Downloads]
└─# yara -s malware_rules.yar cridex.vmem
Windows_Executable_Suspicious cridex.vmem
0x5db130e:$api_call1: CreateRemoteThread
0x63b0937:$api_call1: CreateRemoteThread
0xd6f8a96:$api_call1: CreateRemoteThread
0xd809a96:$api_call1: CreateRemoteThread
0x5db4b71:$api_call2: VirtualAllocEx
0x64b717e:$api_call2: VirtualAllocEx
0x660a02e:$api_call2: VirtualAllocEx
0x66982d4:$api_call2: VirtualAllocEx
0x66e1acc:$api_call2: VirtualAllocEx
0xd6f89ce:$api_call2: VirtualAllocEx
0xd8099ce:$api_call2: VirtualAllocEx
0x5db4e95:$api_call3: WriteProcessMemory
0x64b7168:$api_call3: WriteProcessMemory
0x6609c7c:$api_call3: WriteProcessMemory
0x688761a:$api_call3: WriteProcessMemory
0x695c18c:$api_call3: WriteProcessMemory
0x6dac2e2:$api_call3: WriteProcessMemory
0xd6f89e0:$api_call3: WriteProcessMemory
0xd8099e0:$api_call3: WriteProcessMemory
0x486fdde:$api_call4: SetWindowsHookEx
0x60c7f6f:$api_call4: SetWindowsHookEx
0x60c7f81:$api_call4: SetWindowsHookEx
0x66f5ab0:$api_call4: SetWindowsHookEx
0x6877982:$api_call4: SetWindowsHookEx
0x7269ac2:$api_call4: SetWindowsHookEx

┌──(root㉿kali)-[/home/punit/Downloads]
└─# 
```

Spybot.vmem (Malware Sample):



```
┌──(root㉿kali)-[/home/punit/Downloads]
└─# yara -s malware_rules.yar spybot.vmem
Windows_Executable_Suspicious spybot.vmem
0x5a2430e:$api_call1: CreateRemoteThread
0x61e0937:$api_call1: CreateRemoteThread
0x6cf23dc:$api_call1: CreateRemoteThread
0x6cf240c:$api_call1: CreateRemoteThread
0x6cf2a7c:$api_call1: CreateRemoteThread
0x76cb2b4:$api_call1: CreateRemoteThread
0x76cb2e4:$api_call1: CreateRemoteThread
0x76cb918:$api_call1: CreateRemoteThread
0x59e7b71:$api_call2: VirtualAllocEx
0x635717e:$api_call2: VirtualAllocEx
0x643602e:$api_call2: VirtualAllocEx
0x64b62d4:$api_call2: VirtualAllocEx
0x6558acc:$api_call2: VirtualAllocEx
0x7634070:$api_call2: VirtualAllocEx
0x76d0740:$api_call2: VirtualAllocEx
0x59e7e95:$api_call3: WriteProcessMemory
0x6357168:$api_call3: WriteProcessMemory
0x6435c7c:$api_call3: WriteProcessMemory
0x681163a:$api_call3: WriteProcessMemory
0x68eb18c:$api_call3: WriteProcessMemory
0x6b762e2:$api_call3: WriteProcessMemory
0x8b5628:$api_call4: SetWindowsHookEx
0xf778b4:$api_call4: SetWindowsHookEx
0x43cddde:$api_call4: SetWindowsHookEx
0x5de9f6f:$api_call4: SetWindowsHookEx
0x5de9f81:$api_call4: SetWindowsHookEx
0x652cab0:$api_call4: SetWindowsHookEx
0x66dd200:$api_call4: SetWindowsHookEx
0x66dd226:$api_call4: SetWindowsHookEx
0x6882982:$api_call4: SetWindowsHookEx
0x76099c6:$api_call4: SetWindowsHookEx
0x7634630:$api_call4: SetWindowsHookEx
0x76bab68:$api_call4: SetWindowsHookEx
0x76cde24:$api_call4: SetWindowsHookEx
0x76cdf7c:$api_call4: SetWindowsHookEx
0x773251e:$api_call4: SetWindowsHookEx
0x7939ac2:$api_call4: SetWindowsHookEx
0x79dbaba:$api_call4: SetWindowsHookEx
0x7acec48:$api_call4: SetWindowsHookEx
0xfee5c0c:$api_call4: SetWindowsHookEx
```