Recorded Future® Triage

# Memz Analysis	SOC
Security Classification Level: 0	SOC7

Overview Link: https://tria.ge/240525-trfyyaac4v

General

Target
memz.by.iTzDrK_.rar

Size
17KB

Sample
240525-trfyyaac4v

MD5
352c9d71fa5ab9e8771ce9e1937d88e9

SHA1
7ef6ee09896dd5867cff056c58b889bb33706913

SHA256
3d5d9bc94be3d1b7566a652155b0b37006583868311f20ef00283c30314b5c61

SHA512
6c133aa0c0834bf3dbb3a4fb7ff163e3b17ae2500782d6bba72812b4e703fb3a4f939a799eeb17436ea24f225386479d3aa3b81fdf35975c4f104914f895ff23

SSDEEP
384:7FbiYdriLCwBoe6POLT9bxaF851AfS9KL6bPsn/OMrZAGE:7FbldrliOSbxr1AfS9KM+/OMa1

7/10

Score

PERSISTENCE

BOOTKIT

EXECUTION

Targets

Target
Geometry dash auto speed hack.bat

Size
13KB

MD5
4e2a7f369378a76d1df4d8c448f712af

SHA1
1192b4d01254a8704e6d6ae17dc2ec28a7ad5a49

SHA256
5e2cd213ff47b7657abd9167c38ffd8b53c13261fe22adddea92b5a2d9e320ad

SHA512
90e6eedca424e2ee37c78e0c0380db490c049b0378541812734c134510c40c6e4c48c4e213f395339ed99ff337ef087b6056ac5aafb246c1789ca6082dcabd2e

SSDEEP
192:AOyUySI0UaDz2gWsIzImj+BxZ3yqueWQx0IZicyC8Sh31xcjBzyxwn7AVhIlz3:AVODaDSHMqI3yqlxy5L1xcjwrlz3

Score
7/10

BOOTKIT

EXECUTION

PERSISTENCE

Checks computer location settings
Looks up country code configured in the registry, likely geofence.

Executes dropped EXE

Loads dropped DLL

Writes to the Master Boot Record (MBR)
Bootkits write to the MBR to gain persistence at a level below the operating system.
BOOTKIT PERSISTENCE

Drops file in System32 directory

Target

Score

geometry dash auto speed hack.exe

Size
14KB

MD5
19dbec50735b5f2a72d4199c4e184960

SHA1
6fed7732f7cb6f59743795b2ab154a3676f4c822

SHA256
a3d5715a81f2fbeb5f76c88c9c21eeee87142909716472f911ff6950c790c24d

SHA512
aa8a6bbb1ec516d5d5acf8be6863a4c6c5d754cee12b3d374c3a6acb393376806edc422f0ffb661c210e5b9485da88521e4a0956a4b7b08a5467cfaacd90591d

SSDEEP
192:slvxdXSQeWSg9JJS/IcIEiwqZKBkDFR43xWTM3LHn8f26gyr6yfFCj3r:sMVSaSEgIcIqq3agmLc+6gyWqFCj

7/10

BOOTKIT

PERSISTENCE

Checks computer location settings
Looks up country code configured in the registry, likely geofence.

Writes to the Master Boot Record (MBR)
Bootkits write to the MBR to gain persistence at a level below the operating system.

BOOTKIT PERSISTENCE

MITRE ATT&CK Matrix

ATT&CK v13

Initial Access