Recorded Future®
Triage

General

Target
caido-desktop-windows-v0.28.0-e5d2bc6f.msi

Size
40MB

Sample
230918-bv2eyadg5z

MD5
925f2f0a015a0562284e9f69d9d095a5

SHA1
b61a4fd3dcd8ced6a916aa66b51e317415ac4fec

SHA256
e5d2bc6f5f16a752892525ee06bcac94720b8242f983d00cdf2c4872db18b6ed

SHA512
8dd946abe54bd12791e13de7f6a34f678a95497ac5b9905355eb641dbb4b1a6be76f62863ad80a32d71ae9d9a75987e048dec612b64c65fa303ba44a986e6e94

SSDEEP
786432:pAZp+XPtEH/afxtK0CW3asxZwWEJrRwroB7+C+gc11111t2LyW4LUkN6AAexVA2U:pATuEH/afx40CkdwWEVKroB7Ygc11118

Score

8/10

DISCOVERY

PERSISTENCE

Targets

Target
caido-desktop-windows-v0.28.0-e5d2bc6f.msi

Size
40MB

MD5
925f2f0a015a0562284e9f69d9d095a5

SHA1
b61a4fd3dcd8ced6a916aa66b51e317415ac4fec

SHA256
e5d2bc6f5f16a752892525ee06bcac94720b8242f983d00cdf2c4872db18b6ed

SHA512
8dd946abe54bd12791e13de7f6a34f678a95497ac5b9905355eb641dbb4b1a6be76f62863ad80a32d71ae9d9a75987e048dec612b64c65fa303ba44a986e6e94

SSDEEP
786432:pAZp+XPtEH/afxtK0CW3asxZwWEJrRwroB7+C+gc11111t2LyW4LUkN6AAexVA2U:pATuEH/afx40CkdwWEVKroB7Ygc11118

Score

8/10

DISCOVERY

PERSISTENCE

- **Blocklisted process makes network request**
- **Downloads MZ/PE file**
- **Sets file execution options in registry**

Sets file execution options in registry

PERSISTENCE

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

Executes dropped EXE

Loads dropped DLL

Registers COM server for autorun

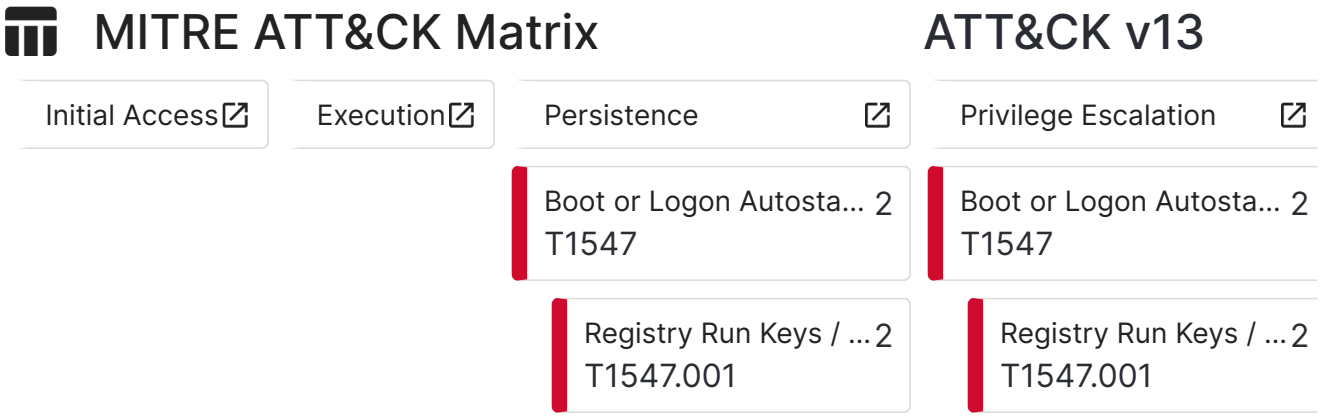
PERSISTENCE

Checks installed software on the system
Looks up Uninstall key entries in the registry to enumerate software on the system.

DISCOVERY

Enumerates connected drives
Attempts to read the root path of hard drives other than the default C: drive.

Checks system information in the registry
System information is often read in order to detect sandboxing environments.



Tasks

static1

Score
1/10

behavioral1

Score
8/10

behavioral2 DISCOVERY PERSISTENCE

Score
8/10