Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

redcanaryco / atomic-red-team Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 5 Actions Wiki Security Insights

Files

f339e7d

Go to file

- .github
- atomic_red_team
- atomics
  - Indexes
  - T1003.001
  - T1003.002
  - T1003.003
  - T1003.004
  - T1003.005
  - T1003.006
  - T1003.007
  - T1003.008
  - T1003
  - T1006
  - T1007
  - T1010
  - T1012
  - T1014
  - T1016
  - T1018
  - T1020
  - T1021.001
  - T1021.002
  - T1021.003
  - T1021.006
  - T1027.001
    - T1027.001.md
    - T1027.001.yaml
  - T1027.002
  - T1027.004
  - T1027
  - T1030
  - T1033
  - T1036.003
  - T1036.004
  - T1036.005

atomic-red-team / atomics / T1027.001 / T1027.001.md

CircleCI Atomic Red Team doc... Generate docs from job=gener... 36d49de · 3 years ago History

Preview Code Blame 62 lines (35 loc) · 2.22 KB Raw

T1027.001 - Binary Padding

Description from ATT&CK

> Adversaries may use binary padding to add junk data and change the on-disk representation of malware. This can be done without affecting the functionality or behavior of a binary, but can increase the size of the binary beyond what some security tools are capable of handling due to file size limitations.
> Binary padding effectively changes the checksum of the file and can also be used to avoid hash-based blocklists and static anti-virus signatures.(Citation: ESET OceanLotus) The padding used is commonly generated by a function to create junk data and then appended to the end or applied to sections of malware.(Citation: Securelist Malware Tricks April 2017) Increasing the file size may decrease the effectiveness of certain tools and detection capabilities that are not designed or configured to scan large files. This may also reduce the likelihood of being collected for analysis. Public file scanning services, such as VirusTotal, limits the maximum size of an uploaded file to be analyzed.(Citation: VirusTotal FAQ)

Atomic Tests

- Atomic Test #1 - Pad Binary to Change Hash - Linux/macOS dd

Atomic Test #1 - Pad Binary to Change Hash - Linux/macOS dd

Uses dd to add a zero to the binary to change the hash.

Upon successful execution, dd will modify `/tmp/evil-binary`, therefore the expected hash will change.

Supported Platforms: macOS, Linux

auto_generated_guid: ffe2346c-abd5-4b45-a713-bf5f1ebd573a

Inputs:

Name	Description	Type	Default Value
file_to_pad	Path of binary to be padded	Path	/tmp/evil-binary

Attack Commands: Run with `sh`!

```
dd if=/dev/zero bs=1 count=1 >> #{file_to_pad}
```

T1036.006
T1036
T1037.001
T1037.002
T1037.004
T1037.005

Cleanup Commands:

```
rm #{file_to_pad}
```

Dependencies: Run with `bash`!

Description: The binary must exist on disk at specified location (#{file_to_pad})

Check Prereq Commands:

```
if [ -f #{file_to_pad} ]; then exit 0; else exit 1; fi;
```

Get Prereq Commands:

```
cp /bin/ls #{file_to_pad}
```