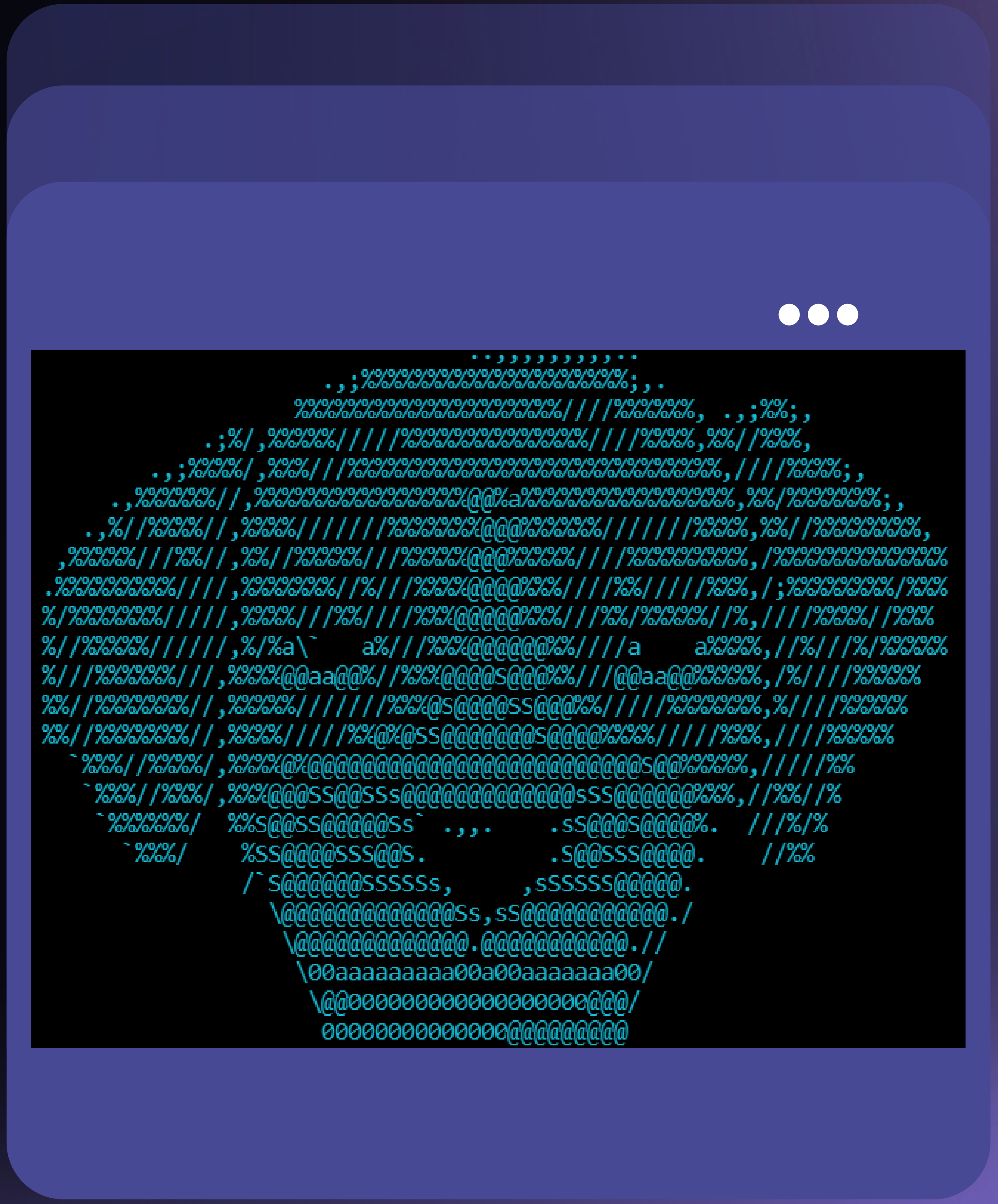
karma v2

Shodan Passive Open Source Intelligence (OSINT) Automated Reconnaissance (framework)

https://github.com/Dheerajmadhukar/karma_v2



Dheeraj Madhukar

>_ Security Researcher [+8 years]

>_ Trainer at CDAC Under The Ministry of Electronics (ACTs & Applied AI Department)

>_ Corporate Trainer at Indian Air Force Under the Ministry of Defense

in /dheerajtechnolegends

/Dheerajmadhukar

TOOL

KARMA_V2

Shodan Open Source Intelligence (OSINT) Automated Reconnaissance (framework)

01
Deep Assets OSINT

02
WAF/CDN bypassed IPs

03
Internal/External Infrastructure

04
Publicly exposed leaks

05
Bug Bounty Recon

KARMA_V2

Features

https://github.com/Dheerajmadhukar/karma_v2/blob/main/README.md

01 Powerful and flexible results via Shodan Dorks

02 SSL SHA1 checksum/fingerprint Search

03 Verify each IP with SSL/TLS certificate issuer match RegEx

04 Provide Out-Of-Scope IPs

05 Find out all ports including well known/uncommon/dynamic

KARMA_V2

Features

https://github.com/Dheerajmadhukar/karma_v2/blob/main/README.md

06 Grab all targets vulnerabilities related to CVEs

07 DevOps/SIEM/DevSecOps Assets Discovery

08 Banner grab for each IP, Product, OS, Services & Org etc.

09 Generate Favicon Hash using python3 mmh3 Module

10 Favicon Technology Detection using nuclei custom template

KARMA_V2

Features

https://github.com/Dheerajmadhukar/karma_v2/blob/main/README.md

11 ASN Scan

12 BGP Neighbour

13 IPv4 & IPv6 Profixes for ASN

14 Sensitive Data/Assets Exposer

Installation

Step 1

```
$ python3 -m pip install shodan mmh3
$ apt install jq lolcat -y
```

Step 2

```
$ go install github.com/tomnomnom/httprobe@master

$ go install github.com/tomnomnom/anew@master

$ GO111MODULE=on go get -v github.com/projectdiscovery/nuclei/v2/cmd/nuclei
```

Step 3

```
$ cat > .token
SHODAN_PREMIUM_API_HERE
```

MODEs

01

-ip

Scan for In-Scope-IPs Validated by CN=*.{target} and Out-Of-Scope-IPs

02

-asn

Detailed Autonomous system number lookup with BGP stats, neighbours, IPv4 & IPv6 Prefixes

03

-cve

Scan hosts for such as OS, Host, Servers, Products, CVEs, Ports are open and which organization owns the IP

MODEs

04

-cveid

Scan a host/domain for specific CVE ID for vulnerabilities & exploits

05

-favicon

Search for Favicon Icons, Calculate Favicon Hashes and Technology Detection with nuclei custom template

06

-cdn

SSL/TLS, Hostnames, IPs Ignored any CDN Nodes [Supported: Akamighost, Cloud(flare||front)]

MODEs

07

-leaks

Look for interesting findings, like leaks, DevOps Assets, SIEM, Open Dashboards etc....

08

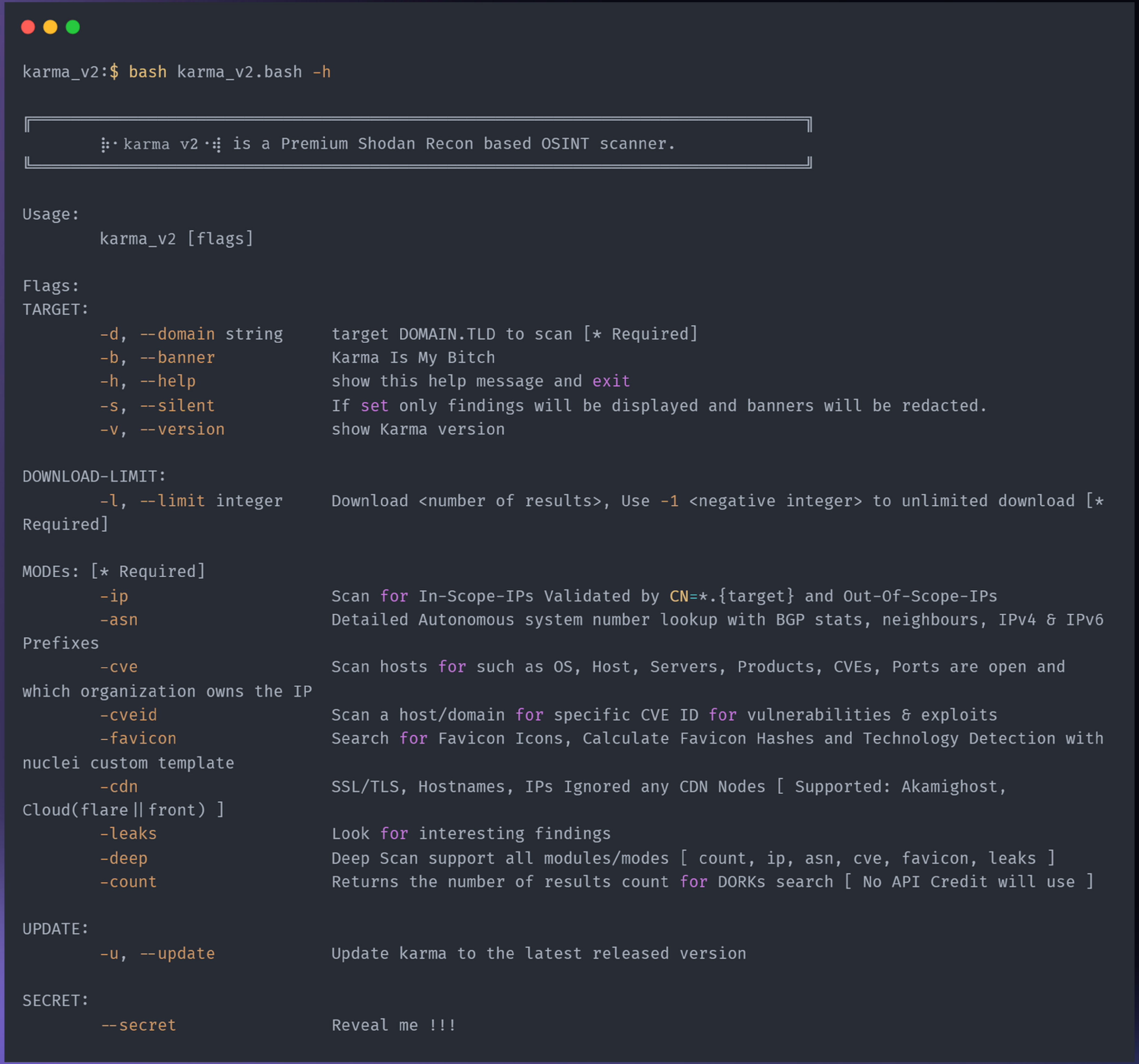
-count

Returns the number of results count for DORKs search [No API Credit will use]

09

-deep

Deep Scan support all modules/modes [count, ip, asn, cve, favicon, leaks]



```
karma_v2:$ bash karma_v2.bash -h

╔══════════════════════════════════════════════════════════════════════════════════╗
        ⣷·karma v2·⣾ is a Premium Shodan Recon based OSINT scanner.
╚══════════════════════════════════════════════════════════════════════════════════╝

Usage:
        karma_v2 [flags]

Flags:
TARGET:
        -d, --domain string     target DOMAIN.TLD to scan [* Required]
        -b, --banner            Karma Is My Bitch
        -h, --help              show this help message and exit
        -s, --silent            If set only findings will be displayed and banners will be redacted.
        -v, --version           show Karma version

DOWNLOAD-LIMIT:
        -l, --limit integer     Download <number of results>, Use -1 <negative integer> to unlimited download [*
Required]

MODEs: [* Required]
        -ip                     Scan for In-Scope-IPs Validated by CN=*.{target} and Out-Of-Scope-IPs
        -asn                    Detailed Autonomous system number lookup with BGP stats, neighbours, IPv4 & IPv6
Prefixes
        -cve                    Scan hosts for such as OS, Host, Servers, Products, CVEs, Ports are open and
which organization owns the IP
        -cveid                  Scan a host/domain for specific CVE ID for vulnerabilities & exploits
        -favicon                Search for Favicon Icons, Calculate Favicon Hashes and Technology Detection with
nuclei custom template
        -cdn                    SSL/TLS, Hostnames, IPs Ignored any CDN Nodes [ Supported: Akamighost,
Cloud(flare||front) ]
        -leaks                  Look for interesting findings
        -deep                   Deep Scan support all modules/modes [ count, ip, asn, cve, favicon, leaks ]
        -count                  Returns the number of results count for DORKs search [ No API Credit will use ]

UPDATE:
        -u, --update            Update karma to the latest released version

SECRET:
        --secret                Reveal me !!!
```

HELP

$ bash karma_v2 -h

THANK YOU :)(: