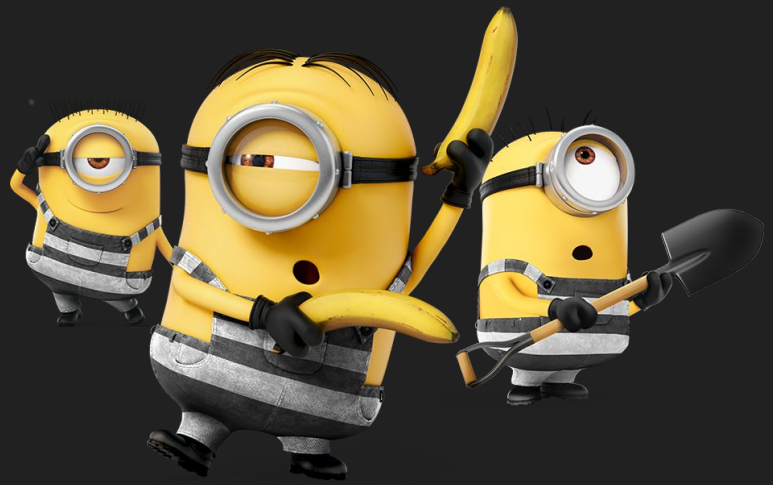


SUBDOMINIONS

Assets enumeration for fun

> WHOAMI

six2dez

> SCREENFETCH

Name Alexis Fernández

Location Madrid, España

Occupation Pentester & Bug Hunter

Website pentestbook.six2dez.com

Projects reconFTW & OneListForAll

GitHub/Twitter six2dez/@six2dez1

> STARTX

DISCLAIMER

This workshop is full of Minions for no apparent reason or relationship, why? Because yes, for the same reason we "drop" a single quote in each web form, for the laughs, what can we do, that's how we are.

And by the way, remember that attacking targets without permission is illegal ;)

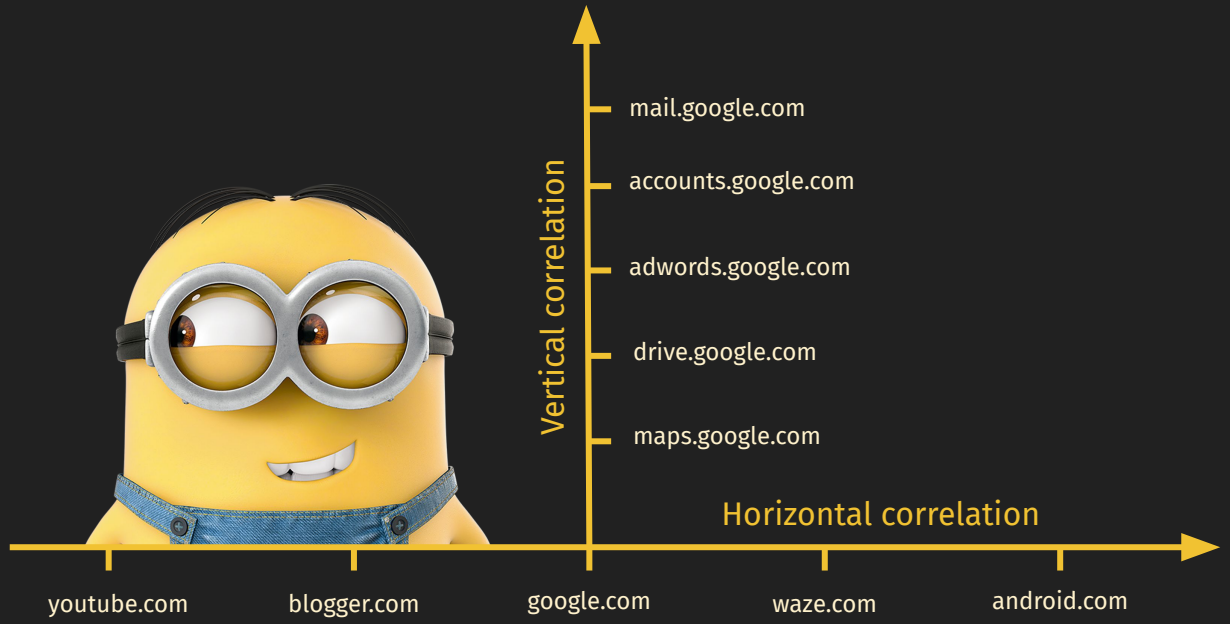
INDEX

- Goals
- First steps
- Root domains
- Subdomains
- Hosts
- Cloud
- Webs & URLs

Goals

- Have a complete "picture" of the target
- Increase the scope
- Detect potentially vulnerable websites
- Find attack vectors
- Define and narrow down main vectors

FIRST STEPS


mail.google.com
accounts.google.com
adwords.google.com
drive.google.com
maps.google.com
Vertical correlation
Horizontal correlation
youtube.com
blogger.com
google.com
waze.com
android.com

FIRST STEPS

- Google
  - First look to the target
  - “About us” section
- Dorks
  - Indexed content in browsers
  - Mainly Google and GitHub
- Metadata
  - Office documents indexed containing metadata
- Emails and users
  - Email addresses, first and last names of employees and potential users
- Leaks
  - Known data breach query

OSINT DEMO

DOMAINS

- Root domain information
  - bgp.he.net - ASNs
  - domainbigdata.com
  - viewdns.info
  - whoisxmlapi.com
- Registrants
  - Name
  - Organization
  - Email
- Reverse whois
- Google Analytics ID
- Favicon Hash

DOMAINS DEMO

SUBDOMAINS

- Passive
  - Third party services
  - Multiple services
  - Outdated information
  - Duplicated info
  - Token/data expense model
- Crtsh
  - DB certificates info
  - Created for fraud detection
  - Only info from websites with certificates
- DNS resolution

SUBDOMAINS

- DNS Brute Force
  - Dictonary-based
  - Bottlenecks
  - Slow but unique results
  - Permutations and alterations
    - Dictionary generation results-based
    - Disk space
- Crawling
  - Passive
  - Active
- DNS Records
- Google Analytics ID

SUBDOMAINS DEMO

Hosts

- Subdomains IP resolution
- Reverse IP Resolution
- CloudFlare IP
- Port Scanning
  - Passive
  - Active
- Vulnerable software versions

HOSTS DEMO

CLOUD

- Cloud assets localization
  - Brute force keywords
- S3 Buckets
- IPs belonging to cloud providers
- DNS redirections

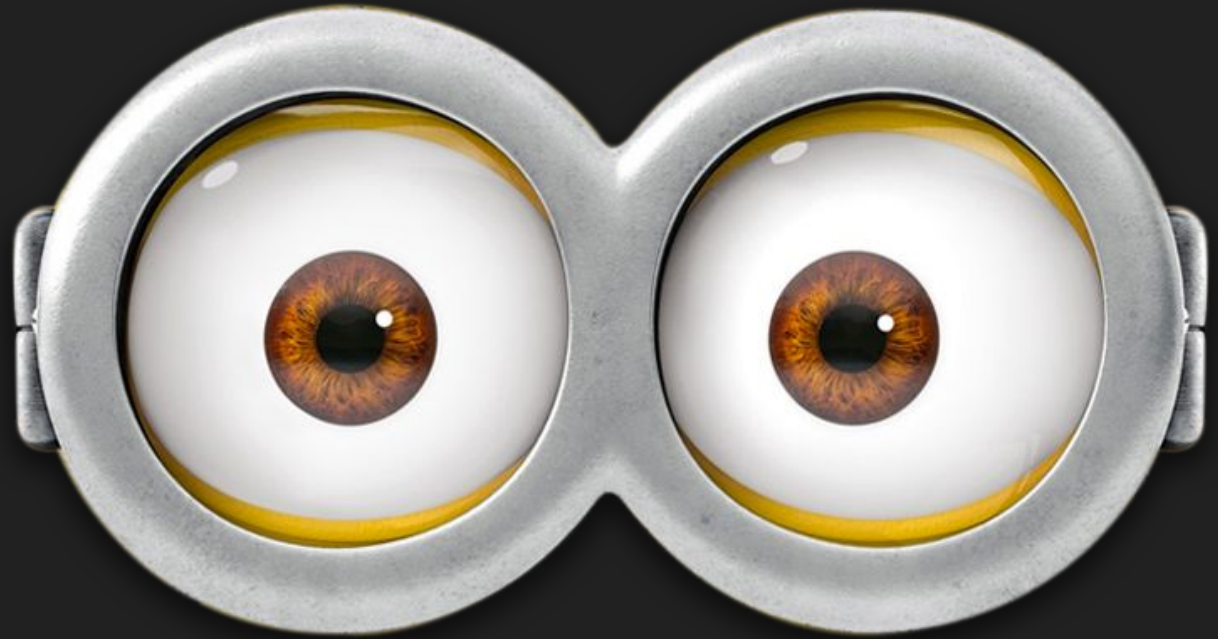
CLOUD DEMO

WEBS & URLS

- Subdomains web resolution
- Uncommon web ports scan
- Identification technologies
  - WAF
  - CMS
- Web screenshotting
- Fuzzing
- URL extraction
  - Crawling
  - Wayback Machine
  - VirusTotal
  - GitHub
- URL processing
  - Filters
  - Patterns
  - JS analysis
  - Classification

WEBS & URLS

Q&A



THANKS