REPORT 22/11/2022

FACCILONGO DOMENICO

FASE DI INFORMATION GATHERING

TASK

- Scegliere un target da cui andremo ad analizzare le informazioni
- Utilizzare i seguenti tool:
  - Google
  - Recon-ng
  - Maltego

ANALISI E VALUTAZIONI

Ho scelto come target il webserver "www.gamestop.it"

- GOOGLE:

  Il comando utilizzato su google è <<intitle:index.of inurl:gamestop>>:

Indice di /files/gamestop/logos

Nome	Ultima modifica	Dimensione	Descrizione
Elenco genitori		-	
Sava Pro Logo Font.zip	2012-10-04 14:01	898K	
capsule_lg.png	2012-10-04 13:43	140K	
capsule_lg.psd	2012-10-04 13:43		
3,5M capsule_main.png	2012-10- 04 13:43	297K	
capsule_main.psd 04-10-2012	13:44	5.0M	
capsule_sm.png 04-10-2012	13:43	40K	
capsule_sm.psd	04-10-2012 13:44	518K	
capsule_sm_small.png	04-10-2012 13:44	28K	
capsule_sm_small.psd	04-10-2012 13:44	451K	
capsule_sm_tiny.png	2012-10-04 13:44		
13K capsule_sm_tiny.psd	2012-10-04 13:44	329K	
game_logo_hi_res.psd	2012-10-04 13:45	10M	
header.png	2012-10-04 13:44	162K	
header.psd	2012- 10-04 13:45		
3.6M leveluplabs_logo_hi_..>	2012-10-04 13:46	19K	
leveluplabs_logo_hi_..>	2012-10-04 13:46	117K	
leveluplabs_logo_hi_..>	2012-10-04 13:46	12K	
leveluplabs_logo_hi_.. >	2012-10-04 13:46	18K	
leveluplabs_logo_hi_..>	2012-10-04 13:46	120K	
leveluplabs_logo_hi_..>	2012-10-04 13:46	12K	
leveluplabs_logo_lo_..>	2012-10-04 13:46		
13K leveluplabs_logo_lo_..>	2012-10-04 13:46	74K	
leveluplabs_logo_lo_..>	2012-10-04 13:46	8.3K	
leveluplabs_logo_lo_..>	2012-10-04 13 :46		
13K leveluplabs_logo_lo_..>	2012-10-04 13:46	76K	
leveluplabs_logo_lo_..>	2012-10-04 13:46	8.4K	

Abbiamo provato anche ad utilizzare la ricerca del numero di telefono utilizzando <<phonebook:gamestop>> ma non ha prodotto risultati in quanto evidentemente il target in questione non possiede un numero di telefono per i clienti.

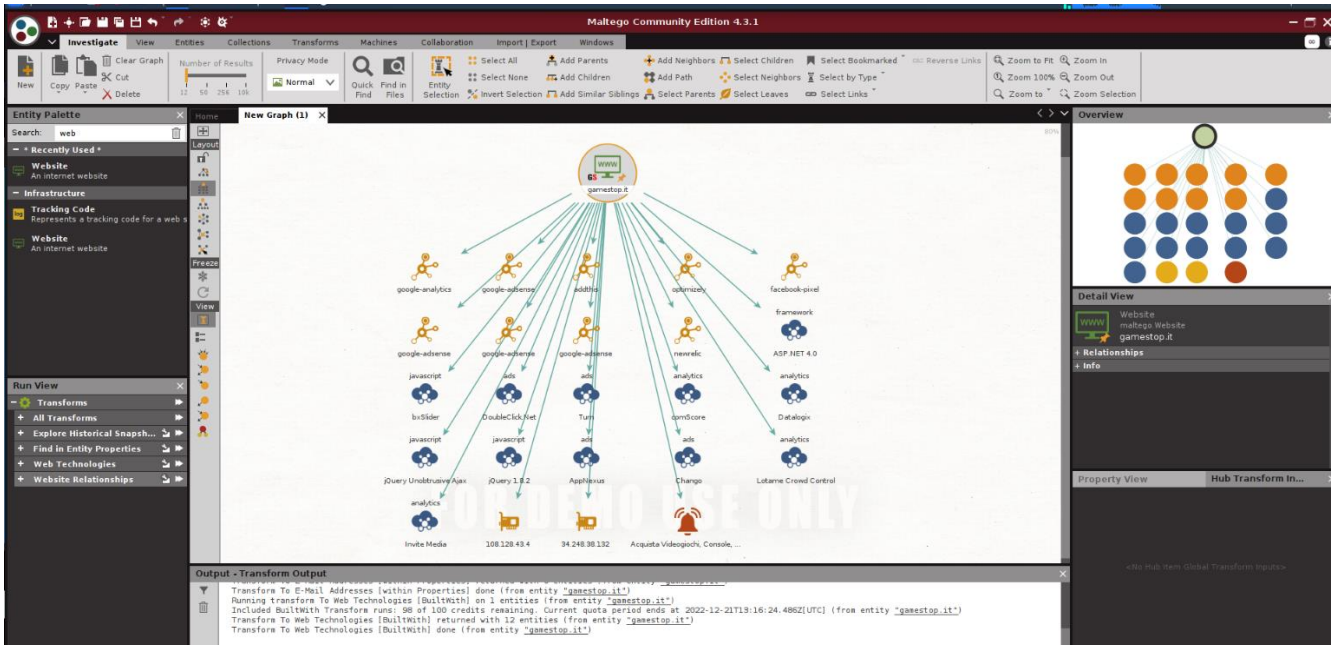
- RECON-NG:

```
[recon-ng][default][whois_pocs] > options set SOURCE gamestop.com
SOURCE => gamestop.com
[recon-ng][default][whois_pocs] > run

GAMESTOP.COM
[*] URL: http://whois.arin.net/rest/pocs;domain=gamestop.com
[*] URL: http://whois.arin.net/rest/poc/NETWO7140-ARIN
[*] Country: United States
[*] Email: ChrisConnors@gamestop.com
[*] First_Name: None
[*] Last_Name: Network Admin
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Grapevine, TX
[*] Title: Whois contact
[*] ----------
[*] Country: United States
[*] Email: AlanBlowers@gamestop.com
[*] First_Name: None
[*] Last_Name: Network Admin
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Grapevine, TX
[*] Title: Whois contact
[*] ----------
[*] URL: http://whois.arin.net/rest/poc/NEA4-ARIN
[*] Country: United States
[*] Email: arinadmin@gamestop.com
[*] First_Name: None
[*] Last_Name: NEA
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Grapevine, TX
[*] Title: Whois contact
[*] ----------
[*] URL: http://whois.arin.net/rest/poc/BIN47-ARIN
[*] Country: United States
[*] Email: brianingram@gamestop.com
[*] First_Name: Brian
[*] Last_Name: Ingram
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Grapevine, TX
[*] Title: Whois contact
[*] ----------
[*] URL: http://whois.arin.net/rest/poc/FRAZI111-ARIN
[*] Country: United States
[*] Email: deannefrazier@gamestop.com
```

Dopo aver avviato il il tool con il comando <<recon-ng>> da terminale, abbiamo scaricato le librerie che ci servono per le informazioni da ottenere.
Di fatti abbiamo effettuato una scansione per i contact di gamestop e abbiamo ottenuto una lista del personale con le loro relative Email e regioni da dove provengono.

- MALTEGO:



Infine l'ultimo tool utilizzato è Maltego il quale ci fornisce molti più dettagli, di fatti abbiamo ricercato ed ottenuto:

- Relationship
- Technology
- WebSite Title
- Ipv4 Address