Page 161

TOP SECRET//SI//REL FVEY

Exploiting Facebooktraffic in the

passive environment to obtain
specific information

NAME REDACTED

Capability Developer
Global Telecommunications Exploitation (GTE)

GCHQ

TOP SECRETtfSItfREL FVEY

This information is exempt from disclosure under the Freedom of information Act 2000 and may be subject to exemption under other UK

information legislation. Refer disclosure requests to GCHQ ! i

CONTACT INFORMATION REDACTED

Page 161

TOP SECRET//S1//REL FVEY

Why OSNs?

i n

- Targets increasing usage of Facebook,
BEBO, MySpace etc.
- A very rich source of information on targets:
- Personal details
- ‘Pattern of Life’
- Connections to associates

- Media

TOP SECRET//SI//REL FVEY

TOP SECRET//SWREL FVEY

Looking to the Passive Environment

• Many targets on Facebook lock down their profiles, so it is not possible to view all of their information...

But passive offers the opportunity to collect this information by exploiting inherent weaknesses in Facebook's security model.

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK

information legislation. Refer disclosure requests to GCHQ on

CONTACT INFORMATION REDACTED

Page 162

TOP SECRET//SI//REL FVEY

Facebook's use of the Akamai CDN

Usemame/Password Authentication

Users

Mobile/Desktop Web-
browser or F ace bo ok
Client

Core Facebook Servers

HTML

HTTP Request for Image

Images

ra

E

m

<

Facebook Content Delivery Network {CDN)
Servers

Profile images, album images...

TOP SECRET//SI//REL FVEY

Thia information is exempt from diadoaune under the Freedom of information Act 2000 and may be subject to exemction under other UK

information legislation. Refer diadosure requests to G ChQ on

CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY

GCHQ

Exploiting the FB CDN

Weaknesses

- Assumed Authentication
- Security through obscurity

It is possible to dissect the CDN URL's generated by Facebook in order to extract the Facebook User ID of the user whose picture the file pertains to. For example, below is a typical profile image URL:

http://profile.ak.fbcdn.net/hprofile-ak-sf2p/

hs621.snc3/27353

REDACTED

2215_q.jpg

The text highlighted in green specifically relates to the specific server within Facebooks CDN. And the text highlighted in yellow is the users Facebook User ID.

TOP SECRET//SI//REL FVEY

Obtaining profile
and album images

CCHQ

fSPRING
BISHOP

Request Profile
Image

Profile Image of
Target

URL pointing to
targets Facebook
Profile Image