The Snowden files: British intelligence agency describes attack on Anonymous

GCHQ, the British signals intelligence agency, prepared the following slides for a top-secret conference in 2012, revealing that it had mounted an online attack on the hacktivist collective known as Anonymous in September 2011.

The slides were leaked by former NSA contractor Edward Snowden and obtained exclusively by NBC News.

NBC News is publishing the documents with minimal redactions to protect individuals. All annotations appear in the original documents prepared by GCHQ.

Hacktivism: Online Covert Action

- Hacktivist groups
- Online Humint
- Effects Operations
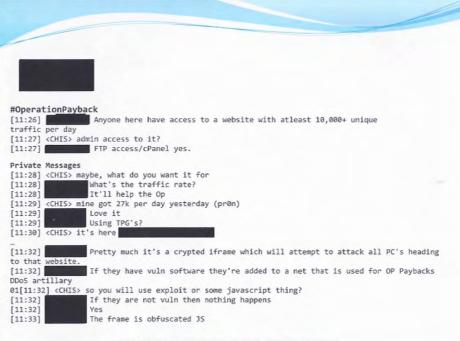
Hacktivist groups

- They are diverse and often have multiple, varied aims
- Anonymous
- LulzSec
- A-Team
- Syrian Cyber Army
- Targets include: Corporations, banks, governments, copyright associations, political parties
- Techniques: DDoS, data theft – SQLi, social engineering
- Aims:

Online HUMINT -CHIS

- 2 Examples from Anonymous IRC Channels:
  - Gzero
  - P0ke

Gzero & ▮▮▮▮

- Asking for traffic
- Engaged with target
- Discovered Botnet with malware analysis & SIGINT
- Outcome: Charges, arrest, conviction

#OperationPayback
[11:26] ████████ Anyone here have access to a website with atleast 10,000+ unique traffic per day
[11:27] <CHIS> admin access to it?
[11:27] ████████ FTP access/cPanel yes.

Private Messages
[11:28] <CHIS> maybe, what do you want it for
[11:28] ████████ What's the traffic rate?
[11:28] ████████ It'll help the Op
[11:29] <CHIS> mine got 27k per day yesterday (pr0n)
[11:29] . ████████ Love it
[11:29] ████████ Using TPG's?
[11:30] <CHIS> it's here ████████

...
[11:32] ████████ Pretty much it's a crypted iframe which will attempt to attack all PC's heading to that website.
[11:32] ████████ If they have vuln software they're added to a net that is used for OP Paybacks DDoS artillary
01[11:32] <CHIS> so you will use exploit or some javascript thing?
[11:32] ████████ If they are not vuln then nothing happens
[11:32] ████████ Yes
[11:33] ████████ The frame is obfuscated JS

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

GZero

```
[15:16] <GZero> yo
[15:16] <GZero> ██████ works with me
[15:16] <GZero> i need traffic
[15:16] <CHIS> hey.
[15:17] <CHIS> what for?
[15:17] <GZero> exploit pack
[15:17] <GZero> will pay you if traffic is good
[15:17] <GZero> u wanna talk?

[15:18] <GZero> http://alpha.b0x.su/hits.txt - Need to make this bigger ;)
[15:19] <GZero> http://pastebin.com/██████ - JS for iframe
[15:19] <GZero> http://alpha.b0x.su/iqjtcoxo8.php - Live URL
[15:19] <GZero> U have traffic?

[15:21] <CHIS> so what is at that page anyway?
[15:21] <GZero> several exploits
[15:21] <CHIS> yeah I've got traffic. got 92k hits yesterday.
[15:22] <GZero> ok
[15:22] <GZero> lets talk :p
```

Infrastructure
WHOIS: gzero ██████

1st Stage implant:
Lead to 2nd stage & WARPIG
botnet, SpyEye malware

Online Humint - Gzero

- JTRIG & SIGINT reporting lead to identification, arrest
- Sentenced for 2 years – April 2012

Hacker jailed for stealing 8 million identities

By Emil Protalinski | April 4, 2012, 3:21pm PDT

Summary: *A British hacker has been sentenced to 26 months for stealing 200,000 PayPal accounts, 2,701 bank card numbers, as well as 8,110,474 names, dates of birth, and postcodes of U.K. residents.*

23-year-old Edward Pearson of York, Northern England, will spend two years and two months behind bars for his hacking spree. The sentence would have been greater if he made more use of the huge amount of stolen data.

The British hacker used the Zeus and SpyEye Trojans to steal confidential data from U.K. victims between January 1, 2010, and August 30, 2011, from an undisclosed source. On his computers, police found 200,000 stolen PayPal accounts, 2,701 bank card numbers, as well as 8,110,474 names, dates of birth, and postcodes of U.K. residents. If all the details of what he had harvested were printed out, it would fill 67,500 double-sided A4 pages, according to authorities.

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

p0ke

- Discussing a database table labelled 'FBI', in Anon Ops IRC
- Engaged with target – exploiting US Government website, US company website

```
#OperationPayback
[19:40] <&p0ke> Topiary: I has list of email:phonenumber:name of 700 FBI tards
[19:40] <&p0ke> :P
[19:41] <Topiary> what about passwords?
[19:41] <&p0ke> It was dumped from another gov db, Topiary
[19:41] <&p0ke> A table named fbi
[19:42] <Topiary> ah, like an FBI affiliated contact userbase?
[19:42] <&p0ke> that was all it contained D:
```

p0ke

Private Messages

```
[20:04]              so what was the site?!
[20:04]              if its special ;)
[20:04] <p0ke> usda.gov

[20:08]              :(. did you get past the site db tho?
[20:09] <p0ke> Yep
[20:13]              so u had a poke around on the network? lol
[20:13] <p0ke> meh a lil
[20:13] <p0ke> Mastercard:              @mail.house.gov
[20:13] <p0ke> IMPAC:              @ocar.army.pentagon.mil
[20:13] <p0ke> VISA:              @gimail.af.mil
```

P0ke - Identification

BBC NEWS TECHNOLOGY

Who loves the hacktivists?
By Ian Mackenzie

Private Messages

...
[21:07]   oh btw have you seen this
[21:08] <p0ke> sexy
[21:09]   cool huh?
[21:11] <p0ke> Ya

...Enabled SIGINT
P0ke:
Name:
Facebook, email accounts

Effects on Hacktivisim

- Op WEALTH – Summer 2011
    - Intel support to Law Enforcement – identification of top targets
    - Denial of Service on Key Communications outlets
    - Information Operations

DDoS

- ROLLING THUNDER
  - RT initial trial info

```
[15:40] <srewder> hello, was there any problem with the irc network? i wasnt able to connect the
past 30 hours.
[15:42] <speakeasy> yeah
[15:42] <speakeasy> we're being hit by a syn flood
[16:44] <speakeasy> i didn't know whether to quit last night, because of the ddos
```

anon_anonz Anonymous
irc.anonops.li tango down :(
3 Sep

anon_anonz Anonymous
720pHighDefention (notice the typo) on YouTube anon _anonz on
twitter nickname: meowitude
2 Sep

anon_anonz Anonymous
irc.anonops.li back up @anonops #anonymous #antisec
2 Sep

IO Outcome

- CHIS with ▮▮▮▮
- 80% of those messaged where not in the IRC channels 1 month later

Conclusion

- Team working – SIGINT, JTRIG, CDO, INOC – was key to success
- Online Covert Action techniques can aid cyber threat awareness
- Effects can influence the target space