

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

TOP SECRETICOMINTIREL TO USA AUS. CAN. GBR. NZL



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:

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



Online HUMINT -CHIS

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

TOP SECRETICOMINTIREL TO USA AUS, CAN, GBR, NZL



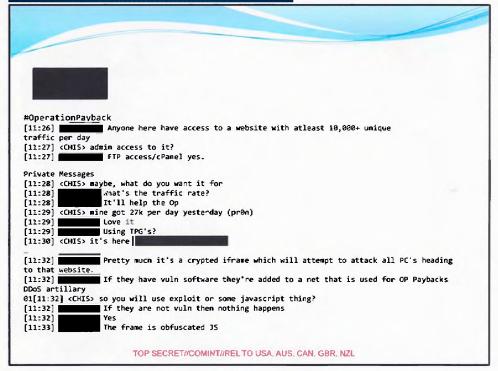
Gzero &

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

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



investigations.nbcnews.com





```
GZero
[15:16] <GZero> yo
[15:16] <GZero> works with me
[15:16] <GZero> i need traffic
                                                Infrastructure
[15:16] <CHIS> hey.
[15:17] <CHIS> what for?
                                                 WHOIS: gzero
[15:17] <GZero> exploit pack
[15:17] <GZero> will pay you if traffic is good
[15:17] <GZero> u wanna talk?
[15:19] <GZero> U have traffic?
                                                        Lead to 2<sup>nd</sup> stage & WARPIG
[15:21] <CHIS> so what is at that page anyway?
                                                        botnet, SpyEye malware
[15:21] <GZero> several exploits
[15:21] <CHIS> yeah I've got traffic. got 92k hits yesterday.
[15:22] <6Zero> ok
[15:22] <GZero> lets talk :p
                       TOP SECRET//COMINT//REL TO USA AUS, CAN, GBR, NZL
```



Online Humint - Gzero

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

Hacker jailed for stealing 8 million identities

Em: Prote nac

Summary: A Brash harder has been sensenced to 26 months for stealing 200,000 PapPal accounts. 2.70s bank conditionabers, as well as 8.100_my names, dates of birth, and postcodes of U.S. residents.

23-mail-old Edward Pearson of York, Northern England, will shend this waars and two worths behind bars for his had any spree. The sentence would have been greater if he made more use of the hope amount of stolen data.

The British hacker used the Zeus and Spotfile Troises to steat confidential data from U.K. victors between Parison 1, 2010, and Jangust 20, 2011. from an unascosed source. On his computers point found 200, 000 steller Parisol accounts 2, 2701 ban's care members, as well as \$1,100,474 names, dates of birth, and postcodes of U.K. renderts. If all the details of alast are had harvested were ported one. If would \$16,7500 double-sided All pages, according to subtrobles.



TOP SECRETI 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] <8p0ke> A table named fbi

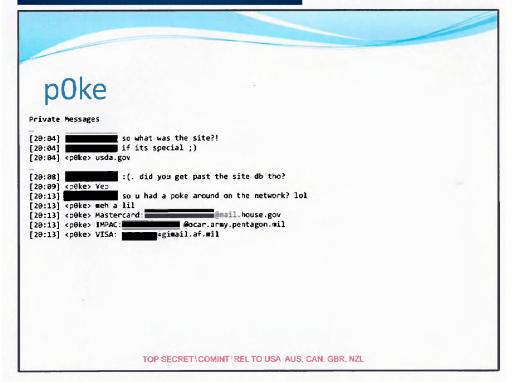
[19:42] <Topiary> ah, like an FBI affiliated contact userbase?

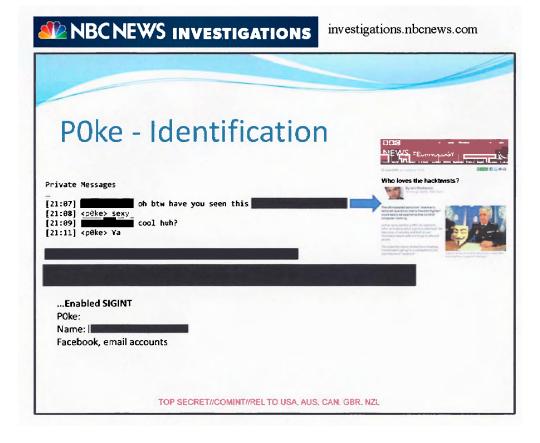
[19:42] <8p0ke> that was all it contained D:

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



investigations.nbcnews.com







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

TOP SECRET//COMINTIREL TO USA, AUS, CAN, GBR, NZL



DDoS

- ROLLING THUNDER
 - RT initial trial info

[15:40] (snewder> 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

ec anonops li tango down (

720pHighDefention (notice the typo) on YouTube anon_anonz on twitter nickname meawitude

anon_anonz isc anonops li back up anonops Fanonymous Fantisec

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

NBC NEWS INVESTIGATIONS

IO Outcome

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

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



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

TOP SECRET//COMINT//REL TO USA AUS CAN GBR NZI