investigations.nbcnews.com

 \mathcal{O}

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

Mentions NBC NEWS INVESTIGATIONS

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:

investigations.nbcnews.com

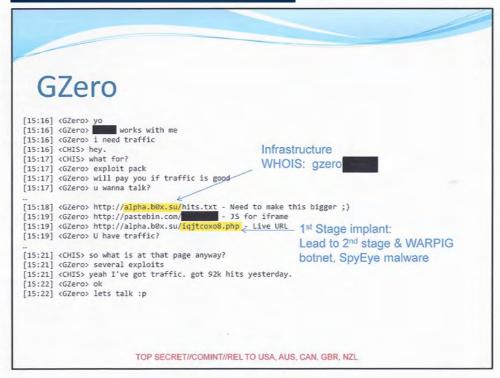
Online HUMINT - CHIS

- 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?</chis>
[11:27] FTP access/cPanel yes.
Private Messages
[11:28] <chis> maybe, what do you want it for</chis>
[11:28] What's the traffic rate?
[11:28] It'll help the Op
[11:29] < <u>CHIS> mine</u> got 27k per day yesterday (pr@n)
[11:29] Love it
[11:29] Using TPG's? [11:30] <chis> it's here</chis>
[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?</chis>
[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
TOP BEOKET/COMMUNICE TO GAN AGG, GAN, OBI, ALL



investigations.nbcnews.com

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 Protainski (April 4, 2012, 3:21per 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 Zous and SprEve Trojans to stead confidential data from U.K. victims between January 1, 2010, and Jaupust 30, 2011, frem an undiscosed source. On this computers, police found 200,000 stellen FayPal accounts, 2,701 bank: card numbers, as well as 2110,474 names, dates of birth, and postoodes of U.K. residents. Y all the details of nuta the hash danuested were printed ox, it nould SII 67,500 double-sided A4 pages, according to authorhities.



p0ke

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

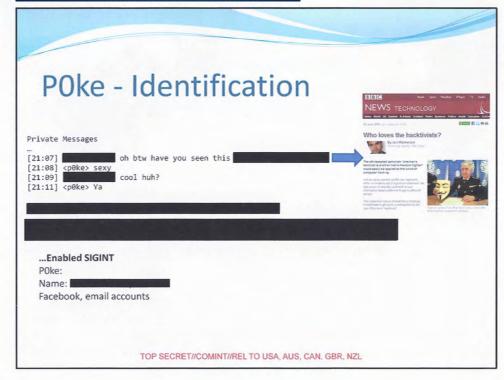
#OperationPayback

[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:

investigations.nbcnews.com

p0ke	
Private Messages	
[20:04] so what was the site?! [20:04] if its special ;) [20:04] <p0ke> usda.gov</p0ke>	
[20:08] cp0ke> Yep :(. did you get past the site db tho? [20:09] <p0ke> Yep</p0ke>	
[20:13] control so u had a poke around on the network? lol [20:13] <poke> meh a lil</poke>	
[20:13] <poke> Mastercard: @mail.house.gov [20:13] <poke> IMPAC: @ccar.army.pentagon.mil [20:13] <poke> VISA: @ggimail.af.mil</poke></poke></poke>	
[2013] Chores ATMY BRUNCH CONTRACT	
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

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 :(



anon_anonz -nonmous 720pHighDefenition (notice the typo) on YouTube anon_anonz on twitter nickname: meowitude



anon_anonz knowneds izc.anonops.li back up @anonops #anonymous #antisec

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