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
Anyone here have access to a website with at least 10,000+ unique traffic per day?

<CHR1> admin access to it?

FTP access/CPanel yes.

Private Messages

<CHR1>: maybe, what do you want it for?
<CHR1>: what's the traffic rate?
<CHR1>: It'll help the OP
<CHR1>: Mind got 27k per day yesterday (pm/rn)
<CHR1>: Love it
<CHR1>: Using TPL's?
<CHR1>: It's here

Pretty much it's a crypted iframe which will attempt to attack all PC's heading to that website.

If they have vuln software they're added to a net that is used for OP Paybacks

DoS artillery

If they are not vuln then nothing happens

Yes

The iframe is obfuscated JS
GZero

[GZero] yo
[35:16] GZero: works with me
[35:16] GZero: i need traffic
[35:16] GHIS: hey:
[35:17] GZero: what for?
[35:17] GZero: exploit pack
[35:17] GZero: will pay you if traffic is good
[35:17] GZero: u wanna talk?
[35:18] GZero: http://alpha.box.su/hits.txt - need to make this bigger ;)
[35:19] GZero: u have traffic?
[35:21] GHIS: so what is at that page anyway?
[35:21] GZero: several exploits
[35:22] GZero: ok
[35:22] GZero: lets talk sp

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

Infrastructure
WHOIS: gzero
Online Humint - Gzero

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

Hacker jailed for stealing 8 million identities

Summary: A British hacker has been sentenced to 16 months for stealing 800,000 PayPal accounts. He has 300,000 stolen credit card numbers, social security numbers, dates of birth, and addresses of U.S. residents.

The hacker used the Zeus and Spycall Trojan to steal confidential data from U.K. victims between January 1, 2008, and August 30, 2013. From an undisclosed source, the hackers stole a bank card number, a number of bank accounts, and 800,000 stolen credit card numbers. The details of the data stolen were printed out, and it would fit in 200 double-sided A4 pages, according to authorities.

TOP SECRET/SECRET/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
[19:48] <&p0ke> Topiary: I have list of email:phonenumber:name of 700 '01 tards
[19:49] <&spike> 'IP
[19:50] <Topiary> what about passwords?
[19:51] <&spike> It was dumped from another gov db, Topiary
[19:51] <&spike> A table named tbi
[19:52] <Topiary> ah, like an FBI affiliated contact us database?
[19:52] <&spike> that was all it contained 0:

TOP SECRET/COMINT/REL TO USA, AUS, CAN, GBR, NZL
p0ke

Private Messages

[28:03] [redacted] so what was the site?! [28:04] if its special ;]
[28:04] <p0ke> usda.gov

[28:06] [redacted] :(. did you get past the site db tho?
[28:09] <p0ke> Yup
[28:13] <p0ke> uh u lii
[28:13] <p0ke> Mastercard@mill.house.gov
[28:13] <p0ke> IMPAC@ocar.army.pentagon.mil
[28:13] <p0ke> VESA@mil.mil
Effects on Hacktivism

- 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] <crowder> hello, was there any problem with the irc network? i wasn't able to connect the past 30 hours.
[15:42] <cspeakeasy> yeah
[15:42] <cspeakeasy> we're being hit by a syn flood
[15:44] <cspeakeasy> i didn't know whether to quit last night, because of the ddoos

anon_anon
irc anonops li tango down!

anon_anon
720p [High Definition] (notice the typo) on YouTube anon_anon on twitter nickname snowslide

anon_anon
irc anonops li back up anonops l'anonymous fartsec
IO Outcome

- CHIS with [redacted]
- 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