



In this final part of the workshop we will look at how Cybercrime is likely to evolve over the next 1-2 years

I will start by first giving a short overview of my team. My team is 100% dedicated to researching the future of Cybercrime, so giving you an idea of how we work should be useful here.

After that we will first look at the current state of Cybercrime. It is critical to fully understand the landscape today before we can look to the future

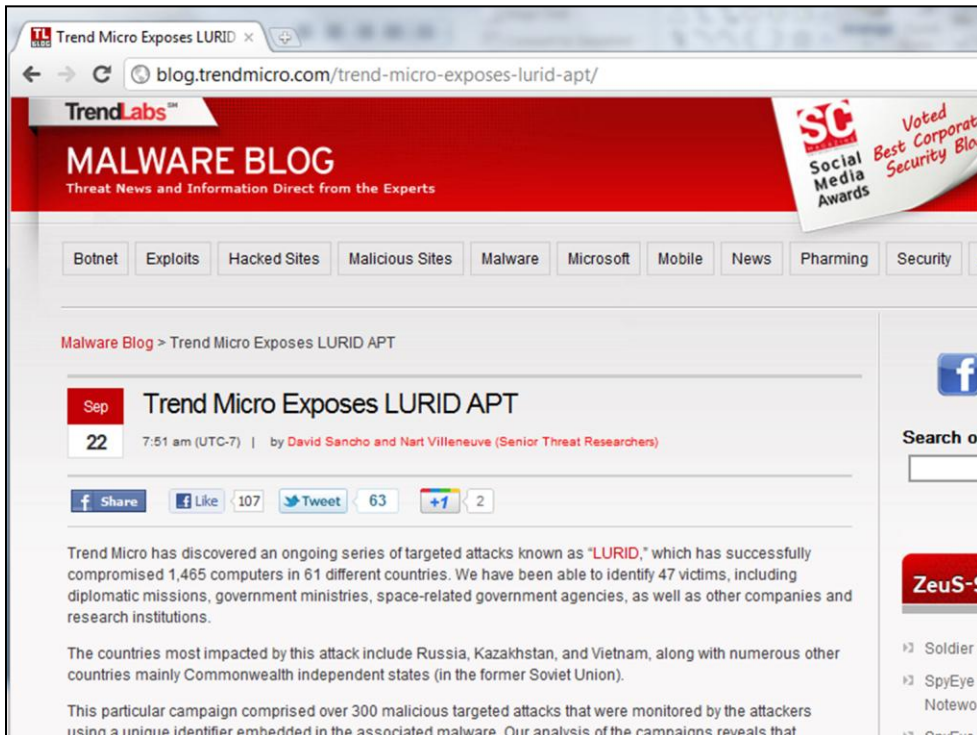
And finally we will finish up this workshop by looking at where Cybercrime is heading in the next 24 months.

Stop me at any stage if you have questions you want to discuss.



20 RESEARCHER – ALL AROUND THE WORLD

2 REASONS – BEST GUYS / DIFFERENT REGIONS = DIFFERENT THREATS



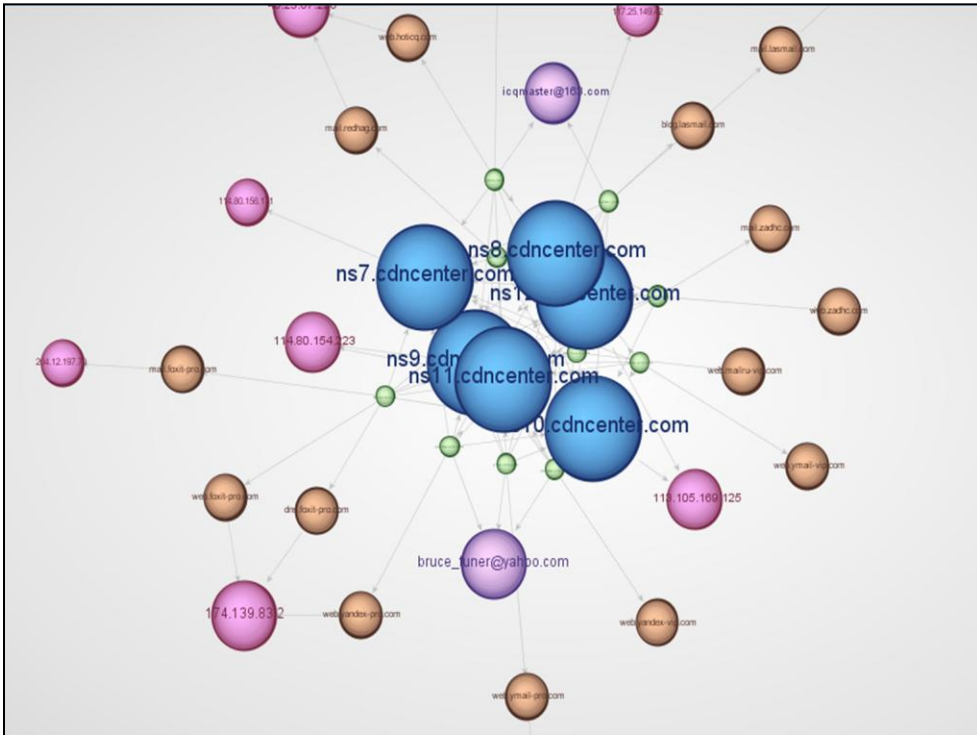
PRIMARILY CYBERCRIME INVESTIGATIONS

E.G. LURID – COMPROMISED RUSSIAN / EX-SOVIET EMBASSIES, LE, SPACE

STEAL INFO – SEND BACK – TARGETED DALAI LAMA BEFORE

CONSTANTLY WORKING ON THESE CASES

SECURITY COMPANY – MAKE MONEY – BUT THIS PROTECTS OUR CUSTOMERS. BLOCK SHUT DOWN



STANDARD DAY – PROFILING CRIMINAL NETWORKS.

GET INTO THEIR HEADS – SEE NEXT MOVE

KNOW THEIR INFRASTRUCTURE

THIS IS LURID – IP TO EMAIL ETC

IRISHTIMES.com Thursday, October 13, 2011 Q Search...

[News](#) | [Sport](#) | [Business](#) | [Comment](#) | [Life](#) | [Society](#) | [Culture](#) |
 [Cars](#) | [Jobs](#) | [Property](#) | [Home Delivery](#) | [Dating](#) | [Shop](#) | [More »](#)

[Ireland](#) | [World](#) | [In Depth](#) | [Today's epaper](#) | [Archive](#) | [Weather](#) | [Rugby World Cup](#) | [Festival Hub](#) | [Race for the Aras](#)

Home » Ireland » Other Stories »

[Like](#) 11 | [Tweet](#) 12 | [+1](#) 0 | [Share](#) 4 |
 Print | RSS | Text Size: A - A

The Irish Times - Friday, September 2, 2011

Two teenagers arrested over cyber attack on FG website

CONOR LALLY and EGIN Mac CONNELL

GARDAÍ INVESTIGATING a cyber attack on the Fine Gael website have arrested two people.

During the attack, which took place in January, the site was modified and the personal information of 2,000 site subscribers was stolen and e-mailed to the media.

The attack was claimed at the time by international cyber-hacking group Anonymous.

Gardaí carried out two arrest and search operations in counties Galway and Offaly yesterday morning during which two teenagers were arrested.

The suspects were detained at their homes, from which the arresting officers took computers for examination.

In this section »

- Council tells Travellers to leave quietly and warns it will proceed with eviction
- Journalists seek to intervene in IRA oral history case
- MEP lodges complaint over Corrib protest with Garda ombudsman
- High Court suspends solicitor over alleged missing €900,000
- Tribunal told car was taken by garda
- Garda retirements planned for months, says ...

ADVERTISEMENT

Wake up, Invest in Brazil

Returning 8-12% per year

Brazilian Agriculture is Booming

Packages from €10,000

Download Information Now

We advise all clients solely applying for investment to consult a qualified independent advisor as to the suitability of this product. As with any investment the value can fall as well as rise.

Latest

- 21:41 Google Q3 profit up 26%
- 21:24 Simpson has top spot in his sights
- 21:14 HSE defends Cork service
- 21:10 Rovers one the brink of another title
- 20:59 Sleep expert testifies in Jackson trial
- 20:39 Cocaine worth €5m seized in Cork

WE CONCENTRATE ON INFRASTRUCTURE BUT ALSO GET THE CRIMINALS

ALWAYS WORK WITH LOCAL LE – LULZSEC IRELAND EXAMPLE



SOMETIME QUICK PROCESS – SOMETIMES 5 YEARS

OPERATION GHOST CLICK – LARGEST EVER

REGULAR WORK WITH LE



CAN ALSO DO TEACHING FOR LARGE ORGS

WORK WITH ACADEMIA – IF SEC RESEARCHERS DO THE PRACTICAL STUFF, THEY DO THE FAR OUT STUFF

WORK CLOSELY WITH UCD FOR EXAMPLE – AND INTERPOL

ANY LANGUAGE - WE CAN DO IT



MY TEAM FOCUS ON NEXT 3 YEARS

BUT LETS LOOK AT CYBERCRIME TODAY – AND WHERE IT IS EVOLVING
TO



CYBERCRIME ALL ABOUT MONEY – MAKES A TONNE

ESTIMATES AS HIGH AS ...

\$ 1 Trillion

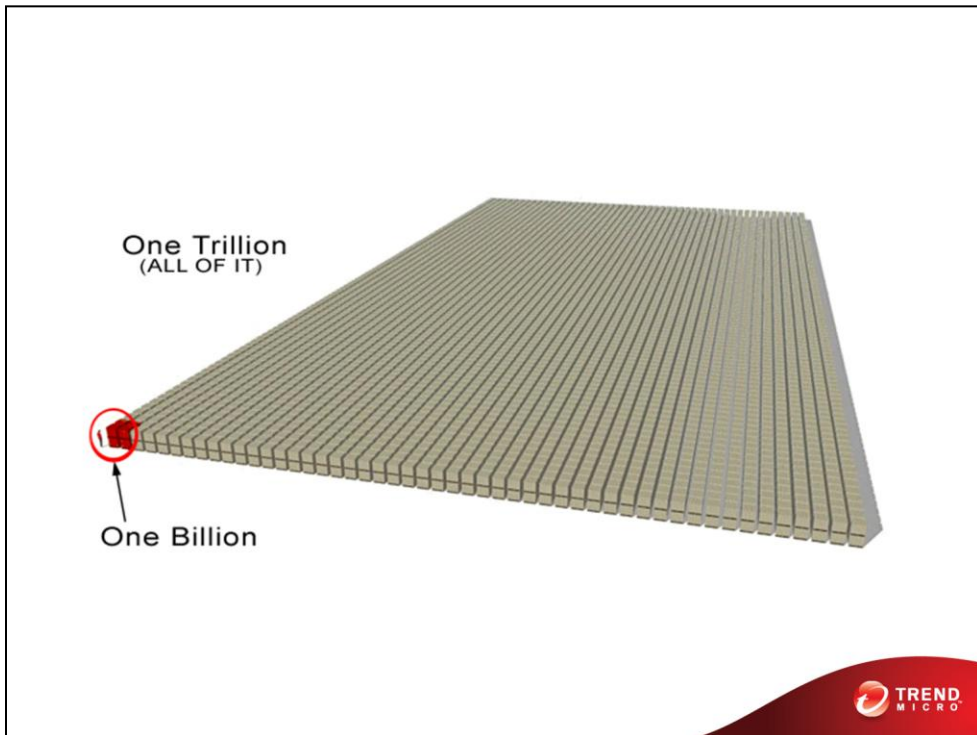


1 TRILLION

MORE MONEY THAN COUNTRIES

MORE THAN DRUGS

TWO PROBLEMS – 1 WITH A BUNCH OF ZEROS



PALLETS ETC

MADE UP NUMBER – NO TAX RETURNS

WILL LOOK AT 2 REAL CASES LATER

HOW DO THEY MAKE THAT MONEY

```
318. Address : Paul Silver - 16 goldney way - Temple Cloud - Bristol,&nbsp;Avon&nbsp;; - BS39 5DU - United  
Kingdom  
319. Balance : &pound;101.14&nbsp;; GBP  
320.  
321. Email : pondexpert@googlemail.com  
322. Password : digweed1  
323. Status : Verified  
324. Address : adrian r horgan - 7 coppice rd, willaston - nantwich,&nbsp;Cheshire&nbsp;; - cw56qa - United  
Kingdom  
325. Balance : &pound;0.00&nbsp;; GBP  
326.  
327. Email : belenkas@inbox.lt  
328. Password : dzeveckaite  
329. Last log in : June 2, 2011  
330. Status : Verified  
331. Address : Arturas Martinkus - suvalku 7-12 - Vilnius03106 - Lithuania  
332. Balance : &#8364;0.00&nbsp;; EUR  
333.  
334. Email : mikerainsford@eircom.net  
335. Password : 52849mgr  
336. Last log in : March 12, 2011  
337. Address : margaret rainsford - lasata - rooska west - bantry,&nbsp;co cork&nbsp;; - none - Ireland  
338. Balance : &#8364;0.00&nbsp;; EUR  
339.  
340. Email : louiseacan28@hotmail.com  
341. Password : jabberwocky  
342. Status : Verified  
343. Address : louise canning - 28 st lukes close - evesham - worcestershire,&nbsp;Worcestershire&nbsp;; -
```

STARTERS – STEAL YOUR INFO

BUNCH OF EMAIL / PASSWORDS ON PASTEBIN

IRISH ADDRESS – ONE OF THOUSANDS

The screenshot shows the Spy Eye v1.2 web interface. At the top, there is a logo of an eye and the text "Spy Eye v1.2". Below the logo, there are several navigation buttons: "Find INFO", "Statistic", "FTP accounts", "Settings", "Screen shots", "BOA Grabber", "CC Grabber", and "Certificate Grabber". A status bar at the top right shows "7142 k" and "+978504".

The main section is titled "Get BOA Accounts v0.23". It contains a form with the following fields:

- Bot GUID:
- Report date region: 17/09/2010 ... 27/09/2010
- Limit:

Below the form, there is a table with the following data:

id	bot_guid
	Eunice COMPUTER_115C60AAE9
Access_ID : CHICHICOL	
state : CA	
passcode : Jd [REDACTED] 7	
passcode : Jd [REDACTED] 7	
acc0 : Checking-5003; \$341.50	
acc1 : Checking-5074; \$123.66	
acc2 : Checking-8192; \$121.91	
acc3 : Bank of America Gold Visa - 4604; \$5,345.08	
... : ?	
controls : Accounts; Bill Pay; Transfers; Investments; Customer Service	
email : eunice_nna@yahoo.com	
q@a0 : In what city were you born? (Enter full name of city only); BAMENDA	
q@a1 : What is the first name of your first child?; CHIBUEZE	
q@a2 : In what city was your mother born? (Enter full name of city only); UMURU OKABIA	
ip : 24.4.244.199	

ANOTHER FROM RUSSIA

ALSO BALANCES / PETS ETC

FAR MORE LIKELY TO BE VICTIM ONLINE

HAVE YOU BEEN HACKED?

SO 1 TRILLION A YEAR – POTENTIALLY – LOOK AT REAL CASES



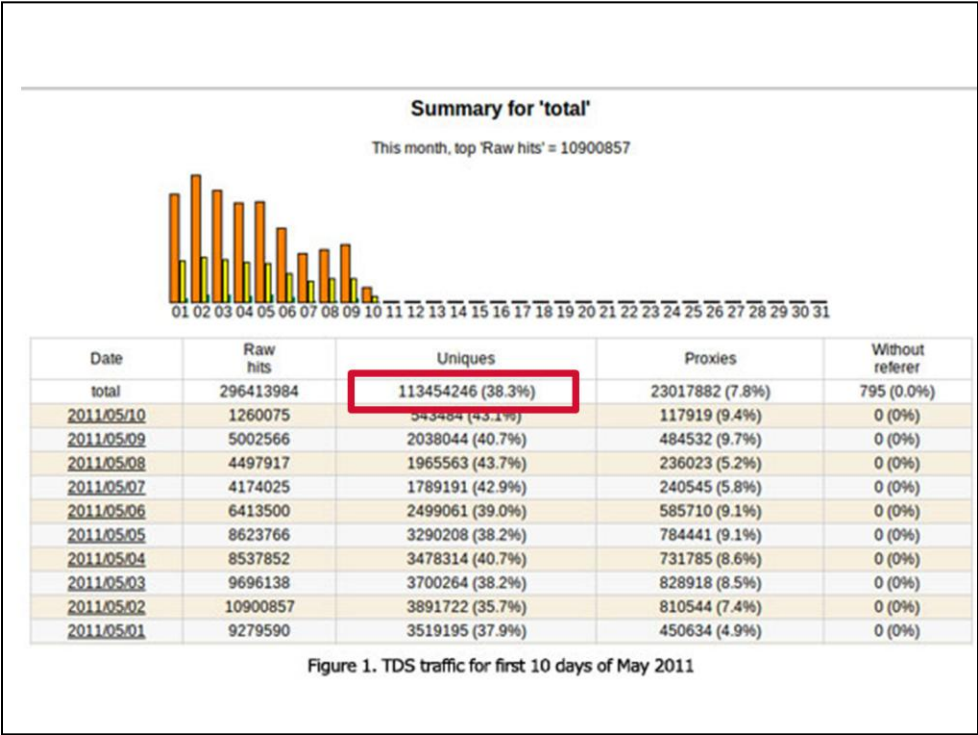
FIRST – FAKE AV (NOT NORTON)

AROUND FOR YEARS.

ONE GANGS LAST YEAR – POISONED GOOGLE IMAGE SEARCHES

FIRST MAC FAKE AV

STATS PAGE WIDE OPEN

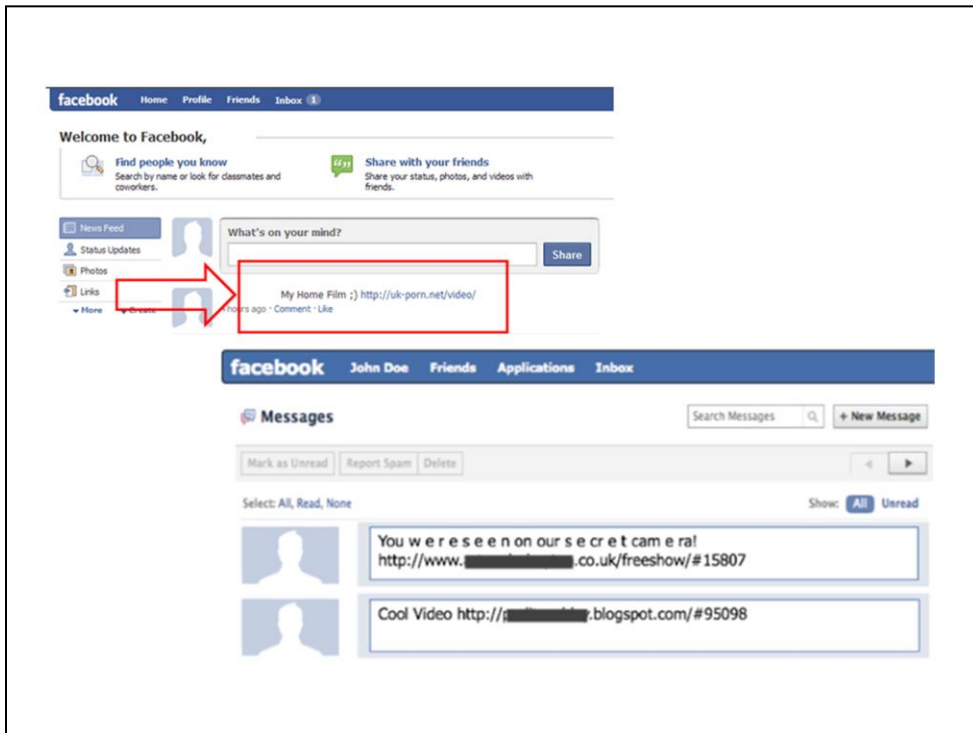


5000 WEBSITES

113 MILLION UNIQUE VISITORS IN 10 DAYS

COULD NOT ACCESS BACKEND

1% = 5 MILLION A DAY (NOT BAD)



ANOTHER FAMOUS GANG – KOOBFACE. WE HAVE PUBLISHED PAPERS

STEALS LOGINS FOR SOCIAL NETWORKS

YOU TRUST YOUR FRIENDS

CLOSELY WORKING WITH FBI / DEPT K FOR 3 YEAR. VERY CLOSE

SECURITY BLOGGER DISCLOSED DETAILS, CRIPPLING INVESTIGATIONS

ATTACKERS GO UNDERGROUND



ANTON KOROTCHENKO – ST PETERSBURG

4 OTHER GANG MEMBERS – 2 MILLION IN 2010

50/50 FAKE AV AND PAY PER CLICK

INTERESTING SMS SCRIPT ON C&C

```


<?
    $phones = array(
    // phone => array(Sun, Mon, ..., Sat)
    //
    // +7911 => array('1100', '1000', '1000', '1000', '1000', '1000', '1100'),
    // +7921 => array('1200', '1200', '1200', '1200', '1200', '1200', '1200'),
    // +7921 => array('1000', '0900', '0900', '0900', '0900', '0900', '1000'),
    // +7921 => array('1300', '0930', '0930', '0930', '0930', '0930', '1300'),
    // +7911 => array('1100', '1000', '1000', '1000', '1000', '1000', '1100')
    );

    $hm = date("Hi");
    $day_of_week = date("w");

    $phones_to_send = array();
    foreach ($phones as $phone => $times) {
        if ($times[$day_of_week] == $hm) {
            $phones_to_send[] = $phone;
        }
    }
}

```

2010-05-28	\$2806.48
2010-05-27	\$3070.46
2010-05-26	\$3121.47
2010-05-25	\$3743.42
2010-05-24	\$6335.55
2010-05-23	\$5944.21
2010-05-22	\$7451.72
Total for 7 days	\$32473.31



AVERAGE 5K / 20K MAX

TIME OF DATY GETS LATER

HARD TO TELL IF 1 TRILLION, BUT ENOURMOUS SUMS INVOLVED

CYBERCRIME MORE THAN STEALING DATA – OTHER MOTIVATIONS.

MIKKO – TED – 3 CATEGORIES

DON'T ENTIRELY AGREE



IN IT FOR MONEY / HACKTIVISTS (ANONYMOUS) / NATION STATES

NEXT YEAR OR TWO – THIS WILL SPLIT

THOSE WHO COMPROMISE LOTS – SMALL MONEY FROM EACH – SPAM

SECOND GOLDEN AGE OF HACKING – RISE OF SKILLED HACKERS

UNLIKE 90S IN IT FOR MONEY. WILL SELL TARGETED FOR 5-6 FIGURES

HAVE LOOKED AT FIRST ONE, LETS LOOK AT TARGETED ATTACKERS



APT

NOWADAYS EVERYTHING YOU READ ABOUT IS APT

PERSONALLY HATE THE PHRASE

ANYONE KNOW WHERE IT COMES FROM? MILITARY PHRASE

PROBLEM – SOME TARGETTED ATTACKS ARE NOT VERY ADVANCED AND THEY DO NO HANG AROUND VERY LONG (SMASH AND GRAB)

TARGETED ATTACK

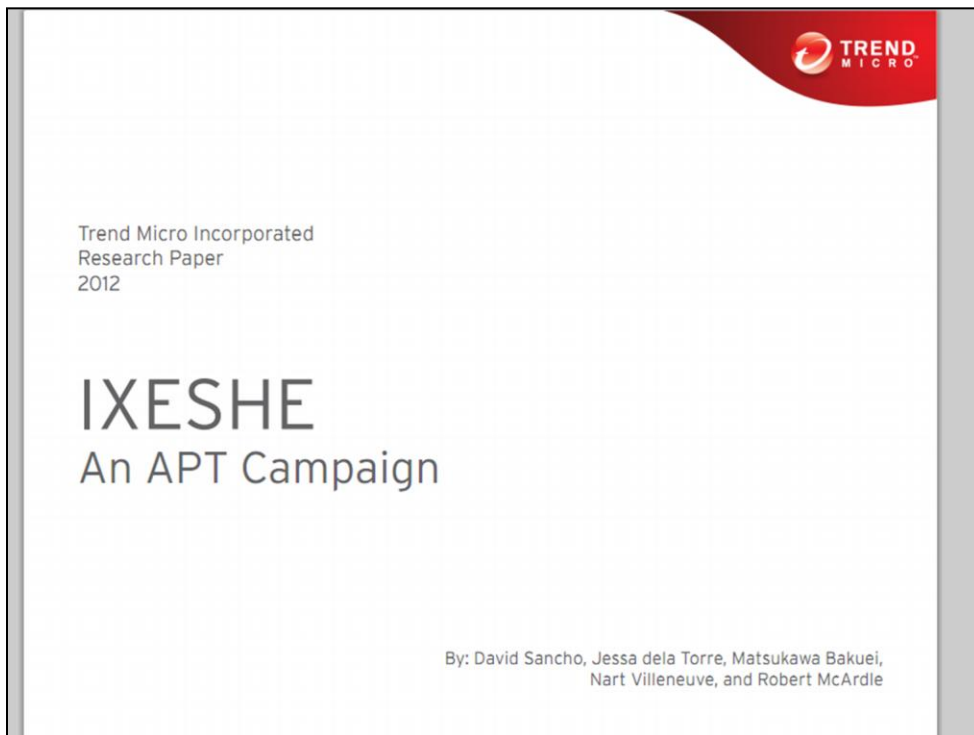
SO I PREFER THE PHRASE TARGETED ATTACK

SOMETIMES WE TALK ABOUT NATION SPONSORED ATTACK, SOMETIME MERCENARY FOR HIRE.

SOME COUNTRIES APPEAR TO USE CYBER ARMIES, OTHERS USE LOCAL HACKING GROUPS

METHODS DIFFER – SOME USE VERY COMPLEX RAT TROJANS – OTHERS NETCAT AND A COMMAND LINE

ONE THING IN COMMON – HIGHLY MOTIVATED ATTACKER – WITH A VERY SPECIFIC TARGET.

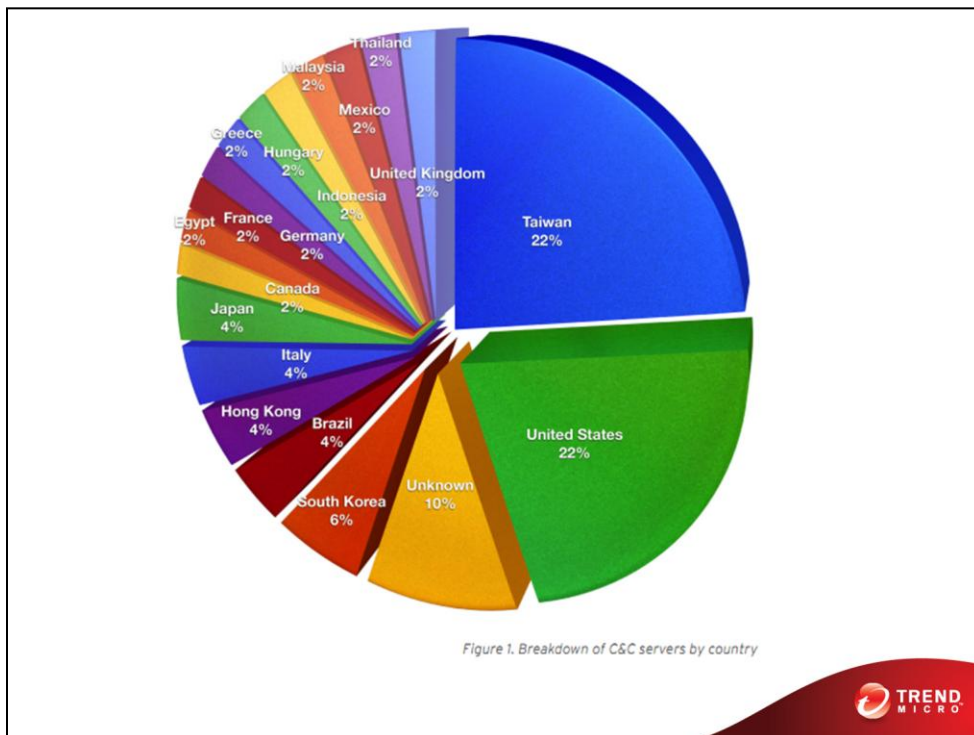


EXAMPLE IXESHE – PRONOUNCED I-SUSHI

TARGETED CAMPAIGN WITH TWO CORE TARGETS – ASIAN GOVERNMENTS (TWO IN PARTICULAR), AND ELECTRONICS COMPANIES

AIM TO STEAL DATA – NOT MONEY

TECHNICALLY – NOT TERRIBLY COMPLEX, RELATIVE SIMPLE ENCRYPTION



C&C SERVERS INTERESTING – VERY WIDESPREAD

SOME INTERESTING APPROACHES ALL TO AVOID DETECTION

C&C ALWAYS PLACE ON COMPROMISED MACHINES – INCLUDING IN THE VICTIMS NETWORK

C&C DOMAINS ALWAYS VIA DYNAMIC DNS PROVIDERS AND USING ANONYMIZER SERVICES – VERY HARD TO TRACE

ACTUALLY ALL PROXIES USING HTRAN – THEY MADE ONE MISTAKE ONCE WHICH LET US FIND REAL C&C

ATTRIBUTION – CODE INDICATES CHINA OR ENGLISH (VERY GOOD COMMAND OF LANGUAGE)



NOW THAT WE HAVE COVERED FINANCIALLY MOTIVATED CRIME – LETS
MOVE ONTO HACKTIVISTS



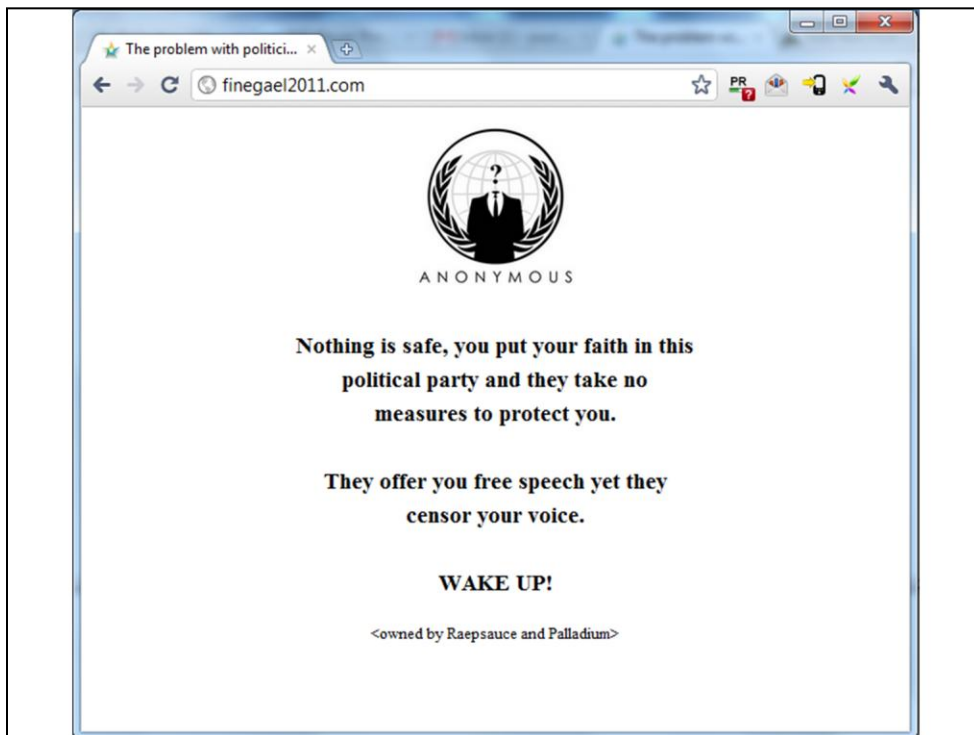
NOT MOTIVATED BY MONEY – POLITICAL REASONS

ANONYMOUS – LOOSE COLLECTION HACKERS, ACTIVISTS, GENERAL INTERNET USERS

ANTI GOVERNMENT

IMPORTANT - NOT IN IT FOR THE MONEY

TWO MAIN STYLES OF ATTACKS THEY FAVOUR

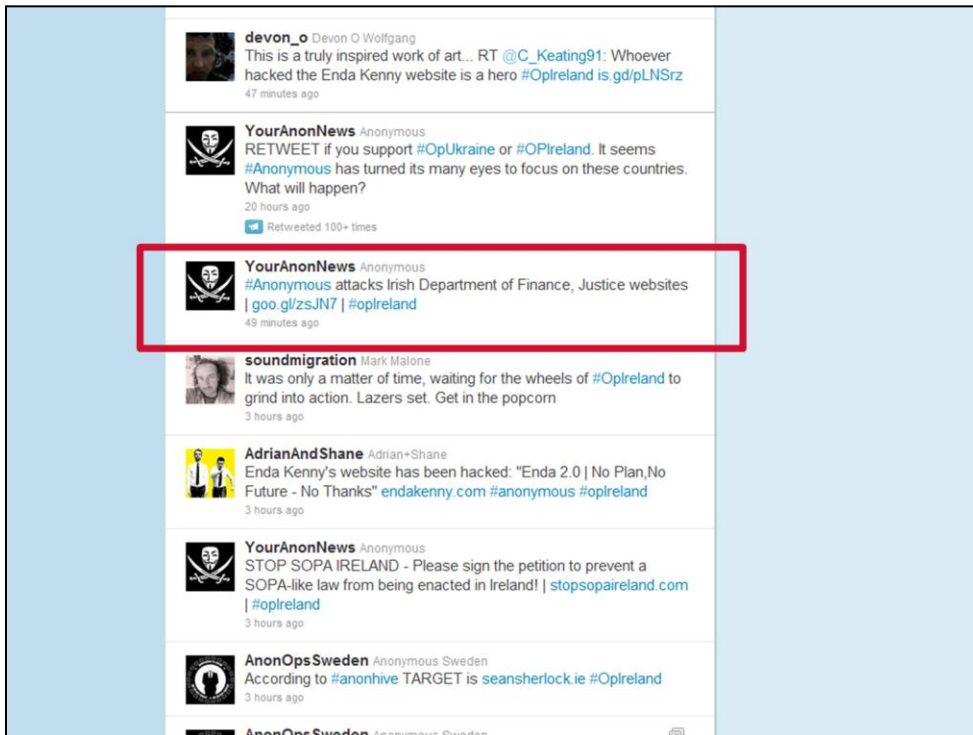


DEFACE POLITICAL SITES – OR COMPANY THEY DISLIKE

SEPT – 2 IRISH MEMBERS OF ANONYMOUS HACK FINE GAEL – ANTI-POLITICAL MESSAGE

BOTH ARRESTED – LULZSEC

ANONYMOUS ALSO DEFACED OTHER GOV, EMBASSYS, SUN, COMPANIES

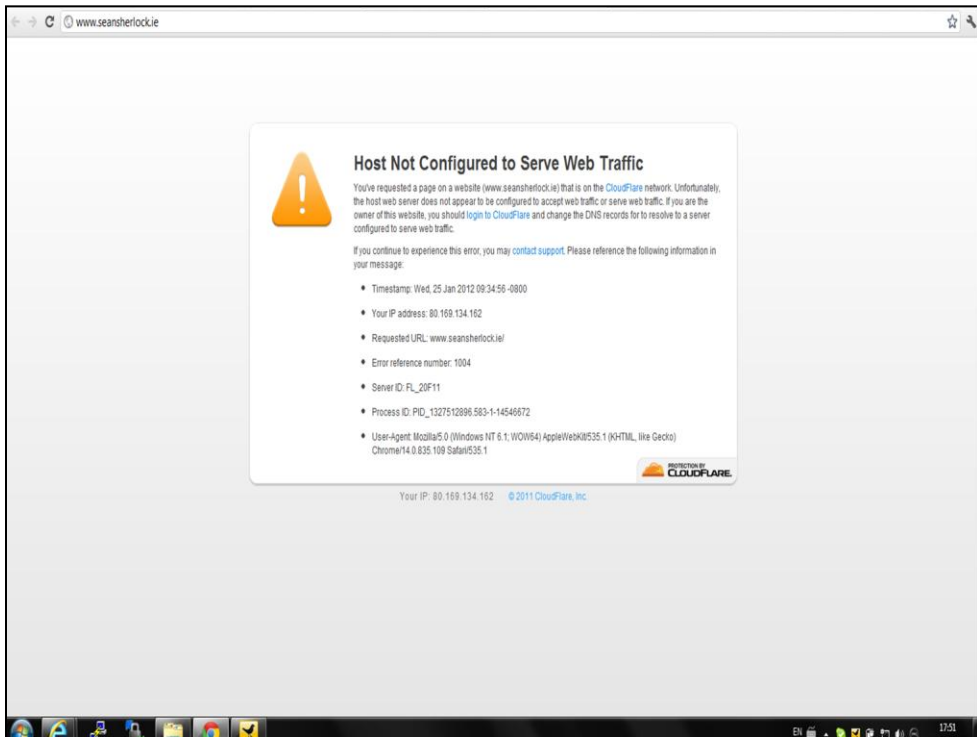


OTHER POPULAR – DDOS – FLOODING A SITE

LAST WEEK ANONYMOUS TARGETED OPIRELAND –

PROTESTING ANTI-COPYRIGHT INFRINGEMENT BILL – SEAN SHERLOCK

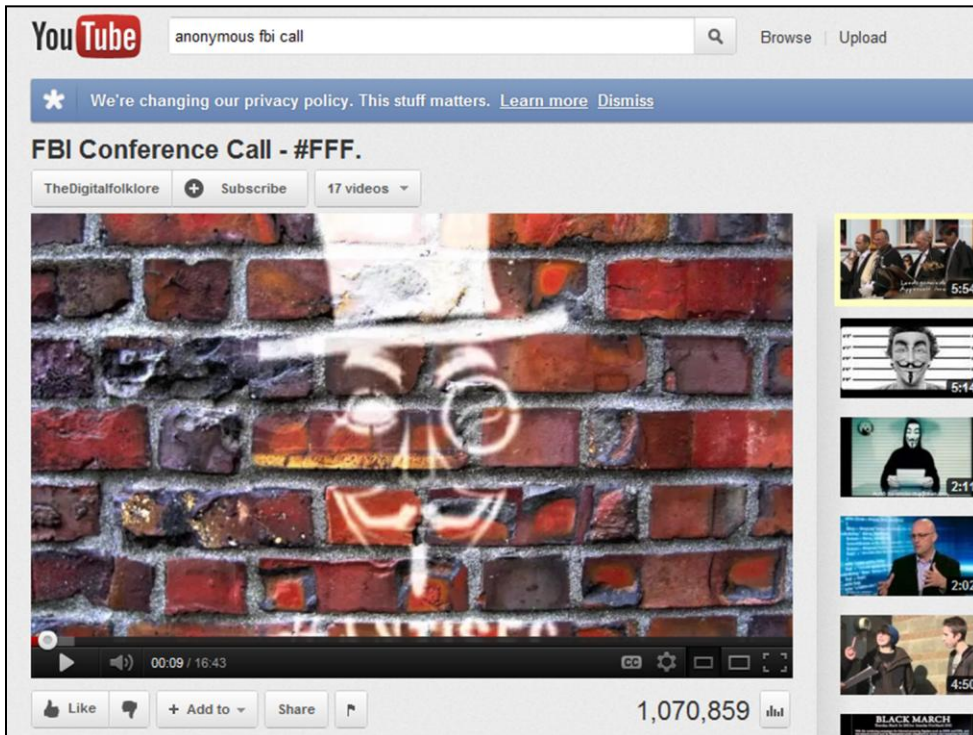
SWEDEN / BRAZIL - ATTACKED JUSTICE AND FINANCE. SOME SUCCESS



SHERLOCKS SITE DOWN FOR DAYS

ALSO REVEALED 20 DFA MEMBERS ON PASTEBIN

PUBLICALLY TO THE WORLD



ANOTHER GROUP ON TARGET LIST – LE

FEW WEEKS AGO – HIGHEST PROFILE YET

FBI PERSONAL EMAIL – ABLE TO JOIN A CALL

FBI / SCOTLAND YARD / OTHERS (IRELAND)

ACTUALLY DISCUSSING ANON – INCLUDING IRISH GUYS

RECORDED – YOUTUBE – 1 MILLION VIEWS



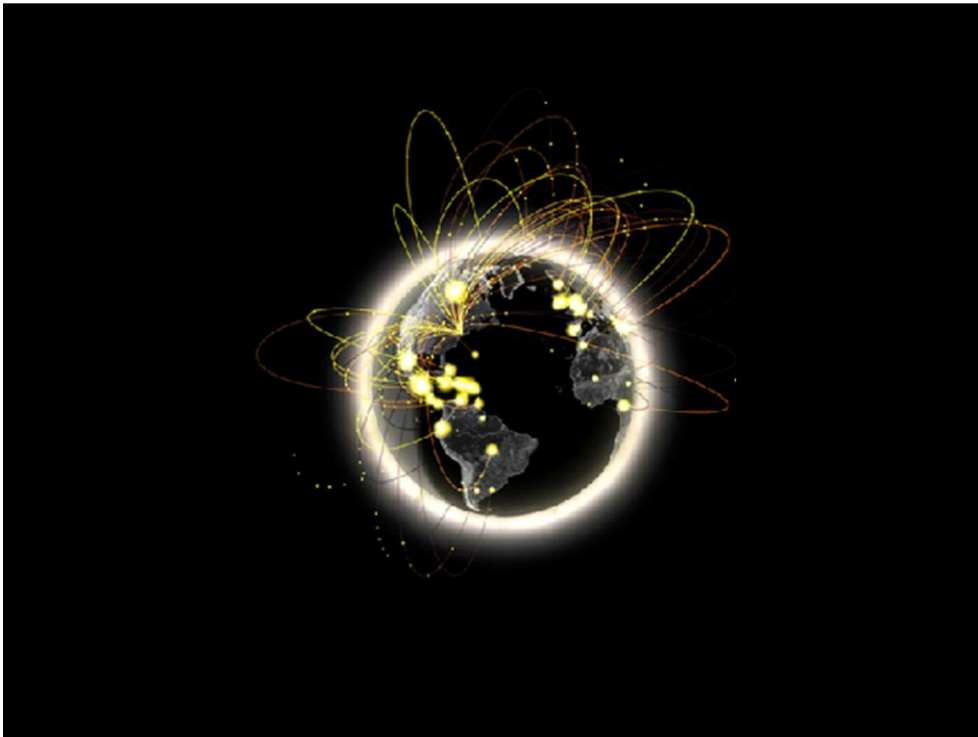
NOT JUST ANONYMOUS

DECEMBER – ANTI-PUTIN TRIUMPHAL SQUARE – ELECTION

USING TWITTER HASHTAG – PRO-PUTIN BOTS TO FLOOD

THESE ATTACKS SIMPLY POLITICAL PROTEST IN INTERNET WORLD

NOT ALL BAD – RAISED AWARENESS . PREFER PUBLIC HACK THAN SILENT HACK



DISCUSSED CYBERCRIMINAL / HACKTIVISTS – NOT NATION STATES

SPYING ON EACH OTHER SINCE DAWN OF TIME – NO CHANGE.

IN FACT INCREASED - EXAMPLES



What does the Stuxnet malware do?

WHAT DOES IT DO

WORM INFECTS SIEMENS S7-300

ONLY IF 984

WHAT DO THEY DO? WHERE?



984 FIND THEM IN NATANZ

CENTRIFUGE – URANIUM TO WEAPONS GRADE

STUXNET DESIGNED TO DESTROY THIS

NOT FIRST CYBERWEAPON – LOTS OF PRESS. MOST LIKELY US / ISRAEL
– NEEDED MACHINES TO TEST

MOST NATIONS HAVE ARMY – CHINA THOUSANDS NAVY

CYBERWAR – HARD TO DEFEND AGAINST. TAKE IRELAND – ESB, GOV,
HEALTH

BUT ALSO NON – GOV – EIRCOM, VODAFONE, TESCO , GUINNESS
(ECONOMY / EXPORTS)

BBC Mobile News | Social | Weather | Travel | TV

NEWS

Home UK Africa

US Election 2012

1 June 2011 Last updated

Google e
'Chinese

Hackers persona
top US o
journalist

The US c
password
monitorin

Chir
Get

By Michael

Tweet

Nov. 19, 2011 (11:05 am) By: *Matthew Humphries*

Chinese hackers took control of NASA satellite for 11 minutes



Landsat-7 and Terra EOS satellites

Hackers From China Accessed U.S. Chamber Network, Journal Says

December 21, 2011, 3:38 AM EST

E-mail Print

ks | china | government

**ig US
largest**

Innovation

UNLESS YOU RUN NUCLEAR / ESB – NOT BIG DEAL.

NOT IMMUNE!

CHINA HACKING EVERYTHING NOT NAILED DOWN – NOT ALONE

MAKES SENSE – CAN MANUFACTURE, NEED IDEAS

EASIER TO STEAL FERRARI PLANS

CHINA GOING TO GET BLAME ANYHOW – WHY BOTHER HIDE



NATIONS NOT JUST HACKING EACH OTHER – ALSO CITIZENS

LAST YEAR DIGINTOR – DUTCH CERT BODY.

WINDOWS HAS THE ROOT.

COULD ISSUE CERT FOR ANY SITE

BEFORE MOST DUTCH , THEN +90% IRAN

NEEDED ABILITY TO INTERCEPT

NOT JUST IRAN – GERMANY AND OTHERS



SO THREE CLASSES OF ATTACKERS – MONEY, HACKTIVISTS, NATION STATES

CYBERCRIME DOES NOT STAY STILL – WILL EVOLVE OVER NEXT YEAR



WHAT DOES 2012 AND 2013 HOLD – HERE IS WHAT I SEE



MAC MACWARE ON RISE – WILL CONTINUE

WHO HAS A MAC IN COMPANY – CTO – PEOPLE WITH THE SECRETS
ATTACKERS WANT.

SECURITY SOFTWARE NOT AS MATURE – SOME PEOPLE DO NOT EVEN
THINK THEY CAN BE INFECTED.

WILL RISE IN 2012 – BUT TARGETED NOT WIDESPREAD



MOBILE – APPLE / GOOGLE BATTLING IT OUT.

MORE TIME SPENT ON THESE OVER DESKTOPS – ATTACKERS KNOW THIS

HAVE ALREADY DISCUSSED IN DEPTH – SOME NEW ATTACKS. SOME TRADITIONAL ONES DO NOT WORK

PICTURE 10000 – BATTERY TOO WEAK FOR DDOS / SPAM – SAME INFO CAN BE STOLEN FROM LAPTOP

WILL BE TARGETED – FLEXISPY

ALSO NFC – JAPAN – CAN STEAL STRAIGHT FROM YOUR POCKET



LASTLY HTML5 – NEXT STANDARD FOR THE WEB

GIVES AWESOME STUFF

-BETTER AUDIO / VIDEO

-GEOLOCATION

-DRAG AND DROP

GOING TO MAKE THE WEB FANTASTIC – BUT ALSO SOME DANGEROUS SIDES



LAST YEAR PAPER SHOWING HTML5 CAN BE USED TO CREATE BOTNET IN BROWSER. DEMOED POC IN DUBLIN , AGAIN IN LIMERICK.

CAN DDOS, SPAM, GEOLOCATION, SOCIAL ENG

THINK FOR A SECOND – ATTACKERS CODE – EVERY OS, EVERY DEVICE, EVERY LANGUAGE

BIGGEST IMPACT IN CYBERCRIME FOR SOME TIME

[DEMO THIS HERE]



FURTHER OUT TECHNOLOGIES TO KEEP AN EYE ON IN 2013

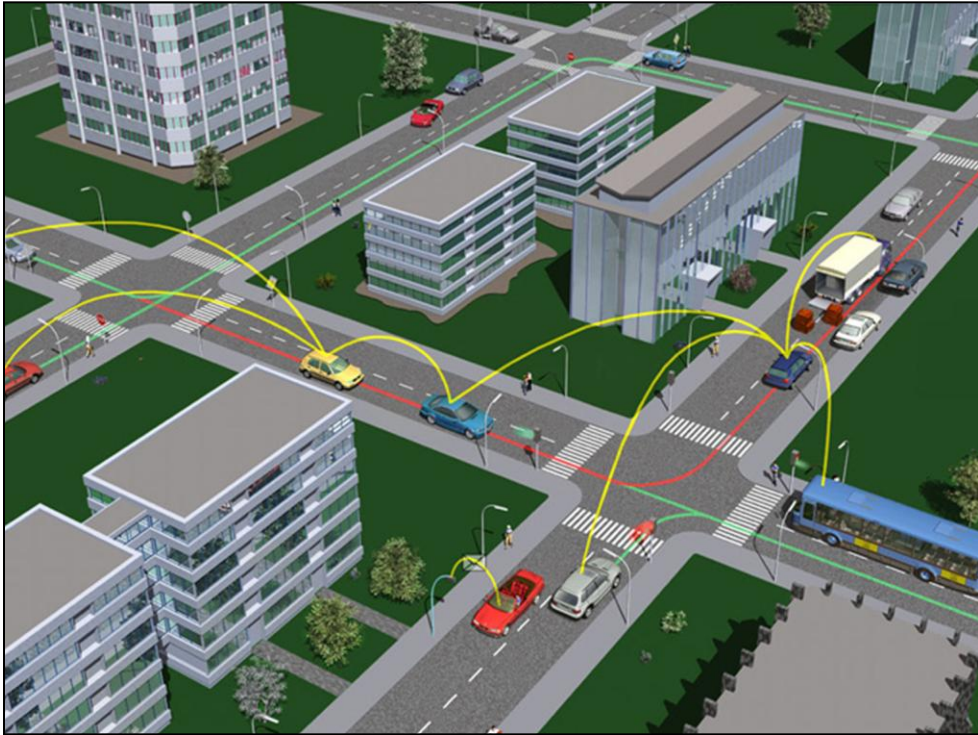
ANYONE KNOW WHAT THIS IS?

GOOGLE GLASS – ANDROID POWERED AUGMENTED REALITY

HAS THE POTENTIAL TO SINGLE HANDEDLY CHANGE HOW WE
INTERACT WITH THE WEB

OR MAYBE ONLY FOR GEEKS

WHAT HAPPENS WHEN I CAN HACK WHAT YOU CAN SEE?



ANOTHER AREA TO LOOK AT – VEHICLE COMMUNICATIONS SYSTEM AKA CAR-TO-CAR COMMUNICATION

GERMAN MANUFACTURERS IN PARTICULAR

CARS-TO-CARS

CARS-TO-X E.G. TRAFFIC, INSURANCE DRIVING FIGURES

POTENTIAL HACKS – TRACK CARS, ALTER TRAFFIC

ONE RESEARCH WE DID – KERNEL ACCESS TO THE ENGINE VIA THE ENTERTAINMENT SYSTEM!!



LETS FINISH WITH A MAGAZINE ARTICLE FROM 1981, ON THE FUTURE OF COMPUTERS

WE CAN NEVER 100% PREDICT THE FUTURE, OTHERWISE WE COULD ALL RETIRE ALREADY 😊

BUT IT IS CLEAR WE HAVE SOME VERY BUSY AND INTERESTING YEARS AHEAD OF US!

THANK YOU