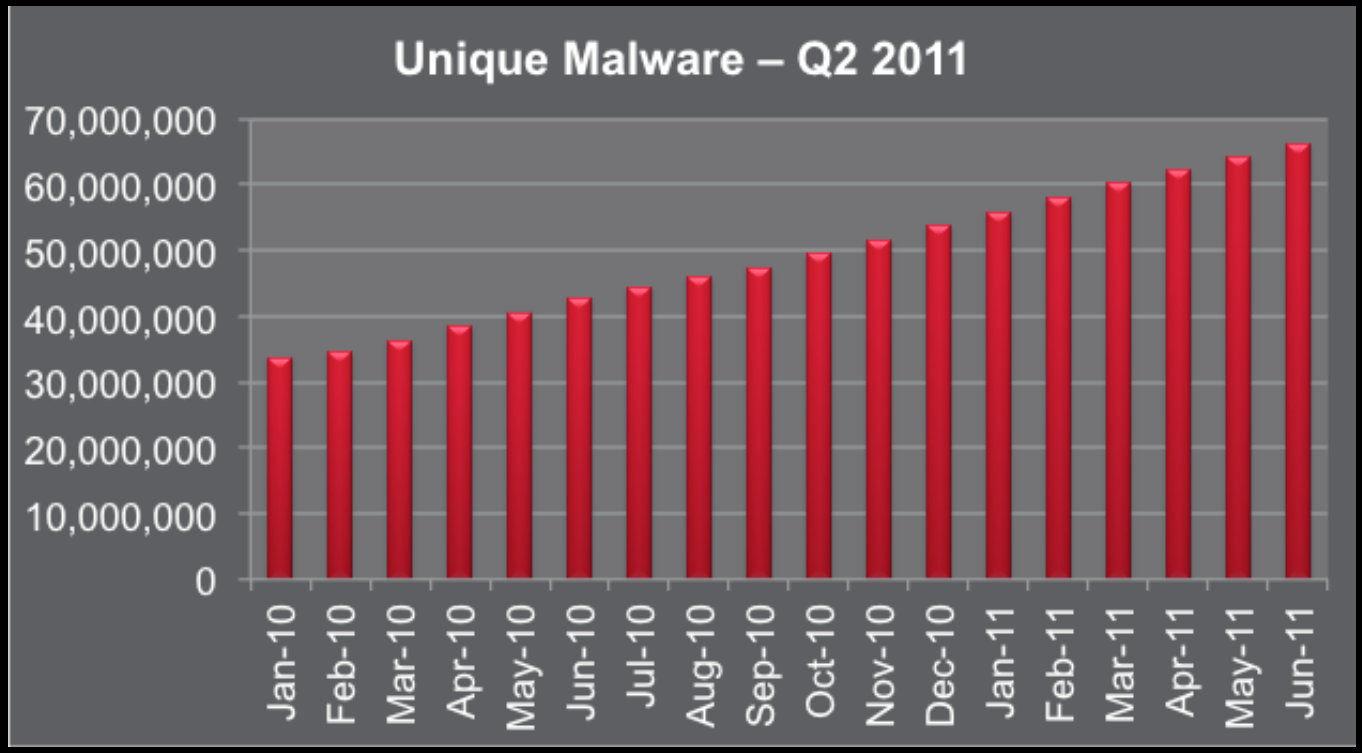

McAfee
An Intel Company
Threat Trends in 2011
The Signals and the Noise
Jim Walter, McAfee Labs
Manager – McAfee Threat Intelligence Services
November 22, 2011
SAFE NEVER SLEEPS.

Key Focus Points

- Malware continues to grow exponentially (given)
  - Mobile Malware Boom (Android)
  - Rogue Security and sys utils on OS X
  - Kits and Crimeware
- Client application target growth
  - Adobe vs. MS
  - ICS / Embedded / Financial, Medical, and more
- The Rise and Plateau of Hacktivism. . . For now. . .
  - What does it all mean?
  - What matters?
  - Who is benefitting?
  - Intra-group attacks

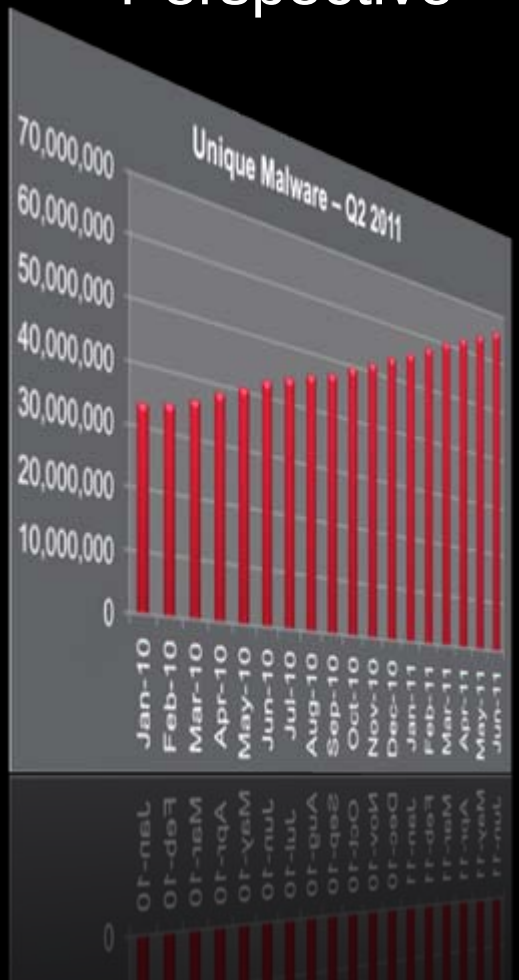
Key Focus Points

- Malware continues to grow exponentially (given)



Malware Trends

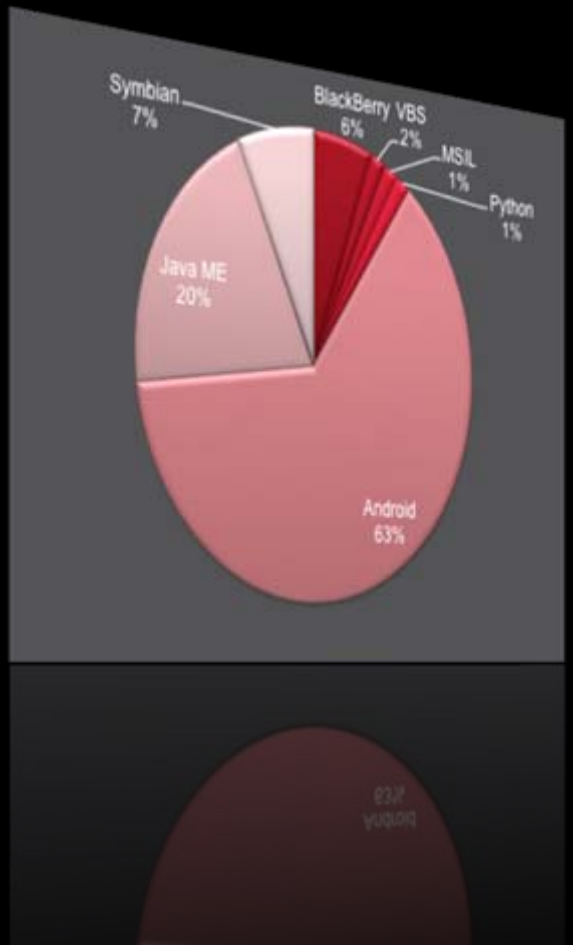
- Malware continues to grow exponentially
  - Perspective



- From Q1 ‘10 onward and average of 2.5 million new, unique samples per month
- Rootkits/stealth malware - ~60k per month.
- Static families are still king (Trojans, non-self replicating or file-infecting). Includes FakeAlerts, PWS, BD, Autoruns, etc.
- PWS and Autorun between 200k and 400k per month.
- Global Botnet-related infections steadily recovering from previous ‘blows’ (Rustock and Bredolab, Waledac, Kelihos takedowns)

Malware Trends

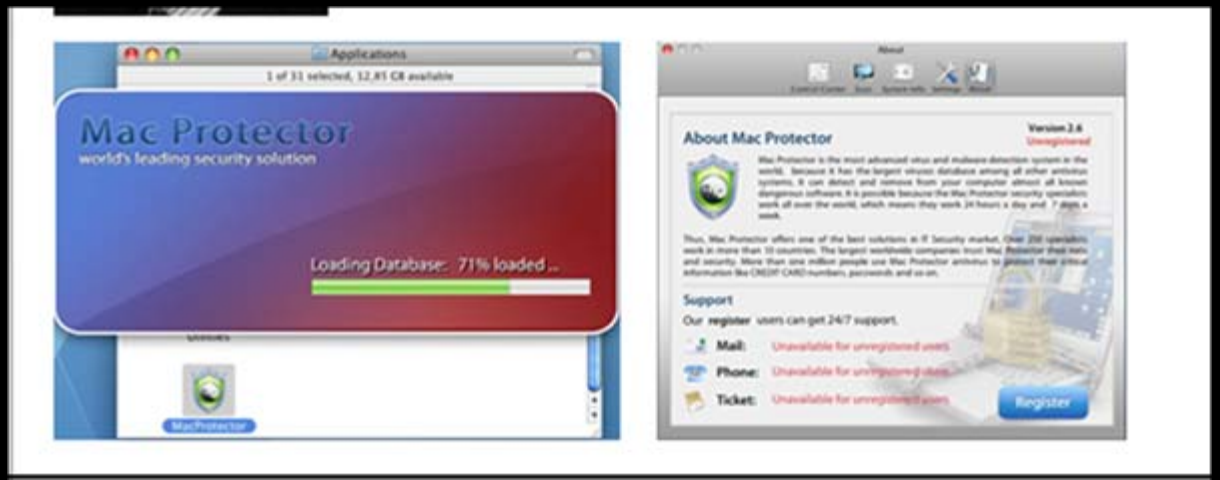
- Malware continues to grow exponentially
  - Mobile



- Currently seeing 1.2 – 1.4k unique per month
- Android threats account for 63% of all mobile platforms.
  - Including much older and seasoned platforms.
- Biggest iOS (Apple) issue is device and software vulnerabilities (and exploits thereof), as opposed to live, in-the-wild malware
- Malicious mods of popular released apps is the primary delivery method
  - Android/Jmsonez.A
  - Android/ Smsmecap.A
  - Android/DroidKungFu

Malware Trends

- Malware continues to grow exponentially
  - New platforms for rogue security / util products



Families
- MacDefender
- FlashFake
- iMunizator
- MacSweeper
  - etc. etc. etc.

Malware Trends

- Crimeware – Kits and Prevalence

```
ReadFile
SpyEye.exe
SpyEye v1.2.99 Patch
Process not loaded, please add SpyEye.exe on the sam
CRC32 not match
3,2,1 ready  ? gogogo: Mart!k, b1sh0p try to rip thi
spyeye.exe
Error writing to target process
Process not loaded, please add SpyEye.exe on the sam
SpyEye Builder v
%s.%s.%s    [ Xyl
```

BLEEDINGLIFE 3.0 STATISTICS SETTINGS BLACKLIST SCAN PAYLOAD GENERATE IFRAME

SECURITY SETTINGS

Admin Username:

*Username to your Admin Account.

Admin Password:

*Password to your Admin Account.

SAVE SETTINGS

Guest Username:

*Username to your Guest Account.

Guest Password:

*Password to your Guest Account.

SAVE SETTINGS

SCAN4YOU ACCOUNT

EXPLOIT SETTINGS

Enable Exploits:

- Adobe LibTiFF
- Adobe Util.printf
- Adobe Flash10o
- Java TC
- Java MIDI
- Java RMI
- Java Skylined
- MDAC
- Java Signed Applet
- Java Codebase Trust

Note: This exploit requires that your hosting account have a dedicated IP.

Select the exploits you would like to use.
Exploit attempts will only be made using selected items.

SAVE SETTINGS

Malware Trends

- Crimeware – Kits and Prevalence

- Notable in 2011 so far
  - Weyland-Yutani BOT Version 1.0
    - (has OS X versions)
  - BlackHole 1.1 and higher (custom builds and patches)
  - BestPack
  - Phoenix 2.7 and higher
  - Eleonore 1.6.5+
  - Yes EK 4.0
  - Various Leaks
    - Full ZeuS and SpyEye builders and source
    - Incognito
    - BleedingLife 3

Clients / Targets

- Adobe far outnumbers MS for client / app exploitation.

- >16k exploit samples per/mo.
- Over 60 individual Adobe vulns targeted in 2011, and counting
- Adobe (and other) ‘hot’ exploits are being built into mass-produced malware and exploit kits every day.

Clients & Targets

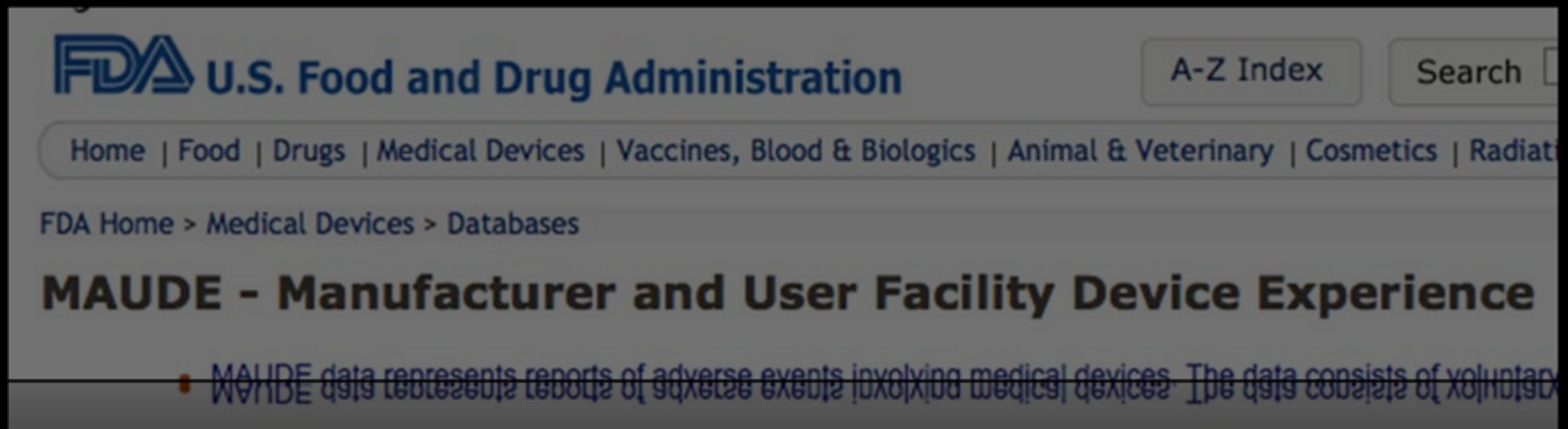
- ICS, Embedded*, SCADA
  - Stuxnet was interesting
  - Currently seeing ~10 new, confirmed, ICA or SCADA-related vulns per month. Nearly always accompanied by PoCs.
  - Very active ‘independent’ research community
    - Luigi Auriemma
    - Joel Langill (SCADAhacker)
    - Digital Bond
  - Time (last ~5 years) has brought more visibility and more knowledge.

Clients & Targets

- Other targeted systems and industries of interest
  - Public Utilities
  - Location-specific / Targeted PLC systems
    - Prison automation systems (fencing, door controls)
  - Device or human tracking systems
  - Energy / Utility control and monitoring
  - Financial / Trading systems
  - Traffic Control (from central intelligence to signal control)

Clients & Targets

- Medical !!!
  - Externally / remotely manageable implanted devices
  - Pacemakers
  - Implantable Defibrillators
  - Software flaws – usual issues, self-update flaws, firmware issues, human error resulting in flawed usability,
  - Device transmission interception



Clients & Targets

- MAUDE DB Examples

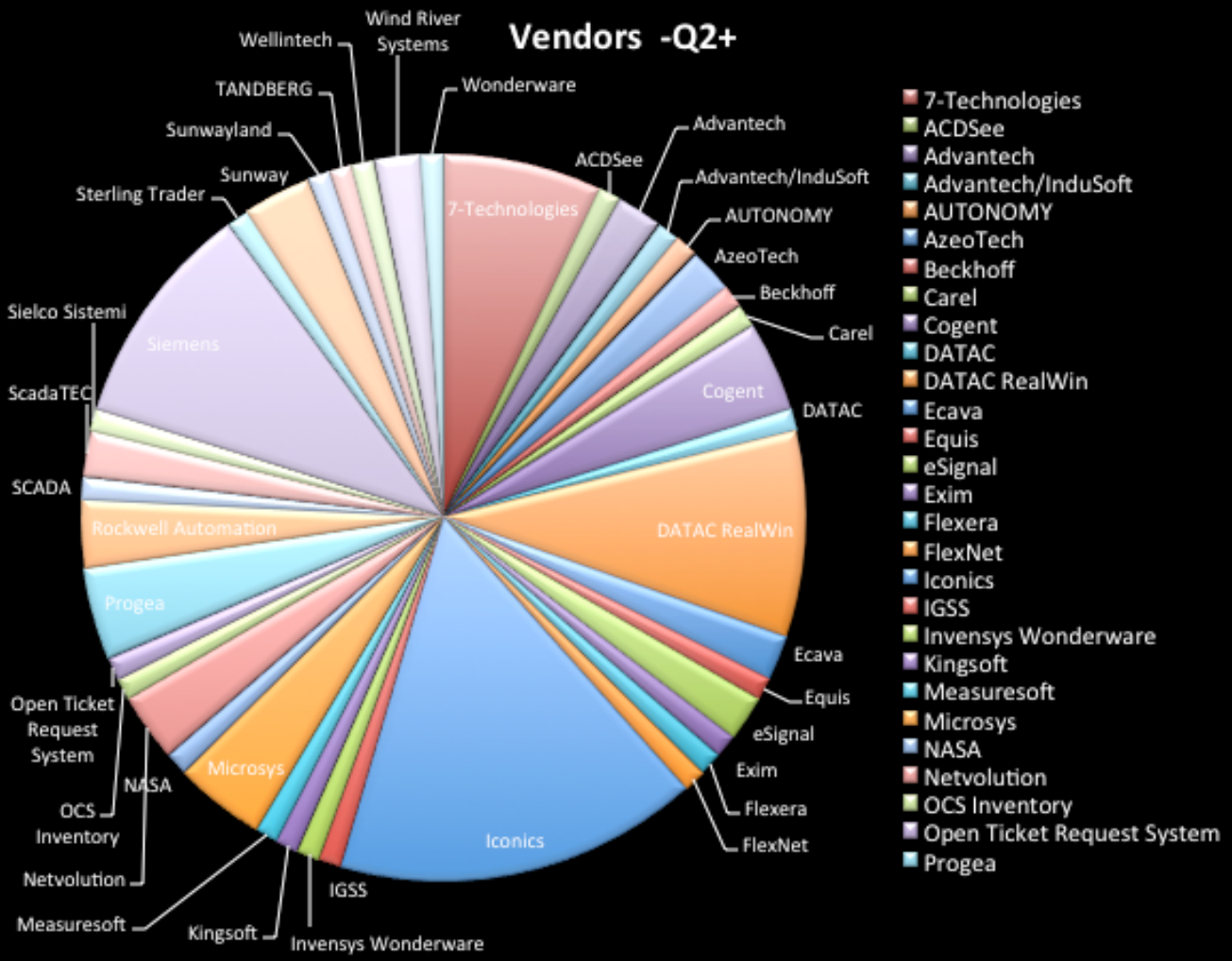
5 records meeting your search criteria returned - **Product Problem:** *Malfunction* **Event Type:** *Death* **Report D**

New Search

Manufacturer	Brand Name
THORATEC CORP.	HEARTMATE II
MEDTRONIC CRYOCATH L	MEDTRONIC ARCTIC FRO
COOK, INC.	COOK AIRWAY EXCHANGE
ST. JUDE MED, INC.	ST. JUDE MECHANICAL
MOOG MEDICAL DEVICE	CURLIN 4000CMS

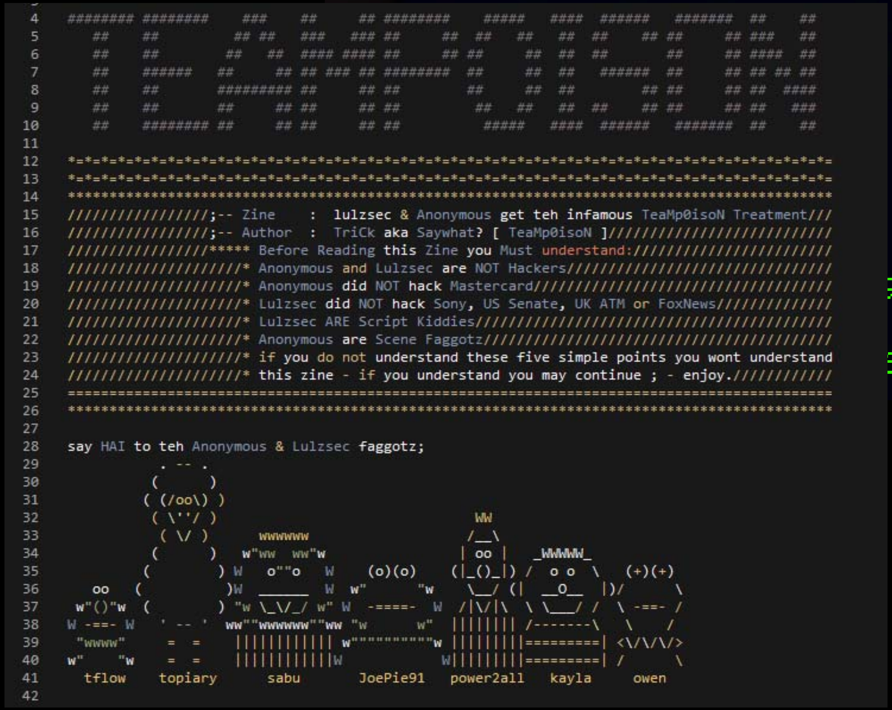
Clients & Targets

- Giant ICS/PLC/SCADA/Vertical-specific Pie



Hacktivism

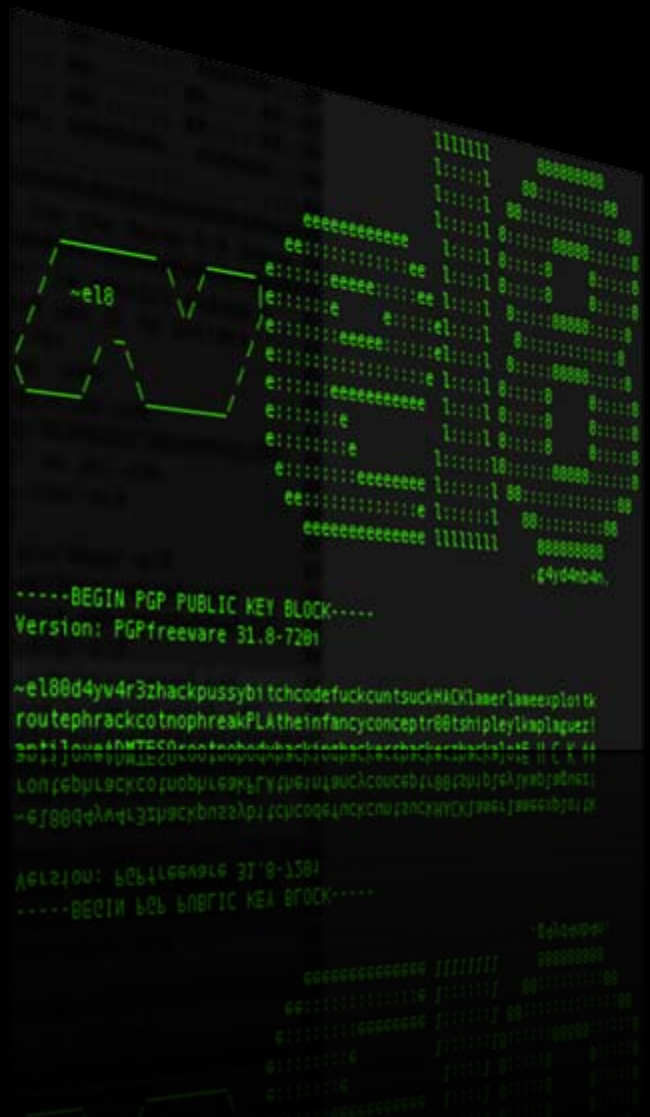

Twitter: @CabinCr3w
954 in the Bronx)


////////////////;-- Zine : lulzsec & Anonymous get teh infamous TeaMp0isoN Treatment///
////////////////;-- Author : TriCk aka Saywhat? [TeaMp0isoN]////////////////////////
////////////////***** Before Reading this Zine you Must understand://///////////////////
////////////////////* Anonymous and Lulzsec are NOT Hackers///////////////////////////////
////////////////////* Anonymous did NOT hack Mastercard///////////////////////////////////
////////////////////* Lulzsec did NOT hack Sony, US Senate, UK ATM or FoxNews/////////////
////////////////////* Lulzsec ARE Script Kiddies///
////////////////////* Anonymous are Scene Faggotz///
////////////////////* if you do not understand these five simple points you wont understand
////////////////////* this zine - if you understand you may continue ; - enjoy.///////////
say HAI to teh Anonymous & Lulzsec faggotz;
tflow topiary sabu JoePie91 power2all kayla owen

Hacktivism

- “Hacktivism” as a concept is not new
- The “marketing” prowess of groups like Anonymous and LulzSec / AntiSec is significant
- All these groups have a relatively small, skilled, head. The body is a mass of varied skill, buying into the ‘marketing’ and ‘idea’ of identifying themselves with these groups
- 2010-2011: significant in particular to the rise and visibility of Anonymous, LulzSec, and the wider AntiSec movement. (The origins of Anonymous go back to 2002/2003 and *chan)

Hacktivism



- Some Goals and Ideals
  - Cyberspace-specific, open consciousness and culture
  - Expose and end Government and Corporate greed and corruption.
  - Disruption of operations and business for those identified as hostile, inhumane and unfair
  - Mass exposure for new ideas
  - Mobilization of the masses – creating and fostering an environment of activism (cyber and ‘real’).

Hacktivism

Operation Facebook

Operations Payback,

Arab Spring Activities

Operation Malaysia

Attack on HBGary Federal

Operation CashBack

Anon-Ware

Operation Didgeridie

Operation Anti-Security

Oregon Tea Party raid

2011 Bank of America document release

Opposition to Los Zetas

Operation BART

Operation Titstorm

Operation Bradical

Indian Anti-corruption

2011 Wisconsin protests

Operation Avenge Assange

Operation Zimbabwe

Operation Orlando

Operation Payback III

Occupy Wall Street

Operation Attack on Fine Gael website

Operation Leakspin

Spanish Police Disclosure

Operation DarkNet

Operation Westboro Baptist Church

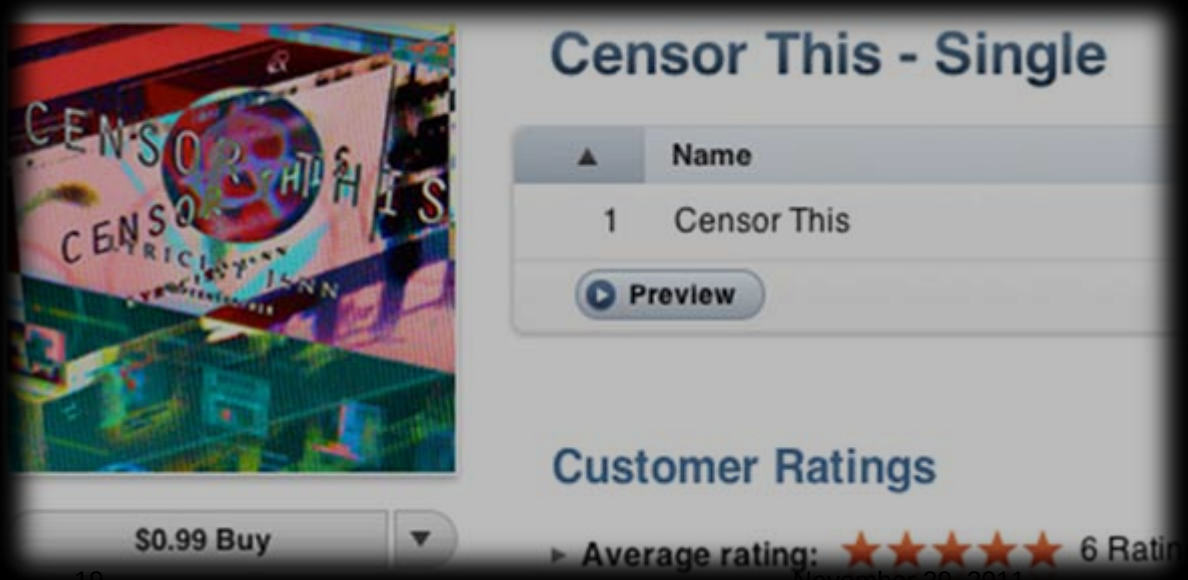
Operation Sony

Operation Intifada

Hacktivism

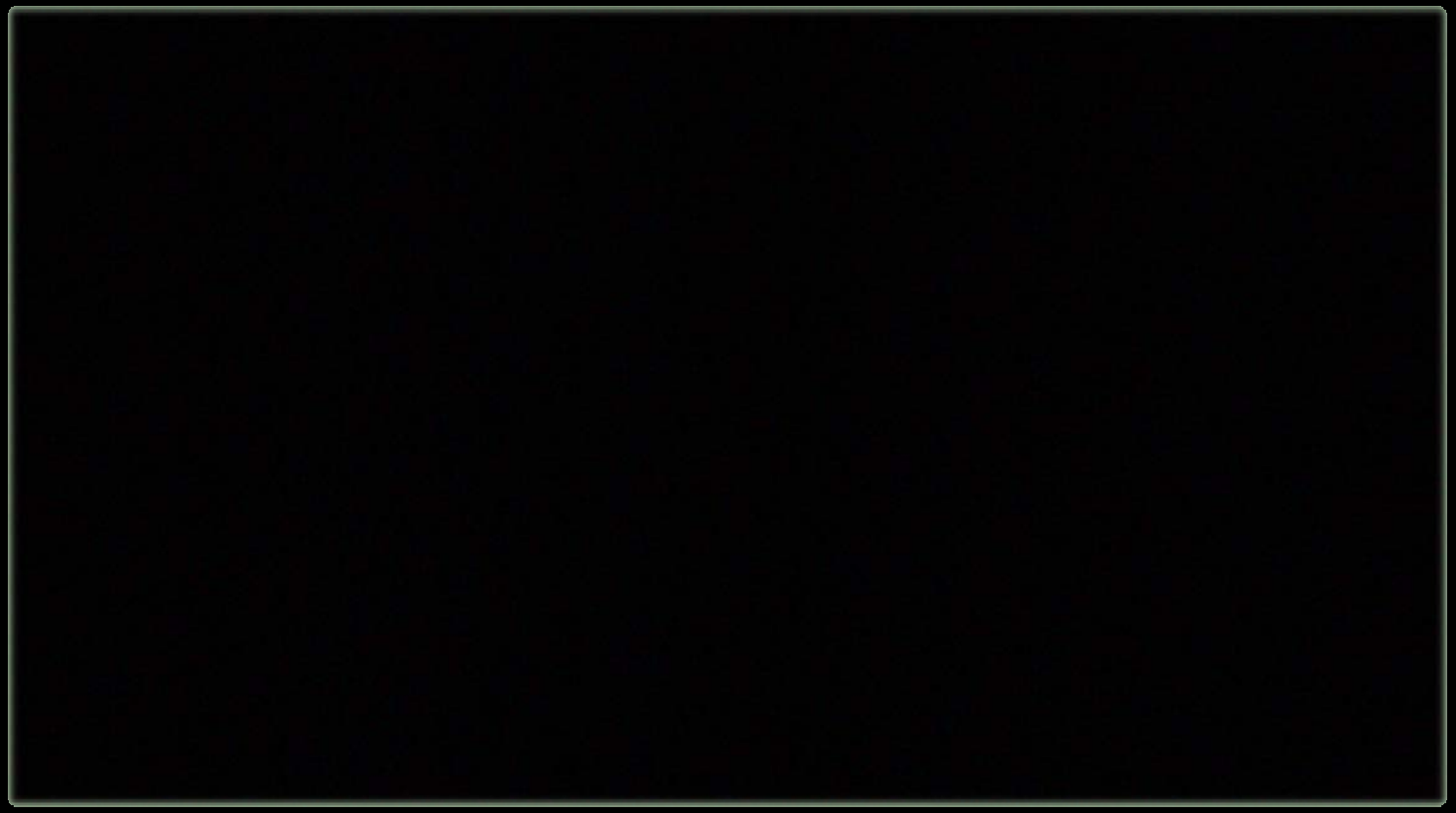
Loss of focus, loss of credibility

- #RefRef hype and failure (and more, OpFacebook, etc.)
- Infiltration of the 'inner-circle' by outside agencies
- Repeated dox'ing and exposure by other groups
- Attacks on Anon/Lulz/AntiSec sites and resources by other groups
- Forays into 'music' and other areas??
- Evolution from "Hacktivists" to plain "Activists"



Hacktivism

Anonymous and TeaMp0isoN !



Hacktivism

#RefRef Failure

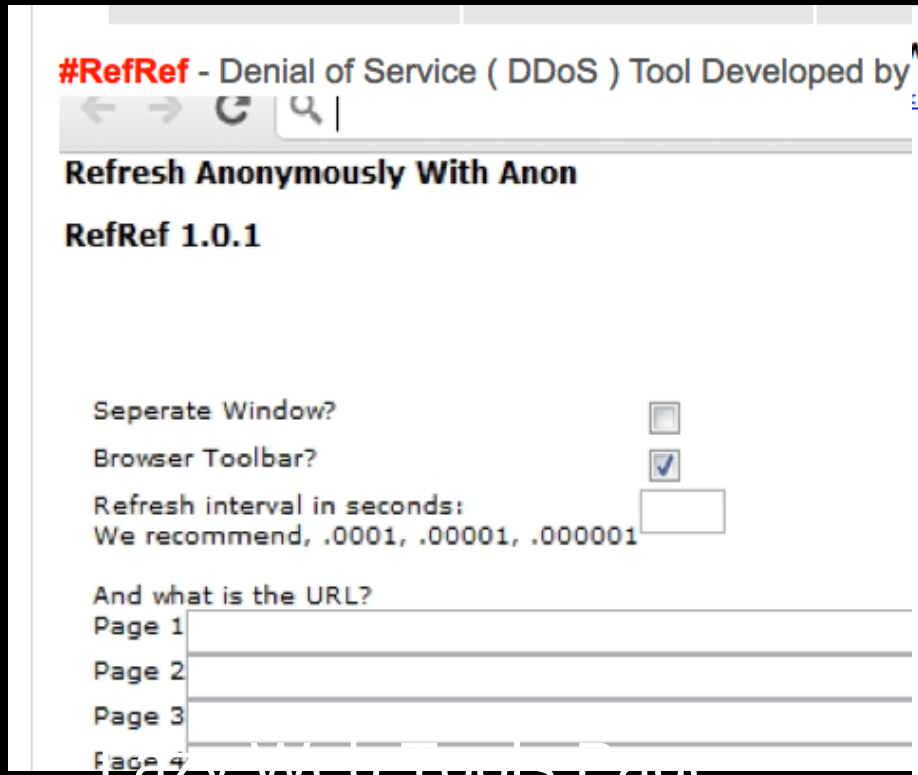
[14:13] <p0ke> On a serious note, I am now @AnonCMD
[14:13] <p0ke> wait.. wut
[14:13] <NOOKem> ^thefuck?
[14:13] <TheMiNd> blowfish go fuck yourself
[14:13] <kill9> when its not going to be released
[14:13] <%AnonCMD> I am the original anoncmd #refref bro
[14:13] <%AnonCMD> We are not releasing
[14:13] <fatjack> that was coiincidence
[14:13] <%AnonCMD> It never existed
03[14:13] * Joins: Wolfy (Howling@the.moon.tonight)
[14:13] <Wolfy> !up
03[14:13] * Lulzboat sets mode: +o Wolfy
[14:13] <fatjack> the ref is a lie

Back to top	
hack3r41	22 Sep : 05:23
	I have been hearing that RefRef is joke, meaning it is bullshit. If someone heard different let me know.
Back to top	

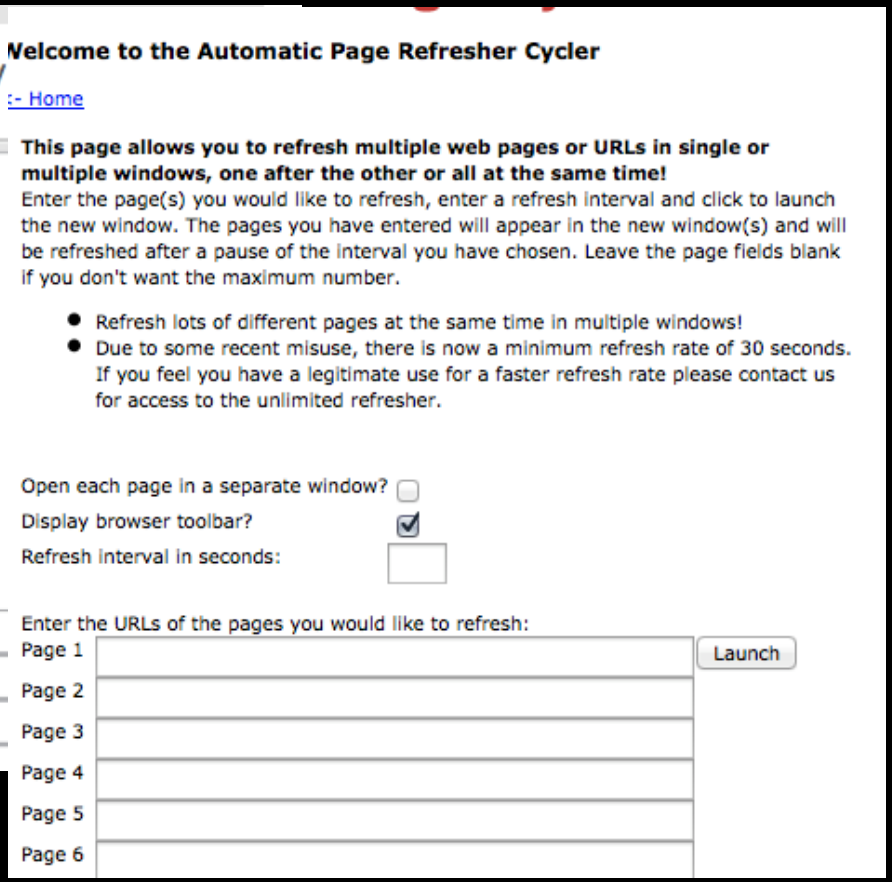
Hacktivism

#RefRef Failure

#RefRef Screenshot posted on THN – 7/30/11

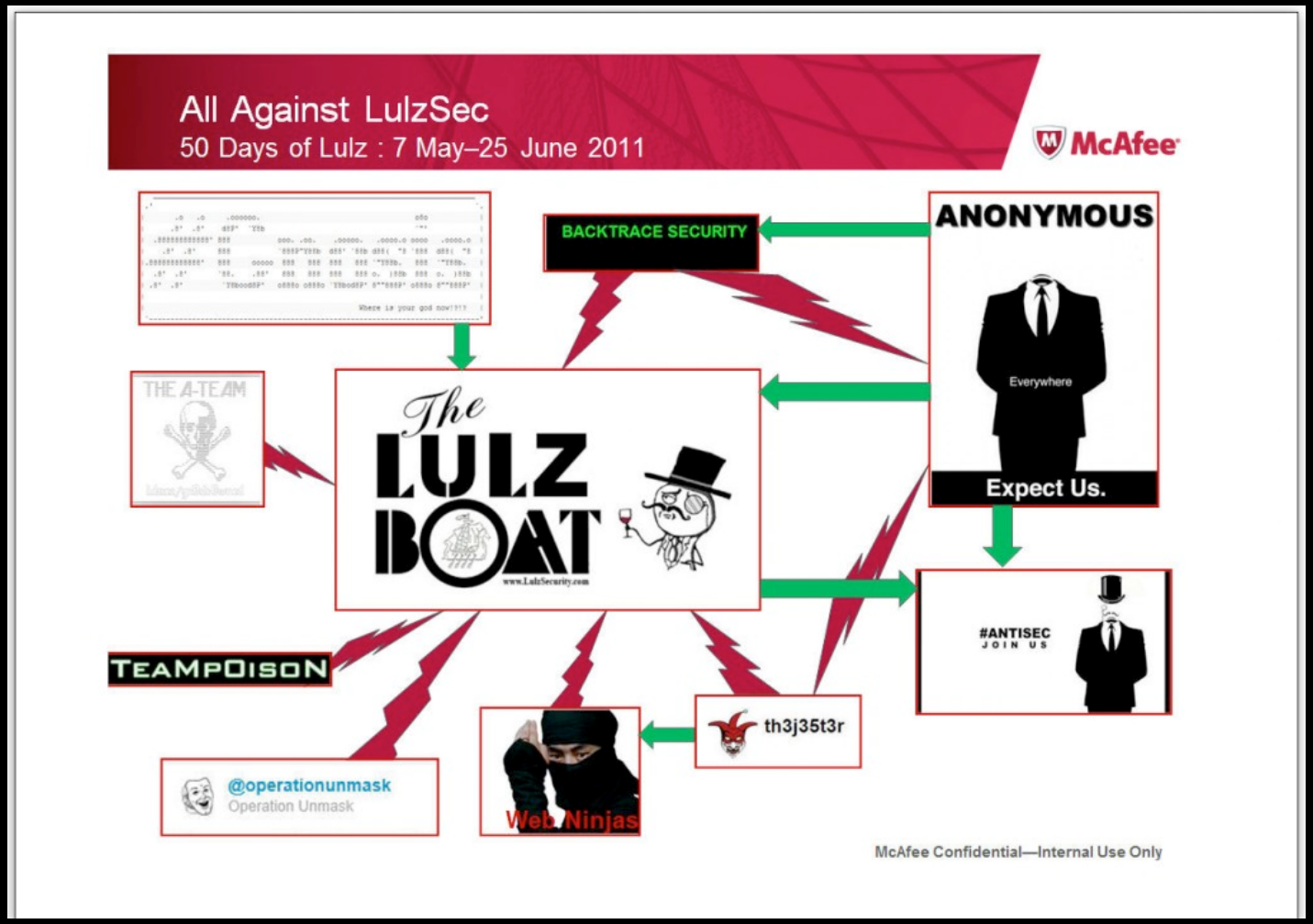


Lazy Web Tools Page Cycler – from 2008 !



Hacktivism

Targeting between groups



Hacktivism

Arrests, and other Legal actions

LulzSec/Anonymous: What are the police doing?

Visits, house searches, arrests…

These figures should be seen only as trends

COUNTRY	TOTAL	Younger than 18	18–28 years old	Older than 28	Unknown age
United States	97	5	16	7	69
Turkey	32	8			24
Italy	15	5	10		
United Kingdom	14	4	10		
Netherlands	6	1	1		4
Spain	3				3
France	1	1			

Nothing in Germany!

Two investigations policies: here (for example in USA) authorities track bots and activists, there (for example in France) they limit themselves to command servers and leaders.

In Turkey, it is just an interior action between the government and youth.


McAfee®
An Intel Company