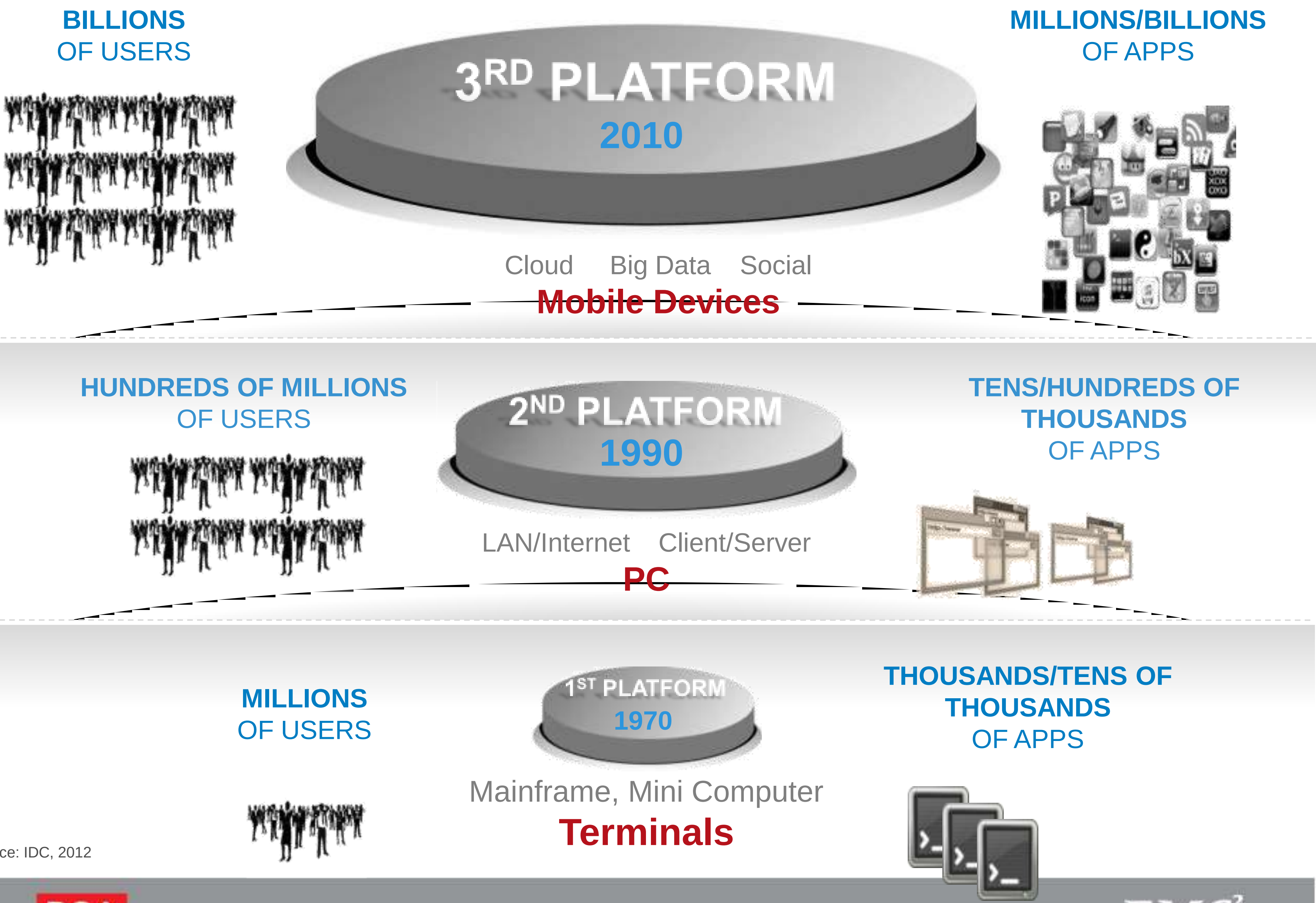
Security and Privacy

Matthew McCormack, CISSP, CSSLP

CTO, Global Public Sector, RSA
The Security Division of EMC



BILLIONS
OF USERS

3RD PLATFORM
2010

MILLIONS/BILLIONS
OF APPS

Cloud Big Data Social

Mobile Devices

HUNDREDS OF MILLIONS
OF USERS

2ND PLATFORM
1990

TENS/HUNDREDS OF
THOUSANDS
OF APPS

LAN/Internet Client/Server

PC

MILLIONS
OF USERS

1ST PLATFORM
1970

THOUSANDS/TENS OF
THOUSANDS
OF APPS

Mainframe, Mini Computer

Terminals

Source: IDC, 2012

RSA EMC²

802.11 Enabled Wine Refrigerator

Destructive Attacks

ATTAC
METHOD

Intrusi Attack

tive ks

Worms/ Viruses

Simple DDoS

Phishing Pharming

Sophisticated Mobile Attacks

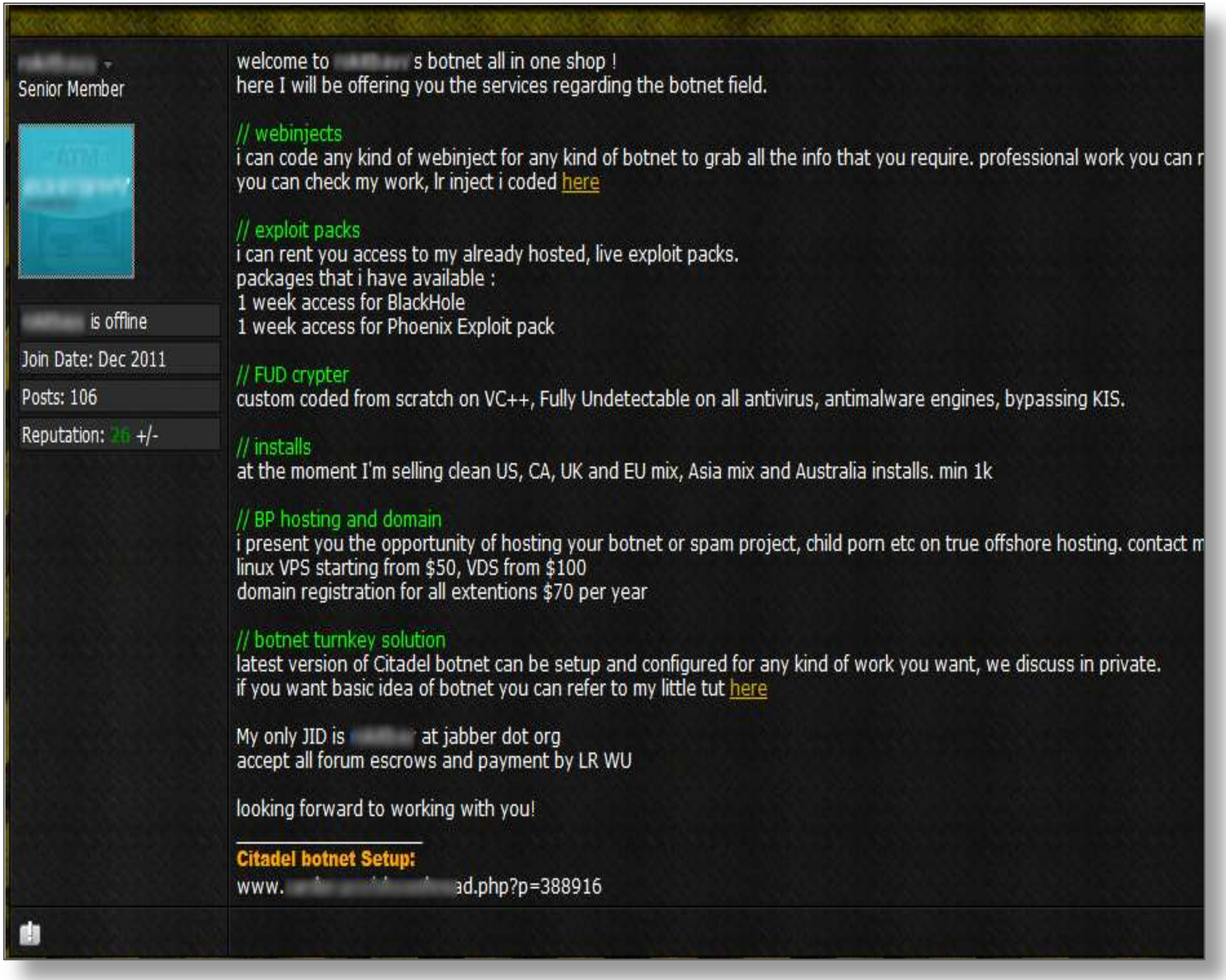
The Unknown??

TIME

2007

0

The Malware Marketplace



[redacted]
Senior Member

[redacted] is offline

Join Date: Dec 2011

Posts: 106

Reputation: 26 +/-

welcome to [redacted] s botnet all in one shop !
here I will be offering you the services regarding the botnet field.

// webinjects
i can code any kind of webinject for any kind of botnet to grab all the info that you require. professional work you can r
you can check my work, lr inject i coded here

// exploit packs
i can rent you access to my already hosted, live exploit packs.
packages that i have available :
1 week access for BlackHole
1 week access for Phoenix Exploit pack

// FUD crypter
custom coded from scratch on VC++, Fully Undetectable on all antivirus, antimalware engines, bypassing KIS.

// installs
at the moment I'm selling clean US, CA, UK and EU mix, Asia mix and Australia installs. min 1k

// BP hosting and domain
i present you the opportunity of hosting your botnet or spam project, child porn etc on true offshore hosting. contact m
linux VPS starting from $50, VDS from $100
domain registration for all extentions $70 per year

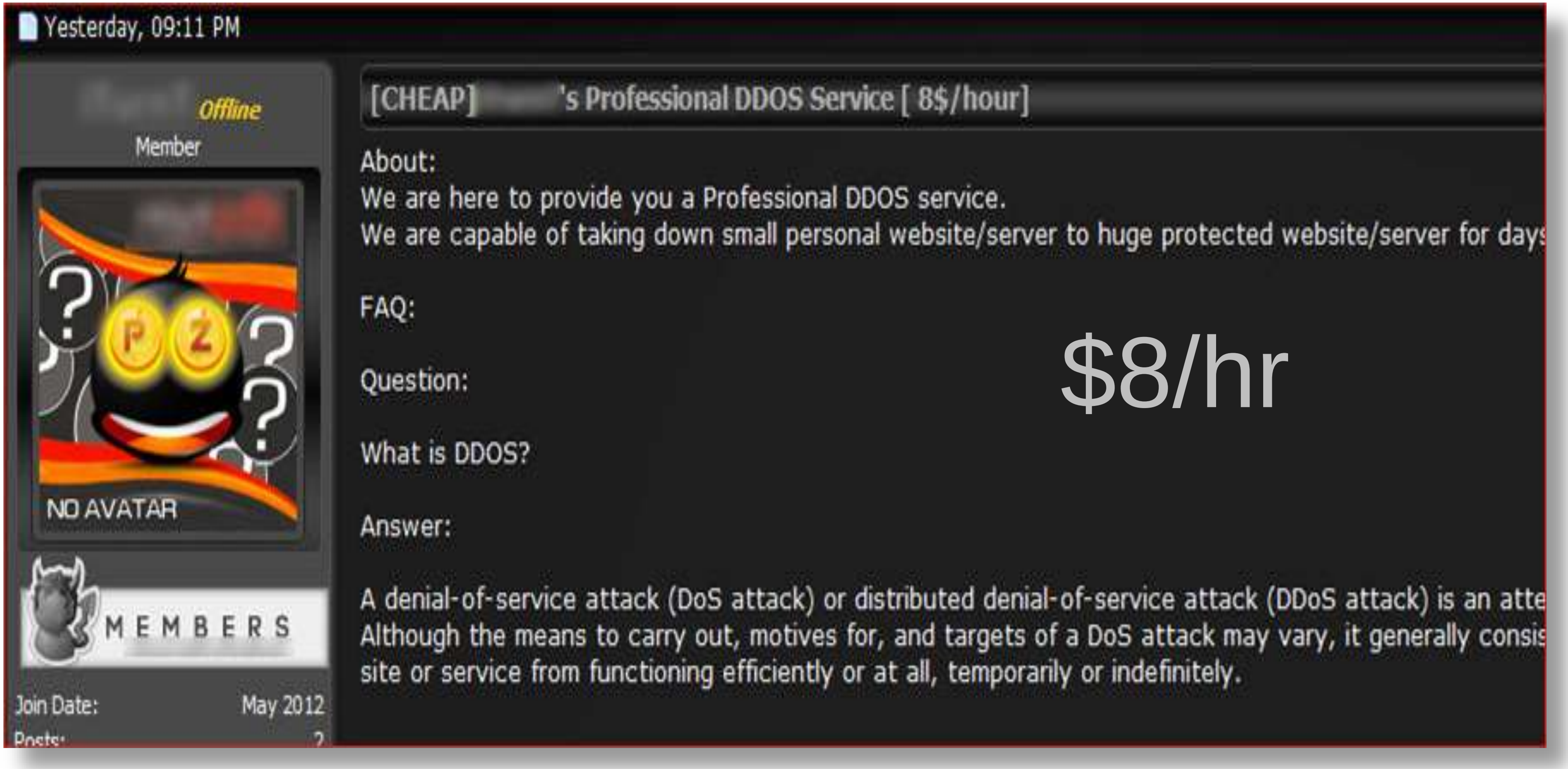
// botnet turnkey solution
latest version of Citadel botnet can be setup and configured for any kind of work you want, we discuss in private.
if you want basic idea of botnet you can refer to my little tut here

My only JID is [redacted] at jabber dot org
accept all forum escrows and payment by LR WU

looking forward to working with you!

Citadel botnet Setup:
www.[redacted]ad.php?p=388916

The Malware Marketplace



Yesterday, 09:11 PM

[redacted] Offline
Member

Join Date: May 2012
Posts: 2

[CHEAP] [redacted] 's Professional DDOS Service [8$/hour]

About:
We are here to provide you a Professional DDOS service.
We are capable of taking down small personal website/server to huge protected website/server for days

FAQ:

Question:

What is DDOS?

Answer:

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an atte
Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consis
site or service from functioning efficiently or at all, temporarily or indefinitely.

$8/hr

Traditional Security is Not Working!

99% of breaches led to compromise within “days” or less with 85% leading to data exfiltration in the same time

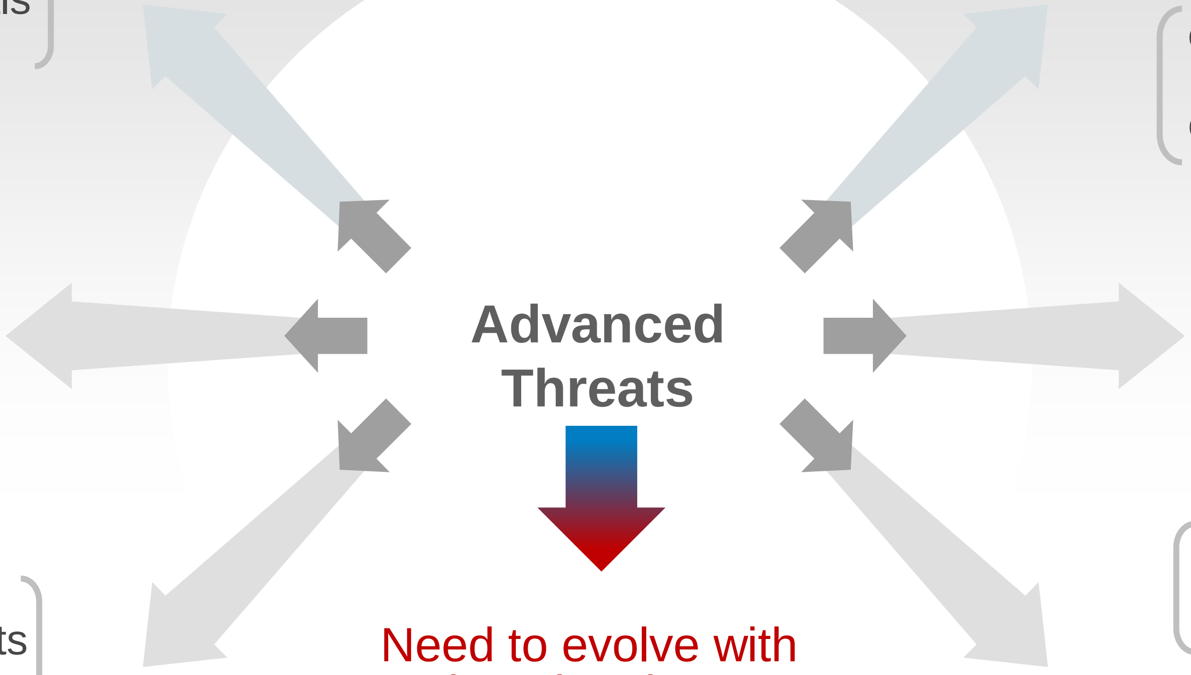
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

85% of breaches took “weeks” or more to discover

84% of data records were stolen as a result of stolen login credentials

Source: Verizon 2012 Data Breach Investigations Report

The Age of Advanced Threats



Who

Cyber Criminals

Nation State Actors

Hacktivists

Advanced Threats

Need to evolve with changing threat environment

How

Well funded
&
well organized

Open Source Intelligence Collection

Zero-day Vulnerability Research

Acutely Targeted Campaigns

Black Market Malware

Supply Chain Tampering

Attack Surface of Social Media

Initial monetizat

al rcialization of al absence of privacy

2013

2020

Social Media

2013 A Yea

RSA hacked 'reduce the tokens

BY TIM STEVENS ▪ MARCH 18TH, 2011 A

If you've ever wondered whether two-factor authentication systems actually boost security, things that spit out pseudorandom numbers you have to enter in addition to a password, the answer is yes, yes they do. But, their effectiveness is of

Bradley Manning gets 35 years in U.S. WikiLeaks case

'Sometimes you have to pay a heavy price to live in a free society,' writes Manning after sentencing

The Associated Press Posted: Aug 21, 2013 10:22 AM ET | Last Updated: Aug 21, 2013 2:45 PM ET

Manning sentenced to 35 years 3:33

WikiLeaks spokesman on Manning sentence 5:45

Listen

Bradley Manning was sentenced today to 35 years in prison for giving hundreds of thousands of secret military and diplomatic documents to WikiLeaks in one of the nation's biggest leak cases since the Pentagon Papers more than a generation ago.

In a brief hearing at Fort Meade, Md., Col. Denise Lind, a military judge, didn't offer any explanation for the sentence.

The soldier will be dishonorably discharged from the U.S. military and forfeit some of his pay, she said.

Stay Connected with CBC N

Mobile Facebook Podcasts Twitter

Must Watch

Vatican policies allowed priests to rape children, UN report says

Reac Exco them

FEATURED STORIES

- Hackers in China Attacked The Times for Last 4 Months
- NYT hackers resurface with new arsenal
- What Happened to the New York Times website

The “Community’ of Attackers

Criminals

Petty criminals

Unsophisticated

Organized crime

Organized, sophisticated supply chains (PII, financial services, retail)

Non-state actors

Terrorists

PII, Government, critical infrastructure

Anti-establishment vigilantes

“Hacktivists”
Targets of opportunity

Nation states

PII, government, defense industrial base, IP rich organizations

Security Models

Reactive → Intelligence Driven

Reactive

Historical

- Perimeter-based
- Static Controls
- Siloed Management System

Intelligence Driven

New

- Risk-based
- Dynamic/Agile Controls
- Contextual/Interactive Management System

Traditional Reactive Defense Methodology

- Firewalls
- Virus Scanning
- USB Disablement
- Employee Background Che
- Intrusion Detection
- Intrusion Prevention
- Policy
- Overall Network Protection

Reactive Model

Firewall

Intrusion Detection

USB Control

Policy

Employee Background Checks

VPN

Traditional Reactive Defense Methodology

- **Firewalls**
- **Virus Scanning**
- **USB Disablement**
- **Employee Background Checks**
- **Intrusion Detection**
- **Intrusion Prevention**
- **Policy**
- **Overall Network Protection**

Today’s Dynamic Risk Management

- 24x7 Coverage
- Social Media Profile Monitoring
- Mobile Devices (BYOD)
- 802.11 Proliferation
- Virus Scanning
- Portable Mass Storage
- Cloud Storage
- Software As a Service Monitoring
- Compliance Automation
- Policy Enforcement
- Continuous Training
- Penetration Testing
- Employee Social Media presence

- Big Data Analytics
- Infrastructure As a Service Monitoring
- Insider Threat / Counter Intelligence
- Digital Forensics
- Ediscovery
- Packet Capture
- Audit Logging
- DLP
- SEIM
- Continuous Monitoring
- Remote Employee
- Automated Code Analysis
- Rapid App Development Security
- Liability Insurance
- Breach Notification

THIS MORNI

York, NY

The New York

Snowden Asks U.S. to Stop Treatin

CBS THIS MORNING SATURDAY

South China Morning Post

南華早報

EXCLUSIVE Whistle-blower Edward Snowden talks to the South China Morning Post

I'LL FIGHT TO STAY IN HK

МИР

удена

двинут

ER SPIEGEL

ENTHÜLLT

Wie der US-Geheimdienst in Deutschland spioniert

GEN AMERIKA

: HELD UND VERRÄTER

Exc

T

governme

destroy pri

and basic libe

theguard

The Washington Post

Man who leaked NSA secrets steps forward

A REPORTER'S ACCOUNT

To leaker, personal risks were clear

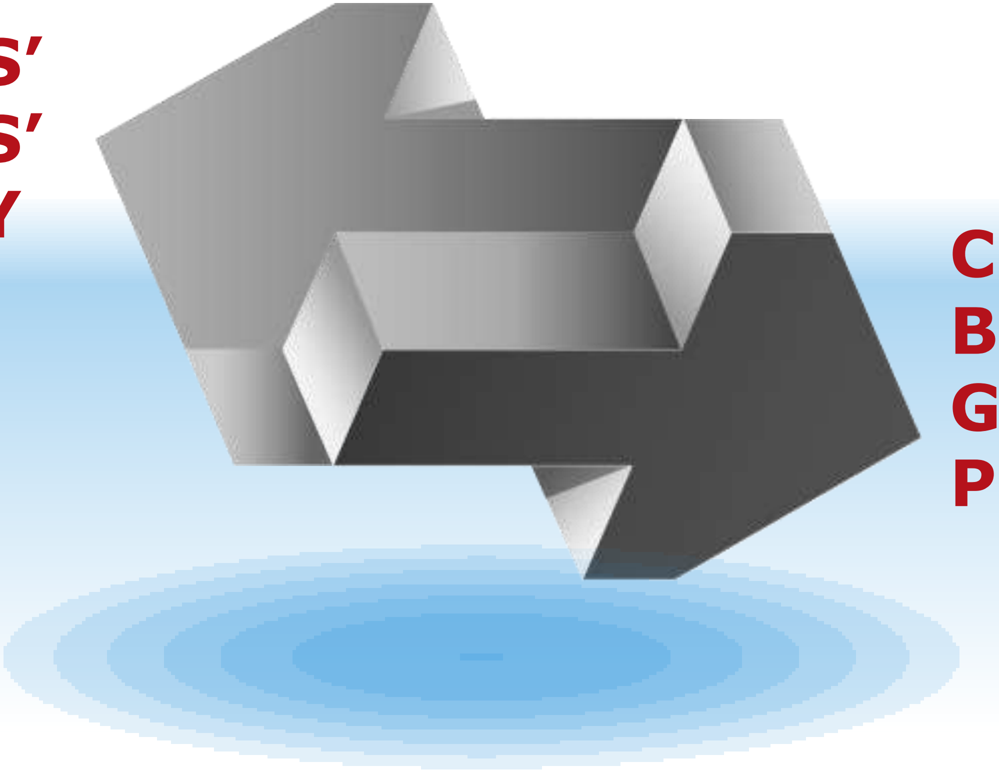
EDWARD SNOWDEN: 'I'M NOT GOING TO HIDE'

Booz Allen consultant could face prosecution

Risks of outsourcing

A historic leak

CUSTOMERS' AND USERS' PRIVACY



CONFLICTING BUSINESS & GOVERNMENT PII USE

CATCH-22

Living in a State of Compromise

Assume you are compromised and plan for failure

- It’s unrealistic to believe you can keep attackers out of your networks
- Focus on core IT security concepts:
  - Minimize impact of compliance
  - Control/Monitor Administrative Privileges
  - Make lateral movement difficult
  - Situational Awareness (Visibility to the Infrastructure)
- Centralize your critical information assets:
  - What/Where they live?
  - How much are they worth?

Incident Response as a Cultural Norm

Not as a function of Information Security

- The clock is ticking from the moment a breach starts, how will you react?
- Well executed plans are often well tested
  - What is your backup email system?
  - Can everyone communicate via encrypted email?
  - Are you using non-affiliated Internet access?
- If you discover a breach …
  - What information would an attacker want?
  - Who has access to it?
  - What are the procedures to remove all access?
  - Who can authorize these steps?
  - What would the impact be to the company?

Security Challenges For 2014

- No perimiter
- Hiring
- Retention
- Contracts written for static defined effort
- Expanding mobile and BYOD environment
- Shrinking Budgets
- “Webified” everything
- Non-Compliant Cloud offerings
- Mass data stores
- Increased PII data storage of customers

Trust in the Digital World

RSA