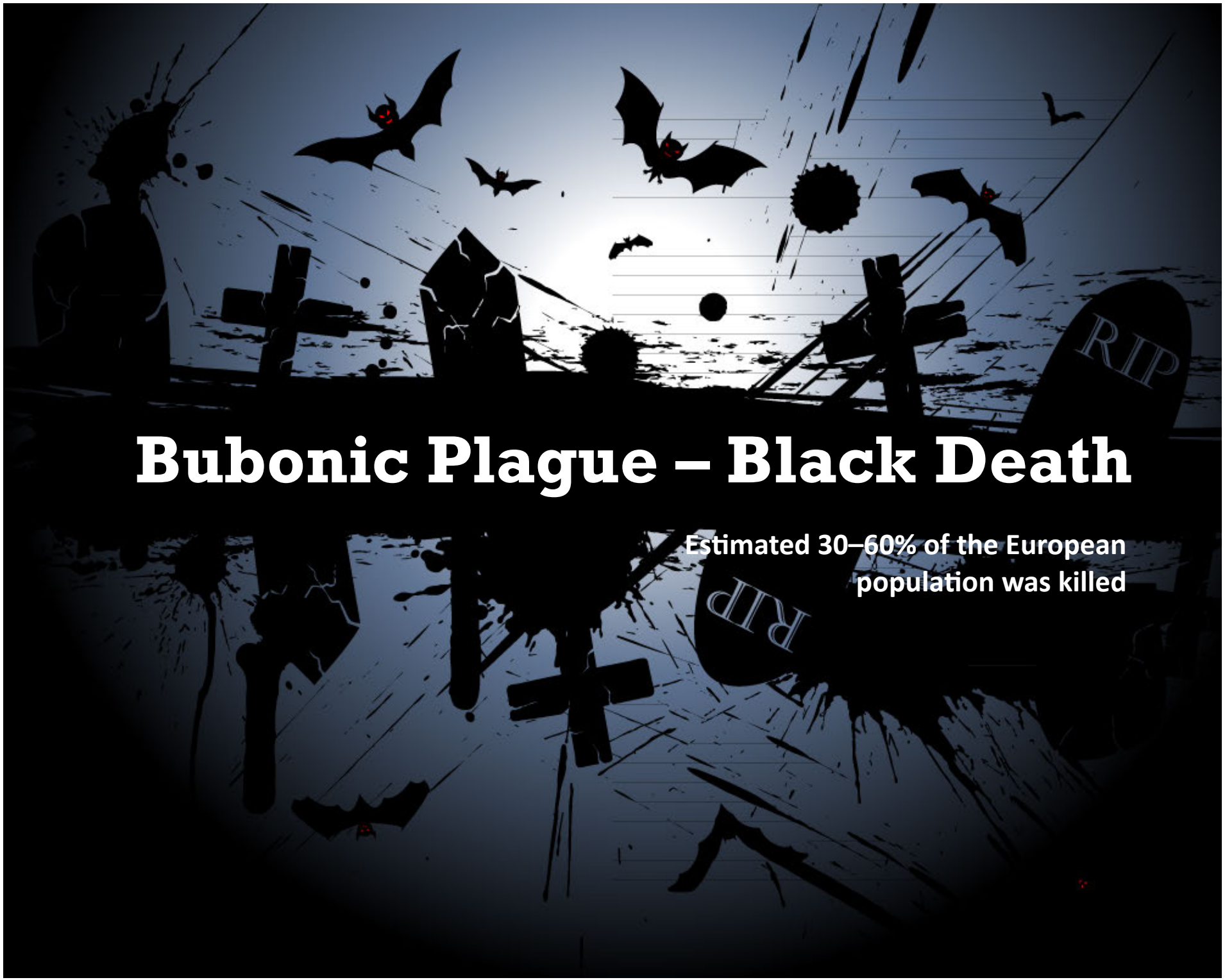
The Cybersecurity Quagmire : Finding the Panacea

Jay Bavisi , President – EC-Council



Bubonic Plague – Black Death

Estimated 30–60% of the European population was killed

Plague Timeline

Quarantine

224 BC

Hygiene

+1500 years

Vaccine

1796

2000 years to solve the problem?

200 years to reach population pre-plague

Unravel the Enigma of Insecurity

Elimination vs. Erradication vs. Control

Elimination

- The reduction of prevalence of a disease in a defined area to zero or the reduction of global prevalence to a negligible amount, e.g. Poliomyelitis and measles

1

Erradication

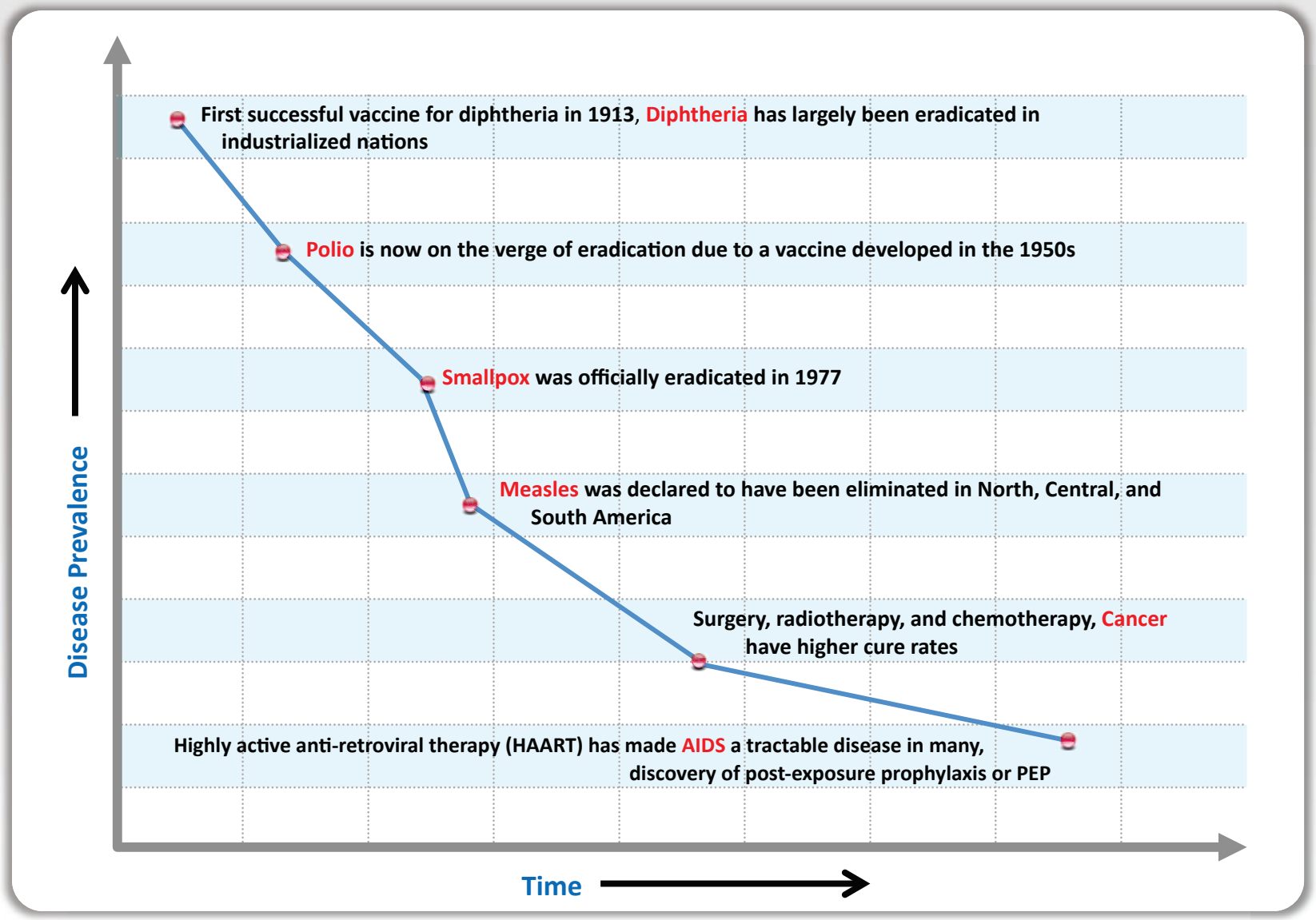
- The permanent reduction of the worldwide prevalence of a disease to zero, e.g. Smallpox

2

Control

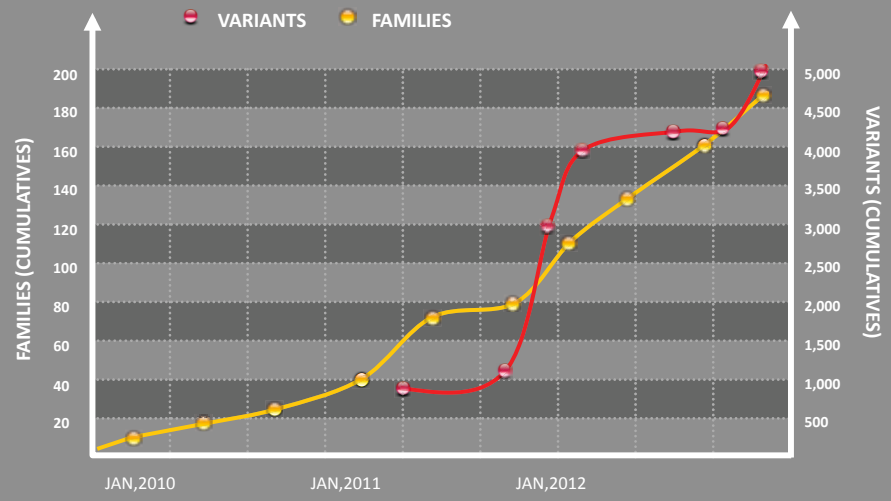
- The reduction in the incidence, prevalence, morbidity or mortality of an infectious disease to a locally acceptable level

3

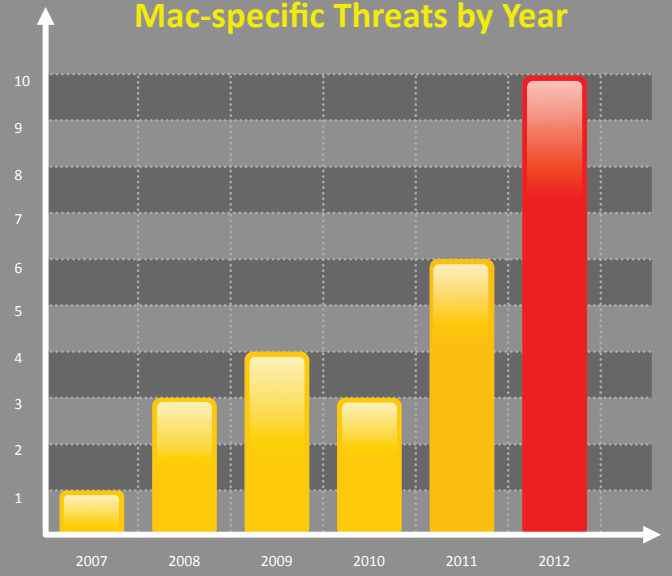


Unravel the Enigma of Insecurity

Cumulative Mobile Android Malware, 2010 to 2012

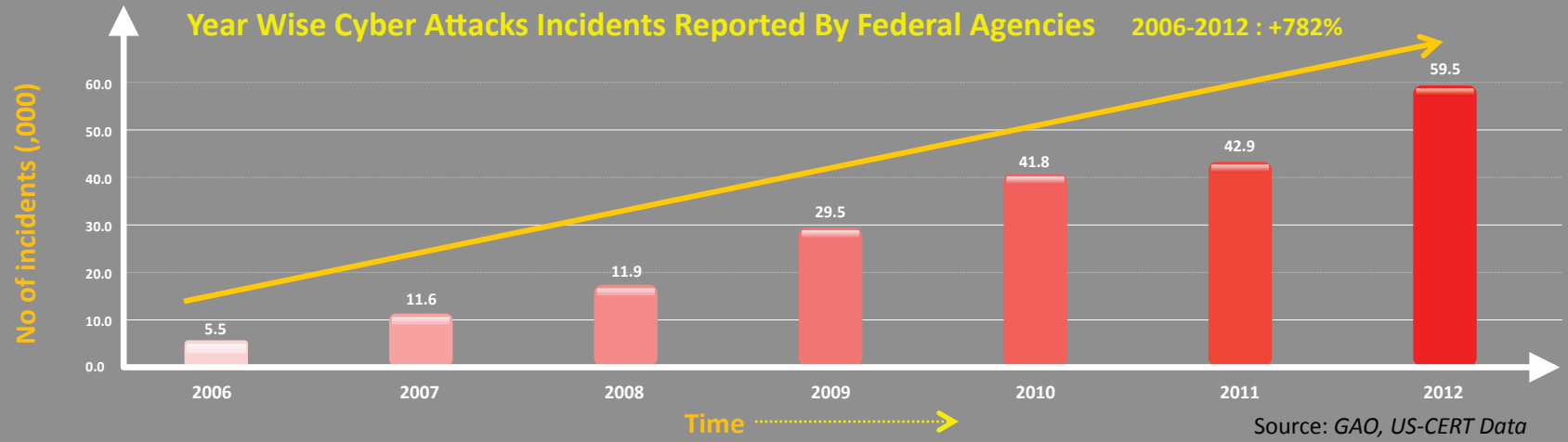


Mac-specific Threats by Year



Year Wise Cyber Attacks Incidents Reported By Federal Agencies

2006-2012 : +782%



Source: *GAO, US-CERT Data*

Unravel the Enigma of Insecurity

Timeline of Targeted attacks

Ghostnet
- March 2009
- Large-scale Cyber spying operation

Hydraq
- January 2010
- Operation "Aurora"

Stuxnet
- June 2010

RSA Attacks

Sykipot/Taidoor Attacks
- Targeting Defense Industry and Governments

Nitro Attacks
- July-October 2011
- Against Chemical Industry

Flamer and Gauss
- May 2012-Aug 2012
- Highly Sophisticated Threat
- Targets Middle East

Elderwood Project
- September 2012
- Main Target: Defense
- Same group identified using Hydraq(Aurora) in 2009

Unravel the Enigma of Insecurity

The Massive Attacks

BIGGEST DDoS ATTACK IN HISTORY hammers Spamhaus

Plucky mail scrubbers battle internet carpet bombers

By John Leyden, 27th March 2013 *http://www.theregister.co.uk*

Anti-spam organisation Spamhaus has recovered from possibly the largest DDoS attack in history.

A massive 300Gbps was thrown against Spamhaus' website but the anti-spam organisation was able to recover from the attack and get its core services back up and running. CloudFlare, the content delivery firm hired by Spamhaus last week to guard against an earlier run of DDoS attacks, was also hit, forcing it into taking the highly unusual step of dropping London as a hub in its network - as a Twitter update by CloudFlare on Monday explained.

RELATED STORIES

Spamhaus-style DDoS attacks: All the hackers are doing it

Rotten spam causing more infections than ever – study

Call centers under attack in targeted cyber-blackmail scheme

Analysis BIGGEST DDoS in history FAILS to slash interweb arteries

Analysis Spamhaus and ISP spar over 'email DoS' blacklisting

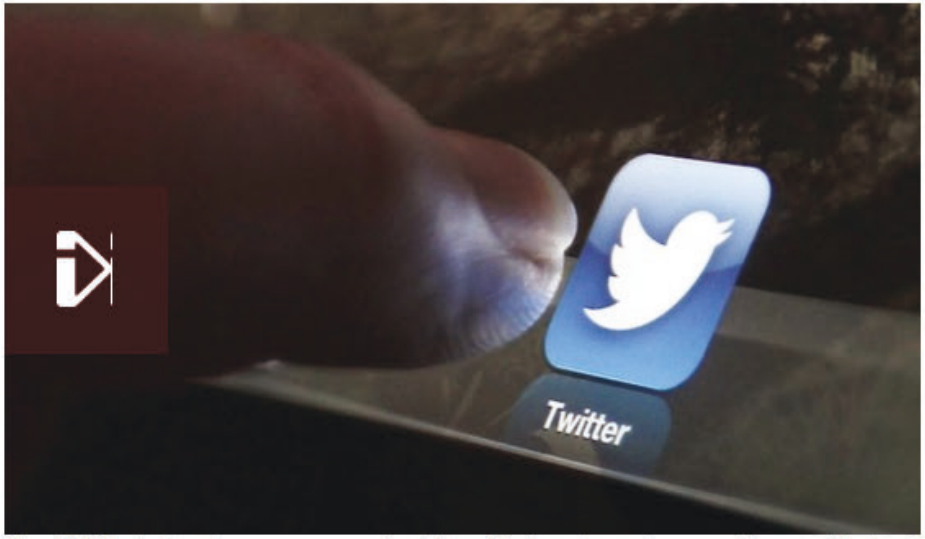
Our peering in London has been dropped due to a large attack. Modifying routes to avoid degradation. Affecting location: London, GB

Spamhaus supplies lists of IP addresses for servers and computers on the net linked to the distribution of spam. The blacklists supplied by the not-for-profit organisation are used by ISPs, large corporations and spam filtering vendors to block the worst sources of junk mail before other spam filtering measures are brought into play.

Spammers, of course, hate this practice so it's no big surprise that Spamhaus gets threatened, sued, and DDoSed regularly. Those affected by what they regard as incorrect listings also object about Spamhaus' alleged vigilante tactics.

Twitter: Hackers target 250,000 users

COMMENTS (251) *http://www.bbc.co.uk*



The BBC's technology correspondent Rory Cellan-Jones is one of those affected

A quarter of a million Twitter users have had their accounts compromised in the latest of a string of high-profile internet security breaches.

Twitter's information security director Bob Lord said about 250,000 users' passwords had been stolen, as well as usernames, emails and other data.

Related Stories

Google boss on China 'IT menace'

'China hackers' attack NY Times

China condemns NY Times 'smear'

Unravel the Enigma of Insecurity

The Massive Attacks

Apple suffers largest hacking attack in its history

By Jim Finkle and Joseph Menn
Reuters
Posted: 02/19/2013 11:40:58 AM PST
Updated: 02/19/2013 05:29:57 PM PST

BOSTON/SAN FRANCISCO -- Apple (AAPL) was recently attacked by hackers who infected Macintosh computers of some employees, the company said Tuesday in an unprecedented disclosure describing the widest known cyber attacks targeting Apple computers used by corporations.

Unknown hackers infected the computers of some Apple workers when they visited a website for software developers that had been infected with malicious software. The malware had been designed to attack Mac computers.

The same software, which infected Macs by exploiting a flaw in a version of Oracle's (ORCL) Java software used as a plug-in on Web browsers, was used to launch attacks against Facebook, which the social network disclosed on Friday.

The malware was also employed in attacks against Mac computers used by "other companies," Cupertino-based Apple said, without elaborating on the scale of the assault.

More Apple coverage

- Apple, Google, Faceb deny giving NSA, FBI to servers
- Cupertino: Apple's ne headquarters will gen 'unacceptable level' o 280, report says
- Officials to seek cure smartphone thefts in Apple, Google
- Apple said to begin iP this month
- Apple to sell audio ad music service, source

http://www.mercurynews.com

Infecting MAC Computers

Chameleon botnet steals $6M per month in click fraud scam

More than 120,000 Windows-based computers running Internet Explorer 9 are infected in the U.S., researchers say.

by Steven Musil | March 19, 2013 8:55 PM PDT
Follow @stevenmusil

http://news.cnet.com

140 0 12 +1 17 More + Comments 0

Security researchers say they have identified a botnet that steals more than $6 million per month by generating fake customer clicks on online display ads.

Dubbed Chameleon, the botnet has infected more than 120,000 Windows-based computers in the U.S., mimicking human behavior on select Web sites to generate billions of ad impressions and fraudulent income for its creators, according to security firm Spider.io.

Click fraud costs Web advertisers in lost revenue by making them pay for illegitimate clicks. Spider.io reported that advertisers paid an average of 69 cents per one thousand impressions generated by the botnet. Researchers estimate Chameleon was responsible for two-thirds of the 14 billion ad impressions served by the 202 affected Web sites, nearly all of which are located in the U.S.

Unravel the Enigma of Insecurity

Chinese hackers steal U.S. weapons systems designs, report says

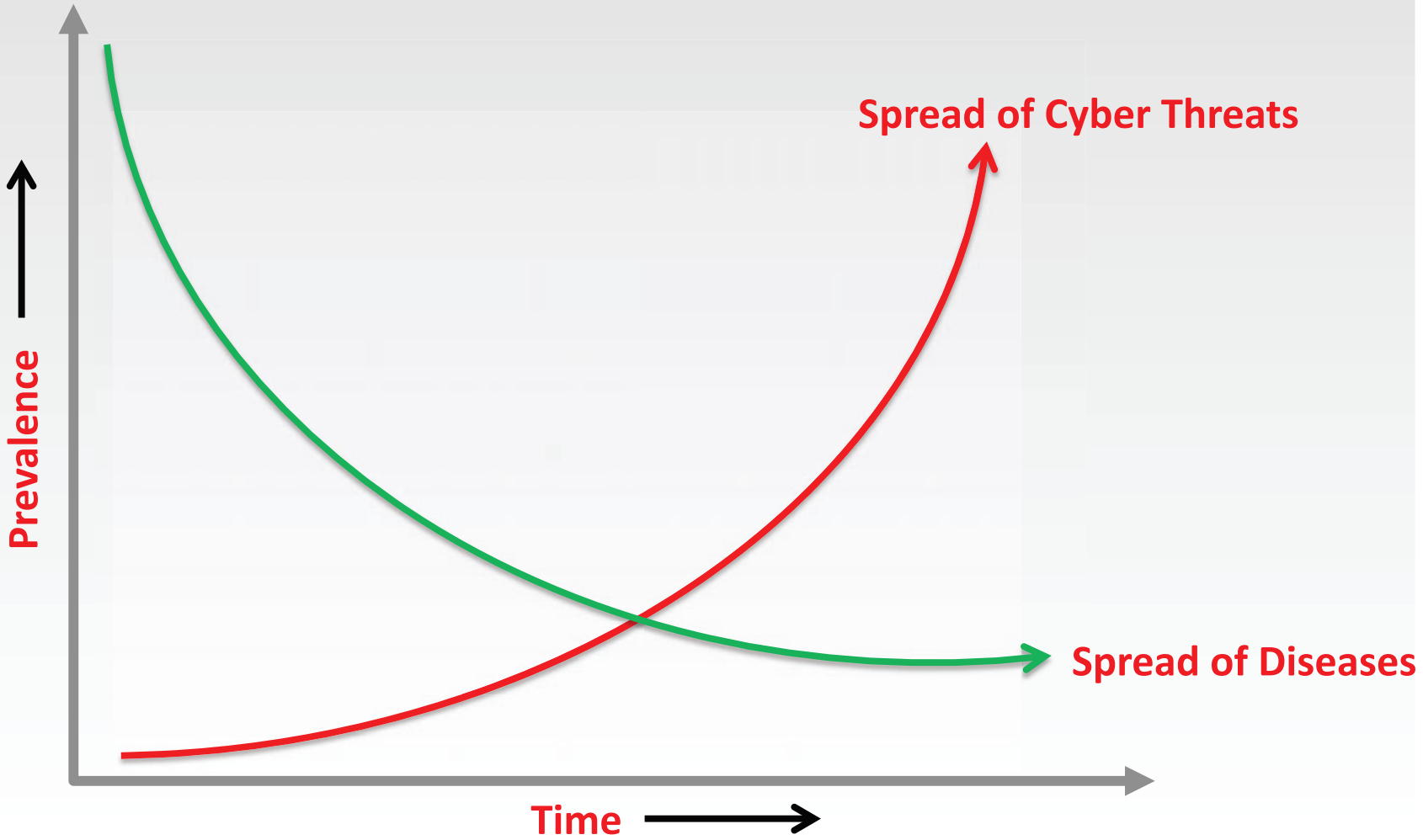
This image provided by the US Navy shows a modified Standard Missile 2 interceptor is launched in 2008 from the guided-missile cruiser USS Lake Erie during a test. A new report says Chinese hackers have stolen designs for several U.S. weapons systems.

By Terril Yue Jones, Bill Trott and Rob Taylor, Reuters

Chinese hackers have **gained access to designs of more than two dozen major U.S. weapons systems**, a U.S. report said on Monday, as Australian media said Chinese hackers had stolen the blueprints for Australia's new spy headquarters.

Citing a report prepared for the Defense Department by the Defense Science Board, the Washington Post said the compromised U.S. designs included those for combat aircraft and ships, as well as missile defenses vital for Europe, Asia and the Gulf.

An Analogy: WE ARE LOSING THE FIGHT !



Cyber Plague

You are in IT !!!!!!!

Large Giants being taken out with hacks invented a long time ago

LinkedIn facebook.

CHASE

Microsoft

The New York Times

SONY
make.believe

Cyberplague Timeline

Quarantine

Cyber Hygiene

Vaccine

Firewall

Education

IDS

Policy

IPS

Unravel the Enigma of Insecurity

Wrong Code vs. Correct Attack

Vulnerable Code (Non-Parameterized stored procedure)

```
1: Try
2: Dim command As SqlCommand = new
   SqlCommand("sp_getAccountBalance(CustomerName.Text)", connection);
3: Dim reader As SqlDataReader = command.ExecuteReader();
4: Catch se As SqlException
5: ' error handling
6: End Try
```

Vulnerable to **SQL injection attack**

This parameterized stored procedure approach helps in **preventing SQL injection attacks**

Secure Code (Parameterized stored procedure)

```
1: Try Dim command As SqlCommand = new SqlCommand("sp_getAccountBalance", connection);
2: command.CommandType = CommandType.StoredProcedure;
3: command.Parameters.Add(new SqlParameter("@CustomerName", CustomerName.Text));
4: Dim reader As SqlDataReader = command.ExecuteReader();
5: Catch se As SqlException
6: ' error handling
7: End Try
```

Wrong Code vs. Correct Attack

Vulnerable Code

```
1:  <configuration>
2:   <system.web>
3:     <sessionState mode = <"inproc" |
       "sqlserver" | "stateserver">
4:      cookieless="true">
5:    </system.web>
6:  </configuration>
```

If cookieless is set to true, then the URL is used to transfer session tokens, which are vulnerable to Session Hijacking and MITM attack

Secure Code

```
1:  <configuration>
2:   <system.web>
3:     <sessionState mode = <"inproc" |
       "sqlserver" | "stateserver">
4:      cookieless="false">
5:    </system.web>
6:  </configuration>
```

If cookieless is set to false, then cookies are used to transfer the session token, which secures the session tokens

Type's of Vaccine

ACTIVE IMMUNIZATION
Measles, Mumps, Yellow Fever, Rotavirus

Ethical Hacker (Antigen and Antibody)

PASSIVE IMMUNIZATION
Tetanus

Secure Code (Antibody)
Immunological Memory

Unravel the Enigma of Insecurity

CASE STUDY

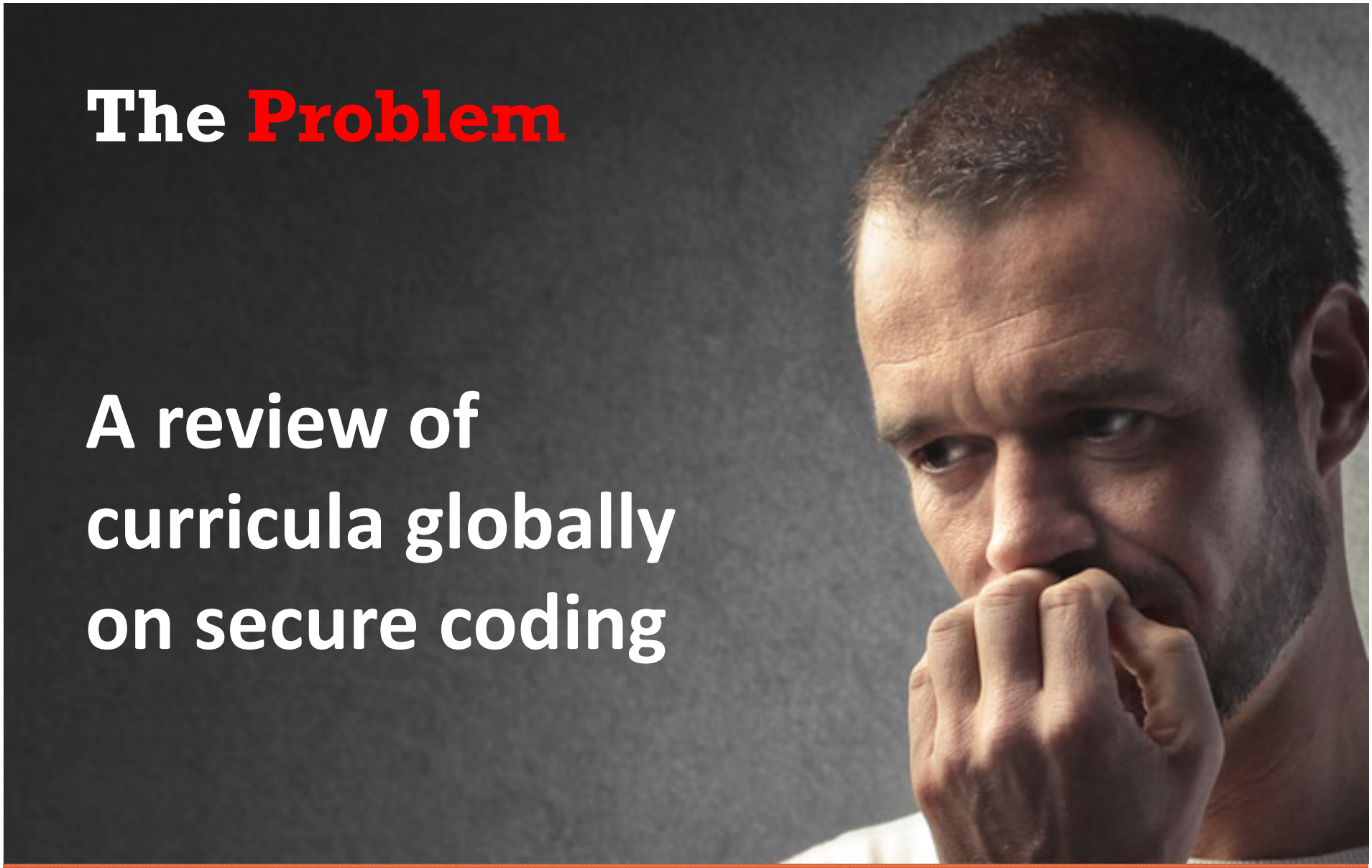
My conversation with a VP Security of a LARGE Banking Group in the US

Unravel the Enigma of Insecurity

CASE STUDY

My discussion with the VP of a Large Software Development House in the US that works for a MAJOR Mobility company

The Problem



A review of curricula globally on secure coding

Unravel the Enigma of Insecurity

Secure Coding Education: Are We Making Progress?

> "While current computer science (CS) programs are adept at teaching programming skills including exposing students to languages commonly used in industry, the focus is often on "making programs work". Students are typically given an assignment with a set of functional goals such as to create a program that reads records from a file, and then performs some calculation based on the values retrieved. In such cases little consideration is given to secure programming issues, and as such students do not learn how to write programs that would be resilient to accidentally or maliciously malformed input in real world conditions."
>
> - *Proceedings of the 16th Colloquium for Information Systems Security Education. 2012*

World's Best Universities

No Comprehensive Secure Coding Program

Unravel the Enigma of Insecurity

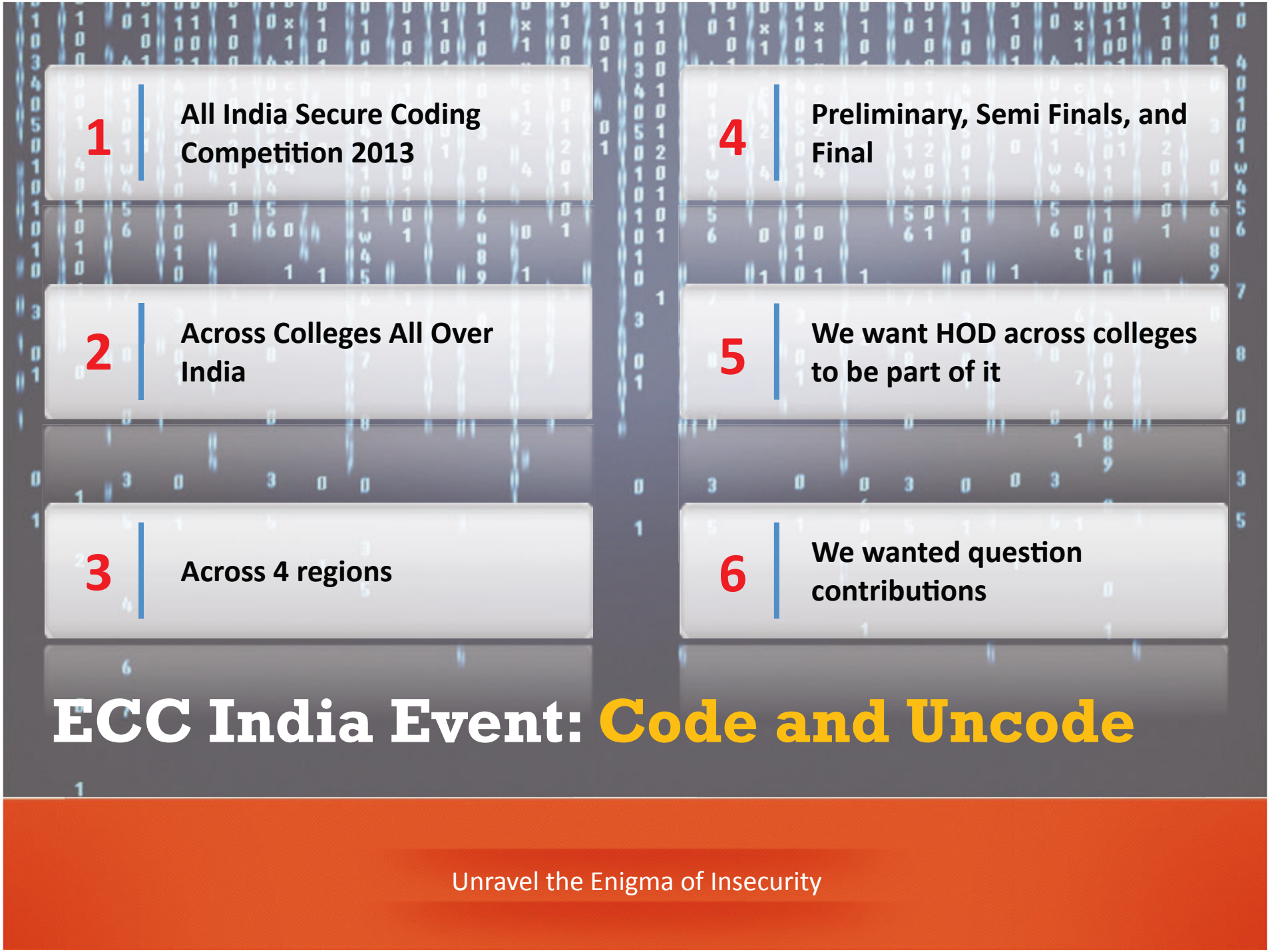
The Point

The Vaccine

Secure Coding

Manufacturing the Panacea

Unravel the Enigma of Insecurity


1
All India Secure Coding Competition 2013
2
Across Colleges All Over India
3
Across 4 regions
4
Preliminary, Semi Finals, and Final
5
We want HOD across colleges to be part of it
6
We wanted question contributions
ECC India Event: Code and Uncode
Unravel the Enigma of Insecurity

Code Uncode Partnerships

NASSCOM®

IT AP
The IT and ITES Industry Association of AP
(Formerly HYSEA)

HCL

Aspro Technologies

modi naturals
Oleev
Go beyond

Seeroo
IT SOLUTIONS Pvt. Ltd.
Powerful Thoughts • Simple Solutions

SRISHTI INNOVATIVE
Quality Beyond Contract

NANO SOFTWARES
Quality Guaranteed

COMPUTER SOCIETY OF INDIA
ESTD. 1965

KRYONNS
Technologies

SYNERZIP
Agile Software Product Development Partner

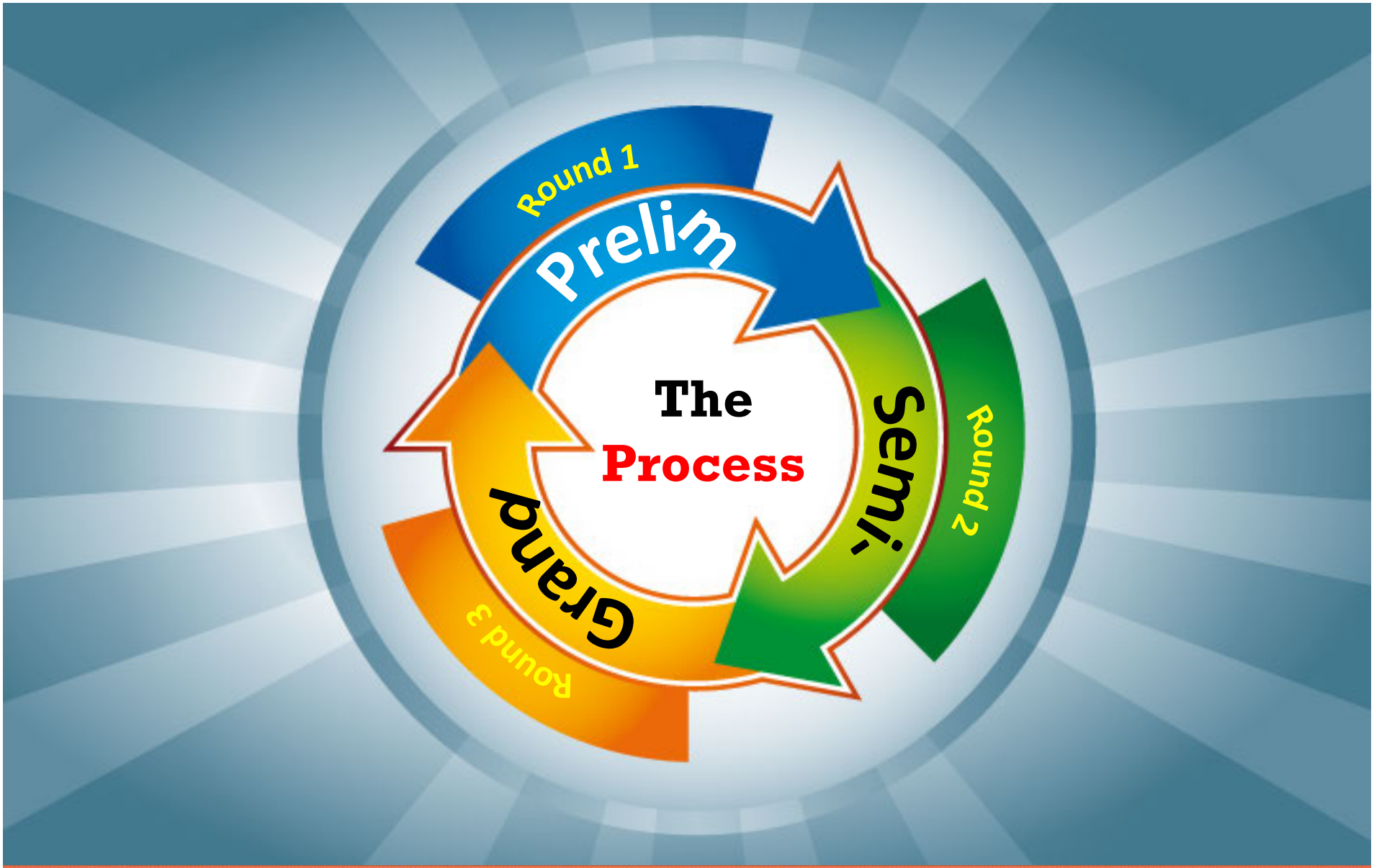
LOVELY PROFESSIONAL UNIVERSITY
Transforming Education Transforming India

THAPAR UNIVERSITY

AMITY UNIVERSITY

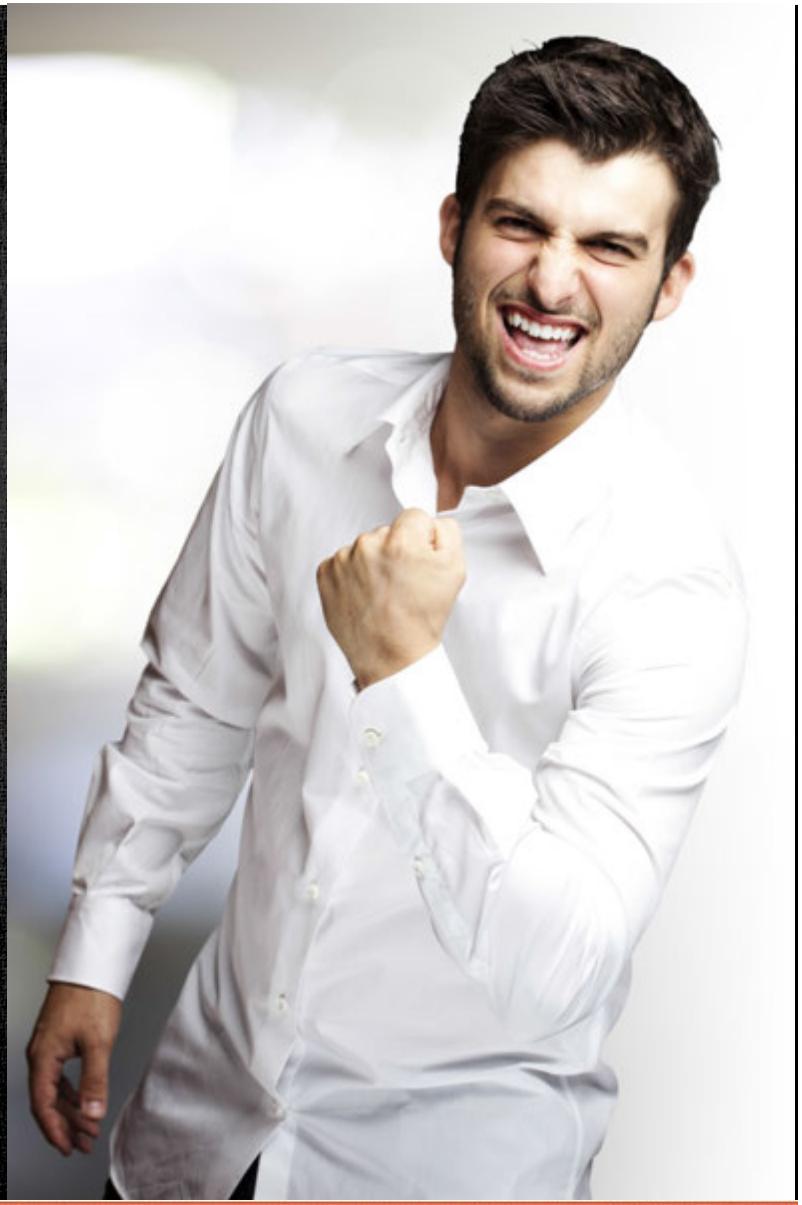
neptune
Neptune Software Group

Unravel the Enigma of Insecurity



Unravel the Enigma of Insecurity

The Result!!!



Solution:

Start Manufacturing the Panacea now!

Unravel the Enigma of Insecurity

Unravel the Enigma of Insecurity