secure 2014

XVIII Konferencja na temat bezpieczeństwa teleinformatycznego

Warszawa, 21 – 23 października 2014 r.

NASK

CERT.PL

Cybercrime Metrics and Threat Data:

Warsaw - Poland

What are the Current Trends? Who? Why? and Where?

Jart Armin – HostExploit – CyberDefcon - CyberROAD

CyberDefcon

CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Jart Armin

CyberDefcon

- NGO - Research group for Cyber threat analysis and Cybercrime intelligence.
- A specialist international cyber attack investigation team
- Cyber Observatory into malicious & threat data.

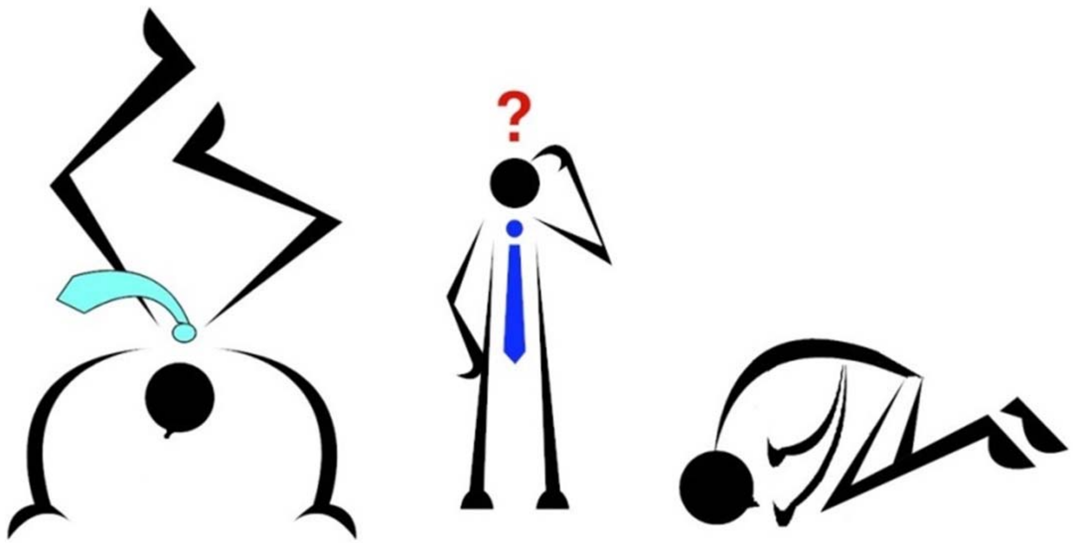
HOST exploit

- Community: Quarterly reports on all the world’s hosts and Internet servers.
- Founder of the non-profit CSF (Cyber Security Foundation).

CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

- EU project aimed to identify current and future issues in the fight against cyber-crime and cyber-terrorism in order to draw a strategic roadmap for cyber security research.



CYBERCRIME METRICS – What’s in the numbers?

Top → Down

CURRENT ESTIMATES (October 2014 – references - http://jart.me/jart_sec2014)

- The annual cost to the global economy from cybercrime is more than **€300 billion Euros** McAfee, Intel, & others
- Cost of cybercrime for the **EU 0.4% of its GDP** = **€13 billion / annum** (2012 IMF)
- Therefore for Poland = **€ 377 million /annum**
- Compare to Germany = **€ 2.6 billion /annum** – UK = **€ 2 billion /annum**
- Cybercrime market globally itself of **€15 billion / annum** HostExploit, GroupIB
- Market for security products and services **€50 billion / annum** IDC
- Compare with EU **0.0005% of its GDP = € 150 million / annum** on Cybercrime R&D e.g H2020

Direct costs of cybercrime is 3% up year on year

Population	Worldwide	Poland
Adults who have experienced cybercrime in their lifetime	61%	60%
Adults who experienced cybercrime in the past 12 months	41%	40%
Adults who have been victim of cybercrime and risky behaviours	50%	49%
Males who have been victim of cybercrime in their lifetime	64%	66%
People aged 18-32 who have been victim of cybercrime in their lifetime	66%	70%
Number of victims in the past 12 months (million)	378	6

Symantec

Effect of Cybercriminal acts (examples)?	< 2.8 billion!
Spam	Current Internet Users - World
Click jacking	
Mal-advertizing	
Browser hijacking	
Unauthorized browser redirects	
Intrusion & user data exfiltration apps (e.g. mobile)	

Top – Down 2 : Filter down to social groups & countries

CYBERCRIME – MEASURING ACTIONS - OBSERVATION

Cyber Metrics

General Cyber Metrics
2.8 Billion users of the Internet (~39% world population)
Over 100 billion emails processed / day
959 million websites — 39 million / month added (4%).
IP addresses - IPv4 = 4,294,967,296 (2^{32}) - IPv6 = of (2^{128})
1.4 million browser user agents - bots

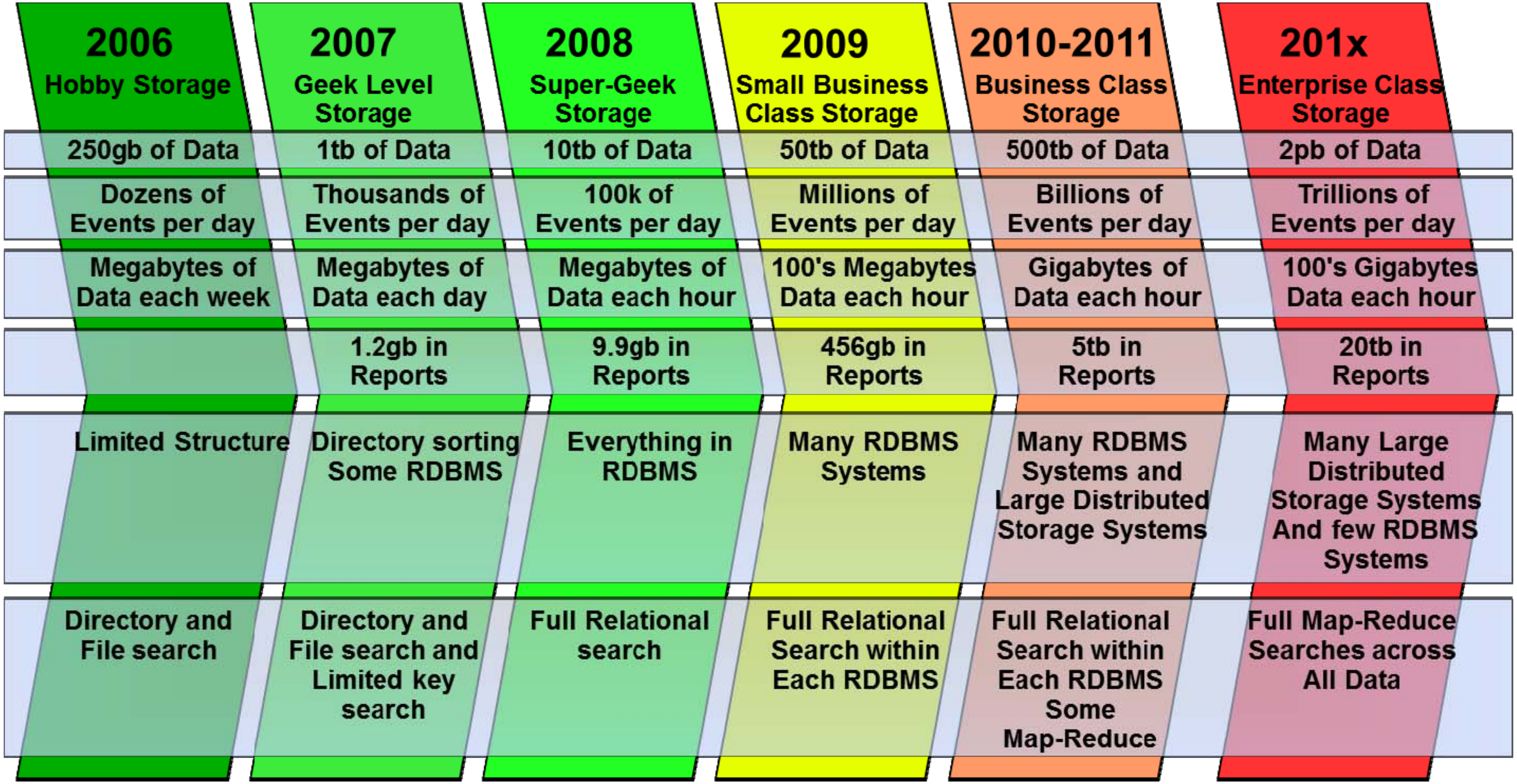
Cybercrime Activity

Measuring malicious events	Source
85% of processed emails are spam	Barracuda
7% of all urls maliscious	Barracuda
Public Block List count: 1,018,203,532 IP addresses	Spamhaus
250 million in total identifiable malware	AV-Test Org
200,000 new malicious programs registered	AV-Test Org
1 million+ measurable cyber-attacks every day	Akamai
330 active Real-time Blackhole Lists (RBL & DNSBL)	Hostexploit
€ 5.9 million is the average annualized cost of data breaches	Ponemon Institute
10.4% net increase cost of data breaches over the past year	Ponemon Institute
250,000 – 500,000 malicious binaries / day	Shadowserver
~280 million malicious binaries collected	Shadowserver
6 / 10 million unique IP's sinkholed / day	Shadowserver
900,000 malicious domains / day	Shadowserver
500 of 52,000 ASNs worldwide (4%) account for hosting 85% of malicious activity	Hostexploit

CyberDefcon

Observing & Measuring the threat – Attacks …… Big Data

Size, growth, & accuracy of Threat Data



2006 Hobby Storage	2007 Geek Level Storage	2008 Super-Geek Storage	2009 Small Business Class Storage	2010-2011 Business Class Storage	201x Enterprise Class Storage
250gb of Data	1tb of Data	10tb of Data	50tb of Data	500tb of Data	2pb of Data
Dozens of Events per day	Thousands of Events per day	100k of Events per day	Millions of Events per day	Billions of Events per day	Trillions of Events per day
Megabytes of Data each week	Megabytes of Data each day	Megabytes of Data each hour	100's Megabytes Data each hour	Gigabytes of Data each hour	100's Gigabytes Data each hour
	1.2gb in Reports	9.9gb in Reports	456gb in Reports	5tb in Reports	20tb in Reports
Limited Structure	Directory sorting Some RDBMS	Everything in RDBMS	Many RDBMS Systems	Many RDBMS Systems and Large Distributed Storage Systems	Many Large Distributed Storage Systems And few RDBMS Systems
Directory and File search	Directory and File search and Limited key search	Full Relational search	Full Relational Search within Each RDBMS	Full Relational Search within Each RDBMS Some Map-Reduce	Full Map-Reduce Searches across All Data

Shadowserver

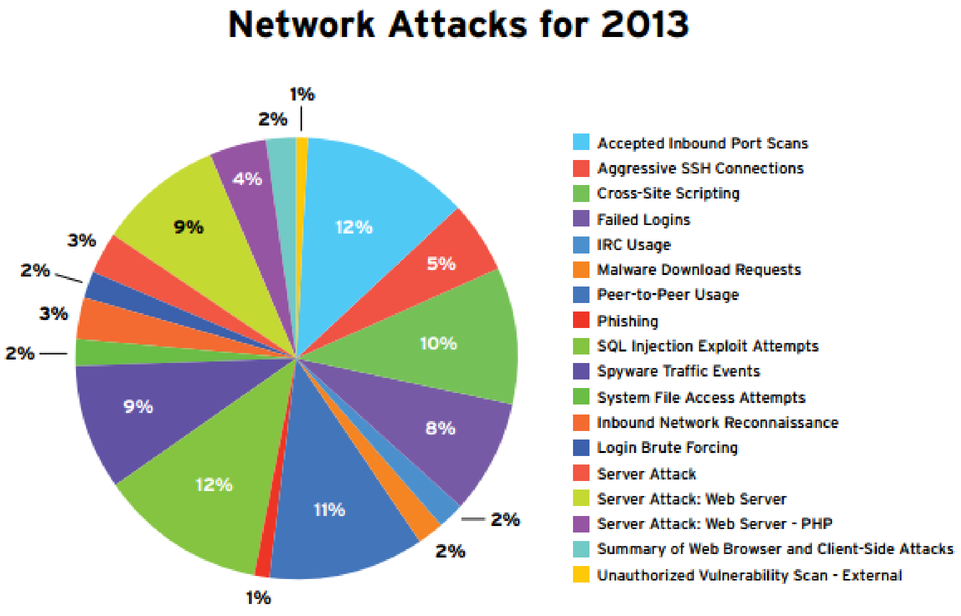
CYBER THREATS - ATTACK OBSERVATION

Based on Attack Traffic (DDoS, etc.)

# ATTACKS / HR	ATTACK ORIGINS	# ATTACKS / HR2	ATTACK TARGETS
4,429	China	11,032	United States
4,240	United States	1,454	Hong Kong
1,143	Mil/Gov	842	Thailand
1,084	Hong Kong	542	Canada
930	Germany	525	Portugal
525	Canada	306	Spain
514	Netherlands	276	Australia
502	Taiwan	265	France
386	Thailand	265	Poland
343	Poland	235	Turkey

# ATTACKS / HR	ATTACKED SERVICE	PORT
1,433	ssh	22
1,246	Domain / DNS	53
565	netbios-dgm	138
824	snmp	161
620	microsoft-ds	445
951	ms-sql-s	1433
572	ms-wbt-server	3389
617	efi-lm	3392

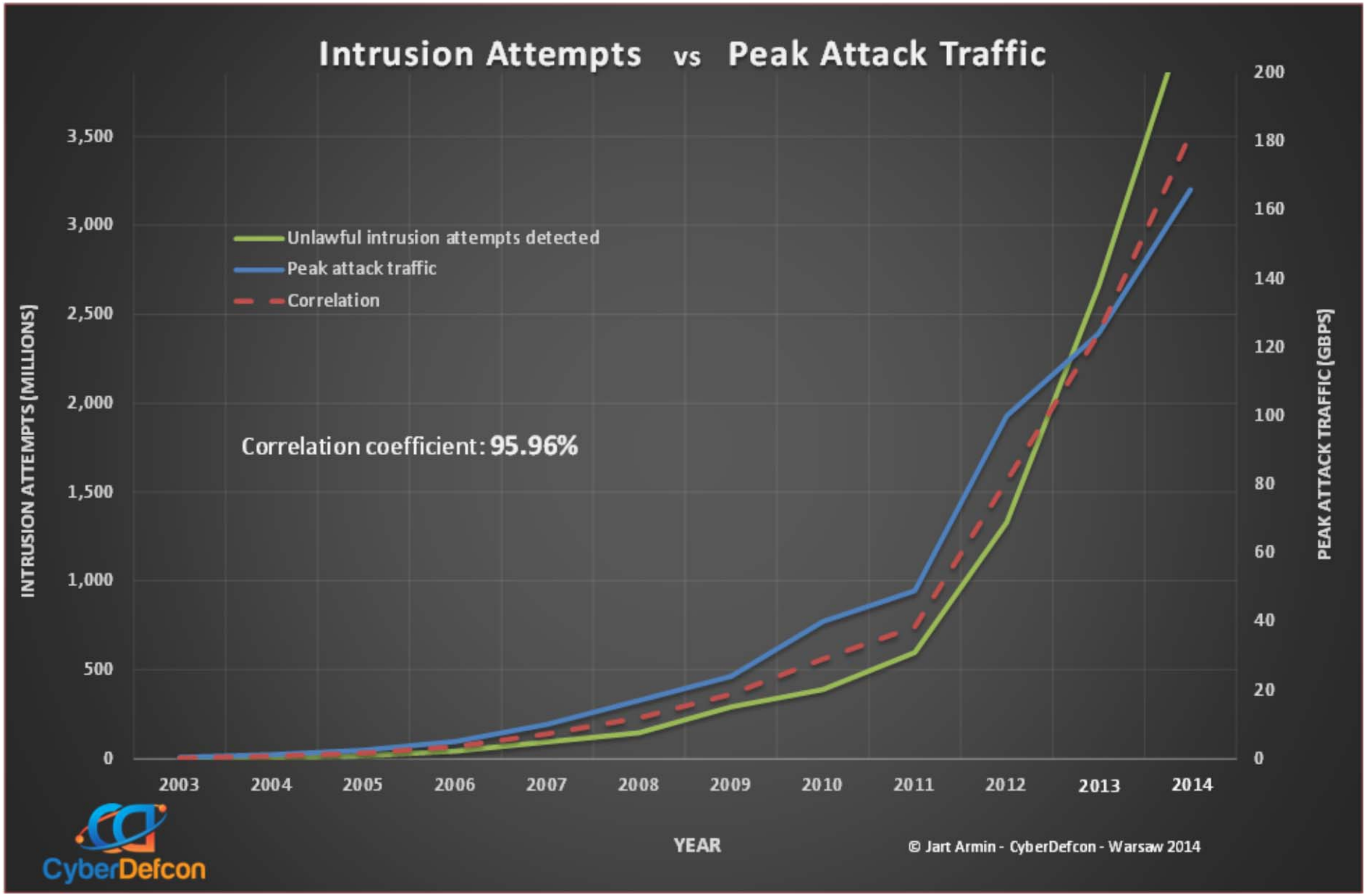
Network Attacks



“Attack traffic,” meaning countries and regions where port probes, worm, malware, viruses, and reflection attacks originate.

Cybercrime? … the results of cybercriminal acts!

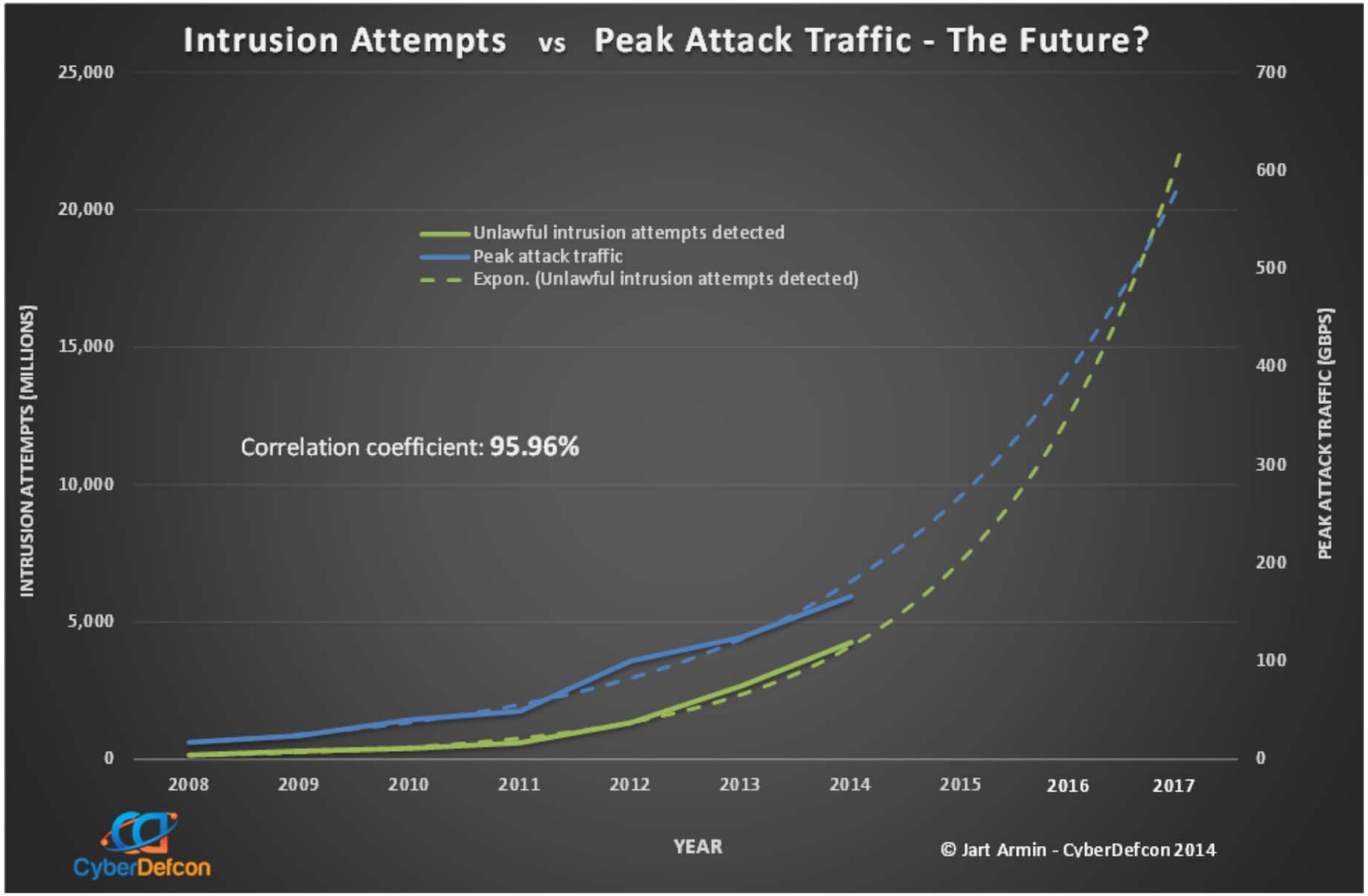
INTRUSION & CYBER ATTACKS - 1



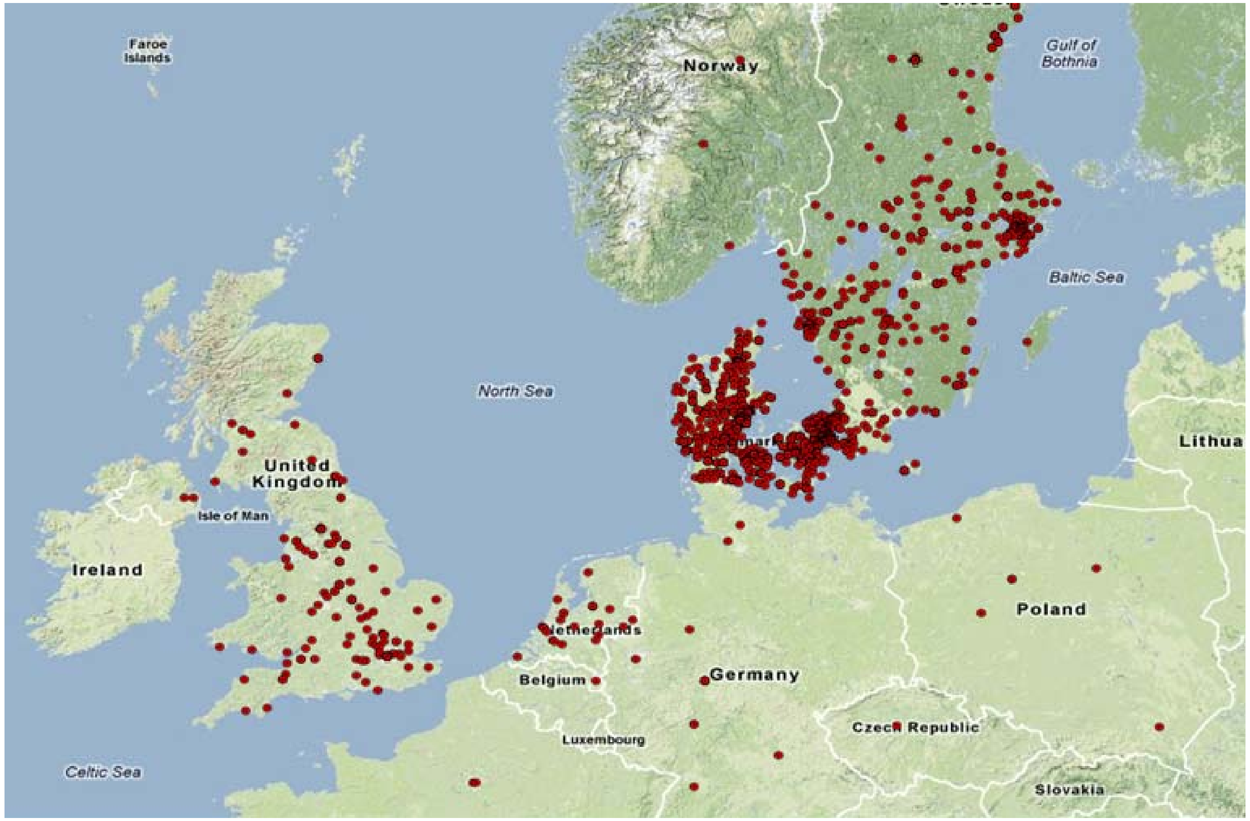
© Jart Armin - CyberDefcon - Warsaw 2014

- Peak attack traffic: 2008 - just over 30 GBPs took out Georgia
- Unlawful intrusion attempts detected: - 2014 - 4+ billion / 2008 – 0.38 billion

INTRUSION & CYBER ATTACKS - 2



- Who or what are the intruders & attackers?
- = probes, botnets, zombies, vulnerability scanners, scrapers, malware, worms, DDoS, reflective traffic via misconfigured open resolvers.



CYBERCRIME METRICS & THREAT DATA (THEORY) – EPIDEMIOLOGY

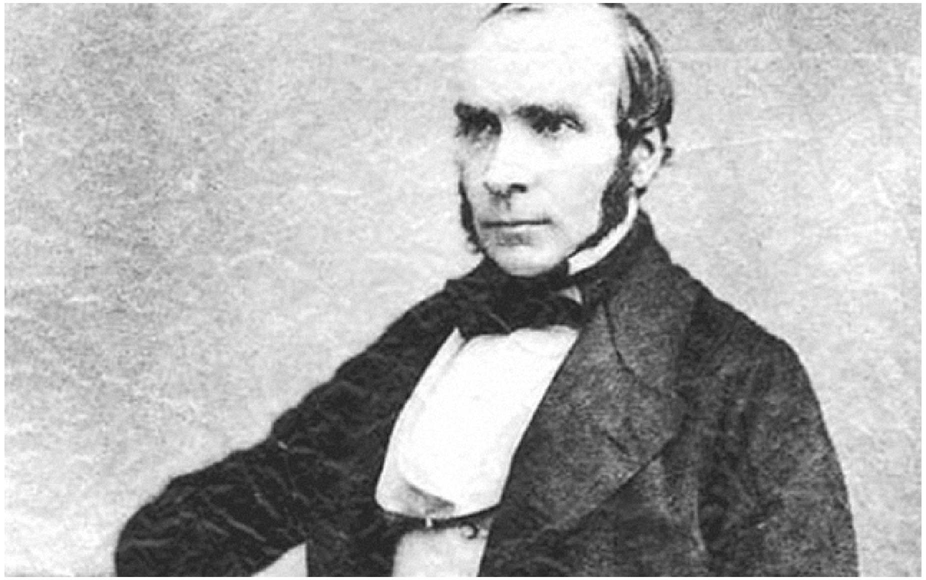
Cholera / Ebola (Disease)

↓

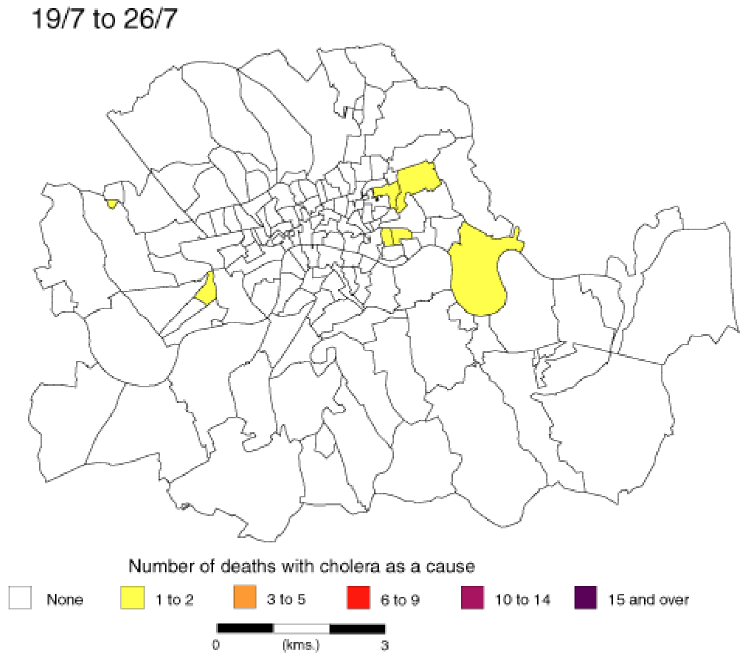
BankTexeasy / Tilon (Banking Malware)

CYBERCRIME & THREAT DATA - EPIDEMIOLOGY

Dr John Snow - Epidemiology



Cholera epidemic of 1854 London

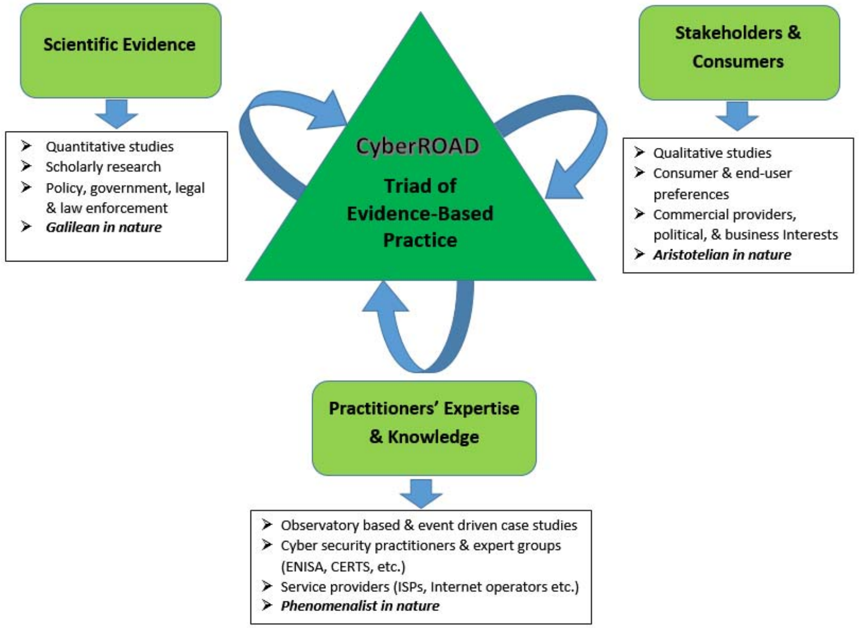


Cybercrime & Cyber Threats – Public Health

- **Epidemiology**: the science that studies the patterns, causes, and effects of health and disease in defined populations.
- Cholera, Bubonic Plague, Aids, Ebola!
- Stuxnet, Zeus, Conficker, BlackEnergy…. + DDoS, Spam…
- Cybercrime & Cyber Threats = the public health analogy – an epidemiological approach. – i.e. patterns & causes
- Just to note: The science of: Public health & epidemiology = >150 years – Cybercrime & Threat Data research = < 10 years
- Policy decisions and evidence-based practice by identifying threats and targets for prevention.
- “All cybercrime, cyber threats are hosted or routed from somewhere and by someone on the Internet”

Cybercrime Data – The Model of Evidence Based Practice

Triad of Evidence-Based Practice for Cybercrime & Threat Data



Scientific Evidence

- Quantitative studies
- Scholarly research
- Policy, government, legal & law enforcement
- ***Galilean in nature***

CyberROAD

Triad of Evidence-Based Practice

Stakeholders & Consumers

- Qualitative studies
- Consumer & end-user preferences
- Commercial providers, political, & business Interests
- ***Aristotelian in nature***

Practitioners' Expertise & Knowledge

- Observatory based & event driven case studies
- Cyber security practitioners & expert groups (ENISA, CERTS, etc.)
- Service providers (ISPs, Internet operators etc.)
- ***Phenomenalist in nature***

A methodological approach

- ***CyberROAD Triad of evidence-based practice***
- to validate all the choices made in cybercrime metrics and threat data
- on the basis of the **available data and interaction of the data** coming from:
  - A. scientific evidence
  - B. practitioners and expertise knowledge (e.g., industry)
  - C. stakeholders and consumers
- This is useful for:
  - D. guaranteeing that the underlying assumptions agree with the available evidence
  - E. defining precise metrics
- Long-term goal of the proposed methodology: making the fight against cybercrime and cyber threats an **empirical science**

Threat Data and Analysis…… Big Data

“Prevention of the disease is better than treatment **or** control”

Security information and event management (SIEM):

- Essentially: gathers, analyses and presents information from network and security devices (log file management and analysis);

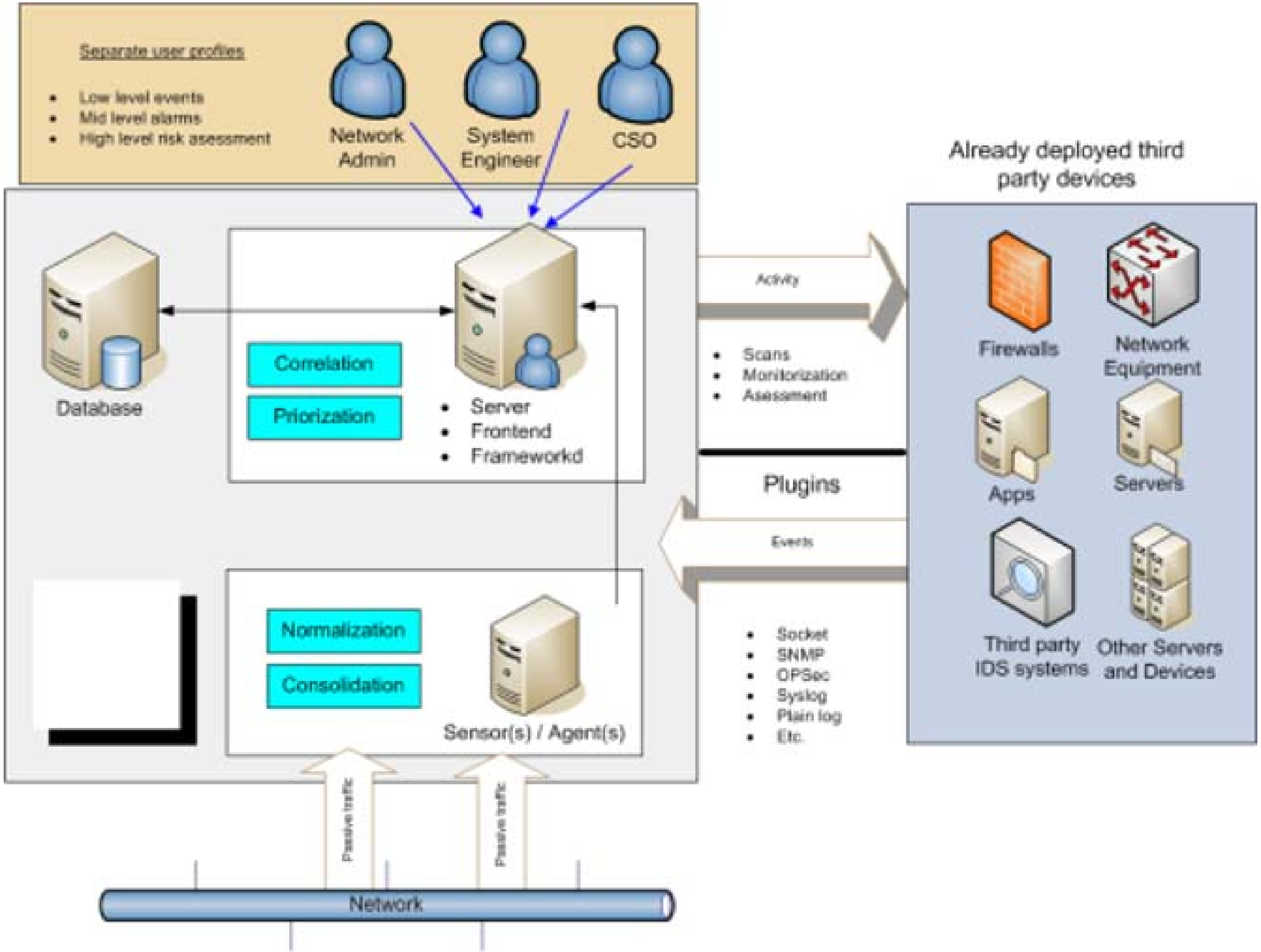
Functions:

- Identity and access management applications
- vulnerability management and policy compliance tools
- operating system, database and application logs
- external threat data

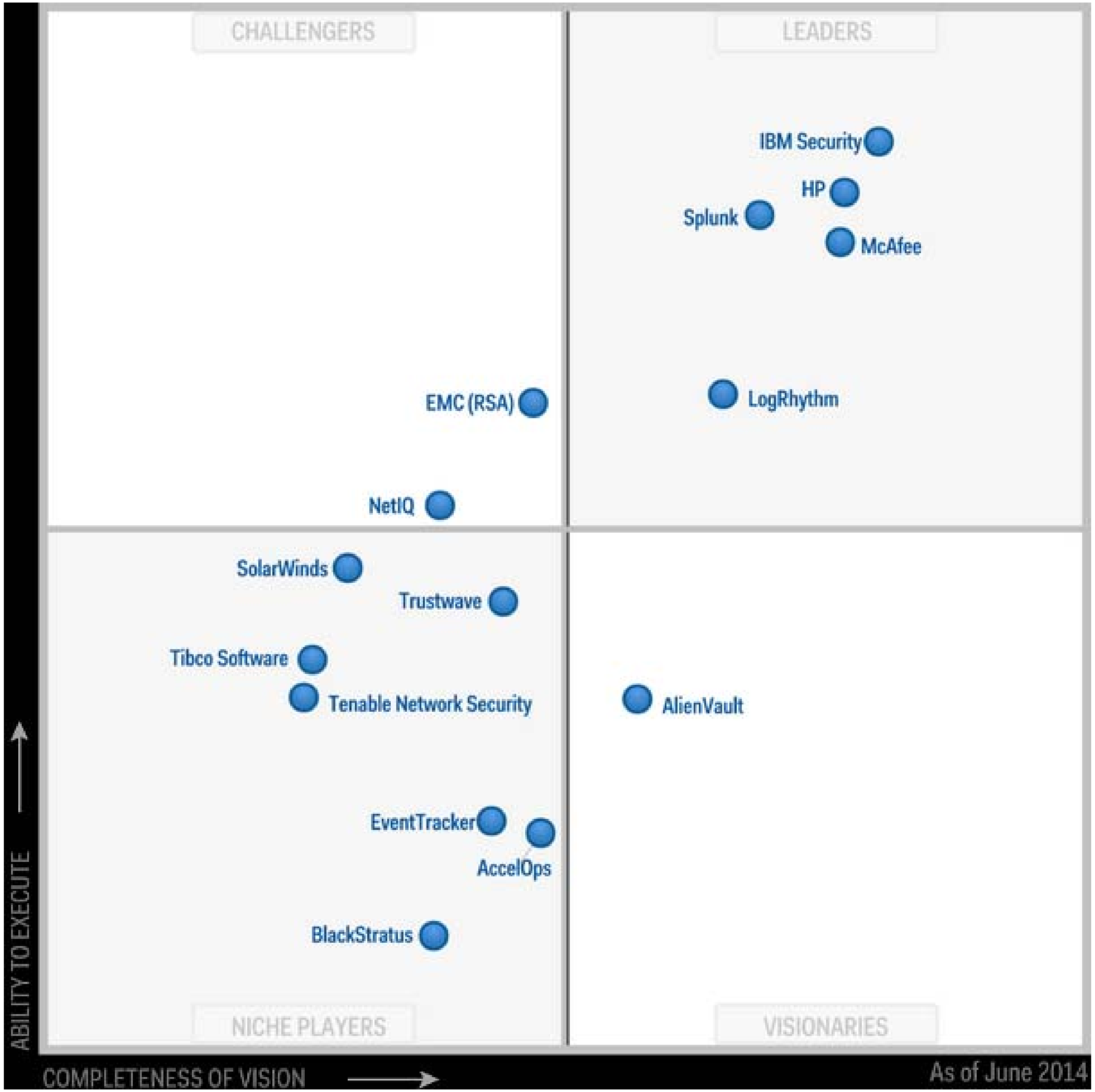
Abilities:

- Interfaces & dashboards – management reporting
- Alerts
- Provides for forensic analysis
- Aggregation of data from many sources
- Auditing
- Internal & external 3rd party compliance

Security information and event management - Deployment



SIEM – Main Players

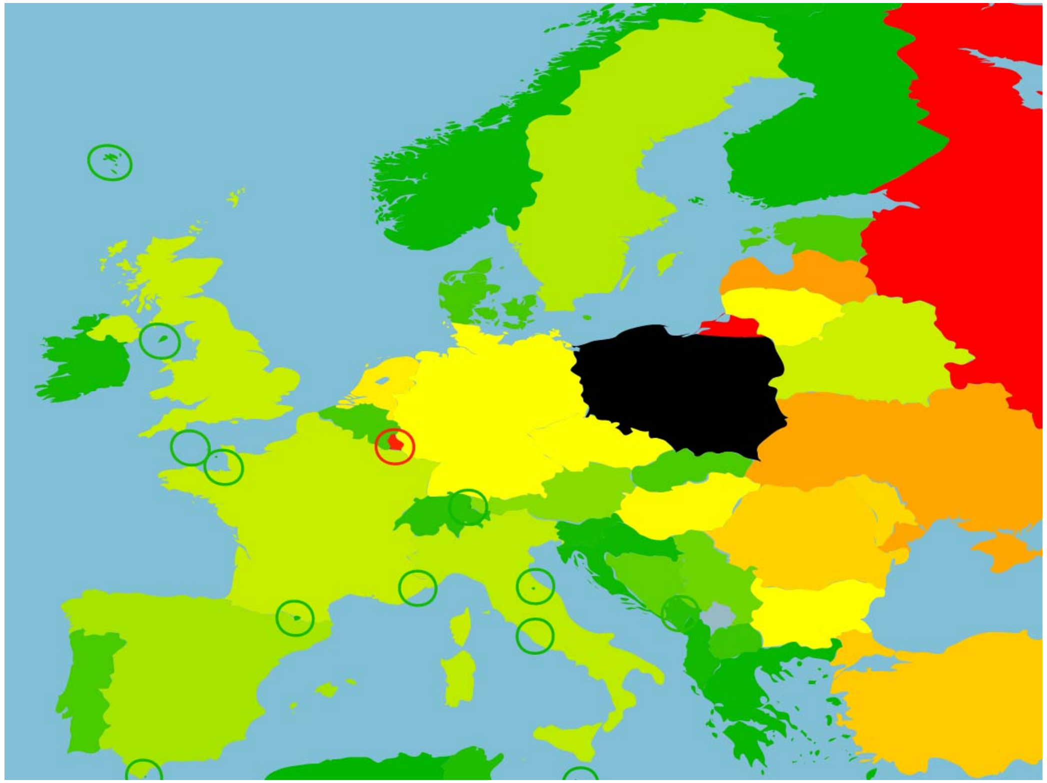


Gartner

SIEM & BEYOND

- Independent evidence shows those applying SIEM or similar solutions are less likely to suffer data breaches.
- Insider threats are 55% of all cybercrime costs per (large) organization – SIEM users reduced the incidence of insider threats
- BYOD – modern SIEM solutions reduce threats from end user's own devices.
- More reliable & secure use of external cloud storage

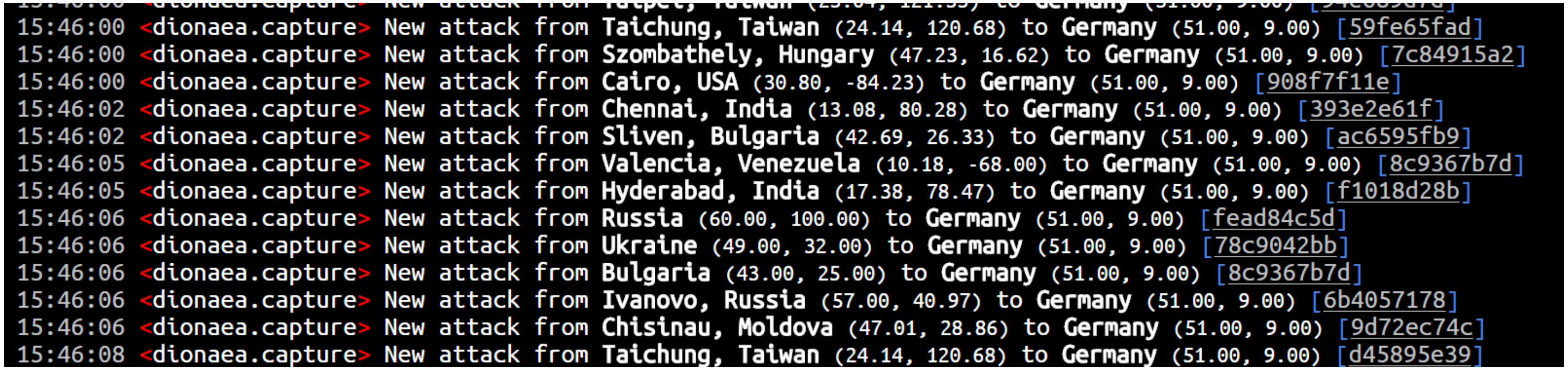
- Big data issue….
- Still ultimately dependent on external threat data for effectiveness
- SIEM can not account for financial data that could help with fraud detection.
- Increased need also for human resource information, metadata about the business, or social media input
- Expensive & cost prohibitive for smaller enterprises
- D.I.Y. Open Source SIEM – e.g. SANS Institute
- Good hackers can still bypass the defences, spoof logs, & audit trail (several major recent examples)



Trending: Threat mapping – Routing and Traffic Reputation – Using the Observatory

CyberDefcon

The Hosting Provider's Problem



```
15:46:00 <dionaea.capture> New attack from Taipei, Taiwan (25.04, 121.53) to Germany (51.00, 9.00) [illegible]
15:46:00 <dionaea.capture> New attack from Taichung, Taiwan (24.14, 120.68) to Germany (51.00, 9.00) [59fe65fad]
15:46:00 <dionaea.capture> New attack from Szombathely, Hungary (47.23, 16.62) to Germany (51.00, 9.00) [7c84915a2]
15:46:00 <dionaea.capture> New attack from Cairo, USA (30.80, -84.23) to Germany (51.00, 9.00) [908f7f11e]
15:46:02 <dionaea.capture> New attack from Chennai, India (13.08, 80.28) to Germany (51.00, 9.00) [393e2e61f]
15:46:02 <dionaea.capture> New attack from Sliven, Bulgaria (42.69, 26.33) to Germany (51.00, 9.00) [ac6595fb9]
15:46:05 <dionaea.capture> New attack from Valencia, Venezuela (10.18, -68.00) to Germany (51.00, 9.00) [8c9367b7d]
15:46:05 <dionaea.capture> New attack from Hyderabad, India (17.38, 78.47) to Germany (51.00, 9.00) [f1018d28b]
15:46:06 <dionaea.capture> New attack from Russia (60.00, 100.00) to Germany (51.00, 9.00) [fead84c5d]
15:46:06 <dionaea.capture> New attack from Ukraine (49.00, 32.00) to Germany (51.00, 9.00) [78c9042bb]
15:46:06 <dionaea.capture> New attack from Bulgaria (43.00, 25.00) to Germany (51.00, 9.00) [8c9367b7d]
15:46:06 <dionaea.capture> New attack from Ivanovo, Russia (57.00, 40.97) to Germany (51.00, 9.00) [6b4057178]
15:46:06 <dionaea.capture> New attack from Chisinau, Moldova (47.01, 28.86) to Germany (51.00, 9.00) [9d72ec74c]
15:46:08 <dionaea.capture> New attack from Taichung, Taiwan (24.14, 120.68) to Germany (51.00, 9.00) [d45895e39]
```

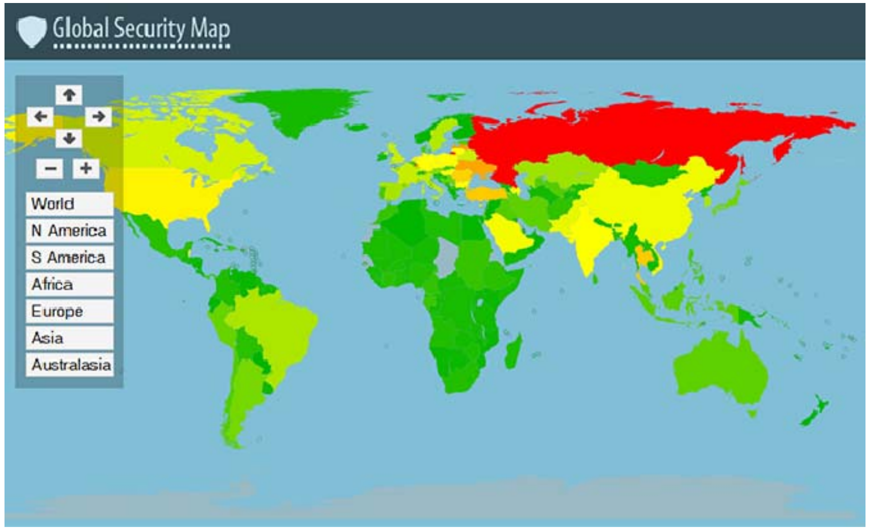
Large ISPs & Telecoms deal with **thousands** of cases of abuse per day

- *Recent analysis with several EU telecoms large %age of traffic malicious or noise*
- *How do they* ***prioritise*** *and filter out the "noise"?*
- *How do they get an* ***objective picture*** *of how clean their servers are?*
- *Prioritize on reputation!*

Reputational Index

Country	Name	ASes	IPs	Rank	Index
CY	CYPRUS	55	1,944,832	216	18.0
	Highest sector	Zeus botnets		1	512.6
	2nd-highest sector	Current events		21	238.3
	3rd-highest sector	Spam		204	32.1
BY	BELARUS	78	2,130,944	6	287.9
	Highest sector	Spam		3	560.2
	2nd-highest sector	Zeus botnets		2	502.4
	3rd-highest sector	Botnet C&Cs		2	375.1
VG	VIRGIN ISLANDS, BRITISH	7	24,320	2	442.8
	Highest sector	Botnet C&Cs		1	901.1
	2nd-highest sector	Phishing		1	874.1
	3rd-highest sector	Current events		1	821.3
PL	POLAND	1,640	22,498,624	4	323.9
	Highest sector	Current events		2	770.9
	2nd-highest sector	Phishing		4	486.0
	3rd-highest sector	Zeus botnets		4	461.3

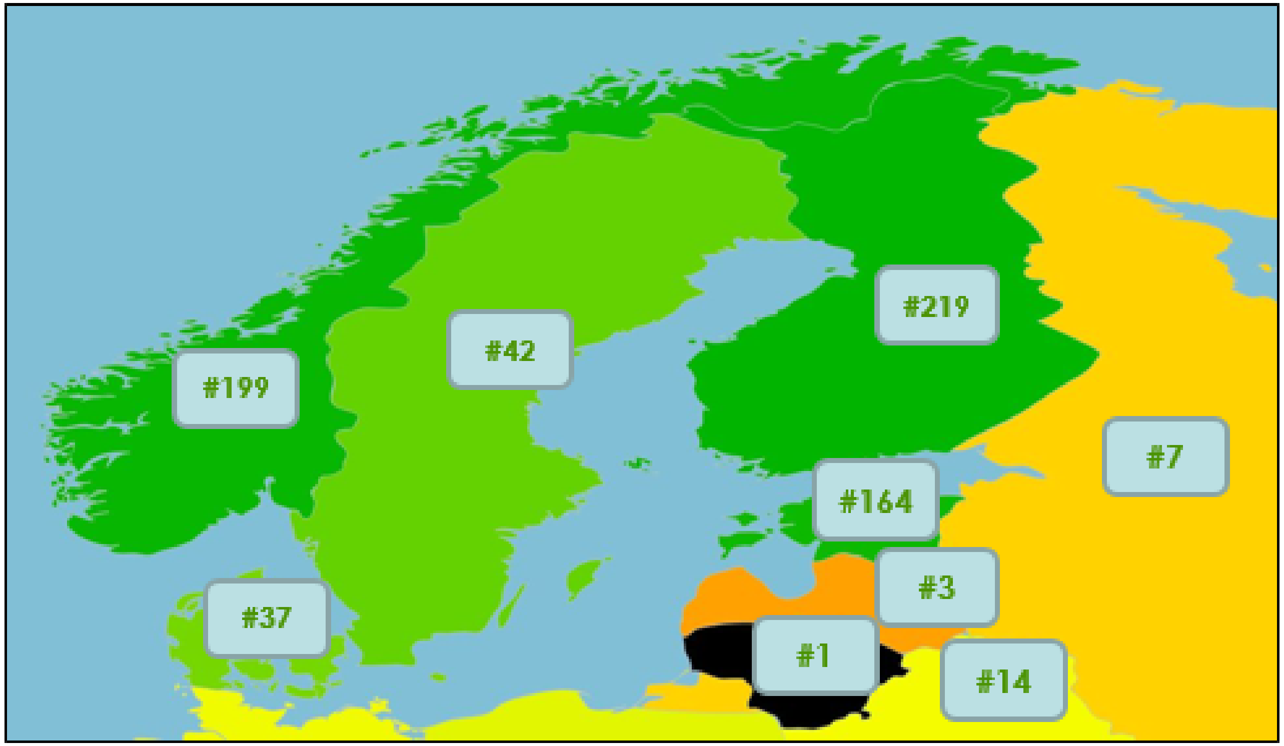
Countries can be scored too



- Making it easy to choose which traffic to route with or accept
- Stop the bad traffic at the boundary
- Hybrid: DPI, event reporting, open data

CyberDefcon

Reputational Indexing



Out of 222:

1 – Lithuania

3 – Latvia

#164 – Estonia

#14 – Belarus

7 – Russian Federation

37 – Denmark

42 – Sweden

199 – Norway

219 - Finland

Once observed – why such a difference between countries ?

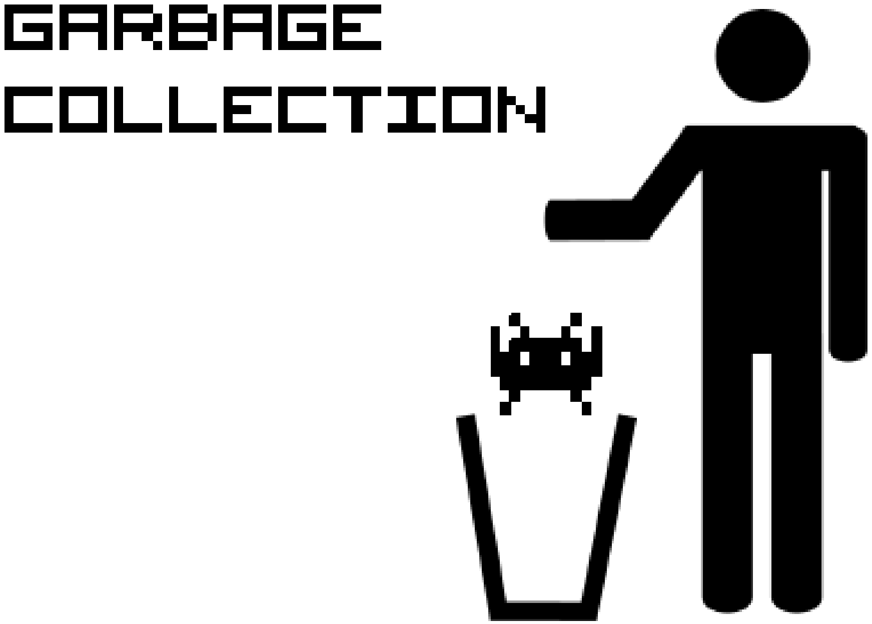
REPUTATIONAL INDEXING

#	Country	HE Index
1	Russian Federation	359.3
2	Luxembourg	315.6
3	Latvia	255.8
4	Ukraine	251.4
5	Virgin Islands, British	247.1
6	Thailand	233.9
7	Turkey	233.7
8	Romania	229.5
9	Moldova, Republic of	225.5
10	Netherlands	209.7
11	Cyprus	208.2
12	United States	203.1
13	Viet Nam	202.8
14	Hungary	195.1
15	Poland	186.7
16	Bulgaria	179.1
17	Lithuania	175.5
18	Czech Republic	174.3
19	India	172.7
20	Germany	171.4

Poland	HE-index
Global HE rank:	#15 of 219
Overall HE index:	186.7
IP transit:	7,485,696
IP originate:	21,301,248
Spam	104
Malware	293.7
Badware	176.1
Botnets	136.9
Phishing	99.4
Data breaches	???
Cybercrime hubs	595.5
Current events	185.4

ASN Poland - Top 5 (1 YEAR)	# sites scanned	# sites hosting malware
home.pl sp. z o.o. (12824)	122,926	8,844 (7%)
nazwa.pl (15967)	67,164	3,732 (6%)
Grupa Onet.pl (12990)	22,010	843 (4%)
Krakowskie e-Centrum Informatyczne JUMP (29522)	27,583	1,014 (4%)
INTERIA.PL Sp z.o.o. (16138)	20,244	611 (3%)

Google



R&D Project: Cleaning up the Garbage in Cyber Space – why?

“The cleaner a nation’s national cyberspace, less attacks on its national infrastructure & lower numbers of cybercrime victims”

Considerations for Our Digital Future?

What?

- Cybercrime define? (starting point: Budapest Convention on Cybercrime)
- Quantification, what are the metrics? What are we dealing with?
- Policies e.g. 'personal data breaches'. Under the revised ePrivacy Directive (2009/136/EC) - telecoms operators and ISP… why not other enterprises?
- Not just keep building walls, we need strategies to remove the threats
- What is the research agenda for defeating cybercrime & cyber threats?

The garbage?

- Infrastructure: Misconfigured, outdated systems, open resolvers - Updating the systems a legal responsibility?
- Tools: Botnets & the Zombies
- Threats: worms, viruses,….

Cleaning up the garbage who is responsible?

World Hosts Report

New "World Hosts Report" available Monday November 3rd 2014

- From www.hostexploit.com
- Reports on all 52,000 ASNs
- Malware, spam, phishing, botnets etc
- Country analysis
- Latest trends
- Upcoming threats

HostExploit's

World Hosts Report

November 2014

Announcement

New Methodology

The HE Index, introduced in December 2009, has become a widely-used metric in the industry for tracking cybercrime and assigning reputations to Autonomous Systems.

HostExploit is pleased to announce a new methodology that enables greater accuracy of data, higher granularity and many more features.

Alongside the new methodology, the following services will be upgraded:

HostExploit

- New website with easier access to archived reports
- Blocklists and other host tools

SiteVet

- New website with members' features
- Higher granularity, from Country level all the way down to Domains and URLs

ISBN 978-0-9838249-6-7

Jart Armin: jart@cyberdefcon.com

References - http://jart.me/jart_sec2014

CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND
CYBER-TERRORISM RESEARCH ROADMAP

No reproduction or use of these slides or content without authors written permission

Questions?

APWG

Unifying the
Global Response
to Cybercrime

a
CYBERDEFCON
service

SWEPT

ACDC

CyberDefcon