Grant Thornton

An instinct for growth™

Computer Forensics: Too Much to Do Too Little Time!

Vijay Rathour – Digital Forensics

Agenda

1. Cyber Attacks – It's Already Too Late
2. Reacting to a Breach
3. Log Analysis
4. Event Investigation
5. Code Analysis
6. Objective and Subjective Risk
7. Hints and Tips

Tails of the (Un)Expected

Cyber Attacks – The Expected Unexpected

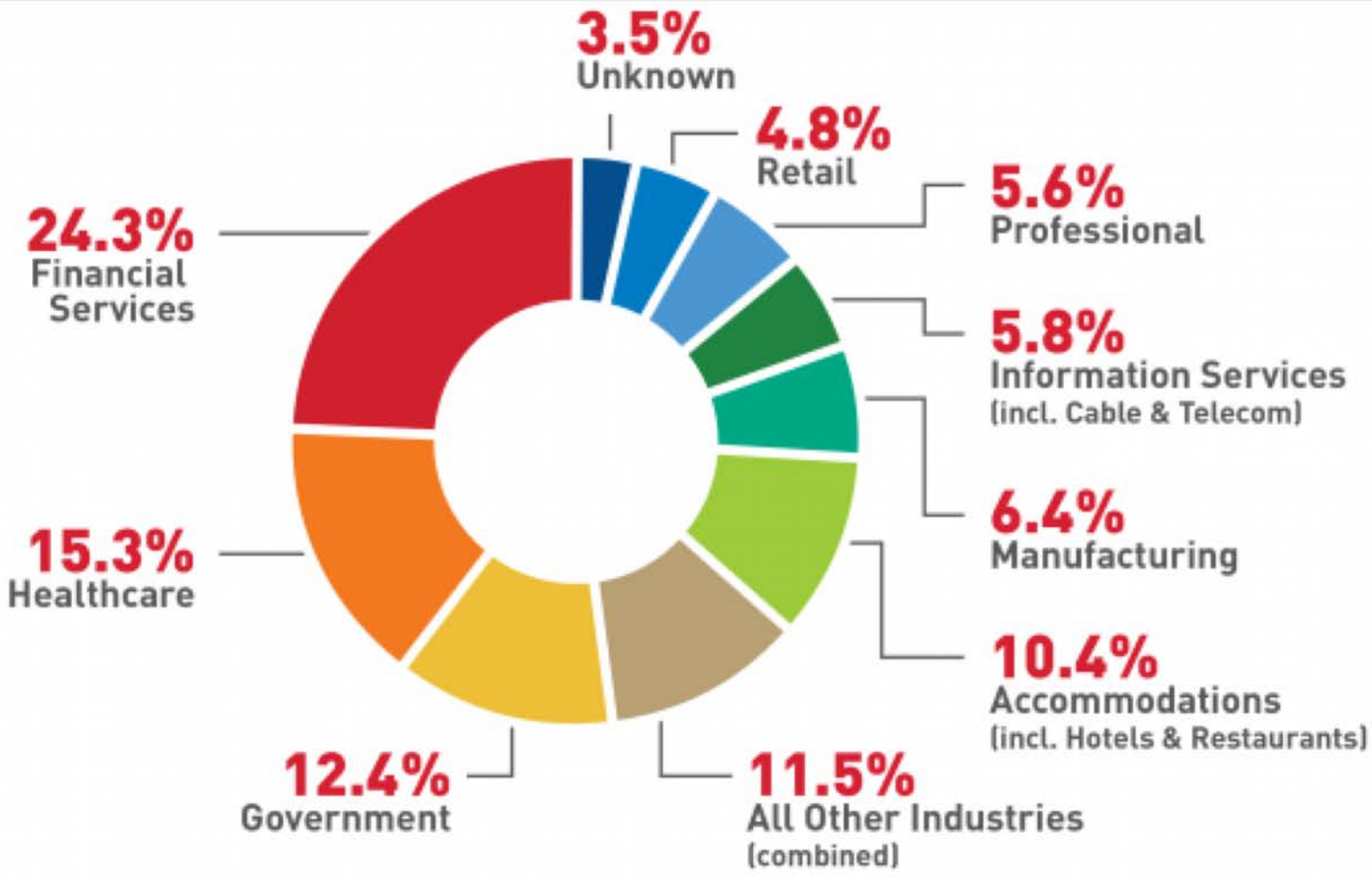
© BBC

Cyber Attacks – Spilt Milk

Average breach cost £2.4m	Attacks completed in minutes 60%	Attacks spread to second victim in one hour 40%	Time to detect a breach 191 Days	Time to contain a breach 66 Days
Average cost per record breached £126	Annual cost of handling phishing £2.5m	Recipients opening phishing messages 60%	Recipients clicking phishing attachments 11%	Recipients clicking phishing links within 1 hour 50%
Exploited vulnerabilities older than 1 year 99.9%	New vulnerabilities exploited within 2 weeks 50%	Malware samples unique to target 70-90%	Organised crime attacks using crimeware 73%	Activist attacks targeting web applications 61%

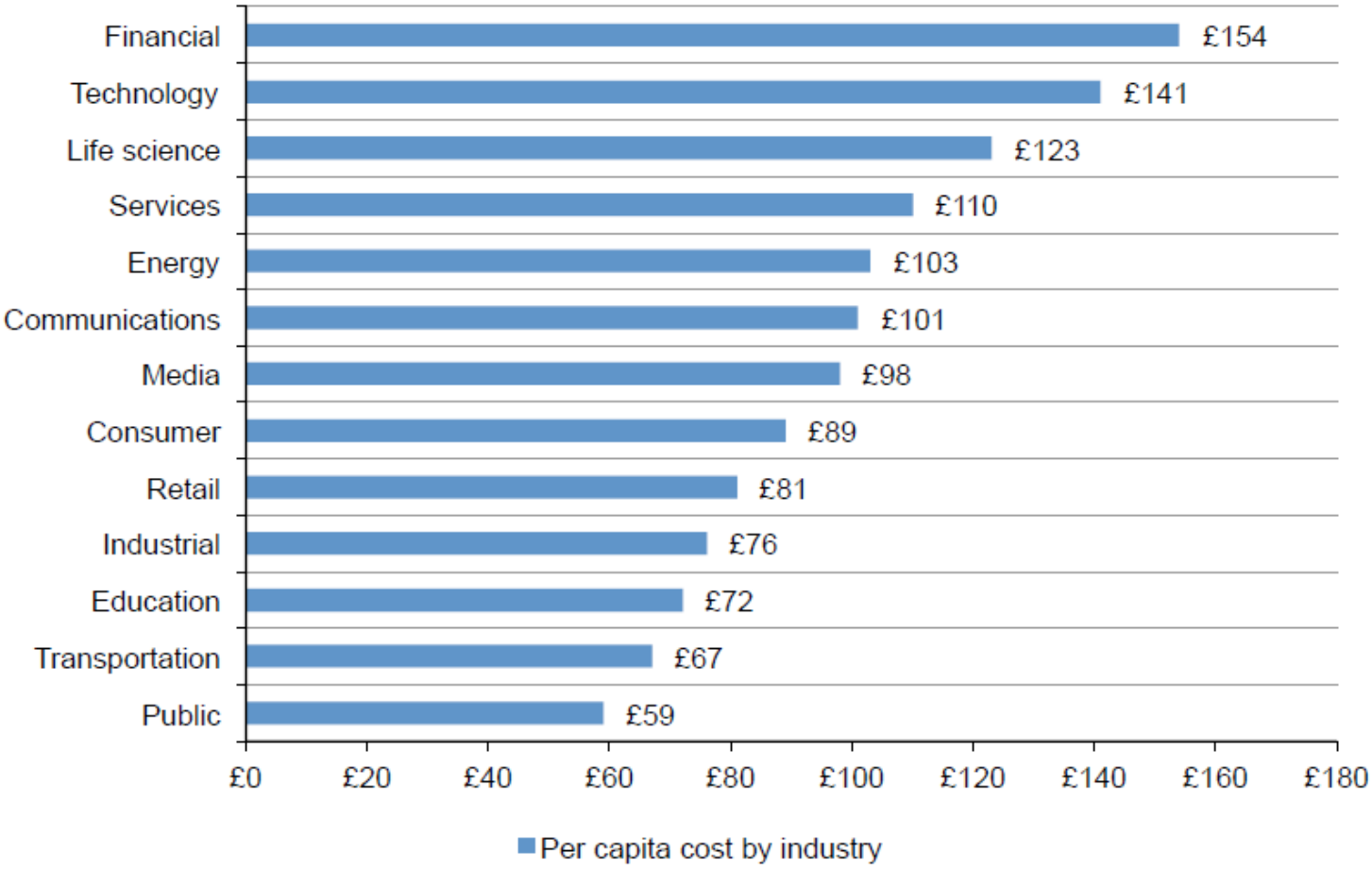
No sector is safe

Notable increase in threats against key industries



Source: Verizon 2017 Data Breach Investigations Report

Cost of a Data Breach – per record lost



Ponemon - 2017 Cost of Data Breach Study

Attack Vectors are Evolving

62%
of breaches featured hacking.

51%
over half of breaches included malware.

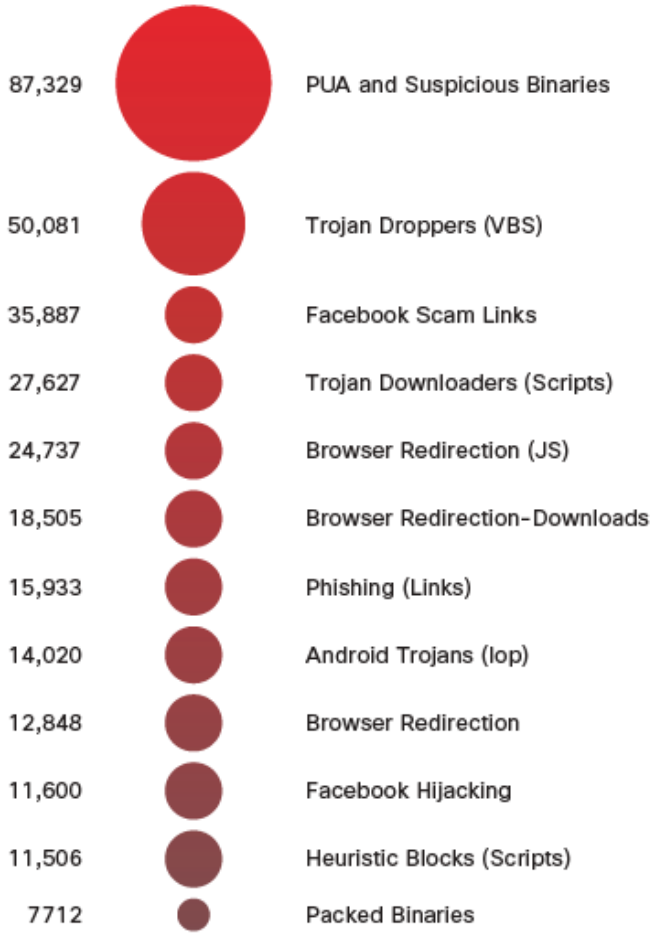
81%
of hacking-related breaches leveraged either stolen and/or weak passwords.

43%
were social attacks.

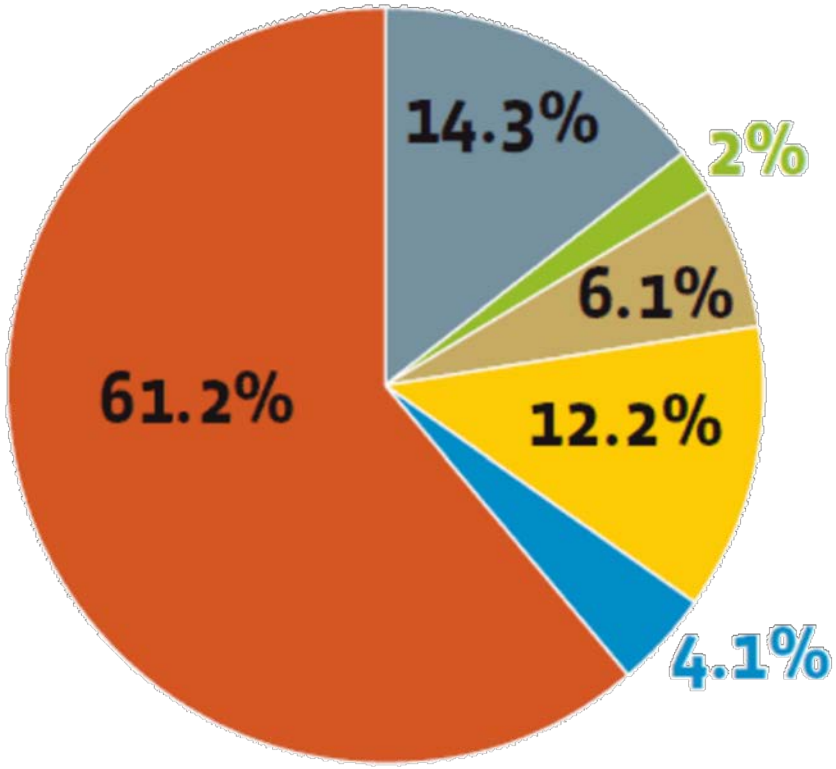
14%
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8%
Physical actions were present in 8% of breaches.

Verizon Report



Human Threats – Training May not be Enough



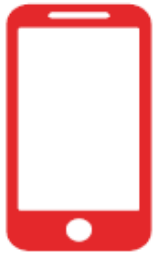
*Numbers don't add to 100 percent because of rounding.

PRIMARY METRICS FOR MEASURING SUCCESS OF AWARENESS PROGRAMS

- Percentage of users completing training.
- Percentage of users covered through at least one awareness initiative.
- Year-over-year reduction in specific types of incidents caused primarily by user error.
- User understanding of security (evidenced by surveys).
- User propensity to behave securely (evidenced by fake phishing attacks and other techniques).
- Other.

Source: Information Risk Executive Council research

Broadened Attack Surface



Mobile Devices

Data in Public Cloud

Cloud Infrastructure

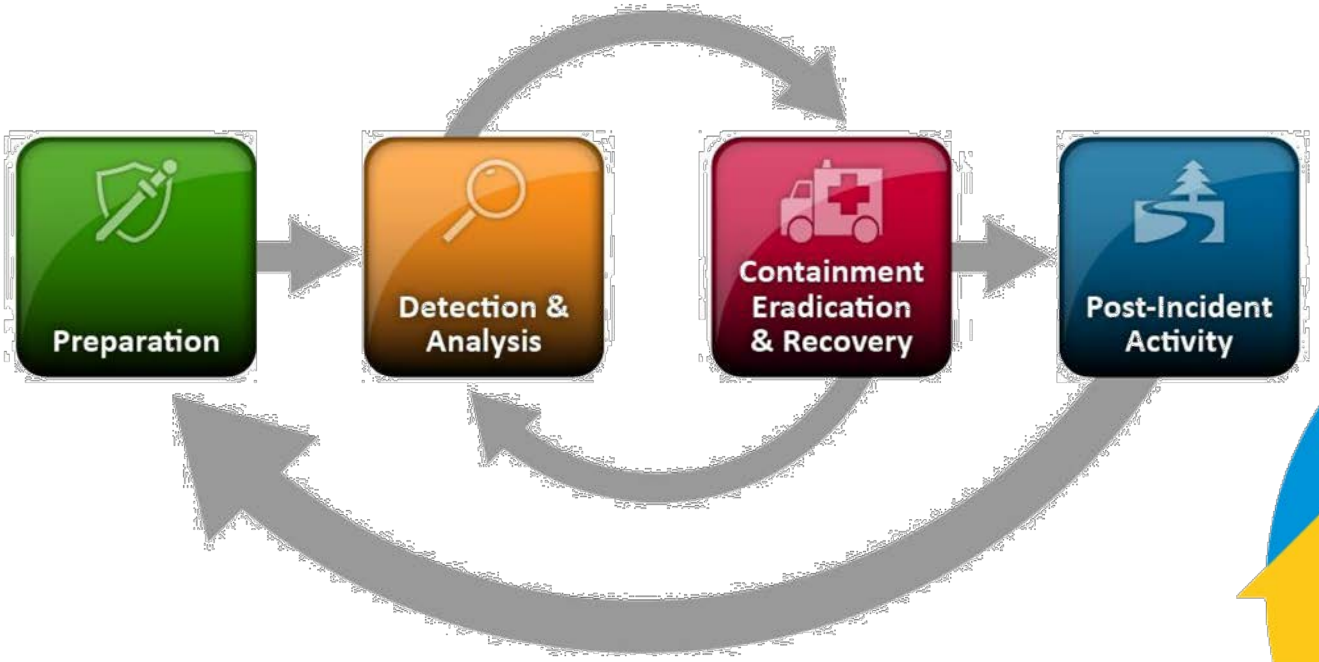
User Behavior
(For Example, Clicking Malicious Links in Email or Websites)

Reacting to a Breach

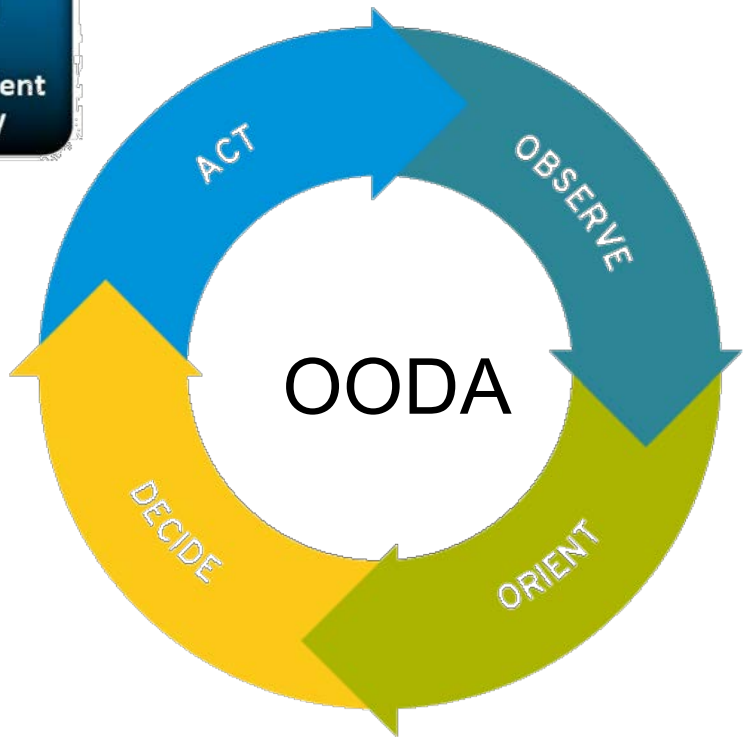
Data Breach Mitigation – Before the Event

- Audit
- Data mapping
- Adequate security controls and penetration testing
- Related policies and procedures
- Cyber insurance
- Breach response team, procedure and contingencies
- Dress rehearsal/ scenario testing

Computer Security Incident Handling Protocols



NIST



Timeline – day of incident, + day 1

Day of Breach

am:

- Customer services notified by customer of breach
- In-house compliance, legal and IT functions all notified
- **IT takes immediate action to secure the data** – note decision on forensics required*
- Insurance

pm:

- Initial estimate suggests that data relating to over [X] data subjects/3rd parties were released
- In-house legal/compliance contacts external counsel
- Preliminary assessment begins

BD +1

- External legal advisers appointed
- External IT security specialists instructed
- External PR and Communications advisors instructed
- **Core breach management team established***
- IT team verify that all data has been removed from the public domain
- Immediate assessment of notification requirements
- **Initial Notifications made to ICO (and potentially others**

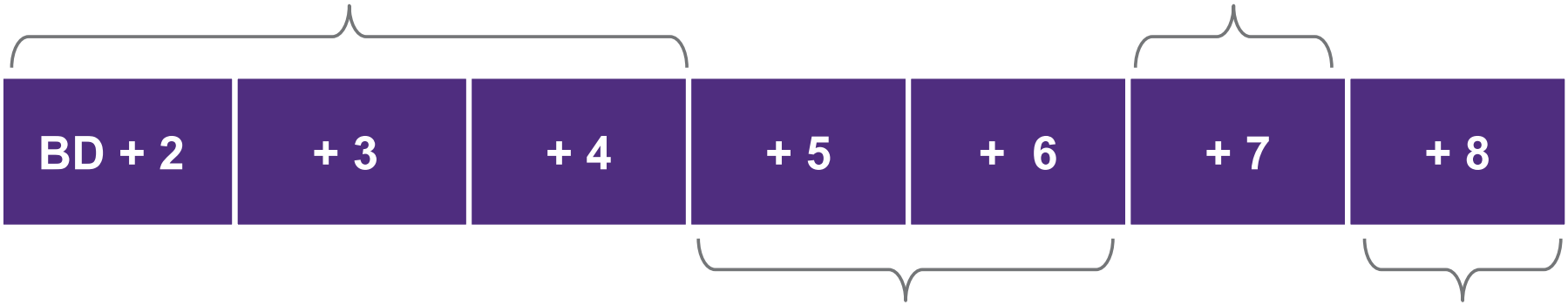
Timeline – first week

BD + 2 - 4

- PR plan formulated and draft statement prepared
- IT security specialists verify that all data is now secure and check all systems for ongoing security.
- Preliminary risk assessment completed
- Assessment made as to whether data subjects should be notified, and **how** to notify

BD + 7

- ICO acknowledges the company's self-reported breach
- A potential new third party service provider is identified and IT specialists perform due diligence



BD + 5 - 6

- Source of the leak is notified, reservation of rights
- Team assesses how data subjects will be handled (helplines; points of contact; assistance required - credit check services for example)
- Team prepare first draft notification letter to be sent to affected data subjects. Insurer given notice and opportunity to comment

BD + 8

- Results of initial investigation are made available and confirm the total amount of data released and other basic facts
- ICO and other applicable regulators updated
- Insurers updated

The Cyber Kill Chain – Complex Movements

ActiveCyber.net

Log Analysis

Event Timeline and Log Analysis

Computer Forensics relies heavily on log analysis:

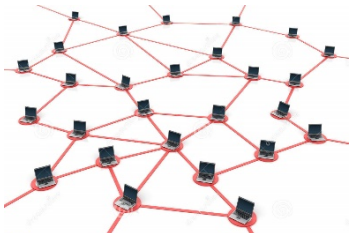
- To help understand what occurred
- When did it happen?
- What systems have been impacted?
- Is the attack over?

Preparation for a breach requires careful consideration

- The amount of logging data (how far back)
- How rich is the logging? (too much/too little)
- Notification Fatigue

Accelerated Log Analysis Tools

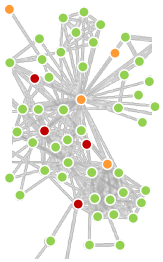
Customer Network History



Have threats been present on the network over the last 12 months?

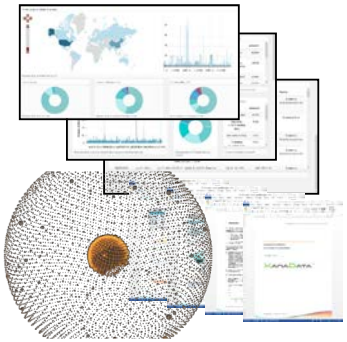
Analyse for Threats

Accelerated Analytics Hardware



Custom Machine Learning & Artificial Intelligence

Comprehensive Threat Landscape



Fast Visualisation, Reporting & Augmented Intelligence

Analysis hardware speeds up security analytics 1000-10,000x

Typical Risk Assessment Dashboard

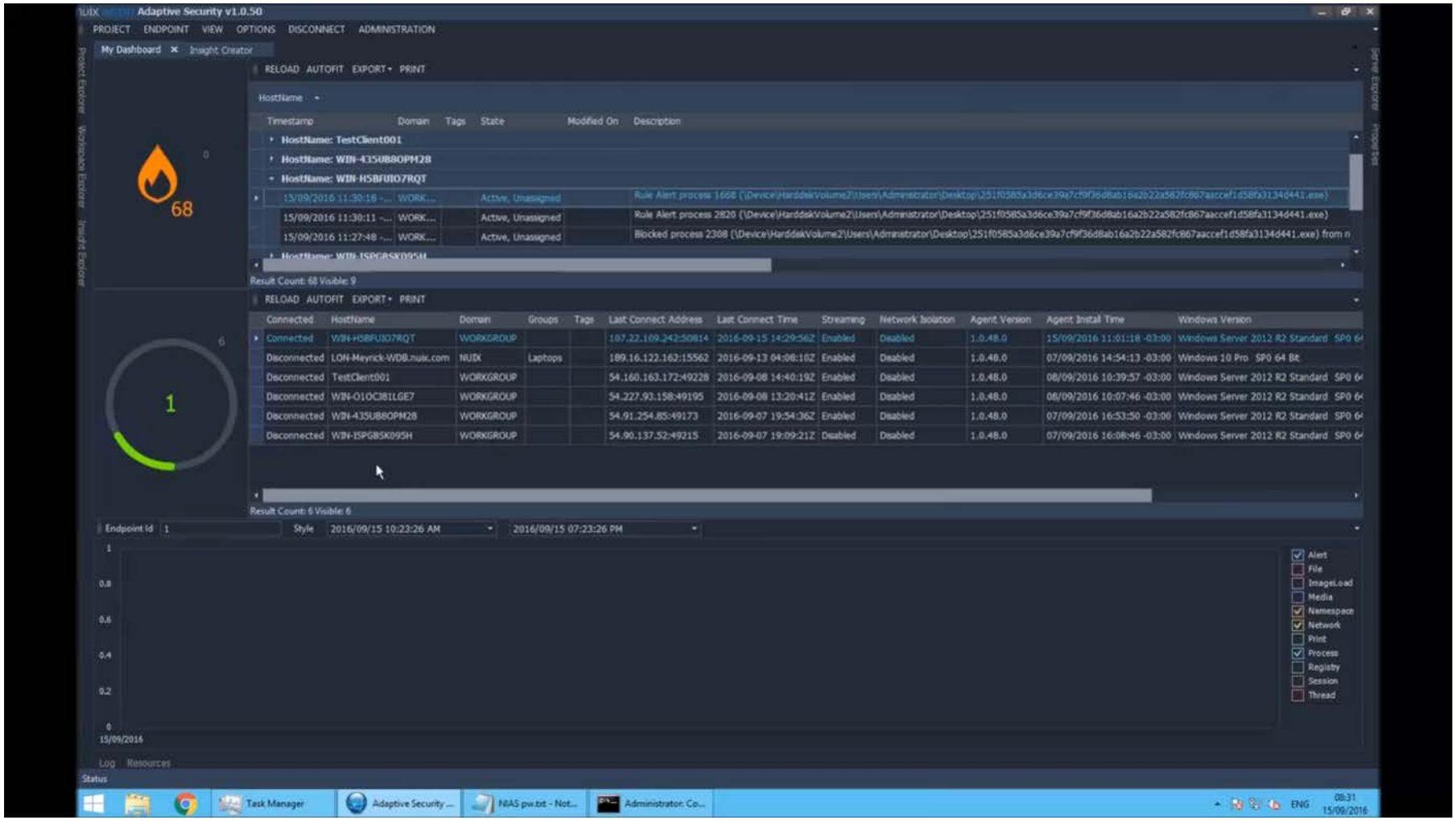
Grant Thornton | An instinct for growth™

Event Investigation

Event Forensics – Analysis Platforms

- **Security intelligence** platform for data breach investigations and forensic analysis
- Processing engine **aggregates information** from thousands of data types at superior speeds
- Data is analysed and correlated in four dimensions—**people, objects, locations and event**s
- Lets you visualise **critical relationships** across a variety of file types with forensic precision

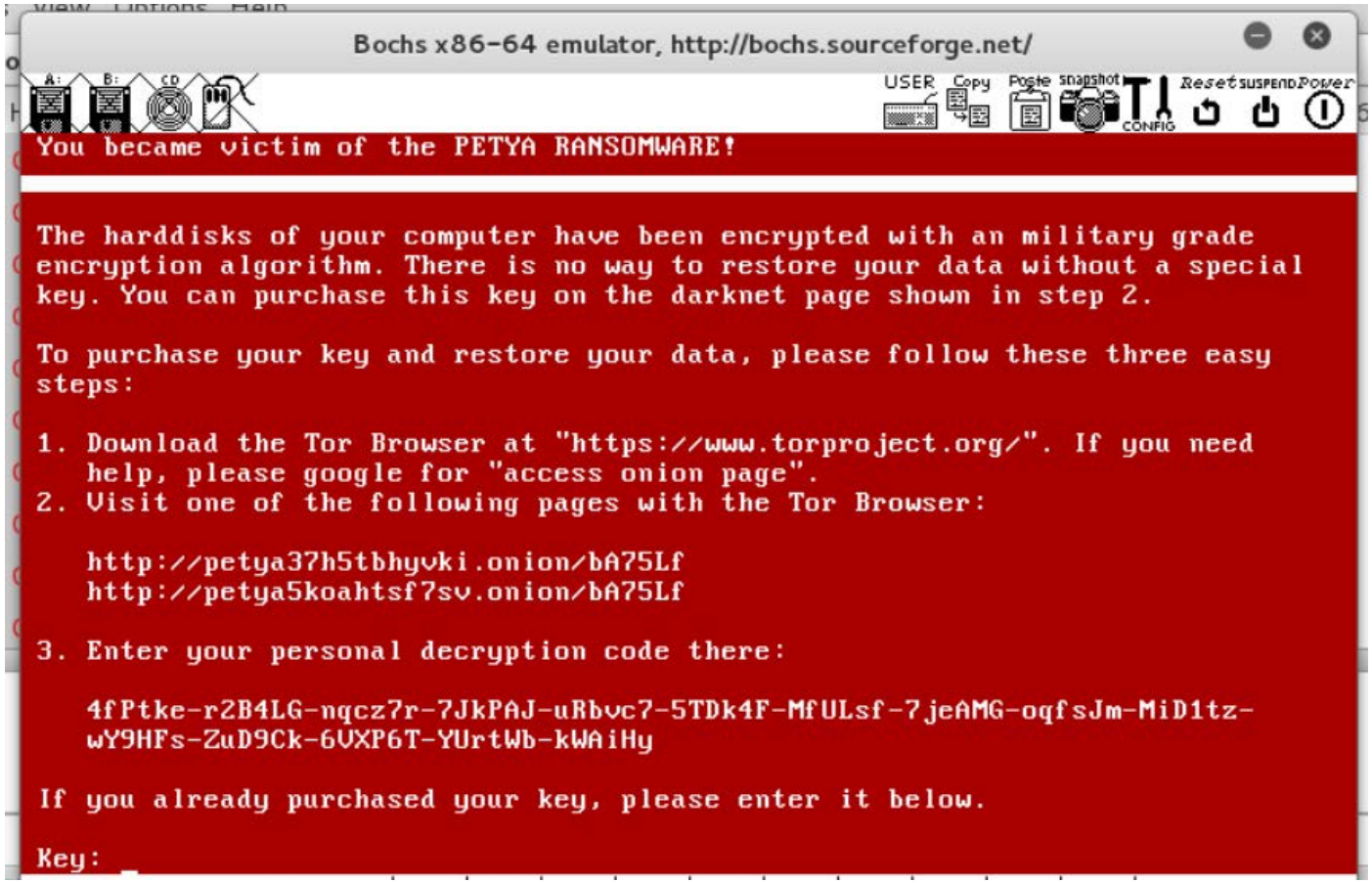
Event Forensics – Analysis Platforms



Code Analysis

Code Analysis

- **Static** and **Dynamic** Analysis
- Petya Analysis
- Sandbox



Dynamic Analysis – Sandboxes / VMs

malwr

770653	68%	274678
Total Analyses	Shared Malware	Unique Domains

Recent Analyses (see more)

Aug. 10, 2017, 6:03 a.m.	e6297c17308c98acfc475916592368a3
Aug. 10, 2017, 6:02 a.m.	17bf398a6b4d951ffce1710ad665bb30
Aug. 10, 2017, 6:01 a.m.	594512b0f2eb19e0f61701a47dc92f82
Aug. 10, 2017, 6 a.m.	428af7fa03ff09ce1cd373abfebad8a3
Aug. 10, 2017, 6 a.m.	322774005cf4f429a7d60736ac6e2697
Aug. 10, 2017, 6 a.m.	84128b0a6bbf984a06312911cfb9c454
Aug. 10, 2017, 6 a.m.	7b81f03c84cefa56ef8519223d72bc2a
Aug. 10, 2017, 5:58 a.m.	0fd841cca0a98c3588e749de84787dbb
Aug. 10, 2017, 5:56 a.m.	dfb5dd011c7e7e151154f04b52721fe2

Recent Domains

www.bing.com
dev.null.vg
scenetavern.win
hallvilla.win
download.cpuid.com
www.piriform.com
www.download.windowsupdate.com
repnytimes.pw
s.pbllib.pw

Dynamic Analysis – Sandboxes / VMs

Signatures

File has been identified by at least one AntiVirus on VirusTotal as malicious

The binary likely contains encrypted or compressed data.

A process attempted to delay the analysis task by a long amount of time.

Installs itself for autorun at Windows startup

Screenshots

Objective & Subjective Risk

Risks are Not Hard to Find

Grant Thornton | An instinct for growth™

Threat Assessment: Pen Testing and Vulnerabilities

Nessus | Scans | Schedules | Policies | Users | smokeymonkey

Basic Test

Export | Audit Trail | Filter Vulnerabilities

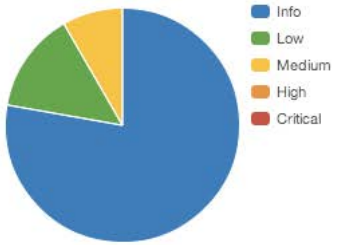
Scans > Hosts 1 | Vulnerabilities 36 | Notes 1 | Hide Details

Severity	Plugin Name	Plugin Family	Count
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Medium Strength Cipher Suites Sup...	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
LOW	SSH Weak MAC Algorithms Enabled	Misc.	1
LOW	SSL Anonymous Cipher Suites Supported	Service detection	1
LOW	SSL Certificate Chain Contains RSA Key...	General	1
LOW	SSL RC4 Cipher Suites Supported	General	1
INFO	Service Detection	Service detection	5
INFO	Nessus SYN scanner	Port scanners	4
INFO	HTTP Methods Allowed (per directory)	Web Servers	2
INFO	HTTP Server Type and Version	Web Servers	2

Scan Details

Name:	Basic Test
Folder:	My Scans
Status:	Completed
Policy:	Basic Test
Targets:	172.31.15.152
Start time:	Sat May 17 04:59:38 2014
End time:	Sat May 17 05:01:19 2014
Elapsed:	2 minutes

Vulnerabilities



Threat Assessment: Pen Testing and Vulnerabilities

burp suite professional

burp intruder repeater window help

target proxy spider scanner intruder repeater sequencer decoder comparer options alerts

results scan queue live scanning options

- http://www.wahh-labs.net
  - admin
  - contacts
  - creditcards
  - employees
  - fileexchange
  - labs
  - news
  - prefs
  - search
- https://www.wahh-labs.net

- SQL injection [4]
- HTTP header injection
- Cross-site scripting (reflected) [2]
  - /search/1/Default.aspx [SearchTerm parameter]
  - /search/4/Default.aspx [SearchTerm parameter]
- Cleartext submission of password [2]
- OS command injection
- XPath injection [2]
- LDAP injection

advisory request response

Cross-site scripting (reflected)

Issue: **Cross-site scripting (reflected)**
Severity: **High**
Confidence: **Certain**
Host: **http://www.wahh-labs.net**
Path: **/search/1/Default.aspx**

Issue detail

The value of the SearchTerm request parameter is copied into the HTML document as plain text between tags. The payload **7b576<script>alert(1)</script>5e12190748156777e** was submitted in the SearchTerm parameter. This input was echoed unmodified in the application's response.

Threat Assessment and Peer Rankings

BITSIGHT

PORTFOLIO ALERTS HELP STEPHEN BOYER

680

Average Portfolio SecurityRating

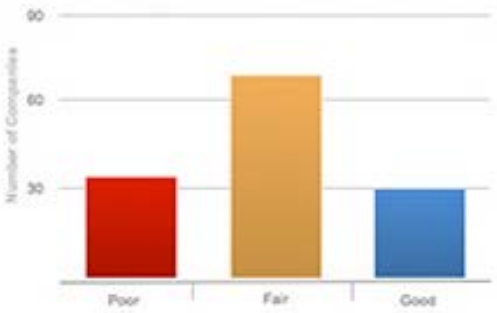
310 - 890

Portfolio Range

123

Companies in Portfolio

SecurityRating Distribution



This Week's Largest Changes

Downgrades

- -6% Black Mesa Research
- -2% AmerTek

Upgrades

- +8% Adipose Industries
- +10% Mumbai Hosting

Portfolio News

- 7-16-2013, YahooNews: Bluth Company hit with especially-aggressive hacker attack.
- 7-13-2013, SlashDot: Legal wrangling nastier in the age of electronic espionage
- 7-2-2013, CNET: One Year Later - How Gekko has cleaned up his act.

Company	Trend	Rating	IP Addresses	Industry
Adipose Industries		700	2,880	Information Technology & Services
AmerTek		670	139,456	Airlines/Aviation
Black Mesa Research		650	509	Mechanical or Industrial Engineering
Bluth Company		340	7,930	Real Estate
Dewey, Cheatum & Howe		720	32	Law Practice
Fashion World		560	390,212	Retail
Gekko & Co.		890	99	Financial Services
Goliath National Bank		500	323,012	Banking
Maritime Insurance of Japan		820	345	Insurance
Mumbai Hosting, Inc.		540	567,022	Web Hosting

Lessons Learned

Tips for Continuous Cyber Health

- Be Proactive!
- Failure to Detect the Attack
- Don’t under-estimate the bad guys
- Over-reacting
- Public relations
- Waiting for Perfect Information
- Don’t waste a good crisis!

Q&A