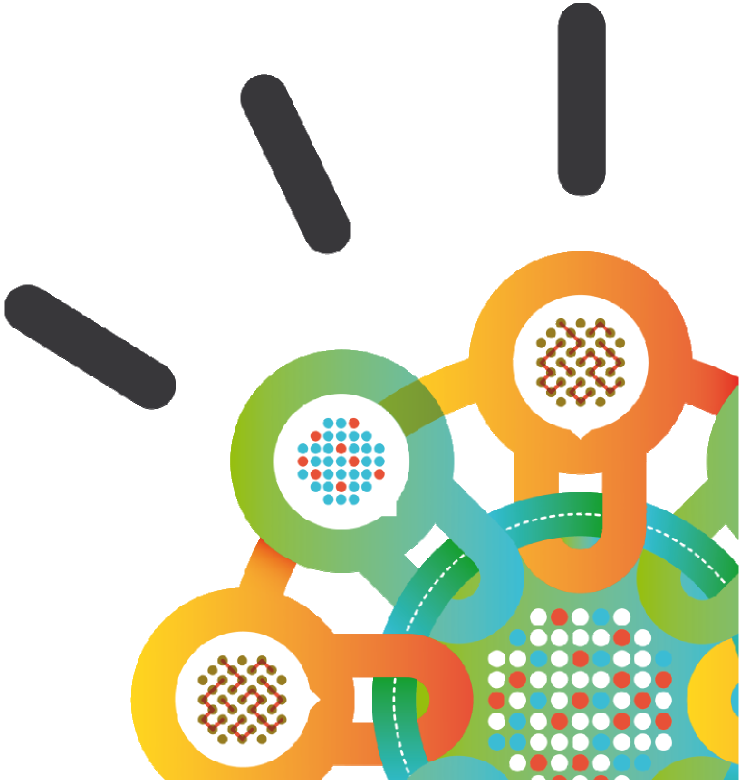
Security Intelligence.
Think Integrated.

Protecting against cyber threats and security breaches

IBM APT Survival Kit

Alberto Benavente Martínez
abenaventem@es.ibm.com
IBM Security Services
Jun 11, 2015 (Madrid, Spain)



© 2015 IBM Corporation

So what is an advanced persistent threat (APT)?

(Hint: Conficker was an APT)

Anatomy of an advanced persistent threat (APT)

Advanced

- Look for vulnerabilities within infrastructure
- Evaluate security controls to identify areas to exploit
- Gain access to privileged systems

+

Persistent

- Can be months or years before detected
- Anti-virus and traditional security controls insufficient
- Pervasive – evolve and proliferate rapidly
- Remember Conficker?

+

Targeted

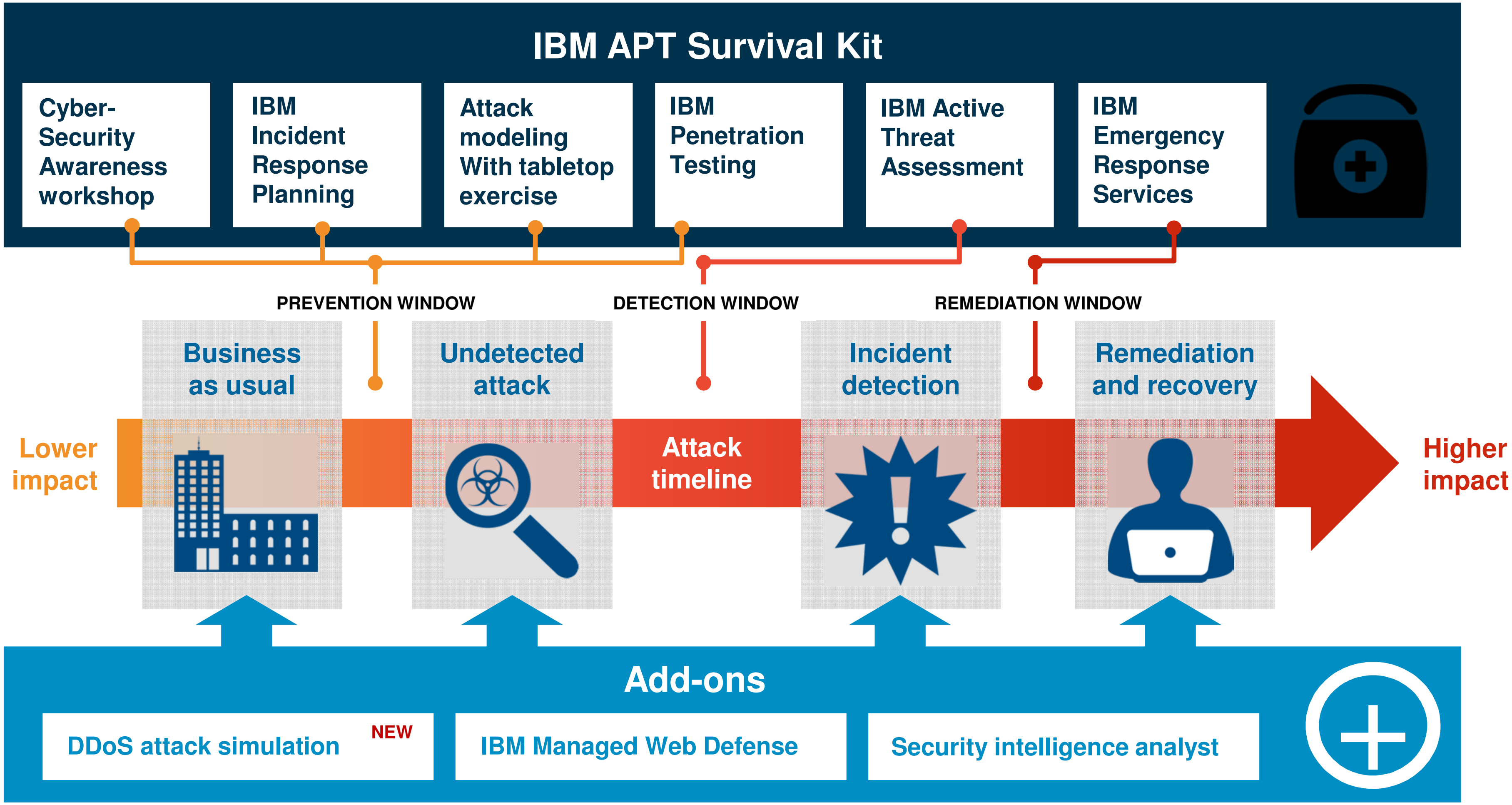
- Toward specific Organizations
- To steal specific data or cause specific damage

© 2015 IBM Corporation

The IBM solution

© 2015 IBM Corporation

IBM APT Survival Kit can help you better prepare for, detect and remediate attacks, reducing the timeline for potential impact



© 2015 IBM Corporation

The straight talk: what do I need to know about these threats?

Cybersecurity awareness workshop

Generate awareness and identify key actions

- **A 2-hour, real-world remote briefing** that goes behind the scenes, using real-world scenarios, illustrative examples and interactive demonstrations to examine the anatomy of modern cyber attacks:
  - ❑ The 5-stage chain attackers typically follow
  - ❑ Common methods and attack surfaces
  - ❑ The role of social media
  - ❑ Technological advancement and operational sophistication
- **Generate executive level awareness** on current threat level, cyber risk profile, global trends, potential attack impact and essential practices
- **Identify actionable steps** that can be taken today to better protect yourself and your organization

© 2015 IBM Corporation

The preparation: how good is my cyber incident response plan?

IBM Incident Response Planning

Plan for cybersecurity incidents

- **Proactive cyber breach defense** that helps your review, develop and test your incident response plan to build the foundation for incident response and recovery
  - ❑ IBM security experts, working hand-in-hand with you
  - ❑ A framework for more effective response
  - ❑ Organizational roles and responsibilities
  - ❑ Types and priorities of each incident
  - ❑ Escalation and communication
- **Don’t get caught off-guard** ; proactively plan response activities in the event of a security breach
- **Make sure you’re equipped** with the right response tools, resources and processes you’ll need in the event of an incident

© 2015 IBM Corporation

The what-ifs: will my business hold up during a breach?

Attack modeling and tabletop exercise

Test your business and operational resiliency

- **Uncover what's in your threat landscape** with detailed threat and attack modeling down to a granular level
  - ❑ Modeled by region, industry and sector
- **Harden your business** against potential cyber incidents
  - ❑ Key objectives and vulnerabilities identified
  - ❑ Countermeasures defined to prevent, or mitigate the effects of threats
- **Verify security paper policy** against known and unknown threats in your landscape
  - ❑ Mock incident testing performed, to measure how your defenses respond

© 2015 IBM Corporation

The real world: is my existing security posture effective against a skilled human attacker?

IBM Penetration Testing

Actively and safely exploit vulnerabilities

- **Not your everyday pen test**, with testing that's deeper and wider than automated tools or manual testing
  - □ Extensive and detailed reporting
  - □ Play-by-play accounts of tests, analysis and remediation
  - □ Effective false positive identification and removal
  - □ Network discovery and reconnaissance
  - □ Internal and external attacks and exploitation attempts
  - □ Everything from phishing exercises to social engineering
- **Gain knowledge of attack surfaces,** not tools, as real-world coding expertise is applied to the latest threat vectors
- **Identify vulnerable systems** with a detailed security roadmap and impact analysis to help prevent network compromise

© 2015 IBM Corporation

The inside scoop: has an APT infiltrated my organization?

IBM Active Threat Assessment

Evaluate your current threat and risk level

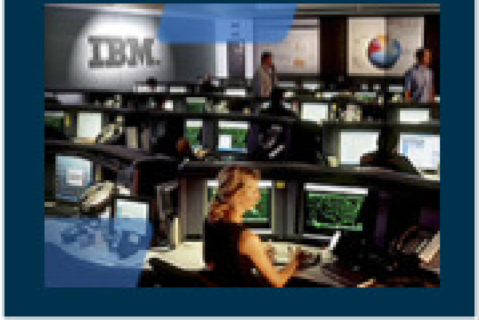
- **Detect potential breaches early** as IBM threat consultants perform detailed analyses of current organizational threats
  - ❑ Coordinated attack simulation
  - ❑ Tool-based scanning of indicators of compromise (IOCs)
  - ❑ Memory and log analysis
  - ❑ Essential practices and critical controls assessment
- **Make sure your bases are covered** by identifying active threats that currently exist in your environment
- **Help avoid a full-blown breach** by uncovering potential threats requiring mitigation

© 2015 IBM Corporation

The 911: help, we've been hacked!

IBM Emergency Response Services

Enable rapid response and recovery from a cyber incident



- **911 for cybersecurity incidents:** IBM helps you combat an security incident, intrusion, or attack, for faster recovery
- **Conduct security wellness checks** with annual planning workshop and ongoing quarterly checkpoints
- **Get 24/7[1], rapid response to a cybersecurity incident** with our around-the-clock global hotline, and help reduce potential adverse impact to your brand, reputation and revenue
- **Gain deep insight** into how and why the incident started with forensic analysis, enabling agile response to law enforcement queries and regulatory requirements
- **Understand trends in attack behaviors** across a range of industries with global threat intelligence from IBM® X-Force®

[1] 24-hours-a-day, 7-days-a-week

© 2015 IBM Corporation

APT add-on: can my website handle a DDOS attack?

Distributed denial-of-service (DDoS) attack simulation

Help ensure web-related service delivery during a DDoS[1] attack

- **Automation meets world-class experts** as security experts use automated tools to simulate web traffic DDoS attacks
  - ❑ Highly customizable, measurable scenarios
  - ❑ Multiple real-life attacks simulated
  - ❑ Mix of valid user and malicious traffic
  - ❑ Can be combined with other attacks
- **Prepare for and help prevent DDoS attacks** with the help of IBM security experts and real-life attack simulations
- **Gain organizational confidence** as you demonstrate website business continuity assurance to the executive team

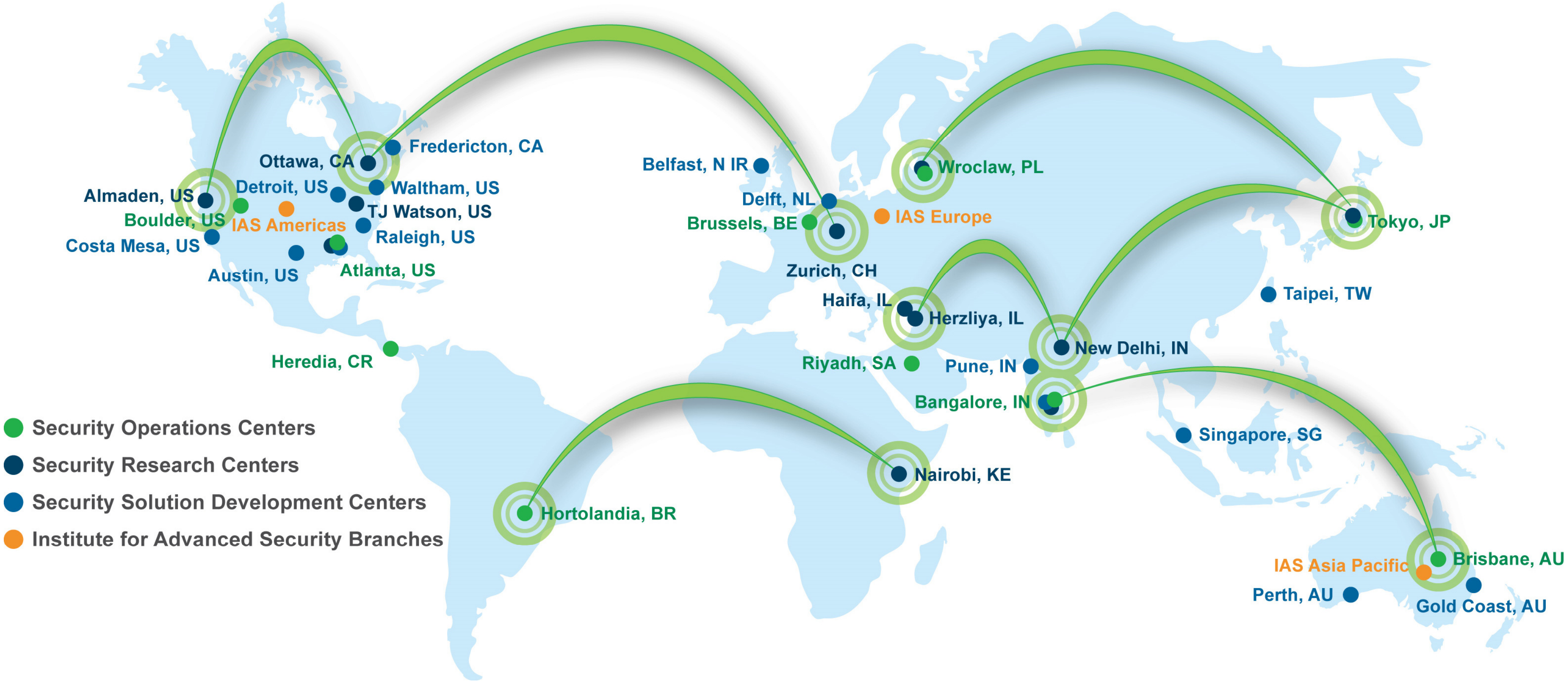
[1] Distributed denial of service

© 2015 IBM Corporation

Why IBM?

© 2015 IBM Corporation

IBM Security has global reach



IBM Security by the numbers

133 + monitored countries (MSS)

3300 + service delivery experts

20000 + devices under contract

270000000 + endpoints protected

15000000000 + events managed per day

We can work with you to customize your IBM APT Survival Kit

IBM Security Services

Intelligence. Integration. Expertise.

Responding to – and recovering from – sophisticated security attacks

Download

IBM Global Technology Services
White Paper

IBM Security Services

Responding to—and recovering from—sophisticated security attacks

The four things you can do now to help keep your organisation safe

IBM

Building a security incident response plan that works

Download

IBM Global Technology Services
Security Services

IBM

Building a security incident response plan that works

A look at the top ten CSIRP (Computer Security Incident Response Plan) mistakes

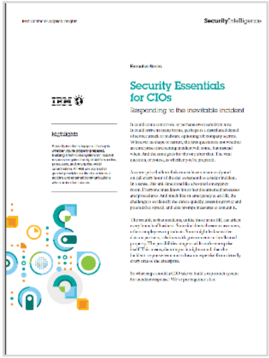
Highlights

Understanding the high cost of security failures

[illegible]

Security Essentials – responding to the inevitable incident

Download


SecurityIntelligence

Executive Series

IBM

Security Essentials for CIOs

Responding to the inevitable incident

Highlights

[illegible]

2014 Cyber Security Index

Download

IBM Global Technology Services
Managed Security Services

Research Report

IBM Security Services 2014 Cyber Security Intelligence Index

Analysis of cyber attack and incident data from IBM's worldwide security operations

IBM

© 2015 IBM Corporation

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY

Thank You

www.ibm.com/security

© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.