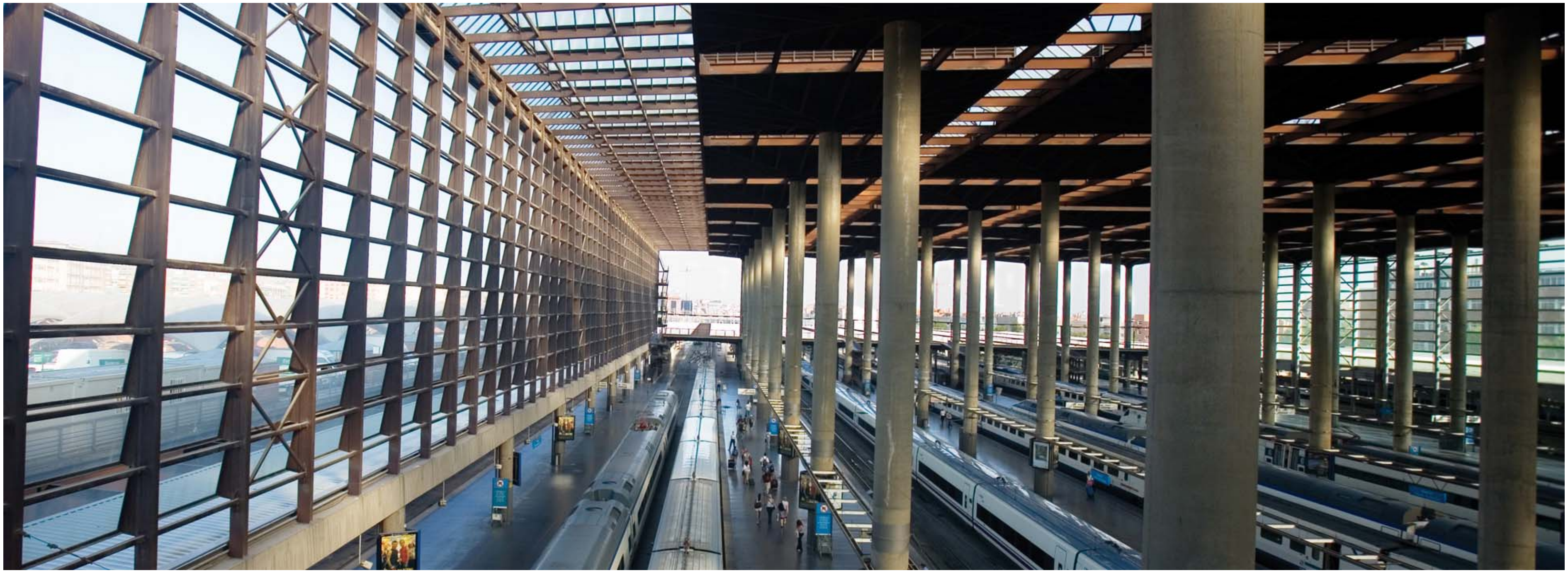
Advanced Cyber Threats

May 20, 2010

By: Ali Golshan



PricewaterhouseCoopers

Agenda

	Page
1) Current Threat Landscape • Rise of Cyber Threats • Where is it all going	2
2) The Disconnect • The Tools & Methodology of the Security Industry • The Tools & Methodology of Current Attackers	10
3) The Risk • Advantage Bad Guys	19
4) What is Needed • A true Paradigm Shift in Security	25

Section 1
Current Threat Landscape

1) **What are Advanced Cyber Threats?**
2) **Cyber Warfare**
3) **Advanced Cyber Threats**
4) **The Shift We Are Seeing**
5) **Who is a Target?**
6) **Repercussions**

Section 1
Current Threat Landscape

1) **What are Advanced Cyber Threats**
   - New Attack Methodology
     - No longer smash and grab
     - Reconnaissance and Preparation involved
   - New Generation of Attackers
     - No longer for Reputation and Recognition
     - After Financial Returns
   - New Generation of Malware
     - Over the past 10 years Malware has become highly sophisticated

Section 1
Current Threat Landscape

1) **What are Advanced Cyber Threats**
   - Cyber Warfare
     - Countries making investment in Cyber Offensive Capabilities
     - Used for destabilization along with conventional Warfare
   - Advanced Cyber Threats
     - No longer for reputation and recognition
     - After Financial Returns
     - Government, or Private backing

Section 1
Current Threat Landscape

2) Cyber Warfare

- Russia-Georgia War (2008)
  - First example of Cyber Attack coinciding with conventional Warfare
  - Targets were Georgian Government Sites, as well as U.S. and British embassies
- Weaponizing the Net
  - 2007 McAfee Report stated approximately 120 countries trying to create weaponize Internet capabilities
  - 2009 Virtual Criminology Report stated U.S. China, Israel, France, and Russia have significantly increased their Cyber Armory.

Section 1
Current Threat Landscape

3) Advanced Cyber Threats

- Operation Aurora Incident (2009)
  - Infiltrated over 30 companies, including Google, and Adobe.
  - Google Honorably admitted to the attacks
- GhostNet
  - Infiltrations discovered in embassies belonging to India, South Korea, Portugal, Germany, and over 10 more.
- Russian Business Network
  - Originated as an Internet Service Provider
  - Provides a platform for launching attacks and malicious activity

Section 1
Current Threat Landscape

4) The Shift We Are Seeing

- Attacks with Purpose
  - Teams of Attackers with specific skills
    - Zeus Trojan creators
  - Tailored towards particular technology, or companies to maximize advantage & financial returns
- Big Economy
  - Cyber Crime 2nd largest Economy on the Net
  - Well Funded, and Backed as much lower risk that conventional Crime
  - Much higher return on investments

Section 1
Current Threat Landscape

5) Who is a Target

- Government Agencies
  - Targeted by Foreign Intelligence Services (FIS)
- Financial Industry
  - Targeted by Transnational Criminal Enterprises
  - •Organizations with IP
  - By FIS & Competitors to bypass Years & Millions of R&D

Section 1
Current Threat Landscape

6) **Repercussions**

- Damage to Reputation
  - Loss of Customers or Partners

  Fall in Stock Price

  - Caused by Panic, or Data Loss
- Loss of Competitive Advantage
  - Years & Millions of R&D stolen by competitors
- Fines & Penalties
  - Imposed by Partners or Agencies
    - Over $22 Million of which related to card brands, and settlements.

Section 2
The Disconnect

1) **Current Solutions**
2) **Modern Malware**
3) **A Case Study, The “Operation Aurora” Incident**
4) **What’s Missing from Conventional Solutions**

Section 2
The Disconnect

1) **Current Solutions**
   - Anti-virus
     - Reactive Solution
     - Matches signatures & patterns
     - Require update to signature database to capture only known Malware
   - Firewalls
     - Relevant when attacks targeting specific network vulnerabilities
     - Now Malware can tunnel through HTTP
     - Next-Gen FW perform deep packet analysis, however still required knowledge of vulnerabilities

Section 2
The Disconnect

1) **Current Solutions**
   - Web Gateways
     - Lists “known-bad” URLs
     - In case of Conficker, random newly generated sites were created for distribution of malicious payload.
   - Network Intrusion Detection & Prevention Systems
     - Monitor network traffic to understand data transmission
     - Shift from IDS to IPS to capture patterns of threats
     - Rather than knowing Threat, required knowledge of vulnerability
     - No protection against Zero-day vulnerabilities

Section 2
The Disconnect

1) **Current Solutions**
   - Heuristics & Behavior Analyzers
     - They are essentially “statistical guesses”, based on correlations of various stats.
     - Step in right direction, however modern Malware shares a large set of behaviors with modern applications.
     - If rules, and heuristics are set too aggressively they will cause too many false positives
     - If not customized, and fine-tuned will allow targeted attacks to pass right through

Section 2
The Disconnect

2) **Modern Malware**

- How Modern Malware Operate
  - Designed and Built by highly skilled developers
  - Built with the mindset to accomplish a very specific goal
  - Understanding the Target system, and Zero-day vulnerabilities within their services
  - Gain access without being noticed
  - Maintain access over a period of time
  - Communicate with outside resources without creating network noise
  - Launched with the goal of extracting high value assets

Section 2
The Disconnect

3) A Case Study, The “Operation Aurora” Incident

- Aurora utilized:
  - Social Engineering
  - Zero-day Vulnerabilities
  - The gaps created by conventional Security
  - Aurora Targeted:
  - Theft of email archives
  - Confidential data
  - A well-defined list of Enterprises

Section 2
The Disconnect

3) A Case Study, The "Operation Aurora" Incident

- How Aurora Operated:
  - Attacks began in 2009 using a zero-day IE 6.0 vulnerability
  - Would lure users to click a link, directing them to a malicious Web site.
  - Once system compromised, a Trojan was installed
  - Once installed the Trojan would communicate with the Command & Control for variety of commands
  - New payloads would allow for further compromise of the companies systems.

Section 2
The Disconnect

3) A Case Study, The “Operation Aurora” Incident

- How Aurora Operated:
  - Attacks began in 2009 using a zero-day IE 6.0 vulnerability
  - Would lure users to click a link, directing them to a malicious Web site.
  - Once system compromised, a Trojan was installed
  - Once installed the Trojan would communicate with the Command & Control for variety of commands
  - New payloads would allow for further compromise of the companies systems.

FW & IPS Failed →

Section 2
The Disconnect

3) A Case Study, The "Operation Aurora" Incident

- How Aurora Operated:
  - Attacks began in 2009 using a zero-day IE 6.0 vulnerability
  - Would lure users to click a link, directing them to a malicious Web site.
  - Once system compromised, a Trojan was installed
  - Once installed the Trojan would communicate with the Command & Control for variety of commands
  - New payloads would allow for further compromise of the companies systems.

FW & IPS Failed → Attacks began in 2009 using a zero-day IE 6.0 vulnerability

Web Gateway Failed → Would lure users to click a link, directing them to a malicious Web site.

Section 2
The Disconnect

3) A Case Study, The “Operation Aurora” Incident

- How Aurora Operated:
  - **FW & IPS Failed** → Attacks began in 2009 using a zero-day IE 6.0 vulnerability
  - **Web Gateway Failed** → Would lure users to click a link, directing them to a malicious Web site.
  - **Antivirus Failed** → Once system compromised, a Trojan was installed
  - Once installed the Trojan would communicate with the Command & Control for variety of commands
  - New payloads would allow for further compromise of the companies systems.

Section 2
The Disconnect

3) A Case Study, The “Operation Aurora” Incident

- How Aurora Operated:
  - **FW & IPS Failed** → Attacks began in 2009 using a zero-day IE 6.0 vulnerability
  - **Web Gateway Failed** → Would lure users to click a link, directing them to a malicious Web site.
  - **Antivirus Failed** → Once system compromised, a Trojan was installed
  - **FW & IDS Failed** → Once installed the Trojan would communicate with the Command & Control for variety of commands
  - New payloads would allow for further compromise of the companies systems.

Section 2
The Disconnect

3) A Case Study, The “Operation Aurora” Incident

- How Aurora Operated:
  - **FW & IPS Failed** → Attacks began in 2009 using a zero-day IE 6.0 vulnerability
  - **Web Gateway Failed** → Would lure users to click a link, directing them to a malicious Web site.
  - **Antivirus Failed** → Once system compromised, a Trojan was installed
  - **FW & IDS Failed** → Once installed the Trojan would communicate with the Command & Control for variety of commands
  - **Antivirus Failed** → New payloads would allow for further compromise of the companies systems.

Section 2
The Disconnect

4) What's Missing from Conventional Solutions

- A solution to provide security across all Threat Vectors
- A Dynamic Solution vs. Dynamic Attacks
- Protecting against Zero-day vulnerabilities on:
  - Network Layer
  - Application
  - Operating Systems
  - Accurate against Targeted Attacks
  - Not missing attacks
  - Low to 0 false-positives

Section 3
The Risk

1) **Advantage Bad Guys!**
2) **Current Risks**
3) **Costs**
4) **The Real Risk**

Section 3
The Risk

1) **Advantage Bad Guys!**
   - Attackers have the luxury of responding to Security movements
   - Build their attacks to take advantage of our weakness
   - They only need to succeed once
   - We need to succeed every time
   - They need to find only 1 vulnerability
   - We need to protect against every unknown vulnerability
   - Not enough Security Professionals

Section 3
The Risk

2) Current Risks

- 11% of Worlds computers are part of an existing Botnet
- 23% of home computer become infected despite a security solution
- 72% of corporate networks with 100+ users are infected
- 66% of new Trojans are built for theft of Banking information
- According to PandaLabs approximately 90% of email traffic was Spam in 2009
- For the first time, in 2008 production of Malware was higher than legitimate software
- In 2009, 25 Million New Strains of Malware were created!
- Compared to roughly 15 Million in the previous 20 Years!

Section 3
The Risk

2) **Current Risks**

- Much more opportunity for Blackhats
- Entrepreneur have Angels, Blackhats now have Devils
- Attackers with specialized skills for hire
  - Highly Educated
  - In depth understanding of Networks, Applications, Operating systems, and at time internal knowledge
  - Low Barrier to Entry & High Rewards
  - Lack of International Cyber Laws, and very difficult to prove
  - Low Risk & High Rewards have resulted in a fertile Attack Landscape, with massive R&D resources
  - Zero-day vulnerabilities can be sold on the “Black-market” for targeted attacks

Section 3
The Risk

3) Costs

- Cyber Crime is currently costing roughly $250 BILLION Globally per year.
- The average cost of Sophisticated Attack roughly $6.6 Million per incident
- Over 50,000 new Malware programs are released on the Internet Daily!
- In 2009, The Pentagon spent over $100 Million in 6-months, responding and recovering to Cyber Attacks
- In 2009 Cyber Attacks forced the Defense Department to take 1,500 machines off-line
- GhostNet infected machines in over 103 different countries, extracting data

Section 3
The Risk

4) The Real Risk

- Advanced Attacks are only starting to mature
- They are a new Methodology, Not a type of attack
- Attackers are willing to change constantly to take advantage of security solutions
- More resources are being provided for Cyber Criminals
- Much better information sharing than Security Companies
- Most current attacks are Proof of Concept
- The skills and technology for attacks available, ready for someone to pull the trigger
- Security Industry in Denial regarding current solutions

Section 4
What Now?

1) An Intervention for The Security Industry
2) Paradigm Shift
3) Security Needs to Adapt

Section 4
What Now?

1) **An Intervention for The Security Industry**
   - Acceptance the need for truly new & unique technology
   - Accepting “Reducing the Damage” is not the answer
   - Based on a different infrastructure, not detect first, respond later
   - The need to dynamically discover new vulnerabilities
   - Using the R&D going into attacks, for a good cause

Section 4
What Now?

2) Paradigm Shift

- Building new adaptive technology, using combination or practices, from various fields of sciences, and mathematics
- Through creating new technology, we can lead to a new protection methodology
- Better information sharing platforms
- Viewing Enterprise Security spending as a long-term investment
- A few smaller companies really driving this required shift

Section 4
What Now?

3) **Security Needs to Adapt**

- Attackers won’t wait for us to catch up
- Rather than gradual improvements to solutions, renaming heuristics to behavior, to reputation, there is a need for fundamental changes
- More international cooperation is required on all fronts
- Current solutions are designed for old technologies
- Technologies such as Cloud, and Virtualization won’t be able to become fully adopted unless security concerns are remedied
- More Adaptive Security Solutions

Thank You!

PwC