APRICOT2015 Security Workshop:

Assets and Threats

Sheryl Hermoso, APNIC
sheryl@apnic.net

Acknowledgment

- This presentation is based on the original materials created by
  - **Merike Kaeo** of Double Shot Security
  - Contact: merike@doubleshotsecurity.com

Basic Terms

- Threat
  - Any circumstance or event with the potential to cause harm to a networked system
- Vulnerability
  - A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
- Risk
  - The possibility that a particular vulnerability will be exploited
    - Risk analysis: The process of identifying security risks, determining their impact, and identifying areas requiring protection

Threat

- “a motivated, capable adversary”
- Examples:
  - Human Threats
    - Intentional or unintentional
    - Malicious or benign
  - Natural Threats
    - Earthquakes, tornadoes, floods, landslides
  - Environmental Threats
    - Long-term power failure, pollution, liquid leakage

Vulnerability

- A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
  - Software bugs
  - Configuration mistakes
  - Network design flaw
  - Lack of encryption
- Where to check for vulnerabilities?
- Exploit
  - Taking advantage of a vulnerability

Risk

- Likelihood that a vulnerability will be exploited
- Some questions:
  - How likely is it to happen?
  - What is the level of risk if we decide to do nothing?
  - Will it result in data loss?
  - What is the impact on the reputation of the company?
- Categories:
  - High, medium or low risk

What Can Intruders Do?

- Eavesdrop - compromise routers, links, or DNS
- Send arbitrary messages (spoof IP headers and options)
- Replay recorded messages
- Modify messages in transit
- Write malicious code and trick people into running it
- Exploit bugs in software to ‘take over’ machines and use them as a base for future attacks

What are Security Goals?

- Controlling Data Access
- Controlling Network Access
- Protecting Information in Transit
- Ensuring Network Availability
- Preventing Intrusions
- Responding To Incidences

Goals are Determined by

- Services offered vs. security provided
  - Each service offers its own security risk
- Ease of use vs. security
  - Easiest system to use allows access to any user without password
- Cost of security vs. risk of loss
  - Cost to maintain

Goals must be communicated to all users, staff, managers, through a set of security rules called "security policy"

Causes of Security Related Issues

- Protocol error
  - No one gets it right the first time
- Software bugs
  - Is it a bug or feature ?
- Active attack
  - Target control/management plane
  - Target data plane
  - More probable than you think !
- Configuration mistakes
  - Most common form of problem

Why Worry About Security?

- How much you worry depends on risk assessment analysis
  - Risk analysis: the process of identifying security risks, determining their impact, and identifying areas requiring protection
- Must compare need to protect asset with implementation costs
- Define an effective security policy with incident handling procedures

Characteristics of a Good Policy

- Can it be implemented technically?
- Are you able to implement it organizationally?
- Can you enforce it with security tools and/or sanctions?
- Does it clearly define areas of responsibility for the users, administrators, and management?
- Is it flexible and adaptable to changing environments?

RFC 2916 - http://www.ietf.org/rfc/rfc2196.txt

What Are You Protecting?

- Identify Critical Assets
  - Hardware, software, data, people, documentation
- Place a Value on the Asset
  - Intangible asset – importance or criticality
  - Tangible asset – replacement value, training costs and/or immediate impact of the loss
- Determine Likelihood of Security Breaches
  - What are threats and vulnerabilities ?

Impact and Consequences

- Data compromise
  - Stolen data
  - can be catastrophic for a financial institution
- Loss of data integrity
  - Negative press or loss or reputation (bank,public trust)
- Unavailability of resources
  - The average amount of downtime following a DDoS attack is 54 minutes.
  - The average cost of one minute of downtime due to DDoS attack is $22,000*

* Based on a Ponemon Institute study (2012)

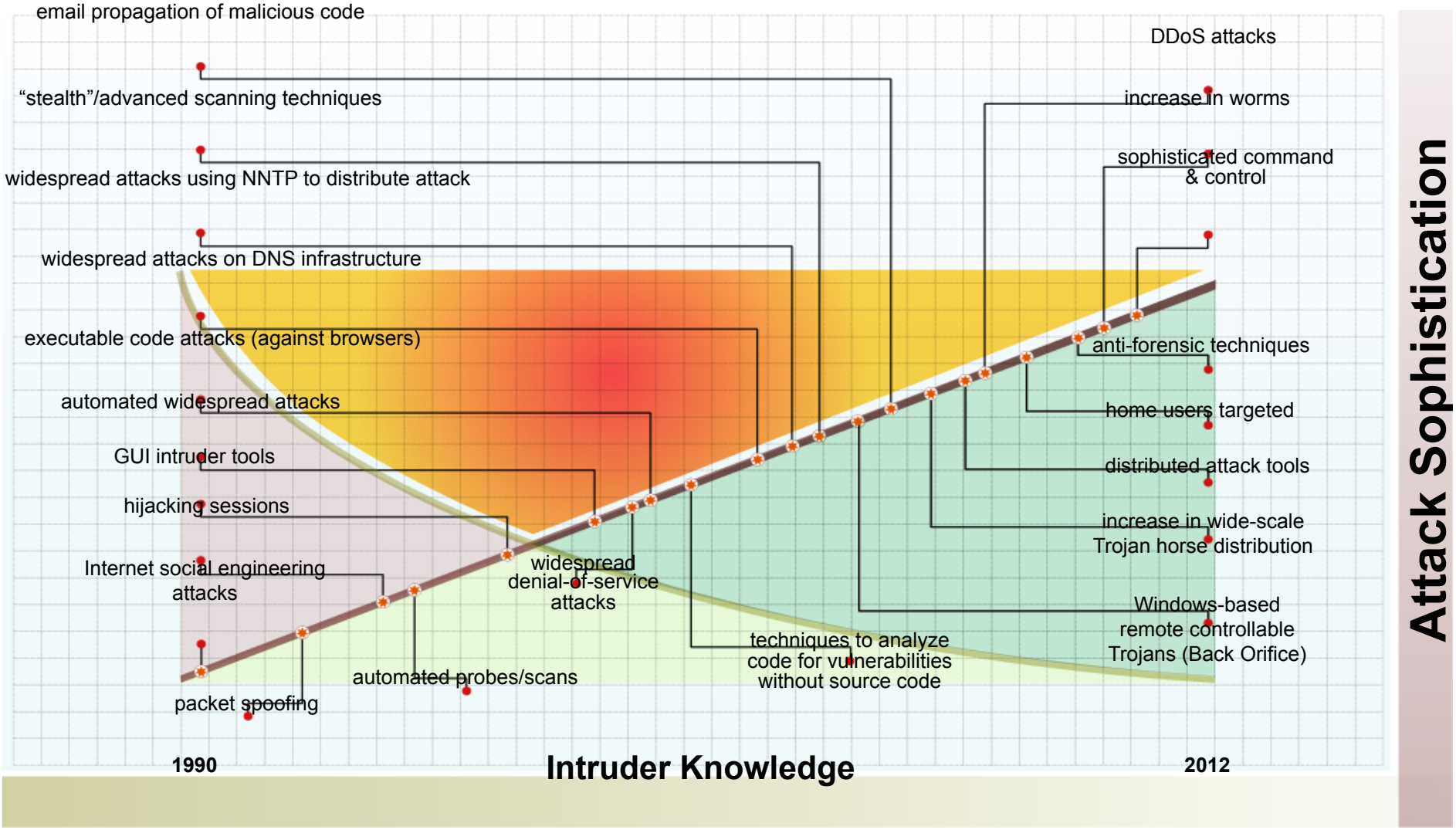
Risk Mitigation vs Cost

Risk mitigation: the process of selecting appropriate controls to reduce risk to an acceptable level.

The ***level of acceptable risk*** is determined by comparing the risk of security hole exposure to the cost of implementing and enforcing the security policy.

Assess the cost of certain losses and do not spend more to protect something than it is actually worth.

Evolution of Attack Landscape



Attack Motivation

- Criminal
  - Criminal who use critical infrastructure as a tools to commit crime
  - Their motivation is money
- War Fighting/Espionage/Terrorist
  - What most people think of when talking about threats to critical infrastructure
- Patriotic/Principle
  - Large groups of people motivated by cause - be it national pride or a passion aka Anonymous

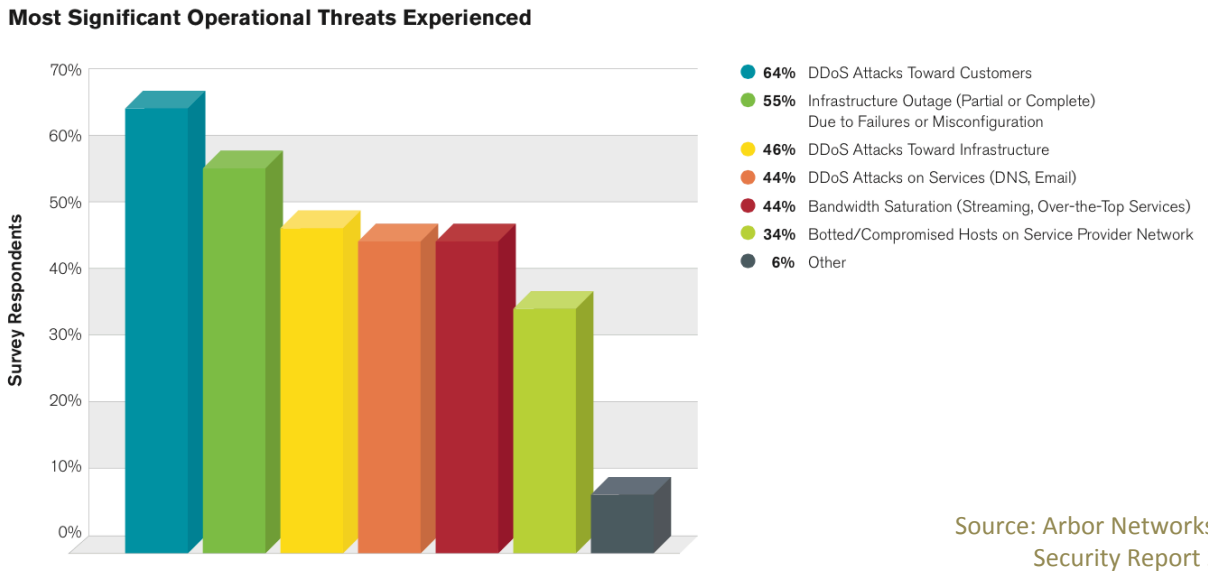
Attack Motivation

- Nation States want **SECRETS**
- Organized criminals want **MONEY**
- Protesters or activists want **ATTENTION**
- Hackers and researchers want **KNOWLEDGE**

Source: NANOG60 keynote presentation by Jeff Moss, Feb 2014

Attack Trends

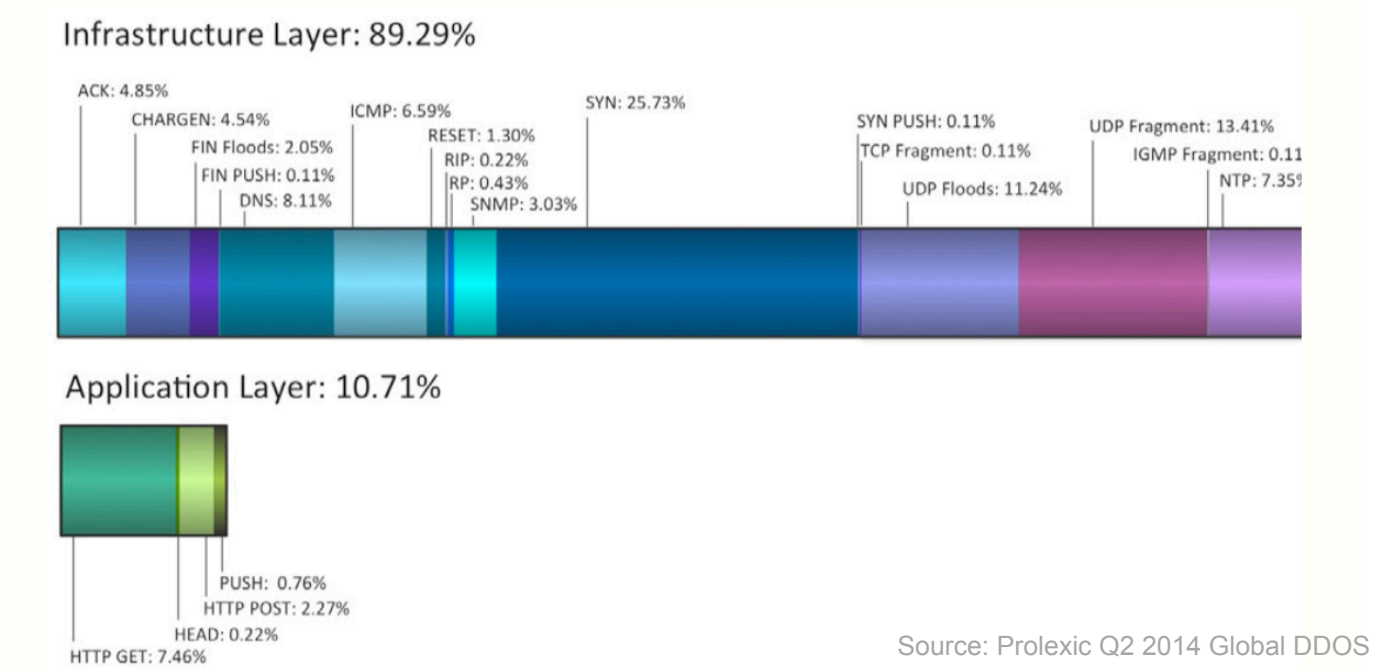
- Key findings:
  - Largest DDoS attack at 309Gbps
  - Multiple attacks over 100Gbps
  - Hacktivism is top commonly perceived motivation behind attacks
  - Customers are the most common target of attacks, with service infrastructure coming second



Source: Arbor Networks Worldwide Infrastructure Security Report 2014

Attack Trends

- Infrastructure-based attacks were the preferred attack vector (more than 80% of DDoS attacks)
  - SYN floods, UDP floods, DNS, ICMP, ACK floods, CHARGEN, SNMP



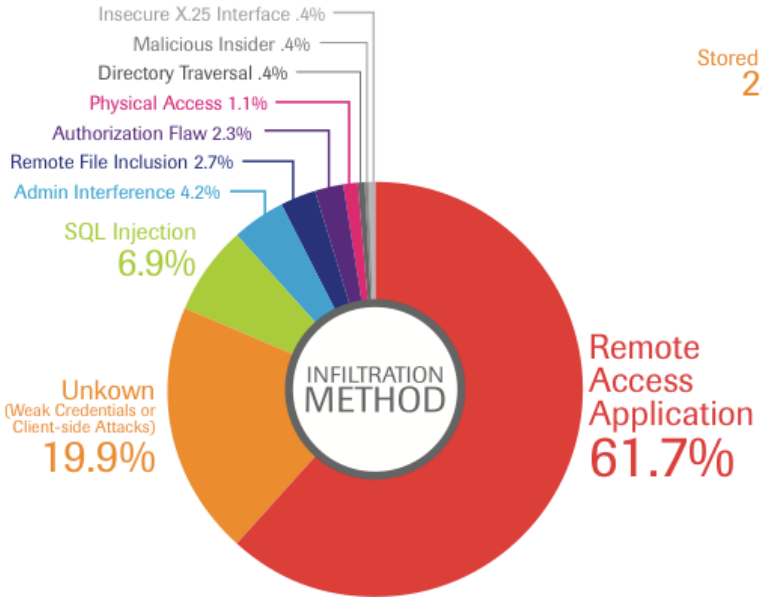
Source: Prolexic Q2 2014 Global DDOS Attack Report

Attack Trends

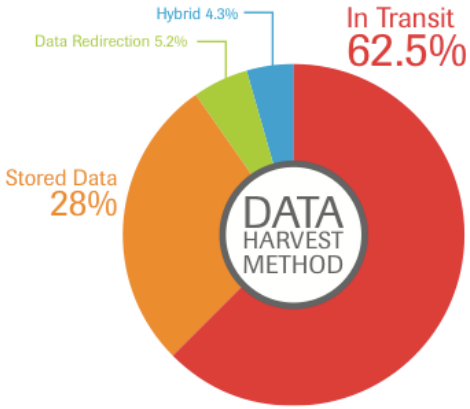
- Downward trend in the use of application-layer attacks
- “To launch significant DDoS layer 7 attack campaigns, attackers need to possess sophisiticated skills. Few attackers are capable of these attacks, as it requires compromising servers and applications by the exploitation of vulnerabilities, and often requires code customization”

Source: Prolexic Q2 2014 Global DDOS Attack Report

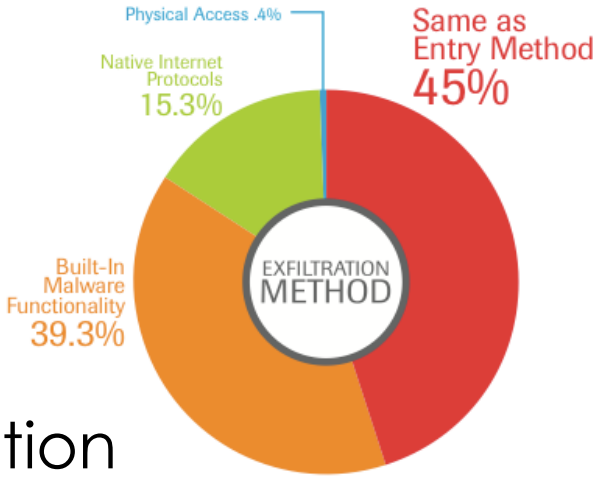
Attack Trends - Breach Sources



Infiltration



Aggregation



Exfiltration

Source: Trustwave 2012 Global Security Report

Most Common Threats and Attacks

- Unauthorized access – insecure hosts, cracking
- Eavesdropping a transmission – access to the medium
  - Looking for passwords, credit card numbers, or business secrets
- Hijacking, or taking over a communication
  - Inspect and modify any data being transmitted
- IP spoofing, or faking network addresses
  - Impersonate to fool access control mechanisms
  - Redirect connections to a fake server
- DOS attacks
  - Interruption of service due to system destruction or using up all available system resources for the service
  - CPU, memory, bandwidth

Questions