Assets and Threat Models

Sheryl Hermoso, APNIC

sheryl@apnic.net

Acknowledgment

- These materials are from
  - **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
    - Denial of Service / Unauthorized Access / Impersonation / Worms / Viruses
- 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

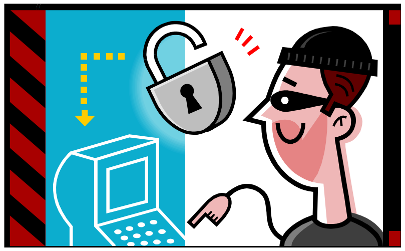
Goals are Determined by

- 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.

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.

Will I Go Bankrupt ?

Is it an embarrassment ?

Past Security Incidents

Hackers modify things to make them better

- 1946: Grace Hopper, a US Naval Officer, finds a moth in an electromechanical computer that caused problems, deems the problem a "bug”
- 1960s: MIT model train group "hacks" their trains to make them perform better
- 1971: Joe Draper aka "Captain Crunch", uses cereal toy to generate 2600 Hz signal that accesses AT&T long distance system for free
- 1983: FBI arrests "the 414" teenage hackers for an estimated 60 computer break-ins into labs
- 1983: Film "War Games" released, introduces public to the concept of hacking
- 1988: Cornell student Robert Morris Jr. releases self-replicating worm on government's ARPAnet
- 1990: Secret Service launches 'Operation Sundevil' to hunt hackers

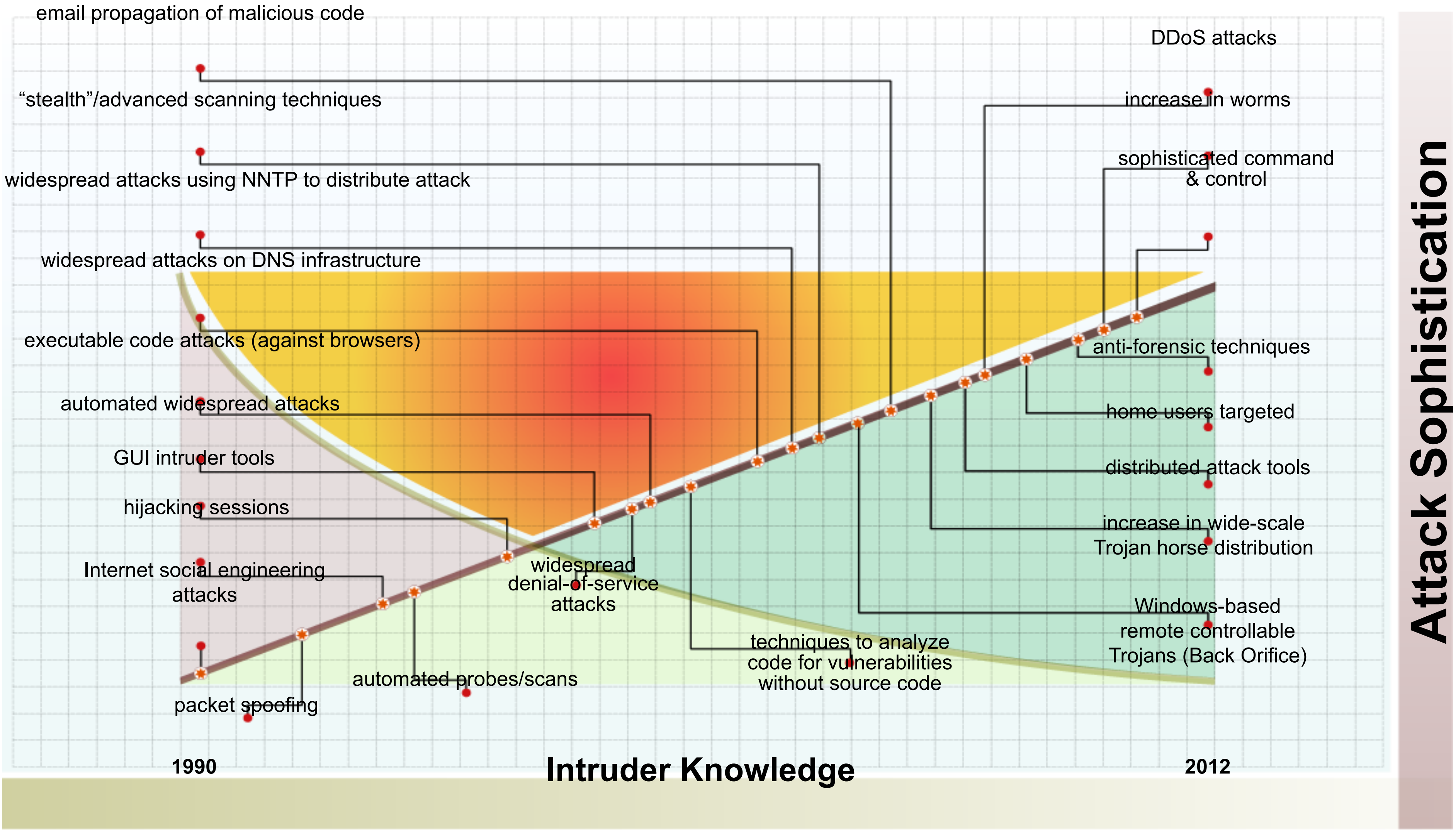
Dark side of hacking

Evolving Security Incidents

- 1994: Russian Vladmir Levin leads a group of hackers that steals millions of dollars from CitiBank through a dial-up service
- Late 1990s: flooding attacks and automated tools start to create noise
- 2000: Infamous DDoS attacks on Yahoo, eBay, CNN
- 2000: Start of infrastructure getting 'interesting' to miscreants
- 2001: Proliferation of DDoS related tools emerging
- 2003: A series of attacks on U.S. computer systems begins and continues for several years. The attacks, codenamed "Titan Rain", are attributed to China
- 2007: Cyber-attacks on Estonian media and government sites occur
- 2008: Widely publicized DNS exploits
- 2008: A bunch of men use 'wardriving' to search for unsecured wireless networks. They then install sniffer programs and steal 40 million credit card numbers

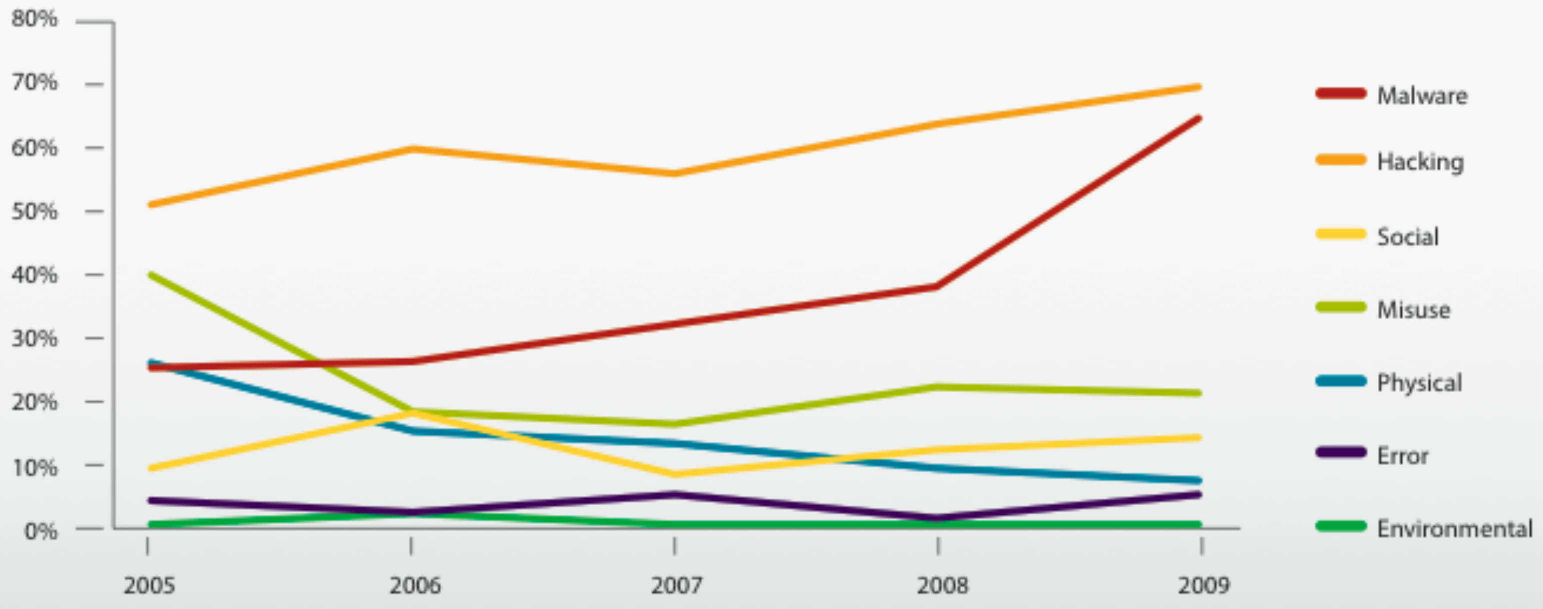
Scale of attack becomes massive

Evolution of Attack Landscape



Realities of Current Security Issues

Figure 16. Threat action categories over time by percent of breaches (Verizon cases)



The following data re Security Breaches is from:
http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Data Breaches - Malware

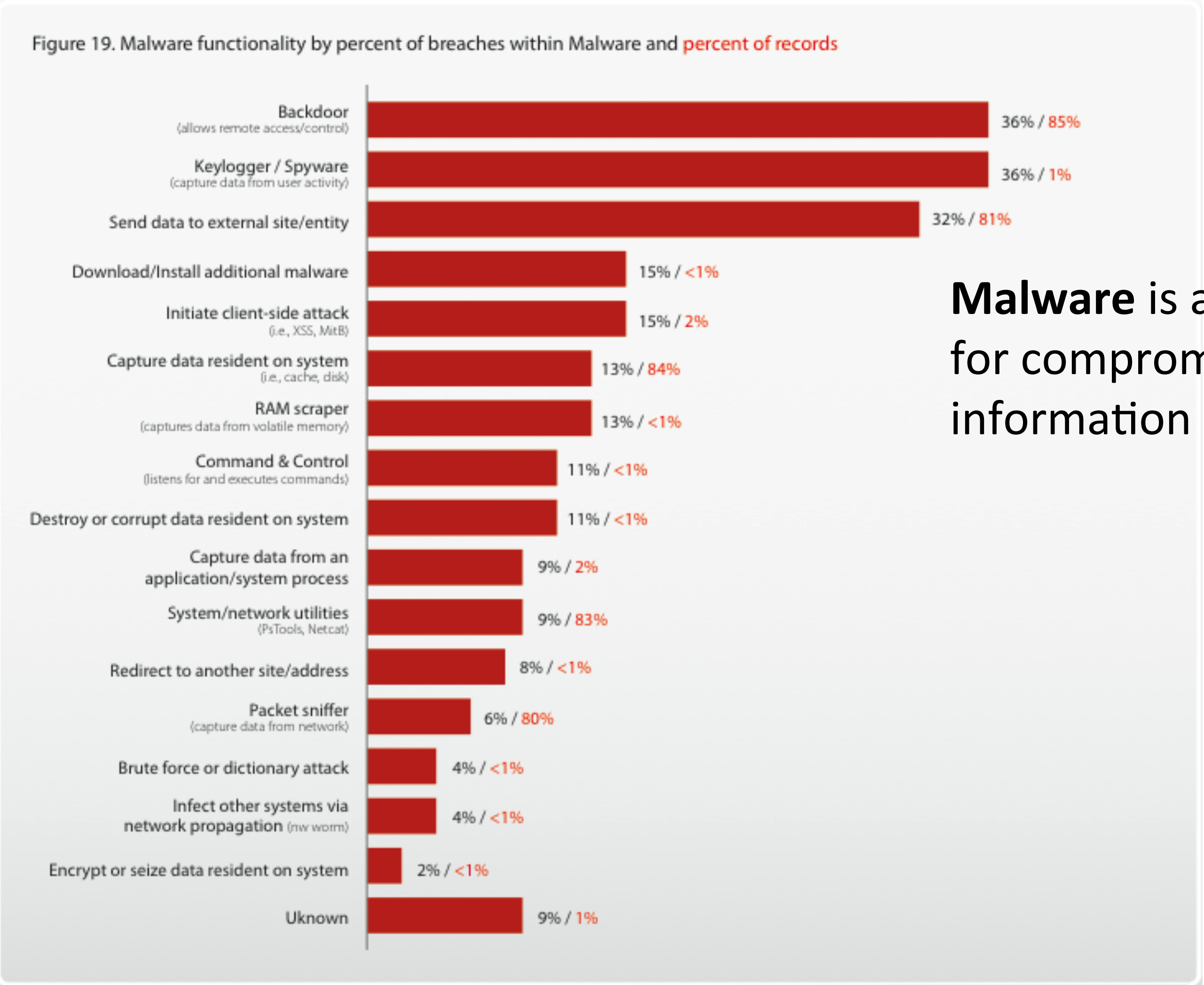


Figure 19. Malware functionality by percent of breaches within Malware and percent of records

Malware is any software developed for compromising or harming information assets.

Data Breaches - Hacking

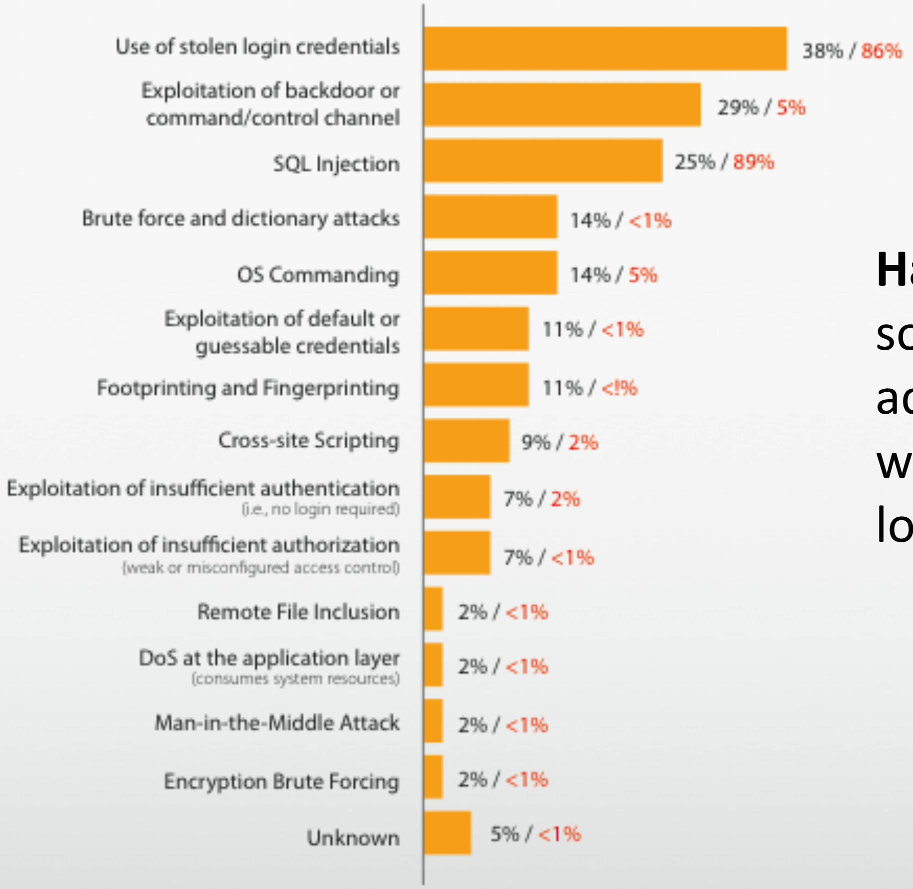


Figure 21. Types of hacking by percent of breaches within Hacking and percent of records

Hacking is any activity where someone attempts to intentionally access or harm information assets without authorization by bypassing logical security mechanisms.

Data Breaches - Misuse

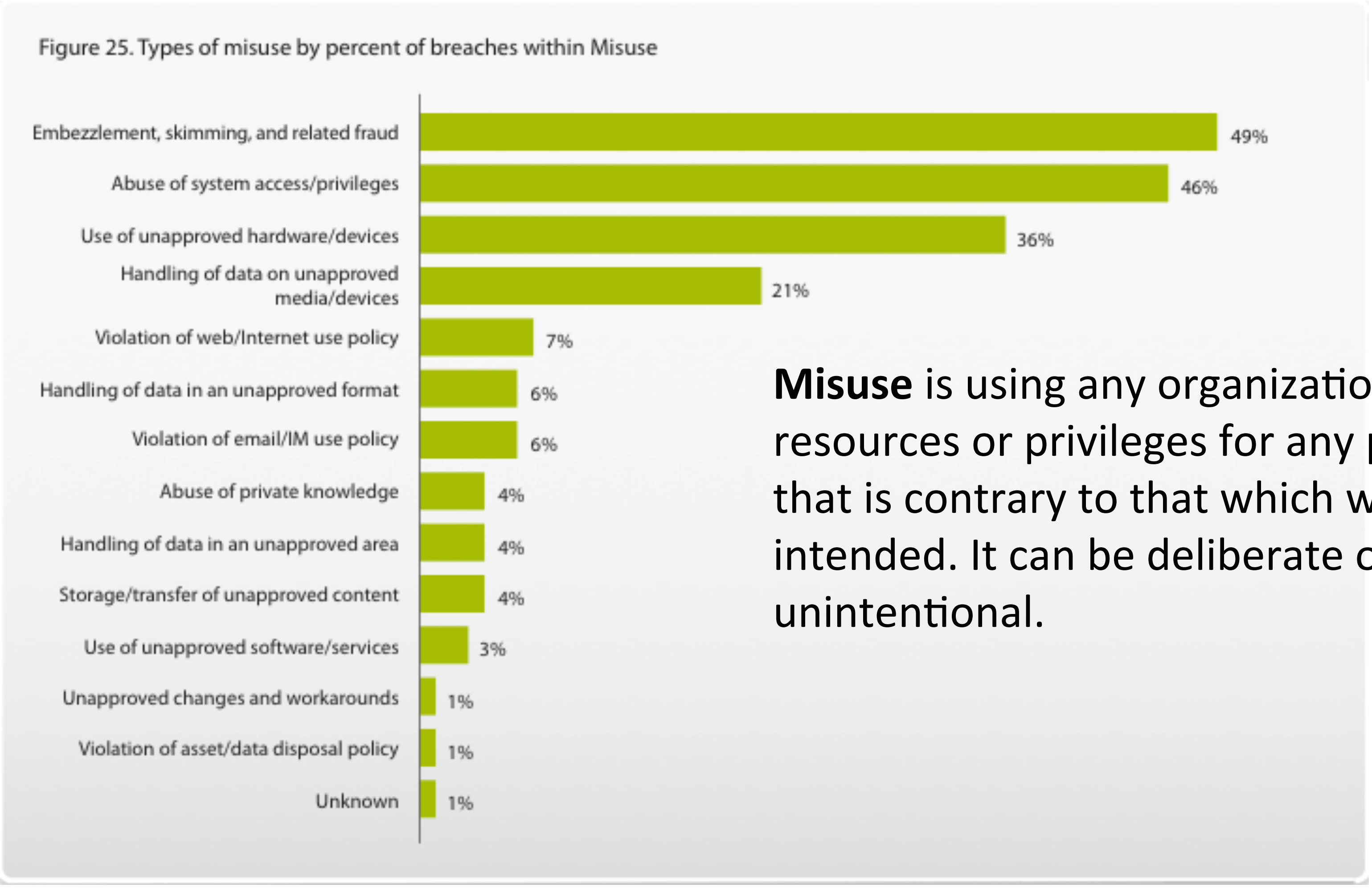


Figure 25. Types of misuse by percent of breaches within Misuse

Misuse is using any organizational resources or privileges for any purpose that is contrary to that which was intended. It can be deliberate or unintentional.

Attack Motivation

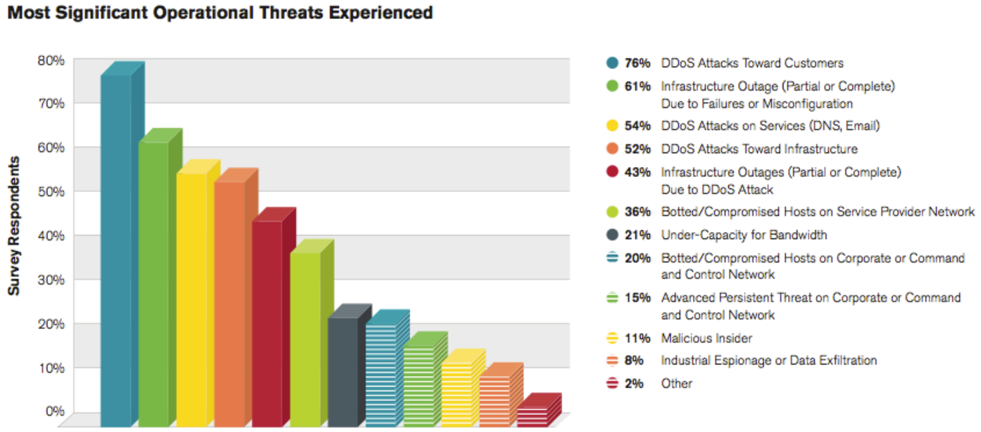
- Criminal
  - Criminal who use critical infrastructure as a tools to commit crime
  - Their motivation is money
- War Fighting/Espionage/Terrorist
  - What most people think of when talking about threats to critical infrastructure
- Patriotic/Principle
  - Large groups of people motivated by cause -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

(copied from NANOG60 keynote presentation by Jeff Moss, Feb 2014)

Attack Trends



- Key findings:
  - Hacktivism and vandalism are the common DDoS attack motivation
  - High-bandwidth DDoS attacks are the 'new normal'
  - First-ever IPv6 DDoS attacks are reported in 2011
  - Trust issues across geographic boundaries

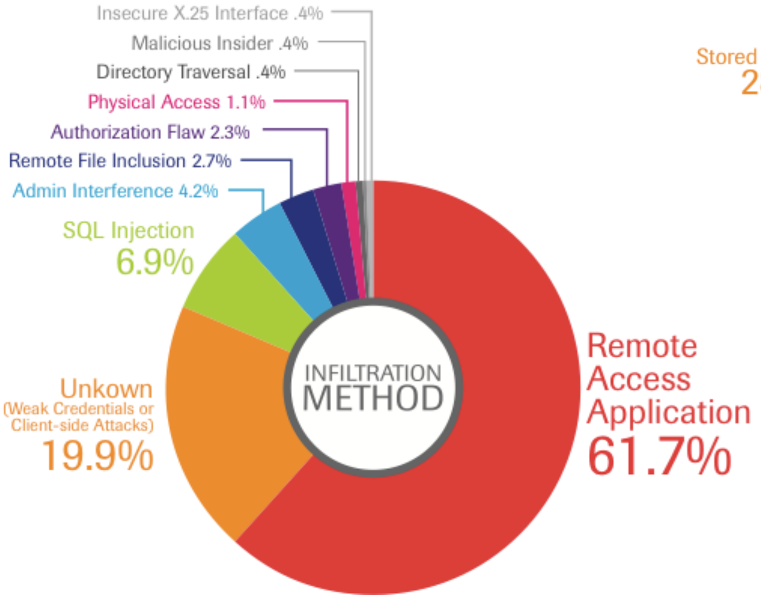
Source: Arbor Networks Worldwide Infrastructure Security Report Volume VIII

Attack Trends

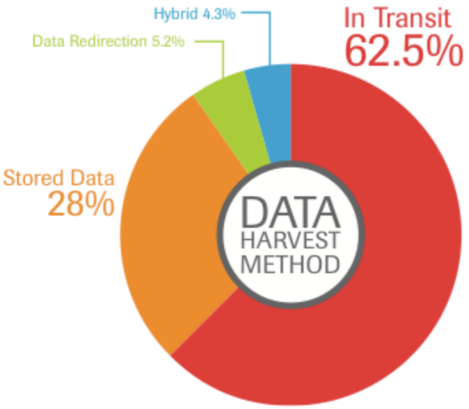
- Use of Distributed Reflection Denial of Service (DrDoS) attacks
- Shift away from SYN floods to UDP-based attacks
  - Chargen Protocol (UDP port 19) for DrDoS attacks
- Infrastructure-directed attacks (L3 and L4)
- For Q3 alone, the peak
  - Bandwidth average: 3.06 Gbps
  - Packets per second (PPS): 4.22 Mpps
  - Duration: 21.33 hours (38 hrs in Q2)
- There's a heightened level of global DDoS attack activity

Source: Prolexic Q3 2013 Global DDOS Attack Report

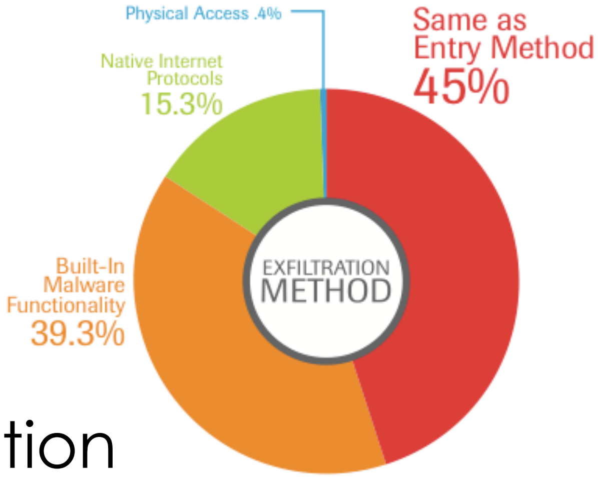
Attack Trends - Breach Sources



Infiltration



Aggregation



Exfiltration

Source: Trustwave 2012 Global Security Report

Summary - 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

Mistakes IT People Make

- Connecting systems to the Internet before hardening them.
- Connecting test systems to the Internet with default accounts/passwords
- Failing to update systems when security holes are found
- Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI
- Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated
- Failing to maintain and test backups
- Running unnecessary services : ftpd, telnetd, finger, rpc, mail, rservices
- Implementing firewalls with rules that don't stop malicious or dangerous traffic - incoming and outgoing
- Failing to implement or update virus detection software
- Failing to educate users on what to look for and what to do when they see a potential security problem