



# ISTR

INTERNET SECURITY THREAT REPORT ⊕ 2013

## Report Overview

Renault Ross CISSP, MCSE, CHSS, CCSK, VCP5

United States Cyber Security & Privacy Architect

Strategic Government Programs



# Highlights of the Report

1 *Targeted Attacks*

2 *Mobile*

3 *Vulnerabilities*

4 *Mac*

# Threat Landscape

A fundamental shift...



Hacking

Cyber Crime

Cyber Espionage

Cyber Warfare

# Hackers for Hire Make Malware Big Business

10 Months

Average length of time zero-day attacks sit and silently collect data

\$250,000

Top payout for hackers that successfully breach and remain undetected

-Forbes, 10/16/2012

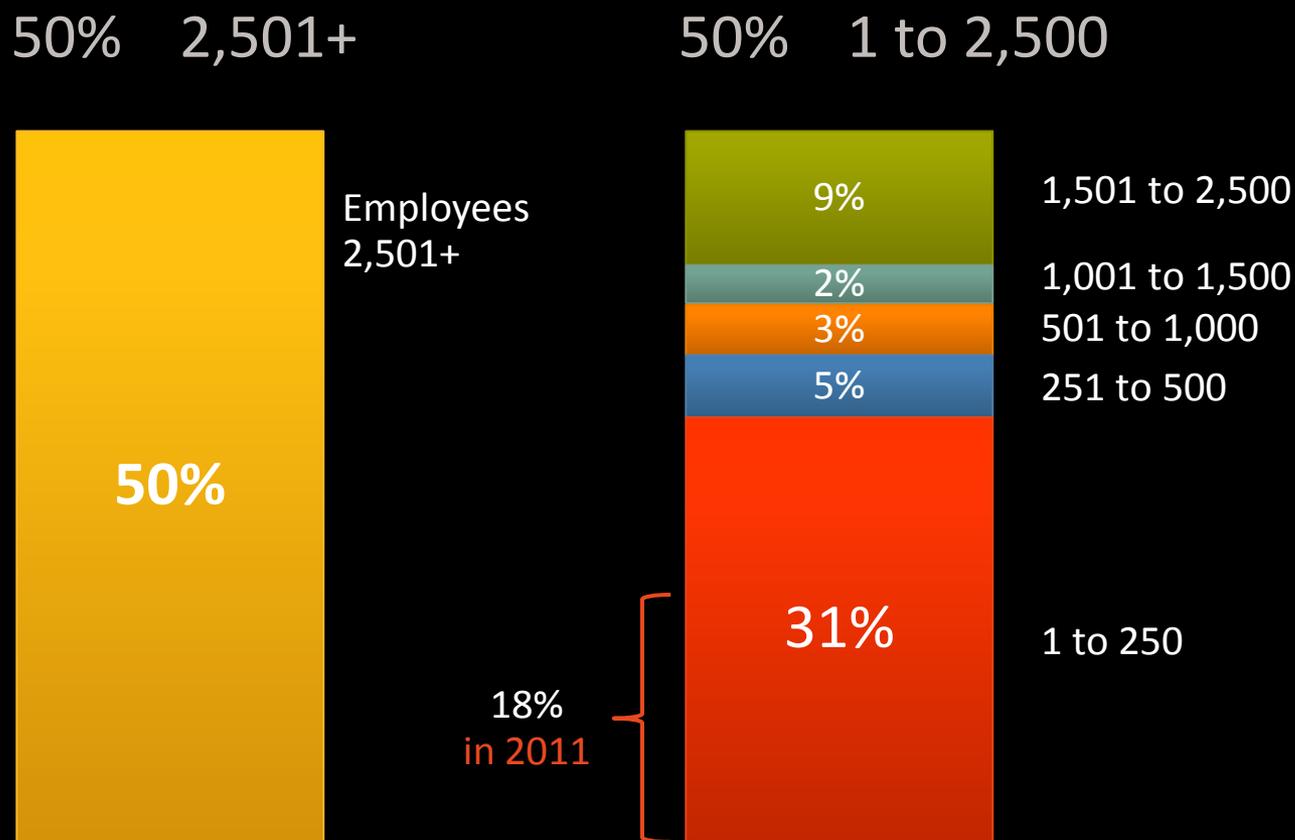


Targeted Attacks

up 42%

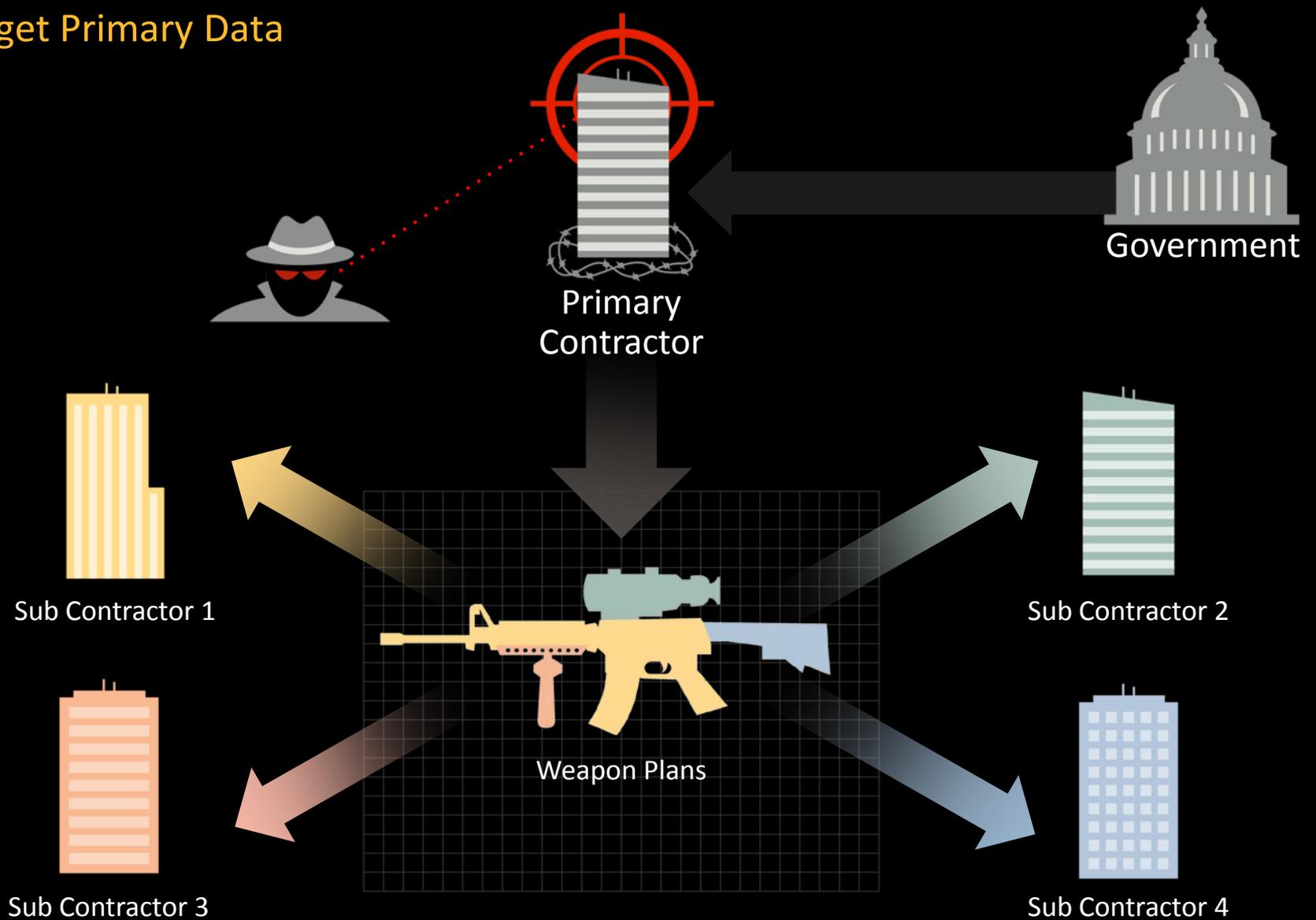
in 2012

# Targeted Attacks by Company Size

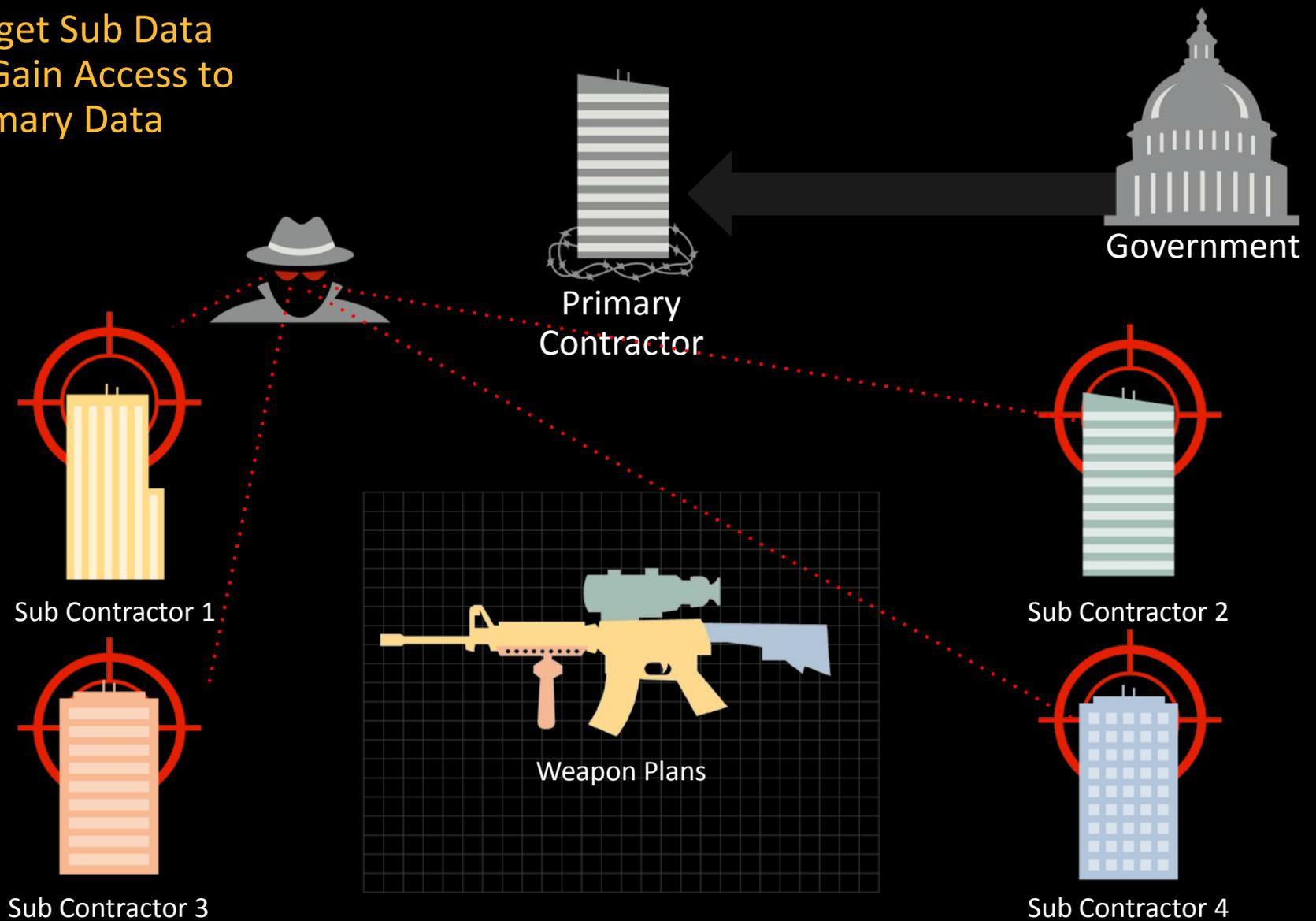


- Greatest growth in 2012 is at companies with <250 employees

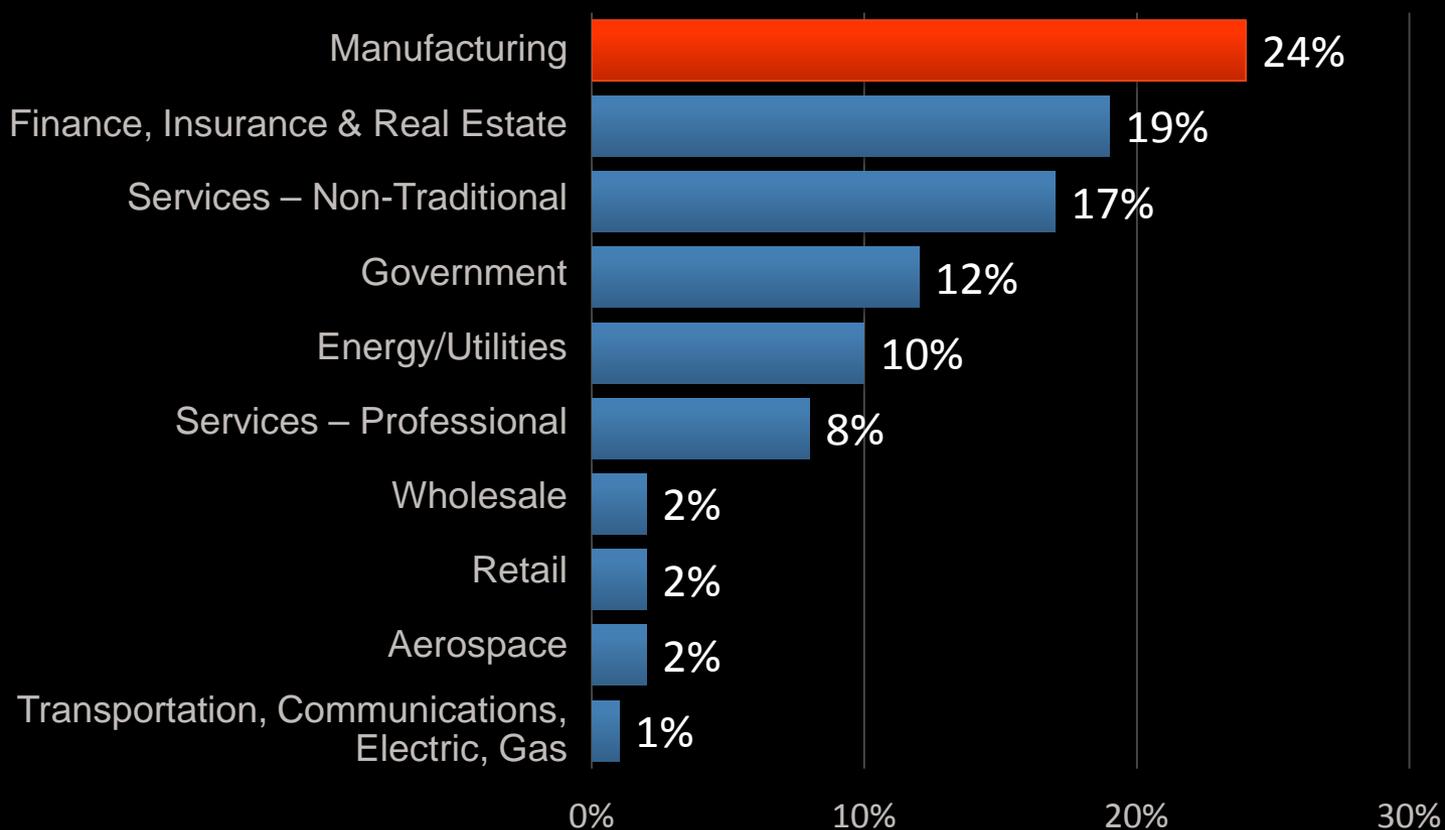
# Target Primary Data



# Target Sub Data to Gain Access to Primary Data

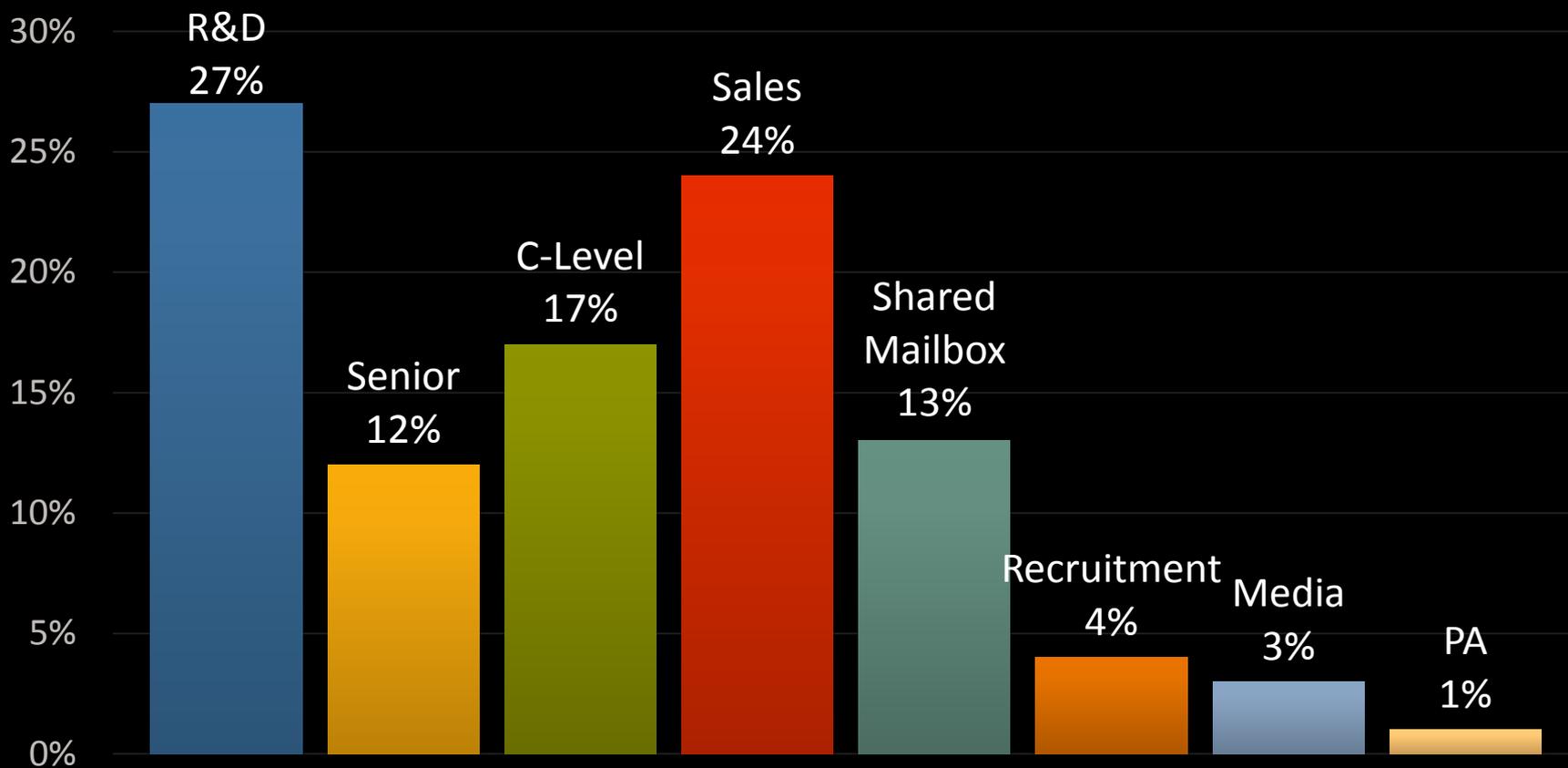


# Targeted Attacks by Industry



- Manufacturing moved to top position in 2012
- But all industries are targeted

## Targeted Attacks by Job Function



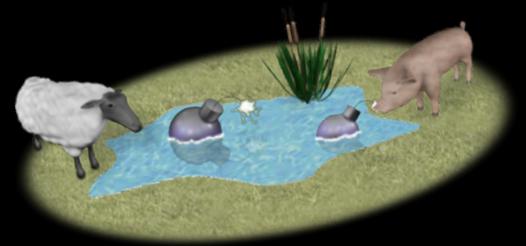
- Attacks may start with the ultimate target but often look opportunistically for any entry into a company

## Spear Phishing



Send an email to a person of interest

## Watering Hole Attack



Infect a website and lie in wait for them

# 2

## Infection vectors

# Effectiveness of Watering Hole Attacks

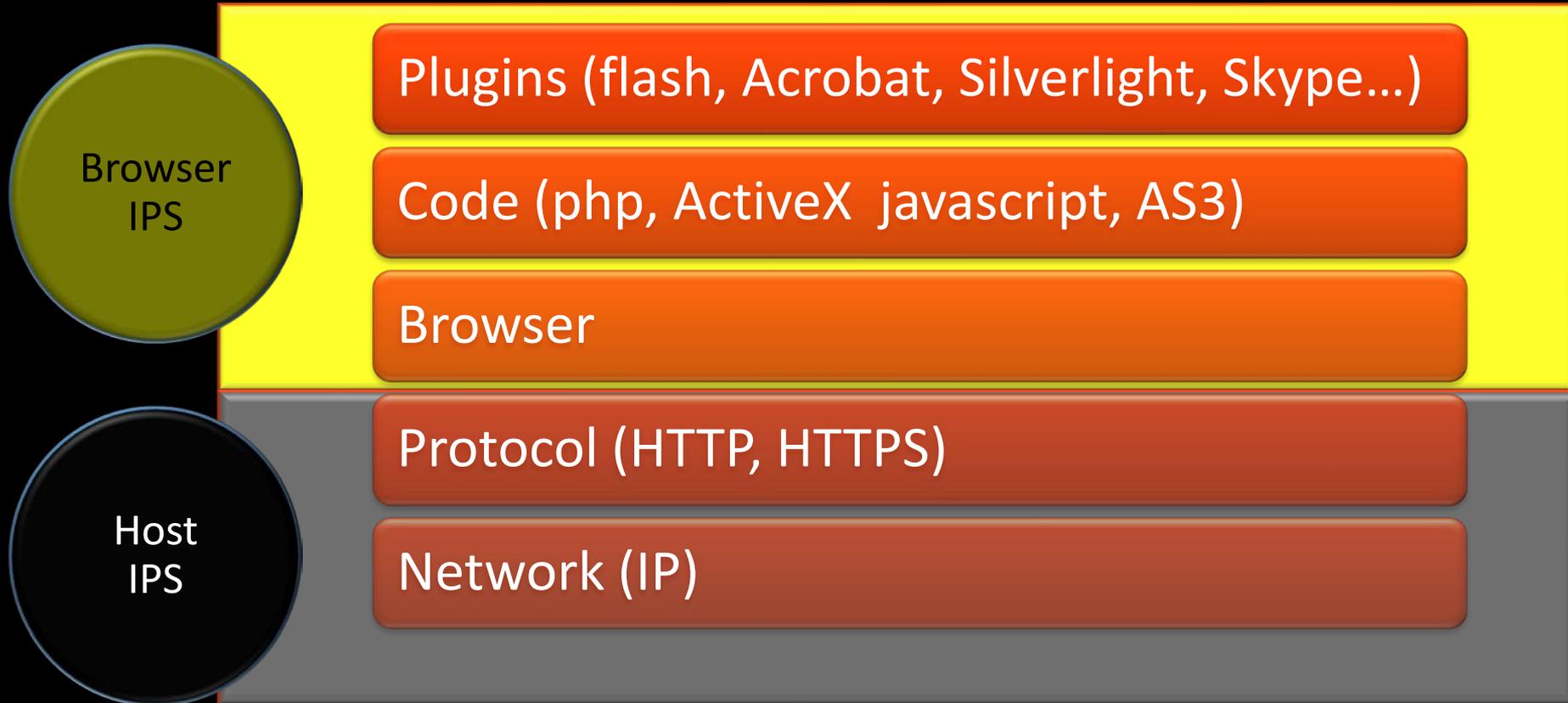
**1** Watering Hole  
Attack in 2012  
**Infected**  
**500 Companies**



All Within  
**24**  
**Hours**

- Watering Hole attacks are targeted at specific groups
- Can capture a large number of victims in a very short time

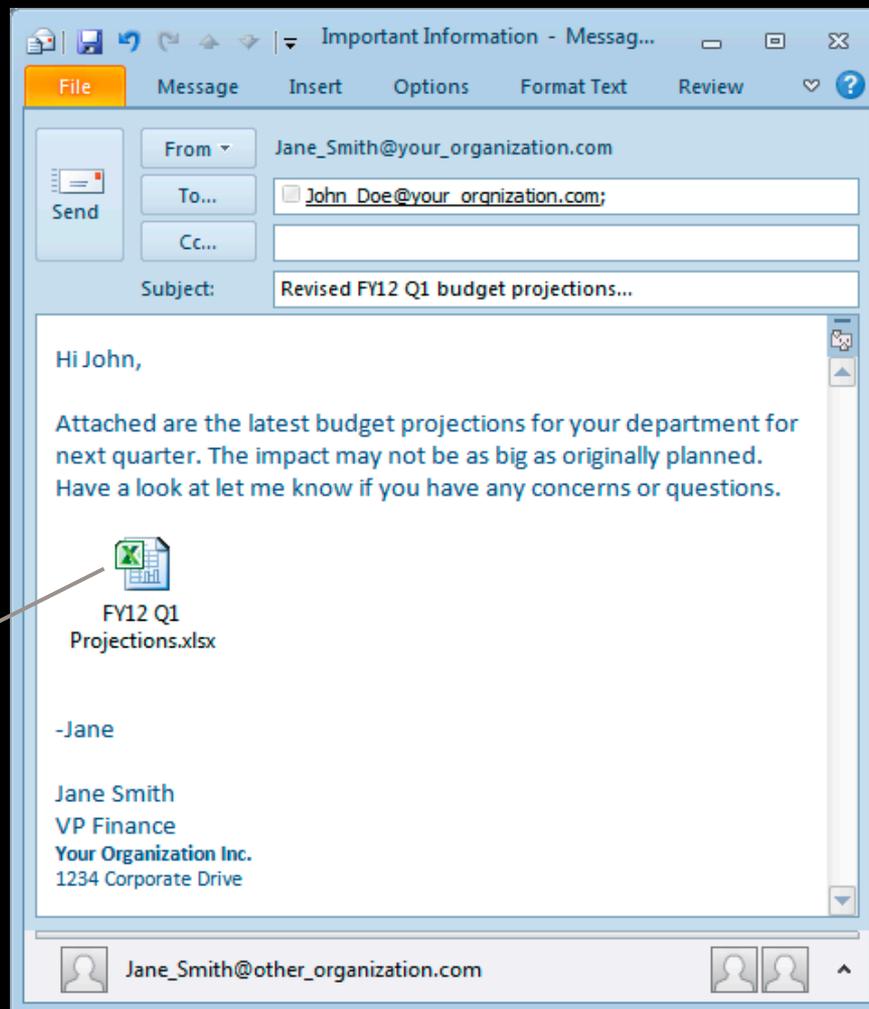
# The vulnerability being exploited is the browser and plugins



## Threat Landscape

# Attack scenario #1

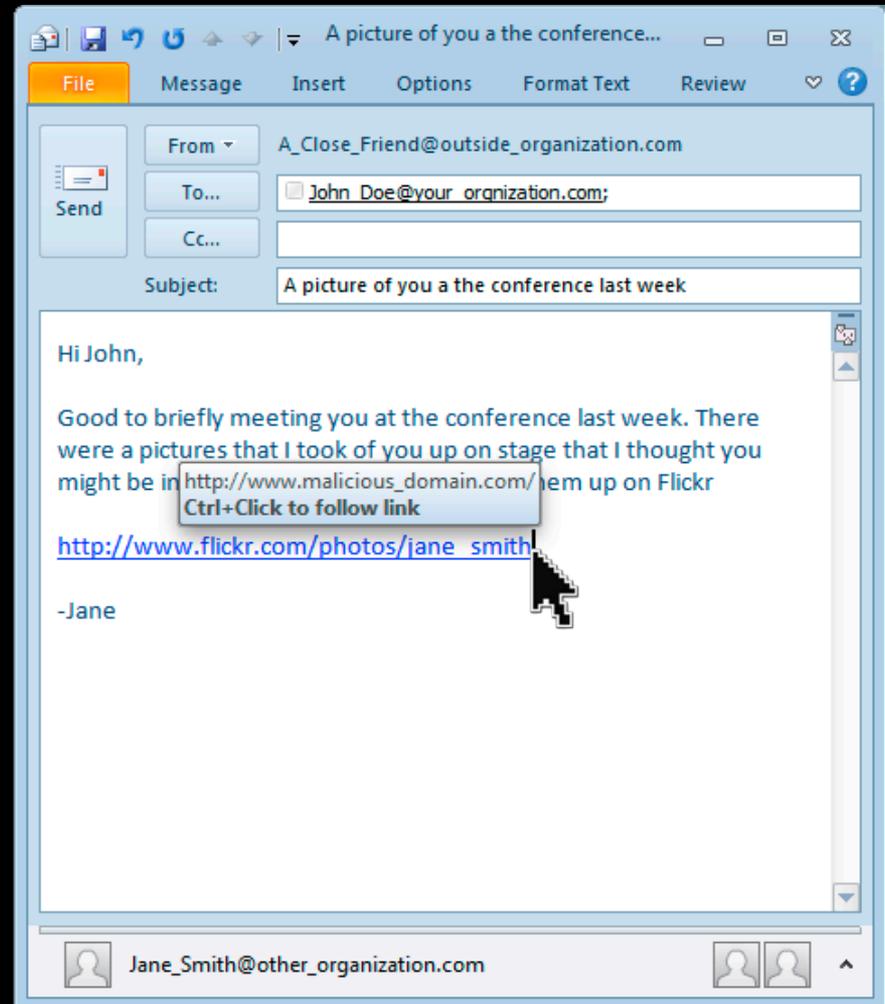
- It can start with an attachment
- Buried inside may be an embedded 'Flash' object
- Which leverages a vulnerability to deliver malware



## Threat Landscape

### Attack scenario #2

- More likely it will be a link
- Seems innocuous, right?
- Well not so fast...
- Hover over the link to see the real link buried underneath
- Clicking the link brings you to a malicious web site



# Mobile Trends

# Vulnerabilities & Mobile Malware

Platform	Vulnerabilities
Apple iOS	387
Android	13
Blackberry	13
Windows Mobile	2



Device Type	# of Threats
Apple iOS Malware	1
Android Malware	103
Symbian Malware	3
Windows Malware	1

- Today there is no significant link between mobile OS vulnerabilities and exploitation by malware
- In the future that may change

# Vulnerability Patching



# Malicious apps are the avenue



## Trends

# Mobile Threats

- Can you tell which one is the right legitimate app?



- Most malware for mobiles are Trojans posing as legitimate apps
- Mobiles will be targeted more when used for financial transactions



## Verify apps?

Allow Google to check all apps installed to this device for harmful behavior?

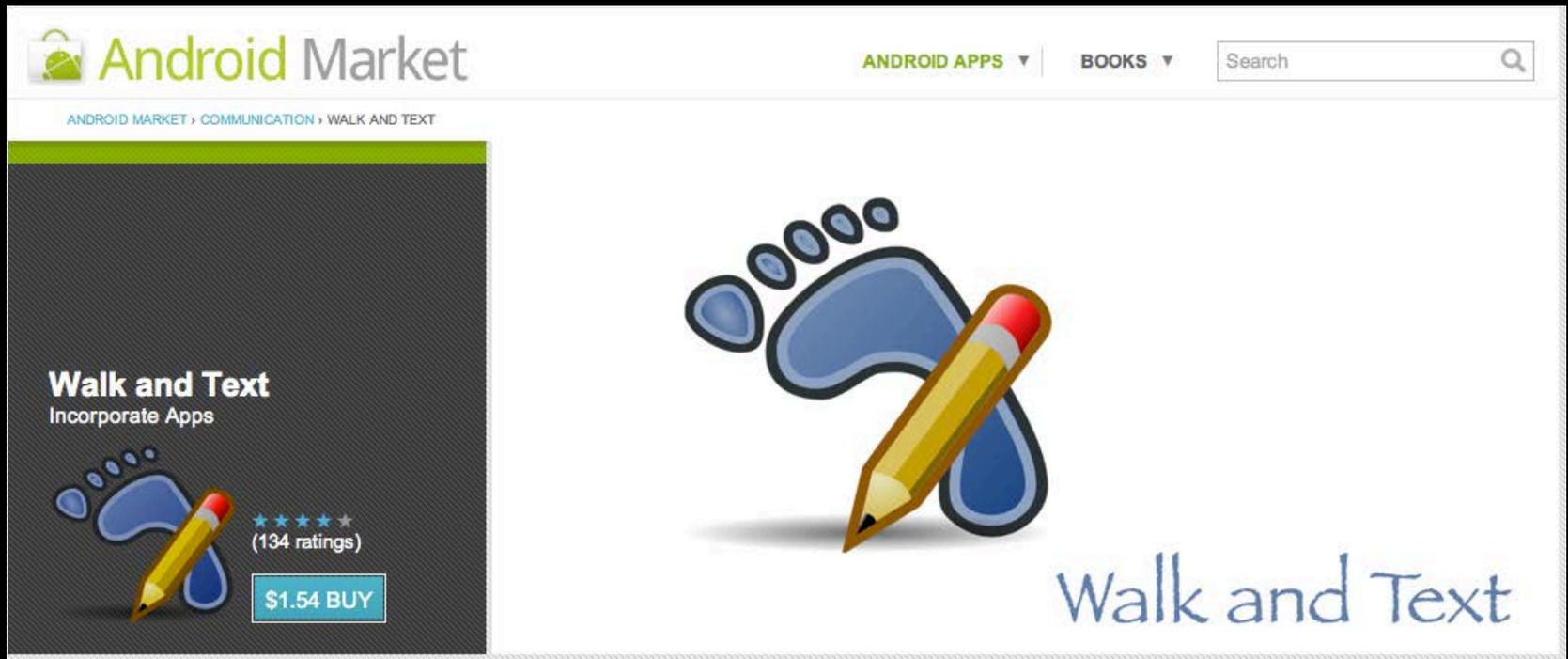
To learn more, go to Settings > Security.

Disagree

Agree

# Mobile Threats

“Have you heard, there’s an app for that...”



The image shows a screenshot of the Android Market interface. At the top, the 'Android Market' logo is on the left, and navigation options for 'ANDROID APPS' and 'BOOKS' are on the right, along with a search bar. Below the navigation, a breadcrumb trail reads 'ANDROID MARKET > COMMUNICATION > WALK AND TEXT'. The main content area features a large graphic of a blue footprint with a yellow pencil resting on it, and the text 'Walk and Text' in a blue, handwritten-style font. On the left side of this graphic, there is a smaller version of the footprint and pencil, along with a star rating of four stars and '(134 ratings)', and a blue button labeled '\$1.54 BUY'.

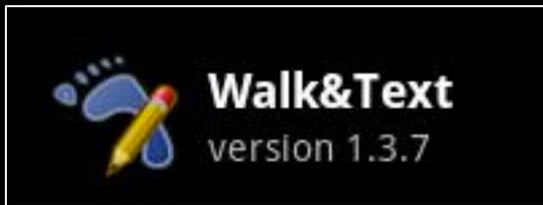
# Mobile Threats

Unfortunately there's also a 'trojanized' version too...

- Found on 3rd party sites and torrents
- Self signed



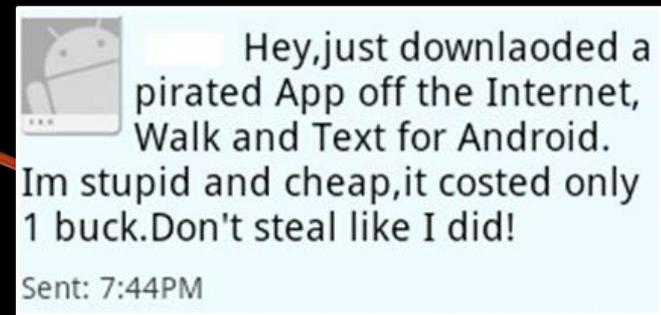
IMEI, Name, Phone Number



It does two things:

1. Sends info to a remote location
2. Sends an SMS to all your contacts

SMS



**Android.Walkinwat**

# Vulnerabilities

## Threat Landscape

# How often are we being attacked?



# 3,050,000,000

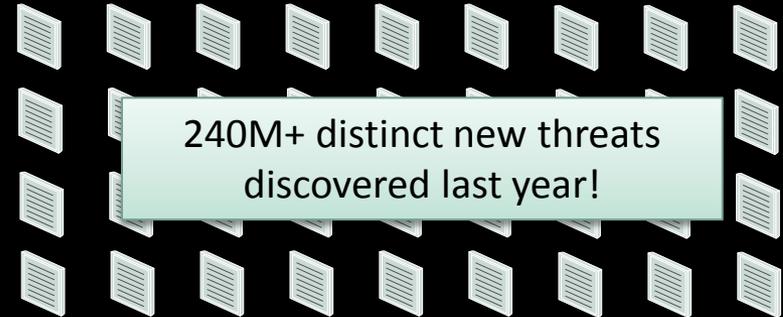
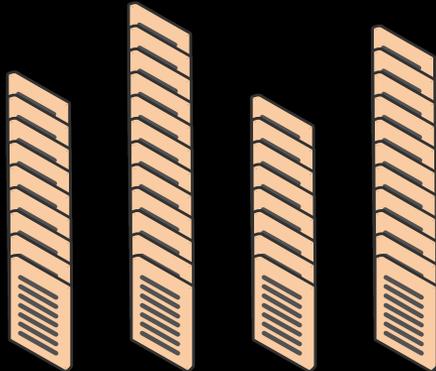
attacks blocked by Symantec in 2010

- 14 new 0day vulnerabilities
- 163 new mobile vulnerabilities
- 6,253 new vulnerabilities
- 286,000,000 new malware variants

In the time it takes to give this presentation, we will block more than 365,000 attacks!

## The Problem

# Malware authors have switched tactics



### From:

A mass distribution of a relatively few threats e.g.

- **Storm** made its way onto millions of machines across the globe

### To:

A micro distribution model e.g.

- The average **Vundo** variant is distributed to 18 Symantec users!
- The average **Harakit** variant is distributed to 1.6 Symantec users!

What are the odds a security vendor will discover all these threats?

## Our Websites are Being Used Against Us

**53%**

of legitimate websites have unpatched vulnerabilities

**24%**

have critical vulnerabilities unpatched

**61%**

of malicious web sites are legitimate sites

# Ransomware

**16**

Number of criminal gangs involved in this cybercrime

**\$5 Million**

Estimated amount extorted from victims in 2012

**500,000**

Average number of attacks seen from one threat in 18 day period



# Your computer has been locked!

## Your computer has been locked due to suspicion of illegal content downloading and distribution.

Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)

18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

**Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to \$250,000.**

**In order to resolve the situation in an above-mentioned way you should pay a fine of \$300.**

### HOW TO UNLOCK YOUR COMPUTER:

1 Take your cash to one of this retail locations:

Walmart K

CVS pharmacy Walgreens

2 Get a MoneyPak and purchase it with cash at the register

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code:

1	2	3
4	5	6
7	8	9
Delete	0	Enter

# Mac Malware



# Mac Malware



## Flashback

But in 2012  
**1 Mac Threat**  
infected 600,000  
Machines.

MacBook Pro

# Beyond the Main Report

- Video
- Infographics
- Podcast
- More ...

[symantec.com/threatreport](http://symantec.com/threatreport)

**Symantec Enterprise** | United States | Shopping | Search

Products & Solutions | Support & Communities | **Security Response** | Try & Buy

Security Response | Annual Threat Report | Add

## Security Response Publications

Symantec Security Response is a worldwide team of security engineers, threat analysts and researchers that develops a variety of content on the latest threats that impact organizations and end users.

**Annual Threat Report** Archives

### Internet Security Threat Report, Volume 18

The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape.

**DOWNLOAD MAIN REPORT**

2012 Threat Landscape  
50 pages, 15 MB (PDF)

**DOWNLOAD APPENDICES**

2012 Collected Data  
60 pages, 20 MB (PDF)

### Key Findings from Internet Security Threat Report, Volume 18

- 42% increase in targeted attacks in 2012.
- 36% of all targeted attacks aimed businesses with less than 250 employees.
- One waterhole attack infected 500 organizations in a single day.
- 14 zero-day vulnerabilities.
- 32% of all mobile threats steal information.
- A single threat infected 600,000 Macs in 2012.
- Spam volume continued to decrease, with 69% of all email being spam.
- The number of phishing sites spoofing social networking sites increased 125%.
- Web-based attacks increased 30%.
- 5,291 new vulnerabilities discovered in 2012, 416 of them on mobile operating systems.

[Share this information](#)

### Infographics

View or share graphics that highlight some of the key findings from this year's report.

#### Mobile Vulnerabilities

2012	<b>411</b>
2011	<b>315</b>
2010	<b>163</b>

[View/share this image](#)

#### Bot Zombies (in millions)

2010	<b>4.5</b>
2011	<b>3.1</b>
2012	<b>3.4</b>

[View/share this image](#)

**Internet Security Threat Report, Volume 18**

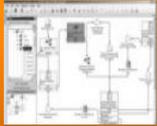
**DOWNLOAD MAIN REPORT**

2012 Threat Landscape  
50 pages, 15 MB (PDF)

**DOWNLOAD APPENDICES**

2012 Collected Data  
60 pages, 20 MB (PDF)

# Industry recommended strategy to protect information



## Develop and Enforce IT Policies

Policy & standards modules, risk manager & vulnerability modules and solutions



## Authenticate Identities

Two-factor authentication, Managed Public Key Infrastructure solutions



## Protect the information

Data Loss Prevention, Encryption, Backup and High availability solutions



## Manage the Infrastructure

Desktop and server patch management, software delivery, assets, ticket management and mobile devices solutions



## Protect the Infrastructure

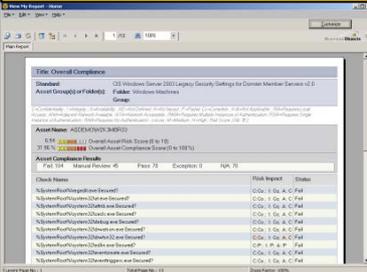
Malicious Endpoint Protection, Web Gateway, Message Gateway, and Critical Systems Protection solutions

1

# Governance Tools to Develop and Enforce IT Policy

# Governance, Risk and Compliance

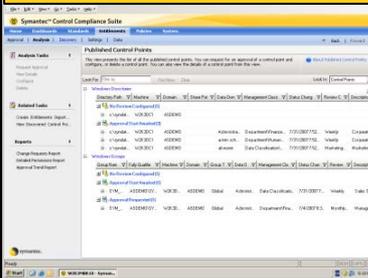
## Audit Reports



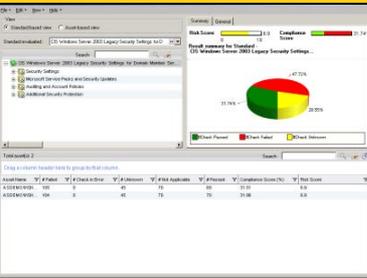
## Dashboards



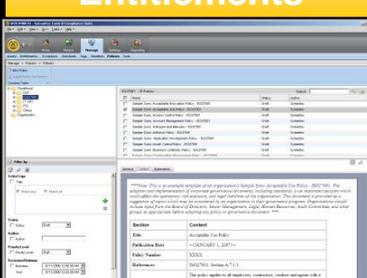
## External Policies



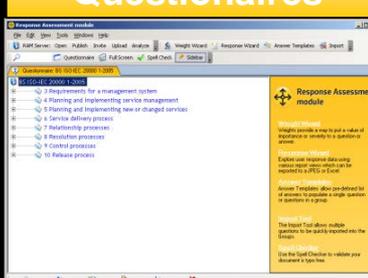
## Standards



## Entitlements



## Questionnaires



## Federated Data Processing and Analysis





# Authenticate Identities

# Strong Authentication and MPKI



**Government**



**Endpoint**



**Application**



**Mobility**





# Data Loss Prevention

## Storage

Data Loss Prevention  
**Network Discover**

Data Loss Prevention  
**Data Insight**

Data Loss Prevention  
**Network Protect**

## Endpoint

Data Loss Prevention  
**Endpoint Discover**

Data Loss Prevention  
**Endpoint Prevent**

## Network

Data Loss Prevention  
**Network Monitor**

Data Loss Prevention  
**Network Prevent**

# Encryption of sensitive data



Whole Disk



Removal Hard-drive



Help Desk



4

# Manage the Infrastructure

# Enterprise Systems Management



Dell Management Console  
Dell Client Manager

vPro™ enabled computer management

HP Client Manager

System Management Platform

Third-Party Solutions

Illustration of various IT hardware including a laptop, server tower, CD/DVD, and desktop monitor.

Mobile Security Management

Backup Management

Application Virtualization

Power Management

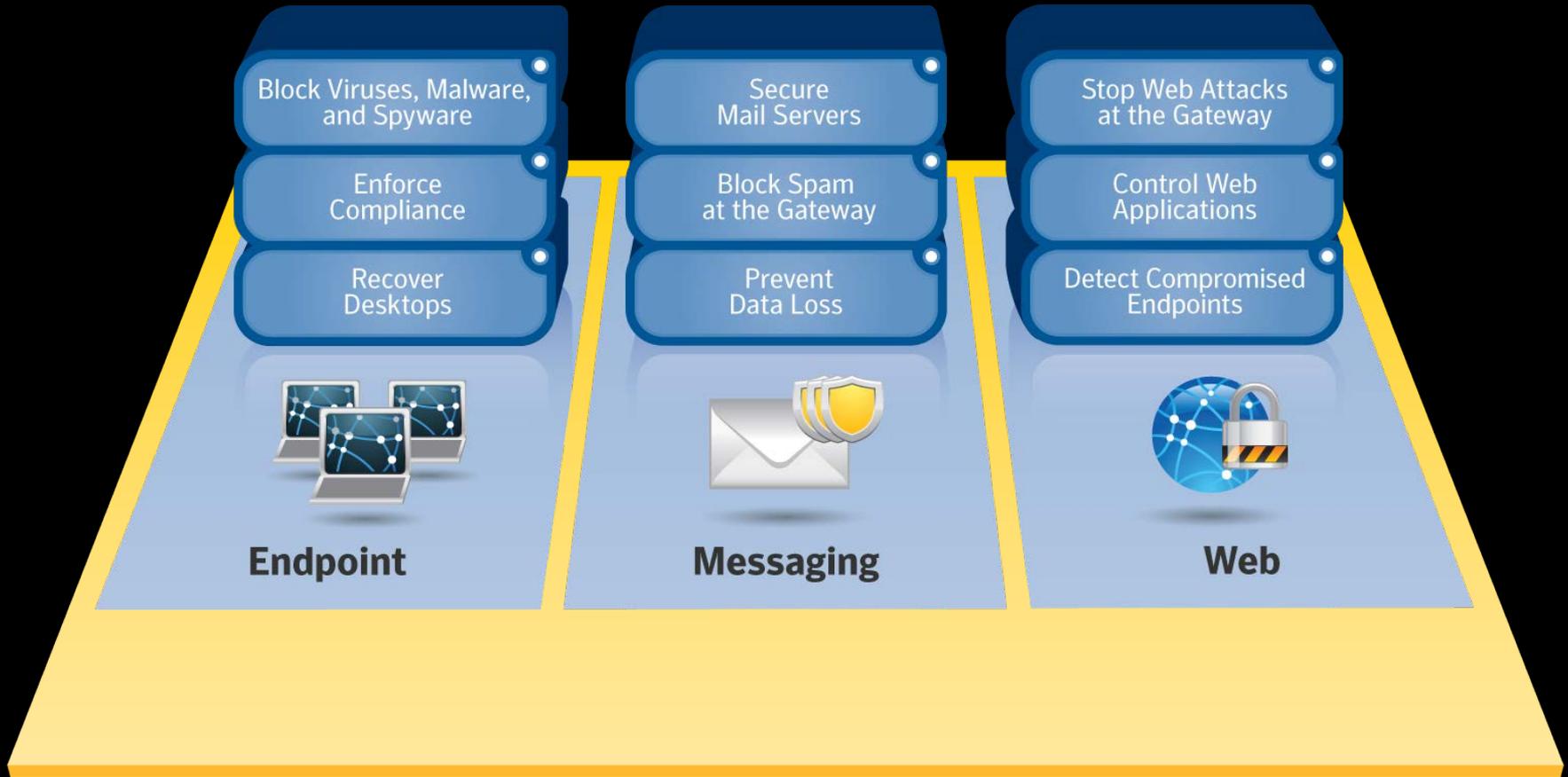
HelpDesk Management

Patch and System Management

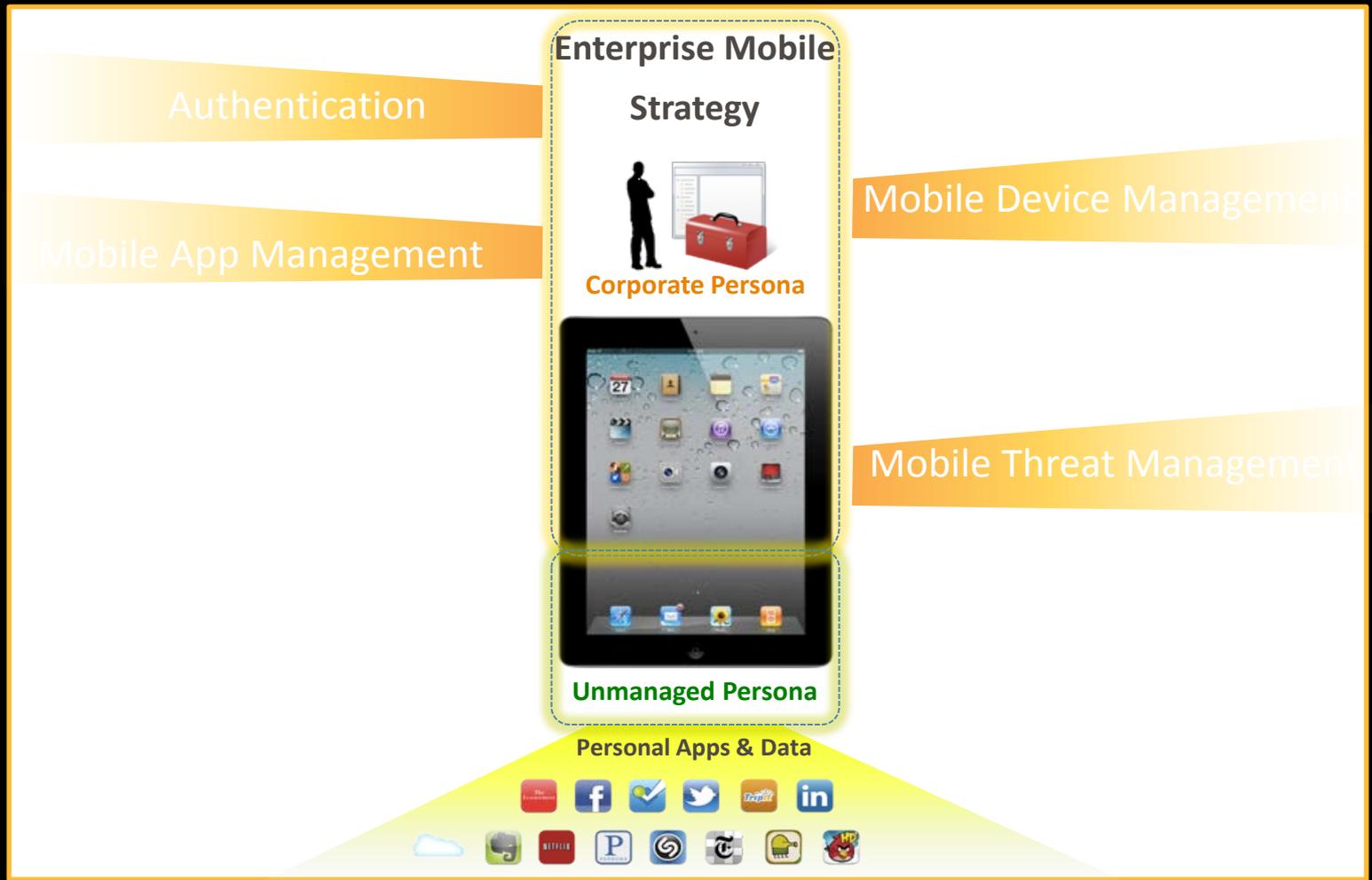
5

# Protect the Infrastructure

# Threat management solutions



# What about a mobility strategy?



# Quiz

- **What is the #1 industry for targeted attacks?**
  - Retail
  - Manufacturing
  - Government
- **True or False: The CEO and Executive board are the #1 targeted individuals of an organization? Why or Why not?**
- **To protect an organization a company must do what first?**
  - Encrypt information
  - Authenticate users
  - Develop corporate policies