Looking Back at Three Years of Targeted Attacks

Lessons Learned on the Attackers' Behaviors and Victims' Profiles

Olivier Thonnard

Principal Research Engineer

OUTLINE

1. Introduction
2. Targeted Attack Intelligence
3. Victims Profiles: Organizations and Individuals
4. Conclusions and Lessons Learned

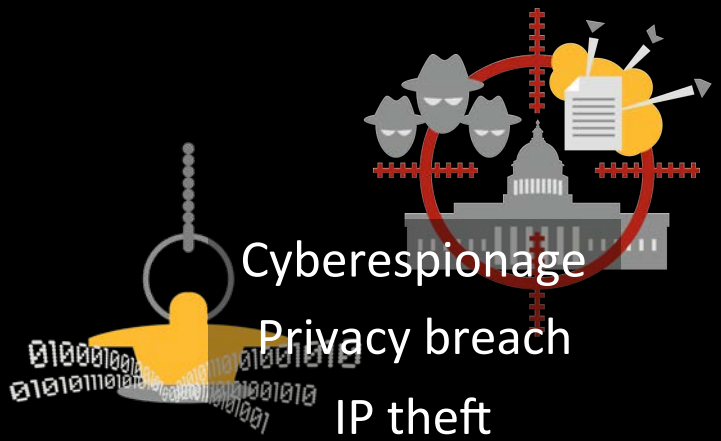
Introduction

Targeted Attacks – Symantec TRIAGE methodology

Characteristics of Targeted Attacks

Targeted

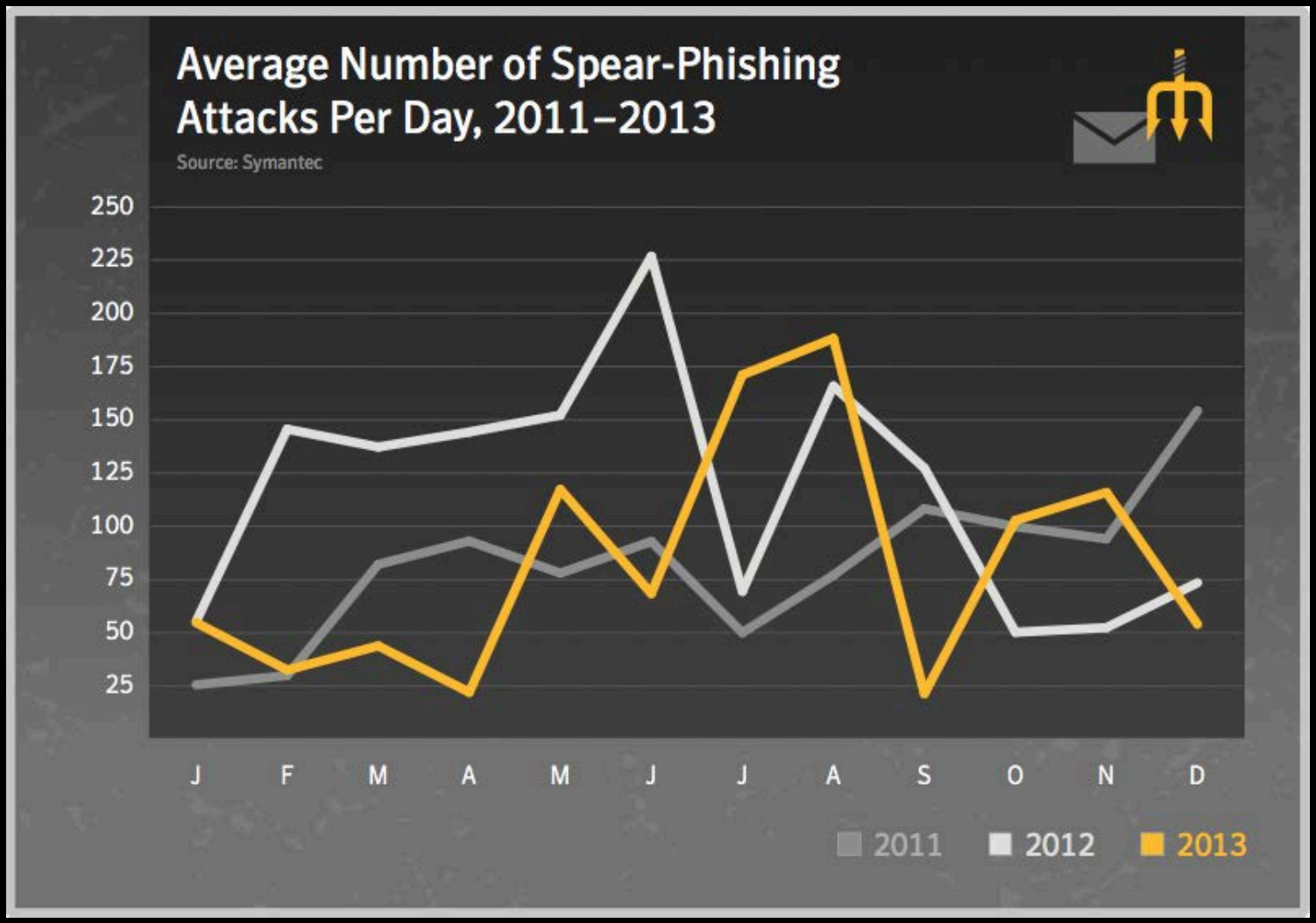
- Attack relevant to interests of recipient
- Low copy number
- Tailored malware, often embedded in weaponized documents
- Obscure business model



Non-targeted

- No regard to recipient
- High volume
- Common malware, often based on exploit kits
- Clear revenue stream

Targeted Attacks – 2011-2013



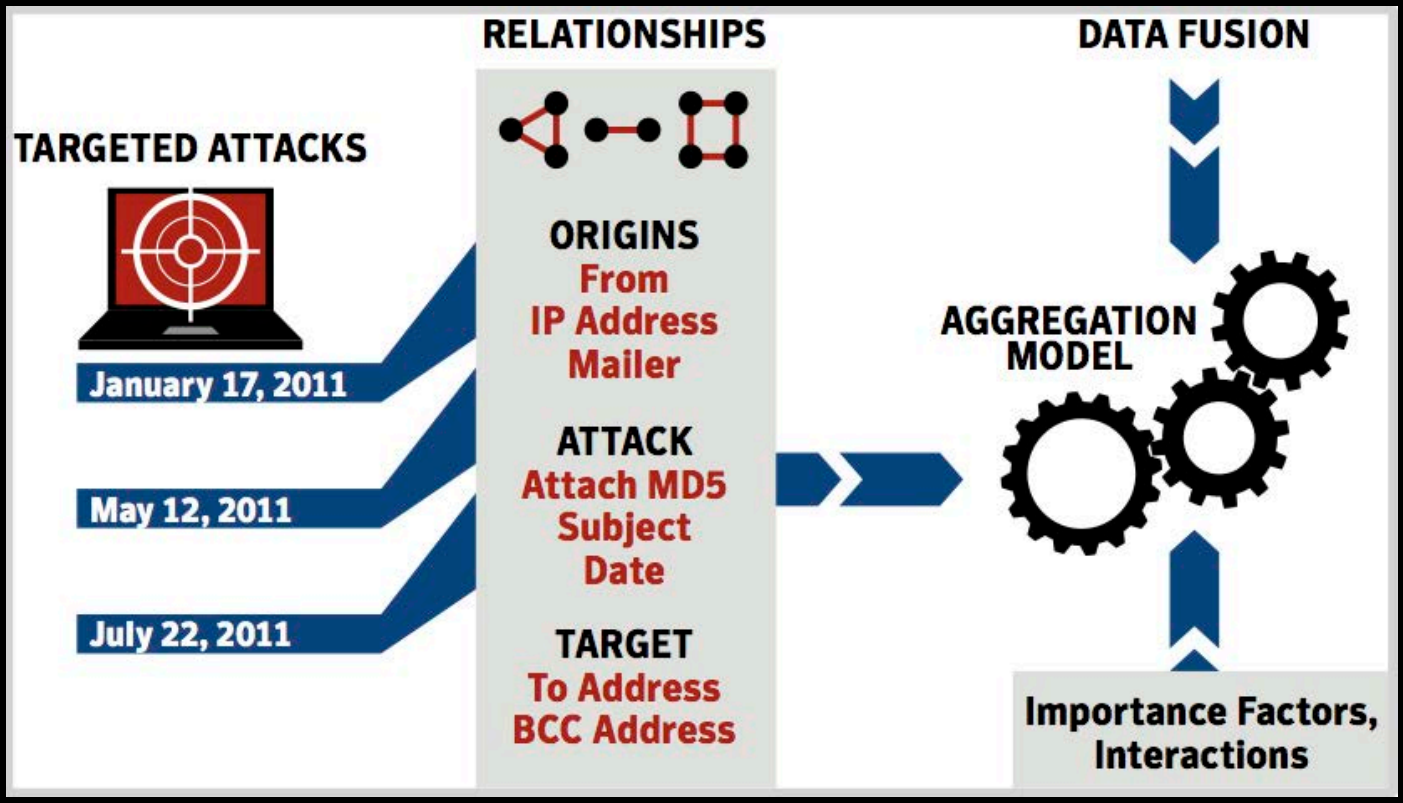
Data Set

Spear Phishing Emails

- **SKEPTIC** (and a combination of various filters/analyzers) used to block targeted attacks sent to Symantec.cloud customers
- Data set: over 100K attack emails blocked between 2011 → 2013
- Every email attachment was further analyzed:
  - AV Signatures from most common AV engines
  - Dynamic analysis: file and registry activities, network activity
- IP addresses of attackers mapped to geographical location
- Targeted recipients and domains mapped to industry sectors
  - Based on the SIC taxonomy

→ The enriched dataset was fed to TRIAGE for multi-dimensional clustering analysis and campaign/threat group identification

Going from isolated attacks to coordinated campaigns (attribution)

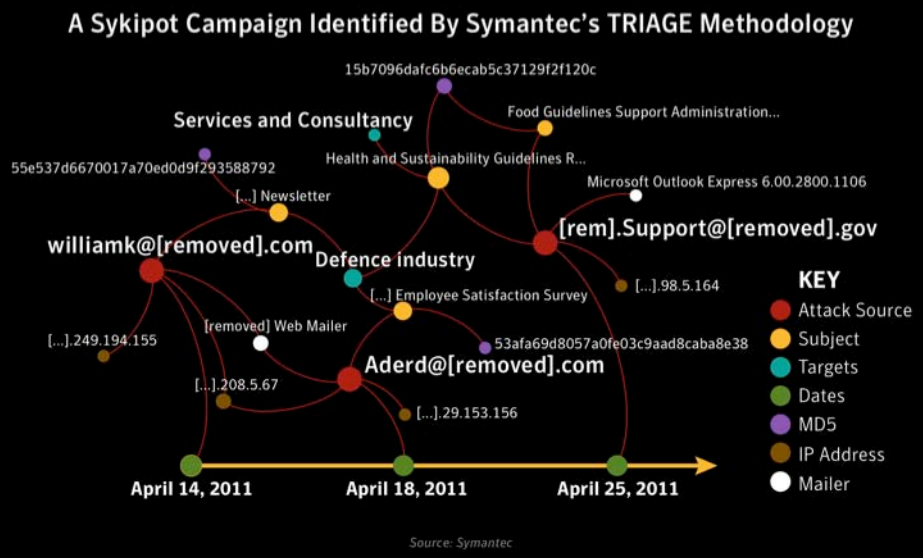


Symantec TRIAGE technology:
identifies attack campaigns performed by various threat groups

An Attack Campaign

A series of emails that:

- Show clear evidence that the subject and target has been deliberately selected.
- Contain at least 3 or 4 strong correlations to other emails, such as the topic, sender address, recipient domain, source IP address, etc.
- Are sent on the same day or across multiple days.



A Sykipot campaign (2011)

Typical Use case:

Bottom-up Forensics Analysis

- **Start from specific IOC's:**
  - **MD5**: 78c3d73e2e2bba6d8811c5dc39edd600
  - Zero-day exploit: **CVE-2012-0779**
  - **C&C**: 126.19.84.7

→ **Any previously identified campaign associated to one of these IOC's ?**

  - Find and visualize all related attacks (campaign analysis)
  - Quickly identify which "threat group" is likely behind these attacks

- **Other way around:**
  - **CommentCrew** is presumably linked to following IOC's:
    - **MD5**: e1117ec1ea73b6da7f2c051464ad9197
    - **C&C**: 50.115.140.211
    - **Exploit**: CVE-2012-0754.B

  → Can we identify an attack campaign associated to these IOC's ?

Why TRIAGE Analytics?

Intelligence Extraction and Attack Investigation

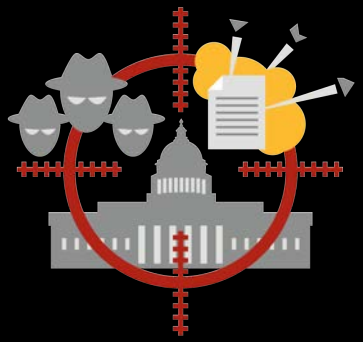
- Identify groups of attacks related to the same campaign, likely orchestrated by a specific "threat group"
- Correlate indicators across data sets, enterprises, geographies, industry sectors, etc
- Determine the patterns and behaviors of the intruders, i.e., their tactics, techniques, and procedures (TTP's)
- Find "how" they operate, rather than "what" they do
- Challenge: Intrusions sourced by the same attackers (group) may have varying degrees of correlation (md5, IP, from/to domains, attachments, etc)

Typical challenge addressed by TRIAGE

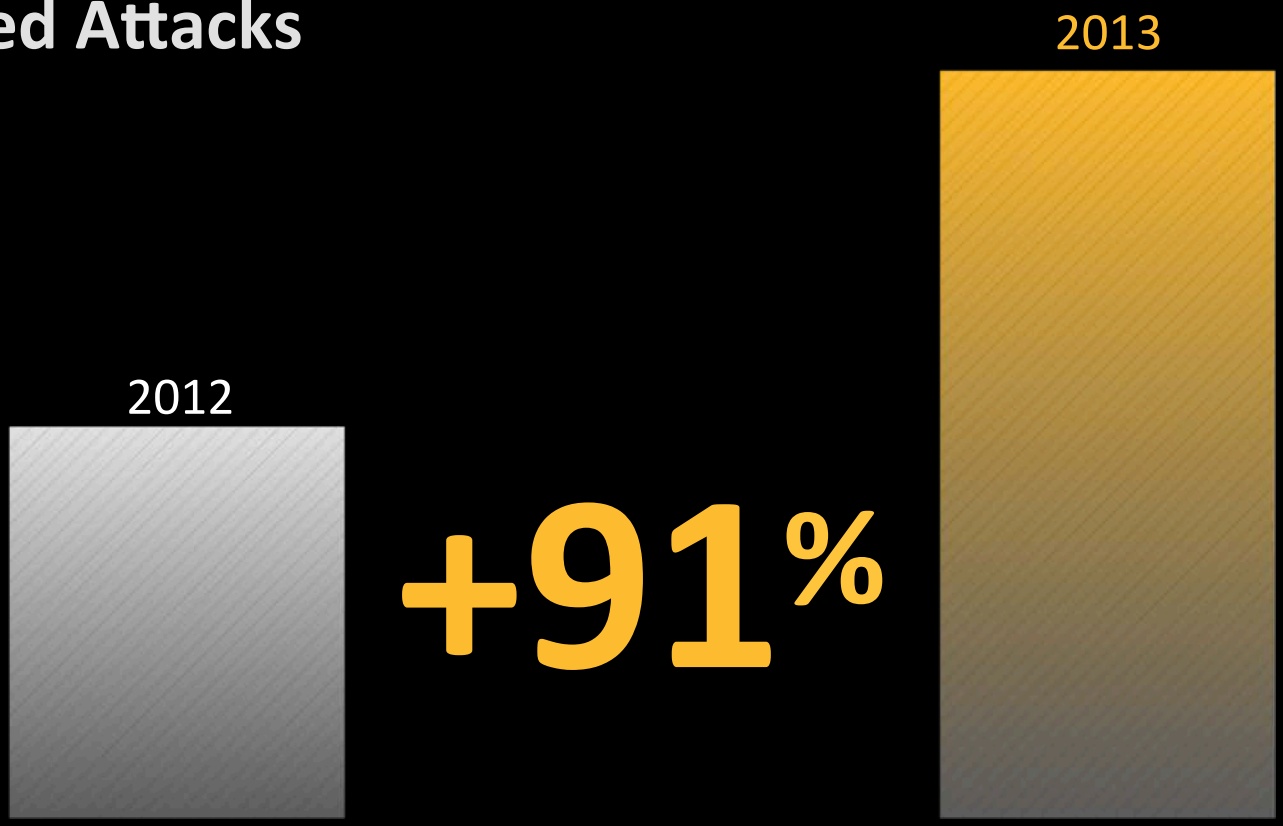
Identify Commonalities and Overlapping Indicators

Phase	Email feature	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	Recipient	[user1]@org1.gov.uk	[user2]@org2.gov.uk	[user3]@org2.gov.uk
Weaponization	Attach_name	Global Pulse Project***.pdf		Agenda – G20***.pdf
	Attach MD5	dd2ed3f7dead4a[***]		2e36081dd7f62e[***]
Delivery	Date	2011-05-13	2011-05-14	2011-07-02
	From addr.	[Att1]@gmail.com	[Att2]@gmail.com	
	Sender IP	74.125.83.***		74.125.82.***
	Subject	FW:Project Document	Project Document	G20 Ds Finance Key Info – Paris July 2011
	Email body	[body1]		[body2]
Exploitation	AV signature	CVE-2011-0611.C		
Persistence	C&C domains	www.webserver.***		[N/A]

Targeted Attack Intelligence

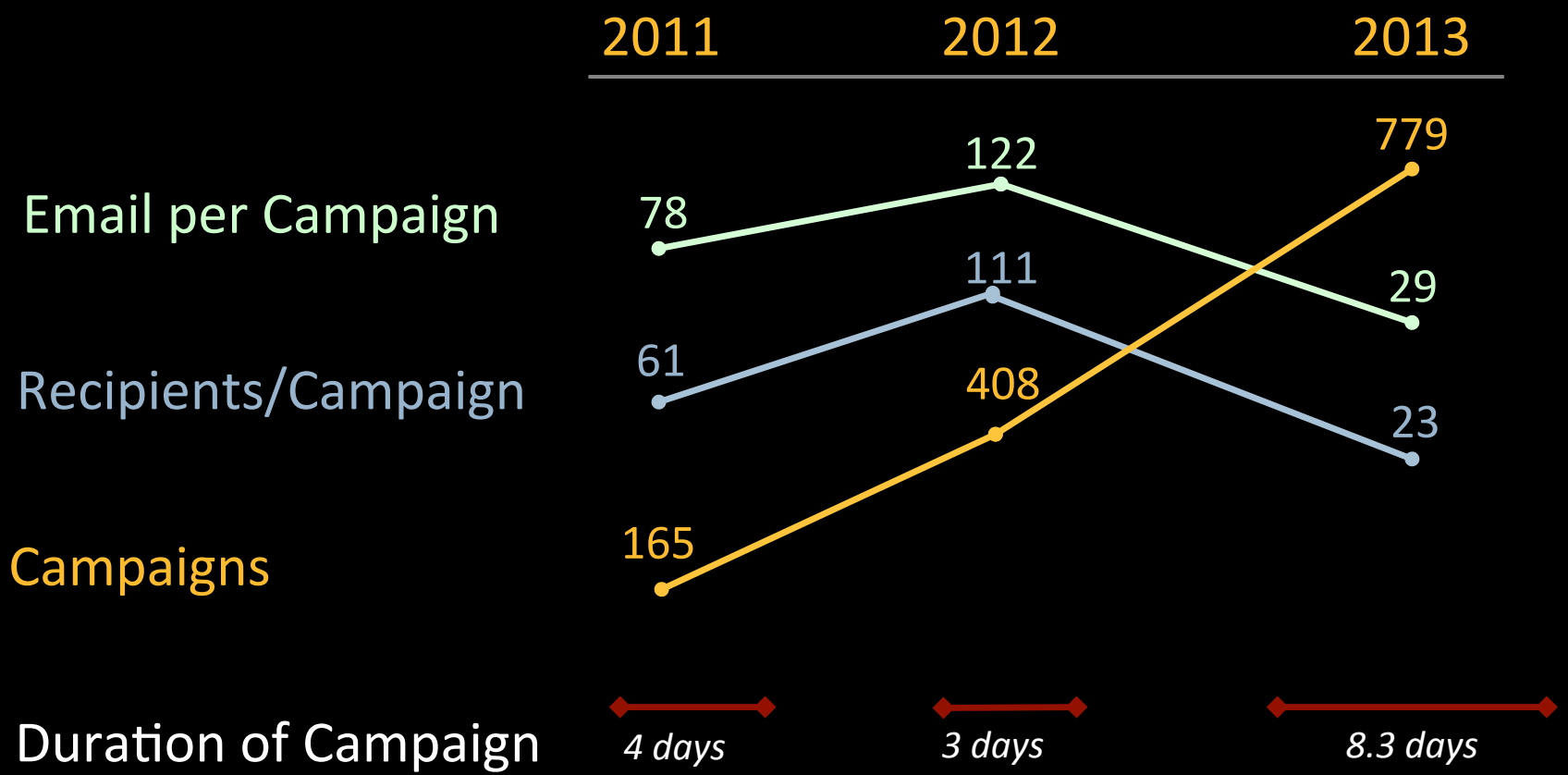


Targeted Attacks

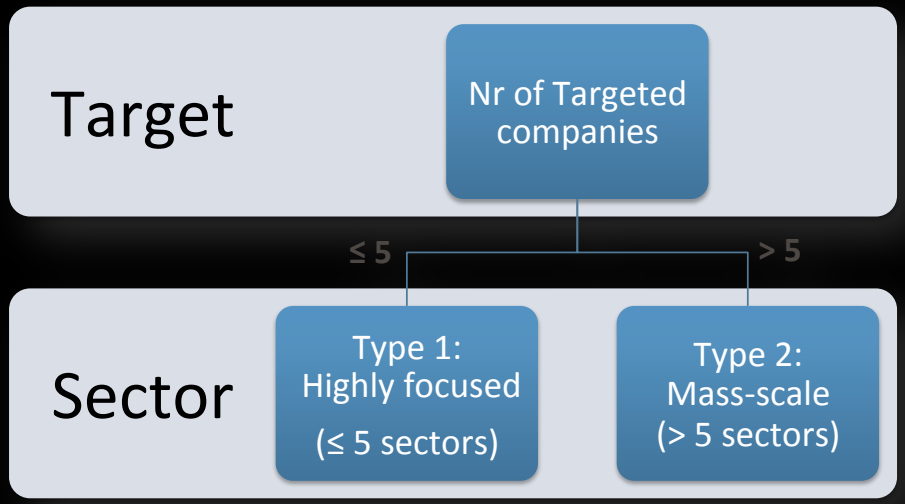


Increase in targeted attack campaigns

Targeted Attack Campaigns



Focused versus Large-scale campaigns

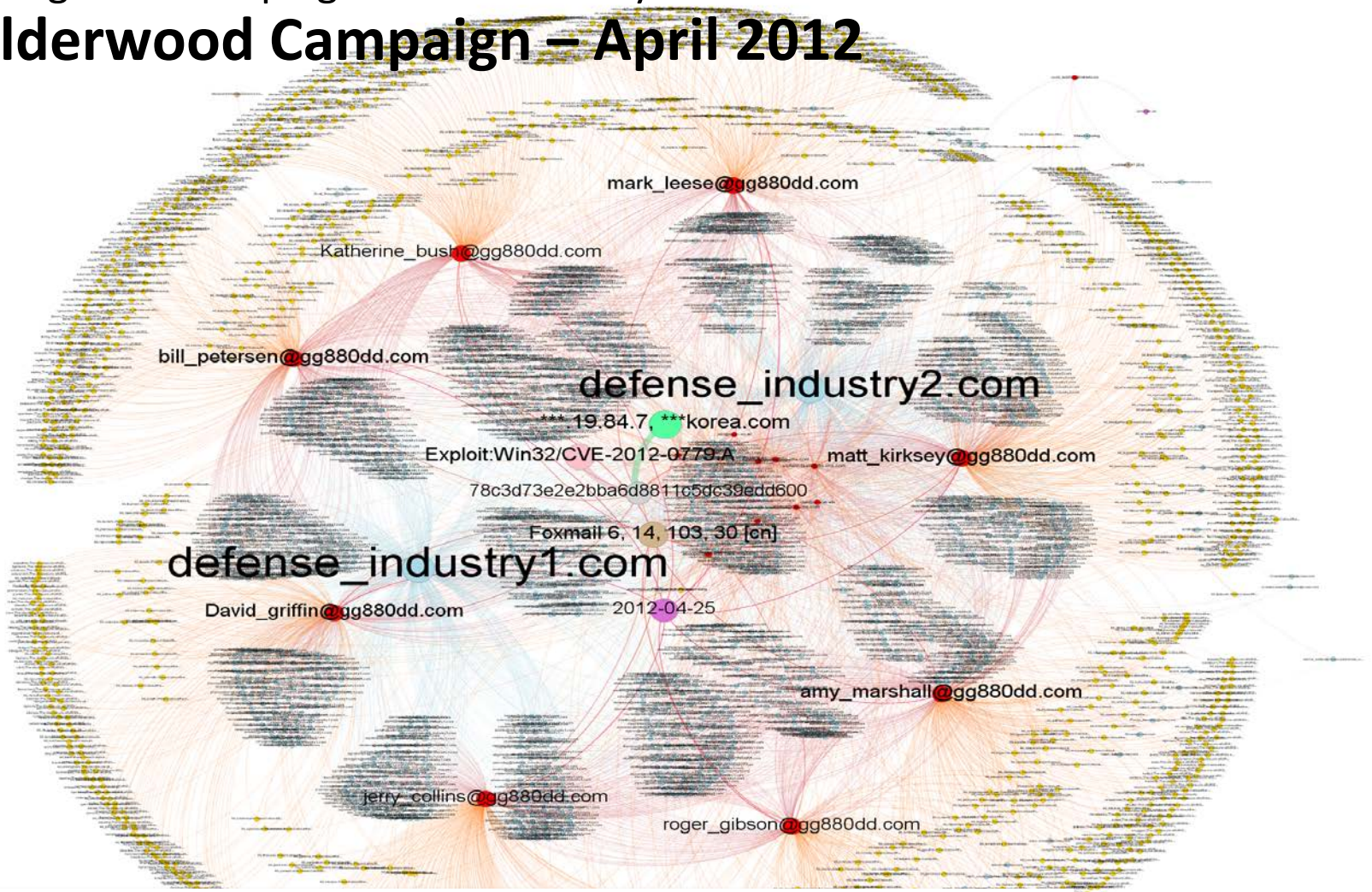


Type 1: More focused campaigns : **68 %**

Type 2: Mass-scale (MOTA): **32 %**

"Targeted" campaign does not always mean small in size!

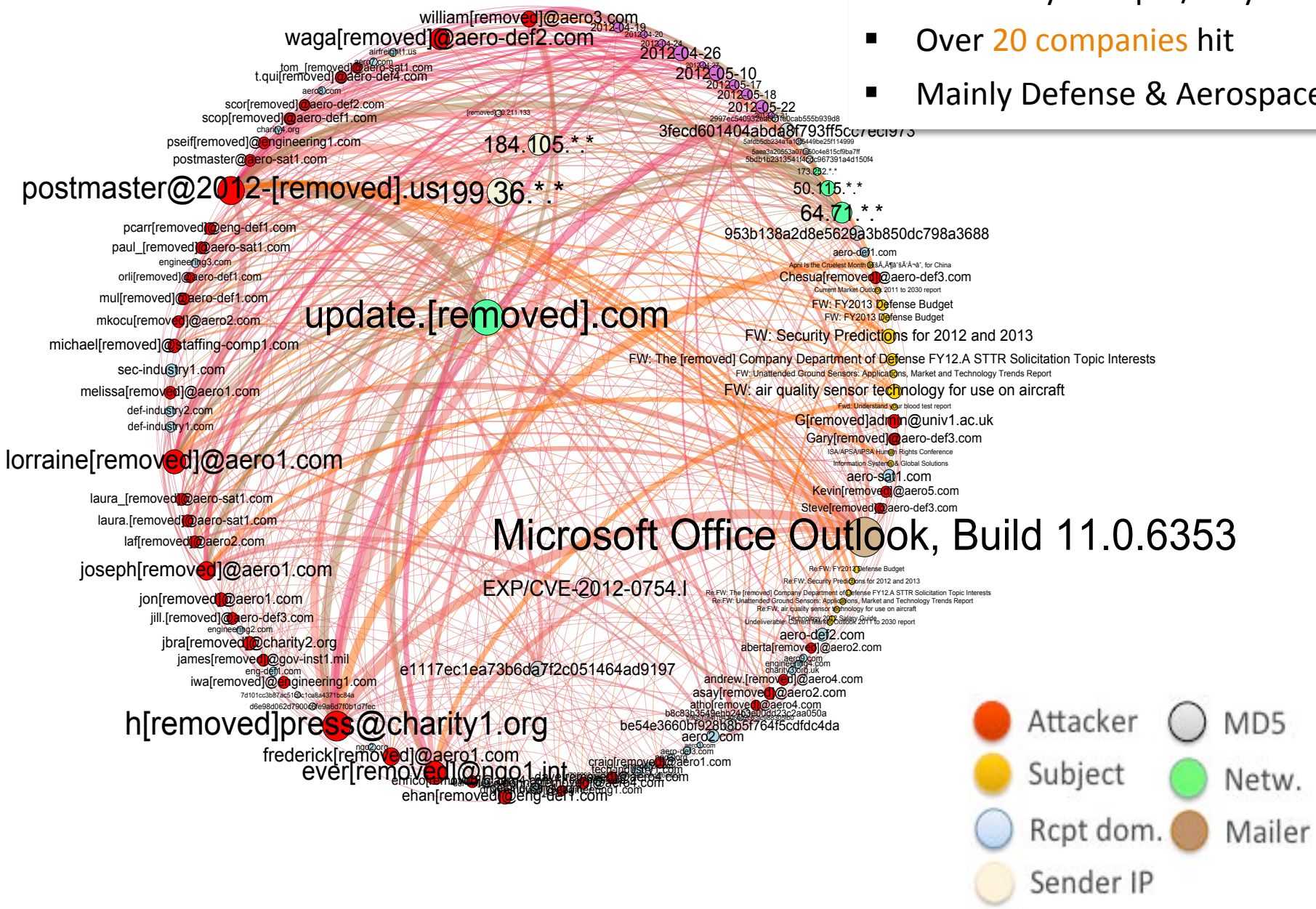
Elderwood Campaign – April 2012



- An Elderwood Campaign that used "gg880dd.com" accounts
- Over 1,800 attacks on **April 25, 2012**
- Exploits CVE-2012-0779 (**disclosed May 5, 2012**)
- Was targeting only 2 large Defense/Manufacturing industries

APT1/CommentCrew - CVE-2012-0754/0158

- 1200+ attacks
- On 10 days in April/May
- Over 20 companies hit
- Mainly Defense & Aerospace

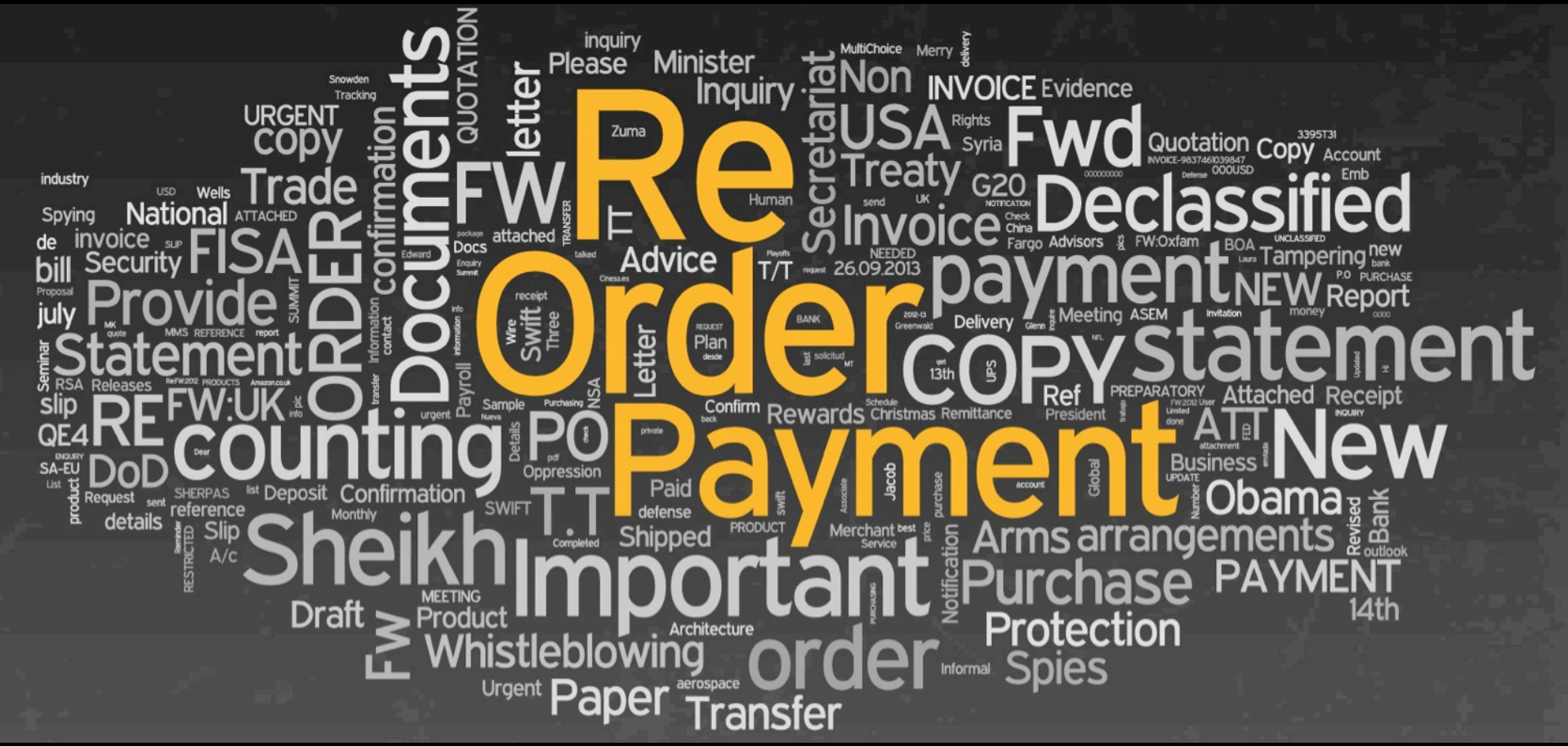


Doc types

Executable type	2013	2012
.exe	31.3%	39%
.scr	18.4%	2%
.doc	7.9%	34%
.pdf	5.3%	11%
.class	4.7%	<1%
.jpg	3.8%	<1%
.dmp	2.7%	1%
.dll	1.8%	1%
.au3	1.7%	<1%
.xls	1.2%	5%

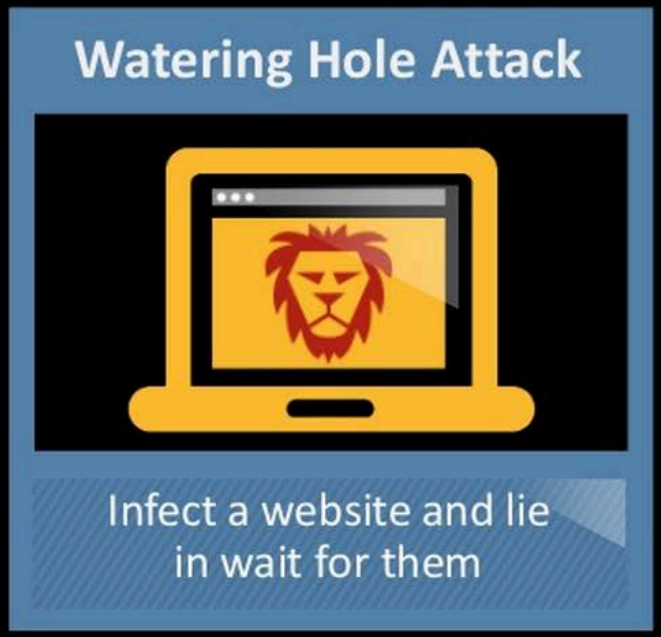
- More than 50 percent of email attachments used in spear phishing attacks were executable files in 2013.
- Microsoft Word and PDF documents are both used regularly, making up 7.9 and 5.3 percent of attachments, respectively. However, these are both down from 2012.
- Java .class files also made up 4.7 percent of email attachments used in spear phishing attacks.

Email Topics Used in Targeted Attacks



- Most frequently occurring words used in targeted spear-phishing email attacks throughout 2013.

“Watering Hole” Attacks (2012-2013)



- Targeted Attacks predominantly start as spear phishing attacks
- In 2012, Watering Hole Attacks emerged (popularized by the Elderwood Gang)

Effectiveness of Watering Hole Attacks

Watering Hole Attack in 2012

Infected 500 Companies

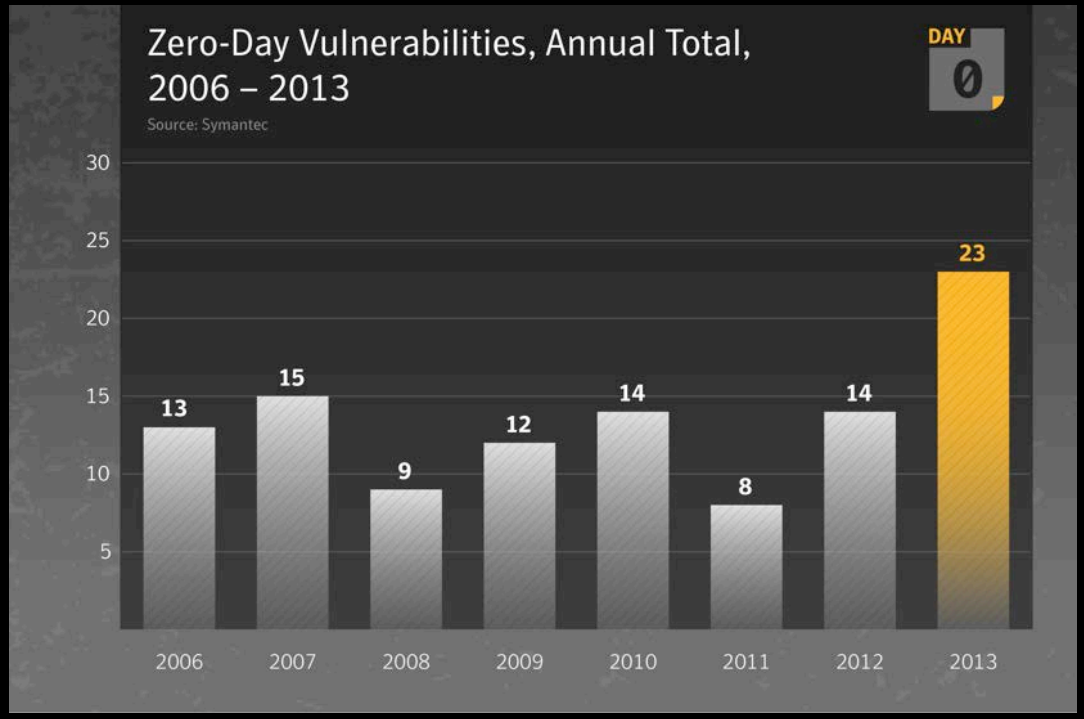
All Within 24 Hours

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

Example of Watering Hole Attack

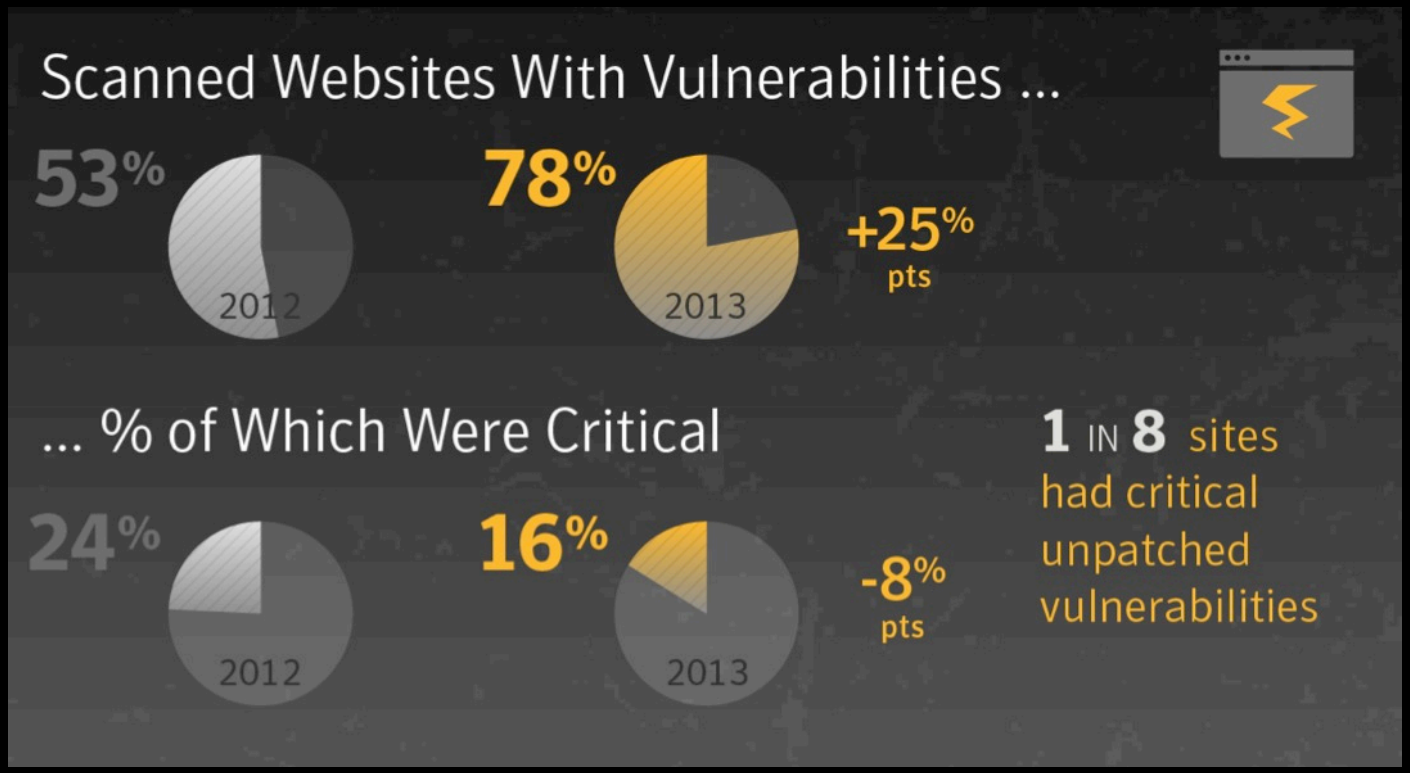
- In 2013 this type of attack will become widely used
- Several high profile companies fell victim to just such an attack

Relationship with Vulnerabilities



- There were a total of 23 zero-day vulnerabilities discovered in 2013. This is up from 14 in 2012.
- There have been more zero-day vulnerabilities discovered in 2013 than in any year since Symantec began tracking them, and more than the past two years combined.

Relationship with Vulnerabilities

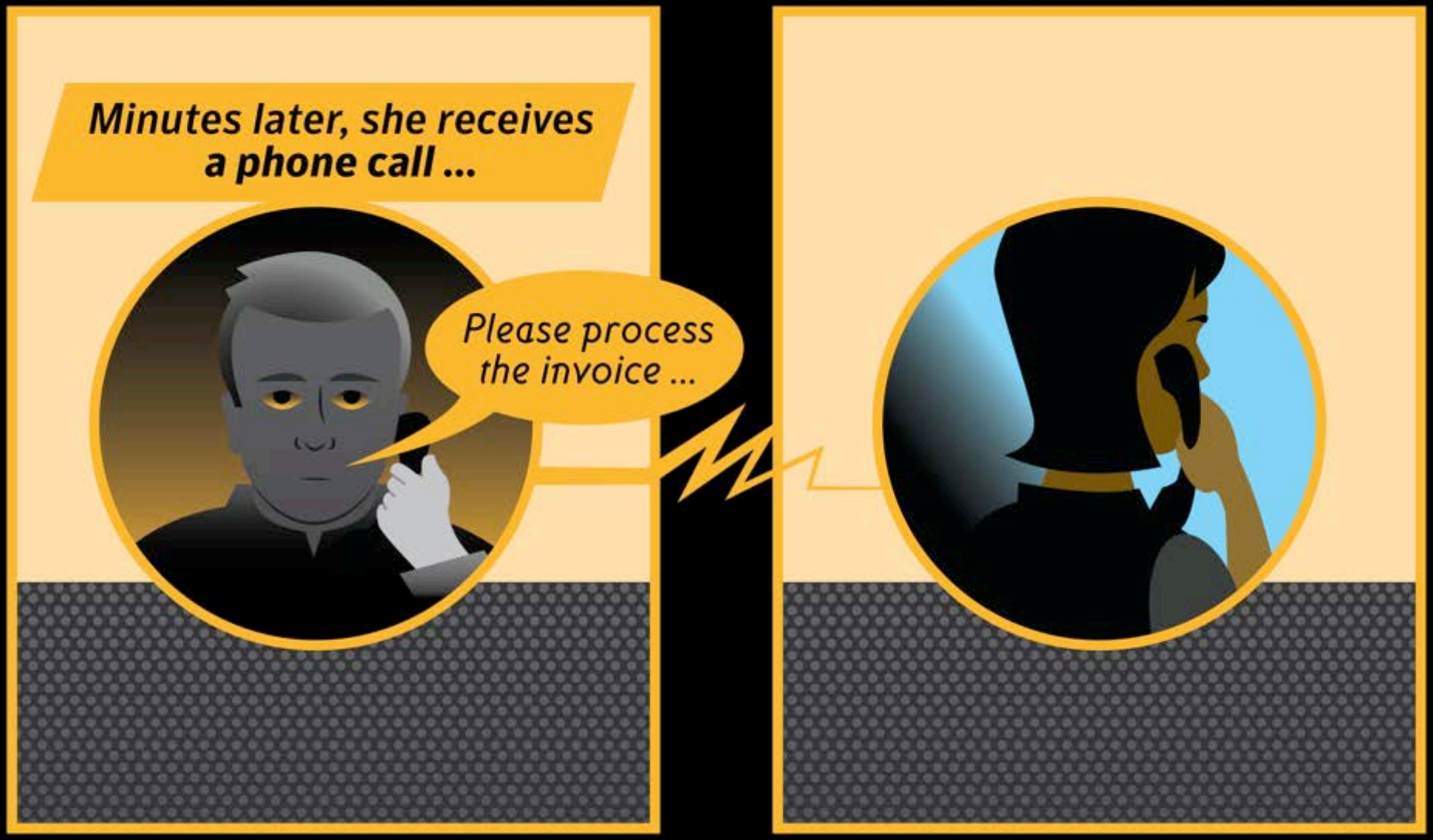


Spear-phishing campaigns are becoming more aggressive …

The "Francophoned" attack campaign

(April 2013)

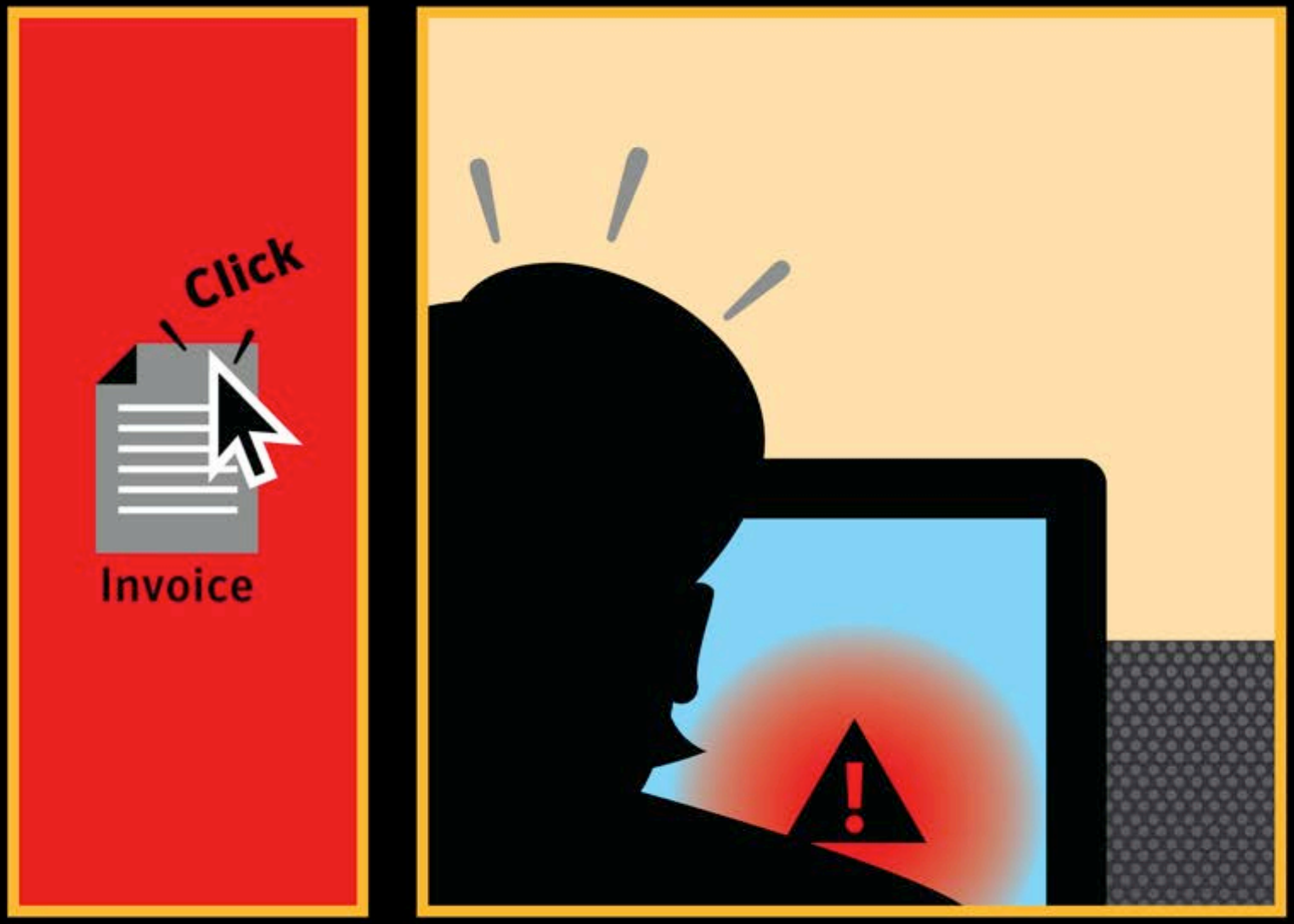
Spear-phishing campaigns are becoming more aggressive …



Attacker impersonates a high-ranked executive,

requesting the victim to open immediately the attachment …

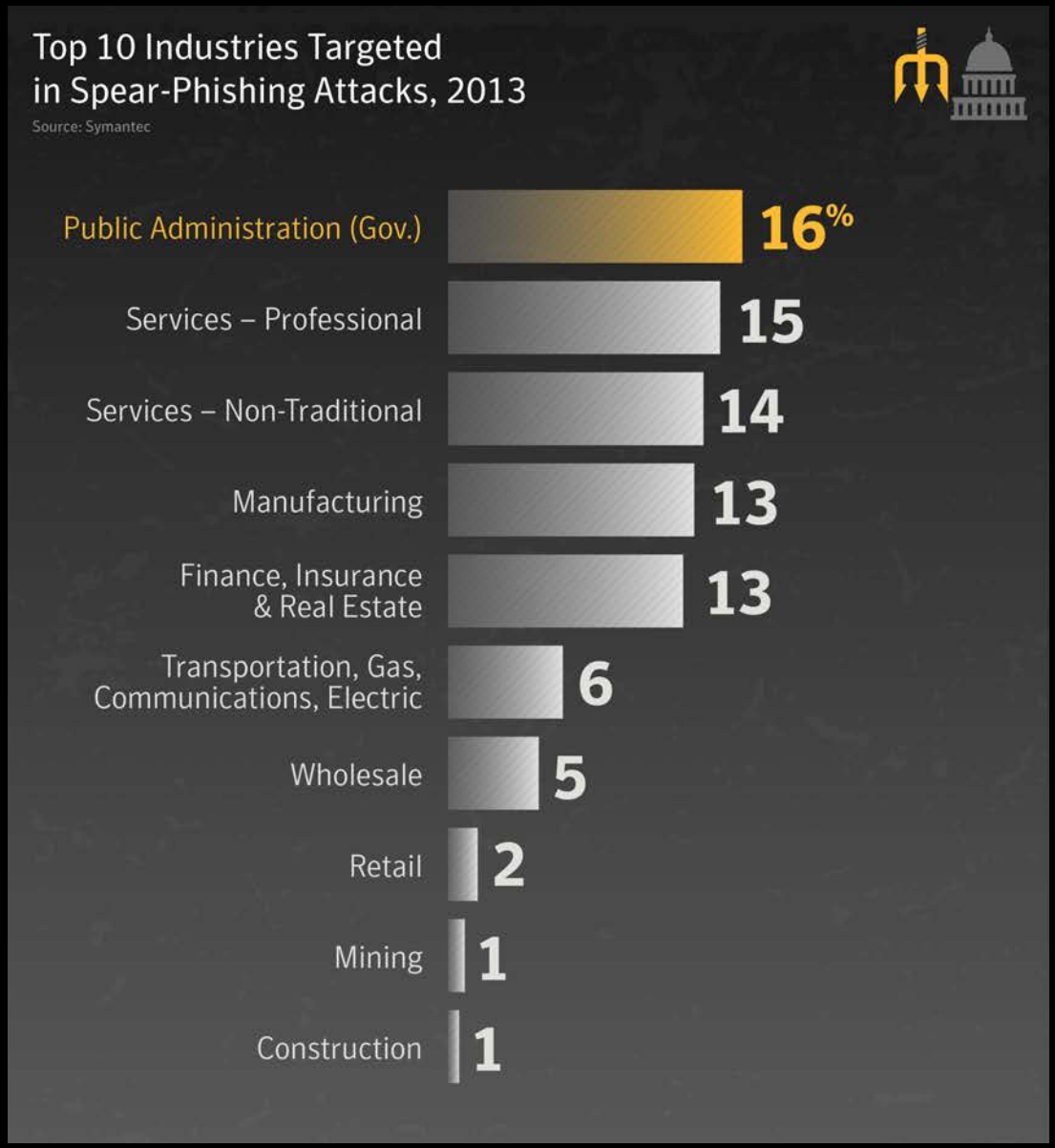
Spear-phishing campaigns are becoming more aggressive …



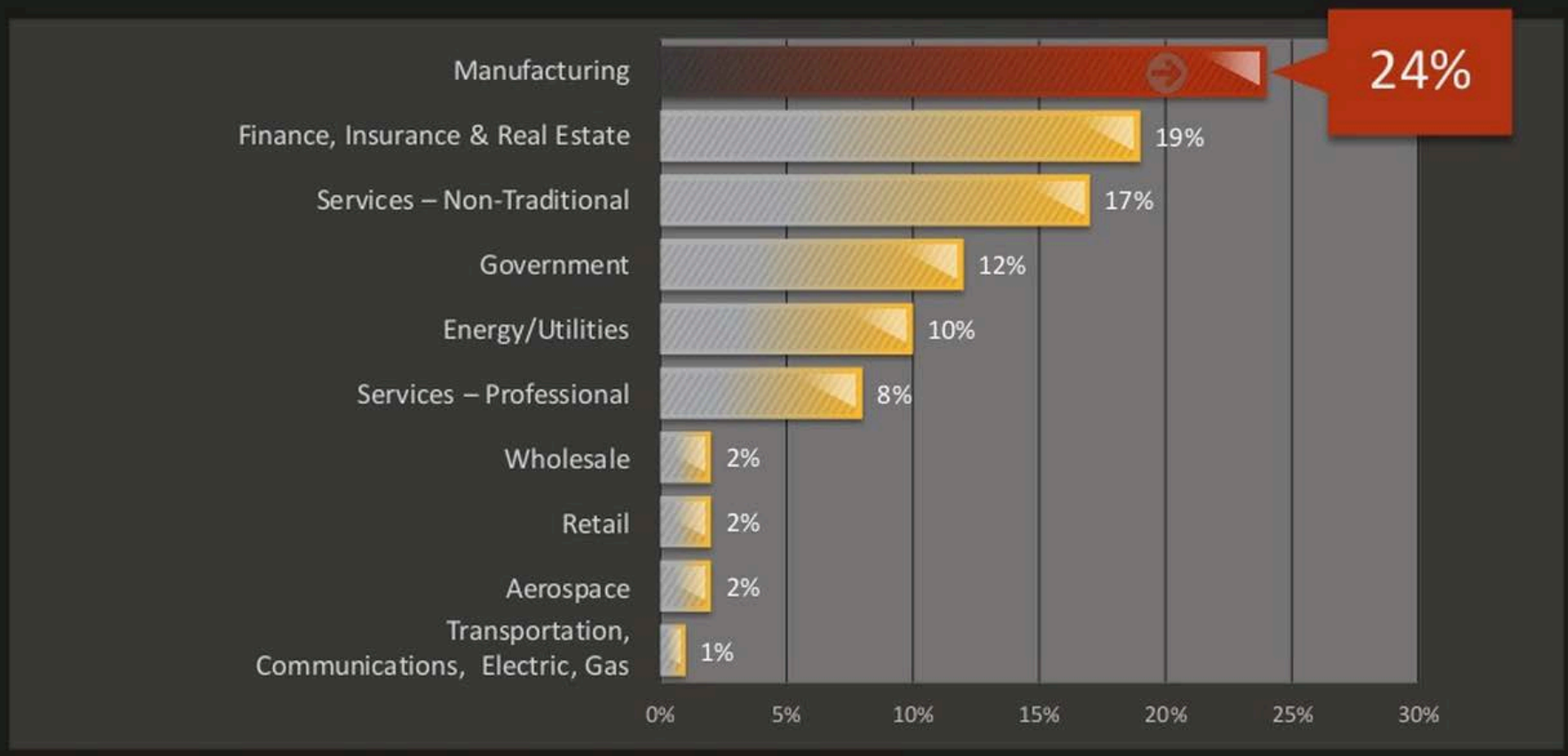
Targeted Attacks: Profiling Victims

Organizations and Individuals

Industries

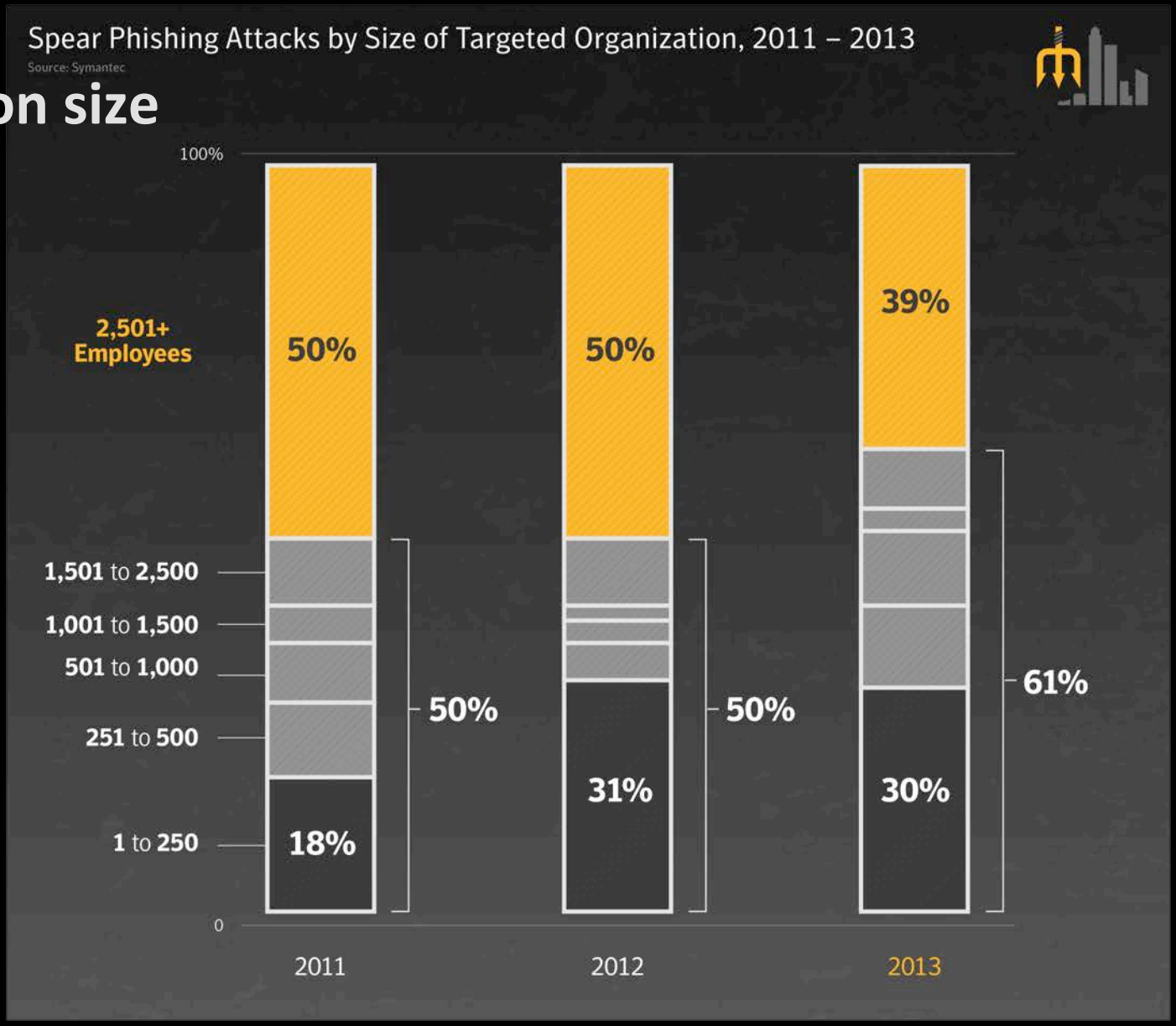

Top 10 Industries Targeted
in Spear-Phishing Attacks, 2013
Source: Symantec
Public Administration (Gov.) 16%
Services – Professional 15
Services – Non-Traditional 14
Manufacturing 13
Finance, Insurance & Real Estate 13
Transportation, Gas, Communications, Electric 6
Wholesale 5
Retail 2
Mining 1
Construction 1

Targeted Attacks by Industry in 2012



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

Organization size



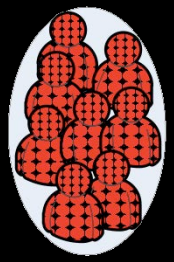
Risk Analysis

Epidemiology Concepts

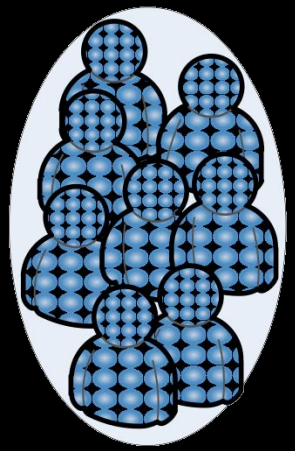
Afflicted group

Identified "Factor"

Similar population



- #subjects with factor
- #subjects without factor



- #subjects with factor
- #subjects without factor

Control group

Epidemiology Concepts

Odds Ratio (OR): Calculate strength of association of factor with "diseased" state by comparing probabilities.

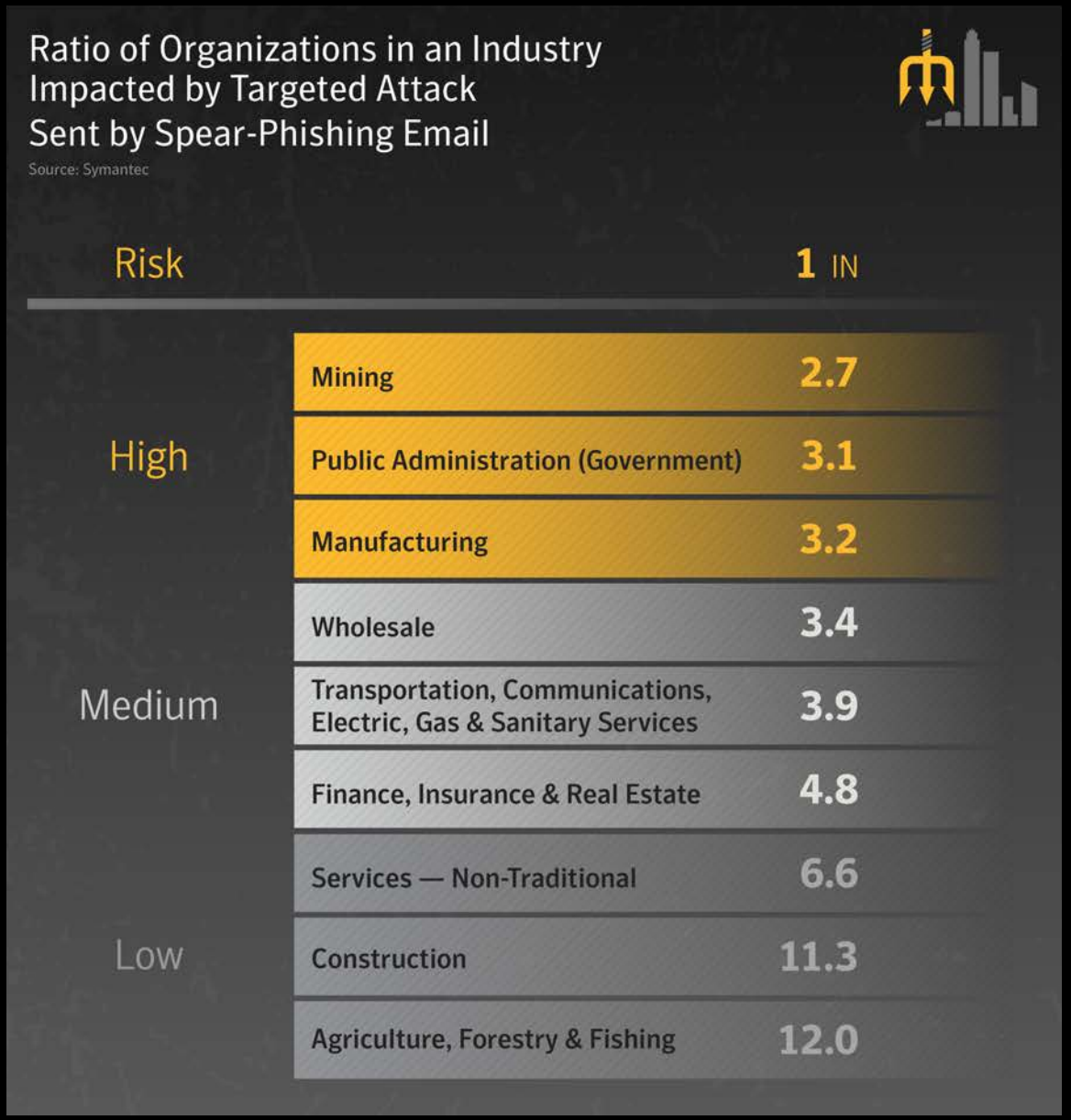
	Diseased (afflicted)	Control (unafflicted)
With risk factor	p_{11}	p_{10}
Without risk factor	p_{01}	p_{00}

$$OR = \frac{p_{11} \times p_{00}}{p_{10} \times p_{01}}$$

Odds ratio > 1 ➔ positive correlation

< 1 ➔ negative correlation

"At-Risk" Industries



“At-Risk” Organizations by Size

"At-Risk" Individuals

Based on data collected from:

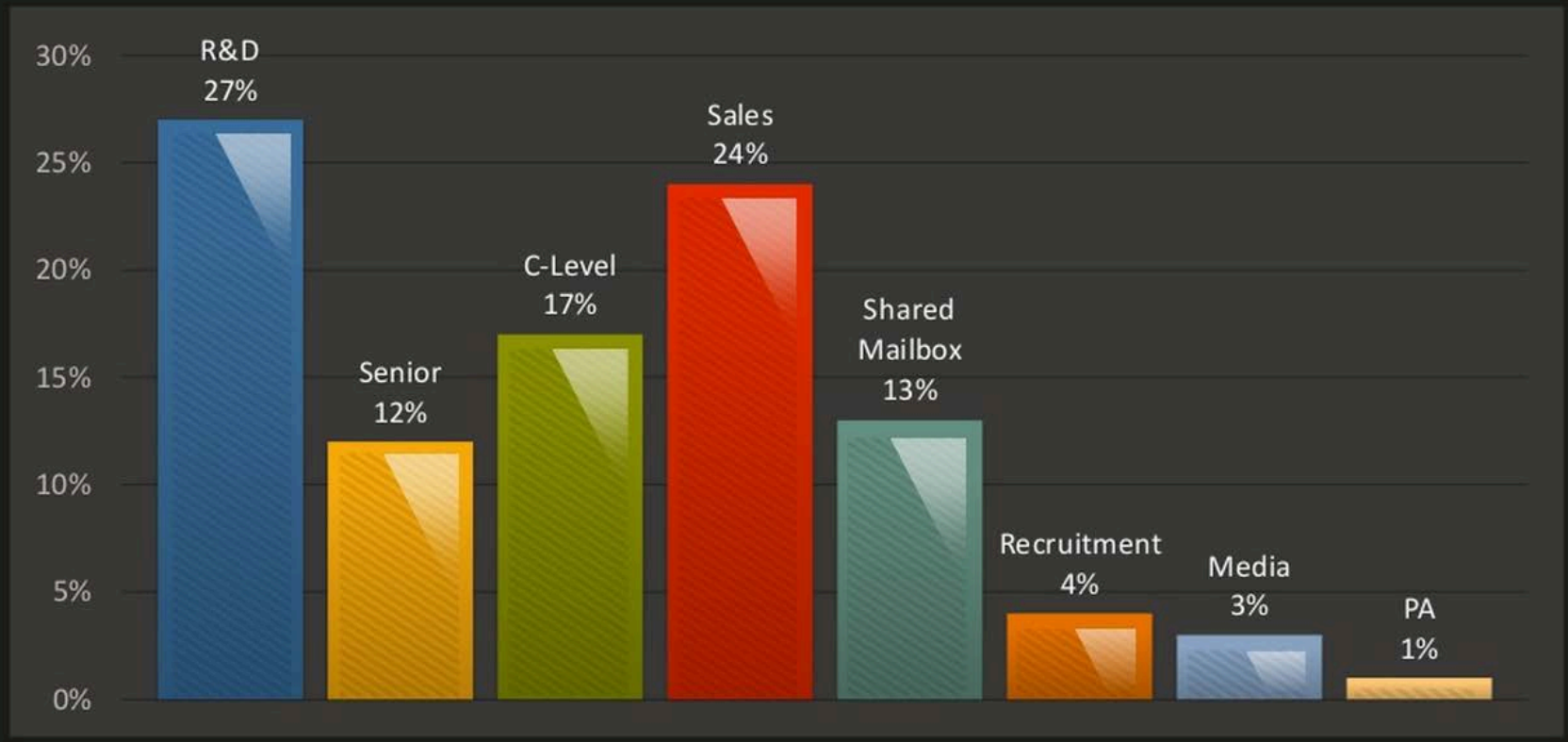
Most Likely To Be Targeted in 2013

Personal Assistant at a Large Mining company

To: JohnDoe@drillanddig.com
Subject: Re: Order Payment
From: Attacker

Please click on this executable to see your order information.

Targeted Attacks by Job Function in 2012



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

Conclusions – Lessons Learned

Targeted Attacks – Lessons Learned

- The Number of **Targeted Attacks has steadily increased** over the last few years
- Campaigns are becoming more persistent, more diverse and widespread (sometimes even automated), more prevalent
- Increases in zero-day vulnerabilities and unpatched web sites facilitate **move to watering hole style** targeted attacks
- Most industries are at elevated risk, in particular in favorable economic markets or government-related areas, and large organisations
- **Users continue to fall for social engineering tricks** and are not applying street smarts to online activity
- Urgent need for more advanced intelligence capabilities to better defend ourselves against such attacks (moving target)

Thwarting Targeted Attacks

Security Intelligence	• Human Intelligence regarding active and anticipated attack campaigns, targeted attacks, and emerging threats
Holistic Security Monitoring	• Use full capabilities of monitoring solutions to provide full visibility into security posture and events across the entire enterprise footprint
Removable Media Device Control	• Restrict removable devices and functions to prevent malware infection
Email & Web Gateway Filtering	• Scan and monitor inbound/outbound email and web traffic and block accordingly
Data Loss Prevention	• Discover data spills of confidential information that are targeted by attackers • Detect and prevent exfiltration of confidential information that are targeted by attackers
Encryption	• Create and enforce security policies so all confidential information is encrypted
Incident Preparedness & Response	• Ensure formal Incident Response capabilities are in place and fully tested • Conduct periodic penetration tests and red-team exercises to evaluate defense and response capabilities from the perspective of an attacker


INTERNET SECURITY THREAT REPORT 2014
ISTR

Thank you!

Olivier Thonnard
Olivier_Thonnard@symantec.com

2013 was the Year of the **Mega Breach**