

# RSA® Conference 2015

Singapore | 22-24 July | Marina Bay Sands

SESSION ID: SPO-F04

## Outgunned in Cyberspace

Craig Hall

Managed Defense Analyst  
FireEye

# CHANGE

Challenge today's security thinking



# JPMorgan Chase Breach



# JPMorgan Chase Breach

Dear Fellow Shareholders,



Jamie Dimon,  
Chairman and  
Chief Executive Officer

## JP MORGAN CYBER SECURITY UPDATE: POST BREACH

*"By the end of 2014, we will have spent more than \$250 million annually with approximately 1,000 people focused on the effort. This effort will continue to grow exponentially over the years."*

# Bank of America Breach



*“All you need is one weak link...”*

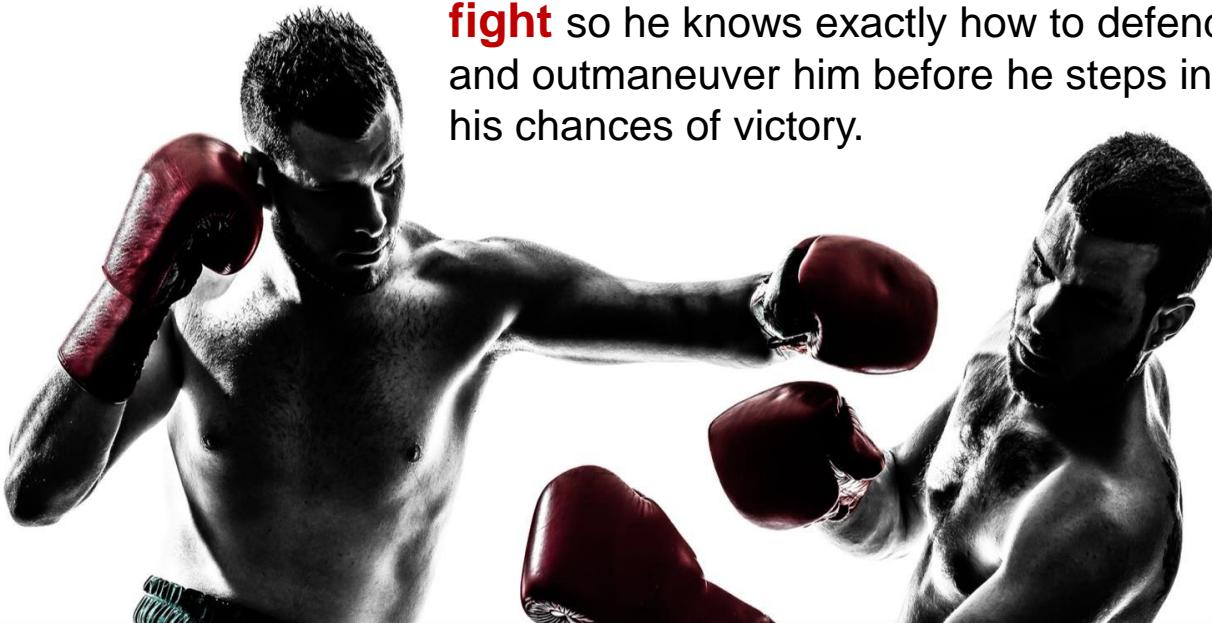


***“Nearly every company is vulnerable...”***



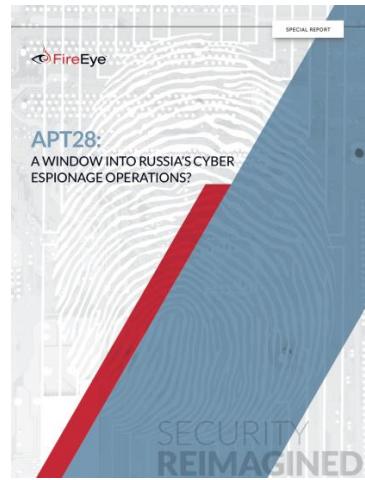
# Do you know your enemy?

**In boxing, a boxer studies his opponent's moves prior to the fight** so he knows exactly how to defend himself against the opponent and outmaneuver him before he steps into the ring, which will increase his chances of victory.



# Threat Intelligence

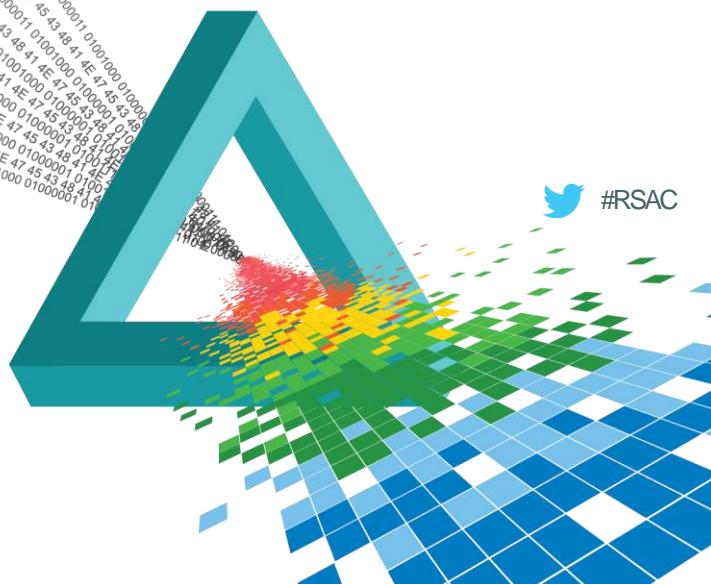
- ◆ APT is a '**WHO**' and not a '**WHAT**'
- ◆ **THREAT INTELLIGENCE** should provide information on THREAT ACTORS





Singapore | 22-24 July | Marina Bay Sands

## 'Theoretical' Case Study



# Two Utilities

TELCO - A



Signature based **TECHNOLOGY**

In-house **EXPERTISE**

No malware/threat actor **INTELLIGENCE**

TELCO - B



FireEye **TECHNOLOGY**

FireEye **EXPERTISE**

FireEye **INTELLIGENCE**

# Traditional In-House Approach

## TELCO - A



## TECHNOLOGY

AntiSpam and AV Filtering



Receives 5 million emails  
a day

- ◆ AV updates slow
- ◆ Sometimes AV will only catch malware **AFTER** infection



## When this happens

- Machine is reimaged
- Possibly send malware sample to their AV vendor

# FireEye Intel Based Approach



## TECHNOLOGY

1. AntiSpam and AV Filtering
2. Malware Detonation – FireEye



Receives 5 million emails  
a day

- ◆ FireEye **TECHNOLOGY** is not Signature based – and finds threats faster than signatures – reducing time to detect
- ◆ FireEye Technology finds the unknown threat “[Invoice.xls](#)”

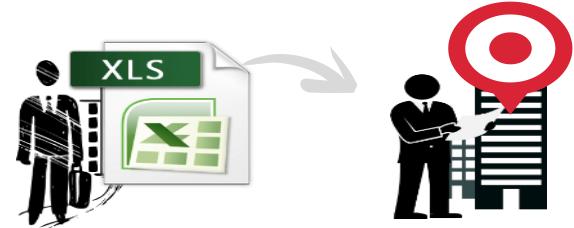
# Unknown Threat: Invoice.xls

**Target:** Telco - B, and trying to appear legitimate

- No signature
- Bypassed existing defenses

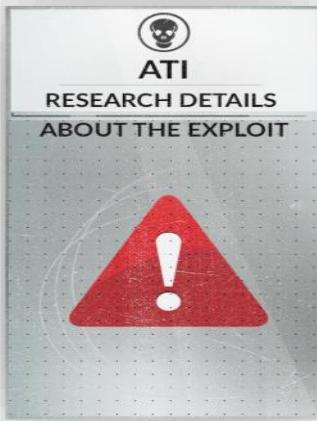
FireEye **TECHNOLOGY** reveals:

1. Invoice.xls designed to attack Excel 2010sp2
2. Excel 2010sp2 is the version Telco B has standardized on
3. Malware phones home to [ServiceABC.skynetw.com](http://ServiceABC.skynetw.com)
4. **ServiceABC** is the name of a VALID internal service in the Telco B network



# Who Is Attacking?

FireEye **INTELLIGENCE** tells us:



**Skypetw.com**  
matches to  
**known threat**  
group: APT5

**APT5**  
targets  
telecom  
companies

→  
**Is looking for**  
intellectual  
property regarding  
satellite  
communications

→  
**Known TTPs**  
Tactics,  
Techniques and  
Procedures

# APT5 Tools Techniques and Procedures



1

Establish a Beachhead using malware



2

Move laterally using standard networking tools (no malware)



3

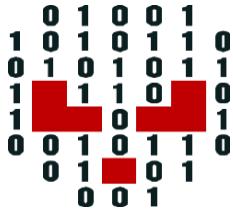
Find desired intellectual property



4

Exfiltrate stolen data using password protected zip files and FTP

# Incident Scope



- APT 5 is behind the attack
- Looking for Satellite IP
- Telco B has Satellite Communication IP
- Alarm bells going off from this single alert



We need to find out

---



Did end user open email attachment?



Did other users get infected?



Did the attacker move laterally once inside the network?

# Detect and Respond

- ◆ Complete Host Based investigation, e.g. : Scraping Endpoint Memory
- ◆ Reveal commands an attacker may have used on an endpoint
  
- ◆ Look for APT5 TTP – Lateral movement using standard networking tools
- ◆ Look for APT5 TTP – Exfiltration of password protected zip file
  
- ◆ Investigation through FireEye as a Service **EXPERTISE** tells us
  - ◆ “NETUSE” command was used to connect to 2 additional servers at TelcoB
  - ◆ Servers required Username and password - “**BobAdmin**” account was used by the attacker. This account is a Domain Admin at TelcoB
  - ◆ Our remediation now extends to this **compromised admin account**
  - ◆ Agent **TECHNOLOGY** tells us 7z (zip) command was used with a “password” option
  - ◆ Agent **TECHNOLOGY** tells us the password that was used to encrypt the file: **itsm9now**

# Incident Scope



## Scope of the attack

- Desktop
- Laptop
- 2 Servers
- Compromised Admin Account “BobAdmin”

## What we need to know

- What was in those exfiltrated .zip files?
- Did they actually make it out?
- What is the business impact?

# Network Forensics

## FireEye TECHNOLOGY

1. Goes back in time and shows us the actual zip file “exfil.zip” that was sent to [serviceABC.skypetw.com](http://serviceABC.skypetw.com)
2. Lets us extract “exfil.zip” and save it to our computer...
3. **But it's password protected**

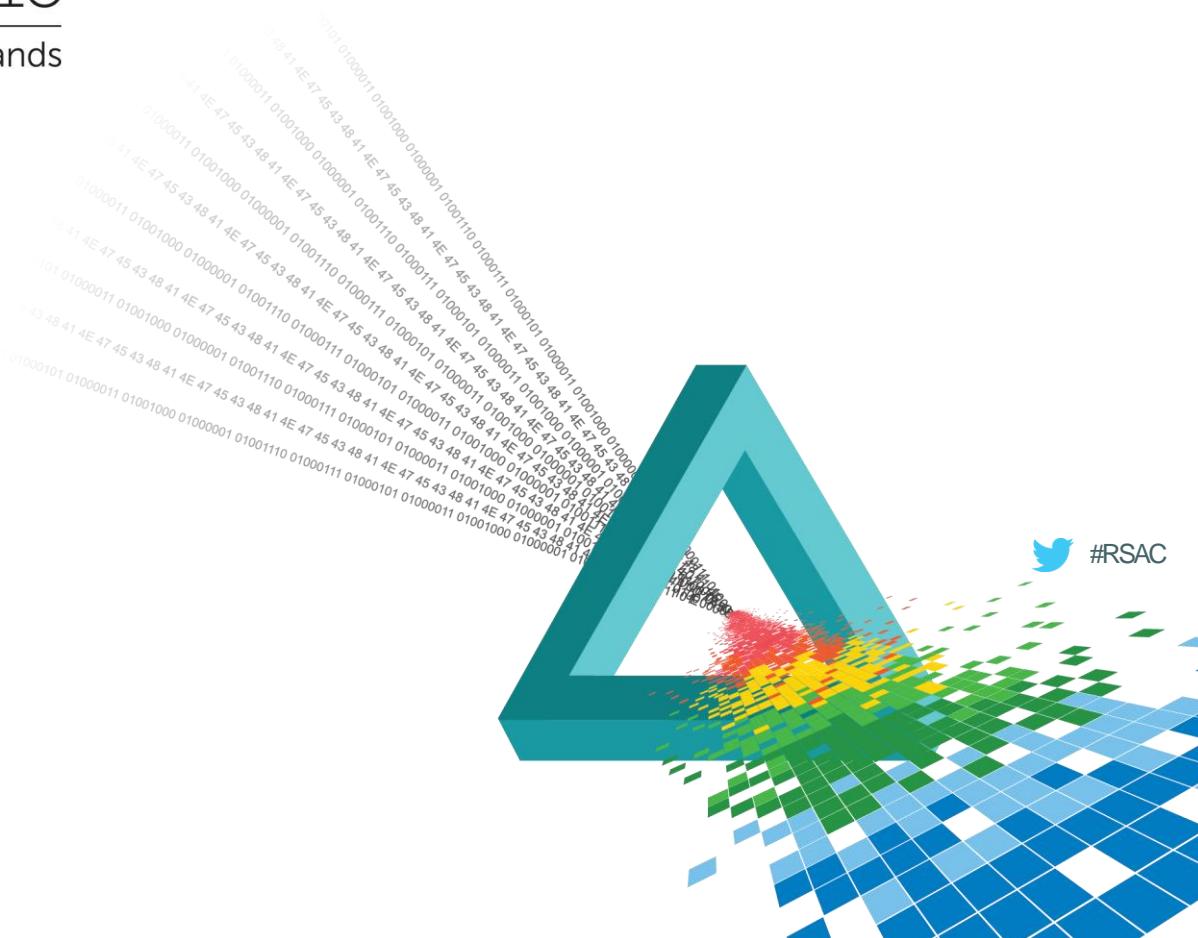
We use the password that we learned from endpoint forensic investigation

See what data was exfiltrated: Satellite Intellectual Property?

# RSA® Conference 2015

Singapore | 22-24 July | Marina Bay Sands

# APT30



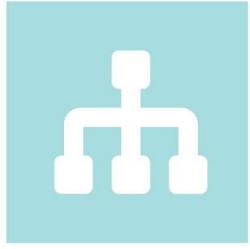
# APT30 Key Findings

10+  
YEARS

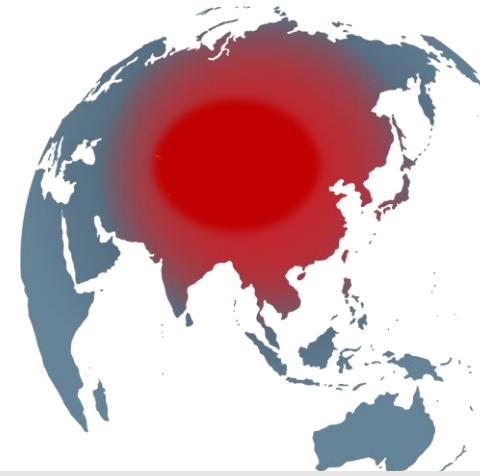
Long-standing  
advanced persistent  
threat (APT)



Focus on Southeast Asia and  
India



Methodical processes and  
modular tools implies a  
structured environment



- Appears to target organizations with **political, economic, and military information**
- Able to target **sensitive air-gap networks.**

# One of longest-operating known threat groups

**10+**  
YEARS

Based on malware metadata,  
compile dates, and domain  
registration date APT30 has  
**operated for at least a  
decade** (2004 – 2015)

Domain	Registration Date	Compile Date Early Sample	Compile Date Recent Sample
km-nyc.com	11 Mar 2004	11 Mar 2005	11 May 2014
km153.com	30 Aug 2007	4 Sep 2007	11 May 2014

<b>Comments</b>	(C) 2004 Microsoft Corporation. 保留所有权利。 Flyeagle science and technology company NetEagle Remote Control Software
<b>File Version</b>	4.2
<b>Internal Name</b>	Neteagle
<b>Legal Copyright</b>	版权所有 (C) 2004—永久
<b>Original Filename</b>	NETEAGLE.EXE
<b>Private Build</b>	
<b>Product Name</b>	NetEagle Remote Control Software
<b>Product Version</b>	4.2
<b>Special Build</b>	

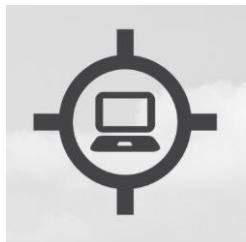
Version information from BACKSPACE controller

# Regional Focus

**96%** of victim organizations located in SE Asia



Confirmed APT 30 Targets					
	India		Thailand		Malaysia
	South Korea		Saudi Arabia		Vietnam



Likely APT30 Targets					
	Nepal		Indonesia		Cambodia
	Bhutan		Brunei		Japan
					Singapore
					Laos

# Regional / Geopolitical Targeting

- ◆ 'Decoy' documents reflect geopolitical themes associated with region
  - ◆ Political transitions
  - ◆ China border disputes
  - ◆ Indian military themes
- ◆ Focus on ASEAN with registration of malicious domain aseanm[.]com
- ◆ Journalists also targeted



# Consistent TTPs

APT30 appears to have a consistent, long-term mission that relies on existing tools to remain sufficient over time

Yesterday's successful tools modified for today

MALWARE / TOOL	COMPILE DATE EARLY SAMPLE	COMPILE DATE RECENT SAMPLE
BACKSPACE	2 Jan 2005	5 Nov 2014
NETEAGLE	20 Jun 2008	6 Nov 2013
SHIPSHAPE	22 Aug 2006	9 Jun 2014
SPACESHIP	23 Aug 2006	5 Jun 2014
FLASHFLOOD	31 Jan 2005	17 Feb 2009

- ◆ Successful enough to *not have to change*
- ◆ Long-term investment in software development

# Summary of APT30



APT30 is a **well-organized** group with a long-term mission that represents a regional threat

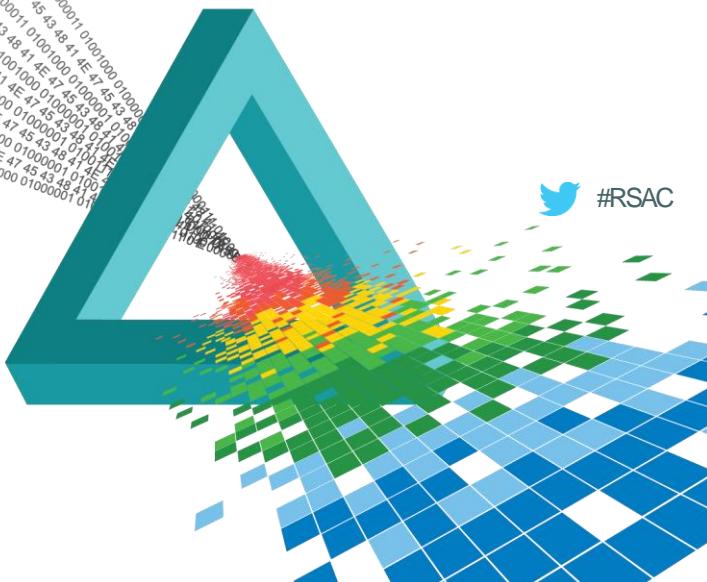
**Targeted activity and state-sponsored** not simply a US problem

Able to target sensitive **Air Gap networks**



Singapore | 22-24 July | Marina Bay Sands

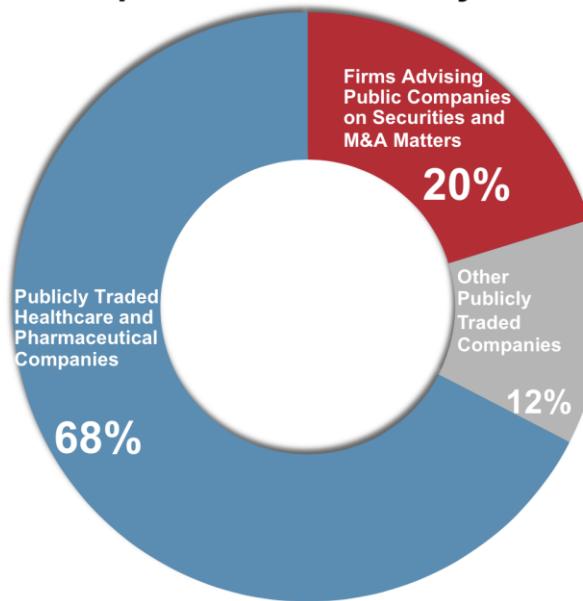
# FIN4 – HACKING WALL ST



# Who Are FIN4?

- ◆ Active since at least mid-2013
- ◆ Likely seeking “black edge”
  - Market catalyst information for trading advantage
- ◆ Deeply familiar with inner workings of public companies
- ◆ Tactics: simple yet insidiously effective

## FIN4 Targets: Over 100 Publicly Traded Companies and Advisory Firms



# Attack Vector

- ◆ Emails originate from **trusted senders**
  - ◆ Links to fake Outlook Web Access portal
  - ◆ Stolen documents weaponized with embedded macros

Subject: employee making negative comments about you and the company  
From: <name>@<compromised company's domain>

I noticed that a user named FinanceBull82 (claiming to be an employee) in an investment discussion forum posted some negative comments about the company in general (executive compensation mainly) and you in specific (overpaid and incompetent). He gave detailed instances of his disagreements, and in doing so, may have unwittingly divulged confidential company information regarding pending transactions.

I am a longtime client and I do not think that this will bode well for future business. The post generated quite a few replies, most of them agreeing with the negative statements. While I understand that the employee has the right to his opinion, perhaps he should have vented his frustrations through the appropriate channels before making his post. The link to the post is located here (it is the second one in the thread):

<http://forum.<domain>/redirect.php?url=http://<domain>%2fforum%2fequities%2f375823902%2farticle.php\par>

Could you please talk to him?

Thank you for the assistance,

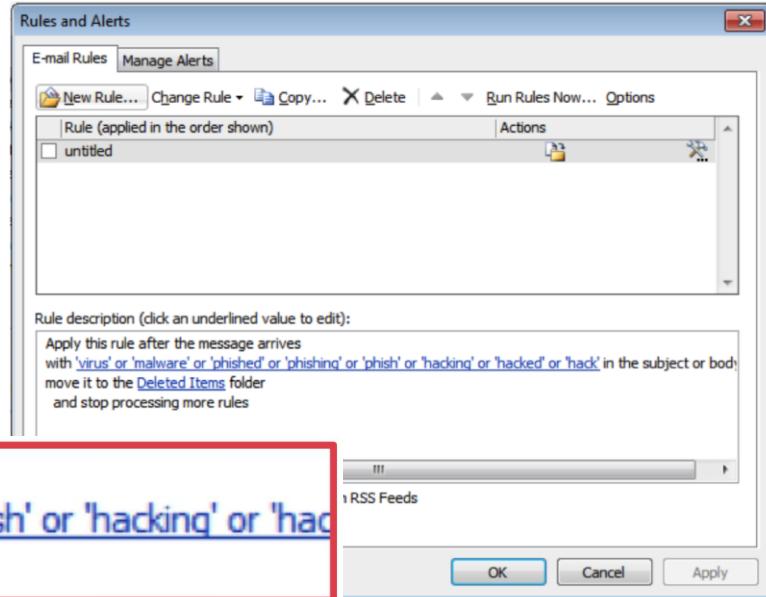
# The Target?



**FIN4 repeatedly targeted the M&A discussions of publicly traded companies.**

# Insidiously Clever?

- ◆ Simple techniques to minimize chances of discovery



Apply this rule after the message arrives  
with 'virus' or 'malware' or 'phished' or 'phishing' or 'phish' or 'hacking' or 'hack'  
move it to the Deleted Items folder



Singapore | 22-24 July | Marina Bay Sands

# Operation Clandestine Wolf



# Who are APT3?

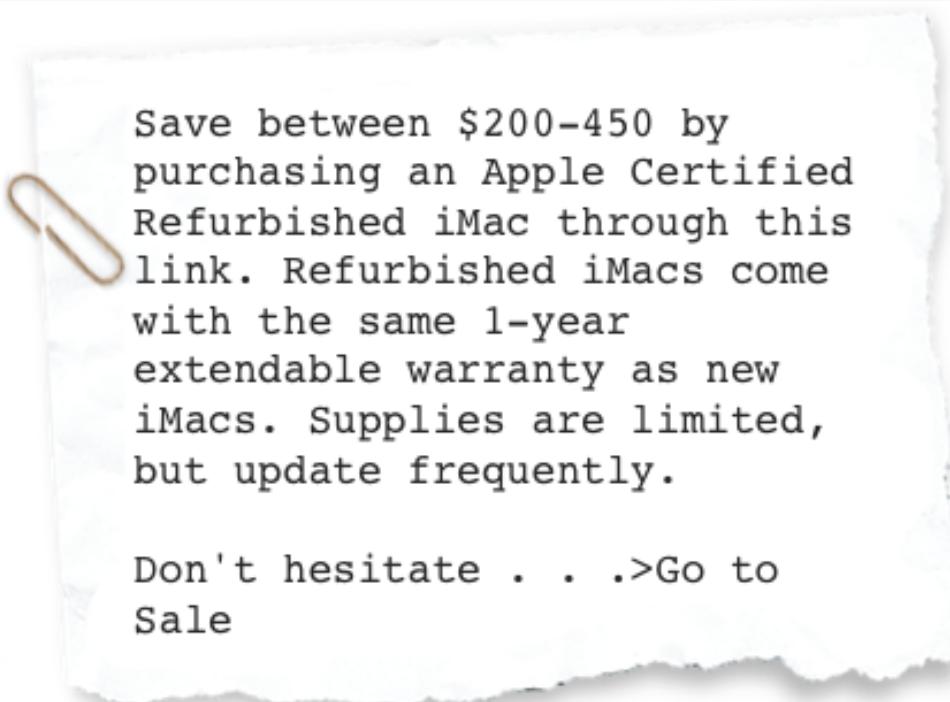
- ◆ State-sponsored group – AKA UPS
- ◆ Attributed to Operation Clandestine Fox in 2014
- ◆ Zero-day exploit sophistication
- ◆ Cool code names

# Clandestine Wolf



- ◆ Spear phishing campaign against:
  - Aerospace and Defense
  - Construction and Engineering
  - High Tech
  - Telecommunications
  - Transportation

# Spearphishing



# Some Technical Details



A large red 'X' is drawn over the ASLR logo.

ASLR

Address Space Layout Randomization



A large red 'X' is drawn over the DEP logo.

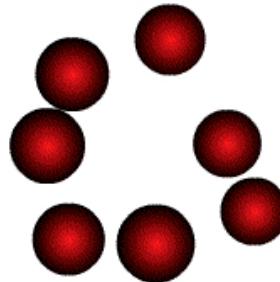
DEP

Data Execution Prevention

# These Red Dots = Compromise

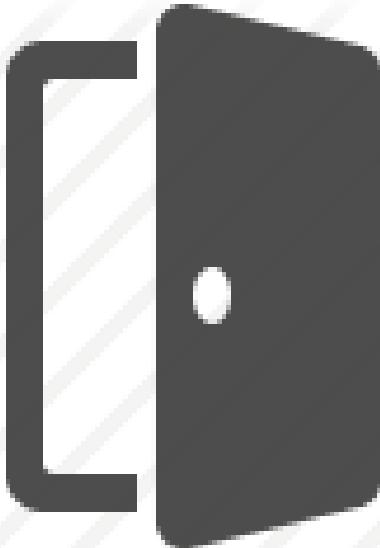


- Valid GIF File
- Malicious Payload appended at end of File
- Malicious Payload is encoded to avoid detection



Malicious GIF Image  
file

# After The Initial Compromise



- Custom Backdoor “Backdoor.APT.CookieCutter” installed
- Quickly steal valid credentials ( to defeat organizations only looking for malware )
- Move laterally to systems with digital assets of value
- Install custom Backdoors
- Never reuse command and control infrastructure

# Remediation

Apply Adobe Out Of Band Security Patch

FireEye IPS detects : CVE-2015-3113

FireEye MVX detects: Backdoor.APT.CookieCutter



# Outgunned in Cyberspace

- ◆ Do you believe that the breach is inevitable?
- ◆ How would you know if you were currently compromised?
- ◆ Do you know who would attack you?
- ◆ Do you know how they would do it?

# Thank You

- ◆ To talk more, email us:

APAC@FireEye.com

# RSA® Conference 2015

Singapore | 22-24 July | Marina Bay Sands

SESSION ID: SPO-F04

## Outgunned in Cyberspace

Craig Hall

Managed Defense Analyst  
FireEye

# CHANGE

Challenge today's security thinking

