MessageLabs

Be certain

Targeted Trojans and Industrial Espionage

Alex Shipp, Imagineer

Agenda

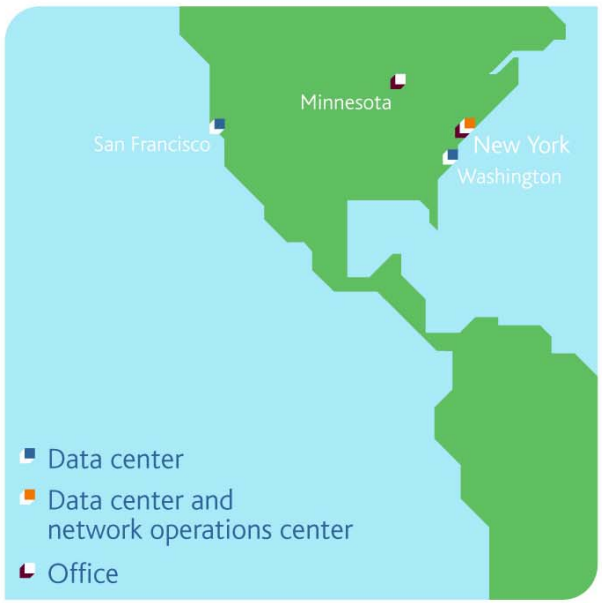
- **Typical attack**
- **Patterns**
- **Predictions**
- **Metrics**

Global Infrastructure:

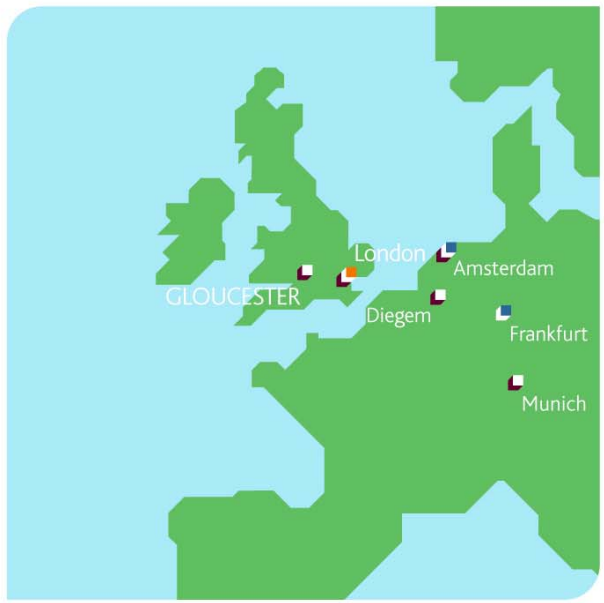
Overview

MessageLabs

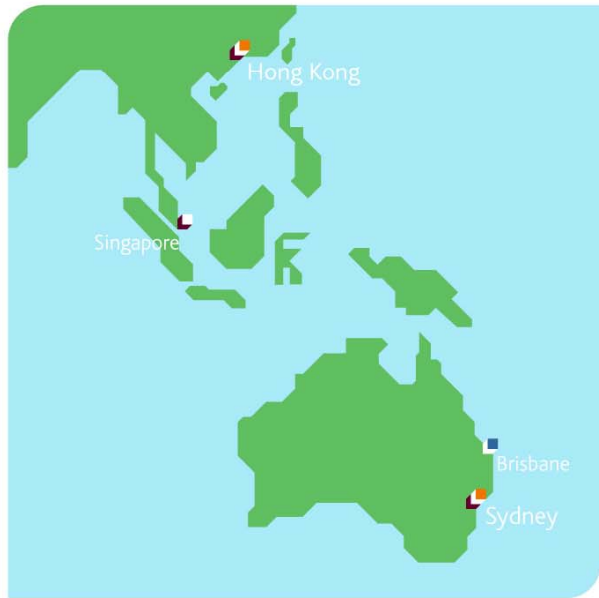
Regional Clusters (Americas)



Regional Clusters (EMEA)



Regional Clusters (APAC)



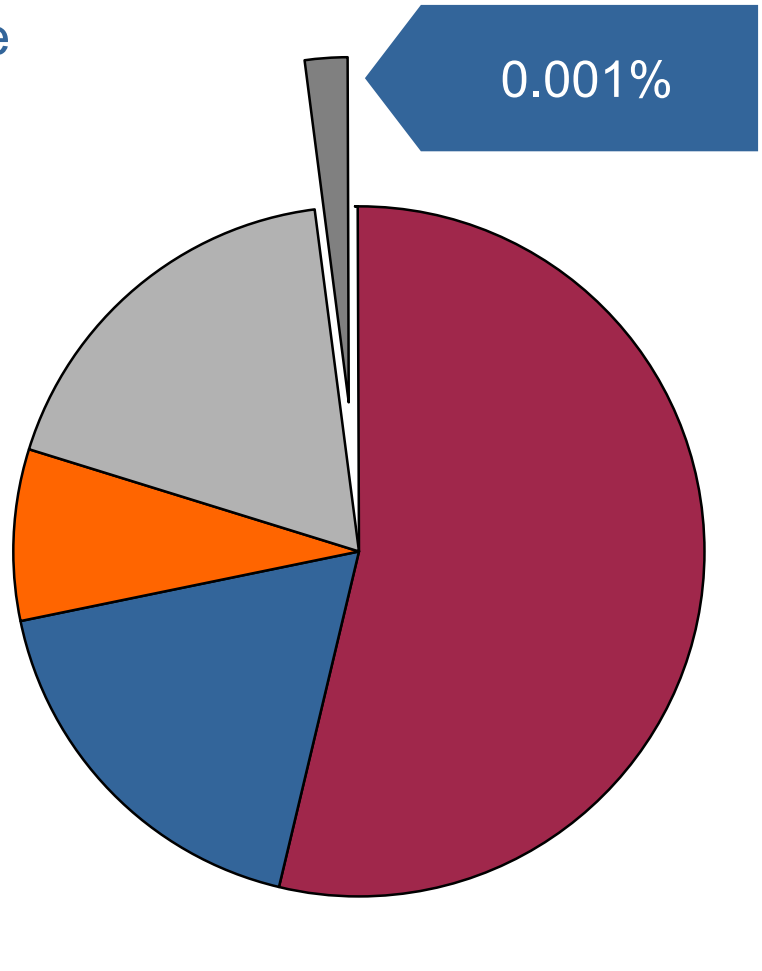
The MessageLabs Global Infrastructure currently spans 13 data centers across four continents and is comprised of regional clusters of multiple data centers and mail processing facilities.

This architecture is load balanced to provide enormous processing power and complete failover protection and is backed up by strong service level agreements for network availability and email loss protection.

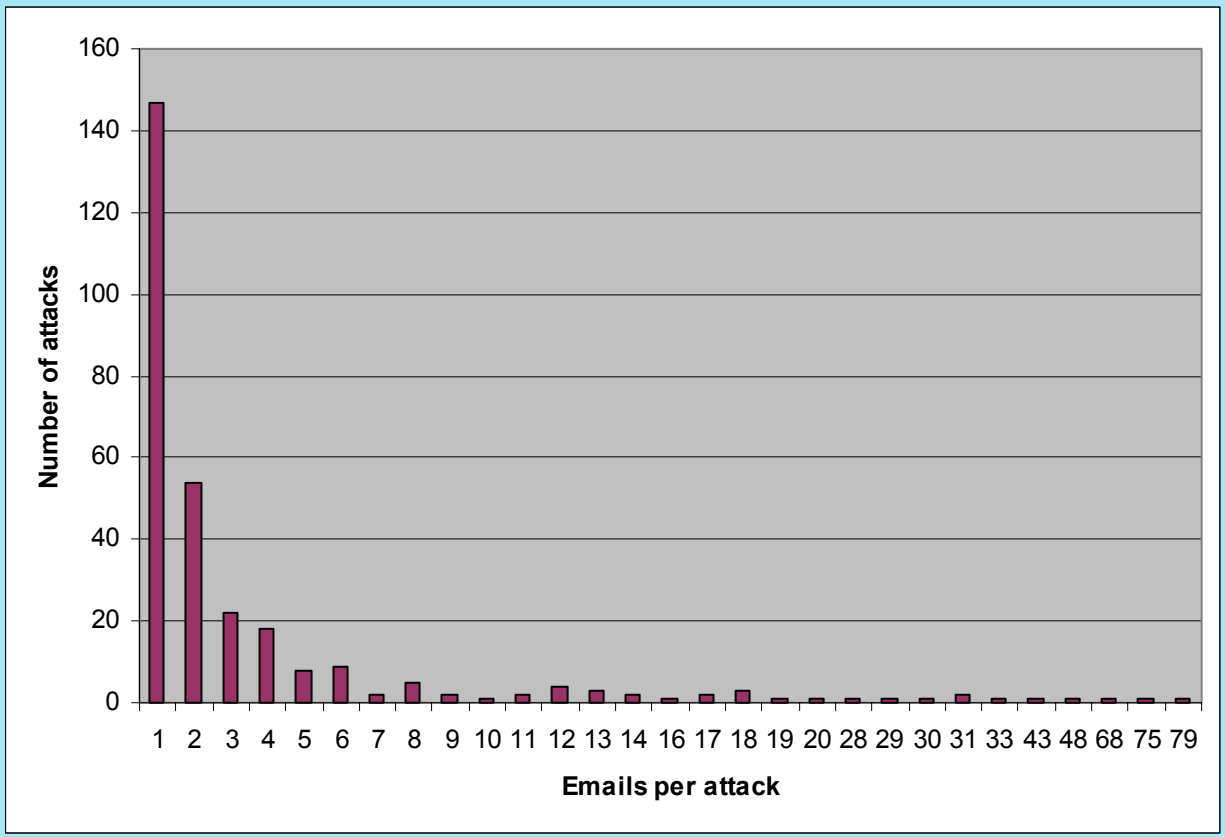
MessageLabs also maintains nine regional offices in eight countries around the world for localized sales, partner management and service & support..

Understanding the Problem
Small scale targeted Trojans

- 0.001% of our malware capture is unlike the rest
- ‘Professional’ targeted malware
- Send to small number of target recipients, typically < 10

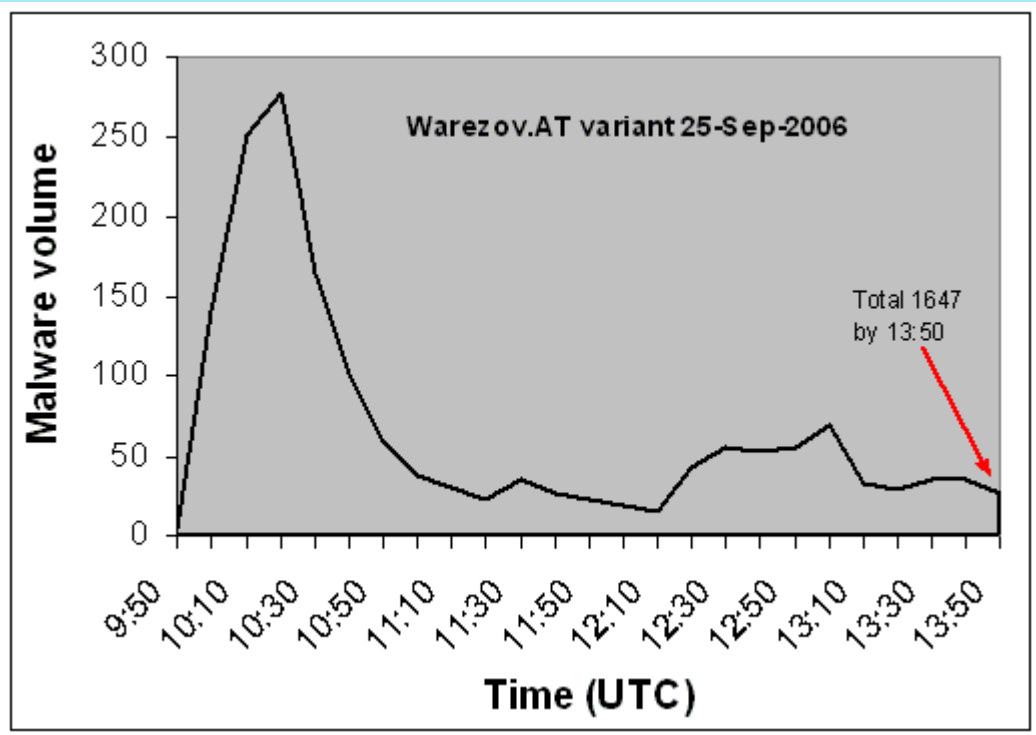


Number of emails per attack, May 2005- May 2006



- Keep infected machines owned
- Keep exploit secret

Typical botnet seeding

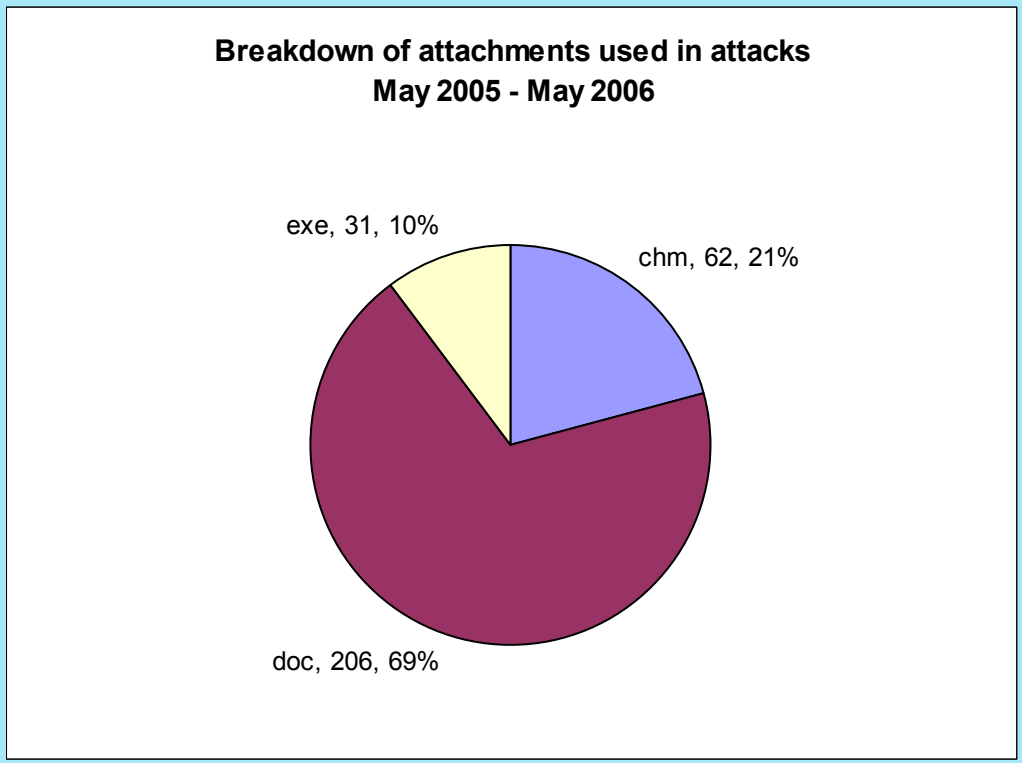


Comparison with typical botnet creation seeding

Social Engineering
Sample subject lines

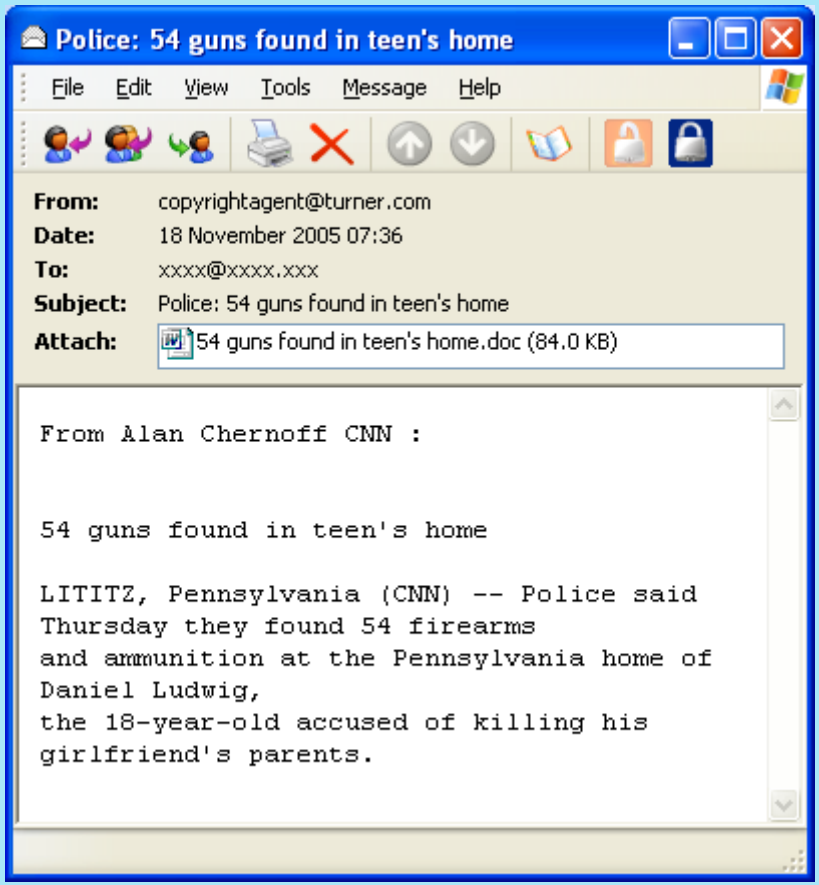
Avian Influenza -Situation in Thailand
Bird flu's truth in mylasia
Center for European Policy Studies' Commentary
Challenge of developing China's Defense
China Hosts a 2nd Taiwan Party Head
China says U.S. & EU textile issues 'very serious'
China-Iran-Russia alliance,the counterpunch to Washington's global ambitions
Chinese army enters into Indian territory
CSIS: Preventing Nuclear Terrorism
Disgraceful Behavior Of Russian
ECMT-Access and Inclusion Draft Summary Record
FBI Arrests Russian U.N. Official
FDC Internet Conference Berlin

Targeted Trojans – Attachment Types



- Breakdown has changed following the paper
  - PPT and XLS also common

Example



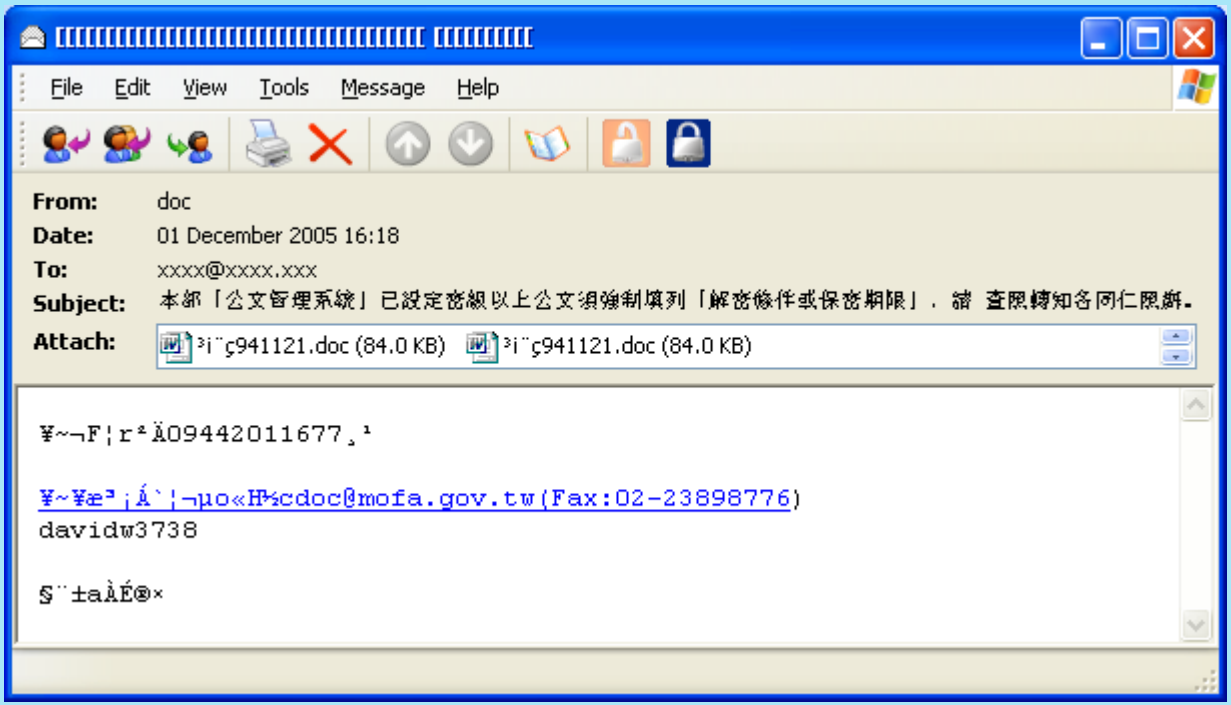
18-Nov-2005

Military, pharmaceutical, petrochemical and legal organisations organizations targeted with crafted word documents which drop and run remote control software.

1 recipient per target.

Emails came from IP belonging to Tianjin Province of China

Example

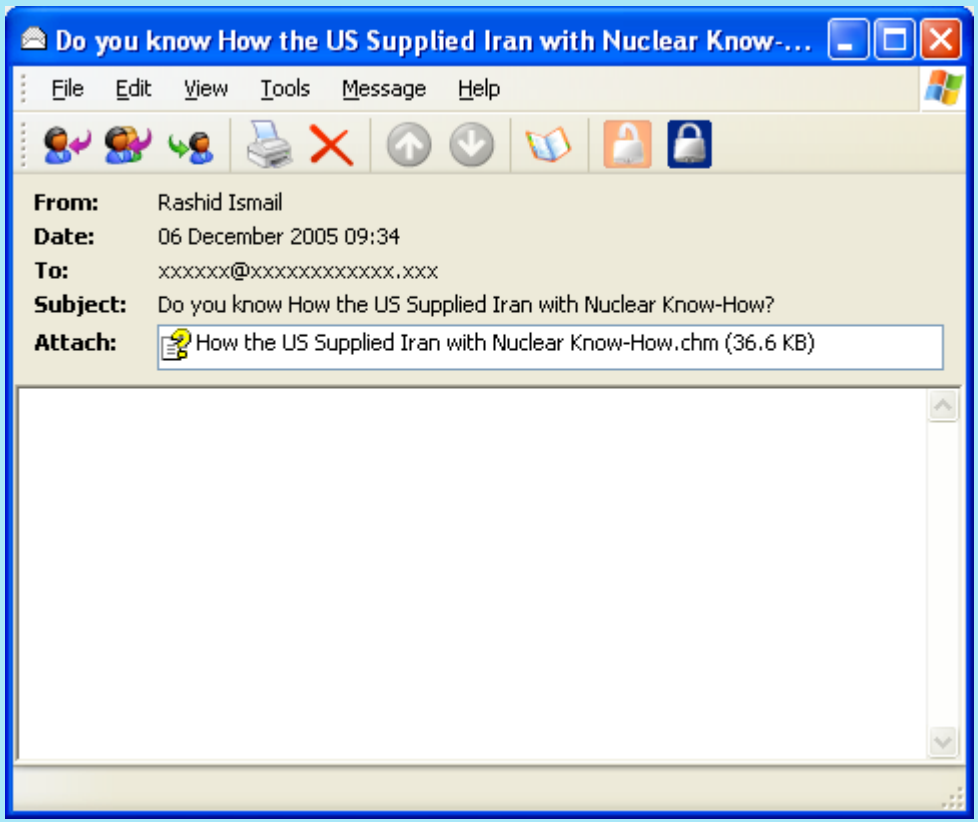


1-Dec-2005

Human rights organizations targeted with crafted word documents which drop and run downloader.

1-2 recipients per target. Came from IP in China.

Example



6-Dec-2005

Human rights organizations targeted with crafted MS Help files which drops and runs a web proxy.

1-2 recipients per target. Came from IP in Western Australia.

Example

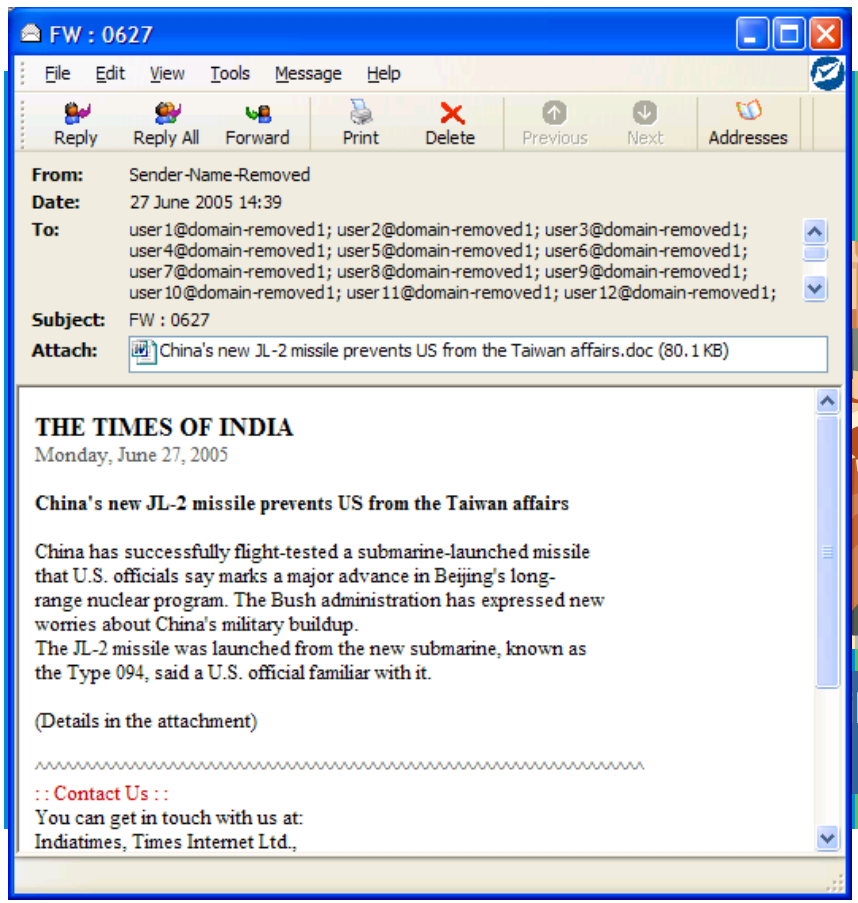
6-Dec-2005

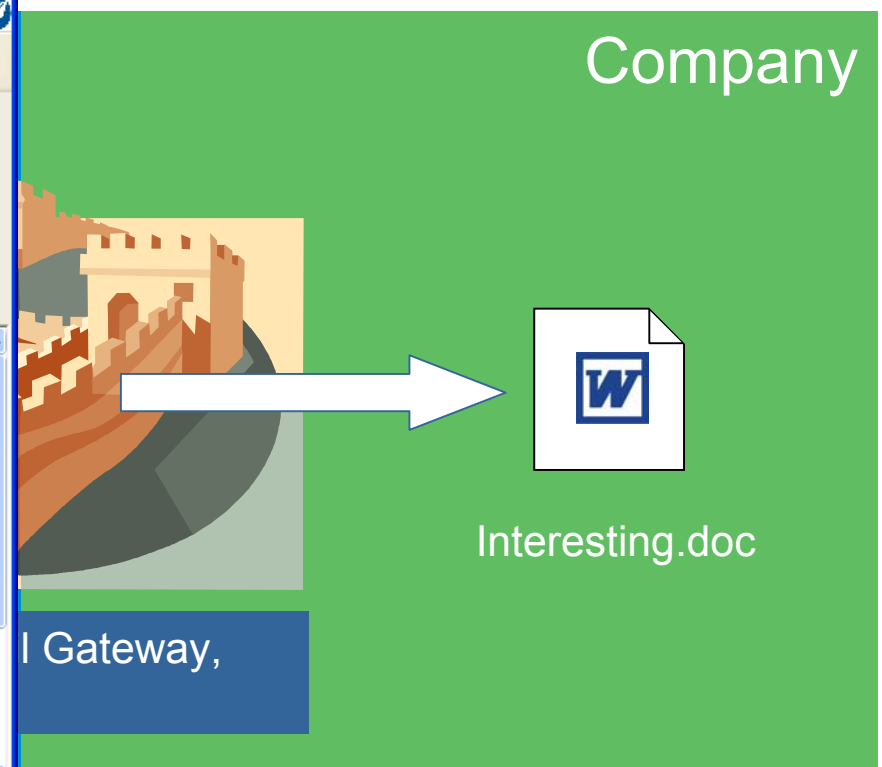
Same human rights organizations targeted with crafted word documents which drop and run downloader.

1-2 recipients per target. Came from same IP in Western Australia.

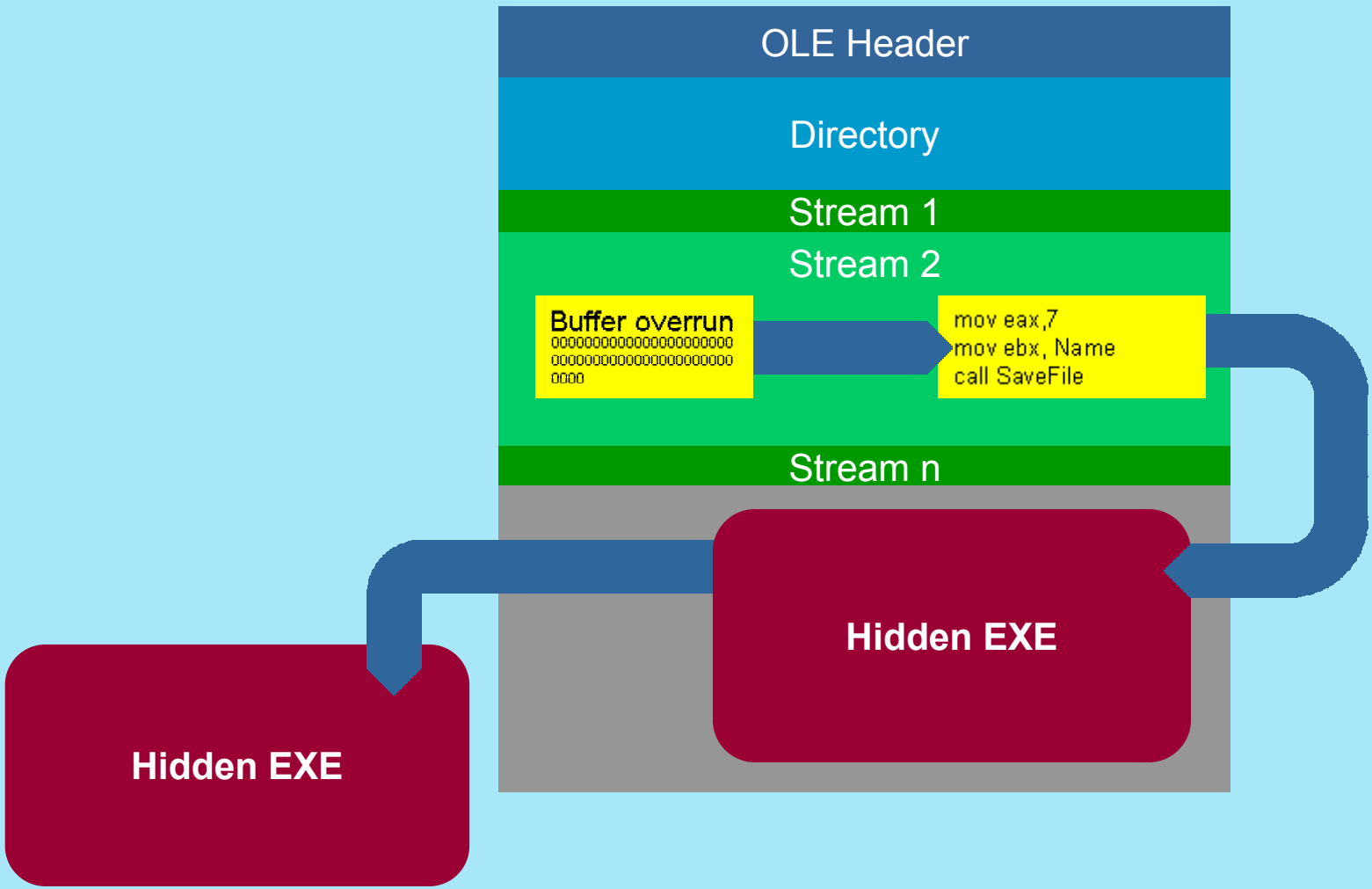
Getting into the Organisation

- Typical example

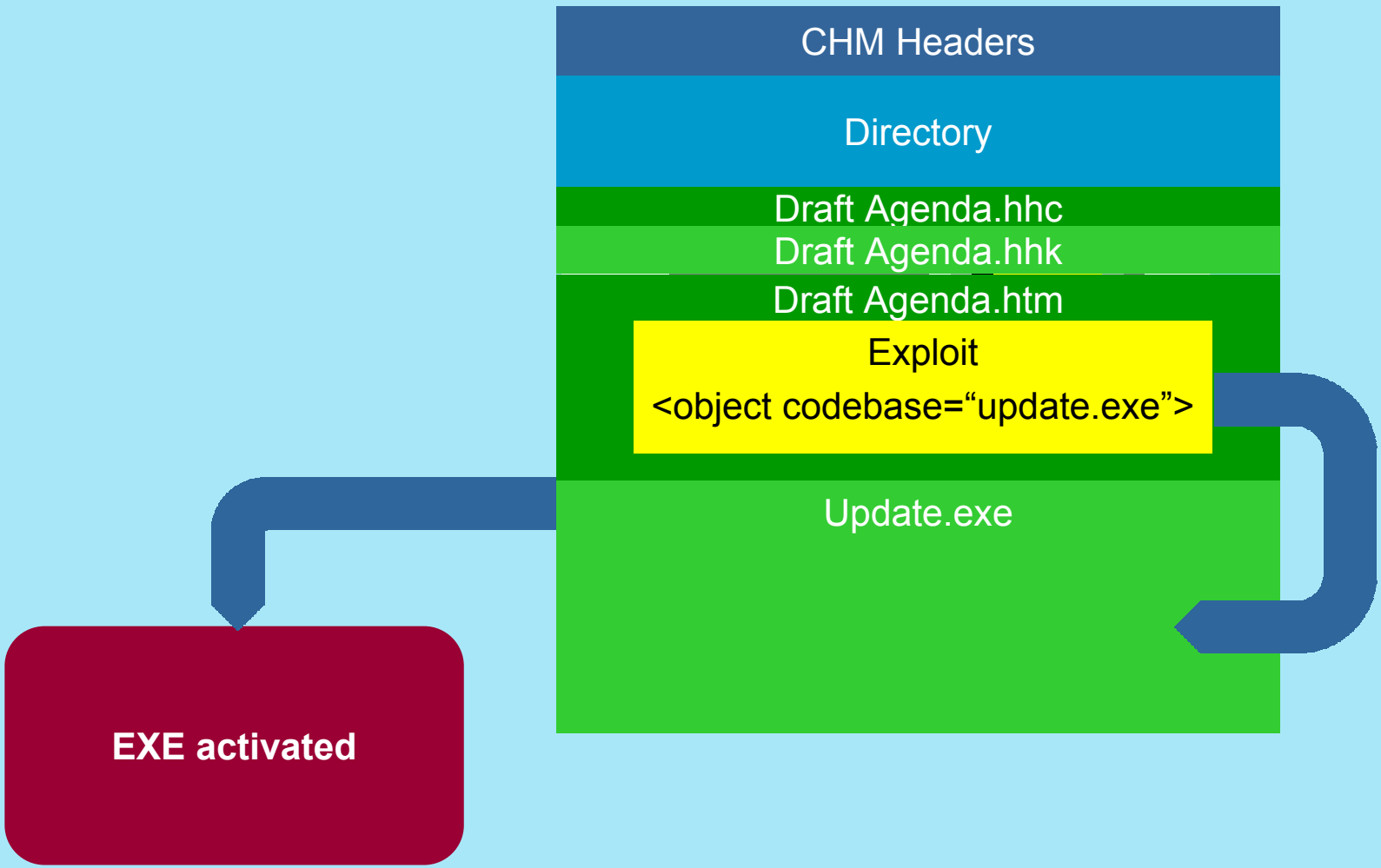




Typical example of exploit in targeted malware



Typical example of exploit in targeted malware



Typical example of exploit in targeted malware (continued)

- **Malicious EXE then typically downloads more components**
  - Network may be compromised
  - Information may be leaked
  - Corporate espionage

Who is being attacked

Targets

Date	Attack vector	Targets	Source
01 Nov 2005	MS Word	ISP	Hong Kong
05 Nov 2005	MS Word	Education	US
11 Nov 2005	MS Help	Petrochemical	US
11 Nov 2005	armoured Exe	Petrochemical, trade, publishing, electonics	China
14 Nov 2005	MS Word	Pharmacutical	China
14 Nov 2005	MS Word	News	Taiwan
14 Nov 2005	MS Help	Legal	Korea
14 Nov 2005	MS Word	Trade, Electronics	61.217.145.123
15 Nov 2005	MS Word	News	211.22.165.180
16 Nov 2005	MS Help	Legal	61.36.170.246
17 Nov 2005	MS Word	Semi-conductor, transport, communications	61.218.104.163
18 Nov 2005	MS Word	Defence, pharmacutical, legal, medical	China
18 Nov 2005	MS Help	Medical	205.118.75.84
30 Nov 2005	MS Word	Trade, paint	221.218.131.92
30 Nov 2005	Exe	NL transport, defense	China
03 Dec 2005	MS Word	Human rights	China
06 Dec 2005	MS Help	Human rights	West Australia
06 Dec 2005	MS Word	Human rights	West Australia
07 Dec 2005	Exe	UK & NL transport, defense, electrical	Taiwan

Recipients - random or selected?

Mr. Mike Ciscmon
Purchasing
IIA Corporation
P.O. Box 1353
Hurt Valley, DM 82030
Subject: RVT Environmental Qualification Testing

Dear Mick:
As XRS proceeds with RVT Environmental Qualification testing, several issues have arisen and we wish to notify you of DRS actions relative to those issues.
“ Solar load test. The RVT will be operational; however, the PCI video option cards (611 and 616) will be non-operational
because of the CDL driver thermal issue which has been brought to AAI’s attention in Art Lowe’s letter, APL:04-0008:3711.
“ Transit drop and loose cargo tests. Both of…

Attack patterns

- **Attack patterns**
  - Very small scale: 1-10 victims
  - Highly targeted recipients
  - Use zero-day exploits
  - Not detected by desktop anti-virus software (no signature)
  - Remain undetected for several months

Detection

MessageLabs

May 2006

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30 Trojan released	31	1	2	3	4

Data from AV-test.org

Detection

Detection Oct 2006

AntiVir, BitDefender, McAfee, WebWasher

No Detection Oct 2006

@Proventia-VPS, Avast!, AVG, ClamAV, Command, Dr Web, eSafe, eTrust-INO, eTrust-VET, Ewido, F-Prot, F-Secure, Fortinet, Ikarus, Kaspersky, Microsoft, Nod32, Norman, Panda, QuickHeal, Rising, Sophos, Symantec, Trend Micro, UNA, VBA32, VirusBuster, YY_Spybot

Data from AV-test.org

Why?

- **Data stealing**
  - Highly targeted organisations
  - Highly targeted recipients
  - Use zero-day exploits
  - Very low volume

How many Gangs?

Attack dates Nov-Dec 05

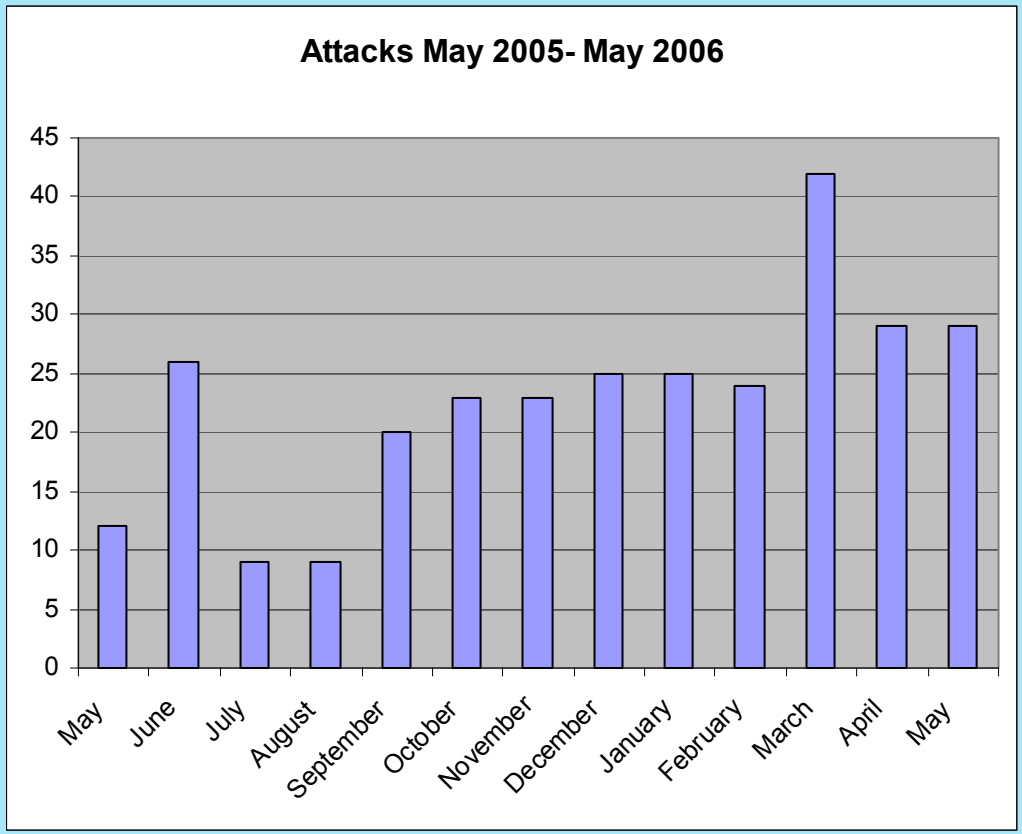
```
Date        Subject
01 Nov 2005 =c3=f7=b1=e7=ca=c7=b7=c7  =bf=aa=c6=f4=d6=c7=bb=db
05 Nov 2005 =c3=f7=b1=e7=ca=c7=b7=c7  =bf=aa=c6=f4=d6=c7=bb=db
11 Nov 2005 China Needs More Tamiflu
11 Nov 2005 =c3=c0=c5=aeFLASH=d3=ce=cf=b7=a3=a8=bd=fb=a3=a9
14 Nov 2005 =c3=f7=b1=e7=ca=c7=b7=c7  =bf=aa=c6=f4=d6=c7=bb=db
14 Nov 2005 =b9q=a4l=c9=ac=b4f=a8=e9
14 Nov 2005 Fw:WorldBank Prices US$8 Billion For Influenza Cases In America And Asia
14 Nov 2005 =b9q=a4l=c9=ac=b4f=a8=e9
15 Nov 2005 TSR=bbO=c6W=a6w=a5=fe=ac=e3=a8s=b6g=b3=f8
16 Nov 2005 Fw:New Law For Bank International Trading 2005
17 Nov 2005 Center for European Policy Studies' Commentary
18 Nov 2005 Police: 54 guns found in teen's home
18 Nov 2005 From Bird to Human, China Needs More Tamiflu !
30 Nov 2005 =c3=f7=b1=e7=ca=c7=b7=c7  =bf=aa=c6=f4=d6=c7=bb=db
30 Nov 2005 GE Transportation Signs Training Agreement with Tusas Engine Industries


03 Dec 2005 =c3=f7=b1=e7=ca=c7=b7=c7  =bf=aa=c6=f4=d6=c7=bb=db
06 Dec 2005 Do you know How the US Supplied Iran with Nuclear Know-How?
06 Dec 2005 Bird flu's truth in mylasia
07 Dec 2005 Subject:  RVT Environmental Qualification Testing
```

How many gangs involved?

- **Gang 1**
  - Most active
  - Wide variety of ploys
  - Often use zero day
- **Gang 2**
  - Targets Hong Kong based organisations
- **Gang 3**
  - Very small scale
  - One email every two weeks
  - From IP in California
  - Military target

Trends



- **Upward trend in attacks**

Metrics

- **How important is this anyway?**
- **Very small probability of attack**
  - **0.001% of all email**
  - **Recipient might not open email anyway**
  - **Recipient might not be running right software for vulnerability**
- **Very high cost if successful**
  - **Company IP is very valuable**
  - **May be worth $millions for a big company**
  - **May be worth everything for a small company**
- **Small number * big number**
  - Hard to put a value & risk rating

Predictions

- **Will continue to increase**
  - Current gangs increase activity
  - Other gangs enter the fray
- Best technique is zero day exploits via email
  - Will see more zero day exploits
  - More file formats than office & help
- Other electronic ways than email
- Other ways than electronically

For more information…

Alex Shipp (ashipp@messagelabs.com)

www.messagelabs.com/intelligence

MessageLabs

Be certain