RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Information Exchange on Targeted Incidents in Practice

SESSION ID: ANF-F03A

Freddy Dezeure

Head of CERT-EU

Set-up

- EU Institutions’ own CERT
- Supports 60+ entities
- Small (16 people) team
- Specialised in targeted attacks

Constituents

- EU Institutions, Bodies and Agencies
- Located in many different countries
- From 40 – 40.000 users
- Cross-sectoral
  - Government, foreign policy, embassies
  - Banking, energy, pharmaceutical, chemical, food, telecom
  - Maritime, rail and aviation safety
  - Law enforcement (EUROPOL, FRONTEX, EUPOL) and justice
  - Research, hi-tech, navigation (GALILEO), defence (EUMS, EDA)
- Very high value targets

APT: difference in speed

- Initial infection very difficult to avoid
- Take control over the infrastructure: 10’ -> 48hours

- Detection: more than 1 year (or never)
- Remediation: 1-6 months

Challenges in information sharing

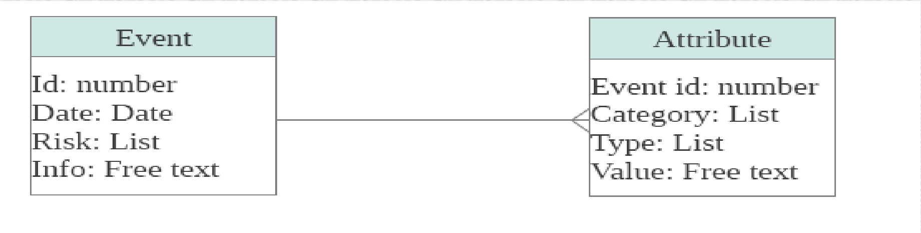
- Information overflow
  - Public information
  - Information without context
  - Overload of irrelevant information
- Information deficit
  - Fear of brand image damage
  - (over) classified
  - Lack of tools

Way forward

- Circles of trust
  - Communities of organizations that trust each other
  - Sharing non-public information
- Data quality
  - Validated at the source
  - In context
- Automated tools
  - Synchronization
  - Correlation

MISP Platform

- Developed by CERT community (BE, NATO, LU, EU)
- Managing threat intelligence (IOCs and context)
- Correlating events
- Sharing validated, relevant, fresh, non-public intelligence



Event

Id: number
Date: Date
Risk: List
Info: Free text

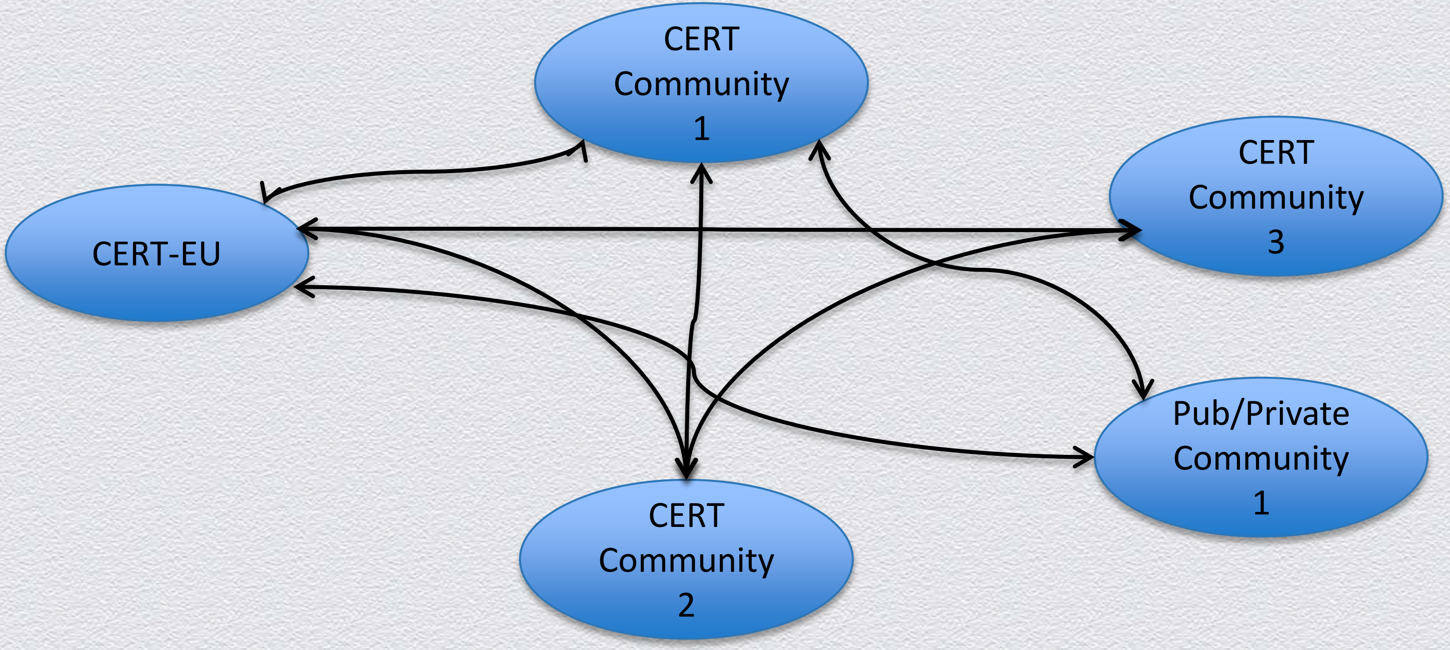
Attribute

Event id: number
Category: List
Type: List
Value: Free text

Input data

- From incidents in the constituency (Input by duty officer / incident handler)
- From trusted groups (Input by threat analyst)
- From commercial subscriptions
- From other information sharing instances

Synchronization with multiple instances



Use Cases

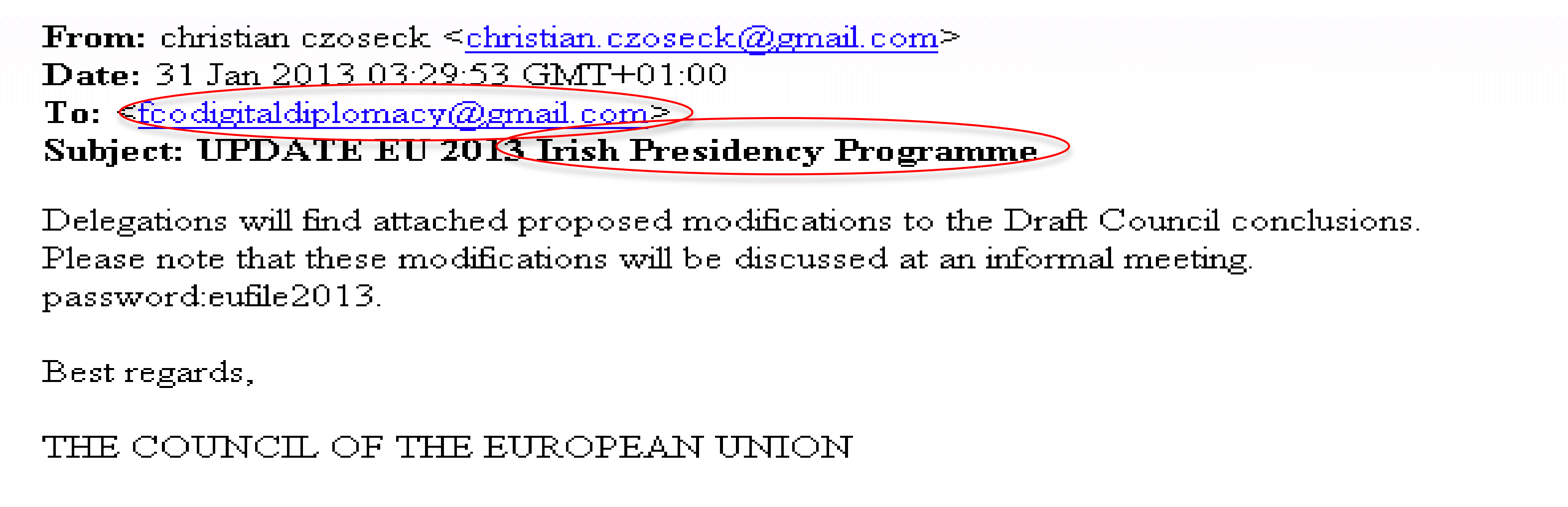
1. Correlating incidents
2. Detecting new incidents
3. Scoping incidents
4. Sharing out

Use Case 1

Handling of new events / information

- Entering data in the repository automatically correlates
- Check initial suspicious data (Email components, Beaconing destination, MD5)
- Find previous incidents (Constituency / partners, Context, Criticality)
- Enrich existing information (Campaigns, Groups, TTPs)

Spear Phishing

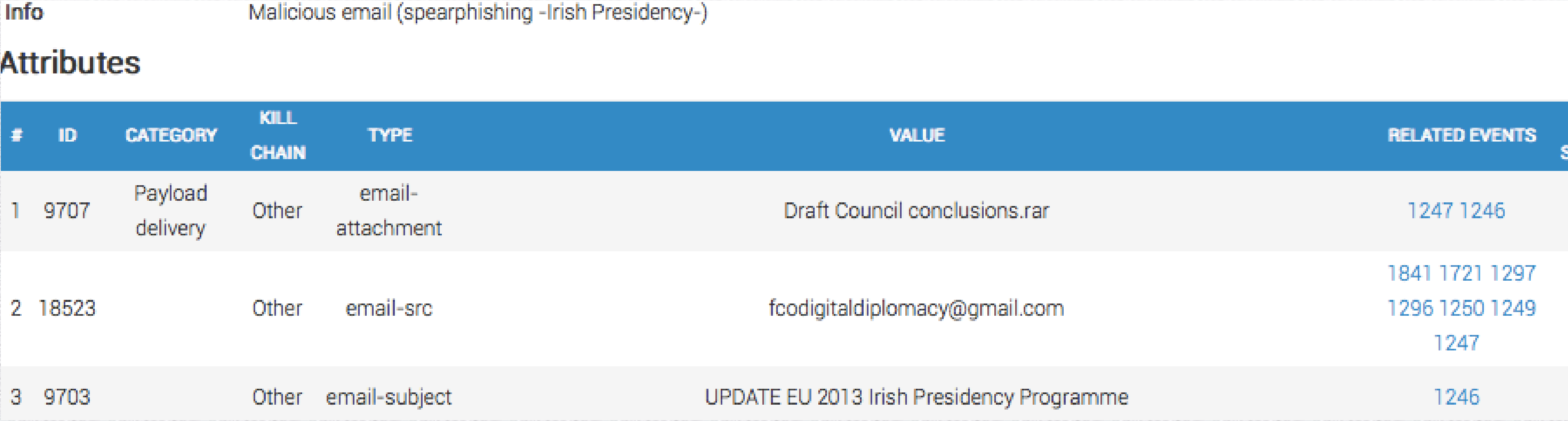


From: christian czoseck <christian.czoseck@gmail.com>
Date: 31 Jan 2013 03:29:53 GMT+01:00
To: <fcodigitaldiplomacy@gmail.com>
Subject: UPDATE EU 2013 Irish Presidency Programme

Delegations will find attached proposed modifications to the Draft Council conclusions.
Please note that these modifications will be discussed at an informal meeting.
password:eufile2013.

Best regards,

THE COUNCIL OF THE EUROPEAN UNION



Info Malicious email (spearphishing -Irish Presidency-)

Attributes

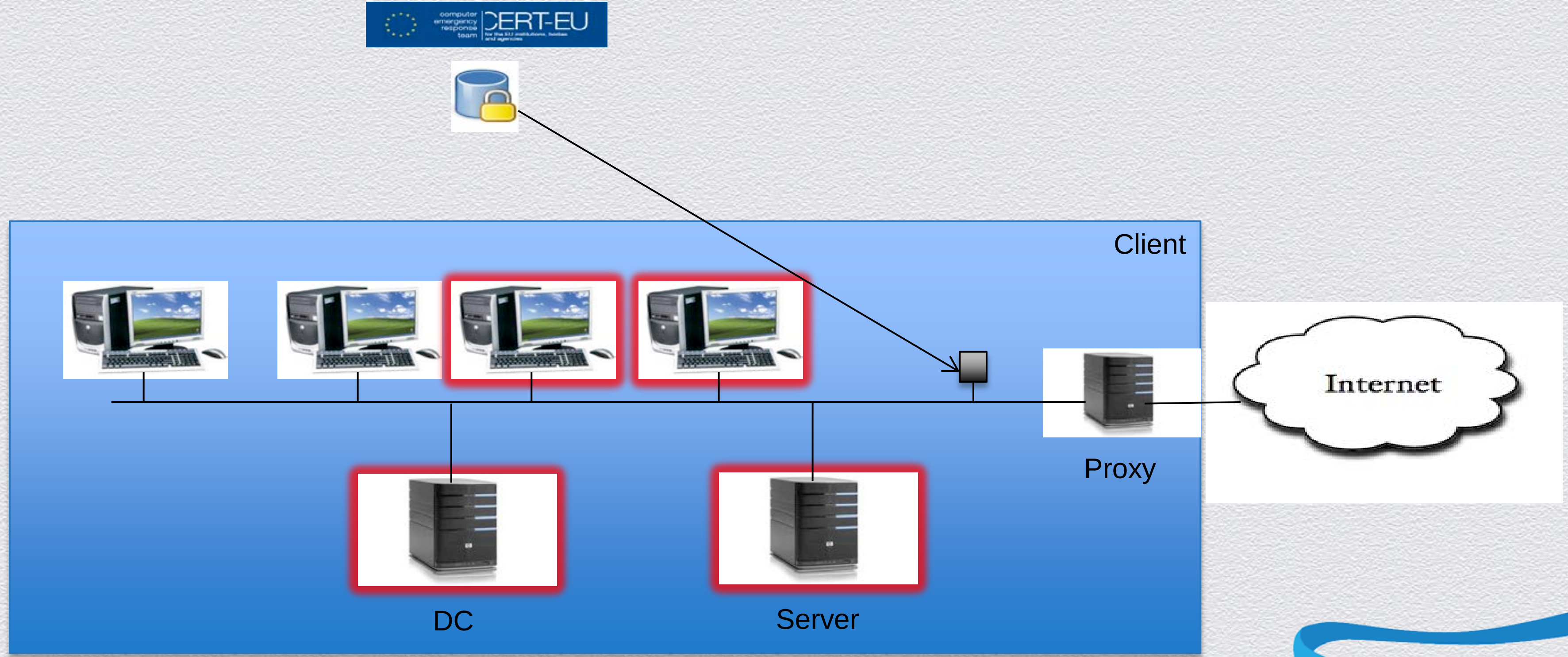
#	ID	CATEGORY	KILL CHAIN	TYPE	VALUE	RELATED EVENTS
1	9707	Payload delivery	Other	email-attachment	Draft Council conclusions.rar	1247 1246
2	18523		Other	email-src	fcodigitaldiplomacy@gmail.com	1841 1721 1297 1296 1250 1249 1247
3	9703		Other	email-subject	UPDATE EU 2013 Irish Presidency Programme	1246

Use Case 2

Detecting new events in the constituency

- Using all the threat intelligence in the repository
- Tools: IDS (SNORT, SURICATA), SIEM
- High value alerts

IDS detection


computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies
Client
Internet
Proxy
DC
Server

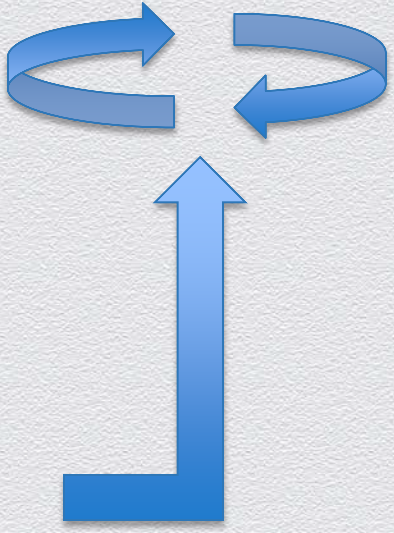
Use Case 3

Scoping during incident response

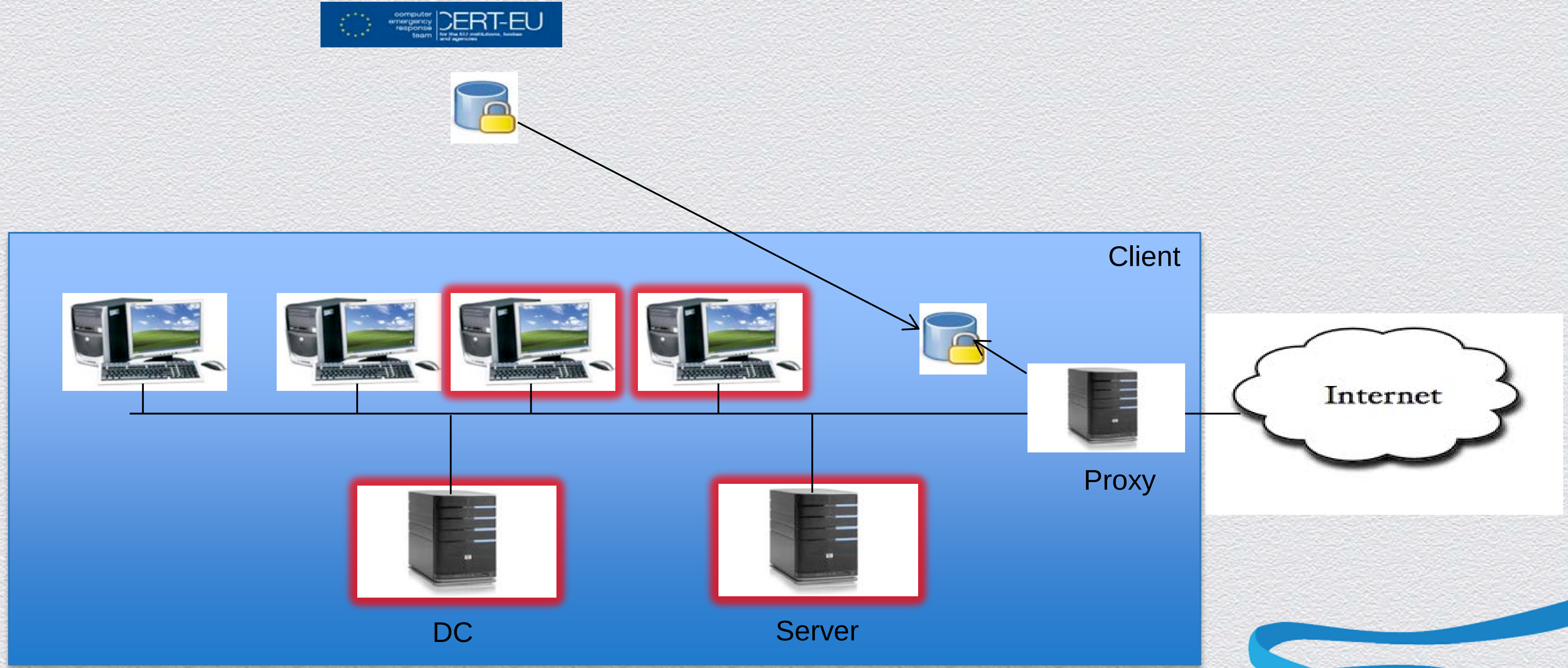
- Using specific incident-related intelligence
- Tools: SIEM, log correlation, h-ids, n-ids
- Enrichment at every stage
- Cross-search through the constituency

Scoping

- Malware reversing
- Internal process
  - Scanning for IOCs in the network and endpoints
- External process
  - Has anybody else seen this?
    - No? -> You're on your own
    - Yes? -> Enrich knowledge on IOCs
  - What's the timeline?



Scoping during incident response


computer emergency response team CERT-EU for the EU institutions, bodies and agencies
Client
Internet
Proxy
DC
Server

2013: Example

- Day 0: Escalation to DA
- Day 1: Detection
- Day 2:
  - Reversing from remotely obtained forensics -> 2 C&Cs
  - Sharing with 10 IT sec partners -> attribution, enrichment of IOCs, additional C&C
- Day 3 -> 6: Enrichment (C&C, decryption), scoping and detection. No new infections.

Use Case 4

Sharing out

- Only information we own is shared
- Constituent agreement to share
- Shared with CERT-EU's circles of trust
- Delivery mechanism
  - Weekly email (csv or xml)
  - ReST API
  - TAXII

Final words

- Timely sharing of relevant information helps to protect us
- Tools are only tools
- Data quality and context are crucial
- Circles of trust are fundamental

Thank you!

http://cert.europa.eu