Cyber Threat Intelligence
CERT-EU vision

KYRIAKOS SATLAS

CERT-EU/CTI team

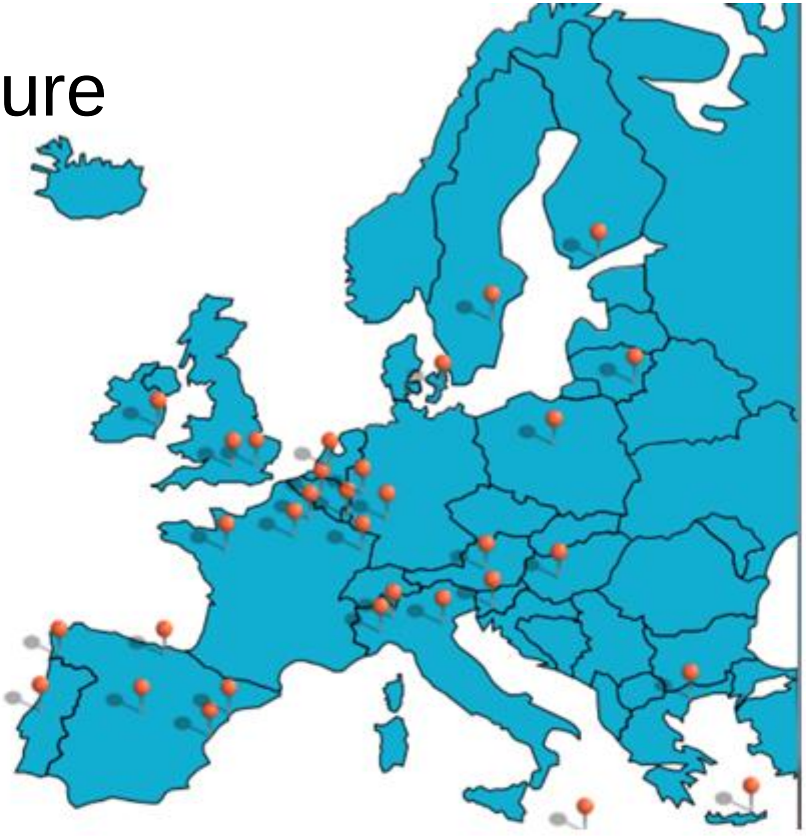
TLP-WHITE

About us

- EU Institutions’ own CERT
- Operational support to 60 organisations, 100.000 users
- Defence against sophisticated, targeted cyber threats
- Hub of information and skills

* Our Challenges

- Spread all over Europe
- Cross-sectoral
- Heterogenous infrastructure
- High-value targets



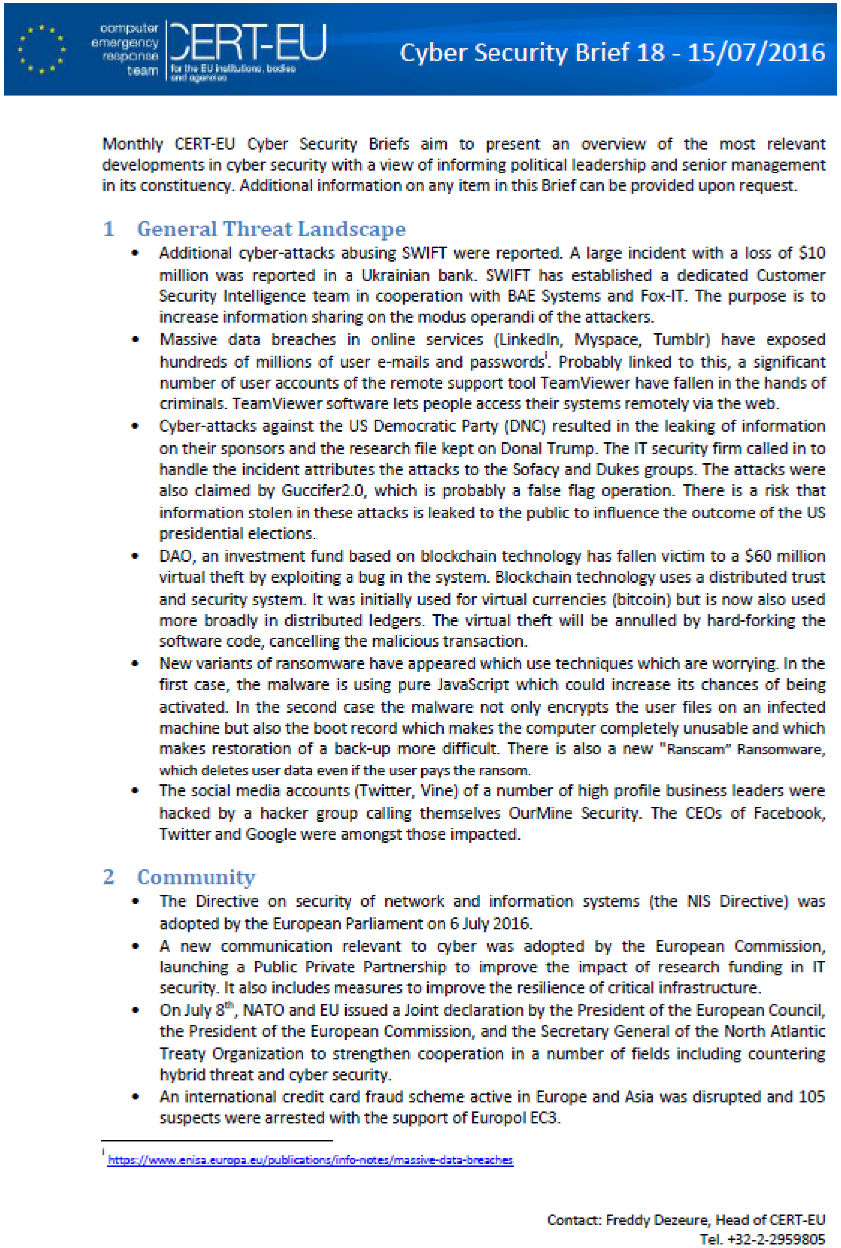
* Services

1. Announcements & advisories
2. Alerts & warnings
3. Incident response support & coordination
4. Cyber threat intelligence
5. Incident response & analysis on site
6. Artefact analysis & actions
7. Development of security tools
8. Intrusion detection & log management
9. Vulnerability assessment & pen testing

Our Products

- Cyber Security Brief
  - Threat Landscape report
    - CITAR Flash
      - CIMBL

Security Briefs



computer emergency response team CERT-EU for the EU institutions, bodies and agencies

Cyber Security Brief 18 - 15/07/2016

Monthly CERT-EU Cyber Security Briefs aim to present an overview of the most relevant developments in cyber security with a view of informing political leadership and senior management in its constituency. Additional information on any item in this Brief can be provided upon request.

1 General Threat Landscape

- Additional cyber-attacks abusing SWIFT were reported. A large incident with a loss of $10 million was reported in a Ukrainian bank. SWIFT has established a dedicated Customer Security Intelligence team in cooperation with BAE Systems and Fox-IT. The purpose is to increase information sharing on the modus operandi of the attackers.
- Massive data breaches in online services (LinkedIn, Myspace, Tumblr) have exposed hundreds of millions of user e-mails and passwords[i]. Probably linked to this, a significant number of user accounts of the remote support tool TeamViewer have fallen in the hands of criminals. TeamViewer software lets people access their systems remotely via the web.
- Cyber-attacks against the US Democratic Party (DNC) resulted in the leaking of information on their sponsors and the research file kept on Donal Trump. The IT security firm called in to handle the incident attributes the attacks to the Sofacy and Dukes groups. The attacks were also claimed by Guccifer2.0, which is probably a false flag operation. There is a risk that information stolen in these attacks is leaked to the public to influence the outcome of the US presidential elections.
- DAO, an investment fund based on blockchain technology has fallen victim to a $60 million virtual theft by exploiting a bug in the system. Blockchain technology uses a distributed trust and security system. It was initially used for virtual currencies (bitcoin) but is now also used more broadly in distributed ledgers. The virtual theft will be annulled by hard-forking the software code, cancelling the malicious transaction.
- New variants of ransomware have appeared which use techniques which are worrying. In the first case, the malware is using pure JavaScript which could increase its chances of being activated. In the second case the malware not only encrypts the user files on an infected machine but also the boot record which makes the computer completely unusable and which makes restoration of a back-up more difficult. There is also a new "Ranscam" Ransomware, which deletes user data even if the user pays the ransom.
- The social media accounts (Twitter, Vine) of a number of high profile business leaders were hacked by a hacker group calling themselves OurMine Security. The CEOs of Facebook, Twitter and Google were amongst those impacted.

2 Community

- The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016.
- A new communication relevant to cyber was adopted by the European Commission, launching a Public Private Partnership to improve the impact of research funding in IT security. It also includes measures to improve the resilience of critical infrastructure.
- On July 8th, NATO and EU issued a Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization to strengthen cooperation in a number of fields including countering hybrid threat and cyber security.
- An international credit card fraud scheme active in Europe and Asia was disrupted and 105 suspects were arrested with the support of Europol EC3.

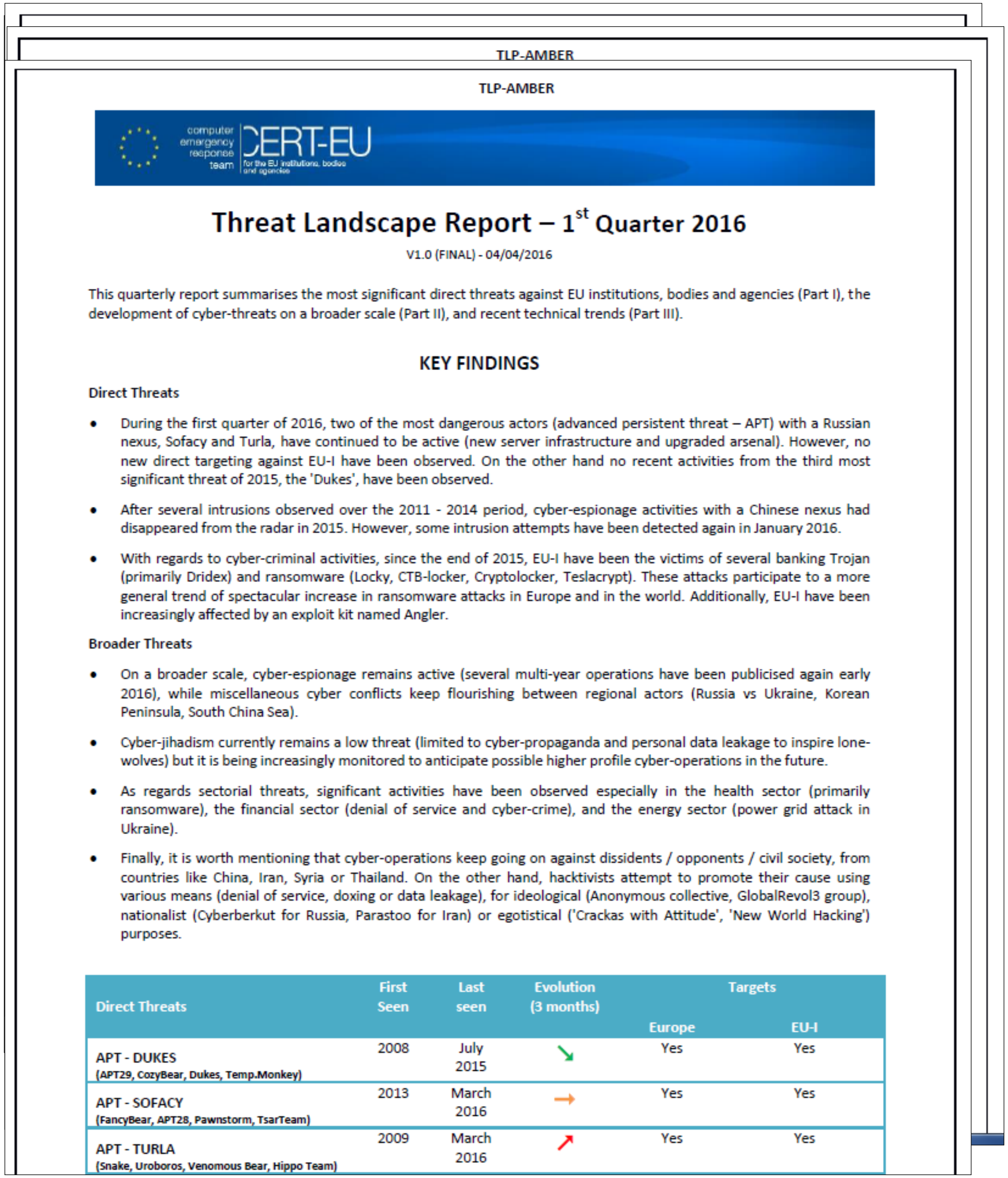
[i] https://www.enisa.europa.eu/publications/info-notes/massive-data-breaches

Contact: Freddy Dezeure, Head of CERT-EU
Tel. +32-2-2959805

- Since 2014
- Monthly
- Open source information, hand-picked and commented
- Direct and broader threats
- Distribution:
  - 300 people from Constituents on technical, managerial and political level
  - CSIRT network

computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

Threat Landscape Reports



TLP-AMBER

TLP-AMBER

computer emergency response team CERT-EU for the EU institutions, bodies and agencies

Threat Landscape Report – 1st Quarter 2016

V1.0 (FINAL) - 04/04/2016

This quarterly report summarises the most significant direct threats against EU institutions, bodies and agencies (Part I), the development of cyber-threats on a broader scale (Part II), and recent technical trends (Part III).

KEY FINDINGS

Direct Threats

- During the first quarter of 2016, two of the most dangerous actors (advanced persistent threat – APT) with a Russian nexus, Sofacy and Turla, have continued to be active (new server infrastructure and upgraded arsenal). However, no new direct targeting against EU-I have been observed. On the other hand no recent activities from the third most significant threat of 2015, the 'Dukes', have been observed.
- After several intrusions observed over the 2011 - 2014 period, cyber-espionage activities with a Chinese nexus had disappeared from the radar in 2015. However, some intrusion attempts have been detected again in January 2016.
- With regards to cyber-criminal activities, since the end of 2015, EU-I have been the victims of several banking Trojan (primarily Dridex) and ransomware (Locky, CTB-locker, Cryptolocker, Teslacrypt). These attacks participate to a more general trend of spectacular increase in ransomware attacks in Europe and in the world. Additionally, EU-I have been increasingly affected by an exploit kit named Angler.

Broader Threats

- On a broader scale, cyber-espionage remains active (several multi-year operations have been publicised again early 2016), while miscellaneous cyber conflicts keep flourishing between regional actors (Russia vs Ukraine, Korean Peninsula, South China Sea).
- Cyber-jihadism currently remains a low threat (limited to cyber-propaganda and personal data leakage to inspire lone-wolves) but it is being increasingly monitored to anticipate possible higher profile cyber-operations in the future.
- As regards sectorial threats, significant activities have been observed especially in the health sector (primarily ransomware), the financial sector (denial of service and cyber-crime), and the energy sector (power grid attack in Ukraine).
- Finally, it is worth mentioning that cyber-operations keep going on against dissidents / opponents / civil society, from countries like China, Iran, Syria or Thailand. On the other hand, hacktivists attempt to promote their cause using various means (denial of service, doxing or data leakage), for ideological (Anonymous collective, GlobalRevol3 group), nationalist (Cyberberkut for Russia, Parastoo for Iran) or egotistical ('Crackas with Attitude', 'New World Hacking') purposes.

Direct Threats	First Seen	Last seen	Evolution (3 months)	Targets	
				Europe	EU-I
APT - DUKES (APT29, CozyBear, Dukes, Temp.Monkey)	2008	July 2015	↘	Yes	Yes
APT - SOFACY (FancyBear, APT28, Pawnstorm, TsarTeam)	2013	March 2016	→	Yes	Yes
APT - TURLA (Snake, Uroboros, Venomous Bear, Hippo Team)	2009	March 2016	↗	Yes	Yes

- Since June 2015
- Quarterly
- Mostly non-public information
- Direct and broader threats
- Key developments and trends
- Distribution:
  - Constituents
  - CSIRT network
  - Presidency

CITAR Flash

- One page report
- It is addressed to both Management and technical audience
- The aim is to raise awareness about on going threats
- The trigger for release is the relevance of an attack or threat to our constituents

CIMBL

- Technical product that is a collection of IoCs
- It is addressed to our Constituents, other CERTs and Partners
- STIX and csv packaging
- Released weekly or on an ad-hoc basis

CERT-EU products eligibility criteria

- Threat Landscape
  - Be a CERT-EU constituent
  - Or
  - Be a Gov/Nat CSIRT of an EU Member State

- CITAR Flash
  - Be a CERT-EU constituent
  - Or
  - Be a Gov/Nat CSIRT of an EU Member State

- Indicators from CERT-EU constituency (via MISP)
  - TLP:AMBER: be a CERT-EU constituent
  - TLP:GREEN: have an NDA with CERT-EU
  - TLP:WHITE: belongs to the MISP community

- "If you meet the criteria and would like to receive our products, please contact us"

Trends

- Data breaches and exposure
  - Equifax (consumer credit reporting agency) – 143 millions individuals impacted
  - Deloitte (accountancy) – Several major customer orgs impacted
  - Accenture (global consulting) – via Amazon Web Services Storage

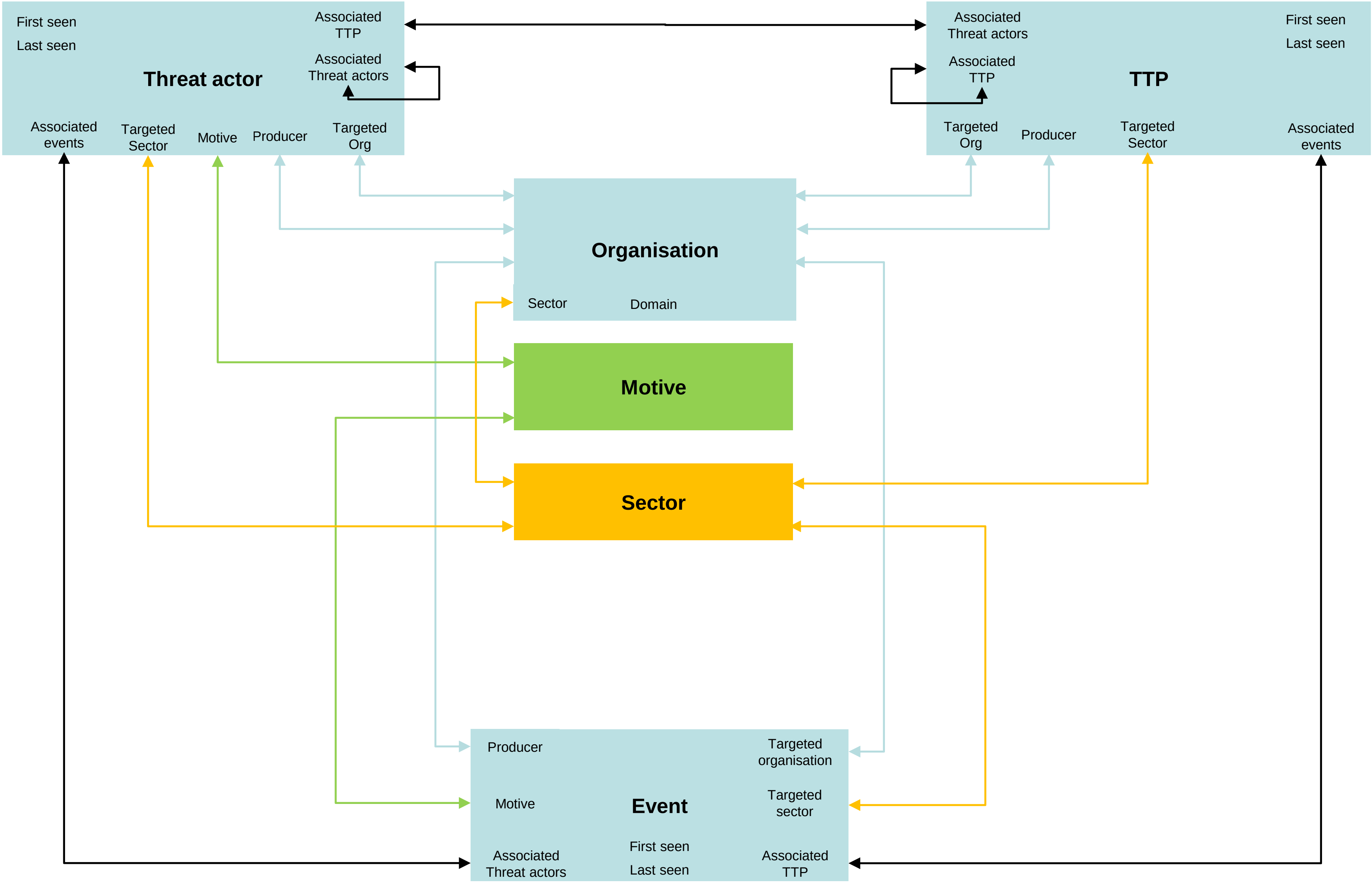
- Supply chain attacks
  - Target the 'weakest link' in the chain and maximize impact
  - Software repositories, Software update, App stores, …

- Cyber weapons
  - Sophisticated cyber attack tools leaked and re-used
  - Wannacry, NotPetya

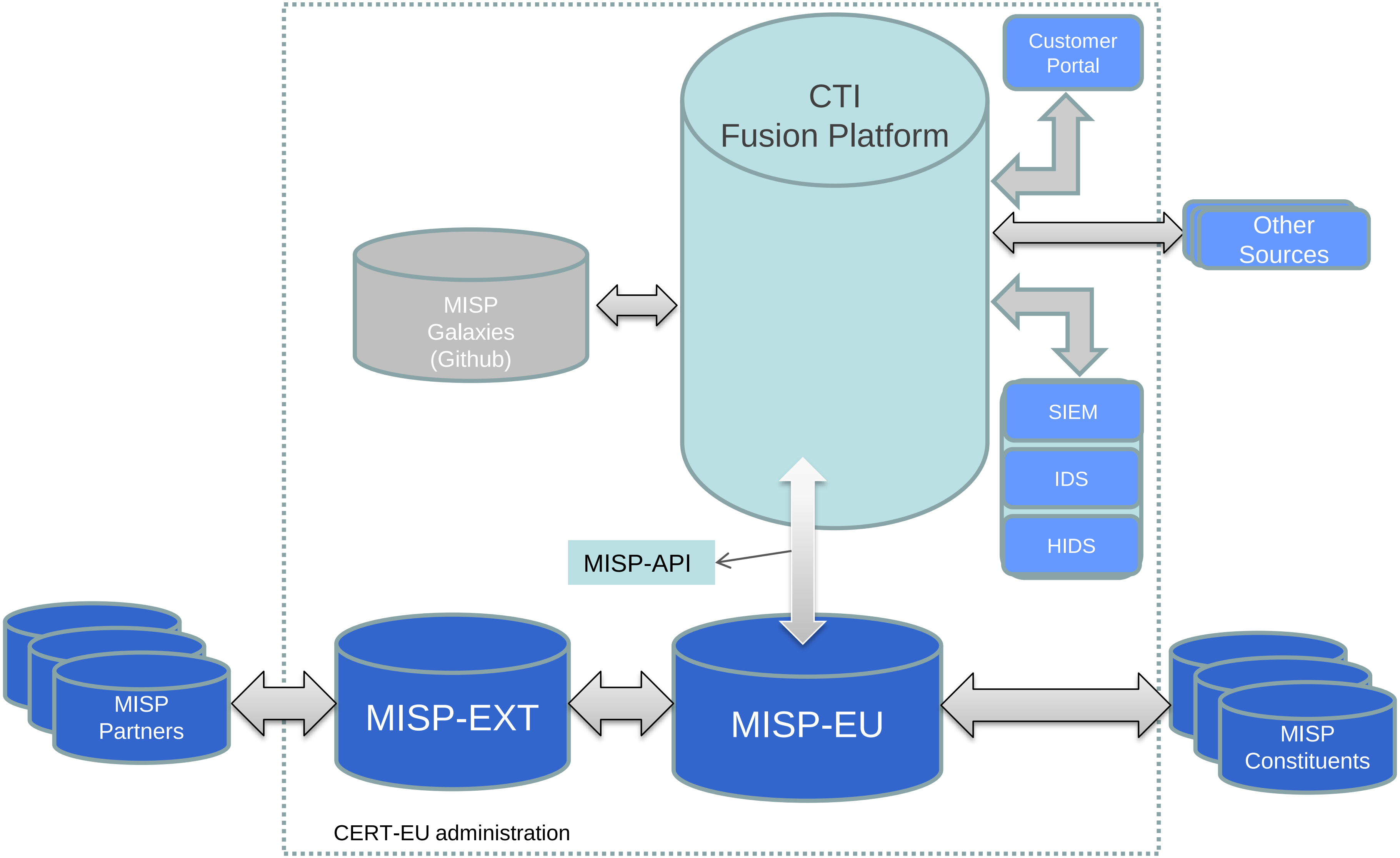
- Crypto currency targeting
  - New techniques to obtain currency for criminal activities

computer emergency response team CERT-EU for the EU institutions, bodies and agencies

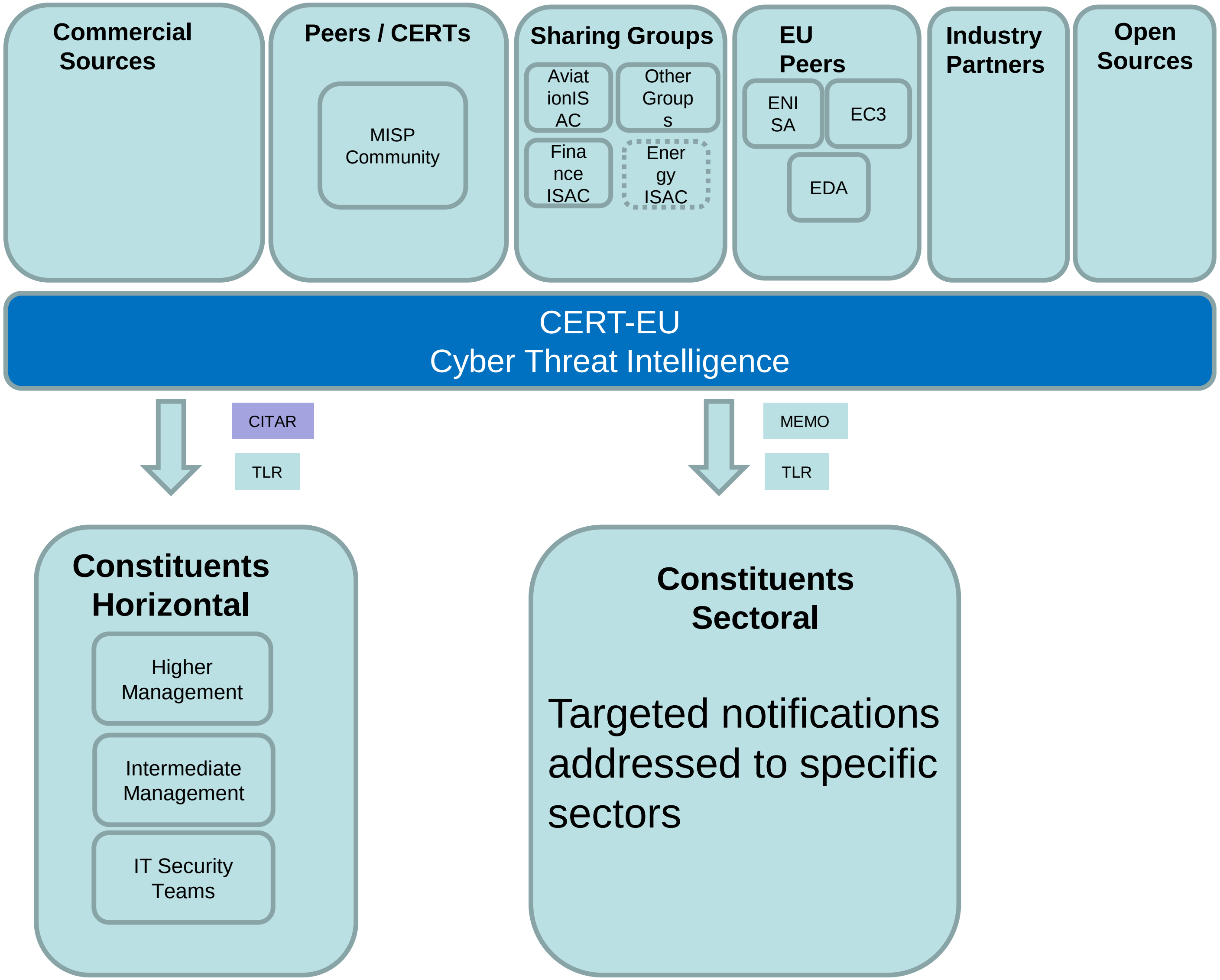
Our Data Model



Indicator Data Flow



Threat Assessment Data Flow



Commercial Sources

Peers / CERTs

MISP Community

Sharing Groups

AviationISAC

Other Groups

Finance ISAC

Energy ISAC

EU Peers

ENISA

EC3

EDA

Industry Partners

Open Sources

CERT-EU
Cyber Threat Intelligence

CITAR

TLR

MEMO

TLR

Constituents Horizontal

Higher Management

Intermediate Management

IT Security Teams

Constituents Sectoral

Targeted notifications addressed to specific sectors

Knowledge Bases
TECHNIQUES TACTIC PROCEDURES

Attack Patterns (G)

- Common techniques used by attackers
- Useful for trends / basic profiling
- Useless for attribution

Attack Patterns (S)

- Special techniques not accessible to any attacker
- May be used for characterisation of malware.

Targeting

Election, Media, Cryptocurrency, ATM, CII, ICS, Electric grid, IoT, iOS,

- Assets being specifically targeted by TA
- profiling of TA

Tactic

Sabotage, disruption, disinformation, information war, illicit trading, etc

- Non technical identification of tactical objectives pursued by attackers

Malware

RAT / backdoor ransomware/ banking trojan etc

- Malware family level
- Focus on malware used in targeted attacks

Exploits

Exploit Kits (Angler, Metasploit, SweetOrange, Nuclear, etc), CVE

- Symmetrical to CVE / Exploit Target

Tools

Shell, Port scanners, Web vulnerability scanners etc,.

- Legitimate tools re-purposed or customised for malicious use.
- Understanding TTP supply chain

Infrastructures

Delivery infra (phishing, watering hole, etc), C2 infra, bots, forums, malware sites, darknets, etc

- Pivoting for attribution

Knowledge Bases THREAT ACTORS

KB1 – Cyber-Criminals

Individuals or groups involved in cyber-criminal activities. Their motive is financial gain

Priority: Low

KB2 – Cyber Warfare

State or state-sponsored groups involved in malicious activities (beyond cyber-espionage) against other states

Priority: Medium

KB3 – Cyber Espionage

Groups or individuals involved in state/strategic espionage or economic espionage (IPR theft)

Priority: High

KB4 - Hacktivists

Groups or individuals involved in hactivist activity to promote a cause or an ideology, or having egotistic motive

Priority: High

KB5 – Hacktivists-Nationalists

State-sponsored or independent groups promoting a nationalist cause.

Priority: Medium

KB6 – Cyber-Jihadists

Groups or individuals involved in jihadism via cyber means: defacement, on-line recruitment, doxxing, etc

Priority: High

ENISA, EDA, EC3, CERT-EU

It is important to synchronize European Institution efforts towards a secure IT environment

Status: Draft Memorandum of understanding

European Institutions Cooperation

- CERT-EU can provide operational experience from the European Institutions IT environment

European Institutions Cooperation

- Products and reports peer review
- Information exchange
- Pre-release notifications

The way forward

- Improve our CTI infrastructure
  - Simplify system’s architecture
  - Closely follow MISP evolution
  - Enhance cooperation with CIRCL and MISP user groups (military and others)
  - Better utilize MISP tactical features

Cyber threat intelligence CERT-EU vision

- Develop strong relationships with other public entities (Constituents, CERTs, Partners) and private entities (Vendors)
- Diversify the sources to increase the quantity of malicious data
- Enhance technical checks to improve quality
- Automate distribution and consumption to reduce delay

QUESTIONS?

Thank you

KYRIAKOS SATLAS
Kyriakos.satlas@ec.europa.eu

TLP-WHITE