Council of the European Union

Brussels, 24 May 2016
(OR. en)

8866/16

CYBER 53
ENFOPOL 160
PROCIV 36
IPCR 8
TELECOM 95
COPEN 179
RELEX 437

NOTE

From:	Presidency
To:	Delegations
Subject:	ENISA Threat landscape 2015

The ENISA Threat Landscape 2015 (ETL 2015)[1] is the result of a comprehensive analysis of cyber-threats that have been encountered in the period between December 2014 and December 2015. ETL 2015 is the fourth in a series of reports issued yearly by ENISA.

Just as previous threat landscape reports, ETL 2015 is based mainly on open source intelligence that is being created mainly within ENISA - an amount of knowledge on the development of cyber-threats created on annual basis. The analysis is followed by a collation of threat information. In this process, cyber-incidents, cyber-threats, cyber-attacks, etc. are put in context to by means of correlated information.

The ETL 2015 looks at the state and the dynamics of the cyber-threat environment and acknowledges as one of the main features its increasing maturity, i.e. a great degree of sophistication both in terms of preparation and execution of cyber-attacks, as for example persistent cyber-attacks based on hardware or attacks against routers, firmware and Internet of things, enhancement of provision of cybercrime as a service, including automated tools for detection and exploitation of vulnerabilities.

[1] https://www.enisa.europa.eu/publications/etl2015

On the basis of the finding ENISA has compiled a Roadmap with aspects to be addressed by the policy, business and research experts.

Therefore, delegations are kindly requested to consider the following suggestions of the report:

1/ Need to streamline and consolidate existing policies, defences and cooperation to accommodate the changes in the threat landscape

2/ Need to undertake specific activities to counter the consumerisation of cybercrime

3/ Make collection, management and sharing of threat intelligence part of the national cyber defence capabilities;

4/ Foster voluntary reporting and perform analyse of the reported incidents

5/ Disseminate cyber-threat knowledge to all players in cyberspace, including end users.

In view of those suggestions delegations are also invited to provide their views on the following questions:

- What conclusions can be drown?
- How can this report be better used?
- Is there a case for having other, less technical reports, such as geopolitical threat evolution?