National Authority Against Electronic Attacks- National CERT

RFC2350(Public)

Version 1.0 -2017.09.26

TLP[1]: WHITE

1. About this document

This document describes the National Authority Against Electronic Attacks-National CERT operation in accordance with RFC 2350.

1.1 Date of Last Update

This is version 1.0, published on September 2017. This version is valid until superseded by a later version.

1.2 Distribution List for Notifications

Changes to this document are not distributed by a mailing-list or any other mechanism. Please address any specific questions or remarks to cert@nis.gr e-mail address. (see § 2.7).

1.3 Locations where this Document May Be Found

The current version of this CERT description document is available at National Authority Against Electronic Attacks-National CERT's website at http://www.cert.gov.gr. Please make sure you are using the latest version.

1.4 Authenticating this Document

This document is signed with National Authority Against Electronic Attacks-National CERT's PGP key. PGP Fingerprint is available at http://www.cert.gov.gr in the respective link (PGP_Public_national_cert.asc)

2. Contact Information

2.1 Name of the Team

National Authority Against Electronic Attacks- National CERT.

2.2 Address

National Authority Against Electronic Attacks- National CERT
4 P. Kanellopoulou,
Athens 10177,
Greece

[1] TLP: The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information.

2.3 Time Zone

EET, Eastern European Time (UTC+2, between last Sunday of October and last Sunday of March)

EEST, Eastern European Summer Time (UTC+3, between last Sunday of March and last Sunday of October)

2.4 Telephone Number

+30 210 6973112

2.5 Facsimile Number

Not available.

2.6 Other Telecommunication

Available upon reasonable requests (e.g. GSM etc).

2.7 Electronic Mail Address

cert@nis.gr

This e-mail address is used for reporting an incident as well as for other business related to National Authority Against Electronic Attacks- National CERT services.

2.8 Public Keys and Other Encryption Information

National Authority Against Electronic Attacks- National CERT has a PGP key, with

KeyID: 0xA3BACE47, and

PGP Fingerprint: 8F58 C6C8 414D DA71 5D01 8310 54D1 3895 FC19 6D8B

The public key and its signatures can be found on the usual large public key servers as well as on National Authority Against Electronic Attacks- National CERT public web site (http://www.cert.gov.gr).

2.9 Team Members

The National Authority Against Electronic Attacks- National CERT team members are available by request.

2.10 Other Information

General information about National Authority Against Electronic Attacks- National CERT as well as links to various recommended security documents, can be found at (http://www.cert.gov.gr)

2.11 Points of Customer Contact

The preferred method for contacting National Authority Against Electronic Attacks-National CERT is via e-mail *cert@nis.gr*. All incidents reports should be sent to *cert@nis.gr.* National Authority Against Electronic Attacks-National CERT encourages its constituents to use secure e-mail (for instance PGP) when exchanging any sensitive information.

Alternatively, the official phone number indicated in §.2.4 may be used.

National Authority Against Electronic Attacks- National CERT's hours of operation are generally restricted to regular business hours (07:30-15:30 on Monday to Friday except Greek holidays).

3 Charter

3.1 Mission Statement

The mission of the National Authority Against Electronic Attacks-National CERT is to attend to the prevention as well as the passive and active encounter of electronic attacks against communication networks, data storage facilities, IT systems and Critical Infrastructures. In addition, the Authority is responsible for processing the data and notifying the competent authorities.

3.2 Constituency

National Authority Against Electronic Attacks-National CERT is the national Greek CERT since 2009. It's constituency is established by Bill 3469/2008 and Presidential Decree 126/2009. The main areas of the National Authority Against Electronic Attacks-National CERT are:

- Protecting against electronic attacks and information security incidents mainly the Public Sector and the Critical National Infrastructures.
- Acting as the single point of contact for foreign CERTs/CSIRTs, as the national CERT.
- Coordinating the activities in case of an elevated situation and implementing the strategic policy decisions nationally and internationally pertaining to the encountering of threats and/or attacks.
- Educating the nation and national IT sector on cyber threat.
- Cooperating with foreign national or other CERT authorities and relevant cyber-stakeholders.

3.3 Sponsorship and/or Affiliation

National Authority Against Electronic Attacks- National CERT is a division in Cyberspace Directorate of the National Intelligence Agency.

National Authority Against Electronic Attacks- National CERT co-operates with other competent relevant authorities in the following situations:

- on national security issues – to the Government.
- on security issues related to the Government's infrastructure or critical infrastructure – to the Government.
- on personal data protection issues – to **the National Data Protection Authority**
- on suspected criminal activity - to Greek Cyber Crime Unit of the Hellenic Police (law enforcement).

3.4 Authority

The National Authority Against Electronic Attacks- National CERT is the agency responsible for encountering-protecting mainly the Public Sector along with the Critical National Infrastructures as established by Bill 3469/2008 and Presidential Decree 126/2009.

4.Policies

4.1 Types of Incidents and Level of Support

Collects evidence from electronic attacks-threats from public and private organizations and critical infrastructure.

Analyses, records and categorizes the type of attacks-threats and treats them according to their type.

Provides information and advice for the protection of PC systems of the Public and Private Sector from attacks-threats, upon request from the concerning entity.

4.2 Co-operation, Interaction and Disclosure of Information

Co-operates with other National or not CERTs as well as Services of the Public Sector and national or international cybersecurity stakeholders about relevant issues.

Coordinates the necessary actions among the cybersecurity stakeholders involved in the attack.

All necessary appropriate security measures are in place to ensure that private and company data are protected. Any release of information is performed on a need-to-know basis when authorized by the owner of the information.

4.3 Communication and Authentication

See § 2.11.

5. Services

5.1 Incident Response

The National Authority Against Electronic Attacks- National CERT assists system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage

Investigating whether indeed an incident occurred and determines the extent of it.

5.1.2 Incident Coordination

The incident coordination includes:

- The determination of the initial cause of the incident.
- The facilitation of communication among the involved players and the involvement of law enforcement, if necessary.
- The incident reporting to other CERTs/CSIRTs.
- The release of announcements to users and relevant stakeholders.

5.1.3 Incident Resolution

The incident resolution includes:

- The collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise.
- The monitoring of the incident in order to determine that it was really resolved.
- The keeping of corresponding incident records.
- The responsibility to operate the systems in a secure manner and resolve incidents remains at all times on the owners of the said systems.

5.2 Activities

Proactive services:

- Issues announcements about imminent threats or electronic attacks, and proposes preventive security measures.
- Adoption of security tools
- Producing security documentation.
- Security awareness rising.
- Vulnerability assessment.

Reactive services:

- Alerts, warnings, sharing of information
- Incident handling, analysis, coordination, on site support.
- Malware analysis.
- Issues announcements about imminent threats or electronic attacks, and proposes reactive security measures.

6. Incident Reporting Forms

Incident Reporting is made by email to the official email.

7. Disclaimers

All precautions have been taken in the preparation of all the information presented by National Authority Against Electronic Attacks- National CERT in any manner (e.g. Internet portal, mailing lists). Nevertheless, the above mentioned information is offered "AS IS" with no guarantee of any kind spoken or not. In no occasion National Authority Against Electronic Attacks- National CERT is responsible for any claim, compensation, errors, omissions, damage or any other possible responsibility from or relevant to the information.