www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 16 May 2013 T-CY (2013)12

## Cybercrime Convention Committee (T-CY)

# T-CY Guidance Note #7

## New forms of Malware

Proposal prepared by the Bureau
For comments by T-CY members and observers
And for consideration by the 9th Plenary of the T-CY (June 2013)

Comments on this draft Guidance Note should be sent to:


Alexander Seger
Secretary Cybercrime Convention Committee
Head of Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

# 1 Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[1]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of new forms of malware.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[2] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to new forms of malware.

## 2 Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

There are many current forms of malware, which has been defined by the Organization for Economic Cooperation and Development as "a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners."[3] Commonly-known forms include worms, viruses, and trojans. Current forms of malware can steal data by copying it and sending it to another address; they can manipulate data; they can hinder the operation of computer systems, including those that control critical infrastructures; ransomware can delete, suppress or block access to data; and specially-tailored malware can target specified computer systems.

According to private and governmental sources, vast numbers of new forms of malware are developed and discovered every year. These new forms vary in their objectives. Like older forms, new forms of malware may steal money, or shut down water systems, or threaten users, and so on.

The numbers and variety of forms of malware are so vast that it would not be possible to describe even currently-known forms in a criminal statute. The Cybercrime Convention deliberately avoids terms such as worms, viruses, and trojans. Because fashions in malware change, using such terms in a convention would quickly make it obsolete and be counterproductive.

It is also not possible, of course, to describe future forms in a statute.

For these reasons, it is important to focus on the objectives and effects of the malware. These are already known and can be described in a statute.

Thus both current and future forms of malware are covered by the following sections of the convention, depending on what the malware actually does. Each provision contains an intent standard

---

[1] See the mandate of the T-CY (Article 46 Budapest Convention).

[2] Paragraph 36 of the Explanatory Report

[3] http://www.oecd.org/internet/ieconomy/40724457.pdf

("without right," "with intent to defraud," etc) which should be taken into consideration when officials decide how to charge a crime.

## 3 T-CY interpretation of the criminalisation of new forms of malware

| **Relevant Articles** | **Examples** |
|---|---|
| Article 2 – Illegal access | Malware can be used to access computer systems. |
| Article 3 – Illegal interception | Malware can be used to intercept non-public transmissions of computer data to, from, or within a computer system. |
| Article 4 – Data interference | Malware damages, deletes, deteriorates, alters or suppresses computer data. |
| Article 5 – System interference | Malware may hinder the functioning of a computer system. |
| Article 6 – Misuse of devices. | Malware is a device as defined in Article 6 (parties that take reservations to Article 6 must still criminalize the sale, distribution or making available of covered devices). This is because it will normally be designed or adapted primarily to commit the offences established by Articles 2 through 5. In addition, the article criminalizes the sale, procurement for use, import, distribution or other making available of computer passwords, access codes, or similar data by which computer systems may be accessed. These elements are frequently present in malware prosecutions. |
| Article 7 – Computer-related forgery. | Malware may input, alter, delete, or suppress computer data with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic. |
| Article 8 – Computer-related fraud. | Malware may cause one person to lose property and cause another person to obtain an economic benefit by inputting, altering, deleting, or suppressing computer data and/or interfering with the function of a computer system. |
| Article 11 – Attempt, aiding and abetting | Malware may be used to attempt or to aid or abet several crimes specified in the treaty. |
| Article 13 – Sanctions | The effects of new forms of malware vary widely. Some malware is relatively trivial; other malware is dangerous to people, to critical infrastructures, or in other ways. The effects may differ in different countries for technical, cultural or other reasons.<br><br>A Party may foresee in its domestic law a sanction that is unsuitably lenient for malware attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13, that criminal offences related to such attacks "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions. |

| | |
|---|---|
| | Parties may also consider aggravating circumstances, for example, if malware attacks affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure. [4] |

## 4 T-CY statement

The above list of Articles related to all forms of malware illustrates the multi-functional criminal use of such attacks.

Therefore, the T-CY agrees that the different aspects of all forms of malware are covered by the Budapest Convention.

_____

[4] See also Article 10 of the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (com (2010) 517 final).

# 5 Appendix: Extracts of the Budapest Convention

**Article 2 – Illegal access**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

**Article 3 – Illegal interception**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

**Article 4 – Data interference**

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

**Article 5 – System interference**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

**Article 6 – Misuse of devices**

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

**Article 7 – Computer-related forgery**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

**Article 8 – Computer-related fraud**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;
b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

**Article 11 – Attempt and aiding or abetting**

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

**Article 13 – Sanctions and measures**

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.