www.coe.int/cybercrime

Strasbourg, 30 November 2022 T-CY(2022)14

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #12
Aspects of ransomware
covered by the Budapest Convention

Adopted by the 27th Plenary of the T-CY (Strasbourg, 29-30 November 2022)

Content

Contact

Alexander Seger
Executive Secretary Cybercrime Convention Committee
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 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.

Offenders, for decades, have committed different forms of cybercrime in order to extort ransoms from organisations and individuals. For example, the theft and subsequent threat of public disclosure of personal data or other sensitive information to coerce payment of ransom is still prevalent. However, over the past decade more complex forms of ransomware and related offences have emerged.[2] These entail the encryption of computer data or systems, thus locking out users, followed by requests for ransom against the (promise of) access to be restored. Offenders may also threaten to release sensitive or personal information, in an attempt to more effectively extract payments from victims.

Such ransomware offences are possible because of technology permitting:

- strong encryption of victims' computer data or systems;
- use of communication systems that are difficult to trace in order to send requests for ransom payments as well as decryption tools;
- payment of ransom in a manner that is difficult to trace such as through virtual currencies that are easier to obfuscate than traditional fiat currencies.

The "WannaCry" and "NotPetya" attacks of 2016/2017 affected computers and attracted major attention worldwide. The COVID-19 pandemic from 2020 onwards led to a greater reliance of societies on information and communication technology, increasing opportunities for exploitation for criminal purposes. This contributed to a further surge in ransomware offences.[3] Attacks against computer systems of hospitals have reportedly led to the death of patients.[4] Further, ransomware offences against critical infrastructure caused a national emergency to be declared in Costa Rica in April 2022. The use of ransomware is now considered a serious form of cybercrime that is affecting essential interests of individuals, businesses, societies and governments.

The T-CY, therefore, at its 26th plenary (10-11 May 2022), decided to prepare a Guidance Note to show how aspects of ransomware offences are criminalised under the substantive criminal law provisions of the Convention on Cybercrime and how the procedural powers and provisions on

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

[2] [See CBT Locker (Curve-TOR-Bitcoin) since 2014.]

NOTE: footnotes in [brackets] will be deleted in the final version.

[3] [According to numerous reports. See for example:
https://www.crowdstrike.com/resources/infographics/ransomware-during-covid-19/
https://home.kpmg/si/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html
https://www.globenewswire.com/en/news-release/2021/12/23/2357418/0/en/Mimecast-The-Rise-of-Ransomware-During-the-COVID-19-Pandemic.html]

[4] [https://www.pandasecurity.com/en/mediacenter/security/first-ransomware-death/
https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/
https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients
https://www.wired.co.uk/article/ransomware-hospital-death-germany]

international co-operation of this treaty may be used to investigate, prosecute and co-operate against ransomware offences.

The present Guidance Notes also makes reference to the Second Additional Protocol to the Convention on Cybercrime (CETS 224) that will provide additional tools for "enhanced co-operation and disclosure of electronic evidence" to Parties to this Protocol once it is in force.

Previous T-CY Guidance Notes on malware, botnets, identify theft and critical infrastructure attacks remain relevant with regard to ransomware offences as well.

2 Ransomware offences

Ransomware is a type of malware that is designed to deny a user access to their computer data or computer system by encrypting such data or systems. The user targeted is then requested to pay a ransom for (the promise of) access to the data or system to be restored.

Ransomware offences typically involve:

1. Preparatory acts, including:

   - the production, sale, procurement or otherwise making available of ransomware, that is, of a "device" in the meaning of Article 6 of the Convention on Cybercrime;
   - the production, sale, procurement or otherwise making available of other devices in the meaning of Article 6 that are used in the preparation of ransomware offences, such as malware to gain unauthorized access to victim systems, or botnets to distribute ransomware;
   - obtaining mailing lists or other relevant information on targets. Some of such preparatory acts may themselves be offences or may be considered aiding or abetting ransomware offences, such as exfiltration of databases using keyloggers, use of botnets, or identity theft.[5]

2. The distribution or installation of ransomware, including:

   - through emails with attachments containing the malware or targeting users of messaging applications with links embedded in messages. Enticing users to access such attachments or links – and thus to install the malware – may be further facilitated through social engineering or other techniques of identity theft;
   - through remote access to a computer system.

3. Encryption of the computer system, or parts of it, or data through the ransomware and thus preventing the user from accessing or otherwise making use of the data or system.

4. Requesting, obtaining and transferring the ransom payment, including:

   - requesting the ransom in exchange for (the promise of) restoring access to the data and/or system which amounts to extortion or blackmail but possibly also other offences;

[5] See relevant Guidance Notes (coe.int)

- communication between the offender and the target through means of communication that are difficult to trace, including use of TOR. Decryption tools may also be communicated in this manner;
- obtaining the ransom in a manner that makes it difficult to trace, typically in the form of cryptocurrency, often followed by the laundering of the proceeds to further hide the identity of the perpetrator and the proceeds.

Since 2021, the market for ransomware is increasingly organised and professional, offering a business model often referred to as ransomware-as-a-service (or RaaS) to commit ransomware offences. This business model has led to cyber criminals involving independent services to negotiate payments, assist victims with making payments, and some services offering a 24/7 help centre to expedite ransom payments and to assist in the restoration of encrypted systems or data.

3 Relevant provisions of the Convention on Cybercrime (ETS 185)

3.1 Criminalisation of offences related to ransomware

Under the Convention on Cybercrime, each Party shall adopt legislative and other measures as may be necessary to establish certain criminal offences under its domestic law, when committed intentionally and without right. The following articles and corresponding offences under the domestic laws of Parties implementing the Convention would be relevant for investigations and criminal proceedings regarding ransomware offenses.

Relevant Articles	**Examples**
Article 2 – Illegal access	Ransomware offences involve illegal access to a computer system of a victim and thus a criminal offence according to Article 2.
Article 3 – Illegal interception	Ransomware variants may include the capability to intercept non-public transmissions of computer data to, from or within a computer system. The procurement of information on targets or of access credentials may also involve the offence of illegal interception.
Article 4 – Data interference	Ransomware is specifically designed for the purpose of interfering with computer data and its use is thus a criminal offence according to Article 4.
Article 5 – System interference	Ransomware may be designed for the purpose of interfering with the functioning of a computer system and its use is thus a criminal offence according to Article 5.
Article 6 – Misuse of devices	Ransomware is malware and thus a device "designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5". Thus, the "production, sale, procurement for use, import, distribution or otherwise making available" of ransomware is a criminal offence according to Article 6.
Article 7 – Computer-related forgery	In order to gain illegal access to victims' systems, ransomware actors often use phishing and other social engineering techniques – which in certain cases may constitute computer-related forgery – that is creating inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic.

Article 8 – Computer-related fraud	Ransomware offences cause the loss of property by interfering with computer data and/or the functioning of a computer system with fraudulent or other dishonest intent of procuring, without right, an economic benefit.
Article 11 – Attempt, aiding and abetting	Offences provided for in the treaty may be attempted, aided or abetted in furtherance of ransomware-related offences. Different persons may be involved, for example, in the production, procurement or otherwise making available of ransomware, or in the procurement of information on targets.
Article 12 – Corporate liability	Ransomware offences covered by Articles 2-11 of the Convention as described above may be carried out by legal persons that would be liable according to Article 12.
Article 13 – Sanctions	Offences related to ransomware that are crimes covered by the Convention may pose a significant threat to individuals and to society, especially when the crimes are directed against critical information infrastructure and cause significant risk to the life or safety of any natural person. Parties should therefore ensure, pursuant to Article 13, that criminal offences related to such acts "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty". This includes ensuring that, under its domestic law, the available sanctions are appropriate given the threat posed by ransomware and take into consideration the full range of criminal liability, including on the basis of attempting, aiding, and abetting criminal activity. Parties may also consider more severe penalties when aggravating circumstances are present, for example, if such acts affect the functioning of critical infrastructure significantly or cause death or physical injury of a natural person or significant material damage.

Therefore, ransomware offences may comprise conduct that is to be criminalised according to Articles 2 to 8 as well as under Article 11 (attempt, aiding or abetting), and that may also entail the liability of legal persons under Article 12 of the Convention on Cybercrime.

Ransomware activities may comprise a wide range of other offences under domestic criminal law.

3.2 Procedural provisions

Under the Convention on Cybercrime "[e]ach Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to" undertake certain procedural measures to investigate the offences according to articles 2-11 of the Convention and to collect evidence in electronic form (see Article 14 of the Convention). These may also be used for investigations and criminal proceedings related to ransomware offences.

Relevant Articles	**Examples**
Article 14 – Scope of procedural provisions	The procedural powers of the Convention (Articles 16-21) may be used in a specific criminal investigation or proceeding not only in respect to the above offences under the Convention but also in respect to the collection of

	evidence in electronic form of any other offence related to ransomware as defined under the domestic law of a Party.
Article 15 – Conditions and safeguards	These conditions and safeguards also apply to criminal investigations and proceedings related to ransomware offences.
Article 16 – Expedited preservation of stored computer data	This power may be used to expeditiously preserve stored computer related to ransomware offences, including, for example, data on the source or path of ransomware distribution or of communications requesting ransom or providing decryption tools if applicable. This power may also be used to order the preservation of other data related to ransomware offences, such as communications between suspects or data stored by suspects that may be evidence of such offences.
Article 17 – Expedited preservation and partial disclosure of traffic data	This power may be used to expeditiously obtain a sufficient amount of traffic data to identify other service providers and the path through which communications related to ransomware offences were transmitted.
Article 18 – Production order	Production orders according to Article 18 may be used to order a person to produce stored computer data related to ransomware offences. This may include service providers, financial institutions including virtual assets service providers and platforms, and other legal or natural persons. These orders are vital to obtaining, for example, subscriber information from providers related to accounts and infrastructure associated with ransomware.
Article 19 – Search and seizure of stored computer data	Search and seizure provisions according to Article 19 may be used to search and seize stored computer data related to ransomware offences.
Article 20 – Real-time collection of traffic data	Powers according to Article 20 may be used for the real-time collection of traffic data related to ransomware offences
Article 21- Interception of content data	Powers according to Article 21 may be used for the interception of certain content data related to ransomware offences, such as, for example, communications between suspects.

Thus, in criminal investigations or proceedings related to ransomware offences, Parties may use expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools to collect electronic evidence.

3.3 International co-operation provisions

Relevant Articles	Examples
General principles and procedures relating to international co-operation of Articles 23 – 28	The general principles and procedures for international co-operation of Articles 23 to 28 of the Convention – that is on extradition, mutual assistance and others – are also applicable to offences related to ransomware. Article 26 may be particularly useful in that a Party possessing valuable information on ransomware offences obtained through its own investigations may, within the limits of its domestic law, forward such information to the other Party without a prior request (see paragraph 260 of the Explanatory Report to the Convention on Cybercrime). According to Article 23 and Article 25.1, Parties to the Convention are required to cooperate with each other, in accordance with the provisions of Articles 23-28, "to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data" and for "the collection of evidence in electronic form of a criminal offence."
Specific provisions on international co-operation of Articles 29 – 35.	The specific provisions of Chapter III of the Convention are available for international co-operation and collection of evidence related to ransomware offences: – Article 29 – Expedited preservation of stored computer data – Article 30 – Expedited disclosure of preserved traffic data – Article 31 – Mutual assistance regarding accessing of stored computer data – Article 32 – Trans-border access to stored computer data with consent or where publicly available – Article 33 – Mutual assistance in the real-time collection of traffic data – Article 34 – Mutual assistance regarding the interception of content data – Article 35 – 24/7 network

Given that ransomware offences typically involve offenders, targets and victims, service providers, financial institutions or computer systems in multiple jurisdictions, effective use of these international co-operation provisions is particularly important.

4 The Second Additional Protocol to the Convention on Cybercrime (CETS 224)

On 12 May 2022, the Second Additional Protocol to the Convention on Cybercrime (CETS 224) was opened for signature. Once in force, this instrument will provide Parties to it with additional tools for "enhanced co-operation and disclosure of electronic evidence". These will be relevant, and in some instances highly relevant, to criminal investigations and proceedings related to ransomware offences, and include:

– Article 6 – Request for domain name registration information directly to an entity in another Party providing domain name registration services;
– Article 7 – Disclosure of subscriber information through direct co-operation with a service provider in another Party;

- Article 8 – Giving effect to orders from another Party for expedited production of subscriber information and traffic data;
- Article 9 – Expedited disclosure of stored computer data in an emergency;
- Article 10 – Emergency mutual assistance;
- Article 11 – Video conferencing;
- Article 12 – Joint investigation teams and joint investigations.

The scope of application of this Protocol is again broad in that it shall be applied not only to criminal offences related to computer systems and data but also to the collection of evidence in electronic form of any criminal offence (see Article 2.1.a).

The conditions and safeguards of Article 13 ensure that the establishment, implementation, and application of the powers and procedures provided for in the Protocol are subject to conditions and safeguards provided for by each Party's domestic law, which must provide for the adequate protection of human rights and liberties. Additionally, given that many Parties to the Protocol may be required, in order to meet their constitutional or international obligations, to ensure the protection of personal data, Article 14 provides for data protection safeguards to permit Parties to meet such requirements and ensures that personal data can be transferred when making use of these expedited forms of co-operation.

5 T-CY statement

The T-CY agrees that:

- offences related to ransomware attacks may comprise conduct that is to be criminalised according to Articles 2 to 8 as well as under Article 11 (attempt, aiding or abetting), and that may entail the liability of legal persons under Article 12 of the Convention on Cybercrime;

- the procedural measures and international-cooperation tools of the Convention may be used to investigate and prosecute ransomware attacks and related offences, as well as their facilitation, participation in such offenses, or preparatory acts;

- the Second Additional Protocol to the Convention on Cybercrime, once in force, will provide its Parties further tools for enhanced co-operation and disclosure of electronic evidence related to ransomware attacks.