Stanford – Vienna
Transatlantic Technology Law Forum
A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 82

Ransomware: Notes on the US Computer Fraud and Abuse Act and the CoE International Convention on Cybercrime

Catalina Goanta & Apostolis Zarras

2021

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Authors

Dr. Catalina Goanta is Assistant Professor in Private Law at the Faculty of Law of Maastricht University, Netherlands, a postdoctoral researcher at Studio Europa (Maastricht Working on Europe), and manages the Maastricht Law and Tech Lab, a unique research group with eight computer scientists in residence at the law school, where she currently supervises one internal and two external PhD students. From February 2018 to February 2019, she was a Niels Stensen Fellow and visited the University of St. Gallen (The Institute of Work and Employment), Switzerland, and Harvard University (The Berkman Center for Internet and Society). She is also a non-residential Fellow of the Stanford-Vienna Transatlantic Technology Law Forum. Her research focuses on content/web monetization, platform governance, and digital consumer protection.

Dr. Apostolis Zarras is Assistant Professor at Delft University of Technology, Netherlands. Previously, he was an assistant professor at Maastricht University, Netherlands, and, before that, a postdoctoral researcher at the Technical University of Munich, Germany. He received his PhD degree in IT Security from the Ruhr-University Bochum, Germany. His research interests include systems, network, and web security. His work focuses on developing new security paradigms, architectures, and software, for secure and trustworthy ICT and IoT systems, as well as investigating malicious activities such as the ones that take place in the dark web and its underground markets. He has been acknowledged with the best paper awards from ACSAC 2018 and CODASPY 2016.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Catalina Goanta & Apostolis Zarras, Ransomware: Notes on the US Computer Fraud and Abuse Act and the CoE International Convention on Cybercrime, Stanford-Vienna TTLF Working Paper No. 82, http://ttlf.stanford.edu.

Copyright

Abstract

It is 2021, and cyberattacks are relentless. Attacks can take many forms, such as ransomware, which according to some estimations, accounted for approximately 4000 attacks per day, with 98% of the attacks relying on social engineering. Only in the US, ransomware attacks in 2020 costed an estimated $915 million. This working paper aims to look into the applicable legislative regimes to ransomware from the perspective of the US Computer Fraud and Abuse Act (CFAA) and the Convention on Cybercrime of the Council of Europe (Budapest Convention). In doing so, in Section 2 the paper first describes ransomware, both from a technical perspective as well from the perspective of the novel business model of Ransomware-as-a-service (RaaS). Section 3 is dedicated to applying the CFAA to ransomware, whereas Section 4 does the same for the Budapest Convention. Section 5 brings together some concluding reflections regarding the two legal regimes.

Table of Contents

1. Introduction

It is 2021, and cyberattacks are relentless. At the same time, the scale of unpreparedness in dealing with information security threats is worrying. In a 2019 study on 244 public sector institutions from United States, United Kingdom, Germany, Australia, Mexico, and Japan, it was determined that up to 88% of these institutions had suffered a damaging attack over the past two years.[1] The first US nation-wide survey regarding local government and cybersecurity paints a similarly grim picture, where, on the one hand, 27.7% of the institutions surveyed reported they were able to detect cyberattacks occurring hourly, and on the other hand, almost 30% of the respondents were not able to report whether they were being attacked.[2] Attacks can take many forms, such as ransomware, which according to some estimations, accounted for approximately 4000 attacks per day, with 98% of the attacks relying on social engineering.[3]

Universities, local government, and state agencies are ideal victims because of infrastructure, funding, and general information security literacy issues.[4] In Europe and the US, ransomware attacks against universities have increased in the past years, as

[1] Tenable, ‘Cybersecurity in Public Sector: 5 Insights You Need to Know’, retrieved from <https://static.tenable.com/marketing/whitepapers/Whitepaper-Cybersecurity_in_Public_Sector.pdf>.

[2] Donald F. Norris, Laura Mateczun, Anupam Joshi and Tim Finin, ‘Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity’ (2019) 79(6) Public Administration Review 895.

[3] European Banking Federation, retrieved from <https://www.ebf.eu/themes/cybersecurity/>.

[4] See for instance Leah Zhang-Kennedy, Hala Assal, Jessica Rocheleau, Reham Mohamed, Khadija Baig and Sonia Chiasson, ‘The aftermath of a crypto-ransomware attack at a large academic institution’, Proceedings of the 27th USENIX Security Symposium, 2018.

universities such as the London School of Economics, Antwerp University, and Maastricht University have suffered setbacks in their activities because of ransomware.

While considerable research exists at the European level in the field of cybersecurity policy-making (e.g., NIS Directive, the EU Cybersecurity Act), gaps remain in the implications of the harms that arise when security incidents take place, ranging from the reporting of data breaches to response coordination or the liability of public institutions for breaching fiduciary duties. These remaining gaps are problematic for two main reasons. First, as regulatory frameworks (public or private) are not developed coherently, insular pockets of expertise arise on similar themes within different fields of law (e.g., data protection, criminology, national security, product liability). Second, given the complex nature of eventual normative research solutions for existing and emerging problems, sustainable interdisciplinarity is severely lacking (e.g., computer science scholarship on the matter could use more law and social science insights, and vice versa).

The recent global health crisis has only worsened these vulnerabilities. The Covid-19 pandemic has forced the world into more online interactions than ever before, and subsequently, cybercrime has been booming. Compared to 2019 standards, malware use increased by 358% and ransomware increased by 435%, while Google has seen a 27% increase in phishing websites between January 2020 and January 2021.[5] The Federal Trade Commission even launched an Identity Theft Awareness

[5] Patricia Stainer, 'Alarming Cybersecurity Statistics for 2021 and the Future' (*Retarus*, 29 April 2021), retrieved from <https://www.retarus.com/blog/en/alarming-cybersecurity-statistics-for-2021-and-the-future/>; Chuck Brooks, 'Alarming Cybersecurity Stats: What You Need To Know For 2021' (Forbes, 2 March 2021), retrieved from <https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=40f81e0c58d3>.

Week seeing how it got about 1.4 million reports of identity theft, double the number from 2019.[6]

As global efforts of teleworking are implemented by private as well as public actors alike, institutions become even more vulnerable to cybercrime.[7] As a result, cybercrime is reported to have increased during the beginning of 2020, as stated by the president of the European Commission, Ursula von der Leyen, in a video on this matter on 24 March.[8] In a study Europol published on 4 April, it came to the conclusion that "the impact of the COVID-19 pandemic on cybercrime has been the most visible and striking compared to other criminal activities", as "phishing and ransomware campaigns are being launched to exploit the [...] crisis and are expected to continue to increase in scope and scale".[9] In general, more people online means more opportunities for cybercrime, the fruition of which, especially in core infrastructures such as banks, hospitals, or municipalities, can have debilitating socio-economic effects. While it is unclear what the long-term effects of the public health crisis will be from the perspective of online security, there is universal agreement among security researchers that cybersecurity risks are not taken sufficiently seriously. This is mainly because cybersecurity literacy is not sufficiently disseminated at the institutional level.

[6] Seena Gressin, 'Identity Theft Awareness Week starts today' (*FTC*, 1 February 2021), retrieved from <https://www.consumer.ftc.gov/blog/2021/02/identity-theft-awareness-week-starts-today>.

[7] Steve Stransky, 'Cyber Attackers Are Exploiting Coronavirus Fears' (*Lawfareblog*, 12 March 2021), retrieved from <https://www.lawfareblog.com/cyber-attackers-are-exploiting-coronavirus-fears>.

[8] Elena Sánchez Nicolás, 'Cybercrime rises during coronavirus pandemic' (*EU Observer*, 25 March 2020), retrieved from <https://euobserver.com/coronavirus/147869>.

[9] Europol, 'Catching The Virus', retrieved from <https://www.europol.europa.eu/newsroom/news/catching-virus>.

In particular, ransomware attacks have spiked in the past years.[10] Only in the US, ransomware attacks in 2020 costed an estimated $915 million.[11] Public institutions seem to be under increased risks, as apart from healthcare, municipalities and universities have also fallen victims to this type of attack in more recent times. In December 2019, New Orleans declared a state of emergency after a ransomware attack that ended up costing the local government $7million.[12] Private companies have not been safe either. In July 2021, around 500 Coop supermarkets were forced to close after the paying systems and self-service checkouts failed to work as a result of the company making the underlying software (Kaseya) had been the victim of a supply chain ransomware attack that also affected the company's customers.[13]

Some of the ransomware attacks of the past years have been conducted with political intentions of destabilizing sovereign interests.[14] However, many of these

[10] Kellen Dwyer, 'It's Time to Surge Resources Into Prosecuting Ransomware Gangs' (*Lawfareblog*, 20 May 2021), retrieved from <https://www.lawfareblog.com/its-time-surge-resources-prosecuting-ransomware-gangs>.

[11] Andra Zaharia, '300+ Terrifying Cybercrime and Cybersecurity Statistics (2021 Edition)' (*Comparitech*, 29 June 2021), retrieved from <https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/>.

[12] Kirsten Korosec, 'New Orleans declares state of emergency following ransomware attack' (*TechCrunch*, 14 December 2019), retrieved from <https://techcrunch.com/2019/12/14/new-orleans-declares-state-of-emergency-following-ransomware-attack/>.

[13] Joe Tidy, 'Swedish Coop supermarkets shut due to US ransomware cyber-attack' (*BBC*, 3 July 2021), retrieved from <https://www.bbc.com/news/technology-57707530>; Charlie Osborne, 'Updated Kaseya ransomware attack FAQ: What we know now' (*ZDNet*, 23 July 2021), retrieved from <https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/>.

[14] Arindrajit Basu and Elonnai Hickok, 'Conceptualizing an International Framework for Active Private Cyber Defence' (2020) 16 Indian J L & Tech. See also the Solar Winds incident, although not ransomware, Steven J. Vaughan-Nichols, 'SolarWinds: The more we learn, the worse it looks' (*ZDNet*, 4 January 2021), retrieved from <https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/>; Jeff Kosseff, 'Hacking Cybersecurity Law' (2020) 2020 U Ill L Rev 811, 835.

attacks are made in the course of ransomware-as-a-service (RaaS),[15] which reflects the monetization interests in commoditized cybercrime on the dark web.[16]

From a legal perspective, cybersecurity has been called one of the most vexing challenges for US policymakers,[17] as cybercrime operates "in the shadows with significant impunity".[18] It leads to a complex web of applicable rules,[19] and this very issue, as Grimmelmann observes, should give us pause.[20] This working paper aims to look into the applicable legislative regimes to ransomware from the perspective of the US Computer Fraud and Abuse Act (CFAA) and the Convention on Cybercrime of the Council of Europe (Budapest Convention).[21] In doing so, in Section 2, the paper first describes ransomware, both from a technical perspective as well from the perspective of the business models it gives rise to. Section 3 is dedicated to applying the CFAA to

[15] Malcolm Harkins and Anthony M Freed, 'The Ransomware Assault on the Healthcare Sector' (2018) 6 JL & Cyber Warfare 148, 149; Mircea-Constantin Scheau and Adrian-Liviu Arsene and Gabriel Popescu, 'Artificial Intelligence/Machine Learning Challenges and Evolution' (2018) 7 Int'l J Info Sec & Cybercrime 11, 15; Sharon D Nelson and John W Simek, 'Ransomware: How Many Bitcoins Are in Your Wallet' (2018) 44 Law Prac 40; Rob Wainwright, 'Fighting Crime and Terrorism in the Age of Technology' (2018) 24 Brown J World Aff 191, 194.

[16] James A Sherer and Melinda L McLellan and Emily R Fedeles and Nichole L Sterling, 'Ransonware - Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web' (2017) 23 Rich JL & Tech 1, 18.

[17] Jeff Kosseff, 'Hacking Cybersecurity Law' (2020) 2020 U Ill L Rev 811, 812.

[18] Maggie Brunner, 'Challenges and Opportunities in State and Local Cybercrime Enforcement' (2020) 10 J Nat'l Sec L & Pol'y 563.

[19] Matthew Larson and Ethan Cantor and Gabrielle Caron and Alessandra Lopez and Duncan Weals, 'Computer Crimes' (2021) 58 Am Crim L Rev 611; Michael J O'Connor, 'The Common Law of Cyber-Trespass' (2020) 85 Brook L Rev 421;

[20] James Grimmelmann, 'Spyware vs. Spyware: Software Conflicts and User Autonomy' (2020) 16 Ohio St Tech L J 25.

[21] Peter G. Berris, *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*; Andrew Burt and Dan Geer, 'The Budapest Convention Offers an Opportunity for Modernizing Crimes in Cyberspace' (*Lawfareblog*, 21 June 2019), retrieved from <https://www.lawfareblog.com/budapest-convention-offers-opportunity-modernizing-crimes-cyberspace>.

ransomware, whereas Section 4 does the same for the Budapest Convention. Section 5 brings together some concluding reflections regarding the two legal regimes.

2. Ransomware: How It Works and How It's Used

2.1 How Ransomware Works: Translating Computer Security Literature

As many concepts which emerge around human behavior, ransomware is not new, and the earlies ransomware attacks are reported to have taken place at the end of the 1980s.[22] Legal scholarship has long been covering ransomware, often also trying to provide definitions or explanations about its technical characteristics. It is generally defined as "malware",[23] "malicious software",[24] or "virus",[25] which "locks users out of their systems, encrypts their files with algorithms that are nearly impossible to break, and then demands a payment to unlock their files",[26] a kind of "virtual blackmail".[27]

[22] Amin Kharaz, Sajjad Arshad, Collin Mulliner, William Robertson, and Engin Kirda, 'UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware', Proceedings of the 25th USENIX Security Symposium, 2016, p. 757.

[23] Alice M Porch, 'Spoiling for a Fight: Hacking Back with the Active Cyber Defense Certainty Act' (2020) 65 SD L Rev 467, 468; Connor McLarren, 'Once More Unto the Breach: How the Growing Threat of Ransomware Affects HIPAA Compliance for Covered Entities' (2018) 15 Ind Health L Rev 305, 306.

[24] Sharon D Nelson and John W Simek, 'Ransomware: How Many Bitcoins Are in Your Wallet' (2018) 44 Law Prac 40, 41; James A Sherer and Melinda L McLellan and Emily R Fedeles and Nichole L Sterling, 'Ransonware - Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web' (2017) 23 Rich JL & Tech 1.

[25] Jordan Butler, 'Finding an Unlikely Combatant in the War against Ransomware: Opportunites for Providers to Utilize off-Site Data Backup within the HIPAA Omnibus and HITECH Amendments' (2018) 11 St Louis U J Health L & Pol'y 317, 320.

[26] Alice M Porch, 'Spoiling for a Fight: Hacking Back with the Active Cyber Defense Certainty Act' (2020) 65 SD L Rev 467, 468.

[27] Igor Vuletic, 'Data-Driven Healthcare and Cybercrime: A Threat We Are Not Aware Of' (2018) 11 Asia Pacific J Health L & Ethics 16.

To complement such assessments and provide a more granular understanding of ransomware, this paper draws insights from computer science research that recognizes two broad categories of ransomware:[28]

- *locker ransomware*, which locks users out of the host machine; and
- *crypto ransomware*, which denies users access to files on the host machine.

As "malicious programs that encrypt user data with the goal of extorting money from the victim in exchange for file decryption",[29] ransomware is a type of malware that entails blocking user access to either the host machine or data on the host machine.[30]

In this section, two characteristics are explored: the malicious nature of ransomware, and its reliance on cryptography.

Generally speaking, malware is an umbrella term referring to malicious software, namely computer programs which "have been with malicious intent".[31] According to the US Institute for Standards and Technology, malware is "a software or

[28] K. Savage, P. Coogan, and H. Lau, 'The evolution of ransomware', Symantec, Mountain View, 2015; Kaspersky, 'Ransomware – definition, prevention and removal', retrieved from <https://www.kaspersky.com/resource-center/threats/ransomware>; Pranshu Bajpai, Aditya K. Sood and Richard Enbody, "A key-management-based taxonomy for ransomware," 2018 APWG Symposium on Electronic Crime Research (eCrime), 2018, p. 2.

[29] Pranshu Bajpai, Aditya K. Sood and Richard Enbody, "A key-management-based taxonomy for ransomware," 2018 APWG Symposium on Electronic Crime Research (eCrime), 2018, p. 1.

[30] M. Satheesh Kumar, J. Ben-Othman and K. G. Srinivasagan, 'An Investigation on Wannacry Ransomware and its Detection', 2018 IEEE Symposium on Computers and Communications (ISCC), 2018, pp. 1-6; Daniel Gonzalez and Thaier Hayajneh, 'Detection and prevention of crypto-ransomware', 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017, pp. 472-478; Camelia Simoiu, Joseph Bonneau, Christopher Gates and Sharad Goel, '"I was told to buy a software or lose my computer. I ignored it": A study of ransomware', Proceedings of the Fifteenth Symposium on Usable Privacy and Security, 2019, p. 157.

[31] Eddy Willems, *Cyberdanger - Understanding and Guarding Against Cybercrime* (Springer 2019) p. 1.

firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system".[32] This term normally covers computer programs such as viruses, worms, and Trojans.[33] Each of those terms is also defined below:

- *viruses* are programs that, when executed, replicate themselves by attaching to the executable code of other programs with the goal of modifying them by inserting their own code.[34]
- *worms* are programs that replicate themselves without relying on any other programs on the host machine.[35] Worms, in contrast to viruses, do not require activation to execute or spread their code.
- *Trojans* are programs that hide their true functions, usually disguised as legitimate software. Upon activation, Trojans can enable cybercriminals to spy on a machine and its user, steal sensitive data, and gain backdoor access to a system. Unlike viruses and worms, they do not inject themselves into other programs or propagate themselves.

Ransomware attacks are often based on social engineering, involving sending phishing emails with attached malware, a trend that has only increased with the digitalization associated with the Covid-19 pandemic.[36] However, ransomware does

[32] NIST, 'Computer Security Resource Center', retrieved from <https://csrc.nist.gov/glossary/term/malware>.

[33] For a brief history of computer viruses, worms and Trojans, see Adam Young and Moti Yung, *Malicious Cryptography* (Wiley 2004), p. 297-298.

[34] William Stallings, *Computer security: principles and practice* (Pearson 2012), p. 182.

[35] See for instance, Changwang Zhang, Shi Zhou and Benjamin Chain, 'Hybrid epidemics--a case study on computer worm conficker' (2015) 10(5) PloS one; Marion Jean-Yves, 'From Turing machines to computer viruses' (2012) Phil. Trans. R. Soc. A. 3703319–3339.

[36] Ronny Richardson, Max M. North and David Garofalo, 'Ransomware: The Landscape Is Shifting' (2021) 17(1) International Management Review 5.

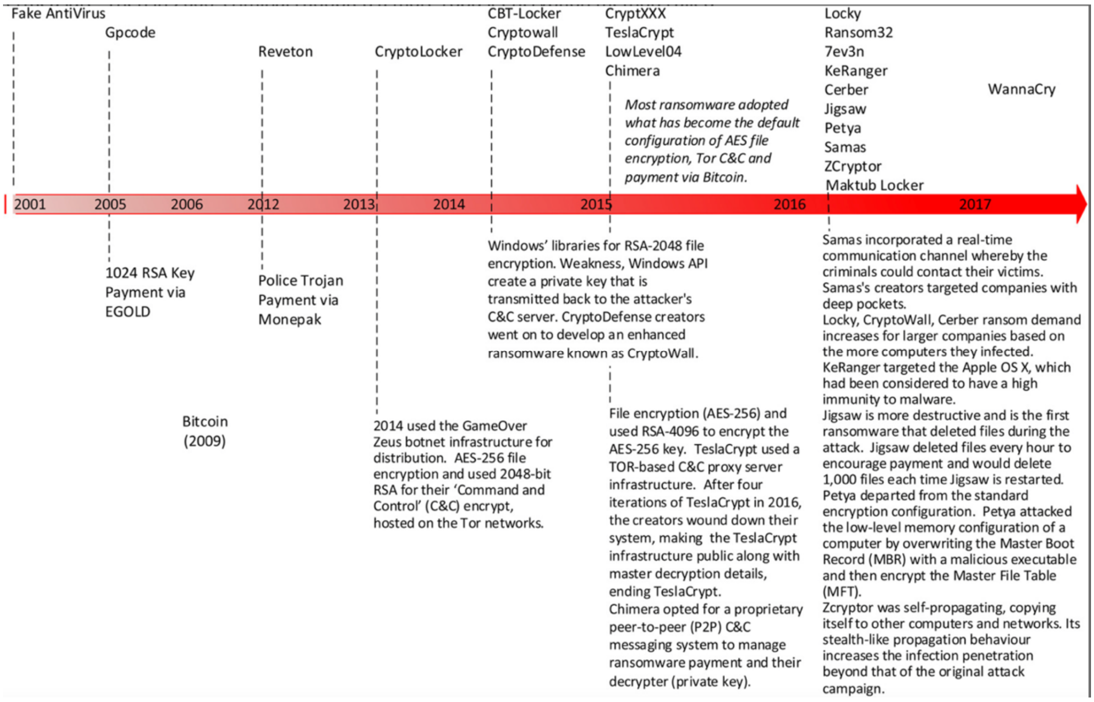
not usually entail executables which act the same way as viruses or worms. Email attachments or downloadable executables from malicious websites can thus be described as Trojans as they will generally have other functions than the ones portrayed to their users. However, the main goal of ransomware (particularly crypto ransomware) is to generate encryption keys that will be used to encrypt a host machine and lock its users out. As Fayi puts it, "the idea of ransomware attacks is, encrypting and locking the files on a computer until the ransom is paid. These attacks usually enter the system by using Trojans, which has malicious programs that run a payload that encrypts and locks the files. The basic goal of this type of attack is getting money, so hackers usually unlock the files when they receive the money, but really there is no guarantee of that".[37]

Moving on to how ransomware relies on cryptography, the basic idea of cryptography has been to convert data into a form that protects its original meaning from eyes for which that data is not meant,[38] and ransomware represents a malicious use of cryptography for criminal interests. By contrast, cryptography applications have been traditionally considered defensive in nature, and in 1996 Young and Yung published the first comprehensive study on what they called "cryptovirology", namely an offensive type of cryptography which could "be used to mount extortion based attacks that cause loss of access to information, loss of confidentiality, and information leakage, tasks which cryptography typically prevents".[39]

[37] Sharifah Yaqoub A. Fayi, 'What Petya/NotPetya Ransomware Is and What Its Remidiations Are' in Shahram Latifi (ed.) *Information Technology – New Generations* (Springer 2018), 15th International Conference on Information Technology, pp 93-100.

[38] For a general overview on the development of cryptography see Catalina Goanta and Marieke Hopman, 'Crypto communities as legal orders' (2020) Internet Policy Review.

[39] Adam Young and Moti Yung, 'Cryptovirology: extortion-based security threats and countermeasures', Proceedings 1996 IEEE Symposium on Security and Privacy, 1996, pp. 129-140.



Most ransomware adopted what has become the default configuration of AES file encryption, Tor C&C and payment via Bitcoin.

Windows' libraries for RSA-2048 file encryption. Weakness, Windows API create a private key that is transmitted back to the attacker's C&C server. CryptoDefense creators went on to develop an enhanced ransomware known as CryptoWall.

2014 used the GameOver Zeus botnet infrastructure for distribution. AES-256 file encryption and used 2048-bit RSA for their 'Command and Control' (C&C) encrypt, hosted on the Tor networks.

File encryption (AES-256) and used RSA-4096 to encrypt the AES-256 key. TeslaCrypt used a TOR-based C&C proxy server infrastructure. After four iterations of TeslaCrypt in 2016, the creators wound down their system, making the TeslaCrypt infrastructure public along with master decryption details, ending TeslaCrypt.

Chimera opted for a proprietary peer-to-peer (P2P) C&C messaging system to manage ransomware payment and their decrypter (private key).

Samas incorporated a real-time communication channel whereby the criminals could contact their victims. Samas's creators targeted companies with deep pockets.

Locky, CryptoWall, Cerber ransom demand increases for larger companies based on the more computers they infected.

KeRanger targeted the Apple OS X, which had been considered to have a high immunity to malware.

Jigsaw is more destructive and is the first ransomware that deleted files during the attack. Jigsaw deleted files every hour to encourage payment and would delete 1,000 files each time Jigsaw is restarted.

Petya departed from the standard encryption configuration. Petya attacked the low-level memory configuration of a computer by overwriting the Master Boot Record (MBR) with a malicious executable and then encrypt the Master File Table (MFT).

Zcryptor was self-propagating, copying itself to other computers and networks. Its stealth-like propagation behaviour increases the infection penetration beyond that of the original attack campaign.

Figure 1. The evolution of ransomware (O'Kane et al 2018)[40]

Generally speaking, the cryptographic algorithms used in ransomware fall into three main categories:[41]

- *Symmetric key algorithms*: the same key is used for encryption and decryption. An example of this algorithm is the Advanced Encryption Standard.[42]

[40] Philip O'Kane, Sakir Sezer and Domhnall Carlin, 'Evolution of Ransomware' (2018) 7(5) IET Networks 321.

[41] Pranshu Bajpai, Aditya K. Sood and Richard Enbody, "A key-management-based taxonomy for ransomware," 2018 APWG Symposium on Electronic Crime Research (eCrime), 2018, pp 2-3. See also Pranshu Bajpai and Richard Enbody, 'Dissecting .NET ransomware: key generation, encryption and operation' (2020) 2 Network Security 8; Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof and Syed Zainudeen Mohd Shaid, 'Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions' (2018) 74 Computers & Security 144.

[42] Pranshu Bajpai, Aditya K. Sood and Richard Enbody, 'A key-management-based taxonomy for ransomware', 2018 APWG Symposium on Electronic Crime Research (eCrime), 2018, pp 2-3.

- *Asymmetric key algorithms*: different keys (one public and one private) are used for encryption and decryption, which makes it slower than symmetric encryption, yet offering a broader application domain. An example of an attack using this type of encryption is CryptoLocker.[43]
- *Hybrid algorithms*: a symmetric cipher is used to encrypt user data faster, and the symmetric key used for this encryption is subsequently encrypted using a public key.

According to Bajpai et al., the hybrid model has been deployed in recent attacks to combine the benefits of both symmetric and asymmetric cryptography, and it consists of the following steps: [44]

1. Ransomware compromises host and commences execution.
2. Cryptographic APIs available on the host are used to generate an encryption key such as an AES-256 key.
3. Ransomware encrypts this symmetric key with a hard-coded asymmetric key (e.g., RSA-2048) and communicates a copy of the now encrypted symmetric key to the attacker.
4. User data is encrypted using the symmetric key.
5. Ransomware securely destroys the symmetric key on the host machine, now making the attacker the sole possessor of the decryption key.
6. A ransom note is displayed to the user while ransomware awaits payment.

As it will be analyzed in Sections 3 and 4, it is important to determine the technical characteristics of ransomware for the purpose of legal qualification,

[43] Wikipedia, retrieved from <https://en.wikipedia.org/wiki/CryptoLocker>.

[44] Pranshu Bajpai, Aditya K. Sood and Richard Enbody, ‘A key-management-based taxonomy for ransomware’ 2018 APWG Symposium on Electronic Crime Research (eCrime), 2018, p. 3.

particularly when it comes to criminal statutory rules.[45] However, until delving into this analysis, we will explore some considerations relating to how ransomware is used, particularly addressing new business models such as RaaS.

2.2 How Ransomware Is Used: Business Models on the Dark Web

As indicated before, the criminal intentions behind ransomware reflect a "longstanding business model for criminal enterprises", namely extorsion.[46] From the perspective of criminal intention, some authors have likened ransomware to kidnapping, as criminals take control of a user's machine and/or files in the hope of receiving financial gain.[47] Regardless of the equivalents used to describe this activity, it is essential to note that RaaS has been said to have changed the way in which criminals take part in ransomware attacks in recent years.[48]

In a recent study, Meland et al. have looked at RaaS value chains on dark markets to identify the severity of the threat posed by this business model.[49] RaaS is a meaningful development in cybercrime as it allows criminals with very low programming literacy to partake in criminal networks that make money out of

[45] Computer science literature has also developed comprehensive research in term of how ransomware can be detected. See for instance, Yuki Takeuchi, Kazuya Sakai and Satoshi Fukumoto, 'Detecting Ransomware using Support Vector Machines' (2018) ACM Proceedings of the 47th International Conference on Parallel Processing Companion (ICPP '18), pp. 1–6; Ahman Almashhadani, Mustafa Kaiiali, Sakir Sezer and Philip O'Kane, 'A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware' (2019) IEEE Access, vol. 7, pp. 47053-47067; Pranshu Bajpai and Richard Enbody, 'An Empirical Study of API Calls in Ransomware' (2020) IEEE International Conference on Electro Information Technology (EIT), pp. 443-448.

[46] Edward A Morse and Ian Ramsey, 'Navigating the Perils of Ransomware' (2016) 72 Bus Law 287.

[47] Edward Cartwright, Julio Hernandez Castro and Anna Cartwright, 'To pay or not: game theoretic models of ransomware' (2019) Journal of Cybersecurity 1.

[48] Per Håkon Meland, Yara Fareed Fahmy Bayoumy and Guttorm Sindre, 'The Ransomware-as-a-Service economy within the darknet' (2020) 92 Computers & Security 101762.

[49] Ibid.

ransomware.[50] Dark web marketplaces allow such criminals to contact ransomware service providers and cheaply obtain tailor-made ransomware that may cater to the characteristics of their prospective victims. This is done, for instance, by selling data products on the dark web, such as the source code that buyers need to compile by themselves or using interfaces that allow buyers to input victim characteristics and tailor their attacks.

In their study, Meland et al. found that RaaS only reflects a small portion of the inventory of the darknet marketplaces investigated therein (Apollon, Berlusconi, Darkbay, Empire, Grey and Samsara), concluding that any reports from security companies published before or at that time (2020) that stated differently were either inaccurate or biased. Moreover, the study maps the value chains in ransomware RaaS as identified below.

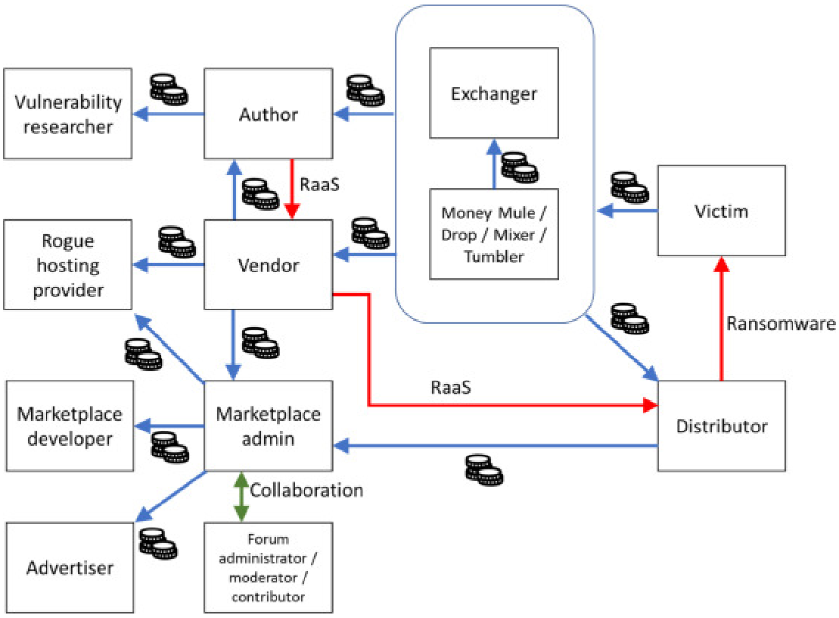


Figure 2. RaaS value chains (Meland et al. 2020)[51]

[50] Philip O'Kane, Sakir Sezer and Domhnall Carlin, 'Evolution of Ransomware' (2018) 7(5) IET Networks 321.

[51] Per Håkon Meland, Yara Fareed Fahmy Bayoumy and Guttorm Sindre, 'The Ransomware-as-a-Service economy within the darknet' (2020) 92 Computers & Security 101762.

Once more, from a legal perspective, it is crucial to factually determine who does what in the ransomware supply chain, as the legal implications of ransomware – ranging from criminal qualifications to other discussions such as the public/private nature of data[52] or seeking damages[53] based on standards of cybernegligence[54] are still up for debate.[55] The following two sections delve into the complexities posed by qualifying ransomware attacks under the CFAA and the Budapest Convention.

3. CFAA and Ransomware

In the United States, the CFAA is a legal regime comprised of both civil and criminal liability for cybercrimes.[56] Beyond its reputation as being the US anti-hacking law, the CFAA has a broader scope of protection, both in the case of cybercrime aimed at government information systems as well as in the case of private harms arising out of cybercrime, as can be observed in Table 1 below.

Offense	**Section**
Obtaining national security information	(a)(1)
Accessing a computer and obtaining information	(a)(2)
Trespassing in a government computer	(a)(3)
Accessing a computer to defraud and obtain value	(a)(4)
Intentionally damaging by knowing	(a)(5)(A)

[52] Thilo Gottschalk, 'The Data-Laundromat? Public-Private-Partnerships and Publicly Available Data in the Area of Law Enforcement' (2020) 6 Eur Data ProtL Rev 21.

[53] Jordan Glassman, 'Too Dangerous to Exist: Holding Compromised Internet Platforms Strictly Liable under the Doctrine of Abnormally Dangerous Activities' (2020) 22 NC JL & Tech 293.

[54] Gabriella C Ferraro, 'Data Breaches Should Not Be a Virtual Certainty: Adopting the NIST Standard for Cybernegligence' (2020) 59 Washburn LJ.

[55] James A Sherer and Melinda L McLellan and Emily R Fedeles and Nichole L Sterling, 'Ransomware - Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web' (2017) 23 Rich JL & Tech 1, 2.

[56] 18U.S.C. §1030.

transmission	
Recklessly damaging by intentional access	(a)(5)(B)
Negligently causing damage and loss by intentional access	(a)(5)(C)
Trafficking in passwords	(a)(6)
Extortion involving computers	(a)(7)

Table 1. Summary of CFAA crimes (Office of Legal Education Executive Office for United States Attorneys)[57]

Enacted in 1984,[58] the CFAA's primary substantive provisions focus on the premise that protected computers, which are accessed without authorization or by exceeding authorized access, should trigger certain liability regimes.[59] Up until 2010, the FCAA had been substantively modified five times,[60] essentially transforming the CFAA into a legal regime that protects trade secrets, personal privacy, or both.[61]

When it comes to ransomware, § 1030(a)(7) has been so far used by prosecutors to address "a variety of threats against computer systems themselves, such as ransomware plots that use software to encrypt the victim's computer files (rendering them unavailable) until payment is received to unlock those systems".[62] Under §

[57] H. Marshall Jarrett, Michael W. Bailie, Ed Hagen and Scott Eltringham, 'Prosecuting Computer Crimes - Computer Crime and Intellectual Property Section Criminal Division', retrieved from <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>.

[58] Sarah Boyer, 'Computer Fraud and Abuse Act: Abusing Federal Jurisdiction' (2009) 6 Rutgers J L & Pub Pol'y 661.

[59] Lee Goldman, 'Interpreting the Computer Fraud and Abuse Act' (2012) 13 Pitt J Tech L & Pol'y 1.

[60] Orin S Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act' (2010) 94 Minn L Rev 1561.

[61] Michael J O'Connor, 'Standing under the Computer Fraud and Abuse Act' (2020) 124 Penn St L Rev 743, 744.

[62] Congressional Research Service, 'Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress', 21 September 2020, retrieved from <https://sgp.fas.org/crs/misc/R46536.pdf>. See also Indictment, United States v. Savandi, No.3:18-cr-00704-BRM, 2018 WL 6798078 (D.N.J. Nov. 27, 2018).

1030(a)(7), it is a crime to "demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion". There is general agreement that this section is applicable to ransomware, given that the latter reflects the extortion of payment in exchange for the provision of cryptographic keys with which the victim's files can be decrypted. Looking at ransomware as a form of computer-enabled extortion has also been further supported by the adopting state-level legislation.[63] However, some states took alternative approaches. Michigan, for instance, made ransomware contraband, thereby prohibiting its possession.[64]

This section is somewhat broader, as the crime of extortion involving computers has also been used to qualify acts involving the hacking of personal computers to obtain sensitive information and subsequently issue threats of releasing the said information unless victims would pay a ransom.[65] In addition, although by 2020, prosecutors have been relying on § 1030(a)(7) to combat ransomware attacks, factual determinations may still raise complications as to the interpretation of the FCAA.

4. The Budapest Convention and Ransomware

Dating from 2001, the Budapest Convention aims to harmonize selected national regulatory standards relating to cybercrime and create cooperation infrastructures for

[63] Maggie Brunner, 'Challenges and Opportunities in State and Local Cybercrime Enforcement' (2020) 10 J Nat'l Sec L & Pol'y 563, 570.

[64] Ibid.

[65] Press Release, U.S. Department of Justice, Member of 'The Dark Overlord' Hacking Group Extradited From United Kingdom to Face Charges in St. Louis (Dec. 18, 2019).

procedural implementations of digital criminal forensic investigations.[66] To date, the Convention has been ratified by 48 countries,[67] out of which 21 non-European, including the United States. The emerging international nature of this legal regime can be considered to be a reflection of the need for global regulatory action on cybercrime, which operates transnationally.[68] Furthermore, the Convention is the only legally binding international treaty aiming to harmonize not only legal standards for cybercrime but also for investigations and criminal justice processes for its ratifying states.[69] The Budapest Convention governs a wide range of cybercrimes envisaged by the Council of Europe back in 2001. Articles 2-8 cover cybercrimes ranging from hacking to interfering with computer systems, as can be seen in Table 2 below. Beyond these specific computer-related cybercrimes, the Convention also includes articles relating to copyright, child pornography, as well as measures for criminal cooperation.

Offense	**Article**
Illegal access	2
Illegal interception	3
Data manipulation	4
Systems interference	5
Misuse of devices	6
Computer-related forgery	7
Computer-related fraud	8

Table 2. Summary of Budapest Convention crimes

[66] Ali Alkaabi, George Mohay, Adrian McCullagh and Nicholas Chantler, 'Dealing with the Problem of Cybercrime' in Ibrahim Baggili (ed.) *Digital Forensics and Cyber Crime* (Springer 2011), pp. 1–18.

[67] Council of Europe, retrieved from <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>.

[68] Jonathan Clough, 'A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation' (2014) 40 Monash U L Rev 698.

[69] Allison Peters and Amy Jordan, 'Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime' (2020) 10 J Nat'l Sec L & Pol'y 487, 499. See also Anna-Maria Osula, 'Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data' (2015) 9 Masaryk U JL & Tech 43, 48.

These provisions reflect the harmonization of criminal qualifications for certain Internet activities, but it leaves sanctions (e.g., jail time) at the discretion of the ratifying countries since criminal law and justice are areas that remain heavily divergent even within the European Union or the Council of Europe member states. The fact that the Convention needs to be further integrated into the criminal statutes of ratifying countries can prove to be a challenge for harmonization. For example, when qualifying cybercrimes, Dutch courts often choose to focus on a broader array of provisions in the Criminal Code than those that reflect the transposition of the Budapest Convention. In a recent judgment dealing with activities relating to phishing and hacking, the Hague court found that the making and selling of phishing panels counted as preparatory works that led to the crime of hacking (Art. 138ab Dutch Criminal Code).[70] Preparatory works usually are part of a more general regime dealing with inchoate offenses, namely criminalizing the steps towards the commission of a different crime.[71] While preparatory works are not as such mentioned in the Convention, hacking is covered by Article 2, which deals with illegal access and which "covers the basic offence of dangerous threats to and attacks against the security (i.e., the confidentiality, integrity, and availability) of computer systems and data."[72]

Regarding ransomware, similarly to the FCAA, the Explanatory Report of the Budapest Convention does not make any specific references to this cybercrime since it pre-dates the proliferation of the ransomware business models, which have led to the

[70] ECLI:NL:RBDHA:2021:6678, retrieved from <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2021:6678>.

[71] Caroline M. Pelser, 'Preparations to commit a crime - The Dutch approach to inchoate offences' (2008) 4(3) Utrecht Law Review 57.

[72] Council of Europe, 'Explanatory Report to the Convention on Cybercrime', retrieved from <https://rm.coe.int/16800cce5b> p. 9.

rise in attacks using this type of malware.[73] However, several of the Articles mentioned in Table 2 can be interpreted to apply to ransomware, such as Article 4 (Data interference), which criminalizes “the damaging, deletion, deterioration, alteration or suppression of computer data without right”, and Article 5 (System interference), which outlaws “the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data”. The Explanatory Report mentions that “suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. The term ‘alteration’ means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.”[74] Article 5 reflects a more scaled type of harm, including the hindering of telecommunication facilities. In a recent judgment, the Rotterdam court analysed ransomware under Article 350a of the Dutch Criminal Code, which is an implementation of Article 4 of the Budapest Convention, but made no reference to Article 161, which implements Article 5 of the Convention.[75]

5. Conclusions: Problems with the legal qualification of ransomware

As it can be seen from the two legal regimes under scrutiny, regulatory frameworks from the 1980s and 2000s are still applied today to deal with the increasing menace of

[73] Ibid.

[74] Ibid, p. 11.

[75] ECLI:NL:RBROT:2018:6152, retrieved from <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2018:6152>.

ransomware as one of the most recent cybercrime waves to jeopardize the interests of individuals and institutions alike, whether public or private. However, as technology advances and produces new iterations of existing phenomena (e.g., malware), a fundamental question arises as to whether earlier legal regimes are still fit to govern new harms or new scales of existing harm. Upon the brief reflection provided by this paper, both the FCAA and the Budapest Convention have sufficient flexibility to deal with the legal implications of ransomware from a criminal perspective. However, two short points need to be made about the fitness of these instruments, dealing on the one hand with the harmonization of legal interpretations and with enforcement and cooperation on the other.

First, as far as the substantive harmonization of legal standards is concerned, the CFAA proposes categories of crimes which, at least for ransomware, focus on the intention to derive financial benefits out of cybercrime (e.g., the extortion element of § 1030(a)(7)). By contrast, the Budapest Convention focuses on defining the technological prerequisites around the acts it discusses (e.g., the suppression element in Articles 4 and 5). For the United States, as a ratifying state of the Budapest Convention, harmonization questions emerge relating to the way in which the FCAA interacts with the Convention. For ratifying states which do not have legal regimes equivalent to the FCAA, and particularly for the Council of Europe Member States, it is important to map how national legislation complements or conflicts with the novel interpretations of the Convention, which may ensure its applicability regardless of the challenges posed by new malware iterations. A glimpse of this issue can be seen in the case-law of Dutch courts, which need to make a choice as to whether to apply the provisions affiliated with Article 4 or Article 5 when qualifying ransomware-related crimes.

Second, substantive qualifications are very much dependent on factual evidence. Given the transnational nature of cybercrime, the collection of evidence remains dependent on investigative powers and legitimacy, specifically when these powers are limited by the geographical borders of jurisdictions and their cyberspace equivalents. Although not discussed in this paper, the question of law enforcement cooperation is a highly relevant matter which ought to be given more attention to in coming years, especially in the light of upcoming legal reforms such as the updating of the Budapest Convention so it is better fit to govern modern cybercrime.[76]

[76] Council of Europe, 'The Budapest Convention on Cybercrime: benefits and impact in practice', retrieved from <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>.