UNIVERZITA KARLOVA

Právnická fakulta

Jan Fousek

Kriminologické a trestněprávní aspekty šíření ransomware

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. Bc. Tomáš Gřivna, Ph.D.

Katedra: Trestního práva, kriminologie a kriminalistiky

Datum vypracování práce (uzavření rukopisu): 13. 6. 2019

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 159 931 znaků včetně mezer.

Jan Fousek

V Praze dne 13. 6. 2019

Obsah

Úvod

Tato diplomová práce se zabývá jednotlivými aspekty, se kterými se setkáváme v oblasti kriminologie a trestního práva v souvislosti s problematikou šíření škodlivého programu (malware) v podobě ransomware. Důvodem, který mě vedl ke zpracování předkládaného tématu, je, dle mého názoru, nedostatečná informovanost o kyberkriminalitě a jejích dopadech na společnost, zejména tu českou. Záměrně se neomezuji na užití slovního spojení české právní prostředí, neboť bychom se pak nacházeli v poměrně úzce vymezené oblasti. Alespoň z hlediska kriminologického je potřeba vycházet i z jiných vědních disciplín, zejména z počítačových věd, kryptovirologie, ale samozřejmě i ze zvláštních právních disciplín, jakými je například právo ICT, nebo i z práva evropské unie, případně práva mezinárodního. Lze říct, že kriminologie je vědní obor, který působí jednak napříč dalšími vědními obory a je tedy multidisciplinární a taktéž těchto dalších věd využívá a spolupracuje s nimi a stává se tak i interdisciplinární.[1]

Vzhledem k nedostatku literárních zdrojů týkající se problematiky ransomware v českém jazyce je nutné, aby práce zahrnovala podstatnou část internetových zdrojů, a to zejména v anglickém jazyce, jejichž uplatnění lze vztáhnout pouze ke kriminologické části práce, neboť úprava trestního práva je dosud výsostným právem daného státu, a tudíž je zásah jiného státu nebo organizace do této matérie poměrně vzácná[2]. Kyberkriminalita je pojmem poměrně stále živým, novým a z právního hlediska neprobádaným, a to především v právní praxi, a proto se v práci snažím reflektovat základní otázky, které jsou s touto problematikou spjaty.

Důležité je také uvést, že se otázkou kriminologických a trestněprávních aspektů fenoménu ransomware již zabýval Johanovský[3] a poměrně stručně a systematicky popsal základní pojmy, které jsou s tímto tématem neodmyslitelně spjaty. Z těchto důvodů je potřebné uvést, že mnou předkládaná práce z práce Johanovského vychází, pracuje s ní, ale zároveň se snaží odlišit. Johanovského diplomovou práci využívám tedy jako přehledný poznámkový aparát, jelikož má tato práce spíše popisný charakter. Pokud jde o základní pojmy, které se týkají kyberkriminality, prostoru, ve kterém je kyberkriminalita páchána (kyberprostor) a jiné pojmy na tyto pojmy navázané (malware, počítačové viry/červi, …), je nevyhnutelné, aby byly opět rozpracovány a

[1] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3, s. 24

[2] Budapešťská úmluva, činnost Europol a jeho Evropského centra pro boj proti kyberkriminalitě, Eurojust, Interpol, mezinárodní justiční spolupráce s NCOZ.

[3] JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware, 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D.

vymezeny, avšak v zájmu účelnosti mé práce se snažím nalézt nový přístup s přihlédnutím k rychle měnícímu se diskurzu. Naopak některé pojmy, které s ransomware souvisí (například kryptoměny, internet či Darkweb) zmiňuji spíše na okraj, neboť se snažím odlišit od obecného popisu ransomware jakožo určitého fenoménu, ale zaměřuji se na šíření ransomware a jeho negativní důsledky.

Práce je rozdělena do dvou hlavních částí, a to části teoretické, která se dále člení na kapitoly týkající se obecně kyberkriminality, obecně malware a následně kriminologických aspektů šíření ransomware a trestněprávních aspektů šíření ramsomware, a to jak z hmotněprávního hlediska, tak z procesněprávního. Jednotlivé kapitoly jsou dále členěny na dílčí podkapitoly a ty zahrnují nejen otázky pachatelů a obětí ransomware či trestněprávní kvalifikace tohoto fenoménu, ale rovněž i pojmy příbuzné, jejichž zmínka by měla sloužit k širšímu pochopení tohoto druhu kyberkriminality. Ten je typický zejména svým distančním charakterem páchání, vysokou mírou latence a poměrně nízkou možností dopadení jejich pachatelů.

Druhou částí práce je část analytická. V této části kombinuji kriminologické výzkumné metody, když se snažím verifikovat hypotézu týkající se růstu čísel evidovaných skutků odpovídají ransomware. Jako zpracovatel této diplomové práce mám vzhledem k výše uvedeným skutečnostem ambici stanovit si jednu hypotézu. Hypotéza je následující: „*Počet zaregistrovaných útoků ransomware Policií ČR v České republice od roku 2016 roste.“* Analytická část je z několika, v této části blížeji specifikovaných, důvodů rozsahově užší než část teoretická. Tato skutečnost je kromě rozsahu získaných dat, ze kterých analýza vyplývá, spojena i se skutečností, že na celou práci je nutné pohlížet jako na celek.

Nakonec bych rád uvedl, že se jedná o diplomovou práci, a tudíž se nejen rozsahem práce držím předepsaných a obvykle uznávaných pravidel pro vypracování práce tohoto druhu. To může mít za následek jisté zjednodušování a sklon k simplifikaci problému. Mou snahou je tedy spíše otevřít diskuzi o dalším zkoumání otázek spojených s ransomware, která by mohla vést k hlubšímu porozumění této problematiky pro právní i mimoprávní praxi.

V neposlední řadě bych ještě dodal v celku logickou poznámku, která se týká technických pojmů v oblasti IT technologií. Kyberkriminalita je spjatá s technologiemi, avšak pro účely této práce, která je určená zejména lidem, kteří se pohybují v oblasti právních a právu příbuzných oborů, nepovažuji za významné zacházet do detailů, které nejsou stěžejní právě pro tyto osoby. Práce je psaná na katedře trestního práva právnické fakulty UK, a i z tohoto důvodu bude text

věnovaný mechanismu páchání trestné činnosti za pomocí digitálních technologií značně zjednodušený.

Nakonec je ještě zapotřebí poznamenat, že velká část pojmů, které se k tématu předkládané diplomové práce vážou, je uváděna v anglickém jazyce a nemá český a zcela přesný překlad. V případech, kde je to vhodné a v běžné praxi užívané, uvádím i český termín, avšak vycházím z premisy, že jednou zmíněný pojem je již dostatečně jasný k tomu, aby byl dále užíván v původním a významově nejpřesnějším vyjádření.

Teoretická část

I. Pojem kyberkriminalita

Někteří autoři se domnívají, že žijeme v době informační[4], což nemohu nijak vyvracet, neboť i já se domnívám, že informace je dnes jednou z největších hodnot a zároveň i zbraní. Nové technologické prostředky lze totiž využít i k páchání trestné činnosti, a to zcela nového typu. Wall tak například píše, že některé formy kyberkriminality představují „stará vína v nových lahvích", čímž myslí, že tyto formy kyberzločinu jsou koherentní, ale novým se stává médium, ve kterém se páchá.[5] Naopak o „novém vínu v nových lahví" hovoří v souvislosti s kyberzločinem, který se přímo váže na existenci počítačové technologie a Internetu, a zahrnuje tak například šíření malware (tedy i ransomware), nebo hacking.[6] Z hlediska udržení stabilního rozvoje společnosti je tak žádoucí, aby byla taková nová kriminalita potírána, neboť kriminalita představuje sociálně patologický jev[7], který je nutný potlačit.

Kybernetická trestná činnost pak představuje kriminalitu nových možností, navíc se neomezuje na pouhou počítačovou kriminalitu, ale má mnohem širší dosah. K tomu, že kyberkriminalita je kriminalitou nových možností se vyjadřuje i Holt[8], který vnímá kyberkriminalitu progresivně a tvrdí, že jde při jejím páchání o stále se pohybující a plynulý cíl, který se neustále mění, vytváří nové příležitosti pro pachatele a přináší nové výzvy společnosti k reakci na ni.

Ransomware je pak jedna z forem malware[9] (škodlivého programu), kterým je páchána kybernetická trestná činnost a je tedy jedním z jejích projevů. Tato trestná činnost, která má mnoho forem, je páchána v prostoru digitálního či virtuálního prostředí, který nazýváme

[4] Například: DE ANGELIS, Gina a Austin SARAT. Cyber crimes. Philadelphia, Pa.: Chelsea House Publishers, c2000. Crime, justice, and punishment. ISBN 0-7910-4252-9, s. 23
[5] Wall, D. S. (1998). Catching cybercriminals: Policing the Internet. International Review of Law, Computers and Technology, 12, 201-218
[6] Tamtéž
[7] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3, s. 24
[8] HOLT, Thomas J. a Adam M. BOSSLER. Cybercrime in progress: theory and prevention of technology-enabled offenses. London: Routledge, 2016. Crime Science Series. ISBN 978-1-138-02416-8.
[9] Obojí bude vysvětleno vzápětí.

kyberprostorem[10]. Pojem kyberprostor, resp. kybernetický prostor (ang. *Cyberspace*) vychází z beletrie a poprvé tento pojem zmínil William Gibson ve své kyberpunkové sci-fi povídce Burning Chrome[11] vydané v roce 1982[12]. O dva roky později pak tento pojem blíže ji rozvedl ve svém románu Neuromancer. Například De Angelis se nicméně domnívá, že samotný koncept kyberprostoru je mnohem starší a souvisí už s vynálezem telekomunikačního zařízení Alexandera Grahama Bella v roce 1878[13].

V každém případě je kybeprostor již všeobecně známý a rozšířený pojem, který má mnoho ekvivalentních označení. Třeba Završnik uvádí pojmy virtuální prostor, cipherspace, kryptoanarchismu, informační dálnice, infosféra, next nature, metavesmír, společenský software (socioware) či telepřítomnost[14], ale můžeme se setkat i s pojmem Cyberpunk Space[15]. Někdy se užívá i pojmu virtuální realita, která je však podle Smejkala pojímán spíše jako jeden z projevů či vlastností kyberprostoru.[16]

Legální definici bychom pak mohli najít v zákoně o kybernetické bezpečnosti, podle něhož se kybernetickým prostorem rozumí „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací*“.[17] Kriminalitu lze podle Cejpa vnímat jako souhrn trestných činů spáchaných za určité období na určitém místě.[18] Lze tedy shrnout, že kyberkriminalita představuje komplex trestných činů spáchaných v kybernetickém prostoru za určitý časový úsek. Kyberkriminalita stejně jako

[10] O protlačení pojmu kyberprostor do vědeckého povědomí se zasadil zejména J. Barlow, což byl zakladatel Electronic Frontier Foundation, tj. společnosti usilující o svobodu jednotlivce v kyberprostoru. K tomu dále srov. GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3, s. 334

[11] V českém jazyce byl titul vydán pod názvem „Jak vypálit Chrome“.

[12] ZAPLETAL, Josef. Aktuální problémy kriminologie: (pro posluchače magisterského studijního programu). Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-316-1, s. 121

[13] DE ANGELIS, Gina a Austin SARAT. Cyber crimes. Philadelphia, Pa.: Chelsea House Publishers, c2000. Crime, justice, and punishment. ISBN 0-7910-4252-9, s. 13

[14] ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). e-ISBN 978-80-7552-759-2, s. 34

[15] DE ANGELIS, Gina a Austin SARAT. Cyber crimes. Philadelphia, Pa.: Chelsea House Publishers, c2000. Crime, justice, and punishment. ISBN 0-7910-4252-9, s. 79. Nutno však dodat, že tento pojem souvisí spíše s apokalyptickou budoucností. Příkladem může být film Blade Runner z roku 1982 či jeho pokračování Blade Runner 2049 z roku 2017.

[16] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 130

[17] § 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen *„zákon o kybernetické bezpečnosti“*)

[18] CEJP, Martin. Kriminologický výzkum: praktická příručka. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-743-6, s. 11

kyberprostor má řadu dalších označení, a to zejména kybernetická kriminalita, kybernetická trestná činnost či kyber zločin (z ang. *Cybercrime*)[19].

Kyberkriminalitu lze z teoretického hlediska dělit na pravou a nepravou. Pravá kyberkriminalita je kriminalita uskutečňovaná v kybernetickém prostoru, která by neexistovala bez internetu, nepravá naopak může probíhat i bez něj (například krádež dat z počítače za pomoci flash disku, viry přenesené na disku atd.).[20] Pro účely této práce, pokud nebude výslovně uveden opak, se má na mysli vždy právě pravá kyberkriminalita. Považuji za nutné taktéž uvést, že pojem kyberkriminality je pojem poměrně široký a ve světle budapešťské úmluvy[21] zahrnuje tři rozdílné oblasti, které jsou předmětem kyberútoku[22]. Jedná se o oblast útoků (trestných činů) směřujících proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů (hovoříme právě o pravé kyberkriminalitě), dále útoků proti počítači nebo související s počítačem, útoky spojené s obsahem (zejména související s dětskou pornografií) a oblast útoků proti autorskému právu a práv souvisejících s právem autorským.

Poměrně často dochází k záměně dvou pojmů, a to kybernetické kriminality a počítačové kriminality.[23] Kybernetická kriminalita představuje širší pojem a zahrnuje kriminalitu zachycenou v kyberprostoru, který je tvořen především propojením komunikačních zařízení, a to za účelem přenosu informací a dat za pomoci různých komunikačních protokolů, zejména pak TCP/IP protokolu. Počítačová kriminalita se omezuje na trestnou činnost spojenou s počítači, tj. nezahrnuje i jiná zařízení, která spolu komunikují.[24] Nicméně je potřeba si uvědomit, že právě postavení počítače, dat a informací tvoří základní kameny, na kterých je kyberzločin vystavěn a nelze jejich důležitost zcela zavrhnout.[25] Počítač se za předpokladu, že útok není veden proti jeho hmotné podstatě[26], stává předmětem útoku, ale představuje rovněž i nástroj trestné činnosti.[27]

---

[19] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf, s. 12

[20] ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). e-ISBN 978-80-7552-759-2, s. 24

[21] Úmluva o počítačové kriminalitě, přijaté v Budapešti dne 8. listopadu 2001 Výborem ministrů Rady Evropy na 109. zasedání (*Convention on Cybercrime, ETS No. 185*) a následně otevřena k podpisu dne 23. listopadu 2001, vyhlášena pod č. 104/2013 Sb. m. s. (dále jen *„Budapešťská úmluva"*)

[22] Trestný čin spáchaný v kyberprostoru je vždy kybernetickým útokem, avšak každý kyberútok nemusí být trestným činem k tomu srov. KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 55

[23] Tím se poměrně detailně zabývá např. GILLESPIE, Alisdair. Cybercrime: key issues and debates. Routledge. 2016. ISBN 9780415712200, kap. 1

[24] Zejména mobilní telefony, tablety, chytré spotřebiče a automobily, drony, případně roboty

[25] ZAVRŠNIK, Aleš. 2017, s. 26, též WALDEN, Ian. Computer crimes and digital investigations. Oxford: Oxford University Press, 2007. ISBN 978-0-19-929098-7.

[26] Tím se rozumí zejména proti hardware, resp. i software, případně firmware.

[27] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 25, též odkazuje na: VLČEK, Martin,

Jak vyplývá z výše uvedeného, kyberkriminalita je neodmyslitelně spjata s daty a informacemi, které jsou nositeli pro člověka významné hodnoty (pokud jde o oblast útoků proti počítačovému systému nebo dat případně útoků spojených s počítačem) či se stávají útočným nástrojem (zejména pokud jde o oblast útoků spojené s obsahem a právu autorskému a jemu příbuzných práv). Data a informace, ač jsou často nesprávně používány promiscue, představují dva rozdílné pojmy. Budapešťská úmluva pro účely jednotného výkladu definuje počítačová data jako „(…) *jakékoliv vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému a to včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem*“.[28] Zákon o kybernetické bezpečnosti pak pro účely tohoto zákona vymezuje pojem bezpečnostní informace.[29] Informace je jak v právu, tak i mimo právní obory nesourodým pojmem.[30] Osobně se přikláním k definici, kterou uvádí Završnik a vychází z premisy, že data představují pojem podstatně širší než informace. Jeho předpokladem je, že data jsou potenciální informace, a to za předpokladu, že jsou přenášeny mezi komunikátorem a příjemcem a zůstávají nepochopena. V opačném případě by se jednalo právě o informace.[31]

II. Pojem malware

Kyberkriminalita by se neobešla bez škodlivých programů, které se různými způsoby snaží znepříjemnit uživateli život ve virtuálním prostoru, ale i mimo něj. Etymologicky představuje malware složeninu dvou slov anglického původu a to malicious (škodlivý, zlovolný, zlomyslný) a software.[32] Malware je tedy škodlivým programem, který se snaží proniknout do systému určitého zařízení, a to s cílem narušit chod tohoto systému, někdy též jen s cílem obtěžovat uživatele[33].

K tomu dochází různými formami, neboť každý malware v sobě může obsahovat jiný typ škodlivého kódu. Tyto formy souvisí s tím, že každý malware může v závislosti na určitém

---

Vladimír SMEJKAL a Tomáš SOKOL. Počítačové právo. Praha: Beck/SEVT, 1995. Právo a hospodářství. ISBN 80-7179-009-5, s. 99; k tomu též: POLČÁK, Radim a Tomáš GŘIVNA. Kyberkriminalita a právo. 1. vyd. Praha: AUDITORIUM, 2008. 220 s. Auditorium. ISBN 978-80-903786-7-4, s. 33, též PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. 2. aktualizované a rozšířené vydání. Plzeň: Aleš Čeněk, 2019. ISBN 978-80-7380-741-2, s. 960

[28] Kapitola I – Užití pojmů, čl. 1 – Definice, bod b. Budapešťské úmluvy

[29] § 2 písm. c) zákona o kybernetické bezpečnosti: …bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací a dat, …

[30] K tomu srov. SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 40 a následující

[31] ZAVRŠNIK, Aleš. Kyberkriminalita. 2017. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). e-ISBN 978-80-7552-759-2, s. 26

[32] K tomu např.: Malware. Eset.com [online]. [cit. 2019-02-25]. Dostupné z: https://www.eset.com/cz/malware/

[33] Tamtéž

škodlivém kódu vykonávat více činností. S touto skutečností souvisí i důvod, proč se v dnešní době používá primárně obecného pojmu malware a opouští se jednotlivé dělení malware na jednotlivé typy.[34] Přístup k dělení malware se velmi liší. Většinou je pro rozdělení malware na různé typy rozhodující způsob jeho šíření. Autoři různých publikací, kteří se o fenomén malware zajímají, uvádějí většinou stejné druhy, a to trojské koně, viry, červi, ransomware, spyware, crimeware a další. V této souvislosti je nutné podotknout, že pojem škodlivý kód (v anglickém originálu *malicious code*) je pojmem širším než škodlivý program (*malware*), neboť zahrnuje i situace, kdy je škodlivý kód součástí něčeho, co není programem, čímž je typicky webová stránka.[35]

Pro aktivaci malware je nutné, aby se dostal do určitého zařízení (např. počítače). Způsoby, jakými se tam dostane, se nazývají vektory útoku a jejich účinnost je zpravidla podmíněna součinností uživatele. Součinnost představuje východisko dělení například pro Šulce, který uvádí Drive-by download malware, Phishing a Trojanizovanou aplikaci.[36] Jedná se o typy malware, kdy první zmíněný je součástí webové stránky a vyžaduje pro svou aktivaci navštívení takové infikované stránky. Druhý zmíněný malware je projevem sociálního inženýrství (z anglického *Social Engineering*), což je technika využívající slabosti lidské mysli a v hackerské hantýrce je též nazývána jako wetware.[37] Nakonec třetí zmíněný je velmi častý malware ve formě trojského koně (z anglického originálu *Trojan Horse*), který se obyčejně skrývá za pro uživatele prospěšný program. Většinou se šíří jako příloha mailu nebo může být obsažen v bezplatných aplikací či hrách.[38]

Závěrem bych rád konstatoval, že malware vnímám zejména jako nástroj k páchání kybernetické trestné činnosti. Vycházím z toho, že útočník využívá svého zařízení, jehož komponentou je software, který mu vedle dalších komponentů umožňuje vytvořit, nebo si pořídit škodlivý software. Nelze opomenout jistý rozkol s výkladovým ustanovením § 118 TZ[39], který dle mého názoru nechává prostor pro výklad toho, co se považuje za zbraň, a to zejména v první části

[34] K tomu KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7., s. 204-205
[35] K tomu JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware, 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D., s. 7
[36] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 40 a n.
[37] Should social engineering a part of penetration testing? Darknet.org.uk [online]. [cit. 2019-02-25]. Dostupné z: https://www.darknet.org.uk/2006/03/should-social-engineering-a-part-of-penetration-testing/
[38] Trojan. Avast.com [online]. [cit. 2019-02-25]. Dostupné z: https://www.avast.com/cs-cz/c-trojan
[39] § 118 TZ: „*Trestný čin je spáchán se zbraní, jestliže pachatel nebo s jeho vědomím některý ze spolupachatelů užije zbraně k útoku, k překonání nebo zamezení odporu anebo jestliže ji k tomu účelu má u sebe; zbraní se tu rozumí, pokud z jednotlivého ustanovení trestního zákona nevyplývá něco jiného, cokoli, čím je možno učinit útok proti tělu důraznějším.*“

znění ustanovení před středníkem. Zde se mimo jiné stanoví, že trestný čin je spáchán se zbraní, jestliže pachatel užije zbraň k útoku, k překonání nebo zamezení odporu. Pokud by bylo možné se omezit pouze na tuto část znění příslušného paragrafu trestního zákoníku, pak bychom jistě mohli tvrdit, že malware je zbraní. Malware v podobě viru bychom mohli považovat za jakousi nášlapnou minu, která vybouchne po její aktivaci kliknutím či jiným způsobem. Malware v podobě červa se snaží proniknout do počítačového systému a odolávat jistému odporu, kterým mu systém zabraňuje dalšímu šíření.

Problém z hlediska legálního vymezení nastává však s druhou částí zmíněného ustanovení za středníkem, neboť zde je jasně stanoveno, co se rozumí zbraní ve smyslu trestního zákoníku, pokud trestní zákon nestanoví jinak. Bohužel antropocentrické pojetí této části by vyžadovalo, aby byl útok směřován právě proti lidskému tělu, a nikoliv proti počítačovému systému nebo jiných nehmotných věcí. Z hlediska kriminologického, resp. z hlediska mimoprávního, se však nebojím považovat zařízení, kterým útočník vytváří malware, nebo si ho pořizuje za účelem útoku, za zbraň stejně tak jako jisté typy malware, zejména ty, které mají povahu miny či jistého automatizovaného tvora nehmotného charakteru, jak jsem popsal výše.

1. Počítačové viry a červi

Již výše bylo popsáno, co se rozumí malware a taktéž jsem naznačil, že existuje jistá klasifikace malware. Typickým projevem kybernetické trestné činnosti proti počítačovému systému jsou však počítačové viry a červi. Ačkoliv se zdá, že jsou tyto dva pojmy ekvivalentní, není tomu tak. Počítačový vir, který se právem takto nazývá, neboť stejně jako virus biologického původu se šíří do hostitelských souborů, které infikuje, a tak se šíří dál[40], je škodlivým kódem. Počítačový vir však na rozdíl od počítačového červa nepůsobí zcela automatizovaně a je potřebná jeho aktivace[41], a to právě infikací.

Počítačový červ má více podob, ale pravděpodobně nejznámější je rozdělení na emailové červy a síťové červy (někdy se užívá pojmu internetoví červi).[42] Síťový červ je typický samočinný malware, který se šíří zcela sám. Obecně v sobě obsahuje řadu jiných škodlivých kódů v podobě

[40] KRUPIČKA, Jiří. Trestněprávní a kriminologické aspekty internetové kriminality. Praha, 2012. Disertační práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Prof. JUDr. Jiří Jelínek, CSc., s. 76
[41] ZAVRŠNIK, Aleš. Kyberkriminalita. 2017. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). e-ISBN 978-80-7552-759-2, s. 91
[42] KRUPIČKA, Jiří. Trestněprávní a kriminologické aspekty internetové kriminality. Praha, 2012. Disertační práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Prof. JUDr. Jiří Jelínek, CSc., s. 76

tzv. nákladu (z anglického originálu *Payload*)[43], což je v podstatě sekundární negativní efekt tohoto červa vedle zpomalení systému a zanešení sítě (resp. převzetím kontroly nad systémem). Emailový červ naproti tomu využívá sociálního inženýrství, neboť tento specifický druh červa je potřebné aktivovat, což je právě typický rys pro počítačové viry, avšak vir ke svému šíření využívá hostitelského souboru (infikovaného souboru).

2. Crimeware, spyware a adwere

Vedle počítačových virů a červů rozeznáváme i řadu jiných malware. Jedním z nich je právě i Crimeware. Tento malware zahrnuje útoky směřující na identitu oběti. Snaží se odcizit osobní údaje nebo jiné citlivé údaje například o přístupu k bankovnímu účtu. K tomu pachatel využívá opět zejména sociálního inženýrství, anebo instalací keyloggerů[44]. Keylogger představuje software, který slouží k snímání akce na klávesnici, což umožňuje efektivní získávání citlivých údajů, zejména hesel[45]. Pokud však chce útočník získat informace, které jsou cílem jeho útoku, musí se k nim nějakým způsobem dostat. Ať už zvolí cestu keylogger nebo social engineering, tak se patrně nevyvaruje tzv. phishingu (někdy je užíváno jako český ekvivalent pojmu *rhybaření*[46]). Podstatou phishingu je za pomoci podvodného jednání přimět uživatele k součinnosti. Takové jednání může spočívat v obstarání si phishing kitu[47], anebo útoků za pomoci trojského koně, který nese keylogger.[48]

Právě s touto agendou souvisí i další malware a tím je spyware (špehovací software). Zejména při používání keyloggerů dochází ke špehování činnosti uživatele. Ten často ani neví, že ho někdo sleduje a dozví se o spyware až pozdě, když navštíví například internetové bankovnictví. Podstatou spyware je tedy jejich obtížné detekování. Jedním z projevů napadení počítače či mobilního

[43] Payload. Searchsecurity.techtarget.com [online]. [cit. 2019-02-25]. Dostupné z: https://searchsecurity.techtarget.com/definition/payload
[44] Crimeware. Searchsecurity.techtarget.com [online]. [cit. 2019-02-25]. Dostupné z: https://searchsecurity.techtarget.com/definition/crimeware
[45] Vedle keyloggerů je možnost užití i tzv. prolamovačů hesel, které jsou založené na automatizovaném generátoru kombinací znaků, srov. též GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3, s. 340
[46] Nejde o překlep, slovo rhybaření vychází z anglického slova fishing (rybařit) a jeho „přesmyčky" phishing (rhybařit); k tomu též: KRUPIČKA, Jiří. Trestněprávní a kriminologické aspekty internetové kriminality. Praha, 2012. Disertační práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Prof. JUDr. Jiří Jelínek, CSc., s. 93
[47] Jedná se o nástroj určený k lovení identifikačních a jiných citlivých údajů. Obsahuje např. nástroje na vytvoření falešné webové adresy, nebo podvodný mail vyzívající k obnovení hesla na konkrétní stránce, kde jsem registrován v domění, že jde o pravou stránku, např. internetové bankovnictví.
[48] Crimeware. Searchsecurity.techtarget.com [online]. [cit. 2019-02-25]. Dostupné z: https://searchsecurity.techtarget.com/definition/crimeware

zařízení je snížení rychlosti procesoru, snížení rychlosti internetového připojení, rychlejší úbytek mobilních dat a rychlejší pokles baterie.[49]

Někdy se za spyware označuje i adwere (jedná se o zkratku z anglického *Advertising-Supported Software*), který je někdy označován jako reklamní software. Adwere však na rozdíl od spyware může mít dvě formy, a to klasického software a malware. Jelikož jsou adwere nejčastěji součástí freeware[50], zobrazují se spolu se spuštěným programem reklamy, a to buď jako bannery nebo pop-up okna, přičemž tyto reklamy mohou být různé intenzity rozšíření. Pokud však byl nainstalován freeware s adware bez vědomí uživatele, jedná se o malware, který může být ve formě spyware.[51] Obecně tedy může spyware sloužit k získání informací o uživateli k tomu, aby adware fungoval lépe a zobrazoval oběti pouze ty reklamy na produkty, o které se zajímá, avšak rozdíl mezi těmito software spočívá v informovanosti oběti o výskytu tohoto malware v jeho počítači.

3. Ostatní malware

Vedle výše zmíněných forem malware existuje i celá řada jiných malware, které jsou často součástí těch již vyjmenovaných. Jedná se o další dílčí útoky, které mají často ničivější dopad než ty původně zamýšlené. Cílem této podkapitoly je doplnit ještě několik dalších patrně nejrozšířenějších malware, se kterými se v současné době můžeme setkat.

Nejvýznamnější je z těchto malware trojský kůň, který sebou nese náklad v několika formách. Jednou z takových forem jsou tzv. zadní vrátka (neboli *Back Door*). Tato zadní vrátka umožňují bezproblémový vzdálený přístup do napadeného systému a vytvářejí tak z daného zařízení jednoduchý cíl pro další útoky. Jednou z nejagresivnějších forem útoků za pomocí trojského koně jsou útoky pomocí zombie počítače (též označovaný jako *Bot*), který představuje zcela ovládnutý počítač napadený trojským koněm. Pokud je takovýchto počítačů více, tvoří síť zombie počítačů (označovaných též jako *Botnet*), které jsou plně automatizované a fungují autonomně. Takováto síť je skvělým nástrojem pro DDoS útoky (z anglického *Denial Distributed of Service*[52]), které jsou často páchány organizovanými skupinami útočníků a mohou způsobit selhání systému pro

[49] Spyware. Searchsecurity.techtarget.com [online]. [cit. 2019-02-25]. Dostupné z: https://searchsecurity.techtarget.com/definition/spyware
[50] Freeware představují bezplatný nebo za symbolickou částku poskytnutý software, který často obsahuje reklamu, nebo vybízí k zakoupení plné verze.
[51] Adware. Searchsecurity.techtarget.com [online]. [cit. 2019-02-25]. Dostupné z: https://searchsecurity.techtarget.com/definition/adware
[52] Česky „distribuované odmítnutí služby“

přetížení kvůli vysokému počtu útoků zejména spamware.[53] Takové útoky, které jsou často namířené i proti veřejným institucím jako jsou nemocnice, školy, vládní instituce, složky dopravní infrastruktury a další, mohou mít velmi vážné důsledky pro jejich fungování.

Zvláštním typem škodlivých programů mohou být tzv. rootkity. Podstata těchto malware spočívá v zakrývání sebe sama a jiných malware.[54] Rootkity jsou často navázané na viry nebo trojské koně, které slouží jako přenašeče škodlivého software do příslušného zařízení. S tím souvisí fakt, že rootkit se nemůže sám šířit.[55] Je tedy vyžadována součinnost uživatele zařízení. Útočník se obyčejně snaží za pomoci rootkitu získat přístup administrátora do počítačového systému a k tomu využívá nižších vrstev operačního systému a snižuje tak možnost k jeho detekování anti-malwarovým sofwarem. Nižší vrstvy operačního systému poskytují těm vyšším základní služby.[56] Zjednodušeně řečeno se jedná o oblast operačního systému, která je pro běžného uživatele skrytá, a tím se stává rootkit významnou bezpečnostní hrozbou.

Dalším malware, o kterém bych se rád zmínil, je scareware[57]. Někdy se pro tento malware užívá označení deception software[58], rouge scanner software[59] nebo fraudware[60].Taktéž ho lze označit za falešný antivir[61]. Scareware je druh škodlivého kódu, který se oběti dostane do zařízení nejčastěji při návštěvě webových stránek, a to přesměrováním formou pop-up oken. Oběti se tak zobrazí, že jeho zařízení bylo infikováno malware a že jako řešení se nabízí stažení a instalace přiloženého antivirového softwaru. Tento software však rozhodně není antivirovým programem. Účelem scareware je vylákat z oběti určitou sumu peněz, kterou falešný antivir vyžaduje pro odstranění domnělého problému, a to v určitém časovém rozpětí. Cílem je však získat citlivé informace o oběti a o to se postará malware, který je součástí škodlivého softwaru. Někdy se scareware považuje za zvláštní druh jiného malware, a tím je ransomware. Problematice scareware jako druhu ransomware se však věnuji v kapitole následující.

---

[53] KRUPIČKA, Jiří. Trestněprávní a kriminologické aspekty internetové kriminality. Praha, 2012. Disertační práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Prof. JUDr. Jiří Jelínek, CSc., s. 77

[54] Rootkits, Part 1 of 3: The Growing Threat. Mcafee.com [online]. 2006 [cit. 2019-02-26]. Dostupné z: http://web.archive.org/web/20060823090948/http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_akapoor_rootkits1_en.pdf, s. 3

[55] Rootkit. Avast.com [online]. [cit. 2019-02-26]. Dostupné z: https://www.avast.com/cs-cz/c-rootkit

[56] KLIMEŠ, Cyril. Architektura operačních systémů [online]. 2018. Brno: Mendelova univerzita v Brně. ISBN 978-80-7509-635-7.

[57] Z anglického *to scare* = vyděsit a software.

[58] *Deception* lze přeložit jako podvod, či klam.

[59] Anglické slovo *Rouge* lze přeložit jako darebák (významově jde spíše o lupiče – často užíváno v MMORPG hrách).

[60] Vychází ze složeniny anglických slov *Fraud* = podvod a *Software*.

[61] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 42

Nakonec bych pro úplnost zmínil i malware, který je meritem celé práce, a tím je ransomware. Jedná se o vyděračský škodlivý software, který však může mít více podob a nemusí vždy naplnit pouze skutkovou podstatu trestného činu vydírání. Problematiku ransomware však rozebírám podrobně v kapitolách následujících, a proto se tu o ní dále nebudu rozepisovat.

III. Pojem ransomware

Ransomware je typem škodlivého softwaru, který nazýváme též pojmem malware. Pojem ransomware je složeninou dvou anglických slov, a to *ransom* čili výkupné a *software*. Někdy je označován jako rogueware (z ang. *rogue* tedy darebák, ničema) nebo scareware (z ang. *scare* tedy děsit)[62]. Smysl ransomware tkví v podmíněném přístupu k zařízení, nebo souborům zaplacením výkupného. S tím souvisí i skutečnost, že ransomware je někdy nazýván i vyděračským softwarem[63]. Do počítače či jiného zařízení se nejčastěji dostává jako „náklad" (*Payload*) trojského koně, který je umístěn na webových stránkách nebo jako příloha mailu.[64] Někdy může existovat spolehlivá webová stránka, jejíž součástí může být reklamní banner, který již v sobě ponese škodlivý kód[65] (malvertising).[66]

1. Typy ransomware

Určitá teorií vytvořená typologie ransomware je významná nejenom z hlediska správné trestněprávní kvalifikace, ale i z jiných hledisek. Obyčejně se rozlišují dva základní typy ransomware, a to zamykací (z angl. *locker ransomware*), někdy označovaný jako nešifrovací a kryptovirální, někdy též označovaný jako šifrovací (z angl. crypto ransomware). Vedle toho se

[62] Ransomware. Avast [online]. [cit. 2019-02-08]. Dostupné z: https://www.avast.com/cs-cz/c-ransomware
[63] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 42
[64] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7., s. 221
[65] Složenina ang. slov *malware* (škodlivý software) a *advertisement* (reklama).
[66] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 49

uvádí i třetí specifický typ ransomware označovaný jako doxware[67], extortionware[68] případně policejní ransomware[69]. Johanovský[70] uvádí i čtvrtý druh ransomware a to scareware[71].

Zamykací ransomware se projevuje tím, že plochu na softwarovém rozhraní nahradí výzva k úhradě výkupného a poučení o následném odblokování počítače. Obvykle tak znemožní uživateli jakoukoliv činnost na jeho zařízení. Odblokování bývalo v minulosti poměrně jednoduché, avšak v dnešní době je kvůli účinnějším verzím odstranění závadného stavu značně komplikované.[72] Zamykací ransomware tedy na rozdíl od kryptovirálního nešifruje soubory, ale pouze napadá operační systém a znemožňuje přístup do počítačového systému, tedy soubory zůstávají zachovány. Pokud bychom rozpoznali druh ransomware, mohlo by to zásadním způsobem ovlivnit úspěšnost boje proti tomuto malware.

Kryptovirální ransomware je typický tím, že naopak šifruje soubory, a to zejména ty, které jsou pro uživatele nejcennější, aby ho útočník donutil zaplatit výkupné. Typicky se jedná o rodinné fotografie nebo důležité pracovní dokumenty. Některé šifrovací ransomware jsou jednodušší na detekování, neboť přejmenovávají soubory, zejména jim přidělují různé přípony, jiné šifrovací ransomware naopak soubory nepřejmenovávají a jejich detekování se stává obtížnějším, avšak hlavička těchto souborů neodpovídá formátu a vytvářejí typické řetězce.[73] Často se jako jedno z prevenčních opatření doporučuje zálohovat důležitá data. Bohužel některé kryptovirální ransomware se dovedou dostat až k dokumentům na připojeném síťovém disku, což je právě místo, které uživatelé zpravidla používají k zálohování.[74] Kryptovirální ransomware se vyznačuje taktéž tím, že má na oběť působit šokově. Tento typ ransomware má být propracován tak, že při jeho zobrazení se člověk vyleká a v daném mentálním rozpoložení zaplatí co nejdříve. Útočníci totiž používají časových podmínek[75]. Může se tak stát, že se bude jednat pouze o domnělý kryptovirální

[67] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 214
[68] Doxware (extortionware). Whatis.techtarget.com [online]. [cit. 2019-02-25]. Dostupné z: https://whatis.techtarget.com/definition/doxware-extortionware
[69] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf, s. 221-222
[70] JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware, 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D., s. 21
[71] Připouštím, že jisté rysy ransomware jsou zde patrné (jak uvádím dále), avšak já se přiklonil k řazení scareware mezi další specifické malware (viz výše).
[72] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 51-52
[73] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 216-217
[74] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, tamtéž
[75] Obvykle stanoví, že v případě včasného nezaplacení budou dokumenty smazány, nebo bude odstraněn dešifrovací klíč. K tomu např. ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk,

ransomware, neboť útočník přesvědčí oběť o možnosti zašifrování v případě nezaplacení ve stanovené době.[76]

Dalším typem ransomware je doxware. Jedná se o exploit[77], který je znám zejména ve dvou základních formách. Jedna z forem představuje situaci, kdy útočník požaduje po oběti zaplacení určité částky pod pohrůžkou zveřejnění určitých citlivých údajů, které se mu o oběti podařilo ukořistit. Druhá forma, která je častěji označována za policejní ransomware představuje situaci, kdy se pachateli podařilo získat portrétní fotografii skrze nabouranou webkameru a tu pak zanesl do výzvy k uhrazení pokuty za nelegální činnost. Útočník se v tomto případě snaží v oběti vyvolat dojem, že jí kontaktoval orgán veřejné moci (resp. orgán činný v trestním řízení) a že spáchala nějaký trestný čin, ovšem dává jí možnost vyvázat se z trestního stíhání zaplacením jakési smyšlené pokuty.[78] Ransomware je tak i schopen stáhnout určitý inkriminovaný materiál[79] (typicky dětská pornografie, nebo nelegálně stažený software) a vydávat jej za kriminalistickou evidenci důkazů.

Někdy lze mezi ransomware řadit i scareware (viz výše). Problém s tím, zda je vhodné řadit scareware mezi ransomware, spočívá v principu jeho fungování. Na rozdíl od výše zmíněných ransomware se liší způsobem, jakým se snaží oběť infikovat. Zpravidla se s ním člověk setká při návštěvě určitých webových stránek s kompromitovaným materiálem (např. pornografické stránky). Obyčejně formou *pop up windows* (vyskakovacích oken) jste přesměrování na jiné stránky, které nesou malware. Oběti se zobrazí okno s upozorněním na napadení zařízení virem. Zpravidla to nemusí být pravda, a jde pouze o to, aby se oběť vylekala. Pro pachatele je tudíž důležité, aby sdělení bylo, pokud možno, co nejvíce uvěřitelné a šokující. Vedle informace o infikaci obsahuje sdělení, že je možné tento problém vyřešit. Nejčastější je právě nabídka „antivirového programu“, který problém odstraní. Takový program může být placený, nebo naopak může být zdarma, aby nalákal oběť svou výhodností. Po stáhnutí a instalaci se do počítačového systému dostane škodlivý software.

Častá je kombinace scareware s adware a spyware. V tento moment nově nainstalovaný program oběti oznámí, že pro odstranění konkrétního problému je nutné si takovou službu zaplatit.

2018. ISBN 978-80-7380-737-5, s. 50

[76] Crypto-ransomware. F-secure.com [online]. [cit. 2019-03-04]. Dostupné z: https://www.f-secure.com/en/web/labs_global/crypto-ransomware

[77] Exploit je softwarový nástroj k páchání kybernetické kriminality. Více k tomuto pojmu najdete v kapitole o pachatelích ransomware.

[78] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 214

[79] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 51

Osobně mám tedy problém se zařazením scareware mezi ransomware, neboť zde absentuje vyděračské jednání. Oběť se může svobodně rozhodnout, zda si produkt zakoupí či nikoliv. Jednání definující scareware je založené spíše na podvodu, neboť pachatel pod falešnou zprávou přinutí oběť stáhnout a nainstalovat škodlivý software, a navíc žádá peníze za odstranění neexistujícího problému. Někdy se pro scareware používá ekvivalentní termín fraudware (z anglického *fraud* tedy podvod a software), což je taktéž jeden z argumentů, proč je zařazení scareware mezi ransomware komplikované. Podvod je však s novými technologiemi, zejména s Internetem, neodmyslitelně spjat, byť je lidstvu znám už od doby, kdy začalo mluvit a vlastnit majetek. K tomu se ostatně vyjadřuje například Button[80]. Z tohoto důvodu nelze scareware zcela opomíjet a zabývám se jím i dále, byť v souvislosti s ransomware.

2. Cíle a motivace pro šíření ransomware

Ransomware je primárně používán pachatelem jako prostředek k obohacení. Cílem ransomware je ve většině případů přimět oběť zaplatit výkupné. Sekundárním cílem může být oběť postrašit nebo alespoň potrápit. Jednotlivé sekundární cíle se liší v závislosti na konkrétním druhu ransomware. Někdy se však může stát, že se primární cíl stane sekundárním, a to v závislosti na úmyslu pachatele. Například pachatel může chtít poškozenému pouze udílet lekci a zajistit, že se o daném ransomware dozví co nejvíce lidí.[81] Důležité je však poznamenat, že ransomware vždy doprovází vyděračské jednání. Pachatel slibuje, že odemkne určitou složku např. s fotografiemi po zaslání platby, nebo že dešifruje přístup do počítačového systému, případně že se napadený uživatel vykoupí ze svých fiktivních prohřešků, a to za podmínky, že uhradí požadované výkupné.

Ransomware je považován za jednu z kybernetických hrozeb[82]. Motivace k šíření takovéto hrozby může být různá a nelze ji vymezit zcela taxativně. Motivaci lze tak spatřovat například v hrozbě za účelem získání finančního prospěchu (což je u ransomware převažující motiv), případně jako dokazování svých schopností, nebo v odplatě.[83] Grabosky uvádí motivace pachatelů, bez ohledu na typ kyberzločinu (zahrnuje tedy i ransomware), jako je chamtivost, chtíč, síla,

[80] BUTTON, Mark a Cassandra CROSS. Cyber frauds, scams and their victims. Abingdon: Routledge, Taylor & Francis Group, 2017. ISBN 978-1-138-93120-6.
[81] ŠRUBAŘ, Michal. Analýza síťové komunikace Ransomware. Brno, 2017. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ryšavý Ondřej, s. 5
[82] KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČOVÁ a Martin KUNC. CyberSecurity. Praha: CZ.NIC, 2019. CZ.NIC. ISBN 978-80-88168-31-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybersecurity.pdf, s. 79
[83] Tamtéž, s. 78

pomsta, dobrodružství a touhu dosáhnout „zakázaného ovoce“.[84] Taktéž spatřuje novost této motivace v bezprecedentnosti kapacity tachnologií, které usnadňují působení na tyto motivace.[85]

Cíl, ke kterému útočník směřuje, je silně ovlivněn právě onou pohnutkou, která v něm vzbudí rozhodnutí k šíření ransomware. Nelze ani s jistotou určit, zda je motivem pouze jedna skutečnost, nebo jich je více. Často se pachatelé kyberzločinu mohou svým činem utvrdit o více skutečnostech. Útočník se například může utvrdit v tom, že dokáže proniknout do cizího systému, že dokáže způsobit škodu, a navíc dokáže z oběti získat finanční obohacení. Nelze ani vyloučit pohnutku mající své kořeny v pouhé zvědavosti, či recesi. Takové pohnutky bychom patrně (vzhledem k případné absenci dostatečné rozumové a mravní vyspělosti) hledali spíše u mladistvých útočníků. Vedle výše zmíněných motivů lze tak jmenovat i touhu překonat subjektivní pocit nedocenění, nebo motiv záležející v krytí jiné trestné činnosti, případně politický či ideologický motiv.[86]

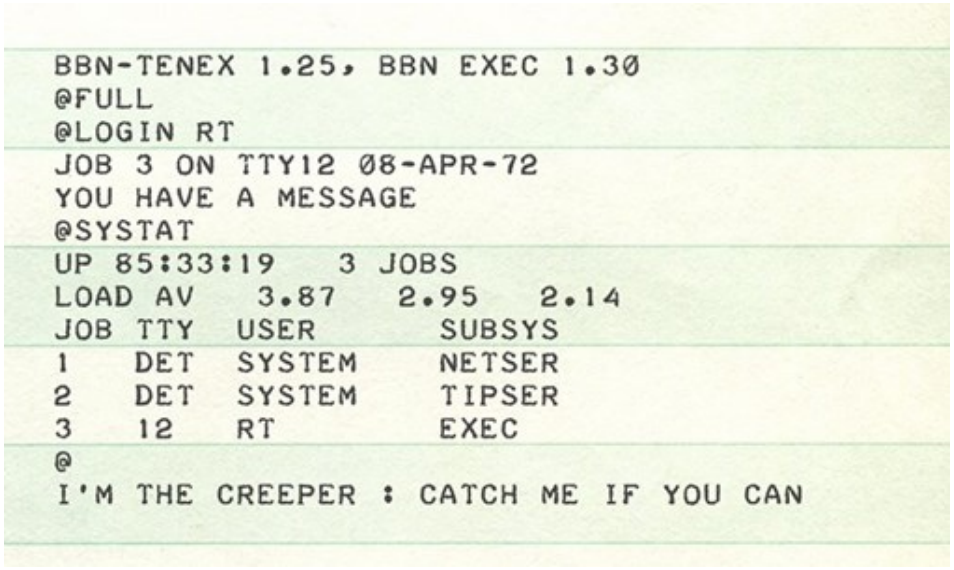
Taktéž nelze opomenout motiv pramenící z vysoké latence kyberkriminality dosahující až 95 procent[87]. Ta plyne zejména z pocitu bezttrestnosti, neodhalitelnosti, či nepolapitelnosti, ale taktéž domněnky, že malé ztráty nikomu neublíží.[88] Je rovněž potřeba poznamenat, že takovéto motivy jsou uvedeny pouze jako typické pohnutky ve vztahu k obecné kyberkriminalitě. Uvádím však takové, které jsou aplikovatelné právě i na ransomware. Nelze taktéž zapomenout, že ransomware má více podob a jednotlivé motivy se tak mohou lišit. Ransomware má však určitou zvláštnost, která pramení z jeho charakteru a tím je téměř výlučná kombinace dvou motivů, respektive cílů. Těmito motivy jsou zištný motiv a motiv zastrašení. Z jiného pohledu se jedná o záměr (cíl) spočívající v způsobení škody (zašifrování dat), v obohacení (získání peněz od oběti) nebo v zastrašení. Oběť ransomware má, snad až na určité výjimky, vždy strach o to, že přijde o své dokumenty uložené v zařízení, případně, že proti ní bude zahájeno trestní stíhání, a zároveň útočník oběť žádá o peníze, což oběť pociťuje jako škodu.

[84] GRABOSKY, Peter N. Virtual Criminality: Old Wine in New Bottles? Social & Legal Studies. Vol 10(2). ISSN 09646639, 243-249
[85] Tamtéž
[86] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. 2. aktualizované a rozšířené vydání. Plzeň: Aleš Čeněk, 2019. ISBN 978-80-7380-741-2, s. 965
[87] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3, s. 530
[88] Tamtéž.

3. Historie ransomware

Důležitým okamžikem pro šíření malware byl vznik Internetu. Za jeho podobou, jak ji známe dnes, stojí rozvoj počítačových sítí. Významná však byla až 60. léta 20. století, neboť to vznikla první experimentální počítačová síť označovaná jako předchůdce dnešního Internetu a to ARPANET[89]. Tato síť však měla sloužit spíše pro resort ministerstva obrany USA než pro veřejnost, což se začalo měnit se zkoumáním této sítě a s vývojem TCP/IP protokolů. Na ARPANET, který rozhodně nebyl jedinou sítí v USA, ale i ve světě, se tak v 80. letech 20. století začaly nabalovat i jiné sítě, a to včetně těch lokálních, čímž vznikl jeden konglomerát vzájemně propojených sítích označovaných za Internet.[90]

Prvním známým malware, který se objevil již na ARPANETU, byl vir *Creeper* (překl. popínavá rostlina). Ten v roce 1971 napsal Bob Thomas z BBN (Bolt, Beranek and Newman Inc.). Obětem se na počítači zobrazil text: „*I'm the Creeper: Catch me if you can*"[91] (viz Obr. č. 1). Reakcí na tento vir byl první antivirový program, který nesl označení *Reaper* (překl. sekačka).[92]



Obr. 1: Creeper. Zdroj: Creeper and Reaper. Core War [online]. [cit. 2019-06-09]. Dostupné z: https://corewar.co.uk/creeper.htm

Historie ransomware je však významná až od roku 1989, kdy výzkumný pracovník Joseph Popp rozeslal medicínským institucím zabývajících se výzkumem AIDS na bootovacím floppy disku první známý ransomware. Jednalo se o 20 000 disků, které měly nést vedle ransomware

[89] ARPANET je zkratkou pro *Advanced Research Projects Agency Network* (ARPA = grantová agentura ministerstva obrany USA, později přejmenovaná na DARPA (D = Defense)
[90] PETERKA, Jiří. Na počátku byl ARPANET... Earchiv.cz [online]. [cit. 2019-03-07]. Dostupné z: http://www.earchiv.cz/a95/a504c502.php3
[91] Přeloženo jako: „Já jsem Creeper: Chyť mě, když to dokážeš".
[92] K tomu Creeper. Corewar.co.uk [online]. [cit. 2019-03-07]. Dostupné z: http://corewar.co.uk/creeper.htm

dotazník k AIDS analýze rizikových osob. Po devadesátém spuštění softwaru se ransomware aktivoval a zobrazila se zpráva o tom, že vypršela softwarová licence a je potřeba zaplatit částku ve výši 189 dolarů, a to na účet společnosti PC Cyborg Corporation. Jednalo se nicméně o šifrovací ransomware, a proto bylo potřeba si pro zachávání dat připlatit ještě 378 dolarů (viz obrázek č. 2). Tento ransomware tak vstoupil ve známost jako AIDS Trojan (pro jeho formu šíření), anebo PC Cyborg.[93]

Obr. 2: Trojan AIDS. Zdroj: The Computer Virus That Haunted Early AIDS Researchers. The Atlantic [online]. [cit. 2019-06-09]. Dostupné z: https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/

V roce 2006 evidovala antivirová společnost Kaspersky Lab zvýšenou snahu tvůrců ransomware o dešifrování.[94] Hackeři totiž začali využívat RSA[95] asymetrické šifrování s veřejným klíčem. Symetrické šifry mají pouze jeden klíč pro zašifrování i odšifrování, zatímco asymetrické šifrování má klíč veřejný a soukromý. To představuje pro útočníka určitou jistotu, že bez privátního klíče nemůže dojít k dešifrování a ransomware tak bude úspěšný.

Ransomware útoků však proběhlo v několika verzích celá řada[96] a nelze se v této kapitole zaobírat všemi. Z tohoto důvodu jsem si vybral pouze dva, nejen z vývojového hlediska významné. Jedná se o CryptoLocker a WannaCry.

---

[93] Srov. The Computer Virus that Haunted Early Aids Researchers. Theatlantic.com [online]. [cit. 2019-03-07]. Dostupné z: https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/ a History Ransomware Attacks: Biggest and Worst Ransomware Attacks of All Time. Digitalguardian.com [online]. [cit. 2019-03-07]. Dostupné z: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

[94] Malware evolution: April-June 2006 [online]. [cit. 2019-03-11]. Dostupné z: https://securelist.com/malware-evolution-april-june-2006/36094/, k tomu též SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 214

[95] RSA je zkratkou vycházející s prvních písmem autorů této metody šifrování (tj. *Rivest, Shamir, Adleman*).

[96] Např. Trojan.Win32.Krotten, Gpcode, Daideneg, Schoolboys, Cryzip, MayArchive, CryptoLocker, WannaCry, Petya, Locky, Cryptowall, TorrentLocker, Fury, Aura, Shade, Teslacrypt.

Pravděpodobně jeden z nejznámějších ransomware byl Cryptolocker[97]. Svůj největší rozmach zaznamenal v roce 2013 a stal se jedním z nejvýdělečnějších ransomware své doby. S tím souvisí i skutečnost, že od září do prosince 2013 stačil napadnout 250 000 systémů a získat kolem 3 milionů dolarů.[98] Svou činnost však ukončil 2. června 2014 v souvislosti s vypnutím Gameover Zeus Botnet, což byla síť infikovaných počítačů, které představovaly mimo jiné i přenašeče útoků CryptoLockerem. Za tímto ukončením stála mezinárodní spolupráce vládních i soukromých institucí a společností s označením operace Tovar.[99]

Útok Cryptolockerem probíhal tak, že po infikaci počítače (nejčastěji jako škodlivá příloha mailu nesoucí Payload ve formě ransomware) a zakódování souborů vyskočilo okno s pokyny útočníka. Ten informoval oběť o zašifrovaných dokumentech, včetně fotek, jiných pro uživatele důležitých souborech a o možnosti dešifrování za pomoci jediného privátního klíče. V případě, že nebude zaplaceno ve stanovené lhůtě bude tento klíč zničen a bude navždy zamezeno dešifrování postižených souborů (Obr. č. 3). Útočníci po zašifrování inkriminovaných složek požadovali k zaplacení částku ve výši 100 až 300 dolarů za využití kryptoměn (nejčastěji Bitcoin).[100]

Obr. č. 3: Cryptolocker. Zdroj: CryptoLocker. How to remove? (Uninstall guide). 2SpyWare [online]. [cit. 2019-06-09]. Dostupné z: https://www.2-spyware.com/remove-cryptolocker.html#ref-1

[97] History Ransomware Attacks: Biggest and Worst Ransomware Attacks of All Time. Digitalguardian.com [online]. [cit. 2019-03-07]. Dostupné z: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
[98] Tamtéž
[99] CryptoLocker – an infamous ransomware virus that was stopped by the Operation Tovar [online]. [cit. 2019-03 11]. Dostupné z: https://www.2-spyware.com/remove-cryptolocker.html#ref-1
[100] Tamtéž

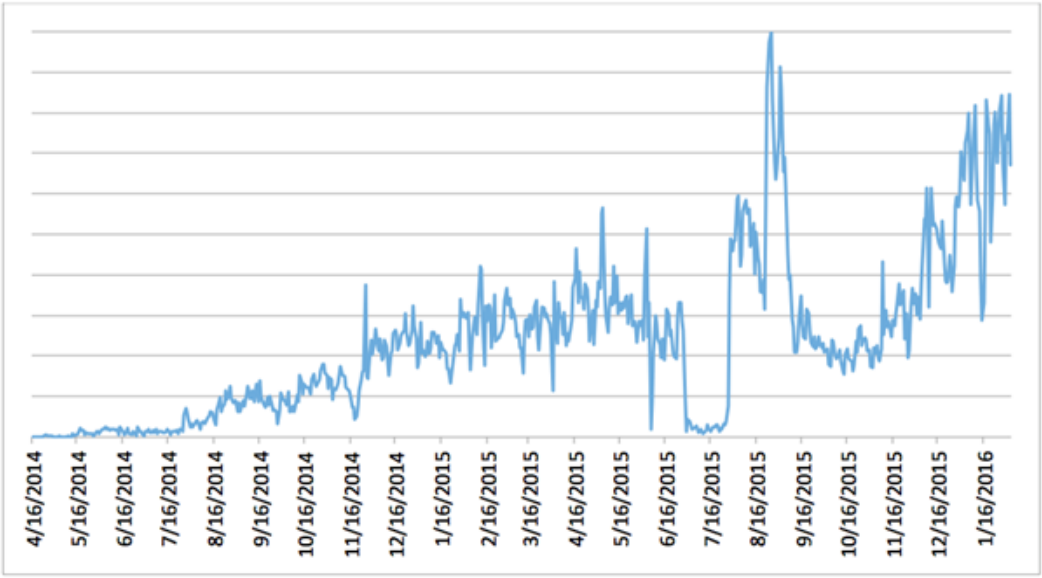
Patrně nejničivější a nejmasivnější byl útok WannaCry z rodiny WannaCryptor ransomware. Večer 12. května 2017 tento ransomware stačil infikovat tisíce počítačů z celého světa a během 24 hodin činilo číslo infikovaných zařízení 185 000 ve více než 100 státech.[101] WannaCry využívá zejména *Eternal Blue exploit*, který byl ukraden organizovanou kyberzločineckou skupinou s názvem *Shadow Brokers* od americké NSA (*National Security Agency*) a umožnil jim jednoduchý přístup prakticky do jakéhokoliv zařízení užívající Windows software.[102]

Samotný WannaCry je v důsledku stejný jako kterýkoliv jiný ransomware tohoto typu, avšak vektor útoku je zcela výjimečný. WannaCry totiž využívá chyby v zabezpečovacím systému Windows. Ten totiž nesprávně implementoval SMB (*Server Messege Block*) protocol, který zajišťuje snadnější komunikaci mezi různými uzly v síti, čehož si všimla NSA a využila tuto chybu k vytvoření *Eternal Blue exploitu*.[103] Specifický pro WannaCry je jev, který se nazývá „*kill switch"*. WannaCry se totiž ihned po prvním spuštění pokusí získat přístup k neznámé dlouhé URL[104]. Pokud se to nepodaří, započne se šifrováním, v opačném případě se vypne. Názory na tento jev se liší. Někteří výzkumníci se domnívají, že jde o jistý uzávěr před útokem, který může být odložen. Marcus Hutchins, který objevil, že se WannaCry snaží o přístup k tomuto URL, však tvrdí, že jde o jistý trik, jak ztížit zkoumání kódu.[105]

Problém ransomware se vztahuje i na mobilní zařízení. Společnost Eset v roce 2016 upozorňovala na stoupající tendenci počtu útoků ransomware na zařízení užívající Android software, a to obvykle ve formě policejního ransomware.[106] Pro ilustraci odkazuji na graf, který Eset uvádí (Obr. č. 4). Lze konstatovat, že ransomware není problém spjatý pouze s počítači. Jeho vývoj je dle mého názoru nejistý, a to vzhledem ke vzrůstající tendenci neplatit výkupné. S tím

[101] Wormable ransomware strain uses freshly leaked exploit to encrypt data. Businessinsights.bitdefender.com [online]. [cit. 2019-03-11]. Dostupné z: https://businessinsights.bitdefender.com/wormable-ransomware-strain-uses-freshly-leaked-exploit-to-encrypt-data
[102] NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history. www.telegraph.co.uk [online]. [cit. 2019-03-11]. Dostupné z: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/
[103] What is Wannacry ransomware, how does it infect, and who was responsible?. Csoonline.com [online]. [cit. 2019-03-11]. Dostupné z: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
[104] URL = *Uniform Resource Locator* (tj. jednotná adresa zdroje)
[105] What is Wannacry ransomware, how does it infect, and who was responsible?. Csoonline.com [online]. [cit. 2019-03-11]. Dostupné z: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
[106] The rise of Android ransomware. Welivesecurity.com [online]. [cit. 2019-03-11]. Dostupné z: https://www.welivesecurity.com/2016/02/18/the-rise-of-android-ransomware/

totiž souvisí skutečnost, že tvůrci ransomware zřídka dostávají svým slovům a dešifrují po zaplacení výkupného.[107]



Obr. č. 4, Počet útoků ransomware. Zdroj: The rise of Android ransomware. Welivesecurity [online]. [cit. 2019-06-09]. Dostupné z: https://www.welivesecurity.com/2016/02/18/the-rise-of-android-ransomware/

4. Kriminologické aspekty ransomware

4.1. Pachatelé ransomware

Předně je potřeba poznamenat, že způsoby páchání kyberzločinů jsou velice pestré, a tudíž ani nelze vymezit typického pachatele kybernetické kriminality.[108] Legálně vzato chápeme pachatele trestného činu jako toho, kdo svým jednáním naplnil skutkovou podstatu trestného činu (též jeho pokusu či přípravy, je-li trestná)[109]. Jak vyplývá z podstaty ransomware, tak pachatelé, kteří ke svému obohacení využívají ransomware, naplní svým jednání alespoň skutkovou podstatu trestného činu vydírání podle § 175 TZ.Kriminologie však chápe pachatele trestného činu podstatně odlišně, a to jako předmět (resp. osobu/subjekt) zkoumání. Pachatelem je tak z pohledu

[107] History Ransomware Attacks: Biggest and Worst Ransomware Attacks of All Time. Digitalguardian.com [online]. [cit. 2019-03-07]. Dostupné z: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

[108] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3, s. 338

[109] K tomu srov. § 22 odst. 1 TZ.

kriminologického i osoba, která ještě trestný čin nespáchala a vůči níž doposud orgány činné v trestním řízení nezahájili trestní stíhání.[110]

Za pachatele počítačové kriminality se zpravidla považovali muži ve věku 17 až 30 let.[111] Dnes již můžeme tento úzus opustit a tvrdit, že nelze určit typického pachatele počítačové, případně kybernetické, kriminality na základě pohlaví a věku, neboť máme příliš mnoho dalších proměnných. Jednou z proměnných tak může být řada různorodých kybernetických trestných činů, kterých se pachatel může dopustit.[112] Nelze však ani opomenout otázku genderu.[113] Trestně odpovědná může být vedle osoby fyzické i osoba právnická. Trestní odpovědnost právnických osob za kybernetickou trestnou činnost je však vzhledem k principu přičitatelnosti specifická, a tudíž se jí budu zabývat pouze okrajově v závěru této podkapitoly. Pokud jde o právní kvalifikaci ransomware, odkazuji tímto na kapitoly následující týkající se této problematiky.

Obecně se z teoretického hlediska rozlišují dva typy pachatelů páchající trestnou činnost v kyberprostoru, a to profesionálové a amatéři.[114] Typickými profesionály jsou tzv. hackeři[115]. Amatéry, ačkoliv to nemusí být pravidlem, jsou crackeři. Média ovšem často tyto rozdílné pojmy zaměňují a stalo se tak, že je široká veřejnost považuje za totožné. Rozdíly jsou však markantní, zejména co do úmyslu pachatele. Hacker představuje fyzickou osobu znalou IT technologií, programování a kladou se na něj i vysoké etické nároky[116]. Crackerem naopak může být člověk, který má pouze povrchní znalosti programování, či žádné. Úmyslem crackera je, jak napovídá anglický původ tohoto slova[117], projít skrz zabezpečovací opatření a čerpat z toho nějaký užitek. Hacker je dost často právě ten, kdo vyvíjí určitý software a zkoumá skuliny v systému, kterými by se mohl do tohoto systému probourat.

---

[110] K tomu GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3, s. 87

[111] K tomu HOLCR, Květoň a Jaroslav FENYK. Kriminológia. Bratislava: Iura Edition, 2008. ISBN 978-80-8078-206-1, s. 361 a KLIMEK, Libor, Jozef ZÁHORA a Květoň HOLCR. Počítačová kriminalita: v európskych súvislostiach. Bratislava: Wolters Kluwer, 2016. ISBN 978-80-8168-538-5, s. 53

[112] K tomu zejména: ZAPLETAL, Josef. Aktuální problémy kriminologie: (pro posluchače magisterského studijního programu). Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-316-1, s. 143-144

[113] Gender je v této souvislosti potřeba vnímat jako historickou a kulturní odlišnost mezi mužem a ženou. Například ženy se historicky vzato méně angažovaly v technických oborech, což může být jeden z aspektů, proč jsou považováni za častější pachatele kybernetické kriminality muži.

[114] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3, s. 339 a též MADLIAK, Jozef, Ján MIHAĽOV, Viktor PORADA a Simona ŠTEFANKOVÁ. Počítačová kriminalita. Karlovarská právní revue. 2008, 4(1), 45-63. ISSN 1801-2191, s. 54

[115] Doslovný překlad anglického slova *hack* není pro námi chtěný význam příliš šikovný, neboť *to hack* znamená projíždět se na koni či sekat, i když významů může být více, tak žádný nevyjadřuje podstatu pojmu *hacker*.

[116] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf, s. 270 a n.

[117] (*crack* = rozlousknout, prolomit)

Dalo by se říct, že právě hacker je zdrojem škodlivého software, avšak hacker tak činí spíše ze zvědavosti, nebo protože se snaží rozvíjet své dovednosti, zatímco crackerovi jde o prospěch. V podstatě by se dalo tvrdit, že právě cracker je onen pravý pachatel, neboť hacker, který prolomí zabezpečovací opatření, se stává crackerem bez ohledu na jeho úmysly. Právě Budapeštská úmluva dává smluvním stranám na výběr, zda budou kriminalizovat i samotný neoprávněný přístup do počítačového systému, nebo zda budou trestat až samotnou škodlivou činnost v těchto systémech uskutečněnou[118]. Česká republika si zvolila variantu, že bude kriminalizovat už jen samotné porušení bezpečnostních opatření za účelem přístupu k počítačovému systému[119]. Tím de facto inkriminovala jednání hackerů, jejichž úmysly často nesměřovaly ke společensky škodlivému výsledku. Jaishankar[120] definuje hackera jako toho, kdo spáchal jeden z 12 počítačových trestných činů ze tří oblastí, kterými jsou softwarové pirátství, hacking a phreaking[121]. Tentýž autor rozděluje hackery na dobré a špatné, přičemž vychází mimo jiné z jakési teorie konformity, v rámci níž záleží na tom, do které sociální skupiny se určitý hacker řadí. Pokud se řadí do skupiny hráčů, pak jde o hackera dobrého, jestliže je však členem hackerských, nebo crackerských skupin, pak se jedná o hackera špatného.[122]

Ransomware tedy zpravidla páchají crackeři, neboť svým jednáním směřují k obohacení ve formě výkupného. Typická činnost crackerů se vyznačuje právě i tím, že si obstarávají tzv. Exploity, resp. exploit kity[123], a obyčejně se mezi nimi rychle šíří.[124] Nástroje v podobě exploit kitů přináší crackerům snadný způsob, jak proniknout do cizího zařízení a nainstalovat zde škodlivý software. Exploit kit obyčejně obsahuje payload, resp. náklad (viz výše), který infikuje hostitele, avšak existují verze propracovanější a nebezpečnější, které infikují síť a následně počítač oběti. Nejčastějším nákladem, který exploit kit obsahuje, je právě ransomware.[125]

Právnické osoby jsou zpravidla pro hackery, resp. Crackery, oblíbeným terčem útoku, avšak tím se zabývám s důrazem na malé a střední podnikatele v kapitole pojednávající o obětech ransomware. Pokud jde o právnické osoby jako o pachatele kybernetické kriminality, pak jde o

[118] Např. ve formě porušení bezpečnostních opatření za účelem získání počítačových dat; k tomu srov. Čl. 2 Budapešťské úmluvy.
[119] K tomu srov. § 230 TZ.
[120] JAISHANKAR, K. Cyber criminology: exploring Internet crimes and criminal behavior. Boca Raton, FL: CRC Press, c2011. ISBN 978-1-4398-2949-3, s. 36-37
[121] Phreaking představuje cracking mobilních zařízení za účelem bezplatného úžívání mobilní sítě
[122] K tomu JAISHANKAR, K. Cyber criminology: exploring Internet crimes and criminal behavior. Boca Raton, FL: CRC Press, c2011. ISBN 978-1-4398-2949-3, s. 40
[123] Exploit kit představuje nástroje využívající programátorskou chybu nejčastěji k infikaci malware.
[124] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3, s. 341
[125] What is an exploit kit. Paloaltonetworks.com [online]. [cit. 2019-03-04]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit

problematiku poměrně neprobádanou. Právnické osoby jednají, jak jsem již výše naznačoval, prostřednictvím svých zástupců (fyzických osob). V závislosti na právní formě právnické osoby rozlišujeme i statutární orgán, který zpravidla jedná ve všech věcech. Pro trestní odpovědnost právnické osoby však postačí, když se jedná i o osobu, která nemá např. kapitálovou vazbu na právnickou osobu, ale která jedná v jejím zájmu a v rámci její činnosti[126]. Rozhodně nelze vyloučit trestní odpovědnost právnických osob právě za kybernetické trestné činy, a to především s ohledem na změnu provedenou zákonem č. 183/2016 Sb., který rozšířil možnost kriminalizace právnických osob, neboť ty se nově mohou dopustit všech trestných činů vymezených v trestním zákoníku vyjmě těch taxativně vymezených v § 7 zákona o trestní odpovědnosti právnických osob[127]. Právnické osoby jsou tedy mimo jiné odpovědné za spáchání ryze počítačových trestných činů[128] a ostatních trestných činů, které se zpravidla aplikují při páchání trestné činnosti v kyberprostoru[129]. Mnohé jsou dokonce poměrně časté a dopouštějí se jich zejména bývalí zaměstnanci.[130] Ti však často bojují proti korporaci a nesou trestní odpovědnost nezávisle na trestní odpovědnosti právnické osoby[131].

Někdy se taktéž užívá rozdělejí hackerů, resp. crackerů na White Hats, Black Hats a Gray Hats.[132] White Hats by se z teoretického hlediska dali zařadit mezi hackery. Snaží se průnikem skrz zabezpečovací systém počítače objevit systémové chyby, zjistit příčiny slabin systému, tyto příčiny odstranit a zajistit tak lepší ochranu před kybernetickými útoky. Black Hats naopak představují klasické crackery, kteří se snaží způsobit uživateli škodu nebo jinou újmu, popřípadě získat pro sobě nebo pro jiného nějaký majetkový prospěch.[133] Do této skupiny lze řadit i pachatele ransomware. Grey Hats jsou jakousi sběrnou skupinou osob, kteří se primárně nesnaží páchat kybernetickou trestnou činnost, ale zejména veřejně upozorňovat na systémové chyby, z čehož mohou profitovat právě Black Hats.[134] Můžeme však rozlišovat i další skupiny hackerů nebo

[126] K tomu též RONOVSKÁ, Barbora. Trestní odpovědnost právnických osob a kyberkriminalita. Trestní právo: odborný časopis pro trestní právo a obory související. 2018, 2018(4), s. 21-22
[127] Novela zákona o trestní odpovědnosti právnických osob. Pravniprostor.cz [online]. [cit. 2019-03-04]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/novela-zakona-o-trestni-odpovednosti-pravnickych-osob, dále jen „ZTOPO“
[128] §§ 230 až 232 TZ; úprava přijatá v souvislosti s Budapešťskou úmluvou; srov. kapitola o hmětnoprávní kvalifikaci
[129] Zejména trestné činy vydírání podle § 175 TZ, podvodu podle § 209 TZ, porušení tajemství dopravovaných zpráv podle § 182 TZ a další.
[130] K tomu též například: POLČÁK, Radim a Tomáš GŘIVNA. Kyberkriminalita a právo. 1. vyd. Praha: AUDITORIUM, 2008. 220 s. Auditorium. ISBN 978-80-903786-7-4, s. 36
[131] Zásada nezávislé a souběžné trestní odpovědnosti fyzických a právnických osob
[132] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3, s. 339 nebo KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf, s. 273
[133] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf, tamtéž
[134] Grey Hat Hacker. Techopedia.com [online]. [cit. 2019-03-25]. Dostupné z:

crackerů podle jejich motivace jako jsou Script Kiddies[135], kteří jsou přirovnáváni k Black Hats, ale využívají pouze zapůjčených škodlivých programů, nebo *Hactivists*, což jsou aktivističtí hackeři, jež jsou motivováni k páchání kyberkriminality například politickou situací v jejich státě působení. Dále lze jmenovat i státem sponzorované hackery, špionážní hackery (*Spy Hackers)* nebo kyber teroristy (*Cyber Terrorists*).[136] Pachatele internetové kriminality[137] rozlišuje též Zeman podle jejich motivu (páchají jen pro zábavu, pro finanční motiv, z emocionálních důvodů, pro politické motivy, kvůli sexuálním impulsům nebo pro závažné psychické onemocnění).[138]

4.2. Prevence

K nejdůležitějším aspektům ochrany před ransomware patří prevence, zejména situační. Vedle prevence, která je bezpochyby tou nejúčinnější ochranou před ransomware máme k dispozici i jiné nástroje ochrany. Ty mohou být buď součástí prevence (například dostatečné bezpečností opatření), nebo se realizují teprve po uskutečněném útoku k odstranění závadného stavu. Proto je taktéž počítačová bezpečnost založena na třech krocích, které vedle prevence zahrnují též detekci a nápravu.[139] Za tímto účelem se snaží zejména anitivirové společnosti poskytnout uživatelům různé typy decryptorů, které mají za úkol odšifrovat zašifrované soubory.[140] Způsoby, jakými se lze proti útoku ransomware bránit, jsou protkány internetem a nevyžadují tak nějaké cílevědomější či náročnější vyhledávání. Z tohoto důvodu se v podkapitole prevence snažím zkompilovat nejúčinější postupy pro ochranu zařízení před útokem ransomware.

Europol[141] vyjmenovává jako nejzásadnější preventční kroky pravidelné aktualizace softwaru[142], používání antivirového softwaru, vyhledávání a stahování softwaru pouze

https://www.techopedia.com/definition/15450/gray-hat-hacker

[135] K tomu též WALL, David. Cybercrime: the transformation of crime in the information age. 2007. ISBN 9780745627359.

[136] 7 Types of Hacker Motivations. Securingtomorrow.mcafee.com [online]. [cit. 2019-03-25]. Dostupné z: https://securingtomorrow.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

[137] Internetová trestná činnost je součástí kybernetické trestné činnosti, často však dochází k používání pojmů kyberkriminalita, internetová kriminalita a počítačová kriminalita promiscue, což nepovažuji za teoreticky přesné vymezení, neboť přinejmenším internetová kriminalita nezahrnuje i jiné počítačová sítě, než je internet. Uzavřeme tedy, že internetová kriminalita je trestnou činností páchanou za využití komunikační sítě vzájemně propojených počítačů využívajících TCP/IP protokol, tedy Internet.

[138] ZEMAN, Daniel. Počítačová a internetová a kriminalita [online]. 2011 [cit. 2019-03-25]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/69852. Vedoucí práce Tomáš Gřivna, s. 13-15

[139] ZAPLETAL, Josef. Aktuální problémy kriminologie: (pro posluchače magisterského studijního programu). Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-316-1, s. 148

[140] Například od společnosti AVG: Bezplatné nástroje na dešifrování ransomwaru. Avg.com [online]. [cit. 2019-04-01]. Dostupné z: https://www.avg.com/cs-cz/ransomware-decryption-tools

[141] Cyber Intelligence Team. Ransomware: What You Need to Know: A Joint Report by Check Point and Europol [online]. The Hague: Europol Public Information, 2016 [cit. 2019-04-01]. Dostupné z: https://www.europol.europa.eu/publications-documents/ransomware-what-you-need-to-know

[142] Zahrnuje nejen operační systém, ale například i webový prohlížeč.

z ověřených webových stránek a pravidelné zálohování dat. Dále upozorňuje i na jednání, kterých by se měl uživatel z důvodu předcházení útoků ransomware vyvarovat. Tím jsou zejména tato jednání: klikání na přílohy, odkazy a bannery neznámého původu; instalování softwaru na svá zařízení od neznámého zdroje; důvěra v oznámení o zastaralém softwaru a nutnosti jeho aktualizace a instalace nebo spouštění neověřených softwarů.

Projekt Národního centra pro boj s informační kriminalitou nizozemské policie, Evropského centra pro boj proti kybernetické kriminalitě při evropské agentuře EUROPOL a antivirové společnosti McAfee s názvem No more ransom uvádí na svých webových stránkách další důležitou prevenční záležitost a tou je, vedle výše zmíněných, povolení funkce >zobrazit přípony souborů<.[143] Během šifrování totiž dochází ke změnám přípon a v případě jejich zobrazení lze efektivně předejít úplnému zašifrování odpojením zařízení od sítě. Národní úřad pro kybernetickou a informační bezpečnost (ČR) doporučuje taktéž neklikat na maily a jejich přílohy, jejichž doručení neočekávám a zároveň nepovolovat makra, které jsou častými stůjci za infikací.[144] Taktéž nelze opomenout i opravné balíčky, které vydávají tvůrci operačního systému k odstranění chyb (tzv. „záplaty“ neboli *patche*).

Nad rámec prevence jde pak doporučená činnost pro oběti útoku ransomware. Ta zahrnuje zejména okamžité ohlášení útoku příslušnému orgánu (například Policii ČR) a kontaktování poskytovatele antivirového programu. Naopak nedoporučuje se platit výkupné, neboť není jistota, že se poškozenému data navrátí.

4.3. Oběť a viktimogenní faktory ransomware

Postavení oběti v oblasti kybernetické kriminality má svá specifika. Předně je nutné poznamenat, že obětí může být vedle osoby fyzické i osoba právnická a dokonce i stát. Dle povahy oběti se taktéž liší přístup pachatelů, a i samotná osoba pachatele. Někdy je taktéž z pohledu sociálně-pozitivistického pachatel vnímán jako oběť svého prostředí, neboť může páchat i z pouhé zvědavosti.[145] Pro účely této podkapitoly však budeme vnímat oběť jako osobu, které byla v důsledku kyberzločinu na ní spáchané omezena práva. Postavení oběti se taktéž liší v souvislosti

[143] Preventivní rady. Nomoreransom.org [online]. [cit. 2019-04-01]. Dostupné z: https://www.nomoreransom.org/cs/prevention-advice.html
[144] Základní kurz kybernetické bezpečnosti určený zaměstnancům NÚKIB, dokument č.j. 537/2019-NÚKIB-E/210, s. 42
[145] POLČÁK, Radim a Tomáš GŘIVNA. Kyberkriminalita a právo. 1. vyd. Praha: AUDITORIUM, 2008. 220 s. Auditorium. ISBN 978-80-903786-7-4, s. 37

s konkrétním útokem v kyberprostoru. Jiná specifika bude mít oběť spammingu a jiná oběť DDoS útoku, případně trestných činů proti nenávisti spáchaných pomocí internetu.

Oběť útoku ransomware můžeme z pohledu úmyslu pachatele rozlišit na náhodnou a zamýšlenou.[146] Náhodné oběti tvoří zejména skupina fyzických osob. Fyzická osoba pak jako uživatel infikuje svoje zařízení (například kliknutím na škodlivou přílohu mailu) a následně je nucena pro obnovení svých dat zaplatit výkupné. V tomto případě se oběť pouze náhodou chytila do pomyslné pachatelovy sítě. Výkupné je v takových případech nastaveno obvykle ve výši 100 až 300 dolarů (viz výše), ale může se samozřejmě lišit v závislosti na místních poměrech. Například v České republice se výkupné pohybuje nejčastěji v rozmezí 7 500 – 17 000 Kč.[147] Pokud by výkupné bylo příliš vysoké, pak by mohla chybět motivace[148] oběti zaplatit. Pro ilustraci společnost KasperskyLab zaznamenala pokles uživatelů, kteří se setkali s ransomware v letech 2017-2018 téměř o 30 % oproti období 2016-2017.[149] Přesto se však toto číslo pohybuje kolem dvou milionů uživatelů, kteří byli napadeni ransomware. Problémem však je, že jakékoliv statistiky týkající se útoků ransomware jsou značně zkreslené. Evidence je totiž podmíněna tím, že útok někdo ohlásí.

Obecně je kyberkriminalita známá vysokou mírou latence, a tedy neochotou tento druh trestné činnosti ohlašovat. To může být způsobeno několika faktory. Jednak oběť zpravidla tuší, že vypátrat pachatele může být pro policii náročné a že míra napáchané škody má charakter spíše osobní povahy (například zašifrování složky s rodinnými fotografiemi), a tudíž se tím policie nebude příliš zabývat. Výraznou nevoli ohlašovat útoky[150] ransomware můžeme spatřovat také u právnických osob, které by mohly ohrozit svou dobrou pověst.[151]

Lze tedy tvrdit, že dalším faktorem, který přispívá k vysoké latenci je i strach ze sekundární viktimizace. Problém latence může být založen i na nižší míře znalosti IT technologií nebo na efektivní obraně. Oběť například nemusí být ochotná přiznat, že k napadení systému výrazně

[146] Podobným způsobem dělí oběti ransomware i Johanovský. Viz JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware, 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D., s. 30 a n.
[147] Základní kurz kybernetické bezpečnosti určený zaměstnancům NÚKIB - dokument č.j. 537/2019-NÚKIB-E/210, s. 41
[148] K motivaci platit výkupné též JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware, 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D., s. 30
[149] Ransomware and malicious crypto miners in 2016-2018. Securelist.com [online]. [cit. 2019-04-01]. Dostupné z: https://securelist.com/ransomware-and-malicious-crypto-miners-in-2016-2018/86238/
[150] K nevoli ohlašovat kybernetické trestný činy též: ZEMAN, Daniel. Počítačová a internetová a kriminalita [online]. 2011 [cit. 2019-03-25]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/69852. Vedoucí práce Tomáš Gřivna., s. 15
[151] K tomu též: POLČÁK, Radim a Tomáš GŘIVNA. Kyberkriminalita a právo. 1. vyd. Praha: AUDITORIUM, 2008. 220 s. Auditorium. ISBN 978-80-903786-7-4, s. 36-37

přispěla. S tím souvisí právě skutečnost, že ransomware vyžaduje interakci oběti s pachatelem. Vyjímkou není ani skutečnost, že oběť neví, že se stala obětí[152] (typicky u DDoS útoků).

Ransomware vyžaduje od oběti jistou součinnost. Taková součinnost má zpravidla dva projevy. Jednak se součinnost projevuje ve fázi infikace a následně ve fázi vyděračské. V první fázi je oběť podvedena, neboť se domnívá, že kliká na odkaz bezpečný a neuvažuje o možné infikaci. V druhé fázi již oběť ví, že se stala předmětem útoku ransomware a snaží se svá data zachránit. Zaplacení výkupného za současného neobnovení dat může přispívat k neohlášení ransomware útoku, stejně tak zaplacení za současného obnovení dat může mít stejné výsledky. V prvé řadě může oběť pociťovat potupu a výčitky za vlastní jednání, což jí může odradit od následného řešení věci s policií. V druhém případě oběť získala svá data zpět a zpravidla neuvažuje o nahlášení útoku z důvodu odstranění nepříznivého stavu. Nelze však vyloučit, že se oběť bude chtít lépe zabezpečit pro budoucí útoky.

Druhou skupinou obětí, jak jsem již zmínil výše, jsou oběti pachatelem zamýšlené. Jedná se zejména o skupinu osob právnických. Pro pachatele je z hlediska organizačního složitější vést útok proti právnické osobě než proti jednotlivci. Zároveň oběť ve formě právnické osoby se vyznačuje určitými specifickými znaky, které je činí pro pachatele lákavějšími cíly. Právnické osoby jsou zpravidla, avšak nikoliv výlučně, založeny za účelem podnikání. Pokud je podnikající právnická osoba úspěšná může být tato skutečnost viktimogenním faktorem pro útok ransomware. Pachatele, ať už samotného nebo jako součást organizované zločinecké skupiny, motivuje domněnka, že útok ransomware na právnickou osobu, byť jediný, může přinést vyšší výnos, než kdyby byl veden proti jednotlivci. Pachatel vychází z toho, že právnická osoba nebude chtít vyřadit svou činnost, byť na jediný den, neboť by to pro ni mohlo znamenat vyšší ztráty, než které by utrpěla zaplacením vysokého výkupného[153]. Zároveň efektivní činnost právnické osoby je zpravidla navázána na určité „know how“, které může být taktéž předmětem útoku.

Významnými obětmi se stávají malé a střední podniky. To může být zapříčiněno zejména nižší mírou ochoty platit za účinnější zabezpečení systému a taktéž vyšší motivací k nahlášení útoku policii. Antivirová společnost Bitdefender ve svém průzkumu zjistila, že pouhých 45 % malých a středních podniků získalo po zaplacení výkupného svá data zpět.[154] Taktéž zjistila, že

[152] ZAPLETAL, Josef. Aktuální problémy kriminologie: (pro posluchače magisterského studijního programu). Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-316-1, s. 145
[153] Obvykle v řádech desetitisíců. Srov. Ransomware targets SMBs due to weaker protection and greater willingness to pay up. Bitdefender [online]. [cit. 2019-02-10]. Dostupné z: https://businessinsights.bitdefender.com/ransomware-targets-us-smbs
[154] Tamtéž.

nejčastější vektor útoku, resp. způsob šíření, má formu přílohy mailu nebo drive-by downloadu. Na rozdíl od obětí v podobě jednotlivců je nutné přimět oběť, aby klikla na škodlivý materiál, který infikuje počítač. Pro pachatele je proto výhodné umístit inkriminovaný materiál do přílohy mailu, neboť je velká šance, že se v rámci pracovní komunikace dostatečně zakamufluje a dojde k jeho otevření. Byť mnoho podniků užívá pro interní komunikaci intranet, nelze vyloučit, že zaměstnanec nebude užívat soukromý mail, nebo že maily bude možné přijímat i zvenčí (přes internet) pro komunikaci s klienty.

Do skupiny osob, které se stávají obětmi z jasně zamýšleného a cíleného jednání pachatele, se řadí i státy jakožto veřejnoprávní korporace. Je však třeba vnímat útok na stát spíše jako útok na státní orgány nebo instituce. Takové útoky mohou mít kyberteroristickou povahu vedenou politickým motivem. Útoky jsou často spojené s vysokými náklady na jejich nápravu. Obětmi jsou tak spíše nepřímo lidé, kteří jsou na státních orgánech či institucích závislé. Není proto výjimkou, že takové útoky jsou vedeny zejména proti poskytovatelům zdravotních služeb nebo služeb dopravních. Taktéž nelze vyloučit útoky přímo ohrožující bezpečnost státu (například směřující proti armádě).

5. Trestněprávní aspekty ransomware

5.1. Obecně k hmotněprávní kvalifikaci ransomware

Správná hmotněprávní kvalifikace ransomware může činit problémy. Tato skutečnost je spjatá zejména s tím, že se ransomware projevuje ve více podobách, které byly rozepsány výše. Vedle toho je pro správnou kvalifikaci rozhodující i typ zařízení, proti kterému útok směřuje. Skutkové podstaty vyjádřené v §§ 230 až 232 TZ reagují na implementaci Budapešťské úmluvy z roku 2001, kterou Česká republika podepsala 9. února 2005 a ratifikovala až 22. srpna 2013 a reflektují pouze počítačovou trestnou činnost[155].

Trestní jednání v podobě útoku ransomware však směřují i proti jiným zařízením[156]. Lze se domnívat, že přijetí těchto specifických a dosti kazuistických skutkových podstat mohou činit

[155] K tomu vedle znění ust. Budapešťské úmluvy a TZ např. i systematické rozdělení kapitoly na ryze počítačové trestné činy podle Smejkala: SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 541 a n. nebo RONOVSKÁ, Barbora. Trestní odpovědnost právnických osob a kyberkriminalita. Trestní právo: odborný časopis pro trestní právo a obory související. 2018, 2018(4), s. 18

[156] Má se na mysli zařízení jako jsou dopravní prostředky s umělou inteligencí (koncept autonomních vozidel), plně automatizované spotřebiče (zejména koncept Smart Homes) nebo roboti.

právě kvalifikační problémy. Osobně považuji za poněkud nešťastnou kriminalizaci právě počítačových trestných činů tak, jak jsou uvedeny ve výše zmíněných paragrafech trestního zákoníku. Mám za to, že se tak nechává poměrně velký prostor pro aplikaci jiných ustanovení, které nejsou charakteristické pro nový typ trestné činnosti v podobě kyberkriminality[157].

Problém spatřuji zejména v krátkozrakosti zákonodárců. Ta spočívá v tom, že kybernetická trestná činnost je trestnou činností budoucnosti. V podstatě lze jednat „bez umazání se" a velmi snadno získávat vysoký prospěch. Stejně tak je možné, že kybernetický útok bude veden jako útok teroristický. Různorodost takových útoků přináší mnoho otázek, neboť není jisté, zda trestní zákoník dokáže takovou rozmanitost zcela pokrýt a zda taková jednání dokáže spravedlivě potrestat, resp. zda se pro ně najdou adekvátní tresty.

Za úvahu stojí, zda by nebylo vhodné zrušit stávající speciální skutkové podstaty trestního zákoníku směřující zejména k ochraně počítačového systému a vytvořit souhrnou speciální skutkovou podstatu kybernetického útoku, který by zahrnoval skutkové podstaty výše zmíněné. Výměra trestu by mohla být stanovena podobně jako je to například u trestného činu opilství podle § 360 TZ, tj. bylo by vymezeno základní rozpětí výměry trestu odnětí svobody s možností užití vyšší sazby (na rozdíl od trestného činu opilství, kde je možnost užití sazby nižší), pakliže by byla současně naplněna skutková podstata jiného závažnějšího trestného činu. Případně jako je tomu nově u zvláštního ustanovení o trestání legalizace výnosů z trestné činnosti, kde se má přihlédnout k výši trestní sazby stanovené na trestný čin, ze kterého pochází výnos z trestné činnosti, a to za předpokladu, že je tato stanovena mírněji (§ 216a TZ). Reagovalo by se tak jednak na nové typy kybernetické trestné činnosti a zároveň by se dostatečně stanovila výměra trestu podle jeho závažnosti. Trestný čin by se pak v případě klasického ransomware mohl kvalifikovat například jako přečin kybernetického útoku ve formě trestného činu vydírání. Podle Koloucha je však trestněprávní ochrana před kybernetickými útoky v ČR dostačující, avšak nepopírá, že útočníci mohou být značně inovativní a stávající úprava nemusí postačovat pro futuro.[158]

Ransomware lze tedy kvalifikovat v závislosti na okolnostech a způsobu jednání (resp. druhu ransomware) různě, avšak jedna kvalifikace je pro ransomware klíčová, neboť je součástí jeho podstaty, a tím je kvalifikace ransomware jako vydírání podle § 175 TZ. Této kvalifikaci tedy věnuji největší pozornost.

[157] Např. trestný čin vydírání podle § 175 TZ; trestný čin podvodu podle § 209 TZ, nebo trestný čin přisvojení pravomoci úřadu podle § 328.
[158] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf, s. 93

5.2. Ransomware jako vydírání podle § 175 TZ

Výše jsem se zmínil o tom, že podstatou ransomware je fakt, že vždy naplní alespoň skutkovou podstatu trestného činu vydírání podle § 175 TZ. Pachatelem vydírání může být kdokoliv, kdo je k tomu způsobilý. Musí jít tedy o osobu, která naplňuje obecné znaky trestného činu, kterými jsou trestním zákoníkem požadovaný věk (§ 25), příčetnost (§ 26) a u mladistvých i rozumová a mravní vyspělost (§ 5 odst. 1 ZSVM[159]).[160] Jednání pachatele rovněž musí být protiprávní a musí být vyloučeno užití subsidiarity trestní represe (§ 12 odst. 2 TZ). Protiprávní by jednání nebylo např. za možného užití ustanovení trestního zákoníku o okolnostech vylučujících protiprávnost (§§ 28–32). Pachatelem může být vedle osoby fyzické i osoba právnická (§ 7 ZTOPO), přičemž zde odkazuji na to, co bylo již napsáno výše[161]. Pachatel rovněž musí jednat tak, aby naplnil skutkovou podstatu trestného činu vydírání. Objektem trestného činu je u vydírání svobodné rozhodování člověka, a to v nejširším slova smyslu[162].

Objektivní stránkou trestného činu je jednání spočívající v tom, že pachatel jiného za užití násilí, pohrůžkou násilí, nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl.[163] Pro dokonání činu postačí, aby bylo jednáno násilím, pohrůžkou násilí nebo jiné těžké újmy a není při tom rozhodné, zda pachatel dosáhl toho, co svým jednáním sledoval.[164] V případě ransomware může nastat i situace, kdy se vyděračské prohlášení zobrazí osobě, která není schopna pohrůžku vnímat, resp. ji není schopna pochopit. V tomto případě se i v duchu usnesení Nejvyššího soudu ČR ze dne 25. 10. 2016, sp. zn. 7 Tdo 1172/2016 bude jednat o pokus vydírání na nezpůsobilém předmětu útoku.[165]

---

[159] ZSVM = z. č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže)

[160] JELÍNEK, Jiří, Katarína TEJNSKÁ, Jana TLAPÁK NAVRÁTILOVÁ, Vladimír PELC, Jiří ŘÍHA a Vojtěch STEJSKAL. Trestní právo hmotné: obecná část, zvláštní část. 6. aktualizované a doplněné vydání. Praha: Leges, 2017. Student. ISBN 978-80-7502-236-3, s. 134-135

[161] Viz kapitola o pachatelích ransomware

[162] ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 1751 a DRAŠTÍK, Antonín. Trestní zákoník: komentář. Praha: Wolters Kluwer, 2015. Komentáře Wolters Kluwer. Kodex. ISBN 978-80-7478-790-4, s. 974

[163] Např. ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, tamtéž

[164] ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, tamtéž

[165] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 224; k tomu i JELÍNEK, Jiří. Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif. 7. aktualizované vydání. Praha: Leges, 2017. Glosátor. ISBN 978-80-7502-230-1, s. 264

Ransomware obyčejně není projevem běžně vnímaného násilí jakožto fyzického ataku[166], ačkoliv ve smyslu výkladového ustanovení trestního zákoníku (§ 119) se lze dopustit trestného činu násilím i pokud pachatel uvedl osobu do stavu bezbrannosti lstí nebo jiným obdobným způsobem. V případě policejního ransomware však můžeme uvažovat o naplnění znaku pohrůžky jiné těžké újmy. K tomu bych rád uvedl rozsudek Nejvyššího soudu ČSR ze dne 8.4.1981, sp. zn. 6 Tz 12/81, podle kterého může být pohrůžkou jiné těžké újmy i zahájení trestního stíhání v důsledku oznámení trestného činu, kterým se poškozenému hrozí, aby něco vykonal, opominul, nebo trpěl.

Pohrůžka jiné těžké újmy je však pojmem těžko definovatelným a v trestním zákoníku bychom ji hledali marně. Soudy si tedy navykly používat tento pojem, který je součástí skutkové podstaty vydírání různě v závislosti na okolnostech případu. Dnes lze však konstatovat, že se vytvořilo alespoň rámcové povědomí o tom, co lze za pohrůžkou jiné téžké újmy spatřovat. K tomu bych uvedl například usnesení Nejvyššího soudu ČR ze dne 15.06.2011, sp. zn. 8 Tdo 612/2011, které jinou těžkou újmu pojímá jako neoprávněné jednání pachatele, který hrozí způsobením následků obdobné intenzity jako u pohrůžky násilí a mohou tedy u člověka vyvolat srovnatelnou obavu např. o svoje zdraví či život. Z tohoto důvodu Nejvyšší soud vyjmenovává okolnosti, které jsou nutné zohlednit při posuzování, zda jde o jinou těžkou újmu. K tomu uvádí například míru narušení osobních, rodinných či pracovních poměrů napadeného, dále k jeho vyspělosti či intenzitě ovlivnění jeho duševního stavu. To je dáno zejména různorodostí projevů u jednotlivých napadených osob. Pokud jde o subjektivní stránku vydírání, pak je potřeba, aby se jednalo o úmyslné zavinění (§ 15 TZ).[167]

Kvalifikovaná skutková podstata vydírání ukládá možnost vyšší výměry trestu odnětí svobody tomu, kdo spáchá trestný čin vydírání se zbraní (§ 175 odst. 2 písm. c) TZ). Výše jsem se zabýval i tím, zda může být zbraní počítač, či jiné zařízení, případně malware. Z legálního hlediska jsem však nenašel východisko, které by mohlo označit i škodlivý software za zbraň, resp. samotný počítač, pokud jej budu užívat běžným způsobem[168]. Judikatura mlčí a zrovna tak i právní teorie.

[166] Podle Šámala se násilím rozumí: „*použití fyzické síly k zamezení nebo překonání kladeného nebo očekávaného odporu*“, k tomu dále ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 1751 a DRAŠTÍK, Antonín. Trestní zákoník: komentář. Praha: Wolters Kluwer, 2015. Komentáře Wolters Kluwer. Kodex. ISBN 978-80-7478-790-4, s. 1752

[167] K tomu též ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 1751 a DRAŠTÍK, Antonín. Trestní zákoník: komentář. Praha: Wolters Kluwer, 2015. Komentáře Wolters Kluwer. Kodex. ISBN 978-80-7478-790-4, s. 1754

[168] Např. nebudu jej po někom házet, nebo jím nebudu někoho mlátit.

Je proto nutné vyjít z toho, že trestný čin lze spáchat se zbraní pouze, pokud směřuje proti lidského tělu (k tomu srov. § 118 TZ). Trestní zákoník nicméně nedefinuje zbraň zcela kategoricky a dává jistý prostor pro jiné interpretace. To vychází z formulace: *„…pokud z jednotlivého ustanovení trestního zákona nevyplývá něco jiného, …“*. Je otázkou, zda může pachatel spáchat ryze počítačové trestné činy uvedené v §§ 230 až 232 bez užití počítače či jiného zařízení. Problematika pojetí zbraně, je dle mého názoru s ohledem na kybernetické trestné činy složitá a osobně se domnívám, že použití exploitů za účelem získání prospěchu (nejčastěji majetkového), by mělo být považováno za spáchání trestného činu se zbraní. Naopak odcizení dat za použití flash disku, za předpokladu, že pachatel nebude překonávat odpor kladený bezpečnostním systémem, nepovažuji za čin spáchaný se zbraní.

Ransomware tedy zablokuje přístup do počítače, nebo zašifruje důležité dokumenty, nebo se vydává za složku veřejné moci a nutí jiného, aby něco konal (typicky zaplatil výkupné nebo falešnou pokutu). Původcem ransomware je vždy pachatel, ať už si ransomware obstaral od tvůrce (*Ransomware as a Service, zkráceně RaaS*[169]) nebo je jím on sám. Pachatel tedy pouze využívá komunikační sítě, aby se spojil s obětí a za pomoci škodlivého softwaru vyžaduje zaplatit výkupné.

Výkupné představuje pro pachatele určitý prospěch (§ 138 TZ). Pachatel, který ke svému obohacení užil ransomware se tak může dopustit i kvalifikované verze vydírání podle odstavce druhého (§ 175 odst. 1, 2 písm. d) TZ), a dokonce i podle odstavce třetího, pokud způsobí takovým činem škodu velkého rozsahu (§ 175 odst. 1, 3 písm. c) TZ). Trestní zákoník pak stanoví značnou škodu (v případě druhého odstavce) na 500 000,- Kč a škodu velkého rozsahu na 5 000 000,- Kč (k tomu § 138 TZ).

Pro úplnost dodávám, že příprava u trestného činu vydírání je trestná právě ve třetím a čtvrtém odstavci. K tomu uvádím § 20 odst. 1 TZ, který rozumí přípravou jednání záležející v úmyslném vytváření podmínek pro zvlášť závažný zločin (§ 14 odst. 3 TZ) a to za předpokladu, že to trestní zákon u příslušného trestného činu výslovně stanoví a dosud nedošlo k pokusu ani dokonání činu. Lze tedy postihnout i samotné opatření si ransomware (viz RaaS) za účelem spáchání vydírání ve třetím odstavci.

[169] Jde o ransomware v pojetí služby nebo zboží. Pachatelé si mohou ransomware zakoupit, typicky na Dark Webu, resp. Darknet Markets, které jsou součástí Deep Webu. Darknet má skrytou IP adresu, avšak je veřejnosti přístupný, na rozdíl od temnější části Deep Webu, kde je zapotřebí speciálních prohlížečů (např. TOR). K tomu více: SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 81-83

Nakonec nelze opomenout, že ransomware se typicky páchá jako pokračující trestný čin (§ 116), neboť dílčí útoky jsou vedeny jednotným záměrem, naplňují skutkovou podstatu stejného trestného činu (byť i v souhrnu) a jsou spojeny stejným nebo obdobným způsobem provedení a rovněž časovou souvislostí a souvislostí v předmětu útoku. Škody způsobené pokračováním vydírání se sčítají, neboť všechny dílčí útoky z pohledu hmotněprávního tvoří jediné jednání s jediným následkem.[170]

Nutné je taktéž poznamenat, že ne každé vydírání spáchané prostřednictvím internetu musí být ve formě ransomware. Laická veřejnost se v této souvislosti zmiňuje o virtuálních trestných činech, které například Gřivna označuje zčásti za činy, jež se řadí do skupiny tradičních trestných činů, které lze v nímat i mimo souvislost s virtuálním světem.[171] Do této kupiny se tak řadí i trestný čin vydírání. Proto například v oblasti MMORPG (*Massively Multiplayer Online Role Playing Games*[172]) docházelo a stále dochází k jednání, jež lze kvalifikovat jako vydírání (např. „nezabiju tvou postavu, když mi zaplatíš výpalné“), a které může mít dopady i v reálném světě (např. krádež účtu s postavou a požadování výpalného v reálné měně pro vrácení postavy). Takové jednání je však běžnou formou vydírání za užití internetu a lze jej plně postihovat na základě trestního zákona.

Nelze taktéž pominout stále se rozvíjející jev, který lze lehce zaměnit s problematikou ransomware. Jde o jednání, jež vykazuje známky, že se jedná o ransomware, ačkoliv chybí určité podstatné znaky. NKCB výkonná složka NÚKIB vydala 4.4.2019 zprávu o novém typu vyděračského mailu.[173] Jedná se o situaci, kdy pachatel tvrdí, že infikoval zařízení poškozeného, který obdržel mail, a to proto, že umístil malware na webové stránky s pornografickým materiálem, které měl poškozený navštívit. Pachatel v tomto případě dále tvrdí, že naboural i webovou kameru a zachycuje masturbaci oběti. Zároveň vyhrožuje oběti tím, že pokud jí do 48 hodin nezaplatí požadovanou částku, odešle inkriminované video všem jeho kontaktům včetně kolegům z práce (viz obrázek č. 5).

---

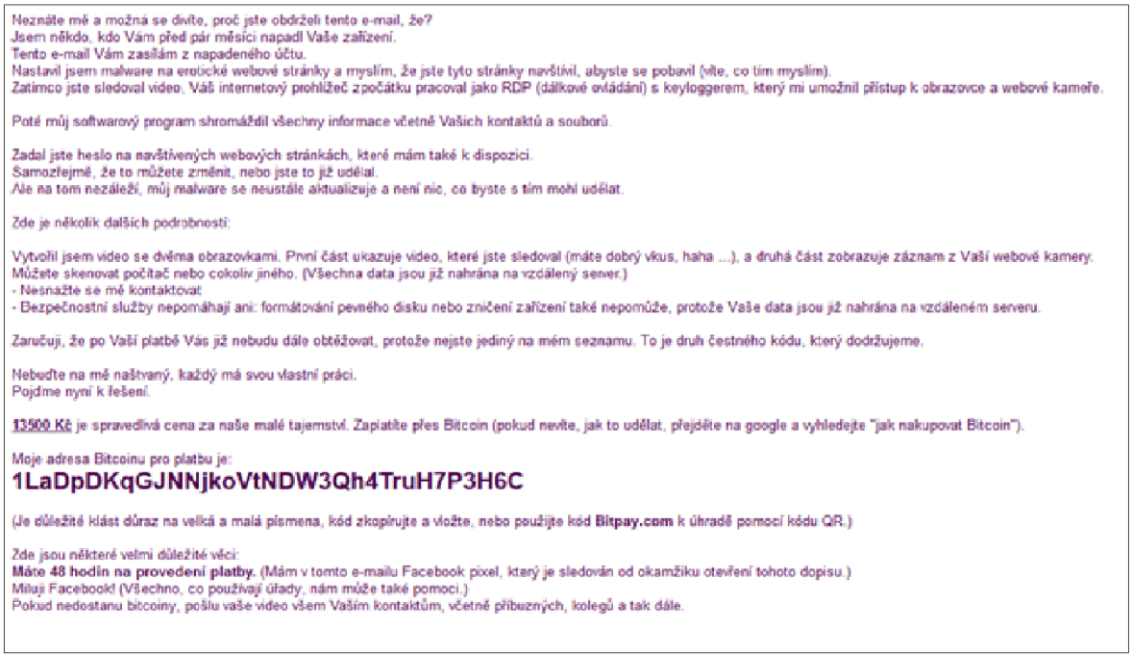
[170] JELÍNEK, Jiří, Katarína TEJNSKÁ, Jana TLAPÁK NAVRÁTILOVÁ, Vladimír PELC, Jiří ŘÍHA a Vojtěch STEJSKAL. Trestní právo hmotné: obecná část, zvláštní část. 6. aktualizované a doplněné vydání. Praha: Leges, 2017. Student. ISBN 978-80-7502-236-3, s. 151

[171] GŘIVNA, Tomáš. Existují virtuální trestné činy? In: GŘIVNA, Tomáš a Marie VANDUCHOVÁ, ed. Pocta Otovi Novotnému k 80. narozeninám [online]. Praha: ASPI, Wolters Kluwer, 2008, s. 28-35. ISBN 978-80-7357-365-2, s. 34

[172] Nelze podat doslovný překlad, ale jde o počítačové hry, které jsou typické tím, že se jich účastní vysoký počet hráčů (fungují prostřednictvím internetu), kteří se mohou volně pohybovat ve virtuálním prostoru, který má vlastní měnu (vlastní ekonomiku) a to vše v reálném čase.

[173] Varování před novým podvodným vyděračským e-mailem. Govcert.cz [online]. 4. 4. 2019 [cit. 2019-04-15]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2693-varovani-pred-novym-podvodnym-vyderacskym-e-mailem/

V takovém případě se nejedná o ransomware. Pachatel pouze vyvolává v poškozeném dojem, že užil malware. Jde tedy o jednání naplňující znaky jak trestného činu podvodu (viz následující kapitola), tak trestného činu vydírání a lze tak uvažovat o jednočinném souběhu nestejnorodém (viz dále). Jinými slovy nelze pachatele postihovat za ryze počítačové delikty.


Nezná te mě a možná se divíte, proč jste obdrželi tento e-mail, že?
Jsem někdo, kdo Vám před pár měsíci napadl Vaše zařízení.
Tento e-mail Vám zasílám z napadeného účtu.
Nastavil jsem malware na erotické webové stránky a myslím, že jste tyto stránky navštívil, abyste se pobavil (víte, co tím myslím).
Zatímco jste sledoval video, Váš internetový prohlížeč zpočátku pracoval jako RDP (dálkové ovládání) s keyloggerem, který mi umožnil přístup k obrazovce a webové kameře.

Poté můj softwarový program shromáždil všechny informace včetně Vašich kontaktů a souborů.

Zadal jste heslo na navštívených webových stránkách, které mám také k dispozici.
Samozřejmě, že to můžete změnit, nebo jste to již udělal.
Ale na tom nezáleží, můj malware se neustále aktualizuje a není nic, co byste s tím mohl udělat.

Zde je několik dalších podrobností:

Vytvořil jsem video se dvěma obrazovkami. První část ukazuje video, které jste sledoval (máte dobrý vkus, haha ...), a druhá část zobrazuje záznam z Vaší webové kamery.
Můžete skenovat počítač nebo cokoliv jiného. (Všechna data jsou již nahrána na vzdálený server.)
- Nesnažte se mě kontaktovat
- Bezpečnostní služby nepomáhají ani: formátování pevného disku nebo zničení zařízení také nepomůže, protože Vaše data jsou již nahrána na vzdáleném serveru.

Zaručuji, že po Vaší platbě Vás již nebudu dále obtěžovat, protože nejste jediný na mém seznamu. To je druh čestného kódu, který dodržujeme.

Nebuďte na mě naštvaný, každý má svou vlastní práci.
Pojďme nyní k řešení.

13560 Kč je spravedlivá cena za naše malé tajemství. Zaplaťte přes Bitcoin (pokud nevíte, jak to udělat, přejděte na google a vyhledejte "jak nakupovat Bitcoin").

Moje adresa Bitcoinu pro platbu je:
1LaDpDKqGJNNjkoVtNDW3Qh4TruH7P3H6C

(Je důležité klást důraz na velká a malá písmena, kód zkopírujte a vložte, nebo použijte kód Bitpay.com k úhradě pomocí kódu QR.)

Zde jsou některé velmi důležité věci:
Máte 48 hodin na provedení platby. (Mám v tomto e-mailu Facebook pixel, který je sledován od okamžiku otevření tohoto dopisu.)
Miluji Facebook! (Všechno, co používají úřady, nám může také pomoci.)
Pokud nedostanu bitcoiny, pošlu vaše video všem Vašim kontaktům, včetně příbuzných, kolegů a tak dále.

Obr. č. 5: Vyděračský dopis. Zdroj: Varování před novým podvodným vyděračským e-mailem. Govcert.cz [online]. 4. 4. 2019 [cit. 2019-04-15]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2693-varovani-pred-novym-podvodnym-vyderacskym-e-mailem/

5.3. Ransomware a podvod (§ 209 TZ)

S fenoménem ransomware lze rovněž spojovat i trestný čin podvodu podle § 209 TZ. Tato kvalifikace však sebou může nést jisté aplikační problémy. Podvod se řadí mezi trestné činy proti majetku a hledali bychom ho tak v hlavě V. zvláštní části trestního zákoníku. Individuálním objektem je cizí majetek.[174] Objektivní stránka tohoto trestného činu spočívá v podvodném jednání. Pachatel tedy jedná tak, že jiného uvede v omyl, využije jeho omylu, případně mu zamlčí podstatné skutečnosti a to tak, že tím způsobí škodu nikoliv nepatrnou[175] na cizím majetku a sebe nebo jiného tím obohatí. Jak uvádí Šámal, podvodné jednání může směřovat i proti osobě odlišné od osoby poškozené.[176] Pokud jde o subjektivní stránku, pak je potřebné úmyslné zavinění.[177]

[174] K tomu též ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 2051
[175] Škoda nikoliv nepatrná představuje podle § 138 TZ škodu dosahující částky nejméně 5000,- Kč.
[176] ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 2052
[177] Vychází z principu odpovědnosti za zavinění; k tomu dále § 13 odst. 2 TZ.

Pachatelem může být, stejně jako je tomu u vydírání, vedle osoby fyzické i osoba právnická (§ 7 ZTOPO).

Kvalifikovat ransomware jako podvod lze za předpokladu, že známe jeho konkrétní druh. Nelze aplikovat § 209 trestního zákoníku, pokud se jedná o běžný ransomware útok ve formě šifrovací nebo zamykací. Smejkal se odvolává na usnesení Nejvyššího soudu ČR ze dne 30. 9. 2004, sp. zn. 11 Tdo 872/2004, v rámci něhož je třeba rozlišit trestný čin povodu od vydírání v kybernetickém prostoru.[178] Nejvyšší soud ČR tak v tomto případě uvedl, že u trestného činu podvodu není provedení majetkové dispozice důsledkem použitého násilí, pohrůžky násilí či jiné těžké újmy, ale podvodného jednání.

Soud dále uvedl, že vydíraná osoba na rozdíl od osoby podvedené jedná pod nátlakem. Z tohoto důvodu lze vyloučit dva výše zmíněné druhy ransomware. Nelze však zavrhnout aplikaci ustanovení trestního zákoníku o podvodu na policejní ransomware. S odkazem na výše zmíněný charakter tohoto druhu ransomware chci podotknout, že do kolize vstupují dvě možné kvalifikace, a to vydírání a podvod. Ačkoliv jsem již psal, že ransomware je typický tím, že vždy naplní skutkovou podstatu trestného činu vydírání, v případě policejního ransomware je situace komplikovanější.

Pro demonstraci musím zopakovat, že policejní ransomware se snaží podvodným jednáním vyvolat v poškozeném dojem, že ho kontaktoval orgán veřejné moci (např. Policie ČR). Čin je však dokonán až v momentě obohacení pachatele nebo jiné osoby[179], pokud tedy poškozený nezaplatí smyšlenou pokutu, dopustí se pachatel pouze pokusu podvodu podle § 21 odst. 1, § 209 odst. 1 TZ. Důkazem problému rozlišení, zda jde v případě policejního ransomware o vydírání nebo podvod, či jejich souběh, budiž i nejednotný a rozporuplný názor Smejkala, který ve starší publikaci své monografie zaujímá postoj inklinující ke kvalifikaci těchto trestných činů v jednočinném souběhu nestejnorodém[180], zatímco z publikace nové z roku 2018 není jeho postoj zcela zřetelný.[181]

Já se však domnívám, že vhodná je aplikace ustanovení o vydírání, byť připouštím, že je možný jednočinný souběh. Ustanovení § 175 TZ a § 209 TZ mají odlišné objekty (první chrání

[178] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 217-218
[179] ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 2058
[180] SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2, s. 149
[181] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 215-219

svobodu rozhodování a druhý cizí majetek), a proto nemám důvod tvrdit, že souběh není možný, avšak skutkovou podstatu § 175 TZ naplní policejní ransomware vždy, neboť je zapotřebí ve světle výše zmíněného rozhodnutí Nejvyššího soudu ČR vnímat trestní oznámení za účelem trestního stíhání jako pohrůžku jinou těžkou újmou.

K dokonání podvodu však nemusí dojít vždy, neboť je nutná součinnost poškozeného v podobě provedení platby za fiktivní prohřešky. Za předpokladu, že se poškozenému zobrazí policejní ransomware a ten se mu nepodvolí a požadovanou částku nezaplatí, pak by bylo možné uvažovat o vyloučení jednočinného souběhu. Například Johanovský poměřuje typovou závažnost trestného činu vydírání a podvodu a uvažuje o faktické konzumpci.[182] Právě i z důvodu typové závažnosti (pro trestný čin podvodu TZ stanovuje v prvním odstavci až 2 roky trestu odnětí svobody, kdežto u vydírání jsou to až 4 roky) je nutné připustit jednočinný souběh nestejnorodý, byť trestný čin podvodu je zde pouze ve stádiu pokusu.

Trestný čin podvodu může být spáchán rovněž v kvalifikované verzi například v případě recidivy (§ 209 odst. 2 TZ) nebo za předpokladu způsobení větší škody (odst. 3 téhož). Příprava je rovněž trestná v pátém odstavci, a to v souvislosti s usnadněním spáchání teroristického trestného činu. Pro úplnost dodávám, že je v případě kvalifikace policejního ransomware možné uvažovat i o souběhu výše zmíněných trestných činů s trestným činem přisvojení pravomoci úřadu (§ 328 TZ). Touto do úvahy připadající kvalifikací se zabývám v podkapitole 5.6.

O podvodném jednání však nelze pochybovat v případě scareware. Připomínám, že zařazení scareware do ransomware není úplně šťastné, neboť lehce podkopává teorii o vyděračském charakteru ransomware. Poškozený si v případě scareware přečte, že jeho počítačový systém byl napaden virem a je možné se ho zbavit nainstalováním „antivirového softwaru“. Stažení tohoto software je obvykle zdarma, aby poškozeného nalákalo svou výhodností, ve skutečnosti se však snaží vymámit z poškozeného peníze, neboť pro odstranění „viru“ je nutné si zaplatit. V tomto případě se domnívám, že je vhodné a na místě aplikovat ustanovení § 209 o podvodu, neboť poškozený má stále možnost svobodně se rozhodnout, zda využije antivir nabízený nebo od jiného poskytovatele. K tomu se přiklání i Johanovský.[183]

[182] JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware, 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D., s. 50-51
[183] Tamtéž, s. 44

5.4. Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ)

S problematikou správné trestněprávní kvalifikace ransomware je neodmyslitelně spjat trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 trestního zákoníku. Jedná se o ustanovení, které bylo přijato jako důsledek členství České republiky v Radě Evropy, jak se o tom zmiňuji výše v úvodní kapitole v souvislosti s přijetím Budapešťské úmluvy o počítačové kriminalitě. § 230 trestního zákoníku je tak výsledkem implementace čl. 2 (Neoprávněný přístup) Budapešťské úmluvy. Podle systematického řazení Budapešťské úmluvy lze Neoprávněný přístup subsumovat pod trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů.[184]

Předmětné ustanovení Úmluvy o počítačové kriminalitě však pouze vyzývá členské státy k přijetí opatření, které bude kriminalizovat úmyslný neoprávněný přístup k celému počítačovému systému nebo jeho části. Úmluva však v tomto ohledu dává státům jistou míru uvážení, zda budou kriminalizovat již samotný neoprávněný přístup, anebo teprve situaci, kdy dojde k neoprávněnému přístupu za překonání bezpečnostního opatření s úmyslem získat počítačová data nebo jiným nečestným úmyslem. Jinými slovy, Úmluva dává státům možnost ponechat netrestné jednání, které spočívá v přístupu k počítačovému systému za předpokladu, že tato osoba následně neprovede nějakou neplechu.

Česká republika se však rozhodla pro jistou kombinaci, neboť kriminalizuje neoprávněný přístup, pokud k němu došlo překonáním bezpečnostního opatření. Povinnost členských států EU kriminalizovat neoprávněný přístup k informačnímu systému, případně neoprávněné zasahování do informačních systémů či údajů vyplývá též ze směrnice Evropského parlamentu a Rady 2013/40/EU o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 205/222/SVV.

V § 230 trestního zákoníku nalezneme dvě skutkové podstaty, které vytyčují předmět ochrany. Odstavec první chrání důvěrnost počítačových dat a počítačového systému, a to včetně jejich částí, naproti tomu odstavec druhý chrání zejména integritu a dostupnost počítačových dat a systémů.[185] Pro přílišnou kazuičnost ustanovení se zabývám pouze jeho aspekty, které z hlediska ransomware považuji za relevantní.

[184] Kapitola II (Opatření, která mají být přijata na vnitrostátní úrovni), Část 1 (Trestní právo hmotné), Oddíl 1 (Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů, Článek 2 (Nezákonný přístup) Budapešťské úmluvy o počítačové kriminalitě 2001

[185] ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 2304

Podle Zelenky je bezpečnostním opatřením každé opatření, které je způsobilé plnit ochrannou funkci počítačového systému.[186] Uvádí též typické způsoby překonání bezpečnostního opatření, zejména pak překonání hesla, a to ať už jeho uhodnutím, užitím prolamovačů hesel nebo pomocí škodlivého kódu.[187] Právě malware v podobě ransomware je jedním z nežádoucích důsledků překonání bezpečnostního opatření. Ransomware tak může naplnit vedle skutkové podstaty vydírání i skutkovou podstatu trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1 TZ a to za předpokladu, že útok nebude dokončen.[188] Pachatel, který využívá ransomware tedy překoná bezpečnostní opatření (např. umístěním škodlivého kódu na webové stránky nebo jako přílohu mailu), a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části.

Pachatelem může být kdokoliv za naplnění obecných znaků trestného činu (tj. nevyžaduje se žádná zvláštní vlastnost, způsobilost nebo postavení ve smyslu § 114 TZ). O tom, že je přístup neoprávněný svědčí, že není povolen majitelem systému či držitelem práv k systému.[189] U útoku v podobě ransomware je jeho kriminalizace zcela na místě, neboť přístup k systému je jenom druhotným cílem pachatele. Ten se snaží zejména o majetkový prospěch a skutečnost, že neoprávněným přístupem k počítačovému systému naplnil skutkovou podstatu i jiného trestného činu, než původně zamýšlel, je mu cizí.

To může být problémem právě u hackerů, kteří naplní skutkovou podstatu podle § 230 odst. 1 TZ jenom z důvodů ověření svých znalostí a schopností. Gřivna[190] v této souvislosti například dodává, že vhodnost kriminalizace takového jednání by se měla omezit na průnik, který umožní spáchání jiného trestného činu, nebo je jeho součástí a připomíná i důležitost principu *ultima ratio*[191]. S tím mohu jedině souhlasit a poznamenat, že ransomware je právě případem, kdy průnik umožňuje spáchání jiného trestného činu a to vydírání, a proto je jeho kriminalizace vhodná.

Pro ransomware je však mnohem přiléhavější aplikace ustanovení § 230 odst. 2 příp. 3 TZ. Například Smejkal kvalifikuje jednání spočívající v odcizení dat a následném vydírání jako trestný

[186] DRAŠTÍK, Antonín. Trestní zákoník: komentář. Praha: Wolters Kluwer, 2015. Komentáře Wolters Kluwer. Kodex. ISBN 978-80-7478-790-4, s. 1477
[187] Tamtéž
[188] JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware, 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D., s. 47
[189] DRAŠTÍK, Antonín. Trestní zákoník: komentář. Praha: Wolters Kluwer, 2015. Komentáře Wolters Kluwer. Kodex. ISBN 978-80-7478-790-4, tamtéž
[190] GŘIVNA, Tomáš. Hlava V. Trestné činy proti majetku (§ 205 až § 323). In ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, 1973-2324, s. 2305
[191] Tresní právo je krajním prostředkem ochrany společnosti před kriminalitou, pokud se jiné prostředky ochrany jeví jako neúčinné (prostředek poslední instance = *ultima ratio*). S tím souvisí i zásada subsidiarity trestní represe uvedená v § 12 odst. 2 TZ

čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. a) TZ v jednočinném souběhu s trestným činem vydírání podle § 175 TZ.[192] Pachatel v tomto případě získá přístup k počítačovému systému nebo k nosiči informací a neoprávněně užije data uložené v počítačovém systému.

Osobně se domnívám, že by takto bylo vhodné kvalifikovat případ útoku policejního ransomware, protože pachatel využívá například fotky poškozeného, aby vzbudil dojem, že je složkou veřejné moci. Nejtypičtější je však pro ransomware útok kvalifikace podle § 230 odst. 2 písm. b) a to spolu s odst. 3 písm. a) a b) TZ. Ransomware totiž zamkne přístup do počítačového systému nebo zašifruje data. Tím se pachatel dopustí jednání, kterým získá přístup do počítačového systému a data uložená v počítačovém systému potlačí (zamezí přístupu k datům), a nebo je učiní neupotřebitelnými (zašifrováním).[193]

Vedle toho se pachatel obohatí, čímž naplní znaky kvalifikované skutkové podstaty § 230 odst. 3, písm. a) TZ, neboť výše zmíněným činem získá neoprávněný prospěch (ve formě výkupného) a rovněž může naplnit znaky uvedené v písmenu b) téhož, pokud úmyslně neoprávněně omezí funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat (malware sebou často přináší výrazné zatížení systému).

Nelze však vyloučit i odst. 4 a 5 téhož ustanovení například v případě, že pachatel získá prospěch značný či dokonce velkého rozsahu, zejména s ohledem na pokračování v trestném činu.[194] Ustanovení kvalifikovaných skutkových podstat o způsobení škod rovněž nelze opomenout, neboť ransomware může útočit i na veřejné instituce (např. nemocnice), kde je způsobení značných škod a vyšších škod průvodním jevem.[195] Nadto lze uvést, že souběh § 230 odst. 1 s odst. 2 TZ je obecně vyloučen pro poměr subsidiarity.[196] Pro úplnost uvádím, že souběh je taktéž vyloučen i v případě trestného činu neoprávněného přístupu k počítačovému systému a

[192] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 553
[193] K vysvětlení pojmů potlačení a učinění dat neupotřebitelnými srov. též: DRAŠTÍK, Antonín. Trestní zákoník: komentář. Praha: Wolters Kluwer, 2015. Komentáře Wolters Kluwer. Kodex. ISBN 978-80-7478-790-4, s. 1478
[194] Tj. ve smyslu § 138 odst. 2 TZ 500 000,- Kč v případě značného prospěchu a 5 000 000,- Kč v případě prospěchu velkého rozsahu.
[195] Srov. též: JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware, 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D., s. 47
[196] KRUPIČKA, Jiří. Trestněprávní a kriminologické aspekty internetové kriminality. Praha, 2012. Disertační práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Prof. JUDr. Jiří Jelínek, CSc., s. 88-89

nosiči informací s trestným činem poškození cizí věci podle § 228 TZ a nebo s neoprávněným užíváním cizí věci podle § 207 TZ a to z důvodu poměru speciality.[197]

Zvláštností je opět kvalifikace ransomware ve formě scareware. Zde je vhodné poznamenat, že scareware se snaží dostat do počítačového systému tím, že bude stažen falešný antivirový software. Pokud k takovému jednání nedojde, pak se ani nenaplní skutková podstata § 230 TZ. Nicméně nelze plně vyloučit, že by v takovém případě nedošlo alespoň k pokusu, neboť pachatel umístil na webové stránky škodlivý kód a formou pop up oken došlo k přesměrování poškozeného na stránky obsahující malware. Tedy jednání směřovalo k dokonání trestného činu a pachatel se jej dopustil v úmyslu trestný čin spáchat, přičemž k dokonání činu nedošlo. Přípravu bych spatřoval v obstarání si ransomware ke spáchání trestného činu podle § 230 TZ, avšak v tomto případě dotčený paragraf neumožňuje trestní odpovědnost za přípravu, nehledě na možnost aplikace § 231 TZ.

Naopak k naplnění skutkové podstaty předmětného ustanovení by došlo, pokud by poškozený stáhnul a nainstaloval falešný antivir. Ten často obsahuje i jiné malware jako je adware nebo spyware a otevírají se tak široké možnosti pro trestněprávní postih. K tomu též Kolouch uvádí, že pokud pachatel využije k překonání bezpečnostního opatření právě malware, který bude do počítačového systému nainstalován, byť poškozeným, lze to považovat za zásah do počítačového systému a posuzovat tak podle § 230 odst. 2 písm. d) TZ. Pachatel totiž kromě získání přístupu k počítačovému systému přinejmenším neoprávněně vkládá data do počítačového systému.

5.5. Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ)

Trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 trestního zákoníku se řadí mezi ryze počítačové trestné činy. Netřeba snad znovu připomínat, že taková kazuistická úprava byla přijata v souvislosti s Úmluvou o kybernetické kriminalitě, která ve svém článku 6 zavazuje ke kriminalizaci zneužívání zařízení. To spočívá v úmyslné a neoprávněné výrobě, prodeji, opatření za účelem zpřístupnění zejména zařízení včetně počítačového programu s cílem spáchat kybernetický trestný čin Úmluvou předvídaný (čl. 2–5), anebo zpřístupnění hesla, případně jiných dat umožňujících přístup do

[197] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. Trestní právo. 2010, 14(7-8), 19-43. ISSN 1211-2860.

počítačového systému nebo jeho části. Z důvodu rozsahu této práce a jejímu celkovému záběru se budu tímto trestným činem zabývat pouze co do nejdůležitějších aspektů ve vztahu k ransomware.

Objektem trestného činu je v případě § 231 TZ *„zájem na ochraně společnosti a osob před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků“* určených ke spáchání tresných činů uvedených v § 182 odst. 1 písm. b), c) nebo § 230 odst. 1, 2 TZ.[198] Zvláštností je u § 231 skutečnost, že z materiálního hlediska kriminalizuje přípravné jednání a z toho důvodu se jedná o předčasně dokonaný trestný čin.[199] Objektivní stránka zahrnuje celou řadu jednání, která se kriminalizují, avšak obecně s přihlédnutím k problematice ransomware směřují k trestněprávnímu postihu toho, kdo si pořídí škodlivý sofware (ransomware), který mu zajistí neoprávněný přístup do počítačového systému. Forma jednání je komisivní a následek je poruchový.[200] Ustanovení § 231 obsahuje jednu základní skutkovou podstatu a dvě kvalifikované.

Základní skutková podstata má kumulativní charakter a musí být splněny všechny znaky, které ji tvoří, a to úmysl spáchat některý z trestných činů uvedených v § 182 odst. 1 písm. b), c) nebo § 230 odst. 1, 2 TZ a jednání, které tvoří objektivní stránku trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Subjektivní stránku tvoří jednání úmyslné (§ 13 odst. 2 TZ), přičemž u okolnosti podmiňující použití vyšší trestní sazby (§ 231 odst. 2 nebo 3) postačí nedbalostní jednání. Pachatelem může být opět kdokoliv (fyzická i právnická osoba) stejně jako u § 230 TZ (viz výše).

Z hlediska ransomware je § 231 TZ významný, neboť kriminalizuje jednání pachatele, který si zakoupil ransomware, a to jako službu (*Ransomware as a Service*). Rovněž ale kriminalizuje jednání i toho, kdo Ransomware as a Service nabízí, případně i tvůrce ransomware. U tvůrce postačí i úmysl enventuální, neboť pachatel musel být srozuměn, že ransomware, který vytvořil bude s největší pravděpodobností využit ke spáchání alespoň § 230 odst. 1 nebo 2 TZ.[201] Kolouch rovněž upozorňuje na důležitost naplnění fakultativního znaku subjektivní stránky trestného činu, a to motivu spočívajícím v úmyslu spáchat některý ze, skutkovou podstatou vyjmenovaných, trestných činů.[202] Kriminalizace samotného držení prostředků uvedených

[198] ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 2317
[199] ŠÁMAL, Pavel a kol. 2012, tamtéž
[200] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf, s. 358
[201] K tomu srov. VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. Trestní právo. 2010, 14(7-8), 19-43. ISSN 1211-2860.
[202] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf, s. 359

v základní skutkové podstatě pod písmeny a) a b) by mohla zabránit činnosti vedoucí k pokroku v oblasti technologií, vývoji nových aplikací nebo činností expertů na kybernetickou bezpečnost, včetně vývoji antivirových software.

5.6. Ransomware a další do úvahy připadající kvalifikace

Vedle výše zmíněných trestněprávních kvalifikací ransomware lze uvažovat, možná spíše de lege ferenda, o dalším možném kvalifikování. Ransomware se projevuje v několika verzích, jak již bylo popsáno, a s touto různorodostí útoků ransomware je spojena i řada variant jejich trestněprávních postihů. Možnosti kvalifikace, které jsem již zmínil, jsou nejspíše nejčastější a nejočekávanější, avšak někdy taková kvalifikace může být značně omezující a nepopíše skutek dostatečně.

Je nutné poznamenat, že dále uvedené možnosti sumbsumpce určitého jednání spojeného s útokem ransomware pod ustanovení trestního zákoníku, vystupují především jako souběhy s trestným činem vydírání. Pro zjednodušení budu uvádět jednotlivé trestné činy, s kterými lze různé projevy ransomware spojovat samostatně, avšak je nutné si tyto individuální skutkové podstaty představit v souběhu zejména s trestným činem vydírání. Souběhy se detailněji zabývá například Johanovský[203] nebo Krupička[204].

Šifrovací a zamykací ransomware se může projevit jako trestný čin obecného ohrožení podle § 272 TZ. S ohledem na historický vývoj ransomware lze jmenovat zejména vůbec první útok ransomware Trojan AIDS a pravděpodobně nejmasivnější útok WannaCry. Oba ransomware útoky byly směřovány proti lékařským institucím. Zejména WannaCry ransomware ve Velké Británii směřoval mimo jiné na nemocnice a jejich počítačové systémy, což vyvrcholilo k odmítání pacientů, a dokonce i k přerušení naplánovaných operací.[205]

Trestného činu obecného ohrožení podle § 272 TZ se dopustí ten, *„…kdo úmyslně způsobí obecné nebezpečí tím, že vydá lidi v nebezpečí smrti nebo těžké újmy na zdraví nebo cizí majetek v nebezpečí škody velkého rozsahu…“*. Domnívám se, že zamezení přístupu do počítačů a systémů, na kterých je zdravotnické zařízení závislé, naplňuje znaky skutkové podstaty trestného činu

[203] JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware, 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D., s. 49-52
[204] KRUPIČKA, Jiří. Trestněprávní a kriminologické aspekty internetové kriminality. Praha, 2012. Disertační práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Prof. JUDr. Jiří Jelínek, CSc., s. 88 a n.
[205] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7, s. 214 nebo UK hospitals hit with massive ransomware attack. Theverge.com [online]. [cit. 2019-03-25]. Dostupné z: https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

obecného ohrožení. Nelze vyloučit i situaci, kdy ransomware útok bude směřován proti systémům složek dopravní infrastruktury. Například útok proti řídícímu počítačovému systému pro řízení letového provozu. V tomto případě lze uvažovat i o naplnění skutkové podstaty trestného činu poškození a ohrožení provozu obecně prospěšného zařízení. § 132 taxativně vymezuje[206], co se rozumí obecně prospěšným zařízením, přičemž námi popsanou situaci lze podřadit pod napadení zařízení pro veřejnou dopravu.

Uvažovat lze i o aplikaci ustanovení trestního zákoníku o poškození cizí věci podle § 228 TZ. Stačí, aby pachatel učinil cizí věc neupotřebitelnou, což se zamknutím či zašifrováním počítače zpravidla stává, a způsobil tak na cizím majetku škodu nikoli nepatrnou. Pachatel může vést útok ransomware nejen proti počítači, ale taktéž proti jiným zařízením jako jsou mobilní telefony, tablety, autonomní automobily, smart home spotřebiče, fotoaparáty a mnoho dalších zařízení, které jsou napojené na internetovou síť.

Významná je z hlediska teoretického i úvaha o aplikaci ustanovení § 328 TZ o přečinu[207] přisvojení pravomoci úřadu. Tato kvalifikace připadá v úvahu u policejního ransomware. Pachatel se de facto vydává za orgán veřejné moci, respektive za Policii ČR, avšak objektivní stránka trestného činu přisvojení pravomoci úřadu vyžaduje, aby byly neoprávněně vykonávány úkony, které jsou vyhrazeny mimo jiné i orgánu státní správy, či jinému orgánu veřejné moci. Jak správně, alespoň dle mého názoru, poznamenává Johanovský[208], se znakem neoprávněného výkonu úkonu (v našem případě Policie ČR) přichází jisté interpretační a aplikační obtíže. Pachatel, který k útoku využil policejní ransomware neužívá prostředků, které má Policie ČR k dispozici, pokud by vedla trestní, nebo správní řízení proti (v našem případě) poškozenému (napadenému ransomware).

Z těchto důvodů je aplikace § 328 TZ komplikovaná a je nutné se na základě současné právní úpravy přiklonit spíše k její neaplikaci v případě policejního ransomware. Pachatel se tedy domnívá, že páchá přečin přisvojení pravomoci úřadu, neboť si je vědom toho, že on sám není policistou, avšak pro účely spáchání jiného trestného činu (například podvodu, nebo vydírání) užívá prostředků, ke kterým Policie ČR nemá pravomoc (dostane se do cizího systému, aby oznámila spáchání trestného činu a umožňuje vykoupení ve formě pokuty). S tím je spojena skutečnost, že pachatel páchá v negativním právním omylu o normativních znacích skutkové

[206] K taxativnímu vymezení pojmu obecně prospěšného zařízení viz například: ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 2804
[207] Trestný čin přisvojení pravomoci úřadu podle § 328 TZ je na základě jeho trestní sazby odnětí svobody (až dvě léta) ve smyslu § 14 odst. 2 TZ přečinem.
[208] JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware, 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D., s. 45

podstaty trestného činu přisvojení pravomoci úřadu (posuzuje se podle zásad určených pro negativní omyl skutkový - § 18 odst. 1 TZ).[209] Přisvojení pravomoci úřadu je však trestným činem úmyslným (§ 13 odst. 2 TZ), a proto by bylo nutné za těchto okolností vyloučit trestní odpovědnost pachatele.[210]

Často se v souvislosti s kyberkriminalitou mluví i o kyberterorismu[211]. Domnívám se tedy, že nelze vyloučit ani možnost aplikace § 312f trestního zákoníku (trestný čin vyhrožování teroristickým trestným činem) v případě, kdy má ransomware sloužit jako pohrůžka kybernetickým útokem širšího rozsahu pod podmínkou, že nebude uhrazena určitá částka, ta pak může sloužit jako prostředek pro financování terorismu (§ 312d TZ). V případě ransomware by byla splněna i podmínka pro aplikaci kvalifikované skutkové podstaty zvlášť závažného zločinu vyhrožování teroristickým trestným činem podle § 312f odst. 1, 2 písm. b) TZ, neboť by bylo vyhrožováno za užití veřejně přístupné počítačové sítě.

Nelze ovšem vyloučit i jinou teroristickou činnost[212] zejména teroristický útok podle § 311 TZ, kde se pachateli nabízí široká možnost způsobu provedení trestného činu. S novelou trestního zákoníku provedené zákonem č. 287/2018 Sb. účinné od 1. 2. 2019 byla rozšířena možnost trestní kvalifikace kybernetického útoku, která svou povahou představuje teroristický útok a to v § 311 odst. 1 písm. e) TZ. S ohledem na výše zmíněné nelze vyloučit ani tuto možnost právní kvalifikace útoku ransomware. Dle důvodové zprávy tak došlo z důvodu naplnění požadavků vyplývajících z ust. čl. 3 směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV.[213]

6. Procesněprávní otázky problému stíhání ransomware

S problematikou ransomware souvisí bezpochyby i otázka jeho trestního postihu. K tomu by nicméně nedošlo, kdyby orgány činné v trestním řízení neměly možnost obstarat si dostatek

[209] ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5, s. 3141

[210] O tom, že omyl skutkový negativní vylučuje trestní odpovědnost za úmyslný trestný čin viz např.: JELÍNEK, Jiří, Katarína TEJNSKÁ, Jana TLAPÁK NAVRÁTILOVÁ, Vladimír PELC, Jiří ŘÍHA a Vojtěch STEJSKAL. Trestní právo hmotné: obecná část, zvláštní část. 6. aktualizované a doplněné vydání. Praha: Leges, 2017. Student. ISBN 978-80-7502-236-3, s. 244-245

[211] Např. RADEMACHEROVÁ, Kristina. Počítačová kriminalita: Vybrané aspekty postihu v mezinárodním prostředí [online]. 2017 [cit. 2019-02-07]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/186324. Vedoucí práce Jiří Jelínek, s. 56-57

[212] Legální definice teroristické trestné činnosti tkví v § 129a odst. 1 TZ.

[213] Vládní návrh zákona č. 287/2018 Sb., kterým se mění z. č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony (sněmovní tisk 79/0, část č. 1/6)

důkazů k usvědčení pachatele. Vzhledem k rozsahu a obsahové stránce diplomové práce se nicméně zabývám pouze určitou výsečí, která souvisí s trestněprocesní úpravou vztahující se k stíhání ransomware. Je taktéž zcela nepochybné, že záležitosti spojené například s vyšetřováním kybernetické kriminality jsou spojeny s aplikovaným vědním oborem, jakým je kriminalistika[214].

V následujících podkapitolách se tedy zabývám pouze určitými zvláštnosti, které jsou spjaté s trestním řízením a rozsahově tak adekvátně nepokrývají část hmotněprávní. Jsem názoru, že problematika trestního řízení v předmětné oblasti otázky ransomware, zejména jeho přípravná část, je zacílena právě na zvláštní kriminalistické vědní disciplíny a jde tak nad rámec celé práce, která má za cíl reflektovat kromě hmotněprávní kvalifikace ransomware i kriminologické aspekty tohoto fenoménu. Následující kategorie jsou tak spíše dokreslující a vyjádřené spíše na okraj.

6.1. Zvláštnosti dokazování

Prostředí kyberprostoru je mimo jiné známé pro svou anonymitu. Pachatelé se jí snaží využít, neboť mají pocit, že se tak dokonale skryjí před hrozící sankcí. Ve skutečnost však nemusí vždy odstranit všechny stopy. Právě v tuto chvíli nastupují na řadu počítačoví experti, kteří v závislosti na způsobu vedení útoku vystopují pachatele, nebo nikoliv. Výsledek tak může být významně ovlivněn činností vyšetřovacích týmů v oblasti kybernetické bezpečnosti (např. Národní/Vládní CERT, týmy CSIRT[215]), ale zejména odborníků, kteří působí na krajských odborech kriminalistické techniky a expertiz[216].

Problémů spojených s řízením je však nespočet nejen při vyšetřování, ale právě i se samotnými důkazy. Digitální stopy jsou charakteristické svou objemností, nízkou životností, vysokou geografickou rozptýleností, ale i svou typickou dynamičností.[217] Vedle toho je obecně pro kyberkriminalitu typická vysoká míra latence, což opět nemusí svědčit úspěchu celého vyšetřování.[218]

Ransomware má jednak mnoho podob, ale i vícero vektorů útoku. Všechny tyto skutečnosti mohou hrát ve vyšetřování svou významnou roli. Například ze skutečnosti, že oznámení o

[214] Ta na rozdíl od kriminologie zkoumá zejména zákonitosti vzniku stop.
[215]Národní, Vládní CERT (*Computer Emergency Response Team*) a CSIRT (*Computer Security Incident Response Team)* jsou týmy zajišťující kybernetickou bezpečnost podle zákona o kybernetické bezpečnosti.
[216] Ačkoliv patří kriminalistická počítačová expertíza k těm nejmladším, tak byla založena už v roce 1993 při Kriminalistickém ústavu Praha (viz: Expertizní obory. Www.policie.cz [online]. [cit. 2019-05-28]. Dostupné z: https://www.policie.cz/clanek/celorepublikove-utvary-kriminalisticky-ustav-praha-zpravodajstvi-test-4.aspx?q=Y2hudW09Mw%3d%3d)
[217] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2, s. 251
[218] POLČÁK, Radim a Tomáš GŘIVNA. Kyberkriminalita a právo. 1. vyd. Praha: AUDITORIUM, 2008. 220 s. Auditorium. ISBN 978-80-903786-7-4, s. 78

požadovaném výkupném obsahuje gramatické chyby, lze vyvodit jednak závěr o tom, že pachatel je cizinec, nebo že si ransomware obstaral (RaaS), případně jde o osobu s nižším vzděláním. K tomu, aby byl pachatel buďto usvědčen nebo ospravedlněn, slouží jednotlivé důkazy. Ty je potřeba získat za pomocí důkazních prostředků. Dle § 89 odst. 2 TŘ může za důkaz sloužit vše, co může přispět k objasnění věci. Byť trestní řád příkladmo vyjmenovává typické důkazní prostředky, nutno při objasnění kybernetické trestné činnosti využít i prostředků jiných, speciálních. Nositeli těchto důkazů jsou tak typicky počítače, případně datové nosiče.[219] Jejich zajištění ve smyslu § 78 (předložení a vydání věci) a § 79 (odnětí věci) TŘ a následná digitální kriminalistická expertíza, však není jediným postupem orgánů činných v trestním řízení vedoucí k získání důkazů.

Jako vhodný důkazní prostředek se jeví i záznam telekomunikačního provozu (zejm. vztahující se na emailovou komunikaci, nebo chatovací či jiné komunikační služby jako je Facebook, Messenger, Skype a jiné) ve smyslu § 88a TŘ, který se používá zejména se zajištěním provozních a lokalizačních údajů[220]. Je však nutné rozlišovat takovýto záznam od jednorázového zajištění dat ve schránkách těchto komunikačních služeb, neboť pak je nutné uplatnit režim podle § 158d odst. 3 TŘ, který představuje operativně pátrací prostředek orgánů činných v trestním řízení sledováním osob a věcí[221] a vyžaduje souhlas soudce, případně toho, do jehož práv a svobod je sledováním zasahováno (odst. 6 téhož ust. TŘ).

Významné u útoku ransomware může být i poskytnutí informace u ISP. Rozlišujeme opět dva režimy, a to podle dožádaného poskytovatele. Podle z. č. 127/2005 Sb., o elektronických komunikacích, se může jednat o poskytovatele telekomunikačních služeb nebo poskytovatele služeb informační společnosti ve smyslu z. č. 480/2004 Sb., o některých službách informační společnosti.[222] Další dva režimy jsou pak navázány na charakter dat. Data, která nepodléhají povinnosti mlčenlivosti a nemají charakter dat, jež jsou zabezpečeny uživatelem (nejčastěji heslem), lze dožádat podle § 8 odst. 1 TŘ, v opačném případě se postupuje podle § 158d odst. 3 TŘ (viz výše).[223]

Méně časté je u ransomware těžení důkazů ze stop paměťových. Typicky získávání informací, resp. důkazů z výpovědí svědků. Svědky totiž můžeme mít pouze v podobě poškozených, zvláště, pokud se páchá distančně. Poškozených může být sice reálně mnoho, avšak počet osob, které útok nahlásí je zpravidla, vzhledem k rozsahu škod, malý. Přitom právě počet

[219] POLČÁK, Radim a Tomáš GŘIVNA. 2008, tamtéž, s. 90
[220] POLČÁK, Radim a kol. 2015, tamtéž, s. 107-108 a § 90 a 91 z. č. 127/2005 Sb., o elektronických komunikacích
[221] POLČÁK, Radim a kol. 2015, tamtéž
[222] Tamtéž, s. 106
[223] Tamtéž, s. 107

nahlášených útoků může významným způsobem přispět k trasování pachatele. Nelze však výpověď svědků úplně zavrhovat a opomíjet, neboť stále se tento důkazní prostředek řadí mezi nejčastější a nejvýznamější. Ransomware je však specifický tím, že útočník se snaží využít anonymity prostředí, ve kterém páchá. Může tak zaútočit velice komplikovaným způsobem, využít několika serverů, používat transakce za pomoci virtuální měny, skrývat svou IP adresu (například formou cibulového směrování[224]), případně ji měnit, využívat cizí zařízení, vystupovat pod falešnými doklady a jinými způsoby se snažit zakrýt svou identitu, čímž se kriminalistům výrazně zhorší jejich výchozí postavení.

6.2. Některé otázky spjaté s distančním páchaním

Dalším problémem stíhání ransomware je možnost páchat tento typ tresné činnosti napříč státy. Ransomware totiž z povahy věci (může prakticky nepadnout kohokoliv, neboť se šíří prostřednictvím komunikační sítě) a zejména ze způsobu šíření může snadno opustit stát, ve kterém vzniknul, což sebou přináší jisté obtíže, se kterými se orgány činné v trestním řízení musí při vyšetřování potýkat. Místní působnost českého trestního zákoníku se vztahuje nejen na trestné činy spáchané na území České republiky, ale i mimo něj. Ustanovení trestního zákoníku se tak vztahují nejen na pachatele, který jednal v cizině a jehož následek nastal na území České republiky, ale i v případě opačném (§ 4 odst. 2 TZ). Obdobná úprava platí i pro účastenství (§ 4 odst. 3 TZ).

S tím je spojena nutnost jisté mezinárodní spolupráce. Například Walden zdůrazňuje ve spojitosti s kybernetickou kriminalitou důležitost spolupráce orgánů činných v trestním řízení v tuzemsku s těmi zahraničními.[225] Takováto spolupráce ve vztahu k ransomware pak spočívá zejména v předávání informací o druzích ransomware, výskytu, napadených objektech či o výší škody. Z taktických důvodů však Policie ČR tyto informace nezveřejňuje.[226]

Pro mezinárodní spolupráci v oblasti kyberkriminality, tedy i ransomware, platí již „zaběhlé“ mezinárodní úmluvy v oblasti trestního práva, jakými jsou například mnohostranné úmluvy sjednávané v rámci Rady Evropy (například Evropská úmluva o vzájemné pomoci ve věcech trestních ze dne 20. 4. 1959, včetně pozdějších dodatkových protokolů, případně Evropská úmluva o předávání trestního řízení z roku 1972), ale i úmluvy lidskoprávní na poli Rady Evropy

[224] Též *Onion routing* viz: ČIKOVSKÝ, Jan. Internetová a počítačová kriminalita [online]. 2013 [cit. 2019-05-27]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/117868. Vedoucí práce Tomáš Gřivna, s. 27-28
[225] WALDEN, Ian. Computer crimes and digital investigations. Oxford: Oxford University Press, 2007. ISBN 978-0-19-929098-7, s. 310
[226] Vyjádření Policejního prezidia PČR ze dne 14.02.2019 k žádosti o informace podle z. č. 106/1999 Sb., o svobodném přístupu k informacím

a OSN (například Evropská úmluva na ochranu lidských práv a základních svobod z roku 1950 a Mezinárodní pakt o občanských a politických právech z roku 1966).

Vedle těchto úmluv lze však jmenovat paralelně či samostatně působící již dříve zmíněnou Budapešťskou úmluvu o počítačové kriminalitě z roku 2001. Vztah Budapešťské úmluvy a ostatních mezinárodních úmluv o vzájemné justiční spolupráci pak upravují články 27 a 28 Budapešťské úmluvy, přičemž tato ustanovení cílí na situaci při neexistenci smluvního vztahu mezi státy. V opačném případě se ustanovení Budapešťské úmluvy považují za doplňující.[227]

Významná je pro české prostředí taktéž činnost Národní centrály proti organizovanému zločinu služby kriminální policie a vyšetřování, která kromě úkolů vyplývající z jeho postavení jakožto národního kontrolního bodu pro kybernetickou kriminalitu a národního kontrolního místa pro hlášení závadních aktivit v síti internet, plní taktéž, kromě metodické a technické podpory ostatních útvarů Policie ČR při potírání kyberkriminality, i funkci spolupráce se zahraničními policejními subjekty v této oblasti.[228] V této souvislosti je třeba se opět dotknout již jednou zmíněného projektu No More Ransom, který taktéž představuje formu spolupráce mezi zahraničními subjekty zejména v oblasti prevence před ransomware.

Významná je taktéž, s odkazem na předchozí podkapitolu, mezinárodní spolupráce v oblasti včasného zajištění digitálních důkazů. Budapešťská úmluva tak požaduje zřízení kontaktních míst, které budou nonstop (24 hodin, sedm dní v týdnu) k dispozici mezinárodním subjektům k zajištění příslušných elektronických důkazů. Tímto místem byl Českou republikou určen Odbor informační kriminality Úřadu služby kriminální policie a vyšetřování Policejního prezidia České republiky.[229]

Je tedy nutné poznamenat, že bez včasné reakce a efektivní spolupráce mezi státy, je sofistikovaný pachatel ransomware téměř nepostižitelný. Těžko si lze představit, že ransomware stvořený například v Japonsku, který se dostal přes Ruskou federaci do Evropy a následně vytvořil škodu ve třech evropských státech, by byl bez mezinárodní justiční spolupráce postižitelný.

[227] RADEMACHEROVÁ, Kristina. Počítačová kriminalita: Vybrané aspekty postihu v mezinárodním prostředí [online]. 2017 [cit. 2019-02-07]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/186324. Vedoucí práce Jiří Jelínek, s. 191

[228] Vyjádření Policejního prezidia PČR ze dne 14.02.2019 k žádosti o informace podle z. č. 106/1999 Sb., o svobodném přístupu k informacím

[229] RADEMACHEROVÁ, Kristina. 2017, tamtéž, s. 194; též Sdělení Ministerstva zahraničních věcí ČR o sjednání Úmluvy o počítačové kriminalitě, vyhlášené pod číslem 104/2013 Sb. m. s.

Analytická část

I. Metodologie

Cílem analytické části této práce je předložit prognózu dalšího vývoje páchání ransomware v následujících letech od roku 2019. Za tímto účelem jsem zvolil výzkumnou techniku analýzy policejní statistiky registrovaných skutků v ČR, spáchaných v prostředí internetu a jiných sítí, a to od roku 2016 do roku 2018. V rámci této analýzy vycházím z dat pořízených požádáním Policejního prezidia České republiky a Národního úřadu pro kybernetickou a informační bezpečnost o veškeré informace týkající se fenoménu ransomware s důrazem na statistiky počtu útoků ransomware podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Ani jedna z výše zmíněných institucí bohužel neposkytla blíže specifikované statistiky, neboť jejich evidence neexistuje. Policejní prezidium České republiky mi nicméně zaslalo informaci v podobě policejní statistiky registrovaných skutků spáchaných v prostředí internetu a jiných sítí, avšak informace zde uvedené trpí jistými nedostatky.

Předně je nutné poznamenat, že tato takticko-statistická klasifikace (dále jen *„TSK“*) zahrnuje trestné činy dle trestního zákoníku, avšak není z nich patrno, zda jde o útok v podobě ransomware. Proto bylo nutné nastudovat a zanalyzovat zejména ustanovení trestního zákoníku, která by bylo vhodné subsumovat pod konkrétní ransomware útok. Jinak řečeno, je nutné v tomto ohledu zohlednit hmotněprávní klasifikaci ransomware tak, jak je podrobně zanalyzována v teoretické částí této práce.

Teoretická příprava vychází z teoretické části této diplomové práce. Zahrnuje tak veškeré poznatky včetně všech zdrojů v této části citovaných. Zkoumaným jevem je fenomén ransomware, který úzce souvisí, vedle kybernetické bezpečnosti, s trestním právem. Ransomware v souvislosti s analytickou částí práce vnímám jako pojem označující trestnou činnost, k jejíž páchání je potřeba šířit malware v podobě ransomware, v kterékoliv formě, které byly rozpracovány v části teoretické (tj. zamykací, šifrovací, policejní) kromě scareware (důvodem je nejasné zařazení scareware mezi ransomware, viz podkapitola 5.3) za užití určitého zařízení. Tuto oblast zkoumání je potřeba odlišit od případů vydírání, či jiné hmotněprávní kvalifikace, které jsou podobné ransomware (viz případ vyděračského mailu zmíněný v podkapitole 5.2).

Vzhledem k výše zmíněné problematice poskytnuté TSK je předmětem zkoumání ransomware jako vydírání podle § 175 TZ, přičemž tím nejsou vyloučené jednočinné souběhy

s jinými trestnými činy do úvahy připadající. TSK neobsahuje informace o objasněnosti, počtu stíhaných trestných činů a další z kriminologického hlediska relevantní informace. To však není na škodu, neboť tyto informace nejsou rozhodující pro cíl výzkumu.

Pro odstranění možných vysokých odchylek je tak vedle zohlednění sdělení NCKB o kybernetických hrozbách vztahujících se k ransomware zejména uvažování jednočinného souběhu § 175 TZ s § 230 TZ. Trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací považuji za přiléhavější pro posuzování malware v podobě ransomware, avšak TSK nerozeznává co do počtu registrovaných skutků mezi §§ 230-232 TZ. Z těchto důvodů zaznamenávám počet skutků u § 230 jako orientační číslo symbolem ~ (tilda). Oblast zkoumání jsem taktéž omezil na území České republiky a prostředí internetu (tj. neuvažuji jiné sítě).

Výběrovým souborem jsou TSK registrovaných skutků spáchaných v prostředí internetu a jiných sítí za roky 2016, 2017 a 2018 na území České republiky.

Hypotéza zní následovně: ***„Počet zaregistrovaných útoků ransomware Policií ČR v České republice od roku 2016 roste.“***

Z metodologického hlediska využívám kombinaci metody historické (analýza období od roku 2016 do roku 2018), topografické (území České republiky od roku 2016) a prognostické (reflektuji předpokládaný vývoj šíření ransomware).

Analýza vývoje ransomware od roku 2016 na území ČR tedy vychází z:

- analýzy odborné literatury, relevantních internetových zdrojů
- analýzy ustanovení trestního zákoníku, a jiných relevantních právních předpisů včetně příslušné judikatury
- analýzy dokumentů poskytnutých NÚKIB a Policejním prezidiem ČR (včetně TSK)
- analýzy některých případů útoků ransomware zveřejňované NÚKIB

II. Analýza dat

V roce 2016 Policie ČR evidovala 94 skutků, které naplnily skutkovou podstatu trestného činu vydírání podle § 175 TZ. Na základě podrobné analýzy, jsem již v teoretické části práce dospěl k závěru, že ransomware vždy představuje vyděračské jednání a naplní tak i skutkovou podstatu vyjádřenou v § 175 TZ. Nelze se však zcela s jistotou domnívat, že všech 94 skutků pokrývají případy ransomware. V tomto ohledu odkazuji na podkapitolu 5.2 teoretické části a

případy podvodného vyděračského mailu. Odchylky bohužel nelze s jistotou určit ani odhadem a je nutné se spokojit pouze s pouhou představou formy vydírání prostřednictvím ransomware. Jako korektiv možných odchylek uvádím počet zpráv vydaných NCKB (NÚKIB) v roce 2016 (pouze 1 případ ransomware Petya[230]).

Významnější pro odstranění odchylek je však uvažování ransomware jako kombinaci (jednočinný souběh) § 175 TZ a § 230 TZ, neboť trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací je jakožto ryze počítačový delikt přiléhavější k posuzování malware v podobě ransomware.

Zdroj: TSK[231]					NCKB[232]
Zkoumané Území	Zkoumaný Rok	Zkoumané prostředí	Zkoumaná právní kvalifikace ransomware	Počet skutků	Počet zpráv o ransomware
ČR	2016	internet	Vydírání - § 175 TZ	~ 94	1
ČR	2016	internet	Neoprávněný přístup k počítačovému systému a nosiči informací - § 230 TZ	~ 475	neuvažuji

Tabulka č. 1: Skutky evidované Policií ČR odpovídající útoku ransomware za rok 2016

V roce 2017 evidovala Policie ČR 109 případů vydírání prostřednictvím internetu. Oproti roku 2016 lze tak zaznamenat mírný nárůst. K nárůstu čísel došlo i v případě páchání Neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 TZ a to na číslo 544. Pokud tedy protneme tyto dvě množiny a budeme předpokládat, že vydírání v podobě ransomware bylo pácháno jako jednočinný souběh § 175 s § 230 TZ, pak dostaneme číslo ~ 109 případů ransomware za rok 2017.

[230] Ransomware Petya. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2335-ransomware-petya/

[231] Viz Seznam ostatních zdrojů: Registrované skutky v ČR spáchané v prostředí internetu a jiných sítí od roku 2016 do roku 2018

[232] Hrozby. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/

Tento rok mimo jiné přinesl do České republiky celkem 4 hrozby ransomware:

- JScript Ransomware RPG[233]
- Ransomware WannaCry[234]
- Petya/Potrwrap/Not Petya[235]
- Bad Rabbit[236]

Zdroj: TSK[237]					NCKB[238]
Zkoumané území	Zkoumaný rok	Zkoumané prostředí	Zkoumaná právní kvalifikace ransomware	Počet skutků	Počet zpráv o ransomware
ČR	2017	internet	Vydírání - § 175 TZ	~ 109	4
ČR	2017	internet	Neoprávněný přístup k informačnímu systému a nosiči informací - § 230 TZ	~ 544	neuvažuji

Tabulka č. 2: Skutky evidované Policií ČR odpovídající útoku ransomware za rok 2017

Policie ČR v roce 2018 zaznamenala nárůst počtu vydírání prostřednictvím internetu za poslední dva roky. Od roku 2016 došlo tedy k zaregistrování o 45 případů více. Nelze však dovozovat, že reálně došlo ke zvýšení spáchaných trestných činů vydírání ve formě ransomware, neboť uvedená statistika neodráží trestné činé činy spáchané v daném roce, ale pouze v tomto roce zaregistrované. Neodráží taktéž všechny trestné činy, ale pouze ty, o kterých se Policie dověděla, ať už sama ze své operativně pátrací činnosti, nebo na oznámení. Nezahrnuje tedy černá čísla.

[233] JScript Ransomware RPG. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2513-jscript-ransomware-rpg/
[234] Ransomware WannaCry. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2529-ransomware-wannacry/
[235] Petya/Petrwrap/NotPetya. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2539-petrwrap-nova-varianta-ransomwaru/
[236] Nový ransomware Bad Rabbit. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2562-novy-ransomware-bad-rabbit/
[237] Viz Seznam ostatních zdrojů: Registrované skutky v ČR spáchané v prostředí internetu a jiných sítí od roku 2016 do roku 2018
[238] Hrozby. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/

Naproti tomu může zahrnovat čísla šedá. Ta mohou být vnímána ve trojím pojetí[239], ačkoliv osobně se v této souvislosti přikláním k tomu, že jde o počet trestných činů, které Policie ČR sice zaevidovala, avšak není znám jejich pachatel[240]. Nárůst můžeme tedy z příslušné TSK spatřovat i od roku 2017 a to o 30 zaregistrovaných případů. NCKB (NÚKIB) dne 29. 6. 2018 konstatuje, že oproti roku 2017 není ransomware již takovou hrozbou, avšak přesto vybízí k ostražitosti a dodržování základních principů prevence.[241] Nárůst je zjevný taktéž u § 230 TZ, kde číslo vyšplhalo až na ~ 633 evidovaných případů.

Zdroj: TSK[242]					NCKB[243]
Zkoumané Území	Zkoumaný rok	Zkoumané prostředí	Zkoumaná právní kvalifikace ransomware	Počet skutků	Počet zpráv o ransomware
ČR	2018	internet	Vydírání - § 175 TZ	~ 139	1
ČR	2018	internet	Neoprávněný přístup k informačnímu systému a nosiči informací - § 230 TZ	~ 633	neuvažuji

Tabulka č. 3: Skutky evidované Policií ČR odpovídající útoku ransomware za rok 2018

[239] 1) pachatel byl stíhán a nebyl odsouzen, 2) Policie ČR se dozvěděla o trestném činu, ale není znám pachatel a 3) případy umělé latence; k tomu viz VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3, s. 144-145

[240] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3, s. 32-33

[241] Ransomware je stále aktuální hrozbou. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2615-opet-ransomware/

[242] Viz Seznam ostatních zdrojů: Registrované skutky v ČR spáchané v prostředí internetu a jiných sítí od roku 2016 do roku 2018

[243] Hrozby. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/

Souhrně lze statistické informace utřídit následovně:

Zdroj: TSK					
Počet registrovaných trestných činů vydírání via internet (§ 175 TZ) v roce 2016	94	Počet registrovaných trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ) v roce 2016	475	Za předpokladu jednočinného souběhu § 175 a § 230 TZ v roce 2016 (tj. potenciální případ ransomware)	~ 94
Počet registrovaných trestných činů vydírání via internet (§ 175 TZ) v roce 2017	109	Počet registrovaných trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ) v roce 2017	544	Za předpokladu jednočinného souběhu § 175 a § 230 TZ v roce 2017 (tj. potenciální případ ransomware)	~ 109
Počet registrovaných trestných činů vydírání via internet (§ 175 TZ) v roce 2018	139	Počet registrovaných trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ) v roce 2018	633	Za předpokladu jednočinného souběhu § 175 a § 230 TZ v roce 2018 (tj. potenciální případ ransomware)	~ 139
Předpokládaný celkový počet registrovaných útoků ransomware za období 2016-2018					~ 342

Tabulka č. 4: Souhrnný přehled skutků evidovaných Policií ČR odpovídající útoku ransomware.

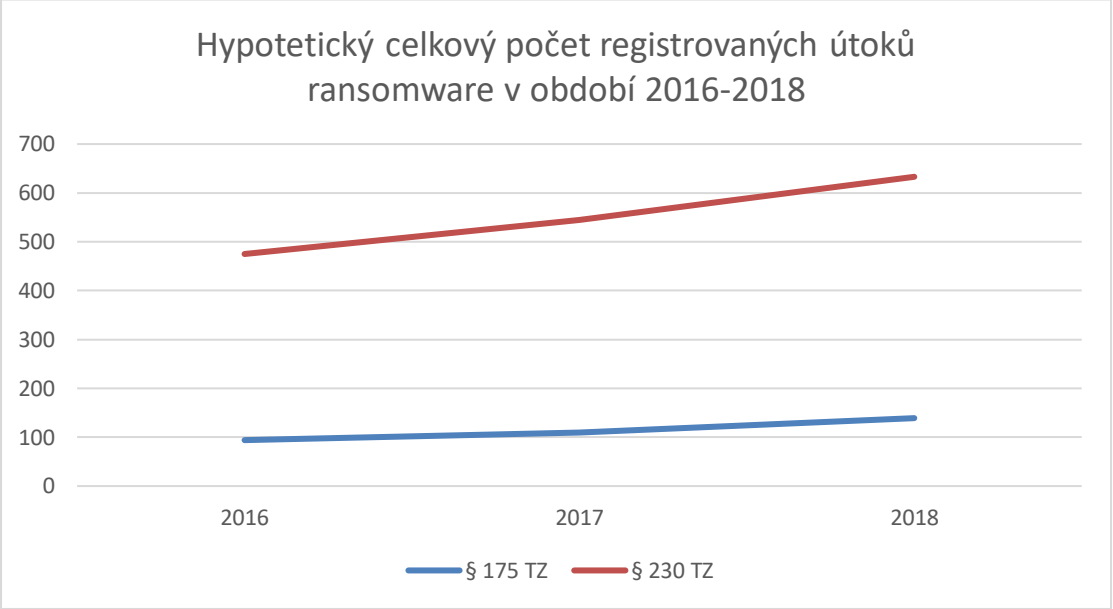
Na základě tohoto teoretického údaje můžeme zjistit intenzitu kyberkriminality páchané šířením ransomware na území ČR. Tu lze určit indexem vyjádřeným jako podíl počtu trestných činů a počtu obyvatel na území ČR vynásobeným počtem obyvatel, na které trestný čin připadá[244]. V našem případě užijeme čísla 100 000.

$$index = \frac{\text{počet registrovaných ransomware útoků (342)}}{\text{počet obyvatel na území ČR (10 649 800}^{245}\text{)}} \text{ x } 100\,000 = 3{,}211$$

[244] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3, s. 141-142

[245] Údaje z ČSÚ k 31. prosinci 2018: Obyvatelstvo. Czso.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.czso.cz/csu/czso/obyvatelstvo_lide

V tomto případě lze konstatovat, že za období 2016-2018 připadaly 3 registrované útoky ransomware na 100 000 obyvatel. Z toho lze dovodit dva závěry. Jednak se lze domnívat, že útoky ransomware nejsou příliš časté, nebo, že je příliš vysoká latence této kyberkriminality. Nicméně důležité je zdůraznit, že počet registrovaných skutků, které naplňují znaky vydírání podle § 175 TZ a neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230, a lze je podřadit pod případy ransomware, přibývá. Pro lepší ilustraci viz graf:



Graf č. 1: Hypotetický celkový počet registrovaných útoků ransomware v období 2016-2018

Z grafu je patrná tendence růstu zaregistrovaných útoků ransomware. Zvyšující se počty zaregistrovaných skutků podle § 175 i § 230 může svědčit jednak o:

1. úspěšnější pátrací činnosti orgánů činných v trestním řízení (v tomto případě Policii ČR)
2. zvýšené ochotě oznamovat útoky ransomware
3. rapidním navýšení počtu útoků
4. útocích na veřejné instituce
5. jiných skutečnostech

Pro ověření hypotézy lze provést test růstu intenzity kyberkriminality ve vztahu k ransomware v náhodně vybraném kraji za období 2016, 2017 a 2018. Vybral jsem pro tyto účely kraj Středočeský.

Středočeský kraj (rok 2016):

$$index = \frac{\text{počet registrovaných ransomware útoků (~94)}}{\text{počet obyvatel na území Středočeského kraje (1 338 982}^{246}\text{)}} \text{ x } 100\,000 = 7{,}02$$

Lze se domnívat, že v roce 2016 připadlo přibližně 7 útoků ransomware na 100 000 obyvatel Středočeského kraje.

Středočeský kraj (rok 2017):

$$index = \frac{\text{počet registrovaných ransomware útoků (~109)}}{\text{počet obyvatel na území Středočeského kraje (1 352 795}^{247}\text{)}} \text{ x } 100\,000 = 7{,}05\ldots$$

Lze se domnívat, že v roce 2017 připadlo přibližně 8 útoků ransomware na 100 000 obyvatel Středočeského kraje.

Středočeský kraj (rok 2018):

$$index = \frac{\text{počet registrovaných ransomware útoků (~139)}}{\text{počet obyvatel na území Středočeského kraje (1 369 332}^{248}\text{)}} \text{ x } 100\,000 = 10{,}15\ldots$$

Lze se domnívat, že v roce 2018 připadlo přibližně 10 útoků ransomware na 100 000 obyvatel Středočeského kraje.

Byť výše uvedená data nemohou přesně určit, jaká jsou skutečná čísla počtu zaregistrovaných útoků ransomware Policií ČR, snažím se alespoň naznačit budoucí předpokládaný vývoj šíření tohoto malware. Domnívám se tedy, že do budoucna lze tak očekávat opětovné navýšení zaregistrovaných skutků, které mohou vykazovat znaky ransomware útoku.

Výsledné hodnoty, o nichž se opírá tento závěr lze však snadno zpochybnit. Zaprvé údaj, který je v TSK uveden u §§ 230–232 udávám jako by se jednalo pouze o skutek naplňující znaky § 230. Zadruhé údaj TSK u § 175 zahrnuje jak případy vyděračských mailů vydávající se za ransomware, tak klasické formy vydírání páchané za pomoci internetu a nevykazují znaky žádného z typů ransomware.

[246] Obyvatelstvo. Czso.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.czso.cz/csu/xs/obyvatelstvo-xs
[247] Tamtéž
[248] Tamtéž

Při extrémně nízkých číslech se tak lze domnívat, že intenzita zaregistrovaných útoků je značně odlišná od mnou uvedených dat. Rovněž bychom nemuseli dospět k závěru, že počty zaregistrovaných útoků ransomware jsou na vzestupu. Příkladem budiž sdělení NÚKIB o bezpečnostních hrozbách v podobě ransomware. V roce 2017 bylo vydáno nejvíce upozornění na možné bezpečnostní hrozby způsobené šířením ransomware, avšak nárůst oproti roku 2016 byl menší, než oproti roku 2018 (viz výše).

Nelze tedy s jistotou potvrdit, že došlo k nárůstu, avšak pro zjednodušení se tak lze domnívat, neboť ransomware se projevuje především vyděračským jednáním a:

- všechna výše zmíněná data u trestného činu vydírání za uplynulá období stoupají, a zároveň
- všechna výše zmíněná data u neoprávněného přístupu k počítačovému systému a nosiči informací za uplynulá období stoupají, a tudíž nelze zcela vyloučit, že stoupá i počet zaregistrovaných útoků ransomware.

Hypotéza: ***„Počet zaregistrovaných útoků ransomware Policií ČR v České republice od roku 2016 roste.“*** však nemůže být bez dalšího (chybí relevantní data) potvrzena.

Závěr

Předkládaná diplomová práce si kladla za cíl stručně popsat problematiku malware s bližším zaměřením na ransomware a dát tak podnět k dalšímu zkoumání tohoto fenoménu. Jak bylo zmíněno v úvodu práce, patrná byla i snaha odlišit se od již existujících prací s obdobným zaměřením. Snažil jsem se zejména popsat místa nezakrytá, nebo je alespoň vyložit odlišně. Ve většině případů jsem měl poslání vylíčit již známé skutečnosti jinak a neznámé stručně popsat. Cílem nebylo za každou cenu používat cizí výrazy a zmínit všechny způsoby šíření ransomware, nebo detailně popsat jeho fungování. Naopak jsem se snažil tyto oblasti pouze nastínit tak, aby bylo snadnější proniknout do tajů škodlivých software.

S vypracováním práce však byly provázány jisté problémy, které je nutné v jejím závěru zmínit. V prvé řadě bylo nezbytné čerpat mnoho informací právě z webových stránek, kde se vyjadřují zejména IT odborníci. Nelze tak ve většině případů zjistit, kdo je autorem, avšak nikdy jsem nečerpal pouze z jediného zdroje a každá teze je tak pečlivě vybrána komparací s několika dalšími.

V druhé řadě je nutné zmínit, že problematika ransomware jako taková není zpravidla zpracovávána samostatně a je jakýmsi vedlejším produktem pojednání o kyberkriminalitě. Z tohoto důvodu bylo nutné neustále subsumovat skutečnosti obecně platné na kyberkriminalitu, jejíž projevy mohou být značně různorodé, na ransomware. Práci tak záměrně trápí určitá nehomogenita, která se projevuje nahodile používanou terminologií, pokud přesné vyjádření v daném případě nepovažuji za nutné, ale lze tuto nestejnorodost spatřovat i v odbočení z ransomware do ostatních, avšak vzájemně provázaných, oblastí. Nelze si tak myslet, že název práce zcela koresponduje s jejím obsahem. I přesto, že zdrojů k ransomware je poměrně dost, neobsahují tyto zdroje příliš mnoho nových informací. Stále se opakující informace k ransomware mě tedy donutily k tomu, abych si vždy o dané problematice vztahující se k ransomware, učinil vlastní úsudek. Tyto úsudky se zpravidla objevují vždy na konci dané kapitoly, či podkapitoly, a snaží se reflektovat moje stanovisko pro daný případ.

Kriminologické aspekty šíření ransomware jsem vystavěl tradičně a jádro této otázky tak stojí zejména na typologii pachatelů ransomware, charakteristických obětech ransomware a základních principech prevence. Vzhledem k tomu, že se stále jedná o neprobádanou oblast, nejevilo se mi jako vhodné činit nějaké závěry, a proto má oblast kriminologických aspektů spíše popisný charakter. Trestněprávní aspekty šíření ransomware jsem však naproti tomu pojal detailněji, neboť tato část práce představovala určité východisko pro část analytickou.

Během studia možné kvalifikace ransomware jsem si uvědomil, že ransomware je delikt, ke kterému je potřebné nějaké zařízení a taktéž vykazuje znaky vydírání, byť někdy má blízko k podvodu. Snažil jsem se tak zejména podtrhnout význam kvalifikace ransomware jako trestný čin vydírání. V práci tak několikrát zdůrazňuji, v jakém jednání lze spatřovat naplnění skutkové podstaty trestného činu vydírání, ale zároveň se snažím poukázat, že se pořád jedná o kyberzločin, který má svá specifika. Na určitá specifika šíření ransomware pak narážím i v části procesní. Trestněprocesní problematika ransomware se však dotýká i kriminalistiky, a proto jsem spíše pro úplnost uvedl pouze některé zvláštnosti.

Teoretická část diplomové práce však směřovala především k části analytické, kde jsem se s neúspěchem pokusil o verifikaci hypotézy znějící: ***„Počet zaregistrovaných útoků ransomware Policií ČR v České republice od roku 2016 roste.“*** Neúspěch přikládám k nedostatku dostupných statistických údajů o ransomware, které mi byly, resp. nebyly, poskytnuty. Nepovažuji to však za naprostý neúspěch, ale spíše za úmyslný pokus o zviditelnění závažnosti ransomware. Považuji naopak za důležité, že jsem se pokusil i z nedostatku dat vyvodit nějaké závěry, a tím snad dal dostatečný popud se problematikou ransomware zabývat i dále. Domnívám se, byť možná naivně, že i samotná existence skutečnosti, že se o problematiku ransomware někdo zajímá a žádá za tímto účelem kompetentní úřady k poskytnutí informací o ransomware, vyburcuje tyto úřady k náležité evidenci útoků ransomware a vytvoří tak relevantní půdu pro budoucí úspěšné zkoumání.

Seznam použitých zdrojů

Seznam použité literatury

BUTTON, Mark a Cassandra CROSS. Cyber frauds, scams and their victims. Abingdon: Routledge, Taylor & Francis Group, 2017. ISBN 978-1-138-93120-6.

CEJP, Martin. Kriminologický výzkum: praktická příručka. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-743-6.

ČIKOVSKÝ, Jan. Internetová a počítačová kriminalita [online]. 2013 [cit. 2019-05-27]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/117868. Vedoucí práce Tomáš Gřivna.

DE ANGELIS, Gina a Austin SARAT. Cyber crimes. Philadelphia, Pa.: Chelsea House Publishers, 2000. Crime, justice, and punishment. ISBN 0-7910-4252-9.

DRAŠTÍK, Antonín. Trestní zákoník: komentář. Praha: Wolters Kluwer, 2015. Komentáře Wolters Kluwer. Kodex. ISBN 978-80-7478-790-4.

GILLESPIE, Alisdair. Cybercrime: key issues and debates. Routledge. 2016. ISBN 9780415712200.

GRABOSKY, Peter N. Virtual Criminality: Old Wine in New Bottles? Social & Legal Studies. Vol 10(2). ISSN 09646639, 243-249

GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3.

GŘIVNA, Tomáš. Existují virtuální trestné činy? In: GŘIVNA, Tomáš a Marie VANDUCHOVÁ, ed. Pocta Otovi Novotnému k 80. narozeninám [online]. Praha: ASPI, Wolters Kluwer, 2008, s. 28-35. ISBN 978-80-7357-365-2.

HEFKA, Rostislav. Internetová a počítačová kriminalita. Praha, 2016. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D.

HOLCR, Květoň a Jaroslav FENYK. Kriminológia. Bratislava: Iura Edition, 2008. ISBN 978-80-8078-206-1.

HOLT, Thomas J. a Adam M. BOSSLER. Cybercrime in progress: theory and prevention of technology-enabled offenses. London: Routledge, 2016. Crime Science Series. ISBN 978-1-138-02416-8.

JAISHANKAR, K. Cyber criminology: exploring Internet crimes and criminal behavior. Boca Raton, FL: CRC Press, c2011. ISBN 978-1-4398-2949-3.

JELÍNEK, Jiří, Katarína TEJNSKÁ, Jana TLAPÁK NAVRÁTILOVÁ, Vladimír PELC, Jiří ŘÍHA a Vojtěch STEJSKAL. Trestní právo hmotné: obecná část, zvláštní část. 6. aktualizované a doplněné vydání. Praha: Leges, 2017. Student. ISBN 978-80-7502-236-3.

JELÍNEK, Jiří. Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif. 7. aktualizované vydání. Praha: Leges, 2017. Glosátor. ISBN 978-80-7502-230-1.

JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

JOHANOVSKÝ, Tomáš. Kriminologické a trestněprávní aspekty fenoménu ransomware. Kriminologické a trestněprávní aspekty fenoménu ransomware. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. JUDr. Bc. Tomáš GŘIVNA, Ph.D.

KLIMEK, Libor, Jozef ZÁHORA a Květoň HOLCR. Počítačová kriminalita v európskych súvislostiach. Bratislava: Wolters Kluwer, 2016. ISBN 9788081685385.

KLIMEŠ, Cyril. Architektura operačních systémů. Brno: Mendelova univerzita v Brně, 2018. ISBN 978-80-7509-635-7.

KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČOVÁ a Martin KUNC. CyberSecurity. Praha: CZ.NIC, 2019. CZ.NIC. ISBN 978-80-88168-31-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf

KRUPIČKA, Jiří. Trestněprávní a kriminologické aspekty internetové kriminality. Praha, 2012. Disertační práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Prof. JUDr. Jiří Jelínek, CSc.

Květoň HOLCR. Počítačová kriminalita: v európskych súvislostiach. Bratislava: Wolters Kluwer, 2016. ISBN 978-80-8168-538-5

MADLIAK, Jozef, Ján MIHAĽOV, Viktor PORADA a Simona ŠTEFANKOVÁ. Počítačová kriminalita. Karlovarská právní revue. 2008, 4(1), 45-63. ISSN 1801-2191.

POLČÁK, Radim a Tomáš GŘIVNA. Kyberkriminalita a právo. 1. vyd. Praha: AUDITORIUM, 2008. 220 s. Auditorium. ISBN 978-80-903786-7-4.

POLČÁK, Radim, František PÚRY, Jakub HARAŠTA, Tomáš ABELOVSKÝ, Petr KLEMENT, Matěj MYŠKA, Václav STUPKA, Alena PEJČOCHOVÁ a Tomáš ELBERT. Elektronické důkazy v trestním řízení. 1. vyd. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7.

PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. 2. aktualizované a rozšířené vydání. Plzeň: Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.

RADEMACHEROVÁ, Kristina. Počítačová kriminalita: Vybrané aspekty postihu v mezinárodním prostředí. Univerzita Karlova, Právnická fakulta. Vedoucí práce Jiří Jelínek.

RONOVSKÁ, Barbora. Trestní odpovědnost právnických osob a kyberkriminalita. Trestní právo: odborný časopis pro trestní právo a obory související. 2018, 2018(4), 17-24.

SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7.

SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5.

ŠRUBAŘ, Michal. Analýza síťové komunikace Ransomware. Brno, 2017. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ryšavý Ondřej.

ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3.

VLČEK, Martin, Vladimír SMEJKAL a Tomáš SOKOL. Počítačové právo. Praha: Beck/SEVT, 1995. Právo a hospodářství. ISBN 80-7179-009-5.

VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. Trestní právo. 2010, 14(7-8), 19-43. ISSN 1211-2860.

WALDEN, Ian. Computer crimes and digital investigations. Oxford: Oxford University Press, 2007. ISBN 978-0-19-929098-7.

WALL, David. Cybercrime: the transformation of crime in the information age. 2007. ISBN 9780745627359.

ZAPLETAL, Josef. Aktuální problémy kriminologie: (pro posluchače magisterského studijního programu). Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-316-1.

ZAVRŠNIK, Aleš. Kyberkriminalita. Vydání první. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). e-ISBN 978-80-7552-759-2.

ZEMAN, Daniel. Počítačová a internetová a kriminalita. Univerzita Karlova, Právnická fakulta. Vedoucí práce Tomáš Gřivna.

Seznam použitých internetových zdrojů

7 Types of Hacker Motivations. Securingtomorrow.mcafee.com [online]. [cit. 2019-03-25]. Dostupné z: https://securingtomorrow.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

Adware. Searchsecurity.techtarget.com [online]. [cit. 2019-02-25]. Dostupné z: https://searchsecurity.techtarget.com/definition/adware

Bezplatné nástroje na dešifrování ransomwaru. Avg.com [online]. [cit. 2019-04-01]. Dostupné z: https://www.avg.com/cs-cz/ransomware-decryption-tools

Creeper. Corewar.co.uk [online]. [cit. 2019-03-07]. Dostupné z: http://corewar.co.uk/creeper.htm

Crimeware. Searchsecurity.techtarget.com [online]. [cit. 2019-02-25]. Dostupné z: https://searchsecurity.techtarget.com/definition/crimeware

CryptoLocker – an infamous ransomware virus that was stopped by the Operation Tovar [online]. [cit. 2019-03-11]. Dostupné z: https://www.2-spyware.com/remove-cryptolocker.html#ref-1

Crypto-ransomware. F-secure.com [online]. [cit. 2019-03-04]. Dostupné z: https://www.f-secure.com/en/web/labs_global/crypto-ransomware

Cyber Intelligence Team. Ransomware: What You Need to Know: A Joint Report by Check Point and Europol [online]. The Hague: Europol Public Information, 2016 [cit. 2019-04-01]. Dostupné z: https://www.europol.europa.eu/publications-documents/ransomware-what-you-need-to-know

Doxware (extortionware). Whatis.techtarget.com [online]. [cit. 2019-02-25]. Dostupné z: https://whatis.techtarget.com/definition/doxware-extortionware

Expertizní obory. Policie.cz [online]. [cit. 2019-05-28]. Dostupné z: https://www.policie.cz/clanek/celorepublikove-utvary-kriminalisticky-ustav-praha-zpravodajstvi-test-4.aspx?q=Y2hudW09Mw%3d%3d

Goldeneye. Bitdefender [online]. [cit. 2019-02-10]. Dostupné z: https://www.bitdefender.com/business/usecases/goldeneye.html

Grey Hat Hacker. Techopedia.com [online]. [cit. 2019-03-25]. Dostupné z: https://www.techopedia.com/definition/15450/gray-hat-hacker

History Ransomware Attacks: Biggest and Worst Ransomware Attacks of All Time. Digitalguardian.com [online]. [cit. 2019-03-07]. Dostupné z: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

Hrozby. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/

JScript Ransomware RPG. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2513-jscript-ransomware-rpg/

Malware evolution: April-June 2006 [online]. [cit. 2019-03-11]. Dostupné z: https://securelist.com/malware-evolution-april-june-2006/36094/

Malware. Eset.com [online]. [cit. 2019-02-25]. Dostupné z: https://www.eset.com/cz/malware/

NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history. www.telegraph.co.uk [online]. [cit. 2019-03-11]. Dostupné z: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

Novela zákona o trestní odpovědnosti právnických osob. Pravniprostor.cz [online]. [cit. 2019-03-04]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/novela-zakona-o-trestni-odpovednosti-pravnickych-osob

Obyvatelstvo - kraj. Czso.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.czso.cz/csu/xs/obyvatelstvo-xs

Obyvatelstvo. Czso.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.czso.cz/csu/czso/obyvatelstvo_lide

Payload. Searchsecurity.techtarget.com [online]. [cit. 2019-02-25]. Dostupné z: https://searchsecurity.techtarget.com/definition/payload

PETERKA, Jiří. Na počátku byl ARPANET... Earchiv.cz [online]. [cit. 2019-03-07]. Dostupné z: http://www.earchiv.cz/a95/a504c502.php3

Petya/Petrwrap/NotPetya. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2539-petrwrap-nova-varianta-ransomwaru/

Preventivní rady. Nomoreransom.org [online]. [cit. 2019-04-01]. Dostupné z: https://www.nomoreransom.org/cs/prevention-advice.html

Ransomware and malicious crypto miners in 2016-2018. Securelist.com [online]. [cit. 2019-04-01]. Dostupné z: https://securelist.com/ransomware-and-malicious-crypto-miners-in-2016-2018/86238/

Ransomware Petya. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2335-ransomware-petya/

Ransomware targets SMBs due to weaker protection and greater willingness to pay up. Bitdefender [online], 7 [cit. 2019-02-10]. Dostupné z: https://download.bitdefender.com/resources/files/News/CaseStudies/study/153/Ransomware-SMB-survey-crea1289-A4-en-EN-web.pdf?adobe_mc=MCMID%3D55420216346940061751835135069182211487%7CMCORGID%3D0E920C0F53DA9E9B0A490D45%2540AdobeOrg%7CTS%3D1549830248

Ransomware WannaCry. Govcert.cz [online]. [cit. 2019-06-04]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2529-ransomware-wannacry/

Ransomware. *Avast* [online]. [cit. 2019-02-08]. Dostupné z: https://www.avast.com/cs-cz/c-ransomware

Rootkit. Avast.com [online]. [cit. 2019-02-26]. Dostupné z: https://www.avast.com/cs-cz/c-rootkit

Rootkits, Part 1 of 3: The Growing Threat. Mcafee.com [online]. 2006 [cit. 2019-02-26]. Dostupné z: http://web.archive.org/web/20060823090948/http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_akapoor_rootkits1_en.pdf

Scareware. Kaspersky [online]. [cit. 2019-03-06]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/scareware

Should Social Engineering be a part of Penetration Testing?Should-social-engineering-a-part-of-penetration-testing. Darknet.org.uk [online]. [cit. 2019-02-25]. Dostupné z: https://www.darknet.org.uk/2006/03/should-social-engineering-a-part-of-penetration-testing/

The Computer Virus that Haunted Early Aids Researchers. Theatlantic.com [online]. [cit. 2019-03-07]. Dostupné z: https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/

The rise of Android ransomware. Welivesecurity.com [online]. [cit. 2019-03-11]. Dostupné z: https://www.welivesecurity.com/2016/02/18/the-rise-of-android-ransomware/

Trojan. Avast.com [online]. [cit. 2019-02-25]. Dostupné z: https://www.avast.com/cs-cz/c-trojan

UK hospitals hit with massive ransomware attack. Theverge.com [online]. [cit. 2019-03-25]. Dostupné z: https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

Varování před novým podvodným vyděračským e-mailem. Govcert.cz [online]. 4. 4. 2019 [cit. 2019-04-15]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2693-varovani-pred-novym-podvodnym-vyderacskym-e-mailem/

Wannacry. Bitdefender [online]. [cit. 2019-02-10]. Dostupné z: https://www.bitdefender.com/business/usecases/wannacry.html

What is an exploit kit. Paloaltonetworks.com [online]. [cit. 2019-03-04]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit

What is Wannacry ransomware, how does it infect, and who was responsible?. Csoonline.com [online]. [cit. 2019-03-11]. Dostupné z: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Wormable ransomware strain uses freshly leaked exploit to encrypt data. Businessinsights.bitdefender.com [online]. [cit. 2019-03-11]. Dostupné z: https://businessinsights.bitdefender.com/wormable-ransomware-strain-uses-freshly-leaked-exploit-to-encrypt-data?pid=wannacryB2B&adobe_mc=MCMID%3D55420216346940061751835135069182211487%7CMCORGID%3D0E920C0F53DA9E9B0A490D45%2540AdobeOrg%7CTS%3D1552315677

Seznam použitých právních předpisů

Budapešťská úmluva o počítačové kriminalitě 2001

Směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV

Směrnice Evropského parlamentu a Rady 2013/40/EU o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 205/222/SVV

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Zákon č. 127/2005 Sb., o elektronických komunikacích

Seznam použité judikatury

Rozsudek Nejvyššího soudu ČSR ze dne 8.4.1981, sp. zn. 6 Tz 12/81

Usnesení Nejvyššího soudu ČR ze dne 30. 9. 2004, sp. zn. 11 Tdo 872/2004

Usnesení Nejvyššího soudu ČR ze dne 15.06.2011, sp. zn. 8 Tdo 612/2011

Usnesení Nejvyššího soudu ČR ze dne 25. 10. 2016, sp. zn. 7 Tdo 1172/2016

Seznam ostatních zdrojů

Registrované skutky v ČR spáchané v prostředí internetu a jiných sítí od roku 2016 do roku 2018

Sdělení Ministerstva zahraničních věcí ČR o sjednání Úmluvy o počítačové kriminalitě, vyhlášené pod číslem 104/2013 Sb. m. s.

Vládní návrh zákona č. 287/2018 Sb., kterým se mění z. č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony (sněmovní tisk 79/0, část č. 1/6)

Vyjádření NÚKIB ze dne 22.03.2019 k žádosti o informace podle z. č. 106/1999 Sb., o svobodném přístupu k informacím – dokument č.j. 537/2019-NÚKIB-E/210

Vyjádření Policejního prezidia PČR ze dne 14.02.2019 k žádosti o informace podle z. č. 106/1999 Sb., o svobodném přístupu k informacím

Základní kurz kybernetické bezpečnosti určený zaměstnancům NÚKIB – dokument č.j. 537/2019-NÚKIB-E/210

Seznam obrázků, tabulek a grafů

Kriminologické a trestněprávní aspekty šíření ransomware

Abstrakt

Tato diplomová práce se zabývá jednotlivými aspekty, se kterými se setkáváme v oblasti kriminologie a trestního práva v souvislosti s problematikou šíření škodlivého programu (malware) v podobě ransomware.

Práce je rozdělena do dvou hlavních částí, a to části teoretické, která se dále člení na kapitoly týkající se obecně kyberkriminality, obecně malware a následně kriminologických aspektů šíření ransomware a trestněprávních aspektů šíření ramsomware, a to jak z hmotněprávního hlediska, tak z procesněprávního. Jednotlivé kapitoly jsou dále členěny na dílčí podkapitoly a ty zahrnují nejen otázky pachatelů a obětí ransomware či trestněprávní kvalifikace tohoto fenoménu, ale rovněž i pojmy příbuzné, jejichž zmínka by měla sloužit k širšímu pochopení tohoto druhu kyberkriminality. Ten je typický zejména svým distančním charakterem páchání, vysokou mírou latence a poměrně nízkou možností dopadení jejich pachatelů.

Druhou částí práce je část analytická. V této části kombinuji kriminologické výzkumné metody, když se snažím verifikovat hypotézu týkající se růstu čísel evidovaných skutků odpovídají ransomware. Hypotéza je následující: *„Počet zaregistrovaných útoků ransomware Policií ČR v České republice od roku 2016 roste.“* Tato hypotéza nakonec nemohla být z důvodů neposkytnutí dostatku relevantních informací potvrzena.

Lze pouze konstatovat, že za období 2016-2018 připadaly 3 registrované útoky ransomware na 100 000 obyvatel České republiky. Z toho lze dovodit dva závěry. Jednak se lze domnívat, že útoky ransomware nejsou příliš časté, nebo je příliš vysoká latence této kyberkriminality. Nicméně důležité je zdůraznit, že počet registrovaných skutků, které naplňují znaky vydírání podle § 175 TZ a neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230, a lze je podřadit pod případy ransomware, přibývá. Lze také předpokládat, že do budoucna lze očekávat opětovné navýšení zaregistrovaných skutků, které mohou vykazovat znaky ransomware útoku.

Cílem této práce je také otevřít diskuzi o dalším zkoumání otázek spojených s ransomware, která by mohla vést k hlubšímu porozumění této problematiky pro právní i mimoprávní praxi.

Klíčová slova: kyberkriminalita, ransomware, Česká republika

Criminological and criminal law aspects of the ransomware spread

Abstract

This diploma thesis examines different aspects of criminology and criminal law with the issue of the malware spread in the form of ransomware.

This text is divided into two main parts. First, the theoretical part consists of the chapters about cybercrime, malware and criminological and criminal law aspects of ransomware spread. It uses the substantive law and also procedural law perspective. All chapters are divided into subchapters dealing with the questions of offenders and victims, criminal law qualification of the ransomware phenomena and with related concepts used for the broader understanding of this kind of cybercrime.

Second, the analytical part follows. This thesis combines different criminological research methods and tries to verify the main hypothesis regarding the increase in the number of ransomware attacks in the Czech Republic. The hypothesis is as follows: "*The number of ransomware attacks registered by the Police of the Czech Republic has been increasing since 2016*". This hypothesis cannot be accepted due to missing relevant data from the Police of the Czech Republic and other institutions.

It can be said that for the period 2016-2018, there was 3 registered ransomware attacks per 100,000 inhabitants of the Czech Republic. Two conclusions can be drawn from this. We can assume that ransomware attacks are not very common, or the latency of this cybercrime is too high. However, it is crucial to emphasize the fact that the number of registered attacks fulfilling the signs of blackmailing law definition (§ 175 TZ) or unauthorized access to the computer system and the information carrier law definition (§ 230) is increasing. Therefore, it can be assumed that the number of registered acts which can be described as ransomware attacks will be growing.

Moreover, the aim of this thesis is to open discussion about a further examination of ransomware attacks which could lead to a deeper understanding of this phenomena.

Keywords: cybercrime, ransomware, Czech Republic