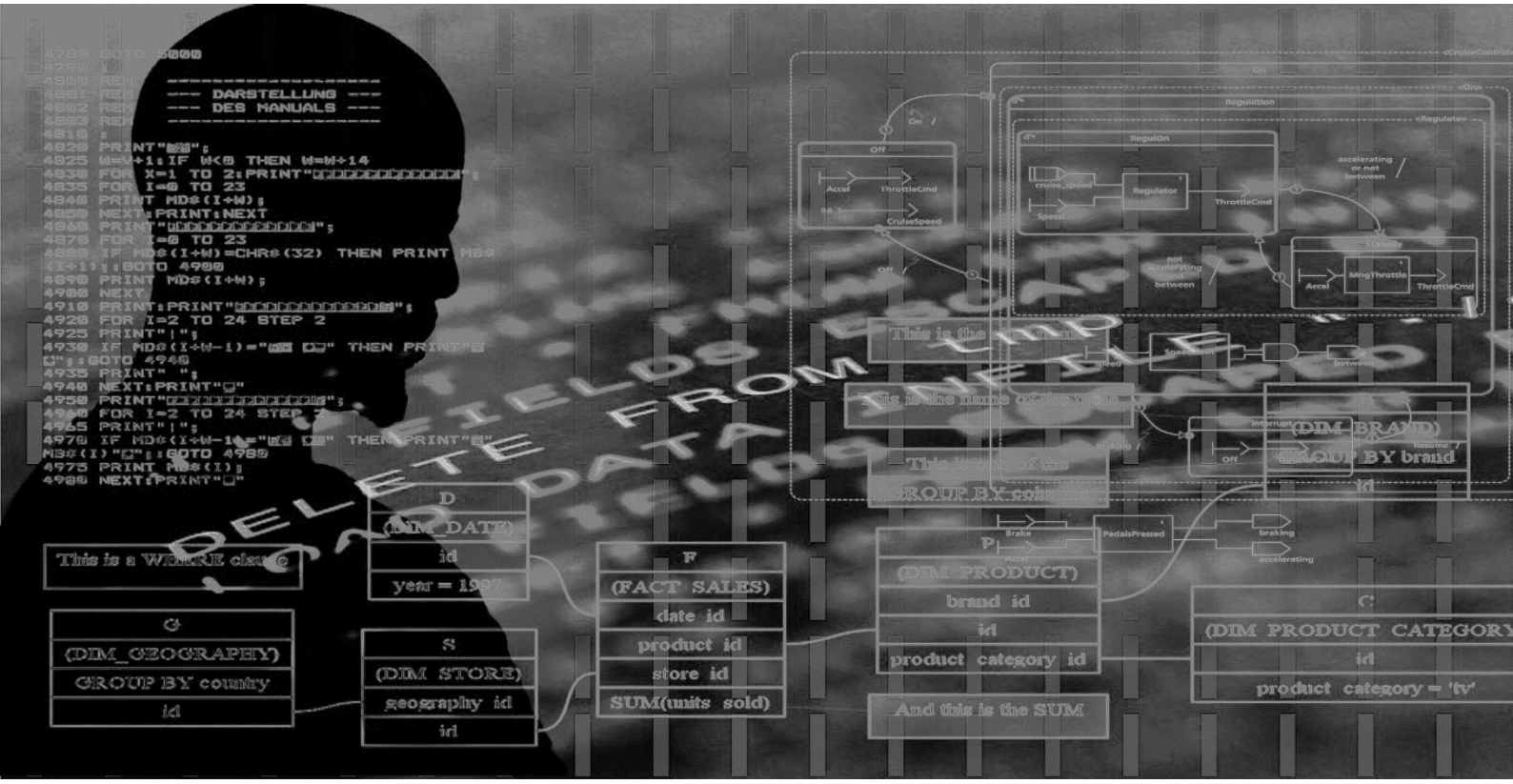


# EVIL CORP: HROZBA PRO ČESKOU REPUBLIKU?

TOMÁŠ SIŘINEK, JAKUB ONDRŮŠEK, MAREK RECHTIK

## ÚVOD

S nástupem pandemie COVID-19 došlo k významnému nárůstu plošných i cílených kybernetických útoků. V rámci České republiky v poslední době čím dál více vyvstává otázka ransomwarových útoků, které se nevyhýbají ani zdravotnickým zařízením, což je v době koronavirové krize zásadní problém. Ransomware je přitom často využívaným nástrojem řady hackerských skupin. Jednou z takových skupin je také skupina Evil Corp, která údajně stojí za vznikem a vývojem různých druhů ransomware. Tato skupina provedla řadu útoků v USA i západní Evropě,[1] přičemž do budoucna není vyloučeno její zaměření také na země regionu střední Evropy včetně ČR.

Cílem této práce tak bude identifikace a následná analýza hrozeb a rizik v kybernetickém prostoru ČR, které vyplývají z působení skupiny Evil Corp. Za tímto účelem se autoři nejprve pokusí identifikovat hlavní osoby, které v dané skupině působí. V rámci charakteristiky skupiny bude zmíněn také význam potenciálních vazeb některých členů skupiny na ruskou státní sféru. Při samotné analýze hrozeb a rizik autoři pomocí identifikace referenčních objektů v ČR a pomocí charakterizace původce hrozby zhodnotí a stanoví míru rizika, kterou skupina Evil Corp představuje pro kyberprostor v ČR.

## METODY VÝZKUMU

Výběr zdrojů dat byl nutně limitován povahou tématu a jeho zpracováním. Jednalo se proto především o vyhledávání skrze internetové vyhledávače, obsahující z meritu věci pouze otevřené zdroje. O problematice budou s velkou pravděpodobností existovat i podrobnější záznamy a zjištění u zpravodajských a vyšetřovacích služeb z různých států světa či s mezinárodní působností. Poskytnutí těchto zdrojů autorům by však z jejich pohledu mohlo ohrozit samotné stíhání, proto autoři nepodnikli v tomto směru žádnou iniciativu. Autoři se přitom při výběru podkladů z otevřených zdrojů snažili dát přednost těm, které splňovaly alespoň některé charakteristiky důvěryhodnosti – uvedený autor, duplicitní zdroje potvrzující informaci, nemanipulativní povaha média či autora aj. Z podstaty tématu však autoři museli do výběru zařadit i některé zdroje, jejichž důvěryhodnost není zcela ověřená, resp. nabízí neověřená/neověřitelná data či tvrzení, které pomáhají dokreslit celkový obraz.

[1] Do obecného povědomí se dostala zejména svým ransomwarovým útokem na společnost Garmin v červenci 2020 (Jennings 2020).

Při analýze dat využili autoři tohoto posudku analýzu hrozeb a rizik. Riziko lze definovat jako *„pravděpodobnost, že dojde ke škodlivé události, jež postihne danou hodnotu*", zatímco hrozba *„je primární, mimo nás nezávisle existující, vnější fenomén, který může nebo chce poškodit nějakou konkrétní hodnotu*" (Zeman 2002a: 58). Z našeho pohledu jsou pak relevantní pouze hrozby intencionální, tedy takové, které úmyslně připravuje či realizuje jedinec, skupina, organizace nebo stát, přičemž platí, že s kapabilitou i motivací aktéra daná hrozba narůstá. Se závažností hrozby a zranitelností (stejně jako s významem chráněné hodnoty) pak narůstá také riziko (Zeman 2002a).

Analýza hrozeb a rizik vychází z podobných postupů a metod, jaké jsou používány také v jiných oborech, než je politologie (resp. pod ni spadající bezpečnostní studia), a to zejména v oborech ekonomických (Frank 2006). V rámci společenskovědních oborů je nicméně tato analýza nicméně poněkud specifická, protože se potýká se zásadními limity v rámci kvantifikace rizika (Zeman 2002b). Ačkoli v některých případech lze o kvantifikovatelnosti rizika uvažovat, v řadě případů mu může být přiřazena semikvantitativní hodnota (např. riziko nízké, střední, vysoké) (Zeman 2002a). Stejně tomu bude také v rámci naší analýzy. Samotná analýza hrozeb a rizik je pak obvykle *„chápána jako proces definování hrozeb a jejich rizika (tj. pravděpodobnosti, aktuálnosti, závažnosti ve vztahu k chránění hodnotě – referenčnímu objektu)*" (Frank 2006: 33). Analýza hrozeb a rizik pak probíhá obecně na základě čtyř kroků (Frank 2006), které jsme se pro účely práce rozhodli modifikovat do následujících třech:

1. Identifikace chráněné hodnoty (tj. posuzovaného referenčního objektu) a stanovení hodnoty referenčního objektu (případně ohodnocení možných dopadů realizace hrozby na její výši, možnou ztrátu či poškození).
2. Identifikace hrozby, přičemž identifikace hrozby představuje proces poznání a určení (potencionálního) původce škody, jeho charakterizování z hlediska destrukčního potenciálu, vztahu k referenčnímu objektu, možnostem dalšího působení atd.
3. Stanovení míry rizika.

## CHARAKTERISTIKA SKUPINY EVIL CORP

Existují indicie, že skupina Evil Corp se vyvinula v roce 2007 odtržením od kyberkriminální skupiny zapojené do distribuce trojanu ZeuS (Scroxton, 2019). Skupina působí z území Ruské federace, konkrétně zejména Moskvy, přičemž členskou základnu lze rozdělit do

několika úrovní (viz Příloha 1). Společníci a finanční zprostředkovatelé nicméně z povahy své práce pobývají v jiných městech či státech nebo často cestují v rámci pašování.

Za lídra skupiny je považován **Maxim Jakubec** (vystupující pod přezdívkou 'Aqua'), původem Ukrajinec, který je zodpovědný za management a dohled nad kyberkriminálními aktivitami skupiny (FBI, n.d.b). Udržoval kontakt s Andrejem Ghinkulem (známým též pod nickem 'Smilex'), který byl v roce 2015 zatčen a extradikován do USA, kde byl odsouzen za distribuci malwaru Dridex, který Jakubec kontroloval (USDT, 2019a). Dle OFAC Jakubec mimoto udržoval styky s Evženem Bogačevem, který je spojován s malwarem 'Zeus' a jeho variantami. Tomu měl Jakubec pomáhat shánět a organizovat síť kontaktů pro praní špinavých peněz z kyberkriminálních aktivit. Americké Ministerstvo spravedlnosti na Maxima Jakubce podalo trestní oznámení a Ministerstvo zahraničí vyhlásilo odměnu 5 milionů USD za informace, které povedou k jeho dopadení FBI.

Kromě toho OFAC zmiňuje také Jakubcovu afiliaci k ruské zpravodajské službě FSB, pro kterou měl pracovat v roce 2017 na projektech, které zahrnovaly také získávání tajných dokumentů a podnikání kybernetických operací. Jakubcův tchán je taktéž bývalým členem speciálních složek FSB (Yapparova, 2019). Jakubec je nakonec spojován a obviněn v Pensylvánii z údajného zapojení do vývoje, distribuce a provádění útoků malwarem 'Bugat', což je jiné označení pro Dridex (Yapparova, 2019). Některé zdroje však zpochybňují Jakubcova zapojení do posledních útoků Evil Corp, např. na Garmin (USDT, 2019a).

Druhým z pomyslného vedení Evil Corpu je **Igor Turašev**, který od roku 2015 pracoval pro Jakubce jako administrátor malwaru Dridex (FBI, n.d.a). V roce 2017 pak měl být přímo začleněn ve vytěžování napadených sítí ve vlastnictví cílů Evil Corpu. Turašev byl také obžalován americkým Ministerstvem spravedlnosti a v současnosti je stíhán FBI. Z všech tří osob, které jsou označovány jako hlavní členové Evil Corpu, je o Turaševovi známo nejméně informací a jeho činnost dle všeho spočívá zejména v samotném technickém procesu orchestrace útoků a úpravy, údržby a distribuce malwaru (USDT, 2019a).

**Denis Gusev** je posledním z trojice vůdčích osobností Evil Corpu. V roce 2017 měl skupině napomáhat v stěhování do nových kancelářských prostor, v roce 2018 pak působit jako finanční zprostředkovatel skupiny. Gusev také vlastní několik firem, resp. v nich vystupuje jako generální ředitel, jejichž majetek by OFAC zmražen, jelikož existuje důvodné podezření, že by mohly sloužit k praní špinavých peněz (USDT, 2019a).

Šest osob, výše uvedených jako spolupracovníci FSB, bylo OFAC identifikováno jako páteřní personál k vykonávání potřebných technických, finančních a logistických úkolů jako např. správa a kontrola malwaru Dridex, výběr cílů dalších útoků nebo praní špinavých peněz (USDT, 2019a). Role zbylých osob se zablokovaným majetkem jsou pravděpodobně méně významné, OFAC je považuje za nápomocné pašeráky ilegálně získaných prostředků, kteří taktéž vykonávají jejich komplexní přenos skrze množství jiných bank a finančních institucí na účty členů Evil Corp (USDT, 2019a).

Vzhledem ke zjištěným charakteristikám lze skupinu Evil Corp z akademického pohledu jednoznačně považovat za zločineckou organizaci, nikoli však organizovaný zločin. Uvažujeme-li Fickenauerovu definici organizovaného zločinu, absentují u Evil Corp pro toto označení důležité atributy kontinuity v čase, užití násilí a omezeného členství, u atributu korupce pak můžeme sice odhadovat, že se pravděpodobně vyskytuje, fakty jej však doposud nijak nelze doložit (dle Šmíd a Kupka, 2012: 26).

### *Potenciální napojení skupiny Evil Corp na ruskou státní sféru*

Podpora ze strany ruského státu či přímé propojení se zpravodajskými službami nelze mimo rodinné vazby Maxima Jakubce definitivně prokázat. Informace o možných konexích jsou taktéž zveřejňovány americkými úřady, ruská strana však tato nařčení popírá a nijak nereaguje na Jakubcova obvinění ani kroky OFAC (Шимаев, 2019). Ruské zpravodajské servery citují stížnosti ruské ambasády v USA z obviňování ruského státu ze spolčení se zločinci a kybernetických zločinů bez relevantních důkazů (Russia Today, 2019). Rusové nicméně poskytli americkým vyšetřovatelům některé dokumenty, které jej mají propojovat s internetovou přezdívkou 'Aqua' a dokazovat jeho stíhání v roce 2010, které však skončilo bezpředmětně (Yapparova, 2019).

Toto stíhání se pak ukazuje býti prvopočátkem možného napojení na FSB skrze osobu právě Maxima Jakubce. Investigativní novinářka Lilia Japarová tvrdí, že poté, co byl v roce 2009 Jakubec obviněn FBI z kybernetické loupeže finančních prostředků municipality v Kentucky, prohledaly koncem roku 2010 ruské bezpečnostní sbory Jakubcův byt za jeho přítomnosti. Ačkoli údaje z prohlídky poskytla ruská strana Američanům, stíhání nijak nepokračovalo (Yapparova, 2019).

Některé ruské soukromé kyberbezpečnostní firmy Jakubcovo zatčení samy uvádí jako nutnost pro zachování kredibility státu, ten však i přes zahraniční i domácí tlaky nic v této věci nepodniká (Пудовкин, 2019). Zatčení obviněných jednotlivců je dle vyšetřovatelů nereálné, dokud se nacházejí na ruské půdě, příležitost však vidí v jejich zahraničních cestách. Více členů skupiny Evil Corp má pocházet z rodin vysoce postavených státních úředníků a hackeři ze skupiny mají disponovat prozatímní státní imunitou výměnou za poskytování informací a plnění úkolů pro FSB (Meduza, 2019).

Ve výsledku se spojení Evil Corpu s FSB, potažmo ruskou státní sférou obecně, jeví na první pohled sporně. Americké a britské vyšetřující úřady a ruští investigativní novináři tvrdí, že existuje, ruská strana tato obvinění označuje za bezpředmětná. Vzhledem k precedentu letargie ruského trestního práva ke svým občanům, obviněným z mezinárodních kybernetických zločinů, u nichž navíc existuje podezření na práci pro státní sféru, se však autoři přiklánějí spíše k oficiálním zdrojům západních vyšetřovacích služeb. Závěrem je proto pravděpodobné, že vazby mezi Evil Corp a FSB, resp. ruskou státní sférou existují, jejich detaily a rozsah jsou však nad rámec dosavadních možností analýzy otevřených zdrojů či zodpovědného odhadu.

## ANALÝZA HROZEB A RIZIK SKUPINY EVIL CORP V KYBERPROSTORU Z POHLEDU ČR

### *1) Identifikace referenčních objektů a stanovení jejich hodnot*

Referenční objekty na území ČR, tj. potenciální cíle, jsou vyhodnoceny především z precedentů předchozích útoků Evil Corp. Těmi jsou především soukromé, státní či polostátní společnosti se značným finančním obratem, tj. odvětví manufaktury, informačních technologií, energetiky či mediálních a telekomunikační technologií, nebo nemocnice. Chráněnými hodnotami jsou pak životy a zdraví lidí v případě nemocničních zařízení, zatímco v případě soukromých společností je chráněnou hodnotou finanční kapitál či citlivé údaje.

V případě potvrzení existence vazeb mezi Evil Corp a Ruské federace prostřednictvím FSB, které jsou vzhledem k výše zmíněným informacím velmi pravděpodobné, by Evil Corp představoval hrozbu i veřejnému sektoru v ČR, resp. těm institucím státní správy, které by RF chtěla poškodit nebo vytěžit. Chráněnou hodnotou jsou tedy citlivé či utajované informace anebo funkčnost a dostupnost systémů a databází státní správy.

Evil Corp demonstroval sofistikované schopnosti v penetraci zabezpečení a sítí významných soukromých korporací, u kterých lze opodstatněně předpokládat značné investice do kybernetické bezpečnosti. Evil Corp rovněž demonstroval schopnosti provádět ransomwarové útoky se závažným dopadem na dostupnost dat. Tyto fakt v kombinaci se současným stavem kybernetické bezpečnosti u veřejných institucí v ČR (NÚKIB n.d.) vede k předpokladu, že Evil Corp by téměř jistě dokázal penetrovat a znepřístupnit sítě, databáze či data institucí státní správy v ČR.

V případě, že by Evil Corp dostal od zpravodajských služeb RF informační podporu, např. ve formě zpravodajských informací o systémech a procesech u cílových institucí, nebo podporu personálního rázu, riziko úspěšné penetrace institucí státní správy by se ještě zvýšilo. V případě ransomwarových útoků proti institucím státní správy na popud RF by účelem útoku téměř jistě nebylo způsobit finanční ztráty (v případě zaplacení výkupného), ale spíše zamezení dostupnosti sítí, databází a dat, resp. zpomalení rozhodovacích/schvalovacích procesů, v určitých kritických momentech. Rovněž lze uvažovat o využití ransomwarových útoků jako o nástroji nátlaku s cílem donutit ČR jednat v souladu se zájmy RF pod pohrůžkou zamezení dostupnosti sítí, databází a dat.

Není jisté, zda Evil Corp disponuje znalostmi a schopnostmi k provedení závažnějšího kybernetického útoku, jehož cílem by byla exfiltrace informací ze systémů či databází institucí státní správy. Byť v případě trojanu Dridex Evil Corp prokázal dílčí schopnosti útoků na důvěrnost, resp. zcizení přihlašovacích údajů do internetového bankovnictví, k exfiltraci těchto údajů byl využit pouze nástroj keylogger zaznamenávající úhozy do klávesnice. Exfiltrační útoky proti institucím státní správy jsou kvalitativně velmi odlišné od výše uvedeného útoku, jehož cílem byl zisk přihlašovacích údajů. Evil Corp by pravděpodobně k provedení úspěšného exfiltračního útoku s kvalitami APT proti institucím veřejné správy potřeboval finanční, znalostní či personální podporu ze strany ruského státu.

### *2) Identifikace nositele hrozby*

Evil Corp je etablovaná kyberkriminální skupina disponující zkušenými vývojáři. Napříč dostupnými zdroji je považováno za fakt, že Evil Corp přímo stojí za vývojem trojanu Dridex a ransomwarů BitPaymer a WastedLocker. Jedná se o velmi sofistikované malware s řadou obfuskačních mechanismů zamezující detekci, jejichž vývoj pravděpodobně trval

několik měsíců. Evil Corp rovněž vykazuje schopnosti úpravy již existujících exploit kitů a nástrojů, které upravuje, resp. vylepšuje, pro své účely (jedná se např. o nástroje Cobalt Strike či SocGholish. Mimo jiné Evil Corp využívá taktiku living off the land (LotL), při které dochází k zneužití legitimních nástrojů, které na svých systémech využívá cíl útoku (např. Powershell, PsExec). LotL je v současnosti populárním způsobem k vedení následných kroků po počátečním nakažení cíle, jelikož je hůře detekovatelný kvůli etablovaným bezpečnostním výjimkám pro dané nástroje. Nadto na straně útočníka upadá potřeba vyvíjet či přidávat do malware dodatečné nástroje pro dosažení cílů útoku.

Analýza ransomwaru dále BitPaymer ukázala, že část kódu byla v některých případech vytvořena několik hodin před útokem, čímž se významně snižuje pravděpodobnost jeho detekce. Bezpečnostní společnosti při analýzách útoků na své klienty dochází k závěru, že Evil Corp dokáže velmi rychle reagovat na detekci jejich malware v síti cíle a upravit je takovými způsoby, které umožní bez výraznější časové prodlevy pokračovat v útoku. Z tohoto vyplývá, že detekce či zastavení dílčího útoku na síť nemusí nutně znamenat úspěch obránce (Antenucci 2020; AFP 2020; ATR Operational Intelligence Team 2019; CERT-FR 2019; Lifars 2019; Osipov 2019; Threat Hunter Team 2020; Toh 2020; Trendmicro 2020).

Byť je Evil Corp vyobrazován jako autor zmíněných malwarů, nutně to neznamená, že skupina stojí za veškerými útoky provedenými pomocí nich. Velmi pravděpodobně dochází k distribuci těchto malwarů k ostatním kyberkriminálním skupinám za úplatu, případně za příslib podílu ze zisku. Může tak docházet k proliferaci směrem k jiným skupinám, jež mají na rozdíl od Evil Corp větší zkušenosti s útoky na specifický byznys či průmyslové odvětví. Tuto možnost je třeba zohlednit při výčtu potenciálních cílů, resp. cíle zasažené těmito malwary nemusí být nutně v zájmu Evil Corp.

Skupina Evil Corp v předešlých letech velmi pravděpodobně spolupracovala s jinými kyberkriminálními skupinami, jako jsou Anunak, FIN7 či TheTrick. Nejpozději od roku 2017 však spolupráce buďto utichla, nebo probíhá s vyšší mírou konspirace, což znemožňuje její vysledování. Lze však odůvodněně předpokládat, že Evil Corp disponuje vazbami a kontakty i na další kyberkriminální skupiny, což tvoří potenciál pro možnou součinnosti, ať už se jedná o vývoj malwaru, shromažďování informací, zisk přístupu k cíli anebo společné operace (CERT-FR 2019; CFCS 2020).

Evil Corp není zkostnatělou kriminální skupinou, výběr jejich cílů a modus operandi prošel a nadále prochází vývojem. Pro příklad zprvu výlučně bankovní trojan Dridex skupina přetvořila v multifunkční nástroj schopný získat vzdálený přístup do sítí a distribuovat jiné formy malwaru poté, co počty případů infekce Dridex upoutaly pozornost britských bezpečnostních složek. Využití původního trojanu k zisku finančních prostředků se tak stalo obtížnějším. Napříč rokem 2016 stál Evil Corp současně s dalšími kyberkriminálními skupinami za šířením ransomwaru Locky. Tento ransomware cílil převážně na domácnosti.

Od roku 2017 je Evil Corp ve výběru svých cílů více diskriminační a pro své útoky volí takové společnosti či instituce, které disponují značným majetkem, případně ochotou zaplatit výkupné, přičemž dominantní zastoupení mají cíle situované v USA a západní Evropě. Ve zmíněném roce Evil Corp začal své útoky prostřednictvím ransomwaru BitPaymer cílit na středně velké podniky (sektory manufaktury, zemědělství, financí). Pomocí ransomwaru BitPaymer bylo napadeno rovněž několik institucí veřejného sektoru, nemocnice a školy, zde však nelze s jistotou tvrdit, že za útoky stála skupina Evil Corp. V červnu roku 2019 demonstroval Evil Corp dovednosti úspěšně zaútočit na jedny z největších a současně nejlépe zabezpečených společností ve Spojených státech, potažmo na světě. Červnová ransomwarová kampaň vedena pomocí nově vyvinutého ransomwaru WastedLocker cílila na 31 soukromých společností etablovaných v USA. Jednalo se převážně o velké korporace, přičemž 8 z nich se se svým ročním obratem umístilo v žebříčku Fortune 500.

Z průmyslových sektorů byly nejčastěji zasaženy manufaktury, informační technologie a média a telekomunikace. Jedná se o sektory, které mohou ztrátou dat či pouhým zdržením co do dostupnosti dat utrpět značné ekonomické ztráty, tudíž u nich lze předpokládat větší platební ochotu. Od povahy cílů se pak odvíjí výše výkupného, která je v případě ransomwarů od skupiny Evil Corp ve srovnání s jinými ransomware netypicky vysoká – jedná se o částky pohybující se od 500 000 až do 10 milionů dolarů za odšifrování souborů. Nebyly nalezeny evidence o tom, že by Evil Corp hrozil zveřejněním informací získaných od obětí jako podnět k zaplacení výkupného. Pravděpodobně je tomu tak kvůli nežádoucí pozornosti od bezpečnostních složek, kterou by tento akt mohl vyvolat (CERT-FR 2019; Cimpanu 2020; Ljubas 2020; National Crime Agency 2020; News 2020; USDT 2019a; USDT 2020; Whittaker 2020).

Před samotným útokem provádí Evil Corp zevrubnou rekognoskaci cíle s cílem získat maximální množství informací k hladkému provedení útoku. Evil Corp pečlivě studuje možnosti vyřazení ochranných nástrojů na koncových zařízeních cílů. Byly zjištěny případy, kdy Evil Corp zneužil e-maily legitimních společností k zisku zkušebních licencí na ochranné nástroje, které nejsou veřejně dostupné. Zisk těchto licencí pak může sloužit k analýze bezpečnostního řešení a navržení kódu k jeho vypnutí či zamezení detekce malware. Ransomware BitPaymer pak demonstroval schopnost deaktivovat některé komerčně využívané antivirové řešení.

Nadto skupina téměř jistě sleduje a aktivně využívá aktuální trendy z oblasti kybernetické bezpečnosti a možných či nově objevených zranitelností. Např. ransomware BitPaymer efektivně utilizoval zranitelnost v bezpečnostním řešení Windows Defender, která byla prvně prezentovaná na bezpečnostní konferenci Black Hat v roce 2018 (Bulazel 2018). Jelikož náprava nově objevených zranitelností ze strany soukromého i veřejného sektoru probíhá zpravidla se zpožděním, mají kriminální skupiny dostatek času takovou zranitelnost vytěžit (Antenucci 2020; ATR Operational Intelligence Team 2019; CERT-FR 2019; Lifars 2019; Osipov 2019; Threat Hunter Team 2020; Trendmicro 2020).

Vzhledem k vektorům útoku, které Evil Corp v současnosti využívá pro doručení malware – spear phishing a wateringhole – plyne, že Evil Corp pečlivě zjišťuje informace o zaměstnancích cílové společnosti, hlavně jejich roli v organizaci a internetové návyky. O zjišťování internetových návyků zaměstnanců svědčí zejména využívání RAT nástroje SocGholish, který Evil Corp využívá k nakažení legitimních webových stránek, jež daný zaměstnanec pravidelně navštěvuje[2]. Konečným důsledkem je pak nakažení počítačových systémů buď přímo v cílené společnosti, nebo v domácím prostředí zaměstnance.

Pokud je nakažen počítačový systém v domácím prostředí zaměstnance, nutně to neznamená neúspěch útoku. Během současné pandemie COVID-19 je řada zaměstnanců soukromého i veřejného sektoru nucena pracovat z prostředí domova. K připojení se k firemním/institucionálním sítím využívají virtuální soukromé sítě (VPN). Právě skrze toto připojení dochází k rozšíření malwaru do systému cíle. Tento způsob byl využíván v případě

[2] Byť je možné uvažovat nad tím, že útočníci nejdříve infikují určitý počet nejnavštěvovanějších stránek – populárním způsobem zjištění oblíbenosti bývá např. Alexa Ranking – a k výběru cíle dochází až po zhodnocení, koho se podařilo nakazit. Tato možnost však není příliš pravděpodobná, jelikož by přinášela disproporční náklady co do zjišťování potentních cílů pro útok.

útoků ransomwaru WastedLocker (Antenucci 2020; ATR Operational Intelligence Team 2019; Lifars 2019; News 2020; Osipov 2019; Threat Hunter Team 2020; Trendmicro 2020).

Jakmile se Evil Corp podaří vstoupit do sítě cíle, probíhá její podrobné mapování. K tomuto účelu zvětší části slouží zisk administrativních opatření ke kontrole centrálních serverů. Útočník tak získá přehled o významných aktivech v síti (úložiště souborů, zálohy aj.), případně o využívání nestandardních bezpečnostních řešení. V tuto chvíli velmi pravděpodobně dochází k případné modifikaci malwaru (viz výše) za účelem snížení pravděpodobnosti jeho detekce. Poté se Evil Corpe uchyluje k instalaci ransomwaru, k té zpravidla dochází během víkendů či svátků, a to za účelem způsobení co největších škod a zpomalení reakce cíle (Antenucci 2020; Osipov 2019; Threat Hunter Team 2020; Trendmicro 2020).

Nadto se ukazuje, že jakmile se skupina Evil Corp dobere k výběru cíle, dokáže být významně trpělivá co do zisku přístupu do sítí a nenechá se odradit prvním neúspěchem (což zpravidla bývá zvykem u méně schopných aktérů). Společnost NCC Group analyzující Evil Corp zmiňuje případ, kdy byl pokus o útok této skupiny ze strany cíle poměrně brzy identifikován a zastaven, skupina však několik následujících měsíců věnovala přípravě na opětovné provedení útoku, který se uskutečnil 6 měsíců od prvního pokusu, tentokrát s úspěchem (Antenucci 2020).

Z výše uvedené charakteristiky schopností a modu operandi skupiny vyplývá, že Evil Corp je sofistikovanou kyberkriminální skupinou schopnou provést významné materiální škody. V současnosti je její zájmem velmi pravděpodobně výlučně finanční obohacení. Pokud by se se však potvrdilo napojení Evil Corp na bezpečnostní složky Ruské federace, resp. vnitřní zpravodajskou službu FSB, a pokud by tyto státní složky měly zájem a dokázaly Evil Corp přimět k aktivitám v kyberprostoru ve prospěch Ruské federace, mohlo by dojít k přetvoření Evil Corp do APT skupiny. V takovém případě by Evil Corp mohla být využita k zisku citlivých či utajovaných informací ze systémů veřejného sektoru cizích států přímo ve prospěch Ruské federace.

### *3) Stanovení míry rizika*

Vzhledem k povaze dostupných proměnných v této analýze nelze k určení míry rizika využít kvantitativní metody, resp. výpočet míry rizika. Výsledné míry rizika byly proto autory určeny na základě vícekriteriální analýzy (více viz níže) a budou se pohybovat na této škále:

- velmi nízké riziko (0-20 %),
- nízké riziko (21-40 %),
- střední riziko (41-60 %),
- vysoké riziko (61-80 %),
- velmi vysoké riziko (81-100 %).

Pro zhodnocení pravděpodobnosti útoku skupiny Evil Corp na referenční objekty soukromých, státních či polostátních entit a nemocnic byla využita následující kritéria:

a) schopnost aktéra realizovat úspěšný útok vůči referenčním objektům,
b) motivovanost provést útok vůči referenčním objektům.

Kritérium motivovanosti bylo dále rozčleněno na:

- míru potenciálního zisku, který by úspěšný útok mohl generovat,
- pravděpodobnost získání požadovaných aktiv při úspěšném útoku,
- riziko nežádoucí pozornosti plynoucí při eventuálním odhalení útoku.

**Ad a)** Schopnost skupiny Evil Corp realizovat úspěšný útok vůči referenčním objektům je napříč referenčními objekty, a teda u soukromých společností působících na území ČR, státních či polostátních podniků působící na území ČR i nemocnic na území ČR, hodnocena jako pozitivní, resp. dostatečná k provedení úspěšného útoku na sítě a databáze těchto referenčních objektů.

Skupina Evil Corp prokázala schopnosti napadnout a úspěšně penetrovat sítě a databáze vysoce výdělečných zahraničních společností, u kterých lze odůvodněně předpokládat značné výdaje na kybernetickou bezpečnost. Z míry generovaného obratu u českých či na území České republiky působících soukromých, státních či polostátních společností lze odůvodněně předpokládat, že budou tyto subjekty vynakládat poměrně menší výdaje na zajištění vlastní kybernetické bezpečnosti oproti výrazně bohatším zahraničním subjektům. Tento předpoklad pak v případě nemocnic potvrzují i výroční zprávy o stavu kybernetické bezpečnosti vydávané NÚKIB (n.d.). Z výše uvedeného vyplývá, že v případě zájmu Evil Corp zaútočit na tyto referenční objekty lze s vysokou jistotou předpokládat úspěšnost takového útoku.

**Ad b)** Motivovanost skupiny Evil Corp k provedení kybernetického útoku na tyto referenční objekty je hodnocena jako vysoce nepravděpodobná. Jestliže má Evil Corp schopnosti k provedení úspěšného útoku vůči subjektům generující výrazně vyšší zisky, a tedy potenciál i ochotu zaplatit mnohonásobně vyšší výkupné k co nejrychlejší obnově svých komerčních aktivit, nejeví se jako pravděpodobné, že by Evil Corp dedikoval svůj čas a úsilí k útoku na subjekty, ze kterých může finančně vytěžit méně, resp. útok na tyto referenční objekty je ekonomicky nevýhodný.

Nadto u státních či polostátních podniků může proti ochotě zaplatit výkupné výrazněji působit státní politika nepodléhat nátlaku útočníků a výkupné neplatit, což pravděpodobnost útoku vůči těmto subjektům snižuje. Riziko nežádoucí pozornosti důsledkem kybernetického útoku hraje dle úsudku autorů výraznější roli u státních či polostátních subjektů, zejména nemocnic. V případě útoků na tyto subjekty lze předpokládat vyšší zájem státu na prošetření takového útoku i vyšší součinnost s vyšetřovacími složkami jiných států. Taková pozornost je pro jakéhokoliv aktéra s kriminálním motivem negativní, jelikož zvyšuje šanci na jeho dopadení.

Byť tedy Evil Corp disponuje schopností k úspěšným útokům na tuto kategorii referenčních objektů, motivovanost k jejich provedení je s výjimkou soukromých společností vnímaná jako velmi nízká. U soukromých společností je riziko útoku odhadováno jako nízké, a to kvůli potenciálně relativně vyššímu finančnímu zisku a větší ochotě zaplatit výkupné, než je tomu u státních či polostátních společností či nemocnic.

### *Alternativní scénář*

Pravděpodobnostní charakter této analýzy vyplývající z povahy zkoumaného tématu nás nutí zhodnotit také riziko provedení útoku skupiny Evil Corp na podnět FSB (vzhledem k potenciálním vzájemným vazbám) proti institucím státní správy v ČR. V tomto případě byla využita již výše zmíněná kritéria spolu s novým kritériem motivovanosti k využití skupiny Evil Corp pro provedení útoků ze strany FSB:

a) schopnost Evil Corp realizovat úspěšný útok vůči referenčním objektům,
b) motivovanost Evil Corp provést útok vůči referenčním objektům,
c) motivovanost FSB využít k provedení útoků vůči referenčním objektům skupinu Evil Corp.

Kritérium motivovanosti bylo opět dále rozčleněno na:

- míru potenciálního zisku, který by úspěšný útok mohl generovat,
- pravděpodobnost získání či zničení požadovaných aktiv při úspěšném útoku,
- riziko nežádoucí pozornosti plynoucí při eventuálním odhalení útoku.

**Ad a)** Schopnosti Evil Corp úspěšně provést útok vůči institucím státní správy se liší dle typu útoku. Pokud by se jednalo o provedení útoku ransomware na popud FSB proti institucím státní správy v ČR, je schopnost realizace takového útoku vnímána jako pozitivní. Stejně jako v předchozím hodnocení schopností Evil Corp lze jejich schopnosti odvozovat od úspěšných útoků proti společnostem Fortune 500, přičemž není jisté, zda by útok na instituce státní správy vyžadoval delší či náročnější rekognoskaci cíle, např. pro realizaci útočného vektoru skrze spear-phishing či watering hole ve srovnání se zmíněnými komerčními společnostmi.

Co se týče špionážního/exfiltračního útoku proti institucím státní správy, zde nelze z empirických dat odvozovat poznatky, které by hovořily ve prospěch Evil Corp úspěšně uskutečnit takový útok. Je reálné, že by skupina dokázala penetrovat sítě a databáze institucí státní správy, avšak klíčovým požadavkem na úspěšné exfiltrační útoky je dlouhodobé udržení přítomnosti v síti cíle a schopnost dlouhodobě a nenápadně exfiltrovat data na dedikovaný řídící server. Evil Corp dosud provedl pouze dílčí exfiltrační útoky při útocích na bankovní instituce pomocí trojanu Dridex, který pro zcizení údajů využíval pouze nepříliš sofistikovaný nástroj keylogger. Zde uvažované útoky jsou kvalitativně velmi odlišné a vyžadují zcela jiné schopnosti, kterými Evil Corp v současnosti pravděpodobně nedisponuje. Lze uvažovat nad poskytnutím informací, schopností či personálu ze strany FSB pro provedení takového útoku, tato varianta je však hodnocena jako nepravděpodobná (viz Ad c).

**Ad b)** Za jinak nezměněných podmínek je motivovanost Evil Corp provést ransomwarové či špionážní útoky proti institucím státní správy v ČR vnímaná jako velmi nepravděpodobná, a to jednak z řádově nižšího potenciálního zisku i pravděpodobnosti jeho získání a řádově vyšší pozornosti ze strany složek vynucujících právo. V případě, že by FSB vyvíjela nátlak na Evil Corp provést takové útoky (např. pod pohrůžkou zatčení příslušníků skupiny), je možné, že by se motivovanost Evil Corp změnila. Tato hypotéza je však vnímaná jako velmi nepravděpodobná (viz Ad c).

**Ad c)** Motivovanost FSB využít Evil Corp k provedení útoků proti institucím státní správy v ČR je hodnocena jako velmi nepravděpodobná. Jako jedinou racionální motivaci FSB k využití Evil Corp jako proxy k provedení útoků je dílčí možnost popřít zapojení státních složek Ruské federace. Avšak z výše uvedených zdrojů vyplývá fakt, že státní orgány a agentury i soukromé kyberneticko-bezpečnostní společnosti jsou si přisouzením geografické lokace k Evil Corp velmi jisté. Stejně tak z těchto zdrojů a probíhajících vyšetřování plyne, že Rusko o působnosti Evil Corp na svém území ví a přinejmenším aktivity skupiny toleruje (alespoň prozatím). To fakticky znamená, že by FSB využitím Evil Corp k provedení útoků na instituce státní správy v ČR (ostatně i proti institucím státní správy v jiných zemích) nezískala žádoucí míru popiratelnosti. Jinými slovy, riziko zisku nežádoucí pozornosti se nezmění do takové míry, aby bylo využití Evil Corp výhodné vzhledem k nedostatků plynoucí z takového využití.

Pokud by FSB chtěla k útokům využít proxy aktéra, bylo by mnohem prozřetelnějším řešením využití takové skupiny, která není kvůli svým aktivitám na pomyslném radaru států a soukromých kyberneticko-bezpečnostních společností a jejíž přinejmenším geografický původ není znám. Nadto i pokud by se takový alternativní proxy aktér našel, lze vznést pochybnosti, že by jej FSB pro takové úkony využila. Zmíněná míra potenciálního zisku je konstantní, resp. stejná při provedení skupinou Evil Corp i službou FSB. Co se však výrazně liší je pravděpodobnost úspěchu zisku či zničení aktiv. Sama FSB disponuje schopnostmi a zdroji, které značně převyšují schopnosti a zdroje nestátních aktérů, a tak pokud útok provede sama FSB, pravděpodobnost úspěchu je vzhledem k povaze a schopnostem tohoto aktéra násobně vyšší.

### *Vyhodnocení rizik*

Z výše stanovených důvodů pak jednotlivá rizika spojená se skupinou Evil Corp stanovujeme následovně:

- Napadení soukromé společnosti působící na území ČR: ***Nízké riziko***
- Napadení státní či polostátní společnosti působící na území ČR: ***Velmi nízké riziko***
- Napadení nemocnice na území ČR: ***Velmi nízké riziko***
- Napadení státní instituce (v případě napojení na FSB): ***Velmi nízké riziko***

# ZÁVĚR

Evil Corp je ruská kyberkriminální skupina působící zejména z oblasti Moskvy. Hlavními členy této skupiny jsou Maxim Jakubec, Igor Turašev a Denis Gusev, přičemž v rámci Evil Corp dále působí několik dalších stálých spolupracovníků, a nakonec i finančních zprostředkovatelů, kteří působí mezinárodně. Evil Corp se zabývá především distribucí malwaru Dridex a ransomwaru WastedLocker, kterými cílí primárně na severoamerické a západoevropské firmy s velkým obratem. Tato skupina pravděpodobně disponuje vazbami na ruskou vnitřní zpravodajskou službu FSB (zejména skrze Maxima Jakubce), nelze je však prokazatelně potvrdit

V rámci ČR lze identifikovat celou řadu referenčních objektů, resp. potenciálních cílů kybernetických útoků. Mezi hlavní ohrožené cíle lze považovat soukromé společnosti (zejména finanční instituce) a v současnosti také nemocnice, případně jiná zdravotnická zařízení. Evil Corp pak představuje hrozbu těmto referenčním objektům, protože za účelem vlastního finančního zisku může skrze kybernetické útoky (primárně skrze využití různých typů ransomware využívaných pro zablokování dat a následné vydírání svých obětí) finančně poškodit české soukromé společnosti nebo např. ohrozit provoz nemocnic. Pokud vezmeme v potaz potenciální vazby Evil Corpu na FSB, je nutné operovat také s potenciální hrozbou napadení českých státních institucí či firem za účelem získání citlivých informací. Na základě stanovených kritérií nicméně byla veškerá rizika vyplývající z působení skupiny Evil Corp v ČR vyhodnocena jako velmi nízká až nízká.

Podle autorů je do budoucna vhodné zaměřit se také na další hackerské skupiny, které mohou ohrozit výše identifikované či jiné referenční objekty v ČR. Analýzy relevantních hackerských skupin mohou zlepšit povědomí o kybernetických hrozbách, kterým stát čelí, a napomoci tak při zajišťování kybernetické bezpečnosti v rámci ČR.

## SEZNAM ZDROJŮ


AFP. (2020). New wave of ransomware from Russian-led hackers: researchers. Indiatimes.com. Převzato z: https://cio.economictimes.indiatimes.com/news/digital-security/new-wave-of-ransomware-from-russian-led-hackers-researchers/76663508.

Antenucci, Stefano. (2020). WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group. Nccgroup.com. Převzato z: https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/.

ATR Operational Intelligence Team. (2019). Spanisg MSSP Targeted by BitPaymer Ransomware. Mcafee.com. Převzato z: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/spanish-mssp-targeted-by-bitpaymer-ransomware/.

Bulazel, Alexei. (2018). Windows Offender. Blackhat.com. Převzato z: https://i.blackhat.com/us-18/Thu-August-9/us-18-Bulazel-Windows-Offender-Reverse-Engineering-Windows-Defenders-Antivirus-Emulator.pdf.

CERT-FR. (2019). BITPAYMER/IENCRYPT RANSOMWARE. Cert.ssi.gouv.fr. Převzato z: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-CTI-006-EN.pdf.

CFCS. (2020). Do cyber criminals dream of trusting relationships? Cfcs.dk. Převzato z: CFCS-do-cyber-criminals-dream-of-trusting-relationships.pdf.

Cimpanu, Catalin. (2020). New WastedLocker ransomware demands payments of millions of USD. Zdnet.com. Převzato z: https://www.zdnet.com/article/new-wastedlocker-ransomware-demands-payments-of-millions-of-usd/.

FBI. (n.d.a). Igor Olechovich Turashev. *FBI*. Převzato z: https://www.fbi.gov/wanted/cyber/igor-olegovich-turashev.

FBI. (n.d.b) Maksim Viktorovich Yakubets. *FBI*. Převzato z: https://www.fbi.gov/wanted/cyber/maksim-viktorovich-yakubets.

Frank, L. (2006). Analýza a predikce bezpečnostních hrozeb a rizik v České republice. Disertační práce, Masarykova univerzita, Fakulta sociálních studií.

Gatlan, Sergiu. (2020, červenec 24). Garmin outage caused by confirmed WastedLocker ransomware attack. *Bleeping computer*. Převzato z: https://www.bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware-attack/.

Jennings, R. (2020, August 8). Garmin Pays Ransom to Evil Corp – Despite Russian Sanctions. Security Boulevard. Převzato z: https://securityboulevard.com/2020/08/garmin-pays-ransom-to-evil-corp-despite-russian-sanctions/.

Lifars. (2019). From Dridex to BitPaymer Ransomware to DoppelPaymer……The Evolution. Lifars.com. Převzato z: https://lifars.com/2019/11/from-dridex-to-bitpaymer-ransomware-to-doppelpaymerthe-evolution/.

Ljubas, Zdravko. (2020). Russian Evil Corp Cybercrime Group Strikes Again. Occrp.org. Převzato z: https://www.occrp.org/en/daily/12659-russian-evil-corp-cybercrime-group-strikes-again.

Meduza. (2019, prosinec 13). Минфин США исключил из санкционного списка три российские компании. Их внесли туда из-за связи с главой хакерской группы Evil Corp. Meduza.io. Převzato z: https://meduza.io/news/2019/12/13/minfin-ssha-isklyuchil-iz-sanktsionnogo-spiska-tri-rossiyskie-kompanii-ih-vnesli-v-chernyy-list-iz-za-svyazi-s-chlenom-evil-corp.

National Crime Agency. (2020) Annual Report and Accounts. Nationalcrimeagency.gov.uk. Převzato z: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/467-national-crime-agency-annual-report-and-accounts-2019-20/file.

News. (2020). Russian hacker group Evil Corp targets US workers at home. Bbc.com. Převzato z: https://www.bbc.com/news/world-us-canada-53195749.

NÚKIB. (n.d.). Zprávy o stavu kybernetické bezpečnosti. Nukib.cz. Převzato z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/.

Osipov, Arnold. (2019). Bitpaymer Ransomware Leveraging New Costum Packer Framework Against Targets Across The U.S. Morphisec.com. Převzato z: https://blog.morphisec.com/bitpaymer-ransomware-with-new-custom-packer-framework.

Russia Today. (2019, prosinec 5). Phishing thieves or yet another phantom menace? US goes after 'Russian-based Evil Corp'. RT.com. Převzato z: https://www.rt.com/news/475135-evil-corp-russian-hackers/.

Scroxton, Alex. (2019, prosinec 5). Two Russians indicted over Dridex and Zeus malware. *ComputerWeekly.com.* Převzato z: https://www.computerweekly.com/news/252475069/Two-Russians-indicted-over-Dridex-and-Zeus-malware.

Šmíd, Tomáš a Kupka, Petr. (2012). Český organizovaný zločin. Brno: MUNI Press.

Threat Hunter Team. (2020). WastedLocker: Symantec Identifies Wave of Attacks Against U.S. Organizations. Symantec.com. Převzato z: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us.

Toh, Ardan. (2020). WastedLocker Ransomware. Proficio.com. Převzato z: https://www.proficio.com/wastedlocker-ransomware/.

Trendmicro. (2020). BitPaymer Malware Information. Trendmicro.com.Převzato z: https://success.trendmicro.com/solution/000261855.

USDT (2019b, prosinec 5). Cyber-related Designations; Counter Terrorism Designation Removal. *US Department of the Treasury.* Převzato z: https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20191205.

USDT (2020, říjen 1). Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments Převzato z: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf?_sm_au_=iVVLSMkbnTNQDfnMvMFckK0232C0F.

USDT. (2019a, prosinec 5). Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware. *US Department of the Treasury.* Převzato z: https://home.treasury.gov/news/press-releases/sm845.

Whittaker, Zack. (2020). Garmin confirms ransomware attack took down services. Techcrunch.com.Převzato z: https://techcrunch.com/2020/07/27/garmin-confirms-ransomware-attack-outage/?guccounter=1.

Yapparova, Liliya. (2019, prosinec 12). The FSB's personal hackers. Meduza.io. Převzato z: https://techcrunch.com/2020/07/27/garmin-confirms-ransomware-attack-outage/?guccounter=1.

Zeman, P. (2002a). Hrozba a riziko. In Zeman, P. (ed.) Česká bezpečnostní terminologie: Výklad základních pojmů. Brno: Masarykova univerzita a Ústav strategických studií Vojenské Akademie v Brně, 85-96.

Zeman, P. (2002b). Důležité pojmy analýzy rizik a rovnice rizika. In Zeman, P. (ed.) Česká bezpečnostní terminologie: Výklad základních pojmů, 60-66.

Пудовкин, Евгений. (2019, prosinec 5). Lamborghini с номером «ВОР»: кого США и Британия назвали хакерами из Evil. RBC.ru. Převzato z: https://www.rbc.ru/politics/05/12/2019/5de92ddb9a7947227d0e62ba.

Шимаев, Роман. (2019, prosinec 6). «Навешивают на Россию ярлык киберпреступника»: США ввели санкции против якобы связанных с ФСБ хакеров. RT.com. Převzato z: https://russian.rt.com/world/article/694535-ssha-sankcii-fbr-hakery-rossiyane.

# PŘÍLOHA 1

### *Členská základna skupiny Evil Corp*

Základním zdrojem pro data o členech a struktuře Evil Corp bylo tiskové prohlášení Úřadu kontroly zahraničních aktiv Ministerstva financí USA (U.S. Department of Treasury, Office of Foreign Assets Control, dále též 'OFAC'). Dne 5. 12. 2019 přikročil OFAC k vyhlášení sankcí a blokaci veškerého majetku Evil Corp, sedmnácti jednotlivců, kteří mají přímý podíl na aktivitách Evil Corp nebo napomáhali, sponzorovali nebo poskytovali materiální či technickou pomoc, zboží či služby ve prospěch Evil Corpu či společností, ve kterých působí Denis Gusev jako generální ředitel.

| Hlavní podezřelí, resp. stálí členové skupiny Evil Corp (dle zprávy OFAC 6/12/2019): |
|---|
| • JAKUBEC, Maxim Viktorovič<br>• TURAŠEV, Igor Olegovič<br>• GUSEV, Denis Alexandrovič |
| Osoby, které dle dostupných zdrojů spolupracují se skupinou Evil Corp: |
| • JAKUBEC, Artem Viktorovič<br>• SMIRNOV, Dmitrij Konstantinovič<br>• TUČKOV, Ivan Dmitrijevič<br>• PLOTNITSKIJ, Andrej (též KOVALSKIJ, Andrej Vjačeslavovič; též STREL, Andrej)<br>• SLOBODSKOJ, Dmitrij Alexejevič<br>• SLOBODSKOJ, Kirill Alexejevič |
| Další osoby perzekuované USDT kvůli poskytování finančního zprostředkovatelství ve prospěch Evil Corp (dle OFAC 6/12/2019): |
| • ALVARES, Carlos<br>• BAŠLIKOV, Alexej<br>• BURCHONOVA, Gulsara<br>• GUBERMAN, David<br>• MANIDIS, Georgios<br>• SAFAROV, Azamat<br>• ŠEVČUK, Tatiana<br>• ZAMULKO, Ruslan |

STRATPOL – Strategic Policy Institute
Štúrova 3, 81102 Bratislava, Slovensko
office@stratpol.sk | www.stratpol.sk

CyberSec.SK
Na vŕšku 8, 811 01 Bratislava, Slovensko
info@cybersec.sk | www.cybersec.sk
ISSN 2729-840X