Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č. j. 1216/2025-NÚKIB-E/630 • BRNO • 16. DUBNA 2025
STRATEGICKÁ ANALÝZA

ÚTOKY HARVEST NOW, DECRYPT LATER: ÚTOČNÍCI MOHOU JIŽ DNES ZÍSKÁVAT DATA K POZDĚJŠÍMU PROLOMENÍ ŠIFROVÁNÍ KVANTOVÝM POČÍTAČEM, ŘEŠENÍM JE VČASNÁ IMPLEMENTACE POSTKVANTOVÉ KRYPTOGRAFIE

SHRNUTÍ

- **Kvantové počítače mají potenciál překonat současné počítače, čímž ale zároveň ohrožují bezpečnost asymetrických šifrovacích standardů. Přestože jejich praktické nasazení je téměř jistě (90–100 %) vzdálenější jak pět let, útočníci mohou s výhledovým využitím kvantových počítačů kalkulovat již dnes.**
- **Už v současnosti mohou útočníci získávat a hromadit data k budoucímu prolomení s metodou nazývanou HNDL – „harvest now, decrypt later" („získej nyní, dešifruj později"). Jedná se o státem sponzorované aktéry, kteří mohou kalkulovat s tím, že budou v horizontu 15 let kvantovými počítači disponovat.**
- **Ačkoliv je z povahy věci těžké HNDL odhalit, je reálná možnost (40–50 %), že již dnes takto motivované útoky probíhají, a je pravděpodobné (55–70 %), že budou probíhat v následujících letech, než dojde k plošnému přijetí postkvantové kryptografie.**
- **Implikace pro ČR: Přechod na postkvantovou kryptografii a mitigace rizik HNDL představují globální výzvu a aktéři hrozeb mohou cílit i na ČR. Klíčový bude význam potenciálních odcizených dat pro útočníka. Ten bude muset při výběru dat pro prolomení brát v potaz náročnost takového úkonu a prioritizovat.**
- **DOPORUČENÍ: Nejefektivnější mitigací rizika HNDL útoků je včasná implementace postkvantových šifrovacích standardů. NÚKIB toto reflektuje skrze její zahrnutí do minimálních požadavků na kryptografické algoritmy.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z informací partnerů NÚKIB, z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Jedná se o analýzu kybernetické bezpečnosti z pohledu NÚKIB na základě jemu dostupných informací.

Jedním z praktických způsobů, jak využít unikátní vlastnosti kvantové mechaniky, jsou kvantové počítače. Tato zařízení mají potenciál během příštích dekád v některých aspektech výrazně předčit schopnosti současných počítačů a způsobit revoluci v mnoha oblastech lidské činnosti. **Zároveň však představují hrozbu pro bezpečnost aktuálně používaných asymetrických šifrovacích standardů (viz Box 1).** Kvantové počítače procházejí intenzivním vývojem a přitahují velké investice.[1] Přesto je obtížné stanovit jasný trend jejich budoucího vývoje. **Je téměř jisté (90–100 %), že nebudou schopny prolomit současnou kryptografii dříve než za pět let. Hrozbu ale představují již dnes skrze možnost útoků na data pro prolomení v budoucnosti.**

BOX 1: Symetrická a asymetrická kryptografie

Symetrická kryptografie používá jeden společný klíč pro šifrování i dešifrování, což znamená, že tento klíč musí být předem bezpečně přenesen mezi stranami. Asymetrická kryptografie naproti tomu využívá dvojici klíčů – veřejný a soukromý –, což umožňuje bezpečně navázat komunikaci i s dosud neznámým účastníkem, protože veřejný klíč lze volně sdílet. Symetrická kryptografie je výrazně rychlejší a méně náročná na výpočetní výkon, což ji činí vhodnou pro šifrování velkého množství dat (jako je například šifrování disků) nebo online komunikaci po bezpečné výměně klíčů. Na druhou stranu asymetrická kryptografie hraje klíčovou roli při distribuci šifrovacích klíčů a autentizaci uživatelů nebo systémů a je základem zabezpečené internetové komunikace (například TLS v rámci protokolu HTTPS).

SOUČASNÉ ASYMETRICKÉ ŠIFROVÁNÍ KVANTOVÉMU POČÍTAČI NEODOLÁ, ÚTOČNÍK SI MŮŽE PROTO JIŽ DNES DATA UKLÁDAT

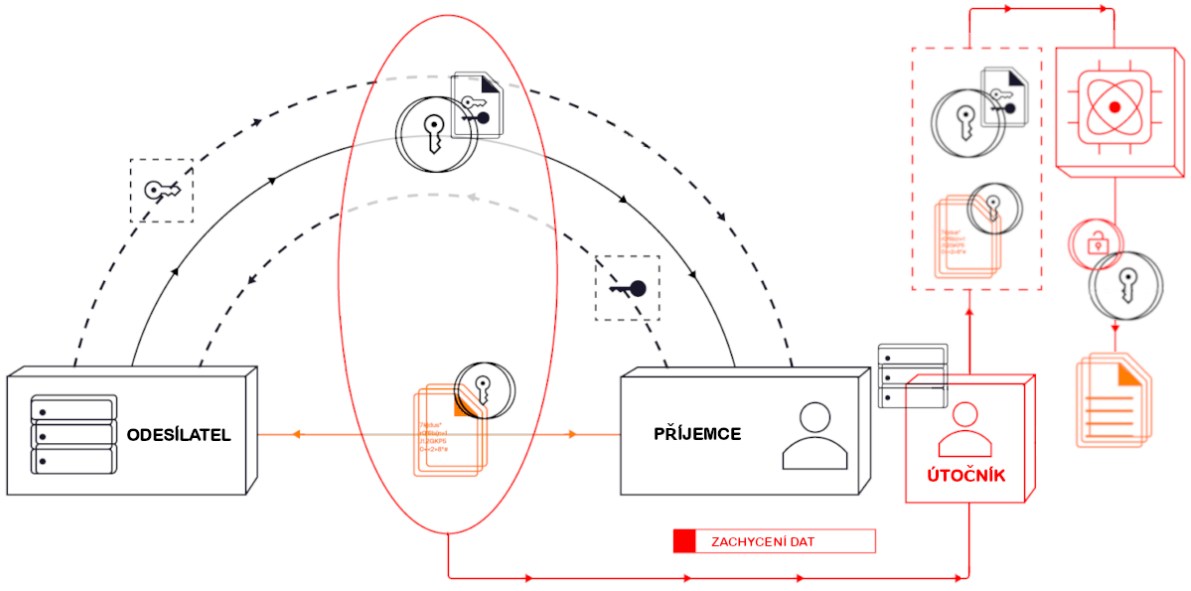
Praxe získávání dat pro pozdější prolomení se nazývá HNDL – „harvest now, decrypt later" („získej nyní, dešifruj později"). Cílem takového útoku je pro útočníka získat data pro prolomení, i když si je vědom, že v současnosti nedisponuje prostředky k tomu data rozšifrovat, ale spoléhá na to, že jimi v budoucnu disponovat může nebo bude. V principu se nejedná o nový koncept, ale s kvantovými počítači nabírá na významu. Kvantové počítače totiž budou velmi pravděpodobně (75–85 %) schopny ohrozit většinu dnes dominantních forem asymetrické kryptografie jako RSA, ECC, DH nebo DSA.[2] Algoritmy, které by mohly tyto formy šifrování prolomit, jsou přitom dlouhodobě známé (Shorův algoritmus byl publikován v roce 1994), prolomení je tedy primárně otázkou existence dostatečně výkonného (kvantového) hardwaru.

Prolomení těchto šifrovacích standardů kvantovými počítači by mělo zásadní dopady na bezpečnost digitální infrastruktury, soukromí uživatelů, ekonomiku, a tudíž celkově i národní a globální bezpečnost. **Pro útočníka, který má výhled na to, že by k takovému počítači mohl mít v horizontu pěti až patnácti let přístup, proto vzniká motivace již dnes tato data získávat a ukládat k pozdějšímu prolomení.** Jeho motivaci dále zvyšuje blížící se nástup nové kryptografie, která kvantovým útokům zabrání, a současné pokroky ve vývoji kvantových počítačů. Pro útočníka se tak zvyšuje šance, že kvantový útok bude možný, a zároveň se mu zkracuje okno, po jehož dobu jsou data zašifrována kvantově zranitelnou kryptografií.

HNDL ÚTOKY SE JIŽ MOŽNÁ DĚJÍ, JEJICH DETEKCE JE ALE OBTÍŽNÁ. PODEZŘELÍ JSOU STÁTEM PODPOROVANÍ AKTÉŘI

Existuje reálná možnost (40–50 %), že již dnes HNDL útoky probíhají, resp. že probíhá jejich první fáze, kdy útočníci shromažďují data k pozdějšímu prolomení. Problémem s rizikem HNDL útoků je však jejich vysoce obtížná detekovatelnost, průkaznost a mitigovatelnost. Případný útočník má totiž širokou škálu možností, jak zachycovat posílaná data na internetu (kompromitace síťové infrastruktury, útoky odklánějící internetový provoz – viz Příloha 1). Z tohoto důvodu je významná role efektivní kryptografie, která ochrání data i v případě jejich zachycení. Problematické je především, že je prakticky nemožné zjistit, jak útočník nakládá s odcizenými daty. Zda útočník následně bude skutečně disponovat kvantovým počítačem schopným prolomit současné šifrování (tzv. kryptograficky relevantní kvantový počítač) a odcizená data pomocí kvantového počítače dešifruje, je obtížné předvídat.

Obrázek 1: Schéma HNDL útoku



Zdroj: thesslstore.com

Záležet bude primárně na významu dat a schopnostech útočníka (viz Box 2).

BOX 2: Relevantní témata a prioritizace výkonu

Existuje řada druhů dat, které mohou mít pro útočníka cenu i po patnácti a více letech. Například se jedná o:

- Osobní údaje (jména, rodná čísla, čísla zdravotního pojištění a dokladů atd.)
- Zdravotní záznamy (dlouhodobé diagnózy, biometrické údaje)
- Finanční záznamy (historie transakcí, obchodní vazby)

Jaká data se stanou cílem, se proto bude téměř jistě (90–100 %) odvíjet od priorit a cílů útočníka, který kryptograficky relevantním kvantovým počítačem bude disponovat. Je velmi pravděpodobné (75–85 %), že první iterace kryptograficky relevantních kvantových počítačů bude stále vyžadovat významný čas a prostředky na prolomení kryptografických prvků.

Vzhledem k náročnosti a nákladnosti získání a provozu kvantového počítače se jako možní hlavní aktéři HNDL útoků jeví vyspělé státy. Pachateli první fáze HNDL útoků ale mohou být i kyberkriminální skupiny, které data následně prodávají. Od roku 2010 byla zaznamenána řada podezřelých tzv. deflection útoků (viz Příloha 1), kdy byl zašifrovaný provoz odkláněn například do Ruska nebo Čínské lidové republiky (ČLR).[3] Ačkoliv motivace těchto incidentů není jasně prokazatelná, HNDL útoky jsou jednou z možných motivací.[4] **Poradní výbor prezidenta USA pro bezpečnost telekomunikací (NSTAC) pak v roce 2024 deklaroval, že již můžeme pozorovat útoky s HNDL motivem.[5]** Na pravděpodobnosti HNDL útoků přidává rovněž existence a aplikace postkvantového šifrování (viz níže), které zkracuje okno, během kterého mohou útočníci využitelná data hromadit, a motivuje je tak k co nejrychlejšímu jednání na tomto poli (viz kapitola Implikace). **Je proto reálná možnost (40–50 %), že tyto útoky již dnes probíhají, a je pravděpodobné (55–70 %), že se tyto útoky budou dít v horizontu pěti let.**

POSTKANTOVÁ KRYPTOGRAFIE KVANTOVÝM POČÍTAČŮM ODOLÁ, ALE JEJÍ IMPLEMENTACE JE V POČÁTCÍCH

Riziko kvantových počítačů pro kryptografické algoritmy je dlouhodobě známé. Shorův algoritmus, jenž by na dostatečně výkonném kvantovém počítači mohl šifrování ohrozit, byl publikován v roce 1994.[6] Pokroky ve vývoji kvantových počítačů v druhé dekádě 21. století pak následně vedly k obávám o možnou realizaci kvantových útoků. **Proto jsou aktivně přijímána opatření, jak kvantovým útokům zabránit. Primárním nástrojem je tzv. postkvantová kryptografie, nové šifrovací algoritmy, jež by měly kvantovým počítačům odolat.** Americký Národní institut standardů a technologie (NIST) pořádal mezinárodní soutěžní program, z nějž vzešly nové šifrovací standardy odolné vůči kvantovým útokům (viz Box 3).[7]

BOX 3: Soutěž NIST a vítězné algoritmy

Soutěž o postkvantové šifrování je iniciativou NIST, jejímž cílem je vytvořit standardy kryptografických algoritmů odolných vůči útokům ze strany kvantových počítačů.

Soutěž byla zahájena v roce 2016 v reakci na zrychlující se vývoj kvantových počítačů a s ním stoupajícím rizikem možného prolomení tradičních asymetrických šifrovacích metod (např. RSA, ECC) pomocí kvantových algoritmů, jako je Shorův algoritmus.[8]

Tyto algoritmy využívají odlišné matematické principy než současné šifrovací metody, **přičemž téměř jistě (90–100 %) nejsou zranitelné kvantovými útoky.** Navíc jsou tyto matematické operace zároveň proveditelné i se současným běžně dostupným hardwarem, a neměly by proto představovat velkou zátěž z hlediska implementace. **Postkvantové algoritmy proto začínají být v současnosti implementovány.**

IMPLIKACE: ÚTOČNÍCI MAJÍ MOTIVACI USPÍŠIT HNDL ÚTOKY, ŘEŠENÍM JE NASAZENÍ POSTKVANTOVÉ KRYPTOGRAFIE

Současný vývoj na poli postkvantové kryptografie vytváří prostředí, které útočníky motivuje ke snahám o provádění HNDL útoků. Vzhledem k existenci a implementaci šifrování, jež kvantovým počítačům téměř jistě (90–100 %) odolá, se útočníkům zkracuje

množství času, kdy mohou získat data zašifrovaná s pomocí dnešních nedostatečných standardů. **Zároveň potenciální oběti mohou v současnosti ještě hrozbu kvantových počítačů nedostatečně reflektovat, vzhledem k relativně pomalému vývoji kvantových počítačů a podcenění HNDL rizik.** Pro útočníky tak potenciálně vzniká v následujících pěti letech silná motivace využít příležitosti, než implementace postkvantové kryptografie nabere setrvačnost. **To pravděpodobně (55–70 %) povede k množství takto motivovaných útoků v následujících pěti letech.** Vzhledem k tomu, že plošná implementace postkvantové kryptografie je na počátku, prostor pro HNDL bude v tomto horizontu stále významný (byť se bude průběžně zmenšovat).

Problematika kvantových útoků, postkvantového šifrování a HNDL je globální, a dotýká se proto i ČR. **Je pravděpodobné (55–70 %), že se ČR v následujících pěti letech stane cílem útoku odklánějícího internetový provoz (viz Příloha 1) nebo jiné formy úniku dat, při kterém dojde k získání dat s potenciální hodnotou pro HNDL.** Nelze vyloučit (40–50 %), že se některá z těchto dat stanou během následujících patnácti let cílem kvantového útoku. Zda budou data českých subjektů a občanů vystavena tomuto útoku, závisí především na prioritizaci výpočetního výkonu (viz Box 2) a skrze to na povaze a prioritách útočníka, který bude daným kvantovým počítačem disponovat.

BOX 4: Souhrn dosavadních aktivit NÚKIB směrem k přechodu na postkvantovou kryptografii

Hlavní zájmovou oblastí NÚKIB ve sféře kvantových technologií je zajištění přiměřené reakce na kvantovou hrozbu. Tu lze v současnosti řešit implementací postkvantové kryptografie. NÚKIB proto v současnosti doporučuje přechod k této kvantově odolné kryptografii, která sice nepředstavuje kvantovou technologii jako takovou, jedná se však o úzce související technologii a zásadní nástroj mitigace kvantové hrozby. Aktuálním výstupem NÚKIB je tak sada materiálů, které mají za úkol usnadnit přechod na postkvantové šifrování – konkrétně to jsou minimální požadavky na kryptografické algoritmy, jejich příloha a osvětový dokument ke kvantové hrozbě. Kromě toho je NÚKIB angažovaný v projektech souvisejících s kvantovými technologiemi jako takovými.

DOPORUČENÍ: VČASNÁ A SPRÁVNÁ IMPLEMENTACE POSTKVANTOVÉ KRYPTOGRAFIE EFEKTIVNĚ MINIMALIZUJE RIZIKA HNDL ÚTOKŮ

Hlavním řešením pro kybernetickou bezpečnost v kontextu kvantových počítačů a HNDL útoků je dokončená soutěž NIST a následná implementace vítězných algoritmů. Implementace těchto algoritmů velmi pravděpodobně (75–85 %) ochrání data před kvantovým útokem i v případě, že budou odcizena.

NÚKIB reflektuje potřebu včasné implementace postkvantové kryptografie skrze její zahrnutí do minimálních požadavků na kryptografické algoritmy.

Vzhledem k tomu, že se jedná o nové algoritmy a je zde potřeba zvážit co nejdříve jejich implementaci, klíčovým aspektem pro úspěšné nasazení postkvantové kryptografie bude koncepce kryptografické pružnosti (Cryptographic Agility), tedy schopnosti rychle měnit či kombinovat šifrovací standardy.

Pro úspěšnou implementaci nejen nových šifrovacích standardů, ale i jakýchkoli dalších prvků kybernetické bezpečnosti, by měl být používán aktuální software a pokud možno i hardware. V rámci co nejrychlejší implementace postkvantového šifrování je možné jej kombinovat s jinou osvědčenou konvenční kryptografií v hybridním řešení.

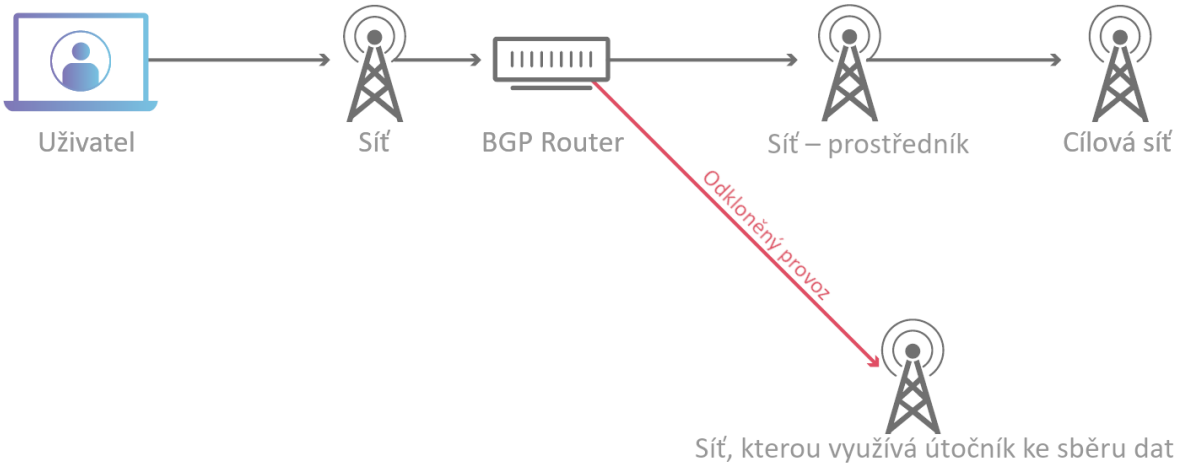
PŘÍLOHA 1: ÚTOKY NA PROTOKOL BGP S CÍLEM ODKLONĚNÍ KOMUNIKACE

Border Gateway Protocol (BGP) je protokol používaný pro výměnu směrovacích informací mezi autonomními systémy na internetu. Je základem fungování internetu, protože umožňuje jednotlivým sítím komunikovat a najít nejefektivnější cestu pro přenos dat.

Útok odklánějící komunikaci (alternativně též BGP highjacking) spočívá v tom, že útočníci záměrně přesměrují internetový provoz. Toho dosahují tím, že falešně oznamují vlastnictví skupin IP adres, tzv. IP prefixů, které ve skutečnosti nevlastní, neovládají a nesměřují na ně.

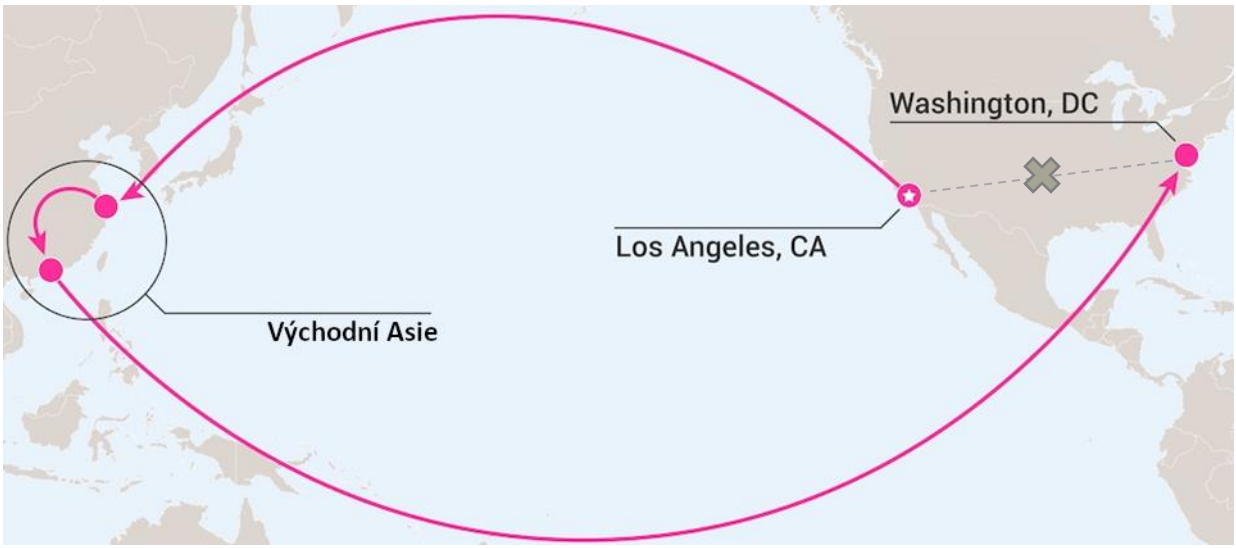
V důsledku odklonění skrze narušení protokolu BGP může být internetový provoz veden špatným směrem, může být monitorován nebo zachycen, nebo může být přesměrován na falešné webové stránky jako součást útoku na cestě.

Obrázek 2: Schéma útoku na protokol BGP s cílem odklonění komunikace



Zdroj: cloudflare.com

Obrázek 3: Diagram internetového provozu odkláněného skrze ČLR v roce 2017



Zdroj: Arstechnica.com

ZDROJE

[1] Quantum Technology Monitor. 2022. McKinsey & Company. quantum–technology–monitor.pdf (mckinsey.com)
[2] **Mastercard.** "Threats Posed by Quantum Computing to Public Key Encryption." *Mastercard Developers*, 2022. https://developer.mastercard.com/blog/threats_posed_by_quantum_computing_to_public_key_encryption/.
[3] Jeff Ferry. "Experts Say China Telecom Diverted US Internet Traffic Through China." *Coalition For A Prosperous America*, November 8, 2018. https://prosperousamerica.org/experts-say-china-telecom-diverted-us-internet-traffic-through-china/, McCullagh, Declan. "Web Traffic Redirected to China Still a Mystery." *CNET*, November 19, 2010. https://www.cnet.com/news/privacy/web-traffic-redirected-to-china-still-a-mystery/., Saarinen, Juha. "China Systematically Hijacks Internet Traffic: Researchers." *iTnews*, October 26, 2018. https://www.itnews.com.au/news/china-systematically-hijacks-internet-traffic-researchers-514537, Wilson, Tim. "U.S.-Based Internet Traffic Was Redirected To China, Researchers Say." *Dark Reading*, November 17, 2010. https://www.darkreading.com/cyber-risk/u-s--based-internet-traffic-was-redirected-to-china-researchers-say., Goodin, Dan. "How China Swallowed 15% of 'Net Traffic for 18 Minutes." *Ars Technica*, November 17, 2010. https://arstechnica.com/information-technology/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes/, Goodin, Dan. "'Suspicious' Event Routes Traffic for Big-Name Sites through Russia." *Ars Technica*, December 13, 2017. https://arstechnica.com/information-technology/2017/12/suspicious-event-routes-traffic-for-big-name-sites-through-russia/.
[4] Je velmi pravděpodobné (75–85 %), že tyto útoky měly širší spektrum cílů, jako zachycování nezašifrovaných dat, zachycování šifrovaných dat prolomitelných konvenčními zranitelnostmi atd. HNDL zůstává ale jednou z reálně možných (40–50 %) motivací.
[5] Greig, Jonathan. "'Store Now, Decrypt Later': US Leaders Prep for Quantum Cryptography Concerns." *The Record*, August 28, 2024. https://therecord.media/us-leaders-prep-for-quantum-cryptography-concerns
[6] Utimaco. "What Is Shor's Algorithm?" *Utimaco*, https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-shors-algorithm.
[7] A Guide to Post–Quantum Cryptography. 2022. Trail of Bits. A Guide to Post–Quantum Cryptography | Trail of Bits Blog
[8] National Institute of Standards and Technology. "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms." *NIST*, July 5, 2022. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP:RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou–li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP:AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need–to–know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Oranžová **TLP:AMBER**	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need–to–know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Zelená **TLP:GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP:CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

PRAVDĚPODOBNOSTNÍ VÝRAZY NÚKIB

Výraz	Pravděpodobnost
Téměř jistě	*90–100 %*
Velmi pravděpodobně	*75–85 %*
Pravděpodobně	*55–70 %*
Nelze vyloučit/Reálná možnost	*40–50 %*
Nepravděpodobně	*20–35 %*
Velmi nepravděpodobně	*0–15 %*