# Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

## 15. března proběhne Cybersecurity Standardisation Conference 2022

Je otevřena registrace na šestý ročník Cybersecurity Standardisation Conference, která je připravována unijními normalizačními orgány (CEN, CENELEC, ETSI) ve spolupráci s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA). Mezi témata, která se budou řešit, patří například umělá inteligence, digitální identita a ochrana dat. Cílem je podpořit dialog mezi policy-makers, průmyslem a dalšími organizacemi za účelem efektivní implementace unijní legislativy v oblasti kybernetické bezpečnosti. Více informací o akci zde.

## GAČR vyhlásila soutěže pro rok 2023

Grantová agentura České republiky (GAČR) vyhlásila výzvy k podávání návrhů projektů do soutěží pro standardní projekty, EXPRO, JUNIOR STAR, POSTDOC INDIVIDUAL FELLOWSHIP a mezinárodní Lead Agency projekty. Návrhy je možné podávat do 7. dubna 2022, výsledky by měly být známy v listopadu a prosinci letošního roku. Konkrétní podmínky k podávání projektů zde.

## Otevřené výzvy v programu Horizont Evropa

Od konce ledna jsou otevřeny výzvy programu Horizont Evropa, aktuálního rámcového programu EU pro výzkum a inovace, týkající se například umělé inteligence, big data a demokracie či problematiky edge computingu. Deadline pro podání výzev je v průběhu měsíce dubna.

## ENISA a CERT-EU: vydání společné publikace s osvědčenými postupy v oblasti kybernetické bezpečnosti

Ve světle narůstajících kybernetických hrozeb pro soukromé i veřejné organizace v EU byla ve spolupráci CERT-EU s agenturou ENISA vydána publikace Boosting Your Organisation's Cyber Resilience obsahující sadu osvědčených postupů s cílem posílit kybernetickou odolnost EU. Vydání publikace je pokračováním strukturované spolupráce mezi oběma institucemi, která má za cíl budovat kapacity, sdílet informace a znalosti. Publikace je k dispozici zde.

## MŠMT klade důraz na kyberprevenci a digitalizaci ve školách

V reakci na Den bezpečnějšího internetu, který se konal 8. února 2022 formou tiskové konference pod záštitou Ministerstva vnitra, je kladen větší důraz na oblast digitalizace a kyberprevence ve školách. Od roku 2022, v rámci Národního plánu obnovy, Ministerstvo školství, mládeže a tělovýchovy (MŠMT) připravuje poskytnutí finančních prostředků na využití digitálních technologií pro školy (více informací zde) a rozšiřuje činnost v oblasti kyberprevence. Ve spolupráci s NÚKIB došlo k aktualizaci kurzu Dávej kyber pro učitele, který pokrývá téma základů kybernetické bezpečnosti s důrazem na školní prostředí.

## Hackeři využívají platformu Microsoft Teams pro šíření malware

(17. 2. 2022; helpnetsecurity.com) Útočníci zneužívají zvyšující se oblíbenosti aplikace Microsoft Teams k šíření malware skrze posílání škodlivých příloh. Spuštěním těchto příloh dochází ke stažení malware, který dokáže vzdáleně převzít kontrolu nad počítačem. Aktéři k získání přístupu do aplikace využívají phishingové útoky a odcizené přihlašovací údaje z ukradených či uniklých databází. Po zajištění přístupu útočníci připojí do chatu .exe soubor s názvem „User Centric“, který imituje podobu legitimního souboru od uživatele, ale ve skutečnosti je to trojský kůň. S ohledem na zveřejnění názvu souboru lze očekávat, že útočníci začnou používat jiný.

**Komentář:** Aktéři se v důsledku pandemie COVID-19, která donutila mnoho organizací pracovat distančně, začali zaměřovat na videokonferenční platformy, jejichž obliba značně vzrostla. Stažením trojského koně tvářícího se jako soubor od důvěryhodného uživatele získávají útočníci možnost vzdálené správy počítače, exfiltrace uživatelských dat a jejich odeslání útočníkovi, případně spouštění škodlivého softwaru pro vlastní účely.

## Byly zveřejněny dešifrovací klíče pro Maze/Egregor/Sekhmet ransomware

(10. 2. 2022; threatpost.com) Dle dostupných informací byly zveřejněny dešifrovací klíče pro všechny tři typy ransomware (Maze, Egregor, Sekhmet). Gang Maze, dříve jeden z nejaktivnějších ransomwarových gangů a průkopník taktiky dvojitého vydírání, údajně zničil všechny zdrojové kódy k ransomware a k této činnosti se už nikdy nevrátí. Zveřejnění kódů tak přichází po více než roce po ohlášení ukončení činnosti skupiny v listopadu 2020.

**Komentář:** Četnost ransomwarových útoků se celosvětově zvyšuje, ransomware představuje jednu z nejzávažnějších kybernetických hrozeb současnosti. Cílem takového útoku je zašifrování souborů a záloh oběti a požadování výkupného za jejich odblokování. V případě taktiky dvojitého vydírání pak dochází ještě k vyhrožování zveřejnění dat v případě nespolupráce. Jednou z nových strategií je trojité vydírání, kdy je požadováno výkupné také po klientech či dodavatelích oběti.

## Nový botnet Kraken útočí také na krypto peněženky

(16. 2. 2022; zerofox.com) Výzkumníci ze společnosti ZeroFox objevili novou variantu botnetu, který je aktivně využíván škodlivými aktéry k instalaci zadních vrátek s cílem krádeže citlivých dat. Dle dostupných informací botnet využívá SmokeLoader malware, který vede k instalaci dalšího škodlivého softwaru a umožňuje rozsáhlé šíření. V současné době se Kraken umí vyhnout detekci Windows Defender a dokáže shromažďovat informace o hostiteli, stahovat a spouštět soubory, pořizovat snímky obrazovky a krást peněženky s kryptoměnami.

**Komentář:** S narůstající oblibou kryptoměn se hackeři snaží hledat nové způsoby, jakými se k těmto zdrojům dostat. Odborníci proto v tomto roce předpovídají nárůst kybernetických útoků na peněženky s kryptoměnami.

Oddělení výzkumu a evropské spolupráce, NÚKIB