136 bezplatných nástrojů proti ransomwaru

MĚLNICKO - Zasáhl vás ransomware? No More Ransom nyní nabízí 136 bezplatných nástrojů pro záchranu vašich souborů.

Dešifrovací nástroje si již stáhlo více než 10 milionů lidí

Počet a závažnost ransomwarových útoků po léta narůstá, přičemž požadavky na výkupné se vyšplhaly na částky, které byly dříve nemyslitelné. I když jsou data alarmující, neznamená to, že jste bezmocní proti high-tech vyděračům, kteří tyto útoky organizují. Iniciativa „No More Ransom“ nabízí přes sto bezplatných dešifrovacích nástrojů pro záchranu vašich souborů.

Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování Policie České republiky, která má ve své gesci potírání kybernetické kriminality, se již před lety zapojila do tohoto úspěšného projektu.

Iniciativa „No More Ransom“, která nyní slaví své šesté výročí, poskytuje klíče k odemykání zašifrovaných souborů a rovněž informace o tom, jak se především infekci ransomwarem vyhnout.

Portál „No More Ransom“ spuštěný v roce 2016 Europolem, nizozemskou policií (Politie) a IT bezpečnostními společnostmi zpočátku nabízel čtyři nástroje pro odemykání různých typů ransomwaru a byl dostupný pouze v angličtině. O šest let později „No More Ransom“ nabízí 136 bezplatných nástrojů pro 165 variant ransomwaru, včetně Gandcrab, REvil/Sodinokibi, Maze/Egregor/Sekhmet a dalších. Do schématu se zapojilo více než 188 partnerů z veřejného i soukromého sektoru, kteří pravidelně poskytují nové dešifrovací nástroje pro nejnovější druhy škodlivého softwaru.

K dnešnímu dni tento systém pomohl více než 1,5 milionu lidí úspěšně dešifrovat jejich zařízení, aniž by museli platit zločincům. Portál je dostupný ve 37 jazycích, aby lépe pomáhal obětem ransomwaru po celém světě.

Není lepší léčba než prevence

Nejlepším lékem proti ransomwaru zůstává pečlivá prevence. Důrazně vám doporučujeme:

- Pravidelně zálohujte data uložená na vašich elektronických zařízeních.
- Sledujte klikání – víte, kam vás odkaz zavede?
- Neotevírejte přílohy v e-mailech od neznámých odesílatelů, i když vypadají důležitě a věrohodně.
- Ujistěte se, že váš bezpečnostní software a operační systém jsou aktuální.
- K ochraně vašich uživatelských účtů použijte dvoufaktorové ověření (2FA).
- Omezte možnost exportu velkého množství podnikových dat na externí portály pro výměnu souborů.
- Pokud se stanete obětí, neplaťte! Nahlaste zločin a navštivte www.nomoreransom.org pro dešifrovací nástroje.

Další informace a tipy k prevenci najdete na **www.nomoreransom.org**

kpt. PhDr. Růžena Randáková, Ph.D.
NCOZ SKPV