Vysokoškoláci pomáhají aktualizovat forenzní aplikaci Maldump

25.9.2023 - | Národní úřad pro kybernetickou a informační bezpečnost

V případech napadení počítače obdrží analytik obraz disku, přičemž jedním ze stěžejních zdrojů informací jsou soubory umístěné v karanténě. Pokud má analytik přístup pouze k offline datům z počítače, neexistuje snadný způsob, jak se k souborům v karanténě dostat a analyzovat je. Maldump je nástroj, který je u podporovaných antivirových řešení schopen exportovat tyto soubory přesunuté do karantény.

Projekt Maldump je vyvíjen jako tzv. open source pod licencí GPL-3.0 a je zveřejněný na GitHubu (https://github.com/NUKIB/maldump). Open source v praxi znamená, že zdrojový kód je veřejně dostupný, díky čemuž může komunita vývojářů kontrolovat případné chyby a zároveň se podílet na vývoji. Maldump aktuálně podporuje deset antivirových řešení, včetně produktů Microsoft Defender, Avast, AVG aj.

Aktualizace jsou realizované formou stáží na NÚKIB, na které se mohou přihlásit například studenti vysokých škol se znalostí programování, vítány jsou však i příspěvky z komunity vývojářů. Po dokončení balíčku změn pak vyjde nová verze projektu. Poslední aktualizace zahrnovala refaktorizaci kódu pro lepší abstrakci a přidání nového argumentu destination, který slouží pro určení složky, do které budou soubory extrahovány. Kromě toho jsme přidali i podporu pro antivirové programy AVG a McAfee.

Věříme, že společným úsilím se nám podaří projekt vylepšit a obohatit ho o množství další funkcionalit. Proto se nebojte tento nástroj využívat a případné chyby nám nahlásit pomocí „issues“. Jedině tak budeme schopni odladit možné problémy a projekt dále zdokonalovat. Pokud vás zaujala možnost studentské stáže, podívejte se na aktuální možnosti zde.

https://www.nukib.cz/cs/infoservis/aktuality/2011-vysokoskolaci-pomahaji-aktualizovat-forenzni-aplikaci-maldump