

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **38** ze dne **30.5.2023**

WinRAR v centru pozornosti

Útočníci vymýšlejí stále nové způsoby, jak minimalizovat "riziko", že nekalou činnost odhalí nějaké to bezpečnostní řešení, či dokonce EDR. Zaujal nás například tento originální způsob mazání souborů, který použila ruská hackerská skupina Sandworm ve společnostech na Ukrajině.

Byl totiž využit populární archivační program WinRAR, u něhož se vědělo, že se již na koncových stanicích nachází. Likvidaci / mazání souborů pak neřešil přímo proces havěti, ale právě WinRAR, který byl pro tuto činnost zneužit. Tenhle program lze totiž ovládat skrze příkazovou řádku a parametr "-df" zajistí, že soubory, které "zabalí" do archivu RAR, následně z disku smaže.

Malware byl na cílové stanice dopraven skrze naplánovanou úlohu, jenž byla distribuována centrálně skrze Group Policy. Síť tak již byla útočníky kompromitována. Ještě bych rád doplnil, že o volání WinRARu se staral prostý dávkový soubor .BAT, který v cyklu procházel disky C: až Z: a hledal v nich soubory dle definovaných přípon. Ty pak předhazoval WinRARu, který je zabalil a následně smazal (+skript pak smazal i samotný archiv).

Motiv útočníků byl jasný – snížit riziko odhalení, neboť legitimní procesy (zde WinRAR) mají přeci jenom větší důvěru ze strany bezpečnostních řešení, než cokoliv jiného, s nižší reputací. Jinak z pohledu nároku na výkon je to možná nejnáročnější způsob mazání.

Zdroj: AVcentrum.cz