SLEDOVÃ•NÃ• ZÃ•SILKY ÄŒESKÃ‰ POÅ TY

ÄŒtvrtek, 13 listopad 2014

Dnes se zaÄ•ala šíÅ™it nová verze havÄ›ti, která se maskuje jako aplikace pro sledování pohybu zásilek ÄŒeské pošty. Základem je podvodný e-mail (phishing) informující o moÅ¾nosti sledování zásilky urÄ•ené pro vás (pÅ™esný obsah neznám – budu rád, pokud mÄ› ho nÄ›kdo zašle). Tato zpráva odkazuje na stránku cs-posta24.org, která se tváÅ™í jako oficiální web ÄŒeské pošty.

V reálu nemá ale s ÄŒeskou poštou vÅ¯bec nic spoleÄ•ného a jde takéÅ¾ o podvodnou aktivitu útoÄ•níkÅ¯. Design je sice témÄ›Å™ shodný s originálem, nicménÄ› narozdíl od nÄ›j obsahuje nÄ›jaké ty pravopisné chyby, slohové nesrovnalosti a pÅ™eklepy (patrné hlavnÄ› v dalších fázích útoku).

Pokud opíšete kontrolní Ä•íslice a stisknete Stáhnout, objeví se následující dialog a po nÄ›kolika sekundách se zobrazi dialog pro staÅ¾ení ZIP souboru.

Tento ZIP archiv obsahuje spustitelný EXE soubor. SpuštÄ›ním tohoto EXE souboru si mÅ¯Å¾ete znaÄ•nÄ› zkomplikovat Å¾ivot. HavÄ›Å¥ ukrytá v tomto souboru se totiÅ¾ postará o zašifrování celé Å™ady datových souborÅ¯, které se vyskytují kdekoliv na pevném disku. UÅ¾ivatel tak mÅ¯Å¾e bÄ›hem chvíle pÅ™ijít o fotografie (typicky JPG), dokumenty (DOCX, XLSX, …) a další dÅ¯leÅ¾ité soubory. Všechny z nich jsou opatÅ™eny další pÅ™íponou .encrypted a od tohoto momentu nejsou Ä•itelné.

NÄ›sledně se zobrazí toto:

Údajným východiskem je zaplacení „výpalného“ útoÄ•níkovi ve formÄ› bitcoinÅ¯ jak ukazuje následující obrázek:

V dobÄ› „focení“ byla cena stanovena na 1,09 BTC, coÅ¾ je opravdu kolem tÄ›ch 10 tisíc KÄ•. Po nÄ›jaké d cena zÅ™ejmÄ› stoupne (coÅ¾ jsem neovÄ›Å™oval, stránka se s tím ale „chlubí“ a provádí odpoÄ•et zbývajícíh do konce „promo akce“). To, jestli útoÄ•níci poskytnou Å™ešení, netuším. Jisté je, Å¾e získané peníze v budoucnu pouÅ¾ijí k dalšímu, jistÄ› i lépe pÅ™ipravenému útoku. Po technické stránce ale dokáÅ¾e útoÄ•ník soubory zcela jistÄ› odšifrovat, coÅ¾ dokazuje i záloÅ¾ka „Dešifrovat soubor zdarma“ v horním menu. Pokud libovolný zašifrovaný soubor vloÅ¾íte, vrátí se pÅ¯vodní funkÄ•ní podoba. NÄ›koho by mohl tento fakt ovlivnit v rozhodování, zda do toho risku v podobÄ› zaplacení výpalného pÅ¯jde.

Tato havÄ›Å¥ patÅ™í do rodiny známé jako Cryptolocker. Podle verze havÄ›ti byl šifrovací klíÄ• buÄ• pÅ™ímo sou infikovaného EXE a nebo byl vygenerován aÅ¾ na poÄ•ítaÄ•i uÅ¾ivatele. V prvním pÅ™ípadÄ› tak existovala šance kl vypátrat a pomocí speciálních aplikací provést dešifrování souborÅ¯ bez nutnosti cokoliv platit. V druhém pÅ™ípadÄ› to byl problém, neboÅ¥ jakmile došlo k zašifrování souborÅ¯, klíÄ• byl odeslán útoÄ•níkÅ¯m a z poÄ•ítaÄ•e uÅ¾ivatele odstranÄ›n. ŠtÄ›stí mohl mít tehdy maximálnÄ› ten uÅ¾ivatel, jehoÅ¾ klíÄ• se podaÅ™ilo získat zátahu na gang, který za útoky stál (napÅ™íklad operace Tovar – wiki, anglicky). Do jaké skupiny patÅ™í zde popisovaná havÄ›Å¥, to aktuálnÄ› netuším. Jakmile budu mít bliÅ¾ší informace, urÄ•itÄ› se s vámi podÄ›lím! IGOR HÁK,http://www.viry.cz/