E-Bezpečí 2018, 3(2): Page 61-63. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1358

E-MAILY O TOM, ŽE PACHATELÉ POMOCÍ VIRU RAT ZÍSKALI VAŠE INTIMNÍ MATERIÁLY, JSOU PODVODNÉ, JDE O SCAM.

Kamil KOPECKÝ

Českým internetem stále kolují vyděračské e-maily, ve kterých jsou příjemci vydírání, že pokud nezaplatí výpalné v kryptoměně bitcoin, budou zveřejněny jejich intimní materiály pořízené prostřednictvím viru RAT. Jde však pouze o podvod - tvz. scam, který se sice tváří vážně a vyvolává u příjemců strach, cílem je však pouze získat od důvěřivých finanční prostředky - a to za nic. Pachatelé samozřejmě žádná intimní videa adresátů nemají.

Ahoj, drahý uživatel volny.cz.
Do vašeho přístroje jsme nainstalovali jeden software RAT. Pro tento okamžik je váš emailový účet napaden (viz "from address", nyní mám přístup k vašim účtům).. Vaše heslo z ebezpeci@volny.cz: 999999 Stahoval jsem všechny důvěrné informace z vašeho systému a dostal jsem další důkazy. Nejzajímavějším okamžikem, který jsem objevil, jsou videozáznamy o vás masturbující. Zveřejnil jsem virus na pornografickém webu, a pak jste jej nainstalovali do svého operačního systému. Po klepnutí na tlačítko Přehrát na porno video, v tom okamžiku byl můj trojan stažen do vašeho zařízení. Po instalaci vám přední

fotoaparát natáčí video pokaždé, když masturbujete, software se synchronizuje s vybraným videem. Prozatím software získal všechny vaše kontaktní informace ze sociálních sítí a e-mailových adres. Pokud potřebujete smazat všechny shromážděné údaje, pošlete mi $550 v BTC (krypto měně).

Toto je moje Bitcoin peněženka: 1PwENLsmQ2Z6b4EJfXDeeXKBj9v878uHRf

Máte 48 hodin po přečtení tohoto dopisu. Po transakci vymažu všechna data. Jinak posílám video se vaším žertíky všem vašim kolegům a přátelům!! V budoucnosti buďte opatrnější Navštivte prosím pouze zabezpečené weby! Sbohem!

Toto je znění jedné z variant tzv. vyděračského emailu, který od září putuje českým internetem.
Variant je hned několik, liší se částka, řetězec bitcoin peněženky a kvalita češtiny (z ní je však zřejmé ve všech případech, že pisatel není rodilý Čech - např. v první verzi emailu zněl předmět “Váš účet byl trhlý”, v dalších verzích “Vydání účtu”). Podvod existuje v celé řadě mutací, např. angličtině, němčině a francouzštině. Vyděrač z výše uvedeného příkladu moc štěstí neměl, na jeho účtu je stále 0 BTC. Někteří další vyděrači však měli více štěstí - např. uživatel s bitcoin-řetězcem 1BSAHXc58m2DQGuzVaKXD15xeDrE4xYZna, který figuruje v jiných verzích tohoto podvodu, již vydělal přibližně 0,55 bitcoinu (asi 80 000,- Kč).

Upozornění Policie ČR

V poslední době se šíří vlny výhružných e-mailů, jejichž obsah se nepatrně obměňuje. Jedná se o fenomén, který se vyskytuje ve větším množství států po celém světě, v různých jazykových mutacích. Pisatelé sdělují příjemci, že přes webovou kameru notebooku získali choulostivé a citlivé informace. Následuje výhružka zveřejnění informací o uživateli a instrukce k uhrazení částky 250 dolarů v bitcoinech ve lhůtě 48 hodin (v této konkrétní vlně).

Odesílatelé těchto e-mailů ve skutečnosti žádnými daty nedisponují. Doufají však, že adresát tomuto tvrzení uvěří a požadovanou částku uhradí.

Policie ČR, jež tyto případy registruje, v důsledku další masivní vlny varuje všechny uživatele elektronické pošty, aby podezřelé e-maily neotvírali (smazali je, či označili jako spam), na uvedené, ani podobné e-maily nereagovali, a nic neplatili. Pokud již došlo k zaplacení, neprodleně věc nahlaste Policii ČR.

Co dělat, když mi dorazí vyděračský virus?

1. **Neklikat na žádné odkazy v mailu a neotvírat přílohy.**
2. **E-mail označit za spam a smazat ho.**

Redakce E-Bezpečí

Zdroje:

http://www.policie.cz/clanek/upozorneni-na-vyhruzne-e-maily.aspx

https://www.zive.cz/clanky/hloupy-podvodny-e-mail-s-virem-rat-se-snazi-vytahnout-bitcoiny-z-uzivatelu-ceskych-freemailu/sc-3-a-195188/default.aspx

https://www.zive.cz/clanky/vim-ze-po-vecerech-koukas-na--a-natocil-jsem-te-u-toho-hrozi-utocnik/sc-3-a-194157/default.aspx

https://www.cnews.cz/cesko-spam-virus-rat-bitcoin

http://www.hoax.cz/scam419/falesne-vydirani---vydani-uctu-20180930/