Malware obsažený ve falešných exekučních výzvách

Policie ČR varuje občany před další vlnou podvodných e-mailů.

I přes předchozí upozornění na hromadně rozesílané e-mailové zprávy s přílohou obsahující škodlivý kód bychom chtěli znovu vyzvat všechny občany, kterým byl takovýto e-mail zaslán, aby nereagovali na obsaženou výzvu k zaslání finančních prostředků. Rovněž Policie ČR důrazně varuje před otevíráním příloh, jelikož v těchto souborech je obsažen škodlivý počítačový kód, který podle doposud zjištěných informací napadá systém počítače.

Policie ČR v posledních dnech zaznamenává zvýšený počet případů, ve kterých dochází k šíření škodlivého počítačového kódu v přílohách e-mailových zpráv, tvz. malware. Předmětem hromadně rozesílaných e-mailových zpráv jsou nyní sdělení, vyzývající k úhradě dlužných částek neexistujících exekucí.

Kromě neoprávněného získání přístupu k počítačovému systému, může být skutečným cílem snaha o získání citlivých informací, včetně možných přístupů do internetového bankovnictví uživatele. Ze strany pachatelů může následně dojít k neoprávněným finančním příkazům.

Exekutorské úřady neposílají exekuční příkazy prostřednictvím emailových zpráv, pokud tedy o to účastník řízení sám nepožádá. V případě, že účastník řízení si vyžádá poslání exekučního příkazu e-mailem, tento příkaz se zasílá ve formátu „pdf“ a je podepsán elektronickým podpisem příslušného exekutora. E-mailová adresa, ze které je příkaz odesílán, by měla za zavináčem korespondovat s názvem příslušného exekučního úřadu.

Exekuční příkaz by měl obsahovat zejména:
- označení exekučního soudu,
- označení soudního exekutora, který na základě pověření soudu vede exekuční řízení (seznam exekučních úřadu naleznete na stránkách Exekutorské komory ČR),
- exekuční titul a orgán, který jej vydal, nebo osobu, která jej vyhotovila,
- označení účastníků včetně rodného čísla povinného,
- způsob provedení exekuce
- označení osob, jimž se doručuje exekuční příkaz,
- výrok, poučení o odvolání, den a místo vydání exekučního příkazu a podpis soudního exekutora.

V případě, že se uživatelé setkali s tímto e-mailem, doporučujeme následující důslednou antivirovou kontrolu celého počítačového zařízení. Pokud došlo k otevření přílohy popsaného emailu, pak je možné konstatovat, že počítačový systém je s největší pravděpodobností kompromitován malwarem a v takovém případě je nutné jeho odborné odstranění.

Policie ČR v tuto chvíli eviduje stovky případů v celé České republice a má proto dostatek materiálu, na základě kterého vede šetření. V rámci preventivních opatření s úzkou budoucí součinností s některými provozovateli služeb v síti internet, Českou bankovní asociací a dalšími zainteresovanými subjekty.

17. července 2014
pplk. Mgr. Petra Strašilová
tisková mluvčí
Policejní prezidium

s přáním pěkného dne

nprap. Anna Štegnerová
vrchní inspektor

tel.: 974 578 207
tel.: 720 166 709

e-mail: sy.tisk@pcr.cz<mailto:sy.tisk@pcr.cz>

KRAJSKÉ ŘEDITELSTVÍ POLICIE PARDUBICKÉHO KRAJE Kancelář ředitele Skupina tisku a prevence

Purkyňova 1907/2
568 14 SVITAVY