OUCH! | August 2016

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Ce sunt programele Ransomware**
- **Ar trebui să plătiți răscumpărarea?**
- **Copiile de siguranță**
- **Măsuri suplimentare de protecție**

Despre ransomware

Ce sunt programele Ransomware?

Programele ransomware sunt o variantă aparte de programe malware ce se propagă vertiginos prin rețeaua Internet în ultima vreme, amenințând cu distrugerea documentelor și a altor tipuri de fișiere ale celor ce devin victimele acestor atacuri. Deși programele ransomware sunt doar una dintre nenumăratele versiuni de malware, au devenit atât de frecvente pentru că sunt extrem de profitabile pentru răufăcători. Odată ce calculatorul vă este infectat cu ransomware, acesta criptează anumite fișiere sau, poate, chiar toate datele de pe discul intern. Sunteți astfel blocat, fără acces la sistem, fără să vă puteți folosi fișierele personale importante, cum ar fi documentele sau fotografiile. Programul malware vă informează apoi că singurul mod în care puteți decripta fișierele personale și obține din nou acces la sistem este să plătiți infractorului o răscumpărare (de-aici și numele de ransomware [1]). Cel mai adesea răscumpărarea trebuie plătită sub formă de monedă digitală, cum ar fi bitcoin. Programele ransomware se propagă asemănător cu alte tipuri de malware. Cea mai des folosită metodă implică trimiterea de mesaje email rău intenționate victimelor, în care răufăcătorii vă păcălesc determinându-vă să deschideți un fișier atașat infectat sau să vizitați o adresă care vă conduce pe un website operat de atacatori.

Editor Invitat

Lenny Zeltser se concentrează asupra protejării operațiunilor IT ale clienților la NCR Corporation și instruiește profesioniști în domeniul securității informației la institutul SANS. Leny este activ pe Twitter la **@lennyzeltser** și publică articole pe **zeltser.com**.

Ar trebui să plătiți răscumpărarea?

E o situație dificilă. Problema este că, cu cât sunt mai mulți cei care plătesc infractorii, cu atât mai motivați sunt aceștia să atace sistemele altora. Pe de altă parte, s-ar putea să nu aveți altă posibilitate de recuperare a datelor personale. Rețineți însă că, fie și dacă ați plătit răscumpărarea, nu există nicio garanție că vă veți recupera fișierele. Aveți de-a face cu infractori în fond, aceștia s-ar putea să nu vă decripteze fișierele sau, chiar dacă vă furnizează o metodă de decriptare în schimbul plății, ceva poate să nu funcționeze corect în timpul procesului de decriptare sau calculatorul v-ar putea fi infectat cu programe malware noi.

Copiile de siguranță

Probabil cea mai bună metodă de recuperare după o infecție cu ransomware, fără să plătiți răscumpărarea, este să vă recuperați fișierele din copiile de siguranță. Astfel, chiar și dacă vă infectați cu ransomware, aveți o metodă de recuperare a fișierelor personale după reinstalarea sau curățarea calculatorului. Rețineți însă că, dacă datele salvate în copiile de

[1] ransom, în original, în limba engleză, înseamnă răscumpărare (n.t.)

Despre ransomware

siguranță pot fi accesate de pe sistemul infectat, programul ransomware le-ar putea șterge sau cripta și pe acestea. Ca atare, este important ca să folosiți pentru salvarea copiilor de siguranță servicii bazate pe tehnologie cloud de la furnizori reputați sau să stocați aceste copii pe discuri externe care nu sunt permanent conectate la sistemul dumneavoastră. În plus, o greșeală frecventă pe care mulți o fac în privința copiilor de siguranță este să presupună că acestea funcționează fără probleme, fără să mai testeze dacă pot recupera efectiv fișierele salvate. Asigurați-vă că testați periodic copiile de siguranță și că puteți să vă recuperați fișierele de care aveți nevoie în cazul în care sistemul vă este infectat cu programe ransomware. Copiile de siguranță sunt de asemenea importante pentru situațiile în care ați șters din greșeală fișiere sau când discul intern al calculatorului se defectează.

Programele ransomware sunt programe ce, odată ce v-au infectat calculatorul, criptează toate fișierele de pe acesta blocându-vă accesul la ele.

Măsuri suplimentare de protecție

O metodă prin care vă puteți proteja de infecțiile cu ransomware, la fel cum vă protejați față de alte tipuri de programe malware, este să nu ajungeți să fiți infectați. Începeți prin a vă asigura că aveți un program antivirus actualizat, obținut de la un furnizor de încredere. Astfel de soluții, cunoscute frecvent ca programe anti-malware, sunt concepute pentru detecția și stoparea propagării acestora din urmă. Cu toate acestea, antivirusul nu poate bloca sau șterge orice program suspect. Răufăcătorii inovează continuu, concepând programe malware noi și mai sofisticate, care pot ocoli detecția. În replică, furnizorii de soluții antivirus își actualizează constant soluțiile cu noi capacități de detecție a programelor malware. În multe privințe aceasta a devenit o competiție în care ambele părți încearcă să o depășească pe cealaltă. Din nefericire infractorii sunt deseori cu un pas înainte, motiv pentru care trebuie să vă asigurați făcând copii de siguranță a datelor și folosind următoarele mijloace suplimentare pentru a vă proteja:

- Răufăcătorii infectează calculatoare sau alte dispozitive exploatând vulnerabilitățile programelor pe care le folosiți. Cu cât programele folosite sunt mai recente, cu atât mai puține vulnerabilități vor fi pe sistemul dumneavoastră și le va fi mai dificil infractorilor să le infecteze. În consecință, asigurați-vă că sistemul de operare, aplicațiile și dispozitivele au activată funcția de instalare automată a actualizărilor.
- Pe calculatorul dumneavoastră folosiți un cont standard care are privilegii limitate, mai degrabă decât să folosiți conturi precum „administrator“ sau „root“. Aceasta oferă o protecție suplimentară prevenind posibilitatea ca unele programe malware să se instaleze singure.
- Răufăcătorii păcălesc deseori victimele determinându-le să instaleze singure programele malware. De exemplu, aceștia vă pot trimite un email care pare legitim și care conține un fișier atașat sau o adresă. Posibil ca mesajul să

Despre ransomware

pară că e trimis de banca cu care lucrați sau de un prieten. Dacă veți fi deschis fișierul atașat sau veți fi accesat adresa inclusă în mesaj, aceasta ar fi activat codul care instalează programul răufăcătorului pe sistemul personal. Dacă un mesaj generează un sentiment acut de urgență, este generator de confuzie sau pare să ofere ceva prea bun ca să fie adevărat sau are o gramatică îndoielnică, e semn că poate fi un atac. Fiți suspicioși, simțul realității este adesea cea mai bună defensivă.

Protejați-vă de programele ransomware fiind vigilenți când deschideți fișiere atașate mesajelor email sau când urmați adrese de site-uri online, asigurați-vă că v-ați actualizat programul antivirus și confirmând că fișierele personale sunt salvate periodic în copii de siguranță de unde pot fi recuperate.

Aflați mai multe

Abonați-vă la buletinul informativ lunar OUCH!, accesați arhiva și aflați mai multe despre programele de instruire asupra domeniului securității informației vizitând pagina web SANS securingthehuman.sans.org/ouch/archives

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Despre phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
Ce sunt programele malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Criptarea:	https://securingthehuman.sans.org/ouch/2016#june2016
Copiile de siguranță:	https://securingthehuman.sans.org/ouch/2015#august2015
Un articol relevant publicat de Microsoft:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
Cursul SANS FOR610 – despre analiza programelor Malware:	https://sans.org/for610

Echipa editorială: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducere: Cosmin Hănulescu