Ce este Ransomware?

Ransomware este un tip de malware care impiedica victima sa acceseze sistemul sau fișierele personale, păstrându-i "ostatici" și solicitând o anumita suma ca rasumparare pentru datele respective. După cum afirmă [1], prima dată când acest tip de atac a fost introdus, a fost la sfârșitul anilor 80, iar răscumpărarea a fost plătită prin poștă. Astăzi tehnologia a avansat, astfel încât autori cer plata în criptomoneda sau card de credit.

În [2] este descrisă o clasificare a ransomware-ului după mijloacele utilizate, așa cum se vede în text, atacul poate varia de la ușor la periculos:

Prima categorie este Scareware, care include software necinstit și escrocherii. Victima poate primi mesaje în care se anunță detectarea de malware și trebuie să plătească pentru a elimina aceste probleme. Aceasta este doar o încercare de a speria victima, dar fișierele sunt în siguranță. Mesajele vor continua, dar nu este nevoie de îngrijorare daca scanați computerul.

O altă categorie sunt Screen Lockers, care sunt periculoase. Când calculatorul este infectat cu acest tip de malware, victima este blocată complet din computerul său. Hackerii folosesc sigla FBI sau o alta sigla cum ar fi cea al Departamentului de Justiție pentru a anunța că a fost găsită o activitate ilegală pe dispozitiv și că trebuie plătită o amendă.

În ultimul rând vorbesc despre Encrypting Ransomware, care este cel mai dăunător tip de ransomware dintre toate cele mentionate mai sus. În acest caz, hackerii vă captureaza fișierele,le criptează și solicită plata de la victimă pentru a da fișierele înapoi. Acest tip este atât de periculos, deoarece nimic nu poate restabili fișierele, numai dacă plătiți, dar chiar și atunci nu puteți fi siguri că veți primi fișierele înapoi - în cea mai mare parte chiar și după plată, fișierele au dispărut.

Vorbind despre categorii, în [1] și [3] sunt sugerate mai multe posibilități de a împărți răscumpărarea.

Autorii împart acest malware prin propagări și prin metoda de plată. Prima metodă este împărțită în trei tipuri, cum ar fi: Kituri de exploatare, pachet de instrumente pregătite anterior, Programe de afiliere, unde este dezvoltat și propagat codul utilizat și, în final, Campaniile Malvertising, unde e-mailurile spam vizează utilizatori diferiți. Trecând la cea de-a doua categorie de clasificare, prin plată, [1] și [3] sunt de acord că există două modalități de plată, mai întâi prin plată directă și a doua prin plată indirectă, ca vouchere preplătite, de exemplu.

După cum am menționat mai sus, ransomware-ul a fost introdus în anul 1980 și este cunoscut sub numele de PC Cyborg sau AIDS. Aceasta ar cripta partiția C: după ce computer a fost repornit de cel puțin 90 de ori și a cerut victimei să trimită banii ($ 189) prin posta. Criptarea era simplă, așa că era ușor să o inverseze și nu reprezenta nici un pericol.

Când lumea a început să fie afectată de ransomware și apoi reintrodusă ulterior la această expresie, victimele erau oamenii obișnuiți cu sisteme individuale. Mai târziu, criminali au realizat potențialul atacului și au început să meargă după afaceri si firme. Acestea au provocat o mulțime de pagube în ramura acestora de activitate, ducând la pierderea de date și scăderea productivității.  
  
La sfârșitul anului 2016, mai mult de 10% dintre toate detectările malware globale au fost clasificate drept ransomware.

Ce trebuie făcut dacă sunteti avizati de acest virus?

Există numeroase moduri diferite în ceea ce privește modul în care vă puteți infecta, cele mai frecvente fiind prin mesajele de tip spam, care pot include atribuiri de ascundere a malware-ului.

Dacă te infectezi, nu trebuie să plătești niciodată răscumpărarea, acest sfat este susținut de FBI și alte agenții care luptă împotriva cererilor de răscumpărare. Plătind tot ce facem este să încurajăm atacatorii să țină sistemele și fișierele noastre "ostatice". Problema este că, chiar dacă plătim, există mai multe modalități de criptare a fișierelor și nu toate pot fi decriptate, deci pericolul constă în faptul că noi putem cripta fișierele noastre mai departe folosind un software greșit de decripare.

Un alt mod de a vă proteja este să instalați software de securitate care scanează computerul și elimină amenințarea. Poate că fișierele nu vor fi restaurate, dar cel puțin problema a dispărut.

Deoarece atacul ransom a apărut din nou, câteva organizații de securitate a informațiilor, precum și agențiile de aplicare a legii, au informează de această amenințare. Vorbind despre aceste agenții, este important să se țină seama de proiectul No More Ransom, care este creat de Unitatea Națională de Criminalistică a Poliției Olandeze și de Centrul European de Criminalistică al Europol, în coordonare cu două companii de securitate Kaspersky Lab și McAfee. O altă mențiune importantă este proiectul FBI Ransomware Prevention & Response, în cadrul căruia Biroul Federal de Investigații a creat secții speciale pentru a educa oamenii despre amenințările de răscumpărare. In final, la fel ca inițiativa din SUA, în Marea Britanie a fost creat National Cybercrime Security Center, această incluzând pagini web dedicate , unde cetățenii primesc informații, sprijin și ocazia de a ajuta alte persoane.

Cum să vă protejați împotriva atacurilor?

Primul lucru este să investiti într-un software de securitate care poate proteja chiar și software-ul vulnerabil de programele malware.

Păstrați fișierele securizate, cu back-up-uri regulate, fie în cloud, unde criptarea este un factor important, fie pe hard discuri externe criptate.

În cele din urmă, trebuie să vă asigurați că software-ul și aplicațiile sunt actualizate. Actualizare înseamnă că bug-urile și vulnerabilitățile au fost reparate și aplicațiile sunt mai sigure acum.

Cel mai important este să te educi și să fii informat. Aflați cum să detectați programele și aplicațiile malițioase și ajutații si pe ceilalți să învețe.