Malware

Pentru mai multe informaţii: SEC.EFF.ORG
Un proiect al Electronic Frontier Foundation

MALWARE, prescurtare de la software rău intenţionat, este orice program care este proiectat să execute acţiuni nedorite pe dispozitivul dvs.

Exemple de malware includ:

- Virusi de calculatoare
- programe care fură parole
- programe care te înregistrează în secret
- programe care şterg în secret datele dvs.

MALWARE PRIN PHISHING

Phishing-ul se întâmplă atunci când un atacator trimite un mesaj, e-mail sau link care pare inofensiv, dar este de fapt maliţios. Phishing-ul implică adesea impersonarea unei persoane pe care o cunoaşteţi sau impersonarea unei platforme în care aveţi încredere.

Notă: Nu toate acţiunile de phishing includ malware. Uneori, un atacator doreşte să fure parolele pentru un serviciu şi poate face acest lucru prin impersonarea unui site web, fără a instala malware pe dispozitivul utilizatorului.

Modalităţi comune de instalare a programelor malware

Deschiderea unui atasament sau fişier maliţios	Ataşamentele maliţioase sunt adesea distribuite în mesaje de phishing.
Clic pe un link maliţios	Linkurile maliţioase sunt adesea distribuite în mesaje de phishing.
Descărcarea de software nelicenţiat	Software-ul care nu poate primi actualizări de securitate creşte riscul (de ex., software care nu provine din Apple App Store sau Google Play Store).
Vizitarea de site-uri web compromise	Uneori, site-urile web sunt preluate şi sunt folosite pentru a găzdui conţinut maliţios.

TIPURI DE MALWARE

Adware	reclame peste tot Acest software malițios încearcă de obicei să afișeze reclame utilizatorului prin suprasolicitarea ferestrelor pop-up sau prin alte metode. Unele adware urmăresc informații despre utilizator sau extrag informații personale. Adware-ul, ca și alte malware, poate fi grupat cu alte programe software, adesea descărcate din surse dubioase, cum ar fi din afara magazinelor oficiale de aplicații sau de pe site-uri care nu aparțin de dezvoltatorul software-ului.
Software de urmărire	când dispozitivul tău îl ajută pe cel care te urmărește Software-ul de urmărire rulează în tăcere și îi oferă atacatorului control total asupra dispozitivului. Software-ul de urmărire poate fi instalat atunci când cineva are acces fizic la dispozitivul dvs. (cum ar fi un membru al familiei sau un partener, “dă-mi voie să-ți folosesc telefonul pentru un moment”) și instalează o aplicație de urmărire sau când un utilizator este păcălit să descarce aplicația.
Troian	ca un cadou care este de fapt un atac deghizat. Când este descărcat, software-ul troian poate funcționa ca aplicația legitimă, dar, în realitate, face lucruri malițioase în fundal. Acesta se găsește adesea în software piratat sau spart sau în software antivirus fals.
Ransomware	este un tip de software care te ține ostatic. Când este descărcat, acest software malițios ține datele unei companii, organizații sau

	persoane ca ostatici. Ransomware a câștigat popularitate în ultimul deceniu și este acum o afacere de mai multe milioane de dolari pentru atacatorii din întreaga lume.
Atac APA	Amenințare persistentă avansată Un atac APA este un malware provenit de la un adversar cu capabilități sofisticate și resurse substanțial mai mari dedicate atingerii obiectivelor sale: compromiterea sistemului dvs. Atacurile APA sunt adesea utilizate simultan cu actori statali care vor încerca să mențină „persistența” sau accesul pe termen lung la sistemul pe care îl vizează.

5 SFATURI PENTRU APĂRAREA ÎMPOTRIVA MALWARE

SFATUL #1: ACTUALIZAȚI-VĂ SOFTWARE-UL

(ȘI VERIFICAȚI CĂ UTILIZAȚI SOFTWARE LICENȚIAT)

Cele mai multe malware-uri profită de vulnerabilitățile cunoscute. Companiile de software remediază adesea aceste vulnerabilități și le distribuie utilizatorilor prin intermediul actualizărilor.

Actualizările de software sunt esențiale pentru securitatea utilizatorilor, deoarece sunt cea mai sigură modalitate de a rămâne la curent cu remedierile vulnerabilităților cunoscute pe care atacatorii le-ar putea exploata.

Dacă nu sunteți sigur cum să obțineți software licențiat, întrebați-vă facilitatorul de securitate digitală de încredere pentru sfaturi și resurse disponibile.

SFATUL #2: COPII DE REZERVĂ PENTRU VIITOR

Faceți copie de rezervă datelor dvs. astăzi și viitorul dvs. vă va fi recunoscător. Dacă vă pierdeți dispozitivul (din cauza malware-ului, furtului sau pur și simplu pentru că nu mai pornește), nu este totul pierdut: fișierele dvs. vor fi în copiile de rezervă. Protejați aceste copii de rezervă utilizând o parolă puternică și criptare.

SFATUL #3: G NDIȚI-VĂ ÎNAINTE SĂ DAȚI CLIC

Partajarea de link-uri și fișiere este o practică comună, dar fiți vigilenți atunci când interacționați cu sau partajați link-uri. Înainte de a face clic, întrebați-vă: pare ciudat acest lucru?

FIȚI ATENȚI LA…

Link-uri scurte și tăiate

Link-urile și e-mailurile pot fi afișate ca fiind mai scurte atunci când sunt vizualizate pe un telefon decât atunci când sunt vizualizate pe un computer. Serviciile de scurtare a link-urilor, cum ar fi bit.ly și altele similare, pot redirecționa către site-uri web malițioase.

Sfat: Încearcă un serviciu precum https://unshorten.it pentru a vedea URL-ul complet extins!

Imitația, cea mai avansată formă de înșelăciune.

Greșelile de tipar, caracterele similare și brandingul copiat sunt folosite pentru a vă înșela. Verificați dacă serviciul este real.

SFAT: Când sunteți pe un serviciu autentic, utilizați un bookmark: acest lucru poate face mai ușoară pentru computerul dvs. să vă ajute să vă amintiți adresele de site-uri web legitime.

"Sfat: Salvați linkul corect în managerul de parole: un manager de parole poate reține site-urile desemnate și poate completa parola pentru dvs."

Fiți atenți la „ingineria socială”, cum ar fi primirea unui mesaj de la cineva care se preface că vă este prieten.

SFAT: Contactați-vă prietenul printr-o altă metodă de comunicare și verificați dacă este chiar el.

Atingere sau clic accidental

Atunci când examinați link-uri pe dispozitivul dvs., o singură atingere sau un singur clic poate deschide accidental link-ul!

Sfat: Dacă utilizați un mouse, profitați de hover pentru a vedea linkul complet.

SFATUL #4: FIȚI ATENȚI LA ACCESUL FIZIC

Uneori, adversarii noștri sunt persoane pe care le cunoaștem sau persoane care ne pot accesa dispozitivele atunci când nu suntem atenți. Utilizarea criptării complete a discului și a unei parole puternice pentru a vă proteja dispozitivul vă poate ajuta să vă apărați de accesul fizic nedorit. Fiți atenți atunci când împrumutați dispozitivul deblocat cuiva. Pentru a citi mai multe, consultați ssd.eff.org.

SFATUL #5: UTILIZAȚI UN ANTIVIRUS

Nu toate antivirusurile sunt create egale; unele software-uri comercializate ca antivirus pot fi malware deghizat. Este recomandat să utilizați antivirusul propriu al producătorului dispozitivului dvs. Dacă preferați software antivirus din părți terțe, verificați:

- recenziile independente ale software-ului

- dacă lista actualizată de malware de pe site-ul web antivirus include tipul de malware şi adversarul de care vă faceţi griji, înainte de a descărca sau instala software antivirus.

*Cercetarea publicată a ameninţărilor poate indica faptul că antivirusul are o echipă activă care se ocupă cu acest tip de malware.

CRED CĂ AM MALWARE. CE AR TREBUI SĂ FAC?

Se întâmplă ceva ciudat pe dispozitivul dvs.? Este afectat un cont specific (cum ar fi social media) sau întregul dispozitiv? Dacă credeţi că dispozitivul dvs. este infectat cu malware, aveţi grijă cum îl utilizaţi în viitor. Utilizaţi un alt dispozitiv pentru a contacta un specialist pentru ajutor.

*Un alt dispozitiv nu ar fi conectat la dispozitivul afectat de malware. Acesta ar putea fi un computer dintr-o bibliotecă sau telefonul unui prieten de încredere, de exemplu.

CONTACTAŢI UN TEHNICIAN DE ÎNCREDERE

Păstraţi un jurnal cu mesajele ciudate pe care le-aţi primit în forma lor originală (de exemplu, dacă este un e-mail, redirecţionaţi e-mailul original cu metadatele antetului, nu o captură de ecran). Includeţi detalii: data, ora şi descrierea. Trimiteţi-le unui tehnician de încredere.

EVALUAŢI PAGUBELE

Ce informaţii sensibile ar fi putut fi compromise? Ar trebui să vă schimbaţi parolele sau conturile? Planificaţi următorii paşi pentru siguranţă prin efectuarea unei evaluări a riscurilor (cunoscută şi ca "cartografierea ameninţărilor").

De ce metadata este important?

Ultima revizuire: 11 martie, 2019

Metadatele sunt deseori descrise ca fiind tot ceea ce este în afară conţinutului comunicărilor dumneavoastră. Vă puteţi gândi la metadate ca la echivalentul digital al unui plic. La fel cum un plic conţine informaţii despre expeditorul, destinatarul şi destinaţia unui mesaj, la fel şi metadatele. Metadatele sunt informaţii despre comunicaţiile digitale pe care le trimiteţi şi le primiţi. Câteva exemple de metadate includ:

- Subiectul e-mailurilor dvs.
- Durata conversaţiilor dvs.

- Intervalul de timp în care a avut loc o conversație
- Locația dvs. atunci când comunicați (precum și cu cine)

Din punct de vedere istoric, în unele țări, inclusiv în SUA, metadatele au beneficiat de o mai mică protecție a vieții private decât conținutul comunicațiilor. De exemplu, în multe țări, poliția poate obține mai ușor lista persoanelor pe care le-ați sunat luna trecută, decât poate aranja o ascultare a liniei dvs. telefonice pentru a auzi ce spuneți de fapt.

Cei care colectează sau solicită accesul la metadate, cum ar fi guvernele sau companiile de telecomunicații, susțin că dezvăluirea (și colectarea) metadatelor nu reprezintă o problemă. Din nefericire, aceste afirmații sunt pur și simplu neadevărate. Chiar și un eșantion minuscul de metadate poate oferi detalii intime din viața unei persoane. Să vedem ce pot afla din metadate guvernele și companiile care le colectează:

- Ei știu că ați sunat la o linie erotică la ora 2:24 dimineața și ați vorbit 18 minute. Dar nu știu despre ce ați vorbit.
- Ei știu că ați sunat la linia de prevenire a sinuciderilor de pe podul Golden Gate. Dar subiectul apelului rămâne un secret.
- Ei știu că ați primit un e-mail de la un laborator de testare HIV, apoi v-ați sunat medicul, apoi ați vizitat un site web al unui grup de sprijin pentru HIV. Toate în aceeași oră. Dar nu știu ce conținea e-mailul sau despre ce ați vorbit la telefon.
- Ei știu că ați primit un e-mail de la un grup de activiști pentru drepturile digitale cu subiectul "Hai să spunem Congresului: opriți SESTA/FOSTA" și că imediat după aceea v-ați sunat reprezentantul din Congres. Dar conținutul acestor comunicări rămâne la adăpost de intruziunea guvernului.
- Ei știu că ați sunat la un ginecolog, și ați vorbit o jumătate de oră. Mai apoi, în aceeași zi, ați sunat la numărul de telefon al clinicii locale de avorturi.

Poate fi dificil să vă protejați metadatele de colectare, deoarece terții adesea au nevoie de metadate pentru a conecta cu succes comunicațiile dumneavoastră. La fel cum un lucrător poștal trebuie să poată citi partea exterioară a unui plic pentru a vă putea livra mesajul, comunicațiile digitale trebuie să fie marcate cu sursa și destinația. Companiile de telefonie mobilă trebuie să știe aproximativ unde se află telefonul dumneavoastră pentru a putea direcționa apelurile către acesta.

Serviciile precum Tor limitează cantitatea de metadate produse prin intermediul metodelor comune de comunicare online. Până când legile vor fi actualizate pentru o mai bună gestionare a metadatelor și până când instrumentele care reduc metadatele la minimum vor deveni mai răspândite, cel mai bun lucru pe care îl puteți face este să fiți conștienți de metadatele pe care le transmiteți atunci când comunicați, de cine poate avea acces la aceste informații și de modul în care acestea pot fi utilizate.

Planul tău de securitate

Ultima revizuire: 1 februarie 2021

Încercarea de a vă proteja mereu toate datele de toată lumea este nepractică şi obositoare. Dar, nu aveţi nicio teamă! Securitatea reprezintă un proces şi, printr-o planificare minuţioasă, puteţi realiza un plan care este potrivit pentru dvs. Securitatea nu este doar despre instrumentele pe care le folosiţi sau despre softurile pe care le downloadaţi. Ea începe cu înţelegerea ameninţărilor unice cu care vă confruntaţi şi cu modul în care puteţi contracara aceste ameninţări.

În domeniul securităţii informatice, o ameninţare reprezintă un eveniment posibil care ar putea submina eforturile de a vă apăra datele. Puteţi contracara ameninţările cu care vă confruntaţi determinând ce trebuie să protejaţi şi de cine trebuie să le protejaţi. Acesta este procesul de planificare a securităţii, adesea denumit cartografierea ameninţărilor (threat modeling).

Acest ghid vă va învăţa cum să vă faceţi un plan de securitate pentru informaţiile dumneavoastră digitale şi cum să determinaţi care sunt cele mai bune soluţii pentru dumneavoastră.

Cum arată un plan de securitate? Să spunem că vreţi să vă ţineţi casa şi bunurile în siguranţă. Aici sunt câteva întrebări pe care ar trebui să vi le puneţi:

Ce aveţi în interiorul casei care merită protejat?

Bunurile ar putea include: bijuterii, electronice, documente financiare, paşapoarte şi fotografii.

De cine vreţi să le protejaţi?

Adversarii pot fi: răufăcători, colegi de cameră sau vizitatori.

Cât de probabil este că va trebui să le protejaţi?

Are cartierul meu o istorie de spargeri? Cât de demni de încredere sunt colegii dvs. de cameră/vizitatorii? Care sunt capacităţile adversarilor mei? Care sunt riscurile pe care trebuie să le luaţi în considerare?

Cât de grave sunt consecinţele dacă eşuaţi?

Aveţi ceva în casă care nu poate fi înlocuit? Aveţi timp sau bani ca să înlocuiţi aceste lucruri? Aveţi o asigurare care să acopere bunurile furate din casa dvs.?

Cât de mult efort sunteţi dispus să faceţi ca să preveniţi aceste consecinţe?

Sunteţi dispus să cumpăraţi un seif pentru documentele sensibile? Vă permiteţi să cumpăraţi un dispozitiv de închidere de calitate superioară? Aveţi timp să vă închiriaţi o cutie de valori la banca dvs. pentru a păstra valorile acolo?

O dată ce v-aţi pus aceste întrebări, sunteţi în poziţia de a evalua ce măsuri să luaţi. Dacă bunurile dumneavoastră sunt valoroase, dar probabilitatea de spargere este scăzută, atunci probabil nu veţi dori să investiţi mulţi bani într-o încuietoare performantă. Dar, dacă probabilitatea de spargere

este ridicată, veți dori să cumpărați cel mai bun dispozitiv de închidere de pe piață și poate să adăugați și un sistem de securitate.

Elaborarea unui plan vă va ajuta să înțelegeți amenințările care sunt unice pentru dumneavoastră și să vă evaluați bunurile, adversarii, capabilitățile adversarilor, dar și probabilitatea riscurilor cu care vă confruntați.

Cum vă alcătuiți propriul plan de securitate? De unde să începeți?

Planificarea securității vă ajută să identificați ce ar putea să se întâmple cu lucrurile pe care le prețuiți și să determinați de cine trebuie să le protejați. Când construiți planul de securitate, răspundeți la aceste cinci întrebări:

- Ce vreau să protejez?
- De cine vreau să le protejez?
- Cât de grave sunt consecințele dacă eșuez?
- Cât de probabil este să fie nevoie să le protejez?
- Prin cât de multe probleme sunt dispus să trec pentru a preveni potențialele consecințe?

Haideți să analizăm mai îndeaproape aceste întrebări.

Ce vreau să protejez?

Un „bun” este ceva pe care îl prețuiți și pe care vreți să-l protejați. În contextul securității digitale, un bun este de obicei un tip de informație. De exemplu, e-mail-urile dvs., listele de contacte, mesajele, locațiile și documentele sunt posibilele bunuri. Device-urile dvs. pot fi considerate, de asemenea, bunuri.

Faceți o listă de bunuri: datele pe care le păstrați, cine are acces la ele și ce îi împiedică pe alții să aibă acces la ele?

De cine vreți să lec protejați?

Pentru a răspunde la această întrebare, este important să identificați cine ar putea dori să vă vizeze pe dumneavoastră sau informațiile dumneavoastră. O persoană sau o entitate care reprezintă o amenințare la adresa bunurilor dumneavoastră este un "adversar". Exemple de adversari potențiali sunt șeful dumneavoastră, fostul partener, concurentul din afaceri, guvernul sau un hacker dintr-o rețea publică.

Faceți o listă cu adversarii dumneavoastră, adică cu cei care ar putea dori să pună mâna pe bunurile dumneavoastră. Lista poate include persoane fizice, agenții guvernamentale sau corporații.

În funcție de cine sunt adversarii dumneavoastră, în anumite circumstanțe, s-ar putea să doriți să distrugeți această listă după ce ați terminat de planificat activitatea de securitate.

Cât de grave sunt consecințele dacă eșuați?

Există multe modalități prin care un adversar ar putea avea acces la datele dumneavoastră. De exemplu, un adversar vă poate citi comunicațiile private în timp ce acestea trec prin rețea sau vă poate șterge sau corupe datele.

Motivele adversarilor diferă foarte mult, la fel ca și tacticile lor. Un guvern care încearcă să împiedice răspândirea unei înregistrări video care prezintă violențe polițienești se poate mulțumi doar să șteargă sau să reducă disponibilitatea acelei înregistrări video. În schimb, un adversar politic ar putea dori să obțină acces la conținut secret și să publice acel conținut fără ca dumneavoastră să știți.

Planificarea securității implică înțelegerea consecințelor grave care decurg dintr-un fapt prin care un adversar care ar reuși să obțină acces la unul dintre bunurile dumneavoastră. Pentru a determina acest lucru, ar trebui să luați în considerare capabilitatea adversarului dumneavoastră. De exemplu, furnizorul dvs. de telefonie mobilă are acces la toate înregistrările telefonice. Un hacker aflat într-o rețea Wi-Fi deschisă poate avea acces la comunicațiile dumneavoastră necriptate. Guvernul dumneavoastră ar putea avea capacități mai puternice.

Scrieți ce ar putea vrea adversarul dumneavoastră să facă cu datele dumneavoastră private.

Cât de probabil este să fie nevoie să le protejați?

Riscul reprezintă probabilitatea ca o anumită amenințare la adresa unui anumit bun să se producă efectiv. Acesta merge mână în mână cu capacitatea. În timp ce furnizorul de telefonie mobilă are capacitatea de a vă accesa toate datele, riscul ca acesta să vă publice online datele private pentru a vă afecta reputația este scăzut.

Este important să se facă distincția între ceea ce s-ar putea întâmpla și probabilitatea ca acest lucru să se întâmple. De exemplu, există riscul ca clădirea dumneavoastră să se prăbușească, dar riscul ca acest lucru să se întâmple este mult mai mare în San Francisco (unde cutremurele sunt frecvente) decât în Stockholm (unde nu sunt).

Evaluarea riscurilor este un proces atât personal, cât și subiectiv. Mulți oameni consideră că anumite amenințări sunt inacceptabile, indiferent de probabilitatea ca acestea să se producă, deoarece simpla prezență a amenințării, indiferent de probabilitate, nu merită costul. În alte cazuri, oamenii nu iau în considerare riscurile ridicate pentru că nu consideră amenințarea ca fiind o problemă.

Scrieți ce amenințări veți lua în serios și care ar putea fi prea rare sau prea inofensive (sau prea greu de combătut) pentru a vă îngrijora.

Prin cât de multe probleme sunteţi dispus să treceţi pentru a preveni potenţialele consecinţe?

Nu există un plan perfect pentru securitate. Nu toată lumea are aceleaşi priorităţi, preocupări sau acces la resurse. Evaluarea riscurilor vă va permite să planificaţi strategia potrivită pentru dumneavoastră, echilibrând comoditatea, costurile şi confidenţialitatea.

De exemplu, un avocat care reprezintă un client într-un caz de securitate naţională ar putea fi dispus să facă eforturi mai mari pentru a proteja comunicările referitoare la acest caz, cum ar fi utilizarea unui e-mail criptat, decât un membru al familiei care trimite în mod regulat prin e-mail videoclipuri amuzante cu pisici.

Scrieţi ce opţiuni aveţi la dispoziţie pentru a vă ajuta să vă reduceţi ameninţările unice. Notaţi dacă aveţi constrângeri financiare, tehnice sau sociale.

Planificarea securităţii ca o practică obişnuită

Nu uitaţi că planul dumneavoastră de securitate se poate modifica pe măsură ce situaţia dumneavoastră se schimbă. Prin urmare, revizuirea frecventă a planului de securitate este o bună practică.

Creaţi-vă propriul plan de securitate în funcţie de situaţia dumneavoastră unică. Apoi, marcaţi-vă în calendar o dată în viitor. Acest lucru vă va îndemna să vă revizuiţi planul şi să reveniţi pentru a determina dacă mai este relevant pentru situaţia dumneavoastră.

Credit for translation and localization goes to Journalist Security Fellowship fellows in partnership with Localization Lab.