Malware

Za više informacija: SEC.EFF.ORG
Projekt Zaklade Electronic Frontier

MALWARE, skraćeno od maliciozni software, svaki je program koji je dizajniran za izvođenje neželjenih radnji na Vašem uređaju

Primjeri malwarea uključuju:

- računalne viruse
- programe koji kradu lozinke
- programe koji Vas tajno snimaju
- programe koji tajno brišu Vaše podatke

MALWARE PUTEM PHISHINGA

Phishing je kada napadač pošalje poruku, email ili link koji izgleda bezazleno, ali je zapravo zlonamjeran. Phishing često uključuje lažno predstavljanje nekoga koga poznajete ili lažno predstavljanje platforme kojoj vjerujete.

Napomena: Ne uključuje svaki phishing malware. Ponekad napadač želi ukrasti lozinke za uslugu i to može učiniti lažnim predstavljanjem web stranice, bez instaliranja malwarea na korisnikov uređaj.

UOBIČAJENI NAČINI INSTALIRANJA MALWAREA

Otvaranje zlonamjernog privitka ili datoteke	Zlonamjerni privitak često se dijeli u phishing porukama.
Klik na zlonamjernu poveznicu	Zlonamjerna poveznica često se dijeli u phishing porukama.
Preuzimanje nelicenciranog softwarea	Software koji ne može primati sigurnosna ažuriranja povećava rizik (npr. ne iz Apple App trgovine ili Google Play trgovine.)

Posjećivanje ugroženih web stranica	Ponekad se web stranice preuzimaju i koriste za smještaj zlonamjernog sadržaja.

VRSTE MALWAREA

Adware	oglasi posvuda Ovaj zlonamjerni software obično pokušava prikazati oglašavanje korisniku putem preopterećenja prozorima koji iskaču ili drugih metoda. Neki adware prate podatke o korisniku ili izvlače osobne podatke. Adware, kao i drugi malware, može biti uvezan s drugim softwareom, često preuzetim iz izvora koji nisu renomirani, kao što su izvori izvan službenih trgovina aplikacija ili od razvojnog programera softwarea.
Stalkerware	Kada Vaš uređaj pomeže Vašem uhoditelju Stalkerware radi tajno i daje napadaču potpunu kontrolu nad uređajem. Stalkerware se može instalirati kada netko ima fizički pristup Vašem uređaju (kao što je član obitelji ili partner, “dopusti mi da se poslužim tvojim telefonom na trenutak”) i instalira stalkerware aplikaciju ili kada je korisnik prevaren da preuzme aplikaciju.
Trojan	kao dar ali ustvari zapakiran napad Kada se preuzme, trojanski software može raditi kao što bi legitimna aplikacija i trebala raditi, ali zapravo radi zlonamjerne radnje u pozadini. Ovo se često nalazi u piratskom ili "krekanom" softwareu ili lažnom antivirusnom softwareu.

Ransomware	Software koji Vas drži kao taoca Kada se preuzme, ovaj zlonamjerni software drži podatke tvrtke, organizacije ili pojedinca za otkupninu. Ransomware je stekao popularnost u posljednjem desetljeću i sada je to posao vrijedan više milijuna dolara za napadače širom svijeta.
Sulm A.P.T.	napad napredne ustrajne prijetnje APT napad je malware od napadača sa sofisticiranim mogućnostima i znatno više resursa posvećenih postizanju njihovih ciljeva: ugrožavanju Vašeg sustava. APT napade često izvode državni akteri koji će pokušati održati "ustrajnost", ili dugoročni pristup, sustavu koji ciljaju.

5 SAVJETA ZA OBRANU OD MALWAREA

SAVJET #1: AŽURIRAJTE SVOJ SOFTWARE

(I PROVJERITE KORISTITE LI LICENCIRANI* SOFTWARE)

Većina malwarea iskorištava poznate ranjivosti. Same software tvrtke često popravljaju te ranjivosti i dostavljaju ih korisnicima putem ažuriranja.

Ažuriranja softwarea stoga su ključna za sigurnost korisnika, jer je to najsigurniji način da ostanete u tijeku s popravkom poznatih ranjivosti koje napadači mogu koristiti.

*Ako niste sigurni kako doći do licenciranog softwarea, pitajte svog ljubaznog voditelja digitalne sigurnosti za savjete i dostupne resurse.

SAVJET #2: SIGURNOSNE KOPIJE ZA BUDUĆNOST

Napravite si sigurnosnu kopiju svojih podataka danas i bit ćete si zahvalni u budućnosti. Ako izgubite svoj uređaj (bilo zbog malwarea, krađe ili se uređaj jednostavno ne uključuje), nije sve izgubljeno: Vaše će datoteke biti u Vašim sigurnosnim kopijama. Zaštitite te sigurnosne kopije pomoću jake lozinke i enkripcije.

SAVJET #3: ZASTANITE PRIJE NEGO ŠTO KLIKNETE

Dijeljenje poveznica i datoteka uobičajena je praksa, ali budite oprezni kada otvarate poveznice ili ih dijelite. Prije nego što kliknete, zapitajte se: je li ovo neobično?

PAZITE NA… SKRAĆENE ILI ODSJEČENE POVEZNICE

Poveznice i emailovi mogu se prikazati kraćim kada se pregledavaju putem telefona nego putem računala. Usluge za skraćivanje poveznica poput bit.ly i slične mogu preusmjeriti na zlonamjerne stranice.

Savjet: isprobajte uslugu kao što je https://unshorten.it da biste vidjeli cijeli proširen URL!

IMITACIJA, NAJVEĆI OBLIK PREVARE

Tipfeleri, slični znakovi i kopije brendova Vas mogu prevariti. Provjerite je li to stvarna usluga.

Savjet: kada ste na autentičnoj web stranici, koristite bookmark: time si možete olakšati pamćenje adresa legitimnih web stranica

Savjet: sačuvajte ispravnu poveznicu u svoj password manager: password manager može zapamtiti određene web stranice i unijeti lozinku umjesto Vas.

Čuvajte se "društvenog inženjeringa", poput primanja poruke od nekoga tko se pretvara da Vam je prijatelj.

Savjet: obratite se svom prijatelju drugim oblikom komunikacije i provjerite je li to doista on.

SLUČAJAN DODIR ILI KLIK

Kada pregledavate poveznice na svom uređaju, jednim dodirom ili klikom možete slučajno otvoriti poveznicu!

Savjet: ako koristite miš, iskoristite prednost prevlačenja miša preko poveznice kako biste vidjeli cijelu vezu.

SAVJET #4: BUDITE OBAZRIVI NA FIZIČKI PRISTUP

Ponekad su naši protivnici ljudi koje poznajemo ili ljudi koji mogu pristupiti našim uređajima kada ne obraćamo pozornost. Korištenje enkripcije cijelog diska i jake lozinke za zaštitu Vašeg uređaja, može pomoći u obrani od neželjenog fizičkog pristupa. Budite oprezni kad nekome posuđujete svoj otključani uređaj. Za više informacija pogledajte ssd.eff.org.

SAVJET #5: KORISTITE ANTIVIRUS

Nisu svi antivirusi jednaki; neki software koji se prodaje kao antivirus može biti prikriveni malware. Možda ćete htjeti koristiti antivirusni program proizvođača Vašeg uređaja. Ako više preferirate druge antiviruse, provjerite:

- neovisne recenzije softwarea

- ima li web stranica antivirusa ažuriran popis malwarea* i napadača koji Vas brinu

*Objavljeno istraživanje prijetnji može ukazati na to da antivirus ima aktivan tim koji se brani od ove vrste malwarea.

MISLIM DA IMAM MALWARE. ŠTO TREBAM NAPRAVITI?

Događa li se nešto čudno na Vašem uređaju? Je li zahvaćen određeni račun (npr. društvenih mreža) ili je zahvaćen cijeli uređaj? Ako se čini kao malware, pazite kako ubuduće koristite i nosite taj zaraženi uređaj—upotrijebite drugi uređaj* kako biste kontaktirali stručnjaka za pomoć.

*Drugi uređaj ne bi bio povezan s zaraženim uređajem. To može biti, na primjer, računalo u knjižnici ili telefon pouzdanog prijatelja.

KONTAKTIRAJTE TEHNIČARA OD POVJERENJA

Vodite zapisnik, poput neobičnih poruka koje ste primili u izvornom obliku (npr. ako je email, proslijedite izvorni email s metapodacima u zaglavlju, a ne snimku zaslona). Uključite detalje: datum, vrijeme i opis. Pošaljite ih tehničaru od povjerenja.

PROCIJENITE ŠTETU

Koji su osjetljivi podaci koji bi mogli biti ugroženi? Trebate li promjeniti neku od svojih lozinki ili račune? Planirajte sljedeće korake za sigurnost tako što ćete napraviti procjenu rizika (tzv. “modeliranje prijetnji”)

Zašto su metapodaci bitni?

Zadnji pregled: 11. ožujka, 2019.

Metapodaci su često opisani kao “sve osim sadržaja Vaših komunikacija”. Možete o metapodacima razmišljati kao o digitalnom ekvivalentu omotnice. Kako omotnica sadržava informacije o pošiljatelju, primatelju, i odredištu poruke, tako iste informacije sadrže i metapodaci. Metapodaci su informacije o digitalnim komunikacijama koje pošaljete i dobijete. Neki primjeri metapodataka su:

- naslov Vaših emailova
- duljina Vaših razgovora
- vremenski okvir u kojem se razgovor dogodio
- vaša lokacija prilikom razgovora (kao i s kim ste razgovarali)

Povijesno, u nekim zemljama - uključujući SAD - su metapodaci imali manju zakonsku zaštitu privatnosti nego sadržaj komunikacije. U mnogim zemljama policija može lakše dobiti ispis Vaših poziva u zadnjih mjesec dana nego što mogu postaviti prisluškivač na Vašu telefonsku liniju kako bi čuli što točno govorite.

Oni koji skupljaju ili traže pristup metapodacima, npr. vlade ili telekomunikacijske tvrtke, tvrde da objavljivanje (i skupljanje) metapodataka ne stvara problem. Nažalost, to nije uopće točno. Čak i mali set metapodataka može dati intimni pogled u život osobe. Pogledajmo što i kako metapodaci mogu otkriti vladi i kompanijama koje ih skupljaju.

- Znaju da ste nazvali liniju za telefonski seks u 2:24 ujutro i razgovarali 18 minuta, no ne znaju o čemu ste razgovarali.
- Znaju da ste zvali telefonsku liniju za prevenciju samoubojstava s mosta Golden Gate. Tema poziva ostaje tajna.
- Znaju da ste dobili email od službe za testiranje na HIV, da ste zatim nazvali svog liječnika, a zatim posjetili web stranicu HIV grupe za podršku u istom satu. Ne znaju što je bilo u emailu ili o čemu ste razgovarali telefonom.
- Znaju da ste primili email od grupe boraca za digitalna prava s naslovom “Recimo Kongresu: Zaustavite SESTA/FOSTA” i odmah nakon toga nazvali svog izabranog predstavnika. No sadržaj tih komunikacija ostaje siguran od vladinog upada.
- Znaju da ste nazvali ginekologa, razgovarali pola sata, a zatim kasnije tog dana nazvali broj lokalne klinike za pobačaje.

Može biti teško zaštititi svoje metapodatke od vanjskog prikupljanja, jer treće strane često trebaju metapodatke za uspješno povezivanje Vaše komunikacije. Baš kao što poštar mora moći pročitati što piše na kuverti kako bi isporučio Vašu pošiljku, digitalne komunikacije često moraju biti označene izvorom i odredištem. Telekomunikacijske tvrtke moraju otprilike znati gdje se nalazi Vaš telefon kako bi na njega usmjerile pozive.

Usluge kao što je Tor nadaju se ograničiti količinu metapodataka koji se proizvode putem uobičajenih metoda online komunikacije. Sve dok se zakoni ne izmjene na način kako bi se bolje bavili metapodacima i dok alati koji ih minimiziraju ne postanu rasprostranjeniji, najbolje što možete učiniti je znati koje metapodatke prenosite kada komunicirate, tko može pristupiti tim informacijama i kako ih se može iskoristiti.

Vaš sigurnosni plan

Zadnji pregled: 01. veljače, 2021.

Pokušavati zaštiti svoje podatke od svakog i stalno je nepraktično i iscrpljujuće. Ali, bez straha! Sigurnost je proces, i kroz pomno planiranje možete složiti plan koji je ispravan za Vas. Sigurnost ne leži samo u alatima koje koristite ili softwareu kojeg preuzmete. Sigurnost počinje sa razumijevanjem unikatnih prijetnji s kojima se suočavate i kako ih možete odbiti.

U računalnoj sigurnosti, prijetnja je potencijalni događaj koji bi mogao potkopati Vaše napore da zaštitite svoje podatke. Prijetnje s kojima se suočavate možete odbiti tako što odredite što Vam je potrebno za zaštitu i od koga morate štititi podatke. Ovo je proces sigurnosnog planiranja, koji se često naziva “modeliranje prijetnji”.

Ovaj vodič će Vas naučiti kako izraditi sigurnosni plan za svoje digitalne informacije i kako odrediti koja rješenja su najbolja za Vas.

Kako izgleda sigurnosni plan? Recimo da želite osigurati svoju kuću i imetak. Mogli bi si postaviti sljedeća pitanja:

Što imam unutar svog doma što je vrijedno štićenja?

Imovina može uključivati: nakit, elektroničke uređaje, financijske dokumente, putovnice ili fotografije

Od koga želim zaštititi svoju imovinu?

Protivnici mogu uključivati: provalnike, cimere ili goste

Koliko je vjerojatno da ću trebati štititi imovinu?

Ima li moje susjedstvo povijest provala? Koliko mogu vjerovati svojim cimerima/gostima? Koje su sposobnosti mojih protivnika? Koje rizike trebam razmotriti?

Koliko su loše posljedice ako ne uspijem zaštititi svoju imovinu?

Imam li nešto u svojoj kući što ne mogu nadomjestiti? Imam li vremena ili novaca s kojim mogu nadomjestiti imovinu? Imam li osiguranje koje pokriva stvari ukradene iz mog doma?

Koliko sam spreman/spremna proći da spriječim te posljedice?

Jesam li voljan/voljna kupiti sef za osjetljive dokumente? Mogu li priuštiti kvalitetnu bravu? Imam li vremena otvoriti sigurnosni pretinac u lokalnoj banci i čuvati vrijednosti tamo?

Nakon što ste si postavili ova pitanja možete procijeniti koje mjere poduzeti. Ako je Vaša imovina vrijedna, ali je vjerojatnost provale niska, možda nećete htjeti investirati previše novca u bravu. Ako je vjerojatnost provale visoka, možda će te htjeti nabaviti najbolju bravu na tržištu, i razmotriti nabavku sigurnosnog sustava.

Stvaranje sigurnosnog plana će Vam pomoći da razumijete prijetnje koje su unikatne za Vas, te da procijenite s čim raspolažete, s čim raspolažu Vaši protivnici, koje su njihove sposobnosti te koje su vjerojatnosti rizika s kojima ste suočeni.

Kako da napravim svoj sigurnosni plan? Gdje da počnem?

Sigurnosno planiranje Vam pomaže identificirati što bi se moglo dogoditi stvarima koje cijenite i da odredite od koga ih trebate zaštititi. Prilikom stvaranja sigurnosnog plana odgovorite na ovih pet pitanja:

- Što želim zaštititi?
- Od koga to želim zaštititi?
- Koliko su loše posljedice ako ne uspijem?
- Koliko je vjerojatno da ću to morati zaštititi?
- Koliko sam spreman/spremna proći da spriječim eventualne posljedice?

Pogledajmo detaljnije svako od ovih pitanja.

Što želim zaštititi?

“Imovina” je nešto što cijenite i želite zaštititi. U kontekstu digitalne sigurnosti, imovina je najčešće neka vrsta informacije. Npr. Vaš email, kontakti, poruke, lokacija i datoteke su moguća imovina. Vaši uređaji također mogu biti imovina.

Napravite popis svoje imovine: podaci koje želite zadržati, gdje se drže ti podaci, tko im ima pristup, i što spriječava druge da im pristupe.

Od koga to želim zaštititi?

Kako bi odgovorili na ovo pitanje, bitno je da identificirate tko bi mogao ciljati na Vas ili na Vaše informacije. Osoba ili entitet koji predstavlja prijetnju Vašoj imovini je “protivnik”. Primjeri potencijalnih protivnika su Vaš šef, bivši partner, poslovna konkurencija, vlada, ili haker na javnoj mreži.

Napravite popis svojih protivnika, ili onih koji bi se možda htjeli dočepati Vaše imovine. Vaš popis može sadržavati pojedince, vladine organizacije ili korporacije.

Ovisno o tome tko su Vam protivnici, pod određenim okolnostima, ovaj popis može biti nešto što bi htjeli uništiti nakon što ste završili sa sigurnosnim planiranjem.

Koliko su loše posljedice ako ne uspijem?

Postoji mnogo načina na koje protivnik može doći do Vaših podataka. Na primjer, protivnik može pročitati Vašu privatnu komunikaciju dok prolazi kroz mrežu, ili može obrisati ili pokvariti Vaše podatke.

Motivi protivnika su šaroliki, isto kao i njihove taktike. Vlada koja pokušava spriječiti širenje videa koji prikazuje policijsko nasilje će se možda zadovoljiti time da jednostavno obriše video ili mu smanji dostupnost. Na drugoj strani, politički protivnik će možda htjeti pristupiti tajnom sadržaju i objaviti ga bez Vašeg znanja.

Sigurnosno planiranje uključuje razumijevanje koliko loše posljedice mogu biti ako protivnik uspješno ostvari pristup Vašoj imovini. Kako bi odredili koliko loše posljedice mogu biti, trebali bi razmotriti sposobnosti svojih protivnika. Na primjer, Vaš teleoperater ima pristup svim Vašim telefonskim zapisima. Haker na otvorenoj Wi-Fi mreži može pristupiti Vašim nekriptiranim komunikacijama. Vaša vlada može imati i snažnije sposobnosti.

Napišite što bi Vaš protivnik mogao htjeti napraviti s Vašim podacima.

Koliko je vjerojatno da ću to morati zaštititi?

Rizik je vjerojatnost da će se određena prijetnja protiv određene imovine stvarno dogoditi. Rizik ide ruku u ruku sa sposobnostima. Iako Vaš teleoperater ima mogućnost pristupa svim Vašim podacima, rizik da će objaviti Vaše privatne podatke online sa ciljem narušavanja Vaše reputacije je nizak.

Važno je razlikovati što se može dogoditi i vjerojatnosti da će se dogoditi. Na primjer, postoji prijetnja da će se Vaša zgrada urušiti, ali je taj rizik puno veći u San Franciscu (gdje su potresi učestali) nego u Stockholmu (gdje nisu).

Procjena rizika je osobni i subjektivni proces. Neki ljudi smatraju neke prijetnje neprihvatljivima bez obzira na vjerojatnost, jer samo postojanje takvih prijetnji na bilo kojoj vjerojatnosti nije vrijedno rizika. U drugim slučajevima, ljudi zanemaruju visoke rizike jer ne smatraju prijetnju problemom.

Napišite koje prijetnje će te uzeti za ozbiljno, a koje bi mogle biti dovoljno rijetke ili bezopasne (ili prekomplicirane za suzbijanje) da bi se brinuli o njima.

Koliko sam spreman/spremna proći da spriječim eventualne posljedice?

Ne postoji savršena opcija za sigurnost. Nemaju svi iste prioritete, brige ili pristup resursima. Vaša procjena rizika će omogućiti da planirate ispravnu strategiju za Vas, balansirajući pritom između pogodnosti, troška i privatnosti.

Na primjer, odvjetnik koji zastupa klijenta u slučaju koji se tiče nacionalne sigurnosti može biti voljan odraditi više da osigura komunikaciju oko slučaja, npr. koristeći enkriptirani email, nego član obitelji koji redovito šalje smiješne videa mačaka.

Napišite koje su Vam opcije dostupne za otklanjanje Vama unikatnih prijetnji. Navedite ako imate ikakvih financijskih, tehničkih ili društvenih ograničenja.

Sigurnosno planiranje kao redovita praksa

Imajte na umu da se Vaš sigurnosni plan može mijenjati kako se Vaša situacija mijenja. Stoga je često revidiranje sigurnosnog plana dobra praksa.

Napravite svoj sigurnosni plan temeljen na Vašoj unikatnoj situaciji, zatim označite u svom kalendaru neki datum u budućnosti. Ovo će Vas podsjetiti da pregledate svoj plan i da provjerite ako je još uvijek relevantan za Vašu situaciju.

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

In partnership with

LOCALIZATION LAB