Malware

Për më shumë informacion: SEC.EEF.ORG
Një projekt i Electronic Frontier Foundation

MALWARE, shkurtim për “malicius software” (software dashakeq), është çfarëdo programi i hartuar për të kryer veprime të padëshiruara në pajisjen tuaj

Shembuj malware-i janë:

- viruse kopmjuteri
- programe që vjedhin fjalëkalimet
- programe që ju incizojnë dhe regjistrojnë fshehtas
- programe që fshijnë fshehtas të dhëna tuajat

MALWARE PËRMES KARREMËZIMI

Karremëzim do të kishte kur dikush që ju sulmon, dërgon një mesazh, email ose lidhje që duket pa hile, por faktikisht është dashakeqe. Karremëzimi shpesh përfshin imitimin e dikujt që e njihni, ose imitimin e një platforme së cilës i zini besë.

Shënim: Jo krejt karremëzimet përfshijnë malware. Ndonjëherë një agresor dëshiron të vjedhë fjalëkalime për te një shërbim dhe mund ta bëjë këtë duke imituar një sajt, pa instaluar malware në pajisjen e përdoruesit.

RRUGË TË RËNDOMTA SE SI INSTALOHET MALWARE-I

Hapja e një bashkëngjitjeje ose dokumenti dashakeq	Shpesh në mesazhe karremëzimi jepet një bashkëngjitje dashakeqe
Klikimi i një lidhje dashakeqe	Shpesh në mesazhe karremëzimi jepet një lidhje dashakeqe
Shkarkim software-i pa licencë	Software-i, për të cilin s’mund të aplikohen përditësime sigurie, shton rrezikun (p.sh., jo

	nga shitorja Apple App apo shitorja Google Play.)
Vizita në sajte të kompromet uar	Ndonjëherë shtihet në dorë kontrolli i sajtit dhe përdoret për të strehuar lëndë dashakeqe.

LLOJE MALWARE-I

Adware	reklama kudo Ky software dashakeq zakonisht provon t'i shfaqë reklama përdoruesit, duke hapur dritare flluska përmbi dritaren e çastit, ose përmes metodash të tjera. Adware tjetër ndjek informacione mbi përdoruesin, ose përfton hollësi personale të tijat. Adware-i, po si malware tjetër, mund të paketohet bashkë me tjetër software, të shkarkuar shpesh nga burime të dyshimta, fjala vjen, jashtë shitoresh zyrtare aplikacionesh, apo prej zhvilluesit të software-it.
Stalkerware	kur pajisja juaj ndihmon ndjekësin tuaj Stalkerware funksionon në heshtje dhe i jep agresorit kontroll të plotë të një pajisjeje. Stalkerware mund të instalohet nga dikush që mund të përdorë nga afër pajisjen tuaj (bie fjala, një anëtar i familjes, ose partnerja, "nëma një minutë telefonin") dhe instalon një aplikacion stalkerware, ose kur një përdorues gënjehet të shkarkojë aplikacionin.
Trojan	shfaqet si dhuratë, por është sulm i maskuar Kur shkarkohet, software-i trojan mund të funksionojë si aplikacioni i ligjshëm të cilin imiton, por në fakt është duke kryer në prapaskenë gjëra të mbrapshta.

	Shpesh ky gjendet në software të kopjuar pa leje apo “të zbërthyer”, apo në software gjoja antivirus.
Ransomware	software që ju mban peng Kur shkarkohet, ky software dashakeq mban peng të dhëna të një shoqërie, një enti, apo një individi, kundrejt një pagese. Ransomware-i fitoi popullaritet në dhjetëvjeçarin e fundit dhe sot është një biznes miliona dollarësh për agresorë anembanë botës.
Sulm A.P.T.	Kërcënim i Avancuar i Vazhdueshëm Një sulm A.P.T. është malware nga një kundërshtar me aftësi të sofistikuara dhe me shumë më tepër burime kushtuar arritjes së qëllimeve të veta: kompromet imit të sistemit tuaj. Sulmet A.P.T. shpesh përdoren njëkohësisht me aktorë në rang shteti, të cilët do të rreken të ruajnë “vazhdueshmërinë”, ose hyrjen afatgjatë në sistemin që kanë vënë në shënjestër.

5 KËSHILLA SI TË MBROHEMI NGA MALWARE-I

KËSHILLA #1: PËRDITËSONI SOFTWARE-IN TUAJ

(& SHIHNI NËSE PO PËRDORNI SOFTWARE TË LICENCUAR*)

Shumica e malware-it përfiton nga dobësi të njohura. Shoqëritë e software-it shpesh i ndreqin vetë këto dobësi dhe ua kalojnë ndreqjet përdoruesve përmes përditësimesh.

Prandaj, përditësimet e software-it janë kritike për sigurinë e përdoruesve, ngaqë janë mënyra më e sigurt për të qenë i përditësuar me ndreqje dobësish të ditura, të cilat mund të shfrytëzohen nga agresorë.

*Nëse s’jeni i sigurt se si të merrni software të licencuar, pyetni specialistin tuaj dashamirës të sigurisë dixhitale, për këshilla dhe burime të gatshme.

KËSHILLË #2: KOPJE REZERVË PËR TË ARDHMEN

Bëni kopje rezervë të të dhënave tuaja sot dhe do t'ia dini vetes për mirë në të ardhmen. Nëse humbni pajisjen tuaj (qoftë për shkak malware-i, qoftë pnga vjedhje, apo se pajisja nuk ndizet më), nuk humbet gjithçka: kartelat tuaja do t'i keni te kopjet rezervë.

Mbrojini këto kopje rezervë duke përdorur një fjalëkalim të fuqishëm dhe fshehtëzim.

KËSHILLË #3 NDALUNI NJË ÇAST, PARA SE TË KLIKONI

Ndarja me të tjerët e lidhjeve dhe kartelave* është praktikë e rëndomtë, por hapni sytë kur ndërveproni me lidhje, apo i ndani me të tjerët. Para se të klikoni, bëjini vetes pyetjen: a duket e çuditshme?

SHIHNI PËR… LIDHJE TË SHKURTUARA & TË CUNGUARA

Lidhjet dhe email-et mund të duken si më të shkurtra, kur shihen në telefon, në vend se në kompjuter. Shkurtues lidhjesh, të tillë si bit.ly & shërbime të ngjashme mund t'ju drejtojnë te sajte keqdashës.

Këshillë: Përdorni shërbime si: https://unshorten.it për të parë URL-në e plotë!

IMITIMI, FORMA MË E MADHE E MASHTRIMIT

Gabimet e shkrimit, shkronja apo shenja të ngjashme dhe elementë marke të kopjuar janë atje për t'ju mashtruar. Verifikoni se është shërbimi i vërtetë.

Këshillë: Kur ndërveproni me një shërbim autentik, përdorni një faqeshënues: kjo mund t'ia bëjë më të lehtë kompjuterit tuaj t'ju ndihmojë të mbani mend adresa sajtesh të ligjshëm.

Këshillë: Ruani lidhjen e saktë te përgjegjësi juaj i fjalëkalimeve: një përgjegjës fjalëkalimesh mund të mbajë mend sajtet që i tregohen dhe të plotësojë për ju fjalëkalimet tuaja.

Hapni sytë për "social engineering," fjala vjen, marrja e një mesazhi nga dikush që hiqet se është shok i juaji.

Këshillë: Lidhuni me shokun tuaj përmes një forme tjetër komunikimi dhe sigurohuni se është vërtet ai.

PREKJE APO KLIKIM PADASHUR

Kur shqyrtoni lidhje në pajisjen tuaj, një prekje apo klikim mund të hapë padashur lidhjen!

Këshillë: Nëse përdorni një mi, përfitoni nga kalimi i kursorit përsipër, që të shihni lidhjen e plotë.

KËSHILLË #4: HAPNI SYTË NGA SHTËNIA NË DORË E PAJISJEVE

Ndonjëherë, kundërshtarët tanë janë persona që i njohim, ose persona që mund të përdorin pajisjet tona, kur ne s'kemi mendjen. Përdorimi i fshehtëzimit të krejt diskut dhe i një fjalëkalimi të fuqishëm, për të mbrojtur pajisjen tuaj, mund të ndihmojë të mbrohet ajo nga futja e duarve të

padëshiruara. Kini mendjen kur i jepni dikujt pajisjen tuaj të shkyçur. Për të lexuar më tepër, shihni te ssd.eff.org.

KËSHILLË 5: PËRDORNI NJË ANTIVIRUS

Jo të gjithë antiviruset janë krijuar njësoj: ndonjë software i reklamuar si antivirus mund të jetë malware i maskuar. Mund të doni të përdorni antivirusin e prodhuesit të pajisjes tuaj. Nëse parapëlqeni software antivirus nga një palë e tretë, shihni për:

- shqyrtime të pavarura të software-it
- nëse sajti i antivirusit ka një listë të përditësuar malware*-i të llojit tuaj dhe për kundërshtarin me të cilin ndesheni

*Punë e botuar kërkimore rreth cenueshmërish mund të tregojë nëse antivirusi ka një ekip aktiv për mbrojtje nga ky lloj malware-i.

MENDOJ SE KAM MALWARE. ÇFARË DUHET TË BËJ?

A po ndodh diçka e çuditshme në pajisjen tuaj? Bëhet fjalë për gjëra që lidhen me një llogari specifike (fjala vjen, mediash shoqërore), apo për tërë pajisjen?

Nëse duket si malware, bëni kujdes si e përdorni dhe mbani atë pajisje të infektuar në të ardhmen—mandej, përdorni një tjetër pajisje* që të lidheni me një specialist për ndihmë.

*Një pajisje tjetër do të ishte e palidhur me pajisjen e prekur nga malware-i. Kjo mund të ishte një kompjuter biblioteke, ose telefoni i një miku të besuar, për shembull.

LIDHUNI ME NJË TEKNIK TË BESUAR

Mbani një regjistër, fjala vjen, mesazhet e çuditshme që morët, në formatin e tyre origjinal (p.sh., nëse është një email, përcillni email-in origjinal me metadata kryesh, jo një foto ekrani). Përfshini hollësi: datë, kohë dhe përshkrim. Dërgojani këto një tekniku të besuar.

VLERËSONI DËMIN

Ç'informacion me zarar mund të jetë kompromet uar? A duhet të ndryshoni ndonjë nga fjalëkalimet apo llogaritë tuaja? Planifikoni hapat pasues për sigurinë, duke bërë një vlerësim të rreziqeve (quajtur ndryshe edhe "modelim kërcënimesh").

Pse Kanë Rëndësi Metadatat?

Rishikimi i Fundit më: 11 mars 2019

Metadata shpesh përshkruhet si gjithçka, hiq përmbajtjen e komunikimeve tuaja. Metadatat mund t'i mendoni si barasvlerësi dixhital i një zarfi. Ashtu si zarfi përmban informacion rreth dërguesit, marrësit dhe vendmbërritjes së një mesazhi, ashtu bëjnë edhe metadatat. Metadatat janë

informacion rreth komunikimeve dixhitale që dërgoni dhe merrni. Disa shembuj te metadatave përfshijnë:

- rreshtin e subjektit të email-eve tuaj
- kohëzgjatjen e bisedave tuaja
- intervalin kohor gjatë të cilit u zhvillua një bisedë
- vendndodhjen tuaj teksa komunikonit (si dhe me kë)

Historikisht, metadatat kanë pasur më pak mbrojtje ligjore të privatësisë, në disa vende - përfshi SHBA - se sa përmbajtja e komunikimeve. Policia, në mjaft vende, më lehtë mund të marrë regjistra rreth se kujt i keni telefonuar muajin e fundit, për shembull, se sa të ujdisë përgjim të linjës tuaj telefonike, për të dëgjuar se ç'thoni faktikisht.

Ata që grumbullojnë metadata, ose kërkojnë hyrje në to, qeveritë apo shoqëri telekomunikacioni, bie fjala, pretendojnë se zbulimi (dhe grumbullimi) i metadatave s'është ndonjë gjë e madhe. Mjerisht, këto pretendime thjesht s'janë të vërteta. Qoftë edhe një pjesë e vockël e metadatave mund të ofrojë një thjerrëz intime në jetën e dikujt. Le të shohim se sa gjëra u zbulojnë metadatat qeverisë dhe shoqërive që grumbullojnë të tilla:

- Ata e dinë se i keni telefonuar një linje seksi në 2:24 të natës dhe keni folur për 18 minuta. Por nuk dinë se për çfarë folët.
- Ata e dinë se i keni telefonuar një linje për parandalimin e vetëvrasjeve nga ura Golden Gate Bridge. Por subjekti i thirrjes mbetet i fshehtë.
- Ata e dinë se keni marrë një email nga një shërbim testimesh për HIV, mandej i telefonuat mjekut tuaj, më tej vizituat sajtin e një grupi ndihme për ata që vuajnë nga HIV, brenda të njëjtës orë. Pornuk njohin përmbajtjen e email-it, apo ç'folët në telefon.
- Ata e dinë se morët një email nga një grup veprimtarësh për të drejta dixhitale, ku në rreshtin e subjektit thuhej "T'i themi Kongresit: Ndalni x projektligj" dhe mandej i telefonuat menjëherë një përfaqësuesi të zgjedhur. Por lënda e këtyre komunikimeve mbetet e parrezik nga ndërhyrje të qeverisë.
- Ata e dinë se i telefonuat një gjinekologu, folët gjysmë ore dhe mandej i telefonuat një klinike lokale abortesh, po atë ditë.

Mbrojtja e metadatave nga grumbullues të jashtëm mund të jetë e vështirë, ngaqë palë të treta shpesh kanë nevojë për to, që komunikimet tuaja të kenë sukses. Ashtu si një postieri i duhet të jetë në gjendje të lexojë ç'shkruhet mbi zarf, që të mundet ta shpjerë letrën atje ku duhet, shpesh në komunikimet dixhitale lypset të jetë shënuar burimi dhe vendmbërritja. Shoqërive të telefonave celularë u duhet të dinë ku gjendet afërsisht telefoni juaj, që të mund të kalojnë thirrje në të.

Shërbime si Tor shpresojnë të kufizojnë sasinë e metadatave që prodhohet përmes metodash të zakonshme komunikimesh internetore. Deri sa ligjet të përditësohen për të trajtuar më mirë metadatat dhe mjetet që i minimizojnë ato të përhapen më shumë, gjëja më e mirë që mund të bëni është të jeni të ndërgjegjshëm rreth metadatave që transmetohen kur komunikoni, cilët mund të hyjnë në ato informacione dhe si mund t'i përdorin ato.

Plani Juaj i Sigurisë

Shqyrtuar Së Fundi më: 1 shkurt 2021

Të rrekeni të mbroni krejt të dhënat tuaja nga gjithkush, gjithë kohën, është jopraktike dhe stërmunduese. Por mos kini frikë! Siguria është një proces dhe përmes planifikimi të peshuar, mund të hartoni një plan që është i duhuri për ju. Siguria s'është thjesht mjetet që përdorni, apo software-i që shkarkoni. Ajo fillon me të kuptuarit e kërcënimeve unike që keni përpara dhe se si mund t'u bëni ballë këtyre kërcënimeve.

Në sigurinë e kompjuterave, një kërcënim është një akt potencial që mund të dëmtojë përpjekjet tuaja për mbrojtjen e të dhënave tuaja. Kërcënimeve që ju dalin mund t'u bëni ballë duke përcaktuar se ç'është e nevojshme të mbroni dhe se prej kujt ju duhet ta mbroni. Ky është procesi i planifikimit të sigurisë, të cilit shpesh i referohen edhe si "modelim kërcënimesh".

Ky udhërrëfyes do t'ju mësojë si të hartoni një plan sigurie për informacionin tuaj dixhital dhe se si të përcaktoni se cilat zgjidhje janë më të mirat për ju.

Me çfarë ngjan një plan sigurie? Le të themi se dëshironi të mbani të parrezik shtëpinë dhe gjërat tuaja. Ja pak pyetje që mund t'i bënit vetes:

Ç'ia vlen të mbrohet, nga gjërat që kam brenda shtëpisë?

Në to mund të përfshiheshin: bizhuteri, aparate elektronike, dokumente financiarë, pasaporta, apo fotografi

Prej kujt dua t'i mbroj?

Në kundërshtarët mund të përfshiheshin: hajdutë, shokë dhome, ose mysafirë

Sa gjasa ka që të më duhet t'i mbroj?

A ka mëhalla ime historik vjedhjesh shtëpish? Sa të besueshëm janë shokët e mi të dhomës/mysafirët e mi? Ç'aftësi kanë kundërshtarët e mi? Cilat rreziqe duhet të marr parasysh?

Sa të rënda janë pasojat, nëse dështoj?

A kam në shtëpi ndonjë gjë të cilën s'mund ta zëvendësoj? A kam kohë, apo para, t'i zëvendësoj këto gjëra? A kam sigurime që mbulojnë gjërat e vjedhura nga shtëpia ime?

Përmes sa andrallave jam i gatshëm të kaloj për t'i shmangur këto pasoja?

A do të blija një kasafortë për dokumente me zarar? A ma mban xhepi të blej një bravë të cilësisë së lartë? Arrij dot të hap një kuti sigurie në bankën time lokale dhe të mbaj atje gjërat e mia me vlerë?

Pasi t'i keni bërë vetes këto pyetje, jeni në gjendje të vlerësoni ç'masa të merrni. Nëse gjërat tuaja janë me vlerë, por gjasat për hyrje vjedhësish në shtëpi janë të vogla, atëherë mund të mos doni të

investoni shumë para për një bravë të fortë. Por nëse gjasat janë të mëdha, do të donit të blinit bravën më të mirë që ka tregu dhe të shihnit mundësinë e shtimit të një sistemi sigurie.

Hartimi i një plani sigurie do t'ju ndihmojë të kuptoni kërcënimet që janë unike për ju dhe të peshoni gjërat tuaja me vlerë, kundërshtarët tuaj dhe aftësitë e tyre, tok me probabilitetin e rreziqeve që keni përballë.

Si ta hartoj planin tim të sigurisë? Nga t'ia filloj?

Planifikimi i sigurisë ju ndihmon të identifikoni se ç'mund të ndodhë me gjërat që çmoni dhe të përcaktoni se prej cilëve lypset t'i mbroni ato. Kur hartohet një plan sigurie, përpiquni t'u përgjigjeni këtyre pesë pyetjeve:

- Çfarë dua të mbroj?
- Prej kujt dua t'i mbroj?
- Sa të rënda janë pasojat, nëse dështoj?
- Sa gjasa ka të më duhet t'i mbroj?
- Përmes sa andrallave jam i gatshëm të kaloj për të shmangur pasoja të mundshme?

Le të shohim më afër secilën prej këtyre pyetjeve.

Çfarë dua të mbroj?

Një "aset" është diçka që e çmoni dhe dëshironi ta mbroni. Në kontekstin e sigurisë dixhitale, një aset zakonisht është një lloj informacioni. Për shembull, email-et tuaj, lista kontaktesh, mesazhe të atypëratyshëm, vendndodhje dhe kartela, të tëra janë asete të mundshëm. Pajisjet tuaja mund të jenë gjithashtu asete.

Hartoni një listë të aseteve tuaja: të dhëna që ruani, ku i ruani, cilët mund të hyjnë në to dhe çfarë i pengon të tjerët të hyjnë në to.

Prej kujt dua t'i mbroj?

Për t'ju përgjigjur kësaj pyetjeje, është e rëndësishme të identifikohen cilët mund të kenë ju si synim, ose informacion tuajin. Një person, ose një njësi që përbën rrezik për burimet tuaja është një "kundërshtar". Shembuj kundërshtarësh potencialë janë, shefi apo padroni juaj, ish-partnerja juaj, konkurrentët e biznesit tuaj, qeveria juaj, ose një hacker në një rrjet publik.

Hartoni një listë të kundërshtarëve tuaj, ose atyre që mund të duan të hedhin në dorë asetet tuaj. Lista juaj mund të përfshijë individë, agjenci qeveritare, ose korporata.

Në varësi të faktit se cilët janë kundërshtarët tuaj, në disa rrethana kjo listë mund të jetë diçka që do të donit ta asgjësonit, pasi të keni mbaruar me planifikimin e sigurisë.

Sa të rënda janë pasojat, nëse dështoj?

Ka mjaft mënyra me të cilat një kundërshtar mund të arrijë të hyjë në të dhënat tuaja. Për shembull, një kundërshtar mund të lexojë komunikimet tuaja private, teksa kalojnë nëpër rrjet, ose mund të fshijë apo korruptojë të dhënat tuaja.

Motivet e kundërshtarëve mund të jenë shumë të ndryshme nga njëri te tjetri, siç janë edhe taktikat e tyre. Një qeveri që rreket të pengojë përhapjen e një videoje ku shfaqet dhunë policore, mund të kënaqet thjesht duke e fshirë, ose të reduktojë parjet e videos. Në kontrast me këtë, një kundërshtar politik mund të dojë të arrijë të hyjë në lëndë të fshehtë dhe ta bëjë publike atë lëndë pa e ditur ju.

Planifikimi i sigurisë përfshin të kuptuarit se sa të rënda mund të jenë pasojat, nëse një kundërshtar arrin të shtjerë në dorë një nga asetet tuaj. Për ta përcaktuar këtë, duhet të merrni parasysh aftësitë e kundërshtarit tuaj. Për shembull, shërbimi i telefonit tuaj celular ka në dorë krejt regjistrimet e telefonatave tuaja. Një hacker në një rrjet të hapët Wi-Fi mund të shohë komunikimet tuaja të pafshehtëzuara. Qeveria juaj mund të ketë aftësi edhe më të fuqishme.

Hidhni në letër se ç'mund të dojë të bëjë kundërshtari juaj me të dhënat tuaja private.

Sa gjasa ka të më duhet t'i mbroj?

Rreziku është probabiliteti që një kërcënim i caktuar kundër një aseti të caktuar të materializohet faktikisht. Shkon krah për krah me aftësinë. Teksa shërbimi i celularit tuaj ka aftësinë të hyjë në krejt të dhënat tuaja, rreziku që ata të postojnë publikisht të dhënat tuaja private, për të dëmtuar reputacionin tuaj, është i pakët.

Është e rëndësishme të bëhet dallimi mes çka mund të ndodhë dhe probabilitetit se do të ndodhë. Për shembull, ka një rrezik se ndërtesa ku banoni mund të rrëzohet, por rreziku se ndodh kjo është shumë më i madh në San Francisko (ku tërmetet janë të zakonshëm), se sa në Stokholm (ku nuk janë).

Peshimi i rreziqeve është një proces sa personal, aq edhe subjektiv. Mjaft vetëve disa rreziqe u duken të papranueshëm, pavarësisht gjasave që të ndodhin, ngaqë për ta, thjesht me praninë e kërcënimit, s'ia vlen më barra qiranë. Në raste të tjera, njerëzve s'u hyjnë në sy rreziqe të mëdha, ngaqë s'e shohin si problem kërcënimin.

Hidhni në letër cilat kërcënime do t'i merrni seriozisht dhe cilat mund të jenë shumë të rralla, apo shumë të padëmshme (ose shumë të zorshme për t'i luftuar) për t'u shqetësuar për to.

Përmes sa andrallave jam i gatshëm të kaloj për të shmangur pasoja të mundshme?

Për sigurinë nuk ka mundësi të përsosur. Jo gjithkush ka të njëjtat përparësi, shqetësime, apo mundësi përdorimi mjetesh dhe burimesh. Peshimi juaj i rreziqeve do t'ju lejojë të planifikoni strategjinë e duhur për ju, e cila vë në baraspeshën leverdinë, koston dhe privatësinë.

Për shembull, një avokat që përfaqëson një klient në një çështje lidhur me sigurinë kombëtare mund të dojë t'i hyjë më thellë mbrojtjes së komunikimeve mbi atë çështje, fjala vjen, duke

përdorur email të fshehtëzuar, se sa një anëtar i familjes që dërgon rregullisht me email video zbavitëse me maçokër.

Hidhni në letër çfarë mundësish keni në dorë për t'ju ndihmuar të zbusni kërcënimet tuaja unike. Nxirrni në pah, nëse keni, kufizime financiare, teknike apo shoqërore.

Planifikime sigurie si praktikë e rregullt

Mbani parasysh se plani juaj i sigurisë mund të ndryshojë, nëse ndryshon situata juaj. Ndaj, rikthimi shpesh te plani juaj i sigurisë është një praktikë e mirë.

Krijojeni planin tuaj të sigurisë duke u bazuar në situatën tuaj unike. Mandej vini një shenjë në kalendari tuaj për një datë në të ardhmen. Kjo do t'ju kujtojë të rishihni planin tuaj dhe ta rikontrolloni, për të përcaktuar nëse ka ende vend për situatën tuaj.

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

In partnership with

LOCALIZATION LAB