Nicoleta :După ce Internetul a ajuns în aproape fiecare locuinţă, iar reţeaua globală a devenit un suport pentru serviciile diverselor companii, viruşii informatici şi alte programe dăunătoare (ransomware, adware, spyware) s-au răspândit din ce în ce mai mult şi au început să producă pagube cu adevărat însemnate, compromiţând nu doar datele de pe calculatoarele utilizatorilor obişnuiţi, ci şi cele de maximă importanţă ale diverselor instituţii, ale băncilor sau chiar ale companiilor aeriene. Este lesne de dedus că serviciile acestora au devenit inaccesibile, iar de aici au rezultat pierderi financiare semnificative, iar în unele cazuri uriaşe. În ziua de azi, este de neconceput un computer fără antivirus sau un program de securitate, mai ales dacă rulează sistemul de operare Windows - cel mai vizat de către programatorii rău intenţionaţi.

Catea:Astazi va vom prezenta cativa daunatori: si anume viermii ,virusii si troianii.

Un vierme este un program de calculator maliţios, autoreplicant, proiectat pentru a infecta calculatoare

1.Cum se răspândesc şi se promovează viermii?

Unii paraziţi, numiţi viermi de mass-mailing, se propagă prin intermediul email-urilor. Aceştia ajung în fişiere ataşate mesajelor de email sau vin integraţi în scrisori. După ce utilizatorul deschide o astfel de scrisoare sau fişier, viermele se va instala silenţios în sistem. Utilizatorul nu va putea observa ceva suspicios deoarece parazitul nu afişează vreun ghid de instalare, dialog sau avertisment.

Viermii răspândiţi în întreaga lume infectează un calculator vulnerabil pe internet, exploatând sistemul de operare ştiut şi vulnerabilităţile programului de securitate instalat. Un astfel de parazit se răspândeşte pe cont propriu, şi nu necesită implicarea utilizatorului.

Mulţi viermi se distribuie în fişiere infectate care ajung ataşate mesajelor instante sau pot fi descărcate de pe reţele de răspândire fişiere sau reţele neprotejate. Astfel de viermi răspândesc fişierul infecţios cu nume utile pentru a înşela utilizatorii în a-l executa. Imediat după ce utilizatorul deschide un astfel de fişier, viermele va infecta silenţios un calculator.

2. Ce face un vierme în calculatorul meu?

Utilizarea unui sistem compromis pentru a se răspândi prin email, reţele de răspândire fişiere, instant messenger, chat-uri online sau reţele deschise.

Infectarea fişierelor, coruperea aplicaţiilor instalate, şi avarierea întregului sistem.

Furtul sau dezvăluirea de informaţii personale sensibile, documente valoroase, parole, nume de autentificare, detalii despre identitate, şi contactele utilizatorului.

Instalarea unui backdoor sau lăsarea unor alţi paraziţi periculoşi.

Modificarea setărilor de sistem esenţiale pentru a scade securitatea generală a sistemului, pentru a-l face mai vulnerabil.

Să degradeze sever viteza de conectare la internet şi performanţa generală a sistemului, cauzând instabilitatea software-urilor. Unii paraziţi sunt prost programaţi; risipesc prea multe resurse ale calculatorului şi intră în conflict cu aplicaţiile instalate.

Nu oferă funcţie de dezinstalare, îşi ascunde procesele, fişierele, şi alte obiecte pentru a-şi complica eliminarea cât mai mult posibil.

3. Cele mai periculoase exemple de viermi

Este probabil cel mai cunoscut şi în acelaşi timp unul dintre cei mai prolifici viruşi de mail. În mai puţin de şase luni, peste 50 de milioane de utilizatori au fost curioşi să afle ce conţine un e-mail cu subiectul "I Love You". Nu ştim exact cum şi de ce, dar printre aceştia s-au numărat şi sisteme ale Pentagonului, CIA şi ale parlamentului britanic. Instituţiile au fost obligate să oprească accesul la e-mail până la eliminarea virusului.Tot în 2000, site-uri gigant precum Amazon şi eBay întâmpină mari probleme din cauza flood-urilor - utilizatorii nu le pot accesa, iar contorul pierderilor se învârte cu o turaţie ameţitoare - per ansamblu, 5,5 miliarde $.

MyDoom, cunoscut şi ca Novarg, Shimgapi, şi Mimail, este viermele cu cea mai rapidă răspândire. Acest parazit se propagă prin email şi reţele de răspândire fişiere. Vine în fişiere infectate ataşate mesajelor de email şi înşeală utilizatorul, încercând să îl facă să creadă că serverele de email normale i-au trimis notificări de eroare la livrare. Imediat după ce utilizatorul execută un astfel de fişier, MyDoom se va instala silenţios în sistem şi îşi va rula sarcina utilă. Viermele setează un backdoor care îi oferă atacatorului de la distanţă acces neautorizat la calculatorul compromis şi efectuează un atac Denial of Service împotriva lui SCO şi a website-ului companiei Microsoft.

Viermele The Iglamer este un parazit de internet notoriu care infectează calculatoarele vulnerabile prin găuri din securitate. Nu se distribuie cu ajutorul email-urilor sau reţelelor, ci infectează calculatoarele în mod direct. Acest virus nu depinde de acţiunile utilizatorului. Iglamer se instalează singur în sistem şi caută alte gazde vulnerabile. Viermele poate să aducă probleme de performanţă calculatorului sau să îl închidă frecvent. De asemenea, compromite sever securitatea sistemelor infectate, deci atacatorii se pot conecta şi le pot controla de la distanţă.

Cum îmi pot fixa calculatorul şi elimina viermele?

Viermii lucrează în aceeaşi manieră ca şi viruşii normali, şi prin urmare, pot fi găsiţi şi eliminaţi din sistem cu ajutorul unui anti-malware eficient. Programele care au fost testate şi sunt recomandate pentru eliminarea viermilor sunt Reimage şi Plumbytes Anti-Malware. Aceşti eliminatori de malware au o bază de date extinsă cu semnături ale paraziţilor, ce poate cu uşurinţă să detecteze şi să elimine anumiţi viermi şi alte componente maliţioase.

VIRUSI

Un virus este un program de calculator maliţios care se răspândeşte în jur infectând fişiere, instalând componente asociate lui sau eliminând fişiere media specifice. Acest program, de obicei, poartă o sarcină utilă, care este selectată de către autorul său în funcţie de intenţiile lui / ei. Un virus normal va infecta sistemul, va corupe sau şterge fişierele şi dosarele, descărca alţi paraziţi periculoşi în sistem, va colecta informaţii despre activitatea de pe Internet a utilizatorului sau va dezvălui informaţii sensitive. Dacă sistemul este infectat de către un virus extrem de periculos, poate să şi distrugă sau să cripteze toate datele ce sunt stocate pe hard disk.

De obicei, viruşii sunt împărţiţi în trei categorii principale:

1. Paraziţi ce sunt proiectaţi pentru a distribui alţi viruşi sau pentru a corupe fişierele legitime din sistem.

Exemple:

Troiani

Nukeri

Viermi

Paraziţi AOL

2. Ameninţările ce sunt capabile de a iniţia o activitate periculoasă în sistem. Acestea pot cauza alerte înşelătoare, scanări false ale sistemului, mesaje de avertizare de blocare a întregului sistem de PC şi alte acţiuni. Exemple:

Rogue anti-spyware

Ransomware

Adware

Browser hijackeri

3. Alţi viruşi. Această categorie include:

Snifferi

Unelte ale sistemului

Unelte de Administrare a Reţelei

Unelte de Administrare de la Distanţă

Unii viruşi nu aparţin acestor categorii, deoarece combină mai multe caracteristici şi funcţii. Astfel de ameninţări, uneori pot fi găsite sub denumirea de viruşi hibrizi, pot fi utilizaţi pentru afişarea de avertismente înşelătoare, să cripteze fişierele utilizatorului, să distribuie alţi viruşi plus alte activităţi adiţionale, ce sunt considerate maliţioase. Este extrem de dificil să descoperiţi şi să eliminaţi aceşti paraziţi din sistem, deoarece aceştia de obicei constau din componente care se reinstalează automat după eliminare. De asemenea, mulţi viruşi prezintă caracteristici extra, care le permit să se ascundă de software-ul antivirus. Astfel de ameninţări pot monitoriza activitatea software-ului antivirus şi să îi intercepteze cererile. Atunci când programul antivirus încearcă să verifice un fişier infectat, virusul va pasa imediat originalul, va curăţa varianta acelui fişier şi va preveni detectarea acestuia în acest mod.

Ce activităţi pot fi cauzate de către un virus?

Atunci când un program maliţios se va infiltra în sistem, va iniţia următoarele activităţi:

Va infecta, suprascrie sau şterge fişierele. Poate dăuna documentelor personale, componentelor esenţiale din sistem şi aplicaţiilor utile. De asemenea, unii viruşi pot distruge întregul sistem prin ştergerea tuturor fişierelor şi dosarelor critice din acesta.

Poate introduce un cod maliţios în registrul master boot (MBR) a unui hard disk pentru a rula o sarcină utilă distructivă înainte ca sistemul de operare să fie încărcat.

Poate adăuga componente dăunătoare programelor reputabile sau le poate modifica setările astfel încât să infecteze documentele deschise sau create cu aceste programe.

Poate dăuna sever unui calculator modificând setările esenţiale de hardware, ştergând memoria CMOS sau coruptând BIOS-ul. Acest lucru poate conduce la pierderi critice de date şi funcţionarea eronată a sistemului de calculator.

Poate crea mii de fişiere şi dosare la întâmplare care pot consuma foarte mult din resursele calculatorului.

Poate afişa numeroase mesaje false, să modifice diverse setări de sistem, să cauzeze redirecţionări şi să efectueze alte acţiuni enervante pentru a complica sarcinile normale ale utilizatorului.

Poate infecta sistemul cu troiani, backdoors, keyloggeri şi alţi paraziţi periculoşi.

Foloseşte un sistem compromis pentru a răspândi alţi malware.

Fură sau criptează date personale sensitive, documente valoroase, parole, nume de autentificare, detalii despre identitate sau contactele utilizatorului.

Evită eliminarea prin auto modificare, criptează fişierele infectate, interceptează cereri ale software-ului antivirus şi aduce modificări comportamentului normal de sistem.

Cauzează încetiniri, scade securitatea sistemului şi cauzează instabilitatea software-ului.

Moduri utilizate de către creatorii de viruşi pentru a-şi răspândi ameninţările:

Viruşii pot infecta un calculator fără cunoştinţa sau consimţământul utilizatorului. Există şase moduri pricipale prin care aceşti paraziţi nesolicitaţi pot intra în sistem:

Viruşii infectează anumite documente, executabili şi alte fişiere de pe surse de încredere. Imediat după ce o victimă deschide un astfel de document sau îl execută, un virus se va instala silenţios în sistem.

Există foarte mulţi viruşi ditribuiţi prin ataşamentele email-urilor. Aceştia pot apărea şi în mesaje instante sau pot veni în scrisori. Aceşti viruşi au nume comune şi, prin urmare, pot înşela un utilizator să le deschidă sau să le execute. Imediat după ce utilizatorul deschide un astfel de mesaj sau fişier, virusul va infecta calculatorul silenţios.

Unii viruşi sunt distribuiţi prin drive-uri externe ce sunt executate automat după ce utilizatorul introduce diskul.

Software-urile piratate şi jocurile video contrafăcute conţin de obicei diverşi viruşi. Imediat după ce utilizatorul începe instalarea unui astfel de joc sau program, parazitul va infecta silenţios sistemul.

Viruşii, de asemenea, pot intra în calculator cu ajutorul altor peste, precum troiani, viermi sau backdoors. Intră în sistem fără aprobarea şi consimţământul utilizatorului.

Care sunt cei mai populari viruşi de pe web?

Există mii de viruşi diferiţi. Următoarele exemple ilustrează cât de ameninţători şi periculoşi pot fi viruşii.

Trojan.LockScreen, cunoscut şi ca Trojan LockScreen, este un virus proiectat pentru a răspândi viruşii serioşi catalogaţi ca şi ransomware. Odată ce acest troian va infecta sistemul, va lăsa fişiere executabile predeterminate precum şi alte componente necesare pentru funcţionalitatea normală a virusului asociat. În principal, Trojan.LockScreen se răspândeşte cu ajutorul mesajelor de e-mail înşelătoare şi a ataşamentelor infectate. Totuşi, puteţi deveni infectat cu această infecţie cibernetică după ce aţi apăsat pe o reclamă de tip pop up dubioasă ce vă oferea să vă actualizaţi programele sau să instalaţi software-urile „cerute". Acest virus care se răspândeşte cu ajutorul lui Trojan.LockScreen poate conduce victima la probleme serioase deoarece este capabil să cripteze toate fişierele din calculator.

Cryptowall este un virus care aparţine catagoriei ransomware. Acest parazit este capabil să modifice toate setările esenţiale din sistem şi să blocheze tot PC-ul. De asemenea, poate cauza alerte false şi să cripteze toate fişierele dumneavoastră. Pentru a-i oferi victimei abilitatea de a-şi decripta fişierele, îi va cere o recompensă. În mod contrar, va distruge cheia de decriptare şi victima îşi va pierde fişierele. Aceşti viruşi pot fi eliminaţi din sistem cu ajutorul unui anti-spyware de încredere, însă această activitate nu ajută la deblocarea fişierelor blocate.

Mystartsearch este considerat un browser hijacker şi program cu potenţial nedorit. Se poate infiltra în calculator fără ştirea oamenilor deoarece se răspândeşte ca şi component opţional al altor programe. Acest virus nu este unul agresiv. Cu toate acestea, poate fi extrem de enervant atunci când este în calculator. Poate cauza un adevărat dezastru în maşina dumneavoastră deoarece vă poate afişa rezultate modificate ale căutărilor care pot conţine conţinut comercial, precum reclame şi banere ce conduc oamenii către website-uri predeterminate. De asemenea, poate colecta informaţii identificabile non-personale şi să transfere aceste date unor terţe. Dacă doriţi să aveţi parte doar de rezultate de încredere în urma căutărilor, ar trebui să staţi departe de MyStartSearch.com.

Koobface este un virus foarte periculos utilizat pentru a fura informaţii personale. S-a răspândit cu ajutorul reţelelor de socializare, precum Facebook, Twitter şi Yahoo Messenger. Imediat după ce se infiltrează în sistem, Koobface preia controlul asupra cookie-urilor şi le utilizează pentru a urmări victima. De asemenea, poate fi utilizat pentru a infecta calculatorul cu un alt malware. Utilizatorul nu poate elimina manual această ameninţare, şi nu poate observa nimic dubios care să îl atenţioneze de faptul că maşina lui / ei este infectată.

Cum să elimin un virus din calculatorul meu?

Viruşii pot fi găsiţi şi eliminaţi din sistem cu ajutorul mai multor metode. Unii dintre aceştia nu sunt consideraţi agresivi, deci puteţi încerca să îi eliminaţi cu ajutorul metodei de eliminare manuală. Totuşi, dacă doriţi să fiţi sigur că fiecare component ce aparţine ameninţării cibernetice a fost eliminat, trebuie să instalaţi un anti-spyware de încredere. Vă recomandăm să utilizaţi aceste programe care sunt capabile să elimine fiecare virus din sistemul PC-ului infectat: Reimage, Malwarebytes. Atenţie la faptul că uneori chiar şi cel mai reputabil anti-spyware poate eşua în a vă ajuta să eliminaţi virusul, deoarece hackerii continuă şi îşi actualizeze ameninţările. Este posibil ca dezvoltatorii de anti-spyware să nu observe la timp aceste modificări, deci anti-spywareul creat de ei poate eşua în a descoperi toate fişierele infectate. Dacă aveţi de a face chiar acum cu aşa ceva, nu e nicio problemă. În acest caz, ar trebui să vă adăugaţi întrebarea pe pagina Întrebaţi-ne şi vă vom ajuta să eliminaţi virusul gratuit.

TROIANI

Un troian (sau un cal troian) este un program de calculator maliţios utilizat pentru a infecta sistemul calculatorului ţintit şi să cauzeze activităţi maliţioase în acesta. De obicei, astfel de programe sunt utilizate pentru a fura informaţii personale, să răspândească alţi viruşi sau pur şi simplu să diminueze performanţa calculatorului. În plus, hackerii îi pot utiliza pentru a obţine acces de la distanţă neautorizat la un calculator compromis, infectând fişierele şi dăunând sistemului. Imediat după ce un troian se infiltrează în calculator, va începe să se ascundă de victimă. Troianii sunt foarte similari viruşilor normali, şi prin urmare, sunt dificil de detectat. Din acest motiv ar trebui să vă bazaţi pe un anti-spyware reputabil. Original, troianii nu se răspândesc singuri. Totuşi, versiunile recente au adăugat componente adiţionale care le pot activa propagarea. Activitatea fiecărui cal troian depinde de intenţiile autorului.

Moduri utilizate pentru infiltrarea în sistem

Unii troiani se pot propaga singuri şi pot infecta sistemul fără ca utilizatorul să fie conştient de acest lucru. Alţii trebuie să fie instalaţi manual în calculator la fel ca orice alt software. De fapt, există cinci moduri majore utilizate de aceşti paraziţi pentru a intra în sistem.

Mulţi troiani sunt distribuiţi cu ajutorul mesajelor de e-mail, reţele de răspândire fişiere şi chat-uri online (precum ICQ, AIM sau IRC). Aceştia pot veni ca şi ataşamente utile, mesaje instante, link-uri în emal sau componente ale aplicaţiilor peer-to-peer. Aceşti troiani au nume normale şi prin urmare, fac ca utilizatorii să le deschidă. Odată ce utilizatorul deschide un astfel de mesaj, calul troian se va instala silenţios în sistem.

Unii troiani pot intra în sistem folosindu-se de vulnerabilităţile browserului web. Autorii acestora rulează website-uri nesecurizate ce conţin coduri maliţioase sau distribuie reclame de tip pop-up nesigure. Oricând utilizatorul vizitează un astfel de site sau apăsă pe un pop-up, un script dăunător va instala instant un parazit. Utilizatorul nu poate observa nimic dubios, deoarece ameninţarea nu afişează nicio setare, dialog sau avertizare.

Uneori, troianii pot fi instalaţi prin intermediul altor paraziţi precum viruşi, viermi, backdoors sau chiar spyware. Aceştia intră în sistem fără ştirea sau consimţământul utilizatorului şi poate afecta pe oricine foloseşte un calculator compromis. Unele ameninţări pot fi instalate manual de utilizatori de calculatoare maliţioşi care au suficiente privilegii pentru instalarea software-ului. Foarte puţini troiani pot să se răspândească prin exploatarea de la distanţă a sistemelor cu anumite vulnerabilităţi de securitate.

Unii troiani sunt deja integraţi în anumite aplicaţii. Chiar şi programele legitime pot avea funcţii nedocumentate precum funcţia de acces de la distanţă. Atacatorul trebuie să contacteze un calculator cu un astfel de software instalat pentru a obţine instant acces neautorizat complet la sistem şi să preia controlul asupra unui anumit program.

Trojan malware

Activităţi care pot fi cauzate de către un cal troian

Majoritatea cailor troiani pot cauza activităţi precum:

Infectarea, coruperea şi suprascrierea fişierelor, componentelor esenţiale din sistem şi a aplicaţiilor instalate. De asemenea, pot distruge întregul sistem prin ştergerea fişierelor critice sau formatarea hard disk-ului.

Furtul de date financiare, precum numărul cardului de credit, nume de autentificare, parole, documente personale valoroase şi alte informaţii confidenţiale.

Să urmărească utilizatorul şi fiecare tastare pe care el sau ea o efectuează pe o tastatură. Calul troian poate de asemenea să efectueze capturi de ecran şi să iniţieze alte activităţi pentru a fura informaţii specifice.

Să trimită toate datele adunate unei adrese de email predefinite, să le încarce pe un server FTP predeterminat sau să le transfere printr-o conexiune de internet ascunsă unei gazde de la distanţă.

Să instaleze un backdoor sau să îşi activeze propriul component pentru a lăsa atacatorul de la distanţă să preia controlul asupra calculatorului compromis.

Să lase alţi paraziţi periculoşi.

Să efectueze Denial of Service (DoS) sau alte atacuri de reţea împotriva unor anumite gazde de la distanţă sau să trimită o cantitate excesivă de email-uri pentru a inunda calculatoarele predefinite.

Să instaleze un server FTP ascuns care poate fi utilizat de persoane maliţioase în diverse scopuri ilegale.

Să elimine antivirusul, anti-spywareul şi alte programe de securitate. De asemenea, calul troian poate să dezctiveze serviciile esenţiale sistemului şi să prevină uneltele standarde ale sistemului din a rula.

Să blocheze accesul utilizatorului la website-uri reputabile şi la alte resurse de securitate.

Să afişeze reclame comerciale nedorite şi pop up-uri.

Să degradeze conexiunea de Internet şi viteza calculatorului. De asemenea, poate diminua securitatea sistemului şi să cauzeze instabilitatea acestuia.

Exemple de cai Troiani

Există mii de troiani diferiţi. Următoarele exemple ilustrează cât de dăunătoare pot fi aceste ameninţări.

Trojan.Cryptolocker este un troian, utilizat pentru a răspândi nişte viruşi foarte periculoşi numiţi Cryptolocker şi Cryptowall. Se crede că acest troian poate fi utilizat şi pentru distribuirea altor malware-uri,

precum programele false anti-spyware, backdoors şi alte ameninţări similare. Se răspândeşte cu ajutorul unor mesaje de securitate false ce pretind că maşina dumneavoastră este infectată cu un posibil virus. Atunci când utilizatorul apasă pe un astfel de mesaj, troianul intră în sistem şi silenţios instalează un ransomware. În plus, va bloca sistemul şi va afişa un mesaj de avertizare imens pe ecranul victimei. De asemenea, puteţi descărca această ameninţare în calculator ca şi ataşament de email sau reclamă de tip pop-up care se oferă să vă actualizeze Java sau Flash Player.

Trojan.ZeroAccess este un alt troian periculos, cunoscut ca şi max++. Notaţi faptul că există foarte multe versiuni ale acestui troian şi că toate au acelaşi ţel – să fure informaţiile personale ale oamenilor. Cu acest scop în minte, aceştia înregistrează fiecare bătaie de tastă a victimei şi pot face continuu capturi de ecran. Acest troian, de obicei, se furişează în sistem de pe diverse resurse de pe internet precum pagini web nesigure sau reţele peer-to-peer, şi începe să acţioneze fără a pierde timpul.

12Trojan.Win32.Krepper.ab este un parazit extrem de periculos şi destructiv, care poate cauza probleme serioase la adresa stabilităţii PC-ului dumneavoastră. De obicei, intră în sistem de pe resurse nesigure de pe internet, reţele de împărtăşire fişiere sau chat-uri online. Lucrează silenţios în fundal aşteptând o dată specifică pentru a-şi rula sarcina utilă. Pe data specifică, virusul Krepper poate încerca să afecteze regiştrii de Windows, să şteargă diverse dosare de sistem critice şi să iniţieze alte acţiuni destructive. Acest parazit detectează, termină şi dezactivează complet software-ul antivirus instalat pe calculatorul compromis. Mai mult, troianul se poate conecta la diverse servere maliţioase şi să descarce alţi paraziţi dăunători de pe acestea.

Eliminarea calului troian şi a altor ameninţări cibernetice

Troianii lucrează în aceeaşi manieră ca şi alţi viruşi de calculatoare şi prin urmare, ar trebui eliminaţi din calculator cu ajutorul unui software de securitate de încredere. Nu ar trebui să încercaţi să eliminaţi un troian manual deoarece poate duce la alte probleme serioase şi la daune sistemului. Pentru a obţine abilitatea de a scana în mod adecvat sistemul şi pentru a găsi toate componentele chestionabile din acesta, ar trebui să instalaţi oricare dintre aceste programe: Reimage, Malwarebytes. Acestea deja au fost aprobate pentru abilitatea lor de a detecta diverşi troiani şi componentele acestora.

Atenţie la faptul că uneori chiar şi un anti spyware avansat poate da greş în eliminarea unui anumit troian. Oricare dintre aceste ameninţări sunt în mod constant actualizate şi uneori aceste actualizări sunt adăugate înainte să fie observate de către dezvoltatorii de software anti-spyware. Dacă vreuna dintre uneltele recomandate nu a reuşit să vă fixeze calculatorul, puteţi oricând să contactaţi echipa noastră şi să le cereţi sfatul.