RISCURI DE NAVIGARE ÎN MEDIUL ONLINE

Doina CALMÎC

Universitatea Tehnică a Moldovei

Abstract: *Tendința mondială de utilizare a Internet-ului atestă, astăzi, o creștere continuă, imposibil de oprit. Serviciile Internet sunt supra solicitate de utilizatori, prin completitudinea pe care o oferă, dar și prin salvarea timpului pierdut. Însă, acest aspect are, cu siguranță și o tentă negativă, deoarece Internetul este cunoscut pentru vulnerabilitatea sa, ce până în acest moment nu a reușit nicicum să fie corectată. Serviciile Internet sunt vulnerabile la o serie de programe malițioase, cum ar fi: virușii, viermii, bombele logice, Calul Troian, adware, spam, spyware, phishing, etc. În acest context, se poate de afirmat că riscul de navigare online atât pentru utilizatori, dar, mai ales pentru organizații, este unul foarte ridicat. Astfel, instruirea utilizatorilor, este un factor extrem de important pentru a reduce impactul atacurilor cibernetice.*

Cuvinte cheie: *spyware, adware, impact, bot, ransomware, virus, vierme, rootkit.*

Analiza programelor malițioase

Programele malițioase sunt utilizate cu diferite scopuri, dar cele mai comune din ele sunt: compromiterea unui sistem informațional, autentificarea neautorizată, modificarea datelor, publicitate necontrolată sau furtul de date sensibile.

În continuare, vor fi analizate, cele mai des întâlnite programe malițioase, și anume:

1. Spyware este proiectat pentru a urmări și spiona utilizatorul, include adesea trackere de activitate, colectarea de taste și captura de date. Într-o încercare de a depăși măsurile de securitate, aplicațiile spyware modifică adesea setările de securitate. Spyware se îmbină deseori cu software legitim sau cu cai troieni.

2. Adware este conceput pentru a difuza anunțuri în mod automat, cel mai des este instalat cu unele versiuni de software. Unele programe adware sunt concepute doar pentru a difuza anunțuri, dar uneori programele adware vin în tandem cu programe spyware.

3. Bot este un program malware conceput pentru a efectua automat acțiuni, de obicei online. În timp ce majoritatea roboților sunt inofensivi, o utilizare tot mai mare a roboților rău intenționați sunt botnet-urile. Mai multe calculatoare sunt infectate cu boturi care sunt programate să aștepte comenzile furnizate de atacator.

4. Ransomware este conceput pentru a deține un sistem informatic sau datele pe care le conține captiv până la efectuarea unei plăți. Ransomware funcționează de obicei prin criptarea datelor din computer cu o cheie necunoscută utilizatorului. Alte versiuni ale programului ransomware pot profita de anumite vulnerabilități ale sistemului prin blocarea sistemului. Ransomware este răspândit de un fișier descărcat sau de o vulnerabilitate software.

5. Scareware este un tip de malware conceput pentru a convinge utilizatorul să ia o acțiune specifică bazată pe frică. Scareware afișează ferestre pop-up care seamănă cu ferestrele de dialog din sistemul de operare. Aceste ferestre transmit mesaje false care declară că sistemul este în pericol sau are nevoie de executarea unui program specific pentru a reveni la funcționarea normală. În realitate, nu au fost evaluate sau detectate probleme și dacă utilizatorul este de acord și șterge programul menționat pentru a fi executat, sistemul său va fi infectat cu programe malware.

6. Rootkit este conceput pentru a modifica sistemul de operare și pentru a crea un backdoor. Atacatorii folosesc apoi backdoor-ul pentru a accesa computerul de la distanță. Majoritatea rootkiturilor profită de vulnerabilitățile software pentru a realiza escaladarea privilegiilor și a modifica fișierele de sistem. Este, de asemenea, obișnuit ca rootkiturile să modifice instrumentele de criminalistică și instrumentele de monitorizare ale sistemului, ceea ce le face foarte greu de detectat. Adesea, un calculator infectat de un rootkit trebuie să fie curățat și reinstalat sistemul de operare.

7. Virusul este un cod executabil malware, care este atașat la alte fișiere executabile, adesea programe legitime. Majoritatea virușilor necesită activarea lor de către utilizatorilor finali și se pot activa la un anumit moment sau dată. Virușii pot fi inofensivi și pot afișa o imagine, sau pot fi distrugători, cum ar fi cei care modifică sau șterg datele. Virușii pot fi, de asemenea, programați să muteze pentru a evita detectarea. Majoritatea virușilor sunt acum răspândiți de unități USB, discuri optice, acțiuni din rețea sau e-mail.

8. Calul Troian este un program malware care efectuează operațiuni rău intenționate sub masca unei operații dorite. Acest cod rău intenționat exploatează privilegiile utilizatorului care îl execută. Adesea, troienii

se găsesc în fişiere imagine, fişiere audio sau jocuri. Un cal troian diferă de un virus deoarece se ataşează la fişiere non-executabile.

9. Viermii sunt cod rău intenţionat care se repetă prin exploatarea independentă a vulnerabilităţilor din reţele. Viermii încetinesc, de obicei, reţelele. În timp ce un virus necesită un program gazdă pentru a rula, viermii pot rula singuri. În afară de infecţia iniţială, aceştia nu mai necesită participarea utilizatorilor. După ce o gazdă este infectată, viermele se poate răspândi foarte repede în reţea. Viermii sunt responsabili pentru unele dintre cele mai devastatoare atacuri pe Internet.

10. Man-In-The-Middle (MitM) permit atacatorului să preia controlul asupra unui dispozitiv fără cunoştinţa utilizatorului. Cu acel nivel de acces, atacatorul poate intercepta şi captura informaţii ale utilizatorului înainte de a le transmite la destinaţia dorită. Atacurile MitM sunt utilizate pe scară largă pentru a fura informaţii financiare. Există multe programe malware şi tehnici care să ofere atacatorilor posibilitatea de a folosi funcţiile MitM.

11. Man-In-The-Mobile (MitMo) este o altă variantă de om-în-mijloc, MitMo este un tip de atac folosit pentru a prelua controlul asupra unui dispozitiv mobil. Când este infectat, dispozitivul mobil poate fi instruit să exfiltreze informaţiile sensibile ale utilizatorilor şi să le trimită atacatorilor. ZeuS, un exemplu de exploatare cu capabilităţi MitMo, permite atacatorilor să transmită mesaje SMS de verificare în doi paşi către utilizatori.

Reducerea impactului

În pofida faptului, că marea majoritate a companiilor mari cunosc deja totalitatea problemelor comune de navigare în Internet, şi depun eforturi considerabile pentru a le diminua impactul şi pentru a le preveni; nici un set de practici de securitate nu este 100% suficient pentru a proteja mediul online. Probabilitatea unui atac este direct proporţională cu importanţa resurselor ce trebuiesc protejate, deoarece este important să se înţeleagă faptul că impactul unui atac pe lângă aspectul tehnic pe care îl poartă ca: furtul de date, deteriorarea proprietăţii intelectuale, sau acces interzis către datele autorizate; mai are şi un aspect moral ce duce la pierderea reputaţiei companiei. Toate măsurile de răspuns la un atac, au un caracter foarte dinamic, astfel, conform părerii experţilor în securitate informaţională, trebuiesc luate câteva măsuri, în cazul în care atacul deja a avut loc, şi anume:

1. Comunicarea, atât cu angajaţii companiei, cât şi cu clienţii; pentru a crea transparenţă, care în asemenea cazuri este crucială.
2. Analiza modului în care a fost posibil atacul şi eliminarea punctelor vulnerabile, ce au fost exploatate de atacatori.
3. Educarea angajaţilor, partenerilor şi clienţilor cu privire la modul de prevenire a atacurilor similare.
4. Furnizarea de detalii cum ar fi: de ce a avut loc acest incident şi ce anume a fost compromis, atât timp cât, de cele mai dese ori, ţinta atacurilor cibernetice o reprezintă datele personale.
5. Asigurarea că toate sistemele funcţionează corect şi nimic altceva nu a mai fost compromis. De cele mai dese ori, atacatorii vor încerca să lase în sistem backdoor-uri, pentru a putea să acceseze sistemul din nou. În acest caz, cu siguranţă că este necesar de a verifica, pentru ca acest lucru să nu fie posibil.

Bibliografie

1. John Aycock, *Spyware and Adware (Advances in Information Security)*, 2011.
2. Oleg Zaytsev, *Rootkits, Spyware/Adware, Keyloggers and Backdoors: Detection and Neutralization*, 2006.
3. *James Kalbach, Designing Web Navigation: Optimizing the User Experience, 2007.*