

Raportul CA de securitatea internetului anticipeaza principalele amenintari online pentru 2008

CA, reprezentat in Romania de SolvIT Networks, a dat publicitatii cel mai nou Internet Security Outlook Report, care previne ca jocurile online, retelele sociale, evenimentele importante ca alegerile prezidentiale din S.U.A. si Jocurile Olimpice de la Beijing sunt principalele potentiale tinte ale atacurilor online in 2008. Studiul bazat pe datele stranse de cercetatorii CA Global Security Advisor, prezinta predictiile pentru 2008 in ceea ce priveste securitatea pe internet, dar si rapoartele trendurilor din 2007.

"Cyber-infractorii merg acolo unde exista oportunitatea si profita de toate punctele slabe existente," a afirmat Brian Grayek, vicepresedintele de Product Management al unitatii CA de Internet Security Business. "Cata vreme protectia securitatii devine mai eficienta in detectarea malware-ului, infractorii online utilizeaza metode tot mai inteligente si mai clandestine de a ne ataca calculatoarele."

Predictiile CA pentru online security in 2008:

1. Bots-ii vor domina anul 2008: Numarul calculatoarelor infectate de botnets va creste brusc in 2008. Datorita incercarilor de a deveni mai greu de detectat, bot-hearderii isi schimba tactica si descentralizeaza arhitecturile via peer-to-peer. Ei utilizeaza din ce in ce mai mult mesageria instant ca principal mod de "imprastiere" a botnetilor.
2. Un malware mai inteligent: Exista noi niveluri de sofisticare in malware. Malware-ul va tinti computerele virtualizate, si cresterea utilizarii tehnicilor de confuzionare sa ascunzi in planul vederii, incluzand steganografia si encriptarile, vor ajuta infractorii sa-si atinga obiectivele
3. Gamerii - bombardati: Gamerii sunt deja un trofeu apreciat si sustragerea acreditarii conturilor lor continua sa fie un obiectiv primar pentru infractorii online. Pe plan istoric gamerii sunt mai interesati de optimizarea propriilor pc-uri pentru o mai ridicata performanta decat pentru o securitate mai buna. In 2008, asseturile virtuale vor egala banii adevarati din lume pentru infractorii online.
4. Social networking sites in the crosshairs: Social networking sites will become increasingly popular and, as a result, more vulnerable. The large number of aggregated potential victims and relatively small concern for computer security make these sites a windfall for cyber thieves.
5. Siteurile de social-networking: Siteurile de social networking vor deveni din ce in ce mai populare si din aceasta cauza, mai vulnerabile. Numarul mare de victime potentiale si o grija relativ mica pentru securitatea calculatoarelor fac aceste siteuri un chilipir pentru cyber-infractori.
6. Date cheie pentru oportunitati: Alegerile prezidentiale din S.U.A. si Jocurile Olimpice de la Beijing ofera oportunitati importante pentru atacuri distructive si coruperea sau furtul informatiilor.
7. Serviciile si siteurile Web 2.0 vor deveni tinte ale atacurilor: Cat timp este relativ simplu sa implementezi serviciile Web 2.0, este o adevarata provocare sa le configurezi astfel incat sa fie sigure in totalitate. Prin urmare multe siteuri de internet care utilizeaza aceste servicii sunt tinte usoare cu un indicator extern ca un site este compromise.
8. Windows Vista la risc: Deoarece firmele si consumatorii individuali achizitioneaza computere noi, piata pentru Vista va creste. Desi este proiectat sa fie cel mai sigur sistem de operare Microsoft, in 2007 au fost raportate 20 de vulnerabilitati, conform Institutului National al Standardelor si Tehnologiei si S.U.A. Cu cat este mai utilizat cu atat va fi mai supus atacurilor.
9. Dispozitivele mobile continua sa fie sigure: Dispozitivele mobile sunt inca sigure, in ciuda zvonurilor despre malwareul mobil. Smartphone-urile si alte dispozitive mobile nu vor fi o adevarata oportunitate pentru infractori in 2008. Proof-of-concept malware pentru dispozitivele mobile nu a fost inca traduse in atacuri semnificative. Singura vulnerabilitate raportata in 2007 a fost pentru Apple iPhone.

"Urmele digitale care sunt colectate si pastrate cand noi utilizam internetul sunt incredibil de valoroase pentru vanzatori si pentru infractorii online," a continuat Grayed. "Am vazut malwareul evoluand de la o industrie-artizanat la o afacere matura de frauda. Socant, dar acum opereaza cu practici si dezvoltari de business similare organizatiilor legitimate pe software. Atitudinea noastra de protejare a intimitatii pe internet si actiunile ulterioare pe care le luam- la munca sau la joaca - pot altera in mod dramatic securitatea online."

Cercetatorii CA au descoperit urmatoarele tendinte in 2007:

- Volumele malware au crescut de 16 ori din ianuarie pana in octombrie 2007.
- Pentru prima data, spionajul rauvoitor a depasit trojanii, cea mai intalnita forma de malware. In 2007, 56% din malwareul intalnit a fost spionaj rauvoitor, 32% a fost trojani, 9% worms, si 2% virusi.
- Adware-ul, trojanii si downloaders-ii au fost cele mai intalnite tipuri de spyware.
- Cei mai intalniti worms in acest an au fost viermii de retea sau de drive detasabil. Unii viermi mutileaza calculatoarele prin care trec. Altii lasa doar un malware aditional sau deschid computere compromise pentru ca acestea sa fie controlate din umbra de un atacator rauvoitor.
- Software-ul care confera o falsa securitate a fost o continua problema si este indicator al valului crescand de aplicatii false. Software-ul contrafacut de securitate reprezinta 6% sin volumul total de spyware in 2007. Software-ul contrafacut de securitate este de obicei distribuit prin reclame online si ofera softare anti-spyware gratuit.
- Metodele de atac converg si amesteca amenintarile cu componente multiple care sunt acum standard.
- Mai mult de 90% din email este spam si mai mult de 80% din spam contine linkuri catre siteuri "rautacioase" sau malware.
- Calitatea spamurilor a fost imbunatatita si nu mai este in mod evident ghicita. Este de asemenea incarcata cu atasamente-imagine, PDF-uri, documente, tabele sau filme - care au un malware sau un link catre un site malitios.
- Malwareul este o problema internationala. Cea mai mare parte a activitatii infractionale isi are originea in Estul-Europei si Asia si este tintita asupra natiunilor care au un numar mare de utilizatori de internet. Aproape 40% din spam a fost distribuit catre Statele Unite. Australia, Anglia, Franta si Germania au fost de asemenea tintite. Malwareul este o problema care a aparut si in America Latina, Coreea de Sud si China.

Raportul CA 2008 Internet Security Outlook este menit sa-i informeze pe consumatori si afacerile de cele mai noi si mai periculoase amenintari, prognozeaza trendurile si furnizeaza sfaturi practice si protectie. Analiza furnizata este bazata pe informatiile de incident de la echipa CA Global Security Advisor, prezentata clientilor si consumatorilor CA din ianuarie pana in octombrie 2007, ca informatie disponibila publicului. Pentru intregul raport CA 2008 Internet Security Outlook, vizitati www.ca.com/securityadvisor.

Echipa CA Global Security Advisor furnizeaza in permanenta expertize demne de incredere, oferind sfaturi legate de securitate lumii de mai mult de 16 ani. Furnizand o resursa completa de management al riscului, Echipa CA Security Advisor este sprijinita de cercetatorii din aceasta industrie de top si profesionisti calificati pentru support. CA Global Security Advisor este disponibil la www.ca.com/securityadvisor. El ofera alerte gratuite de securitate, feeduri RSS, PC scan si un blog obisnuit updatat de echipele de cercetatori din intreaga lume. Intregul portofoliu CA al produselor aflate in raport cu amenintarile, pentru acasa, afaceri mici si mijlocii, si intreprinderi mari sunt updatate si protejate de echipa CA Global Security Advisor.