Risc d'inseguretat a la xarxa d'Internet

2015

Manel Medina

Seguretat a la xarxa

Tot i que els atacs de denegació de servei continuen representant més d'un terç i la força bruta un quart de tots els atacs, l'any passat es van detectar atacs als sistemes de gestió de pàgines web, com Hearthbleed o Shellshock (Bash-shell d'Unix), la qual cosa va provocar la creació de xarxes d'ordinadors contaminats (*botnets*), que pel fet de ser servidors tenien molta més capacitat de generar tràfic maligne que les xarxes d'ordinadors domèstics.

En canvi, els atacs a SSL (protocol https per accedir amb seguretat a pàgines web) han disminuït perquè finalment s'ha millorat el seu codi de programa.

Entre els països des dels quals es controlen les xarxes *botnets* destaca els EUA, amb un percentatge del 21%, poc si es compara amb els atacs de *spam* o *phishing*, però especialment Ucraïna, Algèria, Suècia, Corea del Sud i Egipte.

L'aparició de productes antivirus per a dispositius mòbils, de pagament i gratuïts, així com algunes mesures adoptades per defecte pels sistemes operatius, que obliguen als usuaris a descarregar aplicacions exclusivament des de magatzems de distribució controlats per grans organitzacions, com Google, Apple, etc., que verifiquen la seguretat de les aplicacions que distribueixen des del seu magatzem, han fet que la proliferació de programes contaminats s'hagi estabilitzat.

No obstant això, les estadístiques de programes per a dispositius mòbils contaminats encara és molt alt i requereix continuar amb l'aplicació de mesures de seguretat, sobretot antivirus, anti-*malware* i configuració de *firewalls* (tallafocs), i especialment si tenim en compte que entre els dispositius mòbils hem d'incloure els ordinadors tauleta.

Ordinadors contaminats

Els atacs amb Flash a través de visites a pàgines web estan disminuint, ja que moltes pàgines estan migrant a la nova versió d'HTML5, que no requereix l'execució de Flash i, per tant, evita els problemes derivats d'una possible contaminació de fitxers d'aquest format.

S'han extès molt els atacs tipus Ransomware, que consisteix en el xifrat (o segrest) del disc per fer xantatge al seu propietari. També s'han detectat casos de contaminació de dispositius en el procés de fabricació directament, és a dir, que ja es comercialitzen contaminats. Per exemple, uns controladors (*firmware*) de disc dur d'ordinador programats per a que re.injectin un virus a algun programa emmagatzemat al disc dur després que l'anti-virus l'hagi eliminat.

Cada trimestre es detecten prop de 50 milions de mostres de nou *malware*, gairebé un 50% més que fa un any, i el nombre total de mostres de programes malignes també va créixer pràcticament un 50% en un any. En canvi, el nombre d'arxius binaris malignes signats ha baixat, la qual cosa significa que cada cop es pren més seriosament la utilització de la signatura electrònica per protegir fitxers de programes.

L'any passat es va detectar la tendència als atacs persistents (APT) dirigits a qualsevol tipus d'organització per part d'organitzacions criminals, en benefici propi directe o indirecte a través de llogar la seva infraestructura criminal. Aquest any s'ha constatat que aquests atacs també els realitzen organitzacions governamentals d'intel·ligència o militars, tant de països occidentals com de l'Orient Mitjà o Llunyà. Aquests programes espia es detecten al cap d'una mitjana de més de dos anys d'haver-se instal·lat, cosa que fa pensar que molts

ordinadors que gestionen la producció o servei d'infraestructures crítiques poden estar ja contaminats des de fa molts mesos.

Mesures de seguretat aplicades a les infraestructures crítiques

L'aprovació de la nova Directiva europea de ciberseguretat (NIS) ha provocat la transposició anticipada d'alguns dels seus conceptes a legislacions nacionals com el Codi Penal espanyol.

Aquesta legislació ha tingut com a conseqüència la criminalització dels consells d'administració de les organitzacions que no apliquin mesures de seguretat adients als riscos als quals estan exposades, inclòs l'impacte que un atac a aquestes pot produir en la societat.

En l'àmbit estatal, el CERTSI, equip de coordinació de resposta a incidents de seguretat a indústries i empreses de servei, implantat per l'Institut Nacional de Ciberseguretat INCIBE (antic INTECO), per encàrrec del Centre Nacional per a la Protecció de les Infraestructures Crítiques (CNPIC), ha arribat al nivell de prestació de servei previst a mitjà termini.

Els atacs dirigits (APT) han estat emprats per molts professionals de la ciberseguretat per convèncer els seus directius a fer inversions en sistemes de ciberintel·ligència per tal de preveure aquests atacs.

Tothom se sent víctima potencial d'un atac dirigit i això fa que sigui més fàcil convèncer els usuaris de la necessitat de renunciar a executar "qualsevol programa" en els ordinadors corporatius i, fins i tot, en els privats.

Pràctiques de seguretat dels usuaris: Tecnologia social

Els atacs de *phishing* gairebé s'han doblat el darrer any. Més de la meitat provenen dels EUA (53%), i amb molt menor impacte (del 5% al 3%) d'Alemanya, el Regne Unit, França, els Països Baixos i el Canadà, per aquest ordre. En canvi, els atacs de *spam* han disminuït prop d'un 30%, amb la Xina, Rússia i el Japó com a països amb més *spam*, a més dels que hostatgen *phishing*.

La nova regulació europea de protecció de dades personals (GDPR) obligarà els proveïdors de serveis a explicar amb un llenguatge clar i senzill les seves polítiques de privacitat, la qual cosa evitarà que els usuaris cometin errors en acceptar-les sense conèixer les implicacions que pot tenir en la seva privacitat usar el servei.

El fet que els mitjans de comunicació generalistes publiquin notícies de ciberatacs gairebé cada setmana fa que els ciutadans tinguin molt presents els riscos que afronten en usar serveis i fer compres a Internet.

Entitats com l'Institut Nacional de Ciberseguretat (INCIBE) o l'Anti-Phishing Working Group (APWG) promouen campanyes de conscienciació dels usuaris en els mitjans de comunicació (ràdio, televisió, diaris...) en què expliquen els errors més comuns i les bones pràctiques per evitar-los.

Seguretat en els telèfons mòbils

Adobe està deixant de suportar el seu Flash Player en els dispositius mòbils ja que els navegadors ja porten incorporades eines per visualitzar vídeos. Això eliminarà atacs emprant aquests tipus de fitxers també en els dispositius mòbils, però encara hi ha molts servidors de televisió o jocs en línia que utilitzen aquest format de fitxers.

El primer trimestre del 2015 es va superar l'1,1 milions de nous *malwares* per a mòbils, la qual cosa representa un 40% d'increment sobre el trimestre anterior. I el total de programes maliciosos ja supera els 8 milions, un 80% més que feia un any.

Els desenvolupadors d'aplicacions malicioses han identificat els mètodes de validació i verificació emprats pels portals que les distribueixen. D'aquesta manera amaguen el seu comportament maligne durant els primers dies després que siguin instal·lades, que és quan són auditades, o contaminen en actualitzacions posteriors, un cop descarregades al dispositiu de l'usuari.

Seguretat dels servidors: Al núvol

Les empreses s'estan plantejant seriosament la utilització de serveis en el núvol, públics o privats, i també els governs estan emprant aquesta tecnologia per oferir serveis de govern electrònic als seus ciutadans. Els motius són diversos: d'una banda, per disposar de serveis de seguretat més professionalitzats, i, de l'altra, per estalviar inversions. Però també hi ha grans organitzacions que disposen de recursos per oferir aquests serveis per mètodes tradicionals i estan adoptant tecnologia de núvol per evitar l'ús incontrolat de serveis d'emmagatzematge gratuït al núvol.

La nova Directiva europea de ciberseguretat obligarà els proveïdors de servei al núvol a aplicar mesures de seguretat adients als riscos identificats pels seus clients corporatius. Els requeriments d'aquestes mesures de seguretat seran més rigorosos si s'ofereixen serveis de núvol a clients que per la seva banda són proveïdors de serveis crítics a la societat, ja que aquests estan obligats a aplicar mesures de seguretat adients a l'anàlisi de risc que hagin fet dels seus serveis, i si les subcontracten a tercers, són aquests els que les han de complir.

Fonts:

http://www.scmagazineuk.com/eurobarometer-cyber-security-survey-reveals-dangerous-overconfidence/article/400740/

http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm

http://datonomy.eu/2015/04/01/the-threat-landscape-and-other-cyber-news-from-q1-2015/