



IBM X-Force Report rivela uno stato di insicurezza del web senza precedenti

Il rapporto evidenzia un aumento di oltre il 500 per cento dei link web maligni e una sempre maggiore capacità di sfruttamento delle vulnerabilità

Milano, 3 settembre 2009 - IBM ha pubblicato i risultati del proprio X-Force 2009 Mid-Year Trend and Risk Report. Le conclusioni del rapporto evidenziano uno stato di insicurezza del web senza precedenti, con una convergenza di minacce a client, server e contenuti che delineano un panorama di rischio difficilmente sostenibile.

Secondo il rapporto, vi è stato un aumento del 508 per cento nel numero di nuovi link web maligni scoperti nel primo semestre del 2009. Questo problema non si limita più a domini maligni o a siti web non fidati: l’X-Force Report osserva infatti un aumento della presenza di contenuti maligni su siti considerati sicuri, inclusi comuni motori di ricerca, blog, bacheche informatiche, siti web personali, riviste online e siti con le ultime notizie. La possibilità di ottenere accesso e manipolare i dati rappresenta tuttora la conseguenza principale dello sfruttamento di tali vulnerabilità.

Il rapporto X-Force rivela inoltre che gli exploit del web nascosti, soprattutto file PDF, hanno raggiunto un livello record, mettendo in evidenza una sempre maggiore raffinatezza degli hacker. Le vulnerabilità dei PDF svelate nel primo semestre del 2009 hanno superato quelle svelate rilevate in tutto il 2008: solo dal 1° al 2° trimestre, la quantità di contenuti sospetti, offuscati o nascosti, monitorati dal team IBM ISS Managed Security Services, è quasi raddoppiata.

“I trend evidenziati dal rapporto sembrano indicare che internet ha finito per assumere le caratteristiche del Selvaggio West, dove non è possibile fidarsi di nessuno”, afferma Kris Lamb, Director di IBM X-Force. “Oggi non esiste una navigazione sicura e non è più vero che sono solamente i siti a luci rosse i responsabili del malware. Abbiamo raggiunto un apice in cui ogni sito web dovrebbe essere considerato sospetto e ogni utente è a rischio. La convergenza di minacce dell’ecosistema web sta creando una tempesta perfetta di attività criminale”.

La sicurezza sul web non è più solo un problema di browser o di client e i criminali fanno leva sulle applicazioni web non sicure per colpire gli utenti di siti web legittimi. Il rapporto X-Force ha riscontrato un aumento significativo degli attacchi alle applicazioni web, finalizzati al furto e alla manipolazione dei dati e all’acquisizione del controllo dei computer infetti. Ad esempio, gli attacchi con iniezione di codice SQL, attacchi in cui i criminali iniettano codice maligno in siti web legittimi allo scopo di infettare i visitatori, sono cresciuti del 50 per cento dal 4° trimestre 2008 al 1° trimestre 2009 e sono quasi raddoppiati dal 1° al 2° trimestre.

“Due dei temi principali per il primo semestre del 2009 sono l’aumento di siti che ospitano malware e il raddoppio di attacchi web mascherati”, spiega Lamb. “Questi trend

sembrano rivelare una fondamentale debolezza della sicurezza nell'ecosistema web, in cui l'interoperabilità tra browser, plugin, contenuti e applicazioni server aumenta enormemente la complessità e il rischio. I criminali sfruttano il fatto che non esiste un ambiente di navigazione sicuro e fanno leva sulle applicazioni web non sicure per colpire gli utenti di siti web legittimi”.

Il rapporto 2009 Midyear X-Force rileva inoltre che:

- **Le vulnerabilità si sono stabilizzate.** Nel primo semestre del 2009 sono state scoperte 3.240 nuove vulnerabilità, una riduzione dell'otto percento rispetto al primo semestre 2008. Il tasso di vulnerabilità scoperte negli ultimi anni sembra essersi attestato su un livello elevato. Nel 2007, il numero di vulnerabilità è calato per la prima volta, ma nel 2008 vi è stato un nuovo livello record. Il numero di nuove vulnerabilità scoperte ogni anno sembra oscillare tra sei e settemila.
- **Le vulnerabilità dei PDF sono aumentate.** Le vulnerabilità dei PDF (Portable Document Format) svelate nel primo semestre del 2009 hanno già superato quelle scoperte in tutto il 2008.
- **I trojan rappresentano più della metà di tutto il nuovo malware.** Continuando il trend recente, nel primo semestre 2009, i trojan hanno costituito il 55 percento di tutto il nuovo malware, con un aumento del nove percento rispetto alla prima metà del 2008. I trojan che sottraggono le informazioni sono la categoria predominante.
- **Il phishing si è ridotto drasticamente.** Gli analisti ritengono che i trojan bancari stiano prendendo il posto degli attacchi di phishing mirati a obiettivi finanziari. Nel primo semestre 2009, il 66 percento del phishing aveva come obiettivo il settore finanziario, rispetto al 90 percento nel 2008. I pagamenti online costituiscono il 31 percento del totale di tali attacchi.
- **L'URL spam è ancora il numero uno ma lo spam basato su immagini sta tornando.** Dopo aver quasi raggiunto l'estinzione nel 2008, lo spam basato su immagini ha fatto il suo ritorno nella prima metà del 2009; costituisce, tuttavia, ancora meno del 10 percento di tutto lo spam.
- **Circa metà di tutte le vulnerabilità resta priva di patch.** Analogamente alla fine del 2008, quasi la metà (49 percento) di tutte le vulnerabilità rivelate nel primo semestre 2009 non aveva alcuna patch del fornitore al termine di tale periodo.

Il team di ricerca X-Force cataloga, analizza e conduce ricerche sulle divulgazioni delle vulnerabilità sin dal 1997. Con oltre 43.000 vulnerabilità della sicurezza catalogate, possiede il più grande database delle vulnerabilità del mondo. Questo database unico aiuta i ricercatori X-Force a comprendere le dinamiche che costituiscono la scoperta e la divulgazione delle vulnerabilità.

IBM è uno dei provider leader mondiali di soluzioni di gestione dei rischi e della sicurezza. I clienti di tutto il mondo lavorano con IBM per ridurre le complessità della sicurezza e gestire strategicamente il rischio. L'esperienza e la gamma di soluzioni di gestione del rischio e della sicurezza IBM – dalla ricerca dedicata al software, hardware, servizi e valore dei Business Partner globali - sono insuperate, aiutando i clienti a

proteggere le attività di business e a implementare programmi di gestione del rischio integrati a livello aziendale.

Per ulteriori trend e previsioni di IBM in materia di sicurezza, incluse le rappresentazioni grafiche delle relative statistiche, è possibile consultare il rapporto integrale sul sito: <http://www-935.ibm.com/services/us/iss/xforce/trendreports/>

Per ulteriori informazioni visitate i siti www.ibm.com/security e www.ibm.com/services/it/security

IBM Italia:

Claudia Ruffini

Media Relation, IBM Italia

+39 02 59625792 +39 335 6325093

cla@it.ibm.com

Pleon per IBM:

Michela Mantegazza, Eros Bianchi

Michela.Mantegazza@pleon.com, Eros.Bianchi@pleon.it

tel. 02 0066290