



PUBBLICATO L'ANNUAL SECURITY REPORT DI CISCO

Cisco ha rilasciato l'Annual Security Report per il 2009, che analizza l'impatto dei social media, e in particolare delle applicazioni di social networking, sulla sicurezza della rete evidenziando il ruolo fondamentale che le persone, e non la tecnologia, hanno nel creare opportunità per i criminali informatici. L'Annual Security Report include anche i vincitori del Cisco® Cybercrime Showcase 2009 e discute i trend relativi a cloud computing, spam e crimini informatici che i professionisti dell'IT devono continuamente affrontare.

I social media hanno avuto una crescita esplosiva nel 2009. Solo Facebook ha triplicato il numero di utenti attivi, arrivando a 350 milioni nel corso dell'anno. Si prevede che l'adozione dei social media continuerà a crescere nel 2010, soprattutto perché sempre più aziende considerano il valore dei social network come un requisito di business fondamentale. I social network sono anche diventati un terreno fertile per i criminali informatici, dal momento che i membri di questi siti ripongono una fiducia sconfinata negli altri membri delle loro comunità e, spesso, si dimenticano di prendere le dovute precauzioni per prevenire la diffusione di malware e di virus. L'Annual Security Report fornisce inoltre ulteriori informazioni sulla combinazione, potenzialmente devastante, tra piccole vulnerabilità, comportamenti incauti degli utenti e software di sicurezza non aggiornati, che possono incrementare in modo significativo i rischi per la sicurezza della rete.

La vetrina dei crimini informatici del 2009

Nella vetrina dei crimini informatici del 2009 trovano spazio alcuni professionisti della sicurezza in prima linea nella lotta contro i crimini informatici, oltre ad alcuni attacchi che sono stati particolarmente problematici per gli utenti Internet nel 2009:

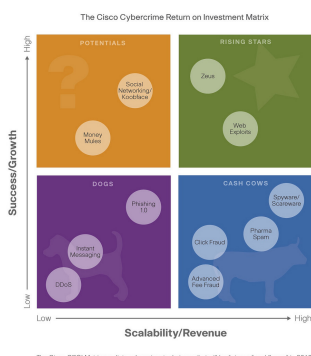
- **Operazione criminale più audace: Zeus.** Un Trojan che diffonde malware attraverso phishing mirato e download drive-by, Zeus va oltre login e password per impadronirsi dei dati bancari. Alcuni toolkit permettono la creazione di varianti di Zeus che sono di difficile individuazione per i programmi antivirus. Nel 2009 la botnet Zeus ha infettato circa 4 milioni di computer nel mondo;
- **Cybercrime "Sign of Hope": Il gruppo di lavoro Conficker.** Questo gruppo, che è composto da membri che si occupano di sicurezza, ha il merito di aver mutato in modo significativo l'impatto del worm Conficker, accreditato come causa di distruzione a partire dal 1 aprile 2009;
- **Innovazione criminale più famosa: Koobface.** Questo worm si è autorigenerato, apparendo prima su Facebook nel 2008 e in seguito su Twitter nel 2009. Koobface invita gli utenti a cliccare su un link a un video YouTube, che lancia il worm. Oltre 3 milioni di computer sono stati infettati da varianti di questo malware.

Growing Spam Problem in Emerging Economies

Country	2009 Volume	2008 Volume	Volume Change
Brazil	7.7	2.7	192.6%
United States	6.6	8.3	-20.3%
India	3.6	1.6	130.4%
South Korea	3.1	1.7	81.2%
Turkey	2.6	3.8	-31.3%
Vietnam	2.5	0.5	387.7%
China	2.4	3.2	-24.3%
Poland	2.4	1.6	43.4%
Russia	2.3	3.7	-38.2%
Argentina	1.5	1.3	16.0%

Volume in trillions per year Source: Cisco Security Intelligence Operations

Several of the world's economic leaders all experienced a decline in spam volume between 2008 and 2009; however, most of the world's developing economies show rising spam levels.



I principali risultati del report

Spam: i social media sono il terreno su cui i criminali informatici ricercano nuove vittime. Lo spam è comunque ancora il mezzo più usato per ingannare le persone, inducendole a scaricare malware acquistando, ad esempio, falsi prodotti farmaceutici. L'Annual Security Report prevede che, nel 2010, il volume degli spam aumenterà con una percentuale che va dal 30 al 40 per cento nel mondo rispetto al 2009. I dati SensorBase di Cisco dimostrano che, mentre gli Stati Uniti e i paesi dell'Unione Europea iniziano a chiudere gli zombie nei loro paesi, il rollout della banda larga nei paesi emergenti (come ad esempio Cina e Vietnam) ne ha fatto una fonte maggiore di spam.

Cloud Computing: 10 anni orsono era impensabile per un'azienda tenere dati sensibili all'esterno dei firewall. Oggi, con l'avvento del cloud computing e delle applicazioni hosted, questa pratica diventa sempre più diffusa. Molti utenti si fidano così tanto del cloud computing che fanno pochissimi controlli sulle entità che ospitano i loro dati sensibili e sull'effettiva sicurezza dei dati. L'Annual Security Report consiglia alle aziende, che intendono esternalizzare i servizi, di richiedere ai fornitori ampie garanzie sulle misure di sicurezza in essere.

Matrice Cisco Cybercrime Return on Investment (CROI): L'edizione 2009 dell'Annual Security Report vede il debutto della matrice CROI, che si basa sulla nota matrice "Growth-Share" del Boston Consulting Group. La matrice di Cisco analizza quali tipologie di crimini informatici saranno tra "i vincenti" e quali tra "i perdenti" nel 2010. In base alle performance del 2009, la matrice prevede una massiccia diffusione di Trojan Zeus bancari e di altri exploit web di semplice implementazione. Scareware, spyware, click fraud, e spam a soggetto farmaceutico continueranno ad essere di grande attualità. Da tenere sotto controllo gli exploit volti a colpire le applicazioni di social networking, come il worm Koobface, che stanno iniziando ad apparire.

Indice Cisco Global ARMS Race: con l'obiettivo di tracciare il livello generale di compromissione delle attività aziendali ed individuali generato dall'attività dei criminali informatici, Cisco ha sviluppato l'indice ARMS, che sarà aggiornato periodicamente. Per il 2009, l'indice ha raggiunto il livello 7.2; ciò significa che tra il 5 e il 10 per cento dei personal computer è compromesso.

http://cisco.com/en/US/prod/vpndevc/annual_security_report.html