



1° aprile 2009: le raccomandazioni di Stonesoft contro i Pesci d'Aprile

Alcune regole per evitare di incorrere in scherzi poco piacevoli

Milano, 31 marzo 2009 - Il 1° di aprile è noto per essere il giorno in cui le minacce alla sicurezza subiscono un sensibile aumento e le tecniche già collaudate vengono riproposte. Uno dei temi più discussi in questi giorni riguarda il probabile aggiornamento del worm di rete Conficker, conosciuto come uno dei peggiori virus della storia di Internet, la cui evoluzione per questa occasione resta ancora un'incognita.

Ben noti sono però gli attacchi degli anni passati: basti pensare al worm ANI che, il 1° aprile 2007, riuscì a diffondersi su scala mondiale grazie a un exploit scoperto all'interno di Windows. E ancora al worm Storm che, l'anno scorso, si diffuse attraverso messaggi di posta elettronica mascherati da Pesce di Aprile. Per quest'anno nessuno può fare previsioni. Motivo per cui Stonesoft Corporation, provider di soluzioni per la sicurezza di rete, invita tutti gli utenti a prestare massima cautela nell'apertura dei messaggi contenenti Pesci di Aprile, ricordando che lo strumento di difesa più efficace resta sempre il buon senso.

"La ragione che determina un aumento significativo delle minacce in concomitanza con il primo di aprile è abbastanza comprensibile", ha spiegato Emilio Turani, Country Manager di Stonesoft Italia, Grecia, Svizzera Italiana e Turchia. "Accade la stessa cosa anche in occasione di altre festività, come per esempio San Valentino. Nonostante le persone si vedano recapitare messaggi da mittenti sconosciuti, la tendenza è quella di aprirli comunque pensando a una semplice e divertente barzelletta da Pesce di Aprile".

Data l'impossibilità di prevedere le minacce, la prevenzione risulta di fondamentale importanza.

"La cosa più importante è ricordare le regole di base. Assicurarsi che tutti i programmi siano aggiornati, soprattutto quelli che riguardano la sicurezza. Inoltre, è importante affidarsi al buon senso. Evitare di navigare su siti sconosciuti, non aprire messaggi né allegati provenienti da indirizzi non riconoscibili e, in generale, assumere un comportamento improntato alla prudenza", ha ricordato Turani. "Per la maggior parte degli utenti Internet queste indicazioni possono sembrare abbastanza comuni, ma abbiamo comunque appurato nel corso degli anni che ricordare di tanto in tanto tali regole può solo giovare".

Stonesoft Corporation

Stonesoft Corporation (OMX: SFT1V) è un produttore innovativo di soluzioni integrate per la sicurezza di rete che permettono di proteggere i flussi informativi aziendali. I clienti Stonesoft

STONESOFT

comprendono realtà aziendali con necessità di business in evoluzione che richiedono una sicurezza di rete avanzata e connettività business always-on. In un unico sistema integrato e gestito centralmente, la soluzione per la connettività StoneGate integra firewall, VPN, IPS e SSL VPN, disponibilità end-to-end e una sofisticata tecnologia di bilanciamento. I principali vantaggi offerti da StoneGate sono il ROI elevato, il migliore rapporto prestazioni-prezzo e il più basso Total Cost of Ownership (TCO). La soluzione virtuale StoneGate protegge le reti e assicura la business continuity di ambienti sia fisici che virtuali.

StoneGate Management Center implementa un meccanismo di gestione unificata per StoneGate Firewall con VPN, IPS e SSL VPN. StoneGate Firewall e IPS operano insieme al fine di fornire una difesa intelligente all'intera rete aziendale, mentre StoneGate SSL VPN offre una sicurezza superiore anche da remoto.

Fondata nel 1990, Stonesoft ha due sedi centrali internazionali a Helsinki e ad Atlanta. Per maggiori informazioni è possibile visitare il sito www.stonesoft.com.

Per ulteriori informazioni alla stampa si prega di contattare:

Pleon - Daniela Sarti, Alice Fracassi

Tel. (+39).02.205620 – E-mail. daniela.sarti@pleon.com, alice.fracassi@pleon.com