

Twitter, FACEBOOK sfruttata da pirati

*Le tecniche di Social Engineering raggiungono nuovi livelli di sofisticazione
Conficker mantiene l'allerta sulla sicurezza*

Arluno, Milano – 10 giugno 2009

Cyberoam, l'innovatore di soluzioni Unified Threat Management (UTM) basate sull'identità, ha pubblicato il **report relativo alle minacce email del 1 ° trimestre 2009**, in collaborazione con il suo partner Commtouch. Mentre Conficker worm è alla ribalta, un punto da evidenziare è che gli aggressori hanno raggiunto nuovi livelli di sofisticazione nelle loro tecniche di Social Engineering, sfruttando la paura le emozioni e le lacune nella sicurezza per perpetrare nuovi attacchi.

Gli spammer hanno ingannato gli utenti di Facebook, Myspace, Twitter nel divulgare informazioni personali. Sfruttando il timore degli utenti di trovare immagini scandalose online, gli spammer hanno inviato wall post proclamando che tali immagini erano apparse su Facebook. Con questa tecnica, utilizzata anche su Facebook, sono stati inviati disperati messaggi da amici presumibilmente impegnati in una disputa finanziaria. Gli utenti che hanno cliccato sul link sono stati ingannati da quella che sembrava una pagina di login di Facebook, ma che in realtà era un sito impostore che ha permesso la raccolta di login e password di ignari utenti.

Gli spammer hanno inviato i messaggi Twitter direttamente agli utenti dei blog e foto divertenti ad essi collegate. Lacune nella sicurezza su Twitter come l'uso di TinyURL per sostituire gli URL lunghi con quelli brevi per rientrare nel limite di 140 caratteri di Twitter, hanno fatto sì che gli utenti non sapessero dove portasse il link prima di essere cliccato.

Il Vice Presidente, Product Management, di Cyberoam, Abhilash Sonwane, ha detto, "*Gli aggressori hanno confermato una volta di più che lavorano su entrambi i lati della equazione utente - piattaforma. Giocano sulle emozioni degli utenti mentre sfruttano le lacune della piattaforma utilizzata. Questi due elementi, usati in combinazione tra loro, sono uno strumento molto efficace per propagare il malware. Mentre Cyberoam offre protezione dalle minacce sempre in evoluzione, noi consigliamo anche di educare gli utenti a contenere in modo efficace le minacce*", ha aggiunto.

Minacce combinate create ad arte con siti mirror simili a quelli ufficiali cercano di carpire email da CNN e servizi fiscali degli Stati Uniti. Mentre Documenti Google sono stati utilizzati per compromettere ZDNet, gli spammer hanno utilizzato "in prestito" le immagini da siti legittimi, come CBS e Pizza Hut per mascherare i loro indirizzi email e bypassare i filtri spam.

Il debito dello spam è saltato dal 3% di tutti i messaggi di spam nel 4 ° trimestre 2008 al primo posto, con 28% di tutti i messaggi di spam nel primo trimestre 2009, riflettendo la situazione economica mondiale.

Cyberoam utilizza la tecnologia Commtouch RPD™ per analizzare grandi volumi di traffico Internet in tempo reale. A differenza dei tradizionali filtri, non si basa sul contenuto delle email, ma su pattern di messaggi per rilevare lo spam, in qualsiasi lingua e formato essi si presentino. Il suo linguaggio ed il contenuto di natura agnostica consente di fornire un'efficace capacità di blocco dello spam.

Cyberoam incorpora RPD™ nei suoi appliance UTM basati sull'identità che evidenziano "**chi sta facendo cosa**" nella rete e consentono la creazione di politiche basate sul nome utente e non solo gli indirizzi IP.

Chi è Cyberoam

Le appliance UTM Identity-based di Cyberoam offrono una protezione completa contro le minacce internet esistenti ed emergenti, compresi virus, worm, Trojan, spyware, phishing, pharming ed altro. Cyberoam garantisce una gamma completa di funzionalità per la sicurezza come stateful inspection firewall, VPN, gateway anti-virus, gateway anti-malware, gateway anti-spam, intrusion prevention system, content filtering in aggiunta a bandwidth management e multiple link management tutto integrato all'interno di una singola piattaforma. Cyberoam è dotata di certificazione CheckMark UTM Level 5 di West Coast Labs, ICSA Lab, una divisione indipendente di Verizon Business, e Virtual Private Network Consortium. Cyberoam ha ricevuto i riconoscimenti "2008 Emerging Vendor of the Year" di Frost & Sullivan, "2007 Global Excellence Awards for Integrated Security Appliance", "Security Solution for Education and Unified Security", "2007 Tomorrow's Technology Today Award for Unified Security", ha ottenuto un punteggio positivo da Gartner nel suo "Marketscope for SMB multi-function firewalls". Cyberoam ha propri uffici a Woburn, MA, USA ed in India. Per ulteriori informazioni visitate il sito www.cyberoam.com/it

Chi è Horus Informatica

Horus Informatica è distributore ufficiale Cyberoam per l'Italia.

Con sede in Arluno – Milano – Horus Informatica è distributore a valore aggiunto 100% channel oriented per il settore ICT e network security. Opera dal 1997 tramite un canale di Business Partner, Rivenditori, VAR e System Integrator presenti su tutto il territorio.

Per maggiori informazioni sull'azienda link at www.horus.it

Per qualunque informazione o approfondimento su prodotti e servizi:

Press Contact

Dip. Marketing e Comunicazione

Tel (+39) 02 - 33510135

Fax (+39) 02 - 33510838

marcom@horus.it

