

L'Evoluzione delle Minacce

Come stanno cambiando le minacce alla sicurezza.

Introduzione

Gli addetti ai lavori nel settore sicurezza dicono spesso che lo scenario sta cambiando, ma i tempi stanno veramente cambiando in un aspetto molto importante del repertorio delle minacce informatiche.

Sta diventando sempre più chiaro il fatto che quelli che negli anni passati erano a caccia dei titoli sui giornali, gli 'autori di virus' che semplicemente volevano fare notizia o raggiungere un primato tra i loro 'colleghi', non costituiscono più la forza trainante che sta dietro il *malware*. Oggi le minacce sono pure nei loro scopi quasi come lo era Wall Street negli anni Ottanta: è solo una questione di soldi. E, per questo buon motivo, il crimine organizzato sta utilizzando sempre di più Internet come strada per fare soldi sporchi in contanti prelevandoli dagli individui o dalle aziende in modo fraudolento. Quanto segue spiega, in modo succinto, il tipo di mezzi che queste persone stanno utilizzando e di conseguenza di che cosa è necessario essere consapevoli nello sforzo di proteggere il proprio business e prevenire gli attacchi.

Quali sono le minacce?

Il punto di partenza logico nello sforzo di capire l'ambiente delle minacce informatiche è quello di conoscere le minacce stesse; quali tipi di minacce ci circondano oggi, quali sono quelle che si stanno affermando con maggior successo e, soprattutto, quali sono quelle più dannose dal punto di vista del business.

Ci sono cinque tipi principali di minacce:

1. Virus
2. Spam
3. Phishing
4. Trojan
5. Applicazioni Legittime, dette anche PUP (*Potentially Unwanted Programmes*) e conosciute anche come "spyware".

Ognuna di queste minacce ha una serie di sottotipologie. Per esempio i "virus" includono nella loro categoria (fate un bel respiro): "macro", "script virus", "mass mailer", "worm" e "file". I "trojan" possono fungere da "backdoor" per l'accesso remoto, comportarsi da "downloader" e scaricare codice dannoso, distruggere i dati, rubare password o semplicemente causare azioni di disturbo. Inoltre, un altro modo di considerare i pericoli di queste minacce è quello di guardare al modo più comune con cui viene compromessa la sicurezza della rete.

In cima alla classifica c'è l'"autopropagazione" (attacchi che si diffondono da soli senza la necessità di intervento da parte dell'utente). Tale modalità conta per oltre il 25% di tutti i

danni (*Fonte – Foundstone 2005*). Al secondo e terzo posto ci sono le minacce “mass mailer” (che richiedono l’intervento dell’utente per potersi diffondere) e quelle “basate su browser”. Queste tre minacce, tutte insieme, rappresentano oltre il 60% dei danni totali registrati. La crescita nell’impiego dei “trojan” è di particolare interesse, anche perché supporta la tesi che il crimine organizzato è sempre più coinvolto nella produzione e diffusione di *malware* (software dannoso) a fini di lucro. Nel 1994 esistevano 74 “trojan” rilevati (che sono programmi che si fanno passare per programmi legittimi in modo da poter entrare in una rete e poi vengono utilizzati, per esempio, per inviare password riservate all’esterno). Nel 2000 la cifra è salita a circa 2000, per raggiungere nel 2005 un totale di oltre 13.000. Il motivo per cui tale fenomeno è interessante è che i Trojan, per loro stessa natura, vengono solitamente utilizzati in attacchi mirati a obiettivi specifici per ottenere informazioni ben precise. In passato gli ‘autori di virus’ e gli *hacker*, se vogliamo, erano semplicemente a caccia di notorietà: diffondevano “virus” o attaccavano siti web con l’obiettivo di diventare i più famosi possibile. Oggi l’obiettivo invece è *non* essere notati; l’ultima cosa che il crimine organizzato vuole, è finire sulla prima pagina dei quotidiani – se l’idea è quella di estorcere danaro a un’azienda rubando dati o password la parola d’ordine è cautela, e questo è il motivo per cui l’utilizzo crescente di “trojan” mirati è significativo.

La crescita dei “BOT” (Robot)

Un’altra tecnica per estorcere danaro a un’azienda che si è diffusa in particolare nel corso dell’ultimo anno, e avvalorata la tesi di un crescente coinvolgimento del *crimine organizzato* nel mondo dell’informatica, è l’utilizzo di eserciti di cosiddetti “BOT” (Robot) per ricattare le organizzazioni. Gli eserciti di “BOT” sono disponibili in affitto – un “BOT” è un Pc (altrimenti innocente) che è stato compromesso e può quindi essere controllato da qualcuno che non sia l’utente proprietario. I casinò online in Uk sono stati ricattati con la minaccia di intasare i loro server bombardandoli con milioni di “BOT” (che generano traffico di rete inutile) con l’effetto di bloccare il sito – unico mezzo di guadagno dei casinò stessi. Perciò, comprensibilmente, data la difficoltà di trovare i responsabili di tali attacchi, i casinò nella maggior parte dei casi hanno preferito cedere al ricatto piuttosto che rivolgersi alla polizia. A partire dal 2001, esistono a oggi, nel 2005, oltre 10.000 varietà note di “BOT”. Un altro punto estremamente importante che i responsabili della sicurezza di un’azienda devono comprendere è l’utilizzo crescente dei cosiddetti “packer”: “virus” che vengono compressi e codificati in archivi in modo da oltrepassare gli “antivirus” e, una volta compattati/decodificati, registrarsi in memoria e non sul disco del Pc. È fondamentale disporre di una soluzione “antivirus” che analizzi la memoria, ma non tutte lo fanno. Ecco perché: una volta installati, questi tool possono attivarsi (dipende per quale scopo sono stati progettati) e ottenere pezzi di codice, come i “key-logger”, e poi compromettere la rete aziendale. È sufficiente che rimangano sul sistema senza essere scoperti anche solo per poco tempo per eseguire quello per cui sono stati programmati. Una complicazione ulteriore è che i “packer” possono essere leggermente modificati per evitare di essere rilevati in modo estremamente facile, il che rende fondamentale disporre di un “antivirus” che non solo analizzi la memoria, ma riconosca anche le diverse famiglie di “packer” tramite le funzioni di rilevamento generico.

Il Grande Fratello ci guarda

Il 45% di tutte le segnalazioni da parte degli utenti finali all'organizzazione AVERT (*AntiVirus and Vulnerability Emergency Response Team*) di McAfee attualmente è rappresentato da *adware*. Piuttosto insidioso: non importa che cosa un *adware* possa fare, l'utente finale potrebbe aver accettato che un fornitore di *adware* veda esattamente dove sta navigando per esempio durante l'azione di barrare la casella "Accetto" alla fine di un accordo di licenza di 20 pagine, senza aver realmente letto l'intero documento in dettaglio. È sufficiente per affermare che una parte di quello che finisce sul Pc degli utenti ha buone intenzioni o al massimo non ha un intento dannoso, mentre un'altra parte non lo è affatto. Molte delle tecniche utilizzate per diffondere l'*adware* sono simili a quelle utilizzate per propagare il *malware*.

Il "phishing"

Praticamente tutti conoscono ormai i termini "phishing" e "pharming", visto l'ampio spazio che nell'ultimo anno e mezzo è stato dedicato sulla stampa a queste forme di *social engineering*. In tutta la storia delle minacce informatiche il punto più debole spesso è rappresentato da un essere umano piuttosto che da una tecnologia di sicurezza. Esistono numerosi esempi di attacchi andati a buon fine che hanno aggirato degli individui per portarli a fornire informazioni riservate per aprire la porta a malintenzionati e farli entrare in un database critico o altri esempi simili. Esistono ricerche in UK che dimostrano che la gente fornisce password o dettagli personali a estranei semplicemente perché gli vengono chiesti. Il "phishing" e il "pharming" sono forme di truffe che sfruttano la nostra natura fiduciosa. Il "phishing" è stato ben pubblicizzato e prevede l'invio di una e-mail a una o più persone che appare come se arrivasse da una banca, un ufficio postale o quant'altro. Tale comunicazione richiede all'utente di inserire, per esempio, la password del conto corrente bancario o i dettagli di log-on e rinvia poi l'e-mail a qualcuno che farà piazza pulita del conto bancario stesso!

Le banche e altre istituzioni interessate solitamente avvisano gli utenti che non riceveranno mai da parte loro richieste di fornire informazioni riservate come queste tramite e-mail, e ciò ha ridotto (ma non eliminato) l'efficacia dei tentativi di "phishing", ma dall'altra parte ha portato allo sviluppo di altri metodi più sofisticati per rubare soldi. I "trojan" hanno un ruolo anche qui; "Pws-Bancban", una volta eseguito su un Pc infetto, ricerca informazioni specifiche legate alle banche ricercando termini come Banco, HSBC, Banespa, Itau Bank, eccetera. Tali informazioni vengono poi catturate e trasferite via e-mail utilizzando un motore SMTP a un indirizzo e-mail @hotpop.com (l'indirizzo esatto viene ommesso appositamente). Il "pharming" è una forma più sofisticata di "phishing", che richiede un minor coinvolgimento da parte dell'utente. Vengono create repliche esatte della videata di login della banca dell'utente che poi quando clicca su un link reindirizzano l'utente su un sito falso. Tale tipologia è più difficile da individuare ma non è, per fortuna, così diffusa.

Siete vulnerabili?

La forma finale di attacco che si sta diffondendo sempre più dato il potenziale di guadagno è lo sfruttamento di vulnerabilità di applicazioni o reti. Le vulnerabilità stesse, naturalmente, non sono nuove, dal momento che esistono fin da quando sono nate la prima applicazione e la prima rete. Quello che va evidenziato è che quello che possiamo definire come il ciclo "time to exploit" o "vulnerability to worm" o meglio ancora "finestra di vulnerabilità" si sta sempre più riducendo. Negli anni passati ci volevano mesi perché un "exploit" specifico

venisse creato per una particolare vulnerabilità. Recentemente, tale periodo di tempo si è ridotto a pochi giorni, creando la prospettiva dei cosiddetti attacchi “zero day”, dove un “exploit” viene lanciato contro una vulnerabilità critica di sistema prima che una patch possa essere implementata. Il tempo medio perché un “exploit” si diffonda è di circa 10 giorni. Nel 1999 era di 280.

Ci sono tre fattori che possono stimolare gli autori di software dannosi nel momento in cui vengono a sapere di una vulnerabilità:

1. *La vulnerabilità è su una applicazione molto utilizzata?*
2. *Il codice sorgente dell'applicazione è pubblico?*
3. *Un “exploit” può essere eseguito da remoto?*

Se la risposta a tutte e tre le domande è un “sì” secco, allora la vulnerabilità rappresenta il sogno di ogni ‘autore di virus’: un modo per raccogliere una enorme quantità di informazioni per far soldi senza troppi sforzi. Come evidenziato prima, la protezione contro gli sfruttamenti delle vulnerabilità sono un incubo. Come decidere quali patch sono più critiche per la vostra azienda? Quali sono gli asset più critici? Dove trovo il tempo per implementare costantemente gli aggiornamenti “antivirus” in tutta l’azienda? Come faccio a trovare le risorse per prendere in considerazione anche solo una delle attività sopra elencate?

Conclusioni: le minacce future

La crescita nell’utilizzo di dispositivi mobili o, meglio, quanto importanti potranno diventare se lo standard 3G soddisferà le aspettative di diffusione degli operatori, diventerà un’area interessante da tenere sott’occhio nei prossimi anni. I dispositivi mobili forniranno agli autori di *malware* e alle gang di criminali informatici un altro obiettivo per perpetrare truffe finanziarie, e potrebbero anche diventare terreno fertile per i ‘vecchi autori di virus’, per i loro vari obiettivi. In primo luogo, dal momento che il *malware* (come descritto in questo documento) supporta moventi volti a guadagnare soldi, l’utilizzo di smart phone come finestra sul mondo dell’utente – molto più di quanto accada oggi con i telefoni attuali – significa che diventeranno un obiettivo sicuro per gli attacchi. Se i dispositivi “mobile” diverranno sufficientemente semplici da utilizzare tanto da sostituire parte di ciò che oggi facciamo utilizzando un desktop (Internet banking, ecc.), allora si trasformeranno in un obiettivo logico per coloro che vogliono appropriarsi di dati riservati. Si tratta di un problema sia per gli operatori (che sosterranno il peso maggiore in termini di protezione) sia per gli utenti finali, in termini di protezione dei telefoni stessi (poiché possono comunicare “via WiFi” e “Bluetooth” oltre che tramite il proprio “service provider”). Stiamo già assistendo a minacce *proof-of-concept*, il che significa che qualcuno sta esaminando il mondo “mobile” alla ricerca di possibili punti di debolezza. Al momento sono ostacolati (proprio come la crescita del settore stesso) dalla moltitudine di architetture e sistemi operativi. Infine, un’altra possibilità è che torni l’era dei ‘vecchi tradizionali autori di virus’ a caccia di notorietà; il mondo delle reti ‘mobile’, con i suoi diversi standard, è paragonabile in qualche modo ai tempi passati nel settore dei Pc/server; gli autori di *malware* sono fiduciosi di essere vicini a quella fama che arriverà con il primo grosso attacco in un nuovo ambiente. In entrambi i casi, quando la casa digitale “connessa” diventerà una realtà, il problema della sicurezza peggiorerà per tutti noi.

Ottavio Campioneschi