Dynamic Network Security

di Paolo Ballanti

Il 2012 sarà l'anno della Dynamic Network Security.

Siamo sempre più convinti della nostra visione, che da sempre è legata alla natura di Software House della nostra azienda e che ci ha permesso di trovarci in una posizione di assoluto privilegio rispetto alla maggioranza dei competitor oggi che la natura algoritmica –e non più lineare– della crescita e dell'evoluzione delle minacce alle reti informatiche è divenuta così evidente.

Crediamo che una buona tecnologia di supporto ai processi della Network Security debba per forza di cose garantire flessibilità, adattabilità, capacità di mutare ruolo e funzionalità a seconda del contesto di utilizzo e delle mutevoli necessità di security odierne di una rete informatica aziendale.

Crediamo anche che essere nella condizione di poter garantire un alto ritorno dell'investimento, argomento da sempre nelle nostre corde e ancora più evidente alla luce delle novità che potrete leggere in questa newsletter, rappresenti un valore primario soprattutto in tempi come questi nei quali aziende, istituzioni e in fin dei conti individui non hanno soldi a sufficienza per permettersi di investire in direzioni o tecnologie "sbagliate".

Viviamo in un mondo caratterizzato dalle sigle e dalle buzzword: per questo da qualche tempo a questa parte stiamo cercando di fare chiarezza su termini e tematiche, sforzandoci di distinguere tra slogan marketing e realtà dei fatti, tra metodologie e motivazioni di attacco, tra capacità tecnologiche reali e dichiarazioni unilaterali dei vendor che popolano il mercato della Security.

Abbiamo ad esempio avuto esperienze di test comparativi indipendenti, effettuati da aziende come:

- NSS Labs (**http://www.nsslabs.com/**)
- e Breakingpoint (**http://www.breakingpointsystems.com/**)

per conto di clienti prospect su più tecnologie di differenti vendor, e ciò che è invariabilmente emerso è che nella stragrande maggioranza dei casi i numeri relativi a performance, throughput e capacità di elaborazione in generale dichiarati dai vendor non corrispondono minimamente alla realtà dei fatti.

La nostra natura di azienda guidata dalla ricerca e sviluppo e dall'integrità finlandese per fortuna ci garantisce da brutte figure in questo senso, e anzi siamo sempre usciti vincitori da queste comparazioni. Nel test condotto da NSS Labs abbiamo addirittura avuto evidenze clamorose: un vendor emergente (e molto marketing-oriented, per essere onesti) che racconta pubblicamente che i numeri da esso dichiarati sono assolutamente reali a differenza di quelli dei suoi competitor ha raggiunto un bel 17% di performance effettive nella vita reale rispetto ai numeri dichiarati sui suoi datasheet di prodotto!!!

Ora: una leggera flessione rispetto ai numeri di laboratorio ci sta sempre, perché il traffico reale è fatto anche di pacchetti molto piccoli e più difficilmente gestibili, ma quello appena descritto è un risultato che un Next Generation Firewall di "nuova" concezione non si può permettere di avere. Per contro, nemmeno a farlo apposta, il nostro FW-1301 ha raggiunto l'83% rispetto ai risultati conseguiti nei nostri laboratori quando messo a gestire traffico di produzione nel medesimo test di NSS Labs. Sono numeri che hanno una tale evidenza che non mi sento di commentarli ulteriormente.

Inoltre, come detto stiamo cercando di parlare ai C-level spiegando loro che al di là degli slogan e delle sigle, ciò che davvero conta è la capacità di una tecnologia di Network Security di abilitare i servizi aziendali e di garantire una reale protezione per gli asset critici della loro azienda. La nostra ricerca sulle Advanced Evasion Technique (AET) è arrivata a un punto di maturazione tale che siamo in grado di dimostrare a qualunque cliente prospect che la tecnologia che attualmente difende la sua rete è INUTILE a fronte di attacchi condotti con tali metodologie.

Lo possiamo provare, nella realtà, a casa del cliente. Vi assicuro che non è una cosa da poco, né da un punto di vista tecnico, né da un punto di vista commerciale. Provate a dare un occhio a questo sito: **http://aet.stonesoft.com** e capirete ciò di cui sto parlando.

Stay tuned.

Quella minaccia non così avanzata

di Francesco Armando

Stuxnet (con i suoi simili) e Advanced Persistent Threat (APT) stanno da tempo monopolizzando i titoli ad effetto della stampa più o meno specializzata. L'insieme di attacchi 0-day, studiati e progettati professionalmente da gruppi più o meno numerosi ma certamente molto capaci, il livello sofisticato della minaccia portata fanno dubitare molti della possibilità di difendersi.

Questo stato d'animo non è giustificato dai fatti: attacchi mirati particolarmente sofisticati vengono portati nei confronti di pochi e ben selezionati bersagli. I signori di LulzSec e quelli etichettati come Anonymous hanno invece dimostrato quello che molti pentester hanno imparato nel tempo: la conoscenza del bersaglio rivela vulnerabilità sfruttabili facilmente.

Quando i titoli hanno gridato la violazione dei server della NATO in realtà era stato compromesso un negozio online, vulnerabile ad un attacco ben noto e piuttosto datato. Altre volte hanno sfruttato il fatto che molti utenti riutilizzano le medesime password su sistemi diversi.

Si tratta di rischi che possono essere mitigati facilmente. Il problema normalmente è nella scalabilità delle soluzioni disponibili.

Al fine di poter applicare politiche di sicurezza consistenti e centralizzate un'organizzazione deve avere l'infrastruttura, la cultura e la capacità di muoversi in questa direzione. Normalmente scegliere un partner come Stonesoft è il miglior modo per partire bene, e chi ben comincia...

Troppi sedicenti esperti nel campo della sicurezza vedono questo tema come l'evoluzione naturale del guardie e ladri cui giocavano a suo tempo. Vogliono dimostrare di essere più intelligenti dei cattivi, di saper schivare i colpi e conoscere le mosse migliori. Non pensano che in realtà si tratta di attività abbastanza noiose, fossero anche chiamate con il loro equivalente inglese di operations.

È una corretta gestione della sicurezza, possibilmente operata con strumenti allo stato dell'arte come quelli che noi usualmente forniamo, che permette di difendersi bene da tutte queste minacce non poi così avanzate. Forse che il file di excel con dentro uno 0-day mirato ad un prodotto Adobe fin troppo bersagliato con il quale è stata violata la difesa di RSA è una cosa così sofisticata ed avanzata?

Da molto tempo il nostro IPS permette di bloccare i file di office che contengono oggetti di questo tipo. D'altronde, il fatto che i documenti di office consentano di sfruttare un loro file system interno a questo scopo non significa che vogliamo portarci in casa qualsiasi cosa vi sia inclusa no?

Una rete pulita e gestita correttamente sarà di aiuto anche nel caso in cui si debba rispondere a minacce davvero avanzate e sofisticate! L'implementazione di tecniche di protezione semplici ed efficaci è possibile, anche in assenza di specchietti per le allodole che facciano ricorso all'ultima buzzword. Si tratta di applicare delle regole in modo consistente, magari evitando che le persone dell'IT siano le prime a violarle.

E' importante che la sicurezza sia gestita direttamente dal top management che si occupa anche dell'IT. Pensare di fare diversamente porta velocemente in una trappola che ha sperimentato anche un'azienda come Sony, che fino a qualche tempo non aveva neppure un CISO!

> Le AET sono il coltellino svizzero delle tecniche di evasione. Le AET utilizzano molteplici tecniche di evasione simultanee per scardinare le difese della rete.

Avere una rete e governarla senza integrare la gestione della sicurezza al suo interno vuol dire andare a cercarsi il problema.

Bisogna farlo prima: dopo non ci riuscirete.

Sony se ne è accorta dopo aver collezionato qualcosa come 170 milioni di dollari di perdite, aver assunto un CISO e ripetuto l'esperienza seppur in scala minore più volte.