

Sconfiggere i botnet del futuro

L'articolo riportato di seguito è un estratto da *Understanding and Blocking the New Botnets*, un white paper di ricerca di Scott Pinzon, CISSP e Corey Nachreiner, CISSP, del team WatchGuard® LiveSecurity®. Per un interessante sguardo ai botnet, su come si sono evoluti e come funzionano oggi, è possibile scaricare una copia gratuita del white paper www.watchguard.com/whitepapers.asp.

I botnet incarnano la minaccia combinata definitiva. Il codice dei botnet contiene quasi tutte le forme possibili di malware: dallo spyware ai downloader, ai rootkit, motori di spamming e altro ancora. Per difendersi ad armi pari, è necessario impiegare più livelli di protezione. La buona notizia è che le tecniche tradizionali sono ancora sorprendentemente efficaci nei confronti dei botnet. Sono suggerite di seguito una serie di contromisure che limitano significativamente la probabilità che infezioni bot possano operare dalla vostra rete.

1. Proteggersi immediatamente

I bot possono attingere a una vasta gamma di attacchi per infettare i sistemi. Tuttavia, i bot più famigerati e dannosi hanno sfruttato i punti vulnerabili *corretti con patch installate dal fornitore sei o diciotto mesi prima*. Nei casi più estremi, i bot hanno tentato di attaccare i punti vulnerabili corretti con patch quattro anni prima. Non sappiamo spiegare perché vi siano continue innovazioni nei sistemi di comunicazione e back-end mentre i bot utilizzano metodi di attacco conosciuti e vecchi. Quello che possiamo immaginare è che i botmaster individuano gli attacchi aspettando che produttori correggano una vulnerabilità con una patch, per quindi decodificarla e scoprirne il difetto.

Ci aspettiamo che l'esplorazione dei difetti più recenti siano i prossimi obiettivi dei botmaster. Ma per ora, è una buona notizia per l'amministratore di rete medio. Se si installa immediatamente una patch quando i produttori rilasciano correzioni per il software che si esegue in rete, è possibile agire più velocemente dei botmaster e resistere ai loro attacchi.

2. Bloccare JavaScript

Quando un computer viene colpito da un attacco basato sul Web che utilizza un bot, invariabilmente questo avviene tramite l'esecuzione di JavaScript. Impostando il browser in modo che avvertano prima di eseguire i JavaScript è possibile eliminare una gran parte dei vettori di infezioni bot. Sugeriamo vivamente agli utenti di affidarsi a Firefox come browser principale, utilizzando il [plug-in NoScript](#) ogni volta che uno script tenta l'esecuzione.

3. Sorvegliare le porte

Questa è una raccomandazione in due parti.

1) Sebbene i bot di ultima generazione possano comunicare tramite le porte che ogni amministratore deve lasciare aperte, la grande maggioranza dei bot comunica ancora tramite IRC (porta 6667) e altre inconsuete, con elevata numerazione (quali 31337 e 54321). Tutte le porte al di sopra della porta 1024 devono essere impostate per bloccare sia il traffico in uscita che quello in entrata, a meno che l'organizzazione non disponga di un'applicazione personalizzata o abbia speciali esigenze di tenere aperta una determinata porta. Anche allora, è necessario fare attenzione quando si apre una porta, implementando criteri quali "apertura solo durante l'orario lavorativo" oppure "rifiuta tutto, a eccezione del traffico proveniente dal seguente elenco di indirizzi IP affidabili". Questa semplice misura impedisce ai bot della varietà garden e slow-adopter di raggiungere il C&C (Command and Control Center) per istruzioni e aggiornamenti, neutralizzando essenzialmente questi bot al loro arrivo.

2) Il traffico botnet che viaggia attraverso le porte necessarie quali la 80 o la 7, spesso si rivela generando traffico quando non ce ne dovrebbe essere. Comunemente i botmaster aggiornano gli zombi tra l'01:00 e le 05:00, quando suppongono che nessuno stia osservando. È importante che controllare il log del server ogni mattina diventi un'abitudine. Se è presente un'attività di navigazione nel Web in ore in cui non vi era nessuno a navigare, è un buon indizio per iniziare a investigare.

Gli amministratori che utilizzano i modelli WatchGuard Firebox® saranno lieti di sapere che i proxy di Firebox non consentono l'entrata di traffico non-standard che tenta di utilizzare porte standard. Ad esempio, lo spamming botnet Mega-D esegue traffico non-standard, homebrew sulla porta HTTP 80. Il proxy HTTP di Firebox individua e blocca tale traffico immediatamente, per impostazione predefinita.

4. Raddoppiare il training di consapevolezza degli utenti

Alcuni bot eseguono scansioni di massa su Internet, individuano i computer vulnerabili e quindi li infettano. Questa pratica è però sempre meno frequente. Più spesso accade che i bot si aprano la strada per la rete

utilizzando metodi di "social engineering" inducendo la vittima a fare clic su un link o ad aprire un file. Analogamente ad alcuni leggendari vampiri, questi bot presentano lo stesso limite: non possono oltrepassare la soglia se non vengano invitati.

Questo approccio "accattivante" si è gradualmente ristretto ancora di più. Gli attaccanti inviavano codice nocivo eseguibile come allegato a un messaggio di posta elettronica. Anche questa pratica è utilizzata sempre di meno. Oggi la maggior parte degli attacchi si basa sul Web. Le email nocive che due anni fa avrebbero contenuto un allegato, oggi contengono un collegamento a un sito nocivo. Siti Web innocui possono essere infettati da Mpack o altro malware illegittimo che infetta i visitatori arrivati tramite clic imprudenti.

È necessario spiegare agli utenti, in termini comprensibili, che non devono mai invitare un vampiro ad entrare nella propria casa. Non devono aprire gli allegati non richiesti e inaspettati; non devono fare clic sui link contenuti nelle email; e devono pensarci due volte prima di fare clic su un link sconosciuto. Per iniziare, provate a distribuire presso utenti a digiuno di conoscenze tecniche il nostro video che mostra come funzionano i download indesiderati: <http://video.google.com/videoplay?docid=-4094518401580008932>. L'applicazione meticolosa dei controlli che abbiamo illustrato consente di eliminare la presenza dei bot dalle reti per anni.

5. Vigilare

Questa raccomandazione sembra troppo ovvia per essere menzionata, almeno quanto "Cercate di non essere infettati!". Nonostante ciò continuiamo ad incontrare amministratori IT che passano troppo tempo a spegnere incendi e gestire help desk con personale insufficiente, che non controllano mai i log di sistema. Non controllano mai l'utilizzo dell'ampiezza di banda. Non sanno chi si sta collegando a quale risorsa della propria rete. Non conoscono tutte le periferiche collegate in rete.

Se vi riconoscete in questa descrizione, non possiamo dirvi altro che siete alla ricerca di guai grossi. Potreste persino avere qualche bot nella vostra rete mentre state leggendo questo documento. Se siete amministratori che raramente controllano i log, è necessario che iniziate a leggerli. Oggi stesso. Una volta che abbiate imparato qual è l'aspetto "normale" di una rete, 30 minuti al giorno è tutto il tempo che dovrete spendere per un controllo a campione.

Se vi riconoscete in questa descrizione, ci sono buone probabilità che più che pigri siate limitati dalla mancanza di personale e risorse. Spiegate ai vostri dirigenti che esiste un vero pericolo, e vedrete se approveranno o no ogni mattina un blocco di mezz'ora per controllare lo stato della rete. Questo lasso di tempo dovrà essere difeso dalle richieste di riunioni, dalle conference call e altre tipiche interruzioni. Questa forma di assicurazione è molto economica in confronto ai costi di una rete compromessa.

Riteniamo che i recenti attacchi senza precedenti dei bot non siano altro che una prefigurazione di quello che accadrà in futuro. Come mai prima accaduto, nei tanti anni della nostra esperienza nel settore della sicurezza su Internet, ogni mese sembra portare scoperte di nuovi attacchi *che i ricercatori non sono in grado di spiegare completamente*.

Si scopre che i botnet sono state minacce combinate, ma non sono diventate le minacce combinate *definitive*. I botmaster ora forniscono gratuitamente l'architettura botnet tradizionale con componenti aggiuntivi che ne migliorano automazione, amministrazione ed evasione. Queste combinazioni di tecnologie sono spaventosamente sofisticate e sorprendentemente funzionali. Qualsiasi osservatore può prevedere con sicurezza che questa tendenza non solo continuerà, ma crescerà.

I cattivi stanno vincendo? Ovviamente no, dal momento che stiamo ancora utilizzando Internet per acquisti e movimenti bancari. Ma il flusso dell'attività dei bot è in aumento, quindi dobbiamo respingerlo, arginando la piena dei bot e rivelando le tecniche dei loro botmaster. Un modo semplice per indebolire il potere di un botmaster è quello di rendere difficile la selezione delle vittime. Le appliance di protezione WatchGuard utilizzano numerosi livelli di protezione, applicati in modo intelligente su molti protocolli, con una potente tecnologia proxy che filtra il traffico in entrata e in uscita per mantenere protetta la rete.

Per informazioni sulle soluzioni di protezione WatchGuard e sulla protezione che forniscono nei confronti di botnet e le altre minacce di rete, visitate il sito www.watchguard.com o contattate un nostro rivenditore.