13 Anno II

INFORMATION SECURITY

La Rivista dell'ICT per la Sicurezza

CIPIC Italia
Associazione Italiana esperti in Infrastrutture Critiche

PRIMO PIANO
Crimini in rete: più pericoli per la vittima, meno rischi per il cybercriminale

PRIMO PIANO
Il pericolo delle frodi nei pagamenti in mobilità

SCENARI
Sicurezza Nazionale al tempo della "Network Warfare"

SOTTO LA LENTE
G Data, il nostro servizio al tuo servizio

Ediser s.r.l. ROC n°17883 ISSN 2037 - 5611
Pubbl. mensile registrata presso il Tribunale di Roma il 7/10/2010 n°379 Poste Italiane S.p.A.
Spedizione in abbonamento postale - 70% Roma Aut. n. C /RM/109 2010

ediser

Botnet: i veri eserciti virtuali

"In guerra è la regola: se le nostre forze sono dieci volte quelle del nemico, questo deve essere circondato; se sono cinque a uno, va attaccato (…); se sono leggermente inferiori, va evitato".

Marco Caselli
GCSEC

Probabilmente Sun Tzu non pensava ai combattimenti informatici nel suo "L'arte della guerra", ma a volte gli scenari reali e quelli virtuali condividono gli stessi principi. La dimensione dell'esercito è uno di questi. Maggiori sono le forze in gioco, più alta è la probabilità che le difese del nemico crollino, sia che si parli di "wall" che di.. firewall!

Così nasce la botnet, l'idea di sfruttare un esercito di computer che esegue silenziosamente gli ordini e gli attacchi da parte del suo padrone, il "bot herder". Ma come fa un cracker a prendere possesso di un così largo numero di macchine e soprattutto cosa può fare con questo esercito?

Beh, la botnet non è altro che un insieme di computer compromessi, connessi su Internet e in attesa di comandi. Ogni elemento (il "bot") è un dispositivo infettato da un malware progettato per aprire un canale di comunicazione con la macchina controllata dal cracker. Tuttavia, in questo modo sarebbe troppo semplice rintracciare i bot master ed infatti, questi ultimi approfittano di sistemi differenti come i server IRC (Internet Relay Chat). Attraverso questo tipo di servizi essi sono in grado di creare un punto d'incontro dove consegnare e di trasmettere le istruzioni per i bot.

Questa è solo la struttura logica, la gestione delle botnet può essere davvero complicata, dato che l'obiettivo principale di un cracker è quello di non essere rintracciato. Inoltre, è importante allo stesso modo aumentare il numero di computer controllati, per questo la botnet è raramente dormiente. Ogni suo componente è sempre occupato a cercare altre vittime. Il malware, se non ri-

ceve istruzion differenti dal suo padrone, monitora la rete e tenta di installarsi su ogni nuovo dispositivo possibile.
Gli attacchi e le attività criminose che un gestore di botnet può compiere sono numerosi e differenti tra loro. Il modo più conosciuto per usare i PC 'zombie' (come vengono generalmente chiamati dato che sembrano inattivi quando invece stanno lavorando per qualcun altro) è sferrare attacchi denial-of-service distribuiti. Un server o un router difficilmente possono gestire un traffico persistente generato da migliaia di macchine e dunque cedono sotto l'effetto della botnet rendendosi indisponibili agli utenti.
Le botnet sono comunemente utilizzate per attività di spionaggio. Gli spyware trasmessi al loro interno sono in grado di raccogliere informazioni sulle attività degli utenti e inviarle ai 'bot herders'. Password, numeri di carte di credito, ma anche i siti web visitati sono dati preziosi che possono essere venduti nel mercato nero.
Un altro business molto redditizio riguarda lo spamming. Nel corso degli anni è stato stimato che circa l'80% del traffico email mondiale proviene da botnet. I messaggi sono di solito pubblicitari o fraudolenti.
Vale la pena notare che le botnet vengono anche usate come supporto per altre frodi informatiche. Il phishing, ad esempio, (la truffa che cerca di ingannare gli utenti con copie di siti web simili a quello originale) può utilizzare una botnet per nascondere i server che ospitano il sito falso. Questo viene fatto attraverso meccanismi chiamati "Fast Flux"; tecniche che modificano continuamente i record DNS per creare un network in continuo cambiamento in cui è quasi impossibile rintracciare le connessioni.
Indipendentemente dai tipi dell'attacco, la forza delle botnet è sempre la dimensione. Se l'anti-crimine informatico non riesce a trovare i server di comando e controllo (le macchine utilizzate di solito per instradare le istruzioni verso i bot) l'eliminazione di botnet formate da migliaia di macchine è praticamente impossibile. Ma i numeri sono molto più alti. La botnet Bredolab nel 2009 ha raggiunto 30.000.000 di unità ed insieme, Rustock e Cutwail, (con solo 1.650.000 bot) nel biennio 2006/2007 hanno inviato qualcosa come 100 miliardi di email spam al giorno!
Infine, ma non meno importante, il mondo cyber ha ora a che fare con Zbot. Questa minaccia è possibilmente più pericolosa delle altre poiché non è ancora chiaro quanto sia estesa la rete di computer compromessi (alcune ipotesi parlano di 3.600.000 bot solo negli Stati Uniti) e per il malware coinvolto: Zeus. Questo applicativo, oltre ad essere uno dei trojan più complessi ed efficaci rilevati finora, è pure molto difficile da rilevare, anche con i software antivirus aggiornati. Tuttavia gli esperti di sicurezza informatica non stanno a guardare. I sistemi di Intrusion Prevention (in particolare la tipologia rate-based) ed i sistemi di Intrusion Detection sono strumenti efficaci e ampiamente utilizzati per mitigare il problema, anche se questi devono sempre essere aggiornati per contrastare nuovi malware. La soluzione definitiva ancora non esiste.
Gli eventi della storia ci insegnano che gli eserciti più numerosi usualmente escono vittoriosi dalle battaglie. Per questo motivo è possibile che nel prossimo futuro le nazioni e le grandi aziende mettano in piedi a loro volta armate di centinaia di computer a difesa dei loro domini informatici. La storia ci racconta delle guerre del passato, le cyber-guerre saranno raccontate nei libri di cyber-storia?

IPv6, una reale necessità

Il protocollo IPv4 ha ormai assegnato quasi tutti gli indirizzi disponibili, circa 4,3 miliardi. È imprescindibile il passaggio al nuovo protocollo IPv6 per evitare il collasso.

Elena Agresti
GCSEC

Internet, nata negli anni '60 durante la guerra fredda, era inizialmente una rete dedicata alle comunicazioni all'interno della comunità scientifica e tra le associazioni governative e amministrative. Chi poteva accedere originariamente a Internet era parte di una élite tecnocratica che non aveva alcun interesse a danneggiare il lavoro degli altri utenti. Ci si preoccupava principalmente dell'affidabilità della rete. Non vi erano problemi di sicurezza, di supporto alla mobilità, di qualità del servizio o di numero di utenti.

Oggi possiamo leggere la posta elettronica o accediamo ai siti di social network da dispositivi diversi come il portatile, il pc, lo smartphone, e da punti diversi della rete. Trasmettiamo file audio e video over IP e stiamo assistendo all'evoluzione verso il mondo di 'Internet of things', in cui una vasta gamma di dispositivi intelligenti come elettrodomestici, telefoni e veicoli supportano la connettività. La possibilità di poter usufruire di servizi come l'e-banking e l'e-commerce ha esposto gli utenti a rischi di perdite finanziare e sensibilizzato ancor più sulle tematiche di sicurezza. Con l'evoluzione dei servizi, Internet deve rispondere a nuove necessità.

Nata per un numero minore di utenti, oggi Internet è al collasso. Il suo protocollo originario, chiamato IPv4, ha assegnato ormai quasi tutti gli indirizzi disponibili, circa 4,3 miliardi. Sono state adottate altre misure come il NAT (Network Address Translation), che consente l'assegnazione di un unico indirizzo ad intere reti. Oggi, infatti, le reti aziendali hanno generalmente solo pochi indirizzi direttamente collegati a Internet; intere reti aziendali sono viste come un singolo host. L'uti-

Gli operatori hanno competenze approfondire su IPv4, ma la mancanza di capability specifiche sull'IPv6 espone le organizzazioni ad un reale rischio per la sicurezza

lizzo del NAT consente quindi la creazione di host e reti nascoste. Mentre aumenta la protezione dei server interni il cui indirizzo IP non è noto, il NAT rende più complicati i controlli di sicurezza e riduce la sicurezza end-to-end.
L'unica soluzione possibile al collasso di Internet è l'adozione di un nuovo protocollo, l'IPv6. l'IPv4 e l'IPv6 funzioneranno in parallelo fino a quando sarà necessario, anche se nel lungo periodo, l'implementazione di IPv6 sarà obbligatoria.
I principali device in commercio prevedono già l'implementazione di entrambi i protocolli per consentire la comunicazione con tutte le tipologie di dispositivi. I principali fornitori di servizi come Google, Facebook, Youtube hanno recentemente adottato l'IPv6 e forniscono i propri servizi sia in Ipv4 che in Ipv6.
Il protocollo IPv6 è nato per rispondere a diverse problematiche, prima tra tutte l'ampiezza dello spazio d'indirizzamento. La capacità d'indirizzamento dell'IPv6 consente l'utilizzo di migliaia di miliardi di nuovi indirizzi Internet, comprendendo tutte le richieste attuali e future. A differenza dell'Ipv4 costituito da quattro gruppi di tre cifre separati da punti del tipo 192.168.2.1, un tipico indirizzo IPv6 è composto da 8 gruppi separati dal carattere ":". Ogni gruppo è composto da un massimo di quattro lettere e numeri del tipo 2001:db8:1f70:999:de8:7648:6e8.
Essendo un protocollo di nuova generazione include nativamente funzionalità aggiuntive come ad esempio l'IPsec che nel protocollo IPv4 era opzionale. In particolare l'IPsec consente l'autenticazione dei messaggi, autenticando l'indirizzo del mittente e verificando che il pacchetto non sia stato alterato durante il percorso. Inoltre, attraverso l'autenticazione e la cifratura dei messaggi, garantisce che solo il destinatario autorizzato sarà in grado di leggere il messaggio.
Inoltre, l'Ipv6 garantisce migliori performance della rete e in particolare di router e bridge/switch prevedendo una dimensione fissa dell'header e semplificando il deployment dei sistemi mobile IP-based. È, infatti, un protocollo multicasting; trasmette un pacchetto a più destinazioni in un'unica operazione d'invio fornendo quindi maggiore velocità soprattutto su mobile. IPv6 garantisce scalabilità e abilita applicazioni innovative come reti di sensori e sistemi embedded.
L'Ipv6 consente ad ogni device di avere un proprio indirizzo IP, semplificando progetti di rete e consentendo anche una più facile configurazione remota.
Nel caso un computer non supportasse l'IPv6, i siti internet saranno configurati per fornire i servizi attraverso le tradizionali connessioni IPv4. Sarà, infatti, applicata la configurazione "dual stack".
Il passaggio a IPv6 non ha e non avrà dunque alcun effetto sull'operatività di Internet e sugli utenti finali. Il periodo di transizione sarà lungo e gli operatori di rete dovranno imparare a definire e conoscere nuove procedure di sicurezza specifiche per l'Ipv6 e dovranno rimanere costantemente aggiornati.
L'adozione di IPv6, pur apportando vantaggi in termini di operatività e sicurezza, porta con sé anche alcuni svantaggi. Pur rispondendo infatti alla mancanza di indirizzi IP, la crescita di indirizzi IP può causare il collasso dei sistemi di filtraggio. Infatti, circa il 90% di strumenti web di filtraggio utilizzati da parte delle imprese, oggi si basa su blacklist. Inoltre, le organizzazioni dovrebbero aggiornare la propria politica di sicurezza con l'adozione dell'Ipv6. Regole firewall e di sicurezza della rete devono essere riconsiderate. La variazione dinamica degli indirizzi IP può rendere difficile l'attuazione, con Ipv6, delle politiche di sicurezza già adottate a causa della diversa struttura dei pacchetti. Inoltre oggi, i prodotti Ipv6-based sono ancora immaturi o mal configurati e quindi maggiormente esposti a vulnerabilità. Malware con IPv6-based command-and-control capability sono già diffusi. Un'analisi condotta da RIPE Labs, ha evidenziato che il 3,5% di tutte le email ricevute proveniva da spam su reti IPv6. Ciò indica che gli spammer hanno già iniziato la "migrazione" verso l'Ipv6.
Gli operatori hanno competenze approfondire su IPv4, ma la mancanza di capability specifiche sull'IPv6 espone le organizzazioni ad un reale rischio per la sicurezza. In molti casi, infatti, l'abilitazione dell'Ipv6, attuata per garantire l'utilizzo di entrambi i protocolli IPv6 e IPv4, se non gestita correttamente, può vanificare le misure che erano state implementate per garantire la sicurezza dell'altro protocollo.
Al fine di accrescere le conoscenze sull'Ipv6 e facilitarne il deployment, sono state pubblicate numerose linee guida da parte dei vendor o di enti di standardizzazione, quali ad esempio il NIST che ha pubblicato l'SP 800-119 "Guidelines

for the Secure Deployment of IPv6" (http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf), l'ICANN o l'OECD che ha studiato la transizione da IPv4 a Ipv6 fornendo un'analisi degli aspetti economici ad essa connessi.
Lo sviluppo dell'Ipv6 è uno degli elementi chiave dell'Agenda Digitale Europea. Durante l'ultimo 'Ipv6 Day', Neelie Kroes, vicepresidente della Commissione Europea responsabile dell'Agenda Digitale, ha esortato i governi, i fornitori di servizi e contenuti Internet e qualsiasi impresa svolga attività commerciali su Internet a passare al più presto all'IPv6, "...altrimenti l'Europa si troverà ad affrontare una situazione insostenibile: enormi distorsioni del mercato, Internet più lenta e ripercussioni negative sull'innovazione."
La Commissione Europea nella comunicazione COM(2008) 313, definisce il piano di azione per il deployment dell'IPv6 in Europa. Il Comitato Economico e Sociale Europeo (CESE) ha espresso anch'esso la sua opinione in merito (2009/C 175/17), concordando sulla necessità di un'azione urgente e incoraggiando la Commissione Europea ad essere più "assertiva sul ruolo leadership che l'Unione Europea dovrebbe adottare per accelerare rapidamente l'adozione di IPv6".
Anche le istituzioni italiane sono consapevoli della rilevanza di tale migrazione al punto che in una delle "mozioni sulla sicurezza da minaccia cibernetica", approvate nella seduta n. 728 del 23/05/2012, il Senato "impegna il Governo ad adottare, con la massima urgenza - in ragione della gravità dei rischi conseguenti all'esaurimento degli indirizzi IPv4 - misure idonee a consentire la disponibilità di nuovi indirizzi IP univoci, con il passaggio all'IPv6 o con l'introduzione di dispositivi tecnici che consentano altrimenti l'identificazione dell'utente".
L'FBI ha invece espresso le sue preoccupazioni in merito all'uso dell'IPv6. Richiede, infatti, che "nell'IPv6 siano abilitate le caratteristiche di tracciabilità al fine di consentire agli agenti federali di identificare i criminali sospetti con lo stesso tipo di facilità avuta con l'IPv4". L'FBI ha anche suggerito che una nuova regolamentazione potrebbe essere necessaria nel caso in cui il settore privato non lo facesse volontariamente.
Un esponente dell'FBI ha dichiarato: "Un problema potrebbe essere la quantità di informazioni che viene detenuta dai provider ed i log storici esistenti. Oggi gli operatori possiedono interi registri dell'IPv4. Secondo come l'IPv6 sarà implementato, tali registri potranno essere o non essere sufficienti per le forze di polizia."
La transizione all'IPv6 è divenuta quindi una reale necessità. Per garantire una corretta transizione, è necessaria una cooperazione ed un'attività di monitoring a livello internazionale. I governi devono incoraggiare l'adozione dell'IPv6. Gli operatori e il settore privato, devono imparare a definire e implementare nuove procedure operative e di sicurezza, predisporre percorsi formativi specifici ed includere la connettività IPv6 negli accordi con i fornitori.