Iniziato nel febbraio 2013, il Progetto Europeo *Advance Cyber Defence Centre* (ACDC) mira a creare una comunità di *stakeholder* che uniscano le loro forze per combattere le botnet. ACDC si rivolge agli utenti di tutta Europa attraverso una Rete di Centri Nazionali di Supporto (CNS).
Il Centro Nazionale Antibotnet italiano, istituito presso il Ministero dello Sviluppo economico, opera assieme agli altri centri europei nel contrasto alla diffusione delle botnet.

Antonello COCCO è dirigente presso il Ministero dello Sviluppo economico dove ricopre il ruolo di Direttore della III divisione "Internet, sicurezza delle reti e delle informazioni e qualità dei servizi ICT".

Tiziano INZERILLI, ingegnere, è funzionario presso il Ministero dello Sviluppo economico, III divisione "Internet, sicurezza delle reti e delle informazioni e qualità dei servizi ICT".

LE MINACCE INFORMATICHE DI TIPO *BOTNET*

di Antonello COCCO e Tiziano INZERILLI

Una *botnet*[1] è una rete di *computer* compromessi da *malware* e comandati a distanza per scopi illegali. Si entra a far parte di una *botnet* inconsapevolmente quando il proprio *computer* non è adeguatamente protetto ed aggiornato. Le *botnet* costituiscono una minaccia insidiosa in quanto un'infezione può rimanere a lungo non rilevata e silente per essere sfruttata successivamente per produrre danni ingenti a sistemi di terze parti.
Gli scenari tipici di infezione prevedono l'apertura di *email* infette o di documenti ad essi allegati, *malware* nascosto in programmi *freeware* scaricati dagli utenti, utilizzo di vulnerabilità specifiche in sistemi ed applicazioni non aggiornate. A volte la semplice navigazione in siti *web*, anche siti ufficiali infettati da *hacker* esperti, può produrre il *download* automatico di programmi in grado di infettare il proprio *computer* e la cattura in una *botnet*.

In generale qualsiasi dispositivo che accede ad Internet che sia un PC, un portatile, palmare o *smart* TV è esposto al rischio di infezione, indipendentemente dal sistema operativo. Con l'avvento del modello Internet delle Cose, ogni dispositivo elettronico è potenzialmente a rischio di infezione da *botnet*[2]. I *computer* con sistemi operativi MAC OS X, ritenuti in passato più sicuri dei sistemi Windows, sono stati interessati recentemente da una *botnet*[3].
Una volta entrati in una *botnet*, le risorse del proprio *computer*, assieme a quelle di migliaia di altri utenti, sono a disposizione per la realizzazione di fini illeciti. Questi vanno dalla semplice diffusione di *email* di *spam*, ai temibili attacchi di tipo DDoS (*Distributed Denial of Service*), al furto di dati, alla memorizzazione di contenuti illegali, o più in generale all'utilizzo dei *computer* infetti per portare attacchi indiretti nascondendo l'identità dell'attaccante controllando da remoto macchine infette. Il potenziale delle *botnet* cresce con il numero dei *computer* compromessi ad essa aggregati ad un ritmo esponenziale raggiungendo anche diversi milioni di *computer*.

In letteratura si ricorda la *botnet* "Mariposa"[4], scoperta nel mese di aprile del 2009 e costituita da 13 milioni di *computer*. Nel 2010[5] un attacco informatico orientato al furto di dati e credenziali di utenti di vasta portata denominato "Kneber bot", con base operativa nell'Europa dell'Est, ha interessato ben 196 nazioni, per un totale di 2.500 aziende interessate e 75.000 personal *computer* manomessi. Più recentemente[6] Europol ed FBI con la cooperazione di Microsoft ed altre industrie ha condotto un'operazione contro la *botnet*, nota col nome di "Zeroaccess", principalmente impiegata per il *mining* dei *bitcoin*, con una dimensione stimata di 1,9 milioni di *computer* nell'ottobre del 2013. Nel giugno del 2014[7] il Dipartimento di Giustizia USA annuncia una operazione internazionale guidata dagli USA per contrastare la *botnet* Gameover Zeus specializzata nel furto di credenziali, anche bancarie, dai *computer* degli utenti infetti, responsabile di più i 100 milioni di dollari di perdite. Nel luglio del 2014[8] l'FBI riferisce dinanzi alla Commissione Giustizia del Senato USA le minacce poste dalle *botnet* e le ultime operazioni effettuate contro di esse, quali Butterfly Bot, Rove Digital, Coreflood, ZeroAccess e GameOver Zeus risultate in numerosi arresti, estradizioni ed altre misure cautelari.
Bollettini di operazione condotte contro le *botnet* da FBI, Europol ed industrie ICT continuano a susseguirsi. Nonostante ciò una *botnet* non può mai ritenersi definitivamente sconfitta. Le operazioni di *takedown* possono non arrivare a colpire tutti i cosiddetti sistemi di controllo C&C (*Command and Control*) utilizzati per il controllo remoto delle *botnet* ed a risalire sino all'arresto del controllore della *botnet*, il *bot herder*. Inoltre il codice malevolo utilizzato in una *botnet* ritenuta sconfitta può essere riutilizzato, anche riadattato, per impedirne la rilevazione e disinfezione e per continuare a determinare danni ingenti di fronte ad una molteplicità di utenti di Internet che non sempre è attenta ai rischi della rete ed alle necessità di aggiornare il proprio *computer*.

In uno scenario talmente incerto, risultano di particolare rilievo anche le azioni cosiddette di mitigazione, orientate alla sensibilizzazione e coinvolgimento degli utenti di Internet sulle *botnet* ad autocontrollarsi da *virus* e rimuovere le eventuali infezioni ed a mantenere il *software* del proprio *computer* costantemente aggiornato. Tra queste citiamo l'iniziativa europea ACDC (*Advance Cyber DEfence Centre*)[9] nella quale è coinvolto l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico, che ha recentemente pubblicato un portale *web* relativo al Centro Nazionale Antibotnet[10] che mira a realizzare politiche attive di sensibilizzazione di utenti di Internet in collaborazione con analoghi centri europei. ©

NOTE

1. http://www.enisa.europa.eu/publications/archive/botnets-2013-the-silent-threat
2. http://www.techrepublic.com/blog/it-security/internet-of-things-botnet-may-include-tvs-and-a-fridge/
3. http://www.eweek.com/c/a/Security/Mac-Botnet-Infects-More-Than-600000-Apple-Computers-699749/
4. http://www.telegraph.co.uk/technology/7913767/FBI-arrests-mastermind-of-Mariposa-botnet-computer-code.html
5. http://www.key4biz.it/Players-Vinti-2010-02-Washington-Post-NetWise-Attacco-Informatico-Criminali-Botnet-Login-eMail-Dati-Sensibili-Informazioni/
6. http://e-channelnews.com/ec_storydetail.php?ref=433944&title=Microsoft,-the-FBI,-Europol-and-industry-partners-disrupt-the-notorious-ZeroAccess-botnet-
7. http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware
8. http://www.fbi.gov/news/testimony/taking-down-botnets
9. http://www.antibot.it/it/content/il-progetto-europeo
10. http://www.antibot.it/ ◊