Collegio Ghislieri – Convegno "PRESI NELLA RETE"
23 novembre 2012

Malware, botnet e underground economy: una panoramica sugli scenari contemporanei

Introduzione

Sono passati trent'anni da quando i primi virus per computer hanno fatto la loro comparsa nel mondo dell'informatica. Da allora, però, le cose sono completamente cambiate: la minaccia si è evoluta, diversificata, specializzata; soprattutto, sono cambiate le motivazioni e gli scopi di chi scrive malware. Ciò che un tempo poteva essere il prodotto di uno studente annoiato o dispettoso, oggi è diventato un sofisticato strumento concepito, progettato e sviluppato per deliberati scopi criminali e di spionaggio. La mentalità imprenditoriale della criminalità organizzata ha saputo cavalcare l'opportunità, costruendo nuove occasioni di profitto e nuovi modelli di business, noi siamo in grado di resistere e contrattaccare?

Per comprendere meglio gli scenari attuali e la loro complessità, è utile fare un passo indietro e ripercorrere in retrospettiva il percorso che ci ha portato ad oggi. La criminalità informatica moderna infatti prospera grazie ad un sistema economico clandestino molto vivace e ad una variegata serie di attività lucrative che sono rese possibili dall'esistenza di colossali botnet, reti composte da milioni di calcolatori infetti appartenenti a utenti e organizzazioni inconsapevoli sparsi in tutto il mondo. Il mattone fondante delle botnet è dunque il bot, o zombie, cioè la singola macchina compromessa, e l'elemento fondamentale del bot è il malware che lo ha reso tale.

Il malware

Anche se il malware è il fondamento di tutto il fenomeno cybercrime, c'è ancora scarsa percezione da parte degli utenti riguardo cosa effettivamente sia il malware e cosa sia in grado di fare. Nell'utente medio, infatti, permane tutt'oggi l'idea di virus informatico che si è radicata negli anni '80, secondo la quale i virus sono quei programmi che danneggiano i computer. Niente di più sbagliato! Ai virus di oggi serve che i computer degli utenti siano pienamente funzionanti e godano anzi di ottima salute, e il loro interesse è di rimanere nascosti il più a lungo possibile senza manifestare alcun segno dell'infezione avvenuta, così da poter sfruttare indisturbati le risorse disponibili. Non è quindi un paradosso che certi malware, anziché danneggiarli, attivino addirittura delle protezioni nei computer che infettano, per evitare che altri malware possano interferire con il loro operato. Nel corso dei decenni i malware si sono specializzati in molte forme: abbiamo worm, trojan, spyware, dialer, keylogger, hijacker, rootkit e ogni altra diavoleria che si possa concepire, ma niente che sia finalizzato a produrre danni ai computer infettati. Infatti, a meno che non vi siate costruiti in cantina un impianto per l'arricchimento dell'uranio, nessuna organizzazione ha interesse a boicottare il vostro computer danneggiandolo, mentre sono in molti a poterne desiderare il controllo per i propri scopi.

Uno po'di storia

In principio dunque fu il malware. Quando alla fine degli anni '40 John von Neumann elaborò la teoria sugli elementi artificiali in grado di autoreplicarsi[1], probabilmente non poteva immaginare a cosa saremmo arrivati, e così neppure gli autori dei primi virus per computer che fecero la

[1] Éric Filiol, Computer viruses: from theory to applications, Volume 1, Birkhäuser, 2005, pp. 19–38 ISBN 2287239391.

loro comparsa negli anni '70, prima dell'era del Personal Computer, su sistemi Tenax o UNIVAC e su rete ARPANET. E' stato negli anni '80, con il graduale avvento dei computer da scrivania, che il termine virus ha cominciato a diventare popolare tra gli utenti dell'informatica e a colonizzarne l'immaginario. Erano tempi molto diversi, e i virus di allora visti con l'occhio smaliziato di oggi fanno quasi tenerezza nella loro ingenuità: il più delle volte si tratta di programmi frutto dal lavoro di un singolo programmatore impegnato in una sfida personale: realizzare un *proof of concept,* dimostrare cioè di essere in grado di realizzare una cosa nuova, sovvertendo il funzionamento ordinario della macchina con qualcosa di imprevisto, spesso nulla più che dispettoso o vagamente fastidioso. **Elk Cloner**[2], ad esempio, scritto da Richard Skrenta nel 1982 per sistemi Apple II, è sì responsabile della prima infezione su vasta scala nella storia dei personal computer (per quanto vasta potesse essere la scala dell'epoca), ma non ha al suo attivo alcun tipo di danno; il suo *payload*, infatti, si limitava all'autopropagazione (via floppy disk) e alla visualizzazione sporadica di una poesiola, senza interferire in altro modo con il funzionamento del computer. Altri virus dell'epoca, però, come **Gotcha** e **Suprise**, non sono altrettanto innocui e introducono intenti dannosi nel payload: la cancellazioni di dati agli utenti. E' un vandalismo gratuito, che non porta alcun guadagno ai creatori se non la sottile e un po' perversa soddisfazione di aver creato qualcosa di pestifero per gli altri. In Italia nasce **Ping Pong**[3], che per il suo modo di manifestarsi è probabilmente, insieme a **Cascade**[4], uno dei virus che più si imprime nell'immaginario comune del software "dispettoso". Una pietra miliare di quegli anni è **The Brain**, noto anche come Lahore o Paki Flu: programmato nel 1986 è il primo virus per PC IBM compatibili e MS-DOS. In qualche modo, l'antesignano di tutti i virus per Windows. Per dare l'idea dell'ingenuità dei tempi: il codice del virus (peraltro innocuo) contiene una sorta di copyright, i nomi degli autori, il loro indirizzo e persino il numero di telefono, tutti veri![5].

In quegli anni quindi i virus sono una minaccia limitata: scarsa capacità di propagazione, vincolata quasi esclusivamente allo scambio di floppy, e scarse capacità offensive, che possono arrivare al massimo al danneggiamento dei dati, eppure la preoccupazione cresce. Virus come **Jerusalem** e, soprattutto, **Michelangelo** vengono annunciati anche dalla stampa generalista come imminenti apocalissi digitali, anche se poi l'apocalisse viene puntualmente rimandata. Si sperimentano però nuove forme di costruzione e propagazione dei virus: nel 1988 Robert Morris, studente al MIT, realizza un programma per Unix con l'intento di misurare l'estensione dell'Internet di allora. Pur nato con i migliori propositi, però, il programma gli sfugge di mano e a causa della sua spiccata capacità di riprodursi in rete provoca dei massicci *denial of service*. E' nato il primo Internet worm[6].

Cominciano anche a nascere i primi *builder kit*, ovvero degli strumenti dedicati agli sviluppatori esplicitamente pensati per agevolare la creazione di nuovi virus. Con **Vienna** i virus diventano polimorfici, con **Frodo** imparano a nascondersi e con **Ghostball** a utilizzare più strategie di propagazione. Alla fine del decennio, nel 1989, qualcuno pensa per la prima volta di sfruttare il lavoro dei virus per un tornaconto economico: nasce infatti con **AIDS** il primo *ransomware* della storia[7], un modello che avrà molta fortuna fino ai giorni nostri: il virus occupa una risorsa (in questo caso cifra i nomi dei file sull'hard-disk con una chiave sconosciuta all'utente) e per restituirla chiede il pagamento di un riscatto.

Per tutti gli anni '90 si svolge una fervida attività di ricerca su tutti i nuovi fronti dell'informatica: arrivano i virus per Amiga e per Windows, i macrovirus per Office, e con la diffusione di Windows 95 e Linux arrivano anche immediatamente i primi virus per queste piattaforme. **Chernobyl** è il primo virus in grado di produrre danni permanenti nell'hardware, corrompendo il BIOS

[2] http://www.skrenta.com/cloner
[3] https://en.wikipedia.org/wiki/Ping-Pong_virus
[4] http://virus.wikia.com/wiki/Cascade
[5] L'anno scorso, in occasione del venticinquesimo anniversario di The Brain, Mikko Hypponen (il CRO di F-Secure) è andato di persona all'indirizzo di Lahore indicato nel codice e ha incontrato i due autori, Basit e Amjad: sono ancora là che gestiscono il loro Internet Service Provider, che non a caso si chiama Brain Telecommunication Ltd. Il video dell'incontro è stato pubblicato qui: http://www.youtube.com/watch?v=lnedOWfPKT0
[6] https://en.wikipedia.org/wiki/Morris_worm
[7] https://en.wikipedia.org/wiki/AIDS_(trojan_horse)

del computer. In questi anni la propagazione avviene via BBS e via Usenet, e mentre fanno la loro comparsa programmi storici quali **BackOrifice** e **NetBus**, sulla fine del decennio arriva qualcosa che cambia le regole: **Melissa**[8] è un worm che si diffonde via e-mail in maniera esponenziale e straordinariamente efficace, gettando le basi per gli sviluppi della successiva decade.

Si succedono **I Love You**, **Anna Kournikova**, **CodeRed**, **Nimda** e la ricerca spazia in ogni campo: javascript, payload iniettati nei browser tramite *iframe*, propagazione tramite reti P2P come Napster, WinMX e Kazaa; aumenta l'impiego di RAT (Remote Administration Tool), spyware e keylogger, si sperimentano i malware per dispositivi mobili sui sistemi Symbian e Palm. Avvicinandosi alla metà degli anni 2000, si percepisce dal fermento che qualcosa di grosso sta per accadere: i virus creati "just for fun" sono sempre meno e volgono ad una rapida estinzione, cedendo il passo a software che non sono più artigianali, ma raffinati prodotti con evidenti scopi lucrativi. Dopo aver a lungo sperimentato, infatti, è ormai chiaro che i malware possono fare ben di più che i dispetti: invece di cancellare i documenti degli utenti, possono rubarli; invece che danneggiare i PC, possono sfruttarli di nascosto, impiegandone le risorse di calcolo, la capacità di storage e la connettività per svolgere qualsiasi attività criminale con forti garanzie di impunità. Infettare un computer non basta ad assicurarsi ingenti guadagni, ma infettarne milioni e metterli in rete tra di loro, in quella che viene chiamata **botnet**, rende l'organizzazione in grado di disporre di milioni di soldati pronti ad eseguire qualsiasi ordine arbitrario.

Il salto epocale avviene nel 2005, quando la scoperta di botnet come **Rustock** e **Storm** (una botnet che arriverà a contare nel giro di un anno oltre un milione e mezzo di bot attivi) palesa la straordinaria organizzazione imprenditoriale che ne ha reso possibile lo sviluppo. Nascono i *crimeware kit* e con essi i nuovi modelli di business che forniscono non semplicemente l'azione criminale come servizio, ma addirittura gli strumenti per il cybercrime pronti all'uso, venduti come prodotto o persino erogati sotto forma di servizio.

Nel 2008 la situazione precipita: le botnet dominano e talvolta si contendono tra loro gli stessi bot, mentre sul finire dell'anno fa la sua comparsa un'altra pietra miliare nello sviluppo del malware: **Conficker** è il più sofisticato virus mai visto, un piccolo capolavoro di ingegneria del software, che nuovamente palesa i consistenti investimenti in ricerca e sviluppo che la criminalità è ormai in grado di impiegare nel settore.

Il sistema funziona e rende bene, tanto che si calcola che nel mondo il giro d'affari derivante da crimini informatici sia nello stesso ordine di grandezza di quello derivante dal narcotraffico internazionale[9]. Compreso questo, negli ultimi anni le attività si sono intensificate: si stima che per la fine dell'anno si arriverà ad aver censito circa 100 milioni di malware diversi, ma 30 milioni sono nati solo nel 2012! E altri trenta milioni soltanto nel biennio precedente. La crescita ha quindi avuto un'impennata senza precedenti e non accenna minimamente a diminuire, come risulta evidente dai grafici realizzati a riguardo da AV-Test[10].

Vettori di diffusione

I vettori utilizzati oggi per propagare le infezioni sono tutti quelli che vedono coinvolti un numero di utenti tale da costituire un'interessante riserva di caccia: le e-mail anzitutto, che restano veicolo privilegiato per spam, phishing, truffe e campagne virali, e subito a seguire il web, costellato di minacce in agguato non solo in siti appositamente costruiti per scopi malevoli, ma anche in siti pienamente legittimi che però una volta violati sono utilizzati per diffondere infezioni sfruttandone, oltre alle risorse tecnologiche, anche la popolarità e la reputazione. Ogni tecnologia è stata sovvertita e impiegata a scopo di abuso: linguaggi di scripting, injection nei database SQL, vulnerabilità dei browser o dei loro plug-in, come Flash e Java, e quando non è possibile attaccare il computer si cerca di

[8] http://virus.wikia.com/wiki/Melissa
[9] Norton Cybercrime Report 2011: http://it.norton.com/cybercrimereport/promo
[10] http://www.av-test.org/en/statistics/malware/

attaccare il *wetware*[11]: con l'utilizzo di strategie spicciole di *social engineering* si cerca di ottenere dall'utente ciò che non si riesce ad ottenere dalla macchina. Ecco quindi un proliferare di esche costruite apposta per ingannare gli utenti sullo scopo dei software o dei contenuti che stanno scaricando: si camuffano i malware per i loro antitetici software di sicurezza (*rogue antivirus*), si iniettano virus nei contenuti più ricercati dai naviganti, quali musica, pornografia, giochi e altri applicativi commerciali che vengono invece offerti "gratuitamente". Ma è solo apparenza: non esiste un pranzo gratis nell'universo, e il prezzo da pagare per il software craccato c'è ed è pure salato, ma abilmente nascosto. D'altro canto ci si potrebbe arrivare per intuito: per quale motivo qualcuno dovrebbe spendere ore di lavoro per rimuovere le protezioni da software commerciali come Photoshop o Office per poi venirceli a regalare, rischiando anche tutte le sanzioni che ne possono derivare? Non sarebbe più prudente da parte nostra diffidare di certi omaggi? Dovremmo aver imparato da secoli a temere gli Achei e i doni che portano... e invece sembra che il principale vettore di diffusione del malware, almeno secondo Microsoft[12], siano i *keygen*, quei richiestissimi programmi che servono a generare codici di licenza validi per attivare abusivamente costosi software commerciali. A volte funzionano davvero, a volte fanno solo finta, ma in ogni caso contengono sempre una sorpresa invisibile sotto forma di malware, che costituisce il prezzo riscosso dal criminale. É così per quasi tutto il software abusivo che si scarica dalle reti P2P, e la cosa non riguarda solo i programmi eseguibili: il malware può efficacemente essere inserito anche in contenuti quali musica, filmati, immagini, documenti PDF ecc., a torto ritenuti non pericolosi.

Ovunque si muovano gli utenti, lì affluirà il malware, ed è quindi normale constatare la presenza di campagne virali nei circuiti di instant messaging come Skype o MSN e nei social network, ma la vera battaglia oggi si combatte sui dispositivi mobili. Anche quegli utenti che dopo anni di ramanzine hanno compreso l'opportunità di disporre sul PC di un antivirus e di un firewall aggiornati, stentano ad assimilare gli stessi concetti quando si tratta di dispositivi mobili come smartphone e pad, che sono quindi una preda facile e ghiotta: scarsa sicurezza, potenza computazionale in crescita, alte probabilità di poter accedere alla rete ventiquattr'ore su ventiquattro, i dispositivi mobili non solo consentono di assolvere a molte delle funzioni di un bot tradizionale, ma hanno anche elevatissime possibilità circa la sorveglianza degli utenti, aumentando quindi le possibilità operative dei criminali. Ad esempio è di quest'anno la scoperta, da parte di un ricercatore Microsoft[13], di un'enorme botnet dedita allo spam composta unicamente da dispositivi Android.

Ogni oggetto tecnologico programmabile e che disponga di una connessione alla rete è già una potenziale preda, per cui forse la prossima frontiera saranno i nuovi dispositivi intelligenti che stanno popolando il mercato consumer, dalle *smart TV* ai sistemi di *infotainment* delle automobili. E' già stata valutata la possibilità teorica (e affatto remota) che presto possa nascere una nuova serie di malware orientata a colpire i dispositivi domestici collegati alla rete, come già avviene con i router casalinghi, per cui potremmo ritrovarci a dover combattere con malware studiati per colpire gli *home theatre* e i televisori: una volta programmati e collegati alla rete, sono come dei computer e come tali possono essere utilizzati a qualsiasi scopo. Chi mai si preoccuperebbe di installare un antivirus su un televisore, quando siamo abituati a considerarlo soltanto un elettrodomestico? E invece, nel momento in cui gli elettrodomestici acquistano connettività dobbiamo cominciare a rivalutarli, perché presto potremmo ritrovarci con intere botnet composte da smart TV infette. E poi chissà, la cosa potrebbe degenerare ulteriormente… Un giorno non lontano potrei svegliarmi e scoprire che durante la notte il mio frigorifero è diventato un signore del cybercrime e che gestisce un giro di riciclaggio di denaro che parte dalla mia cucina e si dirama nel sud-est asiatico. Non c'è mica niente da ridere.

Le botnet

[11] Tutti conoscono la distinzione tra hardware e software, ma molti tralasciano di considerare il wetware, ovvero quella parte del sistema che si localizza solitamente tra la tastiera e la sedia. Eppure non è soltanto una parte evidentemente vitale del sistema, ma anche la più vulnerabile, manipolabile, fallibile e affetta da bug e implementazioni carenti.

[12] Microsoft Security Intelligence Report v13 (https://www.microsoft.com/security/sir)

[13] https://blogs.msdn.com/b/tzink/archive/2012/07/03/spam-from-an-android-botnet.aspx

Il malware dunque ha come scopo principale quello di creare un bot. Ma il bot è solo un piccolo mattone di una grande costruzione. Una volta infetto, il bot deve comunicare con l'esterno per ricevere ordini ed eseguirli. Cercherà quindi di collegarsi ad un sistema di comando e controllo, dal quale lui e i suoi simili riceveranno istruzioni e aggiornamenti. La struttura ovviamente è ridondata, di modo che non sia possibile disattivare la botnet spegnendo un singolo server centrale di comando e controllo, perché di server simili ne esistono sempre in numero elevato, sparsi in diversi paesi del globo.

Le botnet sono una minaccia così efficace perché colpiscono dove è più facile: mirano direttamente agli utenti perché nei grandi numeri è facile trovare debolezze e ingenuità tali da poter essere sfruttate. Il problema però riguarda tutti: non basta mettere al sicuro il proprio PC e tenersi personalmente al riparo da attacchi diretti, perché finché ci saranno bot in numero sufficiente le attività criminali potranno proseguire proficuamente con ricadute dannose per tutta la società.

Le botnet e il cybercrime in Italia

L'Italia non è immune al problema, anzi, sembra al contrario che ne sia particolarmente colpita. Durante l'analisi della botnet GameOver, F-Secure ha rilevato che il 10% degli IP dell'intera botnet, che ha ovviamente estensione globale, sono localizzati in Italia[14]. Ma in Italia non c'è il 10% degli IP di Internet, quindi è evidente una forte sproporzione tra quella che dovrebbe essere l'esposizione all'attacco e quello che è invece il successo risultante.

Altre statistiche riportano un quadro allarmante: per Kaspersky l'Italia è il paese del mondo più a rischio per quanto riguarda le infezioni virali[15], mentre Team Cymru colloca il nostro paese al quinto posto mondiale per le attività di bot[16]. Symantec stima che nel 2012 ci siano state in Italia quasi 8,9 milioni di vittime di cybercrime, che hanno avuto perdite finanziarie dirette per un totale di 2,45 miliardi di euro[17]. Un danno medio di 275 euro a vittima, contro la media globale che è di circa 153 euro. L'Italia quindi non è semplicemente interessata dal fenomeno, ma è di fatto sottoposta ad una concentrazione di attacchi particolarmente intensa e, soprattutto, molto efficace, in grado cioè di sortire effetti molto redditizi.

Prendiamo questo esempio, senza dubbio molto noto: nel corso del 2012 è stata lanciata un'estesa campagna virale di un ransomware che blocca l'avvio del computer e, spacciandosi per una forza di polizia o un'agenzia governativa, richiede il pagamento di una "multa" per restituire all'utente l'accesso al proprio PC. Il malware si camuffa in modo diverso nei vari paesi del mondo, e in Italia è divenuto famigerato sotto le mentite spoglie della Guardia di Finanza, della Polizia di Stato, del CNAIPIC e persino dell'AISI. Se al cittadino avveduto pare implausibile l'idea che una forza di polizia possa ricorrere ad un virus per bloccargli il computer e chiedergli di provvedere al pagamento di un riscatto (per altro tramite sistemi di pagamento alquanto inverosimili per lo Stato), tuttavia esiste un consistente numero di utenti disposti a credere ad una richiesta tanto assurda. In percentuale possono sembrare pochi, meno del 3 per cento, ma i numeri sono sufficienti a garantire guadagni sostanziosi: se i criminali riescono ad infettare in tutto il mondo un milione di PC e il 3 per cento degli utenti colpiti (ovvero 30.000 soggetti) è disposto a pagare 100 euro di riscatto, ecco ottenuti 3 milioni di euro esentasse. Si stima infatti che il rendimento globale della campagna si aggiri sui 5 milioni di dollari all'anno, parte dei quali sicuramente affluisce dal nostro paese[18]. E la campagna sta ancora proseguendo.

Le attività redditizie

Dal malware al bot e dal bot alla botnet, dunque. Ma uno volta che si padroneggiano abusivamente e occultamente milioni di computer sparsi in tutti i paesi del globo, come è possibile ricavarne degli utili? L'unico limite sembrerebbe essere la fantasia.

---

[14] http://www.f-secure.com/weblog/archives/00002424.html
[15] https://www.securelist.com/en/analysis/204792244
[16] https://www.team-cymru.org/Monitoring/Graphs/
[17] http://www.slideshare.net/NortonOnline/2012-norton-cybercrime-report-14207489
[18] https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf

Uno dei metodi più facilmente intuibile è tramite il furto di credenziali. Con l'uso di keylogger mirati è facile intercettare le credenziali di accesso a tutti quei servizi che possono assicurare un guadagno diretto (homebanking, PayPal e simili) o indiretto (servizi quali Ebay possono essere impiegati per truffe, riciclaggio o anche solo per gonfiare la reputazione di altri account in vista di future truffe; l'accesso ad un webmail può consentirne l'uso per campagne virali o di spam ecc. ecc.), non ultima la possibilità di catturare altri dati personali impiegabili per eseguire in un secondo momento dei furti di identità agevolati ed efficienti.

Ma ancora più semplice è utilizzare i bot per il massiccio invio di mail di spam o per le campagne virali utili al mantenimento e alla crescita della botnet stessa, o ancora per il phishing: non solo i bot possono contribuire alla diffusione dei messaggi esca, ma quelli dotati di migliore connettività potranno essere impiegati anche per installare i siti clone su cui far affluire i malcapitati naviganti.

E' possibile anche a questo punto intervenire sulla navigazione degli utenti manipolandola, ad esempio per dirottarli verso gli stessi siti di phishing, oppure alterando i risultati dei motori di ricerca per favorire un cliente a discapito di un suo concorrente, o allo stesso modo sostituire i banner pubblicitari di una pagina, legittimi e debitamente pagati dall'inserzionista, con altri abusivi e pagati molto meno all'organizzazione criminale. E' anche possibile far sì che i bot simulino milioni di click sugli annunci pubblicitari che adottano la formula *pay per click*, realizzando così un truffa molto redditizia, quasi innocua per gli ignari utenti ma molto dannosa per le piattaforme di *advertising*, che prende il nome di *click fraud* e che può essere impiegata anche per danneggiare un avversario, costringendolo a sborsare elevati compensi per dei click che invece non gli porteranno alcun vantaggio commerciale in quanto effettuati dai bot.

Quando si dispone dell'ampiezza di banda di milioni di diverse connessioni ad Internet appartenenti a centinaia di provider in decine di paesi, è facile attuate delle massicce operazioni di DDoS (Distributed Denial of Service): con milioni di richieste simultanee, è possibile far collassare praticamente qualsiasi servizio offerto al pubblico, che non potrà più quindi essere erogato ai legittimi interessati fintanto che "l'inondazione" di richieste non sarà cessata. Così si può ricattare il soggetto erogante, chiedendo il pagamento di un riscatto affinché l'attacco sia interrotto e il servizio possa essere ripristinato. La stessa tattica viene offerta anche al pubblico come strumento per interrompere l'operatività di un concorrente commerciale, causandogli un danno e la plausibile perdita di clienti a vantaggio dei rivali.

Avendo a disposizione le connessioni Internet intestate a milioni di soggetti diversi in tutti il mondo, diventa anche semplice organizzare dei sistemi di riciclaggio molto articolati, che consentano di far sparire le tracce dei proventi illeciti in una fitta rete di transazioni internazionali difficilmente dipanabili dagli investigatori.

E così via, con l'unico limite, si diceva, dato dalla fantasia. Ma anche quando la fantasia dovesse venir meno, i botmaster hanno la possibilità di lucrare sull'esistenza della botnet anche soltanto subaffittandola, noleggiando cioè i bot o una parte di essi ad altre organizzazioni criminali che ne vogliono sfruttare il potenziale pur senza disporre del tempo o del know-how necessari per impiantare e amministrare una propria botnet. E' nato così un nuovo modello di business: il *crimeware as a service*. Le organizzazioni più tecnologicamente avanzate offrono sul mercato nero le risorse necessarie per impiantare un'attività di cybercrime anche senza averne le competenze informatiche. E' quindi possibile acquistare tutta una serie di prodotti o servizi di livello avanzatissimo a dei prezzi che sono davvero alla portata di qualunque tasca: un recente report di Trend Micro[19] ha portata alla luce i listini correnti nel mercato underground russo per i servizi legati al cybercrime, che per certi versi è stato "democraticizzato", ovvero messo nella disponibilità di chiunque. Se parla di 130$ per violare un account Facebook o Twitter; poco più per un account Google; appena 10$ per inviare un milione di mail di spam; dai 30 ai 70$ per noleggiare un'intera botnet per una giornata; 200 per acquistare definitivamente 2000 bot e così via. Spese tutto sommato molto modeste, nella disponibilità anche dei più piccoli risparmiatori, che potrebbero oggi ponderare l'effettiva possibilità di investire in bot...

[19] Russian Underground 101: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

E' evidente che se il controllo di un PC violato vale sul mercato nero appena 10 centesimi di dollaro, questo significa che il mercato è più che mai saturo di offerta e che l'investimento per ottenere il controllo di quel PC è a dir poco esiguo. Essendo la rete abusiva, infatti, tutto il mantenimento dell'infrastruttura della botnet è pressoché a costo zero: sono gli utenti, ignari, a pagare per il mantenimento in esercizio, per l'aggiornamento del parco macchine, per la connettività e i consumi energetici. I margini di profitto sono dunque elevatissimi.

Conclusioni

Difendersi da simili minacce richiede grandi sforzi. I primi a dover prendere immediate contromisure sono gli utenti: poiché essi sono l'obiettivo principale delle botnet, che li colpiscono direttamente in quanto deboli, ignari e mediamente sprovveduti, è indispensabile renderli consapevoli della minaccia e in grado di fronteggiarla in prima persona, attraverso la formazione e la sensibilizzazione che possono consentirgli di equipaggiarsi di strumenti tecnici e di una sana dose di diffidenza e cognizione prima di esporsi ai pericoli della Rete.

Ma tutto questo non basterà: anche se rafforzare gli utenti è irrinunciabile (poiché nel mondo della sicurezza si sa che una catena è robusta quanto il suo anello più debole), abbandonati a loro stessi contro organizzazioni efficienti e motivate non potranno arrivare lontano. Sono indispensabili delle strategie di governance che coinvolgano le istituzioni, i provider e i vendor per fronteggiare la minaccia ad un livello superiore, inaccessibile agli utenti comuni. Sono le istituzioni che possono e devono promuovere la collaborazione internazionale tra Stati, l'armonizzazione delle normative sui cybercrime e i trattati di mutua assistenza tra forze dell'ordine e magistrature di diversi Paesi al fine di reprimere i fenomeni criminali, ricercando anche le sinergie con i provider, che sono gli unici soggetti in grado di provvedere efficacemente dal punto di vista tecnico all'individuazione e all'arginazione delle minacce in corso. Si pensi a quel che accadde nel 2008 in occasione del caso McColo[20]: non fu in conseguenza di un'azione giudiziaria, ma solo grazie all'intervento degli altri provider, che il provider russo McColo venne isolato da Internet in quanto ritenuto responsabile di fornire le infrastrutture necessarie per lo spam. Il repentino calo del 75% del volume di spam mondiale fu una dimostrazione quanto mai eloquente della fondatezza dei sospetti, che non sarebbe stata possibile senza un intervento diretto e congiunto dei provider che fornivano connettività a McColo. Oggi il panorama è cambiato, le botnet sono per loro natura decentrate in tutti i paesi del mondo, ma l'apporto dei provider e dei grandi produttori continua ad essere indispensabile: le chiusure di Kelihos[21] e Waledac[22], ad esempio, si devono in gran parte all'impegno di Microsoft, mentre quando i vendor abbassano la guardia il crimine può alzare il tiro e colpire su larga scala, come nel caso di Nitol[23].

Questo è lo scenario nel quale viviamo. Non è una speculazione sul futuro, è tutto già esistente e sta accadendo anche qui e ora. E' indispensabile acquisirne consapevolezza e approntare senza ulteriori ritardi ogni contromisura utile. Forse l'istituzione di un CERT nazionale non sarà la pallottola d'argento in grado di risolvere ogni problema, ma non disporre di un simile istituto non può certo portare alcun vantaggio nella lotta alla criminalità informatica, che invece sta prosperando come non mai, pressoché incontrastata.

Pavia, 23 novembre 2012

Davide Gabrini, security farmer.

[20] https://en.wikipedia.org/wiki/McColo
[21] http://www.webnews.it/2012/01/24/kelihos-botnet/
[22] http://notebookitalia.it/microsoft-ferma-la-botnet-waledac-7760
[23] http://hackmageddon.com/2012/09/16/the-botnet-factory/