



## La polizia contro la rete di bot

Le aziende di sicurezza informatica Defence Intelligence e Panda Security rendono noto che botnet Mariposa, una vasta rete di computer infetti progettata per impadronirsi di informazioni personali, è stata smantellata dalle autorità e che tre presunti cyber-criminali accusati di controllarla sono stati arrestati dalle forze dell'ordine spagnole. Tra i dati rubati da Mariposa vi sono informazioni relative a conti bancari, carte di credito, username e password di una rete mondiale di 12.7 milioni di computer violati, appartenenti a utenti privati, aziende, agenzie governative e università di oltre 190 paesi. La rete di bot è stata disattivata il 23 dicembre 2009 grazie all'impegno congiunto di diversi esperti, agenzie e corpi di sicurezza, tra i quali Defence Intelligence, Panda Security, l'FBI e la Guardia Civil spagnola.

Con circa 13 milioni di computer colpiti, si stima che Mariposa sia una delle più grandi botnet fin qui individuate. Christopher Davis, CEO di Defence Intelligence, la prima azienda a scoprire questa rete, spiega: "Sarebbe più semplice per me fornire una lista di aziende dell'indice Fortune 1000 e indicare chi non è stato colpito da questa minaccia, piuttosto che elencare tutti coloro che sono stati attaccati".

Dopo la scoperta di Mariposa nel maggio 2009, Defence Intelligence, Panda Security e Georgia Tech Information Security Center hanno creato il Mariposa Working Group con l'obiettivo di unire le forze insieme ad altri esperti e agenzie di sicurezza di differenti paesi, per cercare di eliminare questa botnet e consegnare i criminali alla giustizia. Il principale botmaster, conosciuto come "Netkairo" e "hamlet1917", insieme ai suoi due collaboratori, "Ostiator" e "Johnyloleante" sono stati arrestati.

"Le prime analisi indicano che i botmaster non possedevano conoscenze avanzate di hacking. Questo risulta molto preoccupante in quanto dimostra quanto sia diventato efficace e sofisticato il software di diffusione del malware, che consente a criminali senza esperienza di causare danni e perdite molto significativi", sottolinea Pedro Bustamante, Senior Research Advisor di Panda Security. "Siamo molto orgogliosi dell'impegno coordinato di tutti i componenti del Mariposa Working Group e della rapidità con la quale siamo riusciti a eliminare questa importantissima rete di bot e individuarne i responsabili."

Alla fine del 2009, Mariposa Working Group è riuscito a infiltrarsi nella struttura di controllo di Mariposa e a studiare i canali di comunicazione utilizzati dai presunti botmaster, che rinviavano le informazioni dei computer colpiti ai cyber-criminali, in modo molto simile a quelli utilizzati dalle botnet Zeus, Conficker e Koobface o evidenziati di recente nelle operazioni Google/Aurora.

Dopo aver analizzato i principali server della rete, il 23 dicembre 2009 il Working Group è stato in grado di realizzare l'operazione coordinata di chiusura della rete di bot Mariposa. Panda Security è tuttora all'opera per un'analisi completa del malware e sta coordinando le comunicazioni internazionali tra le aziende specializzate in antivirus per assicurare che le loro firme siano aggiornate. Tra i principali dati emersi finora dall'analisi preliminare di Panda Security vi sono:

- Una volta colpiti dal client bot di Mariposa, il botmaster installava differenti malware (keylogger avanzati, banker trojan come Zeus, o trojan per l'accesso remoto, etc.) per poter realizzare azioni aggiuntive sui PC zombie.
- Il botmaster guadagnava denaro con la vendita di parti della rete di bot, installando toolbar e fornendo dati bancari per servizi online e carte di credito rubati per realizzare transazioni attraverso "muli" all'estero.
- La rete di bot Mariposa si è diffusa in modo molto efficace attraverso le reti peer-to-peer, le penne USB e le messengerie istantanee.

Un report sull'analisi sarà disponibile a giorni al link <http://pandalabs.pandasecurity.com>, mentre una breve descrizione del software della botnet Mariposa, conosciuto come ButterflyBot.A, è presente su <http://www.pandasecurity.com/homeusers/security-info/217587/ButterflyBot.A>.

"Ancora una volta, gli sforzi coordinati di differenti forze di polizia internazionali e della Guardia Civil spagnola, insieme alle principali aziende della sicurezza informatica, hanno permesso di affrontare la minaccia globale del cyber-crimine", commenta Juan Salom, Comandante en Jefe del Grupo de Delitos Telemáticos della Guardia Civil.

Secondo Dave Dagon, del Georgia Tech Information Security Center: "Invece di analizzare i dati con i grafici, abbiamo considerato la botnet come una vera e propria scena del crimine e non un semplice progetto di ricerca".

Mariposa Working Group ha ufficialmente preso il controllo dei canali di comunicazione utilizzati da Mariposa, escludendo dalla rete i creatori. Subito dopo la chiusura della rete in dicembre, come apparente atto di ritorsione, era stato condotto un attacco DdoS (Distributed Denial of Service) contro Defence Intelligence. L'attacco è stato così potente da colpire un grande Internet Service Provider, bloccando la connessione a molti dei suoi clienti per diverse ore.

Secondo un portavoce di CDmon, l'Internet Service Provider spagnolo che ha collaborato nelle indagini e nel quale erano allocati i domini sfruttati dai criminali, "siamo molto soddisfatti di essere stati in grado di supportare questa operazione internazionale, insieme alla Guardia Civil spagnola, a Panda Security, Defence Intelligence e ad altre forze di sicurezza per smantellare questa rete. CDmon è impegnato per fornire Internet di qualità, garantendo in tutti i nostri servizi standard elevati. Questo sforzo collaborativo rappresenta una grande vittoria nella lotta al cyber crimine." "Continueremo a combattere contro la minaccia di botnet e i criminali che vi si celano alle spalle,"

afferma Davis. “Inizieremo con lo smantellamento della loro infrastruttura e non ci fermeremo fino a quando non saranno davanti a un giudice”.

Defence Intelligence e Panda Security stanno tuttora cercando di contattare tutte le aziende attaccate dalla botnet. In caso di sospetti, ci si può rivolgere a questi indirizzi mail:

[compromise@defintel.com](mailto:compromise@defintel.com) oppure [info@pandasecurity.com](mailto:info@pandasecurity.com)