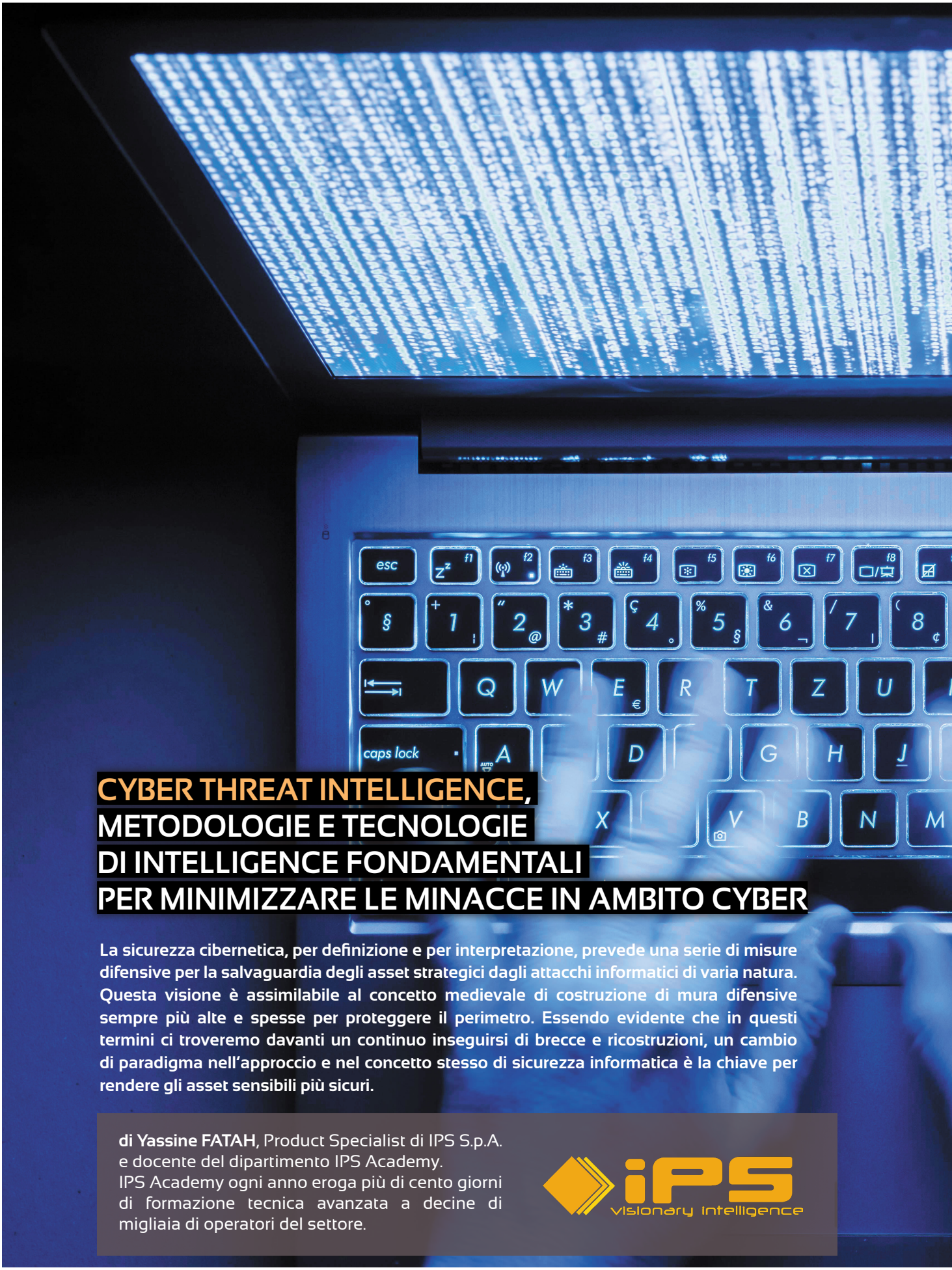

CYBER THREAT INTELLIGENCE, METODOLOGIE E TECNOLOGIE DI INTELLIGENCE FONDAMENTALI PER MINIMIZZARE LE MINACCE IN AMBITO CYBER

La sicurezza cibernetica, per definizione e per interpretazione, prevede una serie di misure difensive per la salvaguardia degli asset strategici dagli attacchi informatici di varia natura. Questa visione è assimilabile al concetto medievale di costruzione di mura difensive sempre più alte e spesse per proteggere il perimetro. Essendo evidente che in questi termini ci troveremo davanti un continuo inseguirsi di brecce e ricostruzioni, un cambio di paradigma nell'approccio e nel concetto stesso di sicurezza informatica è la chiave per rendere gli asset sensibili più sicuri.

di Yassine FATAH, Product Specialist di IPS S.p.A. e docente del dipartimento IPS Academy.
IPS Academy ogni anno eroga più di cento giorni di formazione tecnica avanzata a decine di migliaia di operatori del settore.

Rimanere passivi e ricostruire laddove vi è stata una breccia e imparare le tecniche di attacco solo dopo averle subite ha portato influenti dinastie alla rovina, durante le scorribande dei norreni prima e dei mongoli successivamente nel continente Europeo durante lo scorso millennio. Il vero approccio innovativo arrivò quando nacque il primordiale concetto di **Intelligence**. Sapere prima quando, in che modo, con quali strumenti le strutture saranno attaccate permette di prevenire e mitigare in maniera efficiente tali tentativi. Questo approccio è definito oggi dalla **Cyber Threat Intelligence**, ovvero la sistematica e continuativa scansione del web, dei social network, del dark web e dei forum alla ricerca di potenziali minacce, prima ancora che queste possano anche solo manifestarsi. Avere un team di informatori, in ambito corporate definiti analisti, che conosce la lingua dell'assaltatore, gli strumenti che utilizza, e a che ora intende perpetrare l'attacco, dimostra un approccio proattivo alla sicurezza degli asset fisici. Con gli asset digitali (che controllano anche quelli fisici) il discorso è del tutto simile. Il reparto SOC che è aggiornato near-real-time su modalità e tempi di attacchi ricevuti da organizzazioni simili può imporre e organizzare in anticipo le misure necessarie alla difesa.
La Cyber Threat Intelligence può essere disposta come attività interna all'organizzazione o può anche essere delegata ad un servizio professionale esterno. Lo scopo di questo articolo è analizzare le principali fonti informative utili alla CTI e riportare i maggiori vantaggi di un approccio interno o esterno alle attività di intelligence.

Le metodologie di raccolta dati in ottica Cyber Threat sono molteplici, ma per le aziende (più che per le istituzioni) è fondamentale che queste ricadano nel quadro della **Open Source Intelligence**. Il tema è stato trattato a più riprese, dunque in breve l'OSINT è la raccolta e l'analisi dei dati partendo da fonti pubbliche o pubblicamente condivise con lo scopo di trarne vantaggio. In questo senso l'OSINT ha lo scopo di far emergere minacce concrete o potenziali al perimetro fisico o cibernetico della realtà da proteggere. Rispetto all'approccio inquirente, cambiano le modalità e le norme, ma non la vastità del bacino di dati da analizzare e dunque la necessità di utilizzare un approccio alla ricerca supportato dalla tecnologia. Andando con ordine, analizziamo le più comuni risorse informative open che forniscono informazioni potenzialmente di valore.
La fonte probabilmente più scontata, e in un certo senso anche sopravvalutata, è il **dark web**. Sul dark web si possono trovare, sotto diverse forme, data breach, botnet, vulnerabilità e documenti classificati che, direttamente o indirettamente, possono avere a oggetto le dinamiche dell'impresa o dell'organizzazione statale per cui l'analista sta compiendo la ricerca. In un certo senso sopravvalutata in quanto sempre più di sovente le informazioni sensibili, i malware e i data breach in vendita vengono proposti in forum e social network in quanto la vendita è più veloce, più efficiente e si raggiunge una platea di possibili acquirenti maggiore. In un certo senso si è arrivati al concetto di ***cybercrime as-a-service*** per cui lo sviluppo di un malware non è finalizzato ad uno specifico attacco, ma ha uno scopo commerciale. Questo modello criminale a comparti stagni genera un livello ulteriore di difficoltà nelle attività di reverse engineering post attacco. Il modello a microservizi con vendita anonima sul dark web, sui forum e Telegram rende lo sviluppo di tecniche efficiente in quanto ogni organizzazione si specializza nel comparto dove è più funzionale rendendo inoltre la catena degli eventi molto frazionata. Vediamo ora nel dettaglio le diverse fonti di vulnerabilità e servizi offerti.

Un **data breach** che riporta le credenziali di accesso di un utente è una vulnerabilità fra le più gravi, ma anche fra le più comuni. Sovente un utente usa la email lavorativa per registrarsi a servizi per uso personale i quali, se oggetto di attacco, possono compromettere seriamente i dati personali degli utilizzatori. Difficilmente, nel corso delle varie attività anche preventive, si trovano organizzazioni senza dipendenti le cui credenziali fossero state in passato oggetto di data breach. Dalle realtà aziendali più piccole ai servizi segreti di potenze mondiali. Una volta esposte, le credenziali possono essere usate per accedere alla rete aziendale, al server mail, al portale amministrativo. Anche qualora le credenziali fossero state cambiate o il dipendente usi l'autenticazione a due fattori, le password dicono molto del loro creatore e sono spesso usate come strumento di Social Engineering. La password "giulia2203", anche se non in utilizzo perché desueta, associata al nominativo del dipendete fornisce una quantità di spunti incredibile.

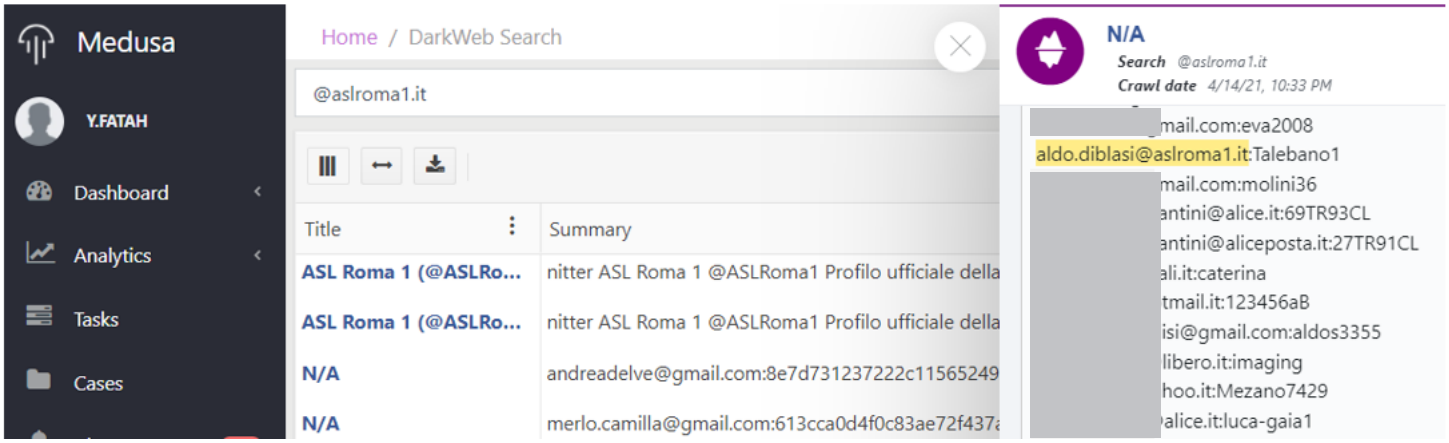

Figura 1 - Ricerca per Dominio Mail Effettuata con il sistema MEDUSA

Ne consegue che, qualcuno interessato a entrare nella rete di un'organizzazione, potrebbe utilizzare un profilo o una email finta per infettare la postazione del dipendente in smart working per far partire poi un ransomware dall'interno. La stessa password potrebbe essere usata poi come criterio di ricerca ed evidenziare altre mail collegate al dipendente oggetto di attenzioni.

Le **Botnet** sono delle reti di pc o telefoni compromessi che vengono usati per diversi motivi. Così come i data breach, si trovano in vendita nel dark web e possono essere usate con moltissimi obbiettivi in mente. Nella migliore delle ipotesi una rete di pc e smartphone infettati dallo stesso agent può contribuire alla capacità computazionali di un miner, per cui piccola parte di CPU (o APU) viene dedicata al mining di criptovalute "da remoto". Nelle peggiori delle ipotesi, le botnet possono servire per lanciare attacchi DDoS, Distrubuted Denial of Service, per bloccare gli apparati sensibili con lo scopo di mettere in difficoltà la struttura informatica di un'organizzazione. Infine esse possono contribuire ad abbassare il livello di sicurezza qualora alcuni dispositivi dell'organizzazione fossero oggetto di malware condiviso. Si parla di malware, in quanto alla base delle botnet vi è del codice malevolo, spesso Zero-day, utilizzato distributivamente senza nessun obbiettivo particolare, ma con lo scopo di infettare il maggior numero di dispositivi. Importante notare che coloro i quali realizzano il malware, non sempre coincidono con gli attori che poi lanciano gli attacchi e quasi mai le due categorie coincidono con gli utilizzatori della botnet. Le organizzazioni criminali lavorano su livelli diversi, specializzandosi nelle sezioni della catena di eventi che porta al risultato finale.

Le **vulnerabilità** sono criticità nel codice di un applicativo che possono essere sfruttate come falle per poter entrare in un sistema. Le vulnerabilità riguardano sia software proprietari che di terze parti e spesso anche di sistemi operativi. Queste si definiscono vulnerabilità Zero-day se non conosciute e sono particolarmente ricercate in quanto solitamente permettono un accesso indisturbato e relativamente più duraturo.
Questi "prodotti" vengono venduti, insieme ai documenti classificati, ai ransomware e altri servizi sul dark web. La criticità di questa fonte risiede proprio nella sua natura. Non è quasi mai possibile effettuare un acquisto certificato e si cade spesso in truffe. Per ovviare a questa problematica sono nati servizi di escrow che agiscono da intermediari fra cliente e fornitore. Si è notato come le attività sopracitate si sono spostate progressivamente verso altre fonti per qualche ragione considerate come più affidabili come Telegram e forum specializzati.
Per quanto riguarda l'app di messaggistica istantanea, gruppi e canali forniscono moltissime informazioni di rilievo. Basta infatti digitare su Google una banale concatenazione di operatori per avere accesso a un database infinito di vulnerabilità, data breach e quanto di più sensibile si stia cercando. Il lettore più curioso proverà a cercare sul motore di ricerca la stringa **site:t.me intext:"CVE"** oppure la stringa **site:t.me intext:"log4j"** e avrà subito chiara la portata del fenomeno Telegram in ottica Cybersecurity e Cyber Threat Intelligence.

I forum specializzati sul web sono molteplici, ma menzioni particolari spettano a Raidforums e Reddit. Il primo funziona da marketplace e fonte di informazioni mentre il secondo, social trasversale, viene usato come vetrina di

azioni particolari e fonte di informazione specialistica.
Infine possiamo citare Pastebin, sito che letteralmente viene usato come cestino anonimo (pastebin vuol dire appunto cestino) dove vengono depositate informazioni di valore per il pubblico dominio. Non possiede una interfaccia di ricerca vera e propria, dunque i dati sono fruibili solamente tramite operatori di ricerca. Interessante potrebbe essere dunque cercare **site:pastebin.com intext:password intext:gov**.

Questo elenco, non esaustivo, di fonti per l'analista Cyber Threat Intelligence rende chiaro come produrre il lavoro manualmente è complicato e dispendioso. Ci troviamo dunque di fronte alla necessità di rendere automatico il lavoro di estrapolazione per migliorare le capacità di valutazione e ricerca di minacce. Tali automatismi possono essere svolti in due modalità:

- utilizzando una piattaforma di Open Source Intelligence correttamente impostata per la raccolta dati mirata e fornita di opportuni strumenti di ricerca e visualizzazione grafica;
- utilizzando un servizio di consulenza esterno, ovvero una piattaforma dove l'analista dovrà solamente ricercare parametri e il lavoro di ricerca e analisi sarà fatto a monte da un team di ricercatori.

Entrambe le soluzioni hanno vantaggi e svantaggi. Probabilmente un'organizzazione privata potrebbe tendere all'utilizzo in cloud di un servizio chiavi in mano customizzato da un team di analisti esterni, mentre un'organizzazione governativa potrebbe preferire gestire in autonomia un meccanismo di raccolta dati on-premises utilizzando i propri analisti e specialisti. L'azienda inoltre, deve sempre coniugare le ragioni economiche alle normative in materia di dati personali, mentre un ente governativo ha accesso potenziale a una serie di informazioni particolari che potrebbe voler combinare con i dati open source estrapolati in ottica Cyber Threat Intelligence.
Come emerso da questo breve articolo, la difesa passiva è un modello che non può tenere il passo con le nuove sfide in campo sicurezza; nemmeno i firewall e gli antivirus sono rimasti ancorati all'approccio prettamente passivo in quanto i modelli di ultima generazione comprendono funzioni di filtro attivo delle minacce e di Machine Learning. È necessario, dunque, un modello proattivo a 360 gradi, coadiuvato da un meccanismo attivo di ricerca minacce, che analizza le fonti pubbliche e le notizie *near-real time* in maniera sistematica e automatizzata. Essere a conoscenza di attacchi perpetrati a realtà vicine può essere la chiave di volta nella difesa dinamica degli asset digitali insieme a tutte le altre misure ormai obbligatorie in materia di sicurezza informatica quali autenticazione a due fattori, formazione e sensibilizzazione dei dipendenti.
La situazione geopolitica attuale nell'est dell'Europa rispecchia molto i temi proposti in questo articolo. Le moderne tecniche di attacco cibernetico sono parte integrante e fondamentale di quella che viene definita *cyber warfare*. È stato emblematico l'attacco di Anonymous agli asset strategici russi. Si è trattato di un attacco con una combinazione di diverse tecniche, fra cui DDoS, sfruttando botnet con endpoint distribuiti in diversi paesi e attività di propaganda online. La cyber warfare è diventata così integrata nell'elaborazione delle strategie militari che ha assunto una valenza quasi deterrente. Similarmente alla potenza nucleare, il potenziale dei danni da attacchi cyber agli asset strategici quali centrali elettriche, gasdotti, ospedali e impianti militari è calcolata nel computo delle strategie di offesa e difesa, sia in tempo di pace che in tempi di conflitto. Investire in formazione, sensibilizzazione e approccio proattivo ad ogni livello può fare oggi la differenza in ottica di difesa degli asset aziendali, ma anche, come visto, in ottica di sicurezza nazionale. ©

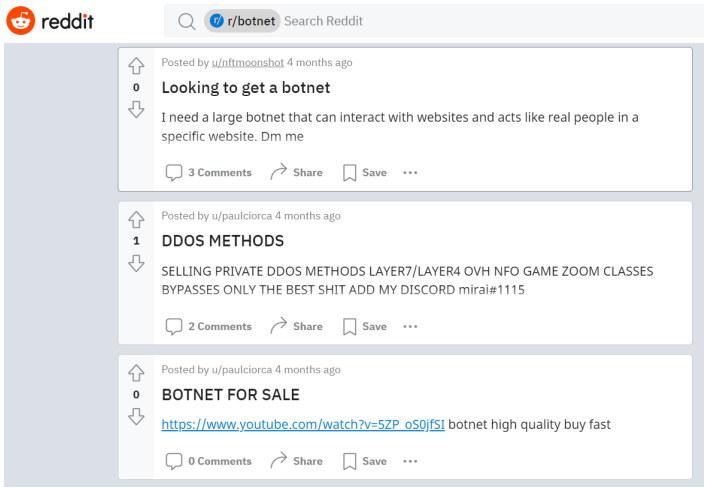

Figura 2 - Botnet in Vendita su Reddit