BRICKS | TEMA

Dai virus informatici al Coronavirus: come spiegare la necessità del distanziamento

a cura di:
Giuseppe Mastronardi

Virus e coronavirus, spoofed, misure di sicurezza covid

Dai virus informatici al Coronavirus: come spiegare la necessità del distanziamento[1]

Mai come in questo momento, caratterizzato da una pandemia che sembra difficilmente controllabile, l'analogia con i virus dei computer può risultare adeguata e utile a comprendere in modo semplificato la dinamica della vulnerabilità agli attacchi da virus.

Partiamo dalla considerazione che ogni computer collegato in rete (via Internet) risulta oggi attaccato da qualche virus, per volontà di qualche malintenzionato. La finalità è di produrre danni per diversi motivi, come perpetrare una frode informatica, sottrarre una somma di denaro su un nostro conto corrente bancario, mettere in atto una estorsione (vedi i Ransomware) con conseguente richiesta di riscatto per poter riottenere l'accesso ai propri dati, o creare panico al punto di doversi dotare di un software, acquistandolo, per la gestione della protezione dati del nostro computer o ancora affidare a un'agenzia privata il controllo e la gestione da remoto della sicurezza del nostro sistema (SOC - Security Operations Center).

Sebbene vi sia certezza dell'esistenza di un qualunque attacco, ogni computer, attraverso software specifici, può essere in grado di difendersi, riconoscendo il tipo di virus, eliminandolo e ponendo rimedio agli eventuali danni creati. Tuttavia, alcuni sistemi operativi di ultima generazione, in particolare nei server, sono già dotati di utility (funzioni) che consentono di attivare procedure di sicurezza, "anticorpi" informatici che si adattano alle diverse necessità mediante tecniche di intelligenza artificiale e algoritmi evolutivi. Queste procedure sono rappresentate dagli Intelligent IDS (Intrusion Detection Systems), sistemi intelligenti di rilevazione delle intrusioni che aiutano i sistemi ad autoproteggersi.

Ma per comprendere meglio la dinamica dell'attacco e l'analogia con i virus biologici dobbiamo fare riferimento agli attacchi DoS (Denial of Service), ovvero negazione del servizio o disabilitazione forzata di alcune funzioni vitali per il sistema. Anche da questo tipo di attacco è possibile difendersi con opportuni "vaccini" o "interferoni", procedure che impediscono ai virus rispettivamente di entrare a far danno nel sistema o sanare sul nascere e perciò con tempestività eventuali danni iniziali. Vi è un solo problema: sebbene queste procedure si attivino ed operino in modo estremamente veloce, cioè alla velocità tipica dei computer, richiedono pur sempre un minimo lasso di tempo per il loro intervento finalizzato a ridurre o eliminare la carica virale.

Ecco che i malintenzionati seri inventano il DDos, cioè il DoS Distribuito, una "rete amplificatrice" di attacco, finalizzata a una diffusione più efficace dell'attacco, andando a colpire la vittima attraverso un "burst attack", cioè una raffica di contaminazioni DoS. Per ottenere questo effetto l'attaccante si avvale della complicità di ignari utenti della rete, che fanno convergere i loro attacchi verso la medesima vittima, pur ignorando di essere stati coinvolti nell'attacco da un processo di "spoofing", cioè mediante un inganno (Fig. 1).

[1] Articolo pubblicato su "La Gazzetta del Mezzogiorno" del 22/11/2020, p. 6.

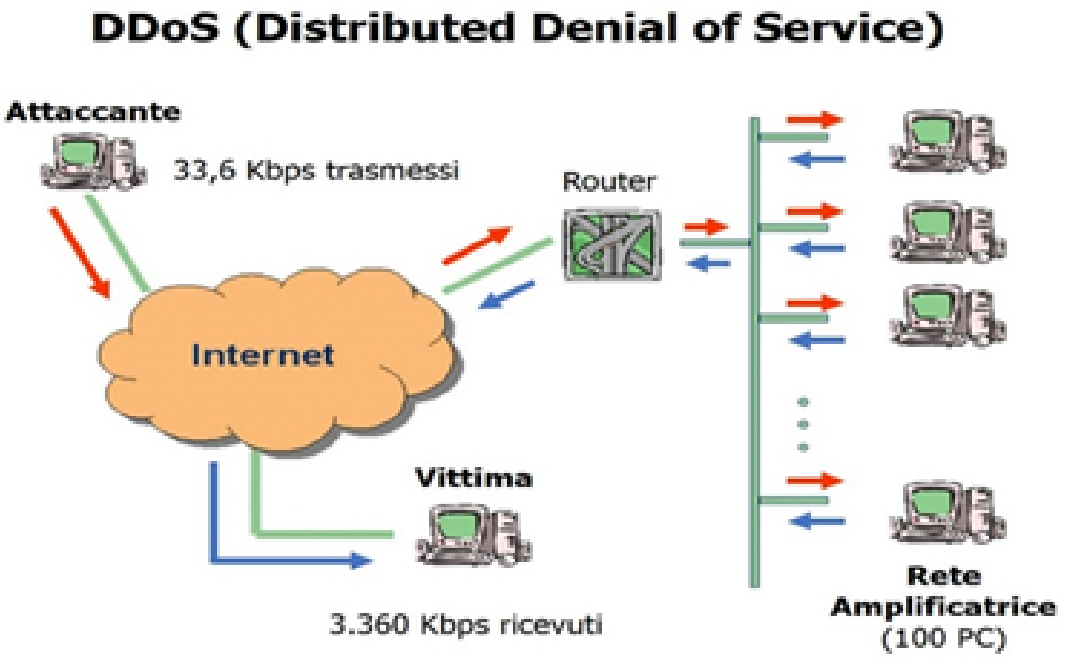

Figura 1 - Burst attack - simulazione di rete

Di fronte a un simile attacco non c'è antivirus, IDS o utility che possa avere tempo utile a soddisfare la difesa del sistema; e così l'intero sistema è compromesso. L'unica possibilità che rimane all'utente di quel computer è limitare i danni andando a disattivare il sistema quanto prima possibile. Prima lo spegne e meno danni subisce.

Nell'attuale situazione pandemica risulta importante comprendere come il potenziale di contagio da parte di più persone sia strettamente legato al concetto di **carica virale** che è rappresentata, per tutti i virus, dal numero di copie di materiale genetico virale presente in un millilitro di materiale biologico prelevato con il tampone.
Pertanto, è prevedibile che il contagio sia direttamente proporzionale alla carica virale; in altri termini maggiore è la carica virale misurata in un tampone e più "efficiente" può diventare la diffusione da parte di un singolo soggetto infettato. Ma se partiamo dal concetto che in una situazione pandemica siamo ormai tutti portatori di contagio (soggetti "spoofed"), sebbene la nostra carica virale sia molto contenuta, tanto da essere considerati esenti o quasi a un test di Coronavirus, è la **rete amplificatrice** che può fare la differenza, ottenuta dall'insieme di tanti soggetti "spoofed", anche solo con carica virale trascurabile, ma vicini alla vittima per un lasso di tempo non trascurabile; il contagio della vittima diventa in questo modo equivalente a quella di un singolo soggetto con alta carica virale a distanza ravvicinata (valutata al di sotto di 150 cm), per un lasso di tempo non trascurabile (superiore a 15 minuti, nonostante l'uso della mascherina, che porta solo a ridurre e non ad annullare la carica virale trasmessa o ricevuta).

Figura 2 - Simulazione di rete amplificatrice per la diffusione del Coronavirus

Dunque, **mascherina** per proteggere i principali varchi d'accesso alle nostre vie respiratorie, e **distanziamento** dagli altri soggetti, comunemente ignari di essere portatori di contagio, al fine di minimizzare l'effetto degli attacchi "distribuiti" dovuti agli assembramenti.

Giuseppe Mastronardi

giuseppe.mastronardi@poliba.it

AICA

Già Professore Ordinario di Sistemi di Elaborazione delle Informazioni al Politecnico di Bari ove è docente del corso di Information Systems Security and Privacy. È coautore di brevetti e software registrati, ha curato testi didattici e atti di congressi e ha pubblicato oltre 200 lavori scientifici, molti su riviste internazionali, su l'analisi e l'elaborazione di segnali e immagini per la medicina, l'industria e la sicurezza, occupandosi nell'ultimo decennio in particolare di computer ethics, tecniche biometriche e digital forensics.
Collabora dal 1978 con Procure e Tribunali italiani nell'identificazione personale mediante confronto di voci e volti, curando numerosi casi nazionali.
Fondatore e Presidente della Sezione Territoriale AICA-Puglia nel 2011, è stato Presidente nazionale di AICA per il triennio 2016-2018.