E-Mail con virus Zero Day

Ho preso un virus ma non ho fatto nulla!

Esclamazione che ho sentito molto spesso nel corso di un 2015 dove gli hacker e i cracker cercano sempre più spesso di trarre profitto dall'ingenuità altrui.

Il metodo più facile per infettare un PC è usare uno ZERO DAY, un virus che nessun antivirus può intercettare; ma come farlo arrivare a destinazione? Mi aspetto che i sistemi antispam riconoscano i mittenti malintenzionati e come tali ne scartino le mail. Bene, allora sfruttiamo i mail server "puliti" per recapitare delle email valide.

Iniziamo con il capire cosa è uno 0-DAY, wikipedia ci è di aiuto con una spiegazione semplice:

> *In informatica si definisce **0-day** qualsiasi vulnerabilità non nota e, per estensione, indica un tipo di attacco informatico che inizia nel "giorno zero", cioè nel momento in cui viene scoperta una falla di sicurezza in un sistema informatico. Questo tipo di attacco può mietere molte vittime proprio perché è lanciato quando ancora non è stata distribuita alcuna patch, e quindi i sistemi non sono ancora protetti.*
>
> *Normalmente si parla di 0-day (o zero-day) riferendosi ad essi come attività espressamente dolose compiute da cracker che si adoperano per trovarle proprio con l'intenzione di guadagnarsi un accesso abusivo ad un sistema informatico vulnerabile.*

….

> *Gli 0-day sono tra i peggiori pericoli del web, in quanto sono noti solo a una ristretta cerchia di cracker, e possono causare numerosi danni prima di essere scoperti.*

Come funziona un antivirus? I virus noti vengono censiti nelle banche dati delle aziende produttrici di software antivirus, i programmi installati sui nostri PC (o server) devono aggiornarsi costantemente al fine di avere le "signature" allineate con la banca dati centrale, questo per evitare virus messi in circolazione dalla data di ultimo aggiornamento possano infettare il sistema.

Ecco, quindi la cosa più importante, non è cosa fate con i vostri sistemi, ma quanto viene eseguito l'update delle signature.

Partendo da questo principio è logico pensare che le aziende produttrici aggiornino il database dei virus ad ogni nuova scoperta e/o segnalazione di software malevolo, bisogna poi attendere che questa informazione arrivi anche al nostro sistema.

Abbiamo quindi un lasso di tempo più o meno breve, ma utile per infettare milioni di dispositivi in giro per il mondo, se agiamo in fretta.

Preparato un virus anche banale non ci resta che metterlo in giro nel minor tempo possibile, sperando che gli utenti eseguano il software pericoloso, per fare questo dobbiamo aver preventivamente avuto accesso (manco a dirlo in modo illegale) a svariati server afflitti da vulnerabilità note per poterli usare come MAILSERVER e distribuire il nostro pacchetto.

Ed eccoci, tutto pronto, prepariamo la mail ad opera d'arte, con una buona traduzione in base alla nazione target, una contraffazione di un'azienda nota per rendere tutto meno sospetto e via, distribuzione in corso.

Ecco perché sempre più spesso vediamo nella nostra casella di posta mail che non aspettavamo, con fatture o preventivi provenienti da aziende note.

Se abbiamo dubbi sul file che ci è stato inviato, visto che il nostro antivirus non lo ha segnalato come malevolo, possiamo usare il servizio che mette a disposizione gratuitamente Virus Total:

https://www.virustotal.com/

Questo ci consente di verificare se e quale antivirus riconosce file sospetto come potenziale virus.

Anche se usiamo servizi come MAILPROTECTION facciamo attenzione ad aprire gli allegati, questo perché nonostante gli antivirus siano aggiornati con un'alta frequenza, ci sarà sempre una fascia oraria in cui ne potrà passare uno.