Malvertising: il Malware via Spot

Author : Salvatore Lombardo

Date : 24 Gennaio 2019

Il Cavallo di legno impiegato da Ulisse nel suo piano strategico per espugnare la città di Ilio è lo strumento bellico più celebre della storia. Al giorno d'oggi il termine "*Cavallo di Troia*", già adottato da tempo nel linguaggio comune, nel gergo informatico viene adoperato per indicare i sotterfugi con cui ingannare i sistemi di sicurezza e/o qualificare una tipologia di malware.

In questo articolo non tratterò però di un codice malevolo con queste caratteristiche, ma piuttosto di una strategia di attacco informatico che utilizza come Cavallo di Troia la pubblicità via web per infettare pc, portali o addirittura intere reti pubblicitarie: il cosiddetto Malvertising (*Malicious-Advertising*).

Si è portati a pensare che le semplici regole di buona pratica per individuare link improbabili, richieste di download sospette siano sufficienti a far focalizzare l'attenzione sulla possibile minaccia. Purtroppo, con il malvertising non è detto che sia necessario il coinvolgimento dell'utente. Le infezioni possono contrarsi semplicemente sfogliando pagine, guardando video on line di siti legittimi, anche loro vittime inconsapevoli.

È sufficiente uno script nascosto in un annuncio per collegare un computer a server remoti e successivamente installare un malware, senza che nessuna pagina o popup del browser venga aperto. Spesso l'utente ignaro si accorge del rischio quando ormai è troppo tardi e il software maligno ha espletato la sua azione.

Un sito legittimo può diventare un vettore malvertising a causa della prassi usuale di esternalizzare il servizio pubblicitario a terze parti, che a loro volta rivendono spazi agli inserzionisti tramite procedure automatizzate e spesso non sufficientemente controllate. Questo punto debole può essere sfruttato dagli attaccanti per inserire il proprio codice maligno.

L'attacco può avvenire:

- tramite il click su di un banner pubblicitario, in tal caso si può essere reindirizzati ad una pagina web diversa oppure può essere avviato un download;
- tramite nessun intervento consapevole da parte dell'utente (cosa più preoccupante!)

durante la consultazione del sito.

In entrambi i casi, solitamente, vengono sfruttate le falle di sicurezza dei browser e le vulnerabilità delle versioni software non aggiornate affinché:

- si possa inserire del codice dannoso su di un sito web;
- si possano compromettere annunci e banner;
- si possano far scaricare contenuti dannosi da server remoti allestiti *ad hoc*.

Gli strumenti per il contagio

Il javascript è uno dei linguaggi di programmazione usati per creare contenuti web. Le pagine web in formato html possono essere rese dinamiche anche grazie all'uso di codice javascript innestato attraverso i tag dedicati (e). Il motivo che rende appetibile ai criminali questo linguaggio è che la sua computazione avviene in locale, direttamente sul client e che è supportato da tutti i browser senza l'utilizzo di alcun plug-in aggiuntivo. La peculiarità di questo codice sta nel fatto che viene eseguito tramite l'accadimento di certi eventi, quali per l'appunto quelli particolarmente adatti per il malvertising:

- il click del mouse in un certo punto;
- l'apertura di una pagina web.

Per uso esclusivamente didattico, di seguito riporto alcuni pezzi di codice javascript che potrebbero essere utili allo scopo:

Codice che chiama ed esegue script da un sito [1]

Codice che reindirizza il browser a un altro sito [2]

```
 if (document.referrer.match(sitolegittimo.xx
))   {window.location("http://sitomalevolo");}
```

Codice per realizzare un popup [3]

```
  var stile = "top=10, left=10, width=250, height=200, status=no, menu
bar=no, toolbar=no sc
rollbars=no";  window.open("http://sitomalevolo", "", stile);
```

Codice per realizzare un banner [4]

var banner_pic = new Array() banner_pic[0] = “pic0.jpg” banner_pic[1] = “pic1.jpg” banner_pic[2] = “pic2.jpg” var banner_url = new Array() banner_url[0] = “**http://sitomalevolo0**” banner_url[1] = “**http://sitomalevolo1**” banner_url[2] =“**http://sitomalevolo2**” var num = Math.floor(Math.random()*banner_pic.length) document.write(‘