Ursnif, il malware più diffuso in Italia che mette a rischio i conti online

Il trojan bancario **Ursnif**, scoperto nell'estate 2018 si è diffuso in questi anni attraverso diverse campagne malspam sfruttando temi di vario genere ed ispirati a situazioni e/o eventi contemporanei. Questo tipo di malware finalizzato alla sottrazione di credenziali relative a servizi di home banking, continua purtroppo a rappresentare una reale minaccia che riappare periodicamente sfruttando sempre strategie diverse.

Non a caso secondo il recente rapporto di Check Point Research (Global Threat Index 05/2020) questo malware è entrato per la prima volta nella top 10 delle minacce rilevate, posizionandosi al quinto posto a livello globale.

Nello specifico in Italia, nel mese di maggio Ursnif si è piazzato al primo posto registrando un impatto sulle organizzazioni di oltre il 14% (contro una media mondiale del 2%).

A confermare ulteriormente questo trend ci sono anche gli ultimi comunicati del CSIRT che allertano riguardo a diverse nuove campagne malspam ancora attive e che coinvolgono specificatamente utenze italiane.

Ursnif – Prima campagna malspam

Nella prima campagna segnalata, un massiccio invio di email invita gli utenti ad aprire una falsa fattura, un file Excel denominato "fattura_38.xls" che, contenendo una macro di tipo Excel4, in realtà si occupa, una volta aperto, di scaricare da

un server di controllo remoto un eseguibile malevolo (“fattura.exe”).

Ursnif – Seconda campagna malspam

L’altra campagna osservata, sempre finalizzata alla diffusione di Ursnif tramite presunte fatture, invita i destinatari a scaricare, fornendo anche delle credenziali di accesso ad un sito web proposto (hxxp://attenzione.hazlotumismapr[.]com/), un file di archivio compresso in cui sarebbe contenuto un ordine di acquisto ma che si rivela essere anche in questo caso un file eseguibile (“pagament1.exe”) che installa il trojan bancario.

Ursnif – Terza campagna malspam

L’ultima campagna malspam osservata, secondo il solito rituale e facendo riferimento ad un ordine di pagamento con codice specifico identificativo, invita i destinatari ad aprire ancora un allegato Excel (“pagamento_722.xls”) ma questa volta contenente una macro malevola di tipo VBA (Visual Basic Application). Qualora si concedesse il permesso ad eseguire la macro, il payload Ursnif verrebbe scaricato attraverso l’esecuzione di uno script Powershell.

Conclusioni

Come dimostrato anche da queste ultime campagne rilevate dal CSIRT, poiché il trojan bancario noto con il come di Ursnif o Gozi, si diffonde prevalentemente tramite messaggi di posta elettronica ed allegati sfruttando quelle abili tecniche di ingegneria sociale usualmente adoperate negli attacchi di phishing, per mitigare il rischio di subirne un'infezione occorre, oltre che dotarsi di un antivirus attendibile e sempre aggiornato, prestare la massima attenzione:

- alla lettura dei messaggi email e dei file che si ricevono;
- nel visitare siti web verosimili ed improbabili.

Imparare a saper interpretare in modo corretto la struttura della nomenclatura di un file, di un indirizzo WEB o di posta elettronica deve diventare un must che bisogna assolutamente perseguire, prendendo responsabilmente coscienza che dietro ad ognuno di questi elementi potrebbe celarsi una trappola informatica.

https://www.key4biz.it/ursnif-il-malware-piu-diffuso-in-italia-che-mette-a-rischio-i-conti-online/310763/