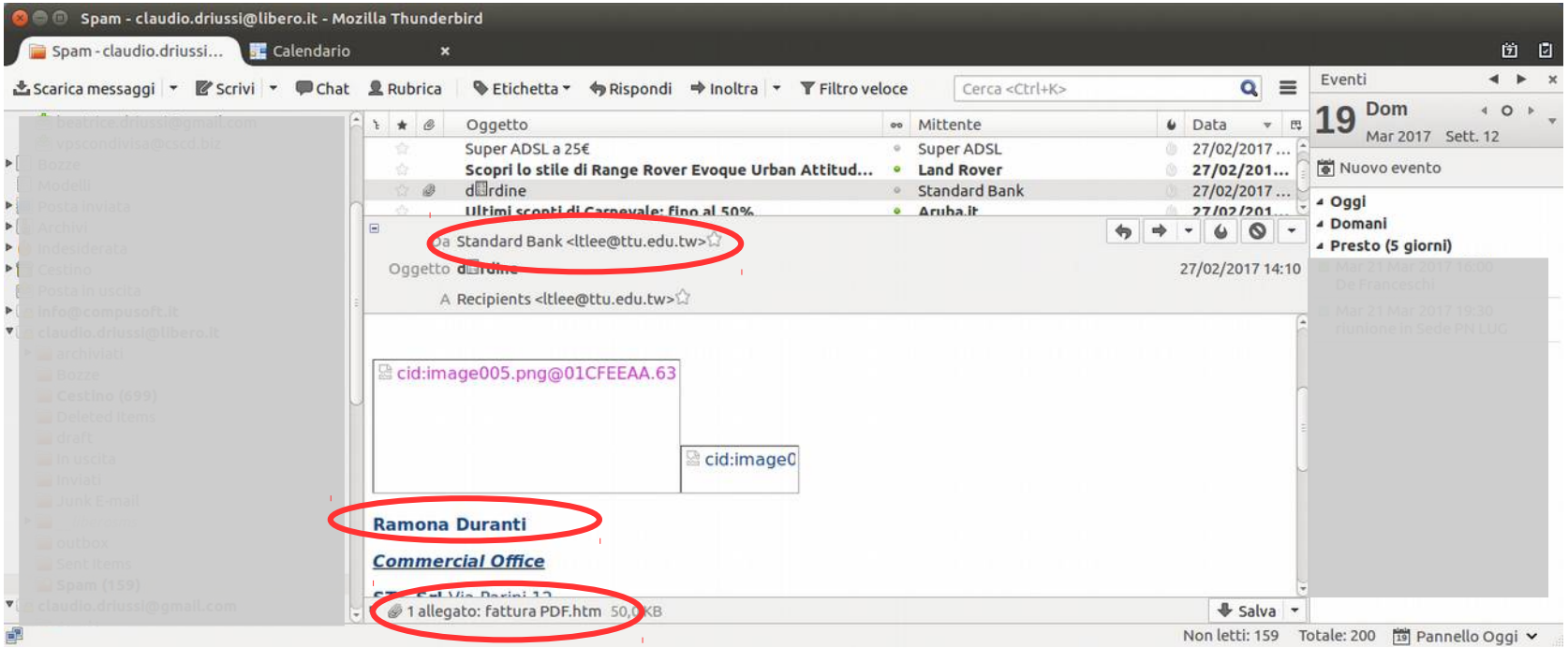
ANATOMIA DI UN VIRUS
by
Compusoft di Claudio Driussi

LA POSTA INDESIDERATA

Tutti noi riceviamo molta spam
spesso sono solo comunicazioni commerciali
che abbiamo autorizzato anche senza saperlo
a volte invece contengono insidie pericolose

IL PRINCIPALE VEICOLO PER I VIRUS SONO LE E-MAIL



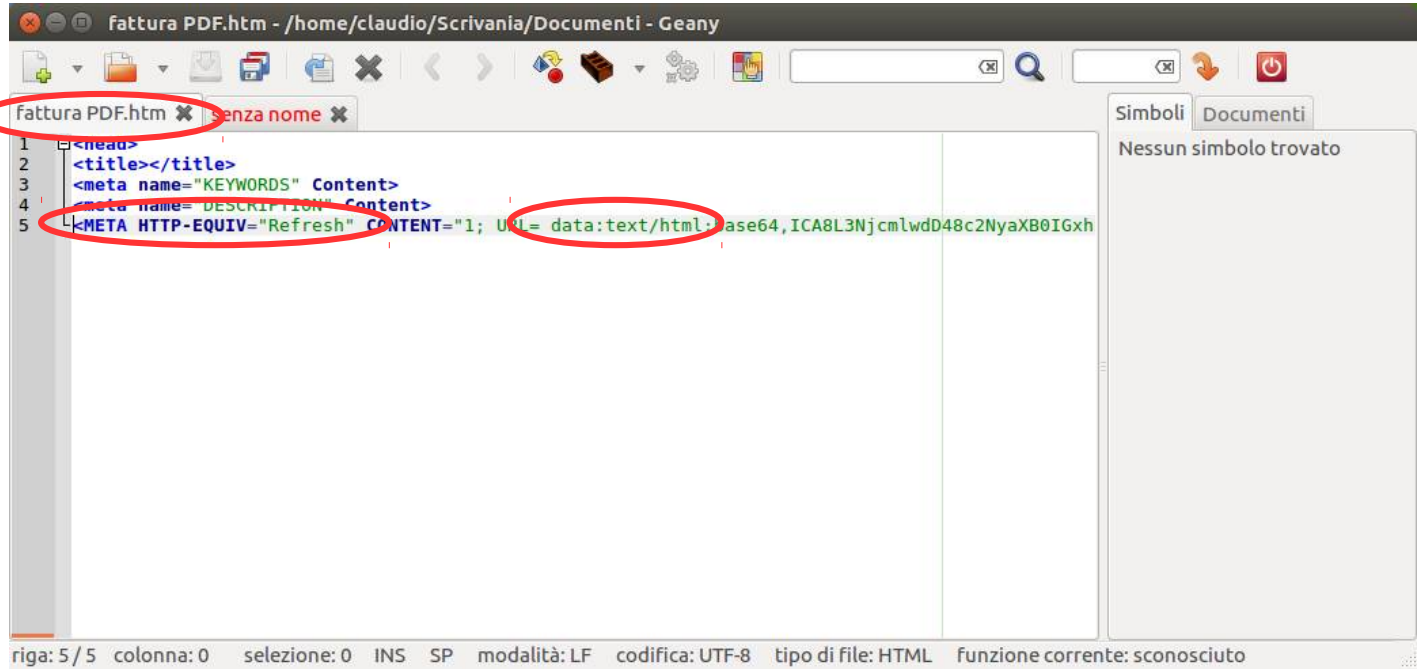
I VIRUS CERCANO DI INGANNARCI

Per carpire la nostra fiducia fanno finta di essere persone che conosciamo, possono farlo perché quando rubano le e-mail rubano anche le rubriche e quindi le relazioni che intratteniamo.

Gli allegati fingono di essere quello che non sono. Dicono di essere un PDF ed invece sono un programma eseguibile o un formato che esegue script come ad esempio un foglio di calcolo o una pagina html.

Il nome di chi spedisce è la persona che conosciamo ma l'indirizzo e-mail del mittente è diverso.

QUESTO VIRUS
FA FINTA DI ESSERE UN PDF



Compusoft di Claudio Driussi – http://compusoft.it

In ambiente Windows le estensioni dei files vengono nascoste per impostazione predefinita

Un file che si chiama **fattura PDF.htm** viene visto come **fattura PDF**

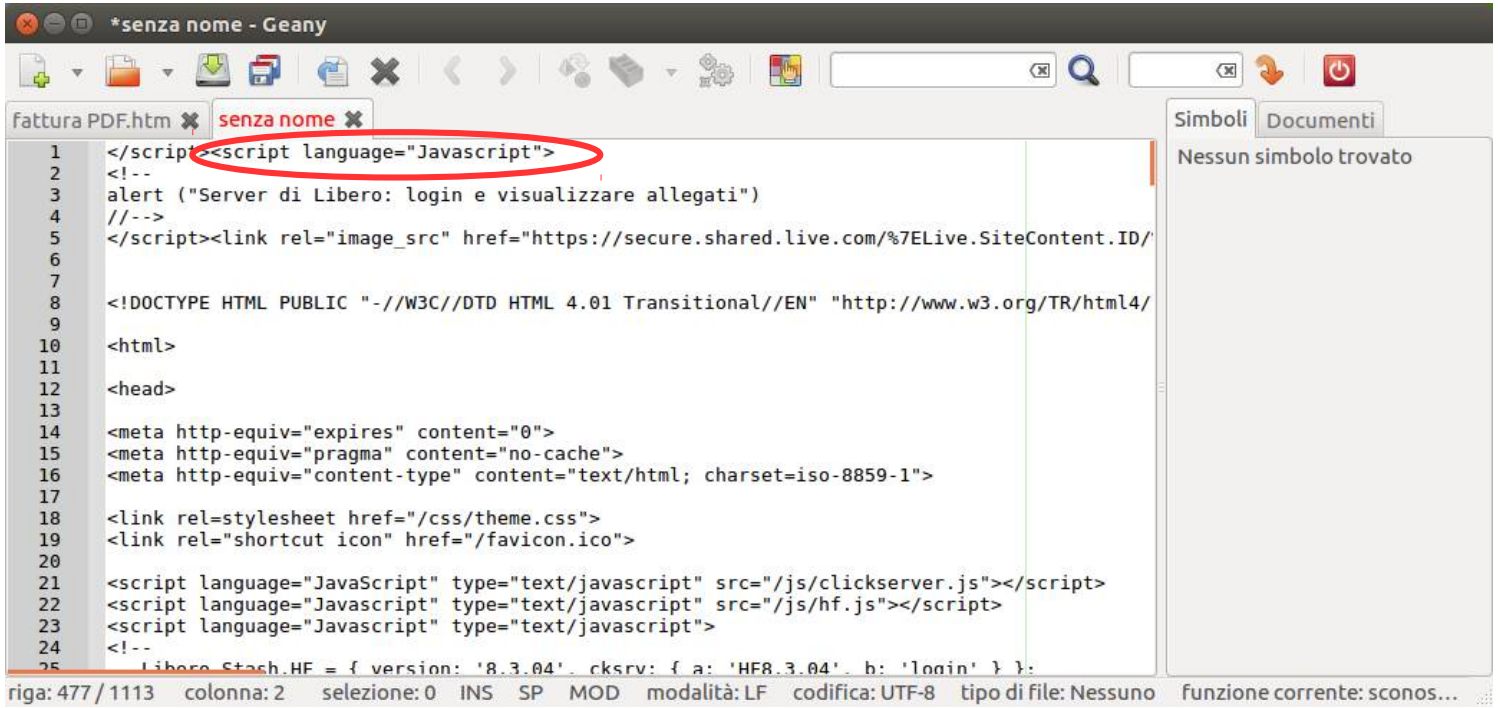
I files html hanno comandi per far partire automaticamente comandi, nel nostro caso parte una pagina codificata nel formato base64

Se scompattiamo il contenuto del comando refresh con un servizio on-line di traduzione da base64 come ad esempio:

https://www.base64decode.org/

Otteniamo il seguente risultato:

LA PAGINA DECODIFICATA FA PARTIRE UN JAVASCRIPT

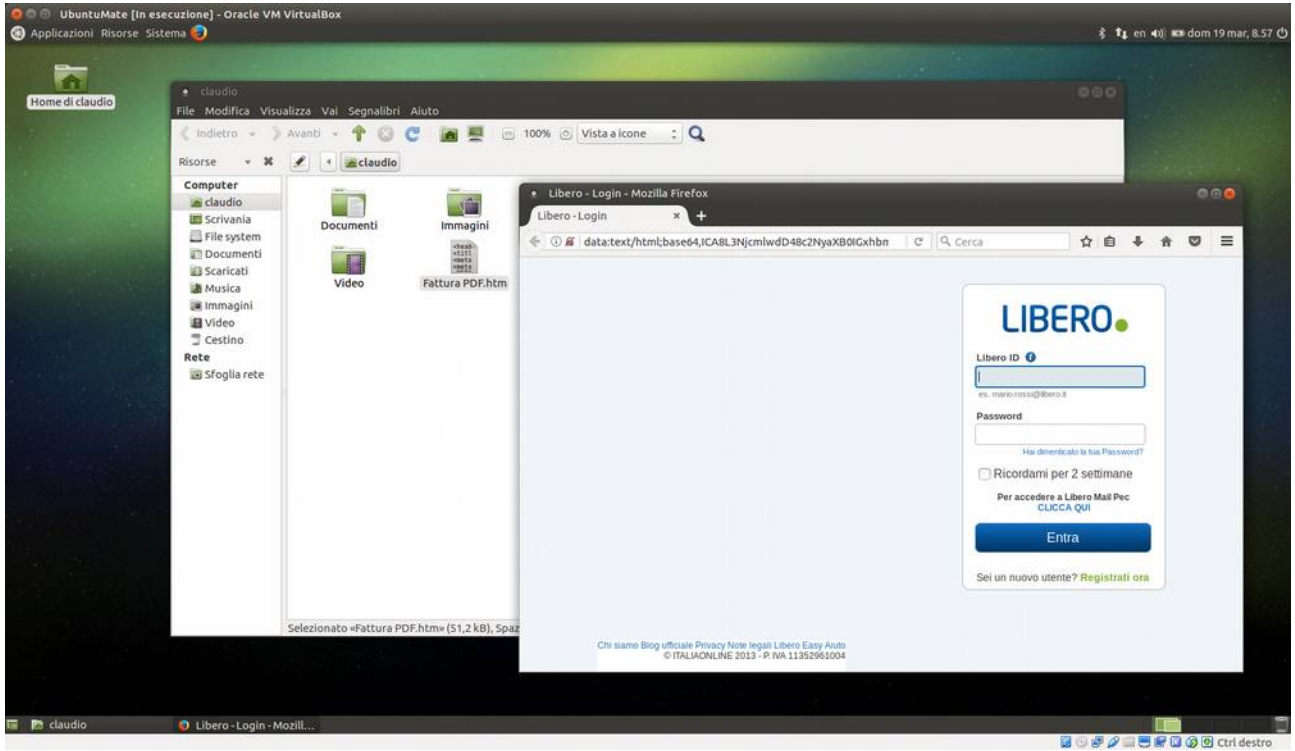


Se salviamo il file sul nostro desktop Windows convinti e poi facciamo doppio click pensando di aprire un PDF, in realtà apriamo una pagina web che lancia uno script che tenta un attacco alla posta di libero.it

Ho voluto provare a lanciare il virus, ma per evitare rischi ho avviato la pagina da una macchina virtuale Linux Ubuntu Mate senza alcuna credenziale.

Come si può vedere nella pagina seguente il virus ha tentato di aprire la mail di libero.it ma non è riuscito a proseguire perché non avevo attivato le credenziali e non avevo richiesto al sito di libero di ricordare le mie credenziali.

Il risultato lo troviamo nella pagina seguente, non ho consentito l'accesso al virus e quindi non so esattamente che cosa fa, ma presumo che rubi credenziali e rubrica.


UbuntuMate [In esecuzione] - Oracle VM VirtualBox
Applicazioni Risorse Sistema
dom 19 mar, 8.57
Home di claudio
claudio
File Modifica Visualizza Vai Segnalibri Aiuto
Indietro Avanti 100% Vista a icone
Risorse claudio
Computer
claudio
Scrivania
File system
Documenti
Scaricati
Musica
Immagini
Video
Cestino
Rete
Sfoglia rete
Documenti
Immagini
Video
Fattura PDF.htm
Selezionato «Fattura PDF.htm» (51,2 kB), Spaz
Libero - Login - Mozilla Firefox
Libero - Login
data:text/html;base64,ICA8L3NjcmlwdD48c2NyaXB0IGxhbn
Cerca
LIBERO.
Libero ID
es. mario.rossi@libero.it
Password
Hai dimenticato la tua Password?
Ricordami per 2 settimane
Per accedere a Libero Mail Pec
CLICCA QUI
Entra
Sei un nuovo utente? Registrati ora
Chi siamo Blog ufficiale Privacy Note legali Libero Easy Aiuto
© ITALIAONLINE 2013 - P. IVA 11352961004
claudio
Libero - Login - Mozill...
Ctrl destro

Chi produce virus tenta di ingannarci, ma con qualche piccolo accorgimento ci possiamo difendere.

Non importa quanto è potente il nostro antivirus, la cosa più importante è la nostra attenzione alla origine delle minacce.

E’ buona norma essere in grado di conoscere esattamente il tipo di file che scarichiamo, andandone a vedere le proprietà o abilitando la visualizzazione dei tipi.

Il programma di posta Mozilla Thunderbird è chiaro nel mostrare l’origine delle informazioni, non so se MS Outlook lo è altrettanto

Domande?

Potete contattarmi:
info@compusoft.it