

[Home](#) » [Wikileaks](#)

## Wikileaks: un nuovo pretesto per sferrare attacchi informatici

16/12/2010 | a cura di [Redazione Data Manager Online](#)

AUDIO



Le previsioni e i consigli di Cyberoam per proteggersi da minacce incombenti

Alla luce degli sviluppi della controversa questione Wikileaks, lo specialista della sicurezza Cyberoam anticipa quelli che saranno i prossimi pericoli provenienti dai cyber criminali che, nel tentativo di imitare Wikileaks, tenteranno di colpire gli utenti internet con azioni legate a phishing, malware e molto altro ancora.

Non vi è mai stata così tanta attenzione riversata sul tema della libertà di espressione come di recente. L'arresto ufficiale del fondatore di Wikileaks, Julian Assange, ha già portato a una guerra di parole senza precedenti e a cyber-attacchi reciproci tra hacker attivisti e governo/aziende.

Attualmente, se si dovesse cogliere il sentimento comune di una moltitudine crescente di sostenitori di Wikileaks, si scoprirebbe che questi sarebbero più che favorevoli a donare denaro per mantenere vivo il proprio sito preferito.

Questo contesto offre un terreno più che fertile ai cyber criminali intenzionati a cavalcare l'onda Wikileaks per colpire vittime ignare attraverso spam, e-mail fraudolente, attacchi di phishing e altro.

Gli internauti devono pertanto essere sempre più cauti nell'affrontare una qualsiasi comunicazione proveniente da un sito web. Di seguito tre importanti consigli su come proteggersi da queste truffe.

Attenzione alle richieste di "donazione": il giro di vite di VISA, Mastercard e dei sistemi di pagamento online come Paypal per il trasferimento di fondi a Wikileaks aumenta la possibilità di e-mail fraudolente che richiedono di inviare denaro ad "agenti" anonimi che lavorano a favore del sito.

I truffatori traggono vantaggio dal fatto che i sistemi di pagamento hanno già creato blacklist di beneficiari di Wikileaks e ciò fornisce una ragione in più agli aspiranti donatori per fidarsi di questi "agenti" anonimi. Queste e-mail fraudolente possono rispecchiare in maniera precisa sia il layout di Wikileaks sia i contatti delle persone chiave associate al sito.

Non cliccare su link sospetti: alcuni dei link presenti in messaggi di spam possono installare malware sul computer dell'utente o dirottare le sessioni del browser con funzionalità rootkit. Andare incontro a rallentamenti, riavvii frequenti e sparizioni di file solo perché si voleva sperimentare il lato divertente di Wikileaks non è proprio un affare!

### Speciale cloud

Sponsor

[Approfondimenti](#)

[News dal mercato](#)

[Vision](#)

### Tags Cloud

accordo commerciale acquisizione Cisco cloud computing cybercrime data center EMC Facebook Google hacker ibm iPad iPhone Kaspersky Lab malware Microsoft mobile nomina partnership Pie Macri risultati finanziari sicurezza sicure informatica smartphone social network software storage virtualizzazione

[more](#)

### Users contents

#### Cloud Money

di [victor](#)

VOTO:

#### L'Agenzia per l'innovazione sceglie ePart come progetto innovativo

di [posytron](#)

VOTO:

Attenzione agli attacchi provenienti da social network: i siti di social networking come Facebook, LinkedIn, ecc. prosperano basandosi sul concetto di fiducia che gli utenti attribuiscono al network e questo li trasforma in terreno fertile per i malware. Inoltre, i cyber criminali sono sempre più abili nello sfruttare i social network per sedurre gli utenti e convincerli a cliccare e installare applicazioni indesiderate sfuggendo al radar degli investigatori che si occupano della sicurezza.

Voto medio:

Awesome

Il tuo voto: Nessuno Media: 5 (1 vote)

Vota

  [Login](#) o [registrati](#) per inviare commenti

## Tags:

[attacco informatico](#) [cybercrime](#) [Cyberoam](#) [hacker](#) [malware](#) [phishing](#) [Wikileaks](#)  
[Sicurezza](#)

## Naviga:

[HOME](#)

[NEWS](#)

[COMMUNITY](#)

[RASSEGNA WEB](#)

[LA RIVISTA](#)

[WHITE PAPERS](#)

[ADV](#)

[CALENDARIO EVENTI](#)

[NEWS DALLE AZIENDE](#)

[NEWSLETTER](#)

[CORSI DI INFORMATICA](#)

[PRIVACY](#)

[APPUNTI UNIVERSITÀ](#)

Data Manager - 20149 Milano - Via L.B. Alberti, 10

tel. ++39 02 33101836 - fax ++39 02 3450749 - email:info@datamanager.it

Copyright © 2008. Fratelli Pini Editori S.r.l.

PI: 11803500153 - Cap. Soc. Euro 42.000,00 i.v. - Cod. Fisc. N. Iscr. CCIAA di Milano 00368320131 - Rea N. MI/824378 - Tutti i diritti riservati

Credits: Sviluppo siti web