Come aggirare i sistemi a doppia autenticazione (phishing-ng)

Gianfranco Ciotti – gciotti@enforcer.it
Igor Falcomatà – ifalcomata@enforcer.it

$ whoami

$ whoareus
ksh: whoareus: not found

Disclaimer

Please, try this (only) at home!

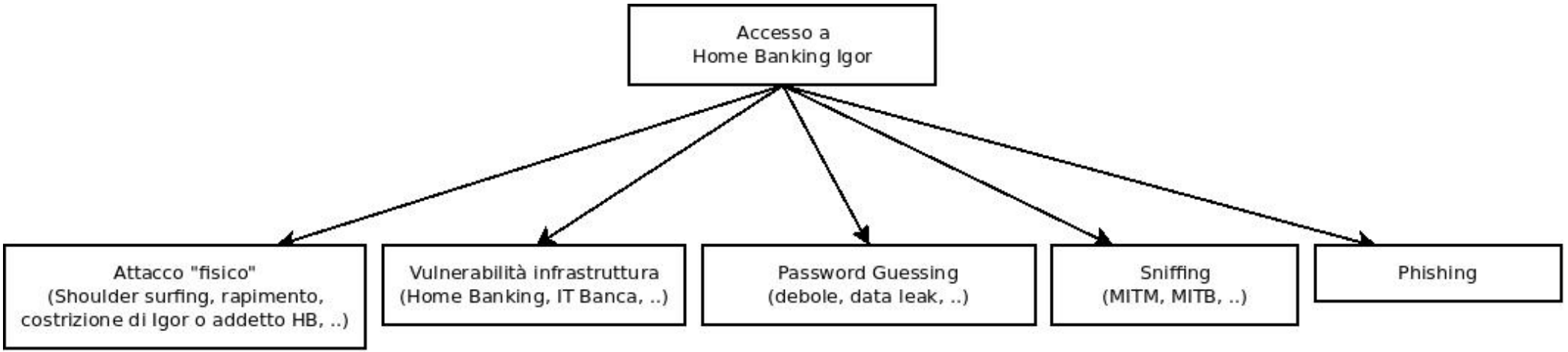
Criminal Intent

Accesso all'home banking di Igor

Criminal Intent

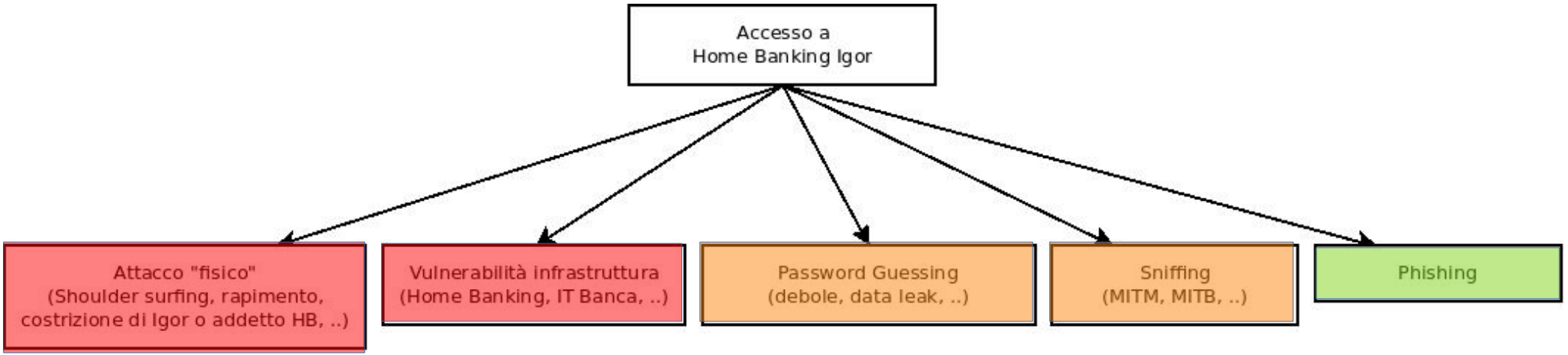
https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Criminal Intent



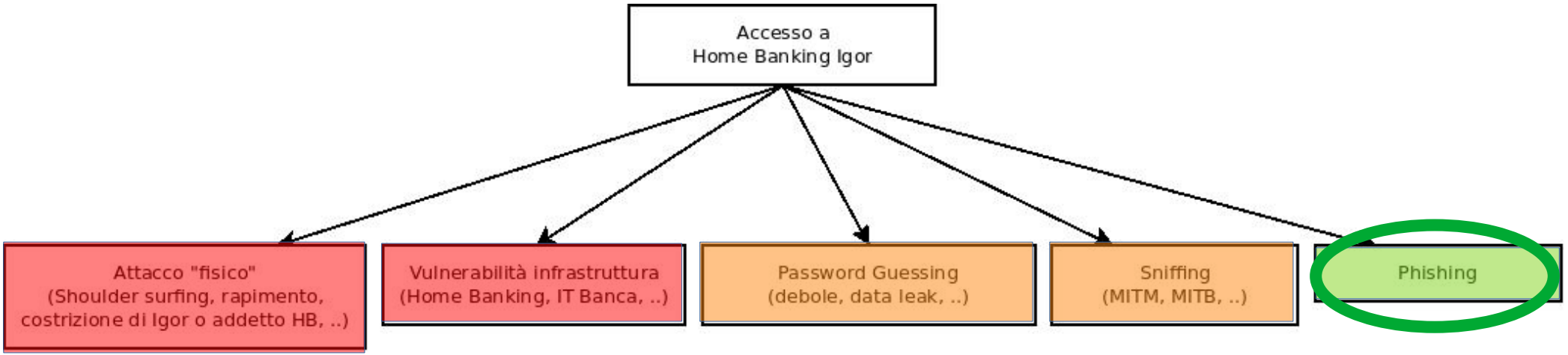
https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Criminal Intent



https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Go phishing!



https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Phishing

Phishing

← **Tweet**

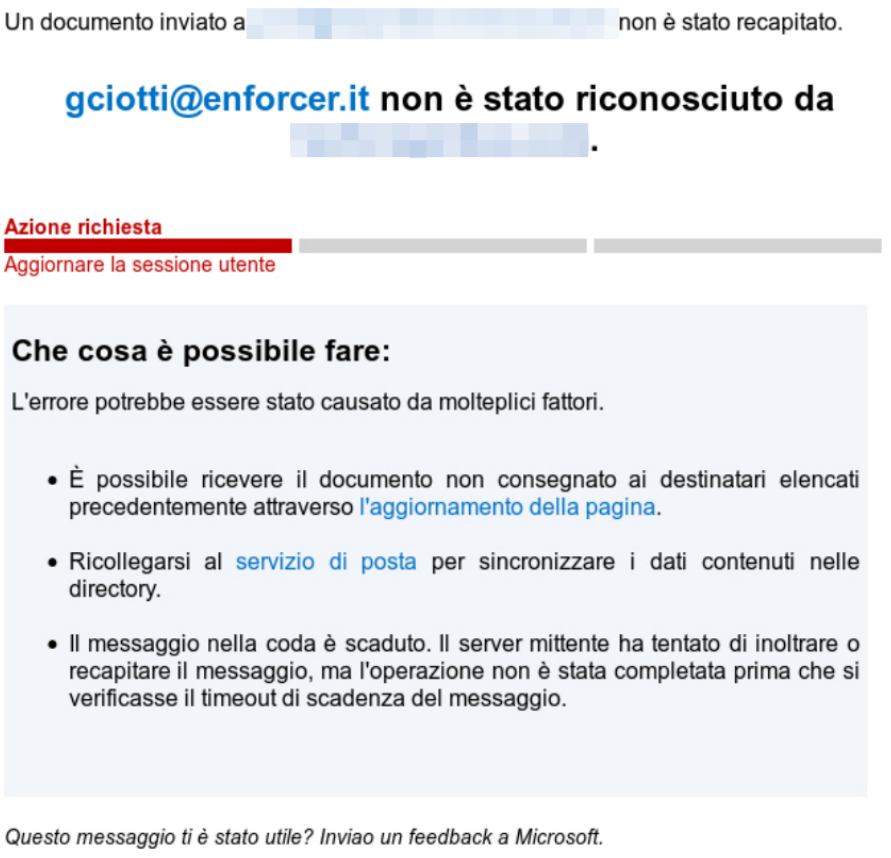
thaddeus e. grugq
@thegrugq

Give a man an 0day and he'll have access for a day, teach a man to phish and he'll have access for life.

8:35 AM · Feb 7, 2015 · Tweetbot for iOS

5.2K Retweets **7.6K** Likes

Phishing



Un documento inviato a [redacted] non è stato recapitato.

gciotti@enforcer.it non è stato riconosciuto da [redacted].

Azione richiesta

Aggiornare la sessione utente

Che cosa è possibile fare:

L'errore potrebbe essere stato causato da molteplici fattori.

- È possibile ricevere il documento non consegnato ai destinatari elencati precedentemente attraverso l'aggiornamento della pagina.
- Ricollegarsi al servizio di posta per sincronizzare i dati contenuti nelle directory.
- Il messaggio nella coda è scaduto. Il server mittente ha tentato di inoltrare o recapitare il messaggio, ma l'operazione non è stata completata prima che si verificasse il timeout di scadenza del messaggio.

Questo messaggio ti è stato utile? Inviao un feedback a Microsoft.

Phishing

Un documento inviato a [redacted] non è stato rec

gciotti@enforcer.it non è stato riconosciut[redacted].

Azione richiesta

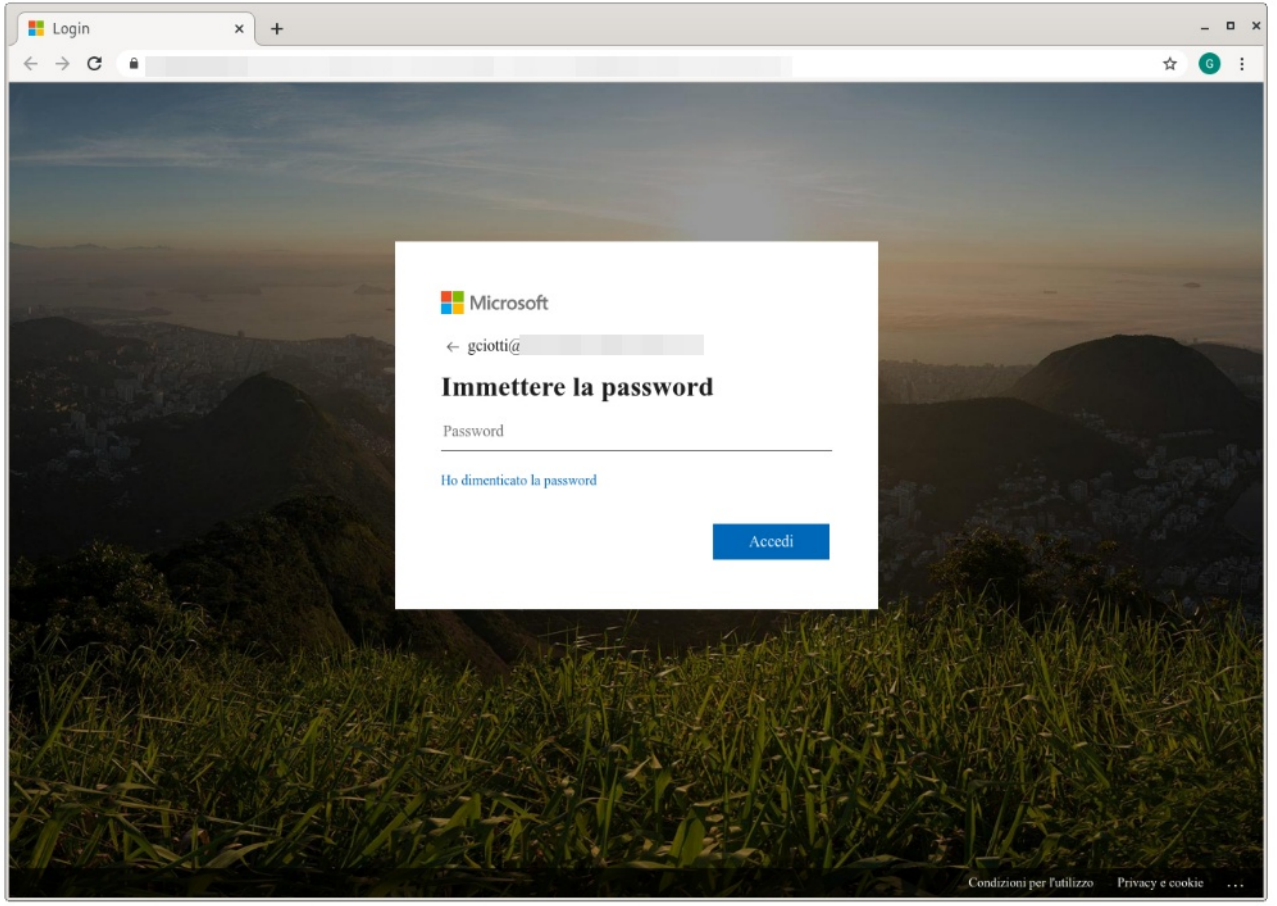
Aggiornare la sessione utente

Che cosa è possibile fare:

L'errore potrebbe essere stato causato da molteplici fattori.

- È possibile ricevere il documento non consegnato ai destinatari precedentemente attraverso l'aggiornamento della pagina.
- Ricollegarsi al servizio di posta per sincronizzare i dati conten directory.
- Il messaggio nella coda è scaduto. Il server mittente ha tentato di ir recapitare il messaggio, ma l'operazione non è stata completata prin verificasse il timeout di scadenza del messaggio.

Questo messaggio ti è stato utile? Inviao un feedback a Microsoft.



Phishing

Un documento inviato a [redacted] non è stato rec

gciotti@enforcer.it non è stato riconosciut[redacted].

Azione richiesta

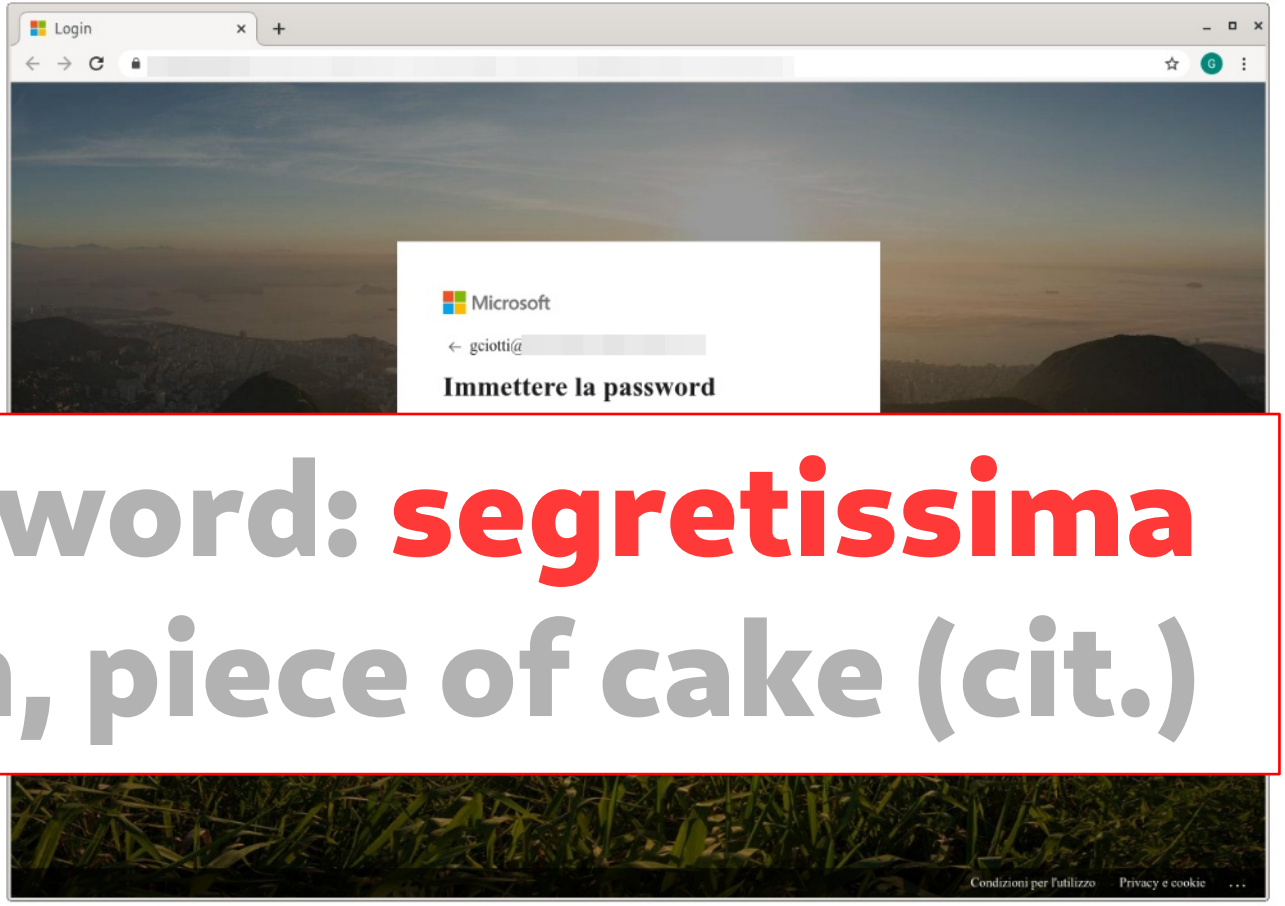
Aggiornare la sessione utente

Che cosa è possibile fare:

L'errore potrebbe essere stato causato da molteplici fattori.

- È possibile ricevere il docume precedentemente attraverso l'ag
- Ricollegarsi al servizio di pos directory.
- Il messaggio nella coda è scad recapitare il messaggio, ma l'op verificasse il timeout di scadenz

Questo messaggio ti è stato utile? Inviao un feedback a Microsoft.



Password: segretissima

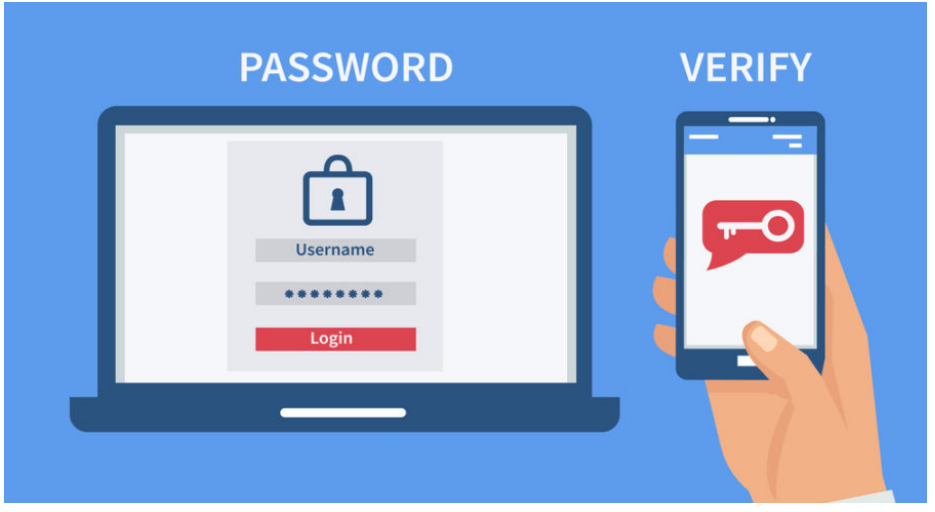
Yeah, piece of cake (cit.)

“Ho la soluzione (cit.)”

2FA (Autenticazione a due fattori) o MFA

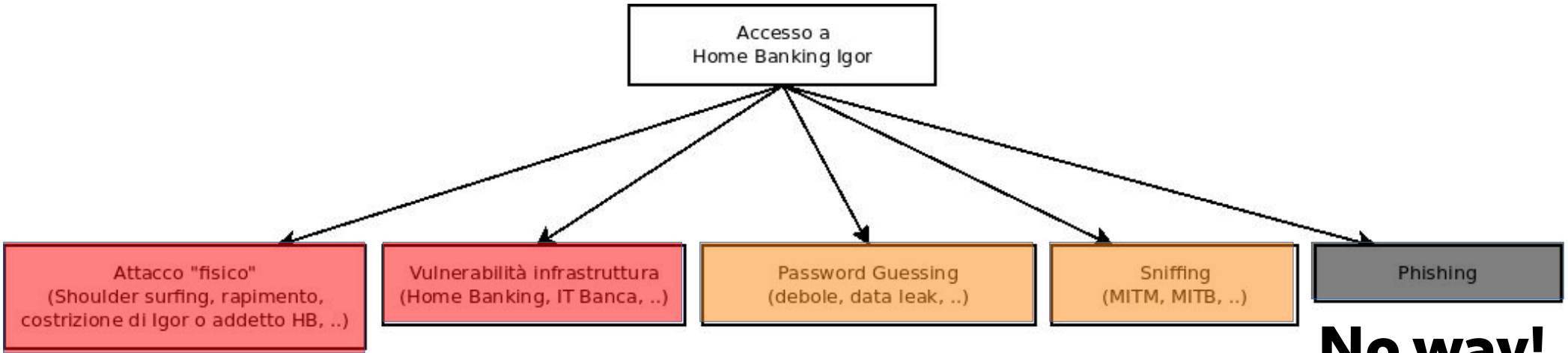
Token HW

Soft token, app, ..



Smart Card

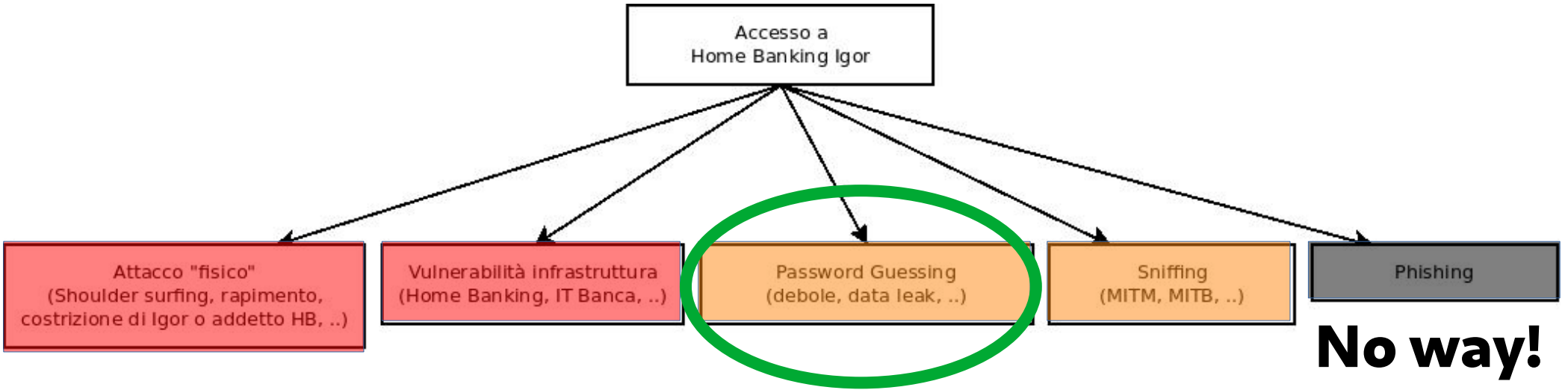
Ripensiamoci..



No way!

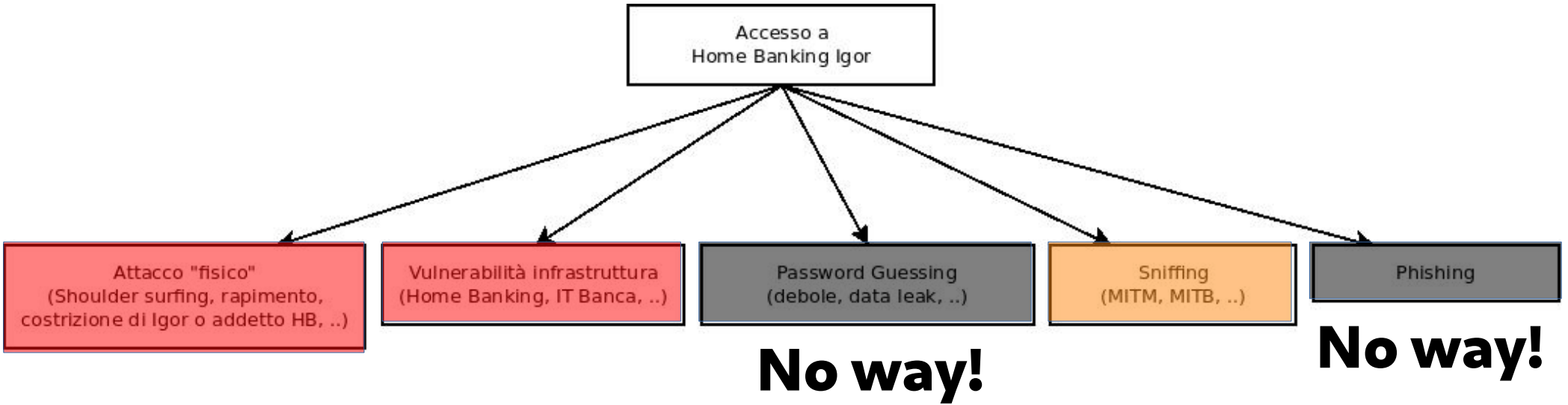
https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Ripensiamoci..



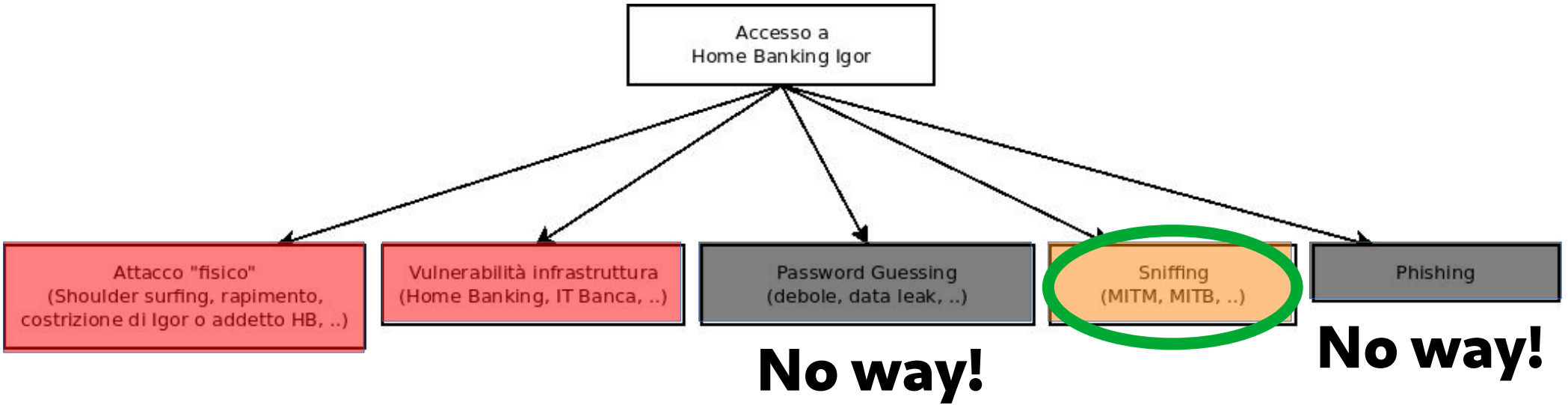
https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Ripensiamoci..



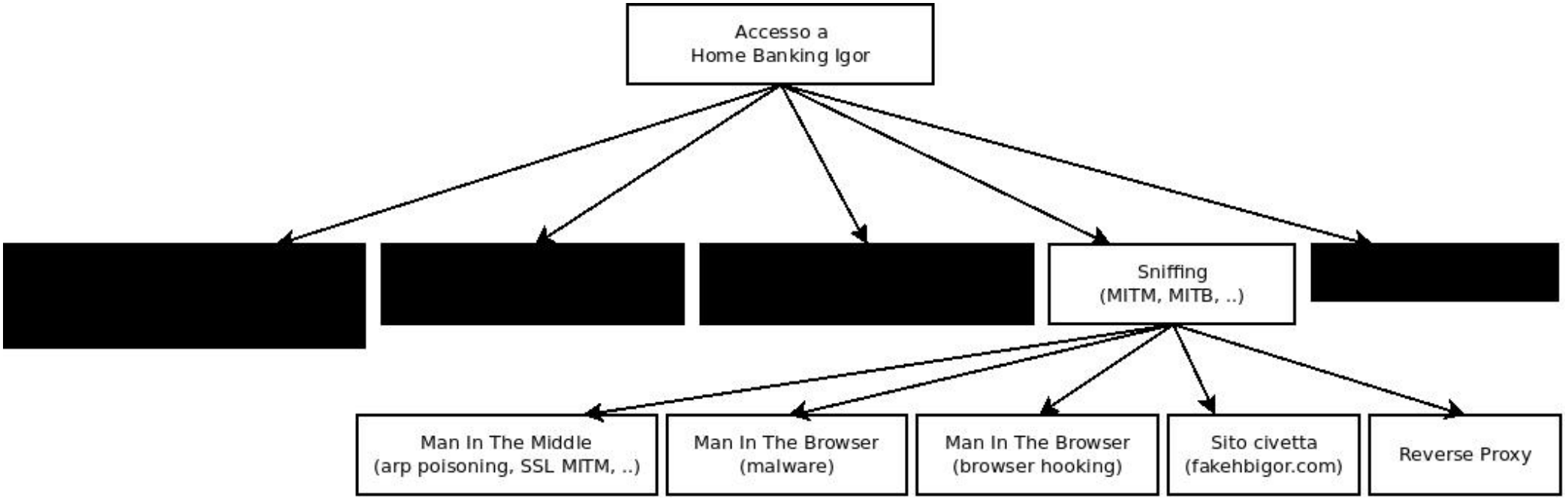
https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Ripensiamoci..



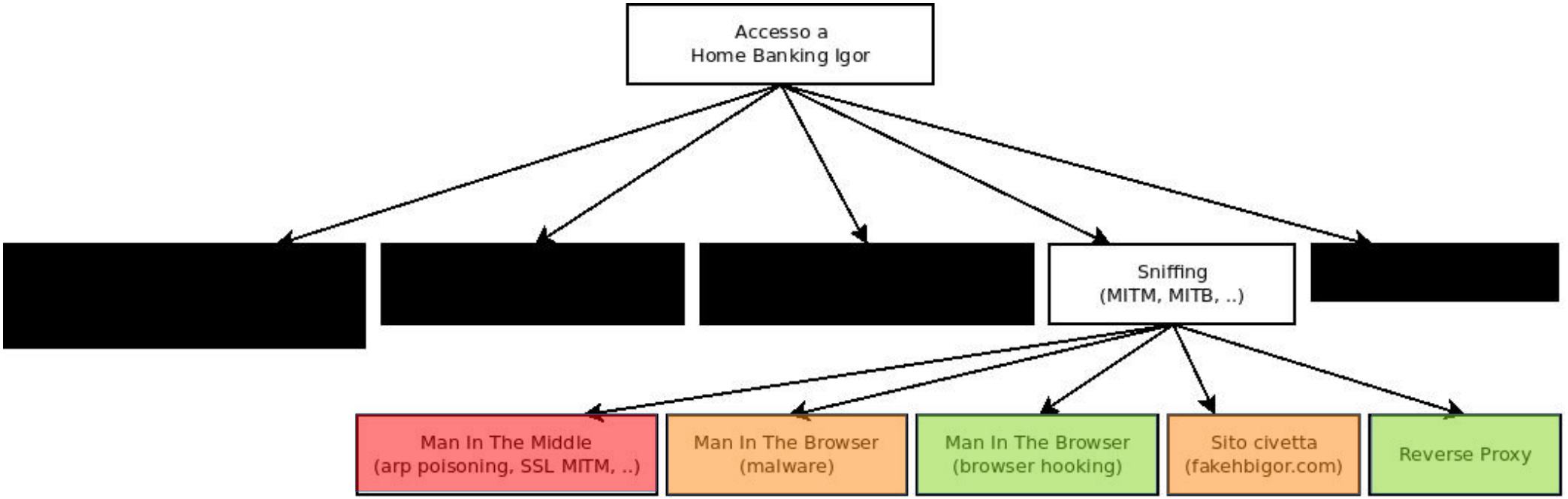
https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Attack Tree



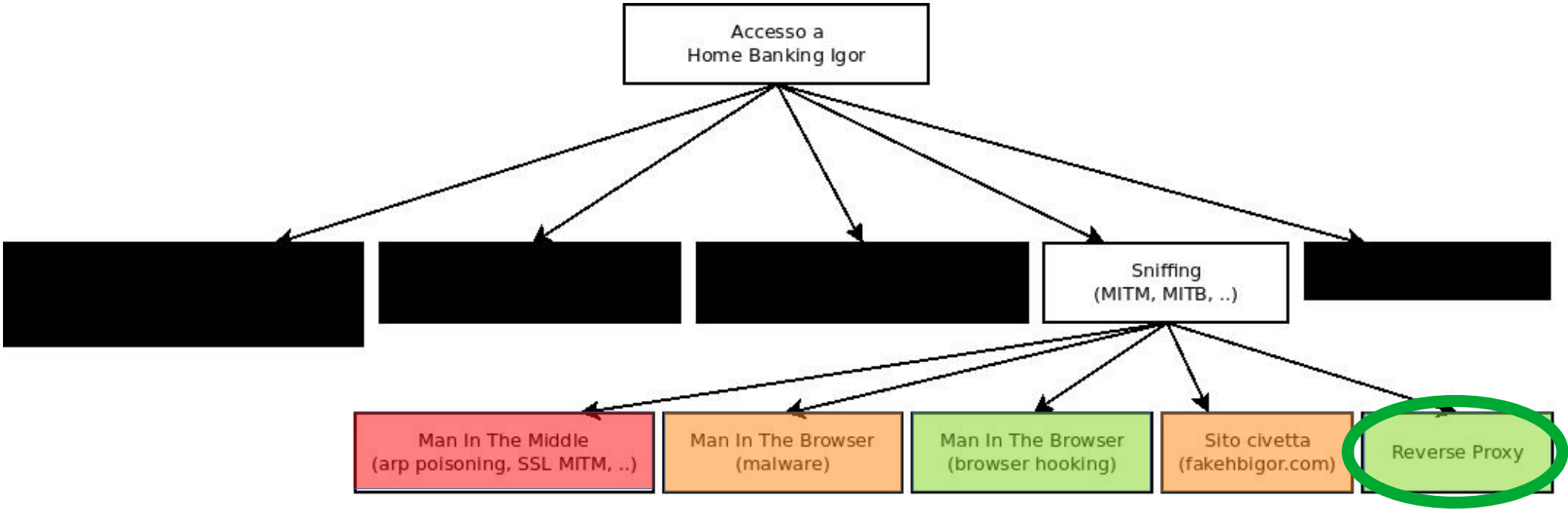
https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Attack Tree



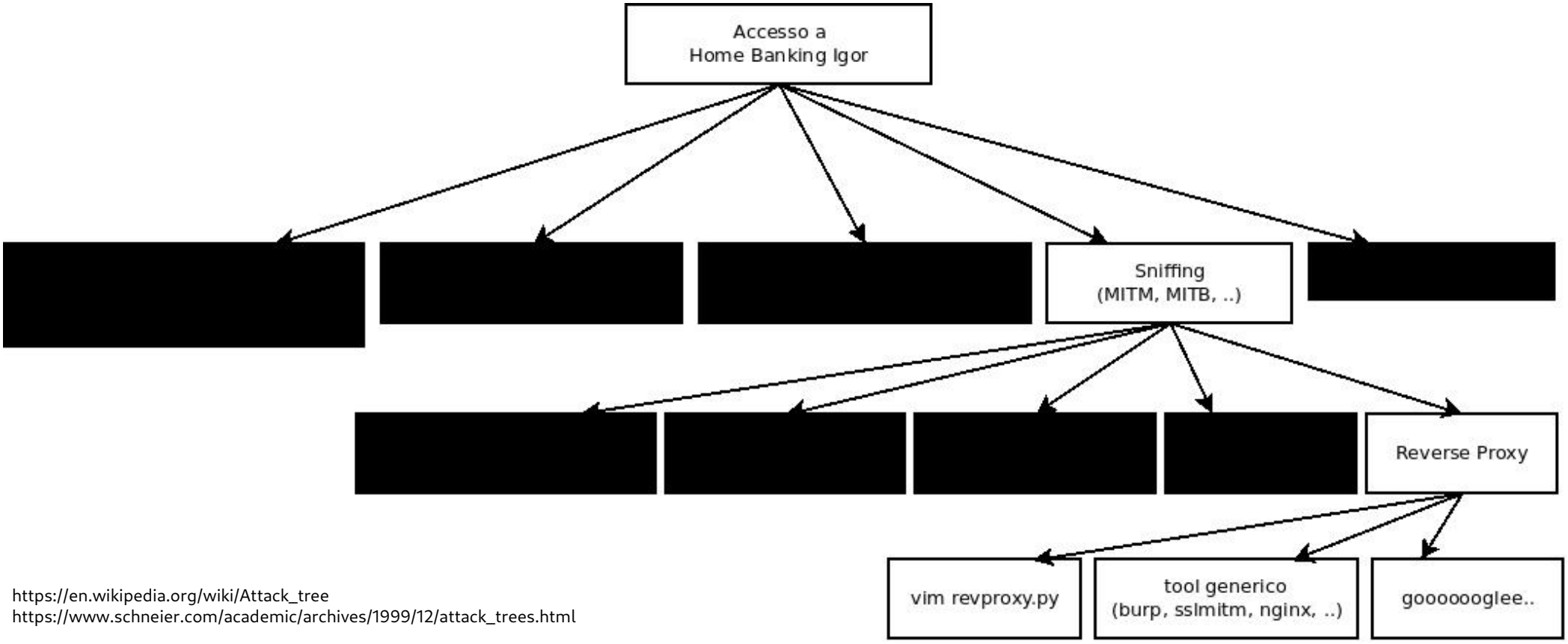
https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Reverse Proxy!



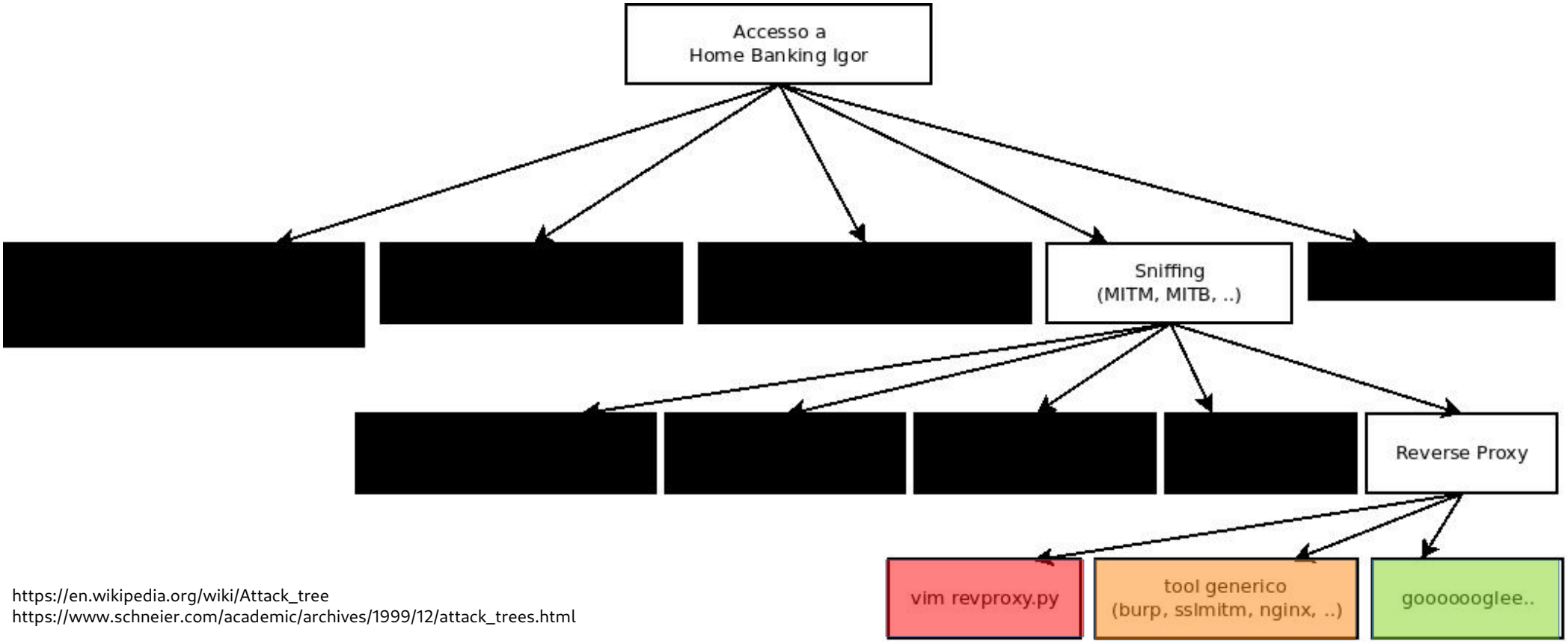
https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Sì, ma quale reverse proxy?



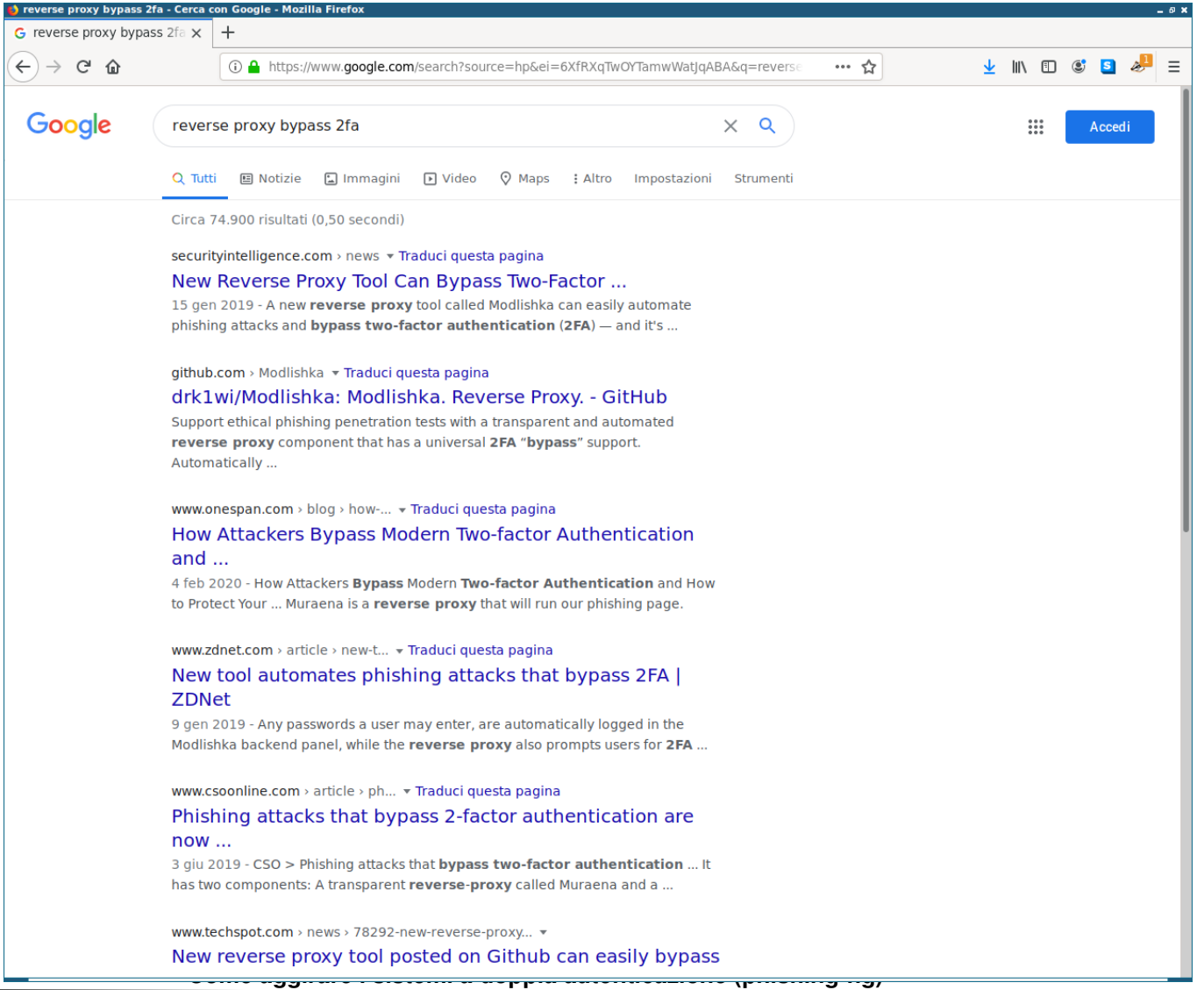
https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Sì, ma quale reverse proxy?

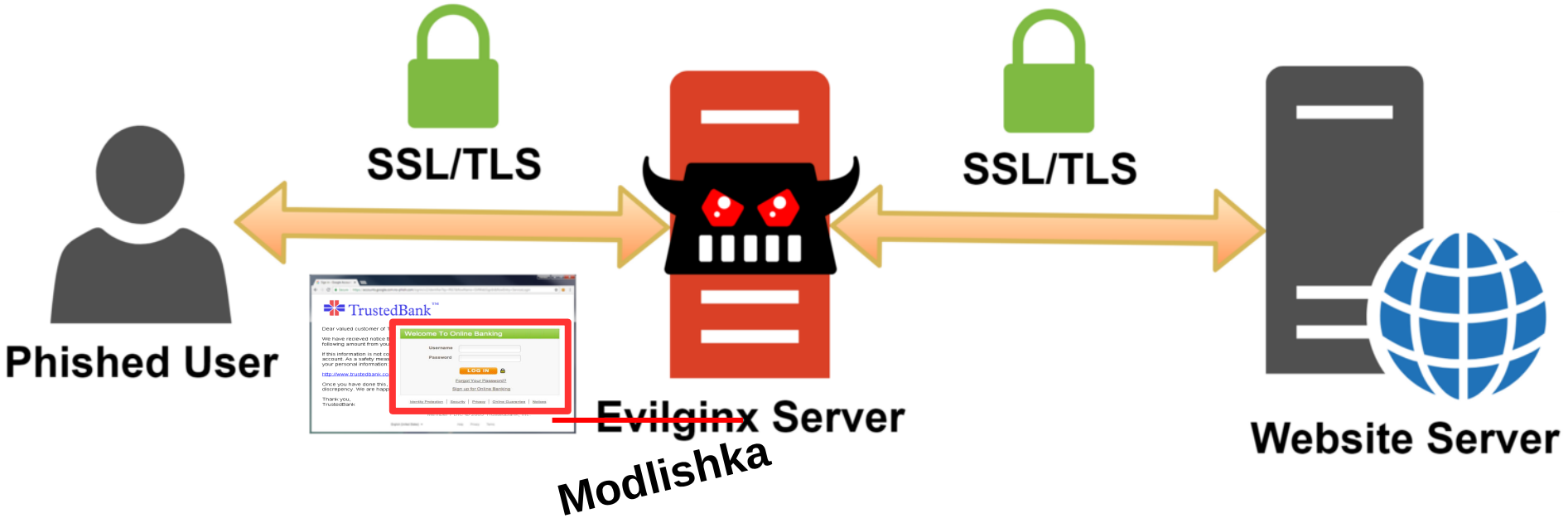


https://en.wikipedia.org/wiki/Attack_tree
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

LMGTFY:

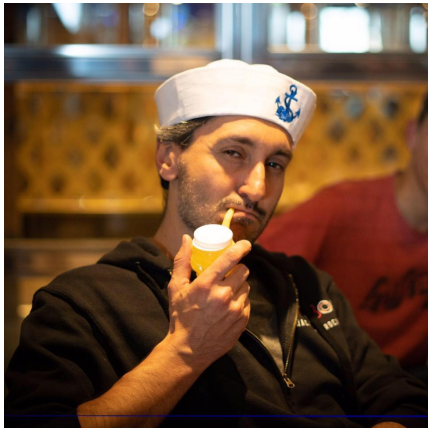

reverse proxy bypass 2fa - Cerca con Google - Mozilla Firefox
reverse proxy bypass 2fa
https://www.google.com/search?source=hp&ei=6XfRXqTwOYTamwWatJqABA&q=reverse
Google
reverse proxy bypass 2fa
Accedi
Tutti
Notizie
Immagini
Video
Maps
Altro
Impostazioni
Strumenti
Circa 74.900 risultati (0,50 secondi)
securityintelligence.com › news Traduci questa pagina
New Reverse Proxy Tool Can Bypass Two-Factor ...
15 gen 2019 - A new reverse proxy tool called Modlishka can easily automate phishing attacks and bypass two-factor authentication (2FA) — and it's ...
github.com › Modlishka Traduci questa pagina
drk1wi/Modlishka: Modlishka. Reverse Proxy. - GitHub
Support ethical phishing penetration tests with a transparent and automated reverse proxy component that has a universal 2FA "bypass" support. Automatically ...
www.onespan.com › blog › how-... Traduci questa pagina
How Attackers Bypass Modern Two-factor Authentication and ...
4 feb 2020 - How Attackers Bypass Modern Two-factor Authentication and How to Protect Your ... Muraena is a reverse proxy that will run our phishing page.
www.zdnet.com › article › new-t... Traduci questa pagina
New tool automates phishing attacks that bypass 2FA | ZDNet
9 gen 2019 - Any passwords a user may enter, are automatically logged in the Modlishka backend panel, while the reverse proxy also prompts users for 2FA ...
www.csoonline.com › article › ph... Traduci questa pagina
Phishing attacks that bypass 2-factor authentication are now ...
3 giu 2019 - CSO > Phishing attacks that bypass two-factor authentication ... It has two components: A transparent reverse-proxy called Muraena and a ...
www.techspot.com › news › 78292-new-reverse-proxy...
New reverse proxy tool posted on Github can easily bypass

(Malicious) Reverse Proxy



E ora proviamo..

https://github.com/drk1wi/Modlishka



HACK IN BO®

Safe Edition

2020

14ª EDIZIONE

DOMANDE ?

Gianfranco Ciotti – gciotti@enforcer.it
Igor Falcomatà – ifalcomata@enforcer.it

Riferimenti

Modlishka - Reverse Proxy
https://github.com/drk1wi/Modlishka
https://blog.duszynski.eu/phishing-ng-bypassing-2fa-with-modlishka/
https://blog.duszynski.eu/client-domain-hooking-in-practice/

EVILGINX 2 - Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication
https://github.com/kgretzky/evilginx2

BEEF - The Browser Exploitation Framework
https://beefproject.com/

Muraena is an almost-transparent reverse proxy aimed at automating phishing and post-phishing activities.
https://github.com/muraenateam/muraena

Burp Suite Community Edition
https://portswigger.net/burp/communitydownload

