PHISHING

1.0 COSE' E PERCHE'

1.1 Definizione e scopo
1.2 Da non confondere

2.0 TIPI DI PHISHING

2.1 Spear Phishing
2.2 Clone Phishing
2.3 Phone Phishing

3.0 SITI WEB FAKE

3.1 Come vengono creati
3.2 Come riconoscerli

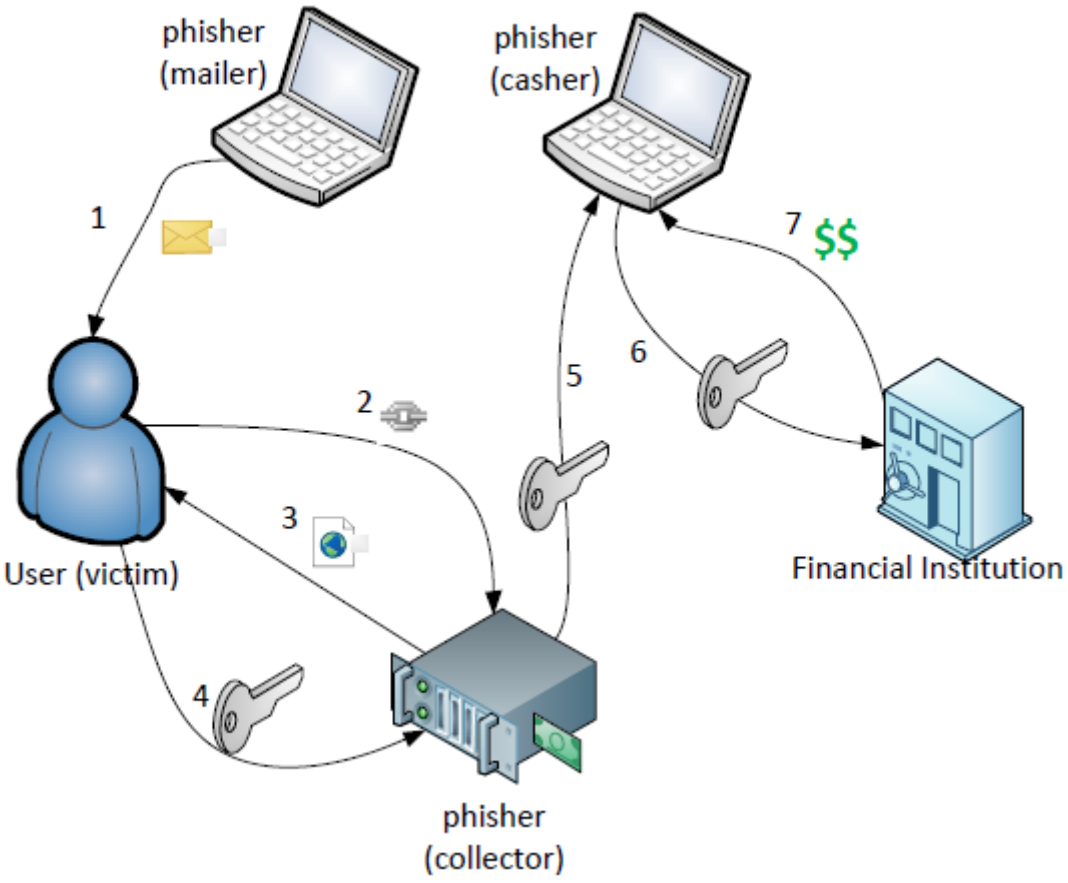
4.0 MALWARE

4.1 Come funzionano
4.2 Semplici contromisure

1.0 COSE' E PERCHE'

1.1 Definizione e scopo

Truffa informatica effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking ecc.), motivando tale richiesta con ragioni di ordine tecnico.
Queste mail possono anche ridirezionare su siti fake dall'aspetto identico all'originale, sempre allo scopo di ingannare l'utente e rubagli informazioni.



Recentemente il phishing si sta evolvendo in furto di informazioni a specifici soggetti per assicurari le informazioni desiderate come informazioni aziendali o informazioni sensibili anche di sicurezza nazionale.

1.2 Da non confondere

Ci sono molti tipi di e-mail inviate a scopo di truffa, ma non bisogna confondere la truffa con il phishing. Ad esempio non è phishing farsi pagare da un utente truffandolo poiche l'utente nonostante usi i propri dati per il pagamento, questi non vengono rubati e il truffatore non potra quindi continuare a prendere soldi dall'account dell'utente truffato.

2.0 TIPI DI PHISHING

2.1 Spear Phishing

Lo spear phishing è attualmente il metodo di phishing più efficace con una media del 91% di successo (dei casi registrati). Questo tipo di phishing consiste nel selezionare un obbiettivo specifico come un'azienda e studiarlo per elaborare una truffa su misura per ottenere specifiche informazioni o dati privati.

2.2 Clone Phishing

Il clone phishing, come dice il nome, consiste nel copiare e-mail di siti bancari nei quali la banca chiede per motivi tecnici di inserire dati personali che verranno poi salvati dal phisher.

```
cat body.htm | mail -a 'From: Twitter <support@twitter.com>' -a '
   Content-Type: text/html' -s 'Reset your Twitter password'
   victim@example.net
```

The file body.htm contains the mail contents in HTML format. The result is shown in Figure 2.

Figure 2: Fake Twitter password reset email received in Gmail

Per aumentare la realisticità solitamente le mail reindirizzano al sito nel quale viene effettuata le richiesta (vedi 3.0).

2.3 Phone Phishing:

Questo tipo di phishing è simile al clone phishing, ma anzi che utilizzare le mail, il phisher invia SMS. I messaggi più comuni cercano di essere accativanti (es. "Hai vinto..." "Sei il 1000 utente..."). I messaggi invitano ad aprire un link nel quale verranno richiesti i dati personali.

3.0 SITI WEB FAKE

3.1 Come vengono creati

Le mail di phishing portano a dei siti fake. Per aummentare la realisticità dei siti fake il phisher usa alcuni accorgimenti:

Inanzi tutto l'aspetto della pagina viene letteralmente copiato dal sito originale, dopodiche con un minimo di esperienza in HTML il phisher risistema i link presenti e alcuni piccoli accorgimenti.

Se un utente dovesse provare a cambiare pagina nel sito tramite un link, verrà quasi sempre reindirizzato ad una pagina: "Sito in manutenzione!".

3.2 Come riconoscerli

Per aumentare ancora la realisticità il phisher usa un indirizzo del sito che confonda l'utente facendogli credere di essere sul sito originale. Ecco alcuni esempi:

gmail.com (originale) >>>> gmeil.com (fake 1)
gmail.com.it (fake 2)
gma1l.com (fake 3)

Inoltre esiste un metodo per far apparire nella barra degli indirizi parti di indirizzo che non appartengono alla pagina effettiva.

Figure 3: Different highlighted domain names show that these website are unrelated

Dall' immagine si nota che nel secondo caso la scritta *yoursunny.com* non è evidenziata, questo perche non fa effettivamente parte dell'indirizzo. Con questo metodo l'utende si convincerà di essere sul sito originale.

I siti che trattano dati privati hanno adottato un metodo di sicurezza per distinguersi dai siti fake, l'HTTPS al posto del classico HTTP. La presenza della S (safe) indica che il sito possiede il certificato di sicurezza e può quindi trattare dati dell'utente in sicurezza. Alcuni siti phisher provano a falsificare la S, ma il browser riconoscerà l'assenza di

(a) http, no padlock (b) padlock on https

Figure 4: A padlock icon appears in address bar when visiting an https website

certificato.

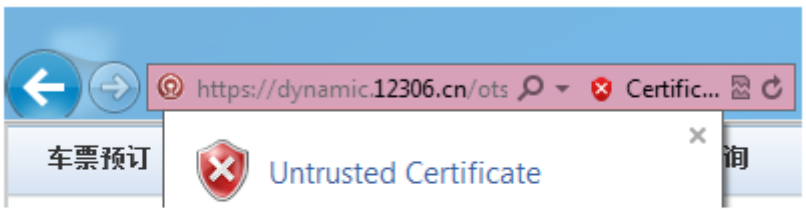


Figure 5: The address bar turns red on invalid certificate

4.0 MALWARE

4.1 Come funzionano

Spesso i phisher utilizzano malware per sempificare il phishing. Il malware più comune ha un effetto tanto semplice quanto efficace: il malware legge tutti gli input di caratteri dalla tastiera prima che questi vengano effettivamente inseriti nel campo di testo. I caratteri in questo modo salvati saranno poi letti dal phisher che cercherà pasword o dati importanti senza alcun disturbo.

4.2 Semplici contromisure:

Le aziende che cercano di protegere i propri dati privati solitamente distribuiscono hai dipendenti dei sofware di sicurezza.

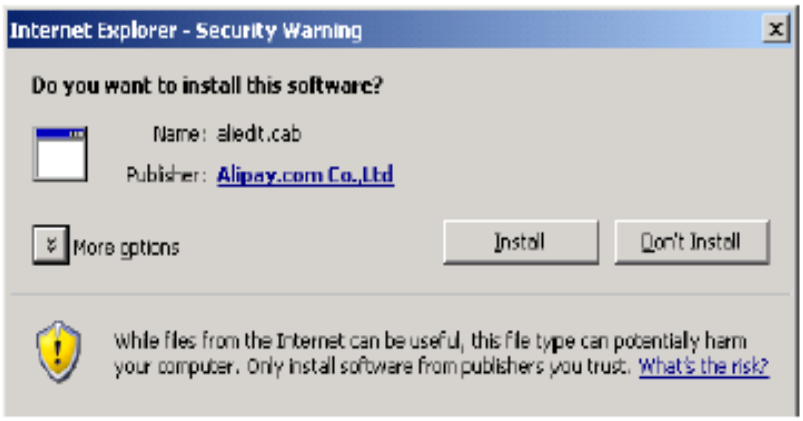


Figure 9: secure text input control from Alipay.com

Questi controllano gli input di testo ancora prima del malware e si assicura che il testo vega letto a sua volta solo dalla casella di testo in cui viene inserito proteggendo così da eventuali malware.