Riconoscere il phishing

Mirko Corosu - INFN Genova
20/12/2022

Perche’ questo incontro

- La grande maggioranza degli incidenti di sicurezza in Sezione hanno come vettore messaggi di phishing
- Dall’inizio della guerra in Ucraina gli attacchi sono aumentati sensibilmente in numero e qualita’ (non solo a Genova)
- La sensibilizzazione e la formazione continua sono parte della prevenzione degli incidenti informatici

> **Phishing is once again the most common vector** for initial access. Advances in sophistication of phishing, user fatigue and targeted, context-based phishing have led to this rise. New lures in social engineering threats are focusing on the Ukraine-Russia conflict in a similar manner to what happened during the COVID situation
>
> **ENISA Threat Landscape 2022**

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Di cosa stiamo parlando?

- Insieme di tecniche utilizzate da un attaccante per convincere una vittima a fornire **informazioni personali**, **dati finanziari** o **codici di accesso**, fingendosi un ente affidabile in una comunicazione digitale.
- Ci focalizzeremo sulla comunicazione via email ma puo' avvenire attraverso altri canali digitali (SMS, notifiche browser, WhatsApp, ecc..)

Informazioni Personali

Dati finanziari

Codici di accesso

Come inizia…..

- Un attacco di phishing inizia con l’invio di un mail che contiene un'offerta allettante o richiede un’azione quale:
  - **Compilare** un modulo (ad es. cambio password)
  - **Rispondere** all’indirizzo di provenienza comunicando informazioni
  - **Cliccare** su un link che conduce ad un sito fasullo
  - Aprire un **allegato infetto** (ad es. uno zip che dovrebbe contenere una fattura).

...e come puo' finire (ogni riferimento a cose e persone...)

- L'utente fornisce le sue credenziali
- L'attaccante le usa per danneggiare siti terzi (ad esempio inviando altre email di phishing/spam)
- I sistemi di controllo interno rilevano l'attivita'
  - A seconda della prontezza dell'azione di blocco e' possibile che i danni si riflettano anche sulla Sezione, ad esempio attraverso l'inserimento in blacklist dei nostri server
- In ogni caso parte la procedura obbligatoria:
  - Il Calcolo analizza il log degli accessi a tutti i servizi per rilevare altre possibili compromissioni
  - Il rapporto sull'incidente viene inviato allo CSIRT INFN che puo' chiedere ulteriori chiarimenti
  - Se l'incidente riguarda dati personali (e le credenziali lo sono), il Calcolo deve inviare un altro rapporto firmato dal Direttore al DPO INFN, che decide se si debba procedere con la segnalazione al Garante della Privacy

...e come puo' finire

- L'utente fornisce le sue credenziali
- L'attaccante le usa per danneggiare siti terzi (ad esempio inviando altre email di phishinf/spam)
- I sistemi di controllo interno rilevano l'attivita'
  - A seconda della prontezza dell'azione di blocco e' possibile che gli effetti si riflettano anche sulla Sezione, ad esempio attraverso l'inserimento in blacklist dei nostri server
- In ogni caso parte la procedura obbligatoria
  - Il Calcolo analizza il log degli accessi a tutti i servizi per rilevare altre possibili compromissioni
  - Rapporto sull'incidente viene inviato allo CSIRT INFN che puo' chiedere ulteriori chiarimenti
  - Se l'incidente riguarda dati personali (e le credenziali lo sono), il Calcolo deve inviare un altro rapporto firmato dal Direttore al DPO INFN, che decide se si debba procedere con la segnalaione al Garante della Privacy

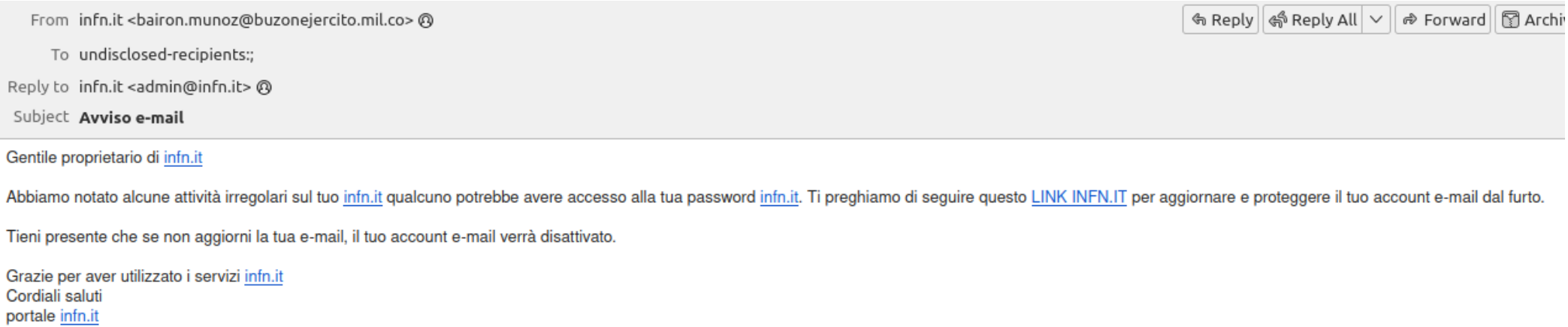
IMPATTO SENSIBILE SULL'ATTIVITA' GESTIONALE AMMINISTRATIVA

Ma puo’ finire molto peggio

- Truffe (anche di centinaia di migliaia di euro)
- Diffusione di dati sensibili
- Danneggiamento della reputazione dell’INFN (es. defacing siti web)
- Complicazioni legali

Esempi di phishing e come riconoscerli

Es. 1: Credenziali (facile)



From infn.it <bairon.munoz@buzonejercito.mil.co>
To undisclosed-recipients:;
Reply to infn.it <admin@infn.it>
Subject **Avviso e-mail**

Reply | Reply All | Forward | Archi

Gentile proprietario di infn.it

Abbiamo notato alcune attività irregolari sul tuo infn.it qualcuno potrebbe avere accesso alla tua password infn.it. Ti preghiamo di seguire questo LINK INFN.IT per aggiornare e proteggere il tuo account e-mail dal furto.

Tieni presente che se non aggiorni la tua e-mail, il tuo account e-mail verrà disattivato.

Grazie per aver utilizzato i servizi infn.it
Cordiali saluti
portale infn.it

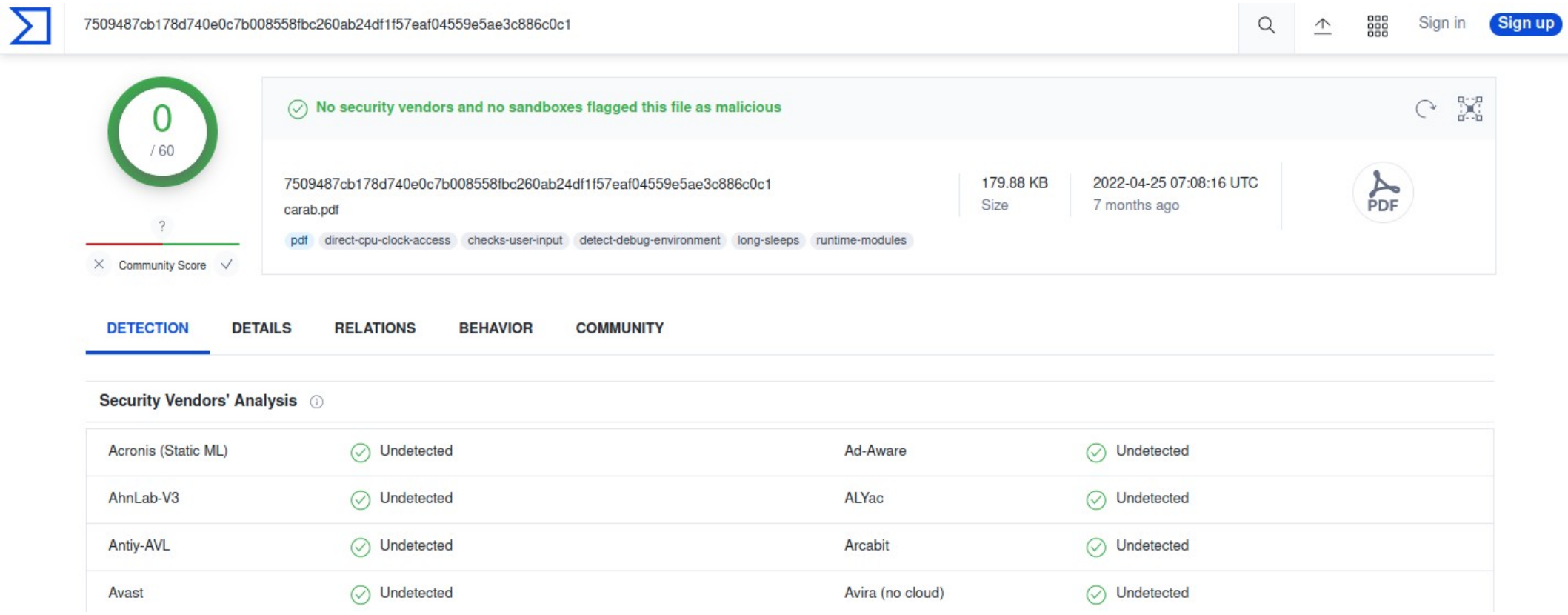
Es. 2: Credenziali (medio)

Pro tip: analisi degli header

```
Return-Path: <server@ge.infn.it>
Received: from mbox3.ge.infn.it ([unix socket])
     by mbox3 (Cyrus v2.3.16-Fedora-RPM-2.3.16-15.el6) with LMTPA;
     Wed, 19 Oct 2022 22:47:41 +0200
X-Sieve: CMU Sieve 2.3
Received: from mxge6.ge.infn.it (mxge6.ge.infn.it [193.206.144.94])
    by mbox3.ge.infn.it (Postfix) with ESMTP id 8F72B142E65
    for <anonimizzato@mbox3.ge.infn.it>; Wed, 19 Oct 2022 22:47:41 +0200 (CEST)
Received: by mxge6.ge.infn.it (Proxmox)
    id 88D6916011A; Wed, 19 Oct 2022 22:47:41 +0200 (CEST)
Delivered-To: anonimizzato@ge.infn.it
Received: from mxge6.ge.infn.it (localhost.localdomain [127.0.0.1])
    by mxge6.ge.infn.it (Proxmox) with ESMTP id 85CCA16030E
    for <anonimizzato@ge.infn.it>; Wed, 19 Oct 2022 22:47:41 +0200 (CEST)
Received-SPF: softfail (ge.infn.it: Sender is not authorized by default to use 'server@ge.infn.it' in 'mfrom' identity,
Received: from correo.mippci.gob.ve (correo.mippci.gob.ve [200.109.238.59])
    by mxge6.ge.infn.it (Proxmox) with ESMTP id 266C416011A
    for <anonimizzato@ge.infn.it>; Wed, 19 Oct 2022 22:47:40 +0200 (CEST)
Received: from correo.mippci.gob.ve (localhost.localhostdomain [127.0.0.1])
    by correo.mippci.gob.ve (Postfix) with ESMTP id 53BBD2194FF
    for <anonimizzato@ge.infn.it>; Wed, 19 Oct 2022 15:15:25 -0430 (VET)
Received: from ge.infn.it (250.250.169.192.host.secureserver.net [192.169.250.250])
    by correo.mippci.gob.ve (Postfix) with ESMTPSA id 7653D703478
    for <anonimizzato@ge.infn.it>; Wed, 19 Oct 2022 14:33:30 -0430 (VET)
From: "ge.infn.it administrator" <server@ge.infn.it>
To: anonimizzato@ge.infn.it
Subject: Your request to deactivate anonimizzato@ge.infn.it from ge.infn.it server is in process
Date: 19 Oct 2022 14:41:32 -0400
```

Es. 3: Sollecito di risposta (facile)

Pro tip: Virustotal.com



Es. 4: Sollecito di risposta (medio)

Da: Prof Dr. [redacted] <direttoredipartimento1@gmail.com>
Inviato: lunedì 12 luglio 2021 18:13
A: anonimizzato@ge.infn.it
Oggetto:

Ciao sei disponibile?
Per favore, ho bisogno urgentemente della tua assistenza

Prof Dr [redacted]

Professore Direttore
Dipartimento di Fisica
Università degli Studi di Genova
Valletta Puggia - Fisica
via Dodecaneso 33, GENOVA
Office: III.044

L'attaccante e' a conoscenza del nome del direttore ed ha raccolto informazioni sull'indirizzo e la denominazione corretta del Dipartimento di Fisica.

Ma… cosa accade se il destinatario dell'attacco risponde?

Es. 5: tentativo di truffa (periglioso)

From Mastro Geppetto <kristy.smitham@loyal.ro>
To Fata Turchina <Fata.Turchina@ge.infn.it>
Subject **Re: Esame orale di Fisica**

Reply

Buon pomeriggio!
Ho raccolto il documento focalizzato sull'ultimo contratto. Si prega di rivederlo qui:

https://onedrive.live.com/download?cid=E385002851465726&resid=E385002851465726%21106&authkey=ALUDgt9fX0s9AFo

Password del file.: TW4565

Salve,
concordo con la soluzione indicata dal prof. Geppetto.

Saluti
Fata Turchina

> On 4 Mar 2021, at 12:53, Mastro Geppetto <> wrote:
>
> Caro Bimbo,
> Le proporrei di lasciare l'orale alle 17, registrando noi la prima parte finché non arriva il testimone.
> Ovviamente la registrazione verrà cancellata al termine dell'orale.
>
> Saluti
> Mastro Geppetto
>
> > Il giorno 3 mar 2021, alle ore 16:26, <> <> ha scritto:

L'attaccante ha in precedenza compromesso il PC dello studente "Bimbo Pinocchio" e utilizza uno stralcio di conversazione realmente avvenuta per tentare di truffare i professori "Mastro Geppetto" e "Fata Turchina"

Quindi?

- Controllare sempre:
  - Reale destinazione di un link (se INFN il dominio deve **terminare** con **infn.it**)
    - Esempio https://web.ge.**infn.it**/calcolo
  - La sicurezza di un allegato sospetto (ad esempio via VirusTotal)
  - Mittente e destinatario possono aiutare ma attenzione: il mittente puo' essere **sovrascitto molto semplicemente**!
- Nel dubbio:
  - Contattare sempre il Servizio Calcolo, inoltrando il messaggio sospetto "come allegato"
  - Non immettere credenziali INFN su pagine web
- Leggere sempre allerte diffuse dagli amministratori


Grazie