
「Cryptmail」スクリプトについて - cryptmail-exploit.py

---

1. 概要

- 暗号メール・スクリプトcryptmail-exploit.pyは、「Cryptmail」を利用して、コマンドプロンプトから暗号メールの送信を可能にするCUIプログラムである
- 「**注**」「Cryptmail」は、ページ遷移とセッション監視を行っていないので、ユーザー認証を省略できる。これを確認するため試験的にログイン情報を必要としないスクリプトを作成した
  - 「Cryptmail」は、すでにfrom詐称対策を実施済みのため、現在このスクリプトは機能しない

2. 動作環境および必要ファイル

- Windows10
- Python3が動作する環境
- Requestモジュールがインストールされていること
- cryptmail-exploit.py 本スクリプト
- e-mail.json 送信元、送信先、件名、本文を記述したファイル

3. 実施手順

3.1. e-mail.jsonの準備

- 送信元（差出人）のメールアドレス、送信先（社内外の宛先）のメールアドレス、メールのタイトル（件名）、メール本文を記述したe-mail.jsonを用意する
- 以下のキーは必須であるため削除してはいけない
  - from: 差出人
  - to: 宛先メールアドレス
  - cc: 宛先メールアドレス（LDAPにない宛先を含めるとエラーになる）
  - subject: 件名
  - body: 本文
- 他のキーも追加してはいけない（ファイル添付も可能だが未実装）
- e-mail.jsonの記述例は以下の通り

```
{
    "from": "aaaa@abcd.com",
    "to": [
        "aaaa@xyzw.com",
        "bbbb@gmail.com"
    ],
    "cc": [
        "aaaa@abcd.com",
        "cccc@abcd.com"
    ],
    "subject": "なにがしの件",
    "body": [
        "なにがし様\r\n",
        "\r\n",
        "お世話になっております。\r\n",
        "なにがし管理窓口です。\r\n",
        "\r\n",
        "今月のなにがし情報を送付します。\r\n",
        "\r\n",
        "・ID\r\n",
        "123456@gmail.com\r\n",
        "\r\n",
        "・パスワード\r\n",
        "pqpqpqpq\r\n",
        "\r\n",
        "以上、よろしくお願いします。\r\n"
    ]
}
```

- `Json`書式に従って記述すること
- 特にコンマの位置に注意すること
- 本文に改行を入れたい場合は、`\r\n`を記入すること

3.2 `cryptmail-exploit.py`の実行

- あらかじめ動作環境に、`Python3`とモジュール`Request`がインストールされていること
- `Request`のインストール手順は次の通り

```
> pip3 install requests
```

- コマンドプロンプトを起動し、**任意の**ユーザー名とパスワードを引数に以下の書式で`cryptmail-exploit.py`を起動する

```
> python3 cryptmail-exploit.py "xxxxx" "yyyyy"
```

- 引数が不足する場合は、使用例を表示して終了する

```
> python3 cryptmail-exploit.py xxx

    Usage: $ python3 cryptmail-exploit.py "username" "password"
```

- 引数が満足する場合は、「`Cryptmail`」からのメールが送信される
- 実行途中、以下のファイルを生成する
- 生成ファイル
    - `login.htm`
    - `index.htm`
    - `check.htm`
    - `send.htm`
    - `complete.htm`
- これらのファイルはサーバー側でなんらかのエラーが発生した場合に確認するためのものである
- サーバーエラーには以下のようなものがある
    - 「ユーザ名またはパスワードが違う」
    - 「差出人のメールアドレスに不正な文字が含まれている」
    - 「社内の宛先に、社外の宛先が含まれている」

以上