



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri



COMPUTER EMERGENCY RESPONSE TEAM  
PUBBLICA AMMINISTRAZIONE

**CERT - PA**  
Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

# HASHR<sub>v.0.3</sub>

---

CERT-PA  
22/10/2018



## Indice

Sommario.....	3
1. Informativa .....	3
2. Ricerca di IoC su intera unità disco.....	4
3. Ricerca di IoC “cifrati” su intera unità disco.....	4
4. Ricerca di IoC su intera unità disco limitatamente a specifiche estensioni di file .....	5
5. Hashr su Linux e MacOS.....	5
6. Note .....	5



## Sommario

Informativa destinata alle Pubbliche Amministrazioni.

### 1. Informativa

Hashr è uno strumento sviluppato in Python 2.7 dagli analisti del CERT-PA **che consente di computare hash dei file e di cercare la corrispondenza su una lista di hash predefinita** (es. IoC di hash).

Nato inizialmente per ricercare indicatori di compromissione di tipo APT (Advanced Persistent Threats) condivisi in forma cifrata, hashr è stato successivamente adattato alle esigenze della Constituency estendendo le funzionalità ai seguenti algoritmi di hash:

- md5
- sha1
- sha256
- imphash (*per file di tipo Portable Executable*)

Il pacchetto include il file eseguibile “*hashr.exe*” per piattaforma Microsoft Windows ed il codice sorgente, rilasciato sotto licenza GPL3, per essere eseguito anche su ambienti Linux e OSX grazie all’interprete Python 2.7.x

```
Processore dei comandi di Windows

CERT-PA

www.cert-pa.it | cert-pa@cert-pa.it
hashr v.0.3

usage: hashr [-h] [-v] [-r] [-d] [--filetype FILETYPE] [-e] [--hashlist FILE]
            [--encrypted] [-o OUTPUT]
            HASH TARGET

hashr is a tool able to compute hash of the files and compare them with a hashlist file.
Using hashr you can verify if IoC malware hashes (like APT) are present in your system.

positional arguments:
  HASH                algorithm supported: md5, sha1, sha256, imphash
  TARGET              file or directory name from which to obtain the hash

optional arguments:
  -h, --help          show this help message and exit
  -v, --version       show program's version number and exit
  -r, --recursive     recursive directory
  -d, --duplicate     show duplicate hashes found
  --filetype FILETYPE filter for extension (use comma separator)
  -e, --exclude       exclude filetype
  --hashlist FILE     load file with homogeneous hashes list
  --encrypted         only for encrypted hashlist
  -o OUTPUT           write output file

EXAMPLE - Search recursively in your system:

hashr md5 c:\ -r --hashlist iocfile.txt
```



Il CERT-PA fornisce con cadenza quasi giornaliera indicatori di compromissione per file malevoli analizzati in laboratorio o pervenuti attraverso attività di infosharing. A tal proposito, a partire dal rilascio di hashr, il CERT-PA provvederà a condividere una apposita lista di IoC che garantisce la piena compatibilità con hashr.

## 2. Ricerca di IoC su intera unità disco

Il caso d'uso più frequente è quello di verificare la presenza di file malevoli sul proprio sistema operativo a partire da una lista di IoC rilasciata per una specifica campagna.

La sintassi da eseguire sul terminale con privilegi di amministratore è la seguente:

```
hashr sha256 C:\ -r --hashlist iochash256.txt
```

Comando	Descrizione
hashr	Tool hashr.exe
sha256	Algoritmo di hash
C:\	Target di destinazione
-r	Ricerca ricorsiva
--hashlist	Specifica la lista di hash
iochash256.txt	Percorso alla lista di hash

Quando hashr individuerà IoC presenti sul sistema i risultati verranno mostrati a video. In alternativa sarà possibile ridirigere l'output su un file di testo aggiungendo alla sintassi il parametro `-o` seguito dal percorso al file di destinazione. Ad esempio:

```
hashr sha256 c:\ -r --hashlist iochash256.txt -o c:\output.txt
```

## 3. Ricerca di IoC "cifrati" su intera unità disco

Casi particolari riguardano la condivisione con la *Constituency* del CERT-PA di indicatori di compromissione forniti in forma cifrata. In tal caso sarà sufficiente aggiungere alla sintassi il parametro `--encrypted`

```
hashr sha256 c:\ -r --hashlist iochash256.txt --encrypted
```



## 4. Ricerca di IoC su intera unità disco limitatamente a specifiche estensioni di file

La sintassi standard consente di analizzare ogni singolo file presente sul disco e di verificare la corrispondenza su una lista di hash predefinita. Nel caso in cui emerge la necessità di lavorare su specifiche estensioni di file sarà possibile utilizzare il parametro `--filetype` seguito dalle estensioni dei file che si desidera analizzare. Ad esempio:

```
hashr sha256 c:\ -r --hashlist iochash256.txt --filetype  
.exe, .dll, .sys
```

In alternativa sarà possibile lavorare per esclusione aggiungendo il parametro `-e` che provvederà ad escludere dalla scansione i tipi di file indicati con `filetype`.

```
hashr sha256 c:\ -r --hashlist iochash256.txt --filetype  
.exe, .dll, .sys -e
```

## 5. Hashr su Linux e MacOS

Per eseguire `hashr` su un sistema operativo Linux o MacOS sarà sufficiente predisporre il sistema di un interprete Python 2.7.x e lanciare `hashr` da sorgente.

```
python hashr.py sha256 /dev/sda -r --hashlist iochash256.txt
```

## 6. Note

- Per gestire la ricorsività su disco C:\ utilizzare `hashr` con utenza amministrativa;
- `Hashr` non è in grado di rilevare file utilizzati da componenti rootkit, in tal caso si consiglia di analizzare il sistema collegando il disco come device esterno;
- Senza opzione `--filetype` il tool esegue un controllo su tutti i file accessibili presenti sul disco.
- Analogamente alla sintassi utilizzata per analizzare file o l'intero device, `hashr` può essere utilizzato semplicemente per computare hash a partire da un singolo file o directory. Ad esempio:

- `hashr sha256 C:\malware.exe`
- `hashr sha256 C:\folder\`