

Information Security Auditing, Certification and Digital Forensics



CERT - AGID

Studente: Ludovico Guercio

AGID e il CERT-AGID

L'AGID (l'agenzia per l'italia in digitale) è un'agenzia pubblica che ha il compito di gestire, coordinare le infrastrutture e piattaforme della pubblica amministrazione.

L'AGID dispone di un team interno, chiamato **CERT-AGID**

(Computer Emergency Response Team), che si impegna nel mantenere e sviluppare tutte i servizi relativi alla sicurezza IT

Nasce dal CERT-PA (2014-2020)

Il CERT-AGID ha il compito di:

- definire strategie, norme tecniche, raccomandazioni per lo sviluppo software (es: linee guide e standard)
- sviluppo di applicativi e tools per le PA
- crescita e diffusione della cultura della sicurezza informatica

[articoli 14bis e 51 del D. Lgs 5 marzo 2005 n. 82 (CAD)]

Cosa offre il CERT-AGID...

sito web ufficiale: <https://cert-agid.gov.it/>

All'interno del sito sono reperibili pubblicamente tutte le risorse che mettono a disposizione (per il pubblico e per le PA):

- ❑ Notizie e osservatorio
- ❑ Documentazioni
- ❑ Strumenti e funzionalità
- ❑ Glossario

CERT - AGID : Notizie

Sezione dove sono riportate le principali notizie dell'attività del team con articoli riassuntivi:

- report riscontri
- analisi e monitoring
- identificazione e mitigazione
- attività phishing e malware

[Notizie](#)[Vulnerabilità](#)[Malware](#)[Data breach](#)[riepilogo](#)

27/05/2022

Sintesi riepilogativa delle campagne malevole nella settimana del 21 – 27 maggio 2022

In questa settimana, il CERT-AGID ha riscontrato ed analizzato, nello scenario italiano di suo riferimento, un totale di 44 campagne malevole con obiettivi italiani, mettendo a disposizione dei suoi enti accreditati i relativi 862 indicatori di compromissione (IOC) individuati. Riportiamo in seguito il dettaglio delle tipologie illustrate nei grafici, risultanti dai dati estratti dalle piattaforme del CERT-AGID e consultabili tramite la pagina [...]

[riepilogo](#)

20/05/2022

Sintesi riepilogativa delle campagne malevole nella settimana del 14 – 20 maggio 2022

In questa settimana, il CERT-AGID ha riscontrato ed analizzato, nello scenario italiano di suo riferimento, un totale di 52 campagne malevole, di cui 51 con obiettivi italiani ed 1 generica che ha comunque interessato l'Italia, mettendo a disposizione dei suoi enti accreditati i relativi 1542 indicatori di compromissione (IOC) individuati. Riportiamo in seguito il dettaglio delle tipologie illustrate nei grafici, risultanti dai dati [...]

[coper](#)[Inps](#)[Intesa SanPaolo](#)

16/05/2022

Il trojan bancario Coper è arrivato anche in Italia

Nel corso delle quotidiane attività di monitoraggio il CERT-AGID ha individuato questa settimana due campagne di phishing, rivolte rispettivamente verso utenti INPS e verso i clienti dell'istituto bancario Intesa Sanpaolo. In entrambi i casi i domini, oltre le pagine di phishing, ospitavano un file APK che da successive analisi si è rivelato essere il trojan [...]

[riepilogo](#)

13/05/2022

Sintesi riepilogativa delle campagne malevole nella settimana del 07 – 13 maggio 2022

In questa settimana, il CERT-AGID ha riscontrato ed analizzato, nello scenario italiano di suo riferimento, un totale di 57 campagne malevole, di cui 54 con obiettivi italiani e 3 generiche che hanno comunque interessato l'Italia, mettendo a disposizione dei suoi enti accreditati i relativi 640 indicatori di compromissione (IOC) individuati. Riportiamo in seguito il dettaglio delle tipologie illustrate nei grafici, risultanti dai dati [...]

CERT - AGID : Vulnerabilità , Malware e DataBreach

Notizie Vulnerabilità Malware Data breach

IoC log4j log4shell

31/01/2022

Il CERT-AGID riduce la frequenza degli aggiornamenti IoC Log4shell

Sin dallo scorso 13 dicembre 2021 il CERT-AGID, grazie anche al contributo del CNAIPIC e delle fonti pubbliche (NCSC-NL e CURATED-INTEL) ha mantenuto costantemente aggiornato il servizio IoC per la mitigazione degli attacchi Log4shell. Come si evince dall'andamento del grafico sopra riportato, l'attività riguardante il monitoraggio degli attacchi che hanno sfruttato il CVE-2021-44228 ha registrato [...]

CVE-2021-44228 IoC log4j log4shell

13/12/2021

CERT-AgID condivide gli IoC per la mitigazione degli attacchi Log4shell

(Lista IoC aggiornata al 31-01-2022 @ 09:11) Come evidenziato anche dal CSIRT Italia, la vulnerabilità censita come CVE-2021-44228 riguardante Apache Log4j sta creando notevoli problemi di sicurezza sui sistemi esposti che utilizzano quel prodotto. Il CERT-AGID, a protezione delle proprie infrastrutture e di quelle della sua constituency, sta raggruppando gli IoC (Indicatori di Compromissione) pubblici [...]

E' online il servizio per la autoverifica della configurazione HTTPS e CMS riservato alla Pubblica Amministrazione

17/11/2021

Il CERT-AGID ha pubblicato un articolo in cui viene illustrata la recente situazione sull'utilizzo del protocollo HTTPS e dei CMS nei siti della Pubblica Amministrazione: Migliora l'utilizzo del protocollo HTTPS nella Pubblica Amministrazione ma i CMS restano poco aggiornati. L'articolo ha analizzato i dati raccolti da due strumenti di scansione sviluppati internamente dagli analisti del [...]

Notizie Vulnerabilità Malware Data breach

dump Luxottica Nefilim ransomware

20/10/2020

Il malware Nefilim fa una vittima illustre: in rete i dati sottratti a Luxottica

Gli autori del ransomware Nefilim non si smentiscono e, a distanza di un mese dall'attacco all'azienda italiana Luxottica, rilasciano al pubblico i dati delle vittime. Il messaggio recapitato alla vittime di Nefilim è chiaro: se la vittima non riesce a pagare il riscatto vedrà pubblicati i propri dati online e quindi accessibili a chiunque. La [...]

Avaddon CVE-2020-5902 Dridex Ursnif Zloader

10/07/2020

Una settimana cyber particolarmente densa di eventi malevoli

Settimana piuttosto articolata sul fronte malware che ha visto le strutture di sicurezza impegnate a fronteggiare l'emergenza Ursnif per quattro giorni consecutivi a cui si sono aggiunte le campagne Dridex, Avaddon e Zloader. La campagna massiva Ursnif, che ha fatto discutere molto questa settimana, è stata veicolata sia tramite allegati XLS sia tramite DOC con [...]

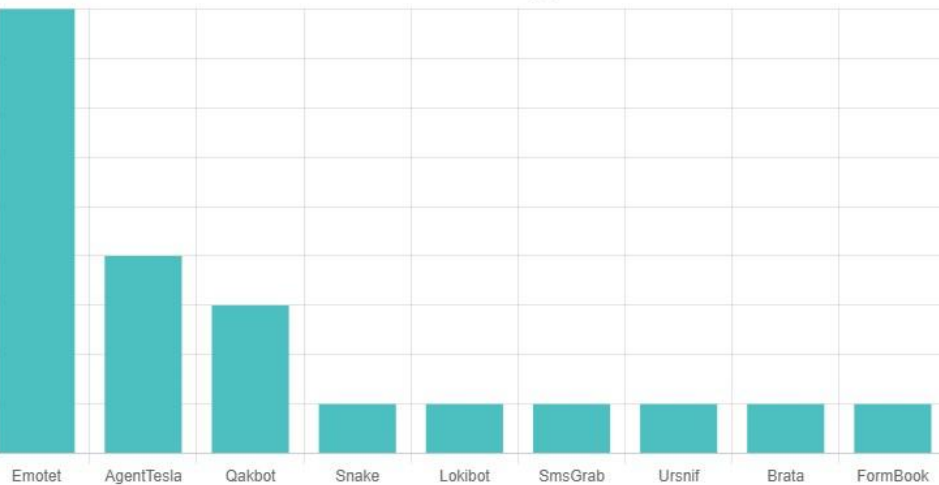
dump Joomla Jrd

03/06/2020

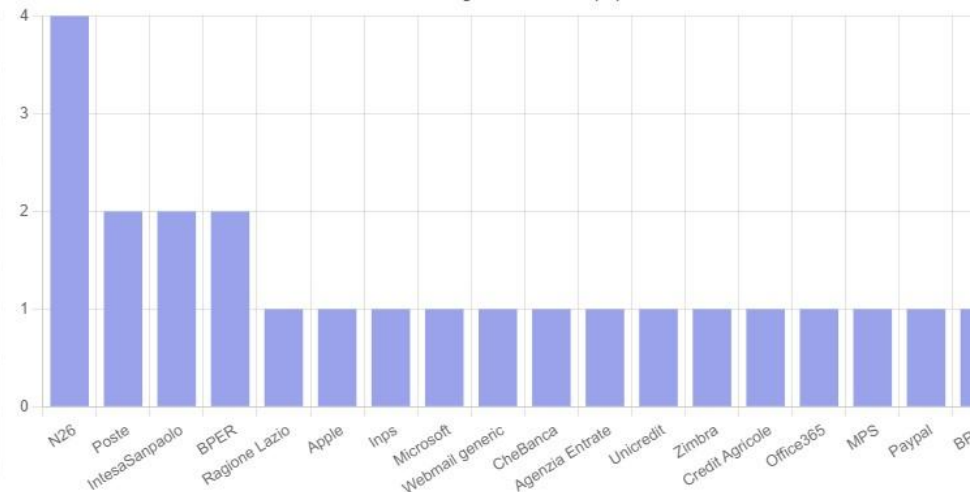
Data breach del portale Joomla! Resources Directory (JRD)

La fuga di informazioni ha interessato 2.700 utenti di JRD, Joomla! Resources Directory (resources.joomla.org), la piattaforma a disposizione della community di sviluppatori e di professionisti che promuovono servizi e funzionalità aggiuntive per il CMS Joomla! L'annuncio dell'incidente arriva da un post sul sito della Community, dal quale si evince che la violazione è avvenuta a [...]

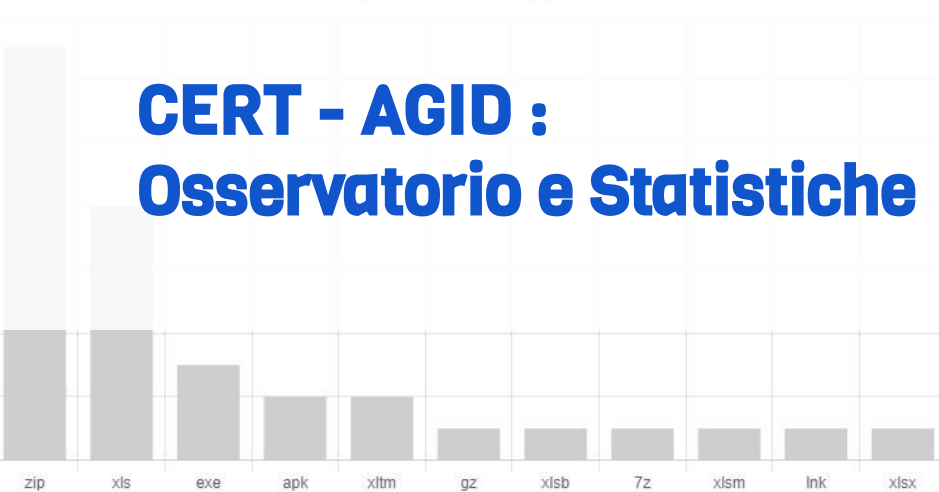
Malware della settimana (9)



Phishing della settimana (18)

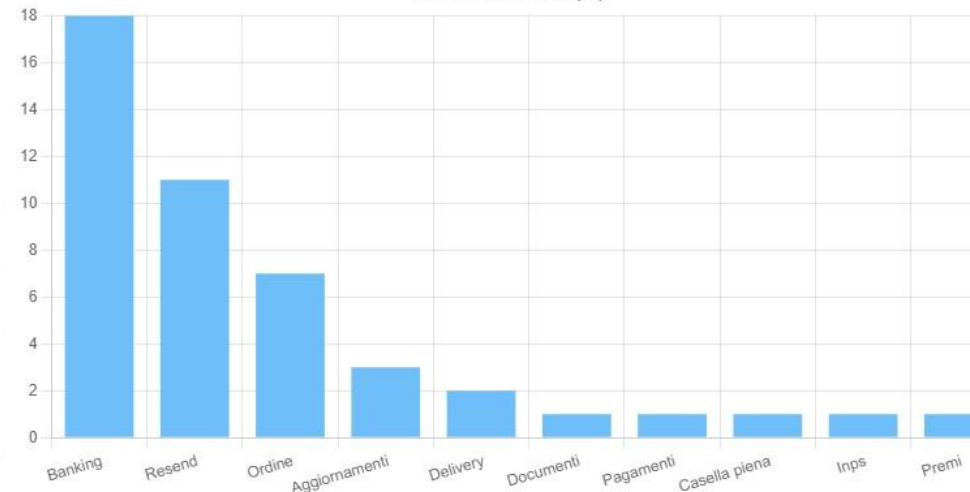


Tipi file della settimana (11)



CERT - AGID : Osservatorio e Statistiche

Temi della settimana (10)



CERT - AGID : Documentazioni

Il CERT-AGID offre una sezione dedicata alla documentazione per le PA e per gli sviluppatori:

- ❑ Misure minime di sicurezza ICT per le PA + moduli implementazione
- ❑ Linee guida per sviluppo sicuro di un software
- ❑ Linee guida per configurare e adeguare la sicurezza di un software

CERT - AGID : Strumenti per la PA

CERT-AGID fornisce funzionalità e software come supporto per la PA

- ❑ Flusso indici di compromissione (IoC)
- ❑ HASHR
- ❑ Servizio di autoverifica HTTPS CMS

CERT - AGID :

Indicatori di Compromissione

Cosa sono gli IoC?

Sono i possibili osservati che possono portare pericoli all'interno di una rete.

Es: URL , dominio, indirizzi IP, hash di un file ecc...

Le PA possono contribuire i flussi di IoC gestiti dal CERT-AGID (su richiesta):

- Ogni tipo di minaccia è segnata da un indicatore
- Il CERT scansiona e monitora gli indirizzi della rete della PA
- Le PA possono controllare l'andamento degli IoC

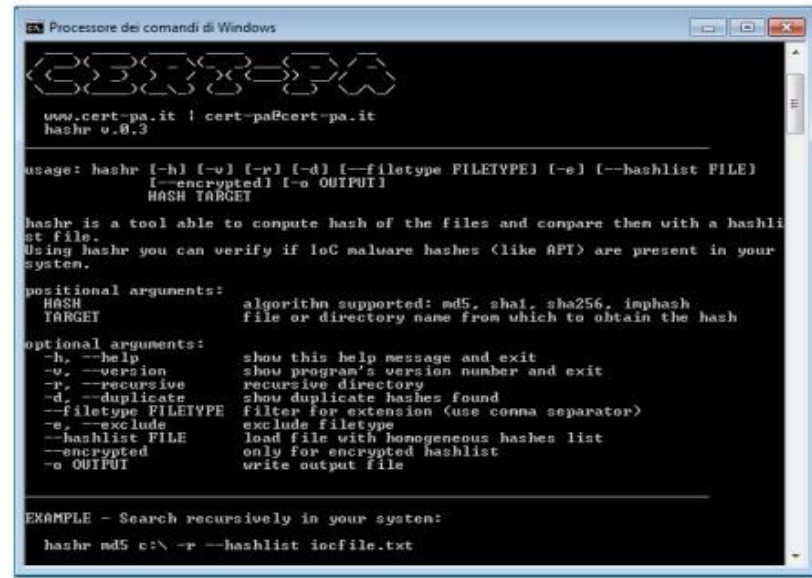
Vantaggi: tempestive segnalazioni e interventi

CERT - AGID : Strumento HASHR

Tool sviluppato dal CERT-AGID

consente di computare hash dei file e di cercare la corrispondenza su una lista di hash predefinita :

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



```
Processore dei comandi di Windows

CERT-AGID

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 hashli
st 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
```

CERT - AGID : Strumento HASHR

Esempio utilizzo:

verificare la presenza di file malevoli sul proprio sistema operativo a partire da una lista di IoC rilasciata

Alla presenza di IoC, essi verranno mostrati

```
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

Esito verifica HTTPS

www.unsitononesistente.gov.it

Host: www.unsitononesistente.gov.it

IP: 192.0.2.241

Testato.

Esito: l'implementazione HTTPS non è più considerata sicura.

Motivo: Supporta TLS 1.0, Supporta TLS 1.1.

SSL/TLS	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	Certificato
Sì	No	No	Sì	Sì	Sì	No	Valido

Aut. nulla	Cifr. nullo	Cifr. deboli	Cifr. CBC	Compressione	HTTPS	HTTP -> HTTPS	HTTPS -> HTTP
No	No	No	No	No	Sì	Sì	No

Esito verifica CMS

Nome CMS	Versione rilevata	Ultima versione disponibile*
Drupal	7	9.1.6

CERT - AGID : Verifica HTTPS e CMS

Le PA possono richiedere al CERT-AGID di analizzare lo status dei loro servizi:

- HTTPS
- CMS

Rilascio finale di un report con esiti (Es: l'implementazione HTTPS è vulnerabile ad attacchi noti)

Il CMS deve essere aggiornato*.

CERT - AGID per la cultura informatica...

DDOS-DOS

Che cos'è?

Il termine Denial of Service nel campo della sicurezza informatica indica un malfunzionamento dovuto ad un attacco informatico che causa la saturazione deliberata delle risorse di un sistema informatico, ad esempio un sito web su un web server, fino a renderlo non più in grado di erogare il servizio.

Un attacco DOS può essere anche di tipo distribuito (DDoS - Distributed Denial of Service). Il DDoS mantiene gli stessi scopi del DOS, ma in questo caso il traffico che colpisce la vittima proviene da molteplici fonti distribuite anche geograficamente. L'attacco DDoS viene portato da più bot (computer infettati) che agiscono contemporaneamente su più livelli (ad esempio su più livelli di rete, su più livelli di applicazione, su più livelli di protocollo). Un attacco DDoS può essere anche di tipo distribuito (DDoS - Distributed Denial of Service). Il DDoS mantiene gli stessi scopi del DOS, ma in questo caso il traffico che colpisce la vittima proviene da molteplici fonti distribuite anche geograficamente. L'attacco DDoS viene portato da più bot (computer infettati) che agiscono contemporaneamente su più livelli (ad esempio su più livelli di rete, su più livelli di applicazione, su più livelli di protocollo).

Perché è rilevante?

L'attacco DoS può comportare il rallentamento o la mancata erogazione del servizio via rete, con conseguenti danni a livello di immagine, economico e sicurezza.

Come mi difendo?

- Implementando filtri su pacchetti di dati alterati (cioè spoofing) e applicando in tempi relativamente brevi una patch di sicurezza.
- Utilizzando sistemi di prevenzione delle intrusioni (IDS/IPS).
- Utilizzando sistemi di prevenzione delle intrusioni (IDS/IPS).
- Utilizzando la tecnica del sinkholing che prevede di indirizzare i bot "malevoli" verso un server "civetta" controllato dalla vittima.

Spoofing

Che cos'è?

Lo spoofing è una tipologia di attacco informatico comunemente utilizzata insieme al Social Engineering per falsificare l'identità di un utente, di un dispositivo elettronico o un certificato.

Perché è rilevante?

Sfruttando questa tecnica l'attaccante potrà impersonare un host o un utente con lo scopo di sottrarre dati sensibili, commettere reati celando in parte la propria identità, o indurre il destinatario della comunicazione a fornire informazioni credendo di cederle all'utente o all'host reale.

Come mi difendo?

I casi più frequenti di spoofing coinvolgono principalmente la posta elettronica, a tal proposito si consiglia di diffidare da qualsiasi messaggio di posta di natura sospetta e di mettere in pratica il buon senso e particolare discrezione quando si forniscono informazioni sensibili.

Defacing

Che cos'è?

Con il termine Defacing (in italiano con defacciare) si intende la modifica illecita della home page di un sito web (la sua "faccia") o la sostituzione di una o più pagine interne. Questo tipo di attacco, viene eseguito all'insaputa di chi gestisce il sito ed è illegale in tutti i paesi del mondo.

Perché è rilevante?

Un sito che è stato oggetto di un deface vede sostituita la propria pagina principale e/o altre pagine interne con una schermata che indica l'azione compiuta da uno o più cracker. Di conseguenza questo attacco, oltre a comportare potenzialmente l'interruzione di uno o più servizi, può creare danni all'immagine di una società o ente pubblico.

Come mi difendo?

Mantenendo aggiornato tutto il software presente sul server web. In particolare applicare regolarmente le patch di sicurezza sul sistema operativo e http server.

Obiettivo : crescita e diffusione dei concetti
di sicurezza informatica

Offerta di un glossario con i principali concetti a tema sicurezza (Es: deep web, dark web, botnet, DDOS, ecc..)

FINE

