IoC - Cert-Agid CAP7.PA.20

La mail di Agid

Gentile Amministrazione,

nel confermarle l'accettazione della richiesta di accreditamento forniamo di seguito gli URL per il raggiungimento del servizio.

Le ricordiamo che il flusso IoC sarà raggiungibile **esclusivamente** dai seguenti indirizzi IP da voi forniti nel modulo di adesione:

- 128.116[redacted]

URL del flusso

Per firewall	https://cert-agid.gov.it/iocs?token=[redacted]b-77cda5d70a54
Per AdBlocker	https://cert-agid.gov.it/iocs?token=[redacted]77cda5d70a54&easylist
Per firewall (con estensione CSV)	https://cert-agid.gov.it/iocs[redacted]0a54/all.csv

Può trovare informazioni più dettagliate sull'utilizzo degli URL e sul loro formato nella pagina Indicatori di Compromissione per protezione della Pubblica Amministrazione sul nostro sito.

Per comodità riportiamo gli URL da usare con il vostro firewall qualora questo necessiti di liste separate per gli indicatori di tipo Dominio e URL o di un'estensione file specifica.

Per firewall (solo domini)	https://cert-agid.gov.it/iocs?token=[redacted]type=domain
Per firewall (solo URL)	https://cert-agid.gov.it/iocs?token=[redacted]70a54&type=url
Per firewall (solo IP)	https://cert-agid.gov.it/iocs?token=[redacted]54&type=ip
Per firewall (solo domini, con estensione CSV)	https://cert-agid.gov.it/iocs[redacted]domain.csv
Per firewall (solo URL, con estensione CSV)	https://cert-agid.gov.it/iocs[redacted]54/url.csv

Cosa succede se mi registro

AGID | Agenzia per l'Italia digitale

Gentile Responsabile per la Transizione al Digitale,

da diversi mesi gli attacchi informatici contro i sistemi della PA sono in notevole aumento e rappresentano una **seria minaccia** per la protezione dei dati sensibili dei cittadini e per la continuità dei servizi pubblici.

Per affiancare le Pubbliche Amministrazioni nelle attività di contrasto alle minacce informatiche, l'Agenzia per l'Italia Digitale mette a disposizione delle PA diversi **servizi e strumenti gratuiti** che offrono informazioni utili a identificare compromissioni o attività malevole all'interno dei sistemi IT (come campagne malware e phishing), a mitigare i danni in caso di violazione e a rimanere aggiornati sulle campagne malevoli e gli attacchi in corso.

In particolare, il **flusso di Indicatori di compromissione** (**Feed IoC**), realizzato dal CERT-AGID, condivide con le Amministrazioni che ne fanno richiesta i dati raccolti e analizzati dall'Agenzia nel corso delle quotidiane attività di monitoraggio e prevenzione.

Gli Indicatori di Compromissione possono includere:

- indirizzi IP sospetti o utilizzati da malintenzionati;

- hash di file malevoli (valori che identificano in modo univoco file pericolosi);

- URL o domini coinvolti in attività malevoli.

La invitiamo, pertanto, a iscrivere al più presto la sua Amministrazione a questo flusso, compilando il modulo di accreditamento disponibile - insieme alle indicazioni operative - al seguente indirizzo:

https://cert-agid.gov.it/scarica-il-modulo-accreditamento-feed-ioc/

Il CERT-AGID offre anche la nuova versione del software hashr, che consente di eseguire scansioni sui sistemi locali alla ricerca di file malevoli; è possibile scaricare hashr e la relativa guida d'uso al seguente indirizzo:

https://cert-agid.gov.it/strumenti/

Utilizzando in sinergia hashr e il Feed IoC aumenterà significativamente la capacità della Sua amministrazione di individuare le minacce informatiche, **incrementando la sicurezza complessiva** delle infrastrutture digitali.

Per ulteriori informazioni, la invitiamo a visitare la sezione Sicurezza del sito istituzionale dell'Agenzia, il sito tematico del CERT-AGID o a contattarci via mail all'indirizzo info@cert-agid.gov.it

Grazie per l'attenzione.
Agenzia per l'Italia Digitale

Indicazioni nel piano triennale

Obiettivo 7.6 – Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA

CAP7.PA.20

CAP7.PA.20 — PIANIFICATA

Data di inizio
Dal **01 Feb 2024**

Descrizione
Le PA dovranno dotarsi degli strumenti idonei all'acquisizione degli IoC ed accreditarsi al CERT-AGID.

Attività operative - descrizione di dettaglio

L'ente ha pianificato l'attività nel corso del 2024.

Azioni importanti da compiere:

Data inizio	Data fine	Budget previsto	Budget speso
01/02/2024	31/12/2024	€ 0	€ 0