



TASSONOMIA DEGLI INCIDENTI

(in attuazione dell'articolo 1, comma 3-bis, del D.L. n. 105/2019)

Allegato A, articolo 3, comma 1			
Identificativo	Categoria	Descrizione	
ICP-C-1	Accesso iniziale (<i>Initial exploitation</i>)	Accesso iniziale (<i>Initial access</i>). Il soggetto ha evidenza dell'effettivo accesso non autorizzato all'interno della rete attraverso vettori di infezione, lo sfruttamento di vulnerabilità di risorse esposte pubblicamente o qualsiasi altra tecnica nota.	
ICP-C-2	Esecuzione (<i>Execution</i>)	Esecuzione (<i>Execution</i>). Il soggetto ha evidenza dell'effettiva esecuzione non autorizzata di codice o malware all'interno della rete aziendale.	
ICP-C-3	Installazione (<i>Establish persistence</i>)	Ottenimento di privilegi di livello superiore (<i>Privilege Escalation</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere permessi di livello superiore su un sistema o una rete.	
ICP-C-4		Persistenza (<i>Persistence</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte su un sistema o all'interno della rete, utili ad ottenere persistenza di codice malevolo o a garantire un accesso.	
ICP-C-5		Evasione delle difese (<i>Defence Evasion</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, di elusione di politiche e/o sistemi di sicurezza, volte ad evitare il rilevamento durante un tentativo di compromissione.	
ICP-C-6		Comando e Controllo (<i>Command and Control</i>). Il soggetto ha evidenza di comunicazioni non autorizzate verso l'esterno della rete.	
ICP-C-7		Movimenti laterali (<i>Lateral Movement</i>)	Esplorazione (<i>Discovery</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili a effettuare attività di ricognizione per acquisire conoscenze sul sistema e sulla rete interna.
ICP-C-8			Raccolta di credenziali (<i>Credential Access</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad acquisire, dall'interno della rete, credenziali valide per l'autenticazione alle risorse di rete o ne rinviene copie non autorizzate.
ICP-C-9	Movimenti laterali (<i>Lateral Movement</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad accedere, controllare o eseguire codice tra le risorse interne della rete.		
ICP-C-10	Azioni sugli obiettivi (<i>Actions on objectives</i>)	Raccolta (<i>Collection</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a ricercare e/o raccogliere, dall'interno della rete, dati riservati e/o sensibili ovvero ne rileva la presenza al di fuori dei sistemi autorizzati alla trattazione degli stessi.	
ICP-C-11		Esfiltrazione (<i>Exfiltration</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad esfiltrare dati dall'interno della rete verso risorse esterne.	
ICP-C-12		Inibizione delle funzioni di risposta (<i>Inhibit Response Function</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a inibire l'intervento delle funzioni di sicurezza, di protezione e di "quality assurance" dei sistemi di controllo industriale predisposte per rispondere a un disservizio o a uno stato anomalo.	
ICP-C-13		Compromissione dei processi di controllo (<i>Impair Process Control</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a manipolare, disabilitare o danneggiare i processi di controllo fisico di sistemi di controllo industriale.	
ICP-C-14		Disservizio intenzionale (<i>Impact</i>). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a manipolare, degradare, interrompere o distruggere i sistemi, i servizi o i dati. In tale ambito rientrano ad esempio gli eventi di tipo <i>Denial of Service/Distributed Denial of Service</i> che hanno impatto sui beni ICT.	
ICP-C -15	Ricognizione (<i>Reconnaissance</i>) riferita ad attività di <i>spearphishing</i>	La ricognizione consiste in tecniche che gli avversari adottano per raccogliere, attivamente o passivamente, informazioni potenzialmente sfruttabili per successive attività. Nella specifica categoria sono da ricomprendere le campagne, ancorché prive di impatto su assetti aziendali, rilevate via posta elettronica (PEO e/o PEC) e costituite da messaggi, altamente personalizzati (<i>spearphishing</i>), indirizzati a utenti multipli della stessa organizzazione e finalizzati alla cattura di informazioni, ad esempio, tramite l'uso di allegati malevoli o collegamenti web.	

Rielaborazione a cura della Divisione Rapporti istituzionali, relazioni esterne e comunicazione di ACN