Elementi essenziali e gestione della sicurezza informatica per il settore energetico

CSP001_C_E

PRESENTAZIONE DI:
RUBEN RIOS
UNIVERSITÀ DI MALAGA, SPAGNA

Ringraziamenti

- *Cofinanziato dall'Unione Europea. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli dell'autore/degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'HADEA. Né l'Unione Europea né l'autorità concedente possono essere ritenute responsabili per essi.*
- *Accordo di progetto n. 101083594*

Argomento 3: Minacce e vulnerabilità nel settore energetico vulnerabilità

Panoramica

- Identificare e classificare le minacce comuni alla sicurezza informatica nel settore energetico, quali malware, ransomware, phishing e ingegneria sociale
- Riconoscere le vulnerabilità specifiche dei sistemi energetici, tra cui software obsoleti, password deboli e vulnerabilità non corrette
- Le minacce e le vulnerabilità specifiche del settore energetico includono attacchi mirati ai sistemi SCADA, alle reti intelligenti e ad altre risorse energetiche critiche
- Comprendere il ruolo dell'errore umano e delle minacce interne nella sicurezza informatica nel settore energetico

Ruben Rios, Università di Malaga, Spagna

Argomento 3: Minacce e vulnerabilità nel settore energetico vulnerabilità nel settore energetico

Panoramica

- **Identificare e classificare le minacce comuni alla sicurezza informatica nel settore energetico, quali malware, ransomware, phishing e ingegneria sociale**
- Riconoscere le vulnerabilità specifiche dei sistemi energetici, tra cui software obsoleti, password deboli e vulnerabilità non corrette
- Le minacce e le vulnerabilità specifiche del settore energetico includono attacchi mirati ai sistemi SCADA, alle reti intelligenti e ad altre risorse energetiche critiche
- Comprendere il ruolo dell'errore umano e delle minacce interne nella sicurezza informatica nel settore energetico

Ruben Rios, Università di Malaga, Spagna

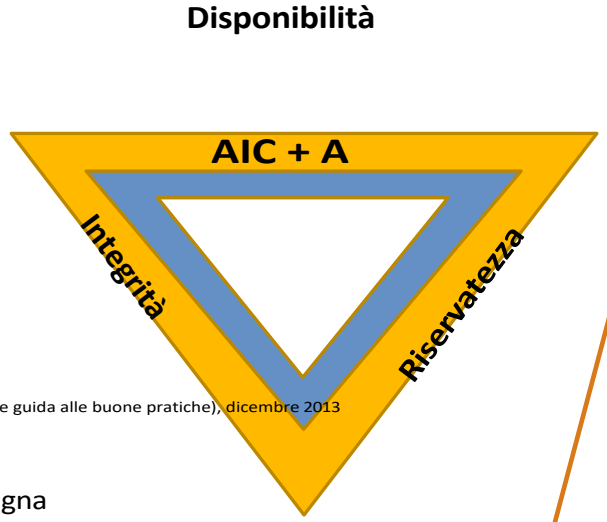
Minacce comuni nei sistemi energetici

- Nel 2013, l'ENISA ha pubblicato il rapporto "*Smart Grid Threat Landscape and Good Practice* Guide" (*Panorama delle minacce alle reti* intelligenti *e guida alle buone pratiche)* con uno studio completo sulle minacce alle reti intelligenti
- Tuttavia, il numero di minacce è aumentato notevolmente negli ultimi anni, come dimostrano sia
  - La matrice degli attacchi fornita da MITRE ATT&CK e
  - dalle relazioni annuali dell'ENISA sul panorama delle minacce nei diversi settori

Fonte: ENISA, "Smart Grid Threat Landscape and Good Practice Guide", dicembre 2013
URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

Minacce comuni nei sistemi energetici

- Nel 2013, l'ENISA ha pubblicato il rapporto "*Smart Grid Threat Landscape and Good Practice* Guide" (*Panorama delle minacce alle reti* intelligenti *e guida alle buone pratiche)* con uno studio completo sulle minacce alle reti intelligenti
- Tuttavia, il numero di minacce è aumentato notevolmente negli ultimi anni, come dimostrano sia
  - La matrice degli attacchi fornita da MITRE ATT&CK e
  - dalle relazioni annuali dell'ENISA sul panorama delle minacce nei diversi settori
- Sulla base di queste fonti, classifichiamo le minacce in questo settore utilizzando il tradizionale **AIC + A**
  - Disponibilità
  - Integrità
  - Integrità
  - Autenticazione



Fonte: ENISA, "Smart Grid Threat Landscape and Good Practice Guide" (Panorama delle minacce alle reti intelligenti e guida alle buone pratiche), dicembre 2013
URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

Minacce comuni nei sistemi energetici

- Più specificamente, le minacce "**AIC + A**" si riferiscono a:
  - **(A) Disponibilità**: Denial of Services (DoS) o mancato utilizzo corretto delle risorse
  - **(I) Integrità**: modifica delle risorse legittime del sistema o generazione di dati o configurazioni falsi
  - **(C) Riservatezza**: accesso non autorizzato alle risorse legittime di un sistema contenente informazioni private o sensibili
  - **(A) Autenticazione**: furto di identità o sostituzione di persona degli utenti

Minacce comuni nei sistemi energetici

- Più specificamente, le minacce "**AIC + A**" si riferiscono a:
  - **(A) Disponibilità**: Denial of Services (DoS) o mancato utilizzo corretto delle risorse
  - **(I) Integrità**: modifica delle risorse legittime del sistema o generazione di dati o configurazioni falsi
  - **(C) Riservatezza**: accesso non autorizzato alle risorse legittime di un sistema contenente informazioni private o sensibili
  - **(A) Autenticazione**: furto di identità o sostituzione di persona degli utenti
- Per AIC+A, esploreremo tre diverse tendenze
  - **Minacce tradizionali** che continuano a presentarsi nei sistemi di alimentazione
  - **Minacce recenti** nei sistemi di alimentazione
  - **Minacce future** nei sistemi di alimentazione

Minacce comuni nei sistemi energetici

- Più specificatamente, le minacce "**AIC + A**" si riferiscono a:
  - **(A) Disponibilità**: Denial of Services (DoS) o mancato utilizzo corretto delle risorse
  - **(I) Integrità**: modifica delle risorse legittime del sistema o generazione di dati o configurazioni falsi
  - **(C) Riservatezza**: accesso non autorizzato alle risorse legittime di un sistema, contenenti informazioni private o sensibili
  - **(A) Autenticazione**: furto di identità o sostituzione di persona degli utenti
- Per quanto riguarda AIC+A, esploreremo tre diverse tendenze
  - **Minacce tradizionali** che continuano a presentarsi nei sistemi di alimentazione
  - **Minacce recenti** nei sistemi di alimentazione
  - **Minacce future** nei sistemi di alimentazione
- Gli obiettivi colpiti potrebbero essere:
  - **Energia** - infrastrutture / rete
  - **Controllo** - componenti cyber-fisici
  - **Utenti/organizzazioni** - informazioni sensibili

Tendenze tradizionali delle minacce nei sistemi di alimentazione

Tendenze attuali delle minacce nei sistemi di alimentazione

Tendenze future delle minacce nei sistemi di alimentazione

CSP001_C_E – ARGOMENTO 3: Ruben Rios, Università di Malaga, Spagna

Tendenze tradizionali delle minacce nei sistemi energetici

Tendenze attuali delle minacce nei sistemi elettrici

Tendenze future delle minacce nei sistemi di alimentazione

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze tradizionali*

- Alcune delle minacce più comuni e tradizionali nei sistemi di alimentazione sono le seguenti:

Minacce tradizionali	Descrizione	A	I	C	A	Effetti su / impatto finale: Energia	Controllo	Utente
Minacce causali	Qualsiasi minaccia involontaria causata da uno sfruttamento imprevisto di un guasto/errore, da un disastro naturale o da **un'azione umana non deliberata**	X	X	X		**X**	X	X

- Dato che gli errori umani sono considerati una delle minacce più potenziali nei prossimi anni, approfondiremo questo argomento nel punto "***Comprendere il ruolo degli errori umani e delle minacce interne nella*** sicurezza informatica ***energetica***".

Fonte: ENISA, "Smart Grid Threat Landscape and Good Practice Guide" (Panorama delle minacce alle reti intelligenti e guida alle buone pratiche), dicembre 2013, URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze tradizionali*

- Alcune delle minacce più comuni e tradizionali nei sistemi di alimentazione sono le seguenti:

						Effetti su / impatto finale		
Minacce tradizionali	**Descrizione**	**A**	**I**	**C**	**A**	**Energia**	**Controllo**	**Utente**
Minacce causali	Qualsiasi minaccia involontaria causata da uno sfruttamento imprevisto di un guasto/errore, da un disastro naturale o da un'azione umana non deliberata	X	X	X		X	X	X
Minacce fisiche	Qualsiasi danno fisico "deliberato" all'infrastruttura e alle sue risorse, come sabotaggio o vandalismo, furto di componenti, fuga di informazioni, ecc.	X	X	X		X	X	X

Fonte: ENISA, "Smart Grid Threat Landscape and Good Practice Guide" (Panorama delle minacce alle reti intelligenti e guida alle buone pratiche), dicembre 2013, URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze tradizionali*

- Alcune delle minacce più comuni e tradizionali nei sistemi di alimentazione sono le seguenti:

Minacce tradizionali	Descrizione	A	I	C	A	Effetti su / impatto finale: Energia	Controllo	Utente
Minacce causali	Qualsiasi minaccia involontaria causata da uno sfruttamento imprevisto di un guasto/errore, da un disastro naturale o da un'azione umana non deliberata	X	X	X		X	X	X
Minacce fisiche	Qualsiasi danno fisico "deliberato" all'infrastruttura e alle sue risorse, come sabotaggio o vandalismo, furto di componenti, fuga di informazioni, ecc.	X	X	X		X	X	X
Denial of Service (DoS) / interruzioni	Qualsiasi mancanza di disponibilità di risorse essenziali, quali la rete elettrica e la sua energia, le risorse di controllo o i dati	X				X	X	X

Fonte: ENISA, "Smart Grid Threat Landscape and Good Practice Guide" (Panorama delle minacce alle reti intelligenti e guida alle buone pratiche), dicembre 2013, URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze tradizionali*

- Alcune delle minacce più comuni e tradizionali nei sistemi di alimentazione sono le seguenti:

						Effetti su / impatto finale		
Minacce tradizionali	**Descrizione**	**A**	**I**	**C**	**A**	**Energia**	**Controllo**	**Utente**
Minacce causali	Qualsiasi minaccia involontaria causata da uno sfruttamento imprevisto di un guasto/errore, da un disastro naturale o da un'azione umana non deliberata	X	X	X		X	X	X
Minacce fisiche	Qualsiasi danno fisico "deliberato" all'infrastruttura e alle sue risorse, come sabotaggio o vandalismo, furto di componenti, fuga di informazioni, ecc.	X	X	X		X	X	X
Denial of Service (DoS) / interruzioni	Qualsiasi mancanza di disponibilità di risorse essenziali, quali la rete elettrica e la sua energia, le risorse di controllo o i dati	X				X	X	X
Attività illecite, abusi	Qualsiasi azione dolosa che possa comportare penetrazione, intrusione, uso/accesso non autorizzato alle risorse, furto d'identità, manipolazione delle risorse, falsificazione dei dati, fuga di dati, DoS o infezione	X	X	X	X		X	X

Fonte: ENISA, "Smart Grid Threat Landscape and Good Practice Guide" (Panorama delle minacce alle reti intelligenti e guida alle buone pratiche), dicembre 2013, URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze tradizionali*

- Alcune delle minacce più comuni e tradizionali nei sistemi di alimentazione sono le seguenti:

						Effetti su / impatto finale		
Minacce tradizionali	**Descrizione**	**A**	**I**	**C**	**A**	**Energia**	**Controllo**	**Utente**
Minacce causali	Qualsiasi minaccia involontaria causata da uno sfruttamento imprevisto di un guasto/errore, da un disastro naturale o da un'azione umana non deliberata	X	X	X		X	X	X
Minacce fisiche	Qualsiasi danno fisico "deliberato" all'infrastruttura e alle sue risorse, come sabotaggio o vandalismo, furto di componenti, fuga di informazioni, ecc.	X	X	X		X	X	X
Denial of Service (DoS) / interruzioni	Qualsiasi mancanza nella disponibilità di risorse essenziali, quali la rete e la sua energia, le risorse di controllo o i dati	X				X	X	X
Attività illecite, abusi	Qualsiasi azione dannosa che possa comportare penetrazione, intrusione, uso/accesso non autorizzato alle risorse, furto d'identità, manipolazione delle risorse, falsificazione dei dati, fuga di dati, DoS o infezione	X	X	X	X	X	X	X
Intercettazione, intercettazione, dirottamento	Qualsiasi attività che comporti l'intercettazione delle comunicazioni, Man-in-the-Middle (MitM), ricognizione, raccolta di informazioni, inoltro di messaggi, ecc.		X	X	X		X	X

Fonte: ENISA, "Smart Grid Threat Landscape and Good Practice Guide" (Panorama delle minacce alle reti intelligenti e guida alle buone pratiche), dicembre 2013, URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

Tendenze tradizionali delle minacce nei sistemi di alimentazione

Tendenze attuali delle minacce nei sistemi di alimentazione

Tendenze future delle minacce nei sistemi di alimentazione

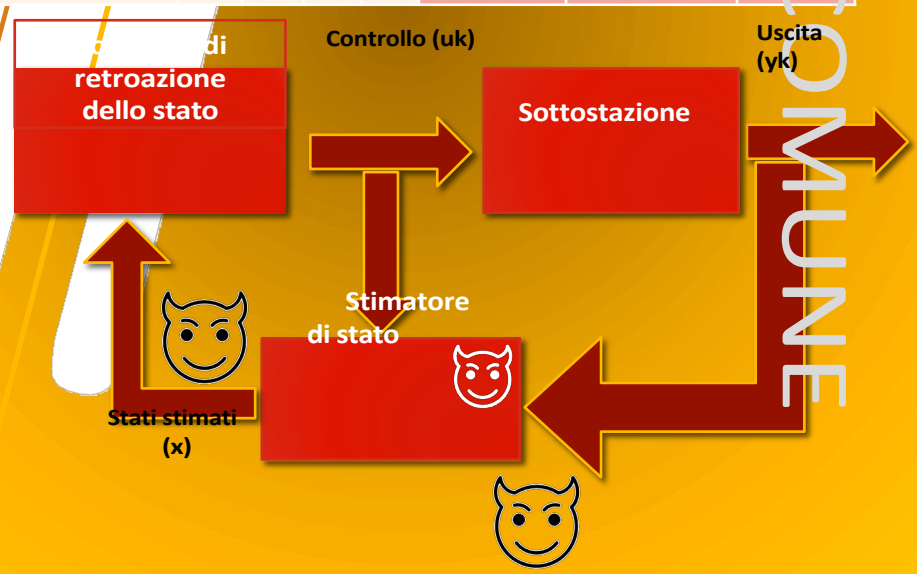
CSP001_C_E – ARGOMENTO 3: Ruben Rios, Università di Malaga, Spagna

Minacce comuni all'AIC+A nei sistemi energetici – *Tendenze attuali*

- Le minacce più recenti includono:

Minacce attuali	Descrizione	A	I	C	A	Effetti su / impatto finale: Energia	Controllo	Utente
Attacchi di tipo False Data Injection (FDI)	Qualsiasi falsificazione dello stato di controllo volta ad alterare le prestazioni dell'infrastruttura. Ciò può variare dalla falsificazione dei pacchetti C&C all'inserimento di misurazioni false nei contatori alle stime dello stato.		X			X	X	X
Attacchi furtivi degli investimenti diretti esteri	Qualsiasi azione FDI ma in modo furtivo		X			X	X	X

- Esistono alcune strategie di attacco FDI basate su:
  - **Flusso di potenza**: i modelli di attacco mirano a modificare la linearità del flusso di potenza
  - **Architettura**: gli attacchi FDI modificano le misurazioni ricevute e gestite dagli stimatori di stato. Nei sistemi centralizzati, l'obiettivo è lo stimatore di stato (1 singolo elemento)
  - **Metodologia**: Modifica delle misurazioni in base al livello di conoscenza del contesto, come le informazioni sulla topologia, la topologia della rete o i modelli di dati applicati (ad esempio, ML e la sua inferenza)



Fonte: H. T. Reda, A. Anwar, A, N. Mahmood, Z. Tari, "A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids" (Una tassonomia delle strategie di difesa informatica contro gli attacchi con dati falsi nelle reti intelligenti), ACM Computing Surveys, 55(14s), 1-37, 2023

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*

- Le minacce più recenti includono:

Minacce attuali	Descrizione	A	I	C	A	Effetti su / impatto finale: Energia	Controllo	Utente
Attacchi di tipo False Data Injection (FDI)	Qualsiasi falsificazione dello stato di controllo per alterare le prestazioni dell'infrastruttura. Ciò può variare dalla falsificazione dei pacchetti C&C all'inserimento di misurazioni false nei contatori alle stime dello stato.		X			X	X	X
Attacchi FDI furtivi	Qualsiasi azione FDI ma in modo furtivo		X			X	X	X
Malware	Software destinato a manipolare il normale funzionamento dei sistemi, all'insaputa o senza l'autorizzazione degli utenti che possiedono tali sistemi	X	X	X	X	X		

- Esistono molti tipi di malware: virus, worm, trojan, ransomware, ...
- Gli obiettivi del malware possono essere molto vari, dall'esfiltrazione/divulgazione di informazioni sensibili all'isolamento o alla distruzione di risorse critiche (ad esempio, controller).

Fonte: ENISA, "ENISA Threat Landscape 2023", 2023,
URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*

- **Virus**: codice software autoreplicante che, una volta eseguito, si "diffonde" nel sistema infettando in modo massiccio altri componenti software, principalmente eseguibili – richiede l'intervento umano
- **Worm**: è anch'esso un codice software autoreplicante, ma senza necessità di intervento umano
- **Trojan / backdoor**: un malware nascosto, i cui codici non sono in grado di autoreplicarsi o infettare altri programmi, ma vengono eseguiti e controllati da remoto da entità maligne per ottenere l'escalation dei privilegi, la fuga di informazioni, la modifica di servizi e dati, ecc.
- **Ransomware**: codice dannoso progettato per bloccare l'accesso al sistema fino al pagamento di un riscatto (ottenendo la chiave di sessione e le condizioni di crittografia).
  - La tecnica si concentra sulla crittografia delle informazioni presenti nel sistema

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*

- Le minacce più recenti includono:

Minacce attuali	Descrizione	Effetti su / impatto finale						
		A	I	C	A	Energia	Controllo	Utente
Attacchi di tipo False Data Injection (FDI)	Qualsiasi falsificazione dello stato di controllo per alterare le prestazioni dell'infrastruttura. Ciò può variare dalla falsificazione dei pacchetti C&C all'inserimento di misurazioni false nei contatori alle stime dello stato		X			X	X	X
Attacchi FDI furtivi	Qualsiasi azione FDI ma in modo furtivo		X			X	X	X
Malware	Software destinato a manipolare il normale funzionamento dei sistemi, all'insaputa o senza l'autorizzazione degli utenti che possiedono tali sistemi	X	X	X	X	X		
Ingegneria sociale	Tecniche per ottenere informazioni sensibili quali credenziali di sicurezza o modalità di accesso, finalizzate alla penetrazione o all'intrusione			X	X		X	X

- Esistono molte tecniche per estrarre informazioni private come le credenziali: **phishing / spear phishing** (tramite e-mail), **vishing** (tramite telefono), **HTTPS phishing** (reindirizzamento a un sito web falso), **pharming** (malware che reindirizza la vittima a un sito web falso), **angler phishing** (post falsi sui social media), ecc.

Fonte: ENISA, "ENISA Threat Landscape 2023", 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
Fonte: FORTINET, "19 tipi di attacchi di phishing, diversi tipi di attacchi di phishing", https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks, 2024

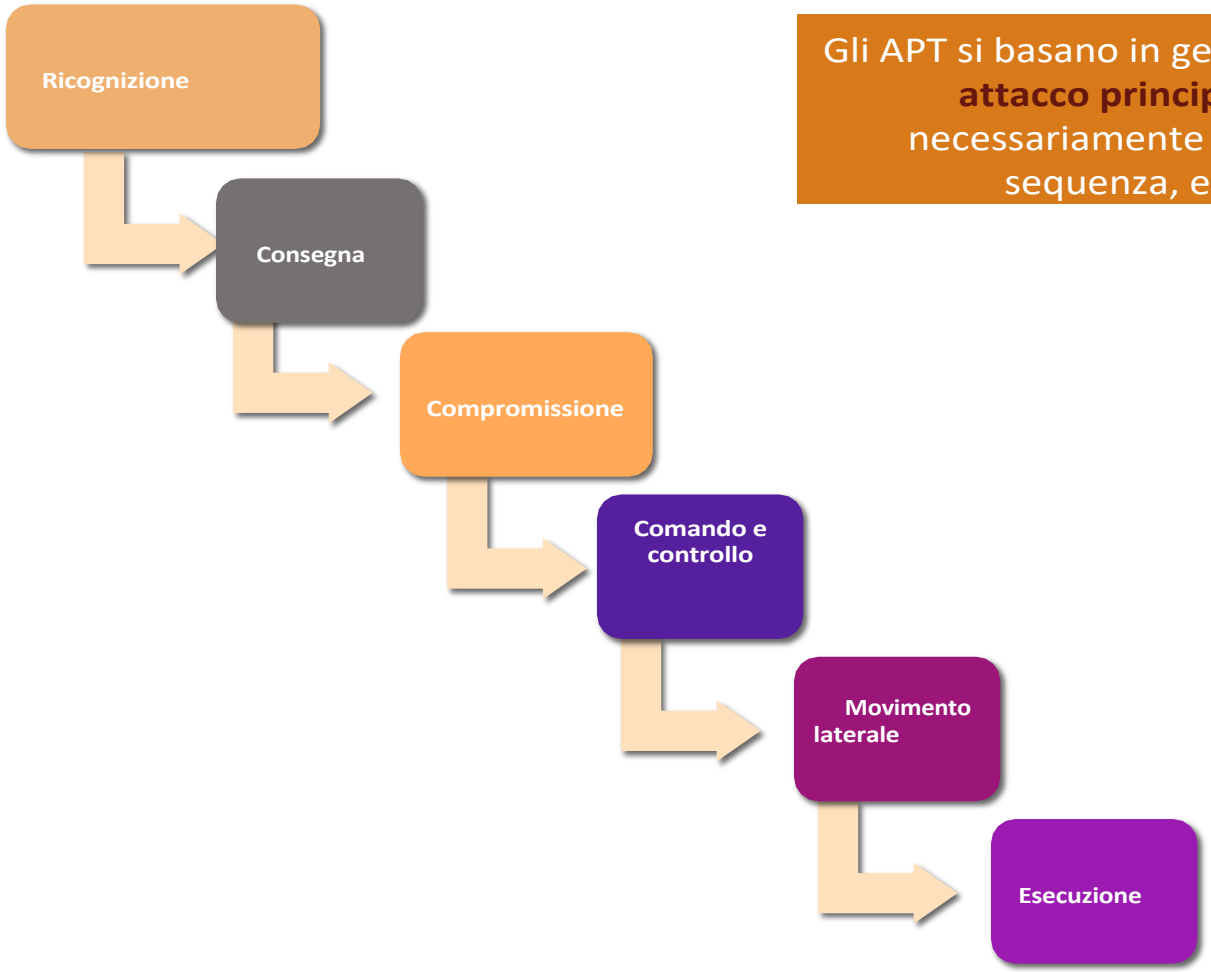
Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*

- Le minacce più recenti includono:

Minacce attuali	Descrizione	A	I	C	A	Effetti su / impatto finale: Energia	Controllo	Utente
Attacchi di iniezione di dati falsi (FDI)	Qualsiasi falsificazione dello stato di controllo volta ad alterare le prestazioni dell'infrastruttura. Ciò può variare dalla falsificazione dei pacchetti C&C all'iniezione di misurazioni false dei contatori alle stime dello stato		X			X	X	X
Attacchi FDI furtivi	Qualsiasi azione FDI ma in modo furtivo		X			X	X	X
Malware	Software destinato a manipolare il normale funzionamento dei sistemi, all'insaputa o senza l'autorizzazione degli utenti proprietari di tali sistemi	X	X	X	X	X	X	X
Ingegneria sociale	Tecniche volte a ottenere psicologicamente informazioni sensibili per la penetrazione o l'intrusione, quali credenziali di sicurezza o modalità di accesso			X	X		X	X
Minacce persistenti avanzate (APT)	Un APT è un attacco sofisticato, solitamente eseguito da avversari dotati di grandi risorse e protratto nel tempo, con l'obiettivo di distruggere dispositivi critici o sottrarre dati sensibili.	X	X	X	X	X	X	X

- Gli APT si concentrano sulla combinazione di più vettori di attacco che includono lo sfruttamento di **vulnerabilità zero-day**, insieme a tecniche "furtive" ed evasive.

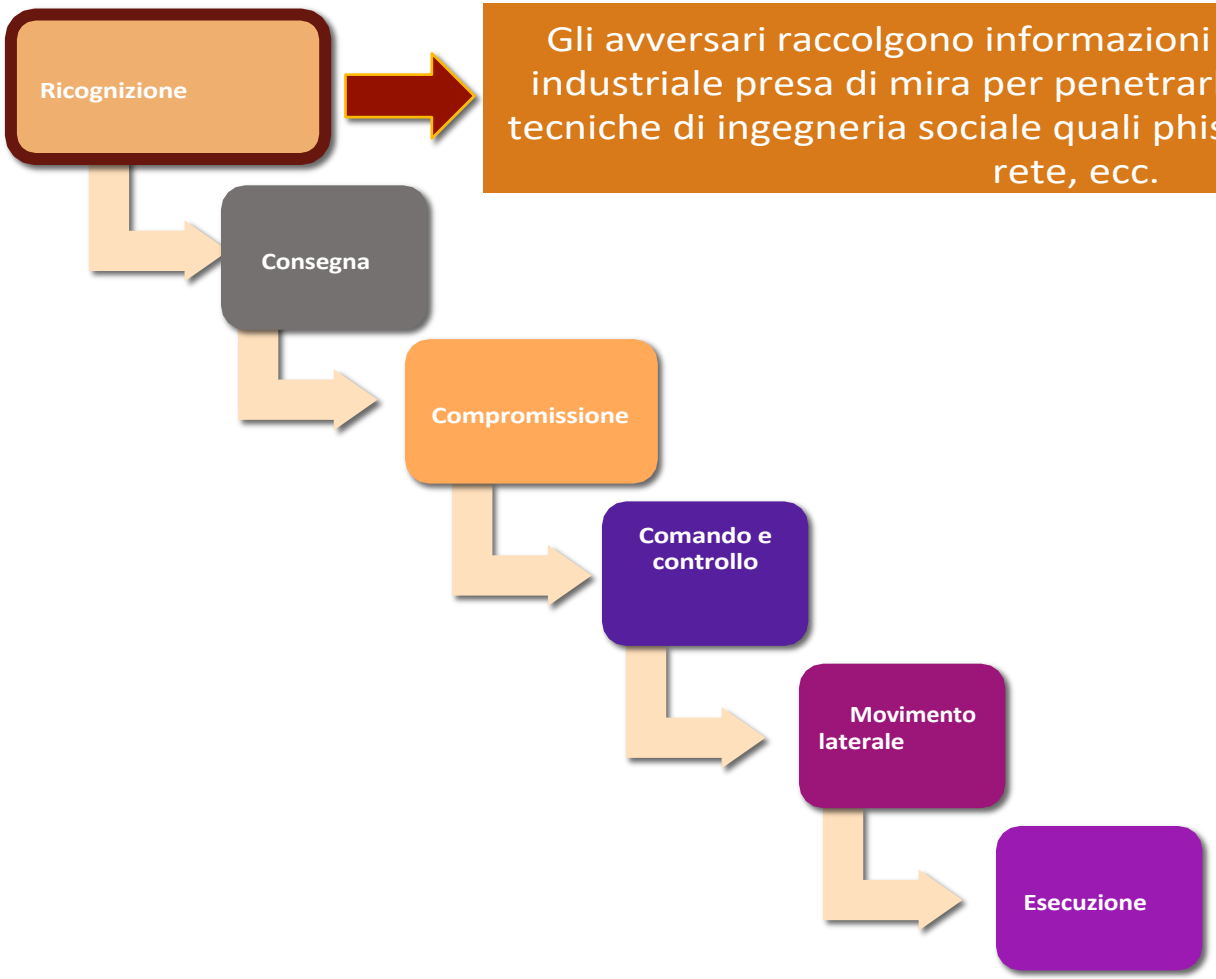
Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*



Gli APT si basano in genere su **6 fasi di attacco principali**, non necessariamente eseguite in sequenza, e tutte

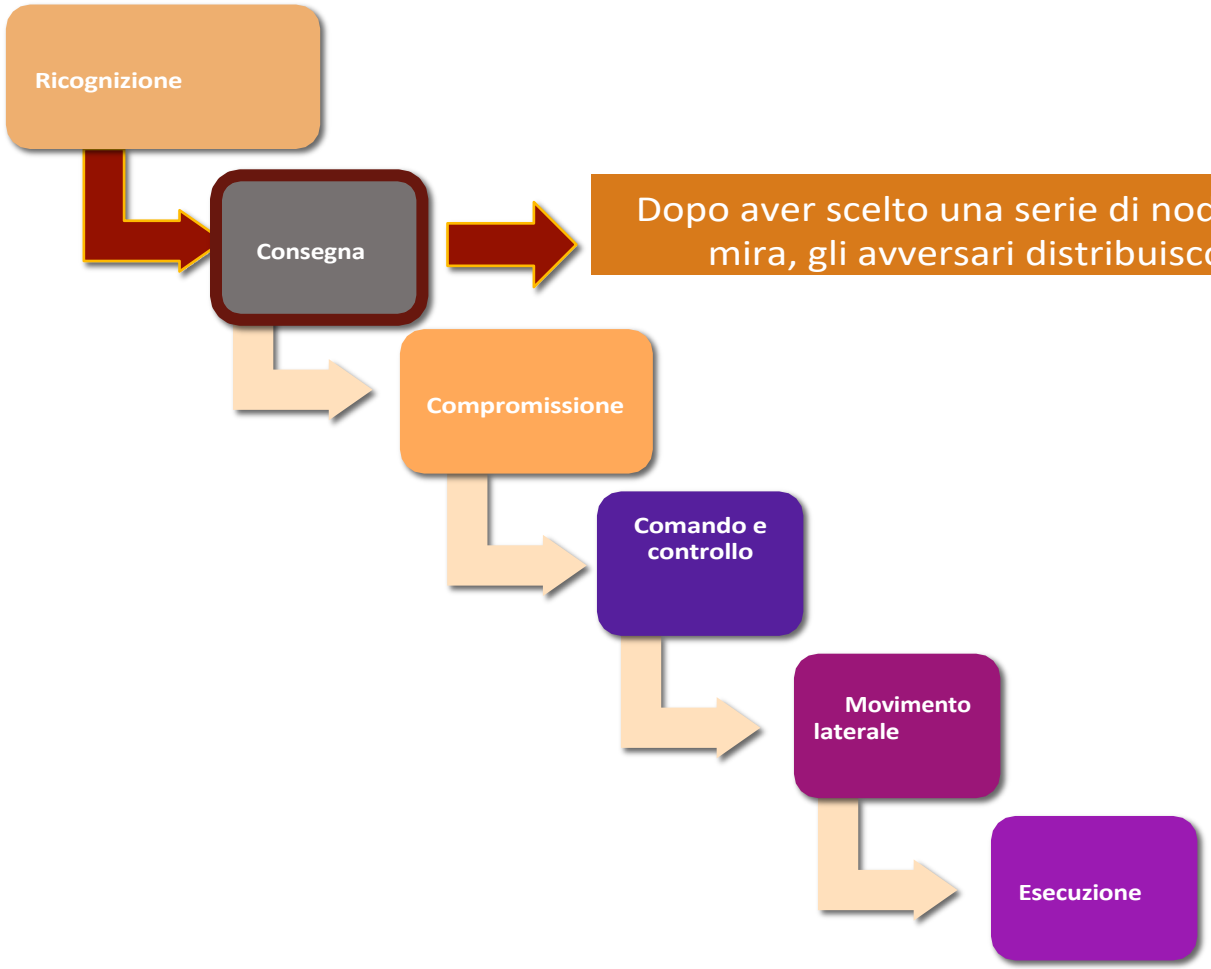
Fonte: J. E. Rubio, R. Roman, C. Alcaraz e Y. Zhang, "Monitoraggio delle minacce persistenti avanzate nelle infrastrutture critiche attraverso le dinamiche di opinione", Simposio europeo sulla ricerca nella sicurezza informatica (ESORICS 2018) vol. 11098, pagg. 555-574, 2018

Minacce comuni all'AIC+A nei sistemi di alimentazione - *Tendenze attuali*



Fonte: J. E. Rubio, R. Roman, C. Alcaraz e Y. Zhang, "Monitoraggio delle minacce persistenti avanzate nelle infrastrutture critiche attraverso le dinamiche dell'opinione", Simposio europeo sulla ricerca nella sicurezza informatica (ESORICS 2018) vol. 11098, pagg. 555-574, 2018

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*

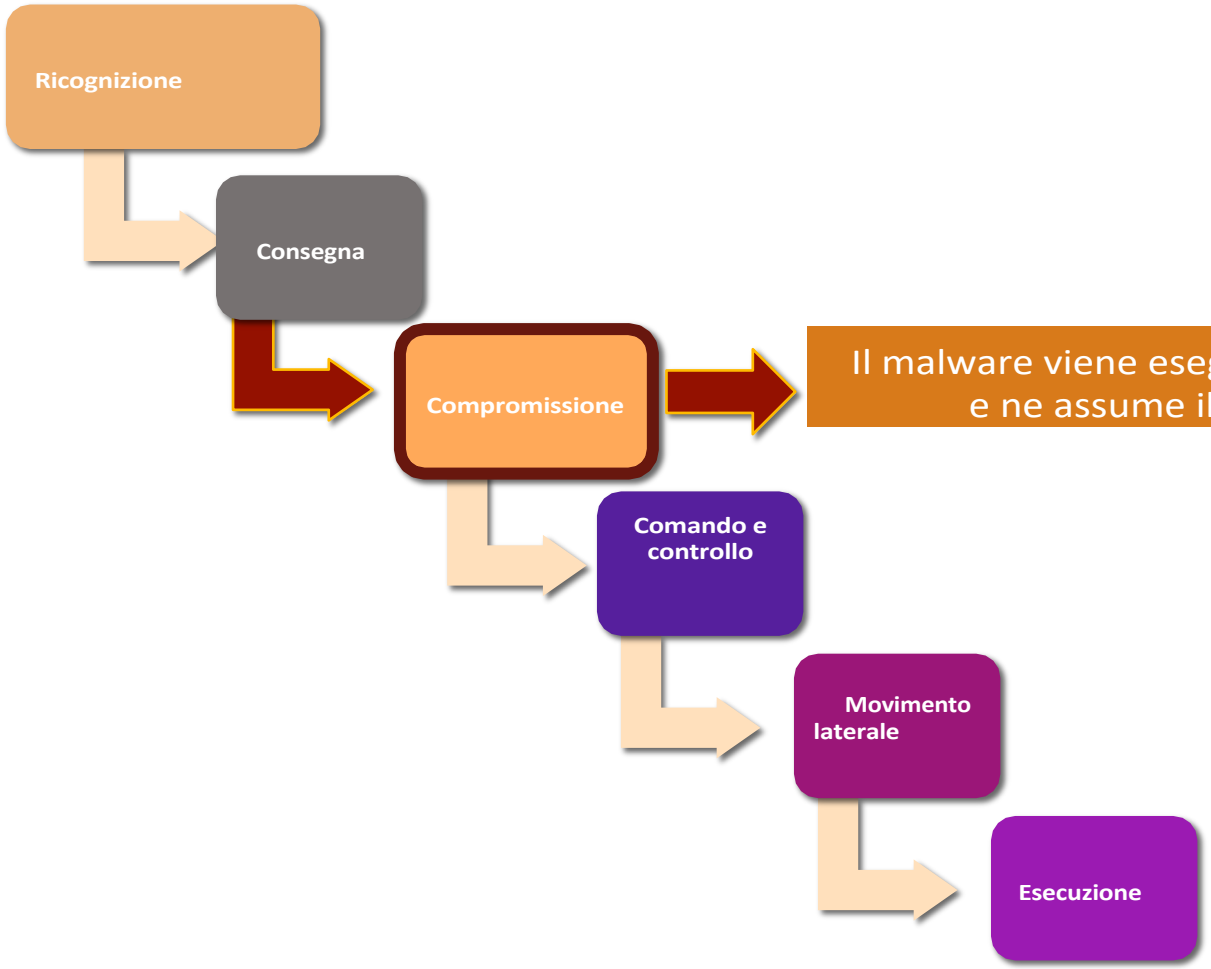


Dopo aver scelto una serie di nodi vulnerabili nella rete industriale presa di mira, gli avversari distribuiscono il malware

TASSONOMIA COMUNE

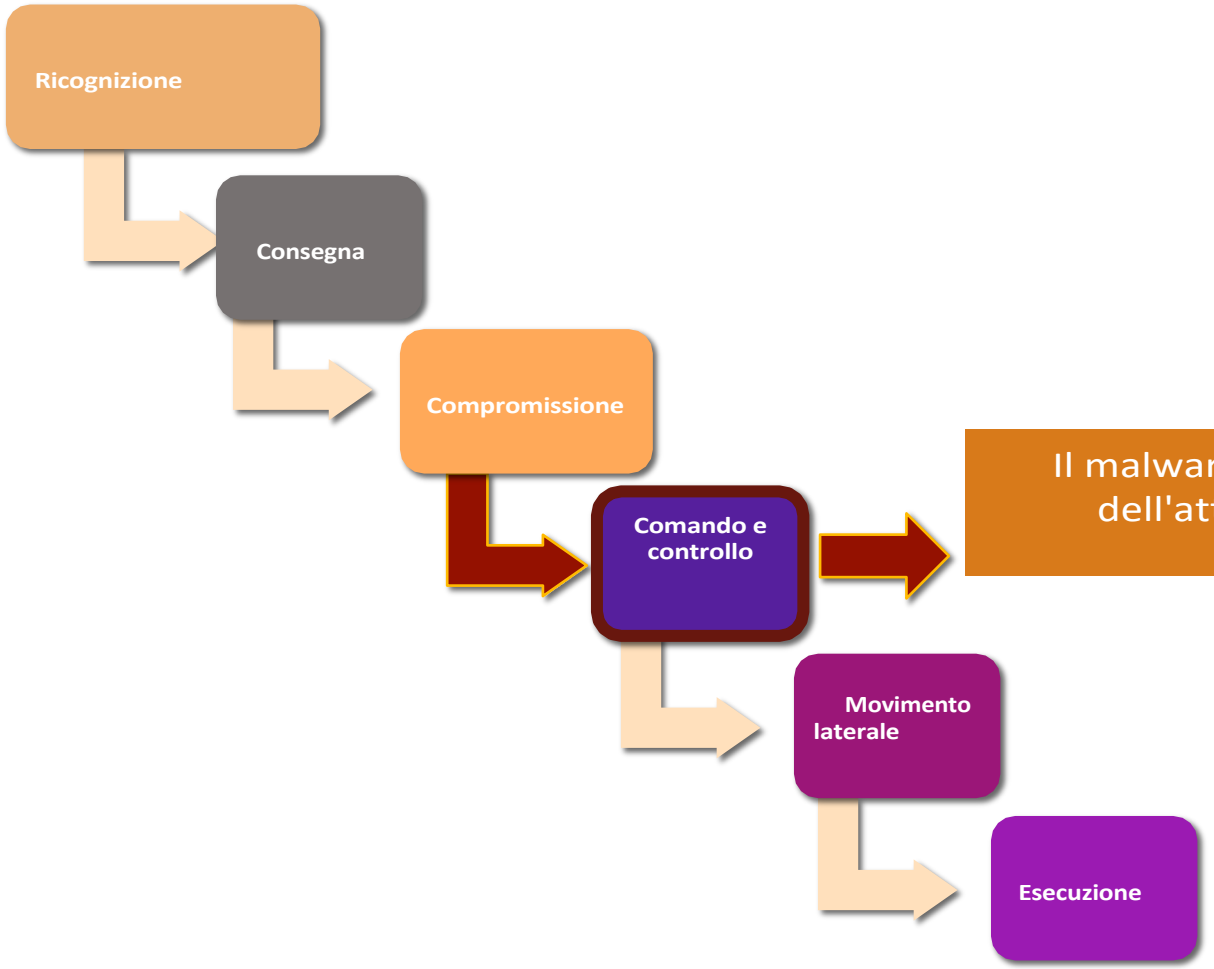
Fonte: J. E. Rubio, R. Roman, C. Alcaraz e Y. Zhang, "Monitoraggio delle minacce persistenti avanzate nelle infrastrutture critiche attraverso le dinamiche di opinione", Simposio europeo sulla ricerca nella sicurezza informatica (ESORICS 2018) vol. 11098, pagg. 555-574, 2018

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*



Fonte: J. E. Rubio, R. Roman, C. Alcaraz e Y. Zhang, "Monitoraggio delle minacce persistenti avanzate nelle infrastrutture critiche attraverso Opinion Dynamics", Simposio europeo sulla ricerca nella sicurezza informatica (ESORICS 2018) vol. 11098, pagg. 555-574, 2018

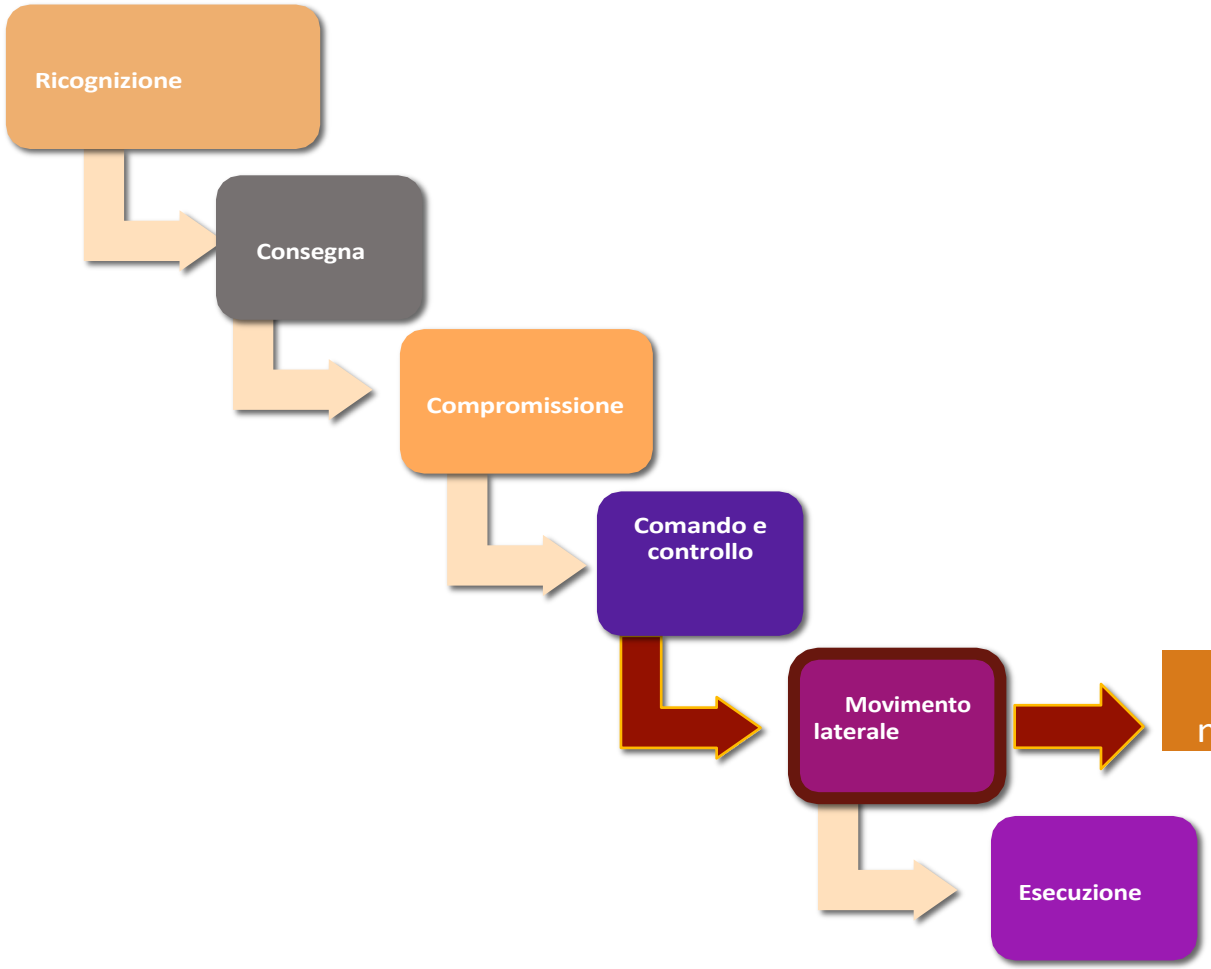
Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*



Il malware apre un canale di comunicazione con l'autore dell'attacco remoto, che verrà utilizzato per inviare comandi, estrarre informazioni, ecc.

Fonte: J. E. Rubio, R. Roman, C. Alcaraz e Y. Zhang, "Monitoraggio delle minacce persistenti avanzate nelle infrastrutture critiche attraverso le dinamiche dell'opinione", Simposio europeo sulla ricerca nella sicurezza informatica (ESORICS 2018) vol. 11098, pagg. 555-574, 2018

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*

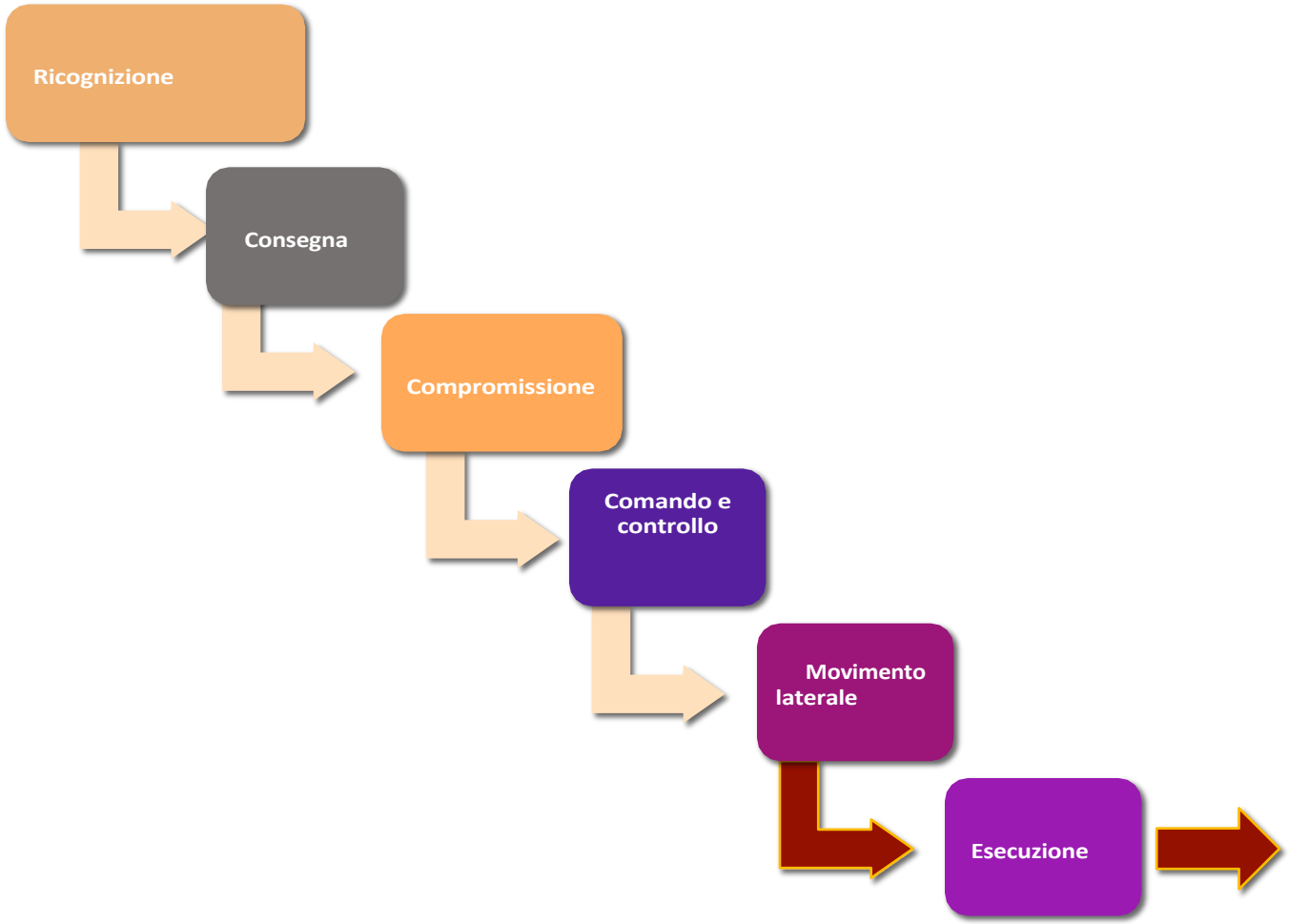


Il malware cerca altri dispositivi da compromettere mentre raccoglie informazioni sensibili

TASSONOMIA COMUNE

Fonte: J. E. Rubio, R. Roman, C. Alcaraz e Y. Zhang, "Monitoraggio delle minacce persistenti avanzate nelle infrastrutture critiche attraverso le dinamiche dell'opinione", Simposio europeo sulla ricerca nella sicurezza informatica (ESORICS 2018) vol. 11098, pagg. 555-574, 2018

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*



Il malware esegue infine l'attacco contro la rete industriale, che comporta **l'estrazione di dati sensibili o la distruzione di risorse**

TASSONOMIA COMUNE

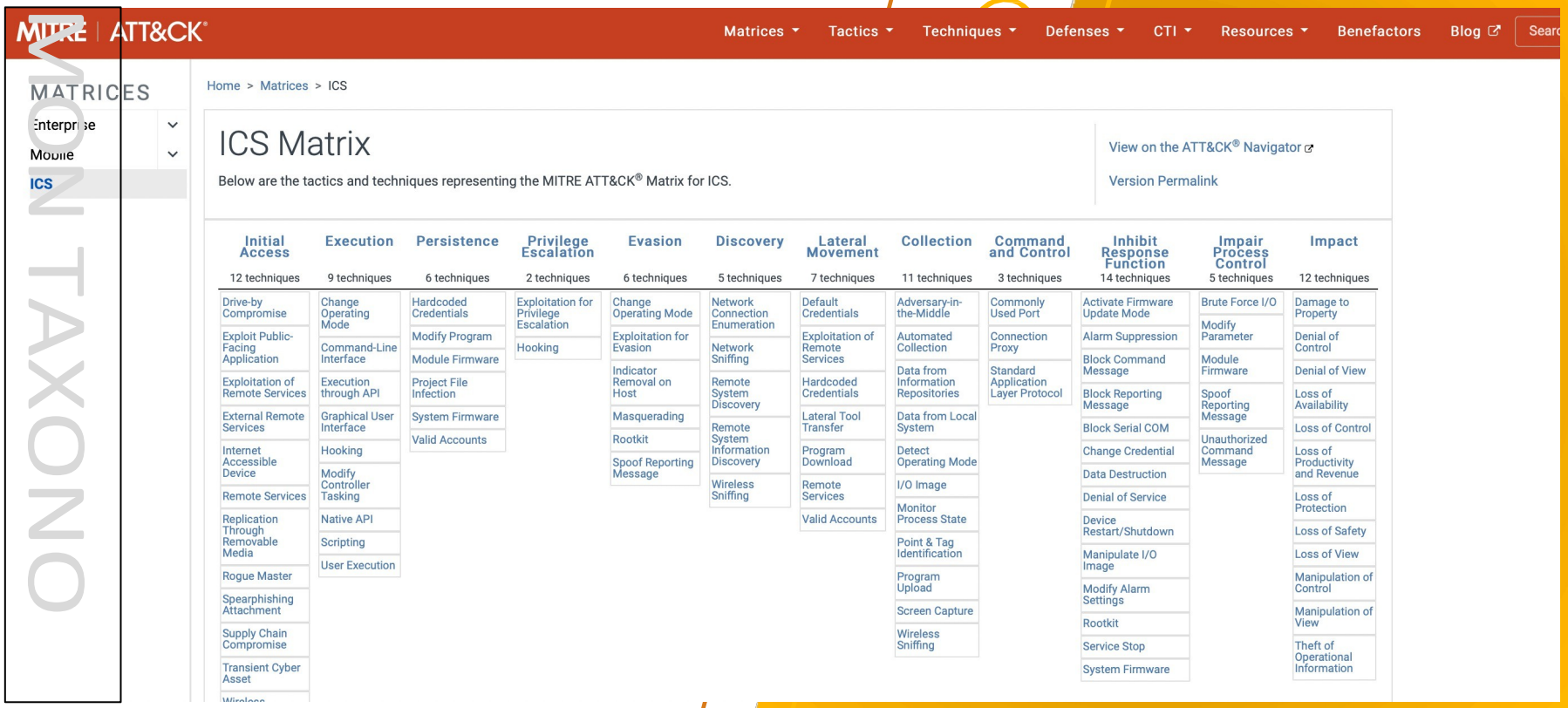
Fonte: J. E. Rubio, R. Roman, C. Alcaraz e Y. Zhang, "Monitoraggio delle minacce persistenti avanzate nelle infrastrutture critiche attraverso le dinamiche dell'opinione", Simposio europeo sulla ricerca nella sicurezza informatica (ESORICS 2018) vol. 11098, pagg. 555-574, 2018

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*

- Per mantenere la persistenza, i **movimenti e le azioni** (ad esempio C&C) devono essere eseguiti **in modo furtivo**
  - Mantenere la pazienza, evitare azioni/movimenti bruschi, nascondere azioni/dati dannosi, ecc.
- Esistono molte tecniche di attacco che rivelano informazioni sull' , riconoscono l'ambiente o sottraggono informazioni ad altri siti esterni, come ad esempio:
  - **Canale laterale**: analizzare i segnali di dati nei canali di comunicazione per ricavare fisicamente informazioni sensibili trasmesse da un peer di rete a un altro
  - **Canale nascosto**: manipolare i bersagli (ad esempio tramite un malware) e camuffare gli ordini C&C in pacchetti o segnali in un e al fine di esfiltrare informazioni quali misurazioni dei sensori o inviare comandi agli attuatori

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*

- MITRE ATT&CK fornisce anche le tattiche e le tecniche corrispondenti a MITRE ATT&CK® Matrice per ICS
- Come illustrato nella figura, le tattiche di attacco coincidono (nella maggior parte dei casi) con la kill chain di un attacco di tipo APT



Fonte della figura: MITRE ATT&CK
URL: https://attack.mitre.org/matrices/ics/, 2024

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze attuali*

- Le minacce più recenti includono:

Minacce attuali	Descrizione	A	I	C	A	Effetti / impatto finale: Energia	Controllo	Utente
Attacchi di iniezione di dati falsi (FDI)	Qualsiasi falsificazione dello stato di controllo volta a modificare le prestazioni dell'infrastruttura. Ciò può andare dalla falsificazione dei pacchetti C&C all'inserimento di misurazioni false nei contatori alle stime dello stato.		X			X	X	X
Attacchi FDI furtivi	Qualsiasi azione FDI ma in modo furtivo		X			X	X	X
Malware	Software progettato per manipolare il normale funzionamento dei sistemi, all'insaputa o senza l'autorizzazione degli utenti proprietari di tali sistemi.	X	X	X	X	X	X	X
Ingegneria sociale	Tecniche volte a ottenere psicologicamente informazioni sensibili per la penetrazione o l'intrusione, quali credenziali di sicurezza o modalità di accesso			X	X		X	X
Minacce persistenti avanzate (APT)	Un APT è un attacco sofisticato, solitamente eseguito da avversari dotati di grandi risorse e protratto nel tempo, con l'obiettivo di distruggere dispositivi critici o sottrarre dati sensibili.	X	X	X	X	X	X	X
Compromissione della catena di fornitura	Qualsiasi corruzione nella catena di fornitura può compromettere l'integrità delle dipendenze software e hardware e la loro affidabilità.	X	X	X	X	X	X	X

Fonte: ENISA, "ENISA Threat Landscape 2023", 2023,
URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Tendenze tradizionali delle minacce nei sistemi di alimentazione

Tendenze attuali delle minacce nei sistemi elettrici

Tendenze future delle minacce nei sistemi energetici (Minacce 2030)

TASSONOMIA COMUNE

Minacce comuni all'AIC+A nei sistemi di alimentazione – *Tendenze future*

- Il rapporto dell'ENISA intitolato "*Identifying Emerging Cyber Security Threats and Challenges for* 2030" (Identificazione delle minacce e delle sfide emergenti in materia di sicurezza informatica per il 2030) prevede alcune potenziali tendenze in materia di minacce per il 2030.

					Effetti su / impatto finale		
Minacce previste	**A**	**I**	**C**	**A**	**Energia**	**Controllo**	**Utente**
Compromissione della catena di approvvigionamento	X	X	X	X	X	X	X
Campagne di disinformazione		X		X			X
Perdita della privacy			X				X
Errore umano	X	X	X		X	X	X
Attacchi mirati (condotti da dispositivi intelligenti)	X	X	X	X	X	X	X
Mancanza di analisi e controllo	X	X			X	X	
Minacce ibride avanzate	X	X	X	X	X	X	X
Abuso dell'intelligenza artificiale	X	X	X	X	X	X	X

-

Fonte: ENISA, "*Identifying Emerging Cyber Security Threats and Challenges for 2030*" (Identificazione delle minacce e delle sfide emergenti in materia di sicurezza informatica per il 2030), 2023, https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

Osservazioni finali

- Abbiamo visto "come" il numero di minacce nei sistemi di alimentazione tende ad aumentare, fornendo una chiara panoramica di:
  - Tendenze **tradizionali** (ma persistenti) delle minacce
  - Tendenze **attuali**
  - Tendenze **possibili** e future
- Per tutte queste tendenze, abbiamo anche esaminato il loro impatto, in particolare su:
  - **Ener**gia e relative infrastrutture
  - **Controllo,** compresi i suoi componenti e le sue reti
  - **Utenti o organizzazioni**
- Nella maggior parte dei casi, il "controllo" può essere l'obiettivo più allettante per gli aggressori
  - Perché? Perché attraverso il controllo, gli aggressori potrebbero sferrare ulteriori attacchi contro l'energia e le sue risorse

Tendenze delle minacce	A	I	C	A	Energia	Controllo	Utente
Tradizionali	4	4	4	2	4	5	5
Attuale	3	5	4	4	5	6	6
Futuro	6	7	6	5	6	6	7

SIGNIFICATO

Riferimenti e fonti

1. ENISA, "Smart Grid Threat Landscape and Good Practice Guide" (Panorama delle minacce alle reti intelligenti e guida alle buone pratiche), dicembre 2013
   URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide
2. H. T. Reda, A. Anwar, A, N. Mahmood, Z. Tari, "A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids" (Una tassonomia delle strategie di difesa informatica contro gli attacchi con dati falsi nelle reti intelligenti), ACM Computing Surveys, 55(14s), 1-37, 2023
3. J. E. Rubio, R. Roman, C. Alcaraz e Y. Zhang, "Monitoraggio delle minacce persistenti avanzate nelle infrastrutture critiche attraverso le dinamiche dell'opinione", Simposio europeo sulla ricerca nella sicurezza informatica (ESORICS 2018) vol. 11098, pagg. 555-574, 2018.
4. ENISA, "ENISA Threat Landscape 2023", 2023,
   URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
5. FORTINET, “19 tipi di attacchi di phishing, diversi tipi di attacchi di phishing”,
   URL: https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks, 2024
6. ENISA, "Identificazione delle minacce e delle sfide emergenti in materia di sicurezza informatica per il 2030", 2023
   URL: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030
7. DeepL Translator per la revisione. URL: https://www.deepl.com/translator

Connettiti con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Grazie

Per qualsiasi domanda, non esitate a contattare:

- Ruben Rios Professore associato Università di Malaga
  ruben.rdp@uma.es