

Gli hacker non cercano solo l'AI: cercano chi decide le sue regole

Maria Cattini | 07/10/2026 | Open source intelligence

Un esperto di politiche sull'intelligenza artificiale riceve una proposta perfettamente compatibile con il proprio lavoro: partecipare a un comitato consultivo sull'AI. Un altro viene invitato a contribuire a un rapporto del Senato americano su controlli alle esportazioni e catene di approvvigionamento.

Non sono le solite email che annunciano una password scaduta o un pacco inesistente. Il mittente sembra conoscere il settore, gli argomenti sono credibili e le persone che firmano i messaggi esistono davvero.

Il problema è che quelle persone non hanno inviato le email.

È il meccanismo documentato da Proofpoint in una ricerca pubblicata il 1° ottobre 2026 su TA419, un attore che la società di sicurezza definisce "China-aligned" e orientato allo spionaggio. Secondo Proofpoint, nel luglio scorso il gruppo ha condotto campagne di credential phishing contro esperti di AI policy negli Stati Uniti, impersonando personalità note dell'economia e delle politiche sull'intelligenza artificiale. Reuters riferisce che i bersagli individuati erano meno di dieci.

La dimensione ridotta della campagna è proprio ciò che la rende interessante.

Qui non sembra esserci la ricerca di migliaia di account da compromettere. La scelta è chirurgica: poche persone, selezionate per ciò che potrebbero conoscere.

Il bersaglio non è sempre chi comanda

Quando pensiamo allo spionaggio legato all'intelligenza artificiale, è naturale immaginare il furto di codice, pesi dei modelli, chip, documenti tecnici o segreti industriali.

TA419 suggerisce di guardare anche altrove.

Proofpoint ha osservato il gruppo colpire esperti appartenenti a think tank, università e organizzazioni del settore legale. Reuters cita inoltre organizzazioni legate alla difesa tra i settori complessivamente presi di mira dal gruppo. L'obiettivo della campagna sull'AI, secondo la valutazione di Proofpoint, sarebbe stato raccogliere informazioni sugli sviluppi della politica e della regolamentazione statunitense dell'intelligenza artificiale.

Questo cambia la domanda.

Se volessimo conoscere in anticipo come potrebbero evolvere i controlli americani sull'esportazione di tecnologie AI, sarebbe necessariamente più utile compromettere l'account di un CEO?

Forse no.

Potrebbe essere molto interessante anche la posta di chi prepara analisi, partecipa a consultazioni, studia le conseguenze di una norma o frequenta le reti professionali nelle quali le diverse opzioni

vengono discusse prima di trasformarsi in decisioni ufficiali.

È un principio utile anche nell'OSINT: **visibilità pubblica e valore informativo non coincidono necessariamente.**

Prima del phishing c'è la ricerca

Il secondo elemento interessante è il lavoro necessario per costruire un'esca credibile.

A partire dall'8 luglio, secondo Proofpoint, TA419 ha impersonato Lynne Edwards Parker, già Principal Deputy Director dell'Office of Science and Technology Policy della Casa Bianca, e Heidi Crebo-Rediker, economista ed esperta di politica estera.

I messaggi proponevano attività coerenti con il profilo delle vittime: entrare in un fantomatico "AI Policy Advisory Committee" oppure collaborare a un rapporto attribuito alla Senate Committee on Foreign Relations dedicato agli export control dell'AI e alle supply chain.

A febbraio il gruppo aveva utilizzato una variante ancora diversa, impersonando un dipendente senior di Anthropic per contattare un analista di AI policy di un think tank americano. L'oggetto della mail riguardava una richiesta di feedback sull'integrazione militare di Claude, tema collegato a un dibattito reale.

Per costruire messaggi del genere bisogna prima comprendere il bersaglio.

Chi è? Di che cosa si occupa? Con chi potrebbe ragionevolmente entrare in contatto? Quale argomento potrebbe convincerlo a rispondere?

È qui che il caso diventa particolarmente interessante dal punto di vista OSINT. Informazioni pubbliche come incarichi, biografie professionali, pubblicazioni, conferenze, aree di ricerca e reti di relazioni possono aiutare un osservatore legittimo a ricostruire un ecosistema. Le stesse informazioni, usate con finalità ostili, possono contribuire a costruire un pretesto molto più convincente del phishing generico.

Non significa che Proofpoint abbia dimostrato quali specifiche fonti OSINT siano state utilizzate da TA419 per selezionare ogni vittima. Il report non lo stabilisce. Possiamo però osservare il risultato: esche fortemente contestualizzate rispetto al lavoro dei destinatari e identità reali utilizzate per renderle credibili.

Il messaggio pericoloso può sembrare quello più normale

Anche la sequenza dell'attacco merita attenzione.

Il primo messaggio non conteneva necessariamente il passaggio decisivo dell'attacco. Proofpoint descrive email iniziali apparentemente innocue, progettate per avviare una conversazione. Soltanto dopo la risposta della vittima arrivava un collegamento abbreviato che conduceva, attraverso più reindirizzamenti, all'infrastruttura di phishing.

È una differenza sostanziale.

La vittima non riceve semplicemente un link sospetto da uno sconosciuto. Prima può essersi instaurata una conversazione apparentemente sensata. Il collegamento arriva quando il contesto che dovrebbe giustificarlo è già stato costruito.

La catena tecnica descritta da Proofpoint era progettata per colpire account Microsoft 365/Entra ID e utilizzava una versione modificata di Frameless BitB, strumento open source basato sulla tecnica Browser-in-the-Browser. L'attacco incorporava anche una componente Adversary-in-the-Middle, o AitM, capace di inserirsi nel processo di autenticazione. Proofpoint descrive un sistema in grado di seguire la vittima attraverso il login, compresa l'autenticazione multifattore, e di catturare i cookie di sessione.

In termini semplici: **avere l'MFA attiva non rende automaticamente innocuo qualsiasi login avviato da un link ricevuto via email.**

Per questo Proofpoint raccomanda, per le organizzazioni esposte a questo tipo di attività, sistemi di autenticazione resistenti al phishing, come le passkey, e invita chi riceve contatti professionali inattesi a verificarli attraverso un canale indipendente.

Il piccolo esercizio OSINT: chi vale davvero in una rete?

Il caso permette di fare un esercizio utile senza cercare informazioni personali né costruire profili invasivi.

Prendiamo una politica pubblica qualsiasi e immaginiamo la rete che la circonda.

Al centro può esserci il decisore politico. Intorno, però, troviamo funzionari, consulenti, ricercatori universitari, think tank, avvocati, aziende, associazioni di settore ed esperti che producono analisi.

L'errore sarebbe ordinare automaticamente queste persone per notorietà.

Dal punto di vista dell'intelligence la domanda più utile è diversa: **chi potrebbe avere accesso anticipato a informazioni che diventeranno importanti in seguito?**

Possiamo sintetizzare il ragionamento così:

persona → ruolo → rete → possibile accesso → pretesto plausibile → valore informativo

È un modello di analisi, non la ricostruzione documentata del processo seguito da TA419. La distinzione è importante. Serve però a capire perché una persona quasi sconosciuta al grande pubblico possa diventare un bersaglio più interessante di un personaggio che compare ogni giorno sui giornali.

Cosa sappiamo davvero su TA419

[Proofpoint afferma di osservare TA419 almeno dall'aprile 2025](#) in campagne mirate contro persone appartenenti a think tank, contractor della difesa, università e studi legali negli Stati Uniti e in Giappone. Tra gli interessi osservati figurano difesa, sicurezza nazionale, energia, relazioni internazionali e politica estera. L'attenzione verso gli esperti di AI policy viene quindi interpretata dai ricercatori come un'estensione di interessi precedenti, non come un'attività completamente nuova.

Sull'attribuzione bisogna mantenere la formulazione corretta.

Proofpoint definisce TA419 un attore “China-aligned” e ritiene probabile che le campagne sostengano più ampi obiettivi di intelligence cinesi. Reuters, riportando il caso, ricorda che Pechino nega il coinvolgimento nelle attività di cyber-spionaggio che le vengono attribuite. Le evidenze pubbliche disponibili non autorizzano quindi a trasformare la valutazione della società di sicurezza nella formula più forte “il governo cinese ha ordinato questo attacco”.

È precisamente il tipo di distinzione che un'analisi OSINT dovrebbe conservare.

La verifica da fare quando un'email sembra perfetta

Il dettaglio più utile di questa storia non è un dominio malevolo, perché i domini possono cambiare. Non è neppure il nome TA419.

È il metodo.

Un messaggio può contenere il nostro argomento di ricerca, citare una discussione realmente in corso, arrivare apparentemente da una persona che avrebbe motivo di contattarci e proporci

esattamente il genere di collaborazione che potremmo aspettarci.

Tutto questo aumenta la plausibilità. **Non dimostra l'autenticità.**

Quando arriva una richiesta inattesa particolarmente coerente con il nostro lavoro, quindi, conviene separare due verifiche: “questa proposta ha senso?” e “questa persona me l'ha davvero inviata?”.

Sono domande diverse.

La seconda richiede un controllo indipendente: contattare la persona attraverso un recapito già conosciuto o reperito autonomamente, verificare con attenzione dominio e indirizzo, evitare di utilizzare come prova di autenticità gli stessi elementi forniti nel messaggio sospetto.

Il caso TA419 lascia così una lezione che va oltre l'AI policy.

Nell'OSINT siamo abituati a usare il contesto per verificare le informazioni. Nel phishing mirato, invece, **il contesto può essere proprio ciò che l'attaccante ha studiato meglio.**

E quando un'email sembra scritta esattamente per noi, questa perfezione non dovrebbe abbassare la soglia di verifica. Dovrebbe alzarla.

Un esperto di politiche sull'intelligenza artificiale riceve una proposta perfettamente compatibile con il proprio lavoro: partecipare a un comitato consultivo sull'AI. Un altro viene invitato a contribuire a un rapporto del Senato americano su controlli alle esportazioni e catene di approvvigionamento.

Non sono le solite email che annunciano una password scaduta o un pacco inesistente. Il mittente sembra conoscere il settore, gli argomenti sono credibili e le persone che firmano i messaggi esistono davvero.

Il problema è che quelle persone non hanno inviato le email.

È il meccanismo documentato da Proofpoint in una ricerca pubblicata il 1° ottobre 2026 su TA419, un attore che la società di sicurezza definisce “China-aligned” e orientato allo spionaggio. Secondo Proofpoint, nel luglio scorso il gruppo ha condotto campagne di credential phishing contro esperti di AI policy negli Stati Uniti, impersonando personalità note dell'economia e delle politiche sull'intelligenza artificiale. Reuters riferisce che i bersagli individuati erano meno di dieci.

La dimensione ridotta della campagna è proprio ciò che la rende interessante.

Qui non sembra esserci la ricerca di migliaia di account da compromettere. La scelta è chirurgica: poche persone, selezionate per ciò che potrebbero conoscere.

Il bersaglio non è sempre chi comanda

Quando pensiamo allo spionaggio legato all'intelligenza artificiale, è naturale immaginare il furto di codice, pesi dei modelli, chip, documenti tecnici o segreti industriali.

TA419 suggerisce di guardare anche altrove.

Proofpoint ha osservato il gruppo colpire esperti appartenenti a think tank, università e organizzazioni del settore legale. Reuters cita inoltre organizzazioni legate alla difesa tra i settori complessivamente presi di mira dal gruppo. L'obiettivo della campagna sull'AI, secondo la valutazione di Proofpoint, sarebbe stato raccogliere informazioni sugli sviluppi della politica e della regolamentazione statunitense dell'intelligenza artificiale.

Questo cambia la domanda.

Se volessimo conoscere in anticipo come potrebbero evolvere i controlli americani sull'esportazione di tecnologie AI, sarebbe necessariamente più utile compromettere l'account di un CEO?

Forse no.

Potrebbe essere molto interessante anche la posta di chi prepara analisi, partecipa a consultazioni, studia le conseguenze di una norma o frequenta le reti professionali nelle quali le diverse opzioni vengono discusse prima di trasformarsi in decisioni ufficiali.

È un principio utile anche nell'OSINT: **visibilità pubblica e valore informativo non coincidono necessariamente.**

Prima del phishing c'è la ricerca

Il secondo elemento interessante è il lavoro necessario per costruire un'esca credibile.

A partire dall'8 luglio, secondo Proofpoint, TA419 ha impersonato Lynne Edwards Parker, già Principal Deputy Director dell'Office of Science and Technology Policy della Casa Bianca, e Heidi Crebo-Rediker, economista ed esperta di politica estera.

I messaggi proponevano attività coerenti con il profilo delle vittime: entrare in un fantomatico "AI Policy Advisory Committee" oppure collaborare a un rapporto attribuito alla Senate Committee on Foreign Relations dedicato agli export control dell'AI e alle supply chain.

A febbraio il gruppo aveva utilizzato una variante ancora diversa, impersonando un dipendente senior di Anthropic per contattare un analista di AI policy di un think tank americano. L'oggetto della mail riguardava una richiesta di feedback sull'integrazione militare di Claude, tema collegato a un dibattito reale.

Per costruire messaggi del genere bisogna prima comprendere il bersaglio.

Chi è? Di che cosa si occupa? Con chi potrebbe ragionevolmente entrare in contatto? Quale argomento potrebbe convincerlo a rispondere?

È qui che il caso diventa particolarmente interessante dal punto di vista OSINT. Informazioni pubbliche come incarichi, biografie professionali, pubblicazioni, conferenze, aree di ricerca e reti di relazioni possono aiutare un osservatore legittimo a ricostruire un ecosistema. Le stesse informazioni, usate con finalità ostili, possono contribuire a costruire un pretesto molto più convincente del phishing generico.

Non significa che Proofpoint abbia dimostrato quali specifiche fonti OSINT siano state utilizzate da TA419 per selezionare ogni vittima. Il report non lo stabilisce. Possiamo però osservare il risultato: esche fortemente contestualizzate rispetto al lavoro dei destinatari e identità reali utilizzate per renderle credibili.

Il messaggio pericoloso può sembrare quello più normale

Anche la sequenza dell'attacco merita attenzione.

Il primo messaggio non conteneva necessariamente il passaggio decisivo dell'attacco. Proofpoint descrive email iniziali apparentemente innocue, progettate per avviare una conversazione. Soltanto dopo la risposta della vittima arrivava un collegamento abbreviato che conduceva, attraverso più reindirizzamenti, all'infrastruttura di phishing.

È una differenza sostanziale.

La vittima non riceve semplicemente un link sospetto da uno sconosciuto. Prima può essersi instaurata una conversazione apparentemente sensata. Il collegamento arriva quando il contesto che dovrebbe giustificarlo è già stato costruito.

La catena tecnica descritta da Proofpoint era progettata per colpire account Microsoft 365/Entra ID e utilizzava una versione modificata di Frameless BitB, strumento open source basato sulla tecnica

Browser-in-the-Browser. L'attacco incorporava anche una componente Adversary-in-the-Middle, o AitM, capace di inserirsi nel processo di autenticazione. Proofpoint descrive un sistema in grado di seguire la vittima attraverso il login, compresa l'autenticazione multifattore, e di catturare i cookie di sessione.

In termini semplici: **avere l'MFA attiva non rende automaticamente innocuo qualsiasi login avviato da un link ricevuto via email.**

Per questo Proofpoint raccomanda, per le organizzazioni esposte a questo tipo di attività, sistemi di autenticazione resistenti al phishing, come le passkey, e invita chi riceve contatti professionali inattesi a verificarli attraverso un canale indipendente.

Il piccolo esercizio OSINT: chi vale davvero in una rete?

Il caso permette di fare un esercizio utile senza cercare informazioni personali né costruire profili invasivi.

Prendiamo una politica pubblica qualsiasi e immaginiamo la rete che la circonda.

Al centro può esserci il decisore politico. Intorno, però, troviamo funzionari, consulenti, ricercatori universitari, think tank, avvocati, aziende, associazioni di settore ed esperti che producono analisi.

L'errore sarebbe ordinare automaticamente queste persone per notorietà.

Dal punto di vista dell'intelligence la domanda più utile è diversa: **chi potrebbe avere accesso anticipato a informazioni che diventeranno importanti in seguito?**

Possiamo sintetizzare il ragionamento così:

persona → ruolo → rete → possibile accesso → pretesto plausibile → valore informativo

È un modello di analisi, non la ricostruzione documentata del processo seguito da TA419. La distinzione è importante. Serve però a capire perché una persona quasi sconosciuta al grande pubblico possa diventare un bersaglio più interessante di un personaggio che compare ogni giorno sui giornali.

Cosa sappiamo davvero su TA419

[Proofpoint afferma di osservare TA419 almeno dall'aprile 2025](#) in campagne mirate contro persone appartenenti a think tank, contractor della difesa, università e studi legali negli Stati Uniti e in Giappone. Tra gli interessi osservati figurano difesa, sicurezza nazionale, energia, relazioni internazionali e politica estera. L'attenzione verso gli esperti di AI policy viene quindi interpretata dai ricercatori come un'estensione di interessi precedenti, non come un'attività completamente nuova.

Sull'attribuzione bisogna mantenere la formulazione corretta.

Proofpoint definisce TA419 un attore "China-aligned" e ritiene probabile che le campagne sostengano più ampi obiettivi di intelligence cinesi. Reuters, riportando il caso, ricorda che Pechino nega il coinvolgimento nelle attività di cyber-spionaggio che le vengono attribuite. Le evidenze pubbliche disponibili non autorizzano quindi a trasformare la valutazione della società di sicurezza nella formula più forte "il governo cinese ha ordinato questo attacco".

È precisamente il tipo di distinzione che un'analisi OSINT dovrebbe conservare.

La verifica da fare quando un'email sembra perfetta

Il dettaglio più utile di questa storia non è un dominio malevolo, perché i domini possono cambiare. Non è neppure il nome TA419.

È il metodo.

Un messaggio può contenere il nostro argomento di ricerca, citare una discussione realmente in corso, arrivare apparentemente da una persona che avrebbe motivo di contattarci e proporci esattamente il genere di collaborazione che potremmo aspettarci.

Tutto questo aumenta la plausibilità. **Non dimostra l'autenticità.**

Quando arriva una richiesta inattesa particolarmente coerente con il nostro lavoro, quindi, conviene separare due verifiche: “questa proposta ha senso?” e “questa persona me l'ha davvero inviata?”.

Sono domande diverse.

La seconda richiede un controllo indipendente: contattare la persona attraverso un recapito già conosciuto o reperito autonomamente, verificare con attenzione dominio e indirizzo, evitare di utilizzare come prova di autenticità gli stessi elementi forniti nel messaggio sospetto.

Il caso TA419 lascia così una lezione che va oltre l'AI policy.

Nell'OSINT siamo abituati a usare il contesto per verificare le informazioni. Nel phishing mirato, invece, **il contesto può essere proprio ciò che l'attaccante ha studiato meglio.**

E quando un'email sembra scritta esattamente per noi, questa perfezione non dovrebbe abbassare la soglia di verifica. Dovrebbe alzarla.