Tutto quello che un articolo può dire senza dire niente

Ovvero come trasformare la prova di un fallimento sistemico in contenuto da engagement

10 marzo 2026

Il 4 marzo è uscito un articolo su una delle testate più seguite del settore *cyber security* italiano: il tema è CyberStrikeAI, un tool *open source* che è stato usato da un *threat actor* per scansionare il web. QUI potete leggere l'articolo.

L'articolo scorre bene, ha un tono autorevole, ha un sacco di screenshot, e nella sostanza è un documento vuoto. Non per quello che dice ma per quello che *non chiede*, per quello che non dà. Permetteteci di spiegarlo punto per punto, con le parole dell'autore stesso, *copia-incolla*, così non ci sbagliamo.

Punto 1. Il guardiano del castello si è addormentato con la porta aperta. E non dorme da solo.

L'articolo descrive come CyberStrikeAI sia stato usato per "scansioni massive alla ricerca di dispositivi esposti", nello specifico dispositivi FortiGate ma ovviamente il discorso vale per qualsiasi altro oggetto simile.

FortiGate è un firewall, un sistema di sicurezza, il guardiano perimetrale che migliaia di aziende usano per “proteggere” le proprie infrastrutture ed è stato attaccato perché… era *raggiungibile*. Sì, ne conveniamo, sembra una battuta ma questa è l’ironia cosmica che nessun articolo del settore ha il coraggio di nominare: **il difensore, oggi, è diventato il vettore**. La soluzione di sicurezza è il bersaglio privilegiato e la risposta implicita dell’industria, anche in questo articolo, è: compriamo un difensore migliore, più veloce, più intelligente. **E sono seri.**

Il problema strutturale, *e cioè che il FortiGate (come tutto il resto) si può trovare, raggiungere e attaccare,* non viene nemmeno sfiorato. Beh, direte voi, non potrebbe che essere così, altrimenti non esisterebbe la “rete”. Mica vero: stringete i denti che fra poco ci arriviamo.

Punto 2. “Strumenti che finiscono inevitabilmente nelle mani del cybercrime”

Citazione diretta:

> *“[…] gli stessi strumenti finiscono inevitabilmente anche nelle mani del cybercrime”.*

La parola chiave è **inevitabilmente**. Non “potenzialmente”, non “in alcuni casi”, no no, “**inevitabilmente”**. Con una scelta lessicale precisa l’autore ammette che l’arsenale offensivo è per sua natura **incontrollabile** e che ogni tool sviluppato per la difesa diventa, con certezza statistica, un’arma per l’attacco.

Beh, nessuna reazione? Questa ammissione dovrebbe far tremare l’intero paradigma difensivo su cui è costruita l’industria della *cyber security*, e invece viene presentata come scenario di contesto, naturale. Folklore. Un accenno e si passa avanti.

Punto 3. “Chi attacca può scandagliare Internet in modo massivo, individuare sistemi esposti”

Altra citazione:

> *“[…] chi attacca può scandagliare Internet in modo massivo, individuare sistemi esposti e preparare attacchi contro infrastrutture distribuite in tutto il mondo. Il ritmo cambia. Molto più veloce.”*

Esatto che più esatto non si può, ce ne compiacciamo. Questa frase suggerisce la domanda che nessuno fa:

> *Se il problema è che i sistemi esposti vengono trovati e attaccati, cosa succederebbe se i sistemi non fossero esposti?*

Intendiamoci bene. Non “filtrati”. Non “protetti”. Non “monitorati”. Semplicemente **irraggiungibili**, non “esistenti”. La domanda è talmente banale da vergognarsi quasi a

scriverla ma la risposta, univoca, cambierebbe tutto. Eppure non ve n'è traccia nell'articolo, neanche una lontana, vaga forma. E non compare in nessun articolo di questo tipo. Mai. Deve essere molto difficile immaginarla.

Punto 4. Il fattore di scala. Ovvero la scoperta dell'acqua calda ma con effetti speciali.

Ecco poi un altro passaggio che vale la pena isolare perché brilla di una luce propria abbagliante (ancora citazione diretta così lasciamo il merito a chi ce l'ha):

> *"Una volta i team di sicurezza potevano organizzare attività mirate, analizzare ambienti specifici e riuscire spesso a contenere le campagne malevole. Oggi, con piattaforme automatizzate e integrate con l'intelligenza artificiale, chi attacca può scandagliare Internet in modo massivo…"*

Grazie. Molto utile saperlo.

Allora permetteteci una domanda: questa "scoperta", cioè che l'automazione moltiplica la capacità offensiva, è la notizia? È questo il contributo intellettuale dell'articolo? Lo chiediamo perché se la risposta è "sì" possiamo tranquillamente sostituirlo con un post di tre righe, risparmiare a tutti il tempo della lettura e tornarcene al bar.

Il problema non è che chi attacca va più veloce: **il problema è che va veloce verso qualcosa che esiste e risponde.** Scusate tanto, ma la scala dell'attacco non sarebbe forse irrilevante se il bersaglio non fosse raggiungibile? Puoi scandagliare Internet in modo massivo quanto vuoi ma se il sistema non è lì, non lo trovi (deve essere questa la parte difficile da capire). Con tutta l'AI del mondo, con tutti i tuoi cento tool orchestrati come ti pare, con tutte le automazioni che vuoi…

Già, ma ragionare in questi termini prevederebbe la solita domanda e cioè se il problema sia la velocità dell'attacco o l'esistenza della superficie. E quella domanda, nell'articolo, non c'è.

Punto 5. Il dato Veracode: la prova che il modello è rotto

"Negli ultimi tempi si stanno individuando più vulnerabilità di quante se ne riescano effettivamente a correggere." Questa è la citazione più pregnante dell'articolo. Ed è anche quella trattata più superficialmente.

Pensateci: viene citata una ricerca che dimostra matematicamente che il *patch management* (la pratica presente, quando non centrale, in ogni strategia difensiva moderna) è **strutturalmente perdente**, per definizione. Il numero di vulnerabilità cresce più velocemente della capacità di correggerle e il divario si allarga, non si restringe.

> *Ripetiamolo 'ché ci fa bene: **si allarga** (altra cosa difficile da capire).*

Guardate che questa è la sentenza di morte del paradigma difensivo attuale non una nota a margine: riesce a esservi chiaro? Ah già, vero, come non detto: adesso c'è il paradigma "proattivo". Viene da piangere.

L'unica reazione ragionevole a questo dato, quindi, sarebbe chiedersi se non sia il modello a essere sbagliato, cioè se correre più veloce su un *tapis roulant* che accelera sia davvero la strategia giusta. L'articolo non se la pone questa domanda (in questo c'è coerenza): prende il dato, lo cita come "dato che fa riflettere" e scivola via alla chetichella. Ma sì, non è mica così importante.

Punto 6. I criminali sono più veloci. Sì, c'è scritto così.

> *"I criminali non devono rispettare procedure, compliance o tempi aziendali. Questo li rende, almeno sul piano operativo, più rapidi, più efficaci di chi difende."*

Perfetto. Chiarissimo. Ineccepibile. Sottoscriviamo. L'attaccante ha un vantaggio strutturale permanente che non dipende dalla tecnologia: ha libertà operativa totale. Nessun processo di approvazione, nessuna finestra di manutenzione, nessun CISO che deve firmare una *change request*.

Fatevene una ragione: questo vantaggio non si colma con più AI, più automazione, più velocità difensiva: è asimmetrico per sua stessa natura! Ma davvero è difficile capire anche questo?

A meno che non si cambi il terreno di gioco questa condizione non potrà MAI cambiare.

E se decidessimo di togliergli il bersaglio? Sì, bene, ma questo richiederebbe pensare in termini di sistema; no, non nel senso di "sistemi informatici" ma di *dinamiche di sistema*, che è esattamente quello che questo tipo di informazione non pratica e non promuove.

Punto 7. "La stessa tecnologia può diventare l'arma principale per rafforzare le difese." Vien voglia di arrendersi.

Eccola, la svolta narrativa. Dopo aver descritto con precisione il problema, dopo aver citato dati che dimostrano il fallimento del modello difensivo, dopo aver dichiarato che i criminali sono strutturalmente più veloci, arriva il colpo di reni:

> *"Eppure non tutto è negativo. La stessa tecnologia che sta aumentando la pressione sulle difese può diventare anche l'arma principale per rafforzarle."* ***Ma non era il contrario fino a poco fa?***

Nessun argomento nuovo. Nessuna logica. Solo un circolo che si autoalimenta. Ripetiamolo: **nessuna logica**. Un'inversione narrativa, questo sì perché, insomma, l'articolo deve pur respirare e il lettore non deve andarsene depresso senno' rischiamo che non torni.

In ogni caso, fermiamoci sulla sostanza: questa affermazione è falsa, o quantomeno non dimostrata.

1. L'AI offensiva scala in modo esponenziale perché automatizza la ricognizione su superfici che esistono e rispondono.
2. L'AI difensiva, **ammesso che riesca a stare al passo**, cosa che i dati Veracode appena citati (!) smentiscono, non fa altro che tentare di aumentare la velocità di risposta a un attacco che è già in corso, reattiva per definizione (a proposito: "reattivo" non è una parolaccia. **TUTTO nei sistemi dinamici è reattivo, la proattività è un'invenzione comunicativa**, smettiamola di giocarci sopra).
3. L'AI difensiva non elimina la superficie, prova solo a costruirci sopra un muro più alto, in attesa del prossimo cattivo che arriverà con una scala più lunga.

Dobbiamo capirlo e accettarlo: l'AI non risolve il problema strutturale ma è il problema strutturale. Lo accelera da entrambe le parti, con il vantaggio permanente di chi attacca, come correttamente dimostrato dall'autore stesso.

Quel passaggio quindi non è analisi, in nessuna misura: è solo rassicurazione. È il modo educato per dire ai lettori, e agli inserzionisti, che non bisogna preoccuparsi troppo, che il mercato ha le risposte, che basta comprare la cosa giusta. Quale cosa giusta? Dicevamo degli inserzionisti…

Punto 8. La conclusione. Un capolavoro del genere.

> *"La sfida nei prossimi anni sarà proprio questa: trasformare la scala della minaccia nella scala della difesa. E chi saprà farlo prima… farà davvero la differenza."*

Rileggiamo insieme quanto riportato dall'articolo nei punti precedenti:

1. Gli strumenti offensivi finiscono *inevitabilmente* nelle mani del *cybercrime*.
2. Chi attacca scandaglia internet in modo massivo e trova sistemi esposti.
3. L'automazione offensiva scala molto più veloce.
4. Si trovano più vulnerabilità di quante se ne correggano.
5. I criminali sono strutturalmente più veloci per ragioni che non dipendono dalla tecnologia.
6. Il divario tra difesa e attacco si *allarga*.

And the winner is? **Dobbiamo correre più forte**.

Dai, siamo seri, questa non è una soluzione, è un **proclama**. È la chiusura di un discorso politico quando non hai niente da dire ma deve sembrare che ce l'abbia. È il "*dobbiamo fare di più e meglio*" del ministro dopo la catastrofe. Suona bene, non impegna nessuno, non dice

niente di verificabile, non propone niente di concreto, non identifica nessun metodo, nessun cambio di paradigma, nessuna direzione che non sia "*avanti miei prodi, più veloci, tutti insieme*". Un'ammucchiata di lemming rispettosi della tradizione, insomma.

E soprattutto, e qui il fastidio cresce parecchio, contraddice quanto affermato poco prima. Se il divario si allarga per ragioni strutturali, "scalare la difesa" non può chiudere il divario: **lo attenua temporaneamente e con costi crescenti** (forse a beneficio dell'inserzionista che professa di saperlo fare?). Beninteso: fino alla prossima notizia di 600 dispositivi compromessi in 55 paesi.

Questo tipo di chiusura ha un nome preciso, si chiama *petizione di principio* e appartiene alla categoria delle *fallacie logiche informali*: la soluzione proposta presuppone come già risolto esattamente il problema che dovrebbe risolvere. A perfezionamento della confezione ammetti tutto il problema per sembrare onesto, poi affidi la chiusura a una frase motivazionale per non deprimere il lettore, non disturbare gli inserzionisti e non essere costretto a proporre qualcosa che metta in discussione il paradigma su cui vive il mercato che ti legge.

Non è analisi: è intrattenimento da convegno.

E c'è di più. Quella conclusione è anche un *falso dilemma*, della stessa categoria di fallacie (*melius abundare*): presenta due sole opzioni ("scala la minaccia", "scala la difesa") come se fossero le uniche esistenti; la terza, uscire dal paradigma dell'esposizione, non viene nominata. Non per dimenticanza, sospettiamo.

Punto 9. La spezia geopolitica. Bonus track.

Nel mezzo dell'articolo si legge, senza fonte specificata, che l'attore dietro la campagna è "probabilmente di lingua russa". Fermiamoci un momento su questa frase: non sul "russo" ma su "probabilmente di lingua".

Nell'attribuzione *cyber*, dire che un *threat actor* è "di lingua russa" significa avere evidenze concrete e tecnicamente verificabili: stringhe di codice in cirillico, commenti nel *source code* in russo, metadati con fuso orario compatibile con Mosca o San Pietroburgo, *pattern* operativi coerenti con orari lavorativi russi, comunicazioni intercettate in russo, artefatti linguistici nelle variabili o nei messaggi di errore ecc.. Sono criteri precisi, documentabili, citabili: sono il mestiere della *threat intelligence attribution*. "Probabilmente di lingua" non è un criterio, è un'impressione.

Questo punto è insieme linguistico, logico ed epistemico: come fa un *threat actor* ad essere *probabilmente* di una lingua? O hai le evidenze che parlano russo, e allora lo dici citando la fonte, oppure non le hai. La lingua non è un'opinione soggetta a gradi di probabilità, non esiste il "probabilmente madrelingua italiano" o il "forse di lingua mandarina": esiste l'evidenza o la sua assenza.

L’avverbio “probabilmente” in questo contesto non è cautela scientifica ma il “paravento grammaticale” con cui si scrive qualcosa di non verificato facendolo sembrare verificato. È il modo in cui si fa *attribution* senza fare *attribution*. Si pianta un’etichetta geopolitica nel testo, la si copre con un avverbio e ci si defila serafici. Se poi si scopre che era sbagliata, tutti tranquilli, l’avverbio assolve da qualsiasi responsabilità.

Questa prestidigitazione giornalistica, nel caso specifico, è tanto più grave perché nell’articolo convive con una descrizione opposta e precisa: il *developer* del tool è cinese, con legami documentati al Ministero della Sicurezza di Stato cinese che ha condiviso il progetto con *Knownsec 404* (organizzazione connessa con l’esercito cinese e protagonista in una fuga di 12.000 documenti interni nel novembre 2025), e che ha ricevuto un riconoscimento dal database nazionale delle vulnerabilità cinese, supervisione diretta del MSS.

E dunque, l’infrastruttura rilevata? Cina, Singapore, Hong Kong, poi USA, Giappone, Svizzera. Fate voi. Perciò, ricapitolando: tutto documentato e cinese, tranne un’attribuzione vaga, priva di fonte e grammaticalmente zoppicante che dice “russo”. Ma cosa volete, nel *cyber security journalism* occidentale, “russo” è diventato un riflesso *pavloviano*: compare in migliaia di report perché è comodo, non richiede prove solide, scalda il pubblico giusto e nessuno ti chiede conto se sbagli perché sei coperto dall’avverbio. È… *geoqualcosa* che non ci interessa definire oltre, tanto ci siamo capiti. Prima però, tre spiegazioni possibili per questa specifica occorrenza (giusto per non lasciare troppa roba appesa):

1. *Copia-incolla da fonti diverse senza verificare la coerenza interna: il “russo” viene da una fonte, il cinese da un’altra e nessuno si è accorto della contraddizione.*
2. *“russo” è la parola magica che funziona sempre, non richiede prove, fa audience, non disturba nessuno (tranne i russi forse, ma chi se ne frega).*
3. *Confusione tra chi ha costruito il tool e chi lo ha usato, che per chi si presenta come esperto di threat intelligence e Red Team sarebbe un errore fuori misura, quindi rimangono solo la 1 e la 2.*

In ogni caso il risultato alla lettura è identico: un articolo che pur mostrando di non sapere con certezza cosa sta descrivendo si propone come riferimento per chi deve capire come difendersi.

Quello che manca. Sempre.

Dicevamo della domanda che questo articolo non fa, che nessun articolo di questo tipo fa, che il settore non fa da decenni:

> *se CyberStrikeAI scansiona il web per trovare sistemi raggiungibili e vulnerabili, cosa succede se non ne trova?*

Non è provocazione, è logica elementare. Se il target non esiste, se cioè non è raggiungibile, non è indirizzabile, non risponde a nessuna scansione **nemmeno durante le sessioni attive** degli utenti autenticati, allora (lo abbiamo detto) CyberStrikeAI può orchestrare tutti i tool che vuole con tutta l'AI del mondo e trovare zero, l'intera *kill chain* automatizzata si ferma al primo passo: la ricognizione.

E questo perché non c'è niente da trovare. Eccola, dunque, la domanda sistemica, quella che rompe il paradigma invece di subirlo.

Nel marzo 2025 abbiamo scritto una lettera aperta all'informazione di settore (ecco il link: https://www.linkedin.com/pulse/lettera-aperta-allinformazione-di-settore-lateralcode-xtiaf) chiedendo esattamente questo: **il coraggio di raccontare l'innovazione che rompe gli schemi invece di amplificare, articolo dopo articolo, la narrativa che protegge il mercato esistente.** Di smetterla con gli articoli-fotocopia, con le *buzzword* rassicuranti, con i tavoli e i simposi che non impediscono, il giorno dopo, la solita rassegna stampa del crimine informatico.

Non abbiamo ricevuto risposte. In compenso abbiamo ricevuto proposte di pubblicazione a pagamento. Beh, dai…

Poi, un giorno come un altro, 600 FortiGate vengono compromessi in 55 paesi *et voilà*, puntuale, esce l'articolo dalla fotocopiatrice.

Non scriviamo articoli di oltre 2.700 parole solo per criticare. Quella domanda sistemica ha una risposta concreta, con brevetto depositato, già utilizzata da 90+ aziende e 33k+ utenti (zero incident, 100% uptime), ***anche se non ve la raccontano****. Non difende la superficie, la elimina.*

ZeroSurface® è l'unica tecnologia di sicurezza informatica perimetrale oggi disponibile che garantisce l'azzeramento di TUTTE le superfici d'attacco delle reti, dei sistemi IoT, dei dispositivi edge, delle API e dei server che pubblicano servizi, ***così come degli stessi servizi di sicurezza*** *fino a oggi disponibili e offerti dal mercato,* ***in qualunque condizione operativa*** *essi si trovino.*
