Lo stack OSI e la tecnologia italiana ZeroSurface®: gli effetti livello per livello

4 dicembre 2025

Il modello OSI è un classico della teoria delle reti: sette piani, dal segnale elettrico fino all'applicazione. Non è pensato come un modello di sicurezza, eppure negli anni è diventato uno schema didattico per raccontare i rischi: per ogni livello gli specialisti hanno elencato attacchi tipici e tecniche di difesa. Il risultato è una lista lunga e scoraggiante di minacce a mano a mano che si sale: *sniffing, spoofing, man-in-the-middle, scanning, session hijacking, phishing, exploit* e via discorrendo…

> *E da decenni la strategia è sempre la stessa: aggiungere barriere, rinforzare mura, inventarsi nuovi filtri, fino ad arrivare alla moderna fede nel real time.*

ZeroSurface® cambia radicalmente la prospettiva. Non costruisce l'ennesimo castello con le mura più alte di tutti: fa sparire il castello. Se "tu non sei tu", se cioè non sei autenticato (in un modo del tutto inedito e sicuro per logica, non per muscoli), il target non esiste. E se il bersaglio non c'è, l'attacco non ha nemmeno il punto di attenzione.

[Il metodo di autenticazione non è argomento di queste righe ma se vuoi approfondire: https://www.linkedin.com/pulse/aaa-cercasi-asimmetria-disperatamente-lateralcode/]

Questo articolo seguerà dunque la convenzione didattica classica — livello per livello, attacco per attacco — ma con una premessa fondamentale:

ZeroSurface® non "risponde" a questi attacchi, li rende semplicemente privi di oggetto. La differenza non è sottile: è strutturale, è sistemica.

Guardando i livelli uno per uno

Livello 1 – Physical

Qui si gioca con il segnale grezzo: cavi, radio, Wi-Fi. Gli attaccanti intercettano pacchetti con sniffer o sonde fisiche. Qui ZeroSurface® non pretende di sostituirsi a serrature e guardie giurate: la protezione fisica resta un altro mestiere e tuttavia, ha un effetto concreto. Poiché il target non è raggiungibile finché non c'è autenticazione, i pacchetti che un attaccante potrebbe intercettare non contengono traffico verso il target protetto. Lo sniffing resta tecnicamente possibile, ma cattura solo "rumore di rete": il target protetto non emette né riceve pacchetti osservabili.

N.b. Una volta autenticato l'utente, esiste un canale di comunicazione bidirezionale e il traffico passa sulla rete fisica. Un attaccante con accesso al mezzo può intercettare passivamente questi pacchetti. Quindi attenzione, ZeroSurface® non sostituisce e non deve sostituire la cifratura del traffico: per proteggere confidenzialità e integrità dei dati in transito, TLS/VPN o altre tecnologie di cifratura sono necessarie e si integrano perfettamente con ZeroSurface® (in realtà ne hanno estremo bisogno).

In conclusione ZeroSurface® non impedisce fisicamente l'intercettazione del mezzo ma rende il target privo di traffico intercettabile prima dell'autenticazione, e complementa (non sostituisce) la cifratura durante le sessioni attive.

Livello 2 – Data Link

ARP spoofing e MAC spoofing sono attacchi classici della rete locale: un attaccante falsifica il proprio indirizzo MAC o manipola le tabelle ARP per deviare traffico o impersonare altri nodi.

ZeroSurface® rende questi attacchi operativamente sterili.

-- Prima dell'autenticazione --

Non esiste traffico da intercettare o deviare. Il target è completamente irraggiungibile. Lo spoofing può avvenire tecnicamente, ma opera nel vuoto: non c'è nulla da falsificare o deviare.

-- Durante la sessione attiva --

Anche dopo l'autenticazione, il target mantiene una caratteristica peculiare documentata nelle nostre dimostrazioni: rimane invisibile a qualsiasi tentativo di connessione o scan, anche proveniente dallo stesso IP e dallo stesso computer dell'utente autorizzato (!). Solo il flusso di comunicazione specifico già stabilito può proseguire.

ZeroSurface® non filtra semplicemente per indirizzo IP sorgente, ma gestisce l'intera sessione di comunicazione. Un attaccante che riesca a falsificare MAC o IP non può né aprire nuove connessioni né inserirsi efficacemente nel flusso esistente. Anche tentativi di scansione delle porte dallo stesso sistema autenticato restituiscono un "host seems down" — il target resta assente per qualsiasi entità che non sia il canale di comunicazione già autorizzato.

-- Dopo la scadenza della sessione --

A maggior ragione il target è irraggiungibile.

Livello 3 – Network

Il "man in the middle" è un altro evergreen: posizionarsi tra due nodi e manipolare i pacchetti. Ma se i pacchetti non ci sono? Senza autenticazione non circola nessun flusso utile. ZeroSurface® trasforma il MITM in un esercizio sterile: l'uomo in mezzo resta nel vuoto. Anche durante una sessione attiva, l'architettura di ZeroSurface® impedisce l'inserimento nella comunicazione. Di nuovo: solo il canale già autorizzato esiste e può proseguire.

Livello 4 – Transport

La prima cosa che fa un attaccante è una scansione: quali porte sono aperte, quali servizi rispondono? Con ZeroSurface®, la risposta è sempre la stessa: nessuna porta, nessun servizio. La ricognizione fallisce in partenza.

Questo comportamento persiste anche durante le sessioni attive: il target resta irraggiungibile (quindi invisibile) anche a scan lanciati dallo stesso sistema autenticato.

L'attaccante non può mappare la superficie d'attacco perché, semplicemente, non esiste superficie da mappare.

Livello 5 – Session

Qui il classico è rubare una sessione, catturando cookie o token e impersonando l'utente. Ma ZeroSurface® non rilascia mai token di sessione. Non c'è nulla da intercettare o riutilizzare.

L'autenticazione avviene tramite la combinazione di un URL funzionale non semantico (FU) e una chiave segreta (iceKey). Questa coppia costituisce l'unica credenziale, e non genera artefatti riutilizzabili come token, cookie o certificati temporanei. L'hijacking non ha terreno da sfruttare.

Livello 6 – Presentation

Questo livello gestisce la codifica e decodifica dei dati (JPEG, ASCII, crittografia…). ZeroSurface® opera a livelli diversi e non ha impatti specifici su questo piano dello stack OSI, se non nelle forme indirette che ora sono più chiare. A questo livello le considerazioni rilevanti per la sicurezza riguardano principalmente la cifratura del traffico che, come detto, è complementare a ZeroSurface® ma non a suo carico.

Livello 7 – Application

Gli exploit colpiscono vulnerabilità nei software. Ma se l'applicazione non è raggiungibile dall'esterno? ZeroSurface® fa sì che solo l'utente autenticato possa accedere al target: gli exploit remoti non hanno più un bersaglio.

Anche vulnerabilità critiche (inclusi 0-day) non possono essere sfruttate se il sistema vulnerabile è (davvero) irraggiungibile, vi pare?

In altre parole, ZeroSurface® cancella il contesto in cui un exploit potrebbe operare: non importa quanto sia grave la vulnerabilità, se il bersaglio non è raggiungibile, l'exploit non può essere lanciato.

Ciò offre una libertà fondamentale: il tempo per reagire. Anche durante la finestra di vulnerabilità in cui una patch non è ancora disponibile, i sistemi protetti da ZeroSurface® non sono mai sotto attacco attivo.

È possibile patchare con calma, dopo colazione con cappuccino e cornetto, senza l'urgenza dettata da compromissioni in corso o potenziali.

A proposito del phishing

Sebbene dietro al phishing ci sia molta ingegneria sociale, ZeroSurface® riduce drasticamente il valore di un attacco phishing riuscito. Vediamo brevemente perché.

L'autenticazione richiede due elementi inscindibili:

1. Un URL funzionale (FU) non semantico e non ricostruibile in cui inserire
2. una iceKey segreta

Anche se un utente fosse ingannato e fornisse la propria iceKey su una pagina clonata, l'inservibilità del FU renderebbe la chiave inutile (la pagina clonata, infatti, non può girare sul FU). Risultato: la coppia {FU + iceKey} non può essere completata. Se vuoi approfondire questo aspetto: https://www.linkedin.com/pulse/perch%C3%A9-icegate-e-la-tecnica-zerosurface-proteggono-davvero/

Da notare inoltre che dopo l'autenticazione con ZeroSurface® non c'è redirect né vengono esposti nuovi endpoint. Il sistema avvisa semplicemente con un generico "Access granted" e solo l'utente autorizzato sa dove e come raggiungere il target ora divenuto accessibile (a lui e solo a lui). Ecco dunque che un phisher non può neanche costruire un'esperienza post-autenticazione convincente poiché questa, di fatto, si concretizza solo nell'avvenuta disponibilità del target.

Ripetiamo: come già chiarito, ZeroSurface® non rilascia token di sessione o altri artefatti riutilizzabili, quindi, anche intercettando tutto il traffico durante un tentativo di phishing,

l’attaccante non ottiene elementi che possano essere riutilizzati per impersonare l’utente in seguito.

ZeroSurface® non elimina il rischio che un utente caschi nel phishing (questo potrà sempre succedere), ma azzera il valore dell’attacco anche in caso di utente distratto.

La sintesi

Ai primi due piani ZeroSurface® non sostituisce la sicurezza fisica: sarebbe folle aspettarsi che una soluzione software faccia la guardia giurata. Ma anche lì ha un effetto concreto: lo sniffing diventa inutile prima dell’autenticazione (ricordiamo che necessita di cifratura durante le sessioni attive) e lo spoofing diventa sterile in quanto il target resta invisibile anche durante le sessioni autenticate.

Dal livello rete in su, invece, la protezione è completa: nessun flusso visibile, nessuna porta scansionabile, nessun token da rubare, nessuna credenziale sufficiente per l’accesso, nessun exploit lanciabile da remoto.

Ecco perché ZeroSurface® non è un altro muro: toglie il terreno stesso su cui l’attaccante potrebbe costruire l’attacco e non perché ogni singolo vettore venga bloccato, ma perché il bersaglio non appartiene allo spazio degli oggetti raggiungibili e quindi non c’è niente da bloccare.

ZeroSurface® non rafforza le mura, cancella il castello.
