Perché i router sono diventati il bersaglio della cyber intelligence

Maria Cattini | 30/07/2026 | Sicurezza digitale

Le campagne di cyber intelligence puntano sempre più ai dispositivi di rete: ecco perché router e firewall sono diventati una priorità per chi difende infrastrutture e aziende.

Quando si parla di sicurezza informatica, l'attenzione si concentra quasi sempre su computer, server, endpoint e identità digitali. È una reazione comprensibile: sono i sistemi che utilizziamo ogni giorno e quelli che custodiscono direttamente dati e applicazioni.

Esiste però un'infrastruttura molto meno visibile che rappresenta un bersaglio estremamente interessante per le operazioni di cyber intelligence: router, firewall, gateway VPN e altri dispositivi che gestiscono il traffico di rete.

Negli ultimi anni le agenzie governative occidentali hanno osservato un crescente interesse da parte di gruppi sponsorizzati dagli Stati verso questa categoria di apparati. Il motivo è semplice: controllare il punto attraverso cui transitano le comunicazioni significa ottenere una posizione privilegiata all'interno di una rete.

Perché un router vale più di un computer compromesso

Un router non contiene necessariamente documenti riservati o database aziendali. Tuttavia possiede una caratteristica molto più interessante dal punto di vista di un'operazione di intelligence: vede passare il traffico.

Chi riesce a compromettere un dispositivo di rete può potenzialmente:

• osservare le comunicazioni che attraversano l'infrastruttura;
• raccogliere informazioni utili sull'architettura della rete;
• individuare nuovi sistemi da raggiungere;
• mantenere una presenza persistente senza attirare immediatamente l'attenzione;
• utilizzare il dispositivo come punto di appoggio per operazioni successive.

Dal punto di vista difensivo, questo significa che il router non dovrebbe essere considerato un semplice "accessorio" della rete, ma un componente strategico.

Perché questi dispositivi sono così vulnerabili

Molte organizzazioni dedicano grande attenzione agli aggiornamenti dei sistemi operativi e degli endpoint, ma non riservano lo stesso livello di cura ai dispositivi di rete.

Non è raro trovare router aziendali che:

• utilizzano firmware ormai non più supportati;
• rimangono operativi per molti anni senza aggiornamenti significativi;
• espongono servizi di amministrazione verso Internet;
• impiegano protocolli di gestione ormai superati;
• conservano credenziali deboli o riutilizzate.

Questa combinazione rende tali apparati particolarmente interessanti per attori avanzati che cercano punti di ingresso stabili e difficili da individuare.

L'avviso delle autorità internazionali

Nel luglio 2026 le principali autorità di cybersecurity occidentali hanno pubblicato un avviso congiunto riguardante attività attribuite ad attori sponsorizzati dallo Stato russo, evidenziando il crescente interesse verso router e infrastrutture di rete vulnerabili.

Tra le principali raccomandazioni figurano:

• mantenere aggiornato il firmware dei dispositivi;
• limitare l'esposizione dei servizi di amministrazione remota;
• utilizzare autenticazione robusta;
• sostituire protocolli di gestione obsoleti con configurazioni più sicure;
• monitorare costantemente gli apparati di rete.

L'obiettivo non è soltanto impedire un accesso iniziale, ma ridurre le possibilità che un eventuale compromesso rimanga invisibile per lunghi periodi.

Un cambio di prospettiva anche per chi si occupa di OSINT

Per chi lavora nell'Open Source Intelligence questo fenomeno rappresenta soprattutto un cambiamento metodologico.

Le campagne attribuite agli Stati mostrano come gli aggressori non cerchino necessariamente il sistema più ricco di dati, ma quello che offre la migliore posizione di osservazione.

È un principio che vale anche nelle attività di analisi: comprendere l'architettura di una rete significa capire dove si trovano i punti di maggiore valore informativo.

La sicurezza, quindi, non dovrebbe iniziare dagli asset più visibili, ma dai nodi che collegano tutto il resto.

Cinque domande da porsi durante un audit

Durante una verifica della sicurezza di un'organizzazione può essere utile iniziare ponendosi alcune domande fondamentali:

• Il firmware del router è ancora supportato dal produttore?
• L'interfaccia di amministrazione è accessibile dall'esterno?
• Sono ancora presenti credenziali predefinite o riutilizzate?
• I protocolli di gestione sono configurati secondo gli standard più recenti?
• I log vengono conservati anche al di fuori del dispositivo?

Si tratta di controlli apparentemente semplici, ma spesso trascurati. Ed è proprio questa trascuratezza che può trasformare un comune router nel primo tassello di un'operazione di intelligence più ampia.

Le campagne di cyber intelligence puntano sempre più ai

dispositivi di rete: ecco perché router e firewall sono diventati una priorità per chi difende infrastrutture e aziende.

Quando si parla di sicurezza informatica, l'attenzione si concentra quasi sempre su computer, server, endpoint e identità digitali. È una reazione comprensibile: sono i sistemi che utilizziamo ogni giorno e quelli che custodiscono direttamente dati e applicazioni.

Esiste però un'infrastruttura molto meno visibile che rappresenta un bersaglio estremamente interessante per le operazioni di cyber intelligence: router, firewall, gateway VPN e altri dispositivi che gestiscono il traffico di rete.

Negli ultimi anni le agenzie governative occidentali hanno osservato un crescente interesse da parte di gruppi sponsorizzati dagli Stati verso questa categoria di apparati. Il motivo è semplice: controllare il punto attraverso cui transitano le comunicazioni significa ottenere una posizione privilegiata all'interno di una rete.

Perché un router vale più di un computer compromesso

Un router non contiene necessariamente documenti riservati o database aziendali. Tuttavia possiede una caratteristica molto più interessante dal punto di vista di un'operazione di intelligence: vede passare il traffico.

Chi riesce a compromettere un dispositivo di rete può potenzialmente:

• osservare le comunicazioni che attraversano l'infrastruttura;
• raccogliere informazioni utili sull'architettura della rete;
• individuare nuovi sistemi da raggiungere;
• mantenere una presenza persistente senza attirare immediatamente l'attenzione;
• utilizzare il dispositivo come punto di appoggio per operazioni successive.

Dal punto di vista difensivo, questo significa che il router non dovrebbe essere considerato un semplice "accessorio" della rete, ma un componente strategico.

Perché questi dispositivi sono così vulnerabili

Molte organizzazioni dedicano grande attenzione agli aggiornamenti dei sistemi operativi e degli endpoint, ma non riservano lo stesso livello di cura ai dispositivi di rete.

Non è raro trovare router aziendali che:

• utilizzano firmware ormai non più supportati;
• rimangono operativi per molti anni senza aggiornamenti significativi;
• espongono servizi di amministrazione verso Internet;
• impiegano protocolli di gestione ormai superati;
• conservano credenziali deboli o riutilizzate.

Questa combinazione rende tali apparati particolarmente interessanti per attori avanzati che cercano punti di ingresso stabili e difficili da individuare.

L'avviso delle autorità internazionali

Nel luglio 2026 le principali autorità di cybersecurity occidentali hanno pubblicato un avviso congiunto riguardante attività attribuite ad attori sponsorizzati dallo Stato russo, evidenziando il crescente interesse verso router e infrastrutture di rete vulnerabili.

Tra le principali raccomandazioni figurano:

• mantenere aggiornato il firmware dei dispositivi;
• limitare l'esposizione dei servizi di amministrazione remota;
• utilizzare autenticazione robusta;
• sostituire protocolli di gestione obsoleti con configurazioni più sicure;
• monitorare costantemente gli apparati di rete.

L'obiettivo non è soltanto impedire un accesso iniziale, ma ridurre le possibilità che un eventuale compromesso rimanga invisibile per lunghi periodi.

Un cambio di prospettiva anche per chi si occupa di OSINT

Per chi lavora nell'Open Source Intelligence questo fenomeno rappresenta soprattutto un cambiamento metodologico.

Le campagne attribuite agli Stati mostrano come gli aggressori non cerchino necessariamente il sistema più ricco di dati, ma quello che offre la migliore posizione di osservazione.

È un principio che vale anche nelle attività di analisi: comprendere l'architettura di una rete significa capire dove si trovano i punti di maggiore valore informativo.

La sicurezza, quindi, non dovrebbe iniziare dagli asset più visibili, ma dai nodi che collegano tutto il resto.

Cinque domande da porsi durante un audit

Durante una verifica della sicurezza di un'organizzazione può essere utile iniziare ponendosi alcune domande fondamentali:

• Il firmware del router è ancora supportato dal produttore?
• L'interfaccia di amministrazione è accessibile dall'esterno?
• Sono ancora presenti credenziali predefinite o riutilizzate?
• I protocolli di gestione sono configurati secondo gli standard più recenti?
• I log vengono conservati anche al di fuori del dispositivo?

Si tratta di controlli apparentemente semplici, ma spesso trascurati. Ed è proprio questa trascuratezza che può trasformare un comune router nel primo tassello di un'operazione di intelligence più ampia.