

Shodan motore di ricerca: L'Arma Segreta dei Ricercatori Tecnologici

Maria Cattini | 28/07/2024 | Risorse

Scavare in Profondità con Shodan.

Il Potere di Shodan.

Nel vasto e sempre crescente universo digitale, l'accesso alle informazioni è la chiave per il successo. E quando si tratta di informazioni relative agli asset tecnologici in rete, Shodan emerge come uno strumento di ricerca cruciale. In questo articolo, esploreremo in profondità Shodan, il "motore di ricerca per Internet delle cose (IoT)" che sta rivoluzionando la ricerca tecnologica.

A differenza dei motori di ricerca che ti aiutano a trovare siti web, Shodan si avvale di sistemi di scansione capaci di individuare qualsiasi cosa sia online: Router, WebCam, GPS, Smart TV, Sistemi di controllo Industriale (ICS), WebServer, Stampanti, Frigoriferi (SI anche quelli oggi vanno online), etc...e altro.

Queste informazioni includono metadati come il software in esecuzione su ogni dispositivo.

Gli usi comuni di Shodan includono **sicurezza di rete, ricerche di mercato, rischio informatico, scansione di dispositivi IoT e monitoraggio ransomware**. Tuttavia, Shodan può essere utilizzato anche per scopi malintenzionati, come trovare dispositivi vulnerabili da attaccare.

Cos'è Shodan?

Shodan è stato lanciato nel 2009 da John Matherly ed è stato definito il motore di ricerca degli hacker.

Shodan è molto più di un semplice motore di ricerca. È un potente strumento di scansione di rete che analizza costantemente il web in cerca di dispositivi connessi. Questi dispositivi possono includere server, telecamere di sicurezza, router, dispositivi IoT e molto altro. Shodan non solo identifica questi dispositivi, ma fornisce anche informazioni dettagliate su di essi, come il tipo di dispositivo, la versione del software utilizzato, le porte aperte e persino dati sensibili accidentalmente esposti online.

La Forza dell'Accesso Pubblico

Una delle caratteristiche più sorprendenti di Shodan è che è un motore di ricerca accessibile a chiunque. Questo significa che sia esperti di sicurezza informatica che appassionati di tecnologia possono utilizzarlo per raccogliere informazioni sulle risorse online. Tuttavia, con un grande potere viene anche una grande responsabilità, ed è fondamentale utilizzare Shodan in modo etico e legale, evitando di violare la privacy o la sicurezza altrui.

Le Potenzialità di Shodan

Shodan offre un ventaglio di potenzialità impressionante:

- Ricerca di Dispositivi Specifici: Gli utenti possono cercare dispositivi specifici in base a criteri come il tipo, il marchio o la posizione geografica.
- Monitoraggio delle Porte: Shodan può identificare le porte aperte su un dispositivo, rivelando potenziali vulnerabilità di sicurezza.
- Visualizzazione delle Webcam: È possibile trovare telecamere di sicurezza e fotocamere Web accessibili in tempo reale.
- Analisi dei Protocolli: Shodan analizza i protocolli di comunicazione utilizzati da dispositivi e server, fornendo informazioni dettagliate sulle loro funzionalità.

Utilizzi Pratici

Le potenzialità di Shodan si estendono in vari ambiti:

1. Sicurezza Informatica: Gli esperti di sicurezza utilizzano Shodan per identificare e proteggere dispositivi e server esposti online, nonché per scoprire vulnerabilità potenziali.
2. Ricerca di Dispositivi IoT: È possibile trovare e monitorare dispositivi IoT, utili sia per scopi di gestione che per la sicurezza.
3. Analisi di Rete: Shodan può essere utilizzato per mappare la struttura di una rete e identificare i dispositivi connessi.

Interfacce Shodan

È possibile interagire con Shodan tramite il sito Web, lo strumento e la libreria dell'interfaccia della riga di comando ufficiale di Python, una varietà di librerie guidate dalla comunità per molte lingue e anche l'API REST ufficiale.

Shodan dispone di diverse funzioni (alcune a pagamento) come la ricerca per immagini, quasi come Google, solo che a differenza di Google le immagini che troverete (come tutto del resto) non sono contenuti volutamente pubblicati dagli utenti...

<https://youtu.be/H4xj13QKVfQ>

Shodan funziona un pò come Google, per cui vi mostro le Query principali per un utilizzo di base:

- city: Cerca dispositivi per Città
- country: Cerca dispositivi per località es. IT
- geo: Cerca dispositivi partendo da coordinate geografiche
- hostname: Cerca risultati per un certo hostname
- net: Cerca dispositivi per IP o NetRange
- os: Cerca un Sistema Operativo es. windows
- port: Cerca dispositivi con una certa porta aperta es. 80, 21, etc...
- before/after: Cerca risultati entro un periodo di tempo

Plugin

Questo componente aggiuntivo recupera i dati raccolti da [Shodan.io](https://shodan.io) del sito Web corrente che stai navigando. Visualizza le informazioni generali come l'organizzazione ma anche le porte aperte.

Il plugin Shodan ti dice dove è ospitato il sito web (paese, città), chi possiede l'IP e quali altri servizi / porte sono aperti.

Il plug-in Shodan per Chrome verifica automaticamente se Shodan dispone di informazioni per il sito Web corrente. Il sito web esegue anche FTP, DNS, SSH o qualche servizio insolito? Con questo plugin puoi vedere tutte le informazioni che Shodan ha raccolto su un determinato sito web / dominio.

Limitazioni e Controversie

Come ogni strumento, Shodan ha le sue limitazioni. Ad esempio, può non essere in grado di identificare dispositivi non connessi a Internet o dispositivi che utilizzano tecniche avanzate di occultamento. Inoltre, l'accessibilità pubblica di Shodan solleva questioni sulla sicurezza e la privacy, che devono essere prese in considerazione attentamente.

Esistono delle [alternative](#) a Shodan, ossia Zoom Eye (l'omologo cinese) e Censys (un progetto dell'Università del Michigan). Ma ai fini lavorativi non possono competere con Shodan.

Scavare in Profondità con Shodan.

Il Potere di Shodan.

Nel vasto e sempre crescente universo digitale, l'accesso alle informazioni è la chiave per il successo. E quando si tratta di informazioni relative agli asset tecnologici in rete, Shodan emerge come uno strumento di ricerca cruciale. In questo articolo, esploreremo in profondità Shodan, il "motore di ricerca per Internet delle cose (IoT)" che sta rivoluzionando la ricerca tecnologica.

A differenza dei motori di ricerca che ti aiutano a trovare siti web, Shodan si avvale di sistemi di scansione capaci di individuare qualsiasi cosa sia online: Router, WebCam, GPS, Smart TV, Sistemi di controllo Industriale (ICS), WebServer, Stampanti, Frigoriferi (SI anche quelli oggi vanno online), etc...e altro.

Queste informazioni includono metadati come il software in esecuzione su ogni dispositivo.

Gli usi comuni di Shodan includono **sicurezza di rete, ricerche di mercato, rischio informatico, scansione di dispositivi IoT e monitoraggio ransomware**. Tuttavia, Shodan può essere utilizzato anche per scopi malintenzionati, come trovare dispositivi vulnerabili da attaccare.

Cos'è Shodan?

Shodan è stato lanciato nel 2009 da John Matherly ed è stato definito il motore di ricerca degli hacker.

Shodan è molto più di un semplice motore di ricerca. È un potente strumento di scansione di rete che analizza costantemente il web in cerca di dispositivi connessi. Questi dispositivi possono includere server, telecamere di sicurezza, router, dispositivi IoT e molto altro. Shodan non solo identifica questi dispositivi, ma fornisce anche informazioni dettagliate su di essi, come il tipo di dispositivo, la versione del software utilizzato, le porte aperte e persino dati sensibili accidentalmente esposti online.

La Forza dell'Accesso Pubblico

Una delle caratteristiche più sorprendenti di Shodan è che è un motore di ricerca accessibile a chiunque. Questo significa che sia esperti di sicurezza informatica che appassionati di tecnologia possono utilizzarlo per raccogliere informazioni sulle risorse online. Tuttavia, con un grande potere viene anche una grande responsabilità, ed è fondamentale utilizzare Shodan in modo etico e legale, evitando di violare la privacy o la sicurezza altrui.

Le Potenzialità di Shodan

Shodan offre un ventaglio di potenzialità impressionante:

- **Ricerca di Dispositivi Specifici:** Gli utenti possono cercare dispositivi specifici in base a criteri come il tipo, il marchio o la posizione geografica.
- **Monitoraggio delle Porte:** Shodan può identificare le porte aperte su un dispositivo, rivelando potenziali vulnerabilità di sicurezza.
- **Visualizzazione delle Webcam:** È possibile trovare telecamere di sicurezza e fotocamere Web accessibili in tempo reale.
- **Analisi dei Protocolli:** Shodan analizza i protocolli di comunicazione utilizzati da dispositivi e server,

fornendo informazioni dettagliate sulle loro funzionalità.

Utilizzi Pratici

Le potenzialità di Shodan si estendono in vari ambiti:

1. Sicurezza Informatica: Gli esperti di sicurezza utilizzano Shodan per identificare e proteggere dispositivi e server esposti online, nonché per scoprire vulnerabilità potenziali.
2. Ricerca di Dispositivi IoT: È possibile trovare e monitorare dispositivi IoT, utili sia per scopi di gestione che per la sicurezza.
3. Analisi di Rete: Shodan può essere utilizzato per mappare la struttura di una rete e identificare i dispositivi connessi.

Interfacce Shodan

È possibile interagire con Shodan tramite il sito Web, lo strumento e la libreria dell'interfaccia della riga di comando ufficiale di Python, una varietà di librerie guidate dalla comunità per molte lingue e anche l'API REST ufficiale.

Shodan dispone di diverse funzioni (alcune a pagamento) come la ricerca per immagini, quasi come Google, solo che a differenza di Google le immagini che troverete (come tutto del resto) non sono contenuti volutamente pubblicati dagli utenti...

<https://youtu.be/H4xj13QKVfQ>

Shodan funziona un pò come Google, per cui vi mostro le Query principali per un utilizzo di base:

- city: Cerca dispositivi per Città
- country: Cerca dispositivi per località es. IT
- geo: Cerca dispositivi partendo da coordinate geografiche
- hostname: Cerca risultati per un certo hostname
- net: Cerca dispositivi per IP o NetRange
- os: Cerca un Sistema Operativo es. windows
- port: Cerca dispositivi con una certa porta aperta es. 80, 21, etc...
- before/after: Cerca risultati entro un periodo di tempo

Plugin

Questo componente aggiuntivo recupera i dati raccolti da [Shodan.io](https://shodan.io) del sito Web corrente che stai navigando. Visualizza le informazioni generali come l'organizzazione ma anche le porte aperte.

Il plugin Shodan ti dice dove è ospitato il sito web (paese, città), chi possiede l'IP e quali altri servizi / porte sono aperti.

Il plug-in Shodan per Chrome verifica automaticamente se Shodan dispone di informazioni per il sito Web corrente. Il sito web esegue anche FTP, DNS, SSH o qualche servizio insolito? Con questo plugin puoi vedere tutte le informazioni che Shodan ha raccolto su un determinato sito web / dominio.

Limitazioni e Controversie

Come ogni strumento, Shodan ha le sue limitazioni. Ad esempio, può non essere in grado di identificare dispositivi non connessi a Internet o dispositivi che utilizzano tecniche avanzate di occultamento. Inoltre, l'accessibilità pubblica di Shodan solleva questioni sulla sicurezza e la privacy, che devono essere prese in considerazione attentamente.

Esistono delle [alternative](#) a Shodan, ossia Zoom Eye (l'omologo cinese) e Censys (un progetto

dell'Università del Michigan). Ma ai fini lavorativi non possono competere con Shodan.