

DARKWEB



**Individua le credenziali
esposte nel dark web**



sinattica
SERVIZI EVOLUTI PER L'AZIENDA

DARKWEB

Credenziali web: Tra sicurezza e rischi

76%

Percentuale di adulti che utilizzano password identiche o molto simili per decine di servizi online.

Oggi le credenziali rappresentano il **metodo più comune per accedere in modo esclusivo a un servizio online o a una risorsa informatica.**

Di fronte a questa tendenza è chiaro che, anche per i cyber criminali, le stesse vengano identificate come **la chiave di accesso alle risorse più preziose di un utente o di un'organizzazione.**

da 1 a 8€

Tipica gamma di prezzo con cui è possibile acquistare credenziali rubate nel mercato del dark web.

In generale, questo traffico illecito può fruttare decine di migliaia di euro. Ciò nonostante, per via della facilità con cui gli hacker riescono ad appropriarsene, **le singole credenziali vengono vendute a prezzi molto convenienti all'interno del dark web** (la parte più oscura e insidiosa del web frequentata da malintenzionati e hacker).

80%

Percentuale di attacchi informatici che avviene sfruttando credenziali deboli o compromesse.

Con l'obiettivo di accaparrarsi un ricco bottino, i criminali prediligono quindi furti di tipo massivo. Ma ad ogni modo, quando delle credenziali vengono violate, **privati e/o imprese coinvolte risultano automaticamente esposte al rischio di nuove aggressioni digitali** dalle gravi ripercussioni economiche e reputazionali.

Come vengono rubate le credenziali?



PHISHING

- Tramite e-mail camuffate da messaggi provenienti da mittenti legittimi.
- Inducendo gli utenti a rivelare i propri nomi utente e le proprie password.
- Sfruttando software malevoli in grado di acquisire credenziali.



WATERING HOLES

- Prendendo di mira gli utenti tramite social media o intranet aziendali.
- Inserendo uno o più malware nel codice di un sito internet o di un'app.
- Utilizzando software malevoli in grado di acquisire credenziali.



MALVERTISING

- Inserendo un software malevolo in reti o network che promuovono pubblicità legittimamente.
- Sviluppando malware capaci di acquisire username, password e altri dati sensibili dei visitatori.



ATTACCHI WEB

- Sfruttando le vulnerabilità delle componenti hardware o software.
- Cercando all'interno della rete un modo per reperire credenziali di accesso.
- Approfittandosi delle falle delle risorse che si collegano a internet.



Quali sono gli obiettivi dei malintenzionati?

 <p>Inviare spam da account di posta elettronica compromessi</p>	 <p>Impadronirsi di siti web per installare malware</p>	 <p>Installare software dannosi su sistemi compromessi</p>
 <p>Compromettere altri account tramite le stesse credenziali</p>	 <p>Impossessarsi di dati sensibili di privati e organizzazioni</p>	 <p>Rubare l'identità degli utenti per estorcergli denaro</p>

In assenza delle adeguate tutele, qualsiasi organizzazione è quotidianamente esposta al rischio di un attacco informatico causato dalla **compromissione di credenziali di servizi aziendali** come:

- **OFFICE 365**
- **VOIP**
- **SERVIZI PAYROLL**
- **ERP**
- **SOCIAL MEDIA**
- **CLOUD**
- **CRM**
- **REMOTE DESKTOP**
- **VPN**
- **CONTACT FORM**

Ciò nonostante, **la maggior parte delle violazioni di dati sfrutta fattori comuni e sottovalutati** come un'inadeguato sistema di protezione, l'utilizzo di password "deboli" e ancora prima la disattenzione e la scarsa consapevolezza dei dipendenti.



La soluzione di Sinattica contro i rischi legati alla compromissione delle credenziali

Dark Web ID è la soluzione adottata da Sinattica per **individuare e monitorare la presenza di credenziali** appartenenti ai domini aziendali **all'interno del dark web**.

Denominato **Dark Scan**, questo processo può avvenire in tre diverse modalità:

One time Scansione eseguita in una singola sessione.	Regular Scansione eseguita ogni 30 giorni.	Continuous Scansione eseguita h. 24, 7 giorni su 7.
--	--	---

Una volta eseguita la scansione e rintracciate le eventuali credenziali, i nostri consulenti elaboreranno un **report** in cui per ogni dominio aziendale verranno elencati **i dati dei singoli e/o dell'organizzazione compromessi**, quindi esposti ai rischi del dark web.

I vantaggi per la tua impresa



RICERCA APPROFONDATA

Dark Web ID permette a Sinattica di verificare la presenza di dati aziendali all'interno di botnet, reti, chatroom e network criminali.



SCANSIONE CONTINUA

Eseguita con continuità, l'attività di scansione consente di rispondere tempestivamente a qualsiasi sottrazione di dati subita.



MAGGIORE PROTEZIONE

Grazie agli esiti del processo è possibile limitare l'utilizzo improprio di credenziali violate e ridurre l'esposizione dell'azienda ai rischi correlati.



sinattica
SERVIZI EVOLUTI PER L'AZIENDA

Contatti



Tel. 030 777 8487
info@sinattica.com



pss@sinattica.com
pss.sinattica.com



Via Cremona, 10
25025, Manerbio (BS)



Rev. Luglio 2022