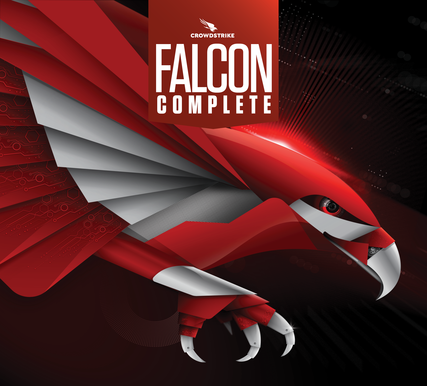

FALCON COMPLETE IN AZIONE

Per difendersi dalle minacce odierne serve un sistema di vigilanza costante affidato a personale competente.

CrowdStrike® Falcon Complete™ è un servizio gestito di rilevamento e gestione degli incidenti informatici (MDR) che assicura analisi approfondite e risposte mirate 24/7.

Scopri la differenza che Falcon Complete può fare per te.

INCIDENT RESPONSE CON UN SISTEMA BEST EFFORT	ATTACCO INFORMATICO Tempo trascorso (ORE: MIN.)	INCIDENT RESPONSE CON IL SISTEMA PROFESSIONALE FALCON COMPLETE
	0:00 L'aggressore ottiene credenziali tramite il **phishing**	
Il malware è bloccato dalla soluzione di protezione degli endpoint locale Generato un avviso di bassa priorità, ignorato in quanto non grave	**0:02** Connessione a un dominio malevolo e tentativo di diffusione di **malware** di secondo livello	**Il malware è bloccato** da Falcon Prevent™ Generato un avviso di bassa priorità
	0:30	L'avviso di bassa priorità **viene analizzato** dal team Falcon Complete Il team Falcon Complete esamina il malware bloccato e scopre che è associato a un gruppo criminale specializzato in attacchi ransomware nel settore finanziario Un analista si assicura che le policy configurate siano in grado di rilevare eventuali nuove attività malevole
	6:00 **L'aggressore accede** al sistema **via RDP** usando credenziali utente valide	
	6:10 L'aggressore si accorge che l'infezione iniziale non è riuscita, sospetta che sia attivo un sistema locale di protezione degli endpoint, adotta una **tattica stealth** e, sfruttando una funzionalità del sistema operativo nativo, avvia attività di ricognizione a livello locale	
L'aggressore individua un nuovo **server di sviluppo non protetto** dall'endpoint locale	**7:30**	L'aggressore **non trova sistemi non protetti** e demoralizzato continua a cercare, anche caricando nuovi congegni
L'aggressore **prende di mira il server non protetto** Il server dovrà essere azzerato e sottoposto a reinstallazione	**7:45**	L'analista di Falcon Complete rileva l'attività dell'aggressore e **inizia le operazioni di analisi e intervento**
	7:55	L'analista di Falcon Complete isola il sistema colpito nella rete **ed espelle l'aggressore**
L'aggressore carica un malware Mimikatz personalizzato e **si procura credenziali da amministratore** Tutti gli account amministratore globali devono essere resettati	**8:00**	Con un avviso di alta priorità al cliente viene chiesto **di resettare l'unico account utente interessato**
L'aggressore **si sposta lateralmente** all'interno dell'ambiente aziendale Serve un'indagine per seguire lo spostamento laterale dell'aggressore	**8:05**	L'analista di Falcon Complete **rimuove tutte le tracce** lasciate dall'aggressore
	8:30	Il cliente riceve una segnalazione con dettagli sull'intrusione, dati di contestualizzazione e consigli per migliorare la security posture **e ridurre il rischio di subire intrusioni analoghe in futuro**
L'aggressore **impiega malware mirato** e si sposta lateralmente nell'ambiente implementando meccanismi di **persistenza** Alcune attività si bloccano, altre generano avvisi di sicurezza, ma la giornata è finita e il personale non è più in ufficio	**18:45**	
Serve un'indagine per seguire lo spostamento laterale dell'aggressore Diversi altri host dovranno essere azzerati e sottoposti a reinstallazione		
Gli addetti alla sicurezza individuano gli avvisi critici e mettono in campo un intervento di emergenza Gli addetti alla sicurezza devono lavorare per giorni e giorni	**31:30**	

CONSEGUENZE DELLO SCENARIO BEST EFFORT: RISPOSTA COSTOSA E CON EFFETTI PESANTI

Ore di laboriose indagini

Reinstallazione dei sistemi scomoda e costosa

Nessuna certezza che l'aggressore non torni

CONSEGUENZE DELLO SCENARIO FALCON COMPLETE: RISPOSTA RAPIDA ED EFFICACE

Intrusione contenuta e neutralizzata nel giro di pochi minuti

Nessun intervento del personale IT

Nessuna interruzione dei processi aziendali, nessun disagio per gli utenti

Certezza che la minaccia sia stata gestita correttamente e in maniera definitiva

CROWDSTRIKE

PER MAGGIORI INFORMAZIONI SU FALCON COMPLETE, VISITA
WWW.CROWDSTRIKE.COM/FALCON-COMPLETE