FALCON COMPLETE IN AKTION

Die Abwehr gegen heutige Bedrohungen verlangt die ständige Wachsamkeit qualifizierter Analysten.

CrowdStrike® Falcon Complete™ ist ein sofort einsatzbereiter MDR-Dienst (Managed Detection and Response) zur verwalteten Bedrohungserkennung und -reaktion, der rund um die Uhr und an 365 Tagen im Jahr hochqualifizierte Untersuchungen und präzise Reaktionen garantiert.

Sehen Sie selbst, welchen Unterschied Falcon Complete für Sie ausmachen kann.

REAKTION AUF SICHERHEITSVORFÄLLE NACH BESTEM VERMÖGEN	GEGNERISCHE AKTIVITÄT Verstrichene Zeit (STD:MIN)	ABWEHR VON SICHERHEITSVORFÄLLEN MIT DEN EXPERTEN VON FALCON COMPLETE
	0:00 Der Angreifer späht Zugangsdaten durch **Phishing** aus.	
Die **Malware** wird von der lokalen Endgerätesschutzlösung **blockiert.** Es wird ein Alarm mit geringer Kritikalität ausgelöst, aber als unkritisch verworfen.	**0:02** Der Angreifer stellt eine Verbindung zu einer bösartigen Domäne her und versucht von dort, eine zweite **Malware** zu implementieren.	Die **Malware** wird von Falcon Prevent™ **blockiert.** Es wird ein Alarm mit niedriger Kritikalität ausgelöst.
	0:30	Das Team von Falcon Complete **untersucht den Alarm.** Das Team von Falcon Complete führt eine Sichtung der blockierten Malware durch und erkennt, dass diese mit einer Gruppe von Bedrohungsakteuren in Zusammenhang steht, die Unternehmen aus dem Finanzwesen mit Ransomware erpressen. Der Analyst prüft, ob die Richtlinien einwandfrei konfiguriert sind, damit mögliche weiter gegnerische Aktivitäten erkannt werden.
	6:00 Der **Angreifer meldet sich** über **RDP** mit gültigen Zugangsdaten im System an.	
	6:10 Der Angreifer stellt fest, dass die erste Malware-Implementierung fehlgeschlagen ist. Er vermutet, dass ein lokaler Endgeräteschutz vorhanden ist. Daher wendet er **verdeckte Taktiken** an und nutzt native OS-Funktionen, um die Lage vor Ort auszuspähen.	
Der Angreifer identifiziert einen neu aufgesetzten **Entwicklungsserver, der (noch) nicht von der lokalen Endgeräteschutzlösung abgedeckt ist.**	**7:30**	Der Angreifer erkennt, dass **keine ungeschützten Systeme** vorhanden sind. Er setzt daher seine Erkundungen fort und lädt zusätzliche Werkzeuge herunter.
Der Gegner **geht weiter zu dem ungeschützten Server.** Der Server muss gelöscht und ein neues Image muss aufgespielt werden.	**7:45**	Der Analyst von Falcon Complete erkennt gegnerische Aktivitäten und **beginnt mit Untersuchungen und Reaktionsmaßnahmen.**
	7:55	Der Analyst von Falcon Complete nimmt das betroffene System vom Netz und **wirft den Angreifer heraus.**
Der Angreifer lädt eine angepasste Mimikatz-Malware herunter, erzeugt einen Dump der Zugangsdaten und **greift die Admin-Zugangsdaten ab.** Alle globalen Admin-Konten müssen zurückgesetzt werden.	**8:00**	Der Kunde wird über eine kritische Eskalation gebeten, das identifizierte **betroffene Benutzerkonto zurückzusetzen.**
Der Angreifer **bewegt sich lateral weiter** im Netzwerk der Organisation. Um die Bewegungen des Angreifers verfolgen zu können, sind weitere Untersuchungen notwendig.	**8:05**	Der Analyst von Falcon Complete **entfernt alle Tools und verbleibenden Artefakte,** die der Angreifer hinterlassen hat.
	8:30	Der Kunde erhält eine Benachrichtigung mit Einzelheiten zum Angriff, einschließlich Hintergrundinformationen und Empfehlungen zur Verbesserung der Sicherheitsaufstellung, damit **künftige ähnliche Angriffe ausgeschlossen werden können.**
Der Angreifer bringt spezielle Malware in Stellung und setzt **Persistenzmechanismen** ein, während er sich lateral weiter in der Organisation fortbewegt. Einige Aktivitäten werden blockiert, andere werden als Sicherheitswarnungen protokolliert. Die Mitarbeiter sind allerdings bereits im Feierabend. Um die Bewegungen des Angreifers verfolgen zu können, sind weitere Untersuchungen notwendig. Mehrere weitere Hosts müssen gelöscht und mit einem neuen Image versehen werden.	**18:45**	
Die Sicherheitsverantwortlichen erkennen kritische Alarme und leiten Notfallmaßnahmen ein. Die Mitarbeiter sind auf Tage hinaus mit der Schadensbehebung beschäftigt.	**31:30**	

DAS ERGEBNIS NACH BESTEM VERMÖGEN: KOSTSPIELIGE REAKTIONEN UND SYSTEMAUSFÄLLE

Stundenlange, arbeitsintensive Untersuchungen

Umständliches und teures Re-Imaging

Die Ungewissheit, ob der Angreifer zurückkehrt, bleibt

DAS ERGEBNIS VON FALCON COMPLETE: SCHNELLE UND WIRKSAME REAKTION

Der Angreifer wurde innerhalb weniger Minuten herausgeworfen. Die Systeme bleiben sicher

Kein Eingriff seitens der eigenen IT-Mitarbeiter

Keine Unterbrechung von Geschäftsprozessen oder Benutzervorgängen

Beruhigende Gewissheit, dass die Bedrohung umfassend und präzise aus der Welt geschafft wurde

CROWDSTRIKE

Mehr über Falcon Complete erfahren Sie auf unserer www.crowdstrike.de/endpoint-security-produkte/falcon-complete/