VECTRA
SECURITY THAT THINKS

E-BOOK

Come bloccare il ransomware: notizie da chi lavora in prima linea

Introduzione

Posto che nessuna azienda vorrebbe scoprire che un attacco ransomware sta mettendo a rischio il suo ambiente informatico, se fosse possibile riconoscere velocemente i segnali di attacco, ci sarebbero buone probabilità di bloccarlo. Ma come si fa? Parleremo proprio di questo con esempi tratti dalla vita reale che illustrano come i nostri clienti più importanti collaborano con il team Vectra Sidekick per reagire alle prime fasi degli attacchi ransomOps ed evitare disastrose interruzioni operative causate dalla diffusione del ransomware.

L'e-book spiega perché per bloccare gli attacchi ransomware è fondamentale rilevare le attività di ricognizione e attacco denominate ransomOps e quali misure stanno adottando i responsabili della sicurezza per sbarrare la strada ai tentativi di intrusione ransomware. Racconteremo anche come i clienti utilizzano Vectra Sidekick Services per rilevare gli attacchi in corso pressoché immediatamente, senza dimenticare di formulare osservazioni e consigli, né di attirare l'attenzione sulle sfide di cui ogni azienda deve essere consapevole.

Una cosa è certa: quando si tratta di bloccare un attacco ransomware, la differenza tra successo e fallimento dipende dalla velocità di reazione e dalla rapidità di intervento. Sbarriamo la strada al ransomware!

Servizio Vectra Sidekick MDR

Vectra Sidekick MDR è un servizio di monitoraggio continuo 24/7 che esegue indagini proattive sulle attività malevole rilevate da Vectra Detect.

Mettendo a disposizione professionisti della sicurezza di comprovata esperienza, SideKick MDR agisce come moltiplicatore di forze per i responsabili della sicurezza e aiuta a utilizzare al meglio l'intelligenza artificiale di Vectra per rilevare precocemente le minacce e bloccare le violazioni. Aggiungi il servizio Sidekick MDR alla piattaforma Vectra per:

- Affiancare ai tuoi responsabili della sicurezza un team di esperti professionisti che li aiuteranno a tenere testa a sofisticati hacker e attacchi ransomware.
- Ottenere informazioni, contesto e chiarezza sui segnali precoci rilevati da Vectra Detect che rivelano la presenza di un attacco informatico, di una minaccia o di un attacco ransomware e agire rapidamente con l'aiuto di esperti analisti.
- Attivare un monitoraggio proattivo 24/7 che comunica quando una minaccia prioritaria o un sospetto ransomware richiede una reazione immediata.
- Personalizzare la tua implementazione Vectra in base alle particolari esigenze del tuo ambiente, dei tuoi obiettivi di business e dei rischi legati al settore in cui operi. Potrai adeguare i controlli, ricevere consigli da esperti, imparare le metriche e i trend specifici dell'ambiente e accelerare le indagini.

Il ransomware è un business

Per quanto odioso possa sembrare, i cybercriminali dediti al ransomware gestiscono un business che, come qualsiasi altro business, ha lo scopo di generare guadagni. Questi criminali hanno una mentalità orientata al profitto, che perseguono grazie alla capacità di violare i sistemi e impadronirsi più velocemente possibile dei dati che contengono chiedendo un riscatto considerevole per la loro restituzione.

La consapevolezza della mentalità che anima queste persone è alla base di molte osservazioni che trovano posto in questo e-book, anche perché comprendere le motivazioni che muovono gli attaccanti è essenziale per mettere a punto qualsiasi strategia di sicurezza. Se l'azienda conosce l'obiettivo che perseguono gli attaccanti e riesce a stabilire con chiarezza quali sono i sistemi e i dati della rete che bloccherebbero l'attività se venissero compromessi, è ben posizionata per contrastare al meglio qualsiasi attacco.

Scopriamo perché le simulazioni di attacco aiutano a fare chiarezza e in che modo i Red Team possono valutare con obiettività l'attuale grado di preparazione.

Partiamo dalle basi

Naturalmente, l'obiettivo primario consiste nell'impedire ai cybercriminali di introdursi nel tuo ambiente. Se, da una parte, le misure preventive non sono mai a prova di errore, tenere presente come funziona una mentalità orientata al profitto può lavorare a tuo favore. Addirittura, puoi ridurre drasticamente il tuo livello di rischio applicando i principi base in materia di autenticazione e risoluzione delle vulnerabilità dal momento che molto spesso l'accesso iniziale avviene sfruttando una vulnerabilità non corretta sulla rete perimetrale, un account senza autenticazione a più fattori o un'analoga leggerezza. In pratica, se le aziende trascurano di adottare i più elementari metodi di prevenzione, gli hacker non hanno la necessità di ricorrere a tattiche laboriose e sofisticate per infiltrarsi.

> L'obiettivo primario consiste nell'impedire ai cybercriminali di introdursi nel tuo ambiente.

Fortunatamente, anche limitandosi ad attivare l'autenticazione a più fattori sulla VPN, l'IDP e gli altri punti di ingresso della rete, si intralcia seriamente il percorso dei cybercriminali, che potrebbero semplicemente decidere di andare a bussare altrove. Lo stesso vale per la gestione delle patch: correggere le vulnerabilità dell'intera rete perimetrale è un buon modo per sviare gli attacchi. Benché nessuna strategia sia a prova di errore, investendo in modo mirato nella prevenzione si renderà la vita più difficile ai cybercriminali.

Preparati a reagire velocemente, giorno e notte

Adottare le misure di sicurezza di base ti aiuta a gestire il rischio, ma non a eliminarlo. Questo accade per una serie di motivi, ma il principale è che basta una svista – un errore di configurazione di un account, una vulnerabilità ignorata, un utente che fa clic su un link pericoloso, un nuovo zero-day nella VPN (finanziato dagli ingenti capitali che l'ecosistema ransomware attira) – per restare esposti. Ne abbiamo viste di tutti i colori.

Un hacker che lancia un attacco ransomware e riesce a introdursi nel tuo ambiente, generalmente si muove RAPIDAMENTE. Anche se ci è capitato di gestire attacchi che progredivano lentamente nell'arco di più giorni, quelli che si risolvono in una serata o nottata sono tutt'altro che rari. Ricordiamoci che per chi ha una mentalità orientata al profitto, il tempo è denaro. Vuoi per l'intento di lasciare ai responsabili della sicurezza il minor tempo possibile per reagire o per una questione di grandi numeri, sono pochi i cybercriminali che scelgono di tenere un basso profilo. Lo dimostra il fatto che i tempi di permanenza complessivi degli attacchi ransomware sono drasticamente diminuiti nell'arco degli ultimi anni.

La notizia positiva per chi si occupa di sicurezza informatica è che, potendo fare affidamento su una tecnologia di rilevamento efficace, la velocità dell'attacco lo rende palese. Utilizzando Vectra, ad esempio, abbiamo rilevato host compromessi nel giro di due minuti dall'accesso iniziale. In ragione della velocità di progressione dell'attacco, tuttavia, è necessario essere pronti a reagire con decisione e in tempi brevi per bloccare la minaccia prima che il ransomware infetti il sistema.

E questa capacità di reagire quasi istantaneamente non può essere limitata agli orari d'ufficio. Abbiamo assistito ad attività preliminari di ricognizione e movimento laterale a qualsiasi ora, verosimilmente quando il cybercriminale ha un po' di tempo libero. A volte avvengono di giorno, altre di notte, altre ancora durante un giorno di ferie. In ogni caso, in base alla nostra esperienza, le operazioni finali di estrazione e criptazione dei dati tendono a verificarsi di notte, durante il fine settimana o nei giorni di ferie, cioè quando le capacità di risposta agli incidenti sono meno reattive.

In pratica, è necessario monitorare la situazione 24 ore su 24, 7 giorni su 7.

Elabora la tua strategia di reazione

La prima mossa che ti permette di reagire a un possibile attacco ransomware è rilevare la presenza dell'attaccante nel tuo ambiente. Decidere come comportarti per bloccare l'attacco simulando scenari diversi è però ugualmente importante. Fino a dove sei disposto a spingerti? In uno dei casi in cui siamo intervenuti, l'attaccante era riuscito ad acquisire i privilegi di amministratore del dominio sul controller di dominio e il team di sicurezza ha dovuto decidere nel giro di un secondo di scollegare completamente tutti i sistemi da Internet per guadagnare tempo. Fortunatamente, la decisione ha sortito l'effetto sperato.

In questo caso il team è riuscito a prevenire in extremis la diffusione del ransomware, ma questo tipo di situazione non è affatto inusuale, tanto che vale la pena chiedersi: se la mia azienda si trovasse nella stessa situazione, che cosa farei? Considererei accettabile questo livello di disruption? Sarei in grado di organizzare una risposta efficace se i miei addetti alla sicurezza dovessero lavorare da remoto senza connessione? Esistono altre opzioni a cui dovrei ricorrere?

Come abbiamo visto, saper reagire in modo rapido e deciso quando siamo sotto pressione è un ingrediente chiave per rispondere in maniera efficace. Definire e testare precocemente la propria strategia potrebbe davvero fare la differenza.

Per bloccare il ransomware, non cercare il ransomware

Nei nuovi attacchi ransomware (ransomOps), la diffusione del codice binario è solo l'ultima fase del piano, pertanto quando si riesce a rilevare la presenza del ransomware, significa che è quasi sicuramente troppo tardi.

Questo aspetto è largamente misconosciuto. Per bloccare un attacco in corso è necessario rilevare e contrastare quanto avviene PRIMA che il ransomware venga diffuso. Nella realtà, ci succede di muoverci senza sapere con precisione che tipo di avversario dobbiamo affrontare e qual è il suo obiettivo finale. In molti casi, assistiamo a un attacco che progredisce rapidamente e a volte individuiamo indizi nel toolset o nell'infrastruttura C2 che ci permettono di supporre con ragionevole precisione che cosa stia succedendo.

A questo punto, il piano di risposta deve affrontare l'intrusione e la progressione dell'attacco in maniera abbastanza ampia perché capire qual è l'obiettivo finale è più una probabilità che una certezza.

L'importanza strategica degli account e dei tool di amministrazione

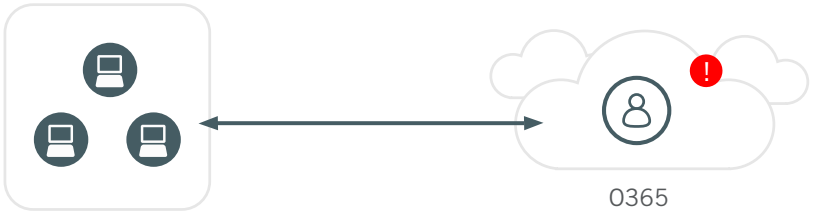
Pur avendo assistito all'uso di exploit per ottenere l'accesso iniziale e allargare l'offensiva tramite il movimento laterale, possiamo affermare che lo stile più moderno di attacco prevede lo sfruttamento delle credenziali, in particolare quelle degli account di servizio e degli amministratori. Insieme ai protocolli amministrativi, l'uso delle credenziali è la tattica prediletta da praticamente tutti gli affiliati del ransomware.

Lo scopo è quello di ottenere privilegi amministrativi di dominio sul controller di dominio, così da poter sferrare la fase finale dell'attacco. Da questo punto privilegiato è facile accedere ai dati più preziosi e diffondere il ransomware a velocità strabiliante usando strumenti di amministrazione, come quelli che applicano policy di gruppo (GPO).

Visto il notevole interesse dimostrato dai cybercriminali per le credenziali, monitorare l'uso di tutti gli account con privilegi è assolutamente cruciale perché risulta essere uno dei metodi di rilevamento degli attacchi in assoluto più affidabili.

Tematiche comuni

Gli analisti di Vectra hanno stilato un elenco delle problematiche relative a utenti, processi e sicurezza che accomunano i clienti presso i quali sono intervenuti.



Accesso iniziale:

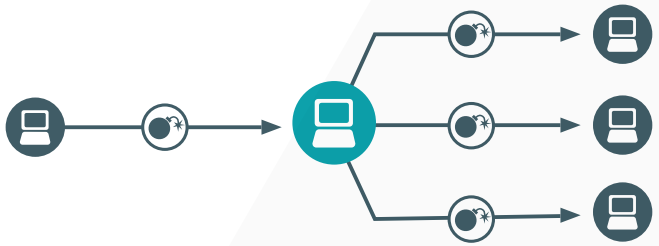
- Gli attaccanti cercano senza sosta le vulnerabilità presenti nei servizi e sistemi esposti a Internet e disponibili pubblicamente.
- I server che eseguono RDP, FTP e VPN sono bersagli comunemente utilizzati per l'accesso iniziale alle aziende e al cloud.
- La mancanza dell'autenticazione a più fattori è una lacuna di sicurezza largamente sfruttata.
- In alcuni casi la progressione dell'attacco ha richiesto ore a partire dall'infiltrazione iniziale, e in altri casi giorni o addirittura settimane. I responsabili della sicurezza dispongono di tempo sufficiente per rilevare il problema e contrastarlo, ma solo se è presente un servizio di vigilanza 24x7.

C2:

- Cobalt Strike sembra essere lo strumento preferito del momento.
- Per ottenere il controllo dei sistemi vengono utilizzati anche gli strumenti di accesso remoto più diffusi, a prescindere che siano stati autorizzati o meno. In un caso, è stato utilizzato il software Cisco AnyConnect per controllare i computer dall'interno con l'ausilio di una persona esterna.

Ricognizione e movimento laterale

- In molti casi, le procedure di scansione sono state aggressive, arrivando a includere la mappatura della rete, il ricorso a query rDNS e l'enumerazione delle condivisioni. Queste procedure di scansione così rapide generalmente hanno permesso di rendere gli attacchi visibili nel giro di pochi minuti dall'infiltrazione iniziale.
- Sono emerse spesso attività di ricognizione finalizzate alla ricerca di credenziali, come le query LDAP e le chiamate RPC per mappare la posizione delle credenziali.
- Le fasi iniziali del movimento laterale prevedevano lo sfruttamento di falle di sicurezza note, mentre le successive ricorrevano principalmente all'utilizzo delle credenziali e dei protocolli amministrativi.



Estrazione dei dati

- I dati di ricognizione da sottoporre ad analisi sono stati spesso caricati su siti gratuiti per la condivisione dei file, come Mega Upload (mega.com) e temp.sh.

Suggerimenti

Ogni giorno i nostri team lavorano a stretto contatto con responsabili della sicurezza e rispondono agli avvisi critici generati dalle soluzioni di rilevamento e risposta alle minacce basate su IA di Vectra. Quando inizia il nostro intervento presso un cliente, non è subito chiaro se la natura del problema riguardi il ransomware. Man mano che la gravità degli avvisi aumenta, siamo in grado di delineare con più chiarezza il contesto della minaccia e stabilire se si tratta di ransomware. Abbiamo individuato vari strumenti e pratiche di sicurezza che rendono più complicato per gli attaccanti mettere a segno campagne di ransomware e che in ultima battuta riescono persino a bloccarle completamente. Eccone una sintesi:

Prevenzione

- Valutare con cadenza regolare il proprio stato di sicurezza esterno e implementare le correzioni prioritarie. Concentrarsi specialmente sull'infrastruttura per l'accesso remoto e i servizi comunemente considerati più vulnerabili come RDP e FTP, che sono bersagli diffusamente sfruttati.
- Ove possibile, attivare l'autenticazione a più fattori su qualsiasi provider di identità o sull'infrastruttura per l'accesso remoto.
- In generale, la predisposizione di controlli preventivi, regole e policy di sicurezza solidi rende più difficile dar vita all'escalation dei privilegi anche quando l'accesso è già avvenuto, il che permette di guadagnare tempo per elaborare una risposta.
- Prestare particolare attenzione agli account con privilegi. Pur se impegnativo dal punto di vista operativo, più ci si affida a jump server e sistemi di gestione degli account con privilegi, minore è la probabilità che un hacker riesca a mettere a segno un'operazione di escalation dei privilegi.

Rilevamento

- Dopo che l'attaccante ha guadagnato accesso al sistema, ma prima che i dati siano stati esfiltrati o che il ransomware sia stato diffuso, c'è ancora tempo per bloccare l'attacco ransomware.
- Investire in strumenti di rilevamento e risposta alle minacce da implementare nella rete, nell'infrastruttura di gestione delle identità, nel cloud e negli endpoint per aumentare le probabilità di rilevamento precoce.

Indagine e risposta

- Gli attacchi ransomware hanno una progressione rapida che non si limita a particolari orari del giorno o della notte. È pertanto cruciale provvedere al monitoraggio costante degli avvisi critici 24x7 potenziando i team di sicurezza interni, adottando soluzioni gestite per il rilevamento e la gestione degli incidenti (MDR) oppure rivolgendosi a provider di servizi di sicurezza gestiti (MSSP).
- L'integrazione dei dati telemetrici provenienti dalla rete, dagli endpoint e dai registri cloud consente di indagare le minacce in modo più chiaro, contestuale e approfondito e di risalire alla causa primaria scatenante.
- Cercare indizi di un'impennata delle attività di scansione della rete perimetrale precedenti al primo accesso, in combinazione con la Open Source INTelligence (OSINT), può consentire di valutare precocemente il probabile responsabile e di reagire con maggiore chiarezza.

Per maggiori informazioni, contatta info@vectra.ai.

E-mail: info@vectra.ai vectra.ai