Akamai

WHITE PAPER

Spezzare la kill chain del ransomware con la suite di soluzioni per la sicurezza aziendale Akamai

Sommario

Introduzione

Sconfiggere il ransomware nei vari passaggi della kill chain utilizzando le soluzioni per la sicurezza aziendale Akamai

Una delle maggiori minacce alla sicurezza che le organizzazioni devono affrontare oggi è il ransomware, una forma di malware progettata per crittografare file importanti su un dispositivo, rendendoli inutilizzabili. Gli operatori di malware richiedono quindi un riscatto in cambio di una chiave di decodifica o di un software in grado di ripristinare i dati originali dei file. Negli ultimi anni, i gruppi criminali di ransomware hanno perfezionato le proprie tattiche e hanno iniziato a esfiltrare i dati delle loro vittime per sfruttarli ulteriormente minacciando di divulgarli pubblicamente o di venderli sul dark web.

Per essere in grado di difendersi da questo tipo di attacco, è importante comprendere il modo in cui operano i gruppi di ransomware per raggiungere i propri obiettivi. Questo documento vi aiuterà esattamente in questo.

Descrizione della kill chain del ransomware

Gli attacchi ransomware sono complessi: la violazione del sistema è solo l'inizio. Per massimizzare il danno, un criminale deve anche diffondere il proprio carico dannoso sull'intera rete prima di iniziare la crittografia. La crittografia di un singolo computer non è sufficiente al criminale per richiedere un riscatto. Affinché l'attacco ransomware abbia successo, il criminale deve eseguire vari passaggi: rilevare le risorse di rete, spostarsi lateralmente, ecc. Questi passaggi vengono spesso denominati la "kill chain del ransomware".

Ogni passaggio di questa catena fornisce molte opportunità di rilevamento e mitigazione. Preparare in anticipo la rete con la suite di soluzioni per la sicurezza aziendale Akamai può ridurre la superficie di attacco e contribuire a mitigare e contenere eventuali danni derivanti dal ransomware prima ancora di accorgervi di essere stati colpiti. Questo documento descrive in dettaglio come utilizzare Akamai Guardicore Segmentation, Enterprise Application Access e Secure Internet Access per rilevare e bloccare l'attività ransomware nei diversi passaggi della kill chain:

Accesso iniziale

La prima fase dell'attacco, in cui i criminali violano la rete interna dall'esterno

Rilevamento

Metodi utilizzati dai criminali per identificare risorse importanti all'interno della rete

Movimento laterale

La fase in cui i criminali penetrano nella rete e compromettono risorse aggiuntive

Command and Control

I diversi modi in cui i criminali mantengono un canale di comunicazione nella rete per inviare informazioni e comandi alle risorse compromesse

Esfiltrazione

Metodi utilizzati dai criminali per esfiltrare dati sensibili rubati in modo occulto

Accesso iniziale

Ogni organizzazione si interfaccia in numerosi modi con Internet. I criminali cercheranno di sfruttare ciascuno di essi per ottenere l'accesso alla rete. Akamai vi consente di proteggere in modo ottimale tali interfacciamenti e di tenere i criminali lontani dalla vostra rete.

Protezione dei server connessi a Internet

> Utilizzate le funzionalità di analisi del payload di Secure Internet Access per proteggere i server collegati a Internet dallo sfruttamento

Secondo Kaspersky, il metodo più comune utilizzato dai criminali per ottenere l'accesso iniziale è lo sfruttamento delle applicazioni connesse a Internet, spesso abusando delle vulnerabilità one-day su sistemi privi di patch. Vulnerabilità come Log4Shell (CVE2021-44228) e ProxyLogon (CVE-2021-26855) vengono ancora oggi sfruttate per violare le reti e distribuire ransomware.

Enterprise Threat Protector può essere configurato per monitorare tutto il traffico web in entrata sui server connessi a Internet; tale traffico viene quindi analizzato e qualsiasi attività dannosa o anomala può essere identificata e bloccata.

Blocco degli URL di phishing

> Utilizzate le funzionalità di ispezione degli URL di Enterprise Threat Protector per rilevare e bloccare i tentativi di phishing

Il phishing è un modo molto comune per violare le reti. I criminali inviano spesso e-mail contenenti link ad allegati dannosi o a pagine di accesso false progettate per rubare credenziali. L'utilizzo del client Enterprise Threat Protector sui vostri endpoint vi consentirà di scansionare in tempo reale tutti gli URL su cui fanno clic i vostri utenti, identificando eventuali collegamenti dannosi o anomali e bloccandoli.

Riduzione della superficie di attacco della VPN

> Utilizzate Enterprise Application Access per consentire un accesso alla VPN sicuro e specifico per l'applicazione e ridurre la superficie di attacco esterna

Nell'odierno ambiente di lavoro ibrido, che spesso include il lavoro da remoto, sta diventando sempre più comune consentire agli utenti di utilizzare una VPN per accedere alla rete aziendale. I criminali si sono adattati e hanno iniziato a sfruttare questa opportunità per accedere alla rete interna. Sempre più spesso si osservano i criminali sferrare attacchi ai personal computer dei dipendenti, compromettendo le loro credenziali della VPN per poi utilizzarle per accedere alla rete interna. In alcuni casi, i criminali prendono di mira anche i server vulnerabili per divulgare le credenziali. Nel novembre 2022, i criminali hanno sfruttato una vulnerabilità nei server VPN Fortinet per ottenere l'accesso iniziale e hanno poi diffuso il ransomware in tutta la rete.

Enterprise Application Access vi consente di ridurre significativamente questo rischio consentendo un accesso alla rete basato sui ruoli e specifico per l'applicazione: non concede agli utenti l'accesso completo all'intera rete come le VPN tradizionali, ma consente solo un accesso limitato ad applicazioni specifiche. In questo modo, anche se un criminale dovesse compromettere le credenziali di un utente ed eludere la protezione MFA, non riuscirà comunque ad accedere alla rete, ma solo a un insieme limitato di applicazioni.

Command and Control

Blocco dei server C2 (Command and Control)

> Utilizzate Akamai Secure Internet Access per bloccare i server C2 di malware noti

Il malware in generale e il ransomware in particolare richiedono la comunicazione con server C2 esterni per inviare comandi e recuperare informazioni dalle risorse infette. Analizzando l'elevato volume di dati di comunicazione di Akamai, siamo in grado di monitorare i domini C2 di ransomware e malware e di tenere traccia delle campagne nuove e in evoluzione. Il client Enterprise Threat Protector ci consente di monitorare l'intera comunicazione DNS in tempo reale e bloccare la comunicazione verso domini dannosi, impedendo al malware di funzionare correttamente e di raggiungere i propri obiettivi.

Rilevamento

Una volta violata la rete, i criminali cercheranno di identificare risorse aggiuntive per comprendere la struttura della rete prima di iniziare a spostarsi lateralmente. Spesso ciò genererà una comunicazione interna, che può essere rilevata da Akamai Guardicore Segmentation.

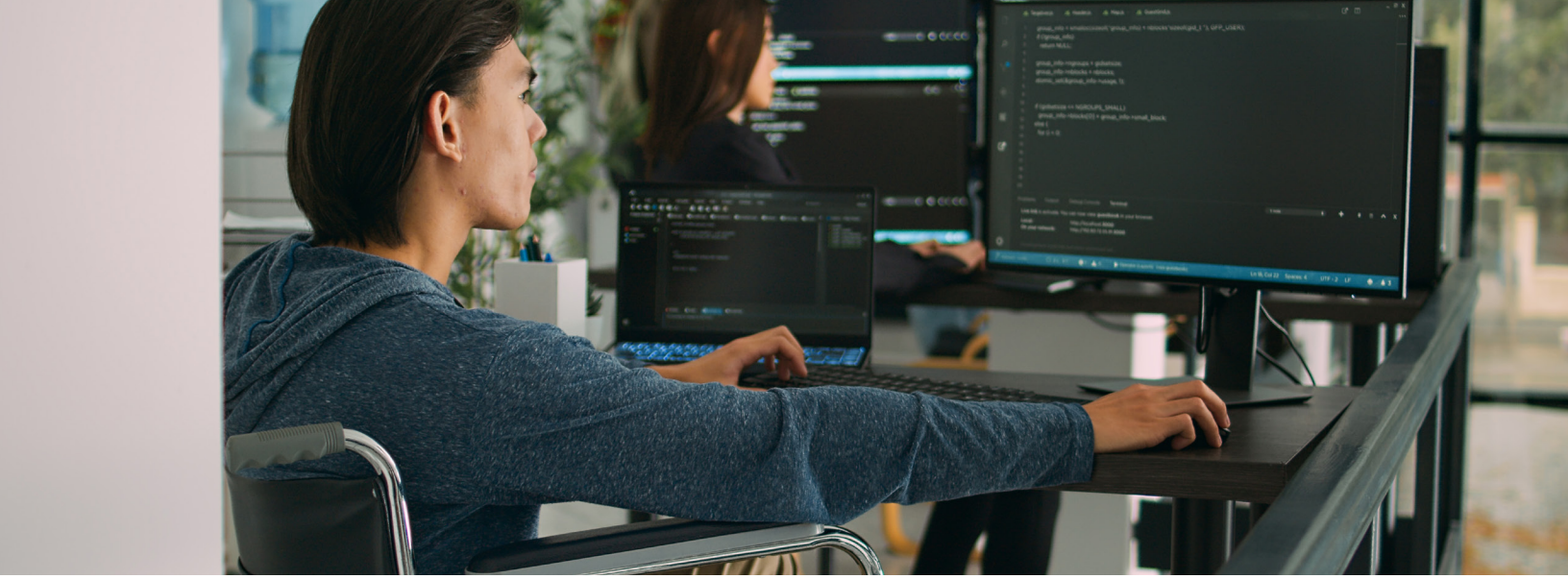
Identificazione delle scansioni di rete

> Utilizzate i rilevatori di Akamai Guardicore Segmentation per identificare le scansioni di rete sospette

Uno dei metodi più comuni utilizzati dai criminali per individuare le reti è l'utilizzo della scansione delle porte per identificare i servizi di rete: molti gruppi di ransomware vengono rilevati utilizzando scanner di rete open source. In un recente rapporto CISA relativo al ransomware LockBit 3.0, è stato dimostrato che il gruppo utilizza "SoftPerfect Network Scanner" per eseguire la scansione delle porte. Un altro esempio è il gruppo di ransomware Nokoyawa che è stato individuato mentre scansionava le reti alla ricerca di server SQL per accedere ai dati sensibili al loro interno.

Akamai Guardicore Segmentation monitora tutte le comunicazioni nella rete e dispone di rilevatori integrati che identificano e segnalano tali scansioni, consentendovi di fermare la diffusione del malware prima che inizi.

Figura 1. Incidenti di scansione di rete in Akamai Guardicore Segmentation



Identificazione per evitare il rilevamento

Utilizzate Akamai Guardicore Segmentation per identificare i tentativi di rilevamento

Quando i criminali violano una rete, non hanno una conoscenza preliminare della sua struttura e delle diverse risorse in essa contenute. Per superare questo ostacolo, dovranno "muoversi nel buio" e cercare di orientarsi manualmente. Akamai Guardicore Segmentation vi consente di sfruttare questa situazione utilizzando il servizio di identificazione, che attira i criminali nei server honeypot, monitora le loro attività e vi avvisa quando vengono rilevate anomalie.

Ad esempio, un criminale viola la rete e utilizza un attacco di forza bruta per sottrarre le credenziali SSH di un server Linux. Akamai Guardicore Segmentation identificherà questa anomalia e inoltrerà il criminale a un honeypot generato dinamicamente. Una volta all'interno dell'honeypot, tutte le azioni del criminale vengono registrate e viene generato un avviso.

Di seguito è riportato l'esempio di uno di questi avvisi:

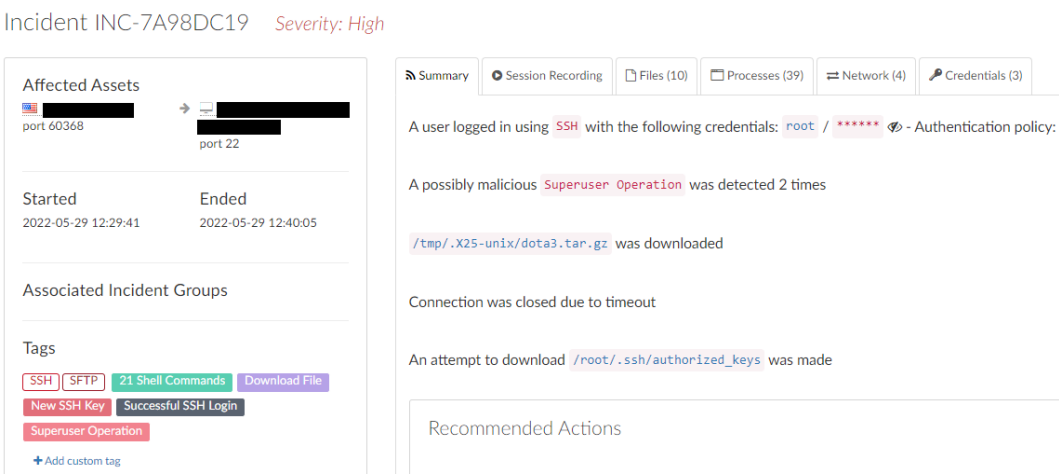


Figura 2. Incidente di identificazione in Akamai Guardicore Segmentation

Movimento laterale

Una volta ottenuto l'accesso alla rete e acquisita familiarità con la sua topologia, il criminale cerca di utilizzarla per spostarsi lateralmente. I moderni gruppi di ransomware violano una rete e poi si spostano lateralmente per compromettere quante più risorse possibile, crittografandole tutte. I prodotti per la sicurezza aziendale di Akamai consentono di limitare le possibilità di movimento laterale e di ridurre al minimo la portata della violazione.

Identificazione degli indicatori host sospetti

> Utilizzate il modulo Insight di Akamai Guardicore Segmentation per identificare gli indicatori host sospetti in vari modi

I criminali utilizzano gli strumenti PowerShell per raggiungere una serie di obiettivi: uno di questi è eseguire movimenti laterali. I dropper PowerShell sono molto comuni e i criminali spesso li utilizzano come primo pezzo di codice che eseguono su una risorsa compromessa. È stato dimostrato che le recenti infezioni del ransomware Quantum fanno esattamente questo: eseguono il codice PowerShell tramite Strumentazione gestione Windows (WMI).

Utilizzando il modulo Insight di Akamai Guardicore Segmentation, potete eseguire query pianificate per scansionare il registro eventi di PowerShell su tutte le vostre risorse, etichettando le risorse con indicatori dannosi e mettendole in quarantena.

Figura 3. Creazione di una query Insight pianificata per rilevare PowerShell dannoso

Ma PowerShell è solo un esempio. È possibile sfruttare Insight per scansionare un'ampia varietà di indicatori di movimento laterale, utilizzando una qualsiasi delle tabelle osquery esistenti, ad esempio:

- Utilizzate la tabella File per rilevare file malware in base a nomi o hash
- Utilizzate la tabella Elementi di avvio per rilevare voci di esecuzione automatica sospette sulle vostre risorse
- Utilizzate la tabella Yara per scansionare i file sulle vostre risorse utilizzando le regole Yara per rilevare i ceppi di malware

Blocco degli attacchi alle LAN

> Utilizzate Akamai Guardicore Segmentation per bloccare e rilevare attacchi ai protocolli di rete locale

Dopo aver violato il paziente zero nella rete, i criminali sfruttano le vulnerabilità dei protocolli LAN come ARP per compromettere altre risorse. Con l'uso di un firewall tradizionale, questi attacchi possono facilmente passare inosservati, poiché vengono eseguiti nel livello 2 e questo tipo di comunicazione non raggiunge il firewall.

L'approccio basato su software di Akamai Guardicore Segmentation consente di monitorare e bloccare tutto il traffico in entrata o in uscita da una risorsa, anche il traffico locale che normalmente non raggiungerebbe il firewall di controllo.

Limitazione delle porte di gestione

> Utilizzate Akamai Guardicore Segmentation per creare policy a livello di processo per ridurre la superficie di attacco sulle porte sensibili

Una volta all'interno della rete, i criminali solitamente eseguono un'escalation dei privilegi sulle risorse compromesse con lo scopo di rubare le credenziali. Dopo aver ottenuto le credenziali, i criminali utilizzano spesso protocolli di gestione come RDP, RPC, SMB e WinRM per eseguire un payload ransomware su tutte le risorse nella rete. Tuttavia, bloccare completamente queste porte spesso non è un'opzione praticabile poiché gli amministratori le richiedono per effettuare le normali attività.

Akamai Guardicore Segmentation consente di applicare policy a livello di processo, permettendovi di determinare quali processi devono comunicare tramite porte di gestione sensibili. Esaminiamo WinRM: è utilizzato da molti programmi di amministrazione, incluso Ansible. Tuttavia, viene spesso sfruttato anche dai criminali che utilizzano strumenti come Evil-WinRM per eseguire movimenti laterali. Utilizzando Akamai Guardicore Segmentation, possiamo creare una policy per consentire le connessioni WinRM in entrata solo dai processi Ansible, bloccando altri processi sulla stessa porta:

Section	Source	Destination	Ports/Protocols	Action
Allow	ansible-operator	Windows Any	5985 TCP | UDP	Allow
Block	Any	Windows Any	5985 TCP | UDP	Block

Figura 4. Esempio di policy di Akamai Guardicore Segmentation per limitare la comunicazione WinRM

Esfiltrazione

Negli ultimi anni, i criminali hanno adattato le loro tattiche di estorsione e hanno iniziato a divulgare file sensibili delle proprie vittime da utilizzare come ulteriore leva. I criminali cercheranno di eludere il rilevamento nella rete mentre esfiltrano i dati dell'organizzazione, ma spesso è ancora possibile rilevarli e bloccarli durante questa fase.

Blocco dei domini di esfiltrazione

> Utilizzate Akamai Guardicore Segmentation per limitare l'accesso ai servizi che potrebbero venire sfruttati per l'esfiltrazione dei dati

I criminali utilizzano spesso strumenti pubblici per estrarre dati dalla rete, un'opzione molto comune sono i servizi di hosting pubblici come MEGA, Dropbox e Google Drive. La difficoltà nel monitorare questi domini è che vengono comunemente utilizzati in modo legittimo all'interno della rete. Ad esempio, l'accesso al dominio MEGA tramite un browser potrebbe essere considerato legittimo, ma farlo utilizzando l'utilità rclone, utilizzata attivamente da diversi gruppi di attacco per esfiltrare dati, sarebbe considerato dannoso.

Utilizzando Akamai Guardicore Segmentation, possiamo ridurre al minimo il rischio derivante da tali strumenti bloccandone i domini da tutti gli endpoint che non richiedono l'accesso e consentendo l'accesso solo tramite applicazioni approvate come i browser.

Difesa multilivello

Per raggiungere l'obiettivo più desiderato, i criminali devono superare diverse fasi di attacco. Ogni passaggio offre agli addetti alla sicurezza la possibilità di bloccare e rilevare l'attività dannosa ad esso associata. Utilizzando i diversi prodotti per la sicurezza di Akamai, gli addetti alla sicurezza possono adottare misure di mitigazione in ogni passaggio della kill chain del ransomware, bloccando immediatamente i criminali e rilevando qualsiasi comportamento anomalo.

Per ulteriori informazioni su Akamai Guardicore Segmentation o per richiedere una demo del prodotto personalizzata, visitate il sito akamai.com/guardicore

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 09/23.