Come si sviluppano i ransomware
con e senza l'Autonomous Response

Indice

Introduzione

In un'era caratterizzata da attacchi in rapido movimento e in continua evoluzione, con tempi di fermo sempre più ridotti e team della sicurezza sempre più sotto pressione, il solo rilevamento non è più sufficiente e la tecnologia con la quale rispondere agli attacchi emergenti è diventata necessaria al fine di evitare le interruzioni informatiche

Darktrace Antigena utilizza una comprensione del "sé" in continua evoluzione per qualsiasi utente e dispositivo aziendale per prendere decisioni istantanee e mettere in pratica azioni mirate, interrompendo gli attacchi in corso senza alcuna conseguenza per la normale operatività aziendale.

Qui di seguito analizzeremo come si sviluppano i ransomware **con e senza l'Autonomous Response.**

Nel primo di quattro scenari, Darktrace era installato in versione di prova, quindi Darktrace Antigena non era impostato in Active Mode, configurazione in cui può agire autonomamente. In questi casi, l'attacco può continuare oppure viene interrotto a causa di un tempestivo intervento umano. Gli ultimi due scenari spiegano cosa accade quando Antigena è configurato per rispondere autonomamente ad un attacco emergente.

Senza l'Autonomous Response

I primi segnali di un ransomware: un attacco improvviso

Presso un fornitore della difesa canadese un pirata informatico era riuscito ad accedere a un server ottenendo le credenziali di un amministratore, diffondendosi poi lateralmente utilizzando comandi WMI. Tuttavia, la catena di eventi insolita e sospetta è stata immediatamente rilevata dall'AI di Darktrace e, con l'Autonomous Response in Active Mode avrebbe immediatamente interrotto l'attacco.

In questo caso, l'attacco è andato avanti e l'AI di Darktrace ha rilevato tutte e 5 le fasi dell'attacco che si sono verificate nelle successive 48 ore, incluse attività C2 e ulteriori movimenti laterali. Quando il pirata informatico ha distribuito un ransomware, i pochi dispositivi in cui Darktrace Antigena era attivo sono stati isolati dall'attacco, mentre i dispositivi non protetti hanno subito la crittografia. Con l'installazione completa dell'Autonomous Response questo attacco sarebbe terminato già all'accesso iniziale.

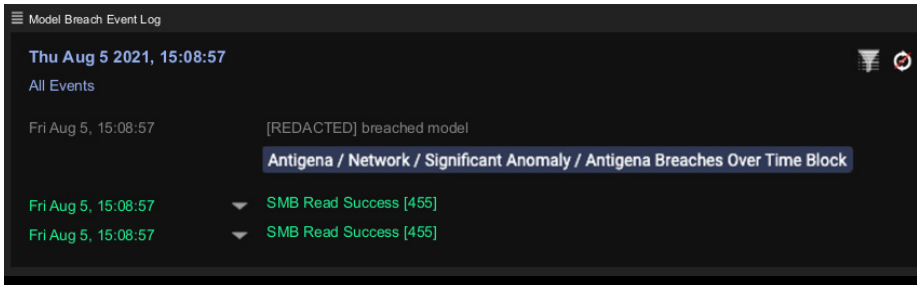


Figura 1: un modello Antigena si attiva quando vengono rilevate più anomalie nel corso del tempo

> “I ransomware che dobbiamo affrontare oggi si muovono troppo velocemente e l'uomo da solo non è in grado di contenerli: l'unico modo per rimanere in vantaggio è avere l'AI di Darktrace, che combatte in modo preciso e proporzionato al nostro posto.”
>
> Leon Shepherd, CIO, Ted Baker

Come l'AI ha bloccato un'intrusione WastedLocker

At an agricultural organization in the US, Darktrace detected a WastedLocker ransomware attack after an employee was deceived into downloading a fake browser update. We can see how Antigena would have instantly blocked the C2 traffic on this and various other channels as they emerged.

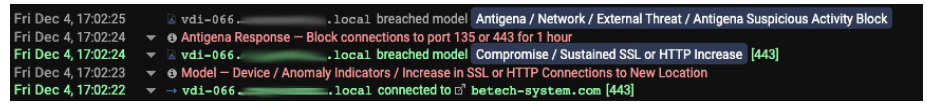


Figura 2: modelli di violazione e azioni che Antigena avrebbe messo in pratica per risolverli

Non appena il pirata informatico ha cambiato tattica e ha tentato ulteriori beaconing, Antigena ha eseguito l'escalation della propria risposta. In nessun momento ha suggerito un'interferenza con un'attività non correlata all'attacco.

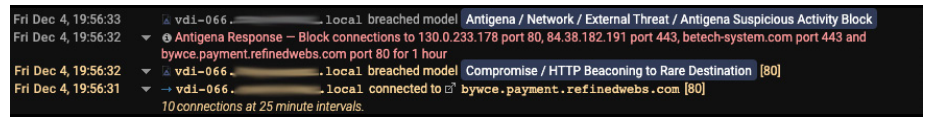


Figura 3: escalation della potenziale risposta di Antigena

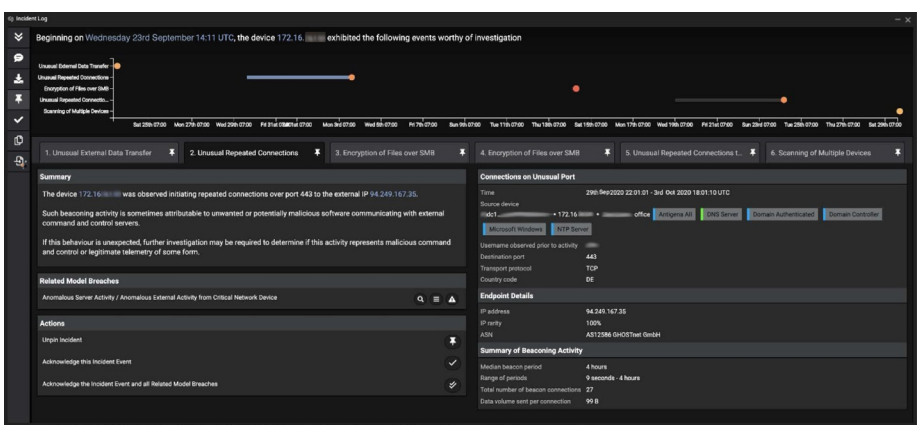
Per fortuna, il team della sicurezza ha reagito in tempo agli allarmi segnalati da Darktrace e, grazie al conciso e utile riepilogo sull'incidente generato automaticamente da Cyber AI Analyst, ha potuto bloccare l'attacco prima che causasse gravi problemi.

I tempi di reazione rapidi sono stati fondamentali nell'evitare un incidente di sicurezza estremamente costoso e dannoso. Fare affidamento sulla sola risposta umana è un gioco pericoloso: se il team non fosse stato particolarmente in allerta e senza i rilevamenti estremamente precisi di Darktrace, l'attacco avrebbe proseguito fino alla fase di crittografia.

Cyber AI Analyst indaga il ransomware Sodinokibi (REvil)

Dopo che le credenziali di un membro del team IT di un'organizzazione retail erano state utilizzate per la compromissione di controller di dominio, l'AI di Darktrace ha rilevato la scrittura di file sospetti e l'eliminazione di script batch e file di log dalla directory principale da parte del pirata informatico. Il controller di dominio aveva poi effettuato connessioni verso numerosi endpoint esterni rari e Darktrace ha rilevato un upload di 28 MB, probabilmente l'esfiltrazione dei dati di ricognizione iniziale.

Nel corso di due settimane, Darktrace ha rilevato l'attivazione di una scansione di rete da parte di un server SQL, connessioni RDP interne insolite utilizzando credenziali di amministratore e caricamenti di dati verso numerosi endpoint di archiviazione Cloud. PsExec era stato utilizzato per installare il ransomware, che ha comportato la crittografia di file.



Beginning on Wednesday 23rd September 14:11 UTC, the device 172.16.[redacted] exhibited the following events worthy of investigation

Summary

The device 172.16[redacted] was observed initiating repeated connections over port 443 to the external IP 94.249.167.35.

Such beaconing activity is sometimes attributable to unwanted or potentially malicious software communicating with external command and control servers.

If this behaviour is unexpected, further investigation may be required to determine if this activity represents malicious command and control or legitimate telemetry of some form.

Related Model Breaches

Anomalous Server Activity / Anomalous External Activity from Critical Network Device

Actions

Unpin Incident

Acknowledge this Incident Event

Acknowledge the Incident Event and all Related Model Breaches

Connections on Unusual Port

Time	29th Sep 2020 22:01:01 - 3rd Oct 2020 18:01:10 UTC
Source device	[redacted]dc1.[redacted] • 172.16[redacted] • [redacted] office Antigena All DNS Server Domain Authenticated Domain Controller Microsoft Windows NTP Server
Username observed prior to activity	[redacted]
Destination port	443
Transport protocol	TCP
Country code	DE

Endpoint Details

IP address	94.249.167.35
IP rarity	100%
ASN	AS12586 GHOSTnet GmbH

Summary of Beaconing Activity

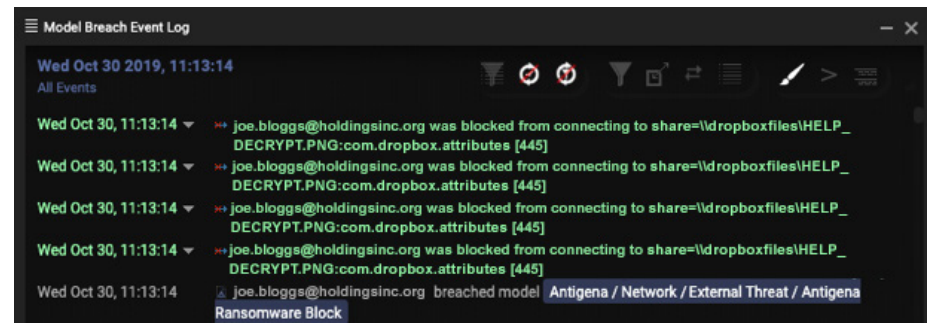
Median beacon period	4 hours
Range of periods	9 seconds - 4 hours
Total number of beacon connections	27
Data volume sent per connection	99 B

Figura 4: Cyber AI Analyst effettua un'indagine

Nonostante i risultati significativi presentati da Cyber AI Analyst in 15 report di incidente, Darktrace era in modalità di prova e nessuno stava monitorando le attività di questa tecnologia. In mancanza dell'Autonomous Response, l'attacco ransomware Sodinokibi ha potuto completarsi, mentre invece Antigena lo avrebbe bloccato fin dalle prime fasi.

Ransomware "a doppia estorsione"

La velocità alla quale un ransomware è in grado di diffondersi è stata evidenziata in questo incidente che si è verificato presso un'azienda energetica canadese, in cui la crittografia è iniziata appena 12 ore dopo la ricognizione iniziale. Darktrace ha rilevato e segnalato ogni fase dell'attacco, inclusi scansione della rete, movimenti RDP e connessioni TeamViewer pericolose. Queste attività, insieme al successivo download di 1,95 TB di dati e alla crittografia iniziale, sono avvenute principalmente fuori dagli orari di lavoro, ma Darktrace la ha identificate come evidenze di un attacco. Con l'Autonomous Response attiva, questo attacco sarebbe stato bloccato già nelle fasi di ricognizione iniziale e movimento laterale.



```
Wed Oct 30 2019, 11:13:14
All Events
Wed Oct 30, 11:13:14   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Wed Oct 30, 11:13:14   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Wed Oct 30, 11:13:14   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Wed Oct 30, 11:13:14   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Wed Oct 30, 11:13:14   joe.bloggs@holdingsinc.org  breached model  Antigena / Network / External Threat / Antigena
                       Ransomware Block
```

Figura 5: Antigena blocca i movimenti laterali e le attività "ransom" del dispositivo infetto

> “L'Autonomous Response combatte gli attacchi ransomware più sofisticati e lo fa pochissimi secondi dopo aver individuato una minaccia emergente.”
>
> Abhay Raman, CSO, Sun Life

Con l'Autonomous Response

Minimizzare l'impatto di REvil distribuito tramite i server Kaseya

Mentre gli Stati Uniti si preparavano per i festeggiamenti del week-end del 4 luglio, il gruppo ransomware REvil ha sfruttato la vulnerabilità del software Kaseya per attaccare più di 1.500 aziende.

Un'azienda in cui era installata l'Autonomous Response è stata protetta da questo attacco quando l'AI di Darktrace ha rilevato traffico SMB insolito e ha quindi applicato il normale "pattern of life" del laptop, evitando che eseguisse connessioni insolite.

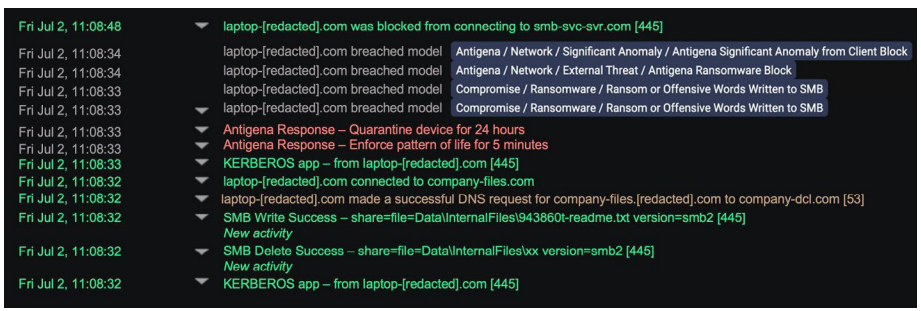


Figura 6: Darktrace rileva un tentativo di crittografia da parte di un dispositivo infetto ed entra in azione

Successivi tentativi da parte del dispositivo infetto di connettersi ad altri dispositivi sono stati bloccati, prevendo così la diffusione dell'attacco. È stato possibile evitare la crittografia dei file di rete solo perché queste azioni sono state eseguite immediatamente e alla stessa velocità dell'attacco, grazie all'Autonomous Response.

Darktrace Antigena risponde ai ransomware entro 1 secondo.

Antigena neutralizza ransomware zero-day

In questo esempio, l'AI di Darktrace ha rilevato un picco nel pattern di connessioni regolari eseguite da un dispositivo, nonché attività SMB sospette e insolite ricerche DNS al contrario, una tattica spesso utilizzata nella fase di ricognizione.

Ulteriori indagini effettuate sull'attività SMB hanno rilevato che una condivisione SMB aveva acceduto a centinaia di file correlati a Dropbox a cui il dispositivo non aveva mai acceduto in precedenza. Inoltre, molti di questi file avevano iniziato a essere crittografati, aggiungendo l'estensione [HELP_DECRYPT].

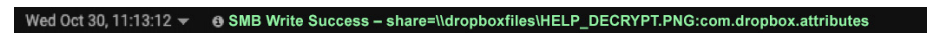


Figura 7: Darktrace rileva attività SMB correlate a file Dropbox

Per fortuna, Antigena era in Active Mode ed è entrato in azione in pochissimi secondi, forzando il normale "pattern of life" e bloccando le connessioni anomale per cinque minuti, bloccando immediatamente la crittografia. Nel frattempo è entrata in azione l'AI di Darktrace e solo quattro file sono stati crittografati con successo.

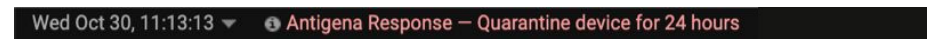


Figura 8: Darktrace Antigena risponde 1 secondo dopo aver rilevato il ransomware

Antigena quindi ha eseguito una seconda azione per bloccare il ransomware ed evitare che si diffondesse ad altri dispositivi. La combinazione di varie attività anomale è stata una prova sufficiente per consentire all'Autonomous Response di neutralizzare la minaccia: il paziente zero è stato messo in quarantena per 24 ore, impedendo connessioni verso il server o qualsiasi altro dispositivo di rete. Antigena pertanto non ha solo bloccato immediatamente l'attività di crittografia, ma anche evitato che i pirati informatici si muovessero lateralmente all'interno della rete tramite scansione, utilizzo di credenziali di

Conclusione

Poiché i ransomware stanno diventando sempre più veloci e i pirati informatici continuano a sperimentare nuove tecniche, l'Autonomous Response è diventata un componente essenziale dello stack di sicurezza. La conoscenza personalizzata sul panorama digitale di un'azienda le consente di rispondere agli attacchi emergenti con precisione chirurgica, contenendo la minaccia senza interrompere le attività aziendali.

Gli esempi descritti in precedenza evidenziano che anche utilizzando i meccanismi di rilevamento più all'avanguardia, senza un meccanismo di risposta proporzionata e alla velocità delle macchine, i ransomware possono ancora causare interruzioni informatiche significative e costose.

L'Autonomous Response protegge i dati critici, ovunque risiedano, in infrastrutture e applicazioni Cloud, e-mail, reti aziendali o dispositivi endpoint.

Informazioni su Darktrace

Darktrace (DARK:L) è il leader globale nella cyber security basata sull'AI e fornisce una tecnologia di prim'ordine che protegge più di 6.500 clienti in tutto il mondo da minacce evolute, inclusi ransomware e attacchi a Cloud e SaaS. L'approccio sostanzialmente differente adottato da Darktrace utilizza la Self-Learning AI per consentire alle macchine di comprendere le attività aziendali al fine di difenderle in modo autonomo. L'azienda, che ha sede a Cambridge, Regno Unito, ha 1.700 dipendenti e più di 30 uffici in tutto il mondo. Darktrace è stata nominata dalla rivista TIME tra le "Most Influential Companies" nel 2021.

Per maggiori informazioni

Visita il sito darktrace.com
info@darktrace.com
Seguici su Twitter