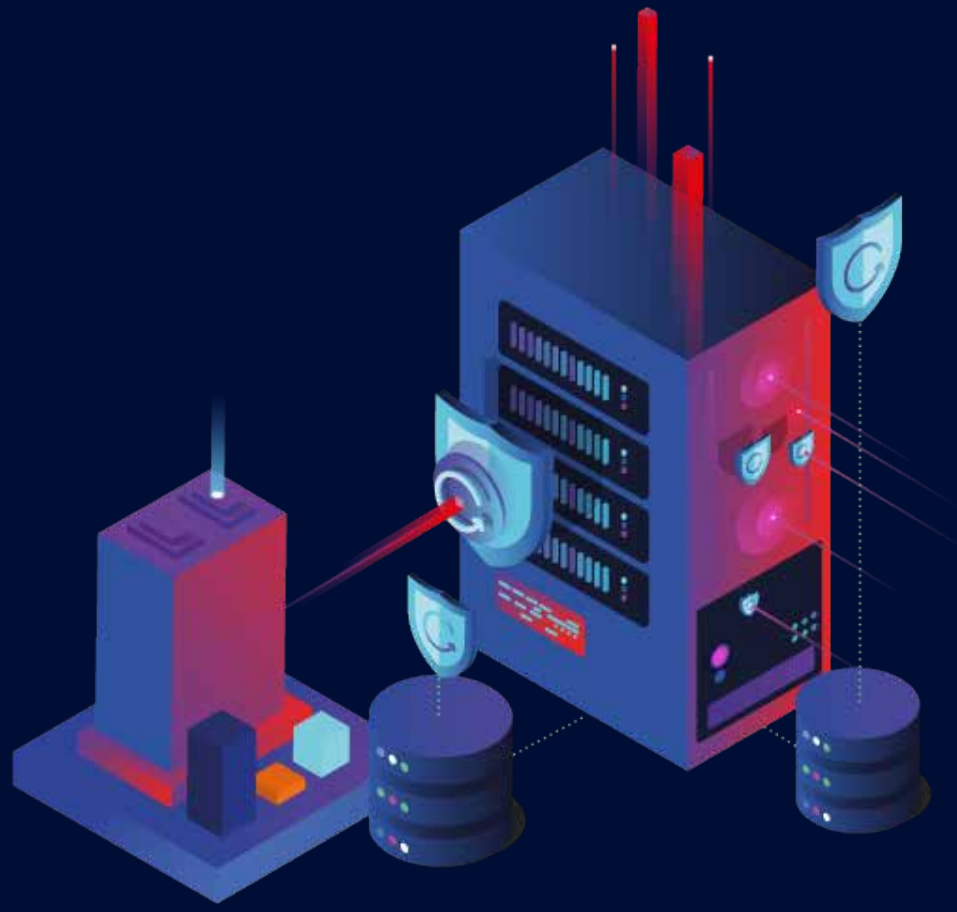
watchguard.it

Comprendere gli attacchi informatici

panda
a WatchGuard brand

Indice:



1.Introduzione

La dinamica realtà dello scenario delle minacce e la frequenza, la sofisticatezza e la natura mirata degli attacchi sferrati dagli avversari richiede un'evoluzione delle prassi operative di sicurezza con misure combinate di prevenzione, rilevamento e risposta contro gli attacchi informatici.

La maggior parte delle organizzazioni dispone di mezzi per rilevare gli attacchi noti, sebbene alcuni possano ancora passare inosservati. In passato la principale difficoltà consisteva nel bloccare gli attacchi sconosciuti, che sono concepiti appositamente per aggirare le protezioni più recenti modificando le firme e i modelli di comportamento.

Molte organizzazioni hanno fatto importanti investimenti per creare un proprio team di ricerca delle minacce e/o per delegare ai fornitori di servizi gestiti il compito inevitabile e cruciale di modificare continuamente le loro tecniche difensive e cercare strumenti e modi migliori per mantenere al sicuro la loro proprietà intellettuale e le loro risorse digitali.

Comprendere il modo di agire di questi avversari e la mappa della strategia di difesa delle organizzazioni rispetto al ciclo di vita degli attacchi mostra loro come rilevare, fermare, interrompere ed effettuare il ripristino da un attacco e in quali ambiti occorre rafforzare le operazioni di sicurezza.

Questo report aiuta i team di sicurezza a comprendere il noto modello del ciclo di vita degli attacchi informatici, definito Cyber Kill Chain (CKC), la sua estensione all'intera rete e in che modo Panda Adaptive Defense Service copre l'intero ciclo di vita a livello di endpoint.

La Cyber Kill Chain è uno strumento eccellente per capire in che modo le organizzazioni possono aumentare notevolmente la possibilità di difendere il loro ambiente rilevando e bloccando le minacce in ogni fase del ciclo di vita dell'attacco. La kill chain ci insegna che, mentre gli avversari devono completare tutte le fasi affinché l'attacco vada a buon fine, noi dobbiamo "solo" fermare e spezzare la catena in qualsiasi fase del processo.

Occorre tenere presente che le risorse più preziose di un'organizzazione sono archiviate negli endpoint e nei server, che tutti gli aggressori vorranno raggiungere per accedere a tali risorse critiche. Fermare gli avversari all'endpoint riduce drasticamente le probabilità di successo di qualsiasi autore di attacchi informatici, semplificando gli sforzi per spezzare la catena e aumentando notevolmente l'efficienza e l'efficacia delle apparecchiature di sicurezza.

Poiché tutti gli aggressori colpiscono gli endpoint per accedere alle risorse critiche dell'organizzazione, bloccare gli avversari a livello di endpoint riduce automaticamente la probabilità di successo di qualsiasi autore di attacchi informatici, semplificando al contempo gli sforzi per spezzare la catena e aumentando notevolmente l'efficienza e l'efficacia delle operazioni di sicurezza.

2.Comprendere la Cyber Kill Chain

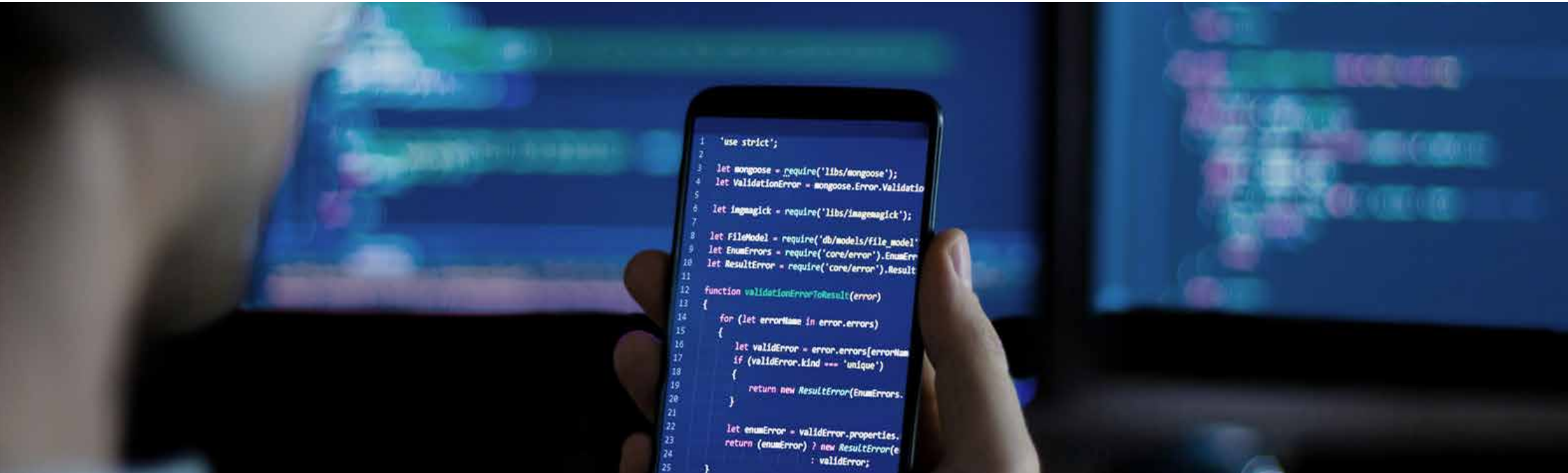
Il framework Cyber Kill Chain è stato inizialmente pubblicato da Lockheed Martin come parte del modello Intelligence Driven Defense[1] per l'identificazione e la prevenzione delle attività di intrusione informatica.

Il modello identifica ciò che gli avversari devono completare per raggiungere il loro obiettivo, cioè prendere di mira la rete, portare in salvo i dati (esfiltrazione) e far sì che l'organizzazione continui a esistere. Grazie a questo modello abbiamo imparato che se si bloccano gli avversari in qualsiasi fase, è possibile spezzare la catena di attacco; gli avversari, infatti, devono completare tutte le fasi affinché il loro attacco abbia successo. Noi, invece, che siamo i difensori, per avere successo dobbiamo solo bloccarli in qualsiasi fase.

Vedremo nella prossima sezione che l'endpoint è un punto inevitabile da cui passano tutti gli attacchi e quindi fermarli a questo livello aumenta enormemente la possibilità di bloccare qualsiasi attacco informatico. Il tasso di successo sarà maggiore se il blocco avviene nelle prime fasi della catena.

Inoltre, ogni intrusione, e le tracce che lascia nell'endpoint, rappresenta un'occasione per capire meglio i nostri avversari e usare la loro persistenza a nostro vantaggio. Una migliore comprensione degli avversari e delle loro tracce consente una progettazione più efficace delle difese.

La Cyber Kill Chain afferma che, per compiere i loro misfatti, gli avversari devono sempre seguire sei passaggi fondamentali.



Cyber Kill Chain esterna

Ricognizione esterna

Questa fase può essere definita come quella di selezione dei bersagli, identificazione dei dettagli dell'organizzazione, requisiti legislativi dei verticali di settore, informazioni sulle scelte tecnologiche, attività di social network e mailing list.

L'avversario cerca essenzialmente di rispondere a queste domande: "Quali metodi di attacco funzioneranno offrendo il massimo livello di successo?" e "Quali sono quelli più facili da eseguire in termini di investimento di risorse?"

Weaponization e pacchetti

Questa fase assume molte forme: sfruttamento di applicazioni web, malware pronto all'uso o personalizzato (scaricato per il riutilizzo o acquistato), vulnerabilità di documenti composti (forniti in PDF, Office o altri formati di documenti) o attacchi di tipo "watering hole".[2]

Viene generalmente preparata con un'intelligenza opportunistica o molto specifica su un bersaglio.

Distribuzione

La trasmissione del payload viene avviata dal bersaglio (ad esempio, un utente accede a un sito web dannoso, attivando un exploit che distribuisce malware, oppure apre un file PDF dannoso) o dall'aggressore (iniezione SQL o compromissione del servizio di rete).

Sfruttamento

Dopo la distribuzione all'utente, al computer o al dispositivo, il payload dannoso compromette la risorsa, aprendosi un varco nell'ambiente.

Ciò avviene di solito sfruttando una vulnerabilità nota per la quale è stata precedentemente resa disponibile una patch. Anche se si verifica lo sfruttamento zero-day, a seconda della vittima, nella maggior parte dei casi non è necessario che gli avversari si sobbarchino questa spesa.

Cyber Kill Chain esterna II

Installazione

Quest'attività comporta spesso un'interazione attiva con parti esterne. Il malware è solitamente furtivo nel suo funzionamento e ottiene persistenza negli endpoint a cui ha accesso. L'avversario può quindi controllare questa applicazione senza che l'organizzazione riceva alcun avviso.

Comando e controllo

In questa fase, gli avversari hanno il controllo delle risorse all'interno dell'organizzazione presa di mira attraverso metodi di controllo (spesso remoti), come DNS, Internet Control Message Protocol (ICMP), siti web e social network. Questo canale è il modo in cui l'avversario indica alla risorsa controllata quale azione successiva eseguire e quali informazioni raccogliere.

I metodi utilizzati per raccogliere i dati sotto comando includono l'acquisizione delle schermate, il monitoraggio dei tasti digitati, la violazione delle password, il monitoraggio della rete per ottenere credenziali e la raccolta di contenuti e documenti sensibili.

Spesso viene identificato un host di staging in cui tutti i dati interni vengono copiati, quindi compressi e/o crittografati e resi pronti per l'esfiltrazione.

Azioni sui bersagli

Questa fase finale riguarda la modalità di esfiltrazione e/o danneggiamento dei dati. L'avversario adotta misure volte a identificare un maggior numero di bersagli, espandere la propria presenza all'interno di un'organizzazione e, aspetto più critico di tutti, esfiltrare i dati.

La CKC viene quindi ripetuta. La CKC è infatti un processo circolare, non lineare, e questa è suo punto di debolezza. Una volta che un avversario entra nella rete, ripete la Cyber Kill Chain, aumentando le ricognizioni ed effettuando movimenti laterali all'interno della rete.

Inoltre, è necessario tenere presente che, mentre la metodologia è la stessa, gli avversari, una volta all'interno dell'ambiente, utilizzano metodi diversi della kill chain interna rispetto a quando sono all'esterno.

Di fatto, quando l'aggressore si trova all'interno della rete, diventa un insider, un utente con privilegi e persistenza, e questo impedisce ai team di sicurezza dell'organizzazione di sospettare l'attacco e di rendersi conto che è già nelle fasi avanzate del modello esteso della Cyber Kill Chain.

3.La versione estesa della Cyber Kill Chain

La Cyber Kill Chain è un processo circolare e non lineare, in cui l'aggressore compie un movimento laterale continuo all'interno della rete. Le fasi che si svolgono all'interno della rete sono le stesse utilizzate quando l'obiettivo era quello di accedere alla rete, anche se con tecniche e tattiche diverse.

La combinazione della Cyber Kill Chain esterna e interna nel settore è definita Cyber Kill Chain estesa. Comporta l'aggiunta di più passaggi, che in realtà costituiscono lo stesso insieme, preceduti solo dalla parola "interna", quindi la Cyber Kill Chain diventa la Cyber Kill Chain interna con le sue fasi specifiche, la ricognizione interna, la weaponization interna e così via.

All'interno della rete di una vittima, ciascuna delle fasi dell'attacco può richiedere da pochi minuti a qualche mese, compreso il tempo di attesa finale che trascorre quando un attacco è pronto per essere sferrato.

L'aggressore, infatti, attenderà il momento migliore affinché l'attacco produca il massimo impatto. Le fasi di ricognizione e weaponization possono richiedere mesi.

È difficile interrompere queste fasi, in quanto vengono eseguite senza che ci sia alcun collegamento con l'aggressore.

Per questo motivo è di vitale importanza che le misure di sicurezza degli endpoint analizzino e supervisionino tutte le applicazioni e tutti i sistemi eseguiti nei dispositivi. Ciò ostacolerà notevolmente il lavoro degli aggressori e l'attacco diventerà per loro non remunerativo.

Ricognizione interna

In questa fase, gli avversari hanno accesso alla workstation di un singolo utente ed estraggono dati per i file locali, le condivisioni di rete, la cronologia del browser e l'accesso a wiki e SharePoint. L'obiettivo è di capire in che modo quel computer possa aiutare a mappare la rete e consentire lo spostamento verso risorse più preziose.

Sfruttamento interno

Gli aggressori sfruttano le patch mancanti, le vulnerabilità delle applicazioni web, i protocolli di trasmissione, lo spoofing o anche elementi più semplici come le credenziali predefinite che permettono loro di passare dalle workstation ai server utilizzando l'escalation dei privilegi, per poter effettuare un movimento laterale all'interno della rete, manipolando i singoli computer presi di mira.

La Cyber Kill Chain

Figura 1. La Cyber Kill Chain estesa. Azioni per ottenere l'accesso all'endpoint preso di mira e manipolazione dell'endpoint per raggiungere l'obiettivo dell'aggressore.

4.Panda Adaptive Defense 360 nella Cyber Kill Chain

Gli aggressori hanno degli obiettivi e sono disposti a spendere una determinata quantità di risorse per raggiungerli. Se i meccanismi di sicurezza degli endpoint sono in grado di aumentare il costo, in termini monetari, di personale o di tempo, rispetto al valore che si aspettano di ottenere, riusciranno nel loro intento con una frequenza minore o addirittura rinunceranno a sferrare l'attacco ai danni dell'organizzazione.

La sicurezza multilivello di WatchGuard con Panda Adaptive Defense 360 assicura che la Cyber Kill Chain venga sempre interrotta, lasciando a mani vuote gli aggressori.

Tutte le organizzazioni devono essere pronte a chiedersi cosa farebbero se l'avversario avesse accesso alla rete aziendale interna, ai nomi utente e alle password, a tutta la documentazione e alle specifiche dei dispositivi di rete, dei sistemi, dei backup e delle applicazioni, e fornire una risposta immediata.

L'obiettivo più grande della strategia di sicurezza degli endpoint di un'organizzazione dovrebbe essere quello di creare un'azienda più resiliente. Non riuscirà a prevenire tutti gli attacchi, ma ne bloccherà un numero maggiore già nelle prime fasi. Uno degli obiettivi è quello di disporre di meccanismi di difesa efficienti della Cyber Kill Chain estesa per rallentare gli aggressori, far sì che la prosecuzione dell'attacco diventi sempre più costosa e rendere il più difficile possibile il passaggio a ciascuna fase successiva.

Se gli avversari non riescono a raggiungere il loro obiettivo in modo conveniente, perseguiranno obiettivi diversi o simili con un'organizzazione bersaglio diversa.

La strategia di sicurezza di un'organizzazione deve tenere conto di come viene eseguito un attacco, dall'esterno e soprattutto dall'interno, poiché gli aggressori, una volta entrati nella rete, hanno accesso agli endpoint e alle loro risorse.

L'approccio tradizionale alla sicurezza dovrebbe essere esteso con metodi basati sulla comprensione della Cyber Kill Chain, fornendo tecnologie che siano in grado di impedire agli aggressori di accedere agli endpoint e anche di bloccarli in ogni possibile fase della Cyber Kill Chain interna.

La mappatura della strategia di difesa al modello CKC esteso mostra come l'organizzazione può prevenire, rilevare, interrompere ed effettuare il ripristino durante le fasi di attacco, allineando la sicurezza di un'organizzazione agli stessi criteri di successo dei suoi avversari.

Si tratta di un obiettivo difficile da raggiungere a causa di una serie di fattori. Le applicazioni sono aumentate sia in termini di complessità che di interconnessione e sono vulnerabili perché la maggior parte del software non è sviluppato utilizzando principi di sicurezza adeguati. Anche i dipendenti e i partner restano un vettore primario di rischio e possono aprire le porte agli attacchi basati sull'ingegneria sociale.

Panda Adaptive Defense 360 risolve questi problemi di sicurezza prevenendo, individuando e rispondendo alle tecniche più avanzate che gli avversari utilizzano in ogni fase della Cyber Kill Chain estesa. Aiuta i team di sicurezza a progettare una strategia di sicurezza allineata alla Cyber Kill Chain estesa senza necessità di aumentare il personale grazie al rilevamento e alla risposta intelligente degli endpoint (EDR).

I pilastri chiave di Adaptive Defense 360

Prevenzione del malware noto

Cercare solo le minacce note non protegge da varianti o attacchi sconosciuti, ma se si aggiungono altri livelli di sicurezza è possibile bloccare preventivamente le minacce note quando queste vengono distribuite nell'endpoint. Per bloccare proattivamente gli aggressori, Panda Adaptive Defense 360 utilizza una vasta raccolta di servizi di reputazione come l'analisi basata sulle firme, le firme generiche, l'euristica, il firewall, la reputazione degli URL, i rilevamenti contestuali, la gestione delle vulnerabilità, il controllo delle applicazioni e altre funzionalità in grado di ridurre il rischio.

Inoltre, Panda Adaptive Defense 360 sfrutta la funzione di intelligenza collettiva per classificare qualsiasi applicazione sconosciuta. L'**intelligenza collettiva** rappresenta il repository di conoscenze consolidate e incrementali relativo a tutte le applicazioni, i file binari e altri file contenenti codice interpretato, sia affidabile che dannoso.

Questo repository nel cloud viene incrementato continuamente dal sistema di IA e dagli analisti esperti e allo stesso tempo viene consultato continuamente dalle soluzioni e dai servizi di Panda Security, prima di qualsiasi esecuzione.

Rilevamento di malware avanzato e sconosciuto

Panda Adaptive Defense 360 rileva e blocca malware sconosciuto e attacchi mirati grazie a un modello di sicurezza basato su tre principi: il monitoraggio approfondito continuo di tutte le applicazioni in esecuzione sugli endpoint, la classificazione automatica dei processi degli endpoint utilizzando Big Data e tecniche di apprendimento automatico in una piattaforma basata su cloud e la possibilità, nel caso in cui un processo non venga classificato automaticamente, di avvalersi di un tecnico esperto che ne analizzi il comportamento approfondito.

Questi tre principi sono alla base del **servizio Zero Trust per le applicazioni**, che classifica le applicazioni come malware o come legittime prima di consentire l'esecuzione dei soli elementi attendibili di ogni endpoint. Trattandosi di un servizio completamente automatizzato, non servono input o decisioni da parte degli utenti finali oppure dei team di sicurezza o IT.

panda
a WatchGuard brand

Rilevamento del comportamento contestualizzato

Il monitoraggio continuo dell'attività presso l'endpoint permette all'agente di agire come un sensore e di comunicare alla piattaforma cloud non solo quali siano i file in esecuzione, ma anche il loro contesto di esecuzione (cosa è successo poco prima, quali utenti stanno cercando di eseguire un determinato comando o una determinata applicazione, che traffico di rete viene generato, quali sono i file di dati ai quali viene effettuato l'accesso, quali sono i parametri e così via).

Ciò permette di identificare, innanzitutto all'endpoint, i comportamenti anomali o le attività sospette e di classificarli come indicatori di attacco (IoA), con un elevato grado di sicurezza e senza falsi positivi.

Rilevamento dinamico degli exploit

Durante la fase di sfruttamento della Cyber Kill Chain estesa, gli aggressori utilizzano gli exploit per colpire le vulnerabilità a livello di codice in modo da poter violare applicazioni e sistemi e installare ed eseguire malware. I download effettuati da Internet costituiscono un vettore comune per l'esecuzione di attacchi di exploit. Panda Adaptive Defense e Panda Adaptive Defense 360 forniscono capacità dinamiche anti-exploit per proteggere sia dagli attacchi basati su applicazioni che da quelli basati sulla memoria.

Panda Adaptive Defense 360 rileva e blocca le tecniche effettive utilizzate dagli aggressori durante la fase di sfruttamento, come heap spray, stack pivot, attacchi ROP e modifiche delle autorizzazioni di memoria, ma rileva anche dinamicamente gli attacchi sconosciuti monitorando tutti i processi in esecuzione sui dispositivi e correla i dati tramite algoritmi di apprendimento automatico nel cloud in grado di bloccare qualsiasi tentativo di sfruttamento noto e sconosciuto.

Le tecnologie anti-exploit di Adaptive Defense bloccano l'avversario nella fase iniziale dell'attacco interno, identificando il momento in cui un'applicazione o un processo affidabile viene compromesso.

Panda Adaptive Defense 360 nella Cyber Kill Chain

Prevenzione e mitigazione

La protezione degli endpoint di nuova generazione deve prevenire e rilevare gli aggressori durante le diverse fasi della Cyber Kill Chain; tuttavia, il rilevamento deve essere seguito da una rapida mitigazione durante le fasi iniziali della kill chain di attacco.

Panda Adaptive Defense 360 mitiga automaticamente l'attacco, bloccando l'esecuzione di qualsiasi applicazione sconosciuta fino a quando non viene convalidata come affidabile dal nostro sistema di apprendimento automatico e dal team di sicurezza informatica, bloccando qualsiasi attività sospetta legata alle tecniche degli autori della minaccia, mettendo in quarantena il malware, terminando un processo compromesso o anche arrestando completamente il sistema allo scopo di ridurre al minimo i danni.

Correzione

Durante l'esecuzione, il malware spesso crea, modifica o elimina le impostazioni del file di sistema e del registro di sistema e cambia le impostazioni di configurazione.

Queste modifiche, o i problemi residui che permangono dopo la loro implementazione, possono causare instabilità o malfunzionamenti del sistema o perfino aprire le porte a nuovi attacchi. Panda Adaptive Defense 360, nei casi residui di esecuzione del malware, ripristina gli endpoint nel loro stato affidabile pre-malware.

Visibilità

Considerata la mutevole realtà del panorama delle minacce e la frequenza, la sofisticatezza e la natura mirata degli attacchi sferrati dagli avversari, nessuna tecnologia di sicurezza può rivendicare un'efficacia al 100%, pertanto la capacità di fornire diagnosi e visibilità degli endpoint in tempo reale è un imperativo.

I team di sicurezza informatica aziendali devono disporre di un piano per gestire le segnalazioni di violazioni, contattare le forze dell'ordine, gestire la pubblicità negativa e altre attività analoghe.

Panda Adaptive Defense 360 fornisce una visibilità chiara e tempestiva delle attività dannose in tutta l'organizzazione. Questa visibilità consente ai team di sicurezza di valutare rapidamente la portata di un attacco e di intraprendere le azioni appropriate.

Risposta da remoto

Quando i sistemi remoti sono l'obiettivo degli aggressori e vengono compromessi, i team IT o di sicurezza devono intervenire rapidamente per capire la natura dell'attacco e porvi rimedio. Coloro ai quali è affidato il compito di fornire la risposta hanno bisogno di visibilità e accesso ai sistemi remoti, poiché gli utenti non possono portare fisicamente un laptop all'IT.

Panda Adaptive Defense offre ai team IT e di sicurezza una profonda visibilità degli endpoint per indagare rapidamente sugli incidenti e comprendere appieno le minacce emergenti; inoltre, consente loro di accedere direttamente al sistema e di eseguire rapidamente un'ampia varietà di comandi per contenere gli aggressori, correggere gli host remoti con azioni quali l'isolamento degli endpoint dalla rete, impedendo la comunicazione da e verso altri endpoint per fermare la diffusione dell'attacco, e terminare i processi mediante il riavvio dell'endpoint.

Grazie a queste funzionalità, Panda Adaptive Defense 360 può ridurre in notevole misura il tempo necessario per rispondere agli attacchi, ovunque si verifichino, e ripristinare rapidamente l'operatività dell'organizzazione.

Panda Adaptive Defense 360 nella Cyber Kill Chain

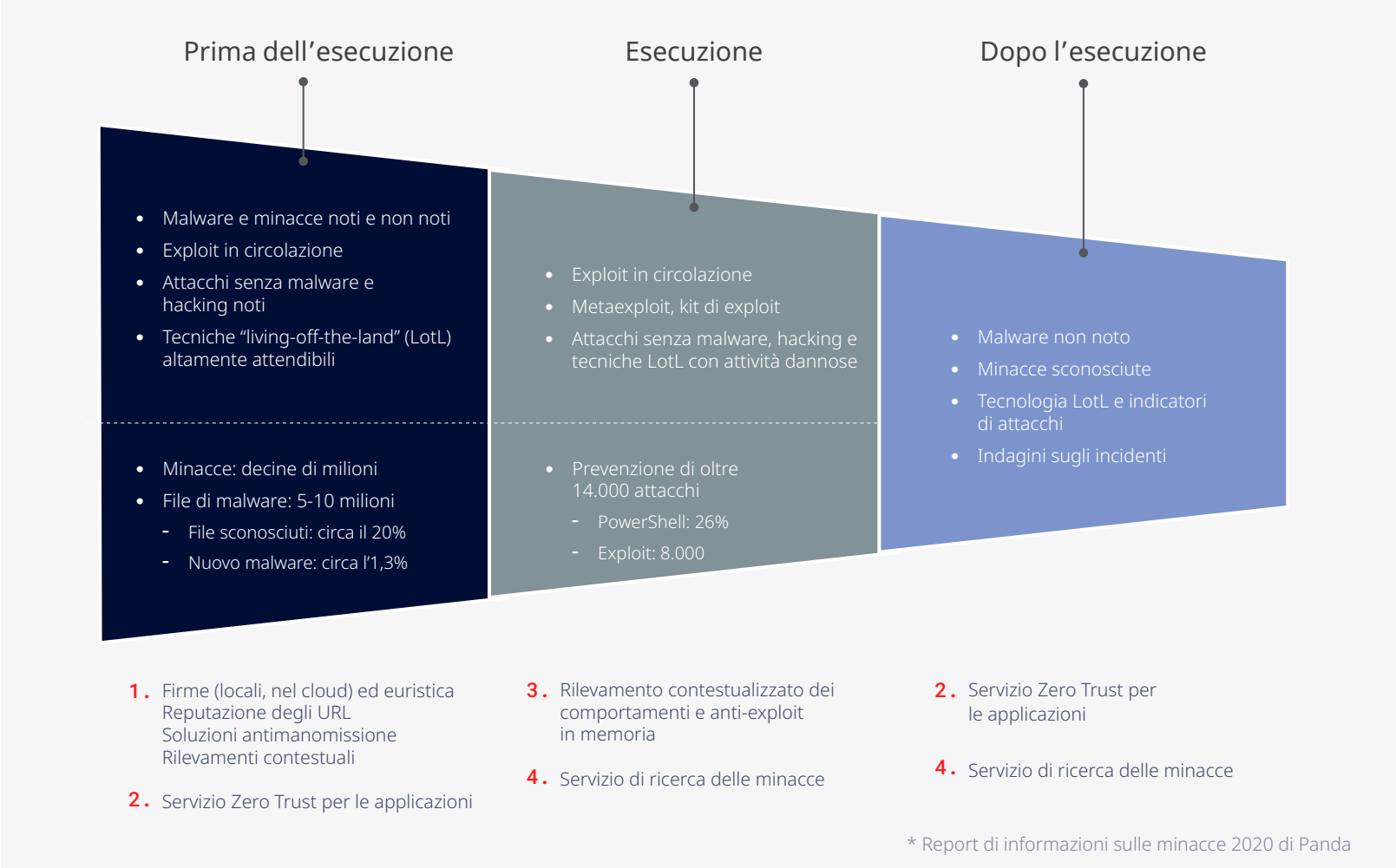


Figura 2. Pilastri della sicurezza Adaptive Defense 360 durante l'applicazione della Cyber Kill Chain estesa.

5.L'anatomia di un attacco ransomware e in che modo Panda Adaptive Defense 360 protegge la tua azienda

La figura 3 illustra come Panda Adaptive Defense 360 gestisce ogni fase della kill chain in un attacco ransomware e in che modo può prevenire e bloccare gli attacchi in corso prima che causino danni.

Spesso, l'aggressore utilizza tecniche semplici per aprirsi un varco in qualsiasi endpoint preso di mira, il più delle volte utilizzando metodi di ingegneria sociale come il phishing. Un utente riceve un'e-mail dove gli viene chiesto di fare clic su un link o di scaricare un file dannoso.

PASSAGGIO 1

A questo punto, AD360 agirà immediatamente:

- Bloccando le e-mail dannose con la tecnologia Email Antispam.
- Utilizzando il filtro degli URL per impedire l'accesso agli URL dannosi noti.

PASSAGGIO 2

Nel caso in cui l'autore della minaccia nonsia bloccato e l'utente finale acceda al sito web dannoso che è stato compromesso, possono verificarsi diverse azioni dannose, come lo sfruttamento di una vulnerabilità del browser o il download di un file Microsoft Office con uno script dannoso.

In ogni caso, Adaptive Defense 360 bloccherà l'aggressore con le tecnologie anti-exploit, sia con il modulo anti-exploit in memoria che blocca gli exploit noti e sconosciuti, sia con la prevenzione delle macro o il rilevamento basato sul contesto che rifiuta le esecuzioni di script dannosi.

PASSAGGIO 3

Ipotizziamo che si verifichi lo scenario peggiore, cioè quello in cui l'autore della minaccia riesca a rilasciare ransomware nel dispositivo. Panda Adaptive Defense 360 impedirà che il dispositivo venga compromesso bloccando il download del malware, sia controllando le firme generiche locali ed eseguendo la scansione del file con tecnologie euristiche, sia eseguendo query nella nostra intelligenza collettiva nel cloud.

Il rilevamento generico basato sulle firme si riferisce al rilevamento e alla rimozione di più minacce utilizzando un'unica firma. Il punto di partenza per il rilevamento generico risiede nel fatto che le minacce efficaci sono spesso copiate da altri o ulteriormente perfezionate dagli autori originali. Il risultato è una serie di varianti di ransomware, ciascuna delle quali distinta ma appartenente alla stessa famiglia. In molti casi, si può arrivare a centinaia, migliaia o addirittura decine di migliaia di varianti.

La scansione euristica è un insieme di tecniche per ispezionare i file sulla base di centinaia di caratteristiche. Determina la probabilità che un programma possa intraprendere azioni dannose quando viene eseguito sul computer di un utente, bloccandolo e rimuovendolo prima che arrivi agli endpoint.

PASSAGGIO 4

Finora, abbiamo esaminato tecnologie che sono efficaci per bloccare gli autori delle minacce, ma che non possono garantire l'assenza di applicazioni dannose in esecuzione sull'endpoint. Tuttavia, riducono notevolmente la quantità di lavoro che il servizio Zero Trust per le applicazioni deve elaborare e questo è il livello di protezione successivo nella Cyber Kill Chain. Ipotizziamo, quindi, che il ransomware venga scaricato e cerchi di essere eseguito sull'endpoint per avviare i suoi comportamenti dannosi ed elusivi.

In questo momento, il servizio Zero Trust per le applicazioni identifica il file binario come sconosciuto, ne rifiuta l'esecuzione, lo carica nel cloud e classifica automaticamente il payload con un cluster complesso e completo di algoritmi di apprendimento automatico, combinando centinaia di attributi, molti dei quali ottenuti dall'esecuzione del campione in un ambiente reale nella nostra infrastruttura cloud.

Nel 99,98% dei casi la classificazione avviene in tempo reale, in quanto non è necessario supervisionare i risultati. Solo in casi eccezionali i nostri esperti di sicurezza informatica devono completare la classificazione, poiché nel processo potrebbero essere stati identificati nuovi comportamenti sospetti.

In ogni caso, il risultato di queste difese della Cyber Kill Chain è un vero e proprio modello Zero Trust in cui non vengono eseguiti file binari, applicazioni o processi dannosi.

PASSAGGIO 5

Quando gli autori di minacce riescono ad accedere agli endpoint senza utilizzare applicazioni dannose, altri componenti della protezione multilivello assumono un ruolo centrale nella Cyber Kill Chain. Ad esempio, se l'autore della minaccia acquisisce il controllo di un endpoint, ottiene persistenza e inizia a esplorare la rete alla ricerca di nuovi obiettivi per gli endpoint utilizzando le tecniche di "living-off-the-land"; a quel punto, le tecnologie di rilevamento basate sul contesto bloccheranno il tentativo di utilizzo illegittimo degli strumenti di sistema, come PowerShell.

PASSAGGI 6/7

La componente chiave in questa efficace implementazione del modello Zero Trust è il fatto che ogni attività eseguita nell'endpoint viene monitorata in tempo reale e valutata dal servizio Zero Trust per le applicazioni e dal servizio di ricerca delle minacce che effettua le attività di rilevamento e indagine sulle attività sospette, notificando o bloccando le attività dannose confermate presso l'endpoint.

Estendi la tua visibilità e proteggi la tua organizzazione indipendentemente dalla posizione fisica. Prova Panda Adaptive Defense 360

https://www.watchguard.com/it/wgrd-products/demos-free-trials

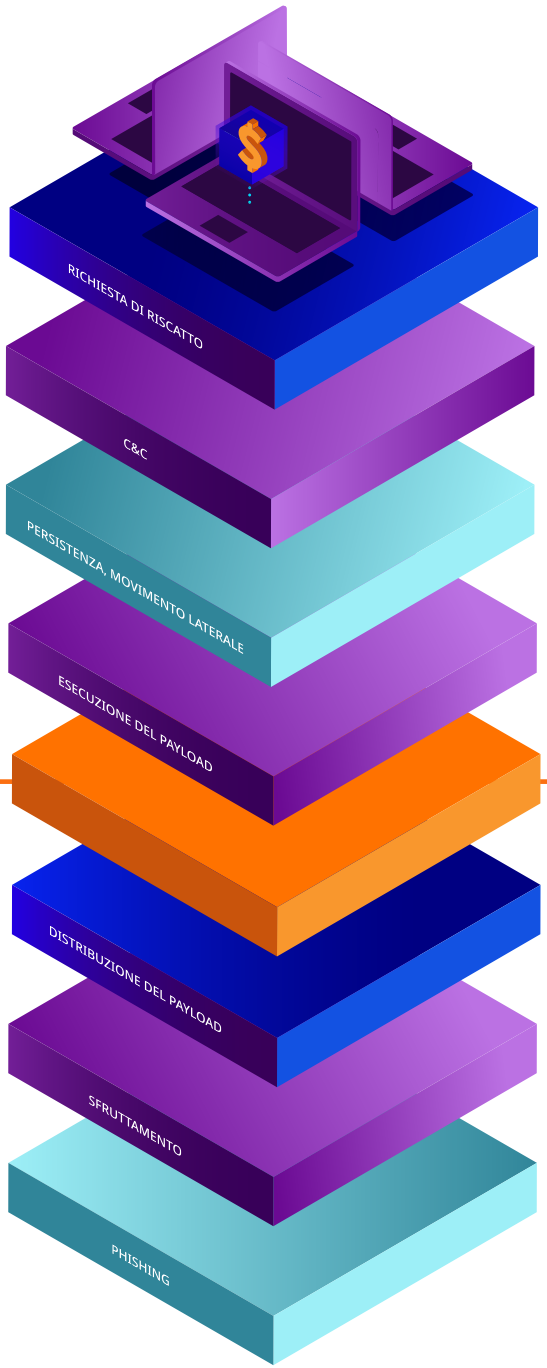
panda
a WatchGuard brand

L'anatomia di un attacco ransomware

1. **L'utente riceve un'e-mail dove gli viene chiesto di fare clic su un link o di scaricare un file dannoso.**
2. The sito web sfrutta una **vulnerabilità del browser** oppure **scarica un file MS Office** con un script dannoso (attacco download drive-by).
3. Quando l'utente **fa clic, il ransomware** viene distribuito all'endpoint.
4. Il ransomware viene eseguito sull'endpoint e **avvia i suoi comportamenti dannosi ed elusivi.**

Non vengono eseguiti file binari, applicazioni o processi dannosi.

5. Dopo aver assunto il controllo di un endpoint, l'autore della minaccia **esplora la rete e cerca nuovi bersagli** (tecniche LotL).
6. Tentativi di ransomware per recuperare la chiave di crittografia **da un server di comando e controllo.**
7. Il ransomware avvia il processo di crittografia dei file sull'endpoint. **Il messaggio visualizzato conferma la presenza del ransomware** sull'endpoint e fornisce istruzioni per il pagamento del riscatto.



Panda Adaptive Defense 360 per la protezione multilivello

1. Blocco dell'e-mail dannosa con **l'applicazione anti-spam.**
   Impedisce l'accesso agli URL dannosi noti con **il filtro degli URL.**
2. Blocco dello sfruttamento di browser noti con **la tecnologia anti-exploit.**
   Blocco dello sfruttamento di elementi sconosciuti con **la tecnologia anti-exploit in memoria.**
   Blocco dell'esecuzione di script con **il rilevamento delle macro o basato sul contesto.**
3. Blocco delle minacce dopo la ricerca nel **repository basato su cloud.**
   Blocco di firme generaliste ed euristica **note/sconosciute.**
4. **Modello Zero Trust:** qualsiasi file binario sconosciuto proveniente dall'esterno (e-mail, web, rete, dispositivo) viene bloccato fino a quando non viene classificato.
   Il servizio Zero Trust per le applicazioni classifica automaticamente il payload nel cloud con **l'apprendimento automatico e l'ambiente reale.**

Non vengono eseguiti file binari, applicazioni o processi dannosi.

5. Blocco dell'utilizzo illegittimo degli strumenti di sistema (PowerShell) con **rilevamento basato sul contesto.**
   Blocco del comportamento dannoso manifestato durante l'esecuzione con **il rilevamento del comportamento contestualizzato.**
6. **Il servizio Zero Trust per le applicazioni** rifiuta l'esecuzione del malware.
   In qualsiasi caso, tutti i processi sono monitorati continuamente e riclassificati dal **servizio Zero Trust per le applicazioni.**
7. La telemetria viene monitorata e analizzata dal **servizio di ricerca delle minacce.**

panda
a WatchGuard brand

6.Riferimenti

- La Cyber Kill Chain di Lockheed Martin: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- Sean T. Mallon, Strategic Cybersecurity Leader ed Executive Consultant al Black Hat 2016: La Cyber Kill Chain estesa
- Difesa basata sulle minacce alla sicurezza informatica di Mitre
- Ciclo di vita dello sviluppo della sicurezza Microsoft
- Gartner Research, G00298058, Craig Lawson, 7 aprile 2016

[1] Eric M. Hutchins, Michael J. Cloppert e Rohan M.Amin, Ph.D., Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.

[2] Attacchi di tipo "watering hole". Un tipo specifico di attacco mirato in cui la vittima appartiene a un gruppo specifico (organizzazione, settore o area geografica). In questo attacco l'aggressore indovina o osserva quali siti web sono maggiormente utilizzati dal gruppo e ne infetta uno o più di uno con il malware. Alla fine alcuni membri del gruppo preso di mira vengono infettati.

Il malware utilizzato da questi aggressori in genere raccoglie informazioni sull'utente. Gli aggressori che cercano informazioni specifiche possono colpire solo gli utenti provenienti da un indirizzo IP specifico. Questo rende gli attacchi anche più difficili da individuare e da ricercare. Il nome deriva dai predatori del mondo naturale, che aspettano l'occasione per attaccare le loro prede in prossimità delle pozze d'acqua ("watering hole"). L'utilizzo dei siti web considerati affidabili dal gruppo rende efficiente questa strategia, anche con gruppi che resistono allo spear phishing e ad altre forme di phishing.

[3] Il rilevamento dinamico degli exploit è l'innovativa tecnologia di Panda Security basata sul monitoraggio di tutti i processi in esecuzione nell'endpoint o nel server e sulla sua analisi nel cloud con tecnologie di apprendimento automatico volte a rilevare i tentativi di sfruttamento delle applicazioni considerate affidabili. L'obiettivo di questa nuova tecnologia è fermare gli attacchi alle workstation e ai server nelle primissime fasi della Cyber Kill Chain. Contenendo l'aggressore e ostacolandone l'accesso al dispositivo in misura tale da compromettere la redditività dell'attacco, si scoraggiano ulteriori tentativi e si ottiene quindi un tasso di rilevamento più elevato.

panda
a WatchGuard brand

VENDITE ITALIA: 800.911.938 VENDITE INTERNAZIONALI: +1.206.613.0895 www.watchguard.it | pandasecurity.com

Ulteriori informazioni sono disponibili sul nostro sito web