Forcepoint Zero Trust Content Disarm and Reconstruction

Blocca le minacce note e sconosciute, gli attacchi zero-day e il malware

Forcepoint

Brochure

Forcepoint Zero Trust Content Disarm and Reconstruction

Blocca le minacce note e sconosciute, gli attacchi zero-day e il malware

Scambi via e-mail, interazioni su web e social media, upload di file, applicazioni web: la tecnologia genera le informazioni digitali che sono la linfa vitale di ogni organizzazione. Queste informazioni digitali sono condivise e comunicate con business partner, clienti, catene di fornitura e lavoratori in locale e da remoto. La condivisione delle informazioni su questa scala ha creato una vasta superficie di attacco che il cybercrimine può sfruttare usando malware nascosto in file, documenti e immagini di uso quotidiano.

Di conseguenza è aumentato il numero di tecnologie di difesa che mirano a contrastare il problema. Ma queste difese, quale più quale meno, sono tutte basate sul concetto del rilevamento. Il loro limite? Possono rilevare soltanto ciò che hanno già "visto". Gli sforzi per renderle più efficaci sono stati molteplici. Le sandbox sono utili, ma gli hacker hanno imparato a identificarle e, in ogni caso, anche le sandbox si basano sul rilevamento delle minacce per contrastarle. L'intelligenza artificiale e gli algoritmi di apprendimento automatico servono, ma di fatto usano potenza di elaborazione soltanto per accelerare il rilevamento di una minaccia già nota. Gli hacker, quindi, cercano costantemente di attaccare le organizzazioni usando malware che le tecnologie di difesa non conoscono e che, perciò, giudicano innocuo.

In conclusione, le difese basate sul rilevamento non bastano.

Forcepoint Zero Trust Content Disarm and Reconstruction (CDR) è diverso. Invece di provare a rilevare il malware, parte dal presupposto che niente è affidabile. Procede quindi estraendo dai file le informazioni di business valide (eliminando o archiviando i file originali), verificando che le informazioni estratte siano correttamente strutturate e poi costruendo nuovi file perfettamente funzionali per trasportare le informazioni a destinazione. Zero Trust CDR è un'autentica rivoluzione per mitigare la minaccia anche dei più sofisticati exploit e attacchi zero-day. Questo passaggio dal rilevamento alla prevenzione è estremamente importante soprattutto alla luce della recente evoluzione della forza lavoro divenuta ibrida e della trasformazione digitale, nonché del conseguente uso di contenuti e dati elettronici ovunque.

Le difese anti-malware devono:

- **Recapitare sempre contenuti sicuri e pienamente funzionali** affinché gli utenti possano essere certi dell'attendibilità dei file che ricevono da mittenti esterni all'organizzazione.
- **Bloccare le minacce zero-day** senza bisogno delle ultime patch o firme per consolidare la difesa.

Vettori d'attacco da proteggere:

- **Browser web**
- **Download da web**
- **Posta sul web**
- **Social media**
- **Upload di file**
- **Mail**
- **Applicazioni web**
- **Condivisione di file**

Blocco di ogni minaccia

I contenuti digitali sono il vettore di elezione per gli attacchi dei cybercriminali con malware ed exploit. Navigazione sul web, e-mail, file caricati e social media... i contenuti digitali vengono regolarmente infettati con minacce note, zero-day e anche impossibili da rilevare, occultate nei file e nelle immagini che usiamo costantemente nel nostro lavoro.

Da oltre 25 anni l'approccio standard per combattere queste minacce è costituito da tecnologie di difesa basate sul rilevamento. Il problema è che il rilevamento è facile da aggirare. Basta cambiare la firma dell'exploit ed ecco che il malware supera le barriere di sicurezza indisturbato. Il rilevamento da solo non basta più a proteggere gli utenti da minacce note e sconosciute, attacchi zero-day e malware.

Forcepoint Zero Trust CDR blocca l'entrata nell'organizzazione del malware basato su file, senza ricorrere al rilevamento. Zero Trust CDR protegge gli utenti anche dalle minacce zero-day e dai malware sconosciuti usando un metodo unico: estrae e recapita solo il contenuto sicuro dei file, senza neanche provare a rilevare le minacce. Questo approccio alla prevenzione dal malware non impone aggiornamenti costanti della difesa con le firme delle ultime minacce zero-day non appena diventano disponibili.

Esperienza d'uso superiore

Le organizzazioni vanno in cerca di soluzioni innovative e più efficaci al problema del malware occulto, ma spesso finiscono per compromettere la user experience. Sottoposti a molteplici scansioni antivirus e trattenuti nelle sandbox per ulteriori scrutini, i file avanzano lenti aggiungendo latenza ai processi aziendali. Il tentativo di proteggere i file "appiattendoli", cioè convertendoli dal formato originario a un formato fisso e non modificabile, significa che l'azienda si ritrova con documenti difficili da condividere, modificare o aggiornare. In molti casi le intenzioni sono buone, ma il risultato finale è il rallentamento dei processi aziendali e una crescente frustrazione degli utenti.

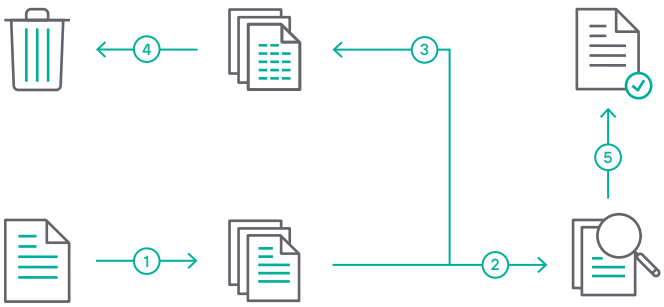
Forcepoint Zero Trust CDR migliora la user experience senza compromettere la sicurezza. Il processo di Zero Trust CDR non fa uso del rilevamento, quindi non bisogna attendere che il sistema analizzi i file e tenti di rilevare le minacce note. Non utilizza neanche le sandbox, quindi non comporta lunghi ritardi nei processi di business essenziali, mentre i file sono isolati per essere sottoposti a ispezione. Zero Trust CDR agisce in una frazione di secondo, rispondendo all'esigenza aziendale di informazioni sia sicure che prontamente disponibili, senza latenza. Zero Trust CDR migliora la user experience, visto che non ostacola la velocità di accesso ai file e in più offre agli utenti dei file perfetti al pixel e completamente modificabili, sempre privi di malware.

Meno lavoro per il team SOC

Anche con le più efficaci strategie di difesa basate sul rilevamento, molti team SOC (Security Operations Center) impiegano comunque troppo tempo e denaro per prevenire, rilevare, analizzare e rispondere agli incidenti di cybersicurezza causati da malware annidato nei file in arrivo.

Con Forcepoint Zero Trust CDR, il team SOC non dovrà più preoccuparsi ogni giorno di gestire le code di file in quarantena e i falsi positivi, di applicare gli aggiornamenti delle firme e di rispondere agli avvisi di potenziali violazioni. Ogni file in arrivo è soggetto al processo Zero Trust CDR, che contenga o meno malware, e ogni file viene ricostruito privo di minacce.

Funzionamento



1. Invece di identificare il malware noto, Zero Trust CDR prende i dati e ne estrae le informazioni utili.
2. Le informazioni estratte vengono trasformate in un formato intermedio e verificate.
3. Questo processo di protezione dalle minacce avanzate garantisce che nessuna minaccia e nessun attacco possano arrivare alla fase successiva.
4. I dati originali vengono archiviati o eliminati insieme al malware, noto o sconosciuto.
5. I nuovi dati vengono poi ricostruiti in modo normalizzato, con le informazioni verificate. I nuovi dati replicano quelli originali, senza la minaccia di possibili malware incorporati e, quindi, in totale sicurezza.

Protezione senza precedenti

- Massima garanzia di dati senza minacce e perfetti al pixel, oltre che completamente modificabili.
- Zero rischi anche con gli attacchi più sofisticati.
- Nessuna esposizione alle cosiddette minacce "Zero Day".

Elevata versatilità

- È compatibile con le tecnologie e difese perimetrali esistenti.
- Trasforma un'ampia gamma di formati di file tra i più diffusi, inclusi tutti i file Office, le immagini e i PDF (i formati usati più spesso dagli hacker).
- Difende una ricca varietà di vettori di attacco, tra cui web, e-mail e upload di file.

Scelta di distribuzione

- Opzioni di distribuzione in locale, virtuale e su cloud.
- Distribuzione e messa in funzione in pochi minuti.

Appendice A. Panoramica sui componenti della soluzione

Forcepoint Zero Trust CDR per Web Gateway	Forcepoint Zero Trust CDR per Web Gateway protegge gli utenti web dal malware nascosto nei download dal web, nella posta sul web e nei social media. Viene distribuito sul perimetro della rete e si integra con il Secure Web Gateway (SWG) esistente. Le regole delle policy nel Web Gateway determinano quali tipi di file passare a Forcepoint Zero Trust CDR per l'elaborazione.
Forcepoint Zero Trust CDR per Remote Browser Isolation	Con Forcepoint Zero Trust CDR per Remote Browser Isolation, gli utenti che navigano in internet con Remote Browser Isolation possano scaricare in sicurezza i file sull'host fisico, sapendo che sono totalmente privi di malware.
Forcepoint Zero Trust CDR per upload di file	Forcepoint Zero Trust CDR per upload di file protegge l'organizzazione dal malware contenuto nei file scaricati da internet e può essere distribuito insieme a un reverse web proxy o come parte di un'applicazione web basata su cloud.
Forcepoint Zero Trust CDR per la posta	Forcepoint Zero Trust CDR per la posta protegge gli utenti dal malware occultato nei messaggi e allegati e-mail. Di solito viene distribuito tra la difesa perimetrale delle e-mail e il server e-mail dell'organizzazione.
Forcepoint Zero Trust CDR per la condivisione file	Forcepoint Zero Trust CDR per la condivisione file assicura che i file in transito tra gli archivi di file su diverse reti siano privi di malware.
Forcepoint Zero Trust CDR per applicazioni web	Forcepoint Zero Trust CDR per applicazioni web assicura che i dati strutturati in transito tre reti siano vincolati a schemi predefiniti, per garantire che non possano essere utilizzati come vettore di un attacco.
API cloud Forcepoint Zero Trust CDR	Oltre alla disponibilità in locale, Forcepoint Zero Trust CDR è disponibile anche tramite API cloud-native per gli sviluppatori che devono integrare il disarmo e la ricostruzione dei contenuti nei loro flussi di lavoro e applicazioni web.

Appendice B. Tipi di file resi innocui da Forcepoint zero Trust CDR

Forcepoint Zero Trust CDR è in grado di trasformare i seguenti tipi di file e renderli innocui:

FILE OFFICE	
TIPO DI FILE	**ESTENSIONE**
Immagine bitmap	BMP
Documento Microsoft Office X	DOCX
Metafile avanzato Microsoft	EMF
Messaggio e-mail	EML
Immagine GIF	GIF
File HTML	HTML
File ICAL	ICAL
JPEG 2000	JP2K
Immagine JPEG	JPEG
Archivio MIME HTML	MHT
Multipurpose Internet Mail Extension	MIME
Adobe PDF	PDF
Immagine PNG	PNG
Microsoft Office X PowerPoint	PPTX
Rich Text	RTF
Testo normale	TXT
Immagine TIFF	TIFF
Metafile Microsoft Windows	WMF
Microsoft Office X Excel	XLSX
Archivio Zip	ZIP

FILE DI DATI STRUTTURATI	
TIPO DI FILE	**ESTENSIONE**
Valori delimitati da virgole	CSV
Dati strutturati JSON	JSON
Google Protocol Buffers 3	Proto3
Dati strutturati XML	XML

I seguenti formati di file vengono trasformati e resi innocui mediante conversione in un formato intermedio:

FORMATO	ORIGINALE	CONVERTITO	FINALE
Microsoft Word legacy	DOC	DOCX	DOC
Microsoft PowerPoint legacy	PPT	PPTX	PPT
Microsoft Excel legacy	XLS	XLSX	XLS
Testo OpenDocument	ODT	DOCX	ODT
Foglio di calcolo OpenDocument	ODS	XLSX	ODS
Presentazione OpenDocument	ODP	PPTX	ODP
Rich Text	RTF	DOCX	RTF
eXtensbile Paper Specification	XPS	PDF	XPS
Formato ebook EPUB	EPUB	PDF	EPUB
Formato ebook Mobipocket	MOBI	DOCX	-
Computer Graphics Metafile	CGM	PDF	-
Adobe Photoshop	PSD	PNG	PSD
Microsoft One Note	ONE	PDF	-
Disegno AutoCAD	DWG	PDF	-
Disegno AutoCAD legacy	DXF	PDF	-
Microsoft Visio legacy	VSD	PDF	-
Microsoft Visio	VSDX	PDF	-
XLS Formatting Object	FO	PDF	-
Archivio 7Zip	7Zip	ZIP	7Zip
Archivio BZip2	BZip2	ZIP	BZip2
Archivio GZIP	Gzip	ZIP	GZip
Archivio Z	Z	ZIP	Z
Archivio TAR	TAR	ZIP	TAR
Archivio Microsoft CAB	CAB	-	ZIP

Forcepoint

forcepoint.com/contact

Informazioni su Forcepoint

Forcepoint è l'azienda leader nel settore della sicurezza informatica per la protezione degli utenti e dei dati. La sua missione è proteggere le aziende e guidarne la crescita e la trasformazione digitale. Le soluzioni human-centric di Forcepoint si adattano in tempo reale alle modalità di interazione tra persone e dati, consentono un accesso sicuro e, allo stesso tempo, permettono ai dipendenti di creare valore. Dalla sua sede di Austin, Texas, Forcepoint crea ambienti sicuri e affidabili per migliaia di clienti in tutto il mondo.

[FP-Zero Trust CDR-Brochure-IT] 10Mar2022