WHITE PAPER

Difesa contro le minacce note, non note ed elusive con WatchGuard Threat Detection and Response

Sommario

Comprendere le minacce malware per le piccole e medie imprese

Se da un lato i recenti attacchi informatici e le ultime violazioni contro grandi organizzazioni sono finite sulle prime pagine dei giornali, dall'altro le minacce alle imprese di medie dimensioni non vengono raccontate. La realtà è che il numero di piccole e medie imprese vittima degli attacchi informatici e del malware avanzato è sproporzionalmente alto. Anzi, secondo la National Cyber Security Alliance, oltre il 70% di tutti gli attacchi mira alle medie imprese.

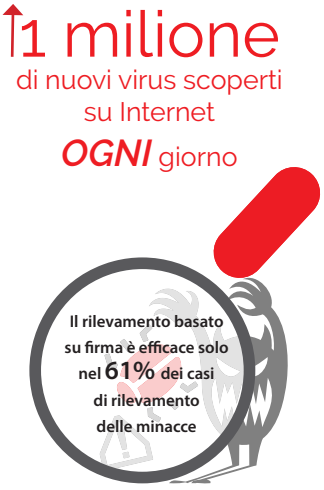
La capacità degli attacchi informatici mirati contro marchi ben noti di finire sui giornali nasconde il ben più grande numero di minacce malware che agisce in profondità. Oggi, le organizzazioni di tutte le dimensioni sono assediate da un oceano di malware in continuo movimento. Ogni giorno viene scoperto un milione di nuovi campioni di malware e si stima che ogni mese vengano rilasciati 12 milioni di campioni di malware per Windows. Con grandi budget per la sicurezza, team di addetti alla sicurezza competenti e tecnologie all'avanguardia a loro disposizione, le grandi aziende sono ben posizionate per proteggersi dalla tempesta di malware che cerca di penetrare dalle porte di servizio. Tuttavia, il malware presenta delle sfide particolarmente preoccupanti per le medie imprese, in quanto devono affrontare le stesse minacce delle grandi aziende, ma potendo contare su una quantità di risorse di gran lunga inferiore.

Da cosa è guidata la minaccia?

I criminali informatici progettano malware sempre più sofisticati, che sfruttano le minacce zero-day e le tecniche di elusione per superare le difese di rete senza essere rilevati. Rilevare il malware e le minacce in questo panorama virulento è vitale. In questo documento spiegheremo perché gli approcci tradizionali al rilevamento del malware non funzionano e illustreremo l'importanza di un approccio correlato che permetta agli utenti di prendere in considerazione in contemporanea i comportamenti a livello di rete e quelli a livello di endpoint, così da poter rilevare ed evitare il malware prima che agisca. Infine, viene analizzata l'importanza del rilevamento e della correzione tempestivi per ridurre i rischi impliciti nelle minacce elusive e mirate.

Malware noto, non noto ed elusivo

Ogni giorno in Internet vengono scoperti un milione di nuovi campioni di malware. Questo numero, tuttavia, è un po' fuorviante, in quanto è parzialmente dovuto alla capacità del malware di trasformarsi a tal punto da eludere i motori di rilevamento basati su firma conosciuti. La realtà è che l'ecosistema delle minacce malware è variegato, in espansione e in continua evoluzione. Per illustrare meglio il paesaggio delle minacce malware e gli approcci necessari per difendere le organizzazioni, classifichiamo le minacce in note, non note ed elusive.



Malware noto

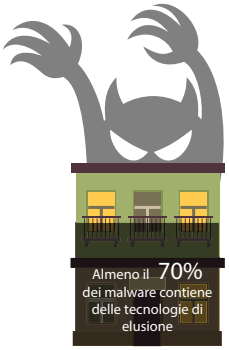
Con malware noto ci riferiamo ai campioni di malware che sono stati rilevati in precedenza e che possono essere identificati tramite le tecniche di rilevamento basate sulla reputazione e sulle firme. Il malware diventa noto quando gli analisti addetti alla sicurezza sono in grado di analizzare la minaccia e creare una firma da distribuire ai motori di rilevamento. Questo processo lento e manuale diventa in breve tempo un'impresa titanica per via dell'abnorme volume di minacce da analizzare. È stato dimostrato che l'efficacia del rilevamento basato sulla firma, anche per minacce vecchie di due settimane, può raggiungere oggi solo il 61%.[1] È necessario specificare, però, che sebbene il rilevamento basato su firma sia inefficace contro le ultime minacce, gli endpoint privi di questo tipo di protezione hanno una probabilità 5,5 volte maggiore di essere infettati.[2]

Malware non noto

Il malware non noto è il malware che non è mai stato rilevato o per il quale non esiste alcuna firma nota. Il malware non noto potrebbe essere un software completamente nuovo oppure una variante di un malware noto, ma trasfigurato in modo tale da evitare il rilevamento basato su firma. Gli approcci euristici possono migliorare notevolmente il rilevamento del malware non noto, in quanto ricercano comandi dannosi all'interno dei file sospetti al fine di identificare le minacce. In modo analogo, risulta efficace anche il monitoraggio degli endpoint alla ricerca di comportamenti che potrebbero indicare la presenza di malware non noto.

Malware elusivo

Per superare le difese, il malware elusivo utilizza i canali di comunicazione crittografati, i rootkit a livello di kernel, gli exploit zero-day e le tecniche di rilevamento ambientale. Il 2014 è l'anno in cui il malware elusivo è diventato predominante; nel giro di pochi mesi l'uso delle tecniche elusive ha visto un'esplosione del 2000%.[3] Oggi, si stima che il 70% del malware contiene qualche forma tecnologica di elusione sofisticata.[4] Il rilevamento del malware elusivo richiede la capacità di analizzare in profondità i file in un ambiente che emuli una piattaforma hardware e un sistema operativo completi.



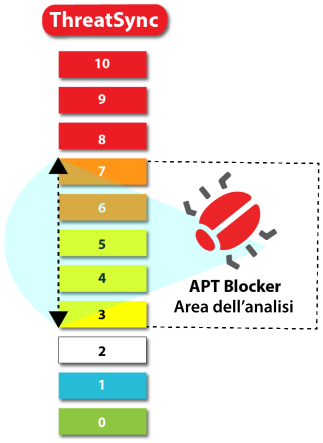
1 https://www.lastline.com/labsblogw
2 https://news.microsoft.com/2013/04/17/malware-infections-5-5-times-more-likely-without-antivirus-software-finds-new-research-from-microsoft/
3 https://www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667
4 https://www.lastline.com/documents/lastLine_deep_content_inspec_tb.pdf

L'importanza della correlazione nel rilevamento e nella prevenzione del malware

Tutti i malware seguono uno schema di infezione che è possibile analizzare per agevolare il rilevamento. Solitamente un attacco inizia quando un utente fa clic su un'e-mail dannosa, in quanto vittima di download drive-by oppure perché ha inserito un'unità USB infetta avviando il processo di infezione. Dopo essere entrato nel sistema target, il malware potrebbe tentare di cercare i dati sensibili, scalare i privilegi, acquisire altri strumenti dannosi o tentare di diffondersi su altre macchine della rete. Ognuno di questi comportamenti lascia delle tracce sull'endpoint e sulla rete e tali tracce potrebbero dare visibilità a una potenziale minaccia. Ciononostante, le organizzazioni impiegano mediamente più di 200 giorni per rilevare una violazione. Sfortunatamente, maggiore è il periodo in cui una violazione rimane non rilevata, maggiori sono le opportunità per gli aggressori di danneggiare l'azienda. Poiché la posta in gioco è alta, ridurre il tempo e le risorse necessarie per rilevare il malware non noto e quello elusivo è un fattore essenziale. La correlazione tra gli eventi di sicurezza della rete e quelli degli endpoint rende possibile tale riduzione. La correlazione permette agli amministratori di identificare le nuove minacce prive di firma, determinare quali endpoint sono stati infettati, seguire il percorso dell'infezione e identificare l'origine della minaccia. Offre agli amministratori la visibilità di cui hanno bisogno per fermare le minacce non note e quelle elusive prima che possano fare danni; possono quindi evitare che gli attacchi andati a buon fine si diffondano ad altre parti dell'organizzazione.

Presentazione di Threat Detection and Response

Le firme rappresentano un sistema di difesa ottimo e necessario contro le minacce note, ma le organizzazioni necessitano di un sistema per fermare il malware non noto e le nuove varianti. Threat Detection and Response di WatchGuard è una potente raccolta di strumenti di difesa contro il malware avanzato in grado di correlare gli indicatori di minaccia dalle appliance Firebox e dagli Host Sensor per consentire una risposta in tempo reale e automatizzata allo scopo di fermare le minacce note, non note ed elusive.



Componenti chiave di TDR:

- ThreatSync. È un innovativo motore di correlazione delle minacce che raccoglie gli eventi di sicurezza dagli endpoint e dalla rete, mette in relazione i dati con i feed sulle minacce di terzi e assegna un punteggio alla minaccia da utilizzare come guida per la risposta automatizzata o manuale.
- Host Sensor. Host Sensor fornisce visibilità all'interno dell'endpoint e agevola la risposta a livello di endpoint nel momento in cui viene rilevata la minaccia. Host Sensor include anche il modulo Host Ransomware Prevention, che blocca l'esecuzione del ransomware su un endpoint prima che si verifichi la crittografia.
- APT Blocker. APT Blocker è un sandbox pluripremiato e di nuova generazione prodotto da Lastline in grado di eseguire un esame completo dei file che di norma richiederebbe un team di analisti della sicurezza esperti per osservare centinaia di migliaia di caratteristiche comportamentali e stabilire il possibile intento doloso. Integrato in TR, APT Blocker è lo strumento primario per assegnare la priorità alle minacce e consente di inoltrare i file per un'analisi più approfondita e di automatizzare gran parte del processo di prioritizzazione.
- WatchGuard Firebox. In TDR, l'appliance Firebox agisce come prima linea di difesa contro il malware in arrivo sulla rete, e allo stesso tempo come sensore di rete di fatto, in quanto acquisisce e invia i dati sugli eventi di sicurezza a ThreatSync affinché esegua la correlazione.

Correlazione e classificazione delle minacce con ThreatSync

ThreatSync raccoglie, mette in relazione e analizza i dati sugli eventi provenienti da Firebox, WatchGuard Host Sensor e dai feed di intelligence sulle minacce. I dati sugli eventi provenienti da altri servizi di sicurezza su Firebox, come APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus e WebBlocker, vengono inviati a ThreatSync, che li associa ai dati degli endpoint raccolti da Host Sensor.

ThreatSync analizza e classifica gli **indicatori** (ovvero i singoli eventi di rete e degli endpoint), quindi mette in relazione gli indicatori così da creare degli **incidenti**, al fine di fornire una classificazione completa della minaccia.

Modello di classificazione delle minacce WatchGuard:

- 8, 9, 10 Grave
- 6, 7 Alta
- 3, 4, 5 Sospetta
- 2 Potenziale
- 1 Corretta
- 0 Benigna

Gli eventi di rete e degli endpoint acquisiti per i quali ThreatSync determina una relazione ricevono automaticamente la classificazione di gravità maggiore, pari a 10.

Classificazione della minaccia e risposta automatica

ThreatSync garantisce visibilità sugli eventi che si verificano a livello di rete e di endpoint e assegna un punteggio completo e una classificazione alle minacce; in questo modo, i team IT individuano le minacce più pericolose, che richiedono attenzione immediata. L'assegnazione di priorità alle minacce consente alle organizzazioni di ridurre i tempi di rilevamento e correzione e di limitare il numero di risorse dedicate necessarie per rimuovere le minacce.

Con le policy abilitate, dopo aver stabilito la presenza di una minaccia, ThreatSync passa immediatamente alla fase di contenimento dell'host infettato, evitando che l'infezione si diffonda ad altre aree della rete. Questa funzionalità può rivelarsi di estrema importanza nella protezione degli ambienti dal caso del cosiddetto "paziente zero", che si ha quando gli endpoint infettati al di fuori della rete introducono il malware al loro rientro.

Dopo aver contenuto l'host, ThreatSync metterà in quarantena il file, eliminerà il processo o la persistenza della chiave di registro sull'endpoint; mostrerà inoltre l'evento di rete mitigato. Queste operazioni possono essere eseguite anche manualmente in un clic grazie alla nostra procedura di correzione.

Intelligence sulle minacce di livello enterprise

ThreatSync utilizza e analizza i feed di intelligence sulle minacce di livello enterprise per garantire che questi siano aggiornati con i più recenti indicatori di compromissione. Questi feed sulle minacce forniscono un elenco delle firme e degli indirizzi IP dei malware noti, gli hash MD5 dei file malware oppure gli URL o nomi di dominio dei server di comando e controllo (C&C) botnet. Questi elenchi possono avere un ruolo chiave nell'impedire alle nuove minacce di infiltrarsi nell'ambiente aziendale e raggiungere dati critici. Molti fornitori si occupano di redigere e gestire questi elenchi e ne consentono l'accesso ai clienti tramite tariffe elevate.
Threat Detection and Response estende le capacità dell'intelligence sulle minacce anche alle piccole e medie imprese. ThreatSync confronta i dati sugli eventi raccolti da Firebox e Host Sensor con i nostri feed sulle minacce, per stabilire rapidamente se la minaccia è già stata individuata altrove. Se la minaccia è inserita nei feed sulle minacce, il nostro strumento si mette all'opera insieme a Firebox e/o Host Sensor per rimuoverla.

Rilevamento del malware sull'endpoint: Host Sensor

Threat Detection and Response sfrutta varie forme di rilevamento attraverso WatchGuard Host Sensor per individuare le minacce malware avanzate.

- Firme: come accennato in precedenza, le firme sono una linea di difesa fondamentale nella lotta contro il malware. È importante avere un ricco arsenale di minacce note riconosciute. WatchGuard Threat Detection and Response utilizza i feed di intelligence sulle minacce di livello enterprise per verificare se un evento sospetto a livello dell'endpoint è in realtà una minaccia nota.
- Euristica : oltre alle firme, TDR utilizza l'euristica statica e dinamica (regole per la decisione) che indicano se un file o processo è sospetto. L'euristica statica o dei file tenta di determinare se un programma è sospetto esaminando la struttura e i contenuti del file in uno stato inattivo o previo all'esecuzione. L'euristica dinamica o di processo effettua una scansione di un processo in esecuzione alla ricerca di caratteristiche sospette associate al processo specifico. Queste due componenti lavorano insieme per identificare dei file apparentemente innocui che possono però rappresentare una potenziale minaccia. In molti casi, questo metodo di rilevamento è in grado di segnalare rapidamente una minaccia nuova o mai vista senza la necessità di eseguirla, oppure durante l'esecuzione di un processo ma prima che questo esegua un'azione. TDR sfrutta più di 175 fattori euristici attraverso WatchGuard Host Sensor.
- Analisi dei comportamenti: Poiché le minacce malware tendono ad avere determinati comportamenti, tenere traccia dei vari passaggi può rappresentare un sistema di rilevamento affidabile delle varianti del malware più complesse, polimorfiche, non viste in precedenza o elusive. Questa forma di rilevamento va oltre l'euristica dinamica in quanto non solo monitora le caratteristiche dei processi in esecuzione, ma identifica le azioni svolte da questi processi all'interno del file system. Alcune tra le azioni potrebbero essere l'impostazione della persistenza, della replica, dell'eliminazione strategica, dell'enumerazione del file system, della crittografia e molte altre ancora. Questa forma di rilevamento monitora la catena di comportamenti e aumenta il profilo di rischio man mano che questi mostrano delle intenzioni via via più dannose. Il nostro modulo Host Ransomware Prevention registra comportamenti solitamente associati agli attacchi ransomware per prevenire questi attacchi prima che la crittografia dei file abbia luogo.

Analisi della rete: WatchGuard Firebox

Per agevolare il loro attacco, i criminali informatici sfruttano diversi server e risorse esterni all'organizzazione target. Il malware avanzato, ad esempio, richiede spesso dei server di comando e controllo per ricevere comandi, far uscire le informazioni, richiedere le chiavi di crittografia e infettare i sistemi. A volte gli aggressori tengono traccia dei sistemi che sono riusciti a infettare e per questo progettano il malware in modo da mandare segnali o chiamate di "controllo" periodiche al fine di comandare e controllare i canali. Un'analisi del traffico di rete, inclusi i tentativi di comunicare con domini e indirizzi IP noti per essere associati a comportamenti dannosi, può fornire un'indicazione della presenza di una minaccia nell'ambiente.

Le appliance Firebox spingono l'attività di rilevamento ancora oltre e consentono a TDR di mettere in relazione i comportamenti di rete e gli eventi acquisiti dai servizi di sicurezza WatchGuard. In qualità di servizi di sicurezza di livello enterprise, APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus e WebBlocker sono progettati per la difesa contro le minacce più recenti, ma ognuno di essi può comunque fornire informazioni che potrebbero indicare la presenza di una minaccia. Gli eventi di sicurezza vengono acquisiti da ognuno di questi servizi di sicurezza e inviati a ThreatSync per la correlazione e la classificazione, al fine di fornire un quadro delle minacce più completo. Le connessioni dannose in uscita bloccate vengono messe in correlazione per rilevare l'endpoint e il processo che le ha iniziate, arrestando il processo stesso.

WebBlocker
Questo servizio fa riferimento a un database sul cloud contenente oltre 50 milioni di siti di tutto il mondo noti per essere dannosi, tra cui siti web in inglese, tedesco, spagnolo, francese, italiano, olandese, giapponese e cinese tradizionale e semplificato.

- **Evento di sicurezza:** collegamento a un sito contenuto in una categoria di contenuto bloccato.

Reputation Enabled Defense
RED identifica le minacce utilizzando una ricerca della reputazione che classifica gli URL come leciti, non leciti o sconosciuti. La ricerca viene fatta su un potente database basato su cloud che aggrega dati provenienti da diversi feed, tra cui alcuni motori antivirus leader del settore.

- **Evento di sicurezza**: tentata una connessione a un sito con una cattiva reputazione.
- **Evento di sicurezza:** tentata la comunicazione con un server di comando e controllo botnet.

Gateway Antivirus
Gateway AV esamina il traffico sui protocolli principali (HTTP, HTTPS, FTP, TCP, UDP, SMTP e POP3) utilizzando l'euristica e le firme continuamente aggiornate al fine di rilevare e bloccare qualsiasi tipo di malware.

- **Evento di sicurezza**: Gateway AntiVirus ha rilevato un virus all'interno del traffico web.
- **Evento di sicurezza:** Gateway AntiVirus ha rilevato un virus all'interno del traffico e-mail.

IntelligentAV
IntelligentAV sfrutta l'intelligenza artificiale (IA) per la difesa contro i malware zero-day in costante evoluzione. Mentre le soluzioni AV basate su firme riescono a rilevare solo le minacce note, IntelligentAV è in grado di prevedere i trend delle minacce e di apprendere dagli attacchi attivi perpetrati contro la rete.

- **Evento di sicurezza:** IntelligentAV ha rilevato un virus all'interno del traffico web.
- **Evento di sicurezza:** IntelligentAV ha rilevato un virus nel traffico e-mail.

APT Blocker
Si focalizza sull'analisi dei comportamenti per determinare se un file è dannoso. APT Blocker identifica e inoltra i file sospetti a una sandbox di nuova generazione basata su cloud, un ambiente virtuale in cui il codice viene analizzato, emulato e infine eseguito per determinarne il potenziale di minaccia.

- **Evento di sicurezza:** APT Blocker rileva e blocca una minaccia nel traffico web.
- **Evento di sicurezza:** APT Blocker rileva e blocca una minaccia nelle comunicazioni e-mail.

Triage delle minacce potenziato da IA con APT Blocker

Se da un lato, le classificazioni delle minacce rappresentano una guida potente nella gestione delle minacce, dall'altro, la natura in continua evoluzione del malware implica che gli indicatori classificati come sospetti potrebbero rappresentare dei segnali di avviso precoce di malware ancora da identificare. Grazie alla perfetta integrazione con WatchGuard APT Blocker, i file sospetti possono essere inviati a una sandbox di nuova generazione nel cloud per un'analisi approfondita e una nuova classificazione. Sfruttando l'IA, ThreatSync viene costantemente addestrato per affrontare migliaia di file, dannosi e non. La soluzione riesce così ad assegnare in modo più accurato i punteggi alle minacce, ad automatizzare la classificazione di file sospetti e a determinare quelli da inviare ad APT Blocker. APT Blocker invia automaticamente i risultati a ThreatSync, per la correzione automatica.

APT Blocker utilizza l'emulazione completa del sistema (CPU e memoria) per acquisire una visione dettagliata dell'esecuzione di un programma malware. Dopo la prima esecuzione attraverso altri servizi di sicurezza come antivirus gateway e prevenzione delle intrusioni, i file vengono catalogati e confrontati con un database esistente. Se il file non è mai stato visto in precedenza, viene analizzato con l'emulatore di sistema, che monitora l'esecuzione di tutte le istruzioni.

APT Blocker analizza tutto ciò che il malware fa, dalle istruzioni della CPU e le connessioni di rete richieste, ai file, alla memoria e ai dispositivi ai quali il malware accede. APT Blocker è anche in grado di rilevare le tecniche di elusione che altre sandbox non colgono, inclusi i ritardi di temporizzazione, l'attesa delle azioni utente, le azioni dannose dell'OS, la crittografia delle comunicazioni all'infrastruttura C&C e la frammentazione di file che vengono eseguiti solo se riassemblati.

In ATP Blocker i file vengono attivamente monitorati sull'endpoint di destinazione, mentre viene portata a terminel'analisi. Se il file è dannoso, ThreatSync lo identifica subito su tutti gli endpoint protetti e avvia la correzione.

Conclusioni

Questo White Paper descrive le capacità della piattaforma Threat Detection And Response nel rilevare, verificare e rispondere alle minacce note, non note ed elusive che potrebbero avere un impatto sulle organizzazioni. Dopo la lettura di questo documento, il lettore avrà acquisito le seguenti conoscenze su TDR:

- TDR rileva il malware noto, non noto ed elusivo non rilevato dalla maggior parte dei prodotti antivirus, grazie a sensori posti sia sugli endpoint che sulla rete.
- TDR non solo individua il malware non rilevato dalle tecnologie di sicurezza esistenti, ma reagisce tempestivamente per contenere l'infezione e rimuovere le minacce.
- La correlazione dei sensori di rete e degli endpoint TDR si unisce ai feed di intelligence sulle minacce di terzi per fornire maggiori capacità di visibilità e verifica delle minacce.
- ThreatSync riduce i falsi positivi tramite l'analisi e la classificazione aggregata delle minacce.
- TDR fornisce una risposta più rapida e più efficiente alle minacce tramite correzioni automatizzate basate sulle policy, le azioni mirate a un singolo processo malware e le azioni di correzione in massa.
- L'elevata integrazione con APT Blocker consente di effettuare un triage delle minacce avanzate e un'analisi profonda dei file sospetti.
- ThreatSync offre email di alert configurabili per incidenti e indicatori rilevati e per le minacce risolte sulla rete e sugli endpoint

Per saperne di più, è possibile visitare www.watchguard.com/tdr

Informazioni su WatchGuard

WatchGuard® Technologies, Inc. è un leader globale nel settore della sicurezza di rete e offre i migliori prodotti e servizi per la tecnologia UTM (gestione unificata delle minacce), i firewall di nuova generazione, il Wi-Fi protetto e l'intelligence di rete, con più di 80.000 clienti in tutto il mondo. La missione della società è di rendere la sicurezza di livello enterprise accessibile ad aziende di tutti i tipi e dimensioni attraverso la semplicità, facendo di WatchGuard la soluzione ideale per le aziende distribuite e le piccole e medie imprese. La sede centrale di WatchGuard si trova a Seattle (stato di Washington, negli Stati Uniti); l'azienda dispone di uffici dislocati in Nord America, Europa, Asia Pacifico e America Latina. Per saperne di più, è possibile visitare WatchGuard.it.

Numero verde Italia: 800-911.938 VENDITE INTERNAZIONALI: +1.206.613.0895 WEB: www.watchguard.it