

IL SANDBOXING NELLA LOTTA ALLE APT

**con un focus sulla soluzione FortiSandbox
e l'APT protection framework di Fortinet**



Note sull'autore

Gaetano Di Blasio è giornalista professionista dal 1997. Da oltre 25 anni segue il settore dell'ICT. Attualmente è Direttore

Responsabile delle riviste SOLUTIONS e SECURITY & BUSINESS di Reportec, di cui è socio e cofondatore

Avvertenze

Pubblicato nel 2015

Tutti i marchi contenuti in questo white paper sono registrati e di proprietà delle relative società. Tutti i diritti sono riservati. Va notato che le informazioni contenute possono cambiare senza preavviso; le informazioni contenute sono reputate essere corrette e affidabili anche se non sono garantite. La descrizione delle tecnologie non implica un suggerimento all'uso dell'una o dell'altra così come il parere espresso su alcuni argomenti da parte di Reportec è puramente personale. La vastità dell'argomento affrontato e la sua rapida evoluzione possono avere portato a inaccuratezze di cui Reportec non si ritiene responsabile, pur avendo espletato i possibili controlli sulla correttezza delle informazioni medesime; il white paper non rappresenta una presa di posizione a favore di una o l'altra delle tecnologie, standard o prodotti ivi riportati né garantisce che le architetture, apparati, prodotti hardware e software siano stati personalmente verificati nelle funzionalità espresse; le descrizioni delle architetture, delle piattaforme, dei servizi e dei dati aziendali sono stati elaborati in base alle informazioni fornite dalle aziende, con le quali gli stessi sono stati analizzati e ridiscussi.

Copyright Reportec – 2015

www.reportec.it

IL SANDBOXING NELLA LOTTA ALLE APT

CON UN FOCUS SULLA SOLUZIONE
FORTISANDBOX
E L'APT PROTECTION FRAMEWORK DI FORTINET

Executive Summary

Sandbox o non sandbox? Dopo alcuni casi in cui il sandboxing non è stato efficace, gli esperti di sicurezza si stanno interrogando sull'utilità di questa soluzione nella lotta agli attacchi mirati. Il punto è che non tutte le sandbox sono uguali.

La questione è importante perché tutti i più recenti report sull'evoluzione delle minacce alla sicurezza informatica, compresi quelli focalizzati sull'Italia, testimoniano la crescita delle minacce avanzate (APT) o mirate.

Più che di singole minacce, si tratta di una tipologia d'attacco molto sofisticato, rivolto a una specifica azienda o, talvolta, a una categoria di imprese. L'attacco consiste in più fasi, per le quali vengono impiegate tecniche miste e anche strumenti adattativi.

Gli attacchi APT sono anche quelli che causano i danni maggiori, del resto richiedono al cyber criminale una cura e uno sforzo che in qualche modo deve essere ripagato.

Occorre, pertanto, un sistema di difesa che sia in grado di fronteggiare l'attacco nelle sue diverse fasi ma, soprattutto, che integri le analisi eseguite in ciascuna di queste ultime mettendo a frutto le soluzioni di intelligence e che sappia smascherare le tecniche di elusione con cui l'attaccante arriva al cuore del sistema aziendale.

Nella lotta alle APT si è rivelato fondamentale l'uso del sandboxing, in particolare in combinazione o all'interno di sistemi per l'intrusion prevention o il firewalling di nuova generazione.

Ben presto, però, il cyber crime è "corso ai ripari", ideando sistemi maligni in grado di ingannare le soluzioni sandbox, tanto da far ritenere che queste fossero insufficienti se non addirittura inutili.

In questo white paper si analizzano le caratteristiche degli attacchi di tipo mirato e i sistemi per contrastarli, concentrandosi in particolare sulle soluzioni di sandboxing, poiché non tutte sono uguali, e sul loro ruolo nella lotta agli APT.

Un focus specifico è dedicato al framework di protezione sviluppato da Fortinet e alla soluzione FortiSandbox di Fortinet.

Sommario

Lo scenario della cyber security war

La lotta agli APT e il ruolo del sandboxing

Il framework di protezione proposto da Fortinet

La soluzione FortiSandbox

Lo scenario della Cyber Security War

La storia della sicurezza informatica è storicamente una rincorsa tra gli hacker "black hat", i cattivi che ideano e usano una minaccia, cioè un sistema per violare l'infrastruttura di qualche organizzazione, e gli hacker "white hat", i buoni che trovano e sviluppano una soluzione che protegge i sistemi informatici da quella minaccia.

In questa ricorsa i buoni sembrano destinati a perdere, perché i cattivi sono più bravi a condividere le informazioni e perché guadagnando più soldi hanno potenzialmente più risorse da investire. Ai white hat non resta che rimboccarsi le maniche per escogitare sistemi sempre più efficaci. Una soluzione preziosa si è rivelato il sandboxing, che recentemente è stato messo sotto accusa dopo che diversi attacchi ne hanno messo in mostra i limiti. Ancora una volta, i buoni realizzano un sistema di protezione e i cattivi trovano il sistema di bypassarlo.

Nella realtà, però, le soluzioni di sandboxing non sono tutte uguali ed efficaci al medesimo modo. Il concetto stesso di sandboxing non si concretizza in una soluzione, ma in un sistema strutturato e integrato di soluzioni e funzionalità di protezione: quello che in inglese viene chiamato framework.

In questo white paper analizzeremo il ruolo fondamentale del sandboxing nella lotta agli attacchi APT (Advanced Persistent Threats) e approfondiremo le caratteristiche della soluzione FortiSandbox di Fortinet, che appunto si colloca all'interno dell'APT Framework proposto dalla multinazionale statunitense.

Da un punto di vista semantico la locuzione "Advanced Persistent Threats" non è correttamente esplicativa, in quanto non si tratta di "minacce", che come prima descritto sono universalmente considerati, cioè sistemi per violare l'infrastruttura di qualche organizzazione.

Più precisamente, si tratta di una tipologia di attacchi. Gli aggettivi "advanced" e "persistent" indicano le caratteristiche principali di tali: l'uso di tecniche sofisticate, la combinazione delle stesse in una strategia basata su più fasi e la tenacia con cui questa viene applicata con continuità fino all'ottenimento dell'obiettivo e oltre. Oltre, perché in casi come lo spionaggio, il malware è progettato per annidarsi e continuare a spiare anche per anni, finché non viene scoperto.

Recentemente, per esempio, sono stati trovati malware che "spiavano" enti governativi e aziende statunitensi, probabilmente di origine russa (un sospetto dovuto alla presenza di caratteri cirillici in alcune stringhe di testo incluse nel codice), come pure sistemi americani che spiavano i partner francesi.

Sarebbe dunque più corretto parlare di "attacchi mirati". Nella realtà, però, l'obiettivo può essere una singola organizzazione, ma anche una categoria di aziende o istituzioni. In questo caso, l'attacco è su larga scala e, secondo taluni, è improprio considerarlo mirato. Per non scendere nei dettagli cercando distinzioni, in letteratura si è affermato il termine APT che useremo in seguito.

Gli APT crescono e richiedono attenzione

Negli anni si è assistito a un costante aumento delle minacce, ma, cosa ancora più grave, a un continuo "miglioramento" delle stesse: in altre parole, sono sempre più sofisticate e difficili da rilevare. Soprattutto: sono più dannose e cattive. Meno poetiche anche: nel 2000 il worm "I Love You" era stato progettato per intasare i POP e riempire i server di file. In pratica, il suo unico scopo era quello di propagarsi il più rapidamente possibile. Fu stabilito un record da battere: effettuare il giro del mondo il più rapidamente possibile. Creò certamente danni e fermi del servizio Internet e di molte intranet interne alle aziende, ma i danni economici furono relativamente contenuti e indiretti.

All'inizio del 2015, lo stesso worm, con piccole ma ingannevoli modifiche, è stato utilizzato per condurre un nuovo tipo di attacco. Questo dà l'idea della complessità del problema: su Internet circolano fantastiliardi di codici conosciuti e sconosciuti: riuscire a filtrarli non è possibile semplicemente con le tecniche di analisi utilizzate dai sistemi tradizionali. Soprattutto non è semplice catalogare un codice senza analizzarlo a fondo, ma la maggior parte del software che attraversa la rete è sconosciuto e non può essere bloccato semplicemente per questo.



Il codice sulla rete passa senza soluzione di continuità dal lecito all'illecito e quest'ultimo può assumere una natura dannosa (fonte Fortinet)

Tutti i rapporti sulla sicurezza, compresi il recente Rapporto OAI (Osservatorio Attacchi Informatici) 2015, che considera esclusivamente gli attacchi verificatisi in Italia, e il Rapporto Clusit 2015, concordano su un dato: gli attacchi APT aumentano e sono quelli che determinano i danni maggiori per le organizzazioni colpite.

Tutte le metodologie di attacco hanno registrato un incremento, secondo il Rapporto OAI, ma quello maggiore è proprio relativo agli attacchi APT (dati congruenti con quelli della Polizia Postale diffusi dal Cnaipic). Proprio in Italia, tra il 2013 e il 2014, risulta il tipo di attacco più aumentato dopo il ramsonware, che l'anno scorso ha visto un boom ovunque nel mondo.

Secondo i rispondenti al questionario OAI, però, le frodi informatiche sono considerate la principale motivazione per gli attacchi futuri, ma, contemporaneamente, sono anche il tipo di attacco meno temuto (preoccupa solo il 13% dei rispondenti). Mentre fanno più paura il social engineering e il furto dei dati dai dispositivi mobili, probabilmente perché sono stati sperimentati quali gli attacchi con gli impatti maggiori.

Il fatto è che gli attacchi denunciati in Italia sono molto pochi. Lo confermano anche i rilevamenti del Rapporto Clusit: mentre nel mondo si sono registrati diversi attacchi considerati gravissimi, nel nostro Paese questi sono stati solo l'1%. Un dato che statisticamente si discosta in maniera eccessiva dal resto del mondo, troppo per essere spiegato solo con la presenza di poche grandi imprese, anche perché all'estero sono anche le medie e piccole organizzazioni a essere colpite.

È opinione degli analisti che permane la tendenza a non denunciare gli attacchi e anche, purtroppo, che molte aziende non si accorgano nemmeno di essere attaccate. Lo conferma indirettamente la rilevazione effettuata sulla

rete di Fastweb, pure inclusa nel rapporto.

Gli esperti del Clusit, inoltre, hanno verificato sul campo che esistono sistemi "in ascolto" sulla rete, pronti a tentare un attacco non appena viene installato un nuovo dispositivo o aggiornato un firmware, per esempio di un router. Quindi, chiunque è online, prima o poi sarà attaccato.

La lotta agli APT e il ruolo del sandboxing

Come accennato, gli attacchi APT combinano diverse tecniche che vengono utilizzate per scopi diversi secondo un approccio in fasi successive: cinque, secondo alcune classificazioni, sei o sette per altre. Non c'è uniformità perché alcune di queste fasi possono mancare o, più spesso, essere accorpate in un'unica azione a seconda dei casi. La sostanza non cambia: ci sono fasi preparatorie, operazioni tese a penetrare il sistema, mosse per prenderne il controllo e l'attacco finale con il raggiungimento dell'obiettivo.

Le sette fasi di un attacco APT sono:

1. Ricognizione: una fase di studio in cui si raccolgono dati, anche sfruttando social media o il social engineering. Le informazioni saranno utili per arrivare a impossessarsi di credenziali lecite con cui entrare nel sistema.
2. Adescamento: Tipicamente attraverso una mail di spear phishing ben confezionata, grazie alle informazioni raccolte nella ricognizione, viene indotto un utente dell'organizzazione target a cliccare su un link verso un sito su cui è annidato un codice maligno.
3. Reindirizzamento: Il codice maligno in questione è un exploit kit che viene installato sulla rete target per consentire al cyber criminale di penetrare nel sistema.
4. Exploit: La fase centrale fondamentale per l'attacco vero e proprio, durante la quale sarà installato il malware che dovrà fornire il controllo all'attaccante al fine di estrarre i dati o compiere la violazione programmata.
5. Installazione: viene installato il sistema, per esempio un Command & Control, che consente di raccogliere i dati cercati o avviare una specifica azione, magari di sabotaggio. È qui che si concentrano i

cosiddetti sistemi di protezione perimetrale, analizzando ogni file che penetra nella rete per rilevare eventuale malware. Ma non è facile farlo tradizionalmente attraverso signature e pattern noti.

6. Call Back: Ottenuto il controllo, il cyber criminale cercherà di raggiungere l'obiettivo prefissato, in genere contattando un server remoto (una cosiddetta chiamata di call back) e attivando il download di strumenti e altro codice maligno per raccogliere e inviare informazioni sul sistema violato, al fine di proseguire al suo interno fino all'obiettivo finale.
7. Chiusura dell'attacco: Il cyber criminale ha terminato e conclude l'attacco.



Le 7 fasi di un attacco APT

La fase di ricognizione e adescamento vengono spesso considerate un tutt'uno, così come quella di call back e di chiusura dell'attacco, ma aldilà di quante fasi si conteggino, l'importante è sapere che in ciascuna di esse è possibile prevenire e proteggere la rete dell'organizzazione dall'attacco. È necessario che il sistema di sicurezza possa intervenire in qualsiasi momento, perché ogni fase può contenere un punto debole dell'attacco, sfruttando il quale impedire la violazione.

Per esempio, la mail di spear phishing potrebbe essere bloccata da una soluzione antispam e/o antiphishing. Il reindirizzamento dovrebbe essere bloccato da una soluzione di Web Filtering. L'exploit deve superare il sistema di intrusion prevention. L'antimalware potrebbe impedire l'installazione del codice maligno e, infine, tutta l'attività di raccolta dei dati e di estrazione degli stessi, nella fase di call back, dovrebbe essere rilevata

dalle soluzioni di application control, IP reputation, antibiot e così via.

Le singole soluzioni non sempre sono in grado di intervenire perché i cyber criminali conoscono molto bene le loro caratteristiche e adattano le caratteristiche del codice utilizzato ai sistemi di sicurezza in uso attraverso tecniche di elusione e mascheramento, alle volte anche banali: per esempio, conoscendo la stringa di caratteri che viene utilizzata in una signature per riconoscere un determinato malware, può bastare modificare un carattere in tale stringa.

Il ruolo del sandboxing

Per aumentare la capacità di rilevare la minaccia potenzialmente contenuta in un codice, in particolare se sconosciuto, si è ricorsi a una soluzione in uso da molti anni, ma per scopi diversi: il sandboxing.

La sandbox, letteralmente scatola di sabbia (ma nell'inglese statunitense l'immagine richiamata alla mente è quella del quadrato di sabbia in cui giocano i bambini più piccoli nei giardini, tipicamente pubblici), è un ambiente isolato che da tempo è utilizzato per le fasi di test, per esempio nello sviluppo del software. In questo ambiente viene relegato il codice e ne viene "simulato" il funzionamento. In pratica, viene eseguito in un ambiente chiuso, verificandone il comportamento. Se rivela una propensione maligna ne sarà impedita la divulgazione all'interno del sistema e saranno anche tratte quante più informazioni possibili per consentire ai sistemi di protezione di rilevarlo immediatamente, se dovesse ripresentarsi.

Sempre più spesso, inoltre, il codice viene annidato in file non eseguibili, pertanto è stato esteso l'uso delle sandbox per l'esecuzione di dati applicativi, come file di Adobe Flash e JavaScript, che possono contenere codice dannoso occulto. Alcune applicazioni, come Adobe Reader X, dispongono di una propria sandbox integrata destinata alle stesse funzioni di sicurezza. Se Reader X rileva, per esempio, codice dannoso quando apre un PDF, lo blocca in una sandbox per impedirgli di infettare il sistema operativo.

Il sandboxing appare dunque una soluzione relativamente semplice, efficace e definitiva, ma i black hat hanno subito cominciato a prendere le contromisure e a ideare codici dal comportamento apparentemente innocuo. Per esempio, introducendo un ritardo temporale, tale per cui una certa azione sarebbe stata eseguita solo dopo un relativamente lungo lasso di tempo. Le analisi, infatti, devono essere rapide, perché non è funzionale

bloccare un codice legittimo per ore o addirittura giorni.

Per accelerare le analisi e al tempo stesso evitare alcune tecniche di elusione, sono stati sistemi di intelligence che utilizzano gli analytics e, con l'aiuto del Cloud è stato possibile realizzare soluzioni di "intelligence", che consentono di diffondere rapidamente il maggior numero di informazioni possibili, in modo da effettuare il giro del mondo per aiutare i sistemi di sicurezza ad attivare nuove misure di sicurezza. In altre parole, sistemi SIEM (Security Information Event Manager) intelligenti sono in grado di identificare minacce, perché magari artefici di attacchi in una parte del Globo e propagare in tempo reale informazioni per evitare che abbiamo effetto dall'altro lato del Pianeta.

Queste soluzioni di intelligence vengono altresì alimentate dalle informazioni raccolte nelle analisi realizzate nelle diverse sandbox, che rimangono essenziali.

I cyber criminali hanno dunque affinato le tecniche di elusione: i codici maligni arrivano anche ad accorgersi di essere in una sandbox, disattivando la componente dannosa, ottenendo magari una buona reputazione che consentirà a una sua copia di agire indisturbata in futuro.

Tra le tecniche di elusione più diffuse si trovano: le logic bomb, per esempio le time bomb già citate, in cui la componente di codice dannosa resta occulta fino al giorno e ora prefissati; rootkit e bootkit che riescono talvolta a compromettere il sistema prima che la sandbox riesca a rilevarli; dropper, un file pulito che rimanda a un URL o a un indirizzo IP, da cui viene scaricato una routine maligna, per cui non viene rilevato se la sandbox non è in grado di attivare una funzione di Web filtering; Fast Flux, algoritmi di generazione di domini per modificare l'URL o l'indirizzo IP a cui si connette un virus; archivi crittografati che rendono il malware illeggibile; binary packer, che nascondono il malware crittografandolo in porzioni di codice alterate, le quali vengono scompattate al momento dell'esecuzione, peraltro, nel caso di JavaScript e ActionScript, questa metodologia può essere legittimamente adoperata per tutelarsi dalle copie contraffatte; malware polimorfico che cambia a ogni esecuzione.

Ce ne sono altre, molte delle quali in sviluppo in questo momento. Ma c'è soprattutto un altro problema implicito nella tecnica del sandboxing, che in teoria dovrebbe produrre un output identico a quello prodotto dal codice quando viene eseguito nell'ambiente reale dell'utente, ma in pratica ci sono troppe variabili in gioco, a cominciare dalle diverse versioni di sistema

operativo e di aggiornamento installato sui vari client che potrebbero trovarsi a eseguire il codice. Per questo è difficile che i risultati coincidano. Tutte queste problematiche hanno portato taluni a considerare inutile questo tipo di analisi, ma non si può fare di tutta un'erba un fascio: non tutte le soluzioni di sandboxing sono uguali.

Il framework ATP di Fortinet

Alla complessità delle minacce implicite in un attacco di tipo ATP occorre rispondere con un approccio concettualmente semplice ma efficace. Per questo gli esperti di Fortinet hanno sviluppato un framework basato su tre azioni: prevenzione, rilevamento, attenuazione.

Una metodologia di difesa complessa rischia di essere troppo lenta e poco preventiva. Il framework semplice comprende una serie di strumenti sia avanzati sia tradizionali per la sicurezza di reti, applicazioni ed endpoint, il rilevamento delle minacce e l'attenuazione dei rischi. Questi strumenti si basano su approfondite analisi sottostanti e sfruttano servizi di intelligence delle minacce capaci di trasformare le informazioni provenienti da molteplici fonti in efficaci misure di protezione. Sebbene gli elementi del framework (e anche le tecnologie integrate) possano operare isolatamente, la protezione risulta ulteriormente solida attuando una strategia di sicurezza olistica.

L'elemento di prevenzione agisce sulle minacce note, che devono essere bloccate immediatamente, ove possibile con l'impiego di firewall di nuova generazione, Secure Email Gateway, sistemi di Endpoint Security e soluzioni analoghe, quali, per esempio, anti-malware, web filtering, intrusion prevention e così via. Sono strumenti consolidati e ancora molto efficaci nel bloccare tutta una serie di minacce con un impatto minimo sulle prestazioni della rete. La tecnologia anti-malware può, per esempio, rilevare e bloccare virus, botnet e anche varianti previste di malware con l'ausilio di risorse quali il linguaggio CPRL (Compact Pattern Recognition Language) brevettato di Fortinet.

Utili anche alcuni accorgimenti strategici, come ridurre i punti di ingresso, diminuendo così la superficie di esposizione.

Da non dimenticare anche il controllo degli accessi e l'implementazione di

VPN, che sono un aspetto importante della prima linea di difesa dagli attacchi mirati.

L'elemento di rilevamento si occupa del traffico che non viene fermato al primo livello e che contiene evidentemente minacce sconosciute. Vengono quindi impiegate avanzate tecnologie di rilevamento delle minacce per esaminare più da vicino il comportamento del traffico di rete, degli utenti e dei contenuti, al fine di identificare attacchi nuovi e originali.

Tra queste il sandboxing, che, però, richiede molte risorse e rischia di rallentare il traffico, per cui viene utilizzato solo per le minacce che non possono essere identificate con metodi tradizionali più efficienti, tra cui il rilevamento botnet e le misure di reputation.

Il terzo elemento dell'APT framework di Fortinet, l'attenuazione si attua una volta identificati potenziali incidenti e nuove minacce in fase di rilevamento. In risposta agli incidenti, le imprese devono provvedere immediatamente alla convalida dei dati e attenuare i danni. Utenti, dispositivi e/o contenuti vanno messi in quarantena, con l'impiego di sistemi automatici o manuali, per tutelare le risorse di rete e i dati aziendali.



L'APT Framework di Fortinet

Il rilevamento delle minacce attiva anche un altro passaggio essenziale,

ovvero il trasferimento, l'handoff, delle informazioni ricavate ai gruppi di ricerca e sviluppo. Possono ora essere realizzate tattiche di protezione. Le minacce prima ignote possono essere analizzate a fondo, per produrre correzioni che tengano conto di tutti i livelli di sicurezza, assicurando a ognuno di essi il giusto insieme di protezioni aggiornate.

In questa fase, l'eliminazione della ridondanza e la creazione di una sinergia tra le diverse tecnologie di sicurezza sono essenziali per implementare una soluzione di protezione della massima efficacia, in cui l'ignoto assuma connotati riconoscibili.

Ovviamente il ciclo non si chiude fino a quando queste informazioni fruibili sulle minacce non vengono messe a disposizione dei diversi punti di applicazione e condivise a livello globale, in modo da rafforzare la prima fase di prevenzione.

Questo handoff è il tassello che purtroppo ancora manca in molte organizzazioni, mentre il trasferimento e la condivisione delle informazioni è la funzione più importante di un framework di protezione dalle minacce.

Non si tratta di tecnologia, ma di strategia: gli attacchi APT si avvalgono di molte tecnologie, diffondendo informazioni su di esse si aumenta la conoscenza delle minacce, incrementando la possibilità di fermare gli attacchi nella fase preventiva.

I tre elementi del framework devono comunicare, perché l'efficacia complessiva dell'ambiente si misura sulla capacità con cui i vari ruoli comunicano tra loro senza interruzioni, trasferendo i dati da un livello all'altro: dalla fase di prevenzione i dati ad alto rischio passano alla fase di rilevamento, mentre le minacce prima ignote vengono trasferite alla fase di analisi e attenuazione.

Le funzioni di intelligence e protezione aggiornata di quest'ultima fase ritrasferiscono quindi i dati ai prodotti operativi nelle prime due fasi, in un ciclo costante che aumenta la sicurezza e rende più efficiente il rilevamento di attacchi sempre più sofisticati.

L'applicazione del framework con le soluzioni Fortinet

Uno dei principali punti di forza di Fortinet è la sinergia tra il software proprietario, le appliance ad alte prestazioni e il team di ricerca di FortiGuard Labs. I ricercatori di FortiGuard Labs, infatti, costituiscono un centro di intelligence che assicura la fluida interazione dei tre elementi. Studiano le minacce prima sconosciute, sviluppano strategie di correzione

complete, concepite dall'inizio alla fine per garantire prestazioni estreme e massima protezione, e forniscono informazioni di sicurezza mirate a potenziare la prevenzione e il rilevamento nel tempo.

FortiGuard Labs sfrutta informazioni in tempo reale sul panorama delle minacce per offrire aggiornamenti completi per l'intera gamma di soluzioni e tecnologie base Fortinet, a scopo di protezione sinergica. Quando emerge una nuova minaccia, la divisione Global Operations di FortiGuard Labs, disponibile 24 ore su 24, 365 giorni all'anno, effettua il push in tempo reale di informazioni di sicurezza aggiornate nelle soluzioni Fortinet, per una protezione istantanea da pericoli sempre in agguato.

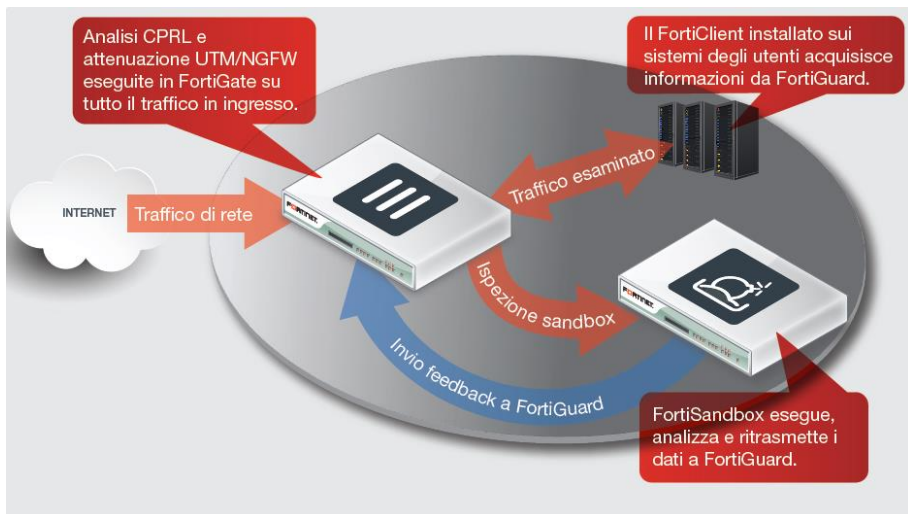
L'handoff dall'Elemento 3 ai primi due elementi, dove si completa di volta in volta il ciclo di protezione dalle minacce avanzate, avviene quando le informazioni sulle minacce acquisite da FortiGuard Labs vengono passate a tutti gli utenti delle soluzioni Fortinet tramite la rete di distribuzione globale di Fortinet. Ma l'azione di Fortinet non finisce qui. Nell'ambito della Cyber Threat Alliance e di altre iniziative correlate, le informazioni raccolte vengono infatti passate a un più ampio gruppo di ricercatori, per estendere ulteriormente la portata del lavoro e arricchire le conoscenze sulle minacce acquisite per ogni organizzazione con l'ausilio del framework.

Le soluzioni Fortinet integrate comprendono i firewall FortiGate di nuova generazione, i Secure Email Gateway FortiMail, gli Endpoint Security FortiClient, i sistemi FortiSandbox e altri prodotti di un ampio ecosistema. Ci soffermiamo su FortiSandbox.

La soluzione FortiSandbox

FortiSandbox supporta l'ispezione di numerosi protocolli in una sola soluzione unificata, semplificando così l'infrastruttura e le operazioni di rete. Si integra con FortiGate e altri prodotti Fortinet che sono progettati per attenuare le minacce avanzate fungendo da prima linea di difesa sul perimetro esterno e al centro della rete. Di fatto, FortiSandbox è un'estensione della soluzione UTM/NGFW di Fortinet e provvede a ritrasmettere le informazioni raccolte a FortiGate e/o FortiGuard. In questo modo, nuovi eventi di attacco generati da minacce scoperte da FortiSandbox possono essere bloccati all'altezza della prima linea di difesa, quando il ciclo di vita prosegue.

La società di analisi e ricerca indipendente specializzata in sicurezza, NSS, ha valutato e raccomandato la soluzione FortiSanbox, sottolineandone le caratteristiche principali che sono: ambiente di runtime virtuale sicuro in cui esporre le minacce sconosciute; esclusivi filtri preliminari multilivello per operazioni veloci ed efficaci di rilevamento delle minacce Accurati report per la visibilità dell'intero ciclo di vita delle minacce; ispezione di molti protocolli in una sola appliance, per semplificare la distribuzione e ridurre i costi; integrazione con FortiGate, per potenziare, senza duplicare, l'infrastruttura di sicurezza; convalida di sicurezza con l'ausilio dei test BDS (Breach Detection System) di NSS.



L'analisi con FortiSandBox

Una delle problematiche riscontrate nelle soluzioni di sandboxing riguarda i sistemi operativi supportati. L'ideale è supportarli tutti, ma nella pratica si tratta di un insostenibile impiego di risorse.

Presso Fortinet hanno scelto un approccio più efficace, valutando con attenzione lo scenario reale di utilizzo più diffuso. Per questo, FortiSanbox assegna risorse ad ambienti virtuali Windows XP e Windows 7/8 sulla base del panorama attuale dei rischi.

Quasi tutte le minacce osservate da FortiGuard Labs sono a 32 bit e sono scritte per l'esecuzione in ambienti Windows XP. Secondo l'opinione degli esperti di Fortinet, Windows XP è un mercato ancora attivo e un facile bersaglio. Fino a quando gli sviluppatori potranno creare malware a 32 bit

che funziona su XP oggi e funzionerà su Windows 7/8 dopo la migrazione, non ci sarà alcun motivo per progettare malware appositamente pensato per Windows 7/8. Sebbene FortiGuard Labs non preveda un assalto a breve termine di minacce a 64 bit, Fortinet è già pronta ad affrontare entrambi i tipi di attacchi con l'azione sinergica del linguaggio CPRL, del motore antivirus e di FortiSandbox.

In ogni caso, quando il panorama dovesse cambiare, assicurano dai FortiGuard Labs, cambieranno anche gli ambienti supportati. In FortiGate e FortiSandbox vengono immediatamente integrati tutti i miglioramenti apportati al rilevamento di nuove tecnologie di evasione e piattaforme bersaglio. FortiSandbox supporta anche il rilevamento indipendente dal sistema operativo con emulazione di codice e prefiltra del motore antivirus.

Un'analisi multilivello con il supporto del linguaggio CPRL

Un primo elemento differenziante, quindi, è la velocità d'esecuzione, che tiene conto della classificazione del codice sulla base del grado di diffusione del malware nelle diverse configurazioni. In questo modo FortiSandbox stabilisce priorità tra i processi di valutazione per velocizzare l'identificazione di codice dannoso.

Tra gli elementi differenzianti di FortiSandbox va segnalata l'analisi multilivello, non solo attuata nell'ambito dell'integrazione con le altre soluzioni Fortinet.

Le difese in uso possono essere potenziate con funzionalità all'avanguardia, per analizzare file sospetti e ad alto rischio in un ambiente controllato e svelare l'intero ciclo di vita di un attacco con il rilevamento dell'attività del sistema e dei callback. Inoltre, va evidenziato che: un motore antivirus applica funzioni di scansione antivirus di primo livello; tramite cloud verifica in tempo reale le informazioni sui malware e accede a informazioni condivise per il rilevamento istantaneo di malware; l'emulazione avviene in un ambiente virtuale di runtime sicuro per l'analisi e la classificazione del comportamento.

Tra le tecnologie proprietarie che differenziano FortiSandbox, una menzione particolare spetta al linguaggio brevettato CPRL (Compact Pattern Recognition Language), sviluppato da FortiGuard Labs per l'esecuzione di ispezioni accurate sul codice.

Secondo i dati forniti dal costruttore, questo linguaggio è in grado di

identificare più di 50mila mascheramenti impiegati dai codici maligni noti. Quindi, se il codice da analizzare utilizza una tecnica di evasione nota, la tecnologia CPRL può rilevarla e consentire a FortiGate di identificare il codice senza inviarlo alla sandbox.

Questo prezioso passaggio incrementa le prestazioni destinando le risorse della sandbox all'elaborazione del solo codice sconosciuto.

Per migliorare il rilevamento delle minacce più sofisticate, inoltre, Fortinet ha integrato in FortiSandbox le avanzate tecniche di analisi di FortiGuard Labs, che sono riuscite a individuare il 99% delle violazioni, identificando la maggioranza di esse in meno di un minuto, come attestato nel rapporto sui BDS (Breach Detection System) di NSS Labs del 2014.

FortiSandbox è disponibile in tre diverse opzioni di distribuzione, per rispondere a diverse esigenze ed è possibile adottarle anche tutte contemporaneamente.

In configurazione autonoma, l'appliance si basa sugli input provenienti da porte di switch con spanning e/o caricamenti di file on-demand eseguiti dagli amministratori tramite GUI. Si tratta dell'infrastruttura più adatta per l'aggiunta di funzionalità di sicurezza ai sistemi di protezione dalle minacce esistenti di vari fornitori.

In combinazione con FortiGate/FortiMail, l'appliance riceve da FortiGate, nella sua funzione di gateway di sicurezza Internet, i file sospetti. In questo modo l'integrazione riduce la complessità della rete ed espande il numero di applicazioni e protocolli supportati, inclusi quelli crittografati con SSL come HTTPS.

Infine, negli ambienti distribuiti può essere utile integrare FortiSandbox centrale con i FortiGate implementati negli uffici distaccati, riducendo così il TCO garantendo la protezione dalle minacce nelle postazioni remote.

Maggiori informazioni su Fortinet e il suo ecosistema di soluzioni ATP sono disponibili all'indirizzo www.fortinet.com/sandbox



Reportec

Copyright Reportec Srl - 2014