Malwarebytes Endpoint Security vs. Ransomware

Contrastare la minaccia crescente dei ransomware

I ransomware sono notoriamente difficili da combattere. Una volta che il dispositivo è stato infettato, le vittime devono decidere se pagare i criminali per ottenere la chiave di sblocco dei dati o perdere per sempre i propri file.

Una recente indagine globale tra i dirigenti IT sponsorizzata da Malwarebytes[1] evidenzia le reali dimensioni di questa minaccia alle aziende. Il 39% delle organizzazioni intervistate ha subito un attacco ransomware nei 12 mesi precedenti. Tra i diversi settori oggetto dell'indagine, i ransomware si sono rivelati più diffusi in quello sanitario e dei servizi finanziari, che comprende banche e assicurazioni.

> Il 39% delle organizzazioni intervistate ha subito un attacco ransomware nei 12 mesi precedenti.

I costi sostenuti a causa dei ransomware sono notevoli, che si tratti della perdita di risorse digitali o dell'obbligo a sborsare ingenti somme. Quasi il 20% delle vittime di ransomware ha dichiarato che il riscatto superava i $10.000. Globalmente, quasi il 40% delle vittime di ransomware ha pagato la somma richiesta. In Canada, l'82% delle organizzazioni che ha deciso di non pagare ha perso i propri file.

Un'inchiesta del senato sugli attacchi ransomware che ha coinvolto il Procuratore generale degli USA e il Segretario del Dipartimento della Sicurezza Interna, svoltasi a dicembre 2015, ha rivelato che circa 234.000 computer sono stati infettati da uno specifico ransomware, chiamato Cryptolocker.[2] Sebbene soltanto poco più dell'1% delle vittime abbia pagato il riscatto, l'estorsione è valsa circa $27 milioni nel giro di due mesi. Un'altra variante di Cryptolocker è servita per estorcere oltre $18 milioni da circa 1.000 vittime tra aprile 2014 e giugno 2015[3].

Inoltre, il numero di attacchi ransomware negli USA è in aumento. L'FBI ha ricevuto segnalazioni per quasi 2.500 attacchi ransomware nel 2015, i quali sono costati alle vittime $24 milioni. Solo nel primo trimestre del 2016, le estorsioni legate ai ransomware hanno aggiunto altri $209 milioni al bilancio.[4] Il risvolto peggiore è che a volte, quando le vittime pagano il riscatto, non sempre i criminali decriptano i file. Inoltre, secondo l'Institute for Critical Infrastructure Technology, non esiste garanzia che il sistema non verrà nuovamente attaccato in seguito al pagamento.[5]

Le conseguenze umane dell'estorsione informatica

Oltre a creare un grave problema economico, i ransomware possono ostacolare alcuni servizi fondamentali. Nel maggio 2016 l'FBI ha diramato un avviso sul notevole aumento dell'attività legata ai ransomware, che comprendeva una serie di gravi attacchi contro gli ospedali.[6] Secondo un rapporto pubblicato su eWeek.com, a febbraio 2016 l'Hollywood Presbyterian Medical Center ha ammesso di aver pagato un riscatto di $17.000 per la decriptazione di dati infettati da un ransomware.

Le organizzazioni sanitarie rappresentano un bersaglio facile per i criminali informatici. La posta in gioco è alta, in quanto legata alla cura dei pazienti, perciò a volte non c'è altra scelta se non pagare per riavere indietro i dati. Anche se la maggior parte delle attività legate ai ransomware non viene segnalata, una dichiarazione dell'HITRUST (Health Information Trust Alliance) indica che circa il 18% degli ospedali di medie dimensioni è stato infettato da crypto-ransomware.[7]

Cosa spinge i criminali informatici?

Niente è come avere successo in qualcosa e, attualmente, esistono una serie di fattori che favoriscono l'ascesa dei ransomware. Come fa notare Adam Kujawa, responsabile della sezione Malware Intelligence di Malwarebytes,

“L'attenzione che i ransomware stanno ricevendo dai media rispecchia con precisione il livello di pericolo che ci troviamo ad affrontare". In altre parole, l'elevata incidenza dei ransomware e la reale minaccia che rappresentano non sono esagerazioni mediatiche. In base alle analisi statistiche di Malwarebytes sull'infiltrazione di ransomware mediante gli attacchi di malvertising, Kujawa sostiene che “i criminali stanno smettendo di usare altri tipi di malware per concentrarsi sui ransomware”.

In parole semplici, i ransomware sono l'arma prediletta dei criminali informatici per i seguenti motivi:

- Sono redditizi, in quanto comportano una richiesta di pagamento diretto che assicura un guadagno istantaneo. Normalmente, i criminali chiedono di essere pagati in criptovalute, come il Bitcoin. Queste valute, per lo più anonime e praticamente irrintracciabili, consentono ai criminali informatici di riciclare i guadagni illegali nella propria valuta locale. Proprio come le grandi aziende legittime, talvolta le organizzazioni criminali che utilizzano i ransomware offrono un "utile" servizio di assistenza clienti, mediante il quale spiegano alle vittime come acquistare la criptovaluta richiesta.
- Sono sempre più facili da utilizzare. I criminali esperti stanno sviluppando ransomware destinati al mercato online, offrendoli sotto forma di servizio (RaaS) ai truffatori con minori capacità tecniche. Di fatto, gli sviluppatori di ransomware stanno destinando i propri malware a una rete di distribuzione composta da "script kiddie", in modo che questi possano disporre di una soluzione preconfigurata in cambio di una percentuale del "bottino".[8]
- Difendersi dai ransomware è molto difficile. Secondo un'indagine tra i dirigenti IT sponsorizzata da Malwarebytes,[9] gli intervistati statunitensi sono preoccupati soprattutto dell'infiltrazione di malware tramite e-mail e browsing. Ad esempio, aprire un allegato e-mail contenente un exploit consente ai malware di sfruttare le falle dei software presenti sul sistema, aprendo la strada ai ransomware. Le pratiche di malvertising prevedono l'installazione di trappole nelle pubblicità di siti web affidabili, mediante le quali è possibile scaricare i ransomware anche senza fare clic sulle pubblicità infette. Basti sapere che nel 2015 Google ha disabilitato oltre 780 milioni di pubblicità infettate dal malvertising. Secondo Malwarebytes, circa il 70% delle campagne di malvertising comportano l'infiltrazione di ransomware.

Reagire alla minaccia con Malwarebytes Endpoint Security

La maggior parte dei software di sicurezza attuali offrono un'efficacia limitata contro i ransomware, che non si comportano come i malware tradizionali: alcuni vengono aggiornati automaticamente ogni giorno e utilizzano un codice polimorfico (mutaforma) per evitare il rilevamento. Questo li rende estremamente difficili da individuare, soprattutto a causa del fatto che le normali soluzioni per la sicurezza degli endpoint utilizzano tecnologie statiche basate sulle firme, che non sono in grado di tenere il passo con l'evoluzione dei ransomware. Inoltre, i ransomware odierni sono estremamente sofisticati e utilizzano metodi di criptazione talmente avanzati da rendere impossibile il recupero dei file senza pagare il riscatto.

Sfortunatamente, i sistemi di backup online e collegati localmente non rappresentano sempre una contromisura efficace, poiché i ransomware cercano attivamente i vari tipi di backup per poi criptare i file in essi contenuti. Per quanto riguarda i backup online, i caricamenti di file automatici possono corrompere i file che l'utente ritiene al sicuro.

Al contrario, Malwarebytes Endpoint Security è progettato per combattere — e sconfiggere — i ransomware avanzati che sfuggono alle altre soluzioni di sicurezza. Si utilizza nelle reti aziendali e protegge gli endpoint dai malware e da altre minacce avanzate, grazie a una potente combinazione multi-livello di tecnologie proattive senza firma, euristiche e comportamentali.

Inoltre, Malwarebytes Endpoint Security offre un ulteriore livello di protezione contro gli attacchi ransomware grazie a una nuova tecnologia dedicata, sviluppata appositamente per rilevare e bloccare ogni tipo di ransomware, noto o sconosciuto, evitando così la criptazione dei file dell'utente. Questa soluzione per la protezione degli endpoint si distingue da tutte le altre che, al massimo, si limitano a mettere insieme una serie di tecnologie obsolete già rivelatesi inefficaci.

Malwarebytes Endpoint Security rompe la catena di attacco dei ransomware con un approccio basato su quattro livelli:

1. Il livello anti-ransomware di Malwarebytes Endpoint Security monitora costantemente gli endpoint e interrompe automaticamente tutti i processi associati a possibili attività ransomware. Comprende un motore di rilevamento in tempo reale dedicato, che non utilizza firme e non richiede aggiornamenti. Inoltre, il suo impatto sul sistema è minimo ed è compatibile con soluzioni di sicurezza di terze parti.

2. Il livello anti-exploit blocca proattivamente gli exploit prima che possano agire. Avvolge le applicazioni e i browser vulnerabili in una serie di strati difensivi, concepiti per stroncare gli attacchi 0-day sul nascere. Grazie all'impiego di tecnologie senza firma che identificano i comportamenti tipici degli exploit, la protezione anti-exploit riesce a rilevare anche malware e ransomware che le altre tecnologie non riescono a individuare senza essere già state esposte a essi.
3. Il livello anti-malware di Malwarebytes Endpoint Security utilizza regole euristiche e comportamentali per rilevare e rimuovere i malware in tempo reale, prima che possano eseguire il proprio codice.
4. Il livello dedicato al bloccaggio dei siti web dannosi evita l'accesso a server di comando e controllo noti o sospetti, in modo che i ransomware non riescano a ottenere le chiavi di criptazione o l'accesso al proprio file eseguibile.

Rompere la catena di attacco dei ransomware con Malwarebytes

Ecco come le tecnologie di Malwarebytes Endpoint Security bloccano un attacco ransomware originato da un exploit associato al malvertising.

Il modo migliore per spiegarlo è scoprire le varie tappe della catena di attacco dei ransomware:

1. Analisi: il criminale analizza l'endpoint grazie a un banner pubblicitario infetto, per identificare sistema operativo, tipo di browser, indirizzo IP e programma di sicurezza.
   Tecnologia Malwarebytes: la protezione avanzata delle applicazioni riduce il grado di vulnerabilità e rende il computer più resiliente, oltre a rilevare proattivamente i tentativi di fingerprinting avanzati (senza firma).

2. Infiltrazione: il modo in cui il criminale introduce exploit e payload sull'endpoint.
   Tecnologia Malwarebytes: la protezione web protegge gli utenti evitando l'accesso a siti web dannosi, reti pubblicitarie e di truffatori e tenendo il sistema a distanza da “cattive compagnie”.

3. Sfruttamento: il criminale sfrutta il codice vulnerabile nel browser, in Adobe Flash, Microsoft Word, ecc. per diffondere il payload del ransomware ed eseguirlo da remoto.
   Tecnologia Malwarebytes: la soluzione di prevenzione degli exploit rileva e blocca proattivamente i tentativi di sfruttamento delle vulnerabilità e di esecuzione remota del codice sulla macchina, ossia uno dei principali vettori di infezione odierni (senza firma). Un apposito sistema garantisce il comportamento corretto delle applicazioni e ne evita lo sfruttamento per infettare la macchina (senza firma).

4. Esecuzione del payload: il criminale esegue il payload del ransomware sul sistema.
   Tecnologia Malwarebytes: il sistema di analisi dei payload è composto da regole euristiche e comportamentali che identificano intere famiglie di malware noti o rilevanti.

5. Comportamento dannoso: il ransomware si attiva sul sistema, utilizzando un server di comando e controllo per scaricare le chiavi di criptazione e bloccare i file.
   Tecnologia Malwarebytes: il sistema di prevenzione dei ransomware è composto da una tecnologia di monitoraggio del comportamento che rileva i ransomware e blocca la criptazione dei file dell'utente (senza firma).
   Il sistema di protezione con funzione callback evita l'accesso ai server di comando e controllo (C&C) e ad altri siti web dannosi.

Riepilogo

Il sempre maggior numero di dispositivi connessi a quello che oggi si definisce "Internet delle cose" (IoT) apre ai ransomware nuove opportunità criminali, specialmente alla luce del fatto che, secondo molti esperti, in futuro verranno sviluppate molte nuove varianti di ransomware.

Malwarebytes Endpoint Security è una piattaforma di protezione degli endpoint che protegge proattivamente i computer sia da minacce note che sconosciute. Malwarebytes Endpoint Security prevede un ulteriore livello di protezione contro gli attacchi ransomware con un'esclusiva tecnologia anti-ransomware che monitora, rileva e blocca automaticamente i ransomware prima che possano raggiungere i file. Oltre a gestire minacce note come Cryptolocker, CryptoWall o CTBLocker, contrasta istantaneamente i nuovi ransomware, proteggendo proattivamente gli utenti dalle minacce sconosciute.

Le aziende possono trarre enormi vantaggi da Malwarebytes Endpoint Security per i seguenti motivi:

- Riduce la vulnerabilità agli attacchi ransomware. Rileva e blocca automaticamente i ransomware noti e sconosciuti, anziché limitarsi ad avvertire l'utente tramite e-mail automatiche, come fanno altri prodotti di sicurezza.
- Blocca la criptazione in tempo reale. Blocca i ransomware prima che possano agire, eliminando l'esigenza di strumenti di decriptazione complicati e spesso inefficaci.
- Combatte i ransomware 0-day (precedentemente non identificati) utilizzando una speciale tecnologia di monitoraggio del comportamento in grado di fermare i ransomware sconosciuti che le altre tecnologie non riescono a rilevare, non avendoli mai visti prima.
- È stato appositamente studiato da zero per contrastare i ransomware in maniera più rapida ed efficace. Malwarebytes ha ideato questa tecnologia al solo scopo di difendere gli utenti dai ransomware. Le altre soluzioni anti-ransomware si basano su tecnologie obsolete o su un insieme di tecnologie riconvertite, originariamente ideate per altri scopi.
- Utilizza tecnologie senza firma nei livelli anti-ransomware e anti-exploit, in modo che la protezione sia efficace anche contro i ransomware che non hanno ancora una firma.
- Contribuisce a mantenere la reputazione dell'azienda, consentendo di evitare i problemi legati alle pubbliche relazioni che solitamente accompagnano un attacco.
- Tutela l'azienda a livello economico, evitando il pagamento di riscatti per la decriptazione dei dati.

Risorse web

Per ulteriori informazioni su Malwarebytes Endpoint Security e le nuove tecnologie anti-ransomware, visita: malwarebytes.com/business/endpointsecurity/
Ultime notizie: blog.malwarebytes.com/
Per richiedere un periodo di prova: malwarebytes.com/business/licensing

Riferimenti

[1]Indagine condotta a giugno 2016 e pubblicata ad agosto 2016 da Osterman Research, Inc
[2]https://www.hsgac.senate.gov/media/minority-media/senators-carper-johnson-seek-information-on-threat-of-ransomware-to-our-nations-cyber-defenses-and-to-the-american-public
[3]Ibid.
[4]http://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746
[5]http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report.pdf
[6]https://blog.malwarebytes.com/101/2016/06/malvertising-and-ransomware-the-bonnie-and-clyde-of-advanced-threats/
[7]http://www.eweek.com/security/ransomware-poses-a-rising-threat-to-hospital-operations.html
[8]http://www.techrepublic.com/article/ransomware-as-a-service-is-exploding-be-ready-to-pay/
[9]Indagine condotta a giugno 2016 e pubblicata ad agosto 2016 da Osterman Research, Inc.

Su di noi

Malwarebytes è l'azienda per la sicurezza informatica di prossima generazione a cui si affidano milioni di persone in tutto il mondo. Malwarebytes protegge in maniera proattiva i privati e le aziende da minacce pericolose quali malware, ransomware ed exploit che sfuggono al rilevamento degli antivirus convenzionali. Il principale prodotto dell'azienda combina la rilevazione euristica e avanzata delle minacce con le tecnologie senza firma per rilevare e arrestare un attacco informatico prima che possa danneggiare i sistemi. Oltre 10.000 aziende in tutto il mondo utilizzano, si affidano e consigliano Malwarebytes. Fondata nel 2008, la sede principale dell'azienda è in California, con uffici in Europa e Asia e conta su un team globale di ricercatori ed esperti della sicurezza.

Santa Clara, CA
malwarebytes.com
corporate-sales@malwarebytes.com
1.800.520.2796