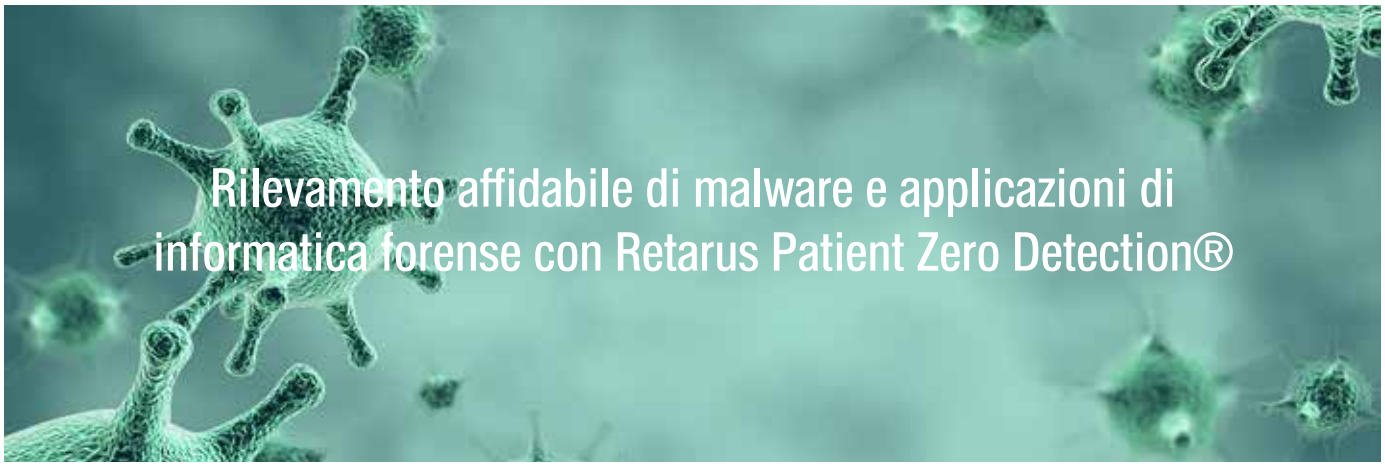

Rilevamento affidabile di malware e applicazioni di informatica forense con Retarus Patient Zero Detection®

La sfida

Le misure di protezione semplici sono da tempo insufficienti. Il numero di virus che attaccano quotidianamente l'infrastruttura di un'azienda è diventato enorme. Se il malware entra nel sistema, diventa fondamentale limitare i danni che può causare. Solo identificando i destinatari dei messaggi infetti, i cosiddetti pazienti zero, è possibile adottare misure tempestive per evitare danni maggiori. Allo stesso tempo, per garantire una protezione completa contro le minacce future, è necessario ottimizzare continuamente le impostazioni del sistema.

Il background

Purtroppo, una gran parte della posta elettronica è costituita da spam, virus o attacchi di phishing mirati. Ogni giorno, in tutto il mondo vengono registrate più di 390.000 nuove istanze di software maligno. Questo significa che mediamente vengono prodotti circa 270 nuovi virus informatici al minuto. I programmi di sicurezza e-mail sono generalmente affidabili nel filtrare le e-mail infette. Tuttavia, nessun filtro antivirus può offrire una protezione del 100%. Quando un virus specifico appare per la prima volta, anche i migliori scanner di virus non conoscono la sua firma. Per questo motivo, oltre ai servizi cloud, molte aziende impiegano scanner di virus in loco o elaborate soluzioni di sandboxing. Ma in questi casi gli amministratori e i destinatari spesso vengono a conoscenza dell'esistenza di nuovi tipi di virus solo quando è già troppo tardi e il malware ha già avuto la possibilità di causare danni. L'origine spesso sconosciuta dell'attacco complica enormemente le azioni di informatica forense.

La soluzione

Retarus Email Security protegge in modo affidabile dagli attacchi malware grazie a una protezione antivirus multilivello, a filtri intelligenti contro lo spam e il phishing e a un esclusivo sistema di blocco degli allegati. La collaudata scansione antivirus a quattro livelli di Retarus, ad esempio, garantisce già oggi un altissimo livello di protezione, filtrando il 35% di virus in più rispetto ai tradizionali servizi di protezione antivirus che si basano solo su due scanner. In combinazione con Retarus Patient Zero Detection®, le aziende possono ora proteggere le loro infrastrutture in modo ancora più sicuro dagli attacchi e sono inoltre in grado di rilevare malware finora sconosciuti.

Vantaggi per i clienti

- Massima protezione per l'infrastruttura IT
- Risposta rapida agli attacchi
- Informatica forense semplificata
- Comunicazione aziendale efficiente
- Ottimizzazione sostenibile delle impostazioni di sistema

I vantaggi in breve

- Identificazione affidabile dei destinatari di malware precedentemente non rilevati
- Avvisi istantanei
- Consegna delle e-mail senza ritardi
- Report e analisi dettagliati
- Integrazione perfetta con Retarus Enterprise Email Archive e Retarus Email Encryption

Caso d'uso

Retarus Email Security utilizza diversi scanner di virus con regole di filtraggio continuamente aggiornate, che già oggi proteggono efficacemente dalla stragrande maggioranza dei messaggi dannosi. L'innovativa tecnologia Patient Zero Detection® Retarus identifica anche le e-mail pericolose già recapitate. A tal fine viene generata un'impronta digitale per ogni allegato trasportato dalle e-mail in arrivo e memorizzata in una banca dati all'interno dell'infrastruttura Retarus. Ciò non comporta alcun ritardo nei tempi di consegna. Quando in un momento successivo uno scanner di virus identifica un malware nello stesso tipo di allegato, Retarus confronta l'impronta digitale dell'allegato dannoso con le informazioni salvate nella banca dati. L'e-mail infetta viene immediatamente cancellata. Se la firma corrisponde a una di quelle già memorizzate nel database, gli amministratori responsabili e, se si desidera, tutti i precedenti destinatari dell'allegato vengono immediatamente avvisati. Con Patient Zero Detection® Real-Time Response, i risultati possono essere elaborati in base a regole per identificare e spostare o eliminare automaticamente le e-mail potenzialmente pericolose nella casella di posta di un utente.

I sistemi colpiti possono essere identificati in pochissimo tempo e possono essere prese misure per evitare che il virus si diffonda in tutta la rete aziendale. In questo modo, è spesso possibile eliminare l'e-mail infetta ancora prima che sia stata aperta. Se un allegato infetto è stato aperto, Retarus Patient Zero Detection® semplifica le operazioni di informatica forense. Report e analisi dettagliate forniscono punti di riferimento concreti per capire in quali file ricercare i virus. Per garantire in futuro una migliore protezione del sistema, le impostazioni dei filtri in Retarus Email Security vengono continuamente ottimizzate sulla base delle informazioni ottenute da Retarus Patient Zero Detection®.

Lo sapevate che…

Secondo Kaspersky, il danno economico medio dovuto a un attacco informatico contro una grande azienda è di 861.000 dollari.

Altri scenari

Crittografia Sicura
I dati sensibili non devono cadere nelle mani sbagliate. Con Retarus Email Encryption le aziende possono proteggere la riservatezza delle comunicazioni e applicare senza problemi le leggi vigenti sulla riservatezza dei dati.

Quarantena Intelligente Delle E-Mail
I digest delle e-mail offrono alle aziende una rapida panoramica di tutti i messaggi contenenti virus e spam che sono stati filtrati. Gli utenti possono recuperare immediatamente e direttamente dalla quarantena le e-mail classificate come spam, senza dover accedere al portale. Per garantire la massima protezione, quando questi messaggi vengono scaricati, viene nuovamente fatto un controllo antivirus.

Attachment Blocker
Con Retarus Attachment Blocker le aziende possono dotare le loro infrastrutture di una sicurezza ancora maggiore contro gli attacchi malware. Questa funzione impedisce agli utenti di ricevere tutti i formati di allegati che l'amministratore classifica come non affidabili.