Protezione da WannaCry e Petya

Un vasto attacco informatico, basato sulla famiglia di malware WannaCry, è stato lanciato nel mese di maggio 2017. WannaCry ha sfruttato una vulnerabilità in alcune versioni di Microsoft Windows. Si stima che più di 300.000 computer in 150 nazioni siano stati infettati durante l'attacco principale, con conseguente richiesta di riscatto.

Il vettore d'attacco iniziale non è chiaro, ma un worm aggressivo aiuta a diffondere il malware. Una patch fondamentale è stata rilasciata da Microsoft a marzo per rimuovere la vulnerabilità alla base nelle versioni supportate di Windows, ma molte aziende non l'hanno ancora applicata.

Per i computer che utilizzano versioni non supportate di Windows (Windows XP, Windows Server 2003) non c'era una patch disponibile. Microsoft ha rilasciato una speciale patch di sicurezza per Windows XP e Windows Server 2003 dopo l'attacco WannaCry.

Circa sei settimane dopo, un altro attacco informatico ha sfruttato la stessa vulnerabilità. Petya non ha avuto un impatto pari a quello di WannaCry, ma questi due attacchi hanno evidenziato l'uso continuo di sistemi operativi obsoleti e non supportati in aree critiche e hanno messo a nudo processi inadeguati di aggiornamento delle patch, seguiti da alcune aziende. Un'analisi approfondita di questi attacchi è dettaglia nel *Report McAfee Labs sule minacce: settembre 2017.*

Policy e procedure per proteggersi dagli attacchi WannaCry e Petya

- **Effettuare il backup dei file:** la procedura più efficace per sventare il ransomware è di effettuare un backup regolare dei file di dati e verificare le procedure di ripristino della rete.
- **Educare gli utenti della rete:** come altro malware, il ransomware spesso infetta un sistema attraverso attacchi di phishing utilizzando allegati email, download o navigazione web cross-scripting.
- **Monitorare e ispezionare il traffico della rete:** questa misura aiuta a identificare il traffico anormale associato ai comportamenti del ransomware.
- **Usare i feed dei dati di intelligence sulle minacce:** questa prassi permette di rilevare le minacce più velocemente.
- **Limitare l'esecuzione di codice:** il ransomware è spesso progettato per l'esecuzione in cartelle ben note del sistema operativo. Se il ransomware non riesce a raggiungere tali cartelle a causa del controllo degli accessi, la crittografia dei dati pericolosi può essere bloccata.
- **Limitare l'accesso amministrativo e al sistema:** alcuni tipi di ransomware sono progettati per usare account predefiniti al fine di eseguire le proprie operazioni. Con questo tipo di ransomware si può aggiungere protezione ulteriore rinominando gli account utente predefiniti e disattivando tutti gli account non necessari, con e senza privilegi.
- **Rimuovere i diritti di amministratore locale:** prevenire l'esecuzione del ransomware in un sistema locale e bloccarne la diffusione sulla base dei privilegi amministrativi. La rimozione dei diritti di amministratore locale blocca inoltre l'accesso a tutte le risorse e ai file di sistema critici presi di mira dal ransomware per la crittografia.
- **Altre prassi relative alle autorizzazioni:** considerare la limitazione della scrittura da parte degli utenti, prevenire le esecuzioni dalle directory degli utenti, creare whitelist delle applicazioni e limitare l'accesso agli archivi e alle condivisioni della rete. Alcuni ransomware richiedono l'accesso in scrittura a specifici percorsi dei file per potersi installare ed eseguire. La limitazione delle autorizzazioni di scrittura a un piccolo numero di directory (per esempio, Documenti e Download) può bloccare alcune varianti del ransomware. Gli eseguibili del ransomware possono essere fermati anche tramite la rimozione delle autorizzazioni di esecuzione da tali directory. Per svolgere le proprie attività molte aziende usano una ridotta serie di applicazioni. L'esecuzione di applicazioni non incluse nelle whitelist, compreso il ransomware, può essere bloccata mantenendo per le applicazioni stesse una policy "solo whitelist". Un'ulteriore prassi per le autorizzazioni è quella di richiedere credenziali per accedere alle risorse condivise, come le cartelle di rete.
- **Mantenere e aggiornare il software:** un'altra importante regola di base per proteggersi dal ransomware è quella di mantenere e aggiornare il software, in particolare le patch del sistema operativo, oltre al software di sicurezza e antimalware.

È estremamente importante ridurre la superficie di attacco, specialmente per il phishing, che è una delle tecniche più usate dal ransomware. Per le email considerare le seguenti prassi.

- **Filtrare i contenuti in uscita:** la protezione delle comunicazioni via email è una procedura fondamentale. La possibilità di successo di un attacco si riduce se gli utenti della rete ricevono meno email di spam, che potrebbero includere contenuti potenzialmente ostili e non sicuri.
- **Bloccare gli allegati:** l'ispezione dell'allegato è una misura importante per ridurre la superficie di attacco. Il ransomware viene spesso inviato come allegato eseguibile. Imporre una policy che impedisca l'invio tramite email di alcune estensioni dei file. Quegli allegati potrebbero essere analizzati con una soluzione di sandbox e poi rimossi dall'appliance per la protezione dell'email

Come i prodotti McAfee possono proteggere da WannaCry

McAfee Network Security Platform (NSP)

McAfee NSP risponde rapidamente per prevenire gli exploit e proteggere le risorse all'interno delle reti. Il team McAfee NSP opera coscienziosamente per sviluppare e distribuire firme definite dall'utente (UDS) per questioni critiche. Entro un periodo di 24 ore durante l'attacco WannaCry, McAfee ha creato e caricato numerose UDS affinché i clienti le distribuissero sui loro sensori di rete. In questo caso, l'UDS era esplicitamente rivolta agli strumenti exploit EternalBlue, Eternal Romance SMB Remote Code Execution e DoublePulsar. McAfee ha inoltre rilasciato indicatori di violazione correlati che potevano essere aggiunti a una blacklist per bloccare minacce potenziali associate al trojan originale.

Maggiori informazioni sulle firme NSP qui.

McAfee Host Intrusion Prevention (HIPS)

McAfee HIPS 8.0 con NIPS Firma 6095 fornisce protezione da tutte e quattro le varianti note di WannaCry. Fare riferimento a KB89335 per le informazioni più recenti su queste configurazioni.

Firma personalizzata N.1: Regola di blocco del registro di sistema WannaCry
Usa sottoregola standard
Tipo di regola = Registro di sistema
Operazioni = Crea, Modifica, Cambia autorizzazioni, includi Chiave del Registro di sistema
Chiave del Registro di sistema = \REGISTRY\MACHINE\SOFTWARE\WanaCrypt0r
Eseguibile = *

Firma personalizzata N.2: Regola di blocco File/Cartella WannaCry
Usa sottoregola standard
Tipo di regola = File
Operazioni = Crea, Scrivi, Rinomina, Cambia attributi sola lettura/nascosti, includi File
File = *.wnry
Eseguibile = *

Configurazioni del modulo di Protezione adattiva dalle minacce in McAfee Endpoint Protection (ENS) e McAfee VirusScan Enterprise (VSE)

McAfee Endpoint Security 10.5—Protezione adattiva dalle minacce

McAfee Endpoint Security 10.5 con il modulo per la Protezione adattiva dalle minacce, Real Protect e il componente per il Contenimento dinamico delle applicazioni (DAC) fornisce protezione contro exploit noti o sconosciuti per WannaCry.

- Configurare le seguenti impostazioni all'interno del modulo per la Protezione adattiva dalle minacce - Policy delle opzioni:
  - Assegnazione regola = Sicurezza. (L'impostazione predefinita è Bilanciata.)
- Configurare le seguenti regole nella policy Protezione adattiva dalle minacce - Contenimento dinamico delle applicazioni:
  - Contenimento dinamico delle applicazioni - Regole per il contenimento

Fare riferimento a KB87843: Elenco delle best practice per le regole di contenimento dinamico delle applicazioni di ENS e impostazione delle regole DAC consigliate per effettuare il "Blocco" come prescritto.

McAfee Endpoint Security 10.1, 10.2 e 10.5—Prevenzione delle minacce

La prevenzione delle minacce di McAfee Endpoint Security 10.x con contenuto AMCore Versione 2978 o successiva offre protezione contro tutte le quattro varianti attualmente note di WannaCry.

McAfee VirusScan Enterprise 8.8

McAfee Endpoint Security 8,8.x con DAT a contenuto 8527 o successivo offre protezione contro tutte le quattro varianti attualmente note di WannaCry.

Misure proattive per la protezione di McAfee Endpoint Security (ENS) e per la protezione degli accessi di McAfee VirusScan Enterprise (VSE)

Le regole di protezione di McAfee ENS e di protezione degli accessi di McAfee VSE prevengono la creazione del file .wnry. Questa regola blocca la routine di crittografia, che crea file crittografati che contengono un'estensione .wncryt, .wncry o .wcry. Implementando il blocco contro i file .wnry, non sono necessari altri blocchi per le tipologie di file crittografati.

Maggiori informazioni sulla configurazione delle regole per la protezione degli accessi di McAfee VSE.

Configurare il sistema di protezione degli endpoint per proteggere dalla crittografia dei file perpetrata da WannaCry (e varianti future ora sconosciute)

I clienti che non utilizzano il modulo per la Protezione adattiva dalle minacce di McAfee ENS potrebbero non disporre della protezione dei contenuti definita da McAfee per varianti non ancora rilasciate. Consigliamo di configurare attività di aggiornamento del repository con un intervallo minimo di refresh per assicurare che i nuovi contenuti vengano applicati non appena rilasciati da McAfee.

Protezioni aggiuntive dalla routine di crittografia possono essere configurate utilizzando le regole di protezione degli accessi di McAfee VSE/ENS o le regole personalizzate di McAfee HIPS. Fare riferimento a KB89335 per le informazioni più recenti su queste configurazioni.

Le regole di protezione degli accessi di McAfee VSE e McAfeee ENS e le firme personalizzate di McAfee HIPS prevengono la creazione del file .wnry.

Le regole prevengono la routine di crittografia, che crea file crittografati che contengono un'estensione .wncryt, .wncry o .wcry.

Implementando il blocco contro i file .wnry, non sono necessari altri blocchi per le tipologie di file crittografati.

Fare riferimento a KB89335 (accessibile a clienti registrati McAfee) per le informazioni più recenti su queste configurazioni.

McAfee Advance Threat Defense (ATD)

L'apprendimento automatico di McAfee ATD è in grado di giudicare dannoso un esemplare sulla base di un'analisi di "media gravità".

McAfee ATD ha osservato quanto segue:

Classificazione del comportamento:

- File offuscato
- Diffusione
- Sfruttamento attraverso shellcode
- Propagazione sulla rete

Analisi dinamica:

- Comportamento ransomware dedotto
- Crittografia dei file
- Contenuto di scripting sospetto creato ed eseguito
- Comportamento come quello di un dropper di macro trojan

Con WannaCry, ad oggi McAfee ATD ha osservato 22 operazioni di processo, tra cui cinque DLL runtime, 58 operazioni di file, modifiche del Registro di sistema, modifiche di file, creazioni di file (dll.exe), iniezioni DLL e 34 operazioni di rete.

McAfee Web Gateway (MWG)

McAfee Web Gateway (MWG) è una famiglia di prodotti (appliance, cloud e soluzione ibrida) di proxy web che fornisce una protezione immediata dalle varianti WannaCry depositate attraverso il web (HTTP/HTTPS) utilizzando molteplici motori di scansione in tempo reale.

Le varianti note saranno bloccate dalla scansione della reputazione e antimalware di McAfee Global Threat Intelligence (GTI) nel momento in cui il traffico web viene elaborato attraverso il proxy.

Il motore Gateway Anti-Malware (GAM) Engine all'interno di MWG fornisce una prevenzione efficace dalle varianti che non sono ancora state identificate con una firma (minacce "zero-day") attraverso il suo processo di emulazione del comportamento condotto su file, HTML e JavaScript. Gli emulatori ricevono informazioni su base regolare dai modelli di apprendimento automatico. Il motore GAM opera unitamente alla scansione di reputazione e antimalware di GTI nel momento in cui il traffico viene elaborato.

L'accoppiamento di MWG con ATD consente ulteriori controlli e un approccio efficace alla prevenzione e al rilevamento.

McAfee Threat Intelligence Exchange (TIE)

McAfee Threat Intelligence Exchange (TIE) migliora ulteriormente lo stato della sicurezza di un cliente. Con la capacità di aggregare decisioni relative alla reputazione rilasciati da ENS, VSE, MWG e NSP, TIE può rapidamente condividere le informazioni sulla reputazione relative a WannaCry con qualsiasi vettore integrato. Grazie alla possibilità di utilizzare GTI per una query gloale sulla reputazione, TIE consente anche ai prodotti integrati di prendere una decisione immediata prima dell'esecuzione del payload del ransomware, sfruttando la reputazione nella cache del database TIE.

Poiché un unico endpoint protegge, effettua il rilevamento da tutte le varianti correlate e aggiorna il punteggio di reputazione in TIE, questo approccio completo estende la protezione diffondendo queste informazioni a tutti gli endpoint integrati con TIE.

Questa condivisione bidirezionale di intelligence delle minacce è duplicata in capacità con MWG e NSP. Così, nel momento in cui la minaccia potenziale tenta di infiltrarsi attraverso la rete o il web, MWG e NSP forniranno protezione e rilevamento e condivideranno queste informazioni con TIE per inoculare gli endpoint, proteggendo immediatamente l'azienda senza ulteriori esecuzioni della variante giudicata pericolosa su un potenziale "paziente zero" all'interno dell'ambiente.

Come i prodotti McAfee possono proteggere da Petya

McAfee protegge dall'attacco iniziale di Petya nella forma di analisi avanzata del comportamento del malware con le tecniche di analisi di Real Protect Cloud e Dynamic Neural Network (DNN) disponibili in McAfee Advanced Threat Defense.

ATD 4.0 ha introdotto una nuova possibilità di rilevamento utilizzando una rete neurale multilivello a retro-propagazione (DNN) che sfrutta l'apprendimento a supervisione parziale. DNN esamina alcune funzionalità esercitate dal malware per ottenere un verdetto positivo o negativo e determinare se il codice è dannoso.

Sia in modalità standalone o collegato a sensori di endpoint McAfee o di rete, il modulo ATD combina l'intelligenza sulle minacce con l'analisi del comportamento di sandbox e l'apprendimento automatico avanzato per fornire una protezione adattabile zero-day. Real Protect, parte della soluzione Dynamic Endpoint, utilizza anche l'apprendimento automatico e l'analisi dei collegamenti per proteggere dal malware senza firme e fornisce informazioni alla soluzione Dynamic Endpoint e il resto dell'ecosistema McAfee. Real Protect combinato con il contenimento dinamico delle applicazioni ha protetto dagli attacchi Petya.

Molteplici prodotti McAfee forniscono protezione aggiuntiva per contenere l'attacco o prevenirne ulteriori esecuzioni.

McAfee Endpoint Security

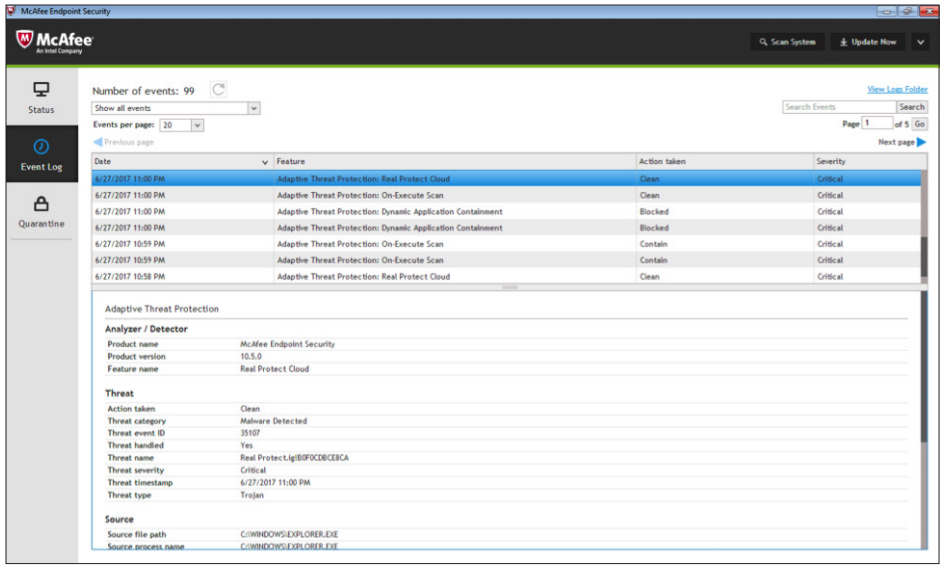
Prevenzione delle minacce

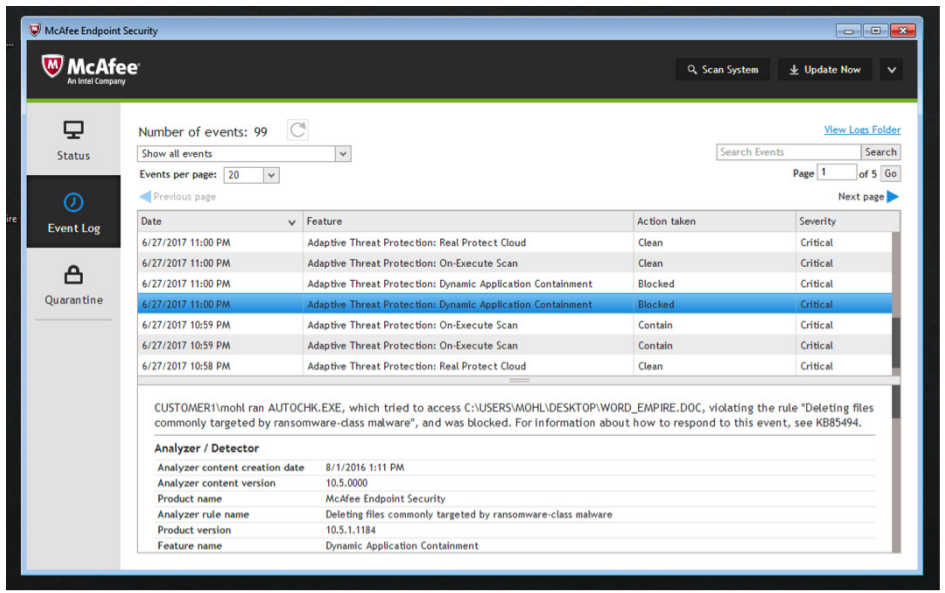
- McAfee Endpoint Security con McAfee Global Threat Intelligence e policy di scansione all'accesso con il livello di sensibilità impostato su "Basso" protegge dagli esemplari e dalle varianti note.
- Scopri le impostazioni consigliate per la reputazione dei file di McAfee GTI nell'articolo KB74983, con ulteriori informazioni nell'articolo KB53735.
- McAfee Threat Intelligence Exchange con GTI protegge dagli esemplari e dalle varianti note.

I sistemi che utilizzano McAfee ENS 10 sono protetti da esemplari e varianti note grazie alle firme e all'intelligence sulle minacce.

Protezione adattiva dalle minacce

- Il modulo di Protezione adattiva dalle minacce (ATP), con assegnazione delle regole configurate in "Modalità bilanciata" (predefinita nelle impostazioni ATP/Opzioni/Assegnazione delle regole),), protegge dale varianti note e sconosciute del ransomware Petya.
- Il modulo ATP protegge da questa minaccia sconosciuta con numerosi livelli di protezione avanzata e contenimento:
  - ATP Real Protect Static utilizza analisi comportamentale pre-esecuzione lato client per controllare le minacce dannose sconosciute prima che vengano lanciate.
  - ATP Real Protect Cloud utilizza l'apprendimento automatico cloud-assisted per identificare e bonificare la minaccia, come mostrato sopra a destra.
- Il componente per il Contenimento dinamico delle applicazioni (DAC) limita con successo la minaccia e previene il verificarsi di danni potenziali (eventi DAC evidenziati in basso a destra).



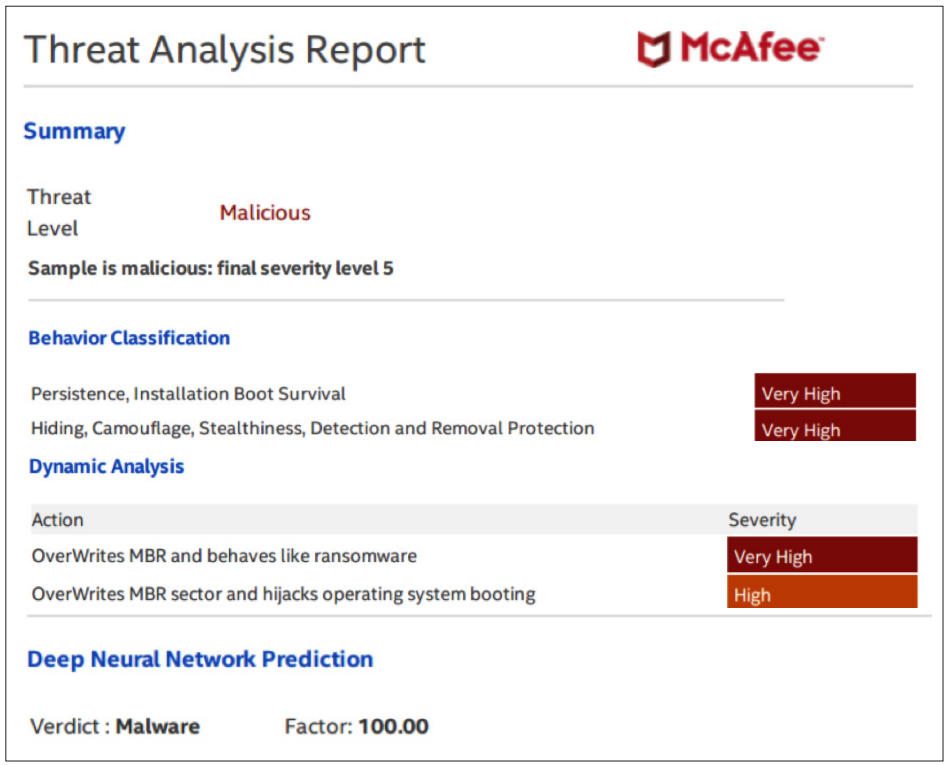


McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense 4.0 con una rete neuronale per il deep learning e una funzione per l'analisi dinamica in sandbox hanno identificato la minaccia e aggiornato proattivamente l'ecosistema di protezione informatica. (Vedere di seguito.)

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) è una soluzione per la gestione delle informazioni e degli eventi di sicurezza che offre informazioni fruibili ed integrazioni per assegnare le priorità, analizzare e rispondere alle minacce. Il Suspicious Activity Content Pack e l'Exploit Content Pack per McAfee ESM sono stati aggiornati con regole, allarmi e liste di osservazioni specifiche per WannaCry, in modo da individuare e identificare le possibili infezioni. Questi aggiornamenti contribuiscono a proteggersi da Petya. Entrambi i pacchetti possono essere scaricati dalla console di McAfee ESM gratuitamente. Le regole predefinite di correlazione all'interno di McAfee ESM possono avvisare gli utenti di livelli aumentati di scansioni orizzontali SMB.



Come per WannaCry, l'attacco Petya presenta un'opportunità di apprendimento per gli analisti del SOC (Security Operations Center). Comprendere e automatizzare queste best practice aiuterà i professionisti della sicurezza a gestire il prossimo attacco.

McAfee Web Gateway

McAfee Web Gateway (MWG) è una famiglia di prodotti (appliance, cloud e soluzione ibrida) di proxy web che fornisce un altro potenziale livello di protezione per le varianti Petya depositate attraverso il web (HTTP/HTTPS) utilizzando molteplici motori di scansione in tempo reale. Le varianti note saranno bloccate dalla scansione della reputazione e antimalware di GTI nel momento in cui il traffico web viene elaborato attraverso il proxy.

Il motore Gateway Anti-Malware Engine all'interno di MWG fornisce una prevenzione efficace dalle varianti "zero-day"che non sono ancora state identificate con una firma attraverso il processo di GAM di emulazione del comportamento condotto su file, HTML e JavaScript. Gli emulatori ricevono informazioni su base regolare dai modelli di apprendimento automatico. Il motore GAM opera unitamente alla scansione di reputazione e antimalware di GTI nel momento in cui il traffico viene elaborato.

L'accoppiamento di MWG con ATD consente ulteriori controlli e un approccio efficace alla prevenzione e al rilevamento.

Prodotti McAfee che utilizzano file DAT

McAfee ha rilasciato un file Extra.DAT che include protezione da Petya. Inoltre, McAfee ha reso disponibile un DAT di emergenza per includere protezione da questa minaccia. I DAT successivi includeranno la protezione. I file DAT più recenti sono disponibili tramite l'articolo del Knowledge Center KB89540.

Ulteriori letture

Dettagli tecnici aggiornati frequentemente sono disponibili all'interno dei seguenti articoli del McAfee Knowledge Center: KB89335, KB87843, KB74983, KB53735 e KB89540.

McAfee
Together is power.

Via Fantoli, 7
20138 Milano, Italy
(+39) 02 554171
www.mcafee.com/it

3530_0917
SETTEMBRE 2017