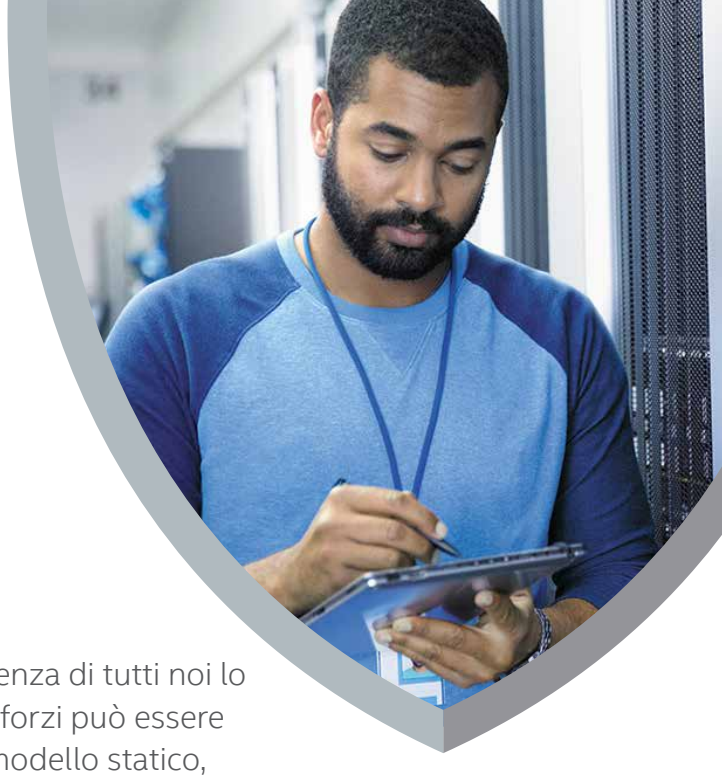
Panoramica sulla soluzione



Abuso di fiducia

Approfittare di chi si fida.

Il detto "la fiducia bisogna guadagnarsela" è vero; l'esperienza di tutti noi lo conferma. D'altro canto, una cosa guadagnata in anni di sforzi può essere distrutta in pochi secondi. La fiducia non è mai stata un modello statico, e questo è diventato ancora più evidente con la crescente dipendenza della popolazione mondiale da Internet.

Che cos'è un abuso di fiducia?

Il **Rapporto McAfee Labs sulle minacce: novembre 2014** contiene un esame approfondito dei modi in cui viene sfruttata la fiducia. Quando siamo online, partiamo dall'assunto che quello che vediamo sia affidabile, che si tratti di un'app scaricata su un dispositivo mobile, di una pubblicità apparentemente innocua su un sito Web molto frequentato o di un'email di una società con cui abbiamo rapporti d'affari. Gli aggressori sfruttano l'istituzione della fiducia in molti modi. Quello preferito è approfittare di vittime ignare. Ecco alcuni dei tipi di attacchi trattati nel rapporto:

- **Malvertising:** quando si scopre che dalle pubblicità innocue sul sito Web di una società è partito un attacco nei confronti di consumatori ignari, questi si chiedono se la loro fiducia non sia mal riposta. **Le reti di pubblicità malevola come "Kyle and Stan"** diffondono il malware tramite il "malvertising" su siti come amazon.com, youtube.com e **su grandi reti pubblicitarie come Double-Click e Zedo**.
- **Malware firmato:** una tattica sempre più comune fra gli autori di malware consiste nell'acquisire da un'autorità di certificazione (CA) certificati che tentano di sfruttare l'affidabilità di società affermate o di spacciarsi per società legittime. Gli aggressori sfruttano la fiducia implicita che accordiamo alle CA. Di recente, una campagna di "malvertising" ha recapitato varianti firmate del trojan CryptoWall tramite la rete pubblicitaria Zedo. A quel che si dice, **sarebbero stati colpiti utenti di siti nelle prime posizioni della classifica Alexa**. La firma digitale emessa per "Trend" tentava probabilmente di spacciarsi per il produttore di antivirus Trend Micro, ed è un esempio perfetto di come si sfrutta la presunzione di "innocenza per associazione".
- **Imitazioni di app:** i marchi commerciali investono notevoli quantità di tempo e risorse per tutelare la clientela dai prodotti contraffatti che cercano di fare leva sulla fiducia dei consumatori nei confronti di un marchio famoso. Poiché ormai le applicazioni sono dotate di funzioni che vanno al di là del mondo digitale, non sorprende che alcuni aggressori intraprendenti abbiano pensato di creare applicazioni che imitano programmi legittimi e solitamente molto diffusi.

  Nell'ultimo trimestre, McAfee ha osservato dei truffatori che tentavano di distribuire un'applicazione apparentemente identica ad Adobe Flash Player 11. A giudicare dal numero dei download nell'app store Google Play e dai dati telemetrici rilevati da McAfee Mobile Security, i truffatori hanno raggiunto il loro scopo, convincendo gli utenti a scaricare l'app "taroccata" malevola.

intel Security

- **DLL side loading:** gli aggressori sanno che, se il loro codice malevolo riesce a sfruttare la scia di un'applicazione affidabile, le probabilità di successo sono maggiori. Il malware approfitta di questo fattore da molti anni, con una tecnica di attacco nota come "DLL side loading" che prevede l'esecuzione di un'applicazione legittima che esegue il codice di una DLL esterna. I malintenzionati progettano il payload in modo che interpreti il ruolo della DLL esterna, inducendo così l'applicazione innocente a eseguire il codice malevolo.

  Nel terzo trimestre, McAfee Labs ha osservato una serie di attacchi sferrati tramite l'applicazione Google Updater. La nuova variante della famiglia di malware PlugX interpreta il ruolo della libreria importata goopdate.dll ma, per mascherare la sua azione, PlugX non si ferma qui. Il modulo goopdate.dll non è altro che un intermediario che legge il contenuto di goopdate.dll.map, un file di dati crittografato malevolo, lo decodifica nella memoria e gli cede il controllo dell'esecuzione.
- **Sistemi operativi e software di rete:** esistono molti esempi di attacchi che abusano della fiducia nei sistemi operativi e nei software di rete e fra l'uno e l'altro di questi sistemi. Alcuni attacchi sfruttano il software che instaura connessioni sicure su Internet. Le applicazioni ignare considerano affidabili le connessioni che ricevono dal sistema operativo, che a sua volta considera affidabile il software di rete che presumibilmente ha stabilito connessioni sicure. Altri attacchi sfruttano le vulnerabilità interne ai sistemi operativi o al software di rete; in molti casi l'anello debole è il software open source incorporato nello stack di questi sistemi.

  BERserk è una vulnerabilità **annunciata di recente** che permette di falsificare le firme e di abusare della fiducia di sistemi operativi e software di rete. BERserk consente ai malintenzionati di sferrare attacchi "man in the middle" (MITM) con la contraffazione delle firme RSA e l'elusione dell'autenticazione ai siti Web che utilizzano SSL/TLS.

Le soluzioni McAfee

La tecnologia di sicurezza McAfee può aiutarvi a proteggervi dagli attacchi che tentano di abusare della fiducia accordata dalla vostra azienda nelle sue operazioni quotidiane. Ecco alcuni dei prodotti McAfee in grado di garantirvi che il modello di fiducia della vostra azienda non venga sfruttato da potenziali aggressori.

McAfee Application Control

Proteggere la vostra azienda e le sue applicazioni legittime dal codice nocivo come BERserk è fondamentale. **McAfee Application Control** vi permette di controllare le applicazioni di cui è autorizzata l'esecuzione nel vostro ambiente mediante policy di whitelisting dinamico e di imposizione sia sugli endpoint connessi che su quelli offline.

- **Whitelisting dinamico:** consente alla vostra organizzazione di gestire con efficienza le applicazioni presenti nella whitelist, compilandola automaticamente via via che i sistemi vengono aggiornati e dotati di patch. McAfee Application Control riduce la vostra esposizione a BERserk impedendo l'esecuzione delle applicazioni che chiamano il codice di verifica delle firme RSA vulnerabile.
- **Reputazione dei file:** l'integrazione con McAfee Global Threat Intelligence permette a McAfee Application Control di interrogare flussi di informazioni in tempo reale sui tipi di file noti — innocui, pericolosi e sconosciuti — per aiutare la vostra azienda a rimanere sempre al corrente delle nuove vulnerabilità come BERserk.
- **Protezione per dispositivi connessi e non connessi:** vengono imposti controlli su tutti i dispositivi, connessi e non connessi: server, macchine virtuali, endpoint e dispositivi fissi come i terminali POS.

Panoramica sulla soluzione

McAfee Email Gateway
Il fatto che un'email nella casella di posta di un utente sia innocua o pericolosa è fonte di notevole preoccupazione per le aziende. Gli aggressori sfruttano lo spear phishing per convincere vittime ignare a innescare esse stesse la compromissione tramite malware incorporato o URL malevoli. **McAfee Email Gateway** garantisce protezione da questi tipi di attacchi con svariate funzioni:

- **ClickProtect:** elimina le minacce che si annidano negli URL incorporati nei messaggi email con la scansione degli URL al momento del clic dell'utente. L'ispezione prevede il controllo della reputazione dell'URL e l'emulazione proattiva da parte di McAfee Gateway Anti-Malware Engine.
- **Integrazione con McAfee Advanced Threat Defense:** rileva il malware sofisticato e sfuggente con l'analisi approfondita del codice, statica e dinamica, eseguita sui file sospetti allegati alle email, bloccando i file pericolosi prima ancora che giungano in una casella di posta.
- **Integrazione con McAfee Global Threat Intelligence:** combina informazioni di rete locali e dati di intelligence globali sulla reputazione forniti da McAfee Global Threat Intelligence per garantire la forma di protezione più completa contro minacce, spam e malware in ingresso.

McAfee Global Threat Intelligence
McAfee Global Threat Intelligence (GTI) è un servizio su cloud di intelligence sulle minacce completo e in tempo reale che permette ai prodotti McAfee di bloccare le minacce informatiche su qualunque vettore: file, Web, messaggistica e rete. Tutelatevi in modo proattivo dagli abusi di fiducia con queste funzioni:

- **Reputazione dei certificati:** interrogate i feed in tempo reale relativi ai certificati noti — autentici e falsificati — per proteggere la vostra azienda da minacce come il malware firmato che può essere distribuito dalle reti pubblicitarie pericolose.
- **Reputazione dei file:** proteggetevi dalle imitazioni di applicazioni sul desktop, e tenetevi aggiornati sulle applicazioni che potrebbero essere vulnerabili agli attacchi dello stesso tipo di BERserk. Interrogate flussi di informazioni sui file — innocui, pericolosi e sconosciuti — in tempo reale per essere costantemente protetti.
- **Intelligence tramite la correlazione fra i vettori:** acquisite e correlate i dati di tutti i principali vettori di minacce — file, Web, email e rete — per rilevare minacce combinate come le reti pubblicitarie che distribuiscono malware firmato, le email di spear-phishing provenienti da mittenti apparentemente affidabili e i download guidati ospitati su siti Web pericolosi o siti "affidabili" compromessi.
- **Security Connected:** integratevi con altri prodotti per la sicurezza McAfee per garantirvi quanti più dati possibili sulle minacce, la correlazione più approfondita fra i dati e l'integrazione più completa fra i prodotti attualmente disponibile per proteggervi dagli attacchi che abusano della fiducia.

McAfee Vulnerability Manager

Gli attacchi come BERserk sono un esempio del panorama delle minacce in costante mutamento che influisce sul modello di fiducia. Capire se si è a rischio e fino a che punto si è vulnerabili a questi nuovi attacchi può essere un'impresa ardua. Ecco in che modo **McAfee Vulnerability Manager** e **McAfee Asset Manager** possono aiutare la vostra azienda a capire vulnerabilità come BERserk e ad adottare le misure più efficaci per porvi rimedio:

- **Scansione completa delle vulnerabilità:** McAfee Vulnerability Manager è una soluzione standalone estremamente scalabile per il rilevamento degli host, la gestione delle risorse, la valutazione delle vulnerabilità e la generazione di rapporti su qualsiasi dispositivo connesso alla rete. McAfee Vulnerability Manager può controllare se si è esposti al rischio BERserk cercando sistemi su cui sono installate versioni di Firefox, Chrome e altri prodotti che chiamano il codice di verifica delle firme RSA vulnerabile.
- **Personalizzazione delle scansioni per nuove minacce:** Foundstone Scripting Language (FSL) Editor può amplificare i controlli e gli aggiornamenti predefiniti per le minacce zero-day e le vulnerabilità come BERserk con script e controlli personalizzati per valutare il vostro ambiente. McAfee Vulnerability Manager è ora in grado di rilevare i sistemi vulnerabili a BERserk con i controlli predefiniti aggiornati al 24 settembre 2014.
- **Flessibilità nella generazione di rapporti e nella remediation:** McAfee Vulnerability Manager e McAfee Asset Manager operano in sinergia per garantire il monitoraggio e la gestione automatici delle scansioni, delle attività di remediation e di imposizione e della generazione di rapporti. In questo modo non dovrete perdere tempo per imparare procedure di emergenza e implementare processi ad hoc, eliminerete gli errori e proteggerete efficacemente un maggior numero di sistemi.
- **Conoscenza del grado di esposizione:** McAfee Asset Manager permette all'azienda di sapere quali sono i sistemi vulnerabili a BERserk correlando le scansioni delle vulnerabilità con le scansioni di rilevamento degli host. Identificare in tempo reale i sistemi con versioni vulnerabili delle applicazioni vi evita di perdere tempo a chiedervi se siete esposti al rischio e vi permette di concentrarvi sugli interventi di remediation.

McAfee Web Gateway

Malvertising, download guidati e URL pericolosi incorporati in URL affidabili sono solo alcuni dei metodi di attacco utilizzati per approfittare della fiducia degli utenti. Con **McAfee Web Gateway** potrete salvaguardare più efficacemente la vostra azienda da questo tipo di minacce.

- **McAfee Gateway Anti-Malware Engine:** l'analisi senza firma degli intenti filtra in tempo reale i contenuti dannosi dal traffico Web. L'emulazione e l'analisi del comportamento proteggono in modo proattivo contro gli attacchi mirati e zero-day. McAfee Gateway Anti-Malware Engine ispeziona i file e ne blocca il download nel caso in cui siano pericolosi. McAfee Web Gateway è la soluzione numero 1 sul mercato per la sua capacità di bloccare lo scaricamento del malware grazie alle sue esclusive funzioni di ispezione.
- **Integrazione con McAfee GTI:** i feed in tempo reale sulla reputazione di file e siti Web e la classificazione dei siti di McAfee GTI garantiscono protezione dalle minacce più recenti perché McAfee Web Gateway blocca i tentativi di connessione a siti Web di cui è nota la pericolosità o a siti che utilizzano reti pubblicitarie malevole.

Panoramica sulla soluzione

McAfee SiteAdvisor® Enterprise

Tenere il passo con un panorama delle minacce in costante evoluzione è difficile, soprattutto quando si tenta di proteggere gli utenti online da minacce come l'abuso di fiducia senza imporre policy restrittive che limitino le loro capacità di fruizione della Rete.

- **Facile identificazione di minacce come i siti Web pericolosi che si fingono legittimi:** grazie a un sistema di valutazione intuitivo con codifica a colori, **McAfee SiteAdvisor Enterprise** offre un ulteriore livello di protezione sul desktop, impedendo la connessione a siti Web di cui è noto l'intento malevolo e informando gli utenti del pericolo.
- **Sicurezza ottimizzata garantita da McAfee GTI:** McAfee GTI fornisce dati di intelligence sulle minacce in tempo reale a McAfee SiteAdvisor Enterprise e gli permette di valutare i siti Web secondo le informazioni più aggiornate.

McAfee Threat Intelligence Exchange

L'abuso di fiducia può assumere molte vesti; disporre di una piattaforma di intelligence in grado di adattarsi nel tempo alle esigenze del vostro ambiente è essenziale. **McAfee Threat Intelligence Exchange (TIE)** riduce in modo significativo l'esposizione agli attacchi grazie alla sua capacità di individuare minacce come i certificati malevoli rilevati nel vostro ambiente.

- **Reputazione dei certificati:** l'integrazione con McAfee GTI permette alla vostra azienda di proteggersi in tempo reale dagli attacchi che sfruttano codice malevolo firmato interrogando i feed in tempo reale relativi ai certificati autentici e falsificati già noti. McAfee TIE può tutelare i vostri endpoint dai certificati illegittimi mediante policy con gestione centralizzata che si possono implementare per proteggere sia gli endpoint connessi, sia gli endpoint offline.
- **Contrasto del DLL side loading, delle imitazioni di applicazioni e di altri tipi di attacchi:** una tecnologia difensiva all'avanguardia decide l'esecuzione o meno dei file combinando una logica basata su regole a seconda del contesto degli endpoint (file, processi e attributi ambientali) con le informazioni collettive sulle minacce.
- **Indicatori di compromissione:** importate gli hash dei file nocivi e i certificati illegittimi già noti in McAfee TIE per immunizzare il vostro ambiente da questi file di pericolosità nota mediante l'imposizione di policy. Se nell'ambiente viene attivato uno degli indicatori di compromissione (IoC), McAfee TIE può interrompere tutti i processi e le applicazioni associati a quell'IoC.

McAfee VirusScan® Mobile Security

- **Protezione dalle imitazioni di applicazioni:** grazie ai dati provenienti da McAfee GTI, **McAfee VirusScan Mobile Security** è in grado di neutralizzare le imitazioni di applicazioni che veicolano malware praticamente in tempo reale. Il prodotto rileva il malware in meno di 200 millisecondi senza interrompere le operazioni o la connettività wireless.

Mettere la vostra azienda al riparo dagli aggressori che tentano di sfruttare questo modello di fiducia dinamico può essere un'impresa ardua. Con la tecnologia di sicurezza McAfee potete proteggervi in modo proattivo dagli attacchi che tentano di abusare della fiducia degli utenti.

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com