Panoramica sulla soluzione

Proteggersi dai programmi potenzialmente indesiderati

I programmi potenzialmente indesiderati (PUP) sono trattati in maniera approfondita nel **Report McAfee® Labs sulle minacce: febbraio 2015**. Qualsiasi applicazione che risulti utile per un utente ma che presenti un rischio intrinseco concreto può essere considerata un programma potenzialmente indesiderato. Le applicazioni in genere non informano gli utenti di questi rischi. A differenza di trojan, virus, rootkit e altre forme di malware, i programmi potenzialmente indesiderati solitamente non rubano le identità o le credenziali bancarie degli utenti, né alterano i file di sistema. Questi programmi rientrano in una "zona grigia" per quanto attiene alla loro classificazione: in molti casi offrono dei vantaggi, ma rappresentano anche un rischio per l'utente. Spesso sono difficili da rilevare e da classificare.

Ecco alcuni dei comportamenti comuni adottati generalmente dai programmi potenzialmente indesiderati:

- Modificano le impostazioni del sistema, ad esempio la configurazione del browser, senza autorizzazione.
- Nascondono un programma non richiesto all'interno di un'applicazione legittima.
- Raccolgono di nascosto informazioni sull'utente, ne registrano le abitudini di navigazione e la configurazione del sistema.
- Nascondono l'installazione dell'applicazione.
- Rendono difficile la disinstallazione.
- Sono distribuiti da pubblicità ambigue o ingannevoli.

I programmi potenzialmente indesiderati possono assumere molteplici forme:

- **Adware**: distribuisce pubblicità principalmente tramite i browser.
- **Cracker/rivelatore di password**: rende visibile la password nascosta di un'applicazione.
- **Strumento di amministrazione remota**: monitora le attività dell'utente sul dispositivo in cui è installato o consente il controllo da remoto del sistema senza l'autorizzazione dell'utente o a sua insaputa.

intel Security

- **Keygen**: genera le chiavi del prodotto di applicazioni legittime.
- **Dirottatore del browser**: modifica la home page, la pagina di ricerca, le impostazioni del browser, ecc.
- **Strumenti di hacking**: applicazioni autonome che possono agevolare le intrusioni nei sistemi o la perdita di dati cruciali.
- **Proxy**: reindirizza o nasconde le informazioni relative all'indirizzo IP.
- **Strumenti di monitoraggio:** applicazioni spyware o keylogger che registrano i tasti premuti sulla tastiera e le comunicazioni personali, monitorano le attività online degli utenti o acquisiscono schermate a loro insaputa.

Ecco le principali differenze fra programmi potenzialmente indesiderati e altri tipi di malware come trojan, ransomware, bot e virus:

Tecniche	Programmi potenzialmente indesiderati	Altro malware: trojan, virus, bot
Metodo di installazione	Normale procedura di installazione delle applicazioni, talvolta con un contratto di licenza. Spesso per l'installazione completa su un sistema sono necessari l'intervento e il consenso dell'utente.	Installato come programma autonomo senza alcun intervento dell'utente. Opera prevalentemente come file indipendente.
Tipo di pacchetto	Distribuiti insieme ad applicazioni innocue e installati di nascosto insieme a queste.	File autonomi con pochi componenti aggiuntivi. Non presentati sotto forma di pacchetti di installazione.
Disinstallazione	A volte il pacchetto contiene un programma di disinstallazione che consente la rimozione del software. Spesso la procedura di disinstallazione è difficile.	Gli eseguibili rendono ancora più complicata l'eliminazione del malware a causa delle associazioni stabilite con altri processi, handle di processi e altri collegamenti complessi. Poiché non si tratta di pacchetti di installazione, non compaiono nel Pannello di controllo.
Comportamento	Visualizzano pubblicità e finestre pop-up o pop-under indesiderate. Modificano le impostazioni del browser, raccolgono dati sull'utente e sul sistema o consentono il controllo da remoto del sistema all'insaputa dell'utente o senza la sua autorizzazione.	Ruba i dati bancari e di identificazione personale, modifica i file di sistema, rende il sistema inutilizzabile, chiede riscatti, ecc.
Natura furtiva	In genere il comportamento non è furtivo.	Può nascondere file, cartelle, voci di registro e traffico di rete.

Fra tutte le categorie di programmi potenzialmente indesiderati, gli adware hanno catalizzato l'attenzione dei fornitori di soluzioni di sicurezza non tanto a causa della pubblicità indesiderata, quanto per il modo in cui abusano della fiducia. Gli adware sono diventati più intelligenti grazie all'implementazione di varie tecniche che ne garantiscono la presenza costante sui sistemi infetti. Ecco alcuni dei metodi che utilizzano:

- Processo autonomo eseguito in memoria
- File DLL COM (Component object model) e non COM con funzioni studiate specificamente per una determinata applicazione
- Chiavi di registro di BHO (browser helper object)
- DLL associate a processi di sistema
- Estensioni e plug-in dei browser
- Servizi di sistema registrati
- Componenti dei driver di dispositivo che eseguono funzioni di controllo dei dispositivi
- Driver filtro di basso livello
- Trojan recapitati come payload

Panoramica sulla soluzione

I programmi potenzialmente indesiderati di solito si propagano abusando della fiducia di utenti innocenti, come illustrato nel **Report McAfee Labs sulle minacce: novembre 2014**. Le più comuni tecniche di distribuzione per i programmi potenzialmente indesiderati comprendono:

- Veicolazione nascosta attraverso applicazioni legittime
- Social engineering
- Vendita di Mi piace su Facebook
- Pubblicazione di messaggi truffa su Facebook
- Uso fraudolento di Google AdSense
- Estensioni e plug-in indesiderati per i browser
- Installazione forzata insieme ad applicazioni legittime

Che cosa può fare Intel Security per aiutarvi a proteggervi dai programmi potenzialmente indesiderati

McAfee Application Control

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 e può essere utile per proteggere la vostra azienda dai programmi potenzialmente indesiderati.

- **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 l'esposizione ai programmi potenzialmente indesiderati impedendo l'esecuzione dell'adware noto.
- **Reputazione dei file**: l'integrazione con **McAfee Global Threat Intelligence** (McAfee GTI) permette a McAfee Application Control di interrogare flussi di informazioni in tempo reale sui tipi di file noti — innocui, pericolosi e sconosciuti — per facilitarne l'inserimento nella whitelist e mantenere la vostra azienda sempre al corrente delle applicazioni già note come programmi potenzialmente indesiderati.
- **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.

McAfee Web Gateway

Malvertising, download guidati e URL pericolosi incorporati in siti Web affidabili sono solo alcuni dei metodi di attacco utilizzati per distribuire programmi potenzialmente indesiderati. **McAfee Web Gateway** è un prodotto efficace con cui potrete ottimizzare la protezione della vostra azienda da questo tipo di minaccia.

- **McAfee Gateway Anti-Malware Engine**: l'analisi senza firma degli intenti filtra in tempo reale i contenuti dannosi dal traffico Web. McAfee Gateway Anti-Malware Engine ispeziona i file e ne blocca il download nel caso in cui siano pericolosi.
- **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 Global Threat Intelligence

McAfee Global Threat Intelligence (McAfee GTI) è un servizio 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 dai programmi potenzialmente indesiderati con queste funzioni:

- **Intelligence tramite la correlazione fra i vettori**: il servizio raccoglie e stabilisce correlazioni fra i dati relativi a tutti i principali vettori di minacce (file, Web, email e rete) per rilevare minacce combinate come le reti pubblicitarie che recapitano malware firmato.
- **Piattaforma completa di intelligence sulle minacce**: raccoglie informazioni sulle minacce da milioni di sensori posti sui prodotti McAfee implementati dai clienti su endpoint, Web, email, sistemi di prevenzione delle intrusioni in rete e firewall.
- **Reputazione dei certificati**: il servizio interroga 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.
- **Security Connected**: integrato con altri prodotti per la sicurezza McAfee per garantire 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 dall'adware.

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 i programmi potenzialmente indesiderati 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

Disporre di una piattaforma di intelligence in grado di adattarsi nel tempo alle esigenze del vostro ambiente è importante. **McAfee Threat Intelligence Exchange** riduce considerevolmente l'esposizione a questi tipi di attacchi grazie all'individuazione delle minacce immediate come file o applicazioni sconosciute in esecuzione nell'ambiente.

- **Informazioni complete sulle minacce**: le informazioni complete sulle minacce provenienti da fonti di intelligence globali sono facilmente personalizzabili. Può trattarsi di feed di McAfee GTI o di terzi, contenenti informazioni locali sulle minacce ricavate da dati su eventi passati o in tempo reale inviate tramite endpoint, gateway e altri componenti della sicurezza.
- **Prevenzione dell'esecuzione e remediation**: McAfee Threat Intelligence Exchange può intervenire e impedire l'esecuzione di applicazioni sconosciute nell'ambiente. Se un'applicazione di cui in un primo tempo era stata consentita l'esecuzione si rivela malevola, McAfee Threat Intelligence Exchange può disabilitare i processi in esecuzione a essa associati in tutto l'ambiente grazie alle sue potenti funzionalità di gestione centralizzata e di imposizione delle policy.

- **Reputazione dei certificati**: l'integrazione con McAfee GTI protegge la vostra azienda 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 Threat Intelligence Exchange 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.

McAfee VirusScan® Enterprise

Con **McAfee VirusScan Enterprise** è semplice rilevare ed eliminare il malware, adware compreso. McAfee VirusScan Enterprise utilizza il premiato motore di scansione McAfee per proteggere i vostri sistemi da virus, worm, rootkit, trojan e altre minacce avanzate.

- **Protezione proattiva dagli attacchi**: integra la tecnologia antimalware e la prevenzione delle intrusioni per proteggere dagli attacchi che sfruttano gli exploit da overflow del buffer indirizzati alle vulnerabilità delle applicazioni.
- **Rilevamento ed eliminazione del malware imbattibili**: protegge da minacce come rootkit e trojan con l'analisi avanzata dei comportamenti. Neutralizza il malware all'istante mediante tecniche come il blocco delle porte, il blocco in base al nome dei file, il blocco di cartelle/directory e delle condivisioni di file e il tracciamento e il blocco delle infezioni.
- **Sicurezza in tempo reale grazie all'integrazione con McAfee GTI**: protezione da minacce note ed emergenti in tutti i vettori di minacce (file, Web, email e reti) con il supporto della più completa piattaforma di intelligence sulle minacce disponibile sul mercato.

Proteggere la vostra azienda dai programmi potenzialmente indesiderati che tentano di insidiare il modello di fiducia tradizionale con comportamenti subdoli e non richiesti può essere problematico. Abbinare la ricerca all'avanguardia nel settore di McAfee Labs e la tecnologia di Intel Security può aiutare la vostra azienda a difendersi dai programmi potenzialmente indesiderati.

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