Panoramica sulla soluzione

# Bloccare i trojan backdoor

Lo strumento di amministrazione remota (Remote Administration Tool, RAT) Adwind è un backdoor trojan basato su Java che attacca varie piattaforme che supportano appunto i file Java. Adwind non sfrutta alcuna vulnerabilità. La circostanza più comune per lo scatenarsi di un'infezione è l'esecuzione del malware da parte dell'utente facendo doppio clic sul file .jar, arrivato come allegato email, oppure aprendo un documento Microsoft Word infetto. L'infezione ha inizio se l'utente ha Java Runtime Environment installato. Quando il file .jar dannoso viene eseguito nel sistema preso di mira, il malware si installa in modo invisibile all'utente e si connette a un server remoto tramite una porta preconfigurata, per ricevere i comandi dell'aggressore ed eseguire ulteriori attività ostili.

## Cenni storici

Adwind si è evoluto dal RAT Frutas. Frutas è un RAT basato su Java, scoperto nel 2013, che è stato largamente usato in campagne email di phishing contro importanti aziende dei settori telecomunicazioni, minerario, pubblico e finanziario in Europa e Asia.

Dall'inizio del primo trimestre 2015 McAfee® Labs ha assistito a un notevole aumento del numero di file .jar inviati e identificati come Adwind.

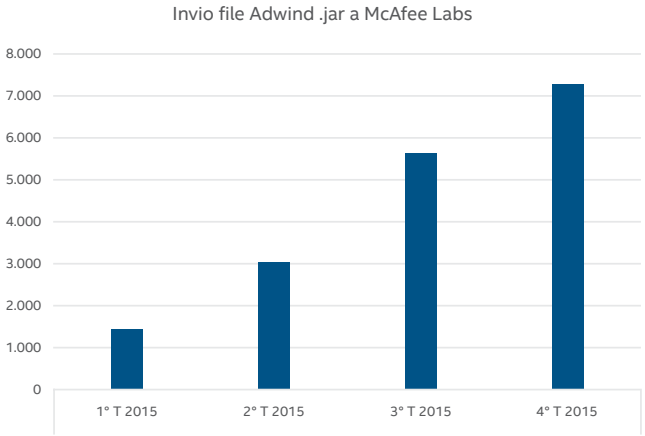


**Figura 1.** Il numero dei file .jar di Adwind inviati a McAfee Labs è aumentato a 7.295 nel quarto trimestre 2015 rispetto ai 1.388 del primo trimestre 2015, con una crescita del 426%.

intel Security

## La catena dell'infezione

Adwind viene tipicamente propagato per mezzo di campagne di spam che impiegano allegati email contenenti malware, pagine web compromesse e download guidati. Il suo meccanismo di distribuzione si è evoluto: le prime campagne di spam duravano giorni o settimane e usavano lo stesso oggetto dell'email o lo stesso nome dell'allegato. Questa uniformità aiutava i programmi di sicurezza a rilevare e mitigare rapidamente Adwind. Ora invece le campagne di spam delle macro sono di breve durata, cambiano frequentemente gli oggetti e creano gli allegati con cura, tutto questo per evitare il rilevamento di Adwind.

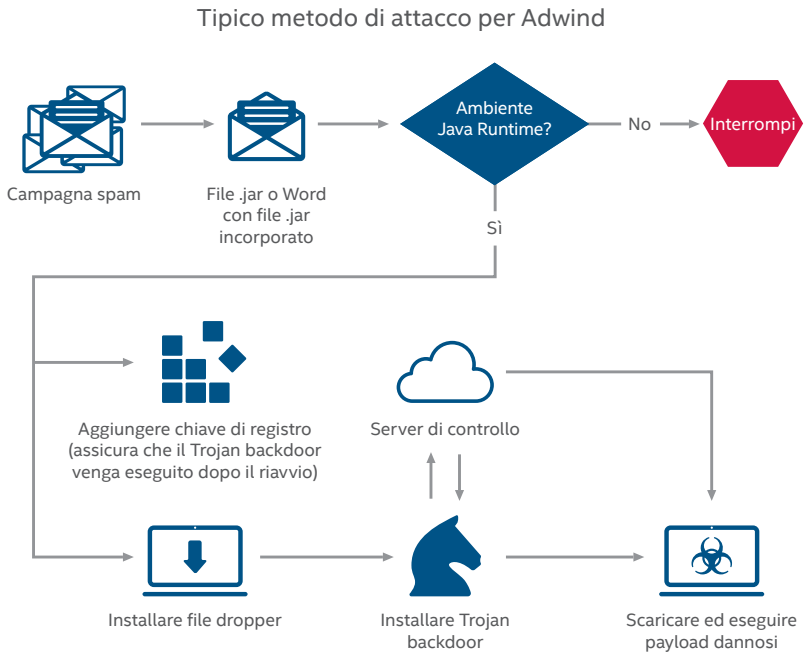


**Figura 2.** La catena d'infezione di Adwind.

Dopo l'infezione di un sistema da parte di Adwind, lo abbiamo osservato registrare le battute sulla tastiera, modificare ed eliminare file, scaricare ed eseguire altro malware, acquisire schermate, accedere alla videocamera del sistema, prendere il controllo di mouse e tastiera, aggiornarsi e svolgere altre attività.

## Come Intel Security aiuta a proteggerti contro Adwind e altri trojan backdoor

La tecnologia Intel Security aiuta a proteggere contro i trojan backdoor come Adwind. Di seguito alcuni prodotti che possono contribuire a bloccare questo tipo di attacco.

### McAfee® Threat Intelligence Exchange

Disporre di una piattaforma di intelligence in grado di adattarsi nel tempo alle esigenze di un ambiente è importante. **McAfee Threat Intelligence Exchange** riduce considerevolmente l'esposizione ai trojan backdoor grazie all'individuazione delle minacce immediate come file o applicazioni sconosciute in esecuzione nell'ambiente.

- **Informazioni complete sulle minacce:** personalizza facilmente le informazioni complete sulle minacce provenienti dalle fonti dislocate in tutto il mondo. Queste ultime possono essere feed di **McAfee Global Threat Intelligence** (McAfee GTI) oppure di terze parti, contenenti le informazioni locali sulle minacce derivanti da eventi passati o in fase di svolgimento, 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 ammessa all'esecuzione viene in seguito giudicata dannosa, McAfee Threat Intelligence Exchange disattiva in tutto l'ambiente i processi in esecuzione a essa associati, grazie alle potenti capacità di gestione centralizzata e di imposizione delle policy del prodotto.
- **Visibilità:** McAfee Threat Intelligence Exchange può rilevare tutti i file eseguibili compressi e la loro esecuzione iniziale all'interno dell'ambiente, oltre a tutte le modifiche che si verificano in seguito. Tale visibilità sulle azioni di un'applicazione o processo, dall'installazione fino al momento contingente, velocizza risposta e remediation.
- **Indicatori di compromissione:** importazione degli hash dei file nocivi e immunizzazione dell'ambiente da queste minacce note mediante l'imposizione di policy. Se nell'ambiente scatta uno degli indicatori, McAfee Threat Intelligence Exchange è in grado di terminare tutti i processi e le applicazioni associati agli indicatori di compromissione.

**McAfee Advanced Threat Defense**

**McAfee Advanced Threat Defense** è un prodotto per il rilevamento del malware multilivello che si avvale di più motori di ispezione. I motori eseguono un controllo basato su firme e reputazione, emulazione in tempo reale, analisi completa del codice statico e sandboxing dinamico su oggetti sospetti per proteggere dal malware che inizialmente deposita un file binario nel sistema preso di mira.

- **Rilevamento basato sulle firme:** rileva virus, worm, rootkit, trojan, buffer overflow e attacchi misti. La knowledgebase completa viene creata e sostenuta da McAfee Labs.
- **Rilevamento basato sulla reputazione:** controlla la reputazione dei file mediante McAfee GTI per rilevare le minacce emergenti.
- **Analisi statica ed emulazione in tempo reale:** consentono di individuare rapidamente minacce zero-day e trojan backdoor non identificati dalle tecniche basate su firma o secondo la reputazione.
- **Analisi completa del codice statico:** esegue il reverse engineering del codice del file per valutarne tutti gli attributi e i gruppi di istruzioni, oltre che per analizzarne in modo completo il codice sorgente senza eseguirlo. Le funzioni esaustive di decompressione aprono tutti i tipi di file compressi e di archivi per abilitare l'analisi completa e la classificazione del malware, consentendo alla tua azienda di comprendere la minaccia posta da malware specifico.
- **Analisi dinamica nella sandbox:** Per un file la cui sicurezza non può essere stabilita attraverso i motori di ispezione precedenti, McAfee Advanced Threat Defense può eseguire il codice del file in un ambiente di runtime virtuale e osservare il comportamento risultante. Gli ambienti virtuali possono essere configurati per soddisfare gli ambienti host. McAfee Advanced Threat Defense supporta immagini personalizzate del sistema operativo di Microsoft Windows XP (32 e 64 bit), Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows Server 2003, Windows Server 2008 (64 bit) e Android.

**McAfee Network Security Platform**

**McAfee Network Security Platform** è un prodotto di sicurezza straordinariamente intelligente, in grado di scoprire e bloccare le minacce più sofisticate presenti nella rete. Utilizzando tecniche avanzate di rilevamento ed emulazione, va ben oltre la mera corrispondenza degli schemi per difendere dagli attacchi occulti con estrema accuratezza. Il nostro approccio integrato e aperto alla gestione della sicurezza ottimizza le operazioni unendo i feed in tempo reale di McAfee GTI ai dati contestuali completi riferiti a utenti, dispositivi e applicazioni per una risposta rapida e accurata agli attacchi che si sviluppano sulle reti.

- **Difese senza firma:** Le minacce avanzate e sconosciute come il malware occulto, le minacce persistenti avanzate (APT), i bot e gli attacchi zero-day spesso aggirano le difese basate su firme. McAfee Network Security Platform dispone di molteplici motori avanzati che non richiedono firme per proteggere da tali minacce avanzate e sconosciute. Il rilevamento senza firma analizza il contenuto web, i file PDF, i file Flash e il comportamento di JavaScript in tempo reale tramite l'emulazione.
- **Endpoint Intelligence Agent:** McAfee Network Security Platform fornire correlazione del traffico degli endpoint in tempo reale e per flusso. L'agente combina l'analisi comportamentale dei flussi del traffico di rete con molteplici sorgenti di intelligence sulla reputazione. Questa tecnologia sfrutta le informazioni nella rete e in ogni host di Windows per rivelare le relazioni fra gli eseguibili e i flussi di traffico nella rete per identificare in tempo reale connessioni di rete ed eseguibili pericolosi. L'agent incorpora informazioni contestuali dettagliate sul processo per gli attacchi, blocca le comunicazioni pericolose, previene la diffusione di malware avanzato e, infine, mette in quarantena e pone rimedio ai sistemi host compromessi.

**McAfee Web Gateway**

Malvertising, download guidati e URL pericolosi incorporati in email di phishing sono alcuni dei metodi di attacco principali utilizzati per distribuire trojan backdoor. **McAfee Web Gateway** è un prodotto efficace con cui potrai ottimizzare la protezione della tua 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. 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.
- **Integrazione con McAfee GTI:** i feed di intelligence 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 ai siti web di cui è nota la pericolosità o ai siti che notoriamente agiscono come server di controllo.

Oltre ai prodotti Intel Security di cui sopra, consigliamo una categoria aggiuntiva di tecnologia per la sicurezza.

- **Protezione del gateway email:** La maggior parte dei trojan backdoor penetra in un sistema attraverso un allegato di un messaggio email, perciò un prodotto efficace per la protezione del gateway email che analizza tutti gli allegati alla ricerca di malware rappresenta una difesa corretta contro questo tipo di attacco.



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