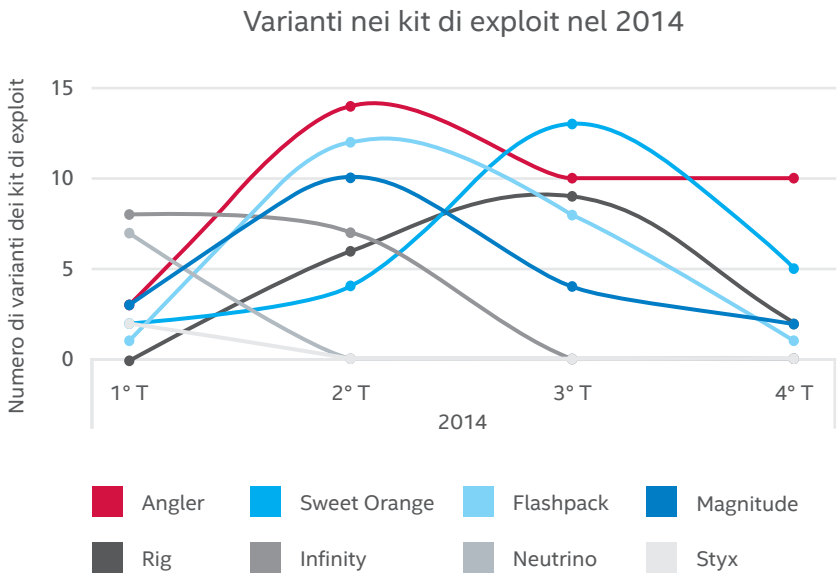
Panoramica sulla soluzione

Sconfiggere il kit di exploit Angler

Un kit di exploit è un pacchetto software pronto all'uso che contiene attacchi preconfezionati e di facile utilizzo contro vulnerabilità note e sconosciute (zero-day). Questi toolkit sfruttano le vulnerabilità sul lato client, prendendo di mira prevalentemente il browser e le applicazioni a cui si può accedere tramite il browser. I kit di exploit sono anche in grado di monitorare le metriche delle infezioni e sono dotati di efficaci sistemi di controllo.

Che cos'è il kit di exploit Angler?

Il kit di exploit Angler è analizzato in modo approfondito nel **Report McAfee® Labs sulle minacce: febbraio 2015**. La prevalenza e la notorietà di Angler sono aumentate nella seconda metà del 2014 a causa di caratteristiche come l'infezione "fileless" (iniezione in memoria), il rilevamento di macchine virtuali e prodotti di sicurezza e la capacità di recapitare una grande varietà di payload fra cui trojan bancari, rootkit, ransomware, CryptoLocker e trojan backdoor. Inoltre, Angler non richiede competenze tecniche specifiche per essere usato in modo efficace, e la sua disponibilità sui mercati "neri" online ne ha determinato la massiccia diffusione.



Fonte: McAfee Labs, 2015

intel Security

Panoramica sulla soluzione

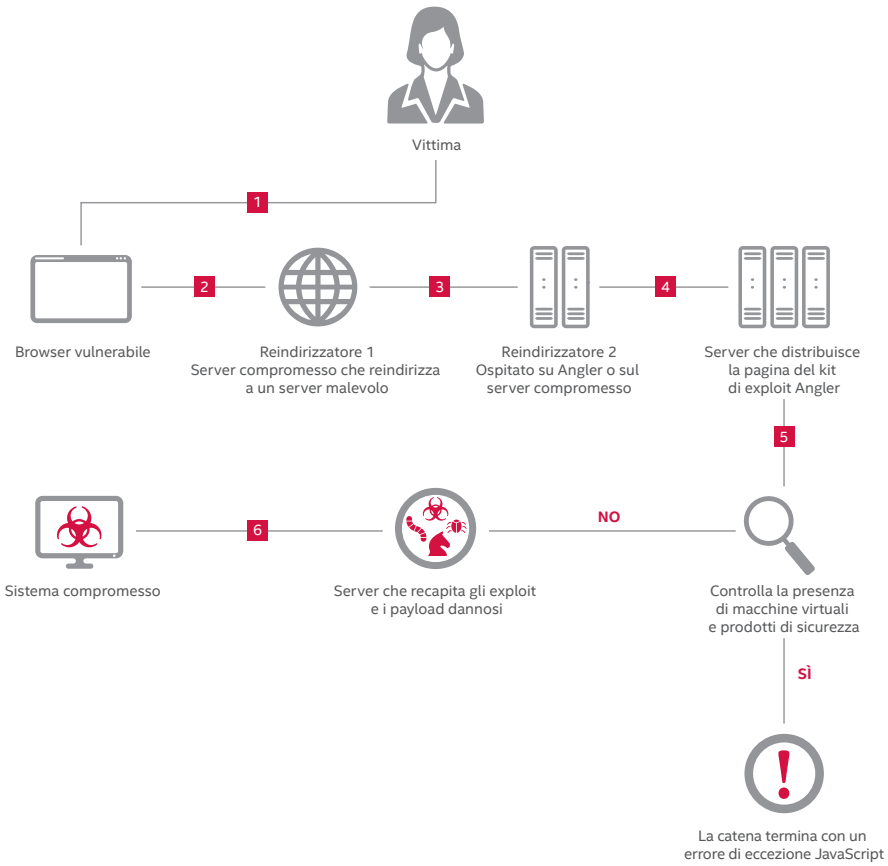
Angler cambia spesso criteri e payload per ostacolare il rilevamento del kit di exploit attivo da parte dei prodotti di sicurezza ed esegue varie manovre elusive per evitare di essere scoperto:

- Utilizza due livelli di reindirizzatori prima di raggiungere la pagina di destinazione.
- Consente di visitare i server Web compromessi che ospitano la pagina di destinazione una sola volta da un determinato indirizzo IP. È chiaro che gli aggressori controllano attivamente gli host.
- Rileva la presenza di macchine virtuali e di prodotti di sicurezza nel sistema.
- Genera garbage e chiamate inutili per rendere più difficile la decompilazione.
- Crittografa tutti i payload al momento del download e li decrittografa sul dispositivo compromesso.
- Utilizza l'infezione fileless (è distribuito direttamente in memoria).

L'infezione dei sistemi da parte del kit di exploit Angler avviene in diversi passaggi:

- La vittima accede a un server Web compromesso tramite un browser vulnerabile.
- Il server Web compromesso la reindirizza a un server intermedio.
- Il server intermedio la reindirizza a un server Web malevolo su cui è ospitata la pagina di destinazione del kit di exploit.
- La pagina di destinazione controlla la presenza di plug-in vulnerabili (Java, Flash e Silverlight) e la loro versione.
- Quando rileva un browser o dei plug-in vulnerabili, il kit di exploit recapita il payload appropriato e infetta il dispositivo.

La catena di infezione del kit di exploit Angler



Proteggersi dal kit di exploit Angler

Ecco alcuni dei metodi consigliati per proteggere i sistemi dal kit di exploit Angler:

- Affidarsi a un fornitore di servizi Internet attento alla sicurezza che implementi procedure antispam e antiphishing efficaci.
- Abilitare gli aggiornamenti automatici del sistema operativo o scaricarne regolarmente gli aggiornamenti per mantenerlo aggiornato con le patch più recenti contro le vulnerabilità note. Installare le patch degli altri sviluppatori software non appena vengono rese disponibili. Un computer dotato di tutte le patch del caso e protetto da un firewall è la difesa migliore contro gli attacchi di trojan e spyware.
- Aprire gli allegati con estrema cautela. Configurare il software antivirus per la scansione automatica di tutti gli allegati di email e messaggi immediati. Accertarsi che i programmi email non aprano automaticamente gli allegati o visualizzino automaticamente la grafica e disattivare il riquadro di anteprima. Non aprire mai le email indesiderate o gli allegati inattesi, anche se provenienti da persone conosciute.
- Fare attenzione al phishing basato sullo spam: evitare di fare clic sui link presenti nelle email o nei messaggi immediati.
- Usare un plug-in del browser per bloccare l'esecuzione di script e di iframe.

Che cosa può fare Intel Security per aiutarvi a proteggervi dal kit di exploit Angler

McAfee Web Gateway

Malvertising, download guidati e URL pericolosi incorporati in siti Web affidabili sono solo alcuni dei metodi di attacco utilizzati per distribuire il kit di exploit Angler. **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. 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 Global Threat Intelligence (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 a siti Web di cui è nota la pericolosità o a siti che utilizzano reti pubblicitarie malevole.

McAfee VirusScan® Enterprise

Con **McAfee VirusScan Enterprise** è semplice rilevare ed eliminare il malware come quello recapitato da Angler. McAfee VirusScan Enterprise utilizza il premiato motore di scansione McAfee per proteggere i vostri file 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.

Panoramica sulla soluzione

McAfee Advanced Threat Defense
McAfee Advanced Threat Defense è una soluzione di rilevamento del malware multilivello che si avvale di più motori di ispezione. Combinando l'analisi basata sulle firme e sulla reputazione eseguita da una serie di motori di ispezione, l'emulazione in tempo reale, l'analisi completa del codice statico e il sandboxing dinamico, McAfee Advanced Threat Defense protegge dai kit di exploit più diffusi come Angler e dal malware che questi distribuiscono.

- **Rilevamento basato sulle firme**: rileva virus, worm, spyware, bot, trojan, overflow del buffer e attacchi misti. La sua knowledge base completa, creata e aggiornata da McAfee Labs, contiene attualmente oltre 150 milioni di firme, comprese quelle di Angler e delle sue varianti.
- **Rilevamento basato sulla reputazione**: controlla la reputazione dei file mediante la rete McAfee GTI per rilevare le minacce emergenti.
- **Analisi statica ed emulazione in tempo reale**: consentono di individuare rapidamente minacce zero-day e malware non identificati dalle tecniche basate su firma o secondo la reputazione.
- **Analisi completa del codice statico**: decompila il codice dei file per valutarne tutti gli attributi e i set di istruzioni e analizzare in modo approfondito il codice sorgente senza eseguirlo. Grazie alle funzioni complete di decompressione, è in grado di aprire qualsiasi tipo di file compresso per l'analisi completa del malware e la sua classificazione. Questo consente alla vostra azienda di capire il genere di minaccia rappresentato da un malware specifico.
- **Analisi dinamica nella sandbox**: esegue il codice del file in un ambiente di runtime virtuale e osserva il comportamento che ne risulta. Gli ambienti virtuali si possono configurare in modo da riprodurre gli ambienti host della vostra azienda e supportano immagini personalizzate dei sistemi operativi Windows 7 (32/64 bit), Windows XP, Windows Server 2003, Windows Server 2008 (64 bit) e Android.

McAfee Network Security Platform
McAfee Network Security Platform è studiato per eseguire ispezioni approfondite del traffico di rete. Il prodotto combina una serie di tecniche di ispezione avanzate (tra cui l'analisi completa del protocollo, la reputazione delle minacce, l'analisi del comportamento e l'analisi avanzata del malware) per rilevare e prevenire sia gli attacchi noti che quelli zero-day sulla rete.

- **Difesa completa contro il malware**: combina la reputazione dei file di McAfee GTI, l'analisi approfondita dei file con ispezione di JavaScript e l'analisi avanzata e senza firma del malware per rilevare e neutralizzare le minacce zero-day, il malware personalizzato e altri attacchi di virus occulti.
- **Sfrutta tecniche di ispezione avanzate**: comprende analisi completa dei protocolli, reputazione delle minacce e analisi del comportamento per rilevare e prevenire sia gli attacchi di rete di tipo noto, sia quelli zero-day.
- **Integrazione con McAfee GTI**: abbina i feed di reputazione dei file in tempo reale, di reputazione degli indirizzi IP e di localizzazione geografica a dati contestuali completi su utenti, dispositivi e applicazioni per rispondere rapidamente e con precisione agli attacchi veicolati tramite la rete.
- **Security Connected**: grazie all'utile integrazione fra i due prodotti, McAfee Network Security Platform può inviare i file sospetti scoperti nel traffico monitorato a McAfee Advanced Threat Defense e negarne o consentirne l'esecuzione a seconda dei risultati ottenuti da McAfee Advanced Threat Defense.

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 associati all'applicazione in tutto l'ambiente grazie alle sue potenti funzionalità di gestione centralizzata e di imposizione delle policy.
- **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. La possibilità di rilevare le azioni di un'applicazione o di un processo fin dall'installazione iniziale consente una risposta e un intervento di remediation più rapidi.
- **Indicatori di compromissione (IoC)**: importate gli hash dei file nocivi in McAfee Threat Intelligence Exchange per immunizzare il vostro ambiente da questi file di pericolosità nota mediante l'imposizione di policy. Se nell'ambiente viene attivato uno degli IoC, McAfee Threat Intelligence Exchange può interrompere tutti i processi e le applicazioni associati a quell'IoC.

La crescente diffusione di kit di exploit facili da utilizzare come Angler fa riflettere sul fatto che il panorama delle minacce è in continua evoluzione. La tecnologia Intel Security può aiutare la vostra azienda a proteggersi in modo proattivo da minacce come il kit di exploit Angler sia sugli endpoint, sia sulla rete.

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