Gli autori degli attacchi sfruttano le falle nella difesa

Gli autori degli attacchi sviluppano e perfezionano in continuazione nuove tecniche in grado di eludere gli strumenti di rilevamento e nascondere l'attività dannosa. I team di sicurezza sono costretti a migliorare le strategie per proteggere l'azienda e gli utenti da attacchi sempre più sofisticati.

Autori degli attacchi

Metodi di attacco diversificati



L'attività di spam dannosa torna a crescere



Java si sono ridotti del 34%

Gli exploit



Vettori preferenziali degli attacchi:



Microsoft Internet Explorer Microsoft

Silverlight

Malvertising 250% Picco di elementi aggiuntivi a ottobre

Elementi aggiuntivi

dannosi vengono scaricati inconsapevolmente da fonti non attendibili





in settori altamente mirati diventino vittima di Clickfraud e Adware



uno dei problemi più pressanti Percentuale di utenti che eseguono

Microsoft Google Internet Explorer Chrome

le ultime versioni:

Responsabili

della sicurezza Difese inefficaci

Prima dell'attacco

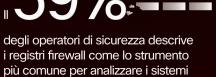
Solo il



strumenti di difesa, mentre gli altri lasciano lacune sfruttabili dagli autori degli attacchi

di tutte le versioni OpenSSL ha più di 50 mesi ed espone potenzialmente chiavi di crittografia e password

Durante l'attacco



compromessi, con dati limitati e assenza di contesto Solo il -3%

oltre il 50% delle aziende non

degli operatori di sicurezza dichiara di sfruttare attività di gestione delle identità e di provisioning, quindi

creano uno stato di infezione invisibile,

persistente e incontrollato.

dispone del contesto relativo alle identità e alle attività degli utenti 12210110111111

Dopo l'attacco



Ad esempio, solo il

degli operatori di sicurezza mette in quarantena o rimuove metodicamente

Una volta all'interno, gli autori degli attacchi

In base a dati del 2014