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

250% SPAM

L'attività di spam dannosa torna a crescere

Downloader **6 volte** più diffusa rispetto agli altri tipi di malware

Gli exploit Java si sono ridotti del **34%**

L'attività dei kit di exploit è scesa de ll' **88%**

Vettori preferenziali degli attacchi:

- PDF
- Adobe Flash
- Microsoft Internet Explorer
- Microsoft Silverlight

Malvertising **250%**

Picco di elementi aggiuntivi a ottobre

Utenti complici

2X

La probabilità che gli utenti in settori altamente mirati diventino vittima di Clickfraud e Adware

Elementi aggiuntivi dannosi vengono scaricati inconsapevolmente da fonti non attendibili

I browser privi di patch rappresentano uno dei problemi più pressanti

Percentuale di utenti che eseguono le ultime versioni:

Microsoft Internet Explorer	Google Chrome
10%	64%

Responsabili della sicurezza

Difese inefficaci

Prima dell'attacco

Solo il **40%** dei CISO dichiara di utilizzare patch e configurazione come strumenti di difesa, mentre gli altri lasciano lacune sfruttabili dagli autori degli attacchi

Il **56%** di tutte le versioni OpenSSL ha più di 50 mesi ed espone potenzialmente chiavi di crittografia e password

Durante l'attacco

Il **59%** degli operatori di sicurezza descrive i registri firewall come lo strumento più comune per analizzare i sistemi compromessi, con dati limitati e assenza di contesto

Solo il **43%** degli operatori di sicurezza dichiara di sfruttare attività di gestione delle identità e di provisioning, quindi oltre il 50% delle aziende non dispone del contesto relativo alle identità e alle attività degli utenti

Dopo l'attacco

Non è stato identificato alcun metodo ottimale per eliminare le cause degli incidenti di sicurezza:

Ad esempio, solo il **55%** degli operatori di sicurezza mette in quarantena o rimuove metodicamente le applicazioni dannose

Una volta all'interno, gli autori degli attacchi creano uno stato di infezione invisibile, persistente e incontrollato.

In base a dati del 2014

Scarica il Report annuale sulla sicurezza 2015
www.cisco.com/go/asr2015

cisco