

## Attacchi in corso su Vulnerabilità in Internet Explorer

**Proto:** N060918.

Con la presente Yoroï desidera informarLa relativamente ad emergenti **cyber-attacchi** volti alla compromissione di client di rete per via dello sfruttamento di vulnerabilità all'interno di **Internet Explorer**. La criticità in questione è nota con l'identificativo **CVE-2018-8373**.

A seguito della pubblicazione dei dettagli tecnici relativi alla problematica, sono stati registrati tentativi di attacco di varia natura che mirano a sfruttare lacune nel motore VBScript all'interno delle recenti versioni dei browser web Microsoft.

La pericolosità di questa vulnerabilità risiede nella limitata interazione utente richiesta: un eventuale attaccante di rete può essere in grado di eseguire codice arbitrario sulla macchina vittima a seguito della sola navigazione su siti web compromessi o malevoli.

La criticità è stata sfruttata all'interno della serie di exploit "*Double Kill*" operati dall'attore malevolo "*Dark Hotel*" in ambito cyber-espionage (rif. Early Warning [NH051b](#)), oltre che in recenti campagne di propagazione di varianti malware RAT/Quasar.


[illegible]

Figura 1. Esempio payload malevolo caricato a seguito dello sfruttamento di CVE-2018-8373

Il Produttore ha trattato la problematica in un apposito [bollettino di sicurezza](#) pubblicato lo scorso Agosto, dove sono stati resi disponibili aggiornamenti di sistema per i browser Internet Explorer 9, 10 e 11.

Le circostanze recentemente osservate, la tipologia di vulnerabilità ed il suo abuso da parte di più attori malevoli, suggeriscono un **crescente rischio** di tentativi di compromissioni facenti uso di schemi di attacco di tipologia *"Watering Hole"*, *"Malvertising"* ed *"Exploit-Kit"*. A questo proposito Yoroj suggerisce di **verificare lo stato di aggiornamento** del Vostro parco macchine Microsoft.

Yoroi consiglia infine di mantenere alto il livello di consapevolezza degli utenti, avvisandoli periodicamente delle minacce in corso e di utilizzare un team di esperti per salvaguardare la sicurezza del perimetro "cyber". Per avere un indice di minaccia in tempo reale si consiglia di visitare il seguente link: [Yoroi Cyber Security Index](#).

Seat	Contact	Legal	Warning system	Social
Yoroi S.r.L.	info@yoroi.company	Terms & Conditions	Subscribe to our early warning system	
Via Giovanni Battista Martini 6, Roma RM, 00198	+39 051 0301005	Privacy Policy	Downloads	
			News	