Scritto da Administrator
Venerdì 19 Luglio 2019 16:06

L'estate è il periodo di relax per gran parte degli Italiani che staccano la spina e si concedono un po’ di meritato riposo.

Sotto l’ombrellone, distratti dalla crema solare e dai giochi d’acqua o in montagna seduti ad ammirare il paesaggio, si fa meno attenzione a cosa si clicca, facilitando il lavoro dei cybercriminali. La principale minaccia informatica per gli Italiani nel periodo estivo continua a essere rappresentata dagli adware , software che durante la navigazione in Internet raccolgono informazioni sulle operazioni effettuate dall'utente, per poi bombardarlo di annunci pubblicitari che si aprono come un’invasione tra le finestre del browser. Non a caso svetta al primo posto della classifica delle minacce informatiche più diffuse in Italia, con il 6% delle rilevazioni (periodo compreso tra il 15 giugno e il 15 luglio 2019) JS/Adware.Agent.AA, che una volta installato sul sistema causa la visualizzazione di contenuti promozionali tra cui pop-up, banner, link di testo e annunci commerciali, che vengono utilizzati per aumentare la popolarità di siti di terze parti. Adware.Agent.AA è inoltre in grado di raccogliere dati sensibili, come le credenziali di accesso all’Internet Banking, che vengono poi usati per finalità fraudolente.

{loadposition user7}

Gli adware rappresentano una minaccia ben nota agli internauti italiani, posizionandosi al primo posto della classifica dei malware più diffusi in Italia in maniera pressoché continua già dal luglio 2018.

Proprio per aiutare gli utenti a difendersi dagli adware e dalle altre minacce informatiche anche nel periodo estivo, ecco alcuni semplici suggerimenti per aumentare il livello di protezione dei dispositivi:

1. Installare e mantenere aggiornato un software antimalware

I malware, come i virus informatici, non sono altro che programmi con la capacità di diffondersi automaticamente e, una volta installati nel sistema, di effettuare una serie di attività più o meno pericolose.

Considerato che ogni giorno vengono creati nuovi virus che grazie a Internet si diffondono con eccezionale rapidità, è fondamentale installare sul proprio PC un antivirus efficace e costantemente aggiornato.

Infatti, un software antivirus non aggiornato con regolarità, ci potrebbe far correre rischi maggiori rispetto al non averlo affatto poiché porterebbe a un falso senso di sicurezza che potrebbe spingerci a trascurare anche le più elementari norme di sicurezza informatica.

2. Controllare gli allegati delle email prima di aprirli

Il vettore di diffusione principale dei malware è storicamente la posta elettronica. In particolare i file allegati alle email. Nella maggior parte dei casi, un virus può trasmettersi esclusivamente tramite file eseguibili (con estensione exe,com,drv e dll) o che contengano una parte di codice pericoloso, come succede per i documenti Office in cui sono inserite macro infette. Per questo in linea generale è consigliabile evitare di aprire gli allegati alle mail ricevute da mittenti sconosciuti. Negli ultimi anni però il fenomeno dello spoofing degli indirizzi email ha reso pericolosa anche l’apertura di file allegati provenienti anche dei contatti affidabili; questa tecnica criminale permette infatti di impostare come mittente un qualsiasi indirizzo che potrebbe far parte della rubrica del destinatario, con la conseguenza di indurre gli utenti ad aprire allegati infetti con maggiore fiducia. Quindi per evitare di cancellare a prescindere qualsiasi email con file allegati è buona norma verificarli con una soluzione antivirus e in caso di ulteriori dubbi chiedere conferma al mittente.

3. Effettuare periodicamente il backup dei dati

La strategia di base ed essenziale per difendersi dai malware è avere un backup costantemente aggiornato. Occorre ricordare che per esempio un ransomware codificherà anche i file sui dischi di rete a cui si è assegnata una lettera e a volte anche quelli a cui non è stata assegnata. Ciò include qualsiasi drive come quelli USB, come anche ogni archivio di rete o nel Cloud. Quindi è fondamentale un regime di backup periodico che sia basato su dispositivi che non siano costantemente connessi alla rete.

4. Non fornire i propri dati personali

Non fornire a utenti sconosciuti informazioni personali o addirittura confidenziali durante le conversazioni online (chat) e non pubblicarle sui social network. Questo per due ragioni fondamentali: in primis perché non possiamo conoscere l’identità dell’altra persona e non possiamo sapere chi utilizzerà quelle informazioni e poi perché i nostri dati potrebbero essere utilizzati come punto di partenza per ricavare le nostre password o per altri scopi illegali.

5. Creare password complesse e non riutilizzarle

E’ vero che è difficile ricordare password complesse per ogni servizio a cui accediamo quotidianamente, ma utilizzare la stessa password per la banca, i social media e per altri tipi di account potrebbe avere conseguenze disastrose nel caso venga compromesso uno qualsiasi di questi sistemi. Un’alternativa utile e facile è la passphrase. Inoltre potete usare un password manager che registrerà tutte le vostre password e vi permetterà di utilizzarle semplicemente ricordando quella master.

6. Aggiornare sempre il sistema operativo del proprio dispositivo e i programmi installati

Mantenete costantemente aggiornato il sistema operativo e i vostri software. In questo modo verranno colmate quelle vulnerabilità che i criminali tentano di sfruttare per infettare il vostro dispositivo. Per farvi risparmiare tempo e ottimizzare la vostra protezione, molti programmi offrono gli aggiornamenti automatici e possono verificare la disponibilità di patch o di nuove versioni, senza che sia necessario il vostro intervento.

Fonte: ESET

{jcomments on}

{loadposition user6}