PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4343 di Lunedì 05 novembre 2018

Allarme rosso per le macchine fax intelligenti

Durante la recente convention di Las Vegas, DEFCON, è stato lanciato un allarme rosso che riguarda le macchine fax intelligenti.

La convention DEFCON di Las Vegas è una delle più importanti al mondo, per mettere in evidenza problemi legati alla sicurezza informatica.

Durante l'incontro di quest'anno è stato pubblicamente annunciato un punto debole delle macchine fax intelligenti, che potrebbe essere sfruttato per infettare milioni di aziende in tutto il mondo.

Vediamo di che si tratta.

Tanto per inquadrare bene lo scenario, al mondo sono in uso all'incirca 45 milioni di macchine fax, sia in abitazioni private, sia in istituzioni pubbliche e private di ogni dimensione. Queste macchine si dividono in due grandi categorie:

- le macchine di tipo tradizionale, con stampante a carta termica, esclusivamente collegate alla rete telefonica, che non sono soggette a questo tipo di attacco;
- le macchine di tipo avanzato, per lo più incorporate in stampanti e scanner, vale a dire stampanti multifunzione, che sono invece soggette a questo tipo di attacco.

I ricercatori di un'azienda specializzata hanno messo in guardia i partecipanti alla convention, illustrando questa vulnerabilità.

I protocolli che vengono utilizzati per la ricezione dei fax da parte di stampanti intelligenti sono stati stabiliti nel 1980 e non sono mai stati aggiornati. Ecco perché un hacker può spedire un messaggio fax, basato su una immagine a colori JPEG, all'interno della quale viene inserito un malware od altro software criminoso.

Quando questa immagine viene ricevuta, essa viene decodificata e memorizzata nella memoria del fax, scanner, stampante, pronta per la stampa. Il malware inserito nell'immagine assume il controllo dell'apparato e può insinuarsi in qualsiasi rete, alla quale la macchina fax sia collegata.

Durante la convention i relatori hanno dimostrato le vulnerabilità di una specifica macchina prodotta dalla HP, che è appunto in grado di comportarsi come stampante, fax e scanner. Questa stampante usa lo stesso protocollo che viene usato da dozzine di altre stampanti multi funzioni e servizi fax on-line.

Secondo la ricerca degli studiosi, quasi la metà di tutte le stampanti laser vendute in Europa è soggetta a questa tipologia di attacco.

Non appena HP è venuta a conoscenza di questa debolezza, ha sviluppato un aggiornamento software, liberamente disponibile sul suo sito, che la mette sotto controllo.

Anche se da molti informatici le macchine fax sono ritenute appartenenti a una vecchia tecnologia, sta di fatto che esse sono utilizzate in un gran numero di campi. Addirittura la legislazione americana nel settore della salute prevede che certi messaggi vengano trasmessi per fax, in quanto si ritengono più affidabili rispetto ad altre forme di comunicazione di dati. Ecco la ragione per cui i fax rappresentano il 75% dei messaggi scambiati, nel mondo della sanità americana.

A livello globale, si parla di 17 milioni di fax scambiati ogni anno.

Sono ancora molti infatti gli operatori, il settore legale, bancario e immobiliare, dove la trasmissione dei dati avviene essenzialmente mediati fax.

Analizzando la situazione gli Stati Uniti, il servizio sanitario nazionale dichiara di possedere più di 9000 macchine fax, che vengono regolarmente usate per trasmettere dati particolari, diretti a vari paesi del mondo. Vale la pena ricordare che in molti paesi la magistratura non accetta i messaggi di posta elettronica come documenti probatori, mentre i fax vengono sempre riconosciuti.

Il problema è che molte aziende non si rendono nemmeno conto del fatto che essi hanno una macchina fax collegata alla loro rete, perché la funzionalità incorporata in stampanti multi funzioni e ciò che l'utente vede è un documento stampato, che potrebbe non essere nemmeno riconosciuto come fax.

Ecco la ragione per la quale non solo si raccomanda di provvedere immediatamente all'aggiornamento software delle stampanti multifunzione utilizzate, ma anche di utilizzare queste macchine su segmenti sicuri di rete, separati da applicazioni e server che trasportano informazioni critiche.

Con questo accorgimento si limita alla possibilità che il malware possa contagiare tutta la rete aziendale.

Adalberto Biasiotti