Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Direttori: Sergio Pellegrino e Giovanni Valcarenghi

Edizione di martedì 24 febbraio 2015

SOLUZIONI TECNOLOGICHE

Lenovo e quella brutta faccenda chiamata Superfish

di **Teamsystem.com**

Proprio qualche settimana fa avevamo parlato delle minacce informatiche che si prevedono per il 2015. Fra le varie voci avevamo citato un aumento degli **adware**, ovvero quei software che prendono possesso del browser del computer e ci propinano pubblicità forzata. Il problema non è affatto superato, anzi. Nell'aria è appena volata una di quelle notizie che ci lasciano a bocca aperta. Stare attenti a quello che si installa nel computer è sempre stata la migliore difesa contro software di questo tipo. Ma cosa accade se il computer ci arriva infetto direttamente dal produttore?

L'affare Superfish

La storia che in questi giorni sta facendo parlare la Rete riguarda **Lenovo**, l'azienda più importante del mondo nella produzione di computer che, secondo quanto sostengono diversi esperti di sicurezza, avrebbe installato nei propri computer venduti **tra settembre 2014 e gennaio 2015** un software chiamato **Superfish** che altro non è se non un adware. Insomma un software che nessuno di noi si sognerebbe mai di installare volontariamente nel proprio PC, viene propinato ai consumatori direttamente dal produttore. E che produttore! Le smentite sono arrivate immediatamente e Lenovo ha subito dichiarato che Superfish però non è stato installato sui Thinkpad, cioè su quella famiglia di computer che vengono principalmente utilizzati per lavoro. Il fatto è che però questo "programmino" è stato installato sugli altri.

Cosa fa Superfish

Come dicevamo, Superfih è un adware che quindi serve a proporci pubblicità forzata. "In our effort to enhance our user experience, we pre-installed a piece of third-party software, Superfish (based in Palo Alto, CA), on some of our consumer notebooks. The goal was to improve the shopping experience using their visual discovery techniques".

Questo quanto dichiarato ufficialmente da Lenovo. Ma il software, stando sempre alle dichiarazioni di alcuni esperti di sicurezza, metterebbe in grave pericolo anche i dati privati degli utenti. Questo perché Superfish è in grado di utilizzare falsi certificati per accedere ai dati anche durante le connessioni "sicure", quelle che avvengono quando per esempio ci colleghiamo al sito della nostra banca. Un software di questo tipo di solito invia a un server

esterno i dati raccolti per determinare le nostre abitudini di acquisito e inviarci pubblicità mirata. Superfish però è in grado di intercettare anche dati che in teoria dovrebbero correre su canali sicuri. Insomma un bel pasticcio che l'**Electronic Frontier Foundation** ha definito una pratica "irresponsabile e di totale abuso della fiducia degli utenti".

I computer a rischio infezione

Nel suo comunicato, Lenovo ha pubblicato una lista dei modelli che potrebbero avere installato il software a bordo. Eccoli:

- G Series: G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45
- U Series: U330P, U430P, U330Touch, U430Touch, U530Touch
- Y Series: Y430P, Y40-70, Y50-70
- Z Series: Z40-75, Z50-75, Z40-70, Z50-70
- S Series: S310, S410, S40-70, S415, S415Touch, S20-30, S20-30Touch
- Flex Series: Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 14(BTM), Flex2 15(BTM), Flex 10
- MIIX Series: MIIX2-8, MIIX2-10, MIIX2-11
- YOGA Series: YOGA2Pro-13, YOGA2-13, YOGA2-11BTM, YOGA2-11HSW
- E Series: E10-30

Se ne possediamo uno, ci conviene fare una verifica su questo sito per controllare se il PC è infetto oppure no.

Qui troviamo il comunicato stampa che l'azienda ha pubblicato immediatamente dopo il fattaccio.