



G&F NOTIZIE

ATTENZIONE AI VIRUS

Rientro in ufficio oggi per migliaia di impiegati e liberi professionisti italiani, dopo il weekend di WannaCry: l'attacco informatico che ha colpito organizzazioni e aziende in molti Paesi del mondo, inclusa l'Italia. Un virus chiamato in gergo ransomware che rende inaccessibili i dati dei nostri computer e, per ripristinarli, chiede un riscatto da pagare in bitcoin, la moneta elettronica. Fino ad ora il malware ha fatto danni limitati nel nostro Paese, raggiungendo un paio di università. Ma continua a far paura e l'allerta rimane alta.

Ecco una serie di consigli pratici per chi si trova di fronte al proprio pc.

G&F s.r.l.

G&F s.r.l.
Via Santuario, 3
12084 Mondovì (CN)

Notizie di rilievo:

> **VIRUS**



Sommarrio:

INTRODUZIONE	1
VIRUS	2

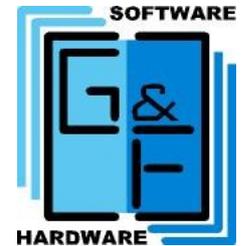
VIRUS WANNACRY

Io, cittadino, come mi difendo da WannaCry? Il malware colpisce chi ha il proprio computer collegato alla Rete e un sistema operativo Windows, dato che il software malevolo si diffonde grazie a Eternal-Blue, una cyber arma della Nsa (l'agenzia per la sicurezza nazionale statunitense), diffusa online lo scorso aprile dal gruppo hacker Shadow Brokers. Uno strumento che sfrutta una vulnerabilità presente nel sistema operativo firmato Microsoft. "Le prime cose da fare - spiega a Repubblica Davide Del Vecchio, membro del comitato direttivo del Clusit, l'associazione italiana per la sicurezza informatica - sono aggiornare sia l'antivirus sia il sistema operativo, dato che questa falla è stata risolta dalla stessa Microsoft con un update che risale allo scorso marzo chiamato MS17-010".

Utile è anche un backup dei dati (o, se già fatto, un aggiornamento), cioè una copia dei propri file. Si può effettuare utilizzando Windows Backup che si trova nel pannello di controllo del nostro pc. Il backup va fatto periodicamente in un hard disk esterno, ad esempio una chiavetta Usb. "In questo modo - prosegue Del Vecchio - se il virus dovesse infettare il pc, una copia dei dati rimarrebbe protetta, dandoci l'opportunità di ripristinarli all'occorrenza".



COME DIFENDERSI



Al momento, sembra che in Italia WannaCry si stia propagando unicamente sfruttando la vulnerabilità sopra menzionata, e non ci sono prove che il virus sia trasmesso tramite email. Questo significa che il software si diffonde in modo autonomo, senza che l'utente debba compiere alcuna azione. Tuttavia, come avverte Francesco Mormile, uno dei fondatori di Hactive Security, azienda che si occupa di sicurezza informatica è "ragionevolmente plausibile che vengano rilasciate delle nuove versioni del malware capaci di diffondersi anche attraverso la posta elettronica, dato che l'email è il metodo tradizionale con cui si propagano i ransomware". Così il suggerimento valido è: "Non aprire link o file che provengono da email sospette".

Io, azienda, come mi proteggo?

Sul piano aziendale, anche in questo caso, aggiornare al più presto il sistema operativo e l'antivirus di tutti i computer presenti all'interno della propria impresa.