PuntoSicuro

# ARTICOLO DI PUNTOSICURO

## Anno 8 - numero 1530 di venerdì 28 luglio 2006

# Ricatto via e-mail

***Cresce l'allarme per gli episodi di "RansomWare".***



Computer in ostaggio di pirati informatici che richiedono il pagamento di un riscatto, per rendere accessibile ai legittimi proprietari il contenuto del disco rigido. E' questa una delle minacce emergenti, denominata Ransomware, rilevata nel rapporto del secondo quadrimestre 2006 redatto dai laboratori Kaspersky, azienda nel campo della sicurezza informatica.

Questi codici malevoli, che possono essere diffusi via e-mail o via web ma anche tramite programmi per telefonini, hanno fatto la loro comparsa nel 2004, sono stati "perfezionati" nel 2005, per avere un picco di diffusione nel 2006; uno tra i più noti è il virus TROY_PGPCODER.A.

La tecnica utilizzata è la seguente. Dopo aver contagiato il PC dell'utente vittima, il codice dannoso ricerca all'interno dell'hard disk i file con determinate estensioni ( ASC - DB - DB1 - DB2 ? DBF ? DOC ? HTM ? HTML ? RTF ? TXT - XLS ? ZIP -RAR - PGP ? JPG). Una volta individuati li rende inaccessibili, criptandoli e zippandoli.
Con questi file è presente anche un file di testo con le condizioni del riscatto: istruzioni per poter ricevere la password per decrittare i file, dietro il pagamento di una somma.
"Le modalità di pagamento cambiano da virus a vurus, - spiega il Bollettino di Sicurezza informatica del Reparto Informazioni e Sicurezza dello Stato Maggiore della Difesa- ad esempio, per quanto riguarda il virus Troy/Ransom-A,, il pagamento avviene tramite la banca "Western Union" per un importo di 10,99 dollari, mentre il trojan Troj/Zippo-A, richiede che il pagamento e lo scambio denaro-password avvenga tramite e-Gold, il servizio di pagamento on-line della banca americana Gold & Silver Reserve, per un importo di 300 dollari. Curiosamente, gli autori di tali codici malevoli, si rendono disponibili a fornire assistenza via e-mail, nel caso la procedura di "unlock" non dovesse funzionare."

I virus RansomWare costituiscono una minaccia crescente, in quanto l'utilizzo da parte degli hacker di chiavi crittografiche più complesse rispetto a quelle ad oggi usate renderebbe estremamente difficoltoso ogni tentativo di sblocco delle informazioni "prese in ostaggio".

"La diffusione di questo tipo di codici malevoli ? osservano gli esperti della Difesa - , riporta alla ribalta la necessità di eseguire copie di backup con una certa frequenza, in quanto per poter risolvere l'infezione in tempi brevi, l'unica via è quella di re-installare una versione precedente dei file "infettati".
Come raccomandazione, si consiglia di effettuare copie di back-up con brevi scadenze e di tenere sempre aggiornato il proprio programma antivirus (si ricorda che gli aggiornamenti dei programmi antivirus ormai hanno cadenza giornaliera se non oraria)."



---

**www.puntosicuro.it**