Il virus del riscatto

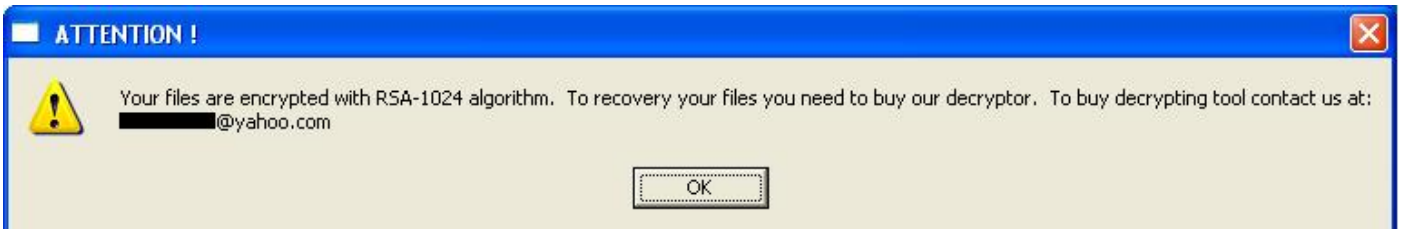
Rossano Ferraris

Sono i cosiddetti Ransomware e sono una categoria di malware molto interessante, poco conosciuti perché non sono molto diffusi ma una volta che si è avuta la fortuna (sfortuna) di conoscerli, è molto difficile scordarseli.
Conosciuti anche con il nome di “virus del riscatto”, i ransomware sono virus che una volta penetrati nel computer, crittano i file del computer della vittima, rendendoli illeggibili, permettendo all’utente di recuperarli solo contattando gli autori del virus, dietro il pagamento di un vero e proprio riscatto in denaro.

L’ultima variante scoperta si chiama GpCode il cui scopo è quello di cancellare i file presenti sul computer, sostituire gli stessi con delle copie crittate, e quindi illeggibili, mantendendo lo stesso nome del documento originale con la dicitura _**CRYPT**.

Ecco cosa succede:

se l’utente ingenuamente avvia il virus compare sul desktop una finestra come la seguente:



Come indicato in figura, il ransomware dice all’utente in maniera chiara e precisa che tutti i files presenti nel suo PC sono stati crittati con chiave a 1024 bit (per i meno esperti: una criptazione con una chiave di questo tipo è praticamente impossibile da decifrare). Inoltre, dice sempre il messaggio, per decifrare i files e recuperarli l’utente è invitato ad acquistare un software di decifratura contattando un indirizzo email. L’indirizzo email è sempre causale e quindi impossibile da localizzare e perseguire penalmente.

Consigli:

l’unica soluzione in questo caso è quella di avere il sangue freddo e di non riavviare il PC. Si è scoperto che i vari files non sono realmente crittati finchè il PC non viene riavviato. Pertanto se il malcapitato utente dovesse trovarsi in questa situazione, l’unico modo per non perdere i propri files è quello di farne una copia e salvarli in un posto sicuro (CD-ROM, HardDisk esterno), dopodichè formattare il PC e re-installare il sistema operativo.
Sappiamo benissimo che non è una delle soluzioni migliori ma al momento è l’unica strategia da adottare a meno che l’utente non abbia il proprio software di sicurezza aggiornato con le ultime definizioni di virus.
Ad oggi la maggior parte dei software di sicurezza possiedono l’aggiornamento relativo a questa variante di malware che viene bloccata prima che questa venga eseguita.