

Sicurezza in Rete: il ritorno di "Ransomware"

Nuova truffa sul web con il malware "Ransomware" che impedisce l'utilizzo del computer per poi richiedere un codice di sblocco, ottenibile collegandosi a siti che pretendono l'acquisto di beni o servizi a pagamento, realizzando una vera e propria estorsione.

Il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche del Servizio polizia postale e delle comunicazioni (Cnaipic) ha verificato l'esistenza di una nuova versione del trojan "Ransomware", noto a molti utenti della rete per averli colpiti già dal 2006 con le precedenti versioni.

In alcune delle precedenti versioni, infatti, la vittima veniva costretta ad acquistare farmaci o altri prodotti su siti russi e solo successivamente veniva fornito il codice di sblocco. Nella versione attuale, il PC infetto mostra all'avvio il seguente messaggio: Attention! Windows activation period is exceeded. This windows copy is illegal and not registered properly. The further work is not possible. For activating this copy of windows you must enter registration code. This code you can find in your windows distribution package. If you not find them you can receive it by the phone: 899 021 233 Registration code must be entered not later then three days, if it entered later the unlocking is not possible.

Di fatto il PC non subirà alcun danno significativo, ma se la vittima dovesse telefonare al numero visualizzato nel messaggio spenderebbe 1,75 euro al minuto e non riceverebbe alcun codice, ma verrebbe semplicemente reindirizzato ad un altro servizio telefonico a pagamento.

Gli utenti italiani non sono i soli destinatari della truffa, perchè il malware è programmato per riconoscere la provenienza geografica e la lingua del target, pertanto sono previste numerazioni anche per utenti di altre Nazioni.

Inoltre il Cnaipic, oltre alle indagine per identificare l'autore della truffa, ha avviato le procedure per bloccare l'utenza 899 021 233, affinché non vi possano essere ulteriori danni per gli utenti della rete.

29/04/2011