Ransomware: il malware del riscatto colpisce gli utenti italiani

Migliaia di utenti italiani sono stati recentemente vittime del malware Ukash, un particolare tipo di minaccia che blocca il pc e chiede un riscatto in denaro per lo sblocco del sistema.

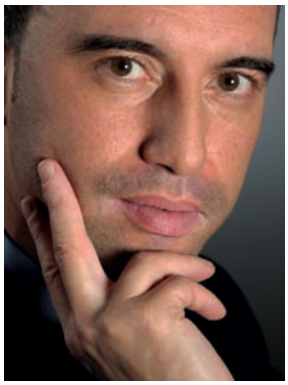
Rossano Ferraris

Tra le varie minacce informatiche figurano i cosiddetti "ransomware" che nel corso di questo anno ormai passato hanno caratterizzato uno scenario abbastanza inquietante nel mondo del Threat Management.

Che cosa è il ransomware

Per definizione il ransomware è quella famiglia di malware che una volta eseguito tiene letteralmente il sistema in ostaggio con lo scopo di estorcere del denaro all'utente vittima se vuole ripristinare le funzionalità operative normali. Il tipico comportamento di questo tipo di malware è caratterizzato dalle seguenti azioni:

- Tutte le funzioni base del sistema operativo ospite vengono disabilitate
- Tutti i programmi attivi in quel momento vengono terminati
- I dati del sistema vengono criptati con codice segreto in modo da non renderli più accessibile e/o leggibili
- Rimuove le funzioni di navigazione Internet
- Viene richiesto un pagamento al fine di ricevere un codice o procedura di sblocco del sistema infetto



Rossano Ferraris, senior research engineer per Total Defense Inc.

Una volta pagato il riscatto i criminali inviano il codice di sblocco del sistema riportandolo allo stato funzionale normale. Tuttavia ci sono stati diversi casi in cui pur avendo pagato per lo sblocco nulla viene inviato all'utente vittima lasciando il problema totalmente irrisolto: dopo il danno anche la beffa! Ovviamente esistono molte varianti ma gli effetti generali sono quelli descritti finora.

Gli strumenti attraverso i quali il malware si propaga sono: e-mail, siti compromessi, rogue software e software p2p (eMule, eDonkey, Limewire, eccetera).

Cosa è successo in Italia recentemente

In questi giorni si è assistito ad una particolare forma di ransomware identificata dalla ricerca operativa

dell'anti-malware industry con il nome di Ukash.
Ukash (**http://www.ukash.com/it/it/home.aspx**) è un metodo di pagamento internazionale utilizzato dagli utenti che vogliono fare transazioni online senza usare carte di credito ma invece tramite voucher rilasciato direttamente dal punto Ukash una volta acquistato.
Il ransomware in questione è stato battezzato 'Ukash' perché è proprio tramite questa forma di pagamento che i 'sequestratori' del sistema chiedono di pagare il riscatto.
Vittime della truffa non sono solo gli utenti italiani ma anche la Polizia che si è trovata numerose richieste di chiarimenti da parte di utenti frodati da questo tipo di malware.
Il ransomware 'Ukash' ha coinvolto direttamente le Forze di Polizia in quanto considerate falsamente le mittenti di un messaggio di intimazione nei confronti di utenti falsamente indicati come possessori di computer usati per operazioni illegali (vedi Figura 1).

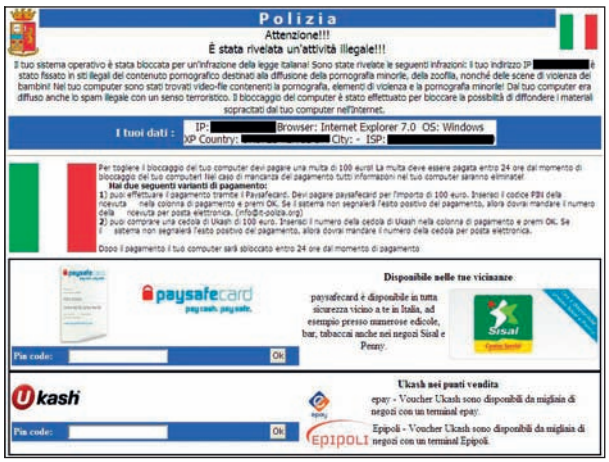
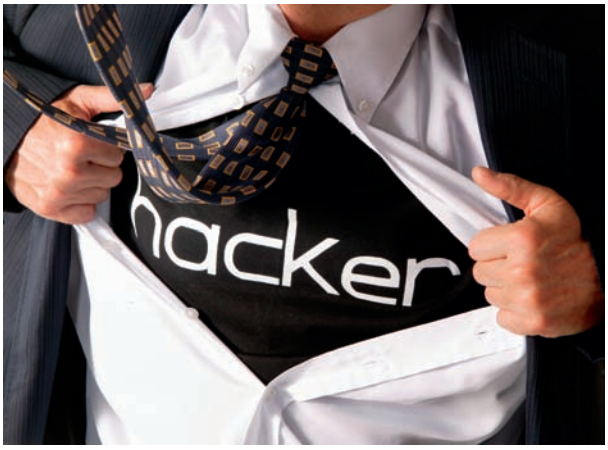


Figura 1 – Banner di sequestro apparso sullo schermo dei pc italiani infetti

Una volta infettati il pc si trova in condizioni di non funzionamento e una delle possibili soluzioni è quella di ripristinare una versione precedente del sistema Windows tramite il disco di ripristino.

Conclusioni

Quella descritta il più delle volte è una situazione non reversibile e per questo motivo la prevenzione nel campo della sicurezza informatica deve essere considerata al top delle priorità.



In questi termini si raccomanda pertanto agli utenti italiani di:

- Aggiornare il proprio software di sistema con le ultime patch di sicurezza
- Tenere aggiornato il proprio software di sicurezza (Internet security suite)
- Evitare se possibile di visitare siti sconosciuti
- Stare attenti a scaricare software piratato

Rossano Ferraris

Rossano Ferraris è laureato in Informatica e possiede le certificazioni SANS (GCIH, GCFA, GREM).
Attualmente ricopre il titolo di Senior Research Engineer per Total Defense Inc. (www.totaldefense.com) ex divisione di CA Tecnologies ISBU.
È membro e co-fondatore del team ISI (Internet Security Intelligence) all'interno del Dipartimento di Ricerca della ISBU (Internet Security Business Unit) con la responsabilità di guidare l'area EMEA nello studio, analisi e tracciamento delle minaccie emergenti. Consulente presso la Procura della Repubblica e le Forze dell'Ordine in materia di analisi forense e tematiche legate ai crimini informatici in Italia.
È inoltre socio AIPSI (capitolo italiano ISSA) e impegnato in attività di sensibilizzazione attraverso interventi pubblici e la scrittura di pubblicazioni sulle insidie provenienti dalla rete.
Rossano Ferraris è co-autore del libro "Qualcuno ci spia: spyware nel tuo pc", edito da Mondadori (2005) e ideatore del blog "SecuritySurfer" (www.securitysurfer.it).