

TG Soft, rapimento senza riscatto

Dal Centro Ricerche Anti Malware di TG Soft la soluzione, gratuita, per rimuovere il pericoloso virus che 'rapisce' il computer per poi chiedere un riscatto per rilasciarlo.

È un virus/malware che il C.R.A.M. (Centro Ricerche Anti Malware di TG Soft) ha analizzato all'inizio di dicembre 2010 battezzandolo 'SafeTad.A'; questa minaccia prende in ostaggio il computer chiedendo 100 dollari per rilasciarlo. La sua rimozione può rendere la vita difficile anche a tecnici esperti, ma TG Soft ha reso disponibile sul suo sito un documento che descrive le modalità di infezione di questo agente con utili consigli per la sua rimozione.

Il SafeTad.A utilizza tecniche più complesse di quelle che sono generalmente utilizzate per garantire la sua esecuzione all'avvio della macchina, riuscendo a inibire il caricamento del sistema operativo; la soluzione raggiunge

questo risultato modificando i settori del disco in cui è residente il Master Boot Record (MBR), sostituendo quello standard con delle routine che invece di caricare il sistema operativo visualizzano sullo schermo un messaggio che avverte l'utente che tutti i dischi presenti sul computer sono stati criptati (vedi figura).

Il messaggio indica che per recuperare i dati si deve raggiungere un sito, immettere il proprio ID e pagare un riscatto di 100 dollari per ricevere una password per sbloccare il computer. Naturalmente le istruzioni fornite sono assolutamente da non seguire.

Analizzando il codice virale si è scoperto che il virus sposta l'MBR originale dal 1° settore (settore 0) al 5° settore del disco, sovrascrivendo

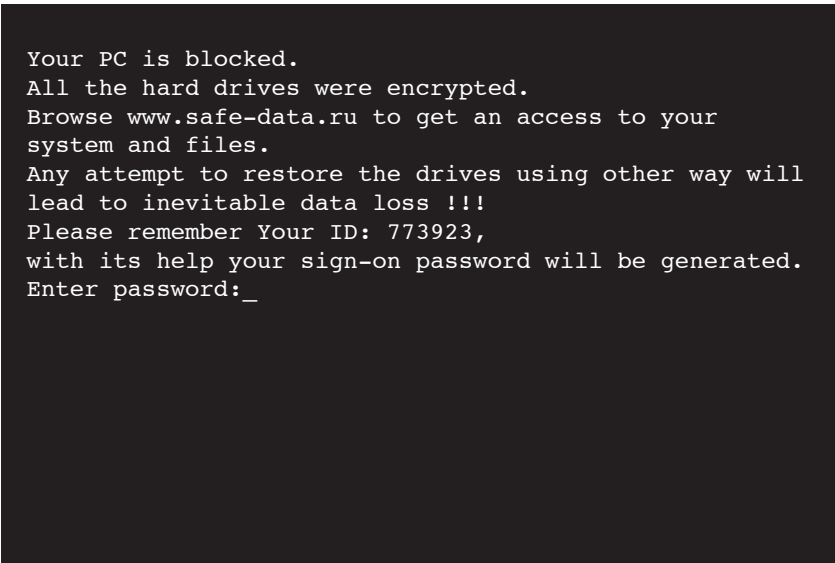
anche i settori 2 e 3 ed eliminando il marcatore standard di fine settore 55AA sostituendolo con un suo marcatore non standard.

Nel secondo settore sono presenti le routine attraverso le quali il virus interagisce con l'utente e controlla la correttezza della password immessa, mentre nel terzo è presente il testo del messaggio sopra riportato. Il quarto settore è lasciato vuoto. Nel caso in cui la password inserita sia corretta, il virus stesso riporta l'MBR originale alla sua posizione di default (settore 0) e azzerava i settori che aveva occupato in precedenza, mentre se la password inserita è errata, dopo la terza immissione viene riavviato il computer. Data la natura del virus, formattare il disco e reinstallare Windows è totalmente inefficace, poiché durante la formattazione e la reinstallazione del sistema operativo non viene sovrascritto l'MBR del disco.

La soluzione

Il C.R.A.M. di TG Soft sconsiglia anche di procedere con un FIXMBR dalla console di ripristino di Windows, perché la tabella delle partizioni del disco è stata spostata dal virus e quindi ripristinare l'MBR standard di Windows porterebbe alla perdita della tabella delle partizioni e quindi a un disco che risulterebbe non partizionato, con la conseguente perdita di tutti i dati presenti.

Nonostante quello che dice il messaggio, i dati sul disco non vengono criptati, per cui sono fa-



```
Your PC is blocked.  
All the hard drives were encrypted.  
Browse www.safe-data.ru to get an access to your  
system and files.  
Any attempt to restore the drives using other way will  
lead to inevitable data loss !!!  
Please remember Your ID: 773923,  
with its help your sign-on password will be generated.  
Enter password: _
```

Un esempio del messaggio visualizzato in occasione dell'avvenuto "rapimento"

cilmente recuperabili una volta ripristinato l'MBR originale insieme alla corretta tabella delle partizioni.

Fin qui l'analisi tecnica resa disponibile dai ricercatori di TG Soft.

Purtroppo, oltre al virus/malware, stanno circolando dall'inizio di gennaio alcune mail, scritte con toni mutuati da mail burla e con informazioni scorrette, che mettono in guardia da questo agente malware ed esortano a inoltrarle con le modalità tipiche della catena di Sant'Antonio segnalando, come accade per le mail hoax (burle), i tipici elementi che fanno leva sul mutuo soccorso degli internauti. Questi messaggi, oltre a creare allarmismo, non danno informazioni tecniche corrette e, in particolare, nessuna informazione sulle possibili soluzioni.

La soluzione, l'unica possibile in

questi casi, è rivolgersi a professionisti, come ad esempio il C.R.A.M. di TG Soft (produttrice di Vir.IT eXplorer Lite – Free Edition e di Vir.IT eXplorer PRO), che studia e pubblica da anni analisi e relazioni sui virus/malware informatici e sulle nuove tecniche utilizzate da questi agenti per diffondersi. Anche per rimuovere SafeTad.A la soluzione c'è ed è disponibile gratuitamente da TG Soft collegandosi al sito www.tgsoft.it. Ricordiamo che la rimozione non può avvenire facendo il boot del sistema operativo che era presente sul computer infetto poiché il suo caricamento è inibito dal virus stesso. Per procedere con ragionevole possibilità di successo è necessario collegare il disco a un altro computer dove sia installato Vir.IT eXplorer sia Lite sia PRO che, al momento della scansione del suo MBR ri-

leverà l'infezione e procederà automaticamente a ricostruire e ripristinare l'MBR originale con la relativa tabella delle partizioni. Completata questa operazione sarà sufficiente ricollegare il disco al computer di competenza.

Vir.IT eXplorer Lite – Free Edition – oltre a essere un utile strumento per rimuovere questo agente è consigliabile venga utilizzato sistematicamente come valida integrazione all'antivirus eventualmente già in uso, aumentando la sicurezza del computer senza penalizzarne le prestazioni.

www.tgsoft.it

G.C.

IP COMMUNICATION - IP PBX - FAX SERVER - TELEFONI IP - GSM GATEWAYS - WIRELESS MESH



ADVANCED NETWORK SOLUTIONS & PRODUCTS
MobiMESH
spin off
Telecom Italia

VoiSmart[®]
The Innovative Way