SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Agosto 2016

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Il Ransomware

Cos'è il Ransomware?

Il Ransomware è un tipo di malware molto particolare che si sta diffondendo rapidamente su Internet, minacciando le vittime di rendere inutilizzabili documenti e file presenti nel computer. Il malware è quindi un software (un programma per computer) utilizzato per compiere azioni maligne. Sebbene il Ransomware costituisca solo una delle tante tipologie di malware, è diventato molto comune a causa del profitto che porta ai criminali. Una volta che avrà infettato il vostro computer, cifrerà con la crittografia alcuni file o addirittura l'intero disco. Vi troverete "chiusi fuori" dal sistema e non potrete più avere accesso a documenti e foto. Il malware vi informerà che il solo modo per rientrare in possesso dei vostri file e ripristinare il sistema è di pagare un riscatto (ransom) ai criminali. Da qui il nome Ransomware. Spesso il riscatto deve essere pagato con qualche forma di moneta elettronica, come il Bitcoin. I Ransomware si diffondono come altri tipi di malware: il metodo più comune è tramite l'invio alle vittime di email maligne, mediante le quali i criminali vi ingannano portandovi ad aprire allegati infetti o a cliccare su link che vi condurranno al sito dell'attaccante.

L'autore di questo numero

Lenny Zeltser lavora in NCR Corp dove con il compito di proteggere le attività IT dei suoi clienti; al contempo si occupa di formazione per il SANS Institute. Potete seguire Lenny su Twitter (**@lennyzeltser**) e sul suo sito **zeltser.com**.

Devo pagare il riscatto?

Il problema, in questo aspetto della vicenda, è che più persone pagano questi criminali, maggiormente i criminali saranno motivati nello spargere l'infezione. È anche da considerare che potreste non avere alternative per ripristinare i vostri file. Tenete comunque conto che, qualora paghiate il riscatto, non c'è alcuna garanzia che riavrete i vostri file: i criminali potrebbero non mettervi più in grado di decifrare i file, o qualora vi consegnino il metodo di decifratura in cambio del pagamento, qualcosa potrebbe andar storto o ancora il vostro computer potrebbe essere infettato con dell'altro malware.

I salvataggi

Il miglior modo per recuperare i file da un'infezione da malware e non pagare il riscatto è di recuperare i file dai salvataggi. In

Il Ransomware

questo modo, anche se venite infettati da un ransomware, avrete il modo per recuperare i file dopo aver ricostruito o cancellato il contenuto del computer. Ricordate che se i vostri salvataggi possono essere acceduti da sistemi infetti, il ransomware potrebbe cancellarli o cifrarli. Per questo motivo è fondamentale salvare i file su servizi cloud che godono di un'ottima reputazione, o conservarli su drive esterni che non siano connessi continuativamente al sistema. Un errore che molti compiono è di non assicurarsi che i salvataggi permettano di recuperare i file. Effettuate test periodici sui salvataggi in modo da accertarvi di poter ripristinare ciò che vi serve in caso di infezione. I salvataggi sono importanti anche perché permettono di ripristinare file qualora vengano cancellati inavvertitamente o in caso di problemi al disco fisso del computer.

Il Ransomware è un malware che, una volta infettato il vostro computer, cifra tutti i file che trova impedendo che possano essere utilizzati.

Ulteriori misure di protezione

Potete proteggervi dalle infezioni da ransomware allo stesso modo con cui vi proteggete da altri tipi di malware. Iniziate accertandovi che il vostro software anti-virus sia aggiornato: questo tipo di strumenti, chiamato anche anti-malware, viene utilizzato per individuare e bloccare i programmi maligni. Un anti-virus, purtroppo, non è in grado di bloccare o rimuovere completamente ogni virus: i criminali informatici sviluppano infatti nuovi e sempre più sofisticati malware in grado di sfuggire alle maglie del controllo. Parallelamente, però, i produttori di anti-virus aggiornano costantemente i loro prodotti con nuove funzionalità per individuare il malware. In un certo senso si può parlare di una corsa agli armamenti, in cui entrambi gli antagonisti tentano di superarsi l'un l'altro. Sfortunatamente i cattivi sono spesso un passo avanti e per questo motivo dovete assicurarvi che i vostri salvataggi periodici funzionino e che implementiate i seguenti ulteriori suggerimenti.

- I criminali infettano computer e dispositivi sfruttando vulnerabilità nel software. Più un software è aggiornato, meno vulnerabilità avrà e più difficile sarà da infettare. Assicuratevi quindi che il sistema operativo, le applicazioni e i dispositivi si aggiornino automaticamente.
- Sui computer, usate un account standard con privilegi limitati anziché account come "Amministratore" o "root". Questo vi fornirà un ulteriore protezione evitando che molti malware si possano installare senza che ve ne accorgiate.

Il Ransomware

- I criminali informatici spesso ingannano le persone per fare in modo che installino del malware. Uno dei metodi più utilizzati è l'invio di un messaggio email, all'apparenza legittimo, contenente un allegato o un link. L'email potrebbe apparire come proveniente dalla vostra banca o da un amico, ma se aprite l'allegato o cliccate sul link attiverete del codice maligno che installerà malware sul vostro sistema. Se un messaggio crea un senso di urgenza, appare confuso, sembra troppo bello per essere vero o la grammatica non è curata, potrebbe trattarsi di un tentativo di frode. Siate sempre cauti: il buon senso è spesso la vostra miglior difesa.

Per proteggersi dal ransomware è necessario porre attenzione quando si aprono allegati di email o si clicca su un link, avere l'anti-virus sempre aggiornato ed effettuare salvataggi regolari dei file.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
securingthehuman.sans.org/ouch/archives

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

Il Phishing:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_it.pdf
Il Malware:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_it.pdf
La crittografia:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201606_it.pdf
I salvataggi:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_it.pdf
Il Ransomware:	https://it.wikipedia.org/wiki/Ransomware

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley