PROTEGGERSI DAGLI ADVANCED PERSISTENT THREATS

Si chiama APT (Advanced Persistent Threst) e si installa generalmente aprendo o facendo clic su allegati o collegamenti fraudolenti in un messaggio email, un messaggio in chat, un post in ambiente social network o un altro sito Web. Potrebbe entrare nel sistema persino durante la semplice visita di un sito Web appositamente creato. Si tratta di un malware molto sofisticato che elude i tradizionali sistemi di difesa (Advanced); si insidia nel computer ***senza essere rilevato*** *ed* ***attende le istruzioni*** *del suo creatore /attaccante (Persistent). Con qualche centinaio di dollari si possono acquistare al mercato nero rendendoli sfruttabili anche* ***senza*** *avere la minima conoscenza tecnica.*

Il **ransomware** è una particolare tipologia di APT che cifra il contenuto dei documenti presenti sul computer e richiede all'utente il pagamento di un riscatto per decifrare i file e tornare ad avere il controllo dei propri documenti e del proprio computer. Attualmente il peggiore ransomware è stato **CryptoLocker**, che da solo ha infettato circa 400.000 sistemi, portando ai criminali profitti dell'ordine dei 325 milioni di dollari.

In questo momento il fenomeno è in aumento esponenziale e le potenziali vittime sono sia le postazioni di lavoro che gli smartphone e i tablet (sia Android che iOS).

A meno che qualcuno non sia riuscito a prendere il possesso del centro di controllo del ransomware o delle chiavi di cifratura utilizzate, **non è possibile** decifrare i file cifrati. L'unica soluzione è quella di avere i file sottoposti regolarmente a backup ed attuare un'adeguata strategia di prevenzione.

La diffusione degli APT avviene principalmente attraverso 3 tipologie di attacco:

1. una mail che contiene un allegato;
2. un sito compromesso che sfrutta una vulnerabilità del browser della vittima;
3. altri malware diffusi via mail/chat/post/sms o via USB che lo incapsulano internamente.

I più diffusi attualmente sono Locky, Cerber, Teslacrypt e le numerose varianti di CryptoLocker che bloccano le vittime attraverso macro malevole o file PDF appositamente creati.

Per prevenire il rischio di infezioni APT e la conseguente perdita di dati e di operatività è necessario un approccio strutturato ed una strategia di sicurezza a vari livelli.

SENSIBILIZZAZIONE DEGLI UTENTI

Senza alcun dubbio, l'azione più efficace per ridurre il rischio di attacchi APT è la sensibilizzazione del personale a queste forme di attacco e la formazione degli utenti che educhi a riconoscere comportamenti sospetti e ad utilizzare le risorse informatiche con accorgimenti mirati.

PATCH MANAGEMENT

Come nel caso di qualsiasi altra tipologia di attacco, una misura precauzionale sempre valida è l'aggiornamento e il fixing continuo dei sistemi, dei browser e delle applicazioni.

RILEVAMENTO APT

Tecnicamente si possono inserire, nei controlli difensivi del sistema informativo, le componenti di rilevamento degli APT nel traffico di rete, di posta e di navigazione.

MONITORAGGIO

Un adeguato controllo di quello che succede nel sistema informativo e degli eventi anomali che lo riguardano è fondamentale per rilevare gli attacchi e difendersi tempestivamente. L'efficacia e l'utilità del monitoraggio si rafforzano poi con un definito e testato processo di gestione degli incidenti.

XECURITY S.R.L.
VIA GALLARATE, 156
20151 MILANO
WWW.XECURITY.IT