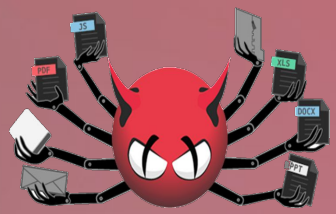
COME SI PRENDE UN RANSOMWARE

Uno dei principali canali di diffusione dei ransomware sono i **banner pubblicitari** dei siti con contenuti per adulti. Ma vengono usate anche e-mail (in maniera molto simile alle email di **phishing**) che invitano a cliccare su un determinato link o a scaricare un certo file.

I cybercriminali possono sfruttare delle vulnerabilità presenti nei vari programmi – come *Java*, *Adobe Flash* e *Adobe Acrobat* – o nei diversi sistemi operativi. In quest'ultimo caso, il software malevolo si propaga in maniera autonoma senza che l'utente debba compiere alcuna azione.

MISURE DI PREVENZIONE

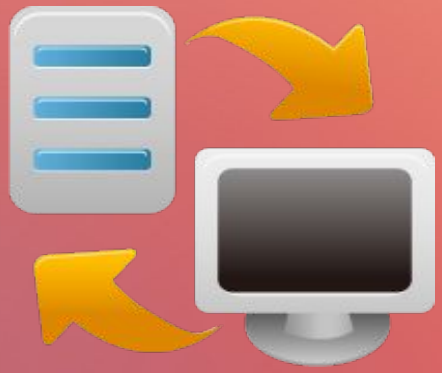
Per cercare di prevenire infezioni da **ransomware**, è consigliato che i sistemi siano continuamente aggiornati alle ultime versioni delle **patch** disponibili.



Il salvavita più efficace contro qualsiasi tipo di pirateria informatica, è la propensione ad effettuare quanto più frequentemente possibile **backup** di sistemi e dati.

COSA FARE IN CASO DI INFEZIONE

1. **Non pagare** mai per il riscatto dei dati. Pagare il riscatto non offre la garanzia di decifratura. Anche l'**FBI** è un fermo sostenitore di questa posizione.
2. **Scollegare** subito i sistemi colpiti. In questo modo si eviterà che l'infezione possa diffondersi ulteriormente.
3. Utilizzare i **backup** più recenti. In questo modo sarà possibile riprendere le attività velocemente.
4. Contattare un'azienda professionale di **data recovery**. In questo modo potrai esplorare le possibilità di recupero dati.



RIFERIMENTI

- http://www.c3t.it/projects/awareness/articoli&brochure/ransomware/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

RANSOMWARE: WANNACRY

Scopri cos'è un ransomware e prendi consapevolezza dei rischi per non subire un attacco come lo WannaCry - "voglio piangere" .

COSA SONO I RANSOMWARE

I **Ransomware** sono un tipo di malware - software malevolo - che cripta o impedisce agli utenti l'accesso ai propri file. Solitamente, quando gli utenti provano ad accedere ai dati, visualizzano una richiesta di pagamento di riscatto per poterne tornare in possesso.
Ci sono 3 principali categorie di ransomware:

- **Scareware**

  Applicazioni o programmi fasulli che sembrano software anti-virus o di ottimizzazione e richiedono il pagamento di una somma di denaro in cambio della risoluzione della presunta minaccia rilevata.

- **Locker Ransomware**

  Blocca l'accesso al computer dell'utente, mostrando una schermata con un messaggio in cui si afferma che il dispositivo è stato utilizzato per commettere un crimine informatico. Per sbloccare il computer l'utente dovrà pagare un riscatto agli **hacker**.

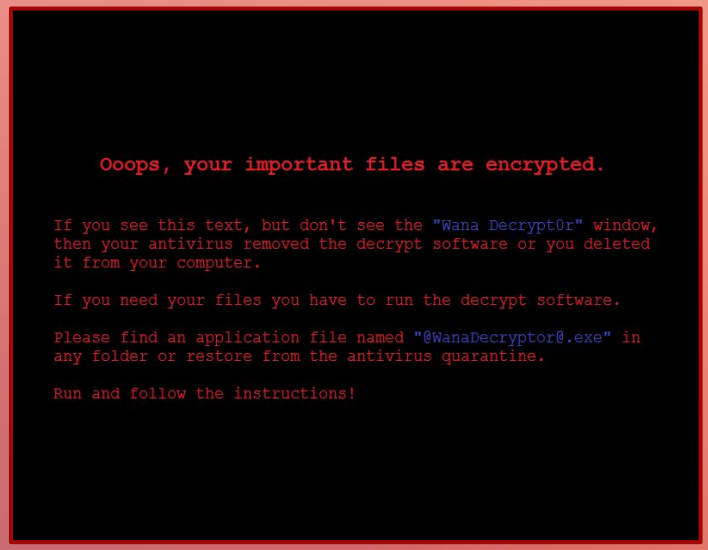
- **Crypto Ransomware**

  Dopo aver ottenuto l'accesso al computer della vittima, il ransomware si infiltra nei dati e nella struttura dei file del computer per crittografare tutti i contenuti. Gli **hacker** chiedono il pagamento di un riscatto per decifrare i file.

Attacchi ransomware sono tipicamente eseguiti con dei **trojan**, cioè programmi apparentemente legittimi ma che nascondono una funzione malevola e distribuiti come allegati o **phishing** nelle e-mail.

IL CASO DI WANNACRY - "VOGLIO PIANGERE"

WannaCry si è diffuso a partire dal 12 Maggio 2017 auto-propagandosi tra i sistemi Windows andando a sfruttare una vulnerabilità nel protocollo **SMB** (Server Message Block) del sistema operativo (un protocollo di livello applicativo comunemente usato per l'accesso condiviso a file e stamponti).



Il malware sostituisce lo sfondo del sistema con una immagine a sfondo nero e istruzioni in rosso su come procedere per riavere i file decodificati.

Il tool di decriptazione è un software grafico multilingua attraverso il quale è possibile interagire con la minaccia: oltre a mostrare il countdown per il termine del possibile riscatto, mostra anche i relativi link **bitcoin** attraverso cui effettuare il trasferimento di denaro.

La cifratura dei file avviene tramite una chiave **AES** a 128 bit (univoca per ogni file) che viene a sua volta cifrata tramite cifratura **RSA** a 2048 bits.

Si stima che l'attacco abbia colpito più di **200.000** computer in **150** paesi, con danni totali che vanno da centinaia di milioni a miliardi di dollari.

La falla sul protocollo **SMB** è stata risolta dalla **Microsoft** con l'aggiornamento **MS17-010**, per cui gli attuali computer (aggiornati) non possono essere infettati da **WannaCry**.

Il malware è formato da due componenti distinte, una che fornisce le funzionalità di **ransomware**, ed una usata per la propagazione. La logica di funzionamento della parte di **ransomware** è la seguente:

- scansione del sistema bersagliando qualsiasi file con determinate estensioni (tra cui tutte le estensioni più famose che possono avere i file personali, es: docx, pptx, xlsx, mp3, mp4, txt, ...);
- cifratura con estensione .WCRY e cancellazione del file originale;
- esecuzione di un **tool di decriptazione** per chiedere un riscatto in Bitcoin di 300 $ (se pagati entro 3 giorni) o 600$ (se pagati entro una settimana). Se il riscatto non viene pagato i file cifrati vengono cancellati.