CRYPTOLOCKER

CryptoLocker è un trojan comparso nel tardo 2013, perfezionato poi nel maggio 2017. Questo malware è una forma di ransomware infettante i sistemi Windows e che consiste nel criptare i dati della vittima, richiedendo un pagamento per la decriptazione

Cryptolocker è un trojan di tipo ransomware: un malware che, una volta eseguito, cifra i documenti presenti sul disco fisso rendendoli inutilizzabili all' utente. Per sbloccare i file viene richiesto il pagamento di un riscatto. Se l'utente non effettuerà il versamento della quota richiesta, la chiave utilizzata per cifrare i suoi dati verrà definitivamente cancellata dai server degli autori di Cryptolocker rendendone impossibile il recupero. Tuttavia, in alcuni casi, anche pagando il riscatto è possibile che la chiave per decifrare i dati non venga inviata alla vittima.
Cryptolocker utilizza solitamente comunicazioni che adottano strategie di social engineering: cerca cioè di ingannare gli utenti portandoli ad aprire documenti verosimili recapitati come allegati ai messaggi di posta elettronica e inviati da mittenti apparentemente legittimi. I file eseguibili vengono spesso zippati e l'estensione "mascherata": non viene visualizzato come "nomefile.exe" ma "nomefile.pdf.exe", "nomefile.docx.exe", etc.
Una volta eseguito il file, il sistema inizia a cifrare i dati in locale e sugli share di rete. In alcuni casi l'esecuzione non viene bloccata dal sistema di rilevazione antivirus semplicemente perché quella scaricata dall'utente è una nuova versione del malware non ancora presente nelle signature.

MITIGARE IL RISCHIO

- Gli utenti dovrebbero porre la massima attenzione alla natura degli allegati che decidono di aprire, in modo particolare al contenuto degli ZIP. Non dovrebbero aprire allegati con estensione .cab, .exe, .lnk. etc. a meno di non essere estremamente sicuri che la mail sia reale.
- Effettuare frequentemente il backup di server e client (backup offline, o comunque non accessibile via rete con credenziali utente o nulle).

Soluzioni di dataprotection:
Arcserve UDP

- Attivare, ove possibile, soluzioni avanzate di End Point Protection. Queste soluzioni sono in grado di rilevare potenziali malware ancora sconosciuti in base al comportamento dell'eseguibile sul sistema operativo nel quale viene eseguito il file; aggiornare frequentemente il database del proprio antivirus, attivando dove possibile i controlli aggiuntivi: controllo delle applicazioni, controlli proattivi, protezione della navigazione e controllo della posta.

Soluzione di endpoint security 100% Cloud:
Panda Cloud Office Protection

- Munirsi di soluzioni di controllo contenuti a livello gateway (UTM firewall, content security gateways) in modo da poter controllare/filtrare il contenuto del traffico; implementare sistemi avanzati di Behaviour Analysis per capire quando, come e dove un'infezione di Cryptolocker si sta attivando in rete.

Soluzione UTM:
Sophos UTM

- Analizzare il contenuto di mail ed allegati tramite sistemi di sicurezza perimetrale, inibire, ove possibile, la ricezione di file eseguibili nelle caselle di posta elettronica.

Soluzione di Mail Protection:
LibraEsva Email Security

Per maggiori informazioni sulle soluzioni i funzionari commerciali di Emilia Informatica sono a vostra disposizione

EMILIA INFORMATICA
get connected

Emilia Informatica S.r.l.
Via Rigolli, 69 - 29122 Piacenza
Tel. 0523.62.70.11 - Fax 0523.60.97.71
CF/P.IVA 01226710331
www.emiliainformatica.it