Il Giunto, Istituto Tecnico Industriale Statale "G. Cardano" - Pavia

Data articolo

19-04-2023

Autori

Ginevra Grumi , Elisa Laboranti, Martina Pozzato e Kamila Zaiduloeva, della classe 3DLS

Ransomware: un riscatto pericoloso

Ransomware: un riscatto pericoloso

“Il ransomware è un programma informatico dannoso (“malevolo”) che può infettare un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l’accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file) per poi chiedere un riscatto (in inglese “ransom”) da pagare per liberarli”.
Questa è la definizione proposta dal Garante per la Protezione dei dati personali che aggiunge come all’utente vengano indicate le modalità di pagamento del riscatto attraverso una finestra che si apre automaticamente sullo schermo del dispositivo infettato, dietro minaccia di vedersi bloccato definitivamente l’accesso ai propri contenuti in caso di mancato pagamento.

Esistono diverse tipologie di ransomware in continua evoluzione, che diventano perciò sempre più pericolosi. Elenchiamo i più comuni.

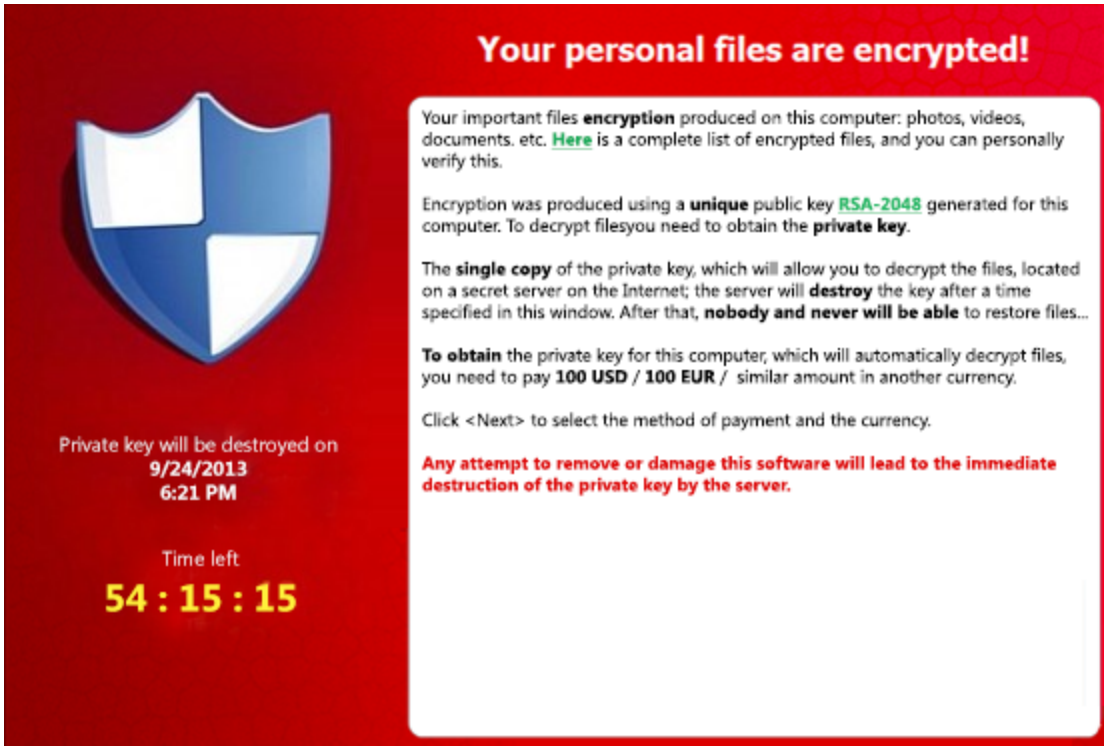
1) Ransomware di crittografia: questo tipo di ransomware crittografa i dati dell’utente e richiede il pagamento di un riscatto per fornire la chiave di decrittografia.

2) Ransomware di blocco: questo tipo di ransomware blocca l’accesso del computer dell’utente e richiede il pagamento di un riscatto per sbloccarlo.

3) Ransomware basato su server: questo tipo di ransomware infetta i server di una rete e richiede il pagamento di un riscatto per ripristinare l’accesso ai dati della rete.

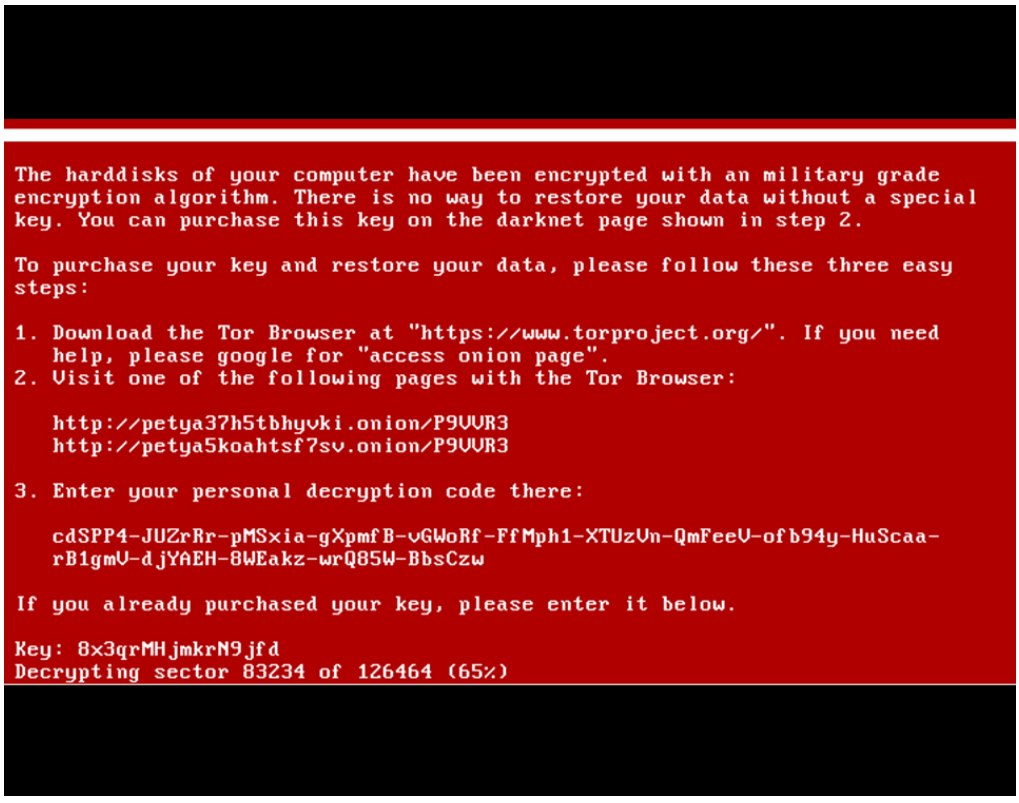
Negli ultimi anni ci sono stati diversi casi di attacchi ransomware a livello mondiale, alcuni dei quali hanno avuto conseguenze devastanti.

Reveton: è un tipo di ransomware che ha fatto la sua comparsa nel 2012.
Il funzionamento di Reveton comprende un malware che infetta il computer dell'utente, bloccando l'accesso al sistema e mostrando un messaggio che sembra provenire da una forza dell'ordine o da un'agenzia governativa. Il messaggio afferma che l'utente ha utilizzato il computer per attività illegali e che deve pagare una multa per evitare ulteriori conseguenze legali. Il messaggio può anche includere il logo e il nome di un'agenzia governativa per sembrare più credibile, ma in realtà è una truffa: il computer dell'utente non è stato bloccato dalle autorità e il pagamento della multa non risolverà il problema. Il successo di Reveton ha ispirato la creazione di altre varianti di ransomware che utilizzano "metodi" di ingegneria sociale per convincere gli utenti a pagare il riscatto.



CryptoLocker: è un tipo di malware ransomware che è apparso per la prima volta nel settembre 2013. CryptoLocker cripta i dati dell'utente e richiede un pagamento in cambio della chiave per decrittografarli.
Il malware si diffonde attraverso email e, una volta che infetta il computer dell'utente, inizia a crittografare i files utilizzando una crittografia a chiave simmetrica. Il malware quindi richiede un pagamento in bitcoin in cambio della chiave per decrittografare i dati. CryptoLocker si è dimostrato particolarmente pericoloso perché utilizzava una crittografia molto forte e le chiavi di decrittografia erano quasi impossibili da ottenere senza pagare il riscatto. Inoltre, il malware rimuoveva in modo sicuro le chiavi di crittografia dopo 3 giorni dall'infezione e ciò rendeva ancora più difficile recuperare i dati. Anche se CryptoLocker è stato arrestato nel 2014 grazie all'azione congiunta delle forze dell'ordine internazionali e dei fornitori di sicurezza informatica, ne circolano varianti che utilizzano tecniche simili per crittografare i dati degli utenti e richiedere un riscatto. Uno dei cybercriminali più ricercati al mondo dall'Fbi è stato il russo Evgeniy Bogachev che, infettando migliaia di computer, è riuscito a rubare centinaia di milioni di dollari.

WannaCry: è un malware protagonista di infezioni nei sistemi di alcune importanti organizzazioni come Portugal Telecom, Telefonica, FedEx, Renault, il Ministero degli Interni Russo, l'Università degli Studi di Milano Bicocca. Oltre 230.000 computer colpiti in circa 150 paesi lo hanno reso uno dei più grandi attacchi ransomware della storia. WannaCry utilizza una vulnerabilità di sicurezza in Windows per diffondersi tra i computer connessi in rete e criptare i dati degli utenti, richiedendo un riscatto in bitcoin in cambio della chiave di decrittografia. Il malware si diffonde attraverso email e, una volta che infetta il computer dell'utente, si diffonde automaticamente attraverso la rete cercando altri computer vulnerabili. Il malware quindi cripta i files dell'utente e richiede un pagamento in bitcoin in cambio della chiave. L'attacco WannaCry ha avuto un impatto significativo su organizzazioni e individui in tutto il mondo e ha portato a un rinnovato interesse per la sicurezza informatica e la gestione delle vulnerabilità.



Not Petya: è noto per essere stato uno dei malware più costosi della storia e si stima abbia arrecato danni per circa 10 miliardi di dollari. Utilizza la stessa vulnerabilità sfruttata da WannaCry e funziona nello stesso modo. Si concentra su aziende e grandi server.

Come proteggersi dal ransomware?
Prima di tutto agendo in modo prudente. Occorre evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti; se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ignora il contenuto. E' importante anche non aprire allegati con estensioni "strane" e non scaricare software da siti sospetti; meglio scaricare app e programmi da market ufficiali.
Inoltre è utile installare sui propri dispositivi un antivirus con estensioni anti-malware e utilizzare dei sistemi di backup che salvino, anche in maniera automatica, una copia dei dati.

Come liberarsi dal ransomware?
Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di non ricevere i codici di sblocco, o addirittura di finire in "liste di pagatori" potenzialmente soggetti a periodici attacchi ransomware. La soluzione consigliata è dunque quella di rivolgersi a tecnici specializzati capaci di sbloccare il dispositivo.

E' sempre consigliabile segnalare o denunciare l'attacco ransomware alla Polizia postale (https://www.commissariatodips.it), anche per aiutare a prevenire ulteriori illeciti.

Ginevra Grumi , Elisa Laboranti, Martina Pozzato e Kamila Zaiduloeva, della classe 3DLS