SICUREZZA INFORMATICA

RANSOMWARE

Rischi e azioni di prevenzione

MINISTERO DELLO
SVILUPPO ECONOMICO

Ver.1.0, 29 aprile 2016

Pagina lasciata intenzionalmente bianca

1. INTRODUZIONE

Già a partire dal 2014 è stato osservato un notevole incremento nella diffusione di *malware* appartenente alla categoria del *ransomware*. La frequenza con cui nuove versioni di questi codici malevoli vengono scoperte è andata aumentando nel tempo, facendo registrare una vera e propria "esplosione" a partire dai primi mesi del 2016.

Il presente documento ha lo scopo di fornire informazioni essenziali sulle caratteristiche di questa famigerata categoria di *malware*, sulle sue varianti e sulle modalità di diffusione, sulle opportune contromisure da prendere e sui comportamenti consigliati da tenere al fine di prevenire la possibilità di cadere vittime di questa tipologia di minaccia informatica.

2. COS'È IL RANSOMWARE

Col termine *ransomware* (dall'Inglese *ransom* = **riscatto**) viene indicata una categoria di *malware* che infetta i computer in maniera similare ai *trojan* e ne limita l'accesso, in diversi modi, ai legittimi proprietari. Esistono diverse varianti di *ransomware*, ma tutte generalmente mostrano una schermata di avviso con la quale viene richiesto all'utente del denaro a titolo di riscatto per poter riottenere il normale accesso al proprio sistema.

Le prime versioni di *ransomware* prevedevano il blocco del sistema, mentre quelle più recenti fanno uso sempre più frequentemente della cifratura dei file presenti sul sistema, che risultano quindi inaccessibili senza un'opportuna "chiave" in possesso dei criminali.

In entrambi i casi viene visualizzata la schermata di avviso in cui si comunica che il sistema resterà bloccato fino a che non verrà pagato un "riscatto". Il pagamento del riscatto è previsto solitamente attraverso moneta virtuale (*bitcoin*) e, pur potendo variare sensibilmente, l'importo si aggira attorno all'equivalente di qualche centinaio di Euro, mediamente circa 200-300.

Il principale meccanismo di diffusione è costituito da Email di *phishing*[1] con allegati file malevoli (contenenti il codice del *malware* o, molto più spesso, un *downloader*) oppure attraverso tecniche di *drive-by-downloading*, ovvero link a siti malevoli dai quali viene scaricato effettivamente il *malware* ad insaputa della vittima.

[1] Linee Guida CERT Nazionale - Minacce: come evitare gli attacchi di phishing e Social Engineering (https://www.certnazionale.it/documenti/2015/03/02/minacce-come-evitare-gli-attacchi-phishing-social-engineering/)

Anche le varianti che prevedono la cifratura dei file (noti come *crypto-ransomware*) si diffondono principalmente con le medesime tecniche, ma spesso utilizzano applicazioni e piattaforme *web-based* di *instant messaging*. Le ultime versioni sfruttano anche le vulnerabilità di siti Web per compromettere i siti stessi rendendo più facile la diffusione all'interno delle organizzazioni.

3. PERCHÉ È COSÌ EFFICACE

I criminali che diffondono *ransomware* utilizzano frequentemente meccanismi psicologici che fanno leva sul panico delle vittime. I messaggi (per lo più scritti in lingua inglese) sono spesso intimidatori, del tipo:

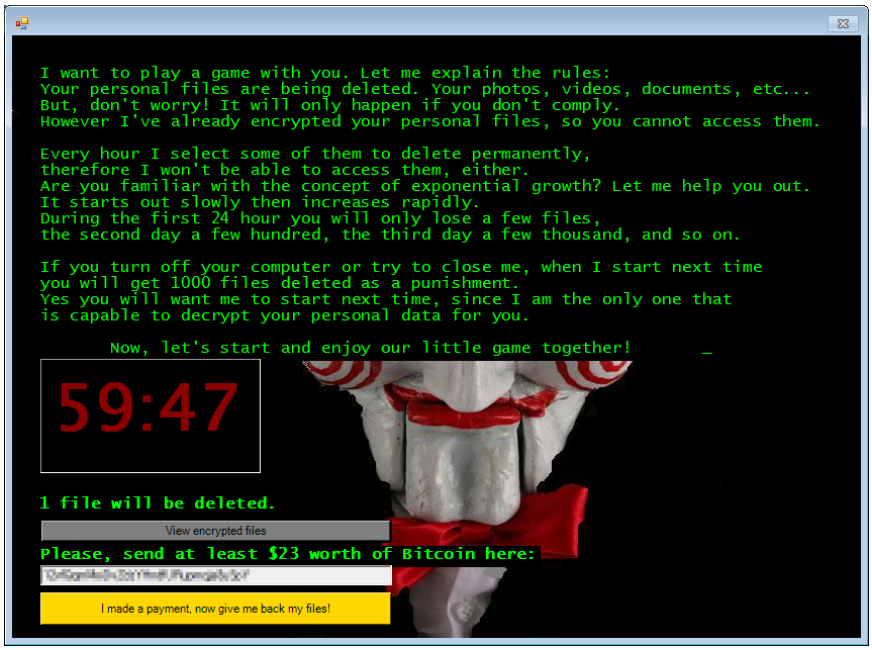
"*Your computer has been infected with a virus. Click here to resolve the issue*" ("Il tuo computer è stato infettato da un virus. Clicca qui per risolvere il problema"). Cliccando spesso la compromissione peggiora, scaricando ulteriore *malware*.

"*Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a ransom*" ("Il tuo computer è stato usato per visitare siti con contenuto illegale. Per sbloccare il computer devi pagare un riscatto"). Cliccando si accede generalmente alle istruzioni per il pagamento.

"*All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data*" ("Tutti i file sul computer sono stati cifrati. Devi pagare un riscatto entro 72 ore per riavere accesso ai tuoi dati"). Anche in questo caso si accede alle istruzioni per il pagamento. Talvolta viene anche visualizzato un conto alla rovescia per esercitare ulteriore pressione psicologica sulle vittime.

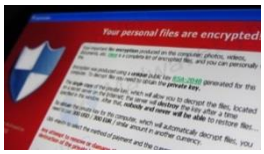
I messaggi sono solo indicativi, spesso le pagine sono più articolate, ma la caratteristica intimidatoria è comune alla quasi totalità di essi.

La schermata di riscatto del ransomware PETYA (fonte: Trend Micro)



Schermata di riscatto del ransomware JIGSAW (fonte: Trend Micro)

4. LE VARIANTI



Nel 2012, dall'analisi di un solo server di *Command and Control* (una macchina usata per compromettere sistemi di diverse vittime, per collezionarne i dati e per gestirne i riscatti) utilizzato per compromettere circa 6.000 computer in un solo giorno, fu possibile stimare che circa il 3% delle vittime si piegarono al pagamento del riscatto. Facendo un rapido conto sull'entità media del riscatto, si ottiene un valore di oltre 25.000 Euro in un solo giorno estorti ad ignare vittime grazie a questa azione criminale.

L'enorme redditività di questo crimine e la possibilità di poterlo perpetrare da remoto ha portato nel tempo allo sviluppo di un numero enorme di varianti successive di questo tipo di *malware*, con conseguente crescente difficoltà nella loro individuazione da parte dei sistemi antivirus.

Il più noto di questi codici malevoli, **CryptoLocker**, è diventato nel tempo sinonimo di *ransomware*, pur rappresentando, in realtà, una delle tantissime varianti della medesima famiglia.

Una delle novità delle versioni di *ransomware* che si sono susseguite nel tempo è stata quella che prevedeva non solo la cifratura dei file presenti sul dispositivo colpito, ma anche di tutti quelli presenti su condivisioni di rete e da questo raggiungibili. In questo modo tali varianti riescono a compromettere interi sistemi di organizzazioni anche di medie/grandi dimensioni attraverso una unica macchina inizialmente colpita.

Il CERT Nazionale dedica grande attenzione ai *ransomware*. All'interno delle news pubblicate sul sito, sono riportate spesso le novità relative alle ultime versioni rilevate in rete, con le loro caratteristiche peculiari, quali vettore di attacco o vittime prescelte. Talvolta sono anche

indicate possibili soluzioni, ma il mezzo più sicuro per proteggersi da questo temibile *malware* rimane senz'altro la prevenzione.

5. CORRELAZIONE CON ALTRI *MALWARE*

I sistemi infettati da *ransomware* sono spesso infettati anche da altri tipi di *malware* che ne consentono la diffusione. Ad esempio, il caso più noto, entrato nella cronaca a metà 2014 a seguito di una vasta campagna internazionale di Polizia, è quello di CryptoLocker: la vittima veniva originariamente infettata attraverso l'incauta apertura di un allegato ad una Email di *phishing*. Questo file malevolo conteneva un *downloader*, denominato Upatre, che a sua volta infettava il sistema con GameOver, una variante del *trojan* Zeus, utilizzato per rubare informazioni relative a credenziali bancarie. La macchina colpita entrava di fatto a far parte di una *botnet*. Una volta infettato il computer, veniva scaricato successivamente anche CryptoLocker che, ad insaputa della vittima, iniziava a cifrare i file sul sistema per poi richiedere il riscatto una volta resi indisponibili tutti o gran parte dei file residenti sul sistema.

6. IMPATTI

Il *ransomware* non colpisce solo gli utenti **residenziali**, ma anche utenze **business**.

Gli impatti negativi, pur essendo gli stessi, possono evidentemente assumere un peso differente nei due casi vista la differente dimensione del target:

- perdita, spesso permanente, di informazioni personali o sensibili;
- interruzione delle attività;
- perdite finanziarie legate alla compromissione dei file o al tentativo di ripristinarli;
- danno potenziale alla reputazione dell'organizzazione.

Il pagamento del riscatto non garantisce che i file possano poi essere ripristinati. Al contrario, l'unica cosa certa è che i criminali raggiungono il loro scopo, estorcendo denaro alle vittime e, spesso, ottenendo ulteriori informazioni su di loro (riferimenti bancari o estremi di pagamento), alimentando così il mercato di queste operazioni criminali.

Inoltre, il ripristino dei file attraverso la chiave di decifratura non assicura che l'infezione sia rimossa.

7. SOLUZIONI

Le compromissioni dovute a questa famiglia di *malware* sono spesso molto pesanti sia per le aziende, sia per i singoli cittadini colpiti e spesso il ripristino del sistema richiede l'intervento di specialisti e risulta, talvolta, impossibile.

Le soluzioni a questo tipo di problema, pertanto, sono da ricercare in azioni preventive piuttosto che reattive. La **prevenzione** è l'unica soluzione efficace contro il *ransomware*.

Più in dettaglio seguono alcuni consigli ed azioni utili per evitare l'infezione o, almeno, per renderne le conseguenze rimediabili:

- **prevedere sempre un backup ed un piano di ripristino per tutte le informazioni "critiche"**: effettuare regolarmente dei backup per limitare il danno dovuto alla loro potenziale perdita sul sistema principale. Una raccomandazione essenziale è quella di mantenere i dati di backup su dispositivi di memorizzazione **fuori linea**, al fine di evitare che la propagazione dell'infezione in rete o su apparati condivisi con l'unità colpita possa compromettere anche la copia di riserva;

- **mantenere sempre aggiornato il proprio sistema operativo ed il software applicativo**, con particolare riferimento ai sistemi **antivirus**, e con le ultime versioni delle *patch* di sicurezza applicate; questa accortezza è valida in generale e contribuisce a fermare la maggior parte dei tentativi di infezione da parte di *malware*, compreso quello appartenente alla famiglia dei *ransomware*;

- **effettuare sempre una scansione con uno o più antivirus** di tutto il software scaricato, prima dell'installazione;

- **utilizzare account con privilegi ridotti** (ovvero **non di amministratore**) per la normale attività sulle macchine, utilizzando account di amministratore solo quando necessario; questa accortezza impedisce l'involontaria installazione di software malevolo;

- **disabilitare l'utilizzo di macro nei documenti di Office** (eventualmente se non dopo conferma) al fine di evitarne l'apertura da allegati malevoli ad Email di *phishing*; in caso contrario il codice malevolo potrebbe essere eseguito ad insaputa della vittima. Per organizzazioni ed aziende la soluzione migliore è quella di bloccare tutti gli allegati da Email provenienti da mittenti non riconosciuti, anche se solo parte delle minacce verrebbe bloccata con una simile accortezza;

- **utilizzare delle "whitelist"** configurando opportunamente le cosiddette *Software Restriction Policies* (SRP) al fine di evitare il lancio di programmi provenienti da sorgenti non riconosciute; la gestione delle SRP dipende dal particolare sistema operativo utilizzato. Questa accortezza riduce enormemente i rischi di lanciare programmi malevoli;

- **non cliccare sui link presenti all'interno delle Email**, soprattutto quando provenienti da fonti non certe o di dubbia autenticità; ricordarsi che non sempre il link evidenziato è quello al quale si viene reindirizzati cliccandoci sopra (il link al quale si viene effettivamente indirizzati viene generalmente visualizzato passandoci sopra con il mouse senza cliccare; una eventuale incongruenza con quanto visualizzato è indice di maliziosità del link stesso);

- **non pagare il riscatto**, in quanto non garantirebbe il ripristino del sistema ma avrebbe il solo effetto certo di alimentare l'attività criminale.