Il ransomware è un tipo di malware (software dannoso) installato illegalmente sul tuo computer, senza la tua autorizzazione. Tramite il ransomware, i criminali riescono a bloccare il computer in remoto: a questo punto si apre una finestra popup che richiede il pagamento di una somma di denaro per sbloccarlo. Il ransomware si installa generalmente aprendo o facendo clic su allegati o collegamenti fraudolenti in un messaggio email, un messaggio istantaneo, un social network o un altro sito Web. Il ransomware può entrare nel computer persino durante la semplice visita di un sito Web fraudolento.

di Andrea Piazza

IL RANSOMWARE E LE MISURE DI PROTEZIONE

Andrea PIAZZA è National Security Officer della filiale italiana di Microsoft, dove coordina le le attività volte a promuovere la consapevolezza e l'adozione delle tecnologie di sicurezza da parte dei clienti, gestendo i rapporti sulle tematiche di sicurezza e cybersecurity con le government élites, i leader accademici e i decisori pubblici.

1. Il problema ransomware

I primi mesi del 2016 sono stati caratterizzati da un numero impressionante di aziende ed enti pubblici che sono stati colpiti da Ransomware: una tipologia di malware 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. Non si tratta certo di un fenomeno nuovo, visto che i primi malware di questa tipologia hanno già alcuni anni di vita, ma la diffusione della minaccia in queste settimane è diventata tale da far sì che ogni azienda ne sia stata impattata in misura più o meno grande, a livello mondiale.
Nelle cronache troviamo casi eclatanti, come quello dell'ospedale americano Hollywood Presbiterian Medical Center che ha pagato 17.000 dollari di riscatto pur di poter ripristinare la sua operatività al più presto. Uno studio della Cyber Threat Alliance mostra come una sola campagna, Cryptowall, abbia portato per i criminali a profitti dell'ordine dei 325 milioni di dollari, avendo portato all'infezione di circa 400.000 sistemi. Il fenomeno in questo momento impatta sistemi di diversi tipo, da Windows ad Android alla piattaforma OS X. A fronte di una tale aggressività dei criminali, quali sono gli strumenti a disposizione di chi si difende? Analizziamo le caratteristiche tipiche di queste minacce per poi approfondire le tecniche di protezione più efficaci.

2. Come funziona un Ransomware

Esistono diverse tipologie di ransomware, ma tutte hanno in comune il fatto di impedire di usare il computer normalmente e di richiedere di compiere qualche azione prima di tornare ad usare il PC. Oltre ai Ransomware che cifrano i file, ne esistono altri che impediscono di accedere al proprio sistema o che bloccano certe applicazioni (come il browser). In genere richiedono di compiere delle specifiche azioni per tornare ad avere accesso ai documenti o al PC:

- Pagare un riscatto (tramite Bitcoin o carta di credito).
- Compilare un'intervista.

Spesso il ransomware accusa l'utente di aver commesso delle azioni illegali e lo minaccia di essere multato da una forza di polizia o da un'agenzia governativa. Si tratta ovviamente di accuse false, che si basano su una tecnica intimidatoria per indurre l'utente a pagare il riscatto prima di aver contattato qualcuno in grado di ripristinare il sistema. Non c'è garanzia che il pagamento del riscatto porti al recupero dell'accesso ai file o al sistema. Tipicamente viene richiesto di effettuare il pagamento attraverso una connessione alla rete di anomizzazione Tor che minimizza per i criminali il rischio di essere individuati.

***Fig. 1**: Quarta versione del malware Crowti (rif. https://www.microsoft.com/security/portal/threat/Encyclopedia/entry.aspx?name=Win32/Crowti)*

3. Meccanismi di infezione

Ci sono 3 meccanismi principali di infezione da Ransomware:

a. una mail di spam che contiene un allegato;
b. un sito compromesso che sfrutta una vulnerabilità (del browser o di plug-in come Java, e Flash Player);
c. altri malware che distribuiscono il Ransomware.

Per esempio nel caso di Cryptowall (noto anche come Win32/Crowti), il Microsoft Malware Protection Center ha identificato che la distribuzione avveniva anche tramite dei kit di exploit (Nuclear, RIG, RedKit V2) che includono la possibilità di sfruttare diverse vulnerabilità, tra cui alcune su Java e Flash. È stato inoltre osservata la distribuzione da parte di altri malware come Upatre, Zbot, e Zemot. Crowti è stato rilevato da Microsoft su 850.000 PC tra Giugno e Novembre 2015.

Tra le famiglie più recenti, che hanno impattato centinaia di migliaia di sistemi, si ricordano Locky e Cerber. Locky è tipicamente distribuito a partire da una mail di spam che include un documento Word, che è usato per eseguire delle Macro in Office. La Macro fa sì che il malware venga scaricato sul sistema e inizi poi la fase di ecnryption dei documenti. Locky può anche utilizzare una tecnica relativamente nuova basata sull'uso dei Javascript per scaricare il malware ed evadere la rilevazione dell'antivirus.
Rispetto ai Ransomware precedenti, Cerber aggiunge un messaggio vocale che segnala all'utente che tutti i suoi documenti sono stati criptati per indurre la vittima a pagare il riscatto. Siamo quindi in presenza del primo Ransomware "parlante".

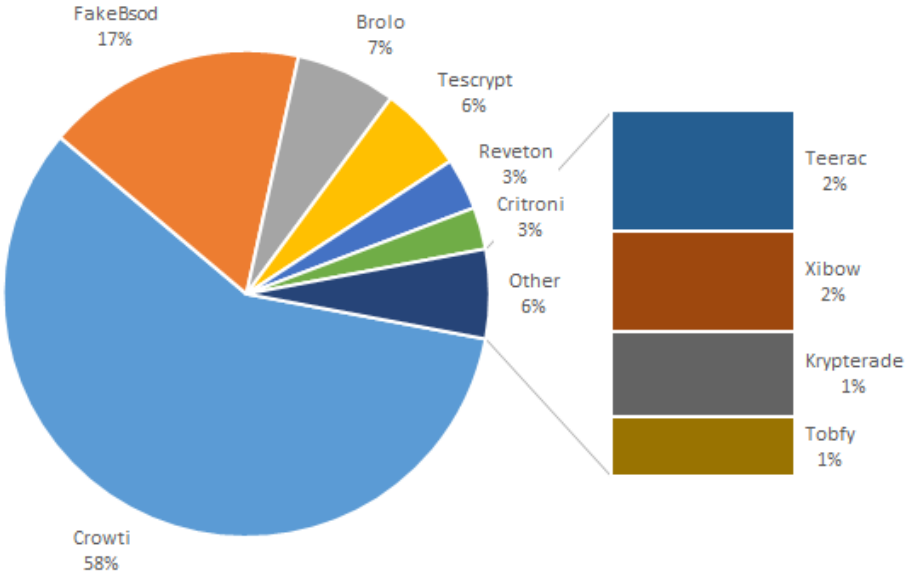

***Fig. 2**: Famiglie di Ransomware più diffuse a novembre 2015*
(rif. https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx)

4. Cosa fare se si è colpiti da un Ransomware

È bene chiarire da subito che non è possibile decifrare i file cifrati dal Ransomware, a meno che qualcuno non sia riuscito a prendere il controllo della botnet e della rete di sistemi che generano e distribuiscono il malware, e da qui a risalire alle chiave di cifratura usate per cifrare in modo unico i documenti di ogni singolo utente con chiavi uniche per documento. Ad oggi questo è stato possibile solo in rari casi.
La soluzione migliore per recuperare i dati è quindi quella di avvalersi dei backup. È fondamentale verificare di avere adottato una strategia di backup tale da consentire il recupero del maggior numero di documenti possibili e tale da impedire nel contempo l'infezione dei backup stessi. In quest'ottica risultano molto utili tecnologie di backup che mantengono diverse versioni dei documenti, consentendo così di risalire a versioni non cifrate del documento.
Se sul computer era attiva la File History (in **Windows 10** e **Windows 8.1**) o la System Protection (in **Windows 7** e **Windows Vista**) prima dell'infezione, è possibile recuperare versioni precedenti dei propri file. Occorre però osservare che alcuni Ransomware cifrano o cancellano anche le versioni di backup dei file, per cui spesso non è possibile affidarsi a queste funzionalità per recuperare i file.
Una volta verificata la presenza di un backup valido, la prima azione da fare è comunque quella di sottomettere il *sample* del malware al proprio fornitore di antivirus, e successivamente fare una scansione completa del sistema per ripulirlo dall'infezione. L'opzione migliore è quella di reinstallare il sistema completamente. Successivamente si può quindi procedere col ripristino da backup dei propri dati. Se i documenti che sono stati cifrati sono memorizzati su uno strumento come **OneDrive** o **OneDrive for Business**, è possibile recuperare eventuali versioni precedenti e non cifrate dei file.
Pagare il riscatto è l'ultima delle opzioni, ma essa non fornisce nessuna garanzia di poter effettivamente recuperare i file, rende la vittima un obiettivo preferenziale per ulteriori attacchi, e infatti si è osservato che dopo il pagamento spesso il Ransomware torna ad infettare il sistema.

5. Soluzioni per prevenire il rischio di Ransomware

Al di là di come recuperare i documenti in caso di infezione, la vera domanda è come fare a prevenire in futuro il rischio di ulteriori infezioni e la conseguente perdita di dati e di operatività. È necessario adottare un approccio strutturato e una strategia di sicurezza a vari livelli, che darà benefici non solo per ridurre l'impatto di questa particolare minaccia ma che deve rientrare in un piano di sicurezza più ampio volto a ridurre il rischio ad un livello accettabile per la specifica organizzazione.
Le aree di interventi principali sono mostrate di seguito, ma il tutto deve essere affiancato da opportune politiche di backup tali da garantire la disponibilità del dato anche a fronte di questi attacchi, e deve rientrare in una strategia di sicurezza complessiva. Approfondiamo ora alcune di queste misure.

➨ Formazione degli utenti

Senza alcuna ombra di dubbio, l'azione più efficace per ridurre il rischio di infezioni da Ransomware è la formazione degli utenti attraverso un programma periodico che educhi gli utenti a riconoscere mail e comportamenti sospetti e a diffidare dall'aprire messaggi inattesi, soprattutto se provenienti da mittenti non conosciuti e da cui comunque abitualmente non si ricevono messaggi. Tra le risorse utili in questo senso si ricorda il Microsoft Security Awareness Training Toolkit e il sito della Polizia Postale (http://www.commissariatodips.it).

➨ Misure di sicurezza sulla posta elettronica

Assicurarsi che le misure minime di protezione della posta elettronica siano correttamente configurate. Tra queste è consigliabile:

- Bloccare a livello di posta gli allegati che possono contenere codice eseguibile: .exe, .cmd, .scr, .lnk, estensioni di scripting (ad esempio .vbs, .js) e tutte le altre estensioni legate a file che possono includere codice eseguibile. Bloccare I file zip nel caso l'antivirus per la posta non ne faccia la scansione.
- Assicurarsi che il sistema anti-spam sia funzionante e aggiornato, avvalendosi di tecnologie come l'uso di Sender Policy framework

Utilizzare strumenti avanzati di protezione della posta che siano in grado di impedire che l'allegato contenente componenti malevole o i link a siti malevoli siano verificati ed eventualmente bloccati prima di raggiungere la caselle di posta dell'utente. Un esempio di queste tecnologie è la componente Advanced Threat Protection (ATP) di Exchange Online.

Application Whitelisting

Usare le funzionalità di Application Whitelisting che sono già presenti nel sistema operativo è una delle misure più efficaci a prevenire l'infezione da Ransomware. Ad esempio questa misura è riconosciuta essere dall'ente di sicurezza del governo australiano (http://www.asd.gov.au/infosec/mitigationstrategies.htm), come la prima misura in assoluto più efficace per prevenire intrusioni.

- Sulle versioni Enterprise di Windows, è possibile usare delle politiche basate su AppLocker per bloccare l'esecuzione di file dalla cartella c:\users\<username>\Appdata, o ancora meglio, definire quale è il software aziendale che deve essere permesso e bloccare di conseguenza tutte le altre tipologie di software non desiderato.
- Su Windows 10 è disponibile la funzionalità chiamata Device Guard che permette di definire esattamente il software consentito: si tratta di una misura specialmente utile in quegli scenari dove l'IT ha un buon controllo del software installato sui propri sistemi, e dove siamo in presenza di sistemi su cui è ben definita la pila software necessaria.
- Su versioni non-Enterprise, usare le Software Restriction Policies.

Misure di sicurezza sull'antivirus

È importante utilizzare un antivirus costantemente aggiornato, e, dove possibile, avvalersi di funzionalità che permettano di ottenere delle signature dinamiche da servizi online. Per coloro che usano un antivirus come Windows Defender o System Center Endpoint Protection questa funzionalità si può abilitare come segue:

- abilitare la funzionalità MAPS "Advanced membership" che migliora del 20% la detection di nuove varianti del virus che vengono rilasciate a decine ogni giorno;
- assicurarsi che in SCEP sia abilitata la scansione delle email e degli allegati.

Aggiornamento dei sistemi

- Mantenere i sistemi allineati al rilascio degli ultimi aggiornamenti di sicurezza, non solo del sistema operativo ma specialmente di applicazioni terze come Java, Shockwave, Silverlight, che sono quelle maggiormente sfruttare per introdurre il virus grazie alla diffusione dell' Angler Exploit kit
- Implementare lo strumento gratuito EMET per limitare gli attacchi sulle applicazioni non aggiornate e gli attacchi 0-day.

Misure di sicurezza sul browser e in Office

- Abilitare in Internet Explorer l'uso del filtro SmartScreen che verifica l'attendibilità del sito visitato e l'assenza di malware noti
- Abilitare la funzionalità di blocco dell'esecuzione dei controlli ActiveX obsoleti per evitare che vengano sfruttate vulnerabilità note in questi componenti.
- Bloccare l'esecuzione delle macro negli strumenti Office, consentendo la sola esecuzione di macro a partire da file che risiedono in una locazione affidabile, come il proprio file server o Sharepoint. Anche questa configurazione può essere controllata a partire da politiche centralizzate. ©

RISORSE

Formazione

- Security Awareness Training Toolkit: https://www.microsoft.com/en-us/download/details.aspx?id=11428
- Sito pubblico di Microsoft con le raccomandazioni contro Ransomware: https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx?c2901eeb-2a9e-438d-8928-1a4a16f316e5=True
- Video (in inglese) che spiega il problema e le possibili mitigazioni: https://channel9.msdn.com/Blogs/Taste-of-Premier/Ransomware101

Posta elettronica

- ATP: https://blogs.office.com/2015/04/08/introducing-exchange-online-advanced-threat-protection per maggiori dettagli)
- Office 365: https://support.microsoft.com/en-us/kb/kbview/2640313
- Exchange: http://blogs.technet.com/b/industry_insiders/archive/2006/01/24/spf-in-sp2-exchange.aspx

Application Whitelisting

- Windows 7 AppLocker Executive Overview: http://msdn.microsoft.com/en-us/library/dd548340(v=ws.10).aspx
- AppLocker Step-by-Step Guide: http://technet.microsoft.com/en-us/library/dd723686(v=WS.10).aspx

EMET

- https://support.microsoft.com/en-us/kb/2458544
- EMET 5.5: https://www.microsoft.com/en-us/download/details.aspx?id=50766. ◊