Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

COMPUTER EMERGENCY RESPONSE TEAM PUBBLICA AMMINISTRAZIONE
CERT - PA

Mitigare gli effetti di WannaCry (WCry, WannaCryptOr)

La campagna ransomware WannaCry, che sta affliggendo oltre 100 paesi in tutto il mondo, sta provocando danni molto elevati, sia sotto il profilo strettamente economico, che in termini di informazioni che non sarà più possibile recuperare.

In questo documento sono riportate una serie di azioni che possono essere assunte per mitigare l'impatto della campagna, soprattutto cercando di evitare l'estensione della compromissione a sistemi che non sono già compromessi. È abbastanza evidente che laddove i dati siano stati già cifrati l'unica strategia possibile è il ripristino da una copia di backup non toccata dal malware. Nell'ultima sezione sono contenute alcune considerazioni su quanto fare per il ripristino in questi casi.

Protezione dalla compromissione.

L'unica vera protezione dalla compromissione è l'eliminazione della vulnerabilità attraverso l'istallazione della patch sviluppata e pubblicata da Microsoft con il Microsoft Security Bulletin MS17-010-Critical:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nel Blog della società sono reperibili ulteriori informazioni utili:

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/?utm_source=t.co&utm_medium=referral

Protezione contro l'azione del malware si può ottenere attraverso l'antivirus, che deve essere aggiornato ad una versione successiva rispetto a quella pubblicata da ciascun produttore dopo il 12 maggio.

È fondamentale tenere presente che se l'antivirus ha il vantaggio di poter "ripulire" una macchina compromessa, cosa che la sola istallazione della patch non può fare, d'altra parte la vulnerabilità non eliminata potrebbe essere sfruttata da una nuova versione del malware che sfugge al controllo dell'antivirus. Perciò è tassativa l'istallazione della patch.

Ulteriori misure atte a ridurre la probabilità di compromissione, e quindi l'estensione di questa, sono:

1. Blocco del protocollo SMB sulla frontiera;
2. Disattivazione del protocollo SMB ove non specificamente richiesto;
3. Blocco sulla frontiera del traffico diretto verso indirizzi ed URL indicati nelle raccolte disponibili sui siti specializzati, quali, ad esempio AlienVault (https://otx.alienvault.com/pulse/5915db384da2585b4feaf2f6/), US-CERT (https://www.us-cert.gov/ncas/alerts/TA17-132A) e lo stesso CERT-PA (https://www.cert-pa.it/documents/10184/0/WCry.IoC.014.infosharing.xlsx/8cd459dd-2f0c-4f62-b139-9ce6f2775b89). Il blocco non deve riguardare il traffico di cui al punto 4.
4. Abilitare il traffico http verso l'URL:
   hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com[1]
   hxxp://www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com[1]
   in modo da attivare il "*kill switch*" presente in alcune versioni del malware e bloccare così la sua attività.

[1] L'URL è indicato con la notazione utilizzata normalmente per evitare che un link possa essere attivato accidentalmente: "hxxp" sta per "http" e "[.]" sta per ".".

5. In alternativa al punto 4 è possibile redirigere tutto il traffico http diretto verso il web server in esso specificato verso un server fittizio che genera una risposta HTTP code 200 per qualsiasi richiesta in arrivo.

Riavvio delle macchine spente.

Le macchine che erano spente al momento della diffusione, per altro molto rapida, del malware e non sono state accese sono sicuramente indenni; vale perciò la pena di usare qualche accorgimento per evitare che la compromissione presente in altri sistemi possa estendersi anche ad esse.

Contemporaneamente l'accensione di una macchina compromessa può provocare la compromissione di tutti i sistemi presenti sulla stessa rete. Ne segue che è opportuno procedere all'accensione dei sistemi con particolare cautela.

Nel caso non si abbia certezza riguardo alla situazione di vulnerabilità o compromissione di un sistema, la procedura che segue consente di ridurre sensibilmente i rischi legati alla sua riaccensione senza richiedere particolari conoscenze tecniche, per cui può essere eseguita, almeno nel caso di reti wired, anche da utenti non particolarmente esperti:

1. Prima di accendere la macchina scollegarla dalla rete locale, disconnettendo il cavo di rete (nel caso di connessioni Wi-Fi occorre disabilitarne l'interfaccia prima che avvenga il caricamento del sistema operativo, tale operazione può non essere alla portata dell'utente).
2. Accendere la macchina scollegata e verificare che l'avvio (bootstrap) avvenga regolarmente. Se si verificano eventi anomali, quali ad esempio ritardi molto prolungati, comparsa di messaggi insoliti, etc., non procedere oltre nel riavvio e chiedere il supporto esperto.
3. Se l'avvio è avvenuto regolarmente, aprire una sessione ed effettuare sull'hard disk della macchina una ricerca per file il cui nome abbia l'estensione .wncry. La ricerca deve terminare senza individuare alcun file, se invece ne viene individuato qualcuno non procedere oltre nel riavvio e chiedere il supporto esperto.
4. Se è stato superato il passo precedente, prima di collegare il sistema alla rete chiudere tutte le applicazioni, in particolare quelle di posta elettronica, che dovessero essere state avviate automaticamente all'apertura della sessione.
5. Ricollegare il sistema alla rete locale e forzare l'aggiornamento dell'antivirus. Attendere che tale operazione sia completata prima di aprire qualsiasi applicazione, in particolare non accedere in nessun modo a sistemi di posta elettronica. Dopo il suo termine il sistema può essere utilizzato normalmente.

Nel caso in cui sul sistema non sia istallata la patch di cui al bollettino MS17-010, prima di collegarlo alla rete, disattivare il protocollo SMB ed istallare la patch insieme con l'aggiornamento dell'antivirus. Il protocollo potrà essere riattivato, nel caso sia necessario, alla fine della procedura.

Particolare attenzione deve essere posta nella gestione dei messaggi di posta elettronica, che potrebbero essere utilizzati come vettore primario di infezione laddove sulla frontiera fosse bloccato il protocollo SMB, come consigliato al punto 1 dell'elenco contenuto nella sezione precedente. In generale debbono essere scrupolosamente osservate le seguenti regole:

a) Non aprire mail inattese o comunque di provenienza incerta, evitando nel modo più assoluto di aprire allegati di cui non si conosce la natura e l'origine.
b) Non cliccare per nessuna ragione su link contenuti all'interno di mail di cui non sia assolutamente certa la provenienza, verificando direttamente con il mittente (e.g. telefonicamente) l'effettivo invio da parte sua del messaggio.

La sicurezza non è mai assoluta

Le indicazioni contenute nel presente documento sono essenzialmente regole di buon senso che riducono il rischio di compromissione da parte di WannaCry, ma non possono annullarlo, anche perché gli attaccanti individuano continuamente nuove strategie per aggirare le misure di contrasto messe a protezione dei sistemi.

Per altro l'accento è stato posto sulla semplicità di attuazione, piuttosto che sulla completezza della copertura dei casi che possono verificarsi.

La migliore protezione nei confronti degli eventi imprevisti, siano essi dolosi, colposi o casuali, è una copia di sicurezza dei dati aggiornata. Nel malaugurato caso che la cifratura dei dati sia già avvenuta, questa è la sola strada che permette il recupero delle informazioni, visto che anche l'eventuale pagamento del riscatto non garantisce l'effettivo ripristino dei file cifrati.

È opportuno, specie se non si è sicuri della completezza del contenuto della copia di sicurezza più aggiornata disponibile, generare una copia di sicurezza completa del sistema con i file cifrati prima di effettuare il ripristino. Oltre che per eventuali indagini, essa potrebbe tornare utile se, in un futuro più o meno prossimo, venisse scoperta la chiave di decodifica dei file cifrati.

Indicatori di Compromissione (IoC)

WCry.IoC.014.infosharing.xlsx