Rimozione e Bonifica Conficker

Premessa: Metodo di diffusione e prevenzione (Importante)

Il Conficker è un Worm, scoperto ormai nel 2008, che infetta le piattaforme Microsoft.
Per diffondersi sfrutta una falla del servizio di rete di Windows (corretta dalla patch MS08-67 ad ***Ottobre 2008***), ma può essere trasmesso anche tramite memorie di massa USB, come pendrive (chiavette) o hard disk esterni infetti, tramite violazione delle credenziali di sistema nel caso in cui la password di amministratore locale sia banale (es. 0000, qwerty, etc) oppure non ci sia una password, o tramite condivisioni di rete con permessi di scrittura. Se un utente con privilegi di amministratore (es. un amministratore di dominio) effettua l'accesso ad una macchina infetta, il Worm si può propagare su altre macchine della rete anche non vulnerabili, sfruttando le credenziali dell'utente loggato.

Il motivo principale per il quale i sistemi, dopo ormai 3 anni dalla scoperta del Conficker, sono ancora vulnerabili, è che per strane credenze popolari, leggende metropolitane e paranoie infondate, non vengono eseguiti regolarmente gli aggiornamenti di sicurezza di Windows che fanno parte della normale manutenzione di un computer.

Come si effettua la manutenzione di tutti i macchinari e gli strumenti di lavoro, anche i Computer vanno controllati e tenuti in buono stato e questo include fare gli aggiornamenti di Windows Update.
Se si trascura la manutenzione del computer, poi ci si ritrova a dover eseguire in poche ore tutto quello che non si è fatto in anni di incuria.

Alcuni consigli e accorgimenti per evitare di infettarsi con il conficker includono:

1. Tenere il sistema operativo aggiornato almeno con le patch di sicurezza critiche.
2. Tenere aggiornato il software antivirus in uso.
3. Evitare di avere account Administrator senza password o con password deboli.
4. Evitare di avere cartelle condivise con diritto di scrittura per tutti (impostarle con restrizioni per chi non è autenticato o per scrittura solo da account ben protetti da password).
5. Vietare l'uso di chiavette USB di cui non si conosca la provenienza sui computer aziendali.
6. Disattivazione dell'esecuzione automatica di programmi da chiavette USB e da CD all'inserimento (vedere articolo KB Microsoft all'indirizzo http://support.microsoft.com/kb/967715 per maggiori dettagli)

Solo Windows 7 e Windows Server 2008 R2 sono stati rilasciati con la vulnerabilità già corretta, tutti gli altri sistemi operativi, da Windows 2000 a Windows Vista, sono vulnerabili finché non si installano le patch di sicurezza.
La prima cosa che il Conficker si preoccupa di fare, infatti, è di togliere al computer l'accesso ai siti di Microsoft, per evitare agli utenti di fare gli aggiornamenti (altro indizio che fa capire che gli aggiornamenti sono molto importanti per evitare infezioni e non il viceversa). Di conseguenza, un buon metodo per vedere se la macchina è ancora infetta oppure se il Conficker è stato effettivamente rimosso, è visitare il sito http://www.microsoft.com e verificare se si riesce ad accedervi o no.
Se la macchina è ancora infetta, per prima cosa bisogna quindi rimuovere il Conficker seguendo passo-passo (senza saltarne, sono tutti necessari) la procedura seguente.

Step 1: Rimozione Trojan.Win32.Conficker:

1. Per la sua natura, per poter essere certi al 100% che il Conficker venga rimosso definitivamente dalla rete, ***è necessario scollegare tutti i computer infetti*** (almeno quelli infetti), perché se si lasciano connessi, appena si riattacca un computer ripulito, viene immediatamente reinfettato perché ancora vulnerabile senza aver installato le patch di Sicurezza Microsoft
2. Dal computer infetto procedere ad Aggiornare Vir.IT eXplorer PRO all'ultima versione disponibile. Riavviare il computer se richiesto. Questa procedura è valida per versioni di Vir.IT eXplorer PRO che abbiano scaricato e sia attivo (quindi con conseguente riavvio del computer se non era ancora aggiornato a quella versione) almeno ***l'aggiornamento 6.8.50*** che include importanti modifiche al motore per una rimozione più agevole del Conficker.
3. da Vir.IT Security Monitor (lo scudo giallo-blu vicino all'orologio di Windows), cliccare sul menu TOOLS e scegliere la voce OPZIONI. ***Impostare FILE TUTTI***. Premere OK per rendere effettivo il cambio delle impostazioni. Se non si imposta File Tutti il Conficker sarà in grado di riattaccare il computer anche con l'antivirus aggiornato.
4. Aprire Vir.IT eXplorer PRO con i diritti di Amministratore (per Windows Vista e 7 è sufficiente fare click con il tasto destro sul collegamento e poi su Esegui come Amministratore, con Windows Xp e 2000 è preferibile eseguire il login con un account che abbia privilegi di amministratore).
5. Eseguire una scansione con Vir.IT eXplorer PRO con diritti di amministratore su tutto il disco. Verrà segnalato un file infetto generalmente all'interno della cartella C:\Windows\system32. A fine scansione verrà chiesto di riavviare il computer per la rimozione del virus.
6. Terminata la scansione è molto importante che venga riavviato il computer per disattivare definitivamente il virus trovato tramite la scansione.

Se il Conficker NON dovesse venire identificato durante la scansione, Vir.IT è già aggiornato all'ultima versione e si accusano i sintomi di infezione da Conficker (rete congestionata, impossibilità di visitare i siti Microsoft, Windows Update non funziona, Windows Defender è stato disattivato, ecc), significa che si tratta di una nuova variante e sarà necessario procedere all'invio dei file di Esecuzione Automatica. VirIT Security Monitor include una procedura che permette di mandarci automaticamente i file necessari.

1. Aprire VirIT Security Monitor cliccando sullo scudo giallo-blu in basso a destra vicino all'orologio di Windows.
2. Nella finestra principale di VirIT Security Monitor cliccare sulla prima icona in alto a sinistra (quella con l'ingranaggio) per aprire le opzioni.
3. Nella finestra delle opzioni selezionare "Web Mail TG Soft" alla voce "Invia file sospetti con" e premere OK per applicare le impostazioni.
4. Premere sul bottone con l'uomo spia in impermeabile per aprire la finestra dei programmi in esecuzione automatica.
5. Nella finestra dei programmi in esecuzione automatica premere sul pulsante [Invia Mail]
6. Scrivere il proprio indirizzo di posta elettronica nel campo mittente e inserire la descrizione del problema nel campo Descrizione (possibile infezione da Conficker).
7. Premere Invia.

Step 2: Installazione Patch di sicurezza Microsoft dopo aver rimosso il Conficker

Per eliminare la vulnerabilità più utilizzata dal Conficker per infettare la macchina, è necessario installare la patch di sicurezza di Ottobre 2008 (che sarebbe dovuta essere installata con Windows Update).

1. *Installazione della patch MS08-067 (958644) per evitare di reinfettarsi con il Conficker:*

La Pacth è scaricabile gratuitamente direttamente dal sito di Microsoft, all'indirizzo:
http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
Bisogna selezionare il proprio sistema operativo dalla lista e poi cambiare la lingua in Italian nella pagina del download.
NB: Il Service Pack 3 per Windows Xp non include questa patch, quindi non è sufficiente installare il solo Service Pack 3

2. *Arrestare il servizio Utilità di pianificazione:*

Per farlo seguire le indicazioni di seguito:

a. Aprire Vir.IT eXplorer Pro, cliccare sul menu TOOLS e poi su VirIT Agent System
b. Nel campo "Tipo Comando" inserire: 2
c. Nel campo "Valore Comando" inserire: Schedule
d. Cliccare sul pulsante INSERISCI.
e. Cliccare su EXIT e riavviare il computer (altrimenti non verrà disabilitato).

A questo punto è *fortemente* consigliato aggiornare il sistema operativo con ***tutte*** le patch di sicurezza rilasciate da Microsoft negli ultimi anni (operazione che andrebbe fatta ogni volta che vengono rilasciate patch di sicurezza per Windows, ovvero una volta al mese).

Per Windows XP:

1. Se non è già installato scaricare e installare il Service Pack 3 per Windosws Xp.
   Link diretto alla pagina di download, basta premere sul pulsante [Scarica] all'interno della pagina:
   http://www.microsoft.com/downloads/details.aspx?displaylang=it&FamilyID=5b33b5a8-5e76-401f-be08-1e1555d4f3d4
2. Una volta installato il Service Pack 3 andare sul sito http://www.windowsupdate.com e fare **tutti** gli aggiornamenti automatici critici che vengono proposti.
3. Ripetere il punto 2 finché sul sito di Windows Update non verranno più proposti aggiornamenti critici.

Dove non sia possibile installare i Service Pack (molto sconsigliato) o non si possono installare tutti gli aggiornamenti di Windows Update, si consiglia di installare manualmente almeno le seguenti patch:

- MS08-67 (KB958644): http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx (se non è già stata installata al punto 1 dello Step 2)
- MS08-68 (KB957097): http://www.microsoft.com/technet/security/bulletin/Ms08-068.mspx
- MS09-001 (KB958687): http://www.microsoft.com/technet/security/Bulletin/MS09-001.mspx

Per Windows 2000:

Come prima cosa bisogna installare il Service Pack 4 (se non è già installato) che contiene tutte le patch cumulative, scaricabile da questo indirizzo:
http://www.microsoft.com/downloads/details.aspx?displaylang=it&FamilyID=1001aaf1-749f-49f4-8010-297bd6ca33a0
Scaricato ed installato il Service Pack 4, visitare il sito http://www.windowsupdate.com e fare tutti gli aggiornamenti consigliati (e facoltativi che riguardano la sicurezza) che propone il sito di Windows Update.

Non basterà una sola passata visto la quantità di aggiornamenti da fare, visitare il sito http://www.windowsupdate.com finché non dirà che non sono più presenti aggiornamenti disponibili.
Dove non si possono installare tutti gli aggiornamenti di Windows Update (per qualche incomprensibile ragione che andrebbe evitata a tutti i costi), si consiglia di installare manualmente almeno le seguenti patch:

- http://www.microsoft.com/downloads/details.aspx?displaylang=it&FamilyID=e22eb3ae-1295-4fe2-9775-6f43c5c2aed3
- http://www.microsoft.com/downloads/details.aspx?displaylang=it&FamilyID=44c971e6-96fc-4bba-8f4a-f9d46bda2b6c
- http://www.microsoft.com/downloads/details.aspx?displaylang=it&FamilyID=e0678d14-c1b5-457a-8222-8e7682760ed4

Per Altri Sistemi Operativi:

A questi indirizzi si trovano le patch indicate in precedenza anche per tutti gli altri sistemi operativi che sono vulnerabili, la pagina è in inglese e prima di scaricare la patch bisognerà cambiare lingua del file da scaricare altrimenti non verrà installata sul computer.
http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx
In ogni caso il metodo migliore per installare le patch è fare Windows Update automaticamente e far installare a Windows gli aggiornamenti di sicurezza.

Una volta rimosso il Conficker e installate le patch di sicurezza, si possono ripristinare le funzionalità che il Conficker ha disattivato per evitare di essere scoperto.

Per ripristinare i file nascosti:

- Windows XP: http://www.tgsoft.it/tools/varie/hiddenfile.zip
  Estrarre il file zip ed eseguire il file di registro estratto (hiddenfile.reg) dando il consenso quando richiesto.
- Windows Server 2003: http://www.tgsoft.it/tools/varie/hidden-server2003.zip
  Estrarre il file zip ed eseguire il file di registro estratto (hidden-server2003.reg) dando il consenso quando richiesto.

Se è stata disattivata anche la modalità provvisoria, consultare il post sul blog TG Soft per ripristinarla correttamente:
http://blognew.aruba.it/blog.malwarelist.org/Nuova_variante_Trojan_Win32_Conficker_AS_8673.shtml
Dopo aver bonificato tutta la rete si può riattivare il servizio delle "Utilità di pianificazione" se necessario.

Per riattivare il servizio di Utilità di pianificazione dal Pannello di Controllo andare su Strumenti di Amministrazione e poi su Servizi.
Selezionare il servizio Utilità di pianificazione e accedere alle sue proprietà, impostare il tipo di avvio in AUTOMATICO ed avviarlo se necessario, altrimenti si avvierà automaticamente al prossimo riavvio del sistema.