Come Sconfiggere e Rimuovere il Worm Conficker

Scritto da ***Alessandro Tani*** (alessandro.tani@homeworks.it)

- Pubblicato il giorno 8 Aprile 2009 - Aggiornato il giorno 18 Maggio 2010 -

---

In questo breve articolo, vorrei spiegare come arginare e poi rimuovere il worm Conficker. Questo worm, si basa su una vulnerabilità nota dei sistemi Windows ed è in grado di paralizzare un intera rete di calcolatori, mandando in tilt l'attività quotidiana di un azienda. Quanto verrà descritto in questo articolo, è liberamente ispirato alla *Knowledge Base* della Microsoft Virus alert about the Win32/Conficker.B worm.

Indice

Licenza

Breve Descrizione del Worm Conficker

Il worm Conficker, anche noto con i nomi di *Downadup* (usato dalla società Symantec) o Kido, è sicuramente uno

dei worm (col termine *worm* s'intende un virus in grado di auto-riprodursi in una rete informatica) più pericolosi mai scritti sinora dagli autori di virus. Il worm Conficker è stato rilevato per la prima volta nel Novembre 2008 (**Conficker.A**), nel Dicembre 2008 è stata scoperta la sua prima variante (**Conficker.B**) e nel Marzo 2009 è stata individuata la sua seconda variante (**Conficker.C**). Nel passaggio da una versione alla successiva, in particolar modo con la prima variante, **Conficker.B**, la capacità infettiva e distruttiva del virus sono andate migliorando.

Nella tabella di seguito riporto un breve riassunto delle principali caratteristiche del Conficker:

Nome Variante	Metodologia di Diffusione	Metodologia d'Infezione	Schermatura
Conficker.A	Sfruttamento della vulnerabilità MS08-67	Download da siti web (protocollo HTTP)	Nessuna
Conficker.B	Sfruttamento della vulnerabilità MS08-67, delle risorse condivise in scrittura utilizzando attacchi di *forza bruta* sulla password dell'utente Administartor locale delle macchine infettate e sui dispositivi removibili come le chiavette USB (file *Autoplay.inf*)	Download da siti web (protocollo HTTP) e parziale supporto alle metodologie Peer-To-Peer	Soppressione di alcune query DNS, inibizione del servizio Windows Update, criptazione delle procedura di scaricamento HTTP e crtipazione delle procedure di scaricamento Peer-To-Peer
Conficker.C	Nessuna	Download migliorato dai siti web (protocollo HTTP) e pieno supporto alle metodologie Peer-To-Peer	Soppressione di alcune query DNS, inibizione del servizio Windows Update, inibizione di alcuni programmi antivirus, analisi sofisticate contro i programmi di sicurezza informatica, criptazione delle procedura di scaricamento HTTP e Peer-To-Peer

Stando alle fonti ufficiali, i paesi più colpiti dal worm Conficker sono:

1. Cina (**28.7%**)
2. Argentina (**11.3%**)
3. Taiwan (**6.7%**)
4. Brasile (**6.2%**)
5. India (**5.8%**)
6. Cile (**5.2%**)
7. Russia (**5%**)
8. Malesia (**2.8%**)
9. Colombia (**2.1%**)
10. Messico (**1.9%**)

Per maggiori informazioni sui meccanismi di funzionamento del worm Conficker, invito il lettore a leggere i seguenti articoli Know Your Enemy: Containing Conficker, The Conficker Mystery, MSRT Released Today Addressing Conficker and Banload, Downadup: Small Improvements Yield Big Returns e W32.Downadup.C Pseudo-Random Domain Name Generation.

L'articolo Know Your Enemy: Containing Conficker è una preziosissima lettura che invito comunque il lettore a leggere.

I Sintomi

Quando una o più postazioni di lavoro di un'azienda viene colpita dal worm Conficker, si possono verificare alcune delle situazioni descritte di seguito:

- una o più account di dominio risulta essere bloccata in maniera inspiegabile;
- i criteri di blocco degli account vengono alterati;
- i servizi **Automatic Updates**, **Background Intelligent Transfer Service (BITS)** e **Error Reporting Services** risultanon disabilitati;
- i Domain Controller risultano lenti a rispondere alle interrogazioni su Active Directory (con conseguente accesso ad esempio alle Mailbox basate su Microsoft Exchange);
- alcuni siti di sicurezza informatica risultano inaccessibili;
- un numero considerevole di processi *anomali* viene pianificato per essere eseguito.

Non sempre, ovviamente, i sintomi descritti possono venire ricondotti al worm Conficker, certo è bene però porvi la massima attenzione e non sottovalutare eventuali segnalazioni che possono venire dai dipendenti aziendali nel loro normale svolgimento delle mansioni quotidiane. Nei giorni in cui questo articolo è stato scritto, la maggior parte dei programmi antivirus ha aggiornato le proprie definizioni di virus, worm e malware con le *impronte* del worm Conficker, pertanto è molto probabile che se il programma antivirus presente in un azienda è aggiornato, questi sia in grado di individuare e segnalare la presenza del worm Conficker. È auspicabile, in simili circostanze, che l'infezione del worm Conficker resti circoscritta. Qualora ciò non avvenisse, si possono prendere in considerazione le indicazioni che riporto nel paragrafo Come Arginare l'Infezione.

Come si Diffonde il Worm Conficker

La pericolosità del worm Conficker verte tutta nella sua efficacia nel riprodursi facilmente e rapidamente all'interno di una rete aziendale. Per sapere come arginare il worm Conficker bisogna conoscere come il worm si propaga nella rete e che cosa cerca di fare dopo che si è installato su una data postazione di lavoro. Per approfondire questo argomento consiglio la lettura degli articoli della Microsoft Worm:Win32/Conficker.B e della Kaspersky Net-Worm.Win32.Kido.bt.

Mentre la prima versione del worm, **Conficker.A**, sfruttava solamente la vulnerabilità MS08-067 come vettore dell'infezione; la sua prima variante, **Conficker.B**, introduceva dei nuovi metodi di diffusione che hanno portato il worm alla ribalta internazionale, come una delle maggiori piaghe d'Internet. I metodi utilizzati dal **Conficker.B** per diffondersi all'interno di una rete aziendale sono:

- sfruttare le postazioni di una rete in cui risulta operativa la vulnerabilità MS08-067;
- sfrutta le credenziali dell'account che sta operando sul computer per accedere in scrittura alla condivisione amministrativa **<Nome_Computer>****ADMIN$** di una macchina remota;
- esegue attacchi di *forza bruta* sulla password dell'utente Administrator locale di una macchina e se riesce

a risalire a questa password, utilizza l'account individuato per tentare di accedere in scrittura alla condivisione amministrativa **<Nome_Computer>\ADMIN$** di una macchina remota;

- sfrutta il file **Autoplay.inf** dei dispositivi removibili, come ad esempio i dischi USB, quando questi vengono collegati ad una postazione infetta, per infettare nuove postazioni di lavoro.

Come si vede, l'eliminazione della vulnerabilità MS08-067, non è sufficiente per arginare la diffusione del worm **Conficker.B**. Sino a quando ci sarà nella rete una macchina infetta col worm Conficker, il Conficker avrà a disposizione uno qualunque dei metodi sopra citati per diffondersi nella rete, col risultato che anche se sulle postazioni viene eliminata la vulnerabilità MS08-067, queste continuano ad essere possibili prede del Conficker. In particolare, lo sfruttamento da parte del worm delle credenziali di collegamento alla macchina per cercare di accedere in scrittura alla risorsa di rete amministrativa **<Nome_Computer>\ADMIN$** di una postazione remota, rende l'eventuale infezione da parte di un server di rete particolarmente grave, in quanto ogni qual volta si accede a quel server con le credenziali di amministratore di dominio, si rischia d'infettare di nuovo col worm Conficker l'intera rete aziendale.

Come Arginare l'Infezione

Se si ha l'impressione o la certezza che molte postazioni di lavoro o server siano stati vittima del worm Conficker, per prima cosa bisogna cercare di arginare la diffusione dell'infezione. Successivamente si dovrà cercare di agire alla radice del problema, ovvero eliminare la vulnerabilità sfruttata dal Conficker. Infine, eliminare dalle varie postazioni colpite, il worm Conficker. Una possibile strategia per arginare la diffusione del worm Conficker potrebbe essere (quanto riportato di seguito è liberamente ispirato dall'articolo Virus alert about the Win32/Conficker.B worm):

- creare un Group Policy Object in grado di limitare la diffusione del worm Conficker;
- aggiornare le postazioni della rete con l'aggiornamento MS08-67 della Microsoft che chiude la falla di sicurezza sfruttata dal worm Conficker;
- rimuovere il worm Conficker utilizzando un apposito programma (ad esempio col Malicious Software Removal Tool della Microsoft), da tutte le postazioni della rete che risultano infette;

In alternativa all'utilizzo dei Group Policy Object, qualora il numero delle postazioni infette o di rete sia basso, si può procedere manualmente su ciascuna postazione della rete (per sapere quali sono le operazioni da svolgere, rimando il lettore a quanto riportato nell'articolo Virus alert about the Win32/Conficker.B worm).

Il Group Policy Object da realizzare dovrà svolgere le seguenti attività:

- rimuovere i permessi di scrittura dalla chiave di registro **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost**;
- togliere i permessi di scrittura alla cartella **%windir%\tasks**;
- disabilitare l'esecuzione del file **Autoplay.inf**;
- disabilitare l'account **Administrator locale**;

Per creare il Group Policy Object da applicare su tutte le postazioni della rete (stando però ben attenti a non applicarla ai **Domain Controller**), si può procedere come segue (nel corso della spiegazione, faremo riferimento alla Group Policy Management Console e daremo per scontato che la **Group Policy Management Console** sia installata almeno su una postazione di lavoro della rete).

Puoi scaricare il backup del Group Policy Object che descriverò di seguito, **Conficker (Computers)**, cliccando qui (codice MD5: **32dd69b78aa8b15c30b4118f1cf1d05b**). Per scaricare il backup del Group Policy Object che neutralizza gli effetti della policy **Conficker (Computers)**, che per comodità ho chiamato **Disable Conficker Policy (Machine)**, direttamente da qui (codice MD5: **4390e952ea86985cbedc6595a59c5b29**). Per sapere come importare il **Group Policy Object** chiamati **Conficker (Computers)** e **Disable Conficker Policy (Machine)**, consulta il paragrafo Come Importare un Group Policy Object.

Rimuovere i permessi di scrittura dalla chiave di registro *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost*

Sulla postazione in cui è stata installata la Group Policy Management Console collegarsi con un utente che appartenga al gruppo degli **Enterprise Admins** ed avviare la **Group Policy Management Console**:

- creare un nuovo *Group Policy Object* (GPO) chiamato **Conficker (Computers)**, per ricordarci che questo GPO dovrà poi venire rimosso quando l'infezione del Conficker sarà debellata e che la GPO in questione verrà applicata alle varie postazioni di lavoro e server del dominio e non agli utenti;
- aprire la sezione **Computer Configuration\Windows Settings\Security Settings\Registry**;
- cliccare col pulsante destro del mouse sopra la voce **Registry** e selezionare la voce **Add Key**;
- nella finestra di dialogo denominata **Select Registry Key**, espandere la voce **Machine** e poi aprire la cartella **Software\Microsoft\Windows NT\CurrentVersion\Svchost**;
- premere il pulsante **OK**;
- nella finestra di dialogo che si apre, togliere il segno di selezione dalla voce **Full Control** dal gruppo **Administrators** e dall'utente **System** (assicurarsi però che sia il gruppo **Administrators**, sia l'utente **System** abbiano i permessi di lettura, **Read**, sulla chiave);
- premere il pulsante **OK** per confermare;
- nella finestra di dialogo denominata **Add Object** selezionare la voce **Replace existing permissions on all subkeys with inheritable permissions** e premere il pulsante **OK**.

In questo modo, il worm Conficker non sarà più in grado di alterare la chiave di registro **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost**.

Si osservi che per rimuovere questa impostazione, bisognerà creare un apposito Group Policy Object che ridia al gruppo **Administrators** i permessi di **Full Control** sulla chiave di registro *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost*. Un esempio di questo Group Policy Object può essere scaricato qui (codice MD5: **4390e952ea86985cbedc6595a59c5b29**). Si osservi

infine che coi soli permessi di **Read** al gruppo **Administrators** ed all'utente **System** sulla chiave di registro *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost*, non risulta possibile aggiornare una postazione con la **Service Pack 1** o la **Service Pack 2** di **Windows XP**, alla **Service Pack 3**. In questo caso, bisognerà spostare la postazione in cui si desidera applicare la **Service Pack 3** o in un *Container* o in una *Organization Unit* che non *ereditino* la GPO **Conficker (Computers)**, di modo che sulla postazione non risulti applicata la GPO **Conficker (Computers)**, o in altri termini, sulla chiave di registro *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost* il gruppo **Administrators** e l'utente **System** abbiano i permessi di **Full Control**. L'autore dell'articolo ha poi riscontrato che sino a quando gli *effetti* della GPO **Conficker (Computers)** sono attivi, non risulta possibile installare correttamente il programma **Internet Information Server**.

Togliere i permessi di scrittura alla cartella *%windir%\tasks*

Il worm Conficker crea un innumerevole pletora di processi pianificati *indesiderati*, alterando il contenuto della cartella **%windir%\tasks**. Per eviare ciò, andiamo a modificare il GPO chiamato **Conficker (Computers)** che abbiamo creato in precedenza:

- aprire la sezione **Computer Configuration\Windows Settings\Security Settings\File System**;
- cliccare col pulsante destro del mouse sopra la voce **File System** e selezionare la voce **Add File**;
- nella finestra di dialogo chiama **Add a file or folder** individuare e selezionare la cartella `%windir%\Tasks`. Premere il pulsante **OK** per confermare;
- nella finestra di dialogo che si apre, togliere i simboli di selezione dalle voci **Full Control**, **Modify** e **Write** sia per il gruppo **Administrators** e sia per l'utente **System**;
- premere il pulsante **OK** per confermare;
- nella finestra di dialogo denominata **Add Object** selezionare la voce **Replace existing permissions on all subfolder and files with inheritable permissions** e premere il pulsante **OK**.

Si osservi che per rimuovere questa impostazione, bisognerà creare un apposito Group Policy Object che ridia ai gruppi **Administrators** e **System** i permessi di **Full Control** sulla cartella *%windir%\tasks*. Un esempio di questo Group Policy Object può essere scaricato qui (codice MD5: **4390e952ea86985cbedc6595a59c5b29**).

Disabilitare l'esecuzione del file *Autoplay.inf*

Il worm Conficker, al pari di altri virus, worm e malware, sfrutta i file **Autoplay.inf** che si trovano nei dispositivi USB o Firewire per propagarsi. Per evitare che ciò accada, bisogna disabilitare l'esecuzione, da parte di Windows, dei file **Autoplay.inf**. Andiamo pertanto ad aggiungere questa funzionalità all'interno del GPO **Conficker (Computers)** che abbiamo creato in precedenza:

- andare nella sezione:
    - **Computer Configuration\Administrative Templates\System** per i domini di Active Directory basati su **Windows 2003**;

    - **Computer Configuration\Administrative Templates\Windows Components\Autoplay Policies** per i domini di Active Directory basati su **Windows 2008**;

- aprire la policy **Turn off Autoplay**;
- nella finestra di dialogo chiamata **Turn off Autoplay**, selezionare la voce **Enabled**;
- nel menù a tendina sottostante, denominato **Turn Off Autoplay on**, selezionare la voce **All drives**;
- premere il pulsante **OK** per confermare;

Disabilitare l'account Administrator locale

Il worm Conficker cerca, tramite *attacchi di forza bruta*, di individuare la password dell'utente **Administrator** locale relativo alla macchina che ha provveduto ad infettare. Poiché l'individuazione di questa password può favorire la sua propagazione nella rete, è bene disabilitare l'account Administrator locale di modo da scongiurare questa eventualità.

Se si decide di disabilitare l'utente Administrator locale delle varie postazion di dominio, bisogna *assolutamente evitare* di applicare il GPO **Conficker (Computers)** ai **Domain Controller**, altrimenti verrebbe disabilitato anche l'utente Administrator del dominio.

Per far ciò, bisogna modificare opportunamente il GPO **Conficker (Computers)** che abbiamo creato in precedenza:

- aprire la sezione **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**;
- aprire la policy **Accounts: Administrator account status**;
- nella finestra di dialogo **Accounts: Administrator account status** selezionare la voce **Define this policy** e poi la voce **Disabled**;
- premere il pulsante **OK** per confermare;
- chiudere l'editor dei Group Policy Object;
- applicare il Group Policy Object **Conficker (Computers)** a tutte le **Organization Unit** che si ritiene opportuno, tranne la Organization Unit chiamata **Domain Controllers**, altrimenti si rischierebbe di disabilitare l'account Administrator del dominio;
- chiudere la **Group Policy Management Console**.

Attendere a questo punto la replicazione del GPO **Conficker (Computers)** fra i vari **Domain Controller** della *Foresta* di *Active Directory*. Questo tipo di repliche di solito richiedono fra i *15 minuti* e i *90 minuti*. In linea di principio, quindi, un attesa di due ore dovrebbe essere più che sufficiente nella maggioranza dei casi. Una volta

preparata la GPO, si può procedere con l'installazione dell'aggiornamento **MS08-67** sulle varie postazioni e server della *Foresta* di *Active Directory*.

Come Aggiornare le Postazioni di Lavoro con l'Aggiornamento MS08-67

Per chiudere la vulnerabilità sfruttata dal worm Conficker, la Microsoft aveva rilasciato nel mese di Ottobre 2008, un opportuno aggiornamento, lo MS08-67. Su ciascuna postazione della *Foresta* di *Active Directory* che risulta priva dell'aggiornamento MS08-67, bisognerà provvedere ad installare la patch di sicurezza MS08-67. Di seguito riportiamo i collegamenti all'aggiornamento **MS08-67** relativi ai sistemi **Windows 2000**, **2003** ed **XP** (per gli aggiornamenti degli altri sistemi Windows, fate riferimento al testo riportato nell'aggiornamento MS08-67).

Si osservi che le postazioni **Windows 7** non soffrono della vulnerabilità MS08-67.

- aggiornamento **MS08-67** per i sistemi Windows 2000 con Service Pack 4;
- aggiornamento **MS08-67** per i sistemi Windows XP con Service Pack 2 e Service Pack 3;
- aggiornamento **MS08-67** per i sistemi Windows 2003 con Service Pack 1 e Service Pack 2;

Il modo migliore per distribuire questi aggiornamenti è il programma Microsoft Windows Server Update Services, o più brevemente **WSUS**. In alternativa, si potrebbe utilizzare un programma per la distribuzione del software, come ad esempio LANDesk. Qualora non si abbia a disposizione un server col programma **WSUS** installato o un programma per la distribuzione del software, si dovrà provvedere ad installare l'aggiornamento **MS08-67** o manualmente, oppure tramite un apposito script. In questo articolo, prenderò in considerazione la realizzazione di uno script in grado di installare l'aggiornamento **MS08-67**.

Si tenga presente che qualora ci si trovi di fronte a dei *collegamenti lenti*, all'interno di uno stesso *Sito di Active Directory*, non è detto che gli script di logon o all'avvio del sistema operativo vengano eseguiti. Per comportamento predefinito, Active Directory, non esegue gli script di logon o all'avvio del sistema operativo in presenza di *collegamenti lenti*.

Per prima cosa bisogna estrarre il contenuto dei file contenenti gli aggiornamenti relativi all'aggiornamento **MS08-67** (per rendere più semplice la spiegazione, supporrò che i file contenenti gli aggiornamenti siano stati scaricati all'interno della cartella *E:\Path\MS08-67* che si trova su un server chiamato *RUSSEL*):

- per l'aggiornamento relativo ai sistemi Windows 2000 con Service Pack 4 eseguire il comando:

```
E:\Patch\MS08-67\Windows2000-KB958644-x86-ENU.EXE /extract:E:\Path\MS08-67\Windows2000
```

- per l'aggiornamento relativo ai sistemi Windows XP con Service Pack 2 e Service Pack 3 eseguire il comando:

```
E:\Path\MS08-67\WindowsXP-KB958644-x86-ENU.exe /extract:E:\Path\MS08-67\WindowsXP
```

- per l'aggiornamento relativo ai sistemi Windows 2003 con Service Pack 1 e Service Pack 2 eseguire il comando:

```
E:\Path\MS08-67\WindowsServer2003-KB958644-x86-ENU.exe
/extract:E:\Path\MS08-67\Windows2003
```

Una volta estratti gli aggiornamenti, condividere la cartella *E:\Path\MS08-67* col nome **MS08-67** ed assegnare i permessi di condivisione ad **Everyone** in modalità **Full Control**.

Nello script Batch che propongo in questo articolo, inserisco i file di registro dell'esecuzione dello script stesso all'interno della cartella *\\RUSSEL\MS08-67*; pertanto affinché l'esecuzione dello script vada a buon fine, l'utente **SYSTEM** deve avere i permessi di scrittura nella cartella *\\RUSSEL\MS08-67*.

Un possibile script per l'installazione del aggiornamento **MS08-67** potrebbe essere:

Nella stesura dello script ho utilizzato il comando osver.exe scritto da Bill Stewart.

```
@echo off
rem ************************************************************************
rem *                                                                      *
rem * NOME SCRIPT: InstPatchMS08-67.cmd                                    *
rem *                                                                      *
rem * Script scritto da Alessandro Tani (Home Works S.p.A)                 *
rem *                                                                      *
rem * Versione 1.0 - Modificato l'ultima volta il 17/03/2009               *
rem *                da Alessandro Tani                                    *
rem * SCOPO:                                                               *
rem *                                                                      *
rem *  Questo script ha il compito di installare la patch                  *
rem *  numero MS08-67 della Microsoft per i sistemi Windows 2000,          *
rem *  2003 ed XP                                                          *
rem *                                                                      *
rem * File di log: \\RUSSEL\MS08-67\%COMPUTERNAME%_MS08-67.log            *
rem *                                                                      *
rem * PREREQUISITI:                                                        *
rem *                                                                      *
rem *  - Il server RUSSEL deve essere operativo e funzionante              *
rem *  - Deve esistere la condivisione \\RUSSEL\MS08-67                     *
rem *                                                                      *
rem * TESTO:                                                               *
rem *                                                                      *
rem *  Nessuno                                                             *
rem *                                                                      *
rem * NOTE:                                                                *
rem *                                                                      *
rem *  Nessuna                                                             *
rem *                                                                      *
rem ************************************************************************

rem Definiamo l'ambiente locale
setlocal enableextensions
echo.

rem Impostiamo le variabili
set LOGPATH=\\RUSSEL\MS08-67\%COMPUTERNAME%_MS08-67.log
set LOGSCRIPT=\\RUSSEL\MS08-67\%COMPUTERNAME%_InstPatchMS08-67.log

rem Impostiamo il file di log
```

```
echo File di log dello script InstPatchMS08-67.cmd > %LOGSCRIPT%
echo Data esecuzione dello script: >> %LOGSCRIPT%
date /t >> %LOGSCRIPT%
echo Inzio esecuzione dello script alle ore: >> %LOGSCRIPT%
time /t >> %LOGSCRIPT%
echo. >> %LOGSCRIPT%
echo Eseguiamo lo script sulla postazione %COMPUTERNAME% >> %LOGSCRIPT%
echo Sulla postazione %COMPUTERNAME% è presente il sistema operativo: >>
%LOGSCRIPT%

rem Controlliamo la versione del sistema operativo ed eseguiamo l'installazione
della patch
\\RUSSEL\MS08-67\osver.exe >> %LOGSCRIPT%
if ERRORLEVEL 7 (
        reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows Server
2003\SP3\KB958644\Filelist" >> %LOGSCRIPT%
        if ERRORLEVEL 1 (
                echo \\RUSSEL\MS08-67\Windows2003\Update\Update.exe /quiet /log:
%LOGPATH% >> %LOGSCRIPT%
                start /wait \\RUSSEL\MS08-67\Windows2003\Update\Update.exe
/quiet /norestart /log:%LOGPATH%
        ) else (
                echo Sulla postazione %COMPUTERNAME% la patch KB958644 è già
presente! >> %LOGSCRIPT%)
        goto END)
if ERRORLEVEL 6 (
        reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows
XP\SP4\KB958644\Filelist" >> %LOGSCRIPT%
        if ERRORLEVEL 1 (
                echo \\RUSSEL\MS08-67\WindowsXP\Update\Update.exe /quiet
/norestart /log:%LOGPATH% >> %LOGSCRIPT%
                start /wait \\RUSSEL\MS08-67\WindowsXP\Update\Update.exe
/quiet /norestart /log:%LOGPATH%
        ) else (
                echo Sulla postazione %COMPUTERNAME% la patch KB958644 è già
presente! >> %LOGSCRIPT%)
        goto END)
if ERRORLEVEL 5 (
        reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows
2000\SP5\KB958644\Filelist" >> %LOGSCRIPT%
        if ERRORLEVEL 1 (
                echo \\RUSSEL\MS08-67\Windows2000\Update\Update.exe /quiet
/norestart /log:%LOGPATH% >> %LOGSCRIPT%
                start /wait \\RUSSEL\MS08-67\Windows2000\Update\Update.exe
/quiet /norestart /log:%LOGPATH%
        ) else (
                echo Sulla postazione %COMPUTERNAME% la patch KB958644 è già
presente! >> %LOGSCRIPT%)
        goto END)

:END

rem Chiudiamo il file di log
echo. >> %LOGSCRIPT%
echo Esecuzione dello script terminata alle ore: >> %LOGSCRIPT%
time /t >> %LOGSCRIPT%
echo. >> %LOGSCRIPT%
echo Fine del file di log >> %LOGSCRIPT%

rem Fine dello script
echo.
endlocal
exit /b
```

Una volta realizzato lo script, conviene procedere come riportato di seguito:

- sulle postazioni server procedere all'installazione della patch in modalità interattiva, eseguendo manualmente lo script `\\RUSSEL\MS08-67\InstPatchMS08-67.cmd`

- sulle postazioni di lavoro del personale, provvedere a creare un apposito GPO con cui far eseguire l'installazione dell'aggiornamento **MS08-67** al riavvio delle postazioni.

L'idea di procedere manualmente all'esecuzione dello script `\\RUSSEL\MS08-67\InstPatchMS08-67.cmd`, sui server, ha senso solamente se il numero dei server è limitato (indicativamente meno di 20 unità). In caso contrario, si dovrebbe prendere seriamente in considerazione la possibilità di eseguire automaticamente l'installazione dell'aggiornamento **MS08-67**, ricorrendo eventualmente ad appositi comandi per l'esecuzione remota come ad esempio il comando psexec.exe della Sysinternals.

Per creare un GPO in grado di svolgere l'esecuzione dello script `\\RUSSEL\MS08-67\InstPatchMS08-67.cmd`, all'avvio di una postazione di lavoro, si può procedere come indicato di seguito:

Si tenga presente che qualora ci si trovi di fronte a dei *collegamenti lenti*, all'interno di uno stesso *Sito di Active Directory*, non è detto che gli script di logon o all'avvio del sistema operativo vengano eseguiti. Per comportamento predefinito, Active Directory, non esegue gli script di logon o all'avvio del sistema operativo in presenza di *collegamenti lenti*.

- collegarsi al server in cui è stata installata la **Group Policy Management Console** con un utente appartenente al gruppo degli **Enterprise Admins**;

- avviare la **Group Policy Management Console** e creare un nuovo *Group Policy Object* chiamato **Setup Patch MS08-67 (Computer)**;

- aprire l'editor dei *Group Policy Object* ed andare nella sezione **Computer Configuration\Windows Settings\Scripts (Startup/Shutdown)**;

- fare doppio clic sulla voce **Startup** che si trova sulla parte destra della finestra;

- nella finestra di dialogo chiamata **Startup Properties**, premere il pulsante **Show Files**;

- copiare lo script **InstPatchMS08-67.cmd** all'interno della cartella proposta e chiudere la finestra;

- tornati alla finestra di dialogo **Startup Properties**, premere il pulsante **Add** e poi il pulsante **Browse**;

- selezionare il file `InstPatchMS08-67.cmd` e premere il pulsante **Open**;

- nella finestra di dialogo dal titolo **Add Script**, confermare l'inserimento del file `InstPatchMS08-67.cmd` premendo il pulsante **OK**;

- tornati alla finestra di dialogo **Startup Properties**, premere il pulsante **OK**;

- chiudere l'editor dei *Group Policy Object*;

- collegare il GPO **Setup Patch MS08-67 (Computer)** alle *Unità Organizzative* che contengono le postazioni di lavoro del personale aziendale;

- chiudere la **Group Policy Management Console**.

Attendere la replica del GPO **Setup Patch MS08-67 (Computer)** e poi avvertire il personale dell'azienda di riavviare quanto prima la propria postazione di lavoro. Controllare i file di log presenti nella cartella `\\RUSSEL\MS08-67` per valutare l'andamento dell'installazione della patch **MS08-67**.

Come Rimuovere il Worm Conficker

I maggiori produttori di programmi antivirus, hanno già messo a disposizione una serie di strumenti per la rimozione mirata del worm Conficker. Anche la Microsoft, mette a disposizione degli amministratori dei sistemi Windows, un utile strumento per la rimozione del worm Conficker e di altri malware, questo strumento si chiama Malicious Software Removal Tool. Il Malicious Software Removal Tool è un semplice programma in grado di essere eseguito sulle piattaforme Windows 2000, 2003, XP e Vista. Quando vengono svolti gli aggiornamenti tramite la procedura di Windows Update, di tanto in tanto, viene scaricato ed eseguito il Malicious Software Removal Tool. Pertanto è molto probabile che le varie postazioni aziendali ne abbiano a disposizione una copia. Ad ogni modo, per poter eliminare il worm Conficker è necessario scaricare almeno la versione 2.7 del Malicious Software Removal Tool.

Al momento in cui questo articolo è stato scritto, risulta disponibile la versione **2.8** del **Malicious Software Removal Tool**.

Per semplicità supporremo che il file windows-kb890830-v2.8.exe contenente la versione 2.8 del Malicious Software Removal Tool sia stato scaricato all'interno della cartella `E:\Path\MS08-67` che si trova sul server *RUSSEL*. Per eseguire il **Malicious Software Removal Tool** è necessario avere i diritti amministrativi sulla postazione in cui lo si vuole eseguire, in alternativa, si deve utilizzare l'utente **SYSTEM**. Per sapere come distribuire ed eseguire il **Malicious Software Removal Tool** all'interno di una rete informatica basata sui sistemi Windows, si può consultare il documento Deployment Windows Malicious Software Removal Tool. Nel seguito di questo articolo, farò vedere come si può automatizzare l'esecuzione del **Malicious Software Removal Tool**, qualora invece si sia interessati solamente alla sua esecuzione manuale, si può procedere come segue:

- per prima cosa estrarre il contenuto del file windows-kb890830-v2.8.exe contenente la versione 2.8 del **Malicious Software Removal Tool**, eseguendo il comando:

  E:\Path\MS08-67\windows-kb890830-v2.8.exe /x

  nella finestra di dialogo **Choose Directory For Extracted Files**, utilizzare il pulsante **Browse** per impostare il percorso in cui si desidera estrarre il contenuto del file windows-kb890830-v2.8.exe; nel nostro esempio, supporremo che il contenuto del file sia stato estratto nella cartella `E:\Path\MS08-67`;

- una volta estratto il contenuto del file windows-kb890830-v2.8.exe sarà sufficiente eseguire il file `mrt.exe`, ad esempio utilizzando il seguente comando:

  \\RUSSEL\MS08-67\mrt.exe

e seguire le istruzioni che compaiono a video. Di solito è sufficiente eseguire una *scansione rapida* (**Quick Scan**), in alternativa, si può svolgere una *scansione completa* (**Full Scan**) o una *scansione personalizzata* (**Customized Scan**). Si tenga però presente che una *scansione completa* (**Full Scan**) può richiedere anche diverse ore di esecuzione.

La scansione manuale può andare bene solamente per i server o per quelle reti in cui il numero di elaboratori è basso. L'esecuzione del programma **Malicious Software Removal Tool**, può venire pianificata sull'intera rete aziendale se si ha a disposizione un programma come il Microsoft Windows Server Update Services. Qualora non si abbia a disposizione il programma Microsoft Windows Server Update Services si può automatizzare l'esecuzione del **Malicious Software Removal Tool** sulle varie postazioni di lavoro aziendali, ricorrendo ad un apposito script. Ad esempio, lo script riportato nella sezione Come Aggiornare le Postazioni con l'Aggiornamento MS08-67 potrebbe venire così modificato:

Nella modifica proposta dello script riportato nel paragrafo Come Aggiornare le Postazioni con l'Aggiornamento MS08-67, ho fatto uso del comando sleep.exe del Windows Server 2003 Resource Kit Tools.

```
@echo off
rem ************************************************************************
rem *                                                                      *
rem * NOME SCRIPT: InstPatchMS08-67.cmd                                    *
rem *                                                                      *
rem * Script scritto da Alessandro Tani (Home Works S.p.A)                 *
rem *                                                                      *
rem * Versione 1.0 - Modificato l'ultima volta il 17/03/2009               *
rem *                da Alessandro Tani                                    *
rem * SCOPO:                                                               *
rem *                                                                      *
rem *  Questo script ha il compito di installare la patch                  *
rem *  numero MS08-67 della Microsoft per i sistemi Windows 2000,          *
rem *  2003 ed XP                                                          *
rem *                                                                      *
rem * File di log: \\RUSSEL\MS08-67\%COMPUTERNAME%_MS08-67.log            *
rem *                                                                      *
rem * PREREQUISITI:                                                        *
rem *                                                                      *
rem *  - Il server RUSSEL deve essere operativo e funzionante              *
rem *  - Deve esistere la condivisione \\RUSSEL\MS08-67                     *
rem *                                                                      *
rem * TESTO:                                                               *
rem *                                                                      *
rem *  Nessuno                                                             *
rem *                                                                      *
rem * NOTE:                                                                *
rem *                                                                      *
rem *  Nessuna                                                             *
rem *                                                                      *
rem ************************************************************************

rem Definiamo l'ambiente locale
setlocal enableextensions
echo.

rem Impostiamo le variabili
set MSRT=0
set LOGPATH=\\RUSSEL\MS08-67\%COMPUTERNAME%_MS08-67.log
set LOGSCRIPT=\\RUSSEL\MS08-67\%COMPUTERNAME%_InstPatchMS08-67.log

rem Impostiamo il file di log
echo File di log dello script InstPatchMS08-67.cmd > %LOGSCRIPT%
echo Data esecuzione dello script: >> %LOGSCRIPT%
date /t >> %LOGSCRIPT%
```

```
echo Inzio esecuzione dello script alle ore: >> %LOGSCRIPT%
time /t >> %LOGSCRIPT%
echo. >> %LOGSCRIPT%
echo Eseguiamo lo script sulla postazione %COMPUTERNAME% >> %LOGSCRIPT%
echo Sulla postazione %COMPUTERNAME% è presente il sistema operativo: >>
%LOGSCRIPT%

rem Controlliamo la versione del sistema operativo ed eseguiamo l'installazione
della patch
\\RUSSEL\MS08-67\osver.exe >> %LOGSCRIPT%
if ERRORLEVEL 7 (
        reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows Server
2003\SP3\KB958644\Filelist" >> %LOGSCRIPT%
        if ERRORLEVEL 1 (
                echo \\RUSSEL\MS08-67\Windows2003\Update\Update.exe /quiet
/norestart /log:%LOGPATH% >> %LOGSCRIPT%
                start /wait \\RUSSEL\MS08-67\Windows2003\Update\Update.exe
/quiet /norestart /log:%LOGPATH%
        ) else (
                echo Sulla postazione %COMPUTERNAME% la patch KB958644 è già
presente! >> %LOGSCRIPT%
                set MSRT=1)
        goto END)
if ERRORLEVEL 6 (
        reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows
XP\SP4\KB958644\Filelist" >> %LOGSCRIPT%
        if ERRORLEVEL 1 (
                echo \\RUSSEL\MS08-67\WindowsXP\Update\Update.exe /quiet
/norestart /log:%LOGPATH% >> %LOGSCRIPT%
                start /wait \\RUSSEL\MS08-67\WindowsXP\Update\Update.exe
/quiet /norestart /log:%LOGPATH%
        ) else (
                echo Sulla postazione %COMPUTERNAME% la patch KB958644 è già
presente! >> %LOGSCRIPT%
                set MSRT=1)
        goto END)
if ERRORLEVEL 5 (
        reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows
2000\SP5\KB958644\Filelist" >> %LOGSCRIPT%
        if ERRORLEVEL 1 (
                echo \\RUSSEL\MS08-67\Windows2000\Update\Update.exe /quiet
/norestart /log:%LOGPATH% >> %LOGSCRIPT%
                start /wait \\RUSSEL\MS08-67\Windows2000\Update\Update.exe
/quiet /norestart /log:%LOGPATH%
        ) else (
                echo Sulla postazione %COMPUTERNAME% la patch KB958644 è già
presente! >> %LOGSCRIPT%
                set MSRT=1)
        goto END)

:END
rem Eseguiamo il Malicious Software Removal Tool
if %MSRT% equ 1 (
        echo. >> %LOGSCRIPT%
        echo Eseguiamo il Malicious Software Removal Tool >> %LOGSCRIPT%
        call \\RUSSEL\MS08-67\sleep.exe 10
        start /wait \\RUSSEL\MS08-67\windows-kb890830-v2.8.exe /q
        copy /y %windir%\debug\mrt.log \\RUSSEL\MS08-67\%COMPUTERNAME%_MSRT.log)

rem Chiudiamo il file di log
echo. >> %LOGSCRIPT%
echo Esecuzione dello script terminata alle ore: >> %LOGSCRIPT%
time /t >> %LOGSCRIPT%
echo. >> %LOGSCRIPT%
```

```
echo Fine del file di log >> %LOGSCRIPT%

rem Fine dello script
echo.
endlocal
exit /b
```

A questo punto non resta che inserire lo script **InstPatchMS08-67.cmd** all'interno di un apposito Group Policy Object come fatto nella sezione Come Aggiornare le Postazioni con l'Aggiornamento MS08-67. Per sapere se il **Malicious Software Removal Tool** è stato eseguito correttamente e se il worm Conficker (o eventuali altri malware) sono stati rimossi, bisogna consultare i file di registro *\\RUSSEL\MS08-67\%COMPUTERNAME%_MSRT.log* relativi a ciascuna postazione di lavoro (per maggiori informazioni sulla lettura del file di registro del programma **Malicious Software Removal Tool**, si può consultare la guida Deployment Windows Malicious Software Removal Tool).

Lo script **InstPatchMS08-67.cmd** deve essere eseguito su tutte le postazioni di lavoro e su tutti i server aziendali.

Oltre all'esecuzione del Malicious Software Removal Tool possono tornare molto utili, quando si deve eseguire una rimozione manuale del worm Conficker, i programmi scritti da Felix Leder e Tillmann Werner dell'Università di Bonn. In particolare, conviene eseguire, una volta portata a termine l'esecuzione del programma Malicious Software Removal Tool, il comando, dal *Prompt dei Comandi* della postazione infetta:

I ricercatori Felix Leder e Tillmann Werner hanno recentemente scoperto che il **Conficker** è in grado di cancellare e neutralizzare tutte le applicazioni che hanno nel loro nome le parole *killer* e *conficker*. Per ovviare a questo, l'applicazione **conficker_mem_killer.exe** è stata rinominata in conciller.exe. Nel proseguimento della spiegazione, faremo riferimento al programma conciller.exe e non più al comando **conficker_mem_killer.exe**.

conciller.exe

Il programma **conciller.exe** esegue un controllo nella memoria dell'elaboratore, per individuare il codice del Conficker e neutralizzarlo. Se il programma **conciller.exe** riesce a trovare il codice del Conficker, comparirà un messaggio simile al seguente:

```
Examining [256] SERVICES.EXE: MATCH at offset 02139B28 of block 02120000
Pattern for Conficker.B found
Injecting shellcode match
```

Terminata l'esecuzione del programma **conciller.exe**, riavviate la postazione sospetta (di norma questo riavvio va fatto in modo *brutale*, ovvero agendo direttamente sul pulsante di accensione della macchina), **collegatevi alla postazione con un utente che non abbia diritti amministrativi ne sulla postazione stessa, ne sul dominio** e consultare i seguenti siti web: http://www.confickerworkinggroup.org/infection_test/cfeyechart.html e http://iv.cs.uni-bonn.de/fileadmin/user_upload/werner/cfdetector/ Questi siti web vi diranno se sulla postazione sospetta, è ancora operativo o meno il worm Conficker.

Si osservi che talvolta i siti web http://www.confickerworkinggroup.org/infection_test/cfeyechart.html e http://iv.cs.uni-bonn.de/fileadmin/user_upload/werner/cfdetector/ possono fornire dei risultati erronei, nel senso che possono segnalare una postazione come *sicura*, anche quando il worm Conficker è ancora in esecuzione in memoria. In questi casi, l'unica soluzione è quella di eseguire il comando **conciller.exe**.

Talvolta l'esecuzione del Malicious Software Removal Tool non riesce ad individuare i file infettati dal worm Conficker. In questi casi può tornare utile eseguire il comando **regnfile_01.exe** realizzato da Felix Leder e Tillmann Werner. Questo comando consente d'individuare le DLL che sono state create dal worm Conficker e grazie a strumenti come Bart PE o Knoppix risulta possibile cancellare o rinominare il file DLL infetto. Per eseguire il comando **regnfile_01.exe** basta digitare al *Prompt dei Comandi*:

`regnfile_01.exe`

Qualora il sito Containing Conficker realizzato da Felix Leder e Tillmann Werner non fosse disponibile, potete scaricare i loro strumenti di rimozione da qui (codice MD5: **a2322a83db56e1f2f3eed2768657d8ef**).

Come Individuare le Postazioni Infettate dal Worm Conficker

Per essere certi di aver debellato completamente il worm Conficker, si possono utilizzare diverse tecniche informatiche. Alcune di queste tecniche hanno un carattere *empirico*, altre un po' più *scientifico*. Poiché le tecniche cosiddette *scientifiche* fanno uso di programmi specializzati, che non sempre le aziende hanno a disposizione, procederò ad elencare per prime le tecniche *empiriche* che si possono utilizzare.

Tecniche Empiriche per Individuare il Worm Conficker

Si possono utilizzare dei metodi molto semplici per essere sicuri che il worm Conficker non sia più operativo nella rete o per individuare le postazioni che risultano ancora infette. Alcuni di questi metodi possono essere (i metodi descritti, avendo una natura *empirica*, non danno la certezza che worm Conficker non sia più operativo nella rete o che una data postazione sia effettivamente infetta, ma forniscono una *ragionevole conclusione* che nella rete il worm sia debellato o che una data postazione sia ancora infetta):

- il *primo metodo* consiste nell'installare una postazione di lavoro con la vulnerabilità **MS08-67** attiva (cioè, sulla postazione non è stata applicato l'aggiornamento **MS08-67**). Ad esempio si potrebbe installare una postazione con **Windows 2000 Professional** aggiornato semplicemente con la **Service Pack 4** o una postazione con **Windows XP Professional** aggiornata alla **Service Pack 2**. La postazione andrebbe inserita nel Dominio di Active Directory aziendale e dotata del sistema antivirus aziendale (in alternativa, si potrebbe utilizzare un programma antivirus gratuito come AntiVir Free Version), avendo cura che sia aggiornato con le impronte virali del worm Conficker. In questo modo, se la postazione, lasciata per qualche tempo in rete, non s'infetta col worm Conficker, è ragionevole pensare che il worm non sia più operativo nella rete;

  Una semplice verifica per vedere se una data postazione di lavoro è effettivamente infetta col wom Conficker, consiste nel visitare, dalla postazione sospetta, i seguenti siti web: http://www.confickerworkinggroup.org/infection_test/cfeyechart.html e http://iv.cs.uni-bonn.de/fileadmin/user_upload/werner/cfdetector/

- il *secondo metodo*, richiede l'utilizzo di una postazione di lavoro, non inserita all'interno del Dominio di Active Directory aziendale, sulla quale è stato installato il programma WireShark. Il programma WireShark consente di analizzare il traffico di rete diretto verso la postazione in questione. Poiché la postazione non fa parte del Dominio di Active Directory aziendale, il traffico SMB (*Server Message Block*), dovrebbe essere minimo o addirittura nullo. Analizzando questo traffico di rete, si potrebbe risalire, in linea di principio, all'indirizzo IP e quindi all'elaboratore, che nella rete aziendale risulta ancora vittima del worm;

- il *terzo metodo* consiste nell'analisi dei file di registro (*log*) del firewall perimetrale. Infatti, a causa del metodo d'aggiornamento del worm Conficker.B e delle sue varianti successive, basato sulle tecniche di *Peer-To-Peer*, viene generato del traffico UDP anomalo. Osservando questo traffico UDP di rete dal firewall perimetrale dell'azienda, è possibile risalire, in linea di principio, alle postazioni della rete che possono ancora essere infette col worm Conficker;

- il *quarto metodo* consiste nell'utilizzare una postazione di lavoro, non necessariamente inserita nel dominio Active Directory, dotata di un sistema antivirus che preveda un componente di **Intrusion**

Prevention System (**IPS**), come ad esempio il Symantec Endpoint Protection. Il modulo **IPS** dovrebbe segnalare e registrare gli eventuali attacchi di una postazione di lavoro colpita dal worm Conficker;

- il *quinto metodo* è quello di utilizzare programmi per la raccolta degli eventi di Windows, come ad esempio il programma EventLog Analyzer. Sfruttando questo tipo di programmi, si possono vedere facilmente gli eventi di **Logon Failure** registrati dai **Domain Controller** di Active Directory. In base a questi eventi, si può risalire al **nome dell'utente** che ha registrato l'evento di Logon Failure (una postazione affetta dal worm Conficker è in grado di generare diverse decine di eventi di Logon Failure al secondo). Noto il nome dell'utente si può risalire al **nome della macchina** su cui sta operando.

Una volta individuate quelle che possono essere le postazioni infette col worm Conficker, si può eseguire una scansione manuale del **Malicious Software Removal Tool**. Ripetendo le prove sopra indicate, si può giungere alla conclusione, qualora fossero tutte negative, che all'interno della rete aziendale il worm Conficker non sia più attivo.

Una semplice verifica per vedere se una data postazione di lavoro è effettivamente infetta col wom Conficker, consiste nel visitare, dalla postazione sospetta, i seguenti siti web: http://www.confickerworkinggroup.org/infection_test/cfeyechart.html e http://iv.cs.uni-bonn.de/fileadmin/user_upload/werner/cfdetector/

Tecniche Avanzate per Individuare il Worm Conficker

Accanto alle tecniche *empiriche* descritte nel paragrafo Tecniche Empiriche per Individuare il Worm Conficker, si possono utilizzare dei metodi di analisi più sofisticati che consentono d'individuare le postazioni ancora infette col worm Conficker con maggiore precisione. Fra le diverse tecniche *avanzate* di analisi della rete, mi limiterò a segnalare le seguenti due:

- il programmatore Gordon Fyodor Lyon ha sviluppato uno degli strumenti più importanti per l'analisi della rete, il programma NMAP. Nella sua ultima versione disponibile al momento in cui questo articolo è stato scritto, la 4.85BETA7, Gordon Fyodor Lyon ha introdotto, grazie al lavoro prezioso di altri collaboratori, un'analisi appositamente dedicata all'individuazione del worm Conficker. Per sapere se in una data rete il worm Conficker è ancora operativo, si può pianificare l'esecuzione del seguente comando (per la scansione di reti molto grandi, consigliamo la lettura dell'articolo How to use Nmap to scan very large networks for Conficker):

```
nmap -PN -T4 -p139,445 -n -v --script smb-check-vulns,smb-os-discovery
<Rete_Da_Analizzare>
```

o

```
nmap -PN -T4 -p139,445 -n -v --script smb-check-vulns,smb-os-discovery
--script-args unsafe=1 <Rete_Da_Analizzare>
```

I comandi di sopra, eseguono anche l'analisi per vedere se la patch MS08-67 risulta installata sulle postazioni analizzate.

Da test effettuati, si è notato che talvolta il servizio **services.exe** di una postazione priva della patch **MS08-67**, in cui viene svolta l'analisi indicata, va in tilt, richiedendo il riavvio della postazione.

Qualora non si volesse eseguire questo controllo, si deve sfruttare il seguente comando:

```
nmap -PN -T4 -p139,445 -n -v --script smb-check-vulns,smb-os-discovery
--script-args safe=1 <Rete_Da_Analizzare>
```

Ad esempio:

```
nmap -PN -T4 -p139,445 -n -v --script smb-check-vulns,smb-os-discovery
--script-args unsafe=1 192.168.1.0/24
```

oppure:

```
nmap -PN -T4 -p139,445 -n -v --script smb-check-vulns,smb-os-discovery
--script-args safe=1 192.168.1.0/24
```

Al termine dell'analisi, per ciascuna postazione analizzata, viene riportato, nel campo **Conficker** la segnalazione **Conficker: Likely INFECTED**, se la postazione è ancora infetta, la segnalazione **Conficker: Likely CLEAN**, se la postazione non è infetta col worm Conficker. Se il numero delle postazioni da analizzare è elevato, conviene reindirizzare il risultato dell'analisi ad un file di testo:

```
nmap -PN -T4 -p139,445 -n -v --script smb-check-vulns,smb-os-discovery
--script-args unsafe=1 192.168.1.0/24 > %SystemDrive
%\Temp\Analisi_Conficker.txt
```

Un possibile esempio di postazione su cui risulta attivo il worm Conficker potrebbe essere:

```
Host 192.168.1.208 is up (0.00s latency).
Interesting ports on 192.168.1.212:
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:04:23:8D:98:5E (Intel)

Host script results:
|  smb-os-discovery: Windows 2000
|  LAN Manager: Windows 2000 LAN Manager
|  Name: HOMEWORKS\PLATONE
|_ System time: 2009-04-07 11:19:40 UTC+2
|  smb-check-vulns:
|  MS08-067: PATCHED (possibly by Conficker)
|  Conficker: Likely INFECTED
|_ regsvc DoS: Check disabled (add --script-args=unsafe=1 to run)
```

La frase **MS08-067: PATCHED (possibly by Conficker)** si riferisce al fatto che il Conficker installa una *mini-patch* al sistema operativo per evitare che altri malware sfruttino la vulnerabilità **MS08-67** per infettare la postazione di lavoro.

- il metodo *principe* per individuare le postazioni infette col worm Conficker, è quello di utilizzare programmi di Network Intrusion Detection System, come ad esempio SNORT. Grazie a questi programmi, risulta possibile da un lato, individuare con certezza le postazioni aziendali che sono ancora infette col worm Conficker e dal altro, prevenire ulteriori infezioni del worm Conficker provenienti da Internet.

Una volta individuate quelle che possono essere le postazioni ancora infette col worm Conficker, si può eseguire una scansione manuale del **Malicious Software Removal Tool**. Analizzando la rete con gli strumenti descritti in

precedenza, si può giungere alla conclusione, qualora fossero tutti negativi i risultati, che all'interno della rete aziendale il worm Conficker non sia più attivo.

Come Evitare di Essere Vittime dei Virus

Sebbene nel mondo vengano prodotti di continuo virus e *codici maligni*, non ci si deve rassegnare all'inevitabile, virus e *codici maligni* si possono evitare! Basta adottare una *buona politica di sicurezza*. Come il worm Conficker dimostra, la Microsoft ha rilasciato sin dal mese di Ottobre 2008 l'aggiornamento che preveniva l'infezione del Conficker, che ricordo è uscito solamente nel Novembre 2008 La considerazioni che valgono oggi per Conficker, valevano anche per le altre infezioni pericolose come il Conficker. Per evitare i virus, o comunque ridurre gli effetti che possono causare, basta seguire alcune semplici regole:

- evitare di fornire privilegi amministrativi ai vari dipendenti aziendali sulle loro postazioni di lavoro (per maggiori informazioni si può consultare l'articolo della Microsoft Applying the Principle of the Least Privilege to User Accounts);
- dotare le postazioni Windows aziendali di un buon programma antivirus ed antispyware, come ad esempio il Symantec Endpoint Protection;
- assicurarsi che il programma antivirus ed antispywere delle varie postazioni Windows si aggiorni regolarmente;
- dotare la propria azienda di un buon sistema di firewall perimetrale opportunamente configurato;
- dotare la propria azienda di un buon programma di Network Intrusion Detection System, come ad esempio SNORT;
- installare il modulo IPS (**Intrusion Prevention System**) del antivirus su tutte le postazioni di lavoro (un ottimo modulo IPS è quello del Symantec Endpoint Protection);
- chiudere in modo selettivo la porta TCP 25 sul firewall aziendale (in altri termini, dalle postazioni di lavoro dei dipendenti non dovrebbe essere possibile inviare email sfruttando server SMTP *esterni* alla rete aziendale);
- dotare l'azienda di una soluzione per il controllo della navigazione Internet da parte dei dipendenti aziendali;
- installare l'ultima versione disponibile di Internet Explorer;
- aggiornare regolarmente le postazioni di lavoro con le ultime HotFix di sicurezza, utilizzando ad esempio il programma Microsoft Windows Server Update Services.

Ringraziamenti

Per la realizzazione di questo articolo vorrei ringraziare il mio amico e collega Kenneth Costa che per primo, in azienda, si è cimentato col worm Conficker, realizzando quella che può essere tranquillamente considerata la prima bozza di questo articolo.

Appendice

Come Importare un Group Policy Object

Per importare un **Group Policy Object** precedentemente salvato, si può procedere come indicato di seguito (nel corso della spiegazione, faremo riferimento alla Group Policy Management Console e daremo per scontato che la **Group Policy Management Console** sia installata almeno su una postazione di lavoro della rete):

- collegarsi al server su cui è installata la **Group Policy Management Console** con un utente appartenente al gruppo dei **Domain Admins**;
- lanciare la **Group Policy Management Console**;
- aprire la cartella **Group Policy Object**;
- creare un nuovo **Group Policy Object**;
- cliccare col pulsante destro del mouse sul **Group Policy Object** precedente creato. Dal menù contestuale selezionare la voce **Import Settings ...**;
- all'apertura della finestra di benvenuto del **Import Settings Wizard**, premere **Next** per andare avanti;
- all'interno della finestra **Backup GPO** premere il pulsante **Next** per andare avanti;
- nella finestra **Backup Location** utilizzare il pulsante **Browse** per individuare la cartella in cui è stata salvata il **Group Policy Object** da importare. Premere **Next** per proseguire;
- selezionare il **Group Policy Object** da importare. Non selezionare la voce **Show only the latest version of each GPO**. Premere **Next** per andare avanti;
- all'interno della finestra **Scanning Backup** viene riportato un report che informa se è necessario utilizzare una Migration Table per importare il **Group Policy Object** o meno. Premere Next per andare avanti;
- se è necessario specificare una **Migration Table**. Selezionare la voce **Using this migration table to map them in destination GPO**. Utilizzare il pulsante **Browse** per caricare il file con estensione **.migtable** creato in precedenza. Premere **Next** per andare avanti;
- giunti nella finestra **Completing the Import Settings Wizard** controllare che le scelte effettuate siano corrette. Premere **Finish** per avviare la procedura d'importazione;
- controllare che la procedura d'importazione termini con successo.

Password utilizzate dal Conficker per attaccare l'account Administrator

Per determinare la password dell'utente **Administrator** locale di un computer, il Conficker utilizza un'attacco di *forza bruta*, sfruttando le seguenti password (Net-Worm.Win32.Kido.bt):

Password			
99999999	9999999	999999	99999
9999	999	99	9
88888888	8888888	888888	88888
8888	888	88	8
77777777	7777777	777777	77777
7777	777	77	7
66666666	6666666	666666	66666
6666	666	66	6
55555555	5555555	555555	55555
5555	555	55	5
44444444	4444444	444444	44444
4444	444	44	4
33333333	3333333	333333	33333
3333	333	33	3
22222222	2222222	222222	22222
2222	222	22	2
11111111	1111111	111111	11111
1111	111	11	1

Password			
00000000	0000000	000000	00000
0000	000	00	0
0987654321	987654321	87654321	7654321
654321	54321	4321	321
21	12	123321	12321
123123	1234567890	123456789	12345678
1234567	123456	12345	1234
123	super	secret	server
computer	owner	backup	database
lotus	oracle	business	manager
temporary	ihavenopass	nothing	nopassword
nopass	Internet	internet	example
sample	secure	public	system
shadow	office	supervisor	superuser
share	adminadmin	mypassword	mypass
pass	Login	login	Password
password	passwd	zxcvbn	zxcvb
zxccxz	zxcxz	qazwsxedc	qazwsx
q1w2e3	qweasdzxc	asdfgh	asdzxc
asddsa	asdsa	qweasd	qwerty

Password			
qweewq	qwewq	nimda	administrator
Admin	admin	a1b2c3	1q2w3e
1234qwer	1234abcd	123asd	123qwe
123abc	fuck	zzzzz	zzzz
zzz	xxxxx	xxxx	xxx
qqqqq	qqqq	qqq	aaaaa
aaaa	aaa	sql	file
web	foo	job	home
work	intranet	controller	killer
games	private	market	coffee
cookie	forever	freedom	student
account	academia	files	windows
monitor	unknown	anything	letitbe
letmein	domain	access	money
campus	explorer	exchange	customer
cluster	nobody	codeword	codename
changeme	desktop	security	love123
boss123	work123	home123	mypc123
temp123	test123	qwe123	abc123
pw123	root123	pass123	pass12

Password			
pass1	admin123	admin12	admin1
password123	password12	password1	default
foobar	foofoo	temptemp	temp
testtest	test	rootroot	root
%Username%	%Username%%Username%	<blank>	